



The ONE!

One Schedule to Rule them All!

Welcome to the "One Schedule to Rule them All!". Thank you for your interest by using this. This is an attempt to make things easier for you, the DEF CON attendee, to figure out the when/what/where during the chaos of DEF CON 31.

It started out simple. I had a Kindle and wanted an ebook of the schedule so I didn't have to wear out the paper pamphlet by pulling it out after every talk to figure out where to go next. Back then there was only the main DEF CON tracks, not really any Villages, and production of the ebooks were easy. Over time the Village system developed with a resulting multiplication in complexity, both for attendees and for my production. The offerings no longer include epub and mobi formats and instead now include html, csv, PDF, ical, public Google calendar, and mysql dump format files. Hopefully you'll find something of use.

The intent is still to be a resource to answer the question at the end of an hour of "What's next?"

As a general rule I do not include:

- Off-site events
- Blatent vender pitch events
- Nonspecific timed events. Unfortunately this means the contests aren't on the regular schedule.
- DEF CON events are emphasized, so BSides Las Vegas and BlackHat tend to not show up

Be sure to check out the Links section at the bottom of this. Most all of the events listed here were derived from these links and a Infoboot data feed. There is much more going on at DEF CON than what is listed here.

Check out the Guides/Tips/FAQs links if you're new to Las Vegas.

Notable suggestions are:

- Bring comfortable shoes, you'll be doing a lot more walking than you expect
- Bring a water bottle to keep hydrated
- Beware of going out doors, there's nothing like LV sun and heat
- Everything in Las Vegas is a longer walk than you think
- Relax, don't try to see everything, you'll never be able to!
- Have FUN!

And finally, this is only as good as the ideas and information used to generate it. I welcome your constructive suggestions and comments. Please send them to qumqats@outel.org

Have a good time at DEF CON 31!

Index of DEF CON 31 Activities

[Maps List](#)

[Maps Browser](#)

[Detailed Village Info](#)

[Villages Table](#)

Hour by Hour list of happenings, start at the top, or go to a specific day.

[Schedule](#)

[- Thursday - Friday - Saturday - Sunday](#)

Sorted list of all the Speakers Names linked to their talk's description.

[Speaker List](#)

Sorted list of all the Talk's titles linked to the talk description.

[Talk Title List](#)

Talk lists for each Village, start at the alphabetic top, or go to a specific Village.

[Village Talk List](#)

[AIV - APV - ASV - BHV - BICV - BTV - CHV - CLV - CON - CPV - DC - DCGVR - DDV - DL - ESV - HHV - HRV - ICSV - IOTV - LPV - MISC - MIV - MUS - PHV - PLV - PSV - PWV - PYV - QTV - RCV - RFV - RTV - SEV - SOC - TCV - TEV - VMV - WS - XRV](#)

Descriptions and Info for all the talks.

[Talk Descriptions](#)

Contests Table

[Contests](#)

Parties, Gatherings, and Events Table

[Parties Gatherings Events](#)

Demolabs Table

[Demolabs](#)

Workshops Table

[Workshops](#)

Paid Trainings Table

[Paid Trainings](#)

DEF CON 31 Vendors

[Vendors](#)

The latest news from defcon.org

[DEF CON News](#)

The answer to your questions about DEF CON overall and for this year.

[DEF CON FAQ](#)

[DEF CON 31 FAQ](#)

[DEF CON .org Links](#)

[Combined Schedule Sources](#)

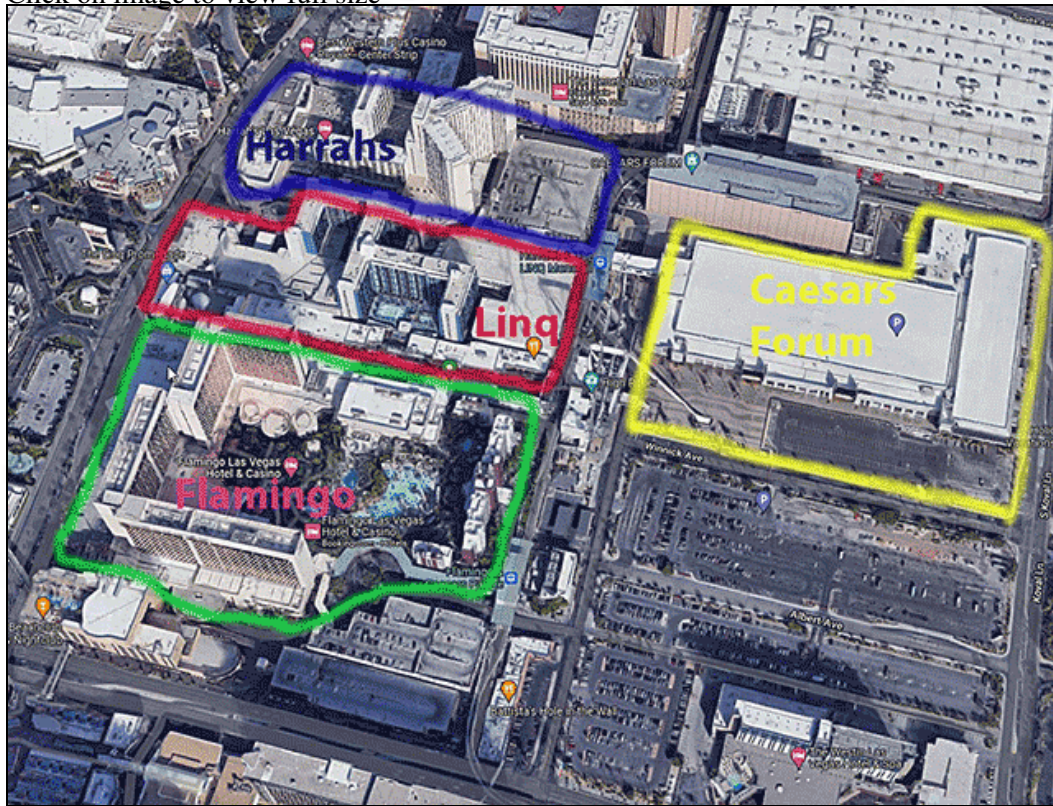
[Interesting Links](#)

[Guides/Tips/FAQs](#)

Maps List

Overview of the Hotels in the area of DEF CON 31

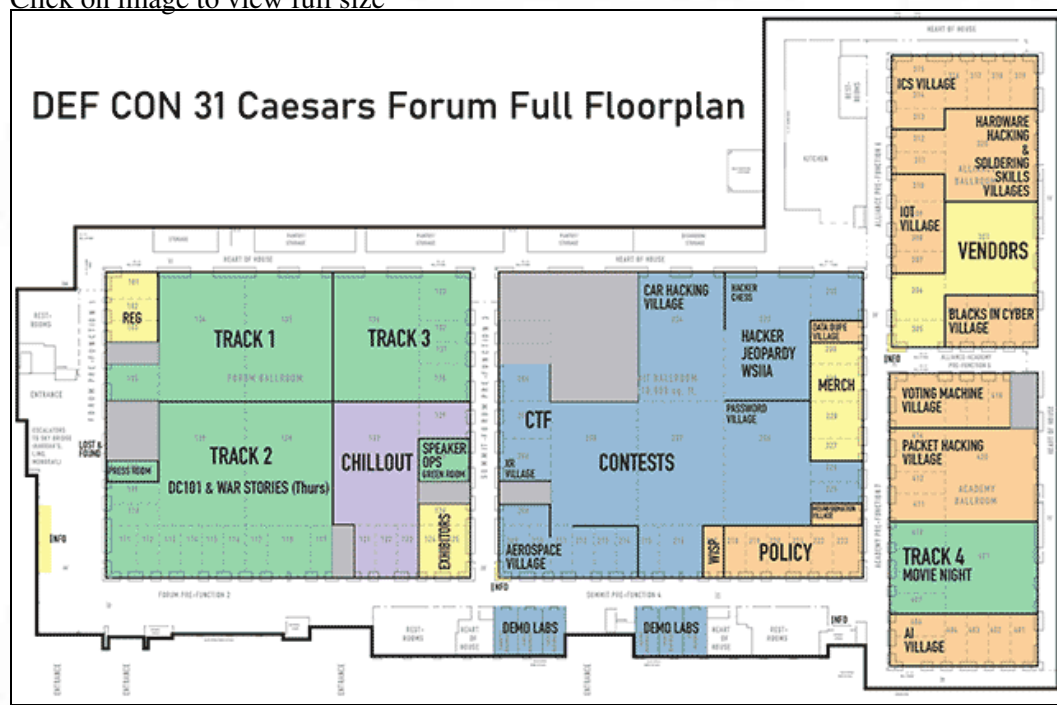
[Click on image to view full size](#)



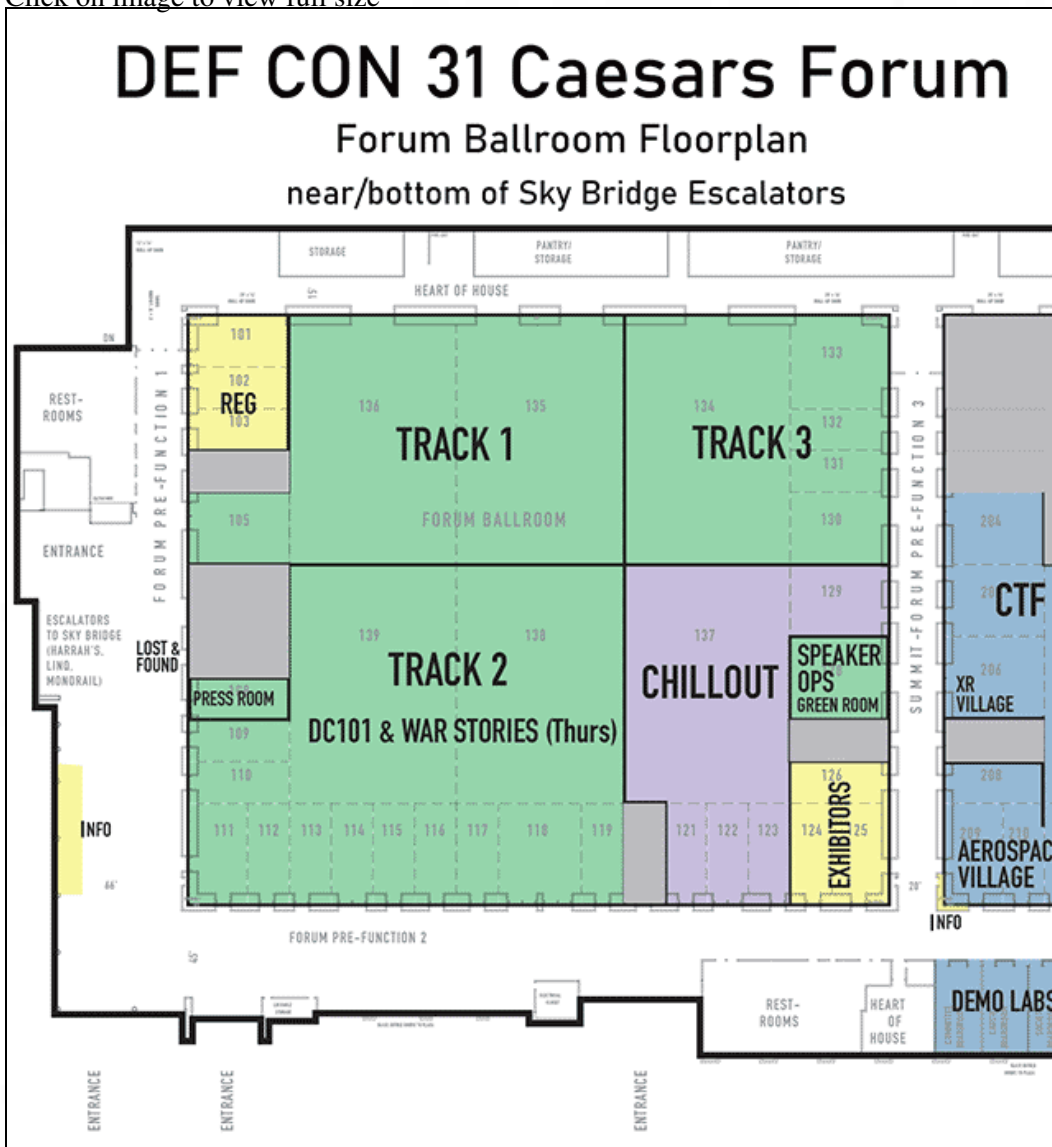
Map Overlay of DEF CON 31 hotels
Red line indicates walking paths between them
[Click on image to view full size](#)



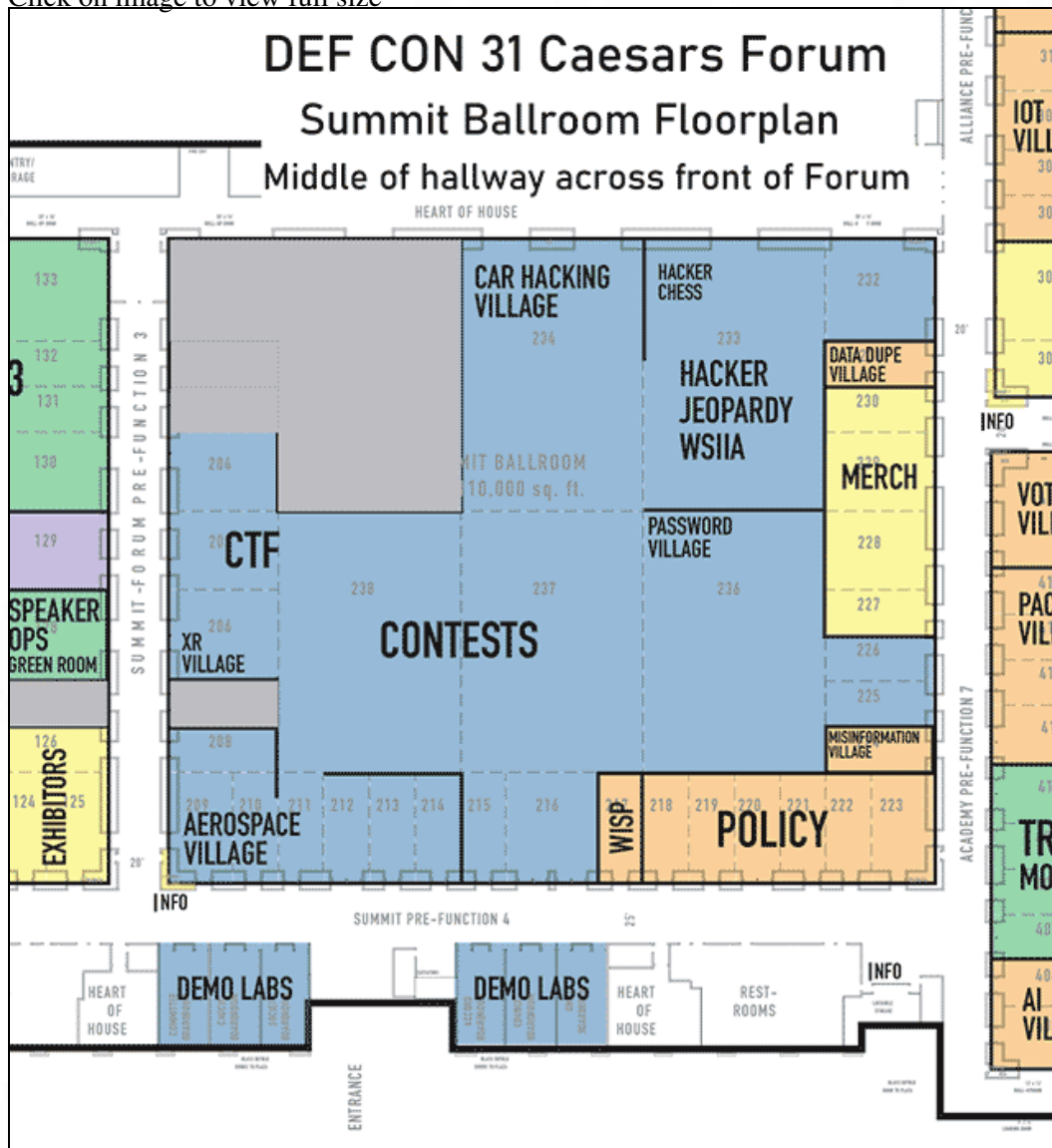
Full floorplan of the Caesars Forum Convention Space
Click on image to view full size



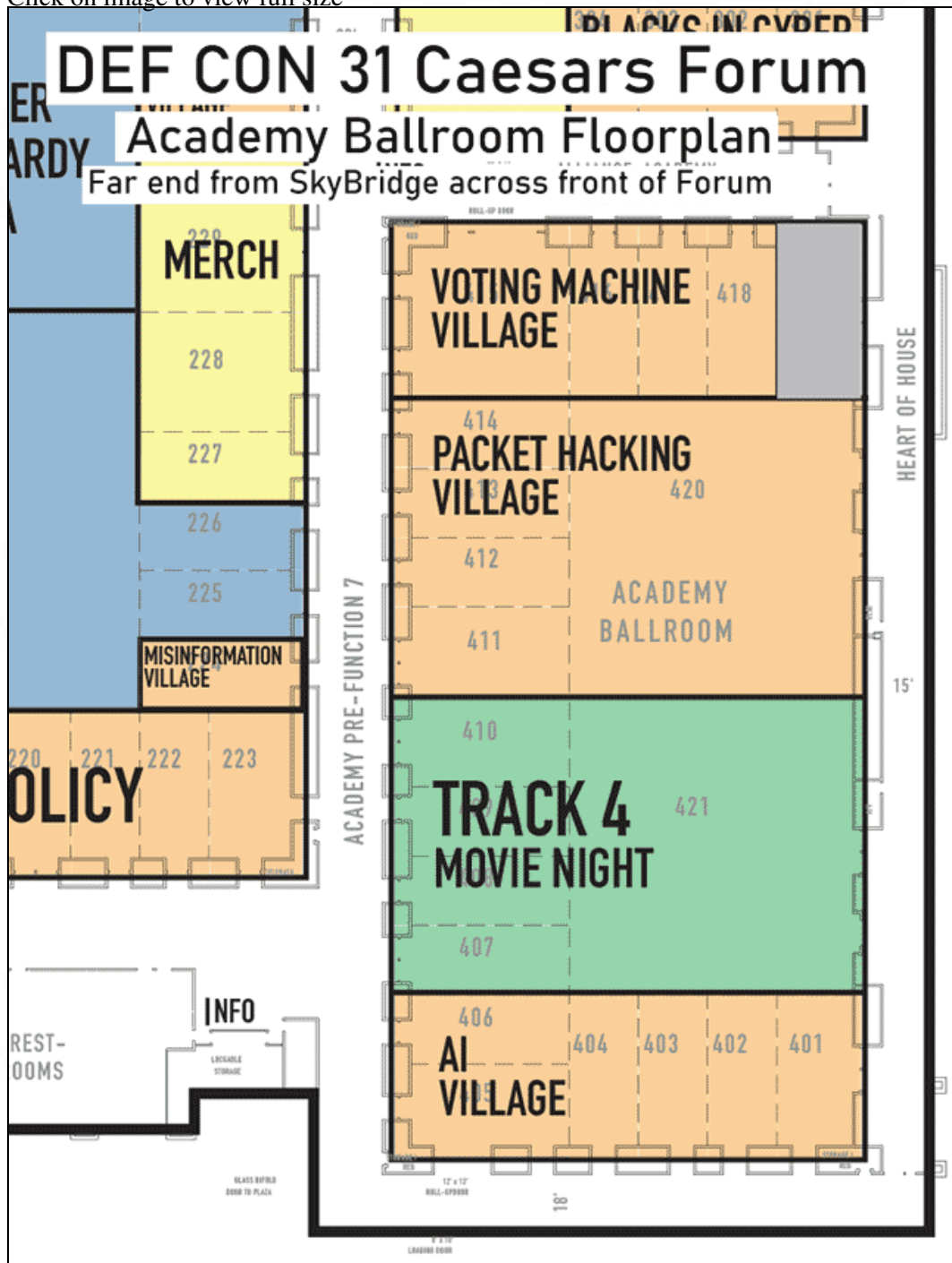
Closeup of the floorplan for the Caesars Forum, Forum Ballroom
Click on image to view full size



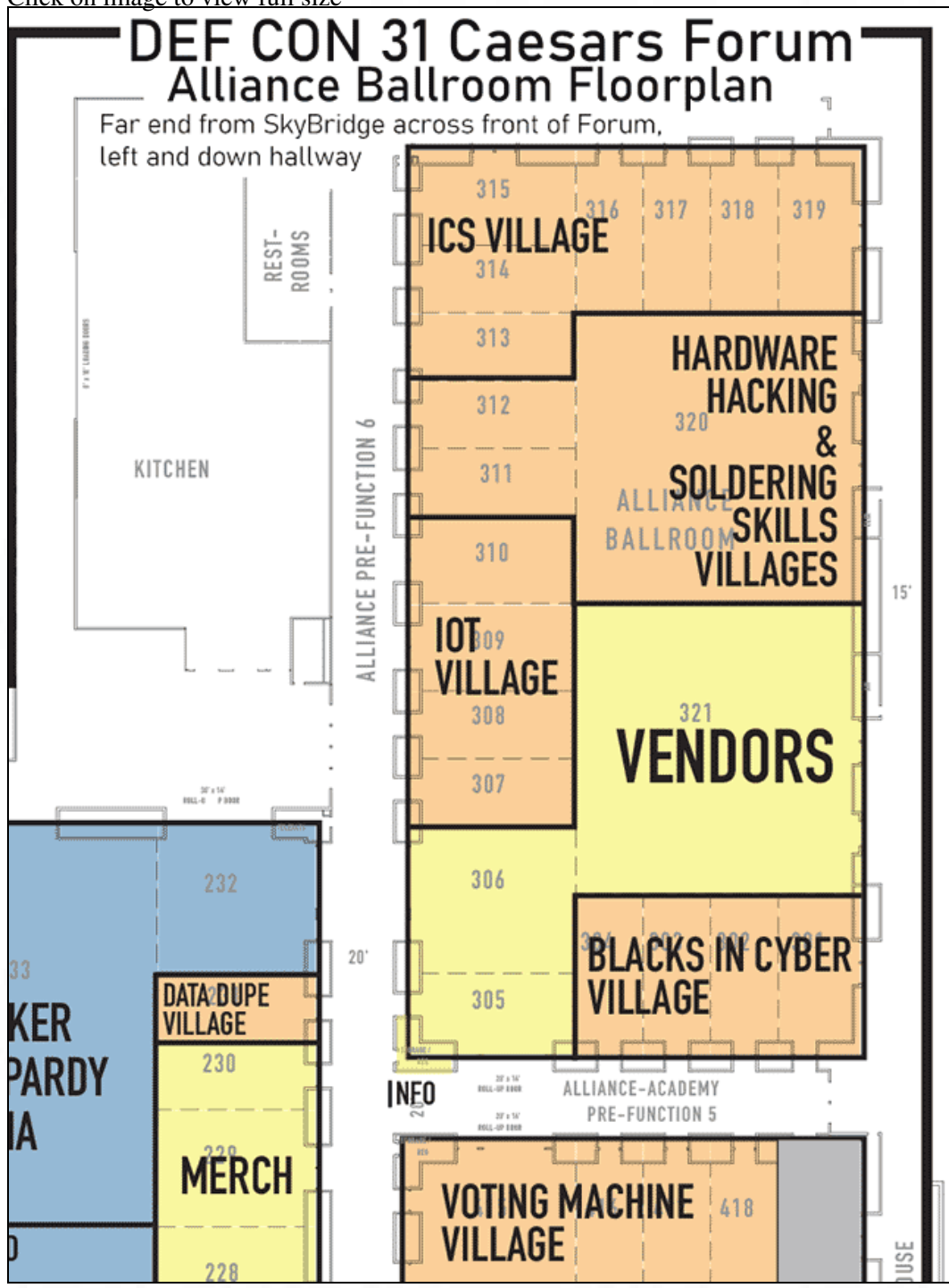
Closeup of the floorplan for the Caesars Forum, Summit Ballroom
Click on image to view full size



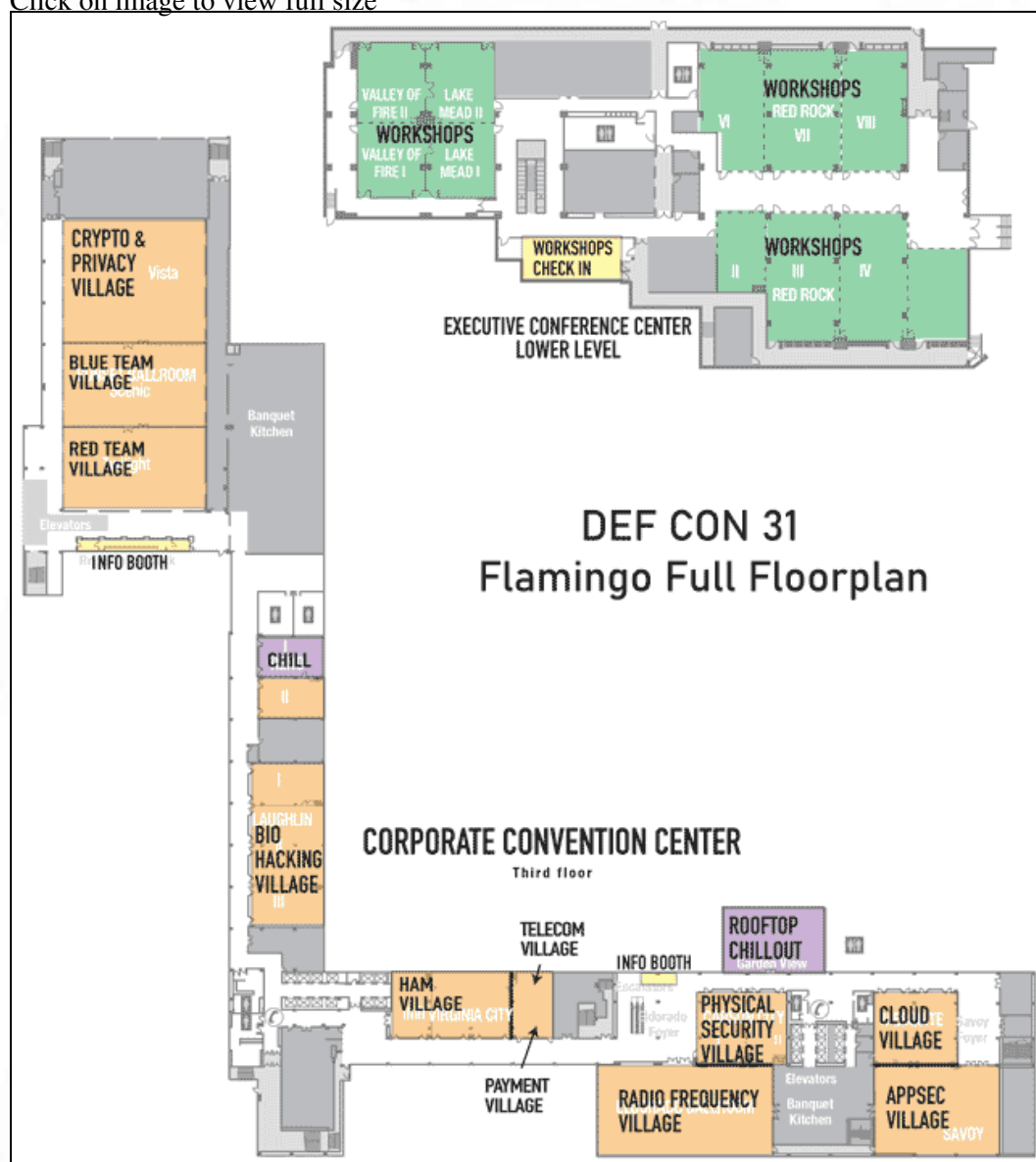
Closeup of the floorplan for the Caesars Forum, Academy Ballroom
Click on image to view full size



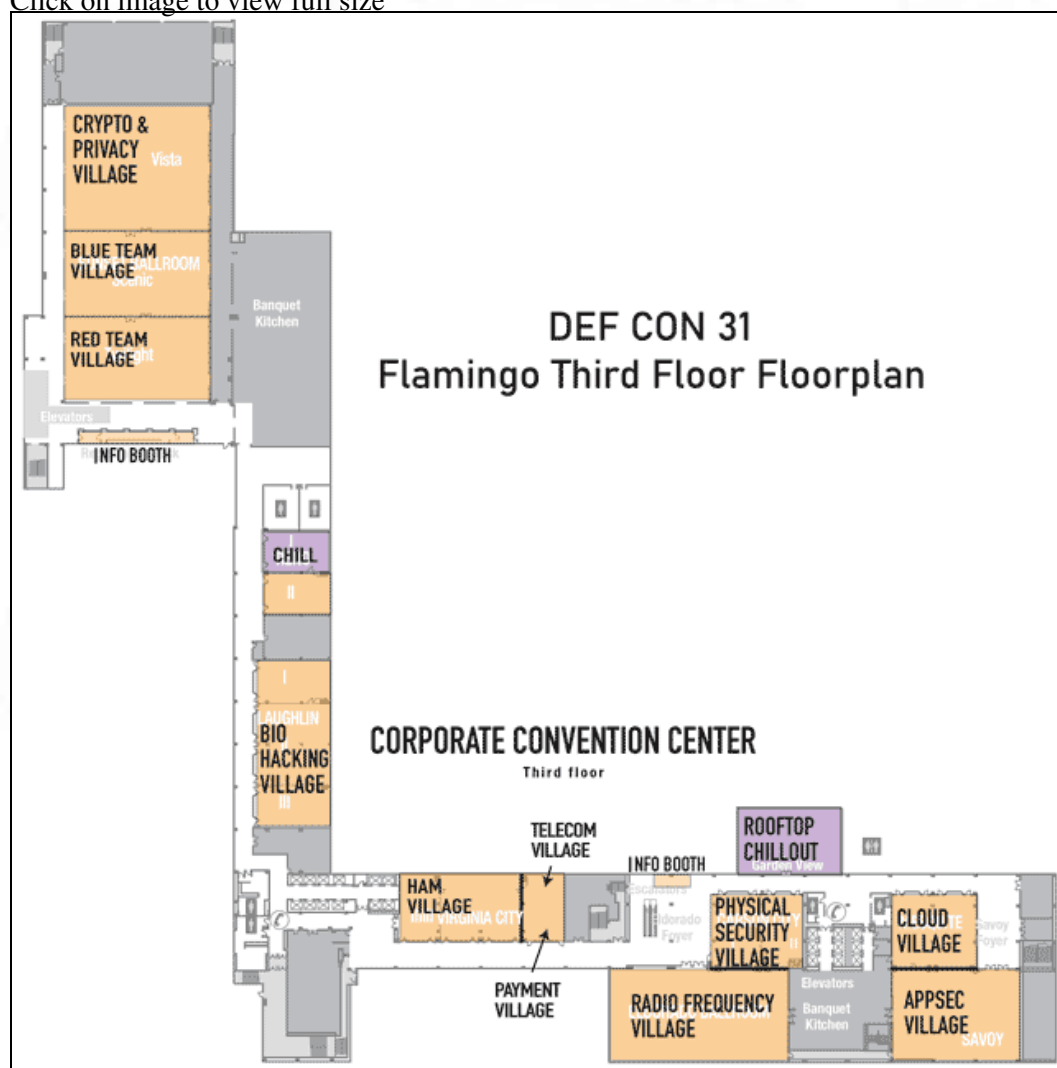
Closeup of the floorplan for the Caesars Forum, Alliance Ballroom
Click on image to view full size



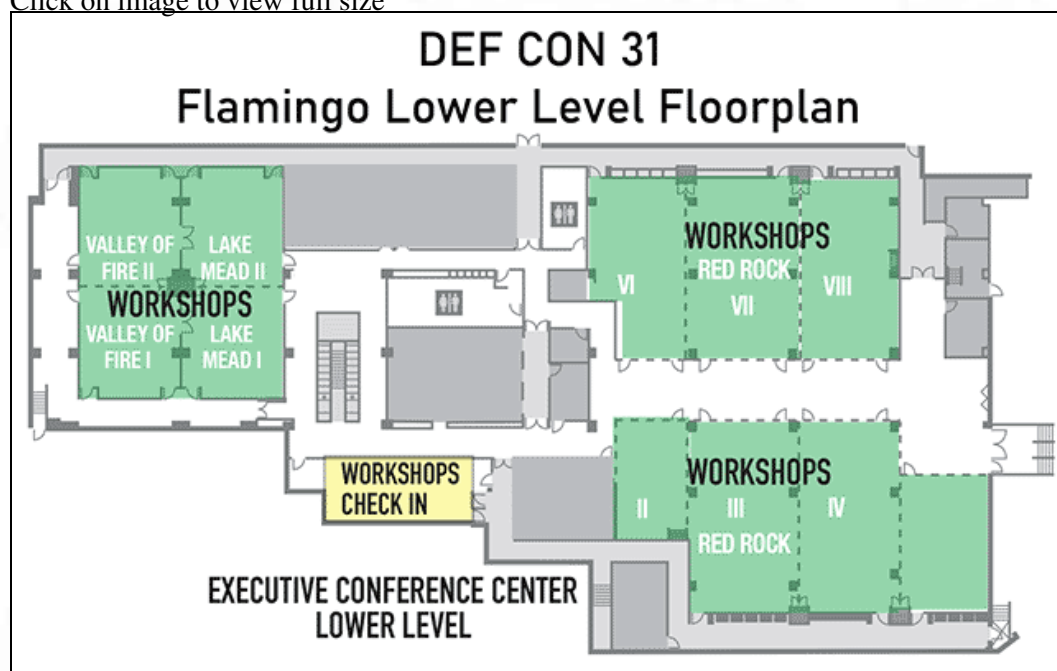
Full floorplan for Flamingo
Click on image to view full size



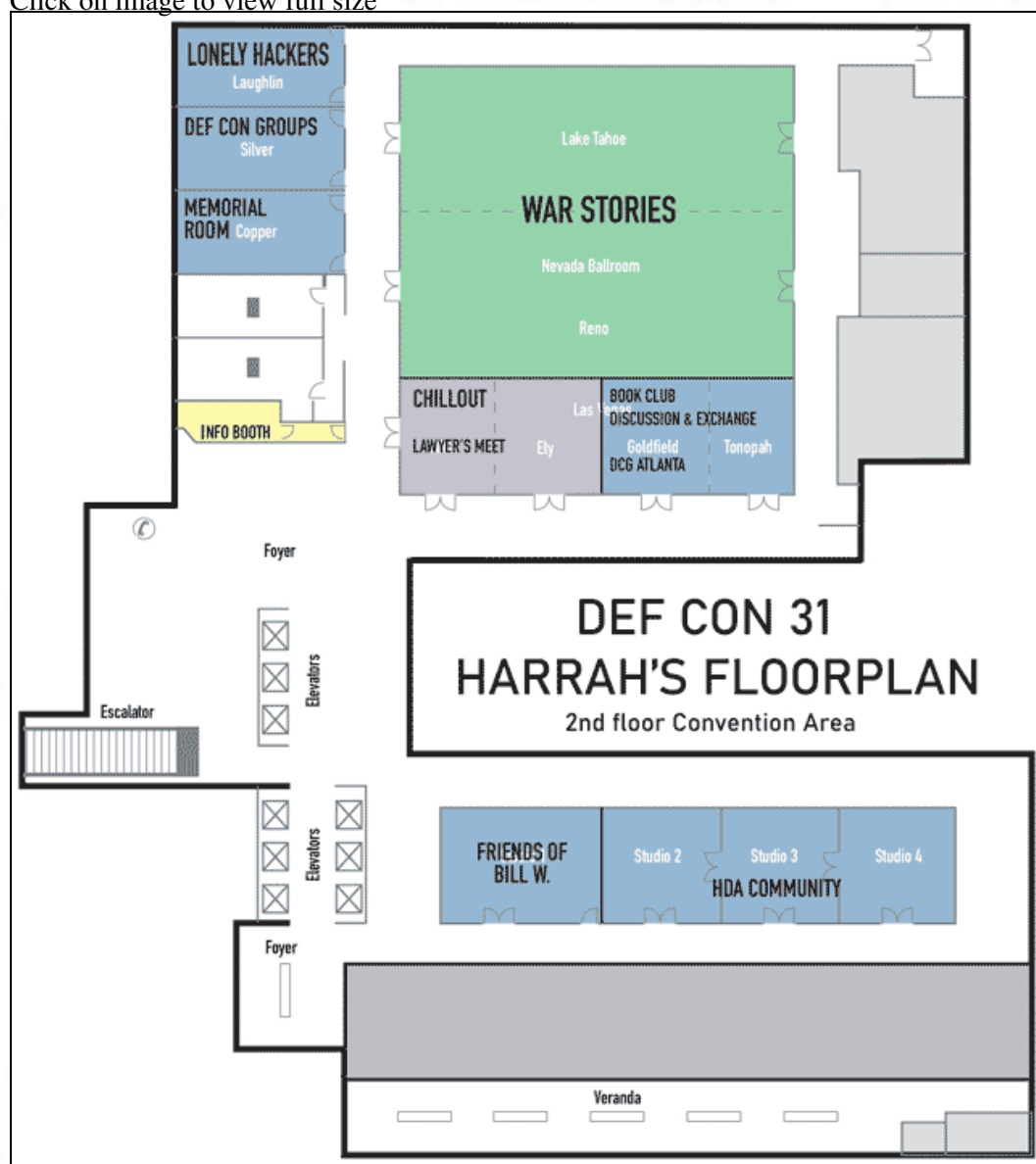
Closeup of the floorplan for the Flamingo, Corporate Convention Center, Third floor
Click on image to view full size



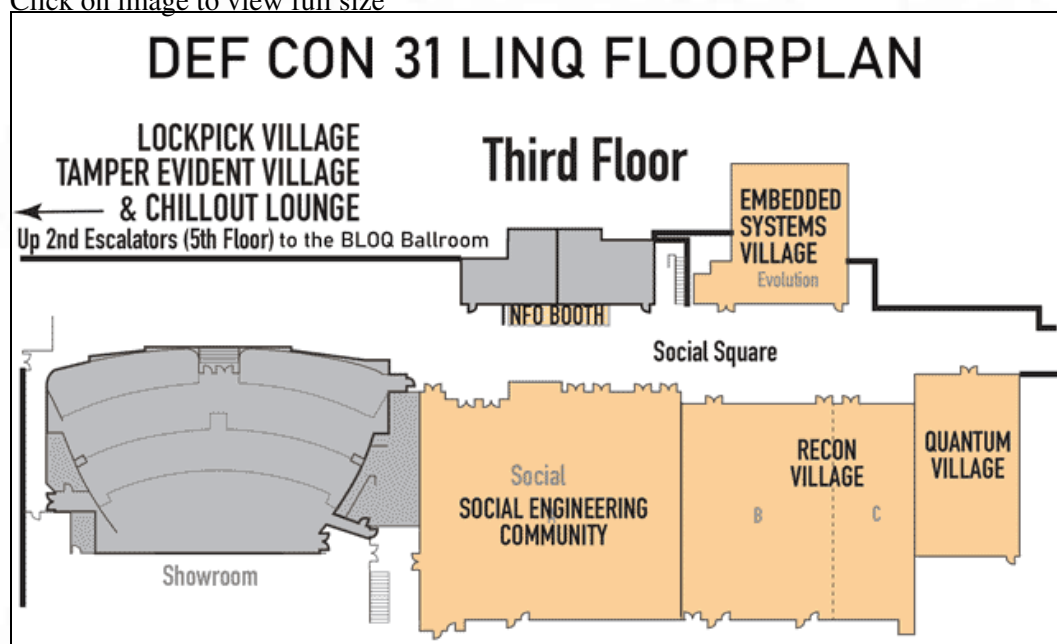
Closeup of the floorplan for the Flamingo, Executive Convergence Center, Lower Level.
Click on image to view full size



Full floorplan for Harrahs
Click on image to view full size



Full floorplan for Linq
Click on image to view full size



Map Browser

- [Overview around DEF CON 31](#)
 - [Map Overlay of DEF CON 31](#)
 - - ◆ [Harrahs Full map](#)
 - ◆ [Linq Full map](#)
 - ◆ [Flamingo Full map](#)
 - ◇ [Flamingo Lower Level](#)
 - ◇ [Flamingo Third Floor](#)
 - ◆ [Caesars Forum Full map](#)
 - ◇ [Caesars Forum Forum BR](#)
 - ◇ [Caesars Forum Summit BR](#)
 - ◇ [Caesars Forum Academy BR](#)
 - ◇ [Caesars Forum Alliance BR](#)
 - ◇ [3D tour of Caesars Forum, like Google StreetView](#)
-



Detailed Village Info

AIV - Artificial Intelligence Village

AIV Village: [Talk List](#)

Home Page: <https://aivillage.org/>

Sched Page: <https://aivillage.org/defcon31/>

DC Forums Page: <https://forum.defcon.org/node/244776>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733090568339536>

Location: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

Social Media Links:

TW [@aivillage_dc](#)

TI [@aivillage](#)

YT [link](#)

DC <https://discord.com/invite/GX5fhfT>



A.I. Village

When: Friday & Saturday: 10:00-18:00, Sunday: 10:00-12:00

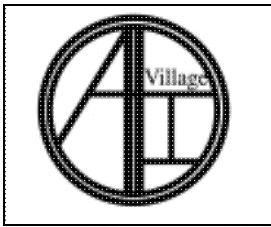
Where: Forums 401-406

Twitter: [@aivillage_dc](#)

Website: <https://aivillage.org/>

AI has exploded in the last couple years and is a new and unique attack surface for hackers. Come learn how ChatGPT, StableDiffusion, malware detectors, ML firewalls, and other AI based products work and how to break them. We will have talks sharing the latest research on these almost futuristic topics, as well as talks on developments in AI in traditional security. We will also host workshops for security experts new to AI to get you up to speed. New to this year are demo stations showing off how various AI technologies work including the guts of large language models, text to image models, and malware detectors. We will also host Prompt Detective where you learn prompt engineering to get various LLMs to perform tasks for you, including ones they are trained not to do.

We are also running the Generative Red Team, the largest ever in person assessment for any group of AI models. Attached Files



Starts August 11, 2023 10:00 Ends August 11, 2023 18:00 Location Forums 401-406

[Return to Index](#)

APV - AppSec Village

APV Village: [Talk List](#)

Home Page: <https://www.appsecvillage.com/>

Sched Page: <https://www.appsecvillage.com/events/dc-2023>

DC Forums Page: <https://forum.defcon.org/node/244879>

DC Discord Chan: <https://discord.com/channels/708208267699945503/790973922949726228>

Location: Flamingo - Savoy - AppSec Village - [Map](#)

Social Media Links:

TW [@AppSec_Village](#)

LI [@appsecvillage](#)

YT <https://www.youtube.com/c/AppSecVillage>

DC <https://discord.gg/5XY8qYXd7R>



Appsec Village

When: Friday to Sat 10:00 - 20:00, Sunday 10:00 to 14:00

Where: Savoy in Flamingo

Twitter: [@AppSec_Village](#)

Website: <https://www.appsecvillage.com/>

The first four AppSec Villages at DEF CON were a resounding success. We learned that whether in person or online, our AppSec community is fantastic. We are pumped to be back bigger and better.

Come immerse yourself in everything the world of application security has to offer. Whether you are a red, blue, or purple teamer, come learn from the best of the best to exploit software vulnerabilities and secure software. Software is everywhere, and Application Security vulnerabilities are lurking around every corner, making the software attack surface attractive for abuse. If you are just an AppSec n00b or launch deserialization attacks for fun and profit, you will find something to tickle your interest at the AppSec Village.

Software runs the world. Everything from IoT, medical devices, the power grid, smart cars, and voting apps - all have software behind them. Such a variety of topics will be reflected in our cadre of guest speakers representing all backgrounds and walks of life.

AppSec Village welcomes all travelers to choose from talks and workshops by expert community members, an all-AppSec-focused CTF, contests that challenge your mind and your skillz, and more. Bring your thirst for knowledge and passion for breaking things, and your visit to AppSec Village will be thrilling! Starts August 13, 2023 10:00 Ends August 13, 2023 14:00 Location Savoy in Flamingo

[Return to Index](#)

ASV - Aerospace Village

ASV Village: [Talk List](#)

Home Page: <https://aerospacevillage.org/>

Sched Page: <https://www.aerospacevillage.org/defcon-31-talks>

DC Forums Page: <https://forum.defcon.org/node/244860>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732393044363444264>

Location: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Social Media Links:

TW [@secureaerospace](#)

LI [@aerospace-village](#)

TW [@hack_a_sat](#)

DC <https://discord.gg/gV4EWuk>

YT <https://www.youtube.com/c/AerospaceVillage>



AEROSPACE VILLAGE

Aerospace Village

When: Friday to Sat 10:00 - 18:00, Sunday 10:00 to 14:00
Where: Summit Ballroom, Forum

Twitter: @secureaerospace

Website: www.aerospacevillage.org

The aviation and space industries, security researchers, and the public share a common goal: safe, reliable, and trustworthy aviation and space operations. For too long, negative perceptions and fractured trust on all sides have held back collaboration between the aviation, space, and security researcher communities that has advanced safety, reliability, and security of other industries. As the traditional domains of aviation safety and cybersecurity increasingly overlap, more effective collaboration between stakeholders ensures we will be safer, sooner, together.

Through the Aerospace Village, the security research community invites industry leaders, researchers and academia interested in aviation and space security, safety, and resilience to attend, understand, collaborate together to achieve our common goals. Empathy and understanding build common ground, while acts and words likely to increase division between these two communities undermine these efforts. The Aerospace Village welcomes those who seek to improve aviation and space security, safety, and resilience through positive, productive collaboration among all ecosystem stakeholders.

Our Goal

The Aerospace Village is a volunteer team of hackers, pilots, and policy advisors who come from the public and private sectors. We believe the flying public deserves safe, reliable, and trustworthy air travel which is highly dependent on secure aviation and space operations.

Our Mission

- Create, sustain, and grow an inclusive community focused on aerospace cybersecurity;
- Inspire the next generation of aerospace cybersecurity leaders;
- Promote and develop aerospace cybersecurity expertise and knowledge.

The Aerospace Village will do this by:

- Building connections, trust, and understanding among all Village participants.
- Developing aerospace security skills among DEF CON attendees through workshops and hands-on activities.
- Promoting constructive dialog through talks and interaction. Starts August 13, 2023 10:00 Ends August 13, 2023 14:00

[Return to Index](#)

BHV - Bio Hacking Village

BHV Village: [Talk List](#)

Home Page: <https://www.villageb.io/>

Sched Page: <https://www.villageb.io/defcon31-2023>

DC Forums Page: <https://forum.defcon.org/node/244865>

DC Discord Chan: <https://discord.com/channels/708208267699945503/735273390528528415>

Location: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

Social Media Links:

TW [@dc_bhv](#)

LI [@biohacking-village](#)

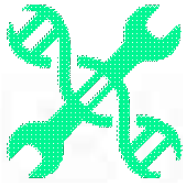
YT <http://youtube.com/biohackingvillage>

TI [@biohackingvillage](#)

DC <https://discord.gg/Q8subDb5>

IG [@biohacking_village](#)

SP [link](#)



BIOHACKING
VILLAGE

Biohacking Village

When: Friday: 10-1800, Saturday: 10-1800 Sunday: 10-1400

Where: Laughlin, Flamingo

Twitter: [@dc_bhv](#)

Website: <https://villageb.io>

THE BIOHACKING VILLAGE, a 501(C)3 organization, (EIN:83-3941279), is uniquely poised to inform global

conversations in health care cybersecurity research. The Biohacking Village brings forth compelling issues in emerging biotechnology, regulations, medical and pharmaceutical manufacturing, cybersecurity, and citizen science. We have been a platform for pursuing greater depth in the bioeconomy, exploring new avenues for collaborations, and innovation. Our participants and attendees include: patients, clinicians, hackers, manufacturers, regulators, hospital administrators, and others seeking healthier futures through meaningful technology. This community delivers hands-on, strident learning labs to influence healthcare, industry, and manufacturing.

DEVICE LAB

A highly-collaborative environment where security researchers test medical instruments, applications, and devices in real-time from participating Medical Device Manufacturers. Any potential issues are reported directly to the manufacturer, and coordinated vulnerability disclosures are produced.

CAPTURE THE FLAG

Featuring the virtual learning environment of St. Elvis Hospital, the CTF offers protocol, regulatory, and biological challenges to access and assess vulnerabilities in real devices.

CATALYST LAB

Providing interaction with thought leaders from the medical device and citizen science communities through training and hands-on workshops and solutions design, to cover the entirety of the biomedical device and security ecosystem.

SPEAKER LAB

Fostering critical thinking, problem solving, human interaction literacy, ethics debates, creativity, and collaboration. Subject matter experts and researchers share the future of their research, reflecting the biological technologies and emerging threats.

TABLETOP EXERCISES

Experiential and immersive sessions of increasing complexity and difficulty regarding vulnerabilities in a series of Machiavellian healthcare industry scenarios. Starts August 13, 2023 10:00 Ends August 13, 2023 14:00 Location Laughlin, Flamingo

[Return to Index](#)

BICV - Blacks in Cybersecurity

BICV Village: [Talk List](#)

Home Page: <https://www.blacksincyberconf.com/bic-village>

Sched Page: <https://www.blacksincyberconf.com/bic-village>

DC Forums Page: <https://forum.defcon.org/node/244885>

Location: Caesars Forum - Alliance - 301-304 - Blacks in Cyber Village - [Map](#)

Social Media Links:

TW [@BlackInCyberCo1](#)

IG [@blackincyberconf](#)

TI [@blacksincybersecurity](#)

YT [link](#)

LI [@blackincyberconference](#)

PT [@blacksincybersecurity](#)

FB [@blackincyberconf](#)



Blacks In Cyber Village

When: Friday: 10:00 AM – 18:00 PM, Saturday: 10:00 AM – 18:00 PM, Sunday: Closed
Where: Alliance 301-303 Forum

Twitter: [@BlackInCyberCo1](https://twitter.com/BlackInCyberCo1)

Website: www.blacksincyberconf.com/bic-village

The Blacks In Cybersecurity (B.I.C.) Village is excited to present at DEF CON 31 in highlighting the ingenuity of the Black and minority communities by way of the presentation of personal hobbyist exploration, research, work experience and contributions that translate to innovation and new perspectives in Cybersecurity.

Our village mission is to bring together Black practitioners in the Cybersecurity field to share knowledge, best practices, and experiences. We are committed to building a community of support, mentorship, and collaboration, and to developing the next generation of Black cybersecurity professionals.

Our village works to create a space to allow for more diverse hobbyists and professionals to engage and contribute. The village seeks to discuss issues in disparity that affect education, literacy, privacy & safety in the digital world as well as be a conducive environment to normalize the discussion of deficiency or prejudices for minority communities.

Our village offerings will include a themed CTF competition, talks throughout the conference duration and opportunities for



TM

interactive learning!

Starts August 12, 2023 10:00 Ends August 12, 2023 18:00 Location Alliance 301-303 Forum

[Return to Index](#)

BTV - Blue Team Village

BTV Village: [Talk List](#)

Home Page: <https://blueteamvillage.org/>

Sched Page: <https://cfc.blueteamvillage.org/dc31/schedule/#>

DC Forums Page: <https://forum.defcon.org/node/244855>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732454317658734613>

Location: Flamingo - Sunset - Scenic - Blue Team Village - [Map](#)

Social Media Links:

TW [@BlueTeamVillage](#)

TI [@blueteamvillage](#)

YT <https://www.youtube.com/c/blueteamvillage>

DC <https://discord.gg/blueteamvillage>

DC <https://discord.com/invite/blueteamvillage>

When: Friday to Sat 10:00 - 20:00, Sunday 10:00 to 14:00

Where: Scenic, Flamingo

Twitter: [@BlueTemVillage](#)

Website: <https://blueteamvillage.org/>

DEFCON Social: @ [blueteamvillage@defcon.social](#)

Blue Team Village (BTV)

Welcome to the other side of the hacking mirror. Blue Team Village (BTV) is both a place and a community built for and by

people who defend computer systems, networks, and people against cyber-attacks. It's a place to gather, talk, share, and learn from each other about the latest tools, technologies, and tactics that our community can use to detect attackers and prevent them from achieving their goals.

Project Obsidian – BTV's Home-Grown Content

The Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Malware Analysis, Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH). Deep dive into technical topics through workshops and exercises that provide practical hands-on experience across each discipline. Project Obsidian workshops provide cybersecurity training that will enable attendees to develop skills needed to be successful in their current and/or future role.

Two of the most valuable takeaways are how to strategically approach a task and the operational processes that support the objectives behind each task. Knowing 'how' to do something is only part of the challenge. Knowing 'when' and 'why' to perform certain tasks adds necessary context to develop the full story of defensive cybersecurity. Starts August 13, 2023 10:00 Ends August 13, 2023 14:00 Location Scenic, Flamingo

[Return to Index](#)

CHV - Car Hacking Village

CHV Village: [Talk List](#)

Home Page: <https://www.carhackingvillage.com/>

Sched Page: <https://www.carhackingvillage.com/defcon-31-talks>

DC Forums Page: <https://forum.defcon.org/node/244891>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732722838942777474>

Location: Caesars Forum - Summit - 234 - Car Hacking Village - [Map](#)

Social Media Links:

TW [@CarHackVillage](#)

YT <http://youtube.com/@carhackingvillage>

DC <https://discord.gg/JWCcTAM>



Carhacking Village

When: Friday 10:00 - 17:00, Saturday 10:00 - 17:00, Sunday 10:00 - 12:00

Where: Contest Area, Forums

Twitter: [@CarHackVillage](https://twitter.com/CarHackVillage)

Website: <https://www.carhackingvillage.com/>

A group of professional and hobbyist car hackers who work together to provide hands-on, interactive car hacking learning, hardware, and interactive contests. The primary goal of the Car Hacking Village is to build a community around discovering weaknesses and exposing vulnerabilities that could significantly impact the safety and security of all drivers and passengers on the road today. Educating security researchers on the functionality of vehicle systems coupled with providing them with the opportunity to gain hands-on experience working side by side with experts in this field is a plus for the attendees. Starts August 13, 2023 10:00 Ends August 13, 2023 12:00 Location Contest Area, Forums

[Return to Index](#)

CLV - Cloud Village

CLV Village: [Talk List](#)

Home Page: <https://cloud-village.org/>

Sched Page: <https://cloud-village.org/#talks>

DC Forums Page: <https://forum.defcon.org/node/244897>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733373172285520>

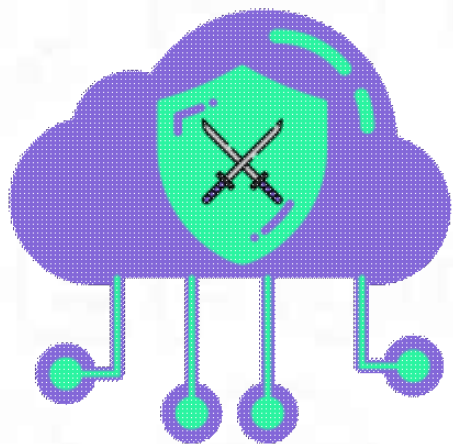
Location: Flamingo - Mesquite - Cloud Village - [Map](#)

Social Media Links:

TW [@cloudvillage_dc](https://twitter.com/cloudvillage_dc)

YT https://www.youtube.com/cloudvillage_dc

DC <https://discord.gg/EygUDJABee>



When: Friday: 10:00 - 17:00, Saturday: 10:00 - 17:00, Sunday: 10:00 - 13:00

Where: Mesquite, Flamingo

Twitter: [@cloudvillage_dc](https://twitter.com/cloudvillage_dc)

Website: <https://cloud-village.org>

With the industry's rapid growth in cloud infrastructure, the presence of an open platform to discuss and showcase cloud research becomes a necessity. Cloud village is an open platform for researchers interested in the area of cloud security. We plan to organise talks, tool demos, CTF and workshops around Cloud Security and advancements.

Our CTF will be a jeopardy style 2.5 days contest where participants will have to solve challenges around Cloud infrastructure, security, recon, etc. These challenges will cover different cloud platforms including AWS, GCP, Azure, Digital Ocean, etc. We will also reward our top 3 teams with awards. Starts August 13, 2023 10:00 Ends August 13, 2023 13:00
Location Mesquite, Flamingo

[Return to Index](#)

CON - Contests

CON Village: [Talk List](#)

[Return to Index](#)

CPV - Crypto Privacy Village

CPV Village: [Talk List](#)

Home Page: <https://cryptovillage.org/>

Sched Page: <https://cryptovillage.org/>

DC Forums Page: <https://forum.defcon.org/node/244871>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732734002011832320>

Location: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

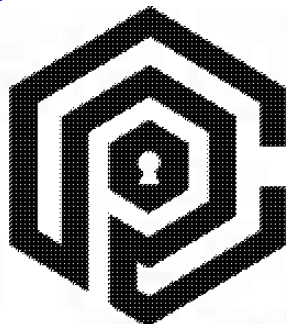
Social Media Links:

TW [@cryptovillage](https://twitter.com/cryptovillage)

SL <https://cryptovillage.slack.com/>

YT [link](#)

TI [@cryptovillage](https://twitter.com/cryptovillage)



**CRYPTO + PRIVACY
V I L L A G E**

Crypto & Privacy Village

When: Friday: 10 - 20:00, Saturday: 10 - 20:00, Sunday: 10 - 14:00

Where: Vista, Flamingo

Twitter: @cryptovillage

Website: <https://cryptovillage.org>

DEFCON social: @ [cryptovillage@defcon.social](https://twitter.com/cryptovillage@defcon.social)

Launched in 2014, Crypto & Privacy Village (CPV) is a community-run village centered on privacy and cryptography that aims to educate and inform the general public, students, educators, hackers, security and privacy professionals, and policymakers. We provide a unique hybrid space that features talks; a chill space for relaxing with friends, doing CTFs, and cross-industry networking; the Gold Bug Challenge and desk for hints and support; privacy-related art installations; and an information desk for questions about privacy and cryptography. Come talk with us about facial recognition technology, privacy enhancing clothing, or crypto backdoor laws! Starts August 13, 2023 10:00 Ends August 13, 2023 14:00 Location Where: Vista, Flamingo

[Return to Index](#)

DC - DEF CON Talks

DC Village: [Talk List](#)

Home Page: <https://defcon.org/html/defcon-31/dc-31-index.html>

Sched Page: <https://defcon.org/html/defcon-31/dc-31-schedule.html>

Social Media Links:

TW [@defcon](#)

FB [@defcon](#)

YT <https://www.youtube.com/user/DEFCONConference>

<http://www.reddit.com/r/defcon>

IG [@wearedefcon](#)

DC <https://discord.gg/defcon>

[Return to Index](#)

DCGVR - DEF CON Groups VR

DCGVR Village: [Talk List](#)

Home Page: <https://www.dcgvr.org/>

Sched Page: <https://www.dcgvr.org/>

DC Forums Page:

Social Media Links:

TW [@DCGVR](#)

TI [@defcon_groups](#)

DC <https://discord.gg/bsX4QXf3rD>

YT [link](#)

[Return to Index](#)

DDV - Data Duplication Village

DDV Village: [Talk List](#)

Home Page: <https://dcddv.org/>

Sched Page: <https://dcddv.org/dc31-schedule>

DC Forums Page: <https://forum.defcon.org/node/244903>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732732641694056478>

Location: Caesars Forum - Summit - 231 - Data Dupe Vlg - [Map](#)

Social Media Links:

TW [@DDV_DC](#)

TI [@defcon_groups](#)

DC <https://discord.gg/bsX4QXf3rD>

YT [link](#)



Data Duplication Village

When:

Thursday: 4:00pm to 7:00pm

Friday: 10:00am to 5:00pm

Saturday: 10:00am to 5:00pm

Sunday: 10:00am to 11:00am (last chance pickup)

Where: Academy 410, Forum

Twitter: [@DDV_DC](#)

The Data Duplication Village is ready for DC 31! We have all the updated bits and bytes available from infocon.org packed up into nice, neat packages. If you're looking for something to fill up all your unused storage, we have a few nice hash tables and all of the DefCon talks. Add to that just about every other security con talk known to human-kind! We provide a "free-to-you" service where of direct access to terabytes of useful data to help build those hacking skills.

Check the schedule and/or dcddv.org for the most up-to-date information.

HOW IT WORKS

The DDV provides a core set of drive duplicators and data content options. We accept 6TB and larger drives on a first come, first served basis and duplicate 'till we can no longer see straight. Bring in your blank SATA3 drives - check them in early - to get the data you want. Come back in about 24 hours to pick up your data-packed drive. Space allowing, we'll accept drives all the way through until Saturday morning - but remember, it's FIFO - get those drives in early!

WHAT YOU GET

We're working on more content right up until the last minute but for dc29, we provided:

- 6TB drive 1-3: All past hacking convention videos that DT could find, built on last years collection and always adding more for your data consuming appetite.

- 6TB drive 2-3: freerainbowtables.com hash tables (1-2)

- 6TB drive 3-3: GSM A5/1 hash tables plus remaining freerainbowtables.com data (2-2)

The DC 30 content will be posted at dcddv.org once finalized

DT and KnightOwl post the up-to-date details in the DC Forum thread and you are encouraged to ask any questions you have there as con approaches. Starts August 13, 2023 10:00 Ends August 13, 2023 11:00 Location Academy 410, Forum

[Return to Index](#)

DL - DEF CON DemoLabs

DL Village: [Talk List](#)

Home Page: <https://forum.defcon.org/node/244767>

[Return to Index](#)

ESV - Embedded Systems Village

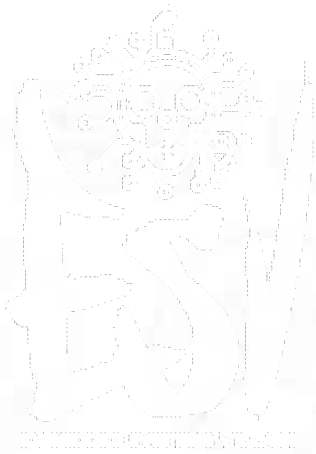
ESV Village: [Talk List](#)

DC Forums Page: <https://forum.defcon.org/node/244910>

Location: LINQ - 3rd flr - Evolution - Embedded Systems Village - [Map](#)

Social Media Links:

TW [@EmbeddedVillage](#)



Embedded Systems Village

Twitter: [@EmbeddedVillage](https://twitter.com/EmbeddedVillage)

When:

Friday: 0900 - 1800

Saturday: 0900 – 1800

Sunday: 0900 - 1400

CTF ONLY in-person. Some labs will be made available virtually.

Where: Linq Evolution

Embedded systems exist at the intersection of hardware and software, built to accomplish a specific task. Often these disciplines are dealt with individually, but understanding the custom relationships between hardware and software is key to performing security research on these devices.

Embedded Systems Village advances the security of embedded systems by hosting hands-on hacking workshops, showcasing new security research demos, and organizing exciting hacking contests to educate attendees and manufacturers on the approach hackers use to attack these devices. Attendees will leave the village with an understanding of how to reduce complex, exotic devices to their underlying embedded components and to extract the information required to use the tools and techniques taught at other villages where embedded systems are on display.

What we will bring:

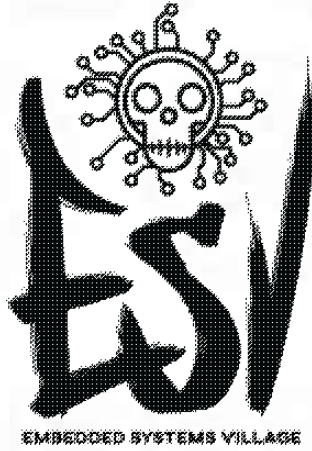
Labs: We have a lab platform that brings everyone from every skill level to the same playing field with step by step instructions that aim to teach individuals specific techniques and skills in a hands-on manner.

Interactive Hacking Content: We want to showcase the weird and cool in the embedded device world, and provide an opportunity for hackers to get hands-on experience hacking them.

Contests: We are working on a brand new CTF contest that will support everyone from the casual player (i.e. someone that only wants to drop in for a few minutes) all the way to the hardcore teams that are willing to spend their full DEF CON engaged in our challenges.

Expect unique devices, new challenge formats and full DEF CON worth of fun.

Expect unique devices, new challenge formats and that WOW factor that our CTFs have had in the past. Building on our lessons learned and experience over the years, we are confident that this track will not disappoint!



Starts August 13, 2023 09:00 Ends August 13, 2023 14:00 Location Linq Evolution

[Return to Index](#)

HHV - Hardware Hacking and Solder Skills Villages

HHV Village: [Talk List](#)

Home Page: <https://dchhv.org/>

Sched Page: <https://dchhv.org/schedule/schedule.html>

DC Forums Page: <https://forum.defcon.org/node/244921>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732728536149786665>

Location: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Social Media Links:

TW [@DC_HHV](#)



Hardware Hacking Village & Soldering Skills Village

When:

Friday: 10:00 - 18:00

Saturday: 10:00 - 18:00

Sunday: 10:00 - 13:00

Where: 312, 311, 320, Forums

Twitter: [@DC_HHV](#)

Website: <https://dchhv.org>

Every day our lives become more connected to consumer hardware. Everyday the approved uses of that hardware are reduced, while the real capabilities expand. Come discover hardware hacking tricks and tips regain some of that capacity, and make your own use for things! We have interactive demos to help you learn new skills.

We have challenges to compete against fellow attendees. We have some tools to help with your fever dream modifications. Come share what you know and learn something new.

Details @ [dchhv.org](#)

Starts August 13, 2023 10:00 Ends August 13, 2023 13:00 Location 312, 311, 320, Forums

[Return to Index](#)

HRV - Ham Radio Village

HRV Village: [Talk List](#)

Home Page: <https://hamvillage.org/>

DC Forums Page: <https://forum.defcon.org/node/244915>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733631667372103>

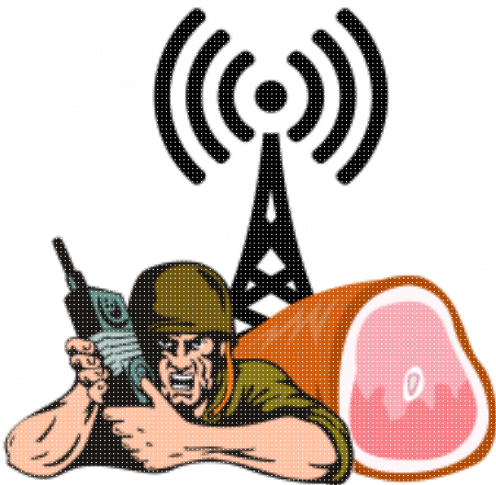
Location: Flamingo - Virginia City - Ham Radio Village - [Map](#)

Social Media Links:

TW [@HamRadioVillage](#)

TI [@HamRadioVillage](#)

DC <https://discord.gg/hrv>



Ham Radio Village

When:

Friday: 10:00 - 18:00

Saturday: 10:00 - 18:00

Sunday: 10:00 to 14:00

Where: Virginia City, Flamingo

Twitter: [@HamRadioVillage](#)

DEFCON Social: <https://defcon.social/@HamRadioVillage>

Website: <https://hamvillage.org>

Ham radio is the original group of electronic hackers, starting long before computers, circuit chips, or even transistors. Continuing this pioneer spirit, Ham Radio Village is here to support advancement of the hobby with a cybersecurity slant. Everything we do today involves wireless communications of some sort, and a basic knowledge of how radio works is crucial. In the HRV, you can learn hand-on with topics such as how to legally use a radio to send commands to a satellite, communicating around the globe when no other methods exist, and how to send and receive real-time location data without relying on any cellular networks. You can put your skills to the test by trying to find the hidden transmitters in the Ham Radio Fox Hunt contest, as well as transmitting memes over the airwaves to defcon attendees. We provide license testing services for those looking to become licensed or upgrade their license class, as well as guidance on how to hack on the medium to achieve the best results and have the most fun! Starts August 13, 2023 10:00 Ends August 13, 2023 14:00 Location Virginia City, Flamingo

[Return to Index](#)

ICSV - Industrial Control Systems Village

ICSV Village: [Talk List](#)

Home Page: <https://www.icsvillage.com/>

Sched Page: <https://www.icsvillage.com/defconevents/def-con-31>

DC Forums Page: <https://forum.defcon.org/node/244927>

DC Discord Chan: <https://discord.com/channels/708208267699945503/735938018514567178>

Location: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

Social Media Links:

TW [@ICS_Village](#)

LI [@icsvillage](#)

YT [link](#)

TI [@ics_village](#)



ICS Village

When:

Friday: 10-8

Saturday: 10-8

Sunday: 10-2

Where: 414,415, 416, 417, 418, 419, Forums

Twitter: [@ics_village](https://twitter.com/ics_village)

Website: www.icsvillage.com

Mission. ICS Village is a non-profit organization with the purpose of providing education and awareness of Industrial Control System security.

Connecting public, industry, media, policymakers, and others directly with ICS systems and experts.

Providing educational tools and materials to increase understanding among media, policymakers, and general population.

Providing access to ICS for security researchers to learn and test.

Hands on instruction for industry to defend ICS systems.

Why. High profile Industrial Controls Systems security issues have grabbed headlines and sparked changes throughout the global supply chain. The ICS Village allows defenders of any experience level to understand these systems and how to better prepare and respond to the changing threat landscape.

Exhibits. Interactive simulated ICS environments, such as Hack the Plan(e)t and Howdy Neighbor, provide safe yet realistic examples to preserve safe, secure, and reliable operations. We bring real components such as Programmable Logic Controllers (PLC), Human Machine Interfaces (HMI), Remote Telemetry Units (RTU), actuators, to simulate a realistic environment throughout different industrial sectors. Visitors can connect their laptops to assess these ICS devices with common security scanners, network sniffers to sniff the industrial traffic, and more!

The Village provides workshops, talks, and training classes. Starts August 13, 2023 10:00 Ends August 13, 2023 14:00
Location 414,415, 416, 417, 418, 419, Forums

[Return to Index](#)

IOTV - Internet Of Things Village

IOTV Village: [Talk List](#)

Home Page: <https://www.iotvillage.org/>

DC Forums Page: <https://forum.defcon.org/node/244939>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732734565604655114>

Location: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Social Media Links:

TW [@iotvillage](#)

TW [@ISEsecurity](#)

TW [@Villageidiotlab](#)

LI [@iotvillage](#)

TI [@iotvillage](#)

YT <https://www.youtube.com/c/IoTVillage/videos>

DC <https://discord.gg/EFKbNFrFaN>



IoT Village

When:

Friday: 10:00 - 18:00

Saturday: 10:00 - 18:00

Sunday: 10:00 - 15:00

Where: 307-310, Forums

Twitter: [@IoTvillage](#)

Website: <https://www.iotvillage.org/>

IoT Village advocates for advancing security in the Internet of Things (IoT) industry through bringing researchers and industry together. IoT Village hosts talks by expert security researchers, interactive hacking labs, live bug hunting in the latest IoT tech, and competitive IoT hacking contests. Over the years IoT Village has served as a platform to showcase and uncover hundreds of new vulnerabilities, giving attendees the opportunity to learn about the most innovative techniques to both hack and secure IoT. IoT Village is organized by security consulting and research firm, [Independent Security Evaluators \(ISE\)](#) .

IoT Village will have our 4 time black badge CTF, 101 labs, live bug hunting, hands on hacking demos, and more!

Starts August 13, 2023 10:00 Ends August 13, 2023 15:00 Location 307-310, Forums

[Return to Index](#)

LPV - Lock Pick Village

LPV Village: [Talk List](#)

Home Page: <https://www.tool.us/>

DC Forums Page: <https://forum.defcon.org/node/244933>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732734164780056708>

Location: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

Social Media Links:

TW [@tool](#)

TI [@tool_us](#)

YT <https://youtube.com/c/TOOOL-US>



Lockpick Village

When:

Friday: 10:00-18:00

Saturday: 10:00-18:00

Sunday: 10:00-14:00

Where: Bloq, Linq

Twitter: [@toool](#)

Website: <https://www.toool.us/>

Want to tinker with locks and tools the likes of which you've only seen in movies featuring secret agents, daring heists, or covert entry teams?

Then come on by the Lockpick Village, run by The Open Organization Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.

The Lockpick Village is a physical security demonstration and participation area. Visitors can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice on locks of various levels of difficulty to try it themselves.

Experts will be on hand to demonstrate and plenty of trial locks, pick tools, and other devices will be available for you to handle. By exploring the faults and flaws in many popular lock designs, you can not only learn about the fun hobby of sport-picking, but also gain a much stronger knowledge about the best methods and practices for protecting your own property.

Starts August 13, 2023 10:00 Ends August 13, 2023 14:00 Location Bloq, Linq

[Return to Index](#)

MISC - Misc

MISC Village: [Talk List](#)

[Return to Index](#)

MIV - MisInformation Village

MIV Village: [Talk List](#)

Home Page: <https://www.misinformationvillage.com/>

Sched Page: <https://www.misinformationvillage.com/defcon31/>

DC Forums Page: <https://forum.defcon.org/node/245077>

Location: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

Social Media Links:

TW [@Misinfovillage](#)

<https://defcon.social/@misinformationvillage>

..

Misinformation Village

When:

Friday 10:00-20:00

Saturday 10:00-20:00

Sunday 10:00-14:00

Where: Contests, Forums.

Website: www.misinformationvillage.com
Social: X / Twit @ [Misinformationvillage](#)
defcon.social: @ [misinformationvillage](#)
E-mail: misinformationvillage@gmail.com

Misinformation is a snowballing, mutating information problem that is affecting human communications, social relationships and has real-world consequences. Misinformation, disinformation and malinformation campaigns undermine democratic institutions, legitimate elections results, public health and public health responses and has created a space for the rise of autocratic regimes and warfare.

We will apply our organizational skills and subject matter expertise to bring together experts from different professions, governments, civil society and private enterprise to come together and create a platform to define and combat misinformation, explore and align missions and tactics to achieve this goal.

Starts August 13, 2023 10:00 Ends August 13, 2023 14:00 Location Contests, Forums

[Return to Index](#)

MUS - Music

MUS Village: [Talk List](#)

Home Page: <https://defconmusic.org>

Sched Page: <https://defconmusic.org/def-con-31-music-lineup/>

Social Media Links:

TW [@defcon_music](#)

YT [link](#)

TI [@defcon_music](#)

TI [@defcon_chill](#)

Music Link All the Things: https://www.twitch.tv/defcon_music https://www.twitch.tv/defcon_chill

<http://www.defconmusic.org/>

[Return to Index](#)

PHV - Packet Hacking Village

PHV Village: [Talk List](#)

Home Page: <https://www.wallofsheep.com/>

Sched Page: <https://www.wallofsheep.com/pages/dc31#talks>

DC Forums Page: <https://forum.defcon.org/node/244945>

DC Discord Chan: <https://discord.com/channels/708208267699945503/708242376883306526>

Location: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Social Media Links:

TW [@wallofsheep](#)

FB [@wallofsheep](#)

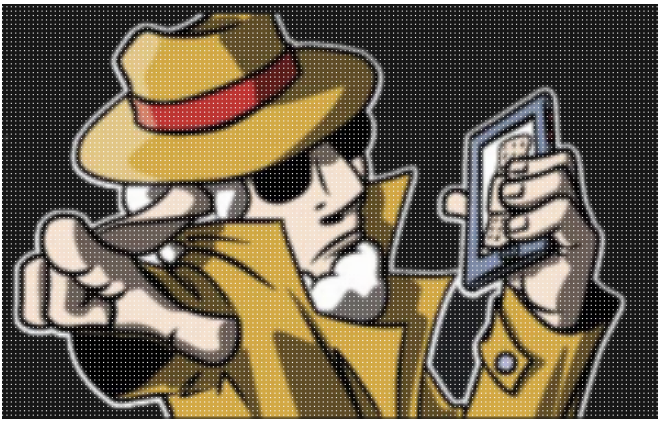
YT <https://youtube.com/wallofsheep>

TI [@wallofsheep](#)

PS <https://www.periscope.tv/wallofsheep>

<https://wallofsheep.tumblr.com/>

IG [@wallofsheep](#)



The Packet Hacking Village

When:

Friday: 9am - 6pm

Saturday: 9am - 6pm

Sunday: 9am - 1pm

Where: Forum 413

Twitter:

Website: <https://www.wallofsheep.com>

The Packet Hacking Village is where you'll find network shenanigans and a whole lot more. There's exciting events, live music, competitions with awesome prizes, and tons of giveaways. PHV welcomes all DEF CON attendees and there is something for every level of security enthusiast from beginners to those seeking a black badge. Wall of Sheep gives attendees a friendly reminder to practice safe computing through strong end-to-end encryption. PHV Speakers, Workshops, and Walkthrough Workshops delivers high quality content for all skill levels. Packet Detective and Packet Inspector offers hands-on exercises to help anyone develop or improve their Packet-Fu. WoSDJCo has some of the hottest DJs at con spinning live for your enjoyment. Finally... Capture The Packet, the ultimate cyber defense competition that has been honored by DEF CON as a black badge event for seven of the eight years of its run.

Starts August 13, 2023 09:00 Ends August 13, 2023 13:00 Location Forum 413

[Return to Index](#)

PLV - Policy Village

PLV Village: [Talk List](#)

Home Page: <https://defcon.org/policy/>

Sched Page: <https://twitter.com/DEFCONPolicy/status/1686024040023003136?s=20>

DC Village Page:

DC Forums Page: <https://forum.defcon.org/node/244979>

Location: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

Social Media Links:

TW [@DEFCONPolicy](#)

[link](#)

Policy@DEFCON

When: Friday to Sat 10:00 - 20:00, Sunday 10:00 to 13:00,
Where: 213-223, Forums
Website: <https://www.defcon.org/html/links/dc-policy.html>

Policy@DEFCON

<https://www.defcon.org/html/links/dc-policy.html>

Hackers are early users and abusers of technology, and that technology is now critical to modern life. As governments make policy decisions about technology Hackers, researchers and academics need to be part of that conversation before decisions are made, not after policies are implemented. To do that DEF CON is a place for everyone on the policy and technology spectrum to interact, learn from each other, and improve technology.

Policy will build connections across and between technical and policy experts and provide opportunities for attendees interested in learning more about how policy and technology intersect and to examine the challenges at this intersection.

Our Policy program will consist of Main stage presentation and panels, daytime sessions in our policy track, and some evening lounges that will provide an off the record and more intimate setting to have policy-focused conversation

Tech policy is going to happen and we believe including diverse expert voices will improve outcomes across the policy-technology spectrum by bridging the gap between technical and policy practitioners. Senior government officials, policy experts, nonprofit and the private sector, security researchers, hackers, academics and technologists from around the world all come together at Policy @ DEF CON. Starts August 13, 2023 10:00 Ends August 13, 2023 13:00 Location 213-223, Forums

[Return to Index](#)

PSV - Physical Security Village

PSV Village: [Talk List](#)

Home Page: <https://www.physsec.org/>

DC Forums Page: <https://forum.defcon.org/node/244958>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732732893830447175>

Location: Flamingo - Carson City - Physical Security Village - [Map](#)

Social Media Links:

TW [@physsec](#)

TI [@bypassvillage](#)

LI [@physsec](#)



Physical Security Village

When: Friday to Sat 10:00 - 20:00, Sunday 10:00 to 14:00

Where: Carson city I & II ,Flamingo

Twitter: [@physsec](#)

Website: <https://physsec.org>

The Physical Security Village explores the world of hardware bypasses and techniques generally outside of the realm of cyber-security and lockpicking. Come learn some of these bypasses, how to fix them, and have the opportunity to try them out for yourself.

We'll be covering the basics, like the under-the-door-tool and latch slipping attacks, as well as an in depth look at more complicated bypasses. Learn about elevator hacking, attacking alarm systems at the sensor and communication line, and cut-away and display models of common hardware to show how it works on the inside.

Looking for a challenge? Show us you can use lock bypass to escape from a pair of standard handcuffs in under 30 seconds and receive a prize! Starts August 13, 2023 10:00 Ends August 13, 2023 14:00 Location Carson city I & II ,Flamingo

[Return to Index](#)

PT - Paid Training

PT Village: [Talk List](#)

Home Page: <https://defcontrainings.myshopify.com/collections/all>

DC Forums Page: <https://forum.defcon.org/node/244768>

[Return to Index](#)

PWV - Password Village

PWV Village: [Talk List](#)

Home Page: <https://passwordvillage.org/>

DC Forums Page: <https://forum.defcon.org/node/244967>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733760742621214>

Location: Caesars Forum - Summit - 236 - Password Village - [Map](#)

Social Media Links:

TW [@PasswordVillage](#)

TI [@passwordvillage](#)

YT [link](#)



Password Village

When:

Friday: 10:00 - 20:00

Saturday: 10:00 - 20:00

Sunday: 10:00 - 14:00

Where: Contest Area, Forums

Twitter: [@passwordvillage](#)

Website: <https://passwordvillage.org>

The Password Village provides training, discussion, and hands-on access to hardware and techniques utilized in modern password cracking, with an emphasis on how password cracking relates to your job function and the real world . No laptop? No problem! Feel free to use one of our terminals to access a pre-configured GPGPU environment to run password attacks against simulated real-world passwords. Village staff and

expert volunteers will be standing by to assist you with on-the-spot training and introductions to Hashcat, as well as other FOSS cracking applications. Already a password cracking aficionado? Feel free to give a lightning talk, show off your skills, help a n00b learn the basics, or engage in riveting conversation with other password crackers.

Starts August 13, 2023 10:00 Ends August 13, 2023 14:00 Location Contest Area, Forums

[Return to Index](#)

PYV - Payment Village

PYV Village: [Talk List](#)

Home Page: <https://www.paymentvillage.org/>

DC Forums Page: <https://forum.defcon.org/node/244951>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733473558626314>

Location: Flamingo - Virginia City - Payment Village - [Map](#)

Social Media Links:

TW [@paymentvillage](#)

TI [@paymentvillage](#)

YT [link](#)

<https://t.me/paymentvillage>



Payment Village

When:

Friday: 10:00 - 18:00

Saturday: 10:00 - 18:00

Sunday: 10:00 - 15:00

Where: Contest Area, Forums

Twitter: [@paymentvillage](#)

Website: <https://www.paymentvillage.org/>

Payment technologies are an integral part of our lives, yet few of us know much about them. Have you ever wanted to learn how payments work? Do you know how criminals bypass security mechanisms on Point of Sales terminals, ATM's and digital wallets?

Payment technologies are an integral part of our lives, yet few of us know much about them. Have you ever wanted to learn how payments work? Do you know how criminals bypass security mechanisms on Point of Sales terminals, ATM's and digital wallets? Come to the Payment Village and learn about the history of payments. We'll teach you how hackers gain access to banking endpoints, bypass fraud detection mechanisms, and ultimately, grab the money!

Starts August 13, 2023 10:00 Ends August 13, 2023 15:00 Location Contest Area, Forums

[Return to Index](#)

QTV - Quantum Village

QTV Village: [Talk List](#)

Home Page: <https://quantumvillage.org/>

DC Forums Page: <https://forum.defcon.org/node/244973>

Location: LINQ - 3rd flr - Quantum Village - [Map](#)

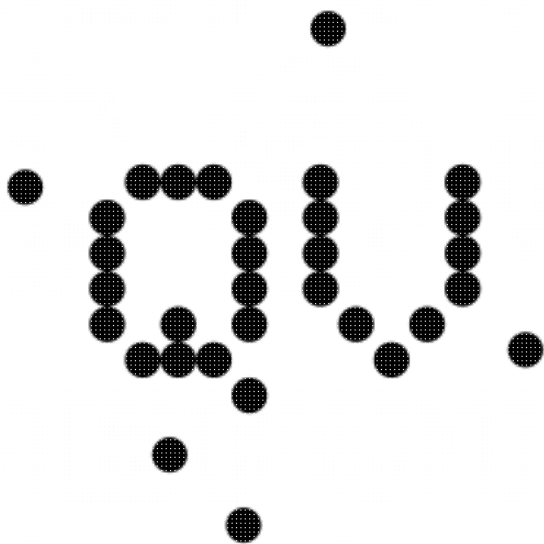
Social Media Links:

TW [@quantum_village](#)

DC <https://discord.gg/6WUjH5cBXu>

LI [@quantumvillage](#)

YT https://youtube.com/@quantum_village/



Quantum Village

When:

Friday: 1000-1900

Saturday: 1000-1900

Sunday: 1000-1300

Where: Innovation, Linq

Twitter: [@quantum_village](https://twitter.com/quantum_village)

Website: <https://quantumvillage.org/>

This is the safe space for anyone to discover, learn, create and break all things around Quantum Technologies. We are committed to helping raise awareness and involvement in the quantum industry and with quantum technologies. We know that in order to avoid the mistakes of past technological surges, we have to engage as many people with as wide a variety of interests and backgrounds as possible.

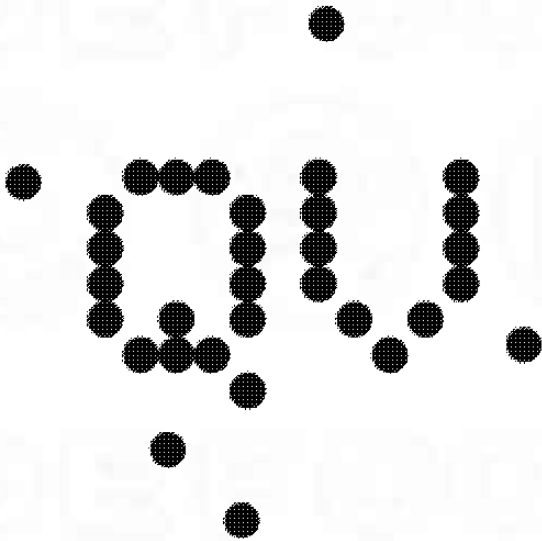
To date, very few (if any) people have actually hacked a quantum computer, and we want to change that! Something we demonstrated last year was that quantum computers are only a small part 'magic' - the rest are familiar API and tech stack technologies we see everywhere. These devices are set to become more and more commonplace as more time, money, and intelligence is spent on improving them - so let's get quantum hacking!

Our ethos is to encourage participants to engage, explore, and discuss topics surrounding this new and burgeoning technology ecosphere that is in many ways very different from what has gone before in technical revolutions - but there are many hallmarks that are the same, and which we can use to shape this new paradigm of computing. That conversation is essential to bring before some of the most talented and brilliant technologists going; the hackers at DEF CON.

We have built on many of the things that were popular last year, but have also improved things and sought feedback from participants to make things even better this coming year! We were standing room only last year, with very popular events and debates alongside our workshops and talks, and we would like to build on the positive energy and momentum that comes from the Quantum Hackers.

We have many ideas for what we want to do with QV this year, and here are some of the more exciting ones:

- Another Quantum CTF - this time, with more resources, more challenges, and a secret project QOLOSSUS challenge that we are collaborating on with some very cool people to build and add to the challenges and immersive labs.
- We plan to bring a real quantum computer and quantum devices to hack! - now that there are commercially available devices and enough interest in DEF CON from quantum computing companies we have engaged with, we believe this is a real possibility.
- We are also attempting to arrange to bring and demonstrate quantum devices that explore how the second quantum revolution that is underway will affect everything from sensors to data storage, and in industries as diverse as tunnel digging to healthcare.
- Our first badge - A mesh networked collaborative group Quantum Simulator with a Quantum Networking simulation working with experts and research groups we are building a collaborative experimental platform for people to explore (and wear) quantum computing.
- We want to have an ice breaker Quantini time cocktail hour for folks with Quantum Computer Music - this would be a great way for Quantum Hackers at DEF CON to have fun and meet others.
- We are considering a return with some more workshops, more debates, and more introductory sessions - developing on from what we presented last year, but showing new developments in both theory and practical quantum hacking and quantum tech. Our aim is to make learning this area as hands-on as possible.
- We are also planning on expanding significantly the work on Quantum Life - more sessions, and more engagement to realise more of the ways that quantum technologies will affect our lives, society at large, and consider ideas of privacy, anonymity, integrity, and beyond, in a post-quantum world.



. Starts August 13, 2023 10:00 Ends August 13, 2023 13:00 Location Innovation, Linq

[Return to Index](#)

RCV - Recon Village

RCV Village: [Talk List](#)

Home Page: <https://www.reconvillage.org/>

Sched Page: <https://reconvillage.org/recon-village-talks-2023-defcon-31/>

DC Forums Page: <https://forum.defcon.org/node/245016>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733566051418193>

Location: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

Social Media Links:

TW [@ReconVillage](#)

FB [@reconvillage](#)

YT <https://www.youtube.com/reconvillage/>



Recon Village

When:

Friday - 10:00 AM - 18:00 PM

Saturday - 10:00 AM - 18:00 PM

Sunday - 10:00 AM - 13:00 PM

Where: Social B and Social C, Linq

Twitter: [@reconvillage](https://twitter.com/reconvillage)

Website: <https://reconvillage.org>

Recon Village is an Open Space with Talks, Live Demos, Workshops, Discussions, CTFs, etc., with a common focus on Reconnaissance. The core objective of this village is to spread awareness about the importance of reconnaissance and open-source intelligence (OSINT) and demonstrate how even a small piece of information about a target can cause catastrophic damage to individuals and organizations.

As recon is a vital phase for infosec as well as investigations, folks should definitely have this skill set in their arsenal. People should check out Recon Village, as they get to learn novel point/recon techniques, play hands-on CTF, and, most of all, have fun. At RV, we keep things simple, and the focus is on generating quality content using talks, CTF, hackathons, etc.

We will also have our Jeopardy Style OSINT CTF Contest throughout the Village timings. Based on the feedback from last year, we plan to make the CTF more challenging this year. The challenges will be around harvesting information about target organizations, their employee's social media profiles, their public svn/gits, password breach dumps, darknet, paste(s) etc., followed by active exploitation, bug hunting, investigation and pentest scenarios of virtual targets. All the target organizations, employees, servers, etc., will be created by our team and hence will not attract any legal issues.

Similar to the previous years, there will be Awesome rewards for CTF winners, along with free t-shirts, stickers, village coins, and other schwaq which attendees can grab and show off.

We will be making changes to our badge as well. P.S. We will not be selling it, though.

This year, we will also be running some large-scale recon projects to analyze patterns across the internet. Starts August 13, 2023 10:00 Ends August 13, 2023 13:00 Location Social B and Social C, Linq

RFV - Radio Frequency Village

RFV Village: [Talk List](#)

Home Page: <https://rfhackers.com/>

DC Forums Page: <https://forum.defcon.org/node/244984>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732732595493666826>

Location: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

Social Media Links:

TW [@rfhackers](#)

TW [@rf_ctf](#)

[link](#)

DC <https://discordapp.com/invite/JjPQhKy>



Radio Frequency Village

When: Friday to Sat 10:00 - 20:00, Sunday 10:00 to 14:00

Where: Eldorado, Flamingo

Twitter: [@rfhackers](#)

Website: <https://rfhackers.com>

After 16 years of evolution, from the WiFi Village, to the Wireless Village, RF Hackers Sanctuary presents: The Radio Frequency Village at DEFCON. The Radio Frequency Village is an environment where people come to learn about the security of radio frequency (RF) transmissions, which includes wireless technology, applications of software defined radio (SDR), Bluetooth (BT), Zigbee, WiFi, Z-wave, RFID, IR and other protocols within the usable RF spectrum. As a security community we have grown beyond WiFi, and even beyond Bluetooth and Zigbee. The RF Village includes talks on all manner of radio frequency command and control as well as communication systems. While everyone knows about the WiFi and Bluetooth attack surfaces, most of us rely on many additional technologies every day. RF Hackers Sanctuary is supported by a group of experts in the area of information security as it relates to RF technologies. RF Hackers Sanctuary's common purpose is to provide an environment in which participants may explore these technologies with a focus on improving their skills through offense and defense. These learning environments are provided in the form of guest speakers, panels, and Radio Frequency Capture the Flag games, to promote learning on cutting edge topics as it relates to radio communications. We promise to still

provide free WiFi.

<https://rfhackers.com/the-crew>

Starts August 13, 2023 10:00 Ends August 13, 2023 14:00 Location Eldorado, Flamingo

[Return to Index](#)

RTV - Red Team Village

RTV Village: [Talk List](#)

Home Page: <https://redteamvillage.io/>

Sched Page: <https://redteamvillage.io/schedule.html>

DC Forums Page: <https://forum.defcon.org/node/245022>

Location: Flamingo - Sunset-Twilight Ballroom - Red Team Village - [Map](#)

Social Media Links:

TW [@RedTeamVillage_](#)

YT <https://www.youtube.com/redteamvillage>

TI [@redteamvillage](#)

DC <https://discord.gg/redteamvillage>



Red Team Village

When:

Friday: 10:00 - 18:00

Saturday: 10:00 - 18:00

Sunday: 10:00 to 12:00

Where: Scenic, Flamingo

Twitter: [@RedTeamVillage_](#)

Website: <https://redteamvillage.io>

Friday: 10:00 - 18:00
Saturday: 10:00 - 18:00

The Red Team Village is focused on training the art of critical thinking, collaboration, and strategy in offensive security. The RTV brings together information security professionals to share new tactics and techniques in offensive security. Hundreds of volunteers from around the world generate and share content with other offensively minded individuals in our workshops, trainings, talks, and conferences. Starts August 13, 2023 10:00 Ends August 13, 2023 12:00 Location Scenic, Flamingo

[Return to Index](#)

SEV - Social Engineering Village

SEV Village: [Talk List](#)

Home Page: <https://www.se.community/>

Sched Page: <https://www.se.community/schedule/>

DC Forums Page: <https://forum.defcon.org/node/245028>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733952867172382>

Location: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Social Media Links:

TW [@sec_defcon](#)

YT [link](#)

TI [@se_community](#)

LI [@social-engineering-community](#)

FB [@Social-Engineering-Community-108883855139272](#)



Social Engineering Community Village

Hours:

Friday: 0830 – 1800

Saturday: 0830 – 1800 and party from 2100 - 0000 (Forums room 117/118)

Sunday: 1000 to 1400

Location:

In the Social Engineering Community Village (LINQ Hotel, 3rd floor, room Social A)

Description:

Welcome to the Social Engineering Community! The SEC village focuses purely on the human aspect of security, Social Engineering, with the goal of enabling people of all ages and backgrounds interested in the subject matter with a venue to learn, discuss, and practice this craft.

This year, over the course of three days at DEF CON, you can expect the following events to take place in the village:

- Vishing Competition (#SECVV) – This competition is where prior selected teams (who have already put WEEKS of work into the competition) place live phone calls inside a soundproof booth in front of SEC audience members with the goal of eliciting as many objectives as possible. Highest score, wins! This competition takes place only on Friday.

- Youth Challenge – Anyone 18 and under is invited to play, where they can compete and learn about more than just social engineering; our challenges include areas in cryptography, network security, ... and don't worry, you won't be alone. We've worked with other villages so you can get help you need and learn on the way!

- Cold Calls – This event lets DEF CON attendees sign up in the village (first come, first serve style) to place live phone calls inside of the soundproof booth. We provide the target and phone number, then give a few objectives (easy, medium, and hard), and start a countdown timer to see if they have the skills to get information from a stranger, with no preparation. There is nothing to prepare for, just bring yourself!

- SE Improv – Struggling to think on your feet? Discover the art of improvisation and transform every conversation into an opportunity! On Saturday, the improv team will start by presenting the benefits of utilizing Improv with Social Engineering and then have the opportunity for audience participation.

- Presentations – Come listen from folks in the field and get a glimpse of the newest techniques and perspectives in our presentations and panels hosted various times between Friday and Saturday in the village.

- Social Engineering Community Party (80's theme) – Want to hang out without the loud music so that you can actually have a conversation? *Put on your raddest 80s gear* and join the Social Engineering Community for a themed get-together for a chance to hang out and meet new people! We'll have a cash bar with both boozy and booze-free options. Forums room 117/118.

Please check out our website and Twitter account to learn more and view the detailed schedule.

Website: <https://www.se.community/>

Twitter: @ [sec_defcon](#) Starts August 13, 2023 10:00 Ends August 13, 2023 14:00 Location LINQ Hotel, 3rd floor, room Social A

[Return to Index](#)

SOC - Social Activities: Parties/Meetups

SOC Village: [Talk List](#)

DC Forums Page: <https://forum.defcon.org/node/244769>

[Return to Index](#)

TCV - Telecom Village

TCV Village: [Talk List](#)

Home Page: <https://telecomvillage.com/>

Sched Page: <https://telecomvillage.com/#schedule>

DC Forums Page: <https://forum.defcon.org/node/244995>

Location: Flamingo - Virginia City - Telecom Village - [Map](#)

Social Media Links:

TW [@TelecomVillage](#)

.

.

Telecom Village

When:

Friday: 10:00 – 20 :00

Saturday: 10:00 - 20:00

Sunday: 10:00 – 13:00

Where: Virginia City, Flamingo

Website: TELECOMVILLAGE.COM

CFP will be open from 1st of May 2023 to 15th of June2023 .

website address : telecomvillage.com

CFP url : <https://docs.google.com/forms/d/e/1F...78UoA/viewform>

The Telecom Village's primary focus would be around Telecom Security. We plan to host multiple hands on events as part of the village so as to give participants an overview security specific challenges in a Telcom Network. This includes: CTFs in telecom signaling security and another one in Private 5G and select set of talks (5), spread across two days.

We are planning a workshop over a day where we will be giving an overview of the 4G/5G network and its security. There will be a small CTF for SS7, Diameter attack on the 3G/4G network and 5G network. The workshop and CTF will focus on use of open-source tools so as to ensure that this Niche within the Security Industry is taken to wider audience.

In the village, we will also be hosting a 4G/5G live network which will have Live Radio and 4G/5G Core. Attendees will be able to understand the call flow of Telecom and the Weaknesses in the call flows.

Starts August 13, 2023 10:00 Ends August 13, 2023 13:00 Location Virginia City, Flamingo

[Return to Index](#)

TEV - Tamper Evident Village

TEV Village: [Talk List](#)

DC Forums Page: <https://forum.defcon.org/node/245000>

Location: LINQ - 5th Floor / BLOQ - Tamper Evident Village - [Map](#)

.

.

Tamper Evident Village

When: Friday to Sat 10:00 - 20:00, Sunday 10:00 to 14:00

Where: Bloq, Linq

Tamper-evident" refers to a physical security technology that provides evidence of tampering (access, damage, repair, or

replacement) to determine authenticity or integrity of a container or object(s). In practical terms, this can be a piece of tape that closes an envelope, a plastic detainer that secures a hasp, or an ink used to identify a legitimate document. Tamper-evident technologies are often confused with "tamper resistant" or "tamper proof" technologies which attempt to prevent tampering in the first place. Referred to individually as "seals," many tamper technologies are easy to destroy, but a destroyed (or missing) seal would provide evidence of tampering! The goal of the TEV is to teach attendees how these technologies work and how many can be tampered with without leaving evidence.

The Tamper-Evident Village includes the following contests and events:

The Box; an electronic tamper challenge. An extremely realistic explosive with traps, alarms, and a timer ticking down. One mistake and BOOM, you're dead. Make every second count! Sign ups on-site when the TEV begins.

Tamper-Evident King of the Hill; a full-featured tamper challenge. Tamper single items at your leisure and attempt to beat the current best. There can be only ONE! No sign ups required, play on-site when the TEV begins.

Badge Counterfeiting Contest; submit your best forgery of a DEF CON human badge. Other target badges are also available for those looking for more counterfeit fun!

For your viewing pleasure, collections of high-security tamper-evident seals from around the world.

Sit-down presentations & demonstrations on various aspects of tamper-evident seals and methods to defeat them.

Hands-on fun with adhesive seals, mechanical seals, envelopes, and evidence bags. Starts August 13, 2023 10:00 Ends August 13, 2023 14:00 Location Bloq, Linq

[Return to Index](#)

VMV - Voting Village

VMV Village: [Talk List](#)

DC Forums Page: <https://forum.defcon.org/node/245034>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733881148506164>

Location: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

Social Media Links:

TW [@votingvillagedc](#)

YT [link](#)



Voting Village

When:

Friday: 10:00 - 20:00

Saturday: 10:00 - 20:00

Sunday: 10:00 - 14:00

Where: 415-418, Forums

Twitter: [@VotingVillageDC](https://twitter.com/VotingVillageDC)

Voting Village is an interactive educational environment that provides the public with the unique opportunity to have a hands-on experience with our current Election Infrastructure. Attendees will be able to interact with multiple different types of voting systems, all of which are currently in use across the country today. Hackers will have the opportunity to test how secure these voting systems truly are, and will report to the Voting Village Lead's any vulnerabilities they find. Voting Village explores all aspects of election security and works to promote a more secure democracy. Attendees of Voting Village will also have access to Harri Hursti, the world's premier hacker and leading election and cyber security expert who has successfully hacked voting machines on multiple occasions. Aside from Harri, attendees will have the option of joining us for our speaker track (TALKS) that will take place every day except for the last Sunday of DEFCON. Our speaker track represents the most relevant government agencies and the top media outlets. Additionally, there will be multiple showings of Harri's HBO documentary, Kill Chain: The Cyber War on America's Elections. We will also have two Capture The Flags (CONTESTS) taking place throughout DEFCON. Starts August 13, 2023 10:00 Ends August 13, 2023 14:00 Location 415-418, Forums

[Return to Index](#)

WS - DEF CON Workshops

WS Village: [Talk List](#)

Home Page: <https://forum.defcon.org/node/244772>

XR V - XR Village

XR V Village: [Talk List](#)

Home Page: <https://xrvillage.org/>

DC Forums Page: <https://forum.defcon.org/node/245207>

Location: Caesars Forum - Summit - 206 - XR Village - [Map](#)

Social Media Links:

TW [@XR Village](#)

LI [@xr-village](#)



..

When:

Friday: 10:00 – 20:00

Saturday: 10:00 – 20:00

Sunday: 10:00 – 14:00

Where: Contest Area, Forums

Twitter: [@XR Village](#)

Website: <https://xrvillage.org/>

Augmented reality (AR), virtual reality (VR), collectively referred to extended reality (XR) technologies have the potential to revolutionize the way we interact with the world around us. However, as with any new technology, there are security and privacy concerns that must be addressed.

These concerns include data privacy, hacking of haptic hardware, software, and XR Infrastructure and public safety. In XR systems, personal information, such as location data and biometric information, can be collected and shared without the user's knowledge or consent.

Current XR development platforms for these technologies do not allow for built in security, safety, and privacy.

The XR Village was created to:

The Vision

To promote Security, Privacy, and Safety for XR software, hardware, and environments including the Metaverse, through awareness, education, policy and legal coordination, and exploitation and remediation of known and unknown vulnerabilities.

The Mission

Provide access to XR devices and applications for the security community for vulnerability testing; provide guidance & collaborative recommendations back to Policy makers, legislators, law enforcement, vendors, users, and the world on best Security, Privacy, and Safety practices in XR

At the Defcon31 XR Village hackers can expect expert XR security talks, policy and legal discussions, and a Hands-on Haptics Hackathon. XR devices will be on hand to demonstrate applications and environments such as BadVR w/Microsoft HoloLens (Example) showing virtual visibility to all surrounding WIFI networks via AR. They and others will show what is already being built in XR environments that may, or may not cross a line for privacy, safety, and security in the space. Specific breakout sessions will be available for hackers to discuss current efforts by XR Vendors to address security concerns.

Expert XR Security Talks will focus on exploitation of XR in the wild: What's been done and what's coming.

A Policy & Legislation panel of Global Governments and Law Enforcement Agencies will discuss challenges with current policies, and their limitations in enforcing privacy, safety, and security in XR. The panel will include a lengthy Q&A for hackers to present their thoughts.

Hackers will get their hands dirty with the Hands-On Haptics Hackathon. They will be given XR headsets within a test environment to identify specific vulnerabilities; with extra credit to anyone who finds new ones.

Hackers will have many different elements of XR to immerse themselves in, challenge their preconceptions of XR, and inspire them to learn more.

Starts August 13, 2023 10:00 Ends August 13, 2023 14:00 Location Contest Area, Forums

[Return to Index](#)

Talk/Event Schedule

Thursday

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

Thursday - 06:00 PDT

[Return to Index](#) - [Locations Legend](#)

MISC - Defcon.run -

Thursday - 07:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DC - Human Registration Open](#) -

[DC - Merch \(formerly swag\) Area Open -- README](#) -

[MISC - cont...\(06:00-11:59 PDT\)](#) - [Defcon.run](#) -

Thursday - 08:00 PDT

[Return to Index](#) - [Locations Legend](#)

[CON](#) - [Hac-Man](#) -

[DC](#) - cont...(07:00-18:59 PDT) - [Human Registration Open](#) -

[DC](#) - cont...(07:00-17:59 PDT) - [Merch \(formerly swag\) Area Open](#) -- [README](#) -

[MISC](#) - cont...(06:00-11:59 PDT) - [Defcon.run](#) -

[Return to Index](#) - [Locations Legend](#)

[CON](#) - cont...(08:00-11:59 PDT) - [Hac-Man](#) -

[DC](#) - cont...(07:00-18:59 PDT) - [Human Registration Open](#) -

[DC](#) - [Shell On Demand Appliance Machine \(S.O.D.A. Machine\) \(pronounced SODA\)](#) -

[DC](#) - cont...(07:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -

[HRV](#) - [Ham In A Day Class](#) - Dan KB6NU

[MISC](#) - cont...(06:00-11:59 PDT) - [Defcon.run](#) -

[WS](#) - [Protecting the AWS ecosystem - Misconfigurations, IAM, and Monitoring \(Pre-Registration Required\)](#) - Rodrigo Montoro

[WS](#) - [Applied Emulation - A Practical Approach to Emulating Malware \(Pre-Registration Required\)](#) - Sean Wilson, Sergei Frankoff

[WS](#) - [Hacking The Metal: An Intro to ARM Assembly Language Programming \(Pre-Registration Required\)](#) - Eigentourist

[WS](#) - [Pentesting Industrial Control Systems: OCP-U-HACK \(Pre-Registration Required\)](#) - Alexandrine Torrents, Arnaud Soullié

[WS](#) - [Introduction to Cryptographic Attacks \(Pre-Registration Required\)](#) - Matt Cheung

Thursday - 10:00 PDT

[Return to Index](#) - [Locations Legend](#)

[CON](#) - cont...(08:00-11:59 PDT) - [Hac-Man](#) -

[DC](#) - cont...(07:00-18:59 PDT) - [Human Registration Open](#) -

[DC](#) - [Boston Infinite Money Glitch: Hacking Transit Cards Without Ending Up In Handcuffs](#) - Matthew Harris,Noah Gibson,Scott Campbell,Zachary Bertocchi

[DC](#) - cont...(07:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -

[HRV](#) - cont...(09:00-17:59 PDT) - [Ham In A Day Class](#) - Dan KB6NU

[MISC](#) - cont...(06:00-11:59 PDT) - [Defcon.run](#) -

[MISC](#) - [CMD+CTRL at DEF CON 31 - Free Play](#) -

[SOC](#) - [Hack the Box Hack-a-thon](#) -

[SOC](#) - [Hack the Box Hack-a-thon](#) -

[WS](#) - cont...(09:00-12:59 PDT) - [Protecting the AWS ecosystem - Misconfigurations, IAM, and Monitoring \(Pre-Registration Required\)](#) - Rodrigo Montoro

[WS](#) - cont...(09:00-12:59 PDT) - [Applied Emulation - A Practical Approach to Emulating Malware \(Pre-Registration Required\)](#) - Sean Wilson,Sergei Frankoff

[WS](#) - cont...(09:00-12:59 PDT) - [Hacking The Metal: An Intro to ARM Assembly Language Programming \(Pre-Registration Required\)](#) - Eigentourist

[WS](#) - cont...(09:00-12:59 PDT) - [Pentesting Industrial Control Systems: OCP-U-HACK \(Pre-Registration Required\)](#) - Alexandrine Torrents,Arnaud Soullié

[WS](#) - cont...(09:00-12:59 PDT) - [Introduction to Cryptographic Attacks \(Pre-Registration Required\)](#) - Matt Cheung

Thursday - 11:00 PDT

[Return to Index](#) - [Locations Legend](#)

[CON](#) - cont...(08:00-11:59 PDT) - [Hac-Man](#) -

[DC](#) - cont...(07:00-18:59 PDT) - [Human Registration Open](#) -

[DC](#) - [UNConventional Cybercrime: How a Bad Anti-Hacking Treaty is Becoming a Law](#) - Bill Budington,Katitza Rodriguez

[DC](#) - (11:30-12:15 PDT) - [Cracking Cicada 3301: The Future of Collaborative Puzzle-Solving](#) -

Artorias,Puck,Taiwo,TheClockworkBird

[DC](#) - cont...(07:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -

[HRV](#) - cont...(09:00-17:59 PDT) - [Ham In A Day Class](#) - Dan KB6NU

[MISC](#) - cont...(06:00-11:59 PDT) - [Defcon.run](#) -

[MISC](#) - cont...(10:00-11:59 PDT) - [CMD+CTRL at DEF CON 31 - Free Play](#) -

[SOC](#) - cont...(10:00-17:59 PDT) - [Hack the Box Hack-a-thon](#) -

[SOC](#) - cont...(10:00-23:59 PDT) - [Hack the Box Hack-a-thon](#) -

[WS](#) - cont...(09:00-12:59 PDT) - [Protecting the AWS ecosystem - Misconfigurations, IAM, and Monitoring \(Pre-Registration Required\)](#) - Rodrigo Montoro

[WS](#) - cont...(09:00-12:59 PDT) - [Applied Emulation - A Practical Approach to Emulating Malware \(Pre-Registration Required\)](#) - Sean Wilson,Sergei Frankoff

[WS](#) - cont...(09:00-12:59 PDT) - [Hacking The Metal: An Intro to ARM Assembly Language Programming \(Pre-Registration Required\)](#) - Eigentourist

[WS](#) - cont...(09:00-12:59 PDT) - [Pentesting Industrial Control Systems: OCP-U-HACK \(Pre-Registration Required\)](#) - Alexandrine Torrents,Arnaud Soullié

[WS](#) - cont...(09:00-12:59 PDT) - [Introduction to Cryptographic Attacks \(Pre-Registration Required\)](#) - Matt Cheung

Thursday - 12:00 PDT

[Return to Index](#) - [Locations Legend](#)

DC - cont...(07:00-18:59 PDT) - [Human Registration Open](#) -

DC - cont...(11:30-12:15 PDT) - [Cracking Cicada 3301: The Future of Collaborative Puzzle-Solving](#) -

Artorias,Puck,Taiwo,TheClockworkBird

DC - (12:30-13:15 PDT) - [New Isn't Always Novel: Grep'ing Your Way to \\$20K at Pwn2Own, and How You Can Too](#) -

James Horseman,Zach Hanley

DC - cont...(07:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -

HRV - cont...(09:00-17:59 PDT) - [Ham In A Day Class](#) - Dan KB6NU

SOC - cont...(10:00-17:59 PDT) - [Hack the Box Hack-a-thon](#) -

SOC - [Friends of Bill W](#) -

SOC - cont...(10:00-23:59 PDT) - [Hack the Box Hack-a-thon](#) -

WS - cont...(09:00-12:59 PDT) - [Protecting the AWS ecosystem - Misconfigurations, IAM, and Monitoring \(Pre-Registration Required\)](#) - Rodrigo Montoro

WS - cont...(09:00-12:59 PDT) - [Applied Emulation - A Practical Approach to Emulating Malware \(Pre-Registration Required\)](#) - Sean Wilson,Sergei Frankoff

WS - cont...(09:00-12:59 PDT) - [Hacking The Metal: An Intro to ARM Assembly Language Programming \(Pre-Registration Required\)](#) - Eigentourist

WS - cont...(09:00-12:59 PDT) - [Pentesting Industrial Control Systems: OCP-U-HACK \(Pre-Registration Required\)](#) - Alexandrine Torrents,Arnaud Soullié

WS - cont...(09:00-12:59 PDT) - [Introduction to Cryptographic Attacks \(Pre-Registration Required\)](#) - Matt Cheung

Thursday - 13:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DC](#) - cont...(07:00-18:59 PDT) - [Human Registration Open](#) -

[DC](#) - cont...(12:30-13:15 PDT) - [New Isn't Always Novel: Grep'ing Your Way to \\$20K at Pwn2Own, and How You Can Too](#) - James Horseman,Zach Hanley

[DC](#) - (13:30-14:15 PDT) - [Damned if you do - The risks of pointing out the emperor is buck naked](#) - RenderMan,Thomas Dang

[DC](#) - cont...(07:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -

[HRV](#) - cont...(09:00-17:59 PDT) - [Ham In A Day Class](#) - Dan KB6NU

[SOC](#) - cont...(10:00-17:59 PDT) - [Hack the Box Hack-a-thon](#) -

[SOC](#) - cont...(10:00-23:59 PDT) - [Hack the Box Hack-a-thon](#) -

Thursday - 14:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DC](#) - cont...(07:00-18:59 PDT) - [Human Registration Open](#) -

[DC](#) - cont...(13:30-14:15 PDT) - [Damned if you do - The risks of pointing out the emperor is buck naked](#) -

[RenderMan](#),[Thomas Dang](#)

[DC](#) - (14:30-15:15 PDT) - [Designing RFID Implants - How flipping the bird opens doors for me](#) - [Miana Ella Windall](#)

[DC](#) - cont...(07:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -

[HRV](#) - cont...(09:00-17:59 PDT) - [Ham In A Day Class](#) - [Dan KB6NU](#)

[SOC](#) - [DEF CON Kids Meetup](#) -

[SOC](#) - cont...(10:00-17:59 PDT) - [Hack the Box Hack-a-thon](#) -

[SOC](#) - cont...(10:00-23:59 PDT) - [Hack the Box Hack-a-thon](#) -

[WS](#) - [DotNet Malware Analysis Masterclass \(Pre-Registration Required\)](#) - [Max 'Libra' Kersten](#)

[WS](#) - [These Port Scans are Trash: Improving Nmap by Writing New Scripts and Libraries \(Pre-Registration Required\)](#) - [Philip Young "Soldier of FORTRAN"](#)

[WS](#) - [Analysis 101 for Incident Responders \(Pre-Registration Required\)](#) - [Kristy Westphal](#)

[WS](#) - [Hide your kids, turn off your Wi-Fi, they Rogue APing up in here \(Pre-Registration Required\)](#) - [Daniel Costantini](#),[James Hawk](#),[Lander Beyer](#)

[WS](#) - [Flipping the Coin: Red and Blue Teaming in Windows Environments \(Pre-Registration Required\)](#) - [Angus "0x10f2c_" Strom](#),[Troy Defty](#)

Thursday - 15:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DC](#) - cont...(07:00-18:59 PDT) - [Human Registration Open](#) -

[DC](#) - cont...(14:30-15:15 PDT) - [Designing RFID Implants - How flipping the bird opens doors for me](#) - Miana Ella Windall

[DC](#) - (15:30-16:15 PDT) - [Nuthin But A G Thang: Evolution of Cellular Networks](#) - Tracy Mosley

[DC](#) - cont...(07:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -

[HRV](#) - cont...(09:00-17:59 PDT) - [Ham In A Day Class](#) - Dan KB6NU

[MISC](#) - [Toxic BBQ](#) -

[SOC](#) - cont...(14:00-15:59 PDT) - [DEF CON Kids Meetup](#) -

[SOC](#) - cont...(10:00-17:59 PDT) - [Hack the Box Hack-a-thon](#) -

[SOC](#) - cont...(10:00-23:59 PDT) - [Hack the Box Hack-a-thon](#) -

[WS](#) - cont...(14:00-17:59 PDT) - [DotNet Malware Analysis Masterclass \(Pre-Registration Required\)](#) - Max 'Libra' Kersten

[WS](#) - cont...(14:00-17:59 PDT) - [These Port Scans are Trash: Improving Nmap by Writing New Scripts and Libraries](#)

[\(Pre-Registration Required\)](#) - Philip Young "Soldier of FORTRAN"

[WS](#) - cont...(14:00-17:59 PDT) - [Analysis 101 for Incident Responders \(Pre-Registration Required\)](#) - Kristy Westphal

[WS](#) - cont...(14:00-17:59 PDT) - [Hide your kids, turn off your Wi-Fi, they Rogue APing up in here \(Pre-Registration](#)

[Required\)](#) - Daniel Costantini,James Hawk,Lander Beyer

[WS](#) - cont...(14:00-17:59 PDT) - [Flipping the Coin: Red and Blue Teaming in Windows Environments \(Pre-Registration](#)

[Required\)](#) - Angus "0x10f2c_" Strom,Troy Defty

Thursday - 16:00 PDT

[Return to Index](#) - [Locations Legend](#)

DC - cont...(07:00-18:59 PDT) - [Human Registration Open](#) -

DC - cont...(15:30-16:15 PDT) - [Nuthin But A G Thang: Evolution of Cellular Networks](#) - Tracy Mosley

DC - (16:30-16:50 PDT) - [Small Leaks, Billions Of Dollars: Practical Cryptographic Exploits That Undermine Leading Crypto Wallets](#) - Nikolaos Makriyannis,Oren Yomtov

DC - cont...(07:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -

HRV - cont...(09:00-17:59 PDT) - [Ham In A Day Class](#) - Dan KB6NU

MISC - [DDV open and accepting drives for duplication](#) -

MISC - cont...(15:00-20:59 PDT) - [Toxic BBQ](#) -

SOC - [Queercon Mixers](#) -

SOC - cont...(10:00-17:59 PDT) - [Hack the Box Hack-a-thon](#) -

SOC - cont...(10:00-23:59 PDT) - [Hack the Box Hack-a-thon](#) -

WS - cont...(14:00-17:59 PDT) - [DotNet Malware Analysis Masterclass \(Pre-Registration Required\)](#) - Max 'Libra' Kersten

WS - cont...(14:00-17:59 PDT) - [These Port Scans are Trash: Improving Nmap by Writing New Scripts and Libraries \(Pre-Registration Required\)](#) - Philip Young "Soldier of FORTRAN"

WS - cont...(14:00-17:59 PDT) - [Analysis 101 for Incident Responders \(Pre-Registration Required\)](#) - Kristy Westphal

WS - cont...(14:00-17:59 PDT) - [Hide your kids, turn off your Wi-Fi, they Rogue APing up in here \(Pre-Registration Required\)](#) - Daniel Costantini,James Hawk,Lander Beyer

WS - cont...(14:00-17:59 PDT) - [Flipping the Coin: Red and Blue Teaming in Windows Environments \(Pre-Registration Required\)](#) - Angus "0x10f2c_" Strom,Troy Defty

Thursday - 17:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DC](#) - cont...(07:00-18:59 PDT) - [Human Registration Open](#) -

[DC](#) - (17:30-18:45 PDT) - [DEF CON 101 - Welcome to DEF CON Panel](#) - Jeff "The Dark Tangent" Moss, fivepenny, Kirsten Renner, Magen, Nikita Kronenberg, deelo

[DC](#) - cont...(07:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -

[HRV](#) - cont...(09:00-17:59 PDT) - [Ham In A Day Class](#) - Dan KB6NU

[MISC](#) - cont...(16:00-18:59 PDT) - [DDV open and accepting drives for duplication](#) -

[MISC](#) - cont...(15:00-20:59 PDT) - [Toxic BBQ](#) -

[SOC](#) - cont...(16:00-17:59 PDT) - [Queercon Mixers](#) -

[SOC](#) - cont...(10:00-17:59 PDT) - [Hack the Box Hack-a-thon](#) -

[SOC](#) - [Friends of Bill W](#) -

[SOC](#) - cont...(10:00-23:59 PDT) - [Hack the Box Hack-a-thon](#) -

[WS](#) - cont...(14:00-17:59 PDT) - [DotNet Malware Analysis Masterclass \(Pre-Registration Required\)](#) - Max 'Libra' Kersten

[WS](#) - cont...(14:00-17:59 PDT) - [These Port Scans are Trash: Improving Nmap by Writing New Scripts and Libraries \(Pre-Registration Required\)](#) - Philip Young "Soldier of FORTRAN"

[WS](#) - cont...(14:00-17:59 PDT) - [Analysis 101 for Incident Responders \(Pre-Registration Required\)](#) - Kristy Westphal

[WS](#) - cont...(14:00-17:59 PDT) - [Hide your kids, turn off your Wi-Fi, they Rogue APing up in here \(Pre-Registration Required\)](#) - Daniel Costantini, James Hawk, Lander Beyer

[WS](#) - cont...(14:00-17:59 PDT) - [Flipping the Coin: Red and Blue Teaming in Windows Environments \(Pre-Registration Required\)](#) - Angus "0x10f2c_" Strom, Troy Defty

Thursday - 18:00 PDT

[Return to Index](#) - [Locations Legend](#)

DC - cont...(07:00-18:59 PDT) - [Human Registration Open](#) -

DC - cont...(17:30-18:45 PDT) - [DEF CON 101 - Welcome to DEF CON Panel](#) - Jeff "The Dark Tangent"

Moss,fivepenny,Kirsten Renner,Magen,Nikita Kronenberg,deelo

MISC - cont...(16:00-18:59 PDT) - [DDV open and accepting drives for duplication](#) -

MISC - cont...(15:00-20:59 PDT) - [Toxic BBQ](#) -

MUS - [Music Set / Entertainment \(Thursday, SYN Stage\)](#) - Bolonium,Deepblue,Dries,Dual Core,NPC Collective,Nina Lowe,PankleDank,The Icarus Kid

MUS - [Music Set / Entertainment \(Thursday, ACK Stage\)](#) - Alexi Husky,DJ Scythe,Delchi,Grind613,Syntax,Talk

Sinn,YTCracker,c0debreaker,matrix

SOC - cont...(10:00-23:59 PDT) - [Hack the Box Hack-a-thon](#) -

Thursday - 19:00 PDT

[Return to Index](#) - [Locations Legend](#)

[MISC](#) - cont...(15:00-20:59 PDT) - [Toxic BBQ](#) -

[SOC](#) - cont...(10:00-23:59 PDT) - [Hack the Box Hack-a-thon](#) -

Thursday - 20:00 PDT

[Return to Index](#) - [Locations Legend](#)

[MISC](#) - cont...(15:00-20:59 PDT) - [Toxic BBQ](#) -

[SOC](#) - cont...(10:00-23:59 PDT) - [Hack the Box Hack-a-thon](#) -

[Return to Index](#) - [Locations Legend](#)

[SOC - cont...\(10:00-23:59 PDT\)](#) - [Hack the Box Hack-a-thon](#) -

[Return to Index](#) - [Locations Legend](#)

[SOC - cont...\(10:00-23:59 PDT\)](#) - [Hack the Box Hack-a-thon](#) -

[Return to Index](#) - [Locations Legend](#)

[SOC - cont...\(10:00-23:59 PDT\)](#) - [Hack the Box Hack-a-thon](#) -

Friday

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

Friday - 06:00 PDT

[Return to Index - Locations Legend](#)

MISC - Defcon.run -

MISC - CycleOverride Defcon Bike Ride -

[Return to Index - Locations Legend](#)

MISC - cont...(06:00-11:59 PDT) - Defcon.run -

Friday - 08:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DC - Human Registration Open](#) -

[DC - Merch \(formerly swag\) Area Open -- README](#) -

[MISC - cont...\(06:00-11:59 PDT\)](#) - [Defcon.run](#) -

[SEV - \(08:30-17:59 PDT\)](#) - [SECV Village Open](#)

[SEV - \(08:30-17:30 PDT\)](#) - [SECV - Youth Challenge](#) -

Friday - 09:00 PDT

[Return to Index](#) - [Locations Legend](#)

[CON - HardWired](#) -

[CON - Social Engineering Community \(SEC\) Vishing Competition](#) -

[CON - Social Engineering Community \(SEC\) Youth Challenge](#) -

[DC - Growing the Community of AI Hackers with the Generative Red Team](#) - Austin Carson,Rumman Chowdhury,Sven Cattell

[DC - cont...\(08:00-19:59 PDT\) - Human Registration Open](#) -

[DC - The Internals of Veilid, a New Decentralized Application Framework](#) - Christien "DilDog" Rioux,Katelyn "Medus4" Bowden

[DC - Welcome to DEF CON 31](#) - Jeff "The Dark Tangent" Moss

[DC - \(09:30-10:15 PDT\) - Secretary of the Department of Homeland Security Alejandro Mayorkas](#) - Alejandro Mayorkas

[DC - Shell On Demand Appliance Machine \(S.O.D.A. Machine\) \(pronounced SODA\)](#) -

[DC - The Hackers, The Lawyers, And The Defense Fund](#) - Charley Snyder,Hannah Zhao,Harley Geiger,Kurt Opsahl,Miles McCain

[DC - cont...\(08:00-17:59 PDT\) - Merch \(formerly swag\) Area Open -- README](#) -

[MISC - cont...\(06:00-11:59 PDT\) - Defcon.run](#) -

[PHV - Honey Pot Workshop](#) -

[PHV - Wall of Sheep](#) -

[PHV - Build Your Own Botnet](#) -

[PHV - Linux Trainer Workshop](#) -

[PHV - NetworkOS: Be The Cloud](#) -

[PHV - RegEx Trainer](#) -

[PHV - Password Lab](#) -

[PHV - Fleet DefCon 31 Workshop](#) -

[PHV - Packet Inspector](#) -

[PHV - Packet Detective](#) -

[SEV - cont...\(08:30-17:59 PDT\) - SECV Village Open](#)

[SEV - cont...\(08:30-17:30 PDT\) - SECV - Youth Challenge](#) -

[WS - House of Heap Exploitation \(Pre-Registration Required\)](#) - Elizabeth St. Germain,Kenzie Dolan,Maxwell Dulin "Strikeout",Nathan Kirkland,Zachary Minneker

[WS - Getting into Trouble with Machine Learning Models \(Pre-Registration Required\)](#) - Robert Koehlmoos

[WS - Android App Hacking - Hacking for Good! \(Pre-Registration Required\)](#) - Kavia Venkatesh,Maria Uretsky,Olivier Tuchon,Sajjad "JJ" Arshad

[WS - Long Live the Empire: A C2 Workshop for Modern Red Teaming \(Pre-Registration Required\)](#) - Dylan "CyberStryke" Butler,Jake "Hubbl3" Krasnov,Kevin "Kent" Clark

[WS - Snakes on a Screen: Taming Offensive IronPython Techniques \(Pre-Registration Required\)](#) - Anthony "Coin" Rose,Gannon "Dorf" Gebauer,Vincent "Vinnybod" Rose

Friday - 10:00 PDT

[Return to Index - Locations Legend](#)

[AIV - AI Village Opening Remarks - AI Village Organizers](#)
[AIV - AI Village Generative Red Team Challenge -](#)
[AIV - \(10:15-10:59 PDT\) - AI Village Keynote: The last attempted AI revolution in security, and the next one - Joshua Saxe](#)
[APV - AppSec Village Keynote: From Camels to Collaboration, A Journey Through Technology AND Humans - Chris Roberts](#)
[ASV - Unmanned Aerial Systems – Platform Security -](#)
[ASV - The Challenge - Lockheed Martin -](#)
[ASV - A-ISAC CTF -](#)
[ASV - Bricks in the Air -](#)
[ASV - ARINC 615a CTF -](#)
[ASV - PTP Flight Challenge -](#)
[ASV - Ask Me Anything About Cybersecurity in Aerospace -](#)
[ASV - Hack The Airport -](#)
[BHV - Securing the Whole System: Corporal to Corporate - David Guffrey,Nina Alli,Rob Suárez](#)
[BHV - \(10:40-11:40 PDT\) - Time, Persistence, Patience - Michael "v3ga_hax" Aguilar](#)
[BICV - BIC Village Opening Keynote - John Threat](#)
[BTV - Blue Team Village Opening Ceremony -](#)
[BTV - \(10:30-11:30 PDT\) - Insider Threats \(InT\): Hindsight and Foresight - aviditas,plug](#)
[BTV - \(10:30-11:30 PDT\) - CTH 101: Part I & II - CerealKiller](#)
[BTV - \(10:30-11:30 PDT\) - IR Analysis: Part I & II - juju43](#)
[CLV - Cloud Village - Keynote - Ben "NahamSec" Sadeghipour](#)
[CLV - \(10:50-11:30 PDT\) - Evading Logging in the Cloud: Bypassing AWS CloudTrail - Nick Frichette](#)
[CON - cont...\(09:00-17:59 PDT\) - HardWired -](#)
[CON - \(10:30-17:59 PDT\) - Capture The Packet Preliminaries -](#)
[CON - IoT Village CTF -](#)
[CON - Hardware Hacking Village CTF -](#)
[CON - Hack-A-Sat 4 \(HAS4\) -](#)
[CON - 5n4ck3y -](#)
[CON - TeleChallenge -](#)
[CON - CMD+CTRL at DEF CON 31 - Booth Open -](#)
[CON - HackFortress -](#)
[CON - The Beverage Cooling Contraption Contest -](#)
[CON - Adversary Wars CTF -](#)
[CON - The Dark Tangent Look-Alike Contest -](#)
[CON - Battle of The Bots -](#)
[CON - Ham Radio Fox Hunting Contest -](#)
[CON - The Gold Bug Challenge -](#)
[CON - The Lonely Hard Drive -](#)
[CON - Tinfoil Hat Contest -](#)
[CON - Car Hacking Village CTF -](#)
[CON - IntelOps - Operation Spacewatch -](#)
[CON - venator aurum - A Treasure Hunt -](#)
[CON - It's In That Place Where I Put That Thing That Time -](#)
[CON - CrackMeIfYouCan -](#)
[CON - Maps of the digital lands -](#)
[CON - Darknet-NG -](#)
[CON - DC's Next Top Threat Model \(DCNTTM\) -](#)
[CON - Octopus Game -](#)
[CON - AutoDriving CTF -](#)
[CON - pTFS Presents: Mayhem Industries – Starphish -](#)
[CON - Trace Labs OSINT Search Party CTF - Sign-ups -](#)

CON - DEF CON Scavenger Hunt -
CON - DEFCON MUD DUMB TERMINAL EDITION -
CON - Dungeons@Defcon -
CON - Red Team CTF -
CON - ? Cube -
CON - Radio Frequency Capture the Flag -
CON - (10:30-17:59 PDT) - Blue Team Village CTF -
CON - Embedded CTF -
CON - cont...(09:00-10:59 PDT) - Social Engineering Community (SEC) Vishing Competition -
CON - cont...(09:00-17:59 PDT) - Social Engineering Community (SEC) Youth Challenge -
CON - Cloud Village CTF -
CON - CMD+CTRL at DEF CON 31 - Competition -
CON - DC Kubernetes Capture the Flag (CTF) -
CON - Radio Frequency Capture the Flag -
CPV - CPV Welcome - Day 1 - CPV Staff
CPV - (10:30-10:45 PDT) - Intro to Ciphers - CPV Staff
DC - Look Ma I'm the CEO! Real-Time Video and Audio Deep-Fake! - Gal Zror
DC - (10:30-11:15 PDT) - Route to bugs: Analyzing the security of BGP message parsing - Daniel dos Santos,Simon Guiot
DC - Vendor Area Open -
DC - cont...(08:00-19:59 PDT) - Human Registration Open -
DC - Contain Yourself: Staying Undetected Using the Windows Container Isolation Framework - Daniel Avinoam
DC - cont...(09:30-10:15 PDT) - Secretary of the Department of Homeland Security Alejandro Mayorkas - Alejandro Mayorkas
DC - (10:30-10:50 PDT) - Making The DEF CON 31 Badge - Mar Williams
DC - Exhibitor Area Open -
DC - The RingHopper Journey or How We Almost Zero-day'd the World - Benny Zeltser,Jonathan Lusky
DC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
DC - Contest Area Open
DC - A Different Uber Post Mortem - Joe Sullivan
DL - Vulnerable by Design: Unguard, The Insecure Cloud-Native Twitter Clone - Christoph Wedenig,Simon Ammer
DL - SucoshScanny - Mustafa Bilgici,Tibet Ögünç
DL - The Metasploit Framework - Spencer McIntyre
DL - T3SF (Technical TableTop Exercises Simulation Framework) - Federico Pacheco,Joaquin Lanfranconi
DL - Katalina - Gabi Cirlig
DL - Strix Interceptor - Lexie Thach
ESV - Embedded Systems Village Activities -
HHV - Soldering Skills Village Activities -
HHV - RoboSumo Play Time -
HHV - Hardware Hacking Rube Goldberg Machine -
HHV - Make Your Own Use -
IOTV - IoT Village Hacking Playground -
IOTV - Critical Infrastructure & IoT Exploitation -
IOTV - Secure or Surrender -
IOTV - The IoT Kill Zone -
IOTV - IoT Village Hardware Hacking Exercises 2023 -
IOTV - Embedded Device Security Workshops -
IOTV - Perform Memory Extraction, Emulation and Shellcode -
IOTV - Hardware Hacking Your Kitchen -
LPV - Lockpick Village Activities -
LPV - (10:15-10:45 PDT) - Intro to Lockpicking - TOOOL
MISC - DDV open and accepting drives for duplication -
MISC - cont...(06:00-11:59 PDT) - Defcon.run -
MIV - Opening Session of MisinfoVillage 2023 - Misinformation Village Staff
MIV - (10:30-10:59 PDT) - Teaching Information Warfare: Strategies in Academic and Government Institutions - Greg Carpenter

PHV - cont...(09:00-17:59 PDT) - [Honey Pot Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [Wall of Sheep](#) -
PHV - cont...(09:00-17:59 PDT) - [Build Your Own Botnet](#) -
PHV - cont...(09:00-17:59 PDT) - [Linux Trainer Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [NetworkOS: Be The Cloud](#) -
PHV - cont...(09:00-17:59 PDT) - [RegEx Trainer](#) -
PHV - cont...(09:00-17:59 PDT) - [Password Lab](#) -
PHV - cont...(09:00-17:59 PDT) - [Fleet DefCon 31 Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [Packet Inspector](#) -
PHV - cont...(09:00-17:59 PDT) - [Packet Detective](#) -
PHV - [Pwning the Pwners with Mindware](#) - Frank "D9" DiGiovanni
PLV - [Building the Hacker Talent Pipeline Through Workforce and Education Ecosystems](#) - Ashley Sequeira,Ayan Islam,Bryony Crown,Randy Pestana,Safa Shahwan Edwards,Sarah Powazek
PLV - [US Cyber Policy 101](#) - Harley Geiger,Lauren Zabierek,Lindsey Forson,Michaela Lee,Suzanne Schwartz
PSV - [Physical Security Village Activities](#) -
PWV - [Password Village Activities](#) -
QTV - [Quantum Village Opening!](#) - Mark Carney,Quantum Village Organizers,Victoria Kumaran
QTV - (10:30-10:59 PDT) - [QOLOSSUS - Quantum Capture the Flag Introduction!](#) - Quantum Quizmasters
RCV - [Keynote - Reshaping Reconnaissance: AI's Role in Open Source Intelligence](#) - Matt Edmondson
RCV - (10:50-11:35 PDT) - [OSINT Situational Awareness](#) - Joe Gray
SEV - cont...(08:30-17:59 PDT) - [SECV Village Open](#)
SEV - cont...(08:30-17:30 PDT) - [SECV - Youth Challenge](#) -
SOC - [Hacker Memorial](#) -
SOC - [DCG Meetups](#)
TCV - [Telecom Village Inauguration](#) - Harshit Mahajan
TEV - [Tamper Evident Village Activities](#) -
VMV - [Voting Village Opening Remarks](#) - Catherine Terranova,Harri Hursti,Matt Blaze
VMV - (10:30-11:25 PDT) - [A Global Perspective On Election Integrity](#) - Bryson Bort,Chris Krebs,Kendall Spencer,Maia Mazurkiewicz
WS - cont...(09:00-12:59 PDT) - [House of Heap Exploitation \(Pre-Registration Required\)](#) - Elizabeth St. Germain,Kenzie Dolan,Maxwell Dulin "Strikeout",Nathan Kirkland,Zachary Minneker
WS - cont...(09:00-12:59 PDT) - [Getting into Trouble with Machine Learning Models \(Pre-Registration Required\)](#) - Robert Koehlmoos
WS - cont...(09:00-12:59 PDT) - [Android App Hacking - Hacking for Good! \(Pre-Registration Required\)](#) - Kavia Venkatesh,Maria Uretsky,Olivier Tuchon,Sajjad "JJ" Arshad
WS - cont...(09:00-12:59 PDT) - [Long Live the Empire: A C2 Workshop for Modern Red Teaming \(Pre-Registration Required\)](#) - Dylan "CyberStryke" Butler,Jake "Hubbl3" Krasnov,Kevin "Kent" Clark
WS - cont...(09:00-12:59 PDT) - [Snakes on a Screen: Taming Offensive IronPython Techniques \(Pre-Registration Required\)](#) - Anthony "Coin" Rose,Gannon "Dorf" Gebauer,Vincent "Vinnybod" Rose
XRV - [Haptics Hack-a-Thon](#) -
XRV - [XR Village Playground](#) -

[AIV](#) - cont...(10:00-17:59 PDT) - [AI Village Generative Red Team Challenge](#) -
[AIV](#) - [AI Village CTF Kickoff and Introduction](#) - Will Pearce
[AIV](#) - (11:30-11:55 PDT) - [LLMs: Loose Lips Multipliers](#) - Kyle Easterly,Mitch Kitter
[APV](#) - [Generative Adversarial Network \(GAN\) based autonomous penetration testing for Web Applications](#) - Ankur Chowdhary
[APV](#) - (11:45-12:30 PDT) - [The attackers guide to exploiting secrets in the universe](#) - Mackenzie Jackson
[APV](#) - [Hands-on GitHub Actions](#) - Magno Logan
[APV](#) - [vAPI : Vulnerable Adversely Programmed Interface](#) - Tushar Kulkarni
[APV](#) - [Spot the True Positives!](#) - Backslash
[APV](#) - [The Ultimate AppSec Trivia Challenge](#) - Probely
[APV](#) - [Defensive Coding and Hardened Javascript](#) - Aaron Kumavis,Zbyszek Tenerowicz
[ASV](#) - cont...(10:00-17:59 PDT) - [Unmanned Aerial Systems – Platform Security](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [The Challenge - Lockheed Martin](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [A-ISAC CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [ARINC 615a CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [PTP Flight Challenge](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Ask Me Anything About Cybersecurity in Aerospace](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Hack The Airport](#) -
[ASV](#) - [Hack-A-Sat 4 Briefing](#) - Hack-A-Sat 4 Team
[BHV](#) - cont...(10:40-11:40 PDT) - [Time, Persistence, Patience](#) - Michael "v3ga_hax" Aguilar
[BICV](#) - [Cyber Hygiene: Security Awareness Training and Education](#) - Dontae Tyler
[BTV](#) - cont...(10:30-11:30 PDT) - [Insider Threats \(InT\): Hindsight and Foresight](#) - aviditas,plug
[BTV](#) - (11:30-12:30 PDT) - [Security Engineering for Adversarial Emulation and Red Teaming](#) - plug,sandw1ch
[BTV](#) - cont...(10:30-11:30 PDT) - [CTH 101: Part I & II](#) - CerealKiller
[BTV](#) - (11:30-12:30 PDT) - [IR 101: Part I, II, III](#) - ChocolateCoat,CountZ3r0,Cyb3rhawk
[BTV](#) - cont...(10:30-11:30 PDT) - [IR Analysis: Part I & II](#) - juju43
[BTV](#) - (11:30-12:30 PDT) - [CTH: \(n\)Map Exploration: A Great Time in Remote Destinations](#) - SamunoskeX
[CLV](#) - cont...(10:50-11:30 PDT) - [Evading Logging in the Cloud: Bypassing AWS CloudTrail](#) - Nick Frichette
[CLV](#) - (11:30-12:10 PDT) - [The Dark Playground of CI/CD: Attack Delivery by GitHub Actions](#) - Kiyohito Yamamoto,Yusuke Kubo
[CON](#) - cont...(09:00-17:59 PDT) - [HardWired](#) -
[CON](#) - cont...(10:30-17:59 PDT) - [Capture The Packet Preliminaries](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [IoT Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hardware Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hack-A-Sat 4 \(HAS4\)](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [5n4ck3y](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL at DEF CON 31 - Booth Open](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[CON](#) - cont...(10:00-13:59 PDT) - [The Beverage Cooling Contraption Contest](#) -
[CON](#) - cont...(10:00-16:59 PDT) - [Adversary Wars CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Dark Tangent Look-Alike Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Battle of The Bots](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Ham Radio Fox Hunting Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Gold Bug Challenge](#) -
[CON](#) - cont...(10:00-19:59 PDT) - [The Lonely Hard Drive](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Tinfoil Hat Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [IntelOps - Operation Spacewatch](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [venator aurum - A Treasure Hunt](#) -

CON - cont...(10:00-17:59 PDT) - [It's In That Place Where I Put That Thing That Time](#) -
 CON - cont...(10:00-17:59 PDT) - [CrackMelfYouCan](#) -
 CON - cont...(10:00-17:59 PDT) - [Maps of the digital lands](#) -
 CON - cont...(10:00-16:30 PDT) - [Darknet-NG](#) -
 CON - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\)](#) -
 CON - cont...(10:00-13:59 PDT) - [Octopus Game](#) -
 CON - cont...(10:00-17:59 PDT) - [AutoDriving CTF](#) -
 CON - cont...(10:00-19:59 PDT) - [pTFS Presents: Mayhem Industries – Starphish](#) -
 CON - cont...(10:00-17:59 PDT) - [Trace Labs OSINT Search Party CTF - Sign-ups](#) -
 CON - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
 CON - cont...(10:00-17:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -
 CON - cont...(10:00-17:59 PDT) - [Dungeons@Defcon](#) -
 CON - cont...(10:00-17:59 PDT) - [Red Team CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [? Cube](#) -
 CON - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
 CON - cont...(10:30-17:59 PDT) - [Blue Team Village CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [Embedded CTF](#) -
 CON - cont...(09:00-17:59 PDT) - [Social Engineering Community \(SEC\) Youth Challenge](#) -
 CON - (11:30-13:30 PDT) - [Social Engineering Community \(SEC\) Vishing Competition](#) -
 CON - cont...(10:00-17:59 PDT) - [Cloud Village CTF](#) -
 CON - cont...(10:00-11:59 PDT) - [CMD+CTRL at DEF CON 31 - Competition](#) -
 CON - cont...(10:00-19:59 PDT) - [DC Kubernetes Capture the Flag \(CTF\)](#) -
 CON - cont...(10:00-12:59 PDT) - [Radio Frequency Capture the Flag](#) -
 CPV - [Certs Fucking Suck, So We Made a Cert: DISCO for Bodily Autonomy](#) - Blunt,Daly
 DC - cont...(10:30-11:15 PDT) - [Route to bugs: Analyzing the security of BGP message parsing](#) - Daniel dos Santos,Simon Guiot
 DC - (11:30-12:15 PDT) - [Civil Cyber Defense: Use Your Resources to Defend Non-Profits as they Combat Human Trafficking and Subvert Authoritarian Regimes](#) - Austin Shamlin,Tiffany Rad
 DC - cont...(10:00-17:59 PDT) - [Vendor Area Open](#) -
 DC - cont...(08:00-19:59 PDT) - [Human Registration Open](#) -
 DC - [mTLS: when certificate authentication done wrong](#) - Michael Stepankin
 DC - (11:30-12:15 PDT) - [I Watched You Roll the Die: Unparalleled RDP Monitoring Reveal Attackers Tradecraft](#) - Andréanne Bergeron,Olivier Bilodeau
 DC - [SpamChannel: Spoofing Emails From 2 Million+ Domains and Virtually Becoming Satan](#) - Marcello "byt3bl33d3r" Salvati
 DC - cont...(10:00-17:59 PDT) - [Exhibitor Area Open](#) -
 DC - [Defending KA-SAT: The detailed story of the response, how it was analyzed, and what was learned](#) - Mark Colaluca,Nick Saunders
 DC - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
 DC - cont...(10:00-17:59 PDT) - [Contest Area Open](#)
 DC - [Warshopping - further dalliances in phreaking smart shopping cart wheels, RF sniffing and hardware reverse engineering](#) - Joseph Gabay
 DL - cont...(10:00-11:55 PDT) - [Vulnerable by Design: Unguard, The Insecure Cloud-Native Twitter Clone](#) - Christoph Wedenig,Simon Ammer
 DL - cont...(10:00-11:55 PDT) - [SucoshScanny](#) - Mustafa Bilgici,Tibet Ögünç
 DL - cont...(10:00-11:55 PDT) - [The Metasploit Framework](#) - Spencer McIntyre
 DL - cont...(10:00-11:55 PDT) - [T3SF \(Technical TableTop Exercises Simulation Framework\)](#) - Federico Pacheco,Joaquin Lanfranconi
 DL - cont...(10:00-11:55 PDT) - [Katalina](#) - Gabi Cirlig
 DL - cont...(10:00-11:55 PDT) - [Strix Interceptor](#) - Lexie Thach
 ESV - cont...(10:00-17:59 PDT) - [Embedded Systems Village Activities](#) -
 HHV - cont...(10:00-17:59 PDT) - [Soldering Skills Village Activities](#) -
 HHV - cont...(10:00-17:59 PDT) - [RoboSumo Play Time](#) -
 HHV - cont...(10:00-17:59 PDT) - [Hardware Hacking Rube Goldberg Machine](#) -
 HHV - cont...(10:00-17:59 PDT) - [Make Your Own Use](#) -

HHV - [The Creation Of The Out-Of-Band Anti Virus Dock \(Oobavd\)](#) - Bosen Zhang,Howard Yang,Pengfei “BigZaddy” Yu,Tan Jing Zhi

ICSV - [What's up, Doc? Using documentation to build better OT security knowledge graphs](#) - Ian Fox

ICSV - (11:30-11:59 PDT) - [Five \(or More\) Maritime Cybersecurity Challenges](#) - Gary C. Kessler

IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hacking Playground](#) -

IOTV - cont...(10:00-17:59 PDT) - [Critical Infrastructure & IoT Exploitation](#) -

IOTV - cont...(10:00-17:59 PDT) - [Secure or Surrender](#) -

IOTV - cont...(10:00-17:59 PDT) - [The IoT Kill Zone](#) -

IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hardware Hacking Exercises 2023](#) -

IOTV - cont...(10:00-17:59 PDT) - [Embedded Device Security Workshops](#) -

IOTV - cont...(10:00-17:59 PDT) - [Perform Memory Extraction, Emulation and Shellcode](#) -

IOTV - cont...(10:00-17:59 PDT) - [Hardware Hacking Your Kitchen](#) -

LPV - cont...(10:00-17:59 PDT) - [Lockpick Village Activities](#) -

MISC - [No Starch Press - Book Signing](#) - Bryson Payne, Go H*ck Yourself

MISC - cont...(10:00-16:59 PDT) - [DDV open and accepting drives for duplication](#) -

MISC - [DC's Next Top Threat Model \(DCNTTM\)](#) - BYODesign Registration -

MISC - cont...(06:00-11:59 PDT) - [Defcon.run](#) -

MISC - [EFF Benefit Poker Tournament at DEF CON 31 - Pre-tournament clinic](#) -

MIV - [Cutting through the noise: What you need to know are the real threats when it comes to AI](#) - Chloé Messdaghi

MIV - (11:30-12:30 PDT) - [If it looks like a duck... Russia's new MDM communication strategies on Social Media after the War in Ukraine](#) - Paula González Nagore

PHV - cont...(09:00-17:59 PDT) - [Honey Pot Workshop](#) -

PHV - cont...(09:00-17:59 PDT) - [Wall of Sheep](#) -

PHV - cont...(09:00-17:59 PDT) - [Build Your Own Botnet](#) -

PHV - cont...(09:00-17:59 PDT) - [Linux Trainer Workshop](#) -

PHV - cont...(09:00-17:59 PDT) - [NetworkOS: Be The Cloud](#) -

PHV - cont...(09:00-17:59 PDT) - [RegEx Trainer](#) -

PHV - cont...(09:00-17:59 PDT) - [Password Lab](#) -

PHV - cont...(09:00-17:59 PDT) - [Fleet DefCon 31 Workshop](#) -

PHV - cont...(09:00-17:59 PDT) - [Packet Inspector](#) -

PHV - cont...(09:00-17:59 PDT) - [Packet Detective](#) -

PHV - [Death by 1000 Likes: How Much Do You Really Leak in Social Media?](#) - Will Kay

PLV - cont...(10:00-11:50 PDT) - [Building the Hacker Talent Pipeline Through Workforce and Education Ecosystems](#) - Ashley Sequeira,Ayan Islam,Bryony Crown,Randy Pestana,Safa Shahwan Edwards,Sarah Powazek

PLV - cont...(10:00-11:50 PDT) - [US Cyber Policy 101](#) - Harley Geiger,Lauren Zabierek,Lindsey Forson,Michaela Lee,Suzanne Schwartz

PSV - cont...(10:00-17:59 PDT) - [Physical Security Village Activities](#) -

PWV - cont...(10:00-17:59 PDT) - [Password Village Activities](#) -

PYV - [Payment Village Workshop](#) - Leigh-Anne Galloway

PYV - [Payment Village Challenges/CTF](#) -

QTV - [No time for NISQy Business](#) - Rafal Janik

RCV - cont...(10:50-11:35 PDT) - [OSINT Situational Awareness](#) - Joe Gray

RCV - (11:35-12:10 PDT) - [Oh The Places You'll Guo: Using Media Variants to Trace the Organization and Behavior of an Coordinated Inauthentic Influence Operation](#) - Patrick Warren

RFV - [RF Village Kickoff](#)

RTV - [Stories from the Trenches](#) - Ben "NahamSec" Sadeghipour,Barrett Darnell,John Hammond,Ryan M. Montgomery,Savannah Lazzara

SEV - cont...(08:30-17:59 PDT) - [SECV Village Open](#)

SEV - cont...(08:30-17:30 PDT) - [SECV - Youth Challenge](#) -

SOC - cont...(10:00-17:59 PDT) - [Hacker Memorial](#) -

SOC - cont...(10:00-17:59 PDT) - [DCG Meetups](#)

TCV - [SS7 Workshop](#) - Akib Sayyed,Zibran Sayyed

TEV - cont...(10:00-17:59 PDT) - [Tamper Evident Village Activities](#) -

VMV - cont...(10:30-11:25 PDT) - [A Global Perspective On Election Integrity](#) - Bryson Bort,Chris Krebs,Kendall Spencer,Maia Mazurkiewicz

VMV - (11:30-12:20 PDT) - [Top 10 Hacks To Watch Out For From An Election Official](#) - John Odum
VMV - (11:30-11:59 PDT) - [VOTEC Corporation](#) - John Medcalf
VMV - (11:45-12:20 PDT) - [Surprise Unboxing](#) - Harri Hursti
WS - cont...(09:00-12:59 PDT) - [House of Heap Exploitation \(Pre-Registration Required\)](#) - Elizabeth St. Germain,Kenzie Dolan,Maxwell Dulin "Strikeout",Nathan Kirkland,Zachary Minneker
WS - cont...(09:00-12:59 PDT) - [Getting into Trouble with Machine Learning Models \(Pre-Registration Required\)](#) - Robert Koehlmoos
WS - cont...(09:00-12:59 PDT) - [Android App Hacking - Hacking for Good! \(Pre-Registration Required\)](#) - Kavia Venkatesh,Maria Uretsky,Olivier Tuchon,Sajjad "JJ" Arshad
WS - cont...(09:00-12:59 PDT) - [Long Live the Empire: A C2 Workshop for Modern Red Teaming \(Pre-Registration Required\)](#) - Dylan "CyberStryke" Butler,Jake "Hubbl3" Krasnov,Kevin "Kent" Clark
WS - cont...(09:00-12:59 PDT) - [Snakes on a Screen: Taming Offensive IronPython Techniques \(Pre-Registration Required\)](#) - Anthony "Coin" Rose,Gannon "Dorf" Gebauer,Vincent "Vinnobod" Rose
XRV - cont...(10:00-15:59 PDT) - [Haptics Hack-a-Thon](#) -
XRV - cont...(10:00-17:59 PDT) - [XR Village Playground](#) -
XRV - [Off the Rails: A demo with Pacific Northwest National Labs](#) -

[AIV - cont...\(10:00-17:59 PDT\) - AI Village Generative Red Team Challenge](#) -
[AIV - Assessing the Vulnerabilities of the Open-Source Artificial Intelligence \(AI\) Landscape: A Large-Scale Analysis of the Hugging Face Platform](#) - Adhishree Kathikar,Aishwarya Nair
[AIV - \(12:30-13:25 PDT\) - Not Just The Pickle: An Overview of Exploitable ML Serialization Formats](#) - Marta Janus
[APV - cont...\(11:45-12:30 PDT\) - The attackers guide to exploiting secrets in the universe](#) - Mackenzie Jackson
[APV - \(12:30-13:15 PDT\) - DevSecOps Worst Practices](#) - Tanya Janca
[APV - cont...\(11:00-12:59 PDT\) - Hands-on GitHub Actions](#) - Magno Logan
[APV - cont...\(11:00-12:59 PDT\) - vAPI : Vulnerable Adversely Programmed Interface](#) - Tushar Kulkarni
[APV - cont...\(11:00-12:59 PDT\) - Spot the True Positives!](#) - Backslash
[APV - cont...\(11:00-12:59 PDT\) - The Ultimate AppSec Trivia Challenge](#) - Probely
[APV - cont...\(11:00-12:59 PDT\) - Defensive Coding and Hardened Javascript](#) - Aaron Kumavis,Zbyszek Tenerowicz
[ASV - cont...\(10:00-17:59 PDT\) - Unmanned Aerial Systems – Platform Security](#) -
[ASV - cont...\(10:00-17:59 PDT\) - The Challenge - Lockheed Martin](#) -
[ASV - cont...\(10:00-17:59 PDT\) - A-ISAC CTF](#) -
[ASV - cont...\(10:00-17:59 PDT\) - Bricks in the Air](#) -
[ASV - cont...\(10:00-17:59 PDT\) - ARINC 615a CTF](#) -
[ASV - cont...\(10:00-17:59 PDT\) - PTP Flight Challenge](#) -
[ASV - cont...\(10:00-17:59 PDT\) - Ask Me Anything About Cybersecurity in Aerospace](#) -
[ASV - cont...\(10:00-17:59 PDT\) - Hack The Airport](#) -
[ASV - Secure Micropatching on the ISS](#) - Henry Haswell
[BTV - cont...\(11:30-12:30 PDT\) - Security Engineering for Adversarial Emulation and Red Teaming](#) - plug,sandw1ch
[BTV - cont...\(11:30-12:30 PDT\) - IR 101: Part I, II, III](#) - ChocolateCoat,CountZ3r0,Cyb3rhawk
[BTV - cont...\(11:30-12:30 PDT\) - CTH: \(n\)Map Exploration: A Great Time in Remote Destinations](#) - SamunoskeX
[CLV - cont...\(11:30-12:10 PDT\) - The Dark Playground of CI/CD: Attack Delivery by GitHub Actions](#) - Kiyohito Yamamoto,Yusuke Kubo
[CLV - From Service Catalog Admin to Account takeover: Privilege Escalation with Service Catalog Launch Constraint](#) - Sarachai Boonyakiat
[CLV - \(12:30-12:59 PDT\) - Attacks as a Service with The DeRF](#) - Kat Traxler
[CON - cont...\(09:00-17:59 PDT\) - HardWired](#) -
[CON - cont...\(10:30-17:59 PDT\) - Capture The Packet Preliminaries](#) -
[CON - Blacks in Cyber Village CTF](#) -
[CON - cont...\(10:00-17:59 PDT\) - IoT Village CTF](#) -
[CON - cont...\(10:00-17:59 PDT\) - Hardware Hacking Village CTF](#) -
[CON - cont...\(10:00-17:59 PDT\) - Hack-A-Sat 4 \(HAS4\)](#) -
[CON - cont...\(10:00-17:59 PDT\) - 5n4ck3y](#) -
[CON - cont...\(10:00-17:59 PDT\) - TeleChallenge](#) -
[CON - cont...\(10:00-17:59 PDT\) - CMD+CTRL at DEF CON 31 - Booth Open](#) -
[CON - cont...\(10:00-17:59 PDT\) - HackFortress](#) -
[CON - cont...\(10:00-13:59 PDT\) - The Beverage Cooling Contraption Contest](#) -
[CON - cont...\(10:00-16:59 PDT\) - Adversary Wars CTF](#) -
[CON - cont...\(10:00-17:59 PDT\) - The Dark Tangent Look-Alike Contest](#) -
[CON - cont...\(10:00-17:59 PDT\) - Battle of The Bots](#) -
[CON - cont...\(10:00-17:59 PDT\) - Ham Radio Fox Hunting Contest](#) -
[CON - cont...\(10:00-17:59 PDT\) - The Gold Bug Challenge](#) -
[CON - cont...\(10:00-19:59 PDT\) - The Lonely Hard Drive](#) -
[CON - cont...\(10:00-17:59 PDT\) - Tinfoil Hat Contest](#) -
[CON - cont...\(10:00-17:59 PDT\) - Car Hacking Village CTF](#) -
[CON - cont...\(10:00-17:59 PDT\) - IntelOps - Operation Spacewatch](#) -
[CON - cont...\(10:00-17:59 PDT\) - venator aurum - A Treasure Hunt](#) -
[CON - cont...\(10:00-17:59 PDT\) - It's In That Place Where I Put That Thing That Time](#) -
[CON - cont...\(10:00-17:59 PDT\) - CrackMelfYouCan](#) -

CON - cont...(10:00-17:59 PDT) - [Maps of the digital lands](#) -
 CON - cont...(10:00-16:30 PDT) - [Darknet-NG](#) -
 CON - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\)](#) -
 CON - cont...(10:00-13:59 PDT) - [Octopus Game](#) -
 CON - cont...(10:00-17:59 PDT) - [AutoDriving CTF](#) -
 CON - cont...(10:00-19:59 PDT) - [pTFS Presents: Mayhem Industries – Starphish](#) -
 CON - cont...(10:00-17:59 PDT) - [Trace Labs OSINT Search Party CTF - Sign-ups](#) -
 CON - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
 CON - cont...(10:00-17:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -
 CON - cont...(10:00-17:59 PDT) - [Dungeons@Defcon](#) -
 CON - cont...(10:00-17:59 PDT) - [Red Team CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [? Cube](#) -
 CON - [Red Alert ICS CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
 CON - cont...(10:30-17:59 PDT) - [Blue Team Village CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [Embedded CTF](#) -
 CON - cont...(09:00-17:59 PDT) - [Social Engineering Community \(SEC\) Youth Challenge](#) -
 CON - cont...(11:30-13:30 PDT) - [Social Engineering Community \(SEC\) Vishing Competition](#) -
 CON - cont...(10:00-17:59 PDT) - [Cloud Village CTF](#) -
 CON - cont...(10:00-19:59 PDT) - [DC Kubernetes Capture the Flag \(CTF\)](#) -
 CON - cont...(10:00-12:59 PDT) - [Radio Frequency Capture the Flag](#) -
 CPV - [Art vs AI: How Artists Hack Computer Vision Systems](#) - Kate
 CPV - (12:30-12:59 PDT) - [Practical advice for navigating edtech privacy](#) - Michelle Levesley
 DC - cont...(11:30-12:15 PDT) - [Civil Cyber Defense: Use Your Resources to Defend Non-Profits as they Combat Human Trafficking and Subvert Authoritarian Regimes](#) - Austin Shamlin,Tiffany Rad
 DC - (12:30-13:15 PDT) - [Defender-Pretender: When Windows Defender Updates Become a Security Risk](#) - Omer Attias,Tomer Bar
 DC - cont...(10:00-17:59 PDT) - [Vendor Area Open](#) -
 DC - cont...(08:00-19:59 PDT) - [Human Registration Open](#) -
 DC - cont...(11:30-12:15 PDT) - [I Watched You Roll the Die: Unparalleled RDP Monitoring Reveal Attackers Tradecraft](#) - Andréanne Bergeron,Olivier Bilodeau
 DC - (12:30-13:15 PDT) - [A Pain in the NAS: Exploiting Cloud Connectivity to PWN your NAS](#) - Noam Moshe,Sharon Brizinov
 DC - [Still Vulnerable Out of the Box: Revisiting the Security of Prepaid Android Carrier Devices](#) - Angelos Stavrou,Mohamed Elsabagh,Ryan Johnson
 DC - cont...(10:00-17:59 PDT) - [Exhibitor Area Open](#) -
 DC - [GhostToken: Exploiting Google Cloud Platform App Infrastructure to Create Unremovable Trojan Apps](#) - Tal Skverer
 DC - (12:30-13:15 PDT) - [Backdoor in the Core - Altering the Intel x86 Instruction Set at Runtime](#) - Alexander Dalsgaard Krog,Alexander Skovsende
 DC - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
 DC - cont...(10:00-17:59 PDT) - [Contest Area Open](#)
 DC - [Lonely Hackers Club - Resume Reviews & Career Advice](#)
 DC - [You're Not George Clooney, and This Isn't Ocean's Eleven](#) - Andrew "Spike" Brandt
 DL - [CNAPPGoat](#) - Igal Gofman,Noam Dahan
 DL - [Dracon](#) - Spyros Gasteratos
 DL - [Build Inspector - A modern Javert on the trail of CI/CD Anomalies and Intruders](#) - Jeremy Banker
 DL - [Ek47 – Payload Encryption with Environmental Keys](#) - Kevin “Kent” Clark,Skyler Knecht
 DL - [FlowMate](#) - Florian Haag,Nicolas Schickert
 DL - [Shufflecake, AKA Truecrypt on Steroids for Linux](#) - Elia Anzuoni,Tommaso "tomgag" Gagliardoni
 ESV - cont...(10:00-17:59 PDT) - [Embedded Systems Village Activities](#) -
 HHV - cont...(10:00-17:59 PDT) - [Soldering Skills Village Activities](#) -
 HHV - cont...(10:00-17:59 PDT) - [RoboSumo Play Time](#) -
 HHV - cont...(10:00-17:59 PDT) - [Hardware Hacking Rube Goldberg Machine](#) -
 HHV - cont...(10:00-17:59 PDT) - [Make Your Own Use](#) -
 HHV - [Introduction To Esp8266/Esp32 Microcontrollers And Building A Wi-Fi Deauthentication Detector](#) - Ryan Zagrodnik

ICSV - ICS Village - TSA Keynote - Tim Weston
 IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking Your Kitchen -
 IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
 IOTV - cont...(10:00-17:59 PDT) - Critical Infrastructure & IoT Exploitation -
 IOTV - cont...(10:00-17:59 PDT) - Secure or Surrender -
 IOTV - cont...(10:00-17:59 PDT) - The IoT Kill Zone -
 IOTV - cont...(10:00-17:59 PDT) - IoT Village Hardware Hacking Exercises 2023 -
 IOTV - cont...(10:00-17:59 PDT) - Embedded Device Security Workshops -
 IOTV - cont...(10:00-17:59 PDT) - Perform Memory Extraction, Emulation and Shellcode -
 LPV - cont...(10:00-17:59 PDT) - Lockpick Village Activities -
 LPV - The "Why" of Lock Picking - Christopher Forte
 MISC - No Starch Press - Book Signing - Joe Gray, Practical Social Engineering
 MISC - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -
 MISC - cont...(11:00-17:59 PDT) - DC's Next Top Threat Model (DCNTTM) - BYODesign Registration -
 MISC - EFF Benefit Poker Tournament at DEF CON 31 - Poker -
 MIV - cont...(11:30-12:30 PDT) - If it looks like a duck... Russia's new MDM communication strategies on Social Media after the War in Ukraine - Paula González Nagore
 MIV - (12:30-12:59 PDT) - Hackathon presentation - Misinformation Village Staff
 PHV - cont...(09:00-17:59 PDT) - Honey Pot Workshop -
 PHV - cont...(09:00-17:59 PDT) - Wall of Sheep -
 PHV - cont...(09:00-17:59 PDT) - Build Your Own Botnet -
 PHV - cont...(09:00-17:59 PDT) - Linux Trainer Workshop -
 PHV - cont...(09:00-17:59 PDT) - NetworkOS: Be The Cloud -
 PHV - cont...(09:00-17:59 PDT) - RegEx Trainer -
 PHV - cont...(09:00-17:59 PDT) - Password Lab -
 PHV - cont...(09:00-17:59 PDT) - Fleet DefCon 31 Workshop -
 PHV - cont...(09:00-17:59 PDT) - Packet Inspector -
 PHV - cont...(09:00-17:59 PDT) - Packet Detective -
 PHV - OSINT for Physical Security Intelligence - Chet Hosmer, Mike Raggo
 PLV - The Promise and Perils of Planetary-Scale ISPs - J. Scott Christianson
 PLV - It's Coming from Inside the House: Next Steps for Addressing U.S. Network Abuse - David Forscey, Emily Paull, Peter Su, Seth McKinnis, Thomas Klein
 PLV - International Cyber Policy 101 - Adam Dobell, Ari Schwartz, Bryony Crown, Peter Brown, Peter Stephens
 PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
 PSV - Lock Bypass 101 - Karen
 PSV - (12:30-12:59 PDT) - Lock Bypass 102 - Karen
 PWV - cont...(10:00-17:59 PDT) - Password Village Activities -
 PYV - cont...(11:00-12:30 PDT) - Payment Village Workshop - Leigh-Anne Galloway
 PYV - cont...(11:00-17:59 PDT) - Payment Village Challenges/CTF -
 QTV - World's Cheapest "QKD" ;) - QKD for fun and non-profit from home - Ben Varcoe, Jose Pisaro, Mark Carney
 RCV - cont...(11:35-12:10 PDT) - Oh The Places You'll Guo: Using Media Variants to Trace the Organization and Behavior of an Coordinated Inauthentic Influence Operation - Patrick Warren
 RCV - How I Found Your Password, and Other Advanced Data Hoarding Techniques - M4x 5yn74x
 RFV - The International Wigle Space Balloon - Lozaning
 RTV - Red Hot (Red Team TTPs) - Ralph May, Steve Borosh
 RTV - Build Your Own Cat-Shaped USB Hacking Tool! (with the Nugget) - Alex Lynd
 RTV - OSINT Skills Lab Challenge - Lee McWhorter, Sandra Stibbards
 RTV - An Introduction to SAML and its Security - Louis Nyffenegger
 RTV - IOCs + APTs = "Let's play a game!" - Hack your way through a hunt! - Leo Cruz
 RTV - Scripting OWASP Amass for a Customized Experience - Jeff Foley
 SEV - cont...(08:30-17:30 PDT) - SECV - Youth Challenge -
 SEV - cont...(08:30-17:59 PDT) - SECV Village Open
 SOC - WISP Chill Out Space with Refreshments -
 SOC - cont...(10:00-17:59 PDT) - Hacker Memorial -
 SOC - Lonely Hackers Club Meetup -

SOC - cont...(10:00-17:59 PDT) - DCG Meetups
SOC - Friends of Bill W -
SOC - HDA / Accessibility Area Open
SOC - HDA Community Meetups
TCV - cont...(11:00-12:59 PDT) - [SS7 Workshop](#) - Akib Sayyed,Zibran Sayyed
TEV - cont...(10:00-17:59 PDT) - [Tamper Evident Village Activities](#) -
VMV - cont...(11:30-12:20 PDT) - [Top 10 Hacks To Watch Out For From An Election Official](#) - John Odum
VMV - cont...(11:45-12:20 PDT) - [Surprise Unboxing](#) - Harri Hursti
VMV - (12:30-13:20 PDT) - [DISARM Workshop](#) - Charles Smith,Dan Meidenbauer
VMV - (12:30-13:15 PDT) - [Ghost in the \(Voting\) Machine: Failures in Election Software Supply Chain Security](#) - Ashlee Benge
WS - cont...(09:00-12:59 PDT) - [House of Heap Exploitation \(Pre-Registration Required\)](#) - Elizabeth St. Germain,Kenzie Dolan,Maxwell Dulin "Strikeout",Nathan Kirkland,Zachary Minneker
WS - cont...(09:00-12:59 PDT) - [Getting into Trouble with Machine Learning Models \(Pre-Registration Required\)](#) - Robert Koehlmoos
WS - cont...(09:00-12:59 PDT) - [Android App Hacking - Hacking for Good! \(Pre-Registration Required\)](#) - Kavia Venkatesh,Maria Uretsky,Olivier Tuchon,Sajjad "JJ" Arshad
WS - cont...(09:00-12:59 PDT) - [Long Live the Empire: A C2 Workshop for Modern Red Teaming \(Pre-Registration Required\)](#) - Dylan "CyberStryke" Butler,Jake "Hubbl3" Krasnov,Kevin "Kent" Clark
WS - cont...(09:00-12:59 PDT) - [Snakes on a Screen: Taming Offensive IronPython Techniques \(Pre-Registration Required\)](#) - Anthony "Coin" Rose,Gannon "Dorf" Gebauer,Vincent "Vinybod" Rose
XRV - cont...(10:00-15:59 PDT) - [Haptics Hack-a-Thon](#) -
XRV - cont...(10:00-17:59 PDT) - [XR Village Playground](#) -
XRV - cont...(11:00-16:59 PDT) - [Off the Rails: A demo with Pacific Northwest National Labs](#) -

Friday - 13:00 PDT

[Return to Index](#) - [Locations Legend](#)

[AIV - cont...\(10:00-17:59 PDT\) - AI Village Generative Red Team Challenge](#) -
[AIV - cont...\(12:30-13:25 PDT\) - Not Just The Pickle: An Overview of Exploitable ML Serialization Formats](#) - Marta Janus
[AIV - \(13:30-13:55 PDT\) - How NOT to Train your Hack Bot: Dos and Don'ts of Building Offensive GPTs](#) - Ari Herbert-Voss,Shane Caldwell
[APV - cont...\(12:30-13:15 PDT\) - DevSecOps Worst Practices](#) - Tanya Janca
[APV - \(13:15-13:59 PDT\) - The Dark Playground of CI/CD: Attack Delivery by GitHub Actions](#) - Kiyohito Yamamoto,Yusuke Kubo
[APV - AMA - Tib3rius](#) - Tib3rius
[APV - IDN-Squatting Detector](#) - Gal Bitensky
[APV - Fix The Flag: A Secure Programming Competition](#) - Pedram Hayati
[APV - The Ultimate AppSec Trivia Challenge](#) - Probely
[APV - Web Shells - What They Are And How To Hunt Them](#) - Joe Schottman
[ASV - cont...\(10:00-17:59 PDT\) - Unmanned Aerial Systems – Platform Security](#) -
[ASV - cont...\(10:00-17:59 PDT\) - The Challenge - Lockheed Martin](#) -
[ASV - cont...\(10:00-17:59 PDT\) - A-ISAC CTF](#) -
[ASV - cont...\(10:00-17:59 PDT\) - Bricks in the Air](#) -
[ASV - cont...\(10:00-17:59 PDT\) - ARINC 615a CTF](#) -
[ASV - cont...\(10:00-17:59 PDT\) - PTP Flight Challenge](#) -
[ASV - cont...\(10:00-17:59 PDT\) - Ask Me Anything About Cybersecurity in Aerospace](#) -
[ASV - cont...\(10:00-17:59 PDT\) - Hack The Airport](#) -
[ASV - Guarding the Galaxy: Ransomware Resilience in CubeSats](#) - Peter Hansen
[ASV - \(13:30-13:55 PDT\) - Moving Target Defense for Space Systems](#) - Chris Jenkins
[BHV - \(13:20-14:10 PDT\) - Making a Sick Badge](#) - Caleb Davis,Nathan Smith
[BICV - Artificial Intelligence and Race: Security or Surveillance?](#) - Fatou Sankare
[BTV - \(13:30-14:30 PDT\) - OT: Why OT Cybersecurity Engineers Drink So Much](#) - ThatDeadGuy
[BTV - \(13:30-14:30 PDT\) - IR 101: Part IV, V](#) - juju43
[BTV - \(13:30-14:30 PDT\) - Forensic Analysis: Part I & II](#) - Danny D. "B4nd1t0" Henderson Jr,Omenscan
[CLV - Identifying and securing Firebase vulnerabilities at scale](#) - Rojan Rijal
[CLV - \(13:25-14:05 PDT\) - Azure DevOps Security](#) - Viktor Gazdag
[CON - cont...\(09:00-17:59 PDT\) - HardWired](#) -
[CON - cont...\(10:30-17:59 PDT\) - Capture The Packet Preliminaries](#) -
[CON - cont...\(12:00-16:59 PDT\) - Blacks in Cyber Village CTF](#) -
[CON - cont...\(10:00-17:59 PDT\) - IoT Village CTF](#) -
[CON - cont...\(10:00-17:59 PDT\) - Hardware Hacking Village CTF](#) -
[CON - cont...\(10:00-17:59 PDT\) - Hack-A-Sat 4 \(HAS4\)](#) -
[CON - cont...\(10:00-17:59 PDT\) - 5n4ck3y](#) -
[CON - cont...\(10:00-17:59 PDT\) - TeleChallenge](#) -
[CON - cont...\(10:00-17:59 PDT\) - CMD+CTRL at DEF CON 31 - Booth Open](#) -
[CON - cont...\(10:00-17:59 PDT\) - HackFortress](#) -
[CON - cont...\(10:00-13:59 PDT\) - The Beverage Cooling Contraption Contest](#) -
[CON - cont...\(10:00-16:59 PDT\) - Adversary Wars CTF](#) -
[CON - cont...\(10:00-17:59 PDT\) - The Dark Tangent Look-Alike Contest](#) -
[CON - cont...\(10:00-17:59 PDT\) - Battle of The Bots](#) -
[CON - cont...\(10:00-17:59 PDT\) - Ham Radio Fox Hunting Contest](#) -
[CON - cont...\(10:00-17:59 PDT\) - The Gold Bug Challenge](#) -
[CON - cont...\(10:00-19:59 PDT\) - The Lonely Hard Drive](#) -
[CON - cont...\(10:00-17:59 PDT\) - Tinfoil Hat Contest](#) -
[CON - cont...\(10:00-17:59 PDT\) - Car Hacking Village CTF](#) -
[CON - cont...\(10:00-17:59 PDT\) - IntelOps - Operation Spacewatch](#) -
[CON - cont...\(10:00-17:59 PDT\) - venator aurum - A Treasure Hunt](#) -
[CON - cont...\(10:00-17:59 PDT\) - It's In That Place Where I Put That Thing That Time](#) -

CON - cont...(10:00-17:59 PDT) - [CrackMelfYouCan](#) -
 CON - cont...(10:00-17:59 PDT) - [Maps of the digital lands](#) -
 CON - cont...(10:00-16:30 PDT) - [Darknet-NG](#) -
 CON - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\)](#) -
 CON - cont...(10:00-13:59 PDT) - [Octopus Game](#) -
 CON - cont...(10:00-17:59 PDT) - [AutoDriving CTF](#) -
 CON - cont...(10:00-19:59 PDT) - [pTFS Presents: Mayhem Industries – Starphish](#) -
 CON - cont...(10:00-17:59 PDT) - [Trace Labs OSINT Search Party CTF - Sign-ups](#) -
 CON - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
 CON - cont...(10:00-17:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -
 CON - cont...(10:00-17:59 PDT) - [Dungeons@Defcon](#) -
 CON - cont...(10:00-17:59 PDT) - [Red Team CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [? Cube](#) -
 CON - cont...(12:00-16:59 PDT) - [Red Alert ICS CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
 CON - cont...(10:30-17:59 PDT) - [Blue Team Village CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [Embedded CTF](#) -
 CON - cont...(09:00-17:59 PDT) - [Social Engineering Community \(SEC\) Youth Challenge](#) -
 CON - cont...(11:30-13:30 PDT) - [Social Engineering Community \(SEC\) Vishing Competition](#) -
 CON - cont...(10:00-17:59 PDT) - [Cloud Village CTF](#) -
 CON - cont...(10:00-19:59 PDT) - [DC Kubernetes Capture the Flag \(CTF\)](#) -
 CPV - [Attacking Decentralized Identity](#) - Brent Zundel,Gabe Cohen
 DC - cont...(12:30-13:15 PDT) - [Defender-Pretender: When Windows Defender Updates Become a Security Risk](#) - Omer Attias,Tomer Bar
 DC - (13:30-14:15 PDT) - [Private Until Presumed Guilty](#) - Allison Young,Diane Akerman
 DC - cont...(10:00-17:59 PDT) - [Vendor Area Open](#) -
 DC - cont...(08:00-19:59 PDT) - [Human Registration Open](#) -
 DC - cont...(12:30-13:15 PDT) - [A Pain in the NAS: Exploiting Cloud Connectivity to PWN your NAS](#) - Noam Moshe,Sharon Brizinov
 DC - (13:30-14:15 PDT) - [Private Keys in Public Places](#) - Tom Pohl
 DC - [Over the Air, Under the Radar: Attacking and Securing the Pixel Modem](#) - Eugene Rodionov,Farzan Karimi,Xiling Gong,Xuan Xing
 DC - cont...(10:00-17:59 PDT) - [Exhibitor Area Open](#) -
 DC - cont...(12:30-13:15 PDT) - [Backdoor in the Core - Altering the Intel x86 Instruction Set at Runtime](#) - Alexander Dalsgaard Krog,Alexander Skovsende
 DC - (13:30-14:15 PDT) - [Fantastic Ethertypes and Where to Find Them](#) - Ricky "HeadlessZeke " Lawshae
 DC - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
 DC - cont...(10:00-17:59 PDT) - [Contest Area Open](#) -
 DC - cont...(12:00-13:59 PDT) - [Lonely Hackers Club - Resume Reviews & Career Advice](#) -
 DC - [Living Next Door to Russia](#) - Mikko Hypponen
 DDV - [What 10 years of drive stats data can tell us](#) - Andy Klein
 DL - cont...(12:00-13:55 PDT) - [CNAPPGoat](#) - Igal Gofman,Noam Dahan
 DL - cont...(12:00-13:55 PDT) - [Dracon](#) - Spyros Gasteratos
 DL - cont...(12:00-13:55 PDT) - [Build Inspector - A modern Javert on the trail of CI/CD Anomalies and Intruders](#) - Jeremy Banker
 DL - cont...(12:00-13:55 PDT) - [Ek47 – Payload Encryption with Environmental Keys](#) - Kevin “Kent” Clark,Skyler Knecht
 DL - cont...(12:00-13:55 PDT) - [FlowMate](#) - Florian Haag,Nicolas Schickert
 DL - cont...(12:00-13:55 PDT) - [Shufflecake, AKA Truecrypt on Steroids for Linux](#) - Elia Anzuoni,Tommaso "tomgag" Gagliardini
 ESV - cont...(10:00-17:59 PDT) - [Embedded Systems Village Activities](#) -
 HHV - cont...(10:00-17:59 PDT) - [Soldering Skills Village Activities](#) -
 HHV - cont...(10:00-17:59 PDT) - [RoboSumo Play Time](#) -
 HHV - cont...(10:00-17:59 PDT) - [Hardware Hacking Rube Goldberg Machine](#) -
 HHV - cont...(10:00-17:59 PDT) - [Make Your Own Use](#) -
 HHV - [Sadprotocol Goes To Hollywood: Hijacking An Ip Camera Stream As Seen In The Movies](#) - Javier Aguinaga,Octavio

Gianatiempo

HRV - [Amateur Radio Digital Modes Primer](#) - Jon Marler

ICSV - cont...(12:00-13:30 PDT) - [ICS Village - TSA Keynote](#) - Tim Weston

ICSV - (13:30-14:59 PDT) - [Open Distro of Malicious Maritime Hacking Tools: What Could Go Wrong?](#) - Austin Reid, Gary C. Kessler, Nina Kollars

IOTV - cont...(10:00-17:59 PDT) - [Hardware Hacking Your Kitchen](#) -

IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hacking Playground](#) -

IOTV - cont...(10:00-17:59 PDT) - [Critical Infrastructure & IoT Exploitation](#) -

IOTV - cont...(10:00-17:59 PDT) - [Secure or Surrender](#) -

IOTV - cont...(10:00-17:59 PDT) - [The IoT Kill Zone](#) -

IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hardware Hacking Exercises 2023](#) -

IOTV - cont...(10:00-17:59 PDT) - [Embedded Device Security Workshops](#) -

IOTV - cont...(10:00-17:59 PDT) - [Perform Memory Extraction, Emulation and Shellcode](#) -

LPV - cont...(10:00-17:59 PDT) - [Lockpick Village Activities](#) -

LPV - [Intro to Lockpicking](#) - TOOOL

MISC - No Starch Press - Book Signing - Craig Smith, The Car Hacker's Handbook

MISC - cont...(10:00-16:59 PDT) - [DDV open and accepting drives for duplication](#) -

MISC - cont...(11:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\) - BYODesign Registration](#) -

MISC - [Free Amateur Radio License Exams](#) -

MISC - cont...(12:00-17:59 PDT) - [EFF Benefit Poker Tournament at DEF CON 31 - Poker](#) -

MIV - [Dissecting Deception: The Role of Twitter in U.S. Political Discourse](#) - Travis Allen

MIV - (13:30-13:59 PDT) - [The Russian Playbook vs. the Chinese Little Red Playbook: Broadening our Understanding of Effective Disinformation Operations](#) - Darren Linvill

PHV - cont...(09:00-17:59 PDT) - [Honey Pot Workshop](#) -

PHV - cont...(09:00-17:59 PDT) - [Wall of Sheep](#) -

PHV - cont...(09:00-17:59 PDT) - [Build Your Own Botnet](#) -

PHV - cont...(09:00-17:59 PDT) - [Linux Trainer Workshop](#) -

PHV - cont...(09:00-17:59 PDT) - [NetworkOS: Be The Cloud](#) -

PHV - cont...(09:00-17:59 PDT) - [RegEx Trainer](#) -

PHV - cont...(09:00-17:59 PDT) - [Password Lab](#) -

PHV - cont...(09:00-17:59 PDT) - [Fleet DefCon 31 Workshop](#) -

PHV - cont...(09:00-17:59 PDT) - [Packet Inspector](#) -

PHV - cont...(09:00-17:59 PDT) - [Packet Detective](#) -

PLV - [Securing the Supply Chain](#) - Camille Stewart Gloster, Eric Goldstein

PLV - cont...(12:00-13:50 PDT) - [It's Coming from Inside the House: Next Steps for Addressing U.S. Network Abuse](#) - David Forscey, Emily Paull, Peter Su, Seth McKinnis, Thomas Klein

PLV - cont...(12:00-13:50 PDT) - [International Cyber Policy 101](#) - Adam Dobell, Ari Schwartz, Bryony Crown, Peter Brown, Peter Stephens

PSV - cont...(10:00-17:59 PDT) - [Physical Security Village Activities](#) -

PSV - (13:30-14:30 PDT) - [Access Control Vulnerabilities: Breaking Into Buildings With Computers](#) - Chad, Shortman

PWV - cont...(10:00-17:59 PDT) - [Password Village Activities](#) -

PYV - cont...(11:00-17:59 PDT) - [Payment Village Challenges/CTF](#) -

RFV - [WIFISHARK](#) - Wasabi

RTV - [Hunting & Exploiting DLL Sideloads](#) - Matthew Nickerson, Nick Swink

RTV - cont...(12:00-14:59 PDT) - [Build Your Own Cat-Shaped USB Hacking Tool! \(with the Nugget\)](#) - Alex Lynd

RTV - [OSINT Skills Lab Challenge](#) - Lee McWhorter, Sandra Stibbards

RTV - cont...(12:00-13:59 PDT) - [An Introduction to SAML and its Security](#) - Louis Nyffenegger

RTV - [AI-Driven Hacker's Toolkit: Using AI to Learn Python and Scapy for Exploitation and Post-Exploitation Techniques](#) - Omar Santos

RTV - cont...(12:00-13:59 PDT) - [Scripting OWASP Amass for a Customized Experience](#) - Jeff Foley

SEV - cont...(08:30-17:30 PDT) - [SECV - Youth Challenge](#) -

SEV - cont...(08:30-17:59 PDT) - [SECV Village Open](#)

SOC - cont...(12:00-15:59 PDT) - [WISP Chill Out Space with Refreshments](#) -

SOC - cont...(10:00-17:59 PDT) - [Hacker Memorial](#) -

SOC - cont...(12:00-17:59 PDT) - [Lonely Hackers Club Meetup](#) -

SOC - cont...(10:00-17:59 PDT) - DCG Meetups
SOC - cont...(12:00-17:59 PDT) - HDA / Accessibility Area Open
SOC - cont...(12:00-17:59 PDT) - HDA Community Meetups
TEV - cont...(10:00-17:59 PDT) - [Tamper Evident Village Activities](#) -
VMV - cont...(12:30-13:20 PDT) - [DISARM Workshop](#) - Charles Smith,Dan Meidenbauer
VMV - cont...(12:30-13:15 PDT) - [Ghost in the \(Voting\) Machine: Failures in Election Software Supply Chain Security](#) -
Ashlee Bengel
VMV - (13:20-14:05 PDT) - [Divided We Fall](#) - Michael Moore
VMV - (13:30-14:20 PDT) - [The Fallacy Of Privacy](#) - Antigone Peyton
XRV - cont...(10:00-15:59 PDT) - [Haptics Hack-a-Thon](#) -
XRV - cont...(10:00-17:59 PDT) - [XR Village Playground](#) -
XRV - cont...(11:00-16:59 PDT) - [Off the Rails: A demo with Pacific Northwest National Labs](#) -

[AIV - cont...\(10:00-17:59 PDT\) - AI Village Generative Red Team Challenge -](#)
[AIV - A Few Useful Lessons about AI Red Teaming - Ram Shankar Siva Kumar](#)
[APV - Living off the Land with Connectwise: How I Built An Attack Platform & Botnet in 23 lines of Python! - Ken Pyle](#)
[APV - cont...\(13:00-14:59 PDT\) - AMA - Tib3rius - Tib3rius](#)
[APV - cont...\(13:00-14:59 PDT\) - IDN-Squatting Detector - Gal Bitensky](#)
[APV - cont...\(13:00-14:59 PDT\) - Fix The Flag: A Secure Programming Competition - Pedram Hayati](#)
[APV - cont...\(13:00-14:59 PDT\) - The Ultimate AppSec Trivia Challenge - Probely](#)
[APV - cont...\(13:00-14:59 PDT\) - Web Shells - What They Are And How To Hunt Them - Joe Schottman](#)
[ASV - cont...\(10:00-17:59 PDT\) - Unmanned Aerial Systems – Platform Security -](#)
[ASV - cont...\(10:00-17:59 PDT\) - The Challenge - Lockheed Martin -](#)
[ASV - cont...\(10:00-17:59 PDT\) - A-ISAC CTF -](#)
[ASV - cont...\(10:00-17:59 PDT\) - Bricks in the Air -](#)
[ASV - cont...\(10:00-17:59 PDT\) - ARINC 615a CTF -](#)
[ASV - cont...\(10:00-17:59 PDT\) - PTP Flight Challenge -](#)
[ASV - cont...\(10:00-17:59 PDT\) - Ask Me Anything About Cybersecurity in Aerospace -](#)
[ASV - cont...\(10:00-17:59 PDT\) - Hack The Airport -](#)
[ASV - Orbiting the White House: Cybersecurity as a Space Imperative - Lauryn Williams,Tanya Simms](#)
[BHV - cont...\(13:20-14:10 PDT\) - Making a Sick Badge - Caleb Davis,Nathan Smith](#)
[BHV - Good Vibrations, Haptic Sensory Augmentation Implants - Quinn D. Mooney](#)
[BHV - \(14:40-15:59 PDT\) - FoldIt - Firas D Khatib](#)
[BTV - cont...\(13:30-14:30 PDT\) - OT: Why OT Cybersecurity Engineers Drink So Much - ThatDeadGuy](#)
[BTV - cont...\(13:30-14:30 PDT\) - IR 101: Part IV, V - juju43](#)
[BTV - cont...\(13:30-14:30 PDT\) - Forensic Analysis: Part I & II - Danny D. "B4nd1t0" Henderson Jr,Omenscan](#)
[CLV - cont...\(13:25-14:05 PDT\) - Azure DevOps Security - Viktor Gazdag](#)
[CLV - MetaHub Demo: Automating Ownership, Context, and Impact Assessment in Security Findings -](#)
[CLV - \(14:35-16:30 PDT\) - Infrastructure as Remote Code Execution - Michael McCabe](#)
[CON - cont...\(09:00-17:59 PDT\) - HardWired -](#)
[CON - cont...\(10:30-17:59 PDT\) - Capture The Packet Preliminaries -](#)
[CON - cont...\(12:00-16:59 PDT\) - Blacks in Cyber Village CTF -](#)
[CON - cont...\(10:00-17:59 PDT\) - IoT Village CTF -](#)
[CON - cont...\(10:00-17:59 PDT\) - Hardware Hacking Village CTF -](#)
[CON - cont...\(10:00-17:59 PDT\) - Hack-A-Sat 4 \(HAS4\) -](#)
[CON - cont...\(10:00-17:59 PDT\) - 5n4ck3y -](#)
[CON - cont...\(10:00-17:59 PDT\) - TeleChallenge -](#)
[CON - cont...\(10:00-17:59 PDT\) - CMD+CTRL at DEF CON 31 - Booth Open -](#)
[CON - cont...\(10:00-17:59 PDT\) - HackFortress -](#)
[CON - cont...\(10:00-16:59 PDT\) - Adversary Wars CTF -](#)
[CON - cont...\(10:00-17:59 PDT\) - The Dark Tangent Look-Alike Contest -](#)
[CON - cont...\(10:00-17:59 PDT\) - Battle of The Bots -](#)
[CON - cont...\(10:00-17:59 PDT\) - Ham Radio Fox Hunting Contest -](#)
[CON - cont...\(10:00-17:59 PDT\) - The Gold Bug Challenge -](#)
[CON - cont...\(10:00-19:59 PDT\) - The Lonely Hard Drive -](#)
[CON - cont...\(10:00-17:59 PDT\) - Tinfoil Hat Contest -](#)
[CON - cont...\(10:00-17:59 PDT\) - Car Hacking Village CTF -](#)
[CON - cont...\(10:00-17:59 PDT\) - IntelOps - Operation Spacewatch -](#)
[CON - cont...\(10:00-17:59 PDT\) - venator aurum - A Treasure Hunt -](#)
[CON - cont...\(10:00-17:59 PDT\) - It's In That Place Where I Put That Thing That Time -](#)
[CON - cont...\(10:00-17:59 PDT\) - CrackMelfYouCan -](#)
[CON - cont...\(10:00-17:59 PDT\) - Maps of the digital lands -](#)
[CON - cont...\(10:00-16:30 PDT\) - Darknet-NG -](#)
[CON - cont...\(10:00-17:59 PDT\) - DC's Next Top Threat Model \(DCNTTM\) -](#)

CON - cont...(10:00-17:59 PDT) - [AutoDriving CTF](#) -
 CON - cont...(10:00-19:59 PDT) - [pTFS Presents: Mayhem Industries – Starphish](#) -
 CON - cont...(10:00-17:59 PDT) - [Trace Labs OSINT Search Party CTF - Sign-ups](#) -
 CON - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
 CON - cont...(10:00-17:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -
 CON - cont...(10:00-17:59 PDT) - [Dungeons@Defcon](#) -
 CON - cont...(10:00-17:59 PDT) - [Red Team CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [? Cube](#) -
 CON - cont...(12:00-16:59 PDT) - [Red Alert ICS CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
 CON - cont...(10:30-17:59 PDT) - [Blue Team Village CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [Embedded CTF](#) -
 CON - cont...(09:00-17:59 PDT) - [Social Engineering Community \(SEC\) Youth Challenge](#) -
 CON - [Social Engineering Community \(SEC\) Vishing Competition](#) -
 CON - cont...(10:00-17:59 PDT) - [Cloud Village CTF](#) -
 CON - cont...(10:00-19:59 PDT) - [DC Kubernetes Capture the Flag \(CTF\)](#) -
 CPV - [Climate Change and its Implications for Security and Privacy: An Uncharted Territory](#) - Chloé Messdaghi
 DC - cont...(13:30-14:15 PDT) - [Private Until Presumed Guilty](#) - Allison Young,Diane Akerman
 DC - (14:30-15:15 PDT) - [Second Breakfast: Implicit and Mutation-Based Serialization Vulnerabilities in .NET](#) - Jonathan Birch
 DC - cont...(10:00-17:59 PDT) - [Vendor Area Open](#) -
 DC - cont...(08:00-19:59 PDT) - [Human Registration Open](#) -
 DC - cont...(13:30-14:15 PDT) - [Private Keys in Public Places](#) - Tom Pohl
 DC - [There are no mushroom clouds in cyberwar](#) - Mieke Eoyang
 DC - (14:30-14:50 PDT) - [DARPA Announces an AI Cyber Initiative, Live at DC 32 and DC 33](#) - Dave Weston,Heather Adkins,Matthew Knight,Michael Sellitto,Omkar Arasaratnam,Perri Adams,Vijay Bolina
 DC - cont...(10:00-17:59 PDT) - [Exhibitor Area Open](#) -
 DC - cont...(13:30-14:15 PDT) - [Fantastic Ethertypes and Where to Find Them](#) - Ricky "HeadlessZeke " Lawshae
 DC - (14:30-15:15 PDT) - [Getting a Migraine - uncovering a unique SIP bypass on macOS](#) - Anurag Bohra,Jonathan Bar Or,Michael Pearse
 DC - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
 DC - cont...(10:00-17:59 PDT) - [Contest Area Open](#)
 DC - [Lonely Hackers Club - Badgelife & Sticker Swap](#)
 DC - [Tracking the Worlds Dumbest Cyber-Mercenaries](#) - Cooper Quintin
 DC - (14:30-14:50 PDT) - ["You can't cheat time" - Finding foes and yourself with latency trilateration](#) - Lorenzo "lopoc" Cococcia
 DDV - cont...(13:00-14:59 PDT) - [What 10 years of drive stats data can tell us](#) - Andy Klein
 DL - [OWASP crAPI: Completely Ridiculous API](#) - Jayesh Ahire,Roshan Piyush
 DL - [OpenSSF Scorecard](#) - Naveen Srinivasan,Neil Naveen
 DL - [EvilnoVNC: Next-Gen Spear Phishing Attacks](#) - Joel Gámez Molina
 DL - [Attack Surface Framework](#) - Mike Henkelman,Prajwal Panchmahalkar
 DL - [Glyph](#) - Corey Hartman
 DL - [Vacuum Robot Hacking](#) - Dennis Giese
 ESV - cont...(10:00-17:59 PDT) - [Embedded Systems Village Activities](#) -
 HHV - cont...(10:00-17:59 PDT) - [Soldering Skills Village Activities](#) -
 HHV - cont...(10:00-17:59 PDT) - [RoboSumo Play Time](#) -
 HHV - cont...(10:00-17:59 PDT) - [Hardware Hacking Rube Goldberg Machine](#) -
 HHV - cont...(10:00-17:59 PDT) - [Make Your Own Use](#) -
 HHV - [Open Sesame! How To Open One Thousand And One Locks In The 21St Century?](#) - Thomas BYGODT
 ICSV - cont...(13:30-14:59 PDT) - [Open Distro of Malicious Maritime Hacking Tools: What Could Go Wrong?](#) - Austin Reid,Gary C. Kessler,Nina Kollars
 IOTV - cont...(10:00-17:59 PDT) - [Hardware Hacking Your Kitchen](#) -
 IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hacking Playground](#) -
 IOTV - cont...(10:00-17:59 PDT) - [Critical Infrastructure & IoT Exploitation](#) -
 IOTV - cont...(10:00-17:59 PDT) - [Secure or Surrender](#) -

IOTV - cont...(10:00-17:59 PDT) - [The IoT Kill Zone](#) -
IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hardware Hacking Exercises 2023](#) -
IOTV - cont...(10:00-17:59 PDT) - [Embedded Device Security Workshops](#) -
IOTV - cont...(10:00-17:59 PDT) - [Perform Memory Extraction, Emulation and Shellcode](#) -
LPV - cont...(10:00-17:59 PDT) - [Lockpick Village Activities](#) -
LPV - [Doors, Cameras, and Mantraps: Oh, my!](#) - Dylan Baklor
MISC - [No Starch Press - Book Signing - Travis Goodspeed, PoC or GTFO Volume 1, 2, & 3](#)
MISC - cont...(10:00-16:59 PDT) - [DDV open and accepting drives for duplication](#) -
MISC - cont...(11:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\) - BYODesign Registration](#) -
MISC - [DC's Next Top Threat Model \(DCNTTM\) - Kids - Learn Threat Modeling](#) -
MISC - cont...(13:00-15:59 PDT) - [Free Amateur Radio License Exams](#) -
MISC - cont...(12:00-17:59 PDT) - [EFF Benefit Poker Tournament at DEF CON 31 - Poker](#) -
MIV - [Holding Leaflets in the Left Hand and Bullets in the Right: A Guide to Understanding Modern Chinese Information Operations](#) - Kieran Green
MIV - (14:30-15:30 PDT) - [Be a Nerd that Talks Good: Up-leveling how we talk about misinformation, to build community trust and awareness](#) - Joel Bengé
PHV - cont...(09:00-17:59 PDT) - [Honey Pot Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [Wall of Sheep](#) -
PHV - cont...(09:00-17:59 PDT) - [Build Your Own Botnet](#) -
PHV - cont...(09:00-17:59 PDT) - [Linux Trainer Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [NetworkOS: Be The Cloud](#) -
PHV - cont...(09:00-17:59 PDT) - [RegEx Trainer](#) -
PHV - cont...(09:00-17:59 PDT) - [Password Lab](#) -
PHV - cont...(09:00-17:59 PDT) - [Fleet DefCon 31 Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [Packet Inspector](#) -
PHV - cont...(09:00-17:59 PDT) - [Packet Detective](#) -
PLV - [What are your thoughts on AI assisted voice cloning being used for scams?](#) - Christine Barker
PLV - [Cyber Policy Adrift – Charting a Path Forward for International Maritime Cybersecurity](#) - Blake Benson,Cliff Neve,Josh Reiter,Nina Kollars
PSV - cont...(10:00-17:59 PDT) - [Physical Security Village Activities](#) -
PSV - cont...(13:30-14:30 PDT) - [Access Control Vulnerabilities: Breaking Into Buildings With Computers](#) - Chad,Shortman
PSV - (14:30-15:30 PDT) - [Flipping Locks: Remote Badge Cloning with the Flipper Zero](#) - Dan,Langston "Shock" Clement
PWV - cont...(10:00-17:59 PDT) - [Password Village Activities](#) -
PYV - cont...(11:00-17:59 PDT) - [Payment Village Challenges/CTF](#) -
QTV - [Doomed to repeat the past: classical hardware exploits made quantum](#) - Jamie Friel
RCV - [Mastering OSINT: Advanced Techniques in the Realm of Big Data](#) - Seyfullah
RCV - (14:25-15:10 PDT) - [Leakonomics 101: The Last Year in Data Leaks](#) - Nick Ascoli
RFV - [Signals! In! Spaaaaaace!](#) - Ark (from WiGLE),wytshadow
RTV - [Hacking Web Apps and APIs with WebSploit Labs](#) - Omar Santos
RTV - cont...(12:00-14:59 PDT) - [Build Your Own Cat-Shaped USB Hacking Tool! \(with the Nugget\)](#) - Alex Lynd
RTV - [Open Source Intelligence \(OSINT\) for Hackers](#) - Lee McWhorter,Sandra Stibbards
RTV - [How to \[NOT\] look like a Red Team](#) - Michael Wylie
RTV - [How to prioritize Red Team Findings? Presenting CRTFSS: Common Red Team Findings Score System Ver. 1.0](#) - Guillermo Buendia
RTV - [Kubernetes Offense](#) - Michael Mitchell
SEV - cont...(08:30-17:30 PDT) - [SECV - Youth Challenge](#) -
SEV - cont...(08:30-17:59 PDT) - [SECV Village Open](#)
SOC - cont...(12:00-15:59 PDT) - [WISP Chill Out Space with Refreshments](#) -
SOC - cont...(10:00-17:59 PDT) - [Hacker Memorial](#) -
SOC - [Book Club Discussion and Exchange](#) -
SOC - cont...(12:00-17:59 PDT) - [Lonely Hackers Club Meetup](#) -
SOC - cont...(10:00-17:59 PDT) - [DCG Meetups](#)
SOC - cont...(12:00-17:59 PDT) - [HDA / Accessibility Area Open](#)
SOC - cont...(12:00-17:59 PDT) - [HDA Community Meetups](#)
TCV - (14:30-15:59 PDT) - [SS7 Workshop](#) - Akib Sayyed,Zibran Sayyed

TEV - cont...(10:00-17:59 PDT) - [Tamper Evident Village Activities](#) -
VMV - cont...(13:20-14:05 PDT) - [Divided We Fall](#) - Michael Moore
VMV - cont...(13:30-14:20 PDT) - [The Fallacy Of Privacy](#) - Antigone Peyton
VMV - [Risk Limiting Audits Of All Contests](#) - Amanda Glazer
VMV - (14:30-15:20 PDT) - [Building Partnerships](#) - Catherine Terranova, Maia Mazurkiewicz, Maria Bique, Sandra Khalil
VMV - (14:50-15:20 PDT) - [Understand Your Trust Assumptions!](#) - Carsten Schürmann
WS - [Machine Learning for N00bs \(Pre-Registration Required\)](#) - Elizabeth Biddlecome, Irvin Lemus, Kaitlyn Handelman, Sam Bowne
WS - [How hackers can send feedback directly to policymakers like the pros \(Pre-Registration Required\)](#) - Amit Elazari, Harley Geiger
WS - [Malware development on secured environment - Write, adapt, overcome \(Pre-Registration Required\)](#) - Yoann Dequeker
WS - [Learning to Hack Bluetooth Low Energy with BLE CTF \(Pre-Registration Required\)](#) - Ryan Holeman
WS - [Advanced WiFi Attacks for Red Team Professionals \(Pre-Registration Required\)](#) - Raúl "r4ulcl" Calvo Laorden
XRV - cont...(10:00-15:59 PDT) - [Haptics Hack-a-Thon](#) -
XRV - cont...(10:00-17:59 PDT) - [XR Village Playground](#) -
XRV - cont...(11:00-16:59 PDT) - [Off the Rails: A demo with Pacific Northwest National Labs](#) -

[AIV](#) - cont...(10:00-17:59 PDT) - [AI Village Generative Red Team Challenge](#) -
[APV](#) - [Finding bugs and scaling your security program with Semgrep](#) - Lewis Ardern
[APV](#) - [Threat modelling fun session with OWASP Cornucopia](#) - Spyros Gasteratos
[APV](#) - [How to Hide Behavior from Security Tools](#) - Mike Larkin
[APV](#) - [FlowMate and CSTC for Advanced Pentesting](#) - Florian Haag,Matthias Göhring
[APV](#) - [Hunt the Hacker - Detect compromises in your repositories!](#) - GitGuardian
[APV](#) - [Faking GitHub Contributions](#) - Alik Koldobsky,Tal Folkman
[ASV](#) - cont...(10:00-17:59 PDT) - [Unmanned Aerial Systems – Platform Security](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [The Challenge](#) - Lockheed Martin -
[ASV](#) - cont...(10:00-17:59 PDT) - [A-ISAC CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [ARINC 615a CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [PTP Flight Challenge](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Ask Me Anything About Cybersecurity in Aerospace](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Hack The Airport](#) -
[ASV](#) - [A Fireside Chat with the TSA Administrator](#) - David Pekoske,Steve Luczynski
[BHV](#) - cont...(14:40-15:59 PDT) - [FoldIt](#) - Firas D Khatib
[BICV](#) - [Career Workshop: New Career Seekers In Cybersecurity](#) - Keith Chapman
[BTV](#) - [SOC Panel: Finding, Keeping, and Caring for the Best People](#) - Alissa Torres,Carson Zimmerman,Christopher Crowley,Russ McRee
[CLV](#) - cont...(14:35-16:30 PDT) - [Infrastructure as Remote Code Execution](#) - Michael McCabe
[CON](#) - cont...(09:00-17:59 PDT) - [HardWired](#) -
[CON](#) - cont...(10:30-17:59 PDT) - [Capture The Packet Preliminaries](#) -
[CON](#) - cont...(12:00-16:59 PDT) - [Blacks in Cyber Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [IoT Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hardware Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hack-A-Sat 4 \(HAS4\)](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [5n4ck3y](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL at DEF CON 31 - Booth Open](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[CON](#) - cont...(10:00-16:59 PDT) - [Adversary Wars CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Dark Tangent Look-Alike Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Battle of The Bots](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Ham Radio Fox Hunting Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Gold Bug Challenge](#) -
[CON](#) - cont...(10:00-19:59 PDT) - [The Lonely Hard Drive](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Tinfoil Hat Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [IntelOps - Operation Spacewatch](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [venator aurum - A Treasure Hunt](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [It's In That Place Where I Put That Thing That Time](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CrackMelfYouCan](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Maps of the digital lands](#) -
[CON](#) - cont...(10:00-16:30 PDT) - [Darknet-NG](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\)](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [AutoDriving CTF](#) -
[CON](#) - cont...(10:00-19:59 PDT) - [pTFS Presents: Mayhem Industries – Starphish](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Trace Labs OSINT Search Party CTF - Sign-ups](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -

CON - cont...(10:00-17:59 PDT) - [Dungeons@Defcon](#) -
CON - cont...(10:00-17:59 PDT) - [Red Team CTF](#) -
CON - cont...(10:00-17:59 PDT) - [? Cube](#) -
CON - cont...(12:00-16:59 PDT) - [Red Alert ICS CTF](#) -
CON - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
CON - cont...(10:30-17:59 PDT) - [Blue Team Village CTF](#) -
CON - cont...(10:00-17:59 PDT) - [Embedded CTF](#) -
CON - cont...(09:00-17:59 PDT) - [Social Engineering Community \(SEC\) Youth Challenge](#) -
CON - cont...(14:00-16:59 PDT) - [Social Engineering Community \(SEC\) Vishing Competition](#) -
CON - cont...(10:00-17:59 PDT) - [Cloud Village CTF](#) -
CON - cont...(10:00-19:59 PDT) - [DC Kubernetes Capture the Flag \(CTF\)](#) -
CPV - [Privacy of Web PKI Revocation](#) - Matthew McPherrin
DC - cont...(14:30-15:15 PDT) - [Second Breakfast: Implicit and Mutation-Based Serialization Vulnerabilities in .NET](#) - Jonathan Birch
DC - (15:30-16:15 PDT) - [Game-Changing Advances in Windows Shellcode Analysis](#) - Bramwell Brizendine, Jake Hince, Max 'Libra' Kersten
DC - cont...(10:00-17:59 PDT) - [Vendor Area Open](#) -
DC - cont...(08:00-19:59 PDT) - [Human Registration Open](#) -
DC - (15:30-16:15 PDT) - [A Comprehensive Review on the Less-Traveled Road: 9 Years of Overlooked MikroTik Pre-Auth RCE](#) - NiNi Chen
DC - [Shall we play a game? Just because a Large Language Model speaks like a human, doesn't mean it can reason like one.](#) - Craig Martell
DC - cont...(10:00-17:59 PDT) - [Exhibitor Area Open](#) -
DC - cont...(14:30-15:15 PDT) - [Getting a Migraine - uncovering a unique SIP bypass on macOS](#) - Anurag Bohra, Jonathan Bar Or, Michael Pearse
DC - (15:30-16:15 PDT) - [Turning my virtual wallet into a skimming device: mPOS solutions](#) - Dan Borgogno, Ileana Barrionuevo
DC - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
DC - cont...(10:00-17:59 PDT) - [Contest Area Open](#)
DC - cont...(14:00-16:59 PDT) - [Lonely Hackers Club - Badgelife & Sticker Swap](#)
DC - [CON trolling the weather](#) - Paz Hameiri
DL - cont...(14:00-15:55 PDT) - [OWASP crAPI: Completely Ridiculous API](#) - Jayesh Ahire, Roshan Piyush
DL - cont...(14:00-15:55 PDT) - [OpenSSF Scorecard](#) - Naveen Srinivasan, Neil Naveen
DL - cont...(14:00-15:55 PDT) - [EvilnoVNC: Next-Gen Spear Phishing Attacks](#) - Joel Gámez Molina
DL - cont...(14:00-15:55 PDT) - [Attack Surface Framework](#) - Mike Henkelman, Prajwal Panchmahalkar
DL - cont...(14:00-15:55 PDT) - [Glyph](#) - Corey Hartman
DL - cont...(14:00-15:55 PDT) - [Vacuum Robot Hacking](#) - Dennis Giese
ESV - cont...(10:00-17:59 PDT) - [Embedded Systems Village Activities](#) -
HHV - cont...(10:00-17:59 PDT) - [Soldering Skills Village Activities](#) -
HHV - cont...(10:00-17:59 PDT) - [RoboSumo Play Time](#) -
HHV - cont...(10:00-17:59 PDT) - [Hardware Hacking Rube Goldberg Machine](#) -
HHV - cont...(10:00-17:59 PDT) - [Make Your Own Use](#) -
HHV - [Radiation Detection For The Rest Of Us - Diy Radiation Spectroscopy](#) - Patrick Kiley
HRV - [HF Radio Demonstration](#) - KitKat
ICSV - [Wired for Safety: Prioritizing Safety in Deadly Systems](#) - Jace Powell
ICSV - (15:30-15:59 PDT) - [OT Vulnerability analysis methodology](#) - Jeonghoon Bae
IOTV - cont...(10:00-17:59 PDT) - [Hardware Hacking Your Kitchen](#) -
IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hacking Playground](#) -
IOTV - cont...(10:00-17:59 PDT) - [Critical Infrastructure & IoT Exploitation](#) -
IOTV - cont...(10:00-17:59 PDT) - [Secure or Surrender](#) -
IOTV - cont...(10:00-17:59 PDT) - [The IoT Kill Zone](#) -
IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hardware Hacking Exercises 2023](#) -
IOTV - cont...(10:00-17:59 PDT) - [Embedded Device Security Workshops](#) -
IOTV - cont...(10:00-17:59 PDT) - [Perform Memory Extraction, Emulation and Shellcode](#) -
IOTV - (15:30-16:29 PDT) - [IoT Village - Free Book Signing with author Ted Harrington](#) -

LPV - cont...(10:00-17:59 PDT) - [Lockpick Village Activities](#) -
 LPV - [How to Lose Access to your Door in Two Easy Steps](#) - jos weyers
 MISC - No Starch Press - Book Signing - Nick Aleks & Dolev Farhi, Black Hat GraphQL
 MISC - cont...(10:00-16:59 PDT) - [DDV open and accepting drives for duplication](#) -
 MISC - cont...(11:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\) - BYODesign Registration](#) -
 MISC - cont...(14:00-15:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\) - Kids - Learn Threat Modeling](#) -
 MISC - cont...(13:00-15:59 PDT) - [Free Amateur Radio License Exams](#) -
 MISC - cont...(12:00-17:59 PDT) - [EFF Benefit Poker Tournament at DEF CON 31 - Poker](#) -
 MIV - cont...(14:30-15:30 PDT) - [Be a Nerd that Talks Good: Up-leveling how we talk about misinformation, to build community trust and awareness](#) - Joel Bengé
 MIV - (15:30-16:30 PDT) - [Digital Media Authentication - A Toolkit for Journalists in the Fight Against Misinformation with Cryptographic Tools](#) - Adam Rose
 PHV - cont...(09:00-17:59 PDT) - [Honey Pot Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [Wall of Sheep](#) -
 PHV - cont...(09:00-17:59 PDT) - [Build Your Own Botnet](#) -
 PHV - cont...(09:00-17:59 PDT) - [Linux Trainer Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [NetworkOS: Be The Cloud](#) -
 PHV - cont...(09:00-17:59 PDT) - [RegEx Trainer](#) -
 PHV - cont...(09:00-17:59 PDT) - [Password Lab](#) -
 PHV - cont...(09:00-17:59 PDT) - [Fleet DefCon 31 Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [Packet Inspector](#) -
 PHV - cont...(09:00-17:59 PDT) - [Packet Detective](#) -
 PLV - [Blocking Pathways into Cybercrime: Current Efforts and Future Opportunities](#) - Greg Francis,Jonathan Lusthaus,Marcia Hofmann,Marcus Hutchins,Will McKeen
 PLV - [A global approach to tackling software resilience](#) - Allan Friedman,Camille Stewart Gloster,Charlie Gladstone,David Rogers
 PSV - cont...(10:00-17:59 PDT) - [Physical Security Village Activities](#) -
 PSV - cont...(14:30-15:30 PDT) - [Flipping Locks: Remote Badge Cloning with the Flipper Zero](#) - Dan,Langston "Shock" Clement
 PSV - (15:30-16:30 PDT) - [Deep Diving Into HID Vulnerabilities: Heart of Darkness](#) - Chad,Shortman
 PWV - cont...(10:00-17:59 PDT) - [Password Village Activities](#) -
 PYV - cont...(11:00-17:59 PDT) - [Payment Village Challenges/CTF](#) -
 QTV - [Hacking Quantum Advantage for Classical Processes; Intro to Quantum-Inspired Use Cases](#) - Konstantinos Karagiannis
 RCV - cont...(14:25-15:10 PDT) - [Leakonomics 101: The Last Year in Data Leaks](#) - Nick Ascoli
 RCV - [Getting ahead of the bad guys with Internet Scanning data.](#) - Vitor Ventura
 RCV - (15:45-16:30 PDT) - [Crushing crumbs of information to eat a whole cake.](#) - Felipe Pr0teus
 RFV - [Protocol Identification for Integration](#) - Eric Escobar
 RTV - [Hacking Web Apps and APIs with WebSploit Labs](#) - Omar Santos
 RTV - [Red Hot \(Red Team TTPs\)](#) - Ralph May,Steve Borosh
 RTV - cont...(14:00-15:59 PDT) - [Open Source Intelligence \(OSINT\) for Hackers](#) - Lee McWhorter,Sandra Stibbards
 RTV - cont...(14:00-15:59 PDT) - [How to \[NOT\] look like a Red Team](#) - Michael Wylie
 RTV - [SSH Tunneling: Evading Network Detection and Creating Proxies](#) - Cory Wolff
 RTV - cont...(14:00-16:59 PDT) - [Kubernetes Offense](#) - Michael Mitchell
 SEV - cont...(08:30-17:30 PDT) - [SECV - Youth Challenge](#) -
 SEV - cont...(08:30-17:59 PDT) - [SECV Village Open](#)
 SOC - cont...(12:00-15:59 PDT) - [WISP Chill Out Space with Refreshments](#) -
 SOC - cont...(10:00-17:59 PDT) - [Hacker Memorial](#) -
 SOC - cont...(14:00-15:59 PDT) - [Book Club Discussion and Exchange](#) -
 SOC - cont...(12:00-17:59 PDT) - [Lonely Hackers Club Meetup](#) -
 SOC - cont...(10:00-17:59 PDT) - [DCG Meetups](#)
 SOC - cont...(12:00-17:59 PDT) - [HDA / Accessibility Area Open](#)
 SOC - cont...(12:00-17:59 PDT) - [HDA Community Meetups](#)
 TCV - cont...(14:30-15:59 PDT) - [SS7 Workshop](#) - Akib Sayyed,Zibran Sayyed
 TEV - cont...(10:00-17:59 PDT) - [Tamper Evident Village Activities](#) -

VMV - cont...(14:30-15:20 PDT) - [Building Partnerships](#) - Catherine Terranova, Maia Mazurkiewicz, Maria Bique, Sandra Khalil

VMV - cont...(14:50-15:20 PDT) - [Understand Your Trust Assumptions!](#) - Carsten Schürmann

VMV - (15:30-16:15 PDT) - [What Makes Hackers Extraordinary - It's A Gift!](#) - D9

VMV - (15:30-16:15 PDT) - [RLA Workshop](#) - Amanda Glazer

WS - cont...(14:00-17:59 PDT) - [Machine Learning for N00bs \(Pre-Registration Required\)](#) - Elizabeth Biddlecome, Irvin Lemus, Kaitlyn Handelman, Sam Bowne

WS - cont...(14:00-17:59 PDT) - [How hackers can send feedback directly to policymakers like the pros \(Pre-Registration Required\)](#) - Amit Elazari, Harley Geiger

WS - cont...(14:00-17:59 PDT) - [Malware development on secured environment - Write, adapt, overcome \(Pre-Registration Required\)](#) - Yoann Dequeker

WS - cont...(14:00-17:59 PDT) - [Learning to Hack Bluetooth Low Energy with BLE CTF \(Pre-Registration Required\)](#) - Ryan Holeman

WS - cont...(14:00-17:59 PDT) - [Advanced WiFi Attacks for Red Team Professionals \(Pre-Registration Required\)](#) - Raúl "r4ulcl" Calvo Laorden

XRV - cont...(10:00-15:59 PDT) - [Haptics Hack-a-Thon](#) -

XRV - cont...(10:00-17:59 PDT) - [XR Village Playground](#) -

XRV - cont...(11:00-16:59 PDT) - [Off the Rails: A demo with Pacific Northwest National Labs](#) -

XRV - [Securing Critical Versions of your Reality](#) - Bryson Bort, Keenan Skelly, Suzanne Borders

Friday - 16:00 PDT

[Return to Index](#) - [Locations Legend](#)

[AIV](#) - cont...(10:00-17:59 PDT) - [AI Village Generative Red Team Challenge](#) -
[AIV](#) - [Unveiling the Secrets: Breaking into AI/ML Security Bug Bounty Hunting](#) - Chloé Messdaghi,Daniel Miessler,Joseph Thacker,Marcello "byt3bl33d3r" Salvati
[APV](#) - cont...(15:00-16:59 PDT) - [Finding bugs and scaling your security program with Semgrep](#) - Lewis Ardern
[APV](#) - cont...(15:00-16:59 PDT) - [Threat modelling fun session with OWASP Cornucopia](#) - Spyros Gasteratos
[APV](#) - cont...(15:00-16:59 PDT) - [How to Hide Behavior from Security Tools](#) - Mike Larkin
[APV](#) - cont...(15:00-16:59 PDT) - [FlowMate and CSTC for Advanced Pentesting](#) - Florian Haag,Matthias Göhring
[APV](#) - cont...(15:00-16:59 PDT) - [Hunt the Hacker - Detect compromises in your repositories!](#) - GitGuardian
[APV](#) - cont...(15:00-16:59 PDT) - [Faking GitHub Contributions](#) - Alik Koldobsky,Tal Folkman
[ASV](#) - cont...(10:00-17:59 PDT) - [Unmanned Aerial Systems – Platform Security](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [The Challenge - Lockheed Martin](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [A-ISAC CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [ARINC 615a CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [PTP Flight Challenge](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Ask Me Anything About Cybersecurity in Aerospace](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Hack The Airport](#) -
[ASV](#) - [Transportation Screening Equipment Cybersecurity Briefing](#) - Edam Colón
[BHV](#) - [Can I put my DNA on the blockchain, mom?](#) - Anne Kim,Michele Orrù
[BHV](#) - (16:30-17:20 PDT) - [My CPAP has a recall, lets open it instead!](#) - José Fernández
[BICV](#) - [Are you really eyeing my network? Network Reconnaissance for n00bs!](#) - RJ McCarley
[BTV](#) - [Monroeville Live: An IR Tabletop for the Rest of Us](#) - Dave Collins,Gwyddia,Litmoose,Matt Mahler,Nathan Case,Nina Alli,Shea Nangle
[CHV](#) - [Redeploying the Same Vulnerabilities: Exploiting Wireless Side-Channels in Electric Vehicle Charging Protocols](#) - Richard Baker,Sebastian Kohler
[CLV](#) - cont...(14:35-16:30 PDT) - [Infrastructure as Remote Code Execution](#) - Michael McCabe
[CON](#) - cont...(09:00-17:59 PDT) - [HardWired](#) -
[CON](#) - cont...(10:30-17:59 PDT) - [Capture The Packet Preliminaries](#) -
[CON](#) - cont...(12:00-16:59 PDT) - [Blacks in Cyber Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [IoT Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hardware Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hack-A-Sat 4 \(HAS4\)](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [5n4ck3y](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL at DEF CON 31 - Booth Open](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[CON](#) - cont...(10:00-16:59 PDT) - [Adversary Wars CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Dark Tangent Look-Alike Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Battle of The Bots](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Ham Radio Fox Hunting Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Gold Bug Challenge](#) -
[CON](#) - cont...(10:00-19:59 PDT) - [The Lonely Hard Drive](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Tinfoil Hat Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [IntelOps - Operation Spacewatch](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [venator aurum - A Treasure Hunt](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [It's In That Place Where I Put That Thing That Time](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CrackMelfYouCan](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Maps of the digital lands](#) -
[CON](#) - cont...(10:00-16:30 PDT) - [Darknet-NG](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\)](#) -

CON - cont...(10:00-17:59 PDT) - [AutoDriving CTF](#) -
CON - cont...(10:00-19:59 PDT) - [pTFS Presents: Mayhem Industries – Starphish](#) -
CON - cont...(10:00-17:59 PDT) - [Trace Labs OSINT Search Party CTF - Sign-ups](#) -
CON - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
CON - cont...(10:00-17:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -
CON - cont...(10:00-17:59 PDT) - [Dungeons@Defcon](#) -
CON - cont...(10:00-17:59 PDT) - [Red Team CTF](#) -
CON - cont...(10:00-17:59 PDT) - [? Cube](#) -
CON - cont...(12:00-16:59 PDT) - [Red Alert ICS CTF](#) -
CON - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
CON - cont...(10:30-17:59 PDT) - [Blue Team Village CTF](#) -
CON - cont...(10:00-17:59 PDT) - [Embedded CTF](#) -
CON - cont...(09:00-17:59 PDT) - [Social Engineering Community \(SEC\) Youth Challenge](#) -
CON - cont...(14:00-16:59 PDT) - [Social Engineering Community \(SEC\) Vishing Competition](#) -
CON - cont...(10:00-17:59 PDT) - [Cloud Village CTF](#) -
CON - cont...(10:00-19:59 PDT) - [DC Kubernetes Capture the Flag \(CTF\)](#) -
CPV - [Cicada 3301: An Exploration of the Cryptographic Enigma](#) - Artorias,Puck,Taiwo,TheClockworkBird
CPV - (16:30-16:45 PDT) - [Intro to Ciphers](#) - CPV Staff
DC - cont...(15:30-16:15 PDT) - [Game-Changing Advances in Windows Shellcode Analysis](#) - Bramwell Brizendine,Jake Hince,Max 'Libra' Kersten
DC - (16:30-17:15 PDT) - [Malware design - abusing legacy Microsoft transports and session architecture](#) - R.J. "BeetleChunks" McDown
DC - cont...(10:00-17:59 PDT) - [Vendor Area Open](#) -
DC - cont...(08:00-19:59 PDT) - [Human Registration Open](#) -
DC - cont...(15:30-16:15 PDT) - [A Comprehensive Review on the Less-Traveled Road: 9 Years of Overlooked MikroTik Pre-Auth RCE](#) - NiNi Chen
DC - (16:30-17:15 PDT) - [Nothing but Net: Leveraging macOS's Networking Frameworks to Heuristically Detect Malware](#) - Patrick Wardle
DC - [Visual Studio Code is why I have \(Workspace\) Trust issues](#) - Paul Gerste,Thomas Chauchefoin
DC - cont...(10:00-17:59 PDT) - [Exhibitor Area Open](#) -
DC - cont...(15:30-16:15 PDT) - [Turning my virtual wallet into a skimming device: mPOS solutions](#) - Dan Borgogno,Ileana Barrionuevo
DC - (16:30-17:15 PDT) - [certmitm: automatic exploitation of TLS certificate validation vulnerabilities](#) - Aapo Oksman
DC - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
DC - cont...(10:00-17:59 PDT) - [Contest Area Open](#)
DC - cont...(14:00-16:59 PDT) - [Lonely Hackers Club - Badgelife & Sticker Swap](#)
DC - [A Series of Unfortunate Events](#) - Ben "NahamSec" Sadeghipour,Corben Leo
ESV - cont...(10:00-17:59 PDT) - [Embedded Systems Village Activities](#) -
HHV - cont...(10:00-17:59 PDT) - [Soldering Skills Village Activities](#) -
HHV - cont...(10:00-17:59 PDT) - [RoboSumo Play Time](#) -
HHV - cont...(10:00-17:59 PDT) - [Hardware Hacking Rube Goldberg Machine](#) -
HHV - cont...(10:00-17:59 PDT) - [Make Your Own Use](#) -
HRV - cont...(15:00-16:30 PDT) - [HF Radio Demonstration](#) - KitKat
ICSV - [I'm On The Hype Train: Bottom's Up!](#) - Joe Slowik
ICSV - (16:30-16:59 PDT) - [Anaotmy of the Top 10 Cybersecurity Terrain for Critical Infrastructure](#) - Mars Cheng
IOTV - cont...(10:00-17:59 PDT) - [Hardware Hacking Your Kitchen](#) -
IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hacking Playground](#) -
IOTV - cont...(10:00-17:59 PDT) - [Critical Infrastructure & IoT Exploitation](#) -
IOTV - cont...(10:00-17:59 PDT) - [Secure or Surrender](#) -
IOTV - cont...(10:00-17:59 PDT) - [The IoT Kill Zone](#) -
IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hardware Hacking Exercises 2023](#) -
IOTV - cont...(10:00-17:59 PDT) - [Embedded Device Security Workshops](#) -
IOTV - cont...(10:00-17:59 PDT) - [Perform Memory Extraction, Emulation and Shellcode](#) -
IOTV - cont...(15:30-16:29 PDT) - [IoT Village - Free Book Signing with author Ted Harrington](#) -
LPV - cont...(10:00-17:59 PDT) - [Lockpick Village Activities](#) -

LPV - [Intro to Lockpicking](#) - TOOOL
 MISC - [No Starch Press - Book Signing](#) - Bradly Smith, DevOps for the Desperate
 MISC - cont...(10:00-16:59 PDT) - [DDV open and accepting drives for duplication](#) -
 MISC - cont...(11:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\) - BYODesign Registration](#) -
 MISC - cont...(12:00-17:59 PDT) - [EFF Benefit Poker Tournament at DEF CON 31 - Poker](#) -
 MIV - cont...(15:30-16:30 PDT) - [Digital Media Authentication - A Toolkit for Journalists in the Fight Against Misinformation with Cryptographic Tools](#) - Adam Rose
 MIV - (16:30-17:59 PDT) - [Film screening: Reality Games Using film and interactive storytelling to inoculate against the disinformation tsunami](#): - Michael Morgenstern
 PHV - cont...(09:00-17:59 PDT) - [Honey Pot Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [Wall of Sheep](#) -
 PHV - cont...(09:00-17:59 PDT) - [Build Your Own Botnet](#) -
 PHV - cont...(09:00-17:59 PDT) - [Linux Trainer Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [NetworkOS: Be The Cloud](#) -
 PHV - cont...(09:00-17:59 PDT) - [RegEx Trainer](#) -
 PHV - cont...(09:00-17:59 PDT) - [Password Lab](#) -
 PHV - cont...(09:00-17:59 PDT) - [Fleet DefCon 31 Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [Packet Inspector](#) -
 PHV - cont...(09:00-17:59 PDT) - [Packet Detective](#) -
 PLV - [I Am A Former National Cybersecurity Director, Ask Me Anything!](#) - Chris Inglis
 PLV - cont...(15:00-16:50 PDT) - [A global approach to tackling software resilience](#) - Allan Friedman,Camille Stewart
 Gloster,Charlie Gladstone,David Rogers
 PSV - cont...(10:00-17:59 PDT) - [Physical Security Village Activities](#) -
 PSV - cont...(15:30-16:30 PDT) - [Deep Diving Into HID Vulnerabilities: Heart of Darkness](#) - Chad,Shortman
 PWV - cont...(10:00-17:59 PDT) - [Password Village Activities](#) -
 PYV - cont...(11:00-17:59 PDT) - [Payment Village Challenges/CTF](#) -
 QTV - [The Quantum Debates](#) -
 QTV - [Debate: The Quantum Village believes individual citizen privacy will be enhanced with the fielding of new quantum technologies.](#) - David Joseph,Troy Mills
 RCV - cont...(15:45-16:30 PDT) - [Crushing crumbs of information to eat a whole cake.](#) - Felipe Pr0teus
 RCV - (16:30-17:15 PDT) - [Nosy Cops: Exposing the Hidden Potential of Police Radio](#) - sally
 RFV - [Badge Cloning With Doppelgänger](#) - Travis Weathers
 RTV - [Malware Hunting an Offensive Approach](#) - Filipi Pires
 RTV - [Hacking Real Web Areas](#) - Ilkin Javadov
 RTV - [IOCs + APTs = "Let's play a game!" - Hack your way through a hunt!](#) - Leo Cruz
 RTV - [Passwords Argh Us](#) - Traveler
 RTV - [Red Team Labs and Games for Kids](#)
 RTV - cont...(14:00-16:59 PDT) - [Kubernetes Offense](#) - Michael Mitchell
 SEV - cont...(08:30-17:30 PDT) - [SECV - Youth Challenge](#) -
 SEV - cont...(08:30-17:59 PDT) - [SECV Village Open](#)
 SOC - [Queercon Mixers](#) -
 SOC - [DEF CON Holland Group Presents: VrijMiBo](#) -
 SOC - cont...(10:00-17:59 PDT) - [Hacker Memorial](#) -
 SOC - [DC 404/DC 678/ DC 770/ DC 470 \(Atlanta Metro\)](#) -
 SOC - cont...(12:00-17:59 PDT) - [Lonely Hackers Club Meetup](#) -
 SOC - cont...(10:00-17:59 PDT) - [DCG Meetups](#)
 SOC - cont...(12:00-17:59 PDT) - [HDA / Accessibility Area Open](#)
 SOC - cont...(12:00-17:59 PDT) - [HDA Community Meetups](#)
 TCV - [SS7 CTF](#) - Akib Sayyed,Zibran Sayyed
 TEV - cont...(10:00-17:59 PDT) - [Tamper Evident Village Activities](#) -
 VMV - cont...(15:30-16:15 PDT) - [What Makes Hackers Extraordinary - It's A Gift!](#) - D9
 VMV - cont...(15:30-16:15 PDT) - [RLA Workshop](#) - Amanda Glazer
 VMV - (16:30-17:30 PDT) - [Election Preparation: 2024](#) - Ashlee Bengé,Jake Braun,John Odum,Michael Moore
 WS - cont...(14:00-17:59 PDT) - [Machine Learning for N00bs \(Pre-Registration Required\)](#) - Elizabeth Biddlecome,Irvin
 Lemus,Kaitlyn Handelman,Sam Bowne

- WS - cont...(14:00-17:59 PDT) - [How hackers can send feedback directly to policymakers like the pros \(Pre-Registration Required\)](#) - Amit Elazari,Harley Geiger
- WS - cont...(14:00-17:59 PDT) - [Malware development on secured environment - Write, adapt, overcome \(Pre-Registration Required\)](#) - Yoann Dequeker
- WS - cont...(14:00-17:59 PDT) - [Learning to Hack Bluetooth Low Energy with BLE CTF \(Pre-Registration Required\)](#) - Ryan Holeman
- WS - cont...(14:00-17:59 PDT) - [Advanced WiFi Attacks for Red Team Professionals \(Pre-Registration Required\)](#) - Raúl "r4ulcl" Calvo Laorden
- XRV - cont...(10:00-17:59 PDT) - [XR Village Playground](#) -
- XRV - cont...(11:00-16:59 PDT) - [Off the Rails: A demo with Pacific Northwest National Labs](#) -
- XRV - [Glad Scientist | Village Vibes Immersive Performance, a data-driven real time audiovisual VR performance](#) -

Friday - 17:00 PDT

[Return to Index](#) - [Locations Legend](#)

[AIV](#) - cont...(10:00-17:59 PDT) - [AI Village Generative Red Team Challenge](#) -
[AIV](#) - [Ghost in the Neurons - ML Webshells](#) - Tom Bonner
[ASV](#) - cont...(10:00-17:59 PDT) - [Unmanned Aerial Systems – Platform Security](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [The Challenge - Lockheed Martin](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [A-ISAC CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [ARINC 615a CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [PTP Flight Challenge](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Ask Me Anything About Cybersecurity in Aerospace](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Hack The Airport](#) -
[ASV](#) - [Pen Test Partners Power Hour](#) - Alex Lomas, Ken Munro
[BHV](#) - cont...(16:30-17:20 PDT) - [My CPAP has a recall, lets open it instead!](#) - José Fernández
[BHV](#) - (17:20-17:59 PDT) - [CVE Insanity](#) - Om Mahida
[BTV](#) - cont...(16:00-17:59 PDT) - [Monroeville Live: An IR Tabletop for the Rest of Us](#) - Dave Collins, Gwyddia, Litmoose, Matt Mahler, Nathan Case, Nina Alli, Shea Nangle
[CHV](#) - [How an automotive security researcher had his car stolen via 'CAN Injection'](#) - Ian Tabor, Ken Tindell
[CON](#) - cont...(09:00-17:59 PDT) - [HardWired](#) -
[CON](#) - cont...(10:30-17:59 PDT) - [Capture The Packet Preliminaries](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [IoT Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hardware Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hack-A-Sat 4 \(HAS4\)](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [5n4ck3y](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL at DEF CON 31 - Booth Open](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Dark Tangent Look-Alike Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Battle of The Bots](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Ham Radio Fox Hunting Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Gold Bug Challenge](#) -
[CON](#) - cont...(10:00-19:59 PDT) - [The Lonely Hard Drive](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Tinfoil Hat Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [IntelOps - Operation Spacewatch](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [venator aurum - A Treasure Hunt](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [It's In That Place Where I Put That Thing That Time](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CrackMelfYouCan](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Maps of the digital lands](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\)](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [AutoDriving CTF](#) -
[CON](#) - cont...(10:00-19:59 PDT) - [pTFS Presents: Mayhem Industries – Starphish](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Trace Labs OSINT Search Party CTF - Sign-ups](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Dungeons@Defcon](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Red Team CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [? Cube](#) -
[CON](#) - [Hack3r Runw@y](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
[CON](#) - cont...(10:30-17:59 PDT) - [Blue Team Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Embedded CTF](#) -
[CON](#) - cont...(09:00-17:59 PDT) - [Social Engineering Community \(SEC\) Youth Challenge](#) -

CON - cont...(10:00-17:59 PDT) - [Cloud Village CTF](#) -
CON - cont...(10:00-19:59 PDT) - [DC Kubernetes Capture the Flag \(CTF\)](#) -
CPV - [Spoofing certificates with MD5 collisions - party like it's 2008!](#) - Tomer,Yoni
DC - cont...(16:30-17:15 PDT) - [Malware design - abusing legacy Microsoft transports and session architecture](#) - R.J.
"BeetleChunks" McDown
DC - (17:30-18:15 PDT) - [Fireside Chat with the National Cyber Director Kemba Walden](#) - Kemba Walden
DC - cont...(10:00-17:59 PDT) - [Vendor Area Open](#) -
DC - cont...(08:00-19:59 PDT) - [Human Registration Open](#) -
DC - cont...(16:30-17:15 PDT) - [Nothing but Net: Leveraging macOS's Networking Frameworks to Heuristically Detect Malware](#) - Patrick Wardle
DC - [HL7Magic: Medical Data Hacking Made Easy](#) - Katie Inns
DC - cont...(10:00-17:59 PDT) - [Exhibitor Area Open](#) -
DC - cont...(16:30-17:15 PDT) - [certmitm: automatic exploitation of TLS certificate validation vulnerabilities](#) - Aapo Oksman
DC - (17:30-17:50 PDT) - [Track the Planet! Mapping Identities, Monitoring Presence, and Decoding Business Alliances in the Azure Ecosystem](#) - nyxgeek
DC - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
DC - cont...(10:00-17:59 PDT) - [Contest Area Open](#)
DC - [Lonely Hackers Club - Name That Noob](#)
DC - [Legend of Zelda: Use After Free \(TASBot glitches the future into OoT\)](#) - Allan "dwangoAC" Cecil
ESV - cont...(10:00-17:59 PDT) - [Embedded Systems Village Activities](#) -
HHV - cont...(10:00-17:59 PDT) - [Make Your Own Use](#) -
HHV - cont...(10:00-17:59 PDT) - [Soldering Skills Village Activities](#) -
HHV - cont...(10:00-17:59 PDT) - [RoboSumo Play Time](#) -
HHV - cont...(10:00-17:59 PDT) - [Hardware Hacking Rube Goldberg Machine](#) -
IOTV - cont...(10:00-17:59 PDT) - [Hardware Hacking Your Kitchen](#) -
IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hacking Playground](#) -
IOTV - cont...(10:00-17:59 PDT) - [Critical Infrastructure & IoT Exploitation](#) -
IOTV - cont...(10:00-17:59 PDT) - [Secure or Surrender](#) -
IOTV - cont...(10:00-17:59 PDT) - [The IoT Kill Zone](#) -
IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hardware Hacking Exercises 2023](#) -
IOTV - cont...(10:00-17:59 PDT) - [Embedded Device Security Workshops](#) -
IOTV - cont...(10:00-17:59 PDT) - [Perform Memory Extraction, Emulation and Shellcode](#) -
LPV - cont...(10:00-17:59 PDT) - [Lockpick Village Activities](#) -
MISC - cont...(11:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\) - BYODesign Registration](#) -
MISC - cont...(12:00-17:59 PDT) - [EFF Benefit Poker Tournament at DEF CON 31 - Poker](#) -
MIV - cont...(16:30-17:59 PDT) - [Film screening: Reality Games Using film and interactive storytelling to inoculate against the disinformation tsunami](#): - Michael Morgenstern
PHV - cont...(09:00-17:59 PDT) - [Honey Pot Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [Wall of Sheep](#) -
PHV - cont...(09:00-17:59 PDT) - [Build Your Own Botnet](#) -
PHV - cont...(09:00-17:59 PDT) - [Linux Trainer Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [NetworkOS: Be The Cloud](#) -
PHV - cont...(09:00-17:59 PDT) - [RegEx Trainer](#) -
PHV - cont...(09:00-17:59 PDT) - [Password Lab](#) -
PHV - cont...(09:00-17:59 PDT) - [Fleet DefCon 31 Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [Packet Inspector](#) -
PHV - cont...(09:00-17:59 PDT) - [Packet Detective](#) -
PLV - [Keeping stores safe: how do we better secure apps and app stores?](#) - Charlie Gladstone,David Rogers
PLV - [Demystifying Hacking for Government Officials](#) - Brad Manuel,Jack Cable,Jason Ingalls,Lindsey Forson,Michael Ross
PSV - cont...(10:00-17:59 PDT) - [Physical Security Village Activities](#) -
PWV - cont...(10:00-17:59 PDT) - [Password Village Activities](#) -
PYV - cont...(11:00-17:59 PDT) - [Payment Village Challenges/CTF](#) -
QTV - cont...(16:00-17:59 PDT) - [The Quantum Debates](#) -
QTV - (17:15-17:59 PDT) - [Debate: NISQ and the future of Quantum Advantage: This village believes the current state of NISQ is already enabling quantum advantage for those who know how to use these technologies](#) - Konstantinos

Karagiannis,Rafal Janik

RCV - cont...(16:30-17:15 PDT) - [Nosy Cops: Exposing the Hidden Potential of Police Radio](#) - sally

SEV - cont...(08:30-17:30 PDT) - [SECV - Youth Challenge](#) -

SEV - cont...(08:30-17:59 PDT) - [SECV Village Open](#)

SEV - (17:15-17:59 PDT) - [A Slice of Deception: The 2023 #SECV Debrief](#) - JC,Snow

SOC - cont...(16:00-17:59 PDT) - [Queercon Mixers](#) -

SOC - cont...(16:00-18:59 PDT) - [DEF CON Holland Group Presents: VrijMiBo](#) -

SOC - cont...(10:00-17:59 PDT) - [Hacker Memorial](#) -

SOC - cont...(16:00-18:59 PDT) - [DC 404/DC 678/ DC 770/ DC 470 \(Atlanta Metro\)](#) -

SOC - cont...(12:00-17:59 PDT) - [Lonely Hackers Club Meetup](#) -

SOC - cont...(10:00-17:59 PDT) - [DCG Meetups](#)

SOC - [Friends of Bill W](#) -

SOC - cont...(12:00-17:59 PDT) - [HDA / Accessibility Area Open](#)

SOC - cont...(12:00-17:59 PDT) - [HDA Community Meetups](#)

TCV - cont...(16:00-17:59 PDT) - [SS7 CTF](#) - Akib Sayyed,Zibran Sayyed

TEV - cont...(10:00-17:59 PDT) - [Tamper Evident Village Activities](#) -

VMV - cont...(16:30-17:30 PDT) - [Election Preparation: 2024](#) - Ashlee Benge,Jake Braun,John Odum,Michael Moore

WS - cont...(14:00-17:59 PDT) - [Machine Learning for N00bs \(Pre-Registration Required\)](#) - Elizabeth Biddlecome,Irvin

Lemus,Kaitlyn Handelman,Sam Bowne

WS - cont...(14:00-17:59 PDT) - [How hackers can send feedback directly to policymakers like the pros \(Pre-Registration Required\)](#) - Amit Elazari,Harley Geiger

WS - cont...(14:00-17:59 PDT) - [Malware development on secured environment - Write, adapt, overcome \(Pre-Registration Required\)](#) - Yoann Dequeker

WS - cont...(14:00-17:59 PDT) - [Learning to Hack Bluetooth Low Energy with BLE CTF \(Pre-Registration Required\)](#) - Ryan Holeman

WS - cont...(14:00-17:59 PDT) - [Advanced WiFi Attacks for Red Team Professionals \(Pre-Registration Required\)](#) - Raúl "r4ulcl" Calvo Laorden

XRV - cont...(10:00-17:59 PDT) - [XR Village Playground](#) -

Friday - 18:00 PDT

[Return to Index - Locations Legend](#)

[CON - Pub Quiz at DEF CON](#) -

[CON - cont...\(10:00-19:59 PDT\) - The Lonely Hard Drive](#) -

[CON - cont...\(10:00-19:59 PDT\) - pTFS Presents: Mayhem Industries – Starphish](#) -

[CON - cont...\(10:00-19:59 PDT\) - DC Kubernetes Capture the Flag \(CTF\)](#) -

[DC - cont...\(17:30-18:15 PDT\) - Fireside Chat with the National Cyber Director Kemba Walden](#) - Kemba Walden

[DC - cont...\(08:00-19:59 PDT\) - Human Registration Open](#) -

[MISC - \(18:30-21:59 PDT\) - Hacking Policy & Prompts - Happy Hour](#) -

[MUS - Music Set / Entertainment \(Friday, ACK Stage\)](#) - Acid T,CTRL/rsm,DJ PatAttack,DJ St3rling,Magik Plan,Scotch and Bubbles,Spice Rack,kampf

[SOC - Blacks in Cyber Lituation Party](#) -

[SOC - cont...\(16:00-18:59 PDT\) - DEF CON Holland Group Presents: VrijMiBo](#) -

[SOC - cont...\(16:00-18:59 PDT\) - DC 404/DC 678/ DC 770/ DC 470 \(Atlanta Metro\)](#) -

Friday - 19:00 PDT

[Return to Index](#) - [Locations Legend](#)

[CON](#) - cont...(18:00-20:30 PDT) - [Pub Quiz at DEF CON](#) -

[CON](#) - cont...(10:00-19:59 PDT) - [The Lonely Hard Drive](#) -

[CON](#) - cont...(10:00-19:59 PDT) - [pTFS Presents: Mayhem Industries – Starphish](#) -

[CON](#) - cont...(10:00-19:59 PDT) - [DC Kubernetes Capture the Flag \(CTF\)](#) -

[DC](#) - cont...(08:00-19:59 PDT) - [Human Registration Open](#) -

[MISC](#) - cont...(18:30-21:59 PDT) - [Hacking Policy & Prompts](#) - [Happy Hour](#) -

[MISC](#) - [Kids Only Karaoke](#) -

Friday - 20:00 PDT

[Return to Index](#) - [Locations Legend](#)

[CON](#) - [cont...\(18:00-20:30 PDT\)](#) - [Pub Quiz at DEF CON](#) -

[CON](#) - [Hacker Jeopardy](#) -

[DC](#) - [Ask the EFF](#) - Cooper Quintin,Corynne McSherry,Hannah Zhao,Mario Trujillo,Rory Mir

[MISC](#) - [Movie Night](#) -

[MISC](#) - [cont...\(18:30-21:59 PDT\)](#) - [Hacking Policy & Prompts](#) - [Happy Hour](#) -

[SOC](#) - [Cult Of The Dead Cow Breaks The Internet \(and you can too!\)](#) -

[SOC](#) - [Hacker Flairgrounds](#) -

[SOC](#) - [Hacker Karaoke 15](#) -

[SOC](#) - [\(20:30-22:59 PDT\)](#) - [Blue Team Village \(BTV\) Pool Party](#) -

[SOC](#) - [\(20:30-22:59 PDT\)](#) - [WISP Community Meet Up at BTV Pool Party](#) -

[SOC](#) - [Lawyers Meet](#) -

Friday - 21:00 PDT

[Return to Index](#) - [Locations Legend](#)

[CON](#) - cont...(20:00-21:59 PDT) - [Hacker Jeopardy](#) -

[DC](#) - cont...(20:00-21:59 PDT) - [Ask the EFF](#) - Cooper Quintin,Corynne McSherry,Hannah Zhao,Mario Trujillo,Rory Mir

[MISC](#) - cont...(20:00-23:59 PDT) - [Movie Night](#) -

[MISC](#) - cont...(18:30-21:59 PDT) - [Hacking Policy & Prompts](#) - [Happy Hour](#) -

[MUS](#) - [Music Set / Entertainment \(Friday, SYN Stage\)](#) - Great Scott,Krisz Klink,TRIODE,Zebbler Encanti Experience,heckseven

[SOC](#) - cont...(20:00-23:59 PDT) - [Cult Of The Dead Cow Breaks The Internet \(and you can too!\)](#) -

[SOC](#) - [GothCon](#) -

[SOC](#) - cont...(20:00-21:59 PDT) - [Hacker Flairgrounds](#) -

[SOC](#) - [The Village People Party: hosted by Car Hacking, ICS, Aerospace, and Biohacking Villages](#) - NGHTHWK

[SOC](#) - cont...(20:30-22:59 PDT) - [Blue Team Village \(BTV\) Pool Party](#) -

[SOC](#) - cont...(20:30-22:59 PDT) - [WISP Community Meet Up at BTV Pool Party](#) -

Friday - 22:00 PDT

[Return to Index](#) - [Locations Legend](#)

[CON](#) - [Whose Slide Is It Anyway?](#) -

[MISC](#) - [cont...\(20:00-23:59 PDT\)](#) - [Movie Night](#) -

[SOC](#) - [cont...\(20:00-23:59 PDT\)](#) - [Cult Of The Dead Cow Breaks The Internet \(and you can too!\)](#) -

[SOC](#) - [QueerCon Party](#) - [DotOrNot](#), [Miss Jackalope](#), [Skittish & Bus](#)

[SOC](#) - [cont...\(20:30-22:59 PDT\)](#) - [Blue Team Village \(BTV\) Pool Party](#) -

[SOC](#) - [cont...\(20:30-22:59 PDT\)](#) - [WISP Community Meet Up at BTV Pool Party](#) -

Friday - 23:00 PDT

[Return to Index](#) - [Locations Legend](#)

[CON](#) - cont...(22:00-23:59 PDT) - [Whose Slide Is It Anyway?](#) -

[MISC](#) - cont...(20:00-23:59 PDT) - [Movie Night](#) -

[SOC](#) - cont...(20:00-23:59 PDT) - [Cult Of The Dead Cow Breaks The Internet \(and you can too!\)](#) -

Saturday

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

Saturday - 00:00 PDT

[Return to Index - Locations Legend](#)

[BHV - Model Based Systems Engineering for Security Engineers](#) - John Volock

[BHV - Virtual Hospital in Space](#) - Aswin Reji

[BHV - Hacking Reproductive Health](#) - JJ Hastings

[BHV - Beyond Ransomware: Protecting Lives and Data from Modern Threat Actors](#) - Ohad Zaidenberg

[BHV - The Megabiome is In Charge: Taking Control of Your Microbial World](#) - Mariam Elgabry

[Return to Index - Locations Legend](#)

MISC - Defcon.run -

[Return to Index - Locations Legend](#)

MISC - cont...(06:00-11:59 PDT) - [Defcon.run](#) -

Saturday - 08:00 PDT

[Return to Index](#) - [Locations Legend](#)

[MISC](#) - cont...(06:00-11:59 PDT) - [Defcon.run](#) -
[SEV](#) - (08:30-17:30 PDT) - [SECV](#) - [Youth Challenge](#) -
[SEV](#) - (08:30-17:59 PDT) - [SECV Village Open](#)

[Return to Index](#) - [Locations Legend](#)

[CON - HardWired](#) -

[CON - Social Engineering Community \(SEC\) Youth Challenge](#) -

[DC - Hack the Future: Why Congress and the White House are supporting AI Red Teaming](#) - Arati Prabhakar,Austin Carson

[DC - \(09:30-18:59 PDT\) - Human Registration Open](#) -

[DC - Assessing the Security of Certificates at Scale](#) - Andrew Chi,Brandon Enright,David McGrew

[DC - \(09:30-10:15 PDT\) - Badge of Shame: Breaking into Secure Facilities with OSDP](#) - Dan "AltF4" Petro,David Vargas

[DC - Smashing the state machine: the true potential of web race conditions](#) - James "albinowax" Kettle

[DC - Shell On Demand Appliance Machine \(S.O.D.A. Machine\) \(pronounced SODA\)](#) -

[DC - ELECTRONizing macOS privacy - a new weapon in your red teaming armory](#) - Wojciech Reguła

[DC - \(09:30-10:15 PDT\) - J4 Gate, The Hustler Poker Cheating Scandal investigation and how Hacking helped me do it](#) - Scott "Duckie" Melnick

[DC - Merch \(formerly swag\) Area Open -- README](#) -

[MISC - cont...\(06:00-11:59 PDT\) - Defcon.run](#) -

[PHV - Honey Pot Workshop](#) -

[PHV - Build Your Own Botnet](#) -

[PHV - Wall of Sheep](#) -

[PHV - Linux Trainer Workshop](#) -

[PHV - NetworkOS: Be The Cloud](#) -

[PHV - RegEx Trainer](#) -

[PHV - Password Lab](#) -

[PHV - Fleet DefCon 31 Workshop](#) -

[PHV - Packet Inspector](#) -

[PHV - Packet Detective](#) -

[RTV - Android Applications and APIs Hacking](#) - Gabrielle Botbol

[RTV - Build Your Own Cat-Shaped USB Hacking Tool! \(with the Nugget\)](#) - Alex Lynd

[RTV - Passwords Argh Us](#) - Traveler

[RTV - Open Source Intelligence \(OSINT\) for Hackers](#) - Lee McWhorter,Sandra Stibbards

[RTV - Red Team Labs and Games for Kids](#)

[RTV - Hacking Meta Quest](#) - Paul D.

[SEV - cont...\(08:30-17:30 PDT\) - SECV - Youth Challenge](#) -

[SEV - cont...\(08:30-17:59 PDT\) - SECV Village Open](#)

[SEV - Anti-Social Engineering: Can You Be a Good Social Engineer Without Being Social](#) - Andrew Lemon

[SEV - \(09:30-09:59 PDT\) - Your Swag is My Swag: Pwning Fortune 500 Companies with Vistaprint](#) - Daniel "Jcache" Goga,Langston "Shock" Clement

[WS - Email Detection Engineering and Threat Hunting Inbox \(Pre-Registration Required\)](#) - Alfie Champion,Josh Kamdjou

[WS - Active Directory Attacks: The Good, The Bad, and The LOLwut \(Pre-Registration Required\)](#) - Aaron Rosenmund,Brandon DeVault,Ryan Chapman

[WS - The Petting Zoo: Breaking into CTFs \(Pre-Registration Required\)](#) - Christopher Forte,Robert Fitzpatrick

[WS - Creating and uncovering malicious containers Redux \(Pre-Registration Required\)](#) - Adrian "threlfall" Wood,David "digish0" Mitchell

[WS - BLE Security 201 \(Pre-Registration Required\)](#) - Maxine "Freqy" Filcher,Zach "justadequate" Reavis

[Return to Index - Locations Legend](#)

[AIV - AI Village Generative Red Team Challenge -](#)
[AIV - \(10:30-11:25 PDT\) - AI Village Keynote 2: AI red teaming tradecraft: a team of teams approach - Daniel Fabian,Mikel Rodriguez,Sarah Hodkinson](#)
[APV - AppSec Village Keynote: Collaborative Security: Fostering Innovation and Resilient Cyber Practices - Maril Vernon](#)
[ASV - Hack The Airport -](#)
[ASV - Unmanned Aerial Systems – Platform Security -](#)
[ASV - The Challenge - Lockheed Martin -](#)
[ASV - A-ISAC CTF -](#)
[ASV - Bricks in the Air -](#)
[ASV - ARINC 615a CTF -](#)
[ASV - PTP Flight Challenge -](#)
[ASV - Ask Me Anything About Cybersecurity in Aerospace -](#)
[BHV - Securing the Whole System: Corpal to Corporate - Lee Cyborg](#)
[BHV - \(10:30-11:10 PDT\) - Homo sapiens sapiens to Homo sapiens nova - the coming speciation - Almost Human \(BJ\)](#)
[BTV - \(10:30-11:30 PDT\) - IR/4n6: Obsidian DFIR - Gang aft agley - Omenscan](#)
[BTV - \(10:30-11:30 PDT\) - DE: Breaking the Rule - Oldmonk](#)
[BTV - \(10:30-11:30 PDT\) - CTH: Log4j - The Silent Menace Among Us - Cyb3rhawk](#)
[CHV - VDA Shenanigans: Attacking & Defending the Truck Part that Gets Left Behind - Alex Reuter,Wyatt Ford](#)
[CLV - Introducing IAM-APE - Tohar Braun](#)
[CLV - \(10:30-11:10 PDT\) - Between a Log and a Hard Place: \(mis\)Adventures in Azure Logs - Dmitriy Beryoza](#)
[CON - cont...\(09:00-17:59 PDT\) - HardWired -](#)
[CON - \(10:30-11:59 PDT\) - Capture The Packet Preliminaries -](#)
[CON - IoT Village CTF -](#)
[CON - Hardware Hacking Village CTF -](#)
[CON - 5n4ck3y -](#)
[CON - TeleChallenge -](#)
[CON - Hack-A-Sat 4 \(HAS4\) -](#)
[CON - Adversary Wars CTF -](#)
[CON - The Dark Tangent Look-Alike Contest -](#)
[CON - CMD+CTRL at DEF CON 31 - Booth Open -](#)
[CON - HackFortress -](#)
[CON - Battle of The Bots -](#)
[CON - Ham Radio Fox Hunting Contest -](#)
[CON - The Gold Bug Challenge -](#)
[CON - The Lonely Hard Drive -](#)
[CON - Car Hacking Village CTF -](#)
[CON - Tinfoil Hat Contest -](#)
[CON - venator aurum - A Treasure Hunt -](#)
[CON - CrackMeIfYouCan -](#)
[CON - It's In That Place Where I Put That Thing That Time -](#)
[CON - Darknet-NG -](#)
[CON - Maps of the digital lands -](#)
[CON - DC's Next Top Threat Model \(DCNTTM\) -](#)
[CON - Octopus Game -](#)
[CON - DEF CON Scavenger Hunt -](#)
[CON - DEFCON MUD DUMB TERMINAL EDITION -](#)
[CON - Red Alert ICS CTF -](#)
[CON - Dungeons@Defcon -](#)
[CON - Red Team CTF -](#)
[CON - ? Cube -](#)
[CON - \(10:30-14:30 PDT\) - Trace Labs OSINT Search Party CTF - CTF Platform Open for Submissions -](#)

CON - Radio Frequency Capture the Flag -
CON - (10:30-17:59 PDT) - Blue Team Village CTF -
CON - Embedded CTF -
CON - cont...(09:00-17:59 PDT) - Social Engineering Community (SEC) Youth Challenge -
CON - Cloud Village CTF -
CON - DC Kubernetes Capture the Flag (CTF) -
CPV - CPV Welcome - Day 2 - CPV Staff
CPV - (10:30-10:59 PDT) - Blindly hunting for Mercenaries - Asheer Malhotra,Vitor Ventura
CPV - (10:30-10:45 PDT) - Intro to Ciphers - CPV Staff
DC - Defeating VPN Always-On - Maxime Clementz
DC - Vendor Area Open -
DC - cont...(09:30-18:59 PDT) - Human Registration Open -
DC - cont...(09:30-10:15 PDT) - Badge of Shame: Breaking into Secure Facilities with OSDP - Dan "AltF4" Petro,David Vargas
DC - (10:30-11:15 PDT) - Calling it a 0-Day - Hacking at PBX/UC Systems - good_pseudonym
DC - Demystifying (& Bypassing) macOS's Background Task Management - Patrick Wardle
DC - Exhibitor Area Open -
DC - cont...(09:30-10:15 PDT) - J4 Gate, The Hustler Poker Cheating Scandal investigation and how Hacking helped me do it - Scott "Duckie" Melnick
DC - (10:30-11:15 PDT) - Unlocking Doors from Half a Continent Away - Sam Haskins,Trevor "t1v0" Stevado
DC - cont...(09:00-11:59 PDT) - Merch (formerly swag) Area Open -- README -
DC - Contest Area Open
DC - D0 N0 H4RM: A Healthcare Security Conversation - Christian "quaddi" Dameff,Jacqueline Burgette,Jeff "r3plicant" Tully,Mark Warner,Nitin Natarajan,Suzanne Schwartz
DCGVR - DEF CON Groups Keynote - Jayson E. Street
DL - Lambda Looter - Doug Kent,Rob Ditmer
DL - Lupo: Malware IOC Extractor - Vishal Thakur
DL - Veilid - Deth Veggie,TC Johnson
DL - Saturday - Joshua Herman
DL - The Wifydra: Multiheaded RF Panopticon - Lozaning
DL - USBvalve - Expose USB activity on the fly - Cesare Pizzi
ESV - Embedded Systems Village Activities -
HHV - Make Your Own Use -
HHV - Soldering Skills Village Activities -
HHV - RoboSumo Play Time -
HHV - Hardware Hacking Rube Goldberg Machine -
ICSV - I am the captain now: Taking remote control of ships engines, helm, azipods, ballasting and plenty more. - Ken Munro
ICSV - (10:30-10:59 PDT) - EMBA - From firmware to exploit - Michael Messner
IOTV - Hardware Hacking Your Kitchen -
IOTV - IoT Village Hacking Playground -
IOTV - Critical Infrastructure & IoT Exploitation -
IOTV - Secure or Surrender -
IOTV - The IoT Kill Zone -
IOTV - IoT Village Hardware Hacking Exercises 2023 -
IOTV - Embedded Device Security Workshops -
IOTV - Perform Memory Extraction, Emulation and Shellcode -
LPV - Lockpick Village Activities -
LPV - (10:15-10:45 PDT) - Intro to Lockpicking - TOOOL
MISC - DDV open and accepting drives for duplication -
MISC - DC's Next Top Threat Model (DCNTTM) - Kids - Learn Threat Modeling -
MISC - Book Exchange -
MISC - cont...(06:00-11:59 PDT) - Defcon.run -
MIV - Disincentivizing misinformation: co-create a new platform business model - Vardon Hamdiu
PHV - cont...(09:00-17:59 PDT) - Honey Pot Workshop -
PHV - cont...(09:00-17:59 PDT) - Build Your Own Botnet -

PHV - cont...(09:00-17:59 PDT) - [Wall of Sheep](#) -

PHV - cont...(09:00-17:59 PDT) - [Linux Trainer Workshop](#) -

PHV - cont...(09:00-17:59 PDT) - [NetworkOS: Be The Cloud](#) -

PHV - cont...(09:00-17:59 PDT) - [RegEx Trainer](#) -

PHV - cont...(09:00-17:59 PDT) - [Password Lab](#) -

PHV - cont...(09:00-17:59 PDT) - [Fleet DefCon 31 Workshop](#) -

PHV - cont...(09:00-17:59 PDT) - [Packet Inspector](#) -

PHV - cont...(09:00-17:59 PDT) - [Packet Detective](#) -

PLV - [What "Secure by Design" means for software breakers and builders](#) - Cassie Crossley,Christopher Butera,Daniel Bardenstein

PLV - [How hackers can work with government, industry, civil society to protect high-risk communities](#) - Adrien Ogee,David Forscey,Mark E. Schreiber,Maurice Kent,Monica M. Ruiz,Sarah Powazek

PSV - [Physical Security Village Activities](#) -

PWV - [Password Village Activities](#) -

QTV - (10:30-10:59 PDT) - [Q-CTF QOLOSSUS Update](#) - Mark Carney

RCV - [Panel Discussion - Bugs, Bounties, & Breaches - Insider Tales from the Trenches](#) - Jason Haddix

RCV - (10:45-11:30 PDT) - [OSINT Privacy Unmasked: Taking Control of Your Digital Footprint in a Hyper-Connected World](#) - Zoey Selman

RTV - [Hunting & Exploiting DLL Sideloads](#) - Matthew Nickerson,Nick Swink

RTV - cont...(09:00-11:59 PDT) - [Build Your Own Cat-Shaped USB Hacking Tool! \(with the Nugget\)](#) - Alex Lynd

RTV - [Red Hot \(Red Team TTPs\)](#) - Ralph May,Steve Borosh

RTV - cont...(09:00-10:59 PDT) - [Open Source Intelligence \(OSINT\) for Hackers](#) - Lee McWhorter,Sandra Stibbards

RTV - [Red Team Labs and Games for Kids](#)

RTV - cont...(09:00-10:59 PDT) - [Hacking Meta Quest](#) - Paul D.

SEV - cont...(08:30-17:30 PDT) - [SECV - Youth Challenge](#) -

SEV - cont...(08:30-17:59 PDT) - [SECV Village Open](#)

SEV - [Cold Calls](#) -

SOC - [Hacker Memorial](#) -

SOC - [DCG Meetups](#)

TCV - [Gazing into the crystal ball: Hacking and Securing Future Telecoms Networks](#) - Ajit Hatti,Akib Sayyed,David Rogers,Galina Pildush

TEV - [Tamper Evident Village Activities](#) -

VMV - [Voting Village Opening Remarks](#) - Catherine Terranova,Harri Hursti,Matt Blaze

VMV - (10:30-12:30 PDT) - [First Timers Workshop](#) - Tailor Herrarte

VMV - (10:30-11:25 PDT) - [I Can Shop Securely Online So Why Can't I Vote Online?](#) - David Jefferson,Harri Hursti,Matt Blaze,Susan Greenhalgh

WS - cont...(09:00-12:59 PDT) - [Email Detection Engineering and Threat Hunting Inbox \(Pre-Registration Required\)](#) - Alfie Champion,Josh Kamdjou

WS - cont...(09:00-12:59 PDT) - [Active Directory Attacks: The Good, The Bad, and The LOLwut \(Pre-Registration Required\)](#) - Aaron Rosenmund,Brandon DeVault,Ryan Chapman

WS - cont...(09:00-12:59 PDT) - [The Petting Zoo: Breaking into CTFs \(Pre-Registration Required\)](#) - Christopher Forte,Robert Fitzpatrick

WS - cont...(09:00-12:59 PDT) - [Creating and uncovering malicious containers Redux \(Pre-Registration Required\)](#) - Adrian "threalfall" Wood,David "digish0" Mitchell

WS - cont...(09:00-12:59 PDT) - [BLE Security 201 \(Pre-Registration Required\)](#) - Maxine "Freqy" Filcher,Zach "justadequate" Reavis

XRV - [Haptics Hack-a-Thon](#) -

XRV - [XR Village Playground](#) -

- [AIV - cont...\(10:00-17:59 PDT\) - AI Village Generative Red Team Challenge -](#)
- [AIV - cont...\(10:30-11:25 PDT\) - AI Village Keynote 2: AI red teaming tradecraft: a team of teams approach - Daniel Fabian,Mikel Rodriguez,Sarah Hodkinson](#)
- [AIV - \(11:30-12:25 PDT\) - Creative Misuse of AI Systems - Eryk Salvaggio](#)
- [APV - Getting More Bang for your Buck:Appsec on a Limited Budget - Vandana Verma Sehgal,Viraj Gandhi](#)
- [APV - \(11:45-12:30 PDT\) - Discovering Shadow Vulnerabilities in Popular Open-Source Projects: A Reverse-Fuzzing Journey - Gal Elbaz,Guy Kaplan](#)
- [APV - Hunt the Hacker - Detect compromises in your repositories! - GitGuardian](#)
- [APV - Secure Code Review Challenge - Alon Lerner](#)
- [APV - Spot the True Positives! - Backslash](#)
- [APV - The Ultimate AppSec Trivia Challenge - Probely](#)
- [APV - JWT Parkour - Louis Nyffenegger](#)
- [ASV - cont...\(10:00-17:59 PDT\) - Hack The Airport -](#)
- [ASV - cont...\(10:00-17:59 PDT\) - Unmanned Aerial Systems – Platform Security -](#)
- [ASV - cont...\(10:00-17:59 PDT\) - The Challenge - Lockheed Martin -](#)
- [ASV - cont...\(10:00-17:59 PDT\) - A-ISAC CTF -](#)
- [ASV - cont...\(10:00-17:59 PDT\) - Bricks in the Air -](#)
- [ASV - cont...\(10:00-17:59 PDT\) - ARINC 615a CTF -](#)
- [ASV - cont...\(10:00-17:59 PDT\) - PTP Flight Challenge -](#)
- [ASV - cont...\(10:00-17:59 PDT\) - Ask Me Anything About Cybersecurity in Aerospace -](#)
- [ASV - Hack-A-Sat 4 Briefing - Hack-A-Sat 4 Team](#)
- [BHV - cont...\(10:30-11:10 PDT\) - Homo sapiens sapiens to Homo sapiens nova - the coming speciation - Almost Human \(BJ\)](#)
- [BHV - How to build a body in your garage - Brennan Marsh-Armstrong](#)
- [BHV - \(11:40-12:40 PDT\) - Surgical Physicians and Cybersecurity - Colin Haines](#)
- [BICV - General-purpose Languages: What Are Your Habits? - D.J. Davis](#)
- [BTV - cont...\(10:30-11:30 PDT\) - IR/4n6: Obsidian DFIR - Gang aft agley - Omenscan](#)
- [BTV - \(11:30-12:30 PDT\) - \(n\)Map Exploration: A Great Time in Remote Destinations - SamunoskeX](#)
- [BTV - cont...\(10:30-11:30 PDT\) - DE: Breaking the Rule - Oldmonk](#)
- [BTV - \(11:30-11:59 PDT\) - Forensics 101 Part I & II - Danny D. "B4nd1t0" Henderson Jr,Gyle_dC](#)
- [BTV - cont...\(10:30-11:30 PDT\) - CTH: Log4j - The Silent Menace Among Us - Cyb3rhawk](#)
- [BTV - \(11:30-12:30 PDT\) - DE: Building a Detection Alert From a Threat Hunt - kobaltfox](#)
- [CHV - Automotive USB Fuzzing: How to fuzzing USB in vehicles to discover the real-world vulnerabilities - Donghyeon Jeong,Euntae Jang,Jonghyuk Song](#)
- [CLV - cont...\(10:30-11:10 PDT\) - Between a Log and a Hard Place: \(mis\)Adventures in Azure Logs - Dmitriy Beryoza](#)
- [CLV - SSO Sloppy, SSO Suspect, SSO Vulnerable - Jenko Hwong](#)
- [CLV - \(11:50-12:20 PDT\) - Google Workspace Red Team Automation with SWAT - Justin Ibarra,Terrance DeJesus](#)
- [CON - cont...\(09:00-17:59 PDT\) - HardWired -](#)
- [CON - cont...\(10:30-11:59 PDT\) - Capture The Packet Preliminaries -](#)
- [CON - cont...\(10:00-17:59 PDT\) - IoT Village CTF -](#)
- [CON - cont...\(10:00-17:59 PDT\) - Hardware Hacking Village CTF -](#)
- [CON - cont...\(10:00-17:59 PDT\) - 5n4ck3y -](#)
- [CON - cont...\(10:00-17:59 PDT\) - TeleChallenge -](#)
- [CON - cont...\(10:00-17:59 PDT\) - Hack-A-Sat 4 \(HAS4\) -](#)
- [CON - cont...\(10:00-16:59 PDT\) - Adversary Wars CTF -](#)
- [CON - cont...\(10:00-17:59 PDT\) - The Dark Tangent Look-Alike Contest -](#)
- [CON - cont...\(10:00-17:59 PDT\) - CMD+CTRL at DEF CON 31 - Booth Open -](#)
- [CON - cont...\(10:00-17:59 PDT\) - HackFortress -](#)
- [CON - cont...\(10:00-17:59 PDT\) - Battle of The Bots -](#)
- [CON - cont...\(10:00-17:59 PDT\) - Ham Radio Fox Hunting Contest -](#)
- [CON - cont...\(10:00-17:59 PDT\) - The Gold Bug Challenge -](#)
- [CON - cont...\(10:00-19:59 PDT\) - The Lonely Hard Drive -](#)

CON - cont...(10:00-17:59 PDT) - [Car Hacking Village CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [Tinfoil Hat Contest](#) -
 CON - cont...(10:00-17:59 PDT) - [venator aurum - A Treasure Hunt](#) -
 CON - cont...(10:00-17:59 PDT) - [CrackMelfYouCan](#) -
 CON - cont...(10:00-17:59 PDT) - [It's In That Place Where I Put That Thing That Time](#) -
 CON - cont...(10:00-16:30 PDT) - [Darknet-NG](#) -
 CON - cont...(10:00-17:59 PDT) - [Maps of the digital lands](#) -
 CON - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\)](#) -
 CON - cont...(10:00-13:59 PDT) - [Octopus Game](#) -
 CON - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
 CON - cont...(10:00-17:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -
 CON - cont...(10:00-16:59 PDT) - [Red Alert ICS CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [Dungeons@Defcon](#) -
 CON - cont...(10:00-17:59 PDT) - [Red Team CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [? Cube](#) -
 CON - cont...(10:30-14:30 PDT) - [Trace Labs OSINT Search Party CTF - CTF Platform Open for Submissions](#) -
 CON - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
 CON - cont...(10:30-17:59 PDT) - [Blue Team Village CTF](#) -
 CON - [Free Amateur Radio License Exams](#) -
 CON - cont...(10:00-17:59 PDT) - [Embedded CTF](#) -
 CON - cont...(09:00-17:59 PDT) - [Social Engineering Community \(SEC\) Youth Challenge](#) -
 CON - cont...(10:00-17:59 PDT) - [Cloud Village CTF](#) -
 CON - cont...(10:00-16:59 PDT) - [DC Kubernetes Capture the Flag \(CTF\)](#) -
 CPV - [Ten Years of CPV - Program Committees](#) - CPV Program Committees,CPV Staff
 DC - [Spread spectrum techniques in disposable drones for anti drone evasion](#) - David Melendez,Gabriela "Gabs" García
 DC - cont...(10:00-17:59 PDT) - [Vendor Area Open](#) -
 DC - cont...(09:30-18:59 PDT) - [Human Registration Open](#) -
 DC - cont...(10:30-11:15 PDT) - [Calling it a 0-Day - Hacking at PBX/UC Systems](#) - good_pseudonym
 DC - (11:30-12:15 PDT) - [Physical Attacks Against Smartphones](#) - Christopher Wade
 DC - [Weaponizing Plain Text: ANSI Escape Sequences as a Forensic Nightmare](#) - STÖK
 DC - cont...(10:00-17:59 PDT) - [Exhibitor Area Open](#) -
 DC - cont...(10:30-11:15 PDT) - [Unlocking Doors from Half a Continent Away](#) - Sam Haskins,Trevor "t1v0" Stevado
 DC - (11:30-12:15 PDT) - [Apple's Predicament: NSPredicate Exploitation on macOS and iOS](#) - Austin Emmitt
 DC - cont...(09:00-11:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
 DC - cont...(10:00-17:59 PDT) - [Contest Area Open](#)
 DC - cont...(10:00-11:45 PDT) - [D0 N0 H4RM: A Healthcare Security Conversation](#) - Christian "quaddi" Dameff,Jacqueline Burgette,Jeff "r3plicant" Tully,Mark Warner,Nitin Natarajan,Suzanne Schwartz
 DC - (11:30-12:15 PDT) - [Mass Owning of Seedboxes - A Live Hacking Exhibition](#) - Anon
 DCGVR - (11:35-12:20 PDT) - [Taking Down Applications with Logic: A Comprehensive Guide to Modern DOS Attacks](#) - Abhijeet Singh
 DL - cont...(10:00-11:55 PDT) - [Lambda Looter](#) - Doug Kent,Rob Ditmer
 DL - cont...(10:00-11:55 PDT) - [Lupo: Malware IOC Extractor](#) - Vishal Thakur
 DL - cont...(10:00-11:55 PDT) - [Veilid](#) - Deth Veggie,TC Johnson
 DL - cont...(10:00-11:55 PDT) - [Saturday](#) - Joshua Herman
 DL - cont...(10:00-11:55 PDT) - [The Wifydra: Multiheaded RF Panopticon](#) - Lozaning
 DL - cont...(10:00-11:55 PDT) - [USBvalve - Expose USB activity on the fly](#) - Cesare Pizzi
 ESV - cont...(10:00-17:59 PDT) - [Embedded Systems Village Activities](#) -
 HHV - cont...(10:00-15:30 PDT) - [Make Your Own Use](#) -
 HHV - cont...(10:00-17:59 PDT) - [Soldering Skills Village Activities](#) -
 HHV - cont...(10:00-17:59 PDT) - [RoboSumo Play Time](#) -
 HHV - cont...(10:00-15:30 PDT) - [Hardware Hacking Rube Goldberg Machine](#) -
 HRV - [How to Crush Field Day and Win Big Prizes](#) - Hamster
 ICSV - [Wrenches, Widgets, and Walkdowns: Unraveling the Tangle of Digital Assets in Industrial Control Systems](#) - Tony Turner
 ICSV - (11:30-11:59 PDT) - [Cyber-Physical Detection and Response: A new Paradigm in IACS Monitoring and Security](#) -

Ryan Heartfield

IOTV - cont...(10:00-17:59 PDT) - [Hardware Hacking Your Kitchen](#) -
IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hacking Playground](#) -
IOTV - cont...(10:00-17:59 PDT) - [Critical Infrastructure & IoT Exploitation](#) -
IOTV - cont...(10:00-17:59 PDT) - [Secure or Surrender](#) -
IOTV - cont...(10:00-17:59 PDT) - [The IoT Kill Zone](#) -
IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hardware Hacking Exercises 2023](#) -
IOTV - cont...(10:00-17:59 PDT) - [Embedded Device Security Workshops](#) -
IOTV - cont...(10:00-17:59 PDT) - [Perform Memory Extraction, Emulation and Shellcode](#) -
LPV - cont...(10:00-17:59 PDT) - [Lockpick Village Activities](#) -
MISC - No Starch Press - [Book Signing - Patrick Wardle, The Art of Mac Malware](#)
MISC - No Starch Press - [Book Signing - Maria Markstedter, Blue Fox: Arm Assembly Internals and Reverse Engineering](#) -
Maria Markstedter
MISC - cont...(10:00-16:59 PDT) - [DDV open and accepting drives for duplication](#) -
MISC - cont...(10:00-11:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\) - Kids - Learn Threat Modeling](#) -
MISC - cont...(10:00-15:59 PDT) - [Book Exchange](#) -
MISC - cont...(06:00-11:59 PDT) - [Defcon.run](#) -
MIV - [Evil Digital Twin: Learn Psychological Manipulation with an Uncensored LLM](#) - Ben D. Sawyer,Matthew Canham
MIV - (11:30-12:30 PDT) - [Navigating the Disinformation Landscape](#) - Eric Curwin
PHV - cont...(09:00-17:59 PDT) - [Honey Pot Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [Build Your Own Botnet](#) -
PHV - cont...(09:00-17:59 PDT) - [Wall of Sheep](#) -
PHV - cont...(09:00-17:59 PDT) - [Linux Trainer Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [NetworkOS: Be The Cloud](#) -
PHV - cont...(09:00-17:59 PDT) - [RegEx Trainer](#) -
PHV - cont...(09:00-17:59 PDT) - [Password Lab](#) -
PHV - cont...(09:00-17:59 PDT) - [Fleet DefCon 31 Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [Packet Inspector](#) -
PHV - cont...(09:00-17:59 PDT) - [Packet Detective](#) -
PLV - [AI Caramba! A DC <> DEF CON interface on machine learning](#) - Austin Carson,Erick Galinkin,Kellee
Wicker,Rumman Chowdhury,Tim Ryder
PLV - [Secure by Design: Ask the Government Anything and Red-Pen Workshop](#) - Bob Lord,Cheri Caddy,Jack Cable,Jen
Easterly,Lauren Zabierek,Oumou Ly,Yael Grauer
PLV - cont...(10:00-11:50 PDT) - [How hackers can work with government, industry, civil society to protect high-risk
communities](#) - Adrien Ogee,David Forscey,Mark E. Schreiber,Maurice Kent,Monica M. Ruiz,Sarah Powazek
PSV - cont...(10:00-17:59 PDT) - [Physical Security Village Activities](#) -
PWV - cont...(10:00-17:59 PDT) - [Password Village Activities](#) -
PYV - [Payment Village Workshop](#) - Leigh-Anne Galloway
PYV - [Payment Village Challenges/CTF](#) -
QTV - [Quantum attacks on next-gen cryptosystems: lattices, annealers, notebooks](#) -
RCV - cont...(10:45-11:30 PDT) - [OSINT Privacy Unmasked: Taking Control of Your Digital Footprint in a Hyper-Connected
World](#) - Zoey Selman
RCV - (11:30-12:05 PDT) - [I Am The Disinformation Campaign](#) - MasterChen
RTV - [\(In\)Direct Syscalls: A Journey from High to Low](#) - Daniel Feichter
RTV - cont...(09:00-11:59 PDT) - [Build Your Own Cat-Shaped USB Hacking Tool! \(with the Nugget\)](#) - Alex Lynd
RTV - [Passwords Argh Us](#) - Traveler
RTV - [Artificial Intelligence for Red Team Operations](#) - Peter Halberg
SEV - cont...(08:30-17:30 PDT) - [SECV - Youth Challenge](#) -
SEV - cont...(08:30-17:59 PDT) - [SECV Village Open](#)
SEV - cont...(10:00-11:30 PDT) - [Cold Calls](#) -
SEV - (11:30-13:30 PDT) - [SE Improv](#) -
SOC - cont...(10:00-17:59 PDT) - [Hacker Memorial](#) -
SOC - cont...(10:00-17:59 PDT) - [DCG Meetups](#)
TCV - [Diameter Workshop](#) - Akib Sayyed,Zibran Sayyed
TEV - cont...(10:00-17:59 PDT) - [Tamper Evident Village Activities](#) -

[VMV](#) - cont...(10:30-12:30 PDT) - [First Timers Workshop](#) - Tailor Herrarte
[VMV](#) - cont...(10:30-11:25 PDT) - [I Can Shop Securely Online So Why Can't I Vote Online?](#) - David Jefferson,Harri Hursti,Matt Blaze,Susan Greenhalgh
[VMV](#) - (11:30-12:15 PDT) - [Chinese Prototype Review](#) - William Baggett
[VMV](#) - (11:30-11:59 PDT) - [VOTEC Corporation](#) - John Medcalf
[WS](#) - cont...(09:00-12:59 PDT) - [Email Detection Engineering and Threat Hunting Inbox \(Pre-Registration Required\)](#) - Alfie Champion,Josh Kamdjou
[WS](#) - cont...(09:00-12:59 PDT) - [Active Directory Attacks: The Good, The Bad, and The LOLwut \(Pre-Registration Required\)](#) - Aaron Rosenmund,Brandon DeVault,Ryan Chapman
[WS](#) - cont...(09:00-12:59 PDT) - [The Petting Zoo: Breaking into CTFs \(Pre-Registration Required\)](#) - Christopher Forte,Robert Fitzpatrick
[WS](#) - cont...(09:00-12:59 PDT) - [Creating and uncovering malicious containers Redux \(Pre-Registration Required\)](#) - Adrian "threfall" Wood,David "digish0" Mitchell
[WS](#) - cont...(09:00-12:59 PDT) - [BLE Security 201 \(Pre-Registration Required\)](#) - Maxine "Freqy" Filcher,Zach "justadequate" Reavis
[XRV](#) - cont...(10:00-15:59 PDT) - [Haptics Hack-a-Thon](#) -
[XRV](#) - cont...(10:00-17:59 PDT) - [XR Village Playground](#) -
[XRV](#) - [Off the Rails: A demo with Pacific Northwest National Labs](#) -

[AIV](#) - cont...(10:00-17:59 PDT) - [AI Village Generative Red Team Challenge](#) -
[AIV](#) - cont...(11:30-12:25 PDT) - [Creative Misuse of AI Systems](#) - Eryk Salvaggio
[AIV](#) - (12:30-13:25 PDT) - [LLM Legal Risk Management, and Use Case Development Strategies to Minimize Risk](#) - Nick Maietta,Robert Hudock
[APV](#) - cont...(11:45-12:30 PDT) - [Discovering Shadow Vulnerabilities in Popular Open-Source Projects: A Reverse-Fuzzing Journey](#) - Gal Elbaz,Guy Kaplan
[APV](#) - (12:30-13:30 PDT) - [Not All Alerts Are Born Equal: Insights from AppSec Experts on Prioritizing Security Alerts](#) - Joe Christian,Kunal Bhattacharya,Shahar Man,Trupti Shiralkar
[APV](#) - cont...(11:00-12:59 PDT) - [Hunt the Hacker - Detect compromises in your repositories!](#) - GitGuardian
[APV](#) - cont...(11:00-12:59 PDT) - [Secure Code Review Challenge](#) - Alon Lerner
[APV](#) - cont...(11:00-12:59 PDT) - [Spot the True Positives!](#) - Backslash
[APV](#) - cont...(11:00-12:59 PDT) - [The Ultimate AppSec Trivia Challenge](#) - Probely
[APV](#) - cont...(11:00-12:59 PDT) - [JWT Parkour](#) - Louis Nyffenegger
[ASV](#) - cont...(10:00-17:59 PDT) - [Hack The Airport](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Unmanned Aerial Systems – Platform Security](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [The Challenge - Lockheed Martin](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [A-ISAC CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [ARINC 615a CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [PTP Flight Challenge](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Ask Me Anything About Cybersecurity in Aerospace](#) -
[ASV](#) - [CON trolling the weather](#) - Paz Hameiri
[ASV](#) - (12:30-13:20 PDT) - [Building Space Attack Chains using SPARTA](#) - Brandon Bailey
[BHV](#) - cont...(11:40-12:40 PDT) - [Surgical Physicians and Cybersecurity](#) - Colin Haines
[BHV](#) - (12:40-13:50 PDT) - [Medical VR](#) - David Nathans,Ernest Liu
[BTV](#) - cont...(11:30-12:30 PDT) - [\(n\)Map Exploration: A Great Time in Remote Destinations](#) - SamunoskeX
[BTV](#) - cont...(11:30-12:30 PDT) - [DE: Building a Detection Alert From a Threat Hunt](#) - kobaltfox
[CHV](#) - [Abusing CAN Bus Protocol Specification for Denial of Service in Embedded Systems](#) - Martin Petran
[CLV](#) - cont...(11:50-12:20 PDT) - [Google Workspace Red Team Automation with SWAT](#) - Justin Ibarra,Terrance DeJesus
[CLV](#) - (12:20-12:59 PDT) - [The Rocky Balboa Guide to Security Research: Getting Back Up When You Get Knocked Down](#) - Liv Matan
[CON](#) - cont...(09:00-17:59 PDT) - [HardWired](#) -
[CON](#) - [Capture The Packet Main Rounds](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [IoT Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hardware Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [5n4ck3y](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hack-A-Sat 4 \(HAS4\)](#) -
[CON](#) - cont...(10:00-16:59 PDT) - [Adversary Wars CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Dark Tangent Look-Alike Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL at DEF CON 31 - Booth Open](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Battle of The Bots](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Ham Radio Fox Hunting Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Gold Bug Challenge](#) -
[CON](#) - cont...(10:00-19:59 PDT) - [The Lonely Hard Drive](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Tinfoil Hat Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [venator aurum - A Treasure Hunt](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CrackMelfYouCan](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [It's In That Place Where I Put That Thing That Time](#) -

CON - cont...(10:00-16:30 PDT) - [Darknet-NG](#) -
 CON - cont...(10:00-17:59 PDT) - [Maps of the digital lands](#) -
 CON - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\)](#) -
 CON - cont...(10:00-13:59 PDT) - [Octopus Game](#) -
 CON - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
 CON - cont...(10:00-17:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -
 CON - cont...(10:00-16:59 PDT) - [Red Alert ICS CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [Dungeons@Defcon](#) -
 CON - cont...(10:00-17:59 PDT) - [Red Team CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [? Cube](#) -
 CON - cont...(10:30-14:30 PDT) - [Trace Labs OSINT Search Party CTF - CTF Platform Open for Submissions](#) -
 CON - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
 CON - cont...(10:30-17:59 PDT) - [Blue Team Village CTF](#) -
 CON - cont...(11:00-16:59 PDT) - [Free Amateur Radio License Exams](#) -
 CON - cont...(10:00-17:59 PDT) - [Embedded CTF](#) -
 CON - cont...(09:00-17:59 PDT) - [Social Engineering Community \(SEC\) Youth Challenge](#) -
 CON - [TOOOL Dozier Drill Lockpicking Challenge](#) -
 CON - cont...(10:00-17:59 PDT) - [Cloud Village CTF](#) -
 CON - cont...(10:00-16:59 PDT) - [DC Kubernetes Capture the Flag \(CTF\)](#) -
 CPV - [Ten Years of CPV - The Gold Bug Challenge](#) - CPV Staff,Gold Bug Challenge Team
 CPV - [About Face! Beginner Intro to Facial Recognition](#) - Kate
 DC - [From Feature to Weapon: Breaking Microsoft Teams and SharePoint Integrity](#) - Nestori Syynimaa
 DC - cont...(10:00-17:59 PDT) - [Vendor Area Open](#) -
 DC - cont...(09:30-18:59 PDT) - [Human Registration Open](#) -
 DC - cont...(11:30-12:15 PDT) - [Physical Attacks Against Smartphones](#) - Christopher Wade
 DC - (12:30-13:15 PDT) - [Video-based Cryptanalysis: Extracting Secret Keys from Power LEDs of Various Non-compromised Devices Using a Video Camera](#) - Ben Nassi,Ofek Vayner
 DC - [Internet censorship: what governments around the globe have in store for you](#) - Christopher Painter,Jeff "The Dark Tangent" Moss,Joel Todoroff,Roger Dingledine
 DC - cont...(10:00-17:59 PDT) - [Exhibitor Area Open](#) -
 DC - cont...(11:30-12:15 PDT) - [Apple's Predicament: NSPredicate Exploitation on macOS and iOS](#) - Austin Emmitt
 DC - (12:30-13:15 PDT) - [An Audacious Plan to Halt the Internet's Enshittification](#) - Cory Doctorow
 DC - cont...(10:00-17:59 PDT) - [Contest Area Open](#)
 DC - [Lonely Hackers Club - Resume Reviews & Career Advice](#)
 DC - cont...(11:30-12:15 PDT) - [Mass Owning of Seedboxes - A Live Hacking Exhibition](#) - Anon
 DC - (12:30-13:30 PDT) - [Metawar](#) - Winn
 DCGVR - cont...(11:35-12:20 PDT) - [Taking Down Applications with Logic: A Comprehensive Guide to Modern DOS Attacks](#) - Abhijeet Singh
 DCGVR - (12:35-13:20 PDT) - [The Curse of Ncurses](#) - Jonathan Bar Or
 DL - [BBOT \(Bighuge BLS OSINT Tool\)](#) - Joel "TheTechromancer" Moore,Paul Mueller
 DL - [Abusing Microsoft SQL Server with SQLRecon](#) - Sanjiv Kawa
 DL - [Red Wizard: user-friendly Red Teaming infrastructure](#) - Ben Brücker
 DL - [Am I Exploitable? \(MI-X\)](#) - Ofri Ouzan,Yotam Perkal
 DL - [Kraken, a modular multi-language webshell for defense evasion](#) - Raul Caro
 DL - [Pcapinator: Rise of the PCAP Machines](#) - Henry Hill,Mike "d4rkm4tter" Spicer
 ESV - cont...(10:00-17:59 PDT) - [Embedded Systems Village Activities](#) -
 HHV - cont...(10:00-15:30 PDT) - [Make Your Own Use](#) -
 HHV - cont...(10:00-17:59 PDT) - [Soldering Skills Village Activities](#) -
 HHV - cont...(10:00-17:59 PDT) - [RoboSumo Play Time](#) -
 HHV - cont...(10:00-15:30 PDT) - [Hardware Hacking Rube Goldberg Machine](#) -
 ICSV - [Fear and Loathing on Plum Island](#) - David Emmerich,Emma Stewart,Jeremy Jones,Joe Minicucci
 IOTV - cont...(10:00-17:59 PDT) - [Hardware Hacking Your Kitchen](#) -
 IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hacking Playground](#) -
 IOTV - cont...(10:00-17:59 PDT) - [Critical Infrastructure & IoT Exploitation](#) -
 IOTV - cont...(10:00-17:59 PDT) - [Secure or Surrender](#) -

IOTV - cont...(10:00-17:59 PDT) - [The IoT Kill Zone](#) -
IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hardware Hacking Exercises 2023](#) -
IOTV - cont...(10:00-17:59 PDT) - [Embedded Device Security Workshops](#) -
IOTV - cont...(10:00-17:59 PDT) - [Perform Memory Extraction, Emulation and Shellcode](#) -
LPV - cont...(10:00-17:59 PDT) - [Lockpick Village Activities](#) -
MISC - No Starch Press - Book Signing - Daniel Reilly, Math for Security
MISC - cont...(10:00-16:59 PDT) - [DDV open and accepting drives for duplication](#) -
MISC - cont...(10:00-15:59 PDT) - [Book Exchange](#) -
MIV - cont...(11:30-12:30 PDT) - [Navigating the Disinformation Landscape](#) - Eric Curwin
MIV - (12:30-13:30 PDT) - [Patient Zero Day: The Leaking of Patients' Private Health Data Contributed To A Medical Infodemic](#) - Andrea Downing
PHV - cont...(09:00-17:59 PDT) - [Honey Pot Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [Build Your Own Botnet](#) -
PHV - cont...(09:00-17:59 PDT) - [Wall of Sheep](#) -
PHV - cont...(09:00-17:59 PDT) - [Linux Trainer Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [NetworkOS: Be The Cloud](#) -
PHV - cont...(09:00-17:59 PDT) - [RegEx Trainer](#) -
PHV - cont...(09:00-17:59 PDT) - [Password Lab](#) -
PHV - cont...(09:00-17:59 PDT) - [Fleet DefCon 31 Workshop](#) -
PHV - cont...(09:00-17:59 PDT) - [Packet Inspector](#) -
PHV - cont...(09:00-17:59 PDT) - [Packet Detective](#) -
PLV - [Hands On a Cyber Policy Crisis: Testing Assumptions and Navigating Challenges through a Cyber Simulation](#) - Safa Shahwan Edwards
PLV - cont...(11:00-13:50 PDT) - [Secure by Design: Ask the Government Anything and Red-Pen Workshop](#) - Bob Lord,Cheri Caddy,Jack Cable,Jen Easterly,Lauren Zabierek,Oumou Ly,Yael Grauer
PLV - [The Coming War on Encryption, Part 3 \(and how you can fight back\)](#) - India McKinney
PSV - cont...(10:00-17:59 PDT) - [Physical Security Village Activities](#) -
PSV - [RFID Hacking](#) - Ege
PSV - (12:30-13:15 PDT) - [Physical pentesting in a post-covid world](#) - Brian Halbach
PWV - cont...(10:00-17:59 PDT) - [Password Village Activities](#) -
PYV - cont...(11:00-12:30 PDT) - [Payment Village Workshop](#) - Leigh-Anne Galloway
PYV - cont...(11:00-17:59 PDT) - [Payment Village Challenges/CTF](#) -
QTV - cont...(11:00-12:30 PDT) - [Quantum attacks on next-gen cryptosystems: lattices, annealers, notebooks](#) -
RCV - cont...(11:30-12:05 PDT) - [I Am The Disinformation Campaign](#) - MasterChen
RCV - [How I Built Recon to Scale with Serverless Architecture](#) - Gunnar Andrews
RFV - [Shipping Wardriving Hardware - Cross-country Wigle on the Cheap](#) - Segfault
RTV - cont...(11:00-16:59 PDT) - [\(In\)Direct Syscalls: A Journey from High to Low](#) - Daniel Feichter
RTV - [Hacking Web Apps and APIs with WebSploit Labs](#) - Omar Santos
RTV - [Red Hot \(Red Team TTPs\)](#) - Ralph May,Steve Borosh
RTV - [Scripting OWASP Amass for a Customized Experience](#) - Jeff Foley
RTV - cont...(11:00-12:59 PDT) - [Artificial Intelligence for Red Team Operations](#) - Peter Halberg
SEV - cont...(08:30-17:30 PDT) - [SECV - Youth Challenge](#) -
SEV - cont...(08:30-17:59 PDT) - [SECV Village Open](#)
SEV - cont...(11:30-13:30 PDT) - [SE Improv](#) -
SOC - cont...(10:00-17:59 PDT) - [Hacker Memorial](#) -
SOC - [Lonely Hackers Club Meetup](#) -
SOC - cont...(10:00-17:59 PDT) - [DCG Meetups](#)
SOC - [Friends of Bill W](#) -
SOC - [HDA / Accessibility Area Open](#)
SOC - [HDA Community Meetups](#)
TCV - cont...(11:00-12:59 PDT) - [Diameter Workshop](#) - Akib Sayyed,Zibrán Sayyed
TEV - cont...(10:00-17:59 PDT) - [Tamper Evident Village Activities](#) -
VMV - cont...(10:30-12:30 PDT) - [First Timers Workshop](#) - Tailor Herrarte
VMV - cont...(11:30-12:15 PDT) - [Chinese Prototype Review](#) - William Baggett
VMV - (12:20-12:50 PDT) - [US private elections: the easy way in for foreign adversaries.](#) - Scheme

[VMV](#) - (12:30-13:20 PDT) - [Review: Surprise Unboxing](#) - Harri Hursti
[VMV](#) - (12:55-13:40 PDT) - [Conflicting Security Reports from Halderman-Springall and from MITRE: Which Is Right?](#) - David Jefferson,Drew Springall,Richard DeMillo
[WS](#) - cont...(09:00-12:59 PDT) - [Email Detection Engineering and Threat Hunting Inbox \(Pre-Registration Required\)](#) - Alfie Champion,Josh Kamdjou
[WS](#) - cont...(09:00-12:59 PDT) - [Active Directory Attacks: The Good, The Bad, and The LOLwut \(Pre-Registration Required\)](#) - Aaron Rosenmund,Brandon DeVault,Ryan Chapman
[WS](#) - cont...(09:00-12:59 PDT) - [The Petting Zoo: Breaking into CTFs \(Pre-Registration Required\)](#) - Christopher Forte,Robert Fitzpatrick
[WS](#) - cont...(09:00-12:59 PDT) - [Creating and uncovering malicious containers Redux \(Pre-Registration Required\)](#) - Adrian "threlfall" Wood,David "digish0" Mitchell
[WS](#) - cont...(09:00-12:59 PDT) - [BLE Security 201 \(Pre-Registration Required\)](#) - Maxine "Freqy" Filcher,Zach "justadequate" Reavis
[XRV](#) - cont...(10:00-15:59 PDT) - [Haptics Hack-a-Thon](#) -
[XRV](#) - cont...(10:00-17:59 PDT) - [XR Village Playground](#) -
[XRV](#) - cont...(11:00-16:59 PDT) - [Off the Rails: A demo with Pacific Northwest National Labs](#) -

[AIV](#) - cont...(10:00-17:59 PDT) - [AI Village Generative Red Team Challenge](#) -
[AIV](#) - cont...(12:30-13:25 PDT) - [LLM Legal Risk Management, and Use Case Development Strategies to Minimize Risk](#) -
Nick Maietta,Robert Hudock
[AIV](#) - (13:30-14:25 PDT) - [The Sinister Synergy of Advanced AI: Automatically Orchestrating Large-scale Scam Campaigns
with Large Generative Models](#) - Ben Gelman,Younghoo Lee
[APV](#) - [For Kids: Castle Defenders](#) - Pentera
[APV](#) - cont...(12:30-13:30 PDT) - [Not All Alerts Are Born Equal: Insights from AppSec Experts on Prioritizing Security
Alerts](#) - Joe Christian,Kunal Bhattacharya,Shahar Man,Trupti Shiralkar
[APV](#) - (13:30-14:15 PDT) - [Dress Code - Analysis of the current status of the Content Security Policy](#) - Felipe Molina
[APV](#) - [How to Hide Behavior from Security Tools](#) - Deepfactor
[APV](#) - [Open Source API Security for devsecops](#) - Ankita Gupta,Ankush Jain
[APV](#) - [The Ultimate AppSec Trivia Challenge](#) - Probely
[APV](#) - [Secure from Scratch: Secure Code Workshop for DEF CON Kids](#) - Or Sahar,Yariv Tal
[ASV](#) - cont...(10:00-17:59 PDT) - [Hack The Airport](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Unmanned Aerial Systems – Platform Security](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [The Challenge - Lockheed Martin](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [A-ISAC CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [ARINC 615a CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [PTP Flight Challenge](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Ask Me Anything About Cybersecurity in Aerospace](#) -
[ASV](#) - cont...(12:30-13:20 PDT) - [Building Space Attack Chains using SPARTA](#) - Brandon Bailey
[ASV](#) - (13:30-13:55 PDT) - [Elon, Twitter and the PIA: How not to achieve privacy in aviation](#) - Martin Strohmeier
[BHV](#) - cont...(12:40-13:50 PDT) - [Medical VR](#) - David Nathans,Ernest Liu
[BHV](#) - (13:50-14:50 PDT) - [Full Stack Disclosures](#) - Edison Alvarez,Alex Mastrov,Matias Katz
[BICV](#) - [Why don't we have Internet, Daddy?](#) - Jess Hoffman
[BTV](#) - (13:30-14:30 PDT) - [So you want to become a Detection Engineer](#) - Ben Bornholm,CerealKiller,kobaltfox,plug
[BTV](#) - (13:30-13:59 PDT) - [CTH 101: Part III, IV, V](#) - Cyb3rhawk
[BTV](#) - (13:30-14:30 PDT) - [Why OT Cybersecurity Engineers Drink So Much](#) - ThatDeadGuy
[CLV](#) - [CloudRecon - finding ephemeral assets in the cloud](#) - Gunnar Andrews,Jason Haddix
[CLV](#) - (13:30-14:10 PDT) - [What the Function: A Deep Dive into Azure Function App Security](#) - Karl Fosaaen,Thomas Elling
[CON](#) - cont...(09:00-17:59 PDT) - [HardWired](#) -
[CON](#) - cont...(12:00-17:59 PDT) - [Capture The Packet Main Rounds](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [IoT Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hardware Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [5n4ck3y](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hack-A-Sat 4 \(HAS4\)](#) -
[CON](#) - cont...(10:00-16:59 PDT) - [Adversary Wars CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Dark Tangent Look-Alike Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL at DEF CON 31 - Booth Open](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Battle of The Bots](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Ham Radio Fox Hunting Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Gold Bug Challenge](#) -
[CON](#) - cont...(10:00-19:59 PDT) - [The Lonely Hard Drive](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Tinfoil Hat Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [venator aurum - A Treasure Hunt](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CrackMelfYouCan](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [It's In That Place Where I Put That Thing That Time](#) -

CON - cont...(10:00-16:30 PDT) - [Darknet-NG](#) -
CON - cont...(10:00-17:59 PDT) - [Maps of the digital lands](#) -
CON - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\)](#) -
CON - cont...(10:00-13:59 PDT) - [Octopus Game](#) -
CON - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
CON - cont...(10:00-17:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -
CON - cont...(10:00-16:59 PDT) - [Red Alert ICS CTF](#) -
CON - cont...(10:00-17:59 PDT) - [Dungeons@Defcon](#) -
CON - cont...(10:00-17:59 PDT) - [Red Team CTF](#) -
CON - cont...(10:00-17:59 PDT) - [? Cube](#) -
CON - cont...(10:30-14:30 PDT) - [Trace Labs OSINT Search Party CTF - CTF Platform Open for Submissions](#) -
CON - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
CON - cont...(10:30-17:59 PDT) - [Blue Team Village CTF](#) -
CON - cont...(11:00-16:59 PDT) - [Free Amateur Radio License Exams](#) -
CON - cont...(10:00-17:59 PDT) - [Embedded CTF](#) -
CON - cont...(09:00-17:59 PDT) - [Social Engineering Community \(SEC\) Youth Challenge](#) -
CON - cont...(12:00-14:59 PDT) - [TOOOL Dozier Drill Lockpicking Challenge](#) -
CON - cont...(10:00-17:59 PDT) - [Cloud Village CTF](#) -
CON - cont...(10:00-16:59 PDT) - [DC Kubernetes Capture the Flag \(CTF\)](#) -
CPV - [Is 2023 the Year of Privacy: How History and States are Posed to Change Privacy?](#) - Anthony Hendricks
CPV - (13:30-13:59 PDT) - [Domain Fronting Through Microsoft Azure and CloudFlare: How to Identify Viable Domain Fronting Proxies](#) - Charles Miller,Michael Brown,Michael Pelosi
DC - [Azure B2C 0-Day: An Exploit Chain from Public Keys to Microsoft Bug Bounty](#) - John Novak
DC - cont...(10:00-17:59 PDT) - [Vendor Area Open](#) -
DC - cont...(09:30-18:59 PDT) - [Human Registration Open](#) -
DC - cont...(12:30-13:15 PDT) - [Video-based Cryptanalysis: Extracting Secret Keys from Power LEDs of Various Non-compromised Devices Using a Video Camera](#) - Ben Nassi,Ofek Vayner
DC - (13:30-14:15 PDT) - [Meduza: How an exiled pirate media outlet breaks through the Kremlin's propaganda firewall](#) - Alex
DC - [Looking into the future, what can we learn about hacking in science-fiction?](#) - Nicolas Minvielle,Xavier Facéline
DC - cont...(10:00-17:59 PDT) - [Exhibitor Area Open](#) -
DC - cont...(12:30-13:15 PDT) - [An Audacious Plan to Halt the Internet's Enshittification](#) - Cory Doctorow
DC - (13:30-14:15 PDT) - [The GitHub Actions Worm: Compromising GitHub repositories through the Actions dependency tree](#) - Asi Greenholts
DC - cont...(10:00-17:59 PDT) - [Contest Area Open](#)
DC - cont...(12:00-13:59 PDT) - [Lonely Hackers Club - Resume Reviews & Career Advice](#)
DC - cont...(12:30-13:30 PDT) - [Metawar](#) - Winn
DCGVR - cont...(12:35-13:20 PDT) - [The Curse of Ncurses](#) - Jonathan Bar Or
DCGVR - (13:35-14:05 PDT) - [Bootsquad: Stomping out squatters](#) - Joe Mast
DL - cont...(12:00-13:55 PDT) - [BBOT \(Bighuge BLS OSINT Tool\)](#) - Joel "TheTechromancer" Moore,Paul Mueller
DL - cont...(12:00-13:55 PDT) - [Abusing Microsoft SQL Server with SQLRecon](#) - Sanjiv Kawa
DL - cont...(12:00-13:55 PDT) - [Red Wizard: user-friendly Red Teaming infrastructure](#) - Ben Brücker
DL - cont...(12:00-13:55 PDT) - [Am I Exploitable? \(MI-X\)](#) - Ofri Ouzan,Yotam Perkal
DL - cont...(12:00-13:55 PDT) - [Kraken, a modular multi-language webshell for defense evasion](#) - Raul Caro
DL - cont...(12:00-13:55 PDT) - [Pcapinator: Rise of the PCAP Machines](#) - Henry Hill,Mike "d4rkm4tter" Spicer
ESV - cont...(10:00-17:59 PDT) - [Embedded Systems Village Activities](#) -
HHV - cont...(10:00-15:30 PDT) - [Make Your Own Use](#) -
HHV - cont...(10:00-17:59 PDT) - [Soldering Skills Village Activities](#) -
HHV - cont...(10:00-17:59 PDT) - [RoboSumo Play Time](#) -
HHV - cont...(10:00-15:30 PDT) - [Hardware Hacking Rube Goldberg Machine](#) -
HHV - [RoboSumo Bracket Competition](#) -
HRV - [Using an SBC for ham radio digital modes that isn't a raspberry pi](#) - Jon Marler
ICSV - cont...(12:00-13:30 PDT) - [Fear and Loathing on Plum Island](#) - David Emmerich,Emma Stewart,Jeremy Jones,Joe Minicucci
ICSV - (13:30-14:59 PDT) - [Panel Discussion -- Designing and Deploying NOC/SOC in a Mobile, Limited Bandwidth](#)

[Maritime Environment](#) - Brad Proctor,Cliff Neve,Danny Joslin,Peter Dreyer,Tom Stites
[IOTV - cont...\(10:00-17:59 PDT\) - Hardware Hacking Your Kitchen](#) -
[IOTV - cont...\(10:00-17:59 PDT\) - IoT Village Hacking Playground](#) -
[IOTV - cont...\(10:00-17:59 PDT\) - Critical Infrastructure & IoT Exploitation](#) -
[IOTV - cont...\(10:00-17:59 PDT\) - Secure or Surrender](#) -
[IOTV - cont...\(10:00-17:59 PDT\) - The IoT Kill Zone](#) -
[IOTV - cont...\(10:00-17:59 PDT\) - IoT Village Hardware Hacking Exercises 2023](#) -
[IOTV - cont...\(10:00-17:59 PDT\) - Embedded Device Security Workshops](#) -
[IOTV - cont...\(10:00-17:59 PDT\) - Perform Memory Extraction, Emulation and Shellcode](#) -
[LPV - cont...\(10:00-17:59 PDT\) - Lockpick Village Activities](#) -
[MISC - No Starch Press - Book Signing](#) - Jos Weyers, Matt Burrough & BandEatoZ, Locksport
[MISC - cont...\(10:00-16:59 PDT\) - DDV open and accepting drives for duplication](#) -
[MISC - cont...\(10:00-15:59 PDT\) - Book Exchange](#) -
[MISC - DC's Next Top Threat Model \(DCNTTM\) - BYODesign Presentation](#) -
[MIV - cont...\(12:30-13:30 PDT\) - Patient Zero Day: The Leaking of Patients' Private Health Data Contributed To A Medical Infodemic](#) - Andrea Downing
[MIV - \(13:30-14:30 PDT\) - Main features of Russia's disinformation and propaganda ecosystem in Spanish-speaking countries](#) - Carlos Galán
[PHV - cont...\(09:00-17:59 PDT\) - Honey Pot Workshop](#) -
[PHV - cont...\(09:00-17:59 PDT\) - Build Your Own Botnet](#) -
[PHV - cont...\(09:00-17:59 PDT\) - Wall of Sheep](#) -
[PHV - cont...\(09:00-17:59 PDT\) - Linux Trainer Workshop](#) -
[PHV - cont...\(09:00-17:59 PDT\) - NetworkOS: Be The Cloud](#) -
[PHV - cont...\(09:00-17:59 PDT\) - RegEx Trainer](#) -
[PHV - cont...\(09:00-17:59 PDT\) - Password Lab](#) -
[PHV - cont...\(09:00-17:59 PDT\) - Fleet DefCon 31 Workshop](#) -
[PHV - cont...\(09:00-17:59 PDT\) - Packet Inspector](#) -
[PHV - cont...\(09:00-17:59 PDT\) - Packet Detective](#) -
[PLV - cont...\(12:00-13:50 PDT\) - Hands On a Cyber Policy Crisis: Testing Assumptions and Navigating Challenges through a Cyber Simulation](#) - Safa Shahwan Edwards
[PLV - cont...\(11:00-13:50 PDT\) - Secure by Design: Ask the Government Anything and Red-Pen Workshop](#) - Bob Lord,Cheri Caddy,Jack Cable,Jen Easterly,Lauren Zabierek,Oumou Ly,Yael Grauer
[PLV - Beyond the Breach: Exploring Cybersecurity Policies with Hacker Perspectives](#) - Andrés Velázquez,Isabella Rolz,Mauro Vignati,Orlando Garces
[PSV - cont...\(10:00-17:59 PDT\) - Physical Security Village Activities](#) -
[PSV - cont...\(12:30-13:15 PDT\) - Physical pentesting in a post-covid world](#) - Brian Halbach
[PSV - \(13:15-13:30 PDT\) - Free Pokemon Card Bus Passes](#) - Jarvis,Malcolm
[PWV - cont...\(10:00-17:59 PDT\) - Password Village Activities](#) -
[PYV - cont...\(11:00-17:59 PDT\) - Payment Village Challenges/CTF](#) -
[QTV - QDoor: Exploiting Approximate Synthesis for Backdoor Attacks in Quantum Neural Networks](#) - Lei Jiang
[RFV - 125khz the Brown note for Cars](#) - Woody
[RTV - cont...\(11:00-16:59 PDT\) - \(In\)Direct Syscalls: A Journey from High to Low](#) - Daniel Feichter
[RTV - How to \[NOT\] look like a Red Team](#) - Michael Wylie
[RTV - Storfield: A Quiet Methodology to Create Attacks in Mature Networks](#) - Cory Wolff
[RTV - cont...\(12:00-13:59 PDT\) - Scripting OWASP Amass for a Customized Experience](#) - Jeff Foley
[RTV - How Most Internal Networks are Compromised: A Set of Common Active Directory Attacks and How to Perform Them from Linux](#) - Scott Brink
[SEV - cont...\(08:30-17:30 PDT\) - SECV - Youth Challenge](#) -
[SEV - cont...\(08:30-17:59 PDT\) - SECV Village Open](#)
[SEV - cont...\(11:30-13:30 PDT\) - SE Improv](#) -
[SEV - \(13:30-15:30 PDT\) - Cold Calls](#) -
[SOC - cont...\(10:00-17:59 PDT\) - Hacker Memorial](#) -
[SOC - cont...\(12:00-17:59 PDT\) - Lonely Hackers Club Meetup](#) -
[SOC - cont...\(10:00-17:59 PDT\) - DCG Meetups](#)
[SOC - cont...\(12:00-17:59 PDT\) - HDA / Accessibility Area Open](#)

[SOC](#) - cont...(12:00-17:59 PDT) - HDA Community Meetups
[TEV](#) - cont...(10:00-17:59 PDT) - [Tamper Evident Village Activities](#) -
[VMV](#) - cont...(12:30-13:20 PDT) - [Review: Surprise Unboxing](#) - Harri Hursti
[VMV](#) - cont...(12:55-13:40 PDT) - [Conflicting Security Reports from Halderman-Springall and from MITRE: Which Is Right?](#) - David Jefferson,Drew Springall,Richard DeMillo
[VMV](#) - (13:30-14:20 PDT) - [Interventions To Address Technology-Facilitated Violence in Democracy](#) - Eric Davis,Hallie Stern,Omri Preiss,Theodora Skeadas
[VMV](#) - (13:55-14:35 PDT) - [Political Polarization](#) - Constantine Nicolaidis
[XRV](#) - cont...(10:00-15:59 PDT) - [Haptics Hack-a-Thon](#) -
[XRV](#) - cont...(10:00-17:59 PDT) - [XR Village Playground](#) -
[XRV](#) - cont...(11:00-16:59 PDT) - [Off the Rails: A demo with Pacific Northwest National Labs](#) -
[XRV](#) - [XR implications on Mobile Security](#) - Whitney Phillips

[AIV](#) - cont...(10:00-17:59 PDT) - [AI Village Generative Red Team Challenge](#) -
[AIV](#) - cont...(13:30-14:25 PDT) - [The Sinister Synergy of Advanced AI: Automatically Orchestrating Large-scale Scam Campaigns with Large Generative Models](#) - Ben Gelman, Younghoo Lee
[APV](#) - cont...(13:00-14:59 PDT) - [For Kids: Castle Defenders](#) - Pentera
[APV](#) - cont...(13:30-14:15 PDT) - [Dress Code - Analysis of the current status of the Content Security Policy](#) - Felipe Molina
[APV](#) - (14:15-14:59 PDT) - [MitmWs: A new way to pentest websocket applications](#) - Jon F
[APV](#) - cont...(13:00-14:59 PDT) - [How to Hide Behavior from Security Tools](#) - Deepfactor
[APV](#) - cont...(13:00-14:59 PDT) - [Open Source API Security for devsecops](#) - Ankita Gupta, Ankush Jain
[APV](#) - cont...(13:00-14:59 PDT) - [The Ultimate AppSec Trivia Challenge](#) - Probely
[APV](#) - cont...(13:00-14:59 PDT) - [Secure from Scratch: Secure Code Workshop for DEF CON Kids](#) - Or Sahar, Yariv Tal
[ASV](#) - cont...(10:00-17:59 PDT) - [Hack The Airport](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Unmanned Aerial Systems – Platform Security](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [The Challenge - Lockheed Martin](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [A-ISAC CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [ARINC 615a CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [PTP Flight Challenge](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Ask Me Anything About Cybersecurity in Aerospace](#) -
[ASV](#) - [Labs and Trust: How to build a successful aviation cybersecurity research programme](#) - Martin Strohmeier
[ASV](#) - (14:30-14:55 PDT) - [Stories from the Trenches: Operating a Aeronautics Cyber Range](#) - Christopher Ottesen
[BHV](#) - cont...(13:50-14:50 PDT) - [Full Stack Disclosures](#) - Edison Alvarez, Alex Mastrov, Matias Katz
[BHV](#) - (14:50-15:30 PDT) - [Lanternyn: Blue Energy](#) - Del de Zela
[BTV](#) - cont...(13:30-14:30 PDT) - [So you want to become a Detection Engineer](#) - Ben Bornholm, CerealKiller, kobaltfox, plug
[BTV](#) - cont...(13:30-14:30 PDT) - [Why OT Cybersecurity Engineers Drink So Much](#) - ThatDeadGuy
[CLV](#) - cont...(13:30-14:10 PDT) - [What the Function: A Deep Dive into Azure Function App Security](#) - Karl Fosaaen, Thomas Elling
[CLV](#) - [Bridging the Gap: Cloud Threat Intelligence for Detection and Offensive Security Practitioners](#) - Alex Delamotte
[CLV](#) - (14:50-15:35 PDT) - [The Human Threat Factor - Cloud Security Misconfigurations](#) - Kat Fitzgerald
[CON](#) - cont...(09:00-17:59 PDT) - [HardWired](#) -
[CON](#) - cont...(12:00-17:59 PDT) - [Capture The Packet Main Rounds](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [IoT Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hardware Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [5n4ck3y](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hack-A-Sat 4 \(HAS4\)](#) -
[CON](#) - cont...(10:00-16:59 PDT) - [Adversary Wars CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Dark Tangent Look-Alike Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL at DEF CON 31 - Booth Open](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Battle of The Bots](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Ham Radio Fox Hunting Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Gold Bug Challenge](#) -
[CON](#) - cont...(10:00-19:59 PDT) - [The Lonely Hard Drive](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Tinfoil Hat Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [venator aurum - A Treasure Hunt](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CrackMeIfYouCan](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [It's In That Place Where I Put That Thing That Time](#) -
[CON](#) - cont...(10:00-16:30 PDT) - [Darknet-NG](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Maps of the digital lands](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\)](#) -

CON - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
CON - cont...(10:00-17:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -
CON - cont...(10:00-16:59 PDT) - [Red Alert ICS CTF](#) -
CON - cont...(10:00-17:59 PDT) - [Dungeons@Defcon](#) -
CON - cont...(10:00-17:59 PDT) - [Red Team CTF](#) -
CON - cont...(10:00-17:59 PDT) - [? Cube](#) -
CON - cont...(10:30-14:30 PDT) - [Trace Labs OSINT Search Party CTF - CTF Platform Open for Submissions](#) -
CON - [DEF CON 31 Beard and Mustache Contest](#) -
CON - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
CON - cont...(10:30-17:59 PDT) - [Blue Team Village CTF](#) -
CON - cont...(11:00-16:59 PDT) - [Free Amateur Radio License Exams](#) -
CON - cont...(10:00-17:59 PDT) - [Embedded CTF](#) -
CON - cont...(09:00-17:59 PDT) - [Social Engineering Community \(SEC\) Youth Challenge](#) -
CON - cont...(12:00-14:59 PDT) - [TOOOL Dozier Drill Lockpicking Challenge](#) -
CON - cont...(10:00-17:59 PDT) - [Cloud Village CTF](#) -
CON - cont...(10:00-16:59 PDT) - [DC Kubernetes Capture the Flag \(CTF\)](#) -
CPV - [Exploring the Impact of PQC on Cryptographic Key Management](#) - Deirdre Connolly,James Howe,Mark Carney,Ryan Hurst,Sandra Guasch Castello,Sofi Celi
DC - [Power Corrupts; Corrupt It Back! Hacking Power Management in Data Centers](#) - Jesse Chick,Sam Quinn
DC - cont...(10:00-17:59 PDT) - [Vendor Area Open](#) -
DC - cont...(09:30-18:59 PDT) - [Human Registration Open](#) -
DC - cont...(13:30-14:15 PDT) - [Meduza: How an exiled pirate media outlet breaks through the Kremlin's propaganda firewall](#) - Alex
DC - (14:30-15:15 PDT) - [Exploiting OPC-UA in Every Possible Way: Practical Attacks Against Modern OPC-UA Architectures](#) - Noam Moshe,Sharon Brizinov
DC - [A SSLippery Slope: Unraveling the Hidden Dangers of Certificate Misuse](#) - Bill Demirkapi
DC - cont...(10:00-17:59 PDT) - [Exhibitor Area Open](#) -
DC - cont...(13:30-14:15 PDT) - [The GitHub Actions Worm: Compromising GitHub repositories through the Actions dependency tree](#) - Asi Greenholts
DC - (14:30-15:15 PDT) - [Contactless Overflow: Code execution in payment terminals and ATM's over NFC](#) - Josep Pi Rodriguez
DC - cont...(10:00-17:59 PDT) - [Contest Area Open](#)
DC - [Lonely Hackers Club - Badgelifa & Sticker Swap](#)
DC - [Off the record war story talks - Signs Ups On Site](#)
DCGVR - cont...(13:35-14:05 PDT) - [Bootsquad: Stomping out squatters](#) - Joe Mast
DCGVR - (14:35-15:20 PDT) - [Enhancing vulnerability research through the use of virtual reality workspaces.](#) - datalocaltmp
DL - [ThreatScraper: Automated Threat Intelligence Gathering and Analysis for VirusTotal](#) - Aaron "AJ" Morath,Scott Graham
DL - [RuleProcessorY & Gramify - Rule Optimization & Password Analysis tools](#) - Niels Loozekoot
DL - [HardHat Command & Control Framework](#) - Jonathan Owens
DL - [ProjectDiscovery Nuclei](#) - Brendan O'Leary,Pj Metz
DL - [ICS Forensics tool](#) - Maayan Shaul,Ori Perez
DL - [BLE CTF](#) - Alek Amrani,Ryan Holeman
ESV - cont...(10:00-17:59 PDT) - [Embedded Systems Village Activities](#) -
HHV - cont...(10:00-15:30 PDT) - [Make Your Own Use](#) -
HHV - cont...(10:00-17:59 PDT) - [Soldering Skills Village Activities](#) -
HHV - cont...(10:00-17:59 PDT) - [RoboSumo Play Time](#) -
HHV - cont...(10:00-15:30 PDT) - [Hardware Hacking Rube Goldberg Machine](#) -
ICSV - cont...(13:30-14:59 PDT) - [Panel Discussion -- Designing and Deploying NOC/SOC in a Mobile, Limited Bandwidth Maritime Environment](#) - Brad Proctor,Cliff Neve,Danny Joslin,Peter Dreyer,Tom Stites
IOTV - cont...(10:00-17:59 PDT) - [Hardware Hacking Your Kitchen](#) -
IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hacking Playground](#) -
IOTV - cont...(10:00-17:59 PDT) - [Critical Infrastructure & IoT Exploitation](#) -
IOTV - cont...(10:00-17:59 PDT) - [Secure or Surrender](#) -
IOTV - cont...(10:00-17:59 PDT) - [The IoT Kill Zone](#) -
IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hardware Hacking Exercises 2023](#) -

IOTV - cont...(10:00-17:59 PDT) - [Embedded Device Security Workshops](#) -
 IOTV - cont...(10:00-17:59 PDT) - [Perform Memory Extraction, Emulation and Shellcode](#) -
 LPV - cont...(10:00-17:59 PDT) - [Lockpick Village Activities](#) -
 MISC - No Starch Press - Book Signing - Micah Lee, Hacks, Leaks and Revelations
 MISC - (14:30-14:59 PDT) - [No Starch Press - Book Signing - Cory Doctorow, Red Team Blues & Choquepoint Capitalism](#) -
 Cory Doctorow
 MISC - cont...(10:00-16:59 PDT) - [DDV open and accepting drives for duplication](#) -
 MISC - cont...(10:00-15:59 PDT) - [Book Exchange](#) -
 MISC - cont...(13:00-14:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\) - BYODesign Presentation](#) -
 MISC - [DEF CON Chess Kids Free-Play](#) -
 MIV - cont...(13:30-14:30 PDT) - [Main features of Russia's disinformation and propaganda ecosystem in Spanish-speaking countries](#) - Carlos Galán
 MIV - (14:30-14:59 PDT) - [156 million targeted: Biggest social phishing cyberattacks during Brazil's election](#) - Douglas Bernardini
 PHV - cont...(09:00-17:59 PDT) - [Honey Pot Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [Build Your Own Botnet](#) -
 PHV - cont...(09:00-17:59 PDT) - [Wall of Sheep](#) -
 PHV - cont...(09:00-17:59 PDT) - [Linux Trainer Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [NetworkOS: Be The Cloud](#) -
 PHV - cont...(09:00-17:59 PDT) - [RegEx Trainer](#) -
 PHV - cont...(09:00-17:59 PDT) - [Password Lab](#) -
 PHV - cont...(09:00-17:59 PDT) - [Fleet DefCon 31 Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [Packet Inspector](#) -
 PHV - cont...(09:00-17:59 PDT) - [Packet Detective](#) -
 PLV - [Let Night City Sleep - Governance Against a Cyberpunk Future](#) - Cameron Byrd, Clayton Dixon
 PLV - [Abating the Eye of Sauron: Help Combat Authoritarian Censorship](#) - David Houston, Michaela Lee
 PLV - [How can we encourage more hackers to engage with policy makers?](#) - Peter Stephens, Thomas Kranz
 PSV - cont...(10:00-17:59 PDT) - [Physical Security Village Activities](#) -
 PSV - [Lock Bypass 101](#) - Terry
 PSV - (14:30-14:59 PDT) - [Lock Bypass 102](#) - Ege
 PWV - cont...(10:00-17:59 PDT) - [Password Village Activities](#) -
 PYV - cont...(11:00-17:59 PDT) - [Payment Village Challenges/CTF](#) -
 QTV - [OpenQuantum: open-source hardware for quantum engineering via trapped atoms](#) - Max Shirokawa Aalto
 RCV - [Easy EASM - the zero dollar attack surface management tool](#) - Jason Haddix
 RCV - (14:25-15:10 PDT) - [Azure AD recon with OSINT tools](#) - Nestori Syynimaa
 RFV - [Wardriving 102: Moving Beyond the Wigle App](#) - bkobe
 RTV - cont...(11:00-16:59 PDT) - [\(In\)Direct Syscalls: A Journey from High to Low](#) - Daniel Feichter
 RTV - cont...(13:00-14:59 PDT) - [How to \[NOT\] look like a Red Team](#) - Michael Wylie
 RTV - [IOCs + APTs = "Let's play a game!" - Hack your way through a hunt!](#) - Leo Cruz
 RTV - [AI-Driven Hacker's Toolkit: Using AI to Learn Python and Scapy for Exploitation and Post-Exploitation Techniques](#) -
 Omar Santos
 RTV - cont...(13:00-16:59 PDT) - [How Most Internal Networks are Compromised: A Set of Common Active Directory Attacks and How to Perform Them from Linux](#) - Scott Brink
 SEV - cont...(08:30-17:30 PDT) - [SECV - Youth Challenge](#) -
 SEV - cont...(08:30-17:59 PDT) - [SECV Village Open](#)
 SEV - cont...(13:30-15:30 PDT) - [Cold Calls](#) -
 SOC - [WISP Chill Out Space with Refreshments](#) -
 SOC - cont...(10:00-17:59 PDT) - [Hacker Memorial](#) -
 SOC - cont...(12:00-17:59 PDT) - [Lonely Hackers Club Meetup](#) -
 SOC - cont...(10:00-17:59 PDT) - [DCG Meetups](#)
 SOC - cont...(12:00-17:59 PDT) - [HDA / Accessibility Area Open](#)
 SOC - cont...(12:00-17:59 PDT) - [HDA Community Meetups](#)
 TCV - (14:30-15:59 PDT) - [Diameter Workshop](#) - Akib Sayyed, Zibrán Sayyed
 TEV - cont...(10:00-17:59 PDT) - [Tamper Evident Village Activities](#) -
 VMV - cont...(13:30-14:20 PDT) - [Interventions To Address Technology-Facilitated Violence in Democracy](#) - Eric

Davis,Hallie Stern,Omri Preiss,Theodora Skeadas

VMV - cont...(13:55-14:35 PDT) - [Political Polarization](#) - Constantine Nicolaidis

VMV - (14:30-15:20 PDT) - [Defense Community](#) - Brian Stearns,Charles Smith,Eric Davis,Glenn Borskey,Jon A.

VMV - (14:40-15:30 PDT) - [Democracy, Are You Citizen Or Subject?](#) - Kendall Spencer

WS - [Introduction to Exploit Development \(Pre-Registration Required\)](#) - Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman,Sam Bowne

WS - [Hands-On TCP/IP Deep Dive with Wireshark - How this stuff really works \(Pre-Registration Required\)](#) - Chris Greer

WS - [The Joy of Reverse Engineering: Learning With Ghidra and WinDbg \(Pre-Registration Required\)](#) - Wesley McGrew

WS - [Digital Forensics and Incident Response Against the Digital Darkness: An Intro to Forensicating Evil \(Pre-Registration Required\)](#) - Michael "S3curityNerd" Register,Michael "mR_F0r3n51c5" Solomon

WS - [Starbase: open source graph security analysis \(Pre-Registration Required\)](#) - Adam Pierson,Austin Kelleher,Guillaume Ross

XRV - cont...(10:00-15:59 PDT) - [Haptics Hack-a-Thon](#) -

XRV - cont...(10:00-17:59 PDT) - [XR Village Playground](#) -

XRV - cont...(11:00-16:59 PDT) - [Off the Rails: A demo with Pacific Northwest National Labs](#) -

XRV - [The of History XR From Fiction to Reality](#) - Bob Gourley,Starr Brown

[AIV - cont...\(10:00-17:59 PDT\) - AI Village Generative Red Team Challenge](#) -
[AIV - you sound confused, anyways - thanks for the jewels.](#) - Adrian "threalfall" Wood
[AIV - \(15:30-15:55 PDT\) - Hackaprompt 2023: Trials and Tribulations](#) - Kenneth Yeung
[APV - SusParams: Hypercharge your web testing with DATA](#) - Jason Haddix
[APV - \(15:45-16:30 PDT\) - Securing the Front Lines: Protecting Front-End Applications from Overlooked Vulnerabilities](#) - Dohyeon Kim,WooWon Kang
[APV - Hunt the Hacker - Detect compromises in your repositories!](#) - GitGuardian
[APV - How to Hide Behavior from Security Tools](#) - Deepfactor
[APV - Fix The Flag - Battle Challenge](#) - Pedram Hayati
[APV - Faking GitHub Reputation](#) - Checkmarx
[APV - Per-mission Impossible: Exploring the Android Permission Model and Intents](#) - Miłosz Gaczkowski,William Taylor
[ASV - cont...\(10:00-17:59 PDT\) - Hack The Airport](#) -
[ASV - cont...\(10:00-17:59 PDT\) - Unmanned Aerial Systems – Platform Security](#) -
[ASV - cont...\(10:00-17:59 PDT\) - The Challenge - Lockheed Martin](#) -
[ASV - cont...\(10:00-17:59 PDT\) - A-ISAC CTF](#) -
[ASV - cont...\(10:00-17:59 PDT\) - Bricks in the Air](#) -
[ASV - cont...\(10:00-17:59 PDT\) - ARINC 615a CTF](#) -
[ASV - cont...\(10:00-17:59 PDT\) - PTP Flight Challenge](#) -
[ASV - cont...\(10:00-17:59 PDT\) - Ask Me Anything About Cybersecurity in Aerospace](#) -
[ASV - Space Pirates on the Loose! - Space-Based Threats to US Interests](#) - Henry Danielson,Sage Meadows
[ASV - \(15:30-16:20 PDT\) - Wingin' It - Pentesting a 737](#) - Alexander Dodd
[BHV - cont...\(14:50-15:30 PDT\) - Lanternyn: Blue Energy](#) - Del de Zela
[BHV - \(15:30-16:10 PDT\) - Enhancing Cybersecurity Resilience in the Brazilian Healthcare Sector: A Novel Red Team and Blue Team Methodology](#) - Arthur Paixão,Diego Mariano
[BICV - Unveiling My Journey to My First CVE: A Tale of Discovery and Achievement](#) - Gaspard Baye
[BTV - \(15:45-16:45 PDT\) - Arson Herders: An IR Guide to Fighting and Lighting Fires](#) - Litmoose,Matt "dis0wn" Wagenknecht,Tina "Mugwump Jones" Velez,Unnamed user
[CLV - cont...\(14:50-15:35 PDT\) - The Human Threat Factor - Cloud Security Misconfigurations](#) - Kat Fitzgerald
[CON - cont...\(09:00-17:59 PDT\) - HardWired](#) -
[CON - cont...\(12:00-17:59 PDT\) - Capture The Packet Main Rounds](#) -
[CON - cont...\(10:00-17:59 PDT\) - IoT Village CTF](#) -
[CON - cont...\(10:00-17:59 PDT\) - Hardware Hacking Village CTF](#) -
[CON - cont...\(10:00-17:59 PDT\) - 5n4ck3y](#) -
[CON - cont...\(10:00-17:59 PDT\) - TeleChallenge](#) -
[CON - cont...\(10:00-17:59 PDT\) - Hack-A-Sat 4 \(HAS4\)](#) -
[CON - cont...\(10:00-16:59 PDT\) - Adversary Wars CTF](#) -
[CON - cont...\(10:00-17:59 PDT\) - The Dark Tangent Look-Alike Contest](#) -
[CON - cont...\(10:00-17:59 PDT\) - CMD+CTRL at DEF CON 31 - Booth Open](#) -
[CON - cont...\(10:00-17:59 PDT\) - HackFortress](#) -
[CON - cont...\(10:00-17:59 PDT\) - Battle of The Bots](#) -
[CON - cont...\(10:00-17:59 PDT\) - Ham Radio Fox Hunting Contest](#) -
[CON - cont...\(10:00-17:59 PDT\) - The Gold Bug Challenge](#) -
[CON - cont...\(10:00-19:59 PDT\) - The Lonely Hard Drive](#) -
[CON - cont...\(10:00-17:59 PDT\) - Car Hacking Village CTF](#) -
[CON - cont...\(10:00-17:59 PDT\) - Tinfoil Hat Contest](#) -
[CON - cont...\(10:00-17:59 PDT\) - venator aurum - A Treasure Hunt](#) -
[CON - cont...\(10:00-17:59 PDT\) - CrackMeIfYouCan](#) -
[CON - cont...\(10:00-17:59 PDT\) - It's In That Place Where I Put That Thing That Time](#) -
[CON - cont...\(10:00-16:30 PDT\) - Darknet-NG](#) -
[CON - cont...\(10:00-17:59 PDT\) - Maps of the digital lands](#) -
[CON - cont...\(10:00-17:59 PDT\) - DC's Next Top Threat Model \(DCNTTM\)](#) -

CON - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
CON - cont...(10:00-17:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -
CON - cont...(10:00-16:59 PDT) - [Red Alert ICS CTF](#) -
CON - cont...(10:00-17:59 PDT) - [Dungeons@Defcon](#) -
CON - cont...(10:00-17:59 PDT) - [Red Team CTF](#) -
CON - cont...(10:00-17:59 PDT) - [? Cube](#) -
CON - cont...(14:00-15:59 PDT) - [DEF CON 31 Beard and Mustache Contest](#) -
CON - [DEF CON Chess Tournament](#) -
CON - (15:30-16:29 PDT) - [Trace Labs OSINT Search Party CTF - Announce CTF Grand Prize Winners](#) -
CON - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
CON - cont...(10:30-17:59 PDT) - [Blue Team Village CTF](#) -
CON - cont...(11:00-16:59 PDT) - [Free Amateur Radio License Exams](#) -
CON - cont...(10:00-17:59 PDT) - [Embedded CTF](#) -
CON - cont...(09:00-17:59 PDT) - [Social Engineering Community \(SEC\) Youth Challenge](#) -
CON - cont...(10:00-17:59 PDT) - [Cloud Village CTF](#) -
CON - cont...(10:00-16:59 PDT) - [DC Kubernetes Capture the Flag \(CTF\)](#) -
CPV - [Cryptosplloit Workshop](#) - Matt Cheung
DC - [Revolutionizing ELF binary patching with Shiva: A JIT binary patching system for Linux](#) - Ryan "ElfMaster" O'Neill
DC - cont...(10:00-17:59 PDT) - [Vendor Area Open](#) -
DC - cont...(09:30-18:59 PDT) - [Human Registration Open](#) -
DC - cont...(14:30-15:15 PDT) - [Exploiting OPC-UA in Every Possible Way: Practical Attacks Against Modern OPC-UA Architectures](#) - Noam Moshe, Sharon Brizinov
DC - (15:30-16:15 PDT) - [Breaking BMC: The Forgotten Key to the Kingdom](#) - Adam Zabrocki, Alex Tereshkin
DC - [Spooky authentication at a distance](#) - Tamas "SkelSec" Jos
DC - cont...(10:00-17:59 PDT) - [Exhibitor Area Open](#) -
DC - cont...(14:30-15:15 PDT) - [Contactless Overflow: Code execution in payment terminals and ATM's over NFC](#) - Josep Pi Rodriguez
DC - (15:30-16:15 PDT) - [ndays are also 0days: Can hackers launch 0day RCE attack on popular softwares only with chromium ndays?](#) - Bohan Liu, GuanCheng Li, Zheng Wang
DC - cont...(10:00-17:59 PDT) - [Contest Area Open](#)
DC - cont...(14:00-16:59 PDT) - [Lonely Hackers Club - Badgelife & Sticker Swap](#)
DC - cont...(14:00-17:59 PDT) - [Off the record war story talks - Signs Ups On Site](#)
DCGVR - cont...(14:35-15:20 PDT) - [Enhancing vulnerability research through the use of virtual reality workspaces.](#) - datalocaltmp
DCGVR - (15:35-16:05 PDT) - [Gender Inclusive Features Across the Health Information System](#) - Squiddy
DL - cont...(14:00-15:55 PDT) - [ThreatScraper: Automated Threat Intelligence Gathering and Analysis for VirusTotal](#) - Aaron "AJ" Morath, Scott Graham
DL - cont...(14:00-15:55 PDT) - [RuleProcessorY & Gramify - Rule Optimization & Password Analysis tools](#) - Niels Loozekoot
DL - cont...(14:00-15:55 PDT) - [HardHat Command & Control Framework](#) - Jonathan Owens
DL - cont...(14:00-15:55 PDT) - [ProjectDiscovery Nuclei](#) - Brendan O'Leary, Pj Metz
DL - cont...(14:00-15:55 PDT) - [ICS Forensics tool](#) - Maayan Shaul, Ori Perez
DL - cont...(14:00-15:55 PDT) - [BLE CTF](#) - Alek Amrani, Ryan Holeman
ESV - cont...(10:00-17:59 PDT) - [Embedded Systems Village Activities](#) -
HHV - cont...(10:00-15:30 PDT) - [Make Your Own Use](#) -
HHV - cont...(10:00-17:59 PDT) - [Soldering Skills Village Activities](#) -
HHV - cont...(10:00-17:59 PDT) - [RoboSumo Play Time](#) -
HHV - cont...(10:00-15:30 PDT) - [Hardware Hacking Rube Goldberg Machine](#) -
HHV - [Generating Rf With Stock Hardware For Drones](#) - David Melendez
HRV - [Modernizing AX.25 packet radio with Modern Packet Message Manager](#) - Jeremy Banker
HRV - [HF Radio Demonstration](#) - KitKat
ICSV - [Your Ship is Leaking... How Social Media Plays a Role in the Uncovering of Critical Maritime Systems](#) - Rae Baker
ICSV - (15:30-15:59 PDT) - [Improving the Speed of Cybersecurity: Seven Cyber Metrics for Maritime Owners and Operators](#) - Tyson Meadors
IOTV - cont...(10:00-17:59 PDT) - [Hardware Hacking Your Kitchen](#) -

IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hacking Playground](#) -
 IOTV - cont...(10:00-17:59 PDT) - [Critical Infrastructure & IoT Exploitation](#) -
 IOTV - cont...(10:00-17:59 PDT) - [Secure or Surrender](#) -
 IOTV - cont...(10:00-17:59 PDT) - [The IoT Kill Zone](#) -
 IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hardware Hacking Exercises 2023](#) -
 IOTV - cont...(10:00-17:59 PDT) - [Embedded Device Security Workshops](#) -
 IOTV - cont...(10:00-17:59 PDT) - [Perform Memory Extraction, Emulation and Shellcode](#) -
 LPV - cont...(10:00-17:59 PDT) - [Lockpick Village Activities](#) -
 MISC - No Starch Press - Book Signing - Jon DiMaggio, The Art of Cyberwarfare
 MISC - cont...(10:00-16:59 PDT) - [DDV open and accepting drives for duplication](#) -
 MISC - cont...(10:00-15:59 PDT) - [Book Exchange](#) -
 MIV - [Misinformation As A Service: Social Engineering techniques applied in service contexts.](#) - Daniel Isler
 MIV - (15:30-16:30 PDT) - [IVY HAUL: A Computational Linguistics Analysis of a Disinformation Actor](#) - Shea Nangle
 PHV - cont...(09:00-17:59 PDT) - [Honey Pot Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [Build Your Own Botnet](#) -
 PHV - cont...(09:00-17:59 PDT) - [Wall of Sheep](#) -
 PHV - cont...(09:00-17:59 PDT) - [Linux Trainer Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [NetworkOS: Be The Cloud](#) -
 PHV - cont...(09:00-17:59 PDT) - [RegEx Trainer](#) -
 PHV - cont...(09:00-17:59 PDT) - [Password Lab](#) -
 PHV - cont...(09:00-17:59 PDT) - [Fleet DefCon 31 Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [Packet Inspector](#) -
 PHV - cont...(09:00-17:59 PDT) - [Packet Detective](#) -
 PHV - [WINE Pairing with Malware](#) - Jared Stroud
 PLV - [Non-State Actors in the Russia/Ukraine Conflict](#) - Dan Grobarcik,Marc Rogers,Mauro Vignati,Stefanie Metka
 PLV - cont...(14:00-15:50 PDT) - [Abating the Eye of Sauron: Help Combat Authoritarian Censorship](#) - David
 Houston,Michaela Lee
 PLV - [All Your Vulns are Belong to Terms & Conditions](#) - Casey Ellis,David Rogers,Harley Geiger,Katie Trimble-Noble
 PSV - cont...(10:00-17:59 PDT) - [Physical Security Village Activities](#) -
 PWV - cont...(10:00-17:59 PDT) - [Password Village Activities](#) -
 PYV - cont...(11:00-17:59 PDT) - [Payment Village Challenges/CTF](#) -
 QTV - [Quantum Technologies on a Raspberry Pi \(and HackRF one\)](#) - Ben Varcoe
 RCV - cont...(14:25-15:10 PDT) - [Azure AD recon with OSINT tools](#) - Nestori Syynimaa
 RCV - [Unlocking the Power of OWASP Amass: Introducing the Open Asset Model for Comprehensive Attack Surface
 Mapping](#) - Jeff Foley
 RCV - (15:55-16:20 PDT) - [Finding Hidden Gems In Temporary Mail Services](#) - Berk Can Geyikci
 RFV - [Antennas](#) - Kent
 RTV - cont...(11:00-16:59 PDT) - [\(In\)Direct Syscalls: A Journey from High to Low](#) - Daniel Feichter
 RTV - [Red Hot \(Red Team TTPs\)](#) - Ralph May,Steve Borosh
 RTV - [OSINT Skills Lab Challenge](#) - Lee McWhorter,Sandra Stibbards
 RTV - [Malware Hunting an Offensive Approach](#) - Filipi Pires
 RTV - cont...(13:00-16:59 PDT) - [How Most Internal Networks are Compromised: A Set of Common Active Directory
 Attacks and How to Perform Them from Linux](#) - Scott Brink
 SEV - cont...(08:30-17:30 PDT) - [SECV - Youth Challenge](#) -
 SEV - cont...(08:30-17:59 PDT) - [SECV Village Open](#)
 SEV - cont...(13:30-15:30 PDT) - [Cold Calls](#) -
 SOC - cont...(14:00-15:59 PDT) - [WISP Chill Out Space with Refreshments](#) -
 SOC - cont...(10:00-17:59 PDT) - [Hacker Memorial](#) -
 SOC - cont...(12:00-17:59 PDT) - [Lonely Hackers Club Meetup](#) -
 SOC - cont...(10:00-17:59 PDT) - [DCG Meetups](#)
 SOC - cont...(12:00-17:59 PDT) - [HDA / Accessibility Area Open](#)
 SOC - cont...(12:00-17:59 PDT) - [HDA Community Meetups](#)
 TCV - cont...(14:30-15:59 PDT) - [Diameter Workshop](#) - Akib Sayyed,Zibran Sayyed
 TEV - cont...(10:00-17:59 PDT) - [Tamper Evident Village Activities](#) -
 VMV - cont...(14:30-15:20 PDT) - [Defense Community](#) - Brian Stearns,Charles Smith,Eric Davis,Glenn Borskey,Jon A.

VMV - cont...(14:40-15:30 PDT) - [Democracy, Are You Citizen Or Subject?](#) - Kendall Spencer

VMV - (15:30-16:20 PDT) - [2024 Election Threat Landscape](#) - Catherine Terranova,Hallie Stern,Rebecca Scott Thein,Sandra Khalil,Sarah Amos

VMV - (15:35-16:15 PDT) - [Influencing Voters Through Social Media, ADTECH, Big Data, and AI](#) - Joe Schniebes

WS - cont...(14:00-17:59 PDT) - [Starbase: open source graph security analysis \(Pre-Registration Required\)](#) - Adam Pierson,Austin Kelleher,Guillaume Ross

WS - cont...(14:00-17:59 PDT) - [Introduction to Exploit Development \(Pre-Registration Required\)](#) - Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman,Sam Bowne

WS - cont...(14:00-17:59 PDT) - [Hands-On TCP/IP Deep Dive with Wireshark - How this stuff really works \(Pre-Registration Required\)](#) - Chris Greer

WS - cont...(14:00-17:59 PDT) - [The Joy of Reverse Engineering: Learning With Ghidra and WinDbg \(Pre-Registration Required\)](#) - Wesley McGrew

WS - cont...(14:00-17:59 PDT) - [Digital Forensics and Incident Response Against the Digital Darkness: An Intro to Forensicing Evil \(Pre-Registration Required\)](#) - Michael "S3curityNerd" Register,Michael "mR_F0r3n51c5" Solomon

XRV - cont...(10:00-15:59 PDT) - [Haptics Hack-a-Thon](#) -

XRV - cont...(10:00-17:59 PDT) - [XR Village Playground](#) -

XRV - cont...(11:00-16:59 PDT) - [Off the Rails: A demo with Pacific Northwest National Labs](#) -

[AIV](#) - cont...(10:00-17:59 PDT) - [AI Village Generative Red Team Challenge](#) -
[AIV](#) - [Ignore the Law: The Legal Risks of Prompt Injection Attacks on Large Language Models](#) - Ram Shankar Siva Kumar
[AIV](#) - (16:30-17:25 PDT) - [ChatGPT: Your Red Teaming Ally](#) - Gavin Klondike
[APV](#) - cont...(15:45-16:30 PDT) - [Securing the Front Lines: Protecting Front-End Applications from Overlooked Vulnerabilities](#) - Dohyeon Kim, WooWon Kang
[APV](#) - (16:30-17:15 PDT) - [Breaking Barriers: A Deep Dive into Bypassing Next-Gen 2FA and MFA Security Measures](#) - Muhammad Shahmeer
[APV](#) - cont...(15:00-16:59 PDT) - [Hunt the Hacker - Detect compromises in your repositories!](#) - GitGuardian
[APV](#) - cont...(15:00-16:59 PDT) - [How to Hide Behavior from Security Tools](#) - Deepfactor
[APV](#) - cont...(15:00-16:59 PDT) - [Fix The Flag - Battle Challenge](#) - Pedram Hayati
[APV](#) - cont...(15:00-16:59 PDT) - [Faking GitHub Reputation](#) - Checkmarx
[APV](#) - cont...(15:00-16:59 PDT) - [Per-mission Impossible: Exploring the Android Permission Model and Intents](#) - Miłosz Gaczkowski, William Taylor
[ASV](#) - cont...(10:00-17:59 PDT) - [Hack The Airport](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Unmanned Aerial Systems – Platform Security](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [The Challenge - Lockheed Martin](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [A-ISAC CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [ARINC 615a CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [PTP Flight Challenge](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Ask Me Anything About Cybersecurity in Aerospace](#) -
[ASV](#) - cont...(15:30-16:20 PDT) - [Wingin' It - Pentesting a 737](#) - Alexander Dodd
[ASV](#) - (16:30-16:55 PDT) - [A Fireside Chat with Chris Roberts and Pete Cooper](#) - Chris Roberts, Pete Cooper
[BHV](#) - cont...(15:30-16:10 PDT) - [Enhancing Cybersecurity Resilience in the Brazilian Healthcare Sector: A Novel Red Team and Blue Team Methodology](#) - Arthur Paixão, Diego Mariano
[BHV](#) - [FaFo: Laboratory Physical and ICS \(Warning: not for the faint of heart\)](#) - Nathan Case
[BICV](#) - [BIC Village Closing Keynote](#) - Kevin Roberts
[BTV](#) - cont...(15:45-16:45 PDT) - [Arson Herders: An IR Guide to Fighting and Lighting Fires](#) - Litmoose, Matt "disOwn" Wagenknecht, Tina "Mugwump Jones" Velez, Unnamed user
[CON](#) - cont...(09:00-17:59 PDT) - [HardWired](#) -
[CON](#) - cont...(12:00-17:59 PDT) - [Capture The Packet Main Rounds](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [IoT Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hardware Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [5n4ck3y](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hack-A-Sat 4 \(HAS4\)](#) -
[CON](#) - cont...(10:00-16:59 PDT) - [Adversary Wars CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Dark Tangent Look-Alike Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL at DEF CON 31 - Booth Open](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Battle of The Bots](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Ham Radio Fox Hunting Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Gold Bug Challenge](#) -
[CON](#) - cont...(10:00-19:59 PDT) - [The Lonely Hard Drive](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Tinfoil Hat Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [venator aurum - A Treasure Hunt](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CrackMelfYouCan](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [It's In That Place Where I Put That Thing That Time](#) -
[CON](#) - cont...(10:00-16:30 PDT) - [Darknet-NG](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Maps of the digital lands](#) -

CON - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model \(DCNTTM\)](#) -
 CON - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
 CON - cont...(10:00-17:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -
 CON - cont...(10:00-16:59 PDT) - [Red Alert ICS CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [Dungeons@Defcon](#) -
 CON - cont...(10:00-17:59 PDT) - [Red Team CTF](#) -
 CON - cont...(10:00-17:59 PDT) - [? Cube](#) -
 CON - cont...(15:00-17:59 PDT) - [DEF CON Chess Tournament](#) -
 CON - cont...(15:30-16:29 PDT) - [Trace Labs OSINT Search Party CTF - Announce CTF Grand Prize Winners](#) -
 CON - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
 CON - cont...(10:30-17:59 PDT) - [Blue Team Village CTF](#) -
 CON - cont...(11:00-16:59 PDT) - [Free Amateur Radio License Exams](#) -
 CON - cont...(10:00-17:59 PDT) - [Embedded CTF](#) -
 CON - cont...(09:00-17:59 PDT) - [Social Engineering Community \(SEC\) Youth Challenge](#) -
 CON - cont...(10:00-17:59 PDT) - [Cloud Village CTF](#) -
 CON - cont...(10:00-16:59 PDT) - [DC Kubernetes Capture the Flag \(CTF\)](#) -
 CPV - [CPV Ten Year Anniversary Gathering](#) - CPV Staff
 DC - [A Broken Marriage: Abusing Mixed Vendor Kerberos Stacks](#) - Ceri Coburn
 DC - (16:30-17:15 PDT) - [All information looks like noise until you break the code: Futureproofing the transportation sector](#) - David Pekoske, Jen Easterly, Kevin Collier
 DC - cont...(10:00-17:59 PDT) - [Vendor Area Open](#) -
 DC - cont...(09:30-18:59 PDT) - [Human Registration Open](#) -
 DC - cont...(15:30-16:15 PDT) - [Breaking BMC: The Forgotten Key to the Kingdom](#) - Adam Zabrocki, Alex Tereshkin
 DC - (16:30-16:50 PDT) - [Your Clocks Have Ears — Timing-Based Browser-Based Local Network Port Scanner](#) - Dongsung “Donny” Kim
 DC - [Runtime Riddles: Abusing Manipulation Points in the Android Source](#) - Laurie Kirk
 DC - cont...(10:00-17:59 PDT) - [Exhibitor Area Open](#) -
 DC - cont...(15:30-16:15 PDT) - [ndays are also Odays: Can hackers launch Oday RCE attack on popular softwares only with chromium ndays?](#) - Bohan Liu, GuanCheng Li, Zheng Wang
 DC - (16:30-17:15 PDT) - [Abortion Access in the Age of Surveillance](#) - Corynne McSherry, Daly Barnett, India McKinney, Kate Bertash
 DC - cont...(10:00-17:59 PDT) - [Contest Area Open](#)
 DC - cont...(14:00-16:59 PDT) - [Lonely Hackers Club - Badgelife & Sticker Swap](#)
 DC - cont...(14:00-17:59 PDT) - [Off the record war story talks - Signs Ups On Site](#)
 DCGVR - cont...(15:35-16:05 PDT) - [Gender Inclusive Features Across the Health Information System](#) - Squiddy
 DCGVR - (16:35-17:35 PDT) - [Hey CryptoBro!: How Are Criminals Laundering, Monetizing, and Targeting Cryptocurrency, NFTs, and Smart Contracts?](#) - Sam Colaizzi
 ESV - cont...(10:00-17:59 PDT) - [Embedded Systems Village Activities](#) -
 HHV - cont...(10:00-17:59 PDT) - [Soldering Skills Village Activities](#) -
 HHV - cont...(10:00-17:59 PDT) - [RoboSumo Play Time](#) -
 HHV - [Hardware Hacking Village Prize Ceremony](#) -
 HRV - cont...(15:00-16:30 PDT) - [HF Radio Demonstration](#) - KitKat
 ICSV - [The Unlikely Romance: Critical Infrastructure Edition](#) - Casey Ellis
 ICSV - (16:30-16:59 PDT) - [Lessons learned when building a Maritime Systems Security Laboratory Testbench](#) - Brien Croteau
 IOTV - cont...(10:00-17:59 PDT) - [Hardware Hacking Your Kitchen](#) -
 IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hacking Playground](#) -
 IOTV - cont...(10:00-17:59 PDT) - [Critical Infrastructure & IoT Exploitation](#) -
 IOTV - cont...(10:00-17:59 PDT) - [Secure or Surrender](#) -
 IOTV - cont...(10:00-17:59 PDT) - [The IoT Kill Zone](#) -
 IOTV - cont...(10:00-17:59 PDT) - [IoT Village Hardware Hacking Exercises 2023](#) -
 IOTV - cont...(10:00-17:59 PDT) - [Embedded Device Security Workshops](#) -
 IOTV - cont...(10:00-17:59 PDT) - [Perform Memory Extraction, Emulation and Shellcode](#) -
 LPV - cont...(10:00-17:59 PDT) - [Lockpick Village Activities](#) -
 LPV - [Intro to Lockpicking](#) - TOOOL

LPV - (16:45-17:45 PDT) - [Totally Tubular: An Impromptu Talk About Tubular Locks and Keys](#) - Deviant Ollam
 MISC - No Starch Press - Book Signing - Fotios Chantzis, Paulino Calderon, & Beau Woods, Practical IoT Hacking
 MISC - cont...(10:00-16:59 PDT) - [DDV open and accepting drives for duplication](#) -
 MIV - cont...(15:30-16:30 PDT) - [IVY HAUL: A Computational Linguistics Analysis of a Disinformation Actor](#) - Shea Nangle
 MIV - (16:30-17:30 PDT) - [Hacks, Leaks, and Revelations: Pandemic Profiteers and COVID-19 Disinformation](#) - Micah Lee
 PHV - cont...(09:00-17:59 PDT) - [Honey Pot Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [Build Your Own Botnet](#) -
 PHV - cont...(09:00-17:59 PDT) - [Wall of Sheep](#) -
 PHV - cont...(09:00-17:59 PDT) - [Linux Trainer Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [NetworkOS: Be The Cloud](#) -
 PHV - cont...(09:00-17:59 PDT) - [RegEx Trainer](#) -
 PHV - cont...(09:00-17:59 PDT) - [Password Lab](#) -
 PHV - cont...(09:00-17:59 PDT) - [Fleet DefCon 31 Workshop](#) -
 PHV - cont...(09:00-17:59 PDT) - [Packet Inspector](#) -
 PHV - cont...(09:00-17:59 PDT) - [Packet Detective](#) -
 PHV - [The Importance of Arts and Crafts in ThreatOps](#) - Pete Hay
 PLV - [We're From the Government and We're Here to Help Secure Open Source Software](#) - Anjana Rajan,Brian Behlendorf,Charlie Gladstone,Jack Cable
 PLV - [How do you solve a problem like Mirai - establishing a policy baseline for the IoT around the world](#) - Kat Megas,Peter Stephens
 PSV - cont...(10:00-17:59 PDT) - [Physical Security Village Activities](#) -
 PWV - cont...(10:00-17:59 PDT) - [Password Village Activities](#) -
 PYV - cont...(11:00-17:59 PDT) - [Payment Village Challenges/CTF](#) -
 QTV - [Quantini Time! Cocktail hour for the Quantum curious and creative](#) -
 QTV - [Quantum Music Workshop: Build Your Own Quantum Synthesizer!](#) - Mark Carney
 RCV - cont...(15:55-16:20 PDT) - [Finding Hidden Gems In Temporary Mail Services](#) - Berk Can Geyikci
 RCV - (16:20-17:05 PDT) - [Riding with the Chollimas: Our 100-Day Quest to Identify a North Korean State-Sponsored Threat Actor](#) - Mauro Eldritch
 RTV - cont...(11:00-16:59 PDT) - [\(In\)Direct Syscalls: A Journey from High to Low](#) - Daniel Feichter
 RTV - [How to prioritize Red Team Findings? Presenting CRTFSS: Common Red Team Findings Score System Ver. 1.0](#) - Guillermo Buendia
 RTV - [OSINT Skills Lab Challenge](#) - Lee McWhorter,Sandra Stibbards
 RTV - [Hacking Web Apps and APIs with WebSploit Labs](#) - Omar Santos
 RTV - cont...(13:00-16:59 PDT) - [How Most Internal Networks are Compromised: A Set of Common Active Directory Attacks and How to Perform Them from Linux](#) - Scott Brink
 SEV - cont...(08:30-17:30 PDT) - [SECV - Youth Challenge](#) -
 SEV - cont...(08:30-17:59 PDT) - [SECV Village Open](#)
 SEV - [Building an Effective Security Culture Program](#) - Jessica Barker,Maxie Reynolds,Rebecca Markwick,Sam Davison
 SOC - [Queercon Mixers](#) -
 SOC - [WISP Peer-to-Peer Mentoring and Networking](#) -
 SOC - cont...(10:00-17:59 PDT) - [Hacker Memorial](#) -
 SOC - cont...(12:00-17:59 PDT) - [Lonely Hackers Club Meetup](#) -
 SOC - cont...(10:00-17:59 PDT) - [DCG Meetups](#)
 SOC - cont...(12:00-17:59 PDT) - [HDA / Accessibility Area Open](#)
 SOC - cont...(12:00-17:59 PDT) - [HDA Community Meetups](#)
 TCV - [Diameter CTF](#) - Akib Sayyed,Zibran Sayyed
 TEV - cont...(10:00-17:59 PDT) - [Tamper Evident Village Activities](#) -
 VMV - cont...(15:30-16:20 PDT) - [2024 Election Threat Landscape](#) - Catherine Terranova,Hallie Stern,Rebecca Scott Thein,Sandra Khalil,Sarah Amos
 VMV - cont...(15:35-16:15 PDT) - [Influencing Voters Through Social Media, ADTECH, Big Data, and AI](#) - Joe Schniebes
 VMV - (16:30-17:30 PDT) - [The Impact Of Misinformation On Elections](#) - Joe Schniebes,Maia Mazurkiewicz,Michael Moore
 WS - cont...(14:00-17:59 PDT) - [Starbase: open source graph security analysis \(Pre-Registration Required\)](#) - Adam Pierson,Austin Kelleher,Guillaume Ross
 WS - cont...(14:00-17:59 PDT) - [Introduction to Exploit Development \(Pre-Registration Required\)](#) - Elizabeth

Biddlecome, Irvin Lemus, Kaitlyn Handelman, Sam Bowne

WS - cont...(14:00-17:59 PDT) - [Hands-On TCP/IP Deep Dive with Wireshark - How this stuff really works \(Pre-Registration Required\)](#) - Chris Greer

WS - cont...(14:00-17:59 PDT) - [The Joy of Reverse Engineering: Learning With Ghidra and WinDbg \(Pre-Registration Required\)](#) - Wesley McGrew

WS - cont...(14:00-17:59 PDT) - [Digital Forensics and Incident Response Against the Digital Darkness: An Intro to Forensicating Evil \(Pre-Registration Required\)](#) - Michael "S3curityNerd" Register, Michael "mR_F0r3n51c5" Solomon

XR - cont...(10:00-17:59 PDT) - [XR Village Playground](#) -

XR - cont...(11:00-16:59 PDT) - [Off the Rails: A demo with Pacific Northwest National Labs](#) -

XR - [Glad Scientist | Village Vibes Immersive Performance, a data-driven real time audiovisual VR performance](#) -

[AIV](#) - cont...(10:00-17:59 PDT) - [AI Village Generative Red Team Challenge](#) -
[AIV](#) - cont...(16:30-17:25 PDT) - [ChatGPT: Your Red Teaming Ally](#) - Gavin Klondike
[APV](#) - cont...(16:30-17:15 PDT) - [Breaking Barriers: A Deep Dive into Bypassing Next-Gen 2FA and MFA Security Measures](#) - Muhammad Shahmeer
[ASV](#) - cont...(10:00-17:59 PDT) - [Hack The Airport](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Unmanned Aerial Systems – Platform Security](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [The Challenge - Lockheed Martin](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [A-ISAC CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [ARINC 615a CTF](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [PTP Flight Challenge](#) -
[ASV](#) - cont...(10:00-17:59 PDT) - [Ask Me Anything About Cybersecurity in Aerospace](#) -
[ASV](#) - [Aerospace Village - 5 Years On](#) - Pete Cooper
[BHV](#) - cont...(16:10-17:10 PDT) - [FaFo: Laboratory Physical and ICS \(Warning: not for the faint of heart\)](#) - Nathan Case
[BHV](#) - [Virtual Reality/Augmented Reality: What’s missing from the pie? When data privacy and security measures aren’t “baked” in from the beginning](#) - LaTica Hammond,Lola Ajayi,Rian Phelps
[BTV](#) - [It’s not that your threat intelligence IOCs are worthless...](#) - Charlie,Lauren Proehl,Mick/nohackme,Silas Cutler
[CON](#) - cont...(09:00-17:59 PDT) - [HardWired](#) -
[CON](#) - cont...(12:00-17:59 PDT) - [Capture The Packet Main Rounds](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [IoT Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hardware Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [? Cube](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [5n4ck3y](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Hack-A-Sat 4 \(HAS4\)](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Dark Tangent Look-Alike Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL at DEF CON 31 - Booth Open](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Battle of The Bots](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Ham Radio Fox Hunting Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [The Gold Bug Challenge](#) -
[CON](#) - cont...(10:00-19:59 PDT) - [The Lonely Hard Drive](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Tinfoil Hat Contest](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [venator aurum - A Treasure Hunt](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [CrackMelfYouCan](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [It's In That Place Where I Put That Thing That Time](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Maps of the digital lands](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [DC’s Next Top Threat Model \(DCNTTM\)](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Dungeons@Defcon](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Red Team CTF](#) -
[CON](#) - cont...(15:00-17:59 PDT) - [DEF CON Chess Tournament](#) -
[CON](#) - [Hack3r Runw@y](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
[CON](#) - cont...(10:30-17:59 PDT) - [Blue Team Village CTF](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Embedded CTF](#) -
[CON](#) - cont...(09:00-17:59 PDT) - [Social Engineering Community \(SEC\) Youth Challenge](#) -
[CON](#) - cont...(10:00-17:59 PDT) - [Cloud Village CTF](#) -
[CPV](#) - cont...(16:00-17:59 PDT) - [CPV Ten Year Anniversary Gathering](#) - CPV Staff

DC - cont...(16:30-17:15 PDT) - All information looks like noise until you break the code: Futureproofing the transportation sector - David Pekoske, Jen Easterly, Kevin Collier

DC - (17:30-17:50 PDT) - Lions and Tigers and Fancy Bears, Oh My!: A Cautionary Tale for our Cyber Future - Jen Easterly, Scott Shapiro

DC - cont...(10:00-17:59 PDT) - Vendor Area Open -

DC - cont...(09:30-18:59 PDT) - Human Registration Open -

DC - Silent Spring: Prototype Pollution Leads to Remote Code Execution in Node.js - Mikhail Shcherbakov, Musard Balliu

DC - Polynonce: An ECDSA Attack and Polynomial Dance - Marco Macchetti, Nils Amiet

DC - cont...(10:00-17:59 PDT) - Exhibitor Area Open -

DC - cont...(16:30-17:15 PDT) - Abortion Access in the Age of Surveillance - Corynne McSherry, Daly Barnett, India McKinney, Kate Bertash

DC - cont...(10:00-17:59 PDT) - Contest Area Open

DC - Lonely Hackers Club - Name That Noob

DC - cont...(14:00-17:59 PDT) - Off the record war story talks - Signs Ups On Site

DCGVR - cont...(16:35-17:35 PDT) - Hey CryptoBro!: How Are Criminals Laundering, Monetizing, and Targeting Cryptocurrency, NFTs, and Smart Contracts? - Sam Colaizzi

ESV - cont...(10:00-17:59 PDT) - Embedded Systems Village Activities -

HHV - cont...(10:00-17:59 PDT) - Soldering Skills Village Activities -

HHV - cont...(10:00-17:59 PDT) - RoboSumo Play Time -

IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking Your Kitchen -

IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -

IOTV - cont...(10:00-17:59 PDT) - Critical Infrastructure & IoT Exploitation -

IOTV - cont...(10:00-17:59 PDT) - Secure or Surrender -

IOTV - cont...(10:00-17:59 PDT) - The IoT Kill Zone -

IOTV - cont...(10:00-17:59 PDT) - IoT Village Hardware Hacking Exercises 2023 -

IOTV - cont...(10:00-17:59 PDT) - Embedded Device Security Workshops -

IOTV - cont...(10:00-17:59 PDT) - Perform Memory Extraction, Emulation and Shellcode -

LPV - cont...(10:00-17:59 PDT) - Lockpick Village Activities -

LPV - cont...(16:45-17:45 PDT) - Totally Tubular: An Impromptu Talk About Tubular Locks and Keys - Deviant Ollam

MIV - cont...(16:30-17:30 PDT) - Hacks, Leaks, and Revelations: Pandemic Profiteers and COVID-19 Disinformation - Micah Lee

MIV - (17:30-17:59 PDT) - Misinformation Village Q and A - Misinformation Village Staff

PHV - cont...(09:00-17:59 PDT) - Honey Pot Workshop -

PHV - cont...(09:00-17:59 PDT) - Build Your Own Botnet -

PHV - cont...(09:00-17:59 PDT) - Wall of Sheep -

PHV - cont...(09:00-17:59 PDT) - Linux Trainer Workshop -

PHV - cont...(09:00-17:59 PDT) - NetworkOS: Be The Cloud -

PHV - cont...(09:00-17:59 PDT) - RegEx Trainer -

PHV - cont...(09:00-17:59 PDT) - Password Lab -

PHV - cont...(09:00-17:59 PDT) - Fleet DefCon 31 Workshop -

PHV - cont...(09:00-17:59 PDT) - Packet Inspector -

PHV - cont...(09:00-17:59 PDT) - Packet Detective -

PLV - cont...(16:00-17:50 PDT) - We're From the Government and We're Here to Help Secure Open Source Software - Anjana Rajan, Brian Behlendorf, Charlie Gladstone, Jack Cable

PLV - Navigating the Digital Frontier: Advancing Cyber Diplomacy in a Connected World - Christopher Painter, Harry Krejsa, Monica M. Ruiz, Océane Thieriot, Orlando Garces

PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -

PWV - cont...(10:00-17:59 PDT) - Password Village Activities -

PYV - cont...(11:00-17:59 PDT) - Payment Village Challenges/CTF -

QTV - cont...(16:00-17:59 PDT) - Quantini Time! Cocktail hour for the Quantum curious and creative -

QTV - Quantum Computer Music Performance, by Scott Oshiro (one half of NpHz) - Scott Oshiro

RCV - cont...(16:20-17:05 PDT) - Riding with the Chollimas: Our 100-Day Quest to Identify a North Korean State-Sponsored Threat Actor - Mauro Eldritch

RCV - The Perils of Generative AI: Implications for Open Source Intelligence Research - Andy Dennis

SEV - cont...(08:30-17:30 PDT) - SECV - Youth Challenge -

SEV - cont...(08:30-17:59 PDT) - SECV Village Open
SEV - [Phishing with Dynamite: Harnessing AI to Supercharge Offensive Operations](#) - Dani Goland,Preston Thornburg
SOC - cont...(16:00-17:59 PDT) - [Queercon Mixers](#) -
SOC - cont...(16:00-17:59 PDT) - [WISP Peer-to-Peer Mentoring and Networking](#) -
SOC - cont...(10:00-17:59 PDT) - [Hacker Memorial](#) -
SOC - cont...(12:00-17:59 PDT) - [Lonely Hackers Club Meetup](#) -
SOC - cont...(10:00-17:59 PDT) - DCG Meetups
SOC - [Friends of Bill W](#) -
SOC - cont...(12:00-17:59 PDT) - HDA / Accessibility Area Open
SOC - cont...(12:00-17:59 PDT) - HDA Community Meetups
TCV - cont...(16:00-17:59 PDT) - [Diameter CTF](#) - Akib Sayyed,Zibran Sayyed
TEV - cont...(10:00-17:59 PDT) - [Tampere Evident Village Activities](#) -
VMV - cont...(16:30-17:30 PDT) - [The Impact Of Misinformation On Elections](#) - Joe Schniebes,Maia Mazurkiewicz,Michael Moore
WS - cont...(14:00-17:59 PDT) - [Starbase: open source graph security analysis \(Pre-Registration Required\)](#) - Adam Pierson,Austin Kelleher,Guillaume Ross
WS - cont...(14:00-17:59 PDT) - [Introduction to Exploit Development \(Pre-Registration Required\)](#) - Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman,Sam Bowne
WS - cont...(14:00-17:59 PDT) - [Hands-On TCP/IP Deep Dive with Wireshark - How this stuff really works \(Pre-Registration Required\)](#) - Chris Greer
WS - cont...(14:00-17:59 PDT) - [The Joy of Reverse Engineering: Learning With Ghidra and WinDbg \(Pre-Registration Required\)](#) - Wesley McGrew
WS - cont...(14:00-17:59 PDT) - [Digital Forensics and Incident Response Against the Digital Darkness: An Intro to Forensics Evil \(Pre-Registration Required\)](#) - Michael "S3curityNerd" Register,Michael "mR_F0r3n51c5" Solomon
XRV - cont...(10:00-17:59 PDT) - [XR Village Playground](#) -
XRV - [Push All the Buttons Digital Twinning with Idaho National Labs in collaboration with DEF CON ICS Village](#) - Kolton Heaps

Saturday - 18:00 PDT

[Return to Index](#) - [Locations Legend](#)

[CON](#) - cont...(10:00-19:59 PDT) - [The Lonely Hard Drive](#) -

[DC](#) - cont...(09:30-18:59 PDT) - [Human Registration Open](#) -

[DCGVR](#) - [Ghost on the wire- check the air](#) - hoodiePony

[MISC](#) - [EFF Tech Trivia](#) -

[MUS](#) - [Music Set / Entertainment \(Saturday, ACK Stage\)](#) - DotOrNot,Dr. McGrew,H4X,Icetre

Normal,NGHTHWK,SK,Z3npi,n0x08

Saturday - 19:00 PDT

[Return to Index](#) - [Locations Legend](#)

[CON](#) - cont...(10:00-19:59 PDT) - [The Lonely Hard Drive](#) -
[DCGVR](#) - [What is a GRC Hacker anyway?](#) - Allen Baranov
[MISC](#) - cont...(18:00-21:59 PDT) - [EFF Tech Trivia](#) -
[SOC](#) - [BlanketFort Con](#) -
[SOC](#) - (19:30-21:59 PDT) - [DEF CON Kids Party](#) -
[SOC](#) - Policy Lounge

Saturday - 20:00 PDT

[Return to Index](#) - [Locations Legend](#)

[CON](#) - [Hacker Jeopardy](#) -

[DCGVR](#) - cont...(19:05-20:05 PDT) - [What is a GRC Hacker anyway?](#) - Allen Baranov

[DCGVR](#) - DCGVR Closing

[DCGVR](#) - After Hours Social / Hang out with DEF CON Group members and DCG VR Staff

[MISC](#) - cont...(18:00-21:59 PDT) - [EFF Tech Trivia](#) -

[SOC](#) - cont...(19:30-21:59 PDT) - [DEF CON Kids Party](#) -

[SOC](#) - [Hacker Karaoke 15](#) -

[SOC](#) - cont...(19:00-21:59 PDT) - Policy Lounge

Saturday - 21:00 PDT

[Return to Index](#) - [Locations Legend](#)

[CON](#) - cont...(20:00-21:59 PDT) - [Hacker Jeopardy](#) -

[DCGVR](#) - cont...(20:10-21:10 PDT) - After Hours Social / Hang out with DEF CON Group members and DCG VR Staff

[MISC](#) - cont...(18:00-21:59 PDT) - [EFF Tech Trivia](#) -

[MUS](#) - [Yarrrrgh Pirate Night - Music Set / Entertainment \(Saturday, SYN Stage\)](#) - FuzzyNop, Miss

Jackalope, Ninjula, O'Craven Pirate Band, Skittish & Bus

[SOC](#) - [Arcade Party](#) -

[SOC](#) - [VetCon](#) -

[SOC](#) - [Hack The Box, Pub Crawl](#) -

[SOC](#) - [Capitol Tech University, Pub Crawl](#) -

[SOC](#) - [University of Advancing Technology, Pub Crawl](#) -

[SOC](#) - [SECV - 80's Themed Party!](#) -

[SOC](#) - cont...(19:30-21:59 PDT) - [DEF CON Kids Party](#) -

[SOC](#) - cont...(19:00-21:59 PDT) - [Policy Lounge](#)

Saturday - 22:00 PDT

[Return to Index - Locations Legend](#)

[SOC - cont...\(21:00-23:59 PDT\) - SECV - 80's Themed Party!](#) -
[SOC - Social Engineering Community Party](#) -

Saturday - 23:00 PDT

[Return to Index](#) - [Locations Legend](#)

[SOC - cont...\(21:00-23:59 PDT\)](#) - [SECV - 80's Themed Party!](#) -

[SOC - cont...\(22:00-23:59 PDT\)](#) - [Social Engineering Community Party](#) -

Sunday

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

Sunday - 06:00 PDT

[Return to Index - Locations Legend](#)

MISC - Defcon.run -

[Return to Index - Locations Legend](#)

MISC - cont...(06:00-11:59 PDT) - [Defcon.run](#) -

[Return to Index - Locations Legend](#)

MISC - cont...(06:00-11:59 PDT) - Defcon.run -

[Return to Index](#) - [Locations Legend](#)

[APV](#) - (09:30-10:15 PDT) - [WAF: Making a Problematic Security Tool Suck Less](#) - Emile Spir,Emmanuelle Lejeail

[CON](#) - [HardWired](#) -

[DC](#) - [Shell On Demand Appliance Machine \(S.O.D.A. Machine\) \(pronounced SODA\)](#) -

[MISC](#) - [cont...\(06:00-11:59 PDT\)](#) - [Defcon.run](#) -

[PHV](#) - [Honey Pot Workshop](#) -

[PHV](#) - [Wall of Sheep](#) -

[PHV](#) - [Build Your Own Botnet](#) -

[PHV](#) - [Linux Trainer Workshop](#) -

[PHV](#) - [NetworkOS: Be The Cloud](#) -

[PHV](#) - [RegEx Trainer](#) -

[PHV](#) - [Password Lab](#) -

[PHV](#) - [Fleet DefCon 31 Workshop](#) -

[PHV](#) - [Packet Inspector](#) -

[PHV](#) - [Packet Detective](#) -

[RTV](#) - [Malware Hunting an Offensive Approach](#) - Filipi Pires

[RTV](#) - [How to prioritize Red Team Findings? Presenting CRTFSS: Common Red Team Findings Score System Ver. 1.0](#) -

Guillermo Buendia

[RTV](#) - [Artificial Intelligence for Red Team Operations](#) - Peter Halberg

[RTV](#) - [Recon for Red Teamers and Bug Hunters 2.0](#) - Jason Haddix

Sunday - 10:00 PDT

[Return to Index - Locations Legend](#)

[AIV - Fuzzing and Symbolic Execution: Offensive Techniques to Unmask Vulnerabilities in Neural Networks](#) - Rafael Turner

[AIV - AI Village Generative Red Team Challenge](#) -

[AIV - \(10:45-11:30 PDT\) - GRT Report Out](#) - Sven Cattell

[APV - cont...\(09:30-10:15 PDT\) - WAF: Making a Problematic Security Tool Suck Less](#) - Emile Spir,Emmanuelle Lejeail

[APV - \(10:15-10:59 PDT\) - Hacking GitHub Actions: Abusing GitHub and Azure for fun and profit](#) - Magno Logan

[APV - Threat modelling fun session with OWASP Cornucopia](#) - Spyros Gasteratos

[APV - Secure Code Review Challenge](#) - Checkmarx

[APV - Hunt the Hacker - Detect compromises in your repositories!](#) - GitGuardian

[APV - Pasteur - A C++ library to eliminate injections](#) - Yariv Tal

[APV - Enhancing Security for ReactJS Applications: Exploring Advanced Defense Techniques](#) - Jim Manico

[ASV - Hack The Airport](#) -

[ASV - Unmanned Aerial Systems – Platform Security](#) -

[ASV - The Challenge - Lockheed Martin](#) -

[ASV - A-ISAC CTF](#) -

[ASV - Bricks in the Air](#) -

[ASV - ARINC 615a CTF](#) -

[ASV - PTP Flight Challenge](#) -

[ASV - Ask Me Anything About Cybersecurity in Aerospace](#) -

[ASV - \(10:30-11:20 PDT\) - The Looming Perils for End Users in Satellite Communications](#) - Vincent Lenders

[BHV - Table Top](#) - Felicity Milman,Jorge Acevedo Canabal,Nathan Case

[BTV - Blue Team Village Game Session](#) - aviditas

[CLV - Call Me Phishmael: Hunting Sensitive Docker Images in Google Container Registry Leaks](#) - Ian Dillon

[CLV - \(10:40-11:20 PDT\) - Tag, You're Exposed: Exploring Azure Service Tags and their Impact on your Security Boundary](#) - Aled Mehta,Christian Philipov

[CON - cont...\(09:00-12:59 PDT\) - HardWired](#) -

[CON - Capture The Packet FINALS](#) -

[CON - IoT Village CTF](#) -

[CON - Hardware Hacking Village CTF](#) -

[CON - ? Cube](#) -

[CON - 5n4ck3y](#) -

[CON - TeleChallenge](#) -

[CON - Adversary Wars CTF](#) -

[CON - Battle of The Bots](#) -

[CON - CMD+CTRL at DEF CON 31 - Booth Open](#) -

[CON - The Dark Tangent Look-Alike Contest](#) -

[CON - The Gold Bug Challenge](#) -

[CON - Ham Radio Fox Hunting Contest](#) -

[CON - The Lonely Hard Drive](#) -

[CON - Car Hacking Village CTF](#) -

[CON - venator aurum - A Treasure Hunt](#) -

[CON - CrackMeIfYouCan](#) -

[CON - Maps of the digital lands](#) -

[CON - Darknet-NG](#) -

[CON - Octopus Game](#) -

[CON - DEF CON Scavenger Hunt](#) -

[CON - DEFCON MUD DUMB TERMINAL EDITION](#) -

[CON - Red Alert ICS CTF](#) -

[CON - Red Team CTF](#) -

[CON - Radio Frequency Capture the Flag](#) -

[CON - Embedded CTF](#) -

[CON - Cloud Village CTF](#) -

CPV - CPV Welcome - Day 3 - CPV Staff
CPV - (10:30-10:45 PDT) - Intro to Ciphers - CPV Staff
DC - Vacuum robot security and privacy - prevent your robot from sucking your data - Dennis Giese
DC - Vendor Area Open -
DC - Human Registration Open -
DC - StackMoonwalk: A Novel approach to stack spoofing on Windows x64 - Alessandro "klezVirus" Magnosi, Arash "waldo-irc" Parsa, Athanasios "trickster0" Tserpelis
DC - Cellular carriers hate this trick: Using SIM tunneling to travel at light speed - Adrian "atrox" Dabrowski, Gabriel K. Gegenhuber
DC - cont...(09:00-15:30 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
DC - Exhibitor Area Open -
DC - Snoop unto them, as they snoop unto us - Michaud "5@V@g3" Savage, Rekcahdam, nullagent
DC - Contest Area Open
DC - War Stories Off The Record AMA -
ESV - Embedded Systems Village Activities -
HHV - Soldering Skills Village Activities -
HHV - RoboSumo Play Time -
ICSV - Let's Talk about Voice - Travis Jühr
ICSV - (10:30-10:59 PDT) - Vulnerability instead of security: How we managed to hack a PSIM system - Lukas Sokefeld
IOTV - IoT Village Hacking Playground -
IOTV - Critical Infrastructure & IoT Exploitation -
IOTV - Secure or Surrender -
IOTV - The IoT Kill Zone -
IOTV - IoT Village Hardware Hacking Exercises 2023 -
IOTV - Embedded Device Security Workshops -
IOTV - Perform Memory Extraction, Emulation and Shellcode -
IOTV - Hardware Hacking Your Kitchen -
LPV - Lockpick Village Activities -
LPV - (10:15-10:45 PDT) - Intro to Lockpicking - TOOOL
MISC - Last chance to pick up drives at the DDV -
MISC - cont...(06:00-11:59 PDT) - Defcon.run -
MIV - Hackathon result's presentation - Misinformation Village Staff
PHV - cont...(09:00-12:59 PDT) - Honey Pot Workshop -
PHV - cont...(09:00-12:59 PDT) - Wall of Sheep -
PHV - cont...(09:00-12:59 PDT) - Build Your Own Botnet -
PHV - cont...(09:00-12:59 PDT) - Linux Trainer Workshop -
PHV - cont...(09:00-12:59 PDT) - NetworkOS: Be The Cloud -
PHV - cont...(09:00-12:59 PDT) - RegEx Trainer -
PHV - cont...(09:00-12:59 PDT) - Password Lab -
PHV - cont...(09:00-12:59 PDT) - Fleet DefCon 31 Workshop -
PHV - cont...(09:00-13:59 PDT) - Packet Inspector -
PHV - cont...(09:00-12:59 PDT) - Packet Detective -
PLV - Putting Your Money Where Your Cyber Is: A Guided Discussion of Software Liability and Security - Andrea Matwyshyn
PSV - Physical Security Village Activities -
PWV - Password Village Activities -
PYV - Payment Village Challenges/CTF -
QTV - Math for Quantum - Mark Carney
RTV - IOCs + APTs = "Let's play a game!" - Hack your way through a hunt! - Leo Cruz
RTV - Passwords Argh Us - Traveler
RTV - cont...(09:00-10:59 PDT) - Artificial Intelligence for Red Team Operations - Peter Halberg
RTV - cont...(09:00-10:59 PDT) - Recon for Red Teamers and Bug Hunters 2.0 - Jason Haddix
SEV - SECV - Youth Challenge -
SEV - Cold Calls -
SEV - SECV Village Open

TCV - RF in the Middle Earth- Fallen 5G - Utku Y

TCV - (10:30-10:59 PDT) - All the things, all the time: Lifting the veil on security in the global mobile industry and how it works with hackers - James Moran

TEV - Tamper Evident Village Activities -

XRV - XR Village Playground -

XRV - Watching Androids Dream of Electric Sheep: Immersive Technology, Biometrics and the Law in collaboration with DEF CON Policy Village - Brittan Heller,Liz "LawyerLiz" Wharton

[AIV](#) - cont...(10:00-12:59 PDT) - [AI Village Generative Red Team Challenge](#) -
[AIV](#) - cont...(10:45-11:30 PDT) - [GRT Report Out](#) - Sven Cattell
[AIV](#) - (11:15-11:45 PDT) - [AI Village Closing Remarks](#) - AI Village Organizers
[APV](#) - [Threat modeling-based application security pipeline](#) - Larkins Carvalho,Nielet D'mello
[APV](#) - (11:45-12:30 PDT) - [Android Applications and APIs hacking](#) - Gabrielle Botbol
[APV](#) - cont...(10:00-11:59 PDT) - [Threat modelling fun session with OWASP Cornucopia](#) - Spyros Gasteratos
[APV](#) - cont...(10:00-11:59 PDT) - [Secure Code Review Challenge](#) - Checkmarx
[APV](#) - cont...(10:00-11:59 PDT) - [Hunt the Hacker - Detect compromises in your repositories!](#) - GitGuardian
[APV](#) - cont...(10:00-11:59 PDT) - [Pasteur - A C++ library to eliminate injections](#) - Yariv Tal
[APV](#) - cont...(10:00-11:59 PDT) - [Enhancing Security for ReactJS Applications: Exploring Advanced Defense Techniques](#) - Jim Manico
[ASV](#) - cont...(10:00-13:59 PDT) - [Hack The Airport](#) -
[ASV](#) - cont...(10:00-13:59 PDT) - [Unmanned Aerial Systems – Platform Security](#) -
[ASV](#) - cont...(10:00-13:59 PDT) - [The Challenge - Lockheed Martin](#) -
[ASV](#) - cont...(10:00-13:59 PDT) - [A-ISAC CTF](#) -
[ASV](#) - cont...(10:00-13:59 PDT) - [Bricks in the Air](#) -
[ASV](#) - cont...(10:00-13:59 PDT) - [ARINC 615a CTF](#) -
[ASV](#) - cont...(10:00-13:59 PDT) - [PTP Flight Challenge](#) -
[ASV](#) - cont...(10:00-13:59 PDT) - [Ask Me Anything About Cybersecurity in Aerospace](#) -
[ASV](#) - cont...(10:30-11:20 PDT) - [The Looming Perils for End Users in Satellite Communications](#) - Vincent Lenders
[BHV](#) - cont...(10:00-12:20 PDT) - [Table Top](#) - Felicity Milman,Jorge Acevedo Canabal,Nathan Case
[BTV](#) - [Project Obsidian Panel](#) -
[CLV](#) - cont...(10:40-11:20 PDT) - [Tag, You're Exposed: Exploring Azure Service Tags and their Impact on your Security Boundary](#) - Aled Mehta,Christian Philipov
[CLV](#) - (11:20-11:59 PDT) - [Security Logging in the cloud, trade-offs to consider and patterns to maximise the effectiveness of security data pipelines](#) - Marco Mancini
[CON](#) - cont...(09:00-12:59 PDT) - [HardWired](#) -
[CON](#) - cont...(10:00-12:59 PDT) - [Capture The Packet FINALS](#) -
[CON](#) - cont...(10:00-13:59 PDT) - [IoT Village CTF](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [Hardware Hacking Village CTF](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [? Cube](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [5n4ck3y](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [TeleChallenge](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [Adversary Wars CTF](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [Battle of The Bots](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [CMD+CTRL at DEF CON 31 - Booth Open](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [The Dark Tangent Look-Alike Contest](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [The Gold Bug Challenge](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [Ham Radio Fox Hunting Contest](#) -
[CON](#) - cont...(10:00-12:59 PDT) - [The Lonely Hard Drive](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [Car Hacking Village CTF](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [venator aurum - A Treasure Hunt](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [CrackMelfYouCan](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [Maps of the digital lands](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [Darknet-NG](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [Octopus Game](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [DEF CON Scavenger Hunt](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [DEFCON MUD DUMB TERMINAL EDITION](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [Red Alert ICS CTF](#) -
[CON](#) - cont...(10:00-11:59 PDT) - [Red Team CTF](#) -
[CON](#) - cont...(10:00-12:59 PDT) - [Radio Frequency Capture the Flag](#) -

CON - [Free Amateur Radio License Exams](#) -
 CON - cont...(10:00-13:59 PDT) - [Embedded CTF](#) -
 CON - cont...(10:00-11:59 PDT) - [Cloud Village CTF](#) -
 DC - [Burrowing Through The Network: Contextualizing The Vulkan Leaks & Historical State-Sponsored Offensive Operations](#) - Joe Slowik
 DC - cont...(10:00-15:59 PDT) - [Vendor Area Open](#) -
 DC - cont...(10:00-13:59 PDT) - [Human Registration Open](#) -
 DC - [Advanced ROP Framework: Pushing ROP to Its Limits](#) - Bramwell Brizendine, Shiva Shashank Kusuma
 DC - [The Art of Compromising C2 Servers: A Web Application Vulnerabilities Perspective](#) - Vangelis Stykas
 DC - cont...(09:00-15:30 PDT) - [Shell On Demand Appliance Machine \(S.O.D.A. Machine\) \(pronounced SODA\)](#) -
 DC - cont...(10:00-13:59 PDT) - [Exhibitor Area Open](#) -
 DC - [Unlocking hidden powers in Xtensa based Qualcomm Wifi chips](#) - Daniel Wegemer
 DC - cont...(10:00-13:59 PDT) - [Contest Area Open](#)
 DC - cont...(10:00-11:59 PDT) - [War Stories Off The Record AMA](#) -
 ESV - cont...(10:00-13:59 PDT) - [Embedded Systems Village Activities](#) -
 HHV - cont...(10:00-12:59 PDT) - [Soldering Skills Village Activities](#) -
 HHV - cont...(10:00-12:59 PDT) - [RoboSumo Play Time](#) -
 ICSV - [The Flaws in Cloud-based ICS Ecosystem](#) - Hank Chen
 ICSV - (11:30-11:59 PDT) - [Hunting Aberrant Maritime Network Traffic with Open-Source Software and Hardware](#) - Chet Hosmer
 IOTV - cont...(10:00-13:59 PDT) - [IoT Village Hacking Playground](#) -
 IOTV - cont...(10:00-13:59 PDT) - [Critical Infrastructure & IoT Exploitation](#) -
 IOTV - cont...(10:00-13:59 PDT) - [Secure or Surrender](#) -
 IOTV - cont...(10:00-13:59 PDT) - [The IoT Kill Zone](#) -
 IOTV - cont...(10:00-13:59 PDT) - [IoT Village Hardware Hacking Exercises 2023](#) -
 IOTV - cont...(10:00-13:59 PDT) - [Embedded Device Security Workshops](#) -
 IOTV - cont...(10:00-13:59 PDT) - [Perform Memory Extraction, Emulation and Shellcode](#) -
 IOTV - cont...(10:00-13:59 PDT) - [Hardware Hacking Your Kitchen](#) -
 LPV - cont...(10:00-13:59 PDT) - [Lockpick Village Activities](#) -
 LPV - [Safecracking for Everyone](#) - Jared Dygert
 MISC - cont...(06:00-11:59 PDT) - [Defcon.run](#) -
 MIV - cont...(10:00-11:30 PDT) - [Hackathon result's presentation](#) - Misinformation Village Staff
 MIV - (11:30-11:59 PDT) - [Misinfo Village Closing / Panel / Summary / Feedback](#) - Misinformation Village Staff
 PHV - cont...(09:00-12:59 PDT) - [Honey Pot Workshop](#) -
 PHV - cont...(09:00-12:59 PDT) - [Wall of Sheep](#) -
 PHV - cont...(09:00-12:59 PDT) - [Build Your Own Botnet](#) -
 PHV - cont...(09:00-12:59 PDT) - [Linux Trainer Workshop](#) -
 PHV - cont...(09:00-12:59 PDT) - [NetworkOS: Be The Cloud](#) -
 PHV - cont...(09:00-12:59 PDT) - [RegEx Trainer](#) -
 PHV - cont...(09:00-12:59 PDT) - [Password Lab](#) -
 PHV - cont...(09:00-12:59 PDT) - [Fleet DefCon 31 Workshop](#) -
 PHV - cont...(09:00-13:59 PDT) - [Packet Inspector](#) -
 PHV - cont...(09:00-12:59 PDT) - [Packet Detective](#) -
 PLV - [Hangover Trivia: Cyber Policy Edition](#) - Kurt Opsahl
 PSV - cont...(10:00-13:59 PDT) - [Physical Security Village Activities](#) -
 PSV - (11:30-11:59 PDT) - [Elevators 101](#) - Karen
 PWV - cont...(10:00-13:59 PDT) - [Password Village Activities](#) -
 PYY - cont...(10:00-13:59 PDT) - [Payment Village Challenges/CTF](#) -
 QTV - [Quantum Life - An open mic space discussing the possible futures granted by quantum technologies](#) - Mark Carney, Victoria Kumaran
 RFV - [War Driver Meetup](#) - RF Village Staff
 RTV - [OSINT Skills Lab Challenge](#) - Lee McWhorter, Sandra Stibbards
 RTV - [Storfield: A Quiet Methodology to Create Attacks in Mature Networks](#) - Cory Wolff
 RTV - [Hacking Web Apps and APIs with WebSploit Labs](#) - Omar Santos
 SEV - cont...(10:00-11:30 PDT) - [Cold Calls](#) -

SEV - cont...(10:00-13:59 PDT) - SECV Village Open
TCV - Telecom Village CTF
TEV - cont...(10:00-13:59 PDT) - Tamper Evident Village Activities -
XRV - cont...(10:00-11:59 PDT) - XR Village Playground -
XRV - Off the Rails: A demo with Pacific Northwest National Labs -
XRV - Most Meta - Live Meta Quest2 Hack - David "Icer" Maynor

[AIV](#) - cont...(10:00-12:59 PDT) - [AI Village Generative Red Team Challenge](#) -
[APV](#) - [Threat modelling fun session with OWASP Cornucopia](#) - Spyros Gasteratos
[APV](#) - cont...(11:45-12:30 PDT) - [Android Applications and APIs hacking](#) - Gabrielle Botbol
[APV](#) - (12:30-13:15 PDT) - [Unveiling the Dual Nature of ChatGPT and Copilot in Secure Development](#) - Kalyani Pawar
[APV](#) - [AMA - Jim Manico](#) - Jim Manico
[APV](#) - [How to Hide Behavior from Security Tools](#) - Deepfactor
[APV](#) - [Faking GitHub Reputation](#) - Checkmarx
[APV](#) - [Secure from Scratch: Secure Code Workshop](#) - Or Sahar
[ASV](#) - cont...(10:00-13:59 PDT) - [Hack The Airport](#) -
[ASV](#) - cont...(10:00-13:59 PDT) - [Unmanned Aerial Systems – Platform Security](#) -
[ASV](#) - cont...(10:00-13:59 PDT) - [The Challenge - Lockheed Martin](#) -
[ASV](#) - cont...(10:00-13:59 PDT) - [A-ISAC CTF](#) -
[ASV](#) - cont...(10:00-13:59 PDT) - [Bricks in the Air](#) -
[ASV](#) - cont...(10:00-13:59 PDT) - [ARINC 615a CTF](#) -
[ASV](#) - cont...(10:00-13:59 PDT) - [PTP Flight Challenge](#) -
[ASV](#) - cont...(10:00-13:59 PDT) - [Ask Me Anything About Cybersecurity in Aerospace](#) -
[ASV](#) - [Hack-A-Sat 4 Awards Ceremony](#) - Hack-A-Sat 4 Team
[BHV](#) - cont...(10:00-12:20 PDT) - [Table Top](#) - Felicity Milman,Jorge Acevedo Canabal,Nathan Case
[BHV](#) - (12:20-13:20 PDT) - [Tuning the human Bio-Field – proven classics forged with AI IOMT](#) - Wayne Burke and Team
[BTV](#) - (12:45-13:45 PDT) - [Blue Team Village Closing Ceremony](#) -
[CLV](#) - [Tales from a detection engineering in AWSland](#) - Rodrigo Montoro
[CLV](#) - (12:40-13:10 PDT) - [CNAPGoat - A multicloud vulnerable-by-design infrastructure deployment tool](#) - Igal Gofman,Noam Dahan
[CON](#) - cont...(09:00-12:59 PDT) - [HardWired](#) -
[CON](#) - cont...(10:00-12:59 PDT) - [Capture The Packet FINALS](#) -
[CON](#) - cont...(10:00-13:59 PDT) - [IoT Village CTF](#) -
[CON](#) - [Hack-A-Sat 4 \(HAS4\) -- Closing Ceremony](#) -
[CON](#) - cont...(10:00-12:59 PDT) - [The Lonely Hard Drive](#) -
[CON](#) - cont...(10:00-12:59 PDT) - [Radio Frequency Capture the Flag](#) -
[CON](#) - cont...(11:00-13:59 PDT) - [Free Amateur Radio License Exams](#) -
[CON](#) - cont...(10:00-13:59 PDT) - [Embedded CTF](#) -
[DC](#) - [LLMs at the Forefront: Pioneering the Future of Fuzz Testing in a Rapidly Changing World](#) - X
[DC](#) - cont...(10:00-15:59 PDT) - [Vendor Area Open](#) -
[DC](#) - cont...(10:00-13:59 PDT) - [Human Registration Open](#) -
[DC](#) - [#NoFilter: Abusing Windows Filtering Platform for privilege escalation](#) - Ron Ben-Yizhak
[DC](#) - [Terminally Owned - 60 years of escaping](#) - David Leadbeater
[DC](#) - cont...(09:00-15:30 PDT) - [Shell On Demand Appliance Machine \(S.O.D.A. Machine\) \(pronounced SODA\)](#) -
[DC](#) - cont...(10:00-13:59 PDT) - [Exhibitor Area Open](#) -
[DC](#) - [Retro Exploitation: Using Vintage Computing Platforms as a Vulnerability Research Playground and Learning Environment](#) - Wesley McGrew
[DC](#) - cont...(10:00-13:59 PDT) - [Contest Area Open](#)
[ESV](#) - cont...(10:00-13:59 PDT) - [Embedded Systems Village Activities](#) -
[HHV](#) - cont...(10:00-12:59 PDT) - [Soldering Skills Village Activities](#) -
[HHV](#) - cont...(10:00-12:59 PDT) - [RoboSumo Play Time](#) -
[HRV](#) - [My Callsign Is My Passport - Responsible Testing And Disclosure Of Amateur Radio Websites](#) - Dan Norte,Lucas Gahler
[ICSV](#) - [The War is Coming: Why Securing OPC-UA is more critical than ever](#) - Hank Chen
[ICSV](#) - (12:30-12:59 PDT) - [Is China Prepping an “Unforgettable Humiliation for GPS & America” \[VIRTUAL\]](#) - Dana Goward
[IOTV](#) - cont...(10:00-13:59 PDT) - [IoT Village Hacking Playground](#) -
[IOTV](#) - cont...(10:00-13:59 PDT) - [Critical Infrastructure & IoT Exploitation](#) -

IOTV - cont...(10:00-13:59 PDT) - [Secure or Surrender](#) -
IOTV - cont...(10:00-13:59 PDT) - [The IoT Kill Zone](#) -
IOTV - cont...(10:00-13:59 PDT) - [IoT Village Hardware Hacking Exercises 2023](#) -
IOTV - cont...(10:00-13:59 PDT) - [Embedded Device Security Workshops](#) -
IOTV - cont...(10:00-13:59 PDT) - [Perform Memory Extraction, Emulation and Shellcode](#) -
IOTV - cont...(10:00-13:59 PDT) - [Hardware Hacking Your Kitchen](#) -
LPV - cont...(10:00-13:59 PDT) - [Lockpick Village Activities](#) -
LPV - [Officially Unofficial Safecracking Tournament](#) - Jared Dygert
PHV - cont...(09:00-12:59 PDT) - [Honey Pot Workshop](#) -
PHV - cont...(09:00-12:59 PDT) - [Wall of Sheep](#) -
PHV - cont...(09:00-12:59 PDT) - [Build Your Own Botnet](#) -
PHV - cont...(09:00-12:59 PDT) - [Linux Trainer Workshop](#) -
PHV - cont...(09:00-12:59 PDT) - [NetworkOS: Be The Cloud](#) -
PHV - cont...(09:00-12:59 PDT) - [RegEx Trainer](#) -
PHV - cont...(09:00-12:59 PDT) - [Password Lab](#) -
PHV - cont...(09:00-12:59 PDT) - [Fleet DefCon 31 Workshop](#) -
PHV - cont...(09:00-13:59 PDT) - [Packet Inspector](#) -
PHV - cont...(09:00-12:59 PDT) - [Packet Detective](#) -
PSV - cont...(10:00-13:59 PDT) - [Physical Security Village Activities](#) -
PSV - (12:30-12:59 PDT) - [Forcible Entry 101](#) - Bill Graydon
PWV - cont...(10:00-13:59 PDT) - [Password Village Activities](#) -
PYV - cont...(10:00-13:59 PDT) - [Payment Village Challenges/CTF](#) -
QTV - [QOLOSSUS; Quantum CTF - Results!](#) -
RFV - cont...(11:00-12:59 PDT) - [War Driver Meetup](#) - RF Village Staff
SEV - cont...(10:00-13:59 PDT) - [SECV Village Open](#)
SEV - [SECV - Awards & Competitor Panel](#) -
SOC - [Hacker Memorial](#) -
SOC - [DCG Meetups](#)
SOC - [Friends of Bill W](#) -
SOC - [HDA / Accessibility Area Open](#)
SOC - [HDA Community Meetups](#)
TCV - cont...(11:00-12:59 PDT) - [Telecom Village CTF](#)
TEV - cont...(10:00-13:59 PDT) - [Tamper Evident Village Activities](#) -

APV - cont...(12:00-13:59 PDT) - [Threat modelling fun session with OWASP Cornucopia](#) - Spyros Gasteratos

APV - cont...(12:30-13:15 PDT) - [Unveiling the Dual Nature of ChatGPT and Copilot in Secure Development](#) - Kalyani Pawar

APV - (13:15-13:59 PDT) - [Scoping for Success \(Building a Great Bug Bounty program\)](#) - Jeffrey Guerra, Logan MacLaren

APV - cont...(12:00-13:59 PDT) - [AMA - Jim Manico](#) - Jim Manico

APV - cont...(12:00-13:59 PDT) - [How to Hide Behavior from Security Tools](#) - Deepfactor

APV - cont...(12:00-13:59 PDT) - [Faking GitHub Reputation](#) - Checkmarx

APV - cont...(12:00-13:59 PDT) - [Secure from Scratch: Secure Code Workshop](#) - Or Sahar

ASV - cont...(10:00-13:59 PDT) - [Hack The Airport](#) -

ASV - cont...(10:00-13:59 PDT) - [Unmanned Aerial Systems – Platform Security](#) -

ASV - cont...(10:00-13:59 PDT) - [The Challenge](#) - Lockheed Martin -

ASV - cont...(10:00-13:59 PDT) - [A-ISAC CTF](#) -

ASV - cont...(10:00-13:59 PDT) - [Bricks in the Air](#) -

ASV - cont...(10:00-13:59 PDT) - [ARINC 615a CTF](#) -

ASV - cont...(10:00-13:59 PDT) - [PTP Flight Challenge](#) -

ASV - cont...(10:00-13:59 PDT) - [Ask Me Anything About Cybersecurity in Aerospace](#) -

ASV - [Hacking Satellites: Houston, We Have a Problem](#) - Jacob Oakley

BHV - cont...(12:20-13:20 PDT) - [Tuning the human Bio-Field – proven classics forged with AI IOMT](#) - Wayne Burke and Team

BHV - (13:20-13:59 PDT) - [Bare Metal Firmware Development and Reverse Engineering](#) - Caleb Davis, Nathan Smith

BTV - cont...(12:45-13:45 PDT) - [Blue Team Village Closing Ceremony](#) -

CLV - cont...(12:40-13:10 PDT) - [CNAPPGoat - A multicloud vulnerable-by-design infrastructure deployment tool](#) - Igal Gofman, Noam Dahan

CON - cont...(10:00-13:59 PDT) - [IoT Village CTF](#) -

CON - cont...(12:00-13:30 PDT) - [Hack-A-Sat 4 \(HAS4\) -- Closing Ceremony](#) -

CON - cont...(11:00-13:59 PDT) - [Free Amateur Radio License Exams](#) -

CON - cont...(10:00-13:59 PDT) - [Embedded CTF](#) -

CPV - [How mathematical implementation issues lead to cryptographic vulnerabilities](#) - Bing Shi

DC - [Exploring Linux Memory Manipulation for Stealth and Evasion: Strategies to bypass Read-Only, No-Exec, and Distroless Environments](#) - Carlos Polop, Yago Gutierrez

DC - cont...(10:00-15:59 PDT) - [Vendor Area Open](#) -

DC - cont...(10:00-13:59 PDT) - [Human Registration Open](#) -

DC - cont...(09:00-15:30 PDT) - [Shell On Demand Appliance Machine \(S.O.D.A. Machine\) \(pronounced SODA\)](#) -

DC - cont...(10:00-13:59 PDT) - [Exhibitor Area Open](#) -

DC - [The Price of Convenience: How Security Vulnerabilities in Global Transportation Payment Systems Can Cost You](#) - Omer Attias

DC - cont...(10:00-13:59 PDT) - [Contest Area Open](#)

ESV - cont...(10:00-13:59 PDT) - [Embedded Systems Village Activities](#) -

IOTV - cont...(10:00-13:59 PDT) - [IoT Village Hacking Playground](#) -

IOTV - cont...(10:00-13:59 PDT) - [Critical Infrastructure & IoT Exploitation](#) -

IOTV - cont...(10:00-13:59 PDT) - [Secure or Surrender](#) -

IOTV - cont...(10:00-13:59 PDT) - [The IoT Kill Zone](#) -

IOTV - cont...(10:00-13:59 PDT) - [IoT Village Hardware Hacking Exercises 2023](#) -

IOTV - cont...(10:00-13:59 PDT) - [Embedded Device Security Workshops](#) -

IOTV - cont...(10:00-13:59 PDT) - [Perform Memory Extraction, Emulation and Shellcode](#) -

IOTV - cont...(10:00-13:59 PDT) - [Hardware Hacking Your Kitchen](#) -

LPV - cont...(10:00-13:59 PDT) - [Lockpick Village Activities](#) -

LPV - cont...(12:00-13:30 PDT) - [Official Unofficial Safecracking Tournament](#) - Jared Dygert

LPV - [Intro to Lockpicking](#) - TOOOL

PHV - cont...(09:00-13:59 PDT) - [Packet Inspector](#) -

PSV - cont...(10:00-13:59 PDT) - [Physical Security Village Activities](#) -

PSV - [Access Control Vulnerabilities: Breaking Into Buildings With Computers](#) - Chad,Shortman
PWV - cont...(10:00-13:59 PDT) - [Password Village Activities](#) -
PYV - cont...(10:00-13:59 PDT) - [Payment Village Challenges/CTF](#) -
SEV - cont...(10:00-13:59 PDT) - [SECV Village Open](#)
SEV - cont...(12:00-13:30 PDT) - [SECV - Awards & Competitor Panel](#) -
SOC - cont...(12:00-13:59 PDT) - [Hacker Memorial](#) -
SOC - cont...(12:00-13:59 PDT) - [DCG Meetups](#)
SOC - cont...(12:00-13:59 PDT) - [HDA / Accessibility Area Open](#)
SOC - cont...(12:00-13:59 PDT) - [HDA Community Meetups](#)
TEV - cont...(10:00-13:59 PDT) - [Tamper Evident Village Activities](#) -

Sunday - 14:00 PDT

[Return to Index - Locations Legend](#)

[DC - Panel: Hacker Court - Interactive Scenario](#) - winn0na

[DC - cont...\(10:00-15:59 PDT\) - Vendor Area Open](#) -

[DC - Contest Closing Ceremonies & Awards](#) -

[DC - cont...\(09:00-15:30 PDT\) - Shell On Demand Appliance Machine \(S.O.D.A. Machine\) \(pronounced SODA\)](#) -

[DC - TETRA tour de force: Jailbreaking digital radios and base stations for fun and secrets](#) - Carlo Meijer, Jos Wetzels, Wouter Bokslag

[PSV - Bypass 101](#) - Terry

[PSV - \(14:30-14:59 PDT\) - Bypass 102](#) - Ege

Sunday - 15:00 PDT

[Return to Index](#) - [Locations Legend](#)

DC - cont...(14:00-15:15 PDT) - [Panel: Hacker Court - Interactive Scenario](#) - winn0na

DC - cont...(10:00-15:59 PDT) - [Vendor Area Open](#) -

DC - cont...(14:00-15:15 PDT) - [Contest Closing Ceremonies & Awards](#) -

DC - (15:30-17:30 PDT) - [DEF CON Closing Ceremonies & Awards](#) - Jeff "The Dark Tangent" Moss

DC - cont...(09:00-15:30 PDT) - [Shell On Demand Appliance Machine \(S.O.D.A. Machine\) \(pronounced SODA\)](#) -

DC - cont...(14:00-15:15 PDT) - [TETRA tour de force: Jailbreaking digital radios and base stations for fun and secrets](#) - Carlo Meijer, Jos Wetzels, Wouter Bokslag

Sunday - 16:00 PDT

[Return to Index - Locations Legend](#)

[DC - cont...\(15:30-17:30 PDT\) - DEF CON Closing Ceremonies & Awards - Jeff "The Dark Tangent" Moss](#)

Sunday - 17:00 PDT

[Return to Index - Locations Legend](#)

[DC - cont...\(15:30-17:30 PDT\) - DEF CON Closing Ceremonies & Awards - Jeff "The Dark Tangent" Moss](#)

Speaker List

Aapo Oksman
Aaron "AJ" Morath
Aaron Kumavis
Aaron Rosenmund
Abhijeet Singh
Acid T
Adam Dobell
Adam Pierson
Adam Rose
Adam Zabrocki
Adhishree Kathikar
Adrian "atrox" Dabrowski
Adrian "threlfall" Wood
Adrian "threlfall" Wood
Adrien Ogee
AI Village Organizers
AI Village Organizers
Aishwarya Nair
Ajit Hatti
Akib Sayyed
Akib Sayyed
Akib Sayyed
Akib Sayyed
Akib Sayyed
Akib Sayyed
Akib Sayyed
Akib Sayyed
Aled Mehta
Alejandro Mayorkas
Alek Amrani
Alessandro "klezVirus" Magnosi
Alex Delamotte
Alex Lomas
Alex Lynd
Alex Lynd
Alex Mastrov
Alex Reuter
Alex Tereshkin
Alex
Alexander Dalsgaard Krog
Alexander Dodd
Alexander Skovsende
Alexandrine Torrents
Alexi Husky
Alfie Champion
Alik Koldobsky
Alissa Torres
Allan "dwangoAC" Cecil
Allan Friedman
Allen Baranov
Allison Young
Almost Human (BJ)

Alon Lerner
Amanda Glazer
Amanda Glazer
Amit Elazari
Andréanne Bergeron
Andrés Velázquez
Andrea Downing
Andrea Matwyshyn
Andrew "Spike" Brandt
Andrew Chi
Andrew Lemon
Andy Dennis
Andy Klein
Angelos Stavrou
Angus "0x10f2c_" Strom
Anjana Rajan
Ankita Gupta
Ankur Chowdhary
Ankush Jain
Anne Kim
Anon
Anthony "Coin" Rose
Anthony Hendricks
Antigone Peyton
Anurag Bohra
Arash "waldo-irc" Parsa
Arati Prabhakar
Ari Herbert-Voss
Ari Schwartz
Ark (from WiGLE)
Arnaud Soullié
Arthur Paixão
Artorias
Artorias
Asheer Malhotra
Ashlee Bengé
Ashlee Bengé
Ashley Sequeira
Asi Greenholts
Aswin Reji
Athanasios "trickster0" Tserpelis
Austin Carson
Austin Carson
Austin Carson
Austin Emmitt
Austin Kelleher
Austin Reid
Austin Shamlin
aviditas
aviditas
Ayan Islam
Backslash
Backslash
Barrett Darnell
Ben "NahamSec" Sadeghipour

Ben "NahamSec" Sadeghipour
Ben "NahamSec" Sadeghipour
Ben Bornholm
Ben Brücker
Ben D. Sawyer
Ben Gelman
Ben Nassi
Ben Varcoe
Ben Varcoe
Benny Zeltser
Berk Can Geyikci
Bill Budington
Bill Demirkapi
Bill Graydon
Bing Shi
bkobe
Blake Benson
Blunt
Bob Gourley
Bob Lord
Bohan Liu
Bolonium
Bosen Zhang
Brad Manuel
Brad Proctor
Bramwell Brizendine
Bramwell Brizendine
Brandon Bailey
Brandon DeVault
Brandon Enright
Brendan O'Leary
Brennan Marsh-Armstrong
Brent Zundel
Brian Behlendorf
Brian Halbach
Brian Stearns
Brien Croteau
Brittan Heller
Bryony Crown
Bryony Crown
Bryson Bort
Bryson Bort
c0debreaker
Caleb Davis
Caleb Davis
Cameron Byrd
Camille Stewart Gloster
Camille Stewart Gloster
Carlo Meijer
Carlos Galán
Carlos Polop
Carson Zimmerman
Carsten Schürmann
Casey Ellis
Casey Ellis

Cassie Crossley
Catherine Terranova
Catherine Terranova
Catherine Terranova
Catherine Terranova
CerealKiller
CerealKiller
Ceri Coburn
Cesare Pizzi
Chad
Chad
Chad
Charles Miller
Charles Smith
Charles Smith
Charley Snyder
Charlie Gladstone
Charlie Gladstone
Charlie Gladstone
Charlie
Checkmarx
Checkmarx
Checkmarx
Cheri Caddy
Chet Hosmer
Chet Hosmer
Chloé Messdaghi
Chloé Messdaghi
Chloé Messdaghi
ChocolateCoat
Chris Greer
Chris Inglis
Chris Jenkins
Chris Krebs
Chris Roberts
Chris Roberts
Christian "quaddi" Dameff
Christian Philipov
Christien "DiDog" Rioux
Christine Barker
Christoph Wedenig
Christopher Butera
Christopher Crowley
Christopher Forte
Christopher Forte
Christopher Ottesen
Christopher Painter
Christopher Painter
Christopher Wade
Clayton Dixon
Cliff Neve
Cliff Neve
Colin Haines
Constantine Nicolaidis
Cooper Quintin

Cooper Quintin
Corben Leo
Corey Hartman
Cory Doctorow
Cory Doctorow
Cory Wolff
Cory Wolff
Cory Wolff
Corynne McSherry
Corynne McSherry
CountZ3r0
CPV Program Committees
CPV Staff
CPV Staff
CPV Staff
CPV Staff
CPV Staff
CPV Staff
CPV Staff
CPV Staff
CPV Staff
CPV Staff
Craig Martell
CTRL/rsm
Cyb3rhawk
Cyb3rhawk
Cyb3rhawk
D.J. Davis
D9
Daly Barnett
Daly
Dan "AltF4" Petro
Dan Borgogno
Dan Grobarcik
Dan KB6NU
Dan Meidenbauer
Dan Norte
Dan
Dana Goward
Dani Goland
Daniel "Jcache" Goga
Daniel Avinoam
Daniel Bardenstein
Daniel Costantini
Daniel dos Santos
Daniel Fabian
Daniel Feichter
Daniel Isler
Daniel Miessler
Daniel Wegemer
Danny D. "B4nd1t0" Henderson Jr
Danny D. "B4nd1t0" Henderson Jr
Danny Joslin
Darren Linvill
datalocaltmp

Dave Collins
Dave Weston
David "digish0" Mitchell
David "Icer" Maynor
David Emmerich
David Forsey
David Forsey
David Guffrey
David Houston
David Jefferson
David Jefferson
David Joseph
David Leadbeater
David McGrew
David Melendez
David Melendez
David Nathans
David Pecoske
David Pecoske
David Rogers
David Rogers
David Rogers
David Rogers
David Vargas
deelo
Deepblue
Deepfactor
Deepfactor
Deepfactor
Deirdre Connolly
Del de Zela
Delchi
Dennis Giese
Dennis Giese
Deth Veggie
Deviant Ollam
Diane Akerman
Diego Mariano
DJ PatAttack
DJ Scythe
DJ St3rling
Dmitriy Beryoza
Dohyeon Kim
Donghyeon Jeong
Dongsung "Donny" Kim
Dontae Tyler
DotOrNot
DotOrNot
Doug Kent
Douglas Bernardini
Dr. McGrew
Drew Springall
Dries
Dual Core
Dylan "CyberStryke" Butler

Dylan Baklor
Edam Colón
Edison Alvarez
Ege
Ege
Ege
Eigentourist
Elia Anzuoni
Elizabeth Biddlecome
Elizabeth Biddlecome
Elizabeth St. Germain
Emile Spir
Emily Paull
Emma Stewart
Emmanuelle Lejeail
Eric Curwin
Eric Davis
Eric Davis
Eric Escobar
Eric Goldstein
Erick Galinkin
Ernest Liu
Eryk Salvaggio
Eugene Rodionov
Euntae Jang
Farzan Karimi
Fatou Sankare
Federico Pacheco
Felicity Milman
Felipe Molina
Felipe PrÓteus
Filipi Pires
Filipi Pires
Filipi Pires
Firas D Khatib
fivepenny
Florian Haag
Florian Haag
Frank "D9" DiGiovanni
FuzzyNop
Gabe Cohen
Gabi Cirlig
Gabriel K. Gegenhuber
Gabriela "Gabs" García
Gabrielle Botbol
Gabrielle Botbol
Gal Bitensky
Gal Elbaz
Gal Zror
Galina Pildush
Gannon "Dorf" Gebauer
Gary C. Kessler
Gary C. Kessler
Gaspard Baye
Gavin Klondike

GitGuardian
GitGuardian
GitGuardian
GitGuardian
Glenn Borskey
Gold Bug Challenge Team
good_pseudonym
Great Scott
Greg Carpenter
Greg Francis
Grind613
GuanCheng Li
Guillaume Ross
Guillermo Buendia
Guillermo Buendia
Guillermo Buendia
Gunnar Andrews
Gunnar Andrews
Guy Kaplan
Gwyddia
Gyle_dC
H4X
Hack-A-Sat 4 Team
Hack-A-Sat 4 Team
Hack-A-Sat 4 Team
Hallie Stern
Hallie Stern
Hamster
Hank Chen
Hank Chen
Hannah Zhao
Hannah Zhao
Harley Geiger
Harley Geiger
Harley Geiger
Harley Geiger
Harri Hursti
Harri Hursti
Harri Hursti
Harri Hursti
Harri Hursti
Harry Krejsa
Harshit Mahajan
Heather Adkins
heckseven
Henry Danielson
Henry Haswell
Henry Hill
hoodiePony
Howard Yang
Ian Dillon
Ian Fox
Ian Tabor
Icetre Normal
Igal Gofman

Igal Gofman
Ileana Barrionuevo
Ilkin Javadov
India McKinney
India McKinney
Irvin Lemus
Irvin Lemus
Isabella Rolz
J. Scott Christianson
Jace Powell
Jack Cable
Jack Cable
Jack Cable
Jacob Oakley
Jacqueline Burgette
Jake "Hubbl3" Krasnov
Jake Braun
Jake Hince
James "albinowax" Kettle
James Hawk
James Horseman
James Howe
James Moran
Jamie Friel
Jared Dygert
Jared Dygert
Jared Stroud
Jarvis
Jason Haddix
Jason Haddix
Jason Haddix
Jason Haddix
Jason Haddix
Jason Ingalls
Javier Aguinaga
Jayesh Ahire
Jayson E. Street
JC
Jeff "r3plicant" Tully
Jeff "The Dark Tangent" Moss
Jeff "The Dark Tangent" Moss
Jeff "The Dark Tangent" Moss
Jeff "The Dark Tangent" Moss
Jeff Foley
Jeff Foley
Jeff Foley
Jeffrey Guerra
Jen Easterly
Jen Easterly
Jen Easterly
Jenko Hwong
Jeonghoon Bae
Jeremy Banker
Jeremy Banker
Jeremy Jones

Jess Hoffman
Jesse Chick
Jessica Barker
Jim Manico
Jim Manico
JJ Hastings
Joaquin Lanfranconi
Joe Christian
Joe Gray
Joe Mast
Joe Minicucci
Joe Schniebes
Joe Schniebes
Joe Schottman
Joe Slowik
Joe Slowik
Joe Sullivan
Joel "TheTechromancer" Moore
Joel Bengé
Joel Gámez Molina
Joel Todoroff
John Hammond
John Medcalf
John Medcalf
John Novak
John Odum
John Odum
John Threat
John Volock
Jon A.
Jon F
Jon Marler
Jon Marler
Jonathan Bar Or
Jonathan Bar Or
Jonathan Birch
Jonathan Lusky
Jonathan Lusthaus
Jonathan Owens
Jonghyuk Song
Jorge Acevedo Canabal
Jos Wetzels
jos weyers
José Fernández
Jose Pisaro
Josep Pi Rodriguez
Joseph Gabay
Joseph Thacker
Josh Kamdjou
Josh Reiter
Joshua Herman
Joshua Saxe
juju43
juju43
Justin Ibarra

Kaitlyn Handelman
Kaitlyn Handelman
Kalyani Pawar
kampf
Karen
Karen
Karen
Karl Fosaaen
Kat Fitzgerald
Kat Megas
Kat Traxler
Kate Bertash
Kate
Kate
Katelyn "Medus4" Bowden
Katie Inns
Katie Trimble-Noble
Katitza Rodriguez
Kavia Venkatesh
Keenan Skelly
Keith Chapman
Kellee Wicker
Kemba Walden
Ken Munro
Ken Munro
Ken Pyle
Ken Tindell
Kendall Spencer
Kendall Spencer
Kenneth Yeung
Kent
Kenzie Dolan
Kevin "Kent" Clark
Kevin "Kent" Clark
Kevin Collier
Kevin Roberts
Kieran Green
Kirsten Renner
KitKat
KitKat
Kiyohito Yamamoto
Kiyohito Yamamoto
kobaltfox
kobaltfox
Kolton Heaps
Konstantinos Karagiannis
Konstantinos Karagiannis
Kristy Westphal
Krisz Klink
Kunal Bhattacharya
Kurt Opsahl
Kurt Opsahl
Kyle Easterly
Lander Beyer
Langston "Shock" Clement

Langston "Shock" Clement
Larkins Carvalho
LaTica Hammond
Lauren Proehl
Lauren Zabierek
Lauren Zabierek
Laurie Kirk
Lauryn Williams
Lee Cyborg
Lee McWhorter
Lee McWhorter
Lee McWhorter
Lee McWhorter
Lee McWhorter
Lee McWhorter
Lee McWhorter
Lei Jiang
Leigh-Anne Galloway
Leigh-Anne Galloway
Leo Cruz
Leo Cruz
Leo Cruz
Leo Cruz
Lewis Ardern
Lexie Thach
Lindsey Forson
Lindsey Forson
Litmoose
Litmoose
Liv Matan
Liz "LawyerLiz" Wharton
Logan MacLaren
Lola Ajayi
Lorenzo "Iopoc" Cococcia
Louis Nyffenegger
Louis Nyffenegger
Lozaning
Lozaning
Lucas Gahler
Lukas Sokefeld
M4x 5yn74x
Maayan Shaul
Mackenzie Jackson
Magen
Magik Plan
Magno Logan
Magno Logan
Maia Mazurkiewicz
Maia Mazurkiewicz
Maia Mazurkiewicz
Malcolm
Mar Williams
Marc Rogers
Marcello "byt3bl33d3r" Salvati
Marcello "byt3bl33d3r" Salvati

Marcia Hofmann
Marco Macchetti
Marco Mancini
Marcus Hutchins
Maria Bique
Maria Markstedter
Maria Uretsky
Mariam Elgabry
Maril Vernon
Mario Trujillo
Mark Carney
Mark Carney
Mark Carney
Mark Carney
Mark Carney
Mark Carney
Mark Carney
Mark Colaluca
Mark E. Schreiber
Mark Warner
Mars Cheng
Marta Janus
Martin Petran
Martin Strohmeier
Martin Strohmeier
MasterChen
Matias Katz
Matt "disOwn" Wagenknecht
Matt Blaze
Matt Blaze
Matt Blaze
Matt Cheung
Matt Cheung
Matt Edmondson
Matt Mahler
Matthew Canham
Matthew Harris
Matthew Knight
Matthew McPherrin
Matthew Nickerson
Matthew Nickerson
Matthias Göhring
matrix
Maurice Kent
Mauro Eldritch
Mauro Vignati
Mauro Vignati
Max 'Libra' Kersten
Max 'Libra' Kersten
Max Shirokawa Aalto
Maxie Reynolds
Maxime Clementz
Maxine "Frey" Filcher
Maxwell Dulin "Strikeout"
Miłosz Gaczkowski

Miana Ella Windall
Micah Lee
Michael "mR_F0r3n51c5" Solomon
Michael "S3curityNerd" Register
Michael "v3ga_hax" Aguilar
Michael Brown
Michael McCabe
Michael Messner
Michael Mitchell
Michael Moore
Michael Moore
Michael Moore
Michael Morgenstern
Michael Pearse
Michael Pelosi
Michael Ross
Michael Sellitto
Michael Stepankin
Michael Wylie
Michael Wylie
Michaela Lee
Michaela Lee
Michaud "5@V@g3" Savage
Michele Orrù
Michelle Levesley
Mick/nohackme
Mieke Eoyang
Mike "d4rkm4tter" Spicer
Mike Henkelman
Mike Larkin
Mike Raggo
Mikel Rodriguez
Mikhail Shcherbakov
Mikko Hypponen
Miles McCain
Misinformation Village Staff
Misinformation Village Staff
Misinformation Village Staff
Misinformation Village Staff
Misinformation Village Staff
Miss Jackalope
Miss Jackalope
Mitch Kitter
Mohamed Elsabagh
Monica M. Ruiz
Monica M. Ruiz
Muhammad Shahmeer
Musard Balliu
Mustafa Bilgici
n0x08
Nathan Case
Nathan Case
Nathan Case
Nathan Kirkland
Nathan Smith

Nathan Smith
Naveen Srinivasan
Neil Naveen
Nestori Syynimaa
Nestori Syynimaa
NGHTHWK
NGHTHWK
Nick Ascoli
Nick Frichette
Nick Maietta
Nick Saunders
Nick Swink
Nick Swink
Nicolas Minvielle
Nicolas Schickert
Nielet D'mello
Niels Loozekoot
Nikita Kronenberg
Nikolaos Makriyannis
Nils Amiet
Nina Alli
Nina Alli
Nina Kollars
Nina Kollars
Nina Lowe
NiNi Chen
Ninjula
Nitin Natarajan
Noah Gibson
Noam Dahan
Noam Dahan
Noam Moshe
Noam Moshe
NPC Collective
nullagent
nyxgeek
O'Craven Pirate Band
Océane Thieriot
Octavio Gianatiempo
Ofek Vayner
Ofri Ouzan
Ohad Zaidenberg
Oldmonk
Olivier Bilodeau
Olivier Tuchon
Om Mahida
Omar Santos
Omar Santos
Omar Santos
Omar Santos
Omar Santos
Omar Santos
Omar Santos
Omenscan
Omenscan

Omer Attias
Omer Attias
Omkar Arasaratnam
Omri Preiss
Or Sahar
Or Sahar
Oren Yomtov
Ori Perez
Orlando Garces
Orlando Garces
Oumou Ly
PankleDank
Patrick Kiley
Patrick Wardle
Patrick Wardle
Patrick Warren
Paul D.
Paul Gerste
Paul Mueller
Paula González Nagore
Paz Hameiri
Paz Hameiri
Pedram Hayati
Pedram Hayati
Pengfei "BigZaddy" Yu
Pentera
Perri Adams
Pete Cooper
Pete Cooper
Pete Hay
Peter Brown
Peter Dreyer
Peter Halberg
Peter Halberg
Peter Hansen
Peter Stephens
Peter Stephens
Peter Stephens
Peter Su
Philip Young "Soldier of FORTRAN"
Pj Metz
plug
plug
plug
Prajwal Panchmahalkar
Preston Thornburg
Probely
Probely
Probely
Puck
Puck
Quantum Quizmasters
Quantum Village Organizers
Quinn D. Mooney

R.J. "BeetleChunks" McDown
Raúl "r4ulcl" Calvo Laorden
Rae Baker
Rafael Turner
Rafal Janik
Rafal Janik
Ralph May
Ralph May
Ralph May
Ralph May
Ralph May
Ram Shankar Siva Kumar
Ram Shankar Siva Kumar
Randy Pestana
Raul Caro
Rebecca Markwick
Rebecca Scott Thein
Rekcahdam
RenderMan
RF Village Staff
Rian Phelps
Richard Baker
Richard DeMillo
Ricky "HeadlessZeke " Lawshae
RJ McCarley
Rob Ditmer
Rob Suárez
Robert Fitzpatrick
Robert Hudock
Robert Koehlmoos
Rodrigo Montoro
Rodrigo Montoro
Roger Dingleline
Rojan Rijal
Ron Ben-Yizhak
Rory Mir
Roshan Piyush
Rumman Chowdhury
Rumman Chowdhury
Russ McRee
Ryan "ElfMaster" O'Neill
Ryan Chapman
Ryan Heartfield
Ryan Holeman
Ryan Holeman
Ryan Hurst
Ryan Johnson
Ryan M. Montgomery
Ryan Zagrodnik
Safa Shahwan Edwards
Safa Shahwan Edwards
Sage Meadows
Sajjad "JJ" Arshad
sally
Sam Bowne

Sam Bowne
Sam Colaizzi
Sam Davison
Sam Haskins
Sam Quinn
SamunoskeX
SamunoskeX
Sandra Guasch Castello
Sandra Khalil
Sandra Khalil
Sandra Stibbards
Sandra Stibbards
Sandra Stibbards
Sandra Stibbards
Sandra Stibbards
Sandra Stibbards
Sandra Stibbards
sandw1ch
Sanjiv Kawa
Sarachai Boonyakiat
Sarah Amos
Sarah Hodgkinson
Sarah Powazek
Sarah Powazek
Savannah Lazzara
Scheme
Scotch and Bubbles
Scott "Duckie" Melnick
Scott Brink
Scott Campbell
Scott Graham
Scott Oshiro
Scott Shapiro
Sean Wilson
Sebastian Kohler
Segfault
Sergei Frankoff
Seth McKinnis
Seyfullah
Shahar Man
Shane Caldwell
Sharon Brizinov
Sharon Brizinov
Shea Nangle
Shea Nangle
Shiva Shashank Kusuma
Shortman
Shortman
Shortman
Silas Cutler
Simon Ammer
Simon Guiot
SK
Skittish & Bus
Skittish & Bus

Skyler Knecht
Snow
Sofi Celi
Spencer McIntyre
Spice Rack
Spyros Gasteratos
Spyros Gasteratos
Spyros Gasteratos
Spyros Gasteratos
Squiddy
STÖK
Starr Brown
Stefanie Metka
Steve Borosh
Steve Borosh
Steve Borosh
Steve Borosh
Steve Borosh
Steve Luczynski
Susan Greenhalgh
Suzanne Borders
Suzanne Schwartz
Suzanne Schwartz
Sven Cattell
Sven Cattell
Syntax
Taiiwo
Taiiwo
Tailor Herrarte
Tal Folkman
Tal Skverer
Talk Sinn
Tamas "SkelSec" Jos
Tan Jing Zhi
Tanya Janca
Tanya Simms
TC Johnson
Terrance DeJesus
Terry
Terry
ThatDeadGuy
ThatDeadGuy
The Icarus Kid
TheClockworkBird
TheClockworkBird
Theodora Skeadas
Thomas BYGODT
Thomas Chauchefoin
Thomas Dang
Thomas Elling
Thomas Klein
Thomas Kranz
Tib3rius
Tibet Ögünç
Tiffany Rad

Tim Ryder
Tim Weston
Tina "Mugwump Jones" Velez
Tohar Braun
Tom Bonner
Tom Pohl
Tom Stites
Tomer Bar
Tomer
Tommaso "tomgag" Gagliardoni
Tony Turner
TOOOL
TOOOL
TOOOL
TOOOL
TOOOL
TOOOL
TOOOL
Tracy Mosley
Traveler
Traveler
Traveler
Traveler
Travis Allen
Travis Juhr
Travis Weathers
Trevor "t1v0" Stevado
TRIODE
Troy Defty
Troy Mills
Trupti Shiralkar
Tushar Kulkarni
Tyson Meadors
Unnamed user
Utku Y
Vandana Verma Sehgal
Vangelis Stykas
Vardon Hamdiu
Victoria Kumaran
Victoria Kumaran
Vijay Bolina
Viktor Gazdag
Vincent "Vinnybod" Rose
Vincent Lenders
Viraj Gandhi
Vishal Thakur
Vitor Ventura
Vitor Ventura
Wasabi
Wayne Burke and Team
Wesley McGrew
Wesley McGrew
Whitney Phillips
Will Kay
Will McKeen

Will Pearce
William Baggett
William Taylor
Winn
winn0na
Wojciech Reguła
Woody
WooWon Kang
Wouter Bokslag
Wyatt Ford
wytshadow
X
Xavier Facéline
Xiling Gong
Xuan Xing
Yael Grauer
Yago Gutierrez
Yariv Tal
Yariv Tal
Yoann Dequeker
Yoni
Yotam Perkal
Younghoo Lee
YTCracker
Yusuke Kubo
Yusuke Kubo
Z3npi
Zach "justadequate" Reavis
Zach Hanley
Zachary Bertocchi
Zachary Minneker
Zbyszek Tenerowicz
Zebbler Encanti Experience
Zheng Wang
Zibran Sayyed
Zibran Sayyed
Zibran Sayyed
Zibran Sayyed
Zibran Sayyed
Zibran Sayyed
Zoey Selman

Talk List

? Cube - CON

? Cube - CON

? Cube - CON

"You can't cheat time" - Finding foes and yourself with latency trilateration - DC

(In)Direct Syscalls: A Journey from High to Low - RTV

(n)Map Exploration: A Great Time in Remote Destinations - BTV

#NoFilter: Abusing Windows Filtering Platform for privilege escalation - DC

125khz the Brown note for Cars - RFV

156 million targeted: Biggest social phishing cyberattacks during Brazil's election - MIV

2024 Election Threat Landscape - VMV

5n4ck3y - CON

5n4ck3y - CON

5n4ck3y - CON

A Broken Marriage: Abusing Mixed Vendor Kerberos Stacks - DC

A Comprehensive Review on the Less-Traveled Road: 9 Years of Overlooked MikroTik Pre-Auth RCE - DC

A Different Uber Post Mortem - DC

A Few Useful Lessons about AI Red Teaming - AIV

A Fireside Chat with Chris Roberts and Pete Cooper - ASV

A Fireside Chat with the TSA Administrator - ASV

A global approach to tackling software resilience - PLV

A Global Perspective On Election Integrity - VMV

A Pain in the NAS: Exploiting Cloud Connectivity to PWN your NAS - DC

A Series of Unfortunate Events - DC

A Slice of Deception: The 2023 #SECVC Debrief - SEV

A SSLippery Slope: Unraveling the Hidden Dangers of Certificate Misuse - DC

A-ISAC CTF - ASV

A-ISAC CTF - ASV

A-ISAC CTF - ASV

Abating the Eye of Sauron: Help Combat Authoritarian Censorship - PLV

Abortion Access in the Age of Surveillance - DC

About Face! Beginner Intro to Facial Recognition - CPV

Abusing CAN Bus Protocol Specification for Denial of Service in Embedded Systems - CHV

Abusing Microsoft SQL Server with SQLRecon - DL

Access Control Vulnerabilities: Breaking Into Buildings With Computers - PSV

Access Control Vulnerabilities: Breaking Into Buildings With Computers - PSV

Active Directory Attacks: The Good, The Bad, and The LOLwut (Pre-Registration Required) - WS

Advanced ROP Framework: Pushing ROP to Its Limits - DC

Advanced WiFi Attacks for Red Team Professionals (Pre-Registration Required) - WS

Adversary Wars CTF - CON

Adversary Wars CTF - CON

Adversary Wars CTF - CON

Aerospace Village - 5 Years On - ASV

AI Caramba! A DC <> DEF CON interface on machine learning - PLV

AI Village Closing Remarks - AIV

AI Village CTF Kickoff and Introduction - AIV

AI Village Generative Red Team Challenge - AIV

AI Village Generative Red Team Challenge - AIV

AI Village Generative Red Team Challenge - AIV

AI Village Keynote 2: AI red teaming tradecraft: a team of teams approach - AIV

AI Village Keynote: The last attempted AI revolution in security, and the next one - AIV

AI Village Opening Remarks - AIV

AI-Driven Hacker's Toolkit: Using AI to Learn Python and Scapy for Exploitation and Post-Exploitation Techniques - RTV

AI-Driven Hacker's Toolkit: Using AI to Learn Python and Scapy for Exploitation and Post-Exploitation Techniques - RTV
All information looks like noise until you break the code: Futureproofing the transportation sector - DC
All the things, all the time: Lifting the veil on security in the global mobile industry and how it works with hackers - TCV
All Your Vulns are Belong to Terms & Conditions - PLV
Am I Exploitable? (MI-X) - DL
AMA - Jim Manico - APV
AMA - Tib3rius - APV
Amateur Radio Digital Modes Primer - HRV
An Audacious Plan to Halt the Internet's Enshittification - DC
An Introduction to SAML and its Security - RTV
Analysis 101 for Incident Responders (Pre-Registration Required) - WS
Anaotomy of the Top 10 Cybersecurity Terrain for Critical Infrastructure - ICSV
Android App Hacking - Hacking for Good! (Pre-Registration Required) - WS
Android Applications and APIs hacking - APV
Android Applications and APIs Hacking - RTV
Antennas - RFV
Anti-Social Engineering: Can You Be a Good Social Engineer Without Being Social - SEV
Apple's Predicament: NSPredicate Exploitation on macOS and iOS - DC
Applied Emulation - A Practical Approach to Emulating Malware (Pre-Registration Required) - WS
AppSec Village Keynote: Collaborative Security: Fostering Innovation and Resilient Cyber Practices - APV
AppSec Village Keynote: From Camels to Collaboration, A Journey Through Technology AND Humans - APV
Arcade Party - SOC
Are you really eyeing my network? Network Reconnaissance for n00bs! - BICV
ARINC 615a CTF - ASV
ARINC 615a CTF - ASV
ARINC 615a CTF - ASV
Arson Herders: An IR Guide to Fighting and Lighting Fires - BTV
Art vs AI: How Artists Hack Computer Vision Systems - CPV
Artificial Intelligence and Race: Security or Surveillance? - BICV
Artificial Intelligence for Red Team Operations - RTV
Artificial Intelligence for Red Team Operations - RTV
Ask Me Anything About Cybersecurity in Aerospace - ASV
Ask Me Anything About Cybersecurity in Aerospace - ASV
Ask Me Anything About Cybersecurity in Aerospace - ASV
Ask the EFF - DC
Assessing the Security of Certificates at Scale - DC
Assessing the Vulnerabilities of the Open-Source Artificial Intelligence (AI) Landscape: A Large-Scale Analysis of the Hugging Face Platform - AIV
Attack Surface Framework - DL
Attacking Decentralized Identity - CPV
Attacks as a Service with The DeRF - CLV
AutoDriving CTF - CON
Automotive USB Fuzzing: How to fuzzing USB in vehicles to discover the real-world vulnerabilities - CHV
Azure AD recon with OSINT tools - RCV
Azure B2C 0-Day: An Exploit Chain from Public Keys to Microsoft Bug Bounty - DC
Azure DevOps Security - CLV
Backdoor in the Core - Altering the Intel x86 Instruction Set at Runtime - DC
Badge Cloning With Doppelgänger - RFV
Badge of Shame: Breaking into Secure Facilities with OSDP - DC
Bare Metal Firmware Development and Reverse Engineering - BHV
Battle of The Bots - CON
Battle of The Bots - CON
Battle of The Bots - CON
BBOT (Bihuge BLS OSINT Tool) - DL
Be a Nerd that Talks Good: Up-leveling how we talk about misinformation, to build community trust and awareness - MIV

Between a Log and a Hard Place: (mis)Adventures in Azure Logs - CLV
Beyond Ransomware: Protecting Lives and Data from Modern Threat Actors - BHV
Beyond the Breach: Exploring Cybersecurity Policies with Hacker Perspectives - PLV
BIC Village Closing Keynote - BICV
BIC Village Opening Keynote - BICV
Blacks in Cyber Lituation Party - SOC
Blacks in Cyber Village CTF - CON
BlanketFort Con - SOC
BLE CTF - DL
BLE Security 201 (Pre-Registration Required) - WS
Blindly hunting for Mercenaries - CPV
Blocking Pathways into Cybercrime: Current Efforts and Future Opportunities - PLV
Blue Team Village (BTV) Pool Party - SOC
Blue Team Village Closing Ceremony - BTV
Blue Team Village CTF - CON
Blue Team Village CTF - CON
Blue Team Village Game Session - BTV
Blue Team Village Opening Ceremony - BTV
Book Club Discussion and Exchange - SOC
Book Exchange - MISC
Bootsquad: Stomping out squatters - DCGVR
Boston Infinite Money Glitch: Hacking Transit Cards Without Ending Up In Handcuffs - DC
Breaking Barriers: A Deep Dive into Bypassing Next-Gen 2FA and MFA Security Measures - APV
Breaking BMC: The Forgotten Key to the Kingdom - DC
Bricks in the Air - ASV
Bricks in the Air - ASV
Bricks in the Air - ASV
Bridging the Gap: Cloud Threat Intelligence for Detection and Offensive Security Practitioners - CLV
Build Inspector - A modern Javert on the trail of CI/CD Anomalies and Intruders - DL
Build Your Own Botnet - PHV
Build Your Own Botnet - PHV
Build Your Own Botnet - PHV
Build Your Own Cat-Shaped USB Hacking Tool! (with the Nugget) - RTV
Build Your Own Cat-Shaped USB Hacking Tool! (with the Nugget) - RTV
Building an Effective Security Culture Program - SEV
Building Partnerships - VMV
Building Space Attack Chains using SPARTA - ASV
Building the Hacker Talent Pipeline Through Workforce and Education Ecosystems - PLV
Burrowing Through The Network: Contextualizing The Vulkan Leaks & Historical State-Sponsored Offensive Operations - DC
DC
Bypass 101 - PSV
Bypass 102 - PSV
Call Me Phishmael: Hunting Sensitive Docker Images in Google Container Registry Leaks - CLV
Calling it a 0-Day - Hacking at PBX/UC Systems - DC
Can I put my DNA on the blockchain, mom? - BHV
Capitol Tech University, Pub Crawl - SOC
Capture The Packet FINALS - CON
Capture The Packet Main Rounds - CON
Capture The Packet Preliminaries - CON
Capture The Packet Preliminaries - CON
Car Hacking Village CTF - CON
Car Hacking Village CTF - CON
Car Hacking Village CTF - CON
Career Workshop: New Career Seekers In Cybersecurity - BICV
Cellular carriers hate this trick: Using SIM tunneling to travel at light speed - DC

certmitm: automatic exploitation of TLS certificate validation vulnerabilities - DC
Certs Fucking Suck, So We Made a Cert: DISCO for Bodily Autonomy - CPV
ChatGPT: Your Red Teaming Ally - AIV
Chinese Prototype Review - VMV
Cicada 3301: An Exploration of the Cryptographic Enigma - CPV
Civil Cyber Defense: Use Your Resources to Defend Non-Profits as they Combat Human Trafficking and Subvert Authoritarian Regimes - DC
Climate Change and its Implications for Security and Privacy: An Uncharted Territory - CPV
Cloud Village - Keynote - CLV
Cloud Village CTF - CON
Cloud Village CTF - CON
Cloud Village CTF - CON
CloudRecon - finding ephemeral assets in the cloud - CLV
CMD+CTRL at DEF CON 31 - Booth Open - CON
CMD+CTRL at DEF CON 31 - Booth Open - CON
CMD+CTRL at DEF CON 31 - Booth Open - CON
CMD+CTRL at DEF CON 31 - Competition - CON
CMD+CTRL at DEF CON 31 - Free Play - MISC
CNAPPGoat - A multicloud vulnerable-by-design infrastructure deployment tool - CLV
CNAPPGoat - DL
Cold Calls - SEV
Cold Calls - SEV
Cold Calls - SEV
CON trolling the weather - DC
CON trolling the weather - ASV
Conflicting Security Reports from Halderman-Springall and from MITRE: Which Is Right? - VMV
Contactless Overflow: Code execution in payment terminals and ATM's over NFC - DC
Contain Yourself: Staying Undetected Using the Windows Container Isolation Framework - DC
Contest Closing Ceremonies & Awards - DC
CPV Ten Year Anniversary Gathering - CPV
CPV Welcome - Day 1 - CPV
CPV Welcome - Day 2 - CPV
CPV Welcome - Day 3 - CPV
Cracking Cicada 3301: The Future of Collaborative Puzzle-Solving - DC
CrackMeIfYouCan - CON
CrackMeIfYouCan - CON
CrackMeIfYouCan - CON
Creating and uncovering malicious containers Redux (Pre-Registration Required) - WS
Creative Misuse of AI Systems - AIV
Critical Infrastructure & IoT Exploitation - IOTV
Critical Infrastructure & IoT Exploitation - IOTV
Critical Infrastructure & IoT Exploitation - IOTV
Crushing crumbs of information to eat a whole cake. - RCV
Cryptosploit Workshop - CPV
CTH 101: Part I & II - BTV
CTH 101: Part III, IV, V - BTV
CTH: (n)Map Exploration: A Great Time in Remote Destinations - BTV
CTH: Log4j - The Silent Menace Among Us - BTV
Cult Of The Dead Cow Breaks The Internet (and you can too!) - SOC
Cutting through the noise: What you need to know are the real threats when it comes to AI - MIV
CVE Insanity - BHV
Cyber Hygiene: Security Awareness Training and Education - BICV
Cyber Policy Adrift – Charting a Path Forward for International Maritime Cybersecurity - PLV
Cyber-Physical Detection and Response: A new Paradigm in IACS Monitoring and Security - ICSV
CycleOverride Defcon Bike Ride - MISC

D0 N0 H4RM: A Healthcare Security Conversation - DC
Damned if you do - The risks of pointing out the emperor is buck naked - DC
Darknet-NG - CON
Darknet-NG - CON
Darknet-NG - CON
DARPA Announces an AI Cyber Initiative, Live at DC 32 and DC 33 - DC
DC 404/DC 678/ DC 770/ DC 470 (Atlanta Metro) - SOC
DC Kubernetes Capture the Flag (CTF) - CON
DC Kubernetes Capture the Flag (CTF) - CON
DC's Next Top Threat Model (DCNTTM) - BYODesign Presentation - MISC
DC's Next Top Threat Model (DCNTTM) - BYODesign Registration - MISC
DC's Next Top Threat Model (DCNTTM) - Kids - Learn Threat Modeling - MISC
DC's Next Top Threat Model (DCNTTM) - Kids - Learn Threat Modeling - MISC
DC's Next Top Threat Model (DCNTTM) - CON
DC's Next Top Threat Model (DCNTTM) - CON
DDV open and accepting drives for duplication - MISC
DDV open and accepting drives for duplication - MISC
DDV open and accepting drives for duplication - MISC
DE: Breaking the Rule - BTV
DE: Building a Detection Alert From a Threat Hunt - BTV
Death by 1000 Likes: How Much Do You Really Leak in Social Media? - PHV
Debate: NISQ and the future of Quantum Advantage: This village believes the current state of NISQ is already enabling quantum advantage for those who know how to use these technologies - QTV
Debate: The Quantum Village believes individual citizen privacy will be enhanced with the fielding of new quantum technologies. - QTV
Deep Diving Into HID Vulnerabilities: Heart of Darkness - PSV
DEF CON 101 - Welcome to DEF CON Panel - DC
DEF CON 31 Beard and Mustache Contest - CON
DEF CON Chess Kids Free-Play - MISC
DEF CON Chess Tournament - CON
DEF CON Closing Ceremonies & Awards - DC
DEF CON Groups Keynote - DCGVR
DEF CON Holland Group Presents: VrijMiBo - SOC
DEF CON Kids Meetup - SOC
DEF CON Kids Party - SOC
DEF CON Scavenger Hunt - CON
DEF CON Scavenger Hunt - CON
DEF CON Scavenger Hunt - CON
DEFCON MUD DUMB TERMINAL EDITION - CON
DEFCON MUD DUMB TERMINAL EDITION - CON
DEFCON MUD DUMB TERMINAL EDITION - CON
Defcon.run - MISC
Defcon.run - MISC
Defcon.run - MISC
Defcon.run - MISC
Defeating VPN Always-On - DC
Defender-Pretender: When Windows Defender Updates Become a Security Risk - DC
Defending KA-SAT: The detailed story of the response, how it was analyzed, and what was learned - DC
Defense Community - VMV
Defensive Coding and Hardened Javascript - APV
Democracy, Are You Citizen Or Subject? - VMV
Demystifying (& Bypassing) macOS's Background Task Management - DC
Demystifying Hacking for Government Officials - PLV
Designing RFID Implants - How flipping the bird opens doors for me - DC
DevSecOps Worst Practices - APV

Diameter CTF - TCV
Diameter Workshop - TCV
Diameter Workshop - TCV
Digital Forensics and Incident Response Against the Digital Darkness: An Intro to Forensicating Evil (Pre-Registration Required) - WS
Digital Media Authentication - A Toolkit for Journalists in the Fight Against Misinformation with Cryptographic Tools - MIV
DISARM Workshop - VMV
Discovering Shadow Vulnerabilities in Popular Open-Source Projects: A Reverse-Fuzzing Journey - APV
Disincentivizing misinformation: co-create a new platform business model - MIV
Dissecting Deception: The Role of Twitter in U.S. Political Discourse - MIV
Divided We Fall - VMV
Domain Fronting Through Microsoft Azure and CloudFlare: How to Identify Viable Domain Fronting Proxies - CPV
Doomed to repeat the past: classical hardware exploits made quantum - QTV
Doors, Cameras, and Mantraps: Oh, my! - LPV
DotNet Malware Analysis Masterclass (Pre-Registration Required) - WS
Dracon - DL
Dress Code - Analysis of the current status of the Content Security Policy - APV
Dungeons@Defcon - CON
Dungeons@Defcon - CON
Easy EASM - the zero dollar attack surface management tool - RCV
EFF Benefit Poker Tournament at DEF CON 31 - Poker - MISC
EFF Benefit Poker Tournament at DEF CON 31 - Pre-tournament clinic - MISC
EFF Tech Trivia - MISC
Ek47 – Payload Encryption with Environmental Keys - DL
Election Preparation: 2024 - VMV
ELECTRONizing macOS privacy - a new weapon in your red teaming armory - DC
Elevators 101 - PSV
Elon, Twitter and the PIA: How not to achieve privacy in aviation - ASV
Email Detection Engineering and Threat Hunting Inbox (Pre-Registration Required) - WS
EMBA - From firmware to exploit - ICSV
Embedded CTF - CON
Embedded CTF - CON
Embedded CTF - CON
Embedded Device Security Workshops - IOTV
Embedded Device Security Workshops - IOTV
Embedded Device Security Workshops - IOTV
Embedded Systems Village Activities - ESV
Embedded Systems Village Activities - ESV
Embedded Systems Village Activities - ESV
Enhancing Cybersecurity Resilience in the Brazilian Healthcare Sector: A Novel Red Team and Blue Team Methodology - BHV
Enhancing Security for ReactJS Applications: Exploring Advanced Defense Techniques - APV
Enhancing vulnerability research through the use of virtual reality workspaces. - DCGVR
Evading Logging in the Cloud: Bypassing AWS CloudTrail - CLV
Evil Digital Twin: Learn Psychological Manipulation with an Uncensored LLM - MIV
EvilnoVNC: Next-Gen Spear Phishing Attacks - DL
Exhibitor Area Open - DC
Exhibitor Area Open - DC
Exhibitor Area Open - DC
Exploiting OPC-UA in Every Possible Way: Practical Attacks Against Modern OPC-UA Architectures - DC
Exploring Linux Memory Manipulation for Stealth and Evasion: Strategies to bypass Read-Only, No-Exec, and Distroless Environments - DC
Exploring the Impact of PQC on Cryptographic Key Management - CPV
FaFo: Laboratory Physical and ICS (Warning: not for the faint of heart) - BHV
Faking GitHub Contributions - APV

Faking GitHub Reputation - APV
Faking GitHub Reputation - APV
Fantastic Ethernets and Where to Find Them - DC
Fear and Loathing on Plum Island - ICSV
Film screening: Reality Games Using film and interactive storytelling to inoculate against the disinformation tsunami: - MIV
Finding bugs and scaling your security program with Semgrep - APV
Finding Hidden Gems In Temporary Mail Services - RCV
Fireside Chat with the National Cyber Director Kemba Walden - DC
First Timers Workshop - VMV
Five (or More) Maritime Cybersecurity Challenges - ICSV
Fix The Flag - Battle Challenge - APV
Fix The Flag: A Secure Programming Competition - APV
Fleet DefCon 31 Workshop - PHV
Fleet DefCon 31 Workshop - PHV
Fleet DefCon 31 Workshop - PHV
Flipping Locks: Remote Badge Cloning with the Flipper Zero - PSV
Flipping the Coin: Red and Blue Teaming in Windows Environments (Pre-Registration Required) - WS
FlowMate and CSTC for Advanced Pentesting - APV
FlowMate - DL
FoldIt - BHV
For Kids: Castle Defenders - APV
Forcible Entry 101 - PSV
Forensic Analysis: Part I & II - BTV
Forensics 101 Part I & II - BTV
Free Amateur Radio License Exams - MISC
Free Amateur Radio License Exams - CON
Free Amateur Radio License Exams - CON
Free Pokemon Card Bus Passes - PSV
Friends of Bill W - SOC
Friends of Bill W - SOC
Friends of Bill W - SOC
Friends of Bill W - SOC
Friends of Bill W - SOC
Friends of Bill W - SOC
Friends of Bill W - SOC
Friends of Bill W - SOC
From Feature to Weapon: Breaking Microsoft Teams and SharePoint Integrity - DC
From Service Catalog Admin to Account takeover: Privilege Escalation with Service Catalog Launch Constraint - CLV
Full Stack Disclosures - BHV
Fuzzing and Symbolic Execution: Offensive Techniques to Unmask Vulnerabilities in Neural Networks - AIV
Game-Changing Advances in Windows Shellcode Analysis - DC
Gazing into the crystal ball: Hacking and Securing Future Telecoms Networks - TCV
Gender Inclusive Features Across the Health Information System - DCGVR
General-purpose Languages: What Are Your Habits? - BICV
Generating Rf With Stock Hardware For Drones - HHV
Generative Adversarial Network (GAN) based autonomous penetration testing for Web Applications - APV
Getting a Migraine - uncovering a unique SIP bypass on macOS - DC
Getting ahead of the bad guys with Internet Scanning data. - RCV
Getting into Trouble with Machine Learning Models (Pre-Registration Required) - WS
Getting More Bang for your Buck: Appsec on a Limited Budget - APV
Ghost in the (Voting) Machine: Failures in Election Software Supply Chain Security - VMV
Ghost in the Neurons - ML Webshells - AIV
Ghost on the wire- check the air - DCGVR
GhostToken: Exploiting Google Cloud Platform App Infrastructure to Create Unremovable Trojan Apps - DC
Glad Scientist | Village Vibes Immersive Performance, a data-driven real time audiovisual VR performance - XRV
Glad Scientist | Village Vibes Immersive Performance, a data-driven real time audiovisual VR performance - XRV

Glyph - DL
Good Vibrations, Haptic Sensory Augmentation Implants - BHV
Google Workspace Red Team Automation with SWAT - CLV
GothCon - SOC
Growing the Community of AI Hackers with the Generative Red Team - DC
GRT Report Out - AIV
Guarding the Galaxy: Ransomware Resilience in CubeSats - ASV
Hac-Man - CON
Hack The Airport - ASV
Hack The Airport - ASV
Hack The Airport - ASV
Hack the Box Hack-a-thon - SOC
Hack the Box Hack-a-thon - SOC
Hack The Box, Pub Crawl - SOC
Hack the Future: Why Congress and the White House are supporting AI Red Teaming - DC
Hack-A-Sat 4 (HAS4) -- Closing Ceremony - CON
Hack-A-Sat 4 (HAS4) - CON
Hack-A-Sat 4 (HAS4) - CON
Hack-A-Sat 4 Awards Ceremony - ASV
Hack-A-Sat 4 Briefing - ASV
Hack-A-Sat 4 Briefing - ASV
Hack3r Runw@y - CON
Hack3r Runw@y - CON
Hackaprompt 2023: Trials and Tribulations - AIV
Hackathon presentation - MIV
Hackathon result's presentation - MIV
Hacker Flairgrounds - SOC
Hacker Jeopardy - CON
Hacker Jeopardy - CON
Hacker Karaoke 15 - SOC
Hacker Karaoke 15 - SOC
Hacker Memorial - SOC
Hacker Memorial - SOC
Hacker Memorial - SOC
HackFortress - CON
HackFortress - CON
Hacking GitHub Actions: Abusing GitHub and Azure for fun and profit - APV
Hacking Meta Quest - RTV
Hacking Policy & Prompts - Happy Hour - MISC
Hacking Quantum Advantage for Classical Processes; Intro to Quantum-Inspired Use Cases - QTV
Hacking Real Web Areas - RTV
Hacking Reproductive Health - BHV
Hacking Satellites: Houston, We Have a Problem - ASV
Hacking The Metal: An Intro to ARM Assembly Language Programming (Pre-Registration Required) - WS
Hacking Web Apps and APIs with WebSploit Labs - RTV
Hacking Web Apps and APIs with WebSploit Labs - RTV
Hacking Web Apps and APIs with WebSploit Labs - RTV
Hacking Web Apps and APIs with WebSploit Labs - RTV
Hacking Web Apps and APIs with WebSploit Labs - RTV
Hacks, Leaks, and Revelations: Pandemic Profiteers and COVID-19 Disinformation - MIV
Ham In A Day Class - HRV
Ham Radio Fox Hunting Contest - CON
Ham Radio Fox Hunting Contest - CON
Ham Radio Fox Hunting Contest - CON
Hands On a Cyber Policy Crisis: Testing Assumptions and Navigating Challenges through a Cyber Simulation - PLV

Hands-on GitHub Actions - APV
Hands-On TCP/IP Deep Dive with Wireshark - How this stuff really works (Pre-Registration Required) - WS
Hangover Trivia: Cyber Policy Edition - PLV
Haptics Hack-a-Thon - XRV
Haptics Hack-a-Thon - XRV
HardHat Command & Control Framework - DL
Hardware Hacking Rube Goldberg Machine - HHV
Hardware Hacking Rube Goldberg Machine - HHV
Hardware Hacking Village CTF - CON
Hardware Hacking Village CTF - CON
Hardware Hacking Village CTF - CON
Hardware Hacking Village Prize Ceremony - HHV
Hardware Hacking Your Kitchen - IOTV
Hardware Hacking Your Kitchen - IOTV
Hardware Hacking Your Kitchen - IOTV
HardWired - CON
HardWired - CON
HardWired - CON
Hey CryptoBro!: How Are Criminals Laundering, Monetizing, and Targeting Cryptocurrency, NFTs, and Smart Contracts? - DCGVR
HF Radio Demonstration - HRV
HF Radio Demonstration - HRV
Hide your kids, turn off your Wi-Fi, they Rogue APing up in here (Pre-Registration Required) - WS
HL7Magic: Medical Data Hacking Made Easy - DC
Holding Leaflets in the Left Hand and Bullets in the Right: A Guide to Understanding Modern Chinese Information Operations - MIV
Homo sapiens sapiens to Homo sapiens nova - the coming speciation - BHV
Honey Pot Workshop - PHV
Honey Pot Workshop - PHV
Honey Pot Workshop - PHV
House of Heap Exploitation (Pre-Registration Required) - WS
How an automotive security researcher had his car stolen via 'CAN Injection' - CHV
How can we encourage more hackers to engage with policy makers? - PLV
How do you solve a problem like Mirai - establishing a policy baseline for the IoT around the world - PLV
How hackers can send feedback directly to policymakers like the pros (Pre-Registration Required) - WS
How hackers can work with government, industry, civil society to protect high-risk communities - PLV
How I Built Recon to Scale with Serverless Architecture - RCV
How I Found Your Password, and Other Advanced Data Hoarding Techniques - RCV
How mathematical implementation issues lead to cryptographic vulnerabilities - CPV
How Most Internal Networks are Compromised: A Set of Common Active Directory Attacks and How to Perform Them from Linux - RTV
How NOT to Train your Hack Bot: Dos and Don'ts of Building Offensive GPTs - AIV
How to [NOT] look like a Red Team - RTV
How to [NOT] look like a Red Team - RTV
How to build a body in your garage - BHV
How to Crush Field Day and Win Big Prizes - HRV
How to Hide Behavior from Security Tools - APV
How to Hide Behavior from Security Tools - APV
How to Hide Behavior from Security Tools - APV
How to Hide Behavior from Security Tools - APV
How to Lose Access to your Door in Two Easy Steps - LPV
How to prioritize Red Team Findings? Presenting CRTFSS: Common Red Team Findings Score System Ver. 1.0 - RTV
How to prioritize Red Team Findings? Presenting CRTFSS: Common Red Team Findings Score System Ver. 1.0 - RTV
How to prioritize Red Team Findings? Presenting CRTFSS: Common Red Team Findings Score System Ver. 1.0 - RTV
Human Registration Open - DC

Human Registration Open - DC
Human Registration Open - DC
Human Registration Open - DC
Hunt the Hacker - Detect compromises in your repositories! - APV
Hunt the Hacker - Detect compromises in your repositories! - APV
Hunt the Hacker - Detect compromises in your repositories! - APV
Hunt the Hacker - Detect compromises in your repositories! - APV
Hunting & Exploiting DLL Sideloads - RTV
Hunting & Exploiting DLL Sideloads - RTV
Hunting Aberrant Maritime Network Traffic with Open-Source Software and Hardware - ICSV
I Am A Former National Cybersecurity Director, Ask Me Anything! - PLV
I am the captain now: Taking remote control of ships engines, helm, azipods, ballasting and plenty more. - ICSV
I Am The Disinformation Campaign - RCV
I Can Shop Securely Online So Why Can't I Vote Online? - VMV
I Watched You Roll the Die: Unparalleled RDP Monitoring Reveal Attackers Tradecraft - DC
I'm On The Hype Train: Bottom's Up! - ICSV
ICS Forensics tool - DL
ICS Village - TSA Keynote - ICSV
Identifying and securing Firebase vulnerabilities at scale - CLV
IDN-Squatting Detector - APV
If it looks like a duck... Russia's new MDM communication strategies on Social Media after the War in Ukraine - MIV
Ignore the Law: The Legal Risks of Prompt Injection Attacks on Large Language Models - AIV
Improving the Speed of Cybersecurity: Seven Cyber Metrics for Maritime Owners and Operators - ICSV
Influencing Voters Through Social Media, ADTECH, Big Data, and AI - VMV
Infrastructure as Remote Code Execution - CLV
Insider Threats (InT): Hindsight and Foresight - BTV
IntelOps - Operation Spacewatch - CON
International Cyber Policy 101 - PLV
Internet censorship: what governments around the globe have in store for you - DC
Interventions To Address Technology-Facilitated Violence in Democracy - VMV
Intro to Ciphers - CPV
Intro to Ciphers - CPV
Intro to Ciphers - CPV
Intro to Ciphers - CPV
Intro to Lockpicking - LPV
Intro to Lockpicking - LPV
Intro to Lockpicking - LPV
Intro to Lockpicking - LPV
Intro to Lockpicking - LPV
Intro to Lockpicking - LPV
Intro to Lockpicking - LPV
Intro to Lockpicking - LPV
Introducing IAM-APE - CLV
Introduction to Cryptographic Attacks (Pre-Registration Required) - WS
Introduction To Esp8266/Esp32 Microcontrollers And Building A Wi-Fi Deauthentication Detector - HHV
Introduction to Exploit Development (Pre-Registration Required) - WS
IOCs + APTs = "Let's play a game!" - Hack your way through a hunt! - RTV
IOCs + APTs = "Let's play a game!" - Hack your way through a hunt! - RTV
IOCs + APTs = "Let's play a game!" - Hack your way through a hunt! - RTV
IOCs + APTs = "Let's play a game!" - Hack your way through a hunt! - RTV
IoT Village - Free Book Signing with author Ted Harrington - IOTV
IoT Village CTF - CON
IoT Village CTF - CON
IoT Village CTF - CON
IoT Village Hacking Playground - IOTV
IoT Village Hacking Playground - IOTV

IoT Village Hacking Playground - IOTV
IoT Village Hardware Hacking Exercises 2023 - IOTV
IoT Village Hardware Hacking Exercises 2023 - IOTV
IoT Village Hardware Hacking Exercises 2023 - IOTV
IR 101: Part I, II, III - BTV
IR 101: Part IV, V - BTV
IR Analysis: Part I & II - BTV
IR/4n6: Obsidian DFIR - Gang aft agley - BTV
Is 2023 the Year of Privacy: How History and States are Posed to Change Privacy? - CPV
Is China Prepping an "Unforgettable Humiliation for GPS & America" [VIRTUAL] - ICSV
It's Coming from Inside the House: Next Steps for Addressing U.S. Network Abuse - PLV
It's In That Place Where I Put That Thing That Time - CON
It's In That Place Where I Put That Thing That Time - CON
It's not that your threat intelligence IOCs are worthless... - BTV
IVY HAUL: A Computational Linguistics Analysis of a Disinformation Actor - MIV
J4 Gate, The Hustler Poker Cheating Scandal investigation and how Hacking helped me do it - DC
JWT Parkour - APV
Katalina - DL
Keeping stores safe: how do we better secure apps and app stores? - PLV
Keynote - Reshaping Reconnaissance: AI's Role in Open Source Intelligence - RCV
Kids Only Karaoke - MISC
Kraken, a modular multi-language webshell for defense evasion - DL
Kubernetes Offense - RTV
Labs and Trust: How to build a successful aviation cybersecurity research programme - ASV
Lambda Looter - DL
Lantern: Blue Energy - BHV
Last chance to pick up drives at the DDV - MISC
Lawyers Meet - SOC
Leakonomics 101: The Last Year in Data Leaks - RCV
Learning to Hack Bluetooth Low Energy with BLE CTF (Pre-Registration Required) - WS
Legend of Zelda: Use After Free (TASBot glitches the future into OoT) - DC
Lessons learned when building a Maritime Systems Security Laboratory Testbench - ICSV
Let Night City Sleep - Governance Against a Cyberpunk Future - PLV
Let's Talk about Voice - ICSV
Linecon - MISC
Linux Trainer Workshop - PHV
Linux Trainer Workshop - PHV
Linux Trainer Workshop - PHV
Lions and Tigers and Fancy Bears, Oh My!: A Cautionary Tale for our Cyber Future - DC
Living Next Door to Russia - DC
Living off the Land with Connectwise: How I Built An Attack Platform & Botnet in 23 lines of Python! - APV
LLM Legal Risk Management, and Use Case Development Strategies to Minimize Risk - AIV
LLMs at the Forefront: Pioneering the Future of Fuzz Testing in a Rapidly Changing World - DC
LLMs: Loose Lips Multipliers - AIV
Lock Bypass 101 - PSV
Lock Bypass 101 - PSV
Lock Bypass 102 - PSV
Lock Bypass 102 - PSV
Lockpick Village Activities - LPV
Lockpick Village Activities - LPV
Lockpick Village Activities - LPV
Lonely Hackers Club Meetup - SOC
Lonely Hackers Club Meetup - SOC
Long Live the Empire: A C2 Workshop for Modern Red Teaming (Pre-Registration Required) - WS
Look Ma I'm the CEO! Real-Time Video and Audio Deep-Fake! - DC

Looking into the future, what can we learn about hacking in science-fiction? - DC
Lupo: Malware IOC Extractor - DL
Machine Learning for N00bs (Pre-Registration Required) - WS
Main features of Russia's disinformation and propaganda ecosystem in Spanish-speaking countries - MIV
Make Your Own Use - HHV
Make Your Own Use - HHV
Making a Sick Badge - BHV
Making The DEF CON 31 Badge - DC
Malware design - abusing legacy Microsoft transports and session architecture - DC
Malware development on secured environment - Write, adapt, overcome (Pre-Registration Required) - WS
Malware Hunting an Offensive Approach - RTV
Malware Hunting an Offensive Approach - RTV
Malware Hunting an Offensive Approach - RTV
Maps of the digital lands - CON
Maps of the digital lands - CON
Maps of the digital lands - CON
Mass Owning of Seedboxes - A Live Hacking Exhibition - DC
Mastering OSINT: Advanced Techniques in the Realm of Big Data - RCV
Math for Quantum - QTV
Medical VR - BHV
Meduza: How an exiled pirate media outlet breaks through the Kremlin's propaganda firewall - DC
Merch (formerly swag) Area Open -- README - DC
Merch (formerly swag) Area Open -- README - DC
Merch (formerly swag) Area Open -- README - DC
MetaHub Demo: Automating Ownership, Context, and Impact Assessment in Security Findings - CLV
Metawar - DC
Misinfo Village Closing / Panel / Summary / Feedback - MIV
Misinformation As A Service: Social Engineering techniques applied in service contexts. - MIV
Misinformation Village Q and A - MIV
MitmWs: A new way to pentest websocket applications - APV
Model Based Systems Engineering for Security Engineers - BHV
Modernizing AX.25 packet radio with Modern Packet Message Manager - HRV
Monroeville Live: An IR Tabletop for the Rest of Us - BTV
Most Meta - Live Meta Quest2 Hack - XRV
Movie Night - MISC
Moving Target Defense for Space Systems - ASV
mTLS: when certificate authentication done wrong - DC
Music Set / Entertainment (Friday, ACK Stage) - MUS
Music Set / Entertainment (Friday, SYN Stage) - MUS
Music Set / Entertainment (Saturday, ACK Stage) - MUS
Music Set / Entertainment (Thursday, ACK Stage) - MUS
Music Set / Entertainment (Thursday, SYN Stage) - MUS
My Callsign Is My Passport - Responsible Testing And Disclosure Of Amateur Radio Websites - HRV
My CPAP has a recall, lets open it instead! - BHV
Navigating the Digital Frontier: Advancing Cyber Diplomacy in a Connected World - PLV
Navigating the Disinformation Landscape - MIV
ndays are also 0days: Can hackers launch 0day RCE attack on popular softwares only with chromium ndays? - DC
NetworkOS: Be The Cloud - PHV
NetworkOS: Be The Cloud - PHV
NetworkOS: Be The Cloud - PHV
New Isn't Always Novel: Grep'ing Your Way to \$20K at Pwn2Own, and How You Can Too - DC
No Starch Press - Book Signing - Cory Doctorow, Red Team Blues & Chokepoint Capitalism - MISC
No Starch Press - Book Signing - Maria Markstedter, Blue Fox: Arm Assembly Internals and Reverse Engineering - MISC
No time for NISQy Business - QTV
Non-State Actors in the Russia/Ukraine Conflict - PLV

Nosy Cops: Exposing the Hidden Potential of Police Radio - RCV
Not All Alerts Are Born Equal: Insights from AppSec Experts on Prioritizing Security Alerts - APV
Not Just The Pickle: An Overview of Exploitable ML Serialization Formats - AIV
Nothing but Net: Leveraging macOS's Networking Frameworks to Heuristically Detect Malware - DC
Nuthin But A G Thang: Evolution of Cellular Networks - DC
Octopus Game - CON
Octopus Game - CON
Octopus Game - CON
Off the Rails: A demo with Pacific Northwest National Labs - XRV
Off the Rails: A demo with Pacific Northwest National Labs - XRV
Off the Rails: A demo with Pacific Northwest National Labs - XRV
Officially Unofficial Safecracking Tournament - LPV
Oh The Places You'll Guo: Using Media Variants to Trace the Organization and Behavior of an Coordinated Inauthentic Influence Operation - RCV
Open Distro of Malicious Maritime Hacking Tools: What Could Go Wrong? - ICSV
Open Sesame! How To Open One Thousand And One Locks In The 21St Century? - HHV
Open Source API Security for devsecops - APV
Open Source Intelligence (OSINT) for Hackers - RTV
Open Source Intelligence (OSINT) for Hackers - RTV
Opening Session of MisinfoVillage 2023 - MIV
OpenQuantum: open-source hardware for quantum engineering via trapped atoms - QTV
OpenSSF Scorecard - DL
Orbiting the White House: Cybersecurity as a Space Imperative - ASV
OSINT for Physical Security Intelligence - PHV
OSINT Privacy Unmasked: Taking Control of Your Digital Footprint in a Hyper-Connected World - RCV
OSINT Situational Awareness - RCV
OSINT Skills Lab Challenge - RTV
OSINT Skills Lab Challenge - RTV
OSINT Skills Lab Challenge - RTV
OSINT Skills Lab Challenge - RTV
OSINT Skills Lab Challenge - RTV
OT Vulnerability analysis methodology - ICSV
OT: Why OT Cybersecurity Engineers Drink So Much - BTV
Over the Air, Under the Radar: Attacking and Securing the Pixel Modem - DC
OWASP crAPI: Completely Ridiculous API - DL
Packet Detective - PHV
Packet Detective - PHV
Packet Detective - PHV
Packet Inspector - PHV
Packet Inspector - PHV
Packet Inspector - PHV
Panel Discussion - Bugs, Bounties, & Breaches - Insider Tales from the Trenches - RCV
Panel Discussion -- Designing and Deploying NOC/SOC in a Mobile, Limited Bandwidth Maritime Environment - ICSV
Panel: Hacker Court - Interactive Scenario - DC
Password Lab - PHV
Password Lab - PHV
Password Lab - PHV
Password Village Activities - PWV
Password Village Activities - PWV
Password Village Activities - PWV
Passwords Argh Us - RTV
Passwords Argh Us - RTV
Passwords Argh Us - RTV
Passwords Argh Us - RTV
Pasteur - A C++ library to eliminate injections - APV

Patient Zero Day: The Leaking of Patients' Private Health Data Contributed To A Medical Infodemic - MIV
Payment Village Challenges/CTF - PYV
Payment Village Challenges/CTF - PYV
Payment Village Challenges/CTF - PYV
Payment Village Workshop - PYV
Payment Village Workshop - PYV
Pcapinator: Rise of the PCAP Machines - DL
Pen Test Partners Power Hour - ASV
Pentesting Industrial Control Systems: OCP-U-HACK (Pre-Registration Required) - WS
Per-mission Impossible: Exploring the Android Permission Model and Intents - APV
Perform Memory Extraction, Emulation and Shellcode - IOTV
Perform Memory Extraction, Emulation and Shellcode - IOTV
Perform Memory Extraction, Emulation and Shellcode - IOTV
Phishing with Dynamite: Harnessing AI to Supercharge Offensive Operations - SEV
Physical Attacks Against Smartphones - DC
Physical pentesting in a post-covid world - PSV
Physical Security Village Activities - PSV
Physical Security Village Activities - PSV
Physical Security Village Activities - PSV
Political Polarization - VMV
Polynonce: An ECDSA Attack and Polynomial Dance - DC
Power Corrupts; Corrupt It Back! Hacking Power Management in Data Centers - DC
Practical advice for navigating edtech privacy - CPV
Privacy of Web PKI Revocation - CPV
Private Keys in Public Places - DC
Private Until Presumed Guilty - DC
Project Obsidian Panel - BTV
ProjectDiscovery Nuclei - DL
Protecting the AWS ecosystem - Misconfigurations, IAM, and Monitoring (Pre-Registration Required) - WS
Protocol Identification for Integration - RFV
pTFS Presents: Mayhem Industries – Starphish - CON
PTP Flight Challenge - ASV
PTP Flight Challenge - ASV
PTP Flight Challenge - ASV
Pub Quiz at DEF CON - CON
Push All the Buttons Digital Twinning with Idaho National Labs in collaboration with DEF CON ICS Village - XRV
Putting Your Money Where Your Cyber Is: A Guided Discussion of Software Liability and Security - PLV
Pwning the Pwners with Mindware - PHV
Q-CTF QOLOSSUS Update - QTV
QDoor: Exploiting Approximate Synthesis for Backdoor Attacks in Quantum Neural Networks - QTV
QOLOSSUS - Quantum Capture the Flag Introduction! - QTV
QOLOSSUS; Quantum CTF - Results! - QTV
Quantini Time! Cocktail hour for the Quantum curious and creative - QTV
Quantum attacks on next-gen cryptosystems: lattices, annealers, notebooks - QTV
Quantum Computer Music Performance, by Scott Oshiro (one half of NpHz) - QTV
Quantum Life - An open mic space discussing the possible futures granted by quantum technologies - QTV
Quantum Music Workshop: Build Your Own Quantum Synthesizer! - QTV
Quantum Technologies on a Raspberry Pi (and HackRF one) - QTV
Quantum Village Opening! - QTV
Queercon Mixers - SOC
Queercon Mixers - SOC
Queercon Mixers - SOC
QueerCon Party - SOC
Radiation Detection For The Rest Of Us - Diy Radiation Spectroscopy - HHV
Radio Frequency Capture the Flag - CON

Radio Frequency Capture the Flag - CON
Radio Frequency Capture the Flag - CON
Radio Frequency Capture the Flag - CON
Recon for Red Teamers and Bug Hunters 2.0 - RTV
Red Alert ICS CTF - CON
Red Alert ICS CTF - CON
Red Alert ICS CTF - CON
Red Hot (Red Team TTPs) - RTV
Red Hot (Red Team TTPs) - RTV
Red Hot (Red Team TTPs) - RTV
Red Hot (Red Team TTPs) - RTV
Red Hot (Red Team TTPs) - RTV
Red Team CTF - CON
Red Team CTF - CON
Red Team CTF - CON
Red Wizard: user-friendly Red Teaming infrastructure - DL
Redeploying the Same Vulnerabilities: Exploiting Wireless Side-Channels in Electric Vehicle Charging Protocols - CHV
RegEx Trainer - PHV
RegEx Trainer - PHV
RegEx Trainer - PHV
Retro Exploitation: Using Vintage Computing Platforms as a Vulnerability Research Playground and Learning Environment - DC
Review: Surprise Unboxing - VMV
Revolutionizing ELF binary patching with Shiva: A JIT binary patching system for Linux - DC
RF in the Middle Earth- Fallen 5G - TCV
RFID Hacking - PSV
Riding with the Chollimas: Our 100-Day Quest to Identify a North Korean State-Sponsored Threat Actor - RCV
Risk Limiting Audits Of All Contests - VMV
RLA Workshop - VMV
RoboSumo Bracket Competition - HHV
RoboSumo Play Time - HHV
RoboSumo Play Time - HHV
RoboSumo Play Time - HHV
Route to bugs: Analyzing the security of BGP message parsing - DC
RuleProcessorY & Gramify - Rule Optimization & Password Analysis tools - DL
Runtime Riddles: Abusing Manipulation Points in the Android Source - DC
Sadprotocol Goes To Hollywood: Hijacking An Ip Camera Stream As Seen In The Movies - HHV
Safecracking for Everyone - LPV
Saturday - DL
Scoping for Success (Building a Great Bug Bounty program) - APV
Scripting OWASP Amass for a Customized Experience - RTV
Scripting OWASP Amass for a Customized Experience - RTV
SE Improv - SEV
Second Breakfast: Implicit and Mutation-Based Serialization Vulnerabilities in .NET - DC
Secretary of the Department of Homeland Security Alejandro Mayorkas - DC
Secure by Design: Ask the Government Anything and Red-Pen Workshop - PLV
Secure Code Review Challenge - APV
Secure Code Review Challenge - APV
Secure from Scratch: Secure Code Workshop for DEF CON Kids - APV
Secure from Scratch: Secure Code Workshop - APV
Secure Micropatching on the ISS - ASV
Secure or Surrender - IOTV
Secure or Surrender - IOTV
Secure or Surrender - IOTV
Securing Critical Versions of your Reality - XRV

Securing the Front Lines: Protecting Front-End Applications from Overlooked Vulnerabilities - APV
Securing the Supply Chain - PLV
Securing the Whole System: Corpal to Corporate - BHV
Securing the Whole System: Corporal to Corporate - BHV
Security Engineering for Adversarial Emulation and Red Teaming - BTV
Security Logging in the cloud, trade-offs to consider and patterns to maximise the effectiveness of security data pipelines - CLV
SECV - 80's Themed Party! - SOC
SECV - Awards & Competitor Panel - SEV
SECV - Youth Challenge - SEV
SECV - Youth Challenge - SEV
SECV - Youth Challenge - SEV
Shall we play a game? Just because a Large Language Model speaks like a human, doesn't mean it can reason like one. - DC
Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) - DC
Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) - DC
Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) - DC
Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) - DC
Shipping Wardriving Hardware - Cross-country Wigle on the Cheap - RFV
Shufflecake, AKA Truecrypt on Steroids for Linux - DL
Signals! In! Spaaaaaace! - RFV
Silent Spring: Prototype Pollution Leads to Remote Code Execution in Node.js - DC
Small Leaks, Billions Of Dollars: Practical Cryptographic Exploits That Undermine Leading Crypto Wallets - DC
Smashing the state machine: the true potential of web race conditions - DC
Snakes on a Screen: Taming Offensive IronPython Techniques (Pre-Registration Required) - WS
Snoop unto them, as they snoop unto us - DC
So you want to become a Detection Engineer - BTV
SOC Panel: Finding, Keeping, and Caring for the Best People - BTV
Social Engineering Community (SEC) Vishing Competition - CON
Social Engineering Community (SEC) Vishing Competition - CON
Social Engineering Community (SEC) Vishing Competition - CON
Social Engineering Community (SEC) Youth Challenge - CON
Social Engineering Community (SEC) Youth Challenge - CON
Social Engineering Community Party - SOC
Soldering Skills Village Activities - HHV
Soldering Skills Village Activities - HHV
Soldering Skills Village Activities - HHV
Space Pirates on the Loose! - Space-Based Threats to US Interests - ASV
SpamChannel: Spoofing Emails From 2 Million+ Domains and Virtually Becoming Satan - DC
Spoofing certificates with MD5 collisions - party like it's 2008! - CPV
Spooky authentication at a distance - DC
Spot the True Positives! - APV
Spot the True Positives! - APV
Spread spectrum techniques in disposable drones for anti drone evasion - DC
SS7 CTF - TCV
SS7 Workshop - TCV
SS7 Workshop - TCV
SSH Tunneling: Evading Network Detection and Creating Proxies - RTV
SSO Sloppy, SSO Suspect, SSO Vulnerable - CLV
StackMoonwalk: A Novel approach to stack spoofing on Windows x64 - DC
Starbase: open source graph security analysis (Pre-Registration Required) - WS
Still Vulnerable Out of the Box: Revisiting the Security of Prepaid Android Carrier Devices - DC
Storfield: A Quiet Methodology to Create Attacks in Mature Networks - RTV
Storfield: A Quiet Methodology to Create Attacks in Mature Networks - RTV
Stories from the Trenches: Operating a Aeronautics Cyber Range - ASV
Stories from the Trenches - RTV

Strix Interceptor - DL
SucoshScanny - DL
Surgical Physicians and Cybersecurity - BHV
Surprise Unboxing - VMV
SusParams: Hypercharge your web testing with DATA - APV
T3SF (Technical TableTop Exercises Simulation Framework) - DL
Table Top - BHV
Tag, You're Exposed: Exploring Azure Service Tags and their Impact on your Security Boundary - CLV
Taking Down Applications with Logic: A Comprehensive Guide to Modern DOS Attacks - DCGVR
Tales from a detection engineering in AWSland - CLV
Tamper Evident Village Activities - TEV
Tamper Evident Village Activities - TEV
Tamper Evident Village Activities - TEV
Teaching Information Warfare: Strategies in Academic and Government Institutions - MIV
TeleChallenge - CON
TeleChallenge - CON
TeleChallenge - CON
Telecom Village Inauguration - TCV
Ten Years of CPV - Program Committees - CPV
Ten Years of CPV - The Gold Bug Challenge - CPV
Terminally Owned - 60 years of escaping - DC
TETRA tour de force: Jailbreaking digital radios and base stations for fun and secrets - DC
The "Why" of Lock Picking - LPV
The Art of Compromising C2 Servers: A Web Application Vulnerabilities Perspective - DC
The attackers guide to exploiting secrets in the universe - APV
The Beverage Cooling Contraption Contest - CON
The Challenge - Lockheed Martin - ASV
The Challenge - Lockheed Martin - ASV
The Challenge - Lockheed Martin - ASV
The Coming War on Encryption, Part 3 (and how you can fight back) - PLV
The Creation Of The Out-Of-Band Anti Virus Dock (Oobavd) - HHV
The Curse of Ncurses - DCGVR
The Dark Playground of CI/CD: Attack Delivery by GitHub Actions - CLV
The Dark Playground of CI/CD: Attack Delivery by GitHub Actions - APV
The Dark Tangent Look-Alike Contest - CON
The Dark Tangent Look-Alike Contest - CON
The Dark Tangent Look-Alike Contest - CON
The DEFCON31 Multi User Dungeon Adventure (DEFCON MUD) Internet Edition - MISC
The Fallacy Of Privacy - VMV
The Flaws in Cloud-based ICS Ecosystem - ICSV
The GitHub Actions Worm: Compromising GitHub repositories through the Actions dependency tree - DC
The Gold Bug Challenge - CON
The Gold Bug Challenge - CON
The Gold Bug Challenge - CON
The Hackers, The Lawyers, And The Defense Fund - DC
The Human Threat Factor - Cloud Security Misconfigurations - CLV
The Impact Of Misinformation On Elections - VMV
The Importance of Arts and Crafts in ThreatOps - PHV
The Internals of Veilid, a New Decentralized Application Framework - DC
The International Wigle Space Balloon - RFV
The IoT Kill Zone - IOTV
The IoT Kill Zone - IOTV
The IoT Kill Zone - IOTV
The Joy of Reverse Engineering: Learning With Ghidra and WinDbg (Pre-Registration Required) - WS
The Lonely Hard Drive - CON

The Lonely Hard Drive - CON
The Lonely Hard Drive - CON
The Looming Perils for End Users in Satellite Communications - ASV
The Megabiome is In Charge: Taking Control of Your Microbial World - BHV
The Metasploit Framework - DL
The of History XR From Fiction to Reality - XRV
The Perils of Generative AI: Implications for Open Source Intelligence Research - RCV
The Petting Zoo: Breaking into CTFs (Pre-Registration Required) - WS
The Price of Convenience: How Security Vulnerabilities in Global Transportation Payment Systems Can Cost You - DC
The Promise and Perils of Planetary-Scale ISPs - PLV
The Quantum Debates - QTV
The RingHopper Journey or How We Almost Zero-day'd the World - DC
The Rocky Balboa Guide to Security Research: Getting Back Up When You Get Knocked Down - CLV
The Russian Playbook vs. the Chinese Little Red Playbook: Broadening our Understanding of Effective Disinformation Operations - MIV
The Sinister Synergy of Advanced AI: Automatically Orchestrating Large-scale Scam Campaigns with Large Generative Models - AIV
The Ultimate AppSec Trivia Challenge - APV
The Ultimate AppSec Trivia Challenge - APV
The Ultimate AppSec Trivia Challenge - APV
The Ultimate AppSec Trivia Challenge - APV
The Unlikely Romance: Critical Infrastructure Edition - ICSV
The Unofficial DEF CON Shoot - MISC
The Village People Party: hosted by Car Hacking, ICS, Aerospace, and Biohacking Villages - SOC
The War is Coming: Why Securing OPC-UA is more critical than ever - ICSV
The Wifydra: Multiheaded RF Panopticon - DL
There are no mushroom clouds in cyberwar - DC
These Port Scans are Trash: Improving Nmap by Writing New Scripts and Libraries (Pre-Registration Required) - WS
Threat modeling-based application security pipeline - APV
Threat modelling fun session with OWASP Cornucopia - APV
Threat modelling fun session with OWASP Cornucopia - APV
Threat modelling fun session with OWASP Cornucopia - APV
ThreatScaper: Automated Threat Intelligence Gathering and Analysis for VirusTotal - DL
Time, Persistence, Patience - BHV
Tinfoil Hat Contest - CON
Tinfoil Hat Contest - CON
TOOOL Dozier Drill Lockpicking Challenge - CON
Top 10 Hacks To Watch Out For From An Election Official - VMV
Totally Tubular: An Impromptu Talk About Tubular Locks and Keys - LPV
Toxic BBQ - MISC
Trace Labs OSINT Search Party CTF - Announce CTF Grand Prize Winners - CON
Trace Labs OSINT Search Party CTF - CTF Platform Open for Submissions - CON
Trace Labs OSINT Search Party CTF - Sign-ups - CON
Track the Planet! Mapping Identities, Monitoring Presence, and Decoding Business Alliances in the Azure Ecosystem - DC
Tracking the Worlds Dumbest Cyber-Mercenaries - DC
Transportation Screening Equipment Cybersecurity Briefing - ASV
Tuning the human Bio-Field – proven classics forged with AI IOMT - BHV
Turning my virtual wallet into a skimming device: mPOS solutions - DC
UNConventional Cybercrime: How a Bad Anti-Hacking Treaty is Becoming a Law - DC
Understand Your Trust Assumptions! - VMV
University of Advancing Technology, Pub Crawl - SOC
Unlocking Doors from Half a Continent Away - DC
Unlocking hidden powers in Xtensa based Qualcomm Wifi chips - DC
Unlocking the Power of OWASP Amass: Introducing the Open Asset Model for Comprehensive Attack Surface Mapping - RCV

Unmanned Aerial Systems – Platform Security - ASV
Unmanned Aerial Systems – Platform Security - ASV
Unmanned Aerial Systems – Platform Security - ASV
Unveiling My Journey to My First CVE: A Tale of Discovery and Achievement - BICV
Unveiling the Dual Nature of ChatGPT and Copilot in Secure Development - APV
Unveiling the Secrets: Breaking into AI/ML Security Bug Bounty Hunting - AIV
US Cyber Policy 101 - PLV
US private elections: the easy way in for foreign adversaries. - VMV
USBvalve - Expose USB activity on the fly - DL
Using an SBC for ham radio digital modes that isn't a raspberry pi - HRV
Vacuum Robot Hacking - DL
Vacuum robot security and privacy - prevent your robot from sucking your data - DC
vAPI : Vulnerable Adversely Programmed Interface - APV
VDA Shenanigans: Attacking & Defending the Truck Part that Gets Left Behind - CHV
Veilid - DL
venator aurum - A Treasure Hunt - CON
venator aurum - A Treasure Hunt - CON
venator aurum - A Treasure Hunt - CON
Vendor Area Open - DC
Vendor Area Open - DC
Vendor Area Open - DC
VetCon - SOC
Video-based Cryptanalysis: Extracting Secret Keys from Power LEDs of Various Non-compromised Devices Using a Video Camera - DC
Virtual Hospital in Space - BHV
Virtual Reality/Augmented Reality: What's missing from the pie? When data privacy and security measures aren't "baked" in from the beginning - BHV
Visual Studio Code is why I have (Workspace) Trust issues - DC
VOTEC Corporation - VMV
VOTEC Corporation - VMV
Voting Village Opening Remarks - VMV
Voting Village Opening Remarks - VMV
Vulnerability instead of security: How we managed to hack a PSIM system - ICSV
Vulnerable by Design: Unguard, The Insecure Cloud-Native Twitter Clone - DL
WAF: Making a Problematic Security Tool Suck Less - APV
Wall of Sheep - PHV
Wall of Sheep - PHV
Wall of Sheep - PHV
War Driver Meetup - RFV
War Stories Off The Record AMA - DC
Wardriving 102: Moving Beyond the Wigle App - RFV
Warshopping - further dalliances in phreaking smart shopping cart wheels, RF sniffing and hardware reverse engineering - DC
Watching Androids Dream of Electric Sheep: Immersive Technology, Biometrics and the Law in collaboration with DEF CON Policy Village - XRV
We're From the Government and We're Here to Help Secure Open Source Software - PLV
Weaponizing Plain Text: ANSI Escape Sequences as a Forensic Nightmare - DC
Web Shells - What They Are And How To Hunt Them - APV
Welcome to DEF CON 31 - DC
What 10 years of drive stats data can tell us - DDV
What "Secure by Design" means for software breakers and builders - PLV
What are your thoughts on AI assisted voice cloning being used for scams? - PLV
What is a GRC Hacker anyway? - DCGVR
What Makes Hackers Extraordinary - It's A Gift! - VMV
What the Function: A Deep Dive into Azure Function App Security - CLV
What's up, Doc? Using documentation to build better OT security knowledge graphs - ICSV

Whose Slide Is It Anyway? - CON
Why don't we have Internet, Daddy? - BICV
Why OT Cybersecurity Engineers Drink So Much - BTV
WIFISHARK - RFV
WINE Pairing with Malware - PHV
Wingin' It - Pentesting a 737 - ASV
Wired for Safety: Prioritizing Safety in Deadly Systems - ICSV
WISP Chill Out Space with Refreshments - SOC
WISP Chill Out Space with Refreshments - SOC
WISP Community Meet Up at BTV Pool Party - SOC
WISP Peer-to-Peer Mentoring and Networking - SOC
World's Cheapest "QKD" ;) -QKD for fun and non- profit from home - QTV
Wrenches, Widgets, and Walkdowns: Unraveling the Tangle of Digital Assets in Industrial Control Systems - ICSV
XR implications on Mobile Security - XRV
XR Village Playground - XRV
XR Village Playground - XRV
XR Village Playground - XRV
Yarrrrgh Pirate Night - Music Set / Entertainment (Saturday, SYN Stage) - MUS
you sound confused, anyways - thanks for the jewels. - AIV
You're Not George Clooney, and This Isn't Ocean's Eleven - DC
Your Clocks Have Ears — Timing-Based Browser-Based Local Network Port Scanner - DC
Your Ship is Leaking... How Social Media Plays a Role in the Uncovering of Critical Maritime Systems - ICSV
Your Swag is My Swag: Pwning Fortune 500 Companies with Vistaprint - SEV

Village Talk List

AIV - Artificial Intelligence Village

Location: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

Home Page: <https://aivillage.org/>

Sched Page: <https://aivillage.org/defcon31/>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733090568339536>

PDT Times	Title	speaker
Friday		
10:00 - 10:10	AI Village Opening Remarks	AI Village Organizers
10:15 - 10:59	AI Village Keynote: The last attempted AI revoluti . . .	Joshua Saxe
10:00 - 17:59	AI Village Generative Red Team Challenge	
11:00 - 11:15	AI Village CTF Kickoff and Introduction	Will Pearce
11:30 - 11:55	LLMs: Loose Lips Multipliers	Kyle Easterly,Mitch Kitte . . .
12:00 - 12:25	Assessing the Vulnerabilities of the Open-Source A . . .	Adhishree Kathikar,Aishwa . . .
12:30 - 13:25	Not Just The Pickle: An Overview of Exploitable ML . . .	Marta Janus
13:30 - 13:55	How NOT to Train your Hack Bot: Dos and Don'ts o . . .	Ari Herbert-Voss,Shane Ca . . .
14:00 - 14:55	A Few Useful Lessons about AI Red Teaming	Ram Shankar Siva Kumar
16:00 - 16:55	Unveiling the Secrets: Breaking into AI/ML Securit . . .	Chloé Messdaghi,Daniel M . . .
17:00 - 17:55	Ghost in the Neurons - ML Webshells	Tom Bonner
Saturday		
10:30 - 11:25	AI Village Keynote 2: AI red teaming tradecraft: a . . .	Daniel Fabian,Mikel Rodri . . .
10:00 - 17:59	AI Village Generative Red Team Challenge	
11:30 - 12:25	Creative Misuse of AI Systems	Eryk Salvaggio
12:30 - 13:25	LLM Legal Risk Management, and Use Case Developmen . . .	Nick Maietta,Robert Hudoc . . .
13:30 - 14:25	The Sinister Synergy of Advanced AI: Automatically . . .	Ben Gelman,Younghoo Lee
15:00 - 15:25	you sound confused, anyways - thanks for the jewel . . .	Adrian "threlfall" Wood
15:30 - 15:55	Hackaprompt 2023: Trials and Tribulations	Kenneth Yeung
16:00 - 16:25	Ignore the Law: The Legal Risks of Prompt Injectio . . .	Ram Shankar Siva Kumar
16:30 - 17:25	ChatGPT: Your Red Teaming Ally	Gavin Klondike
Sunday		
10:00 - 10:25	Fuzzing and Symbolic Execution: Offensive Techniqu . . .	Rafael Turner
10:45 - 11:30	GRT Report Out	Sven Cattell
10:00 - 12:59	AI Village Generative Red Team Challenge	
11:15 - 11:45	AI Village Closing Remarks	AI Village Organizers

[Return to Index](#)

APV - AppSec Village

Location: Flamingo - Savoy - AppSec Village - [Map](#)

Home Page: <https://www.appsecvillage.com/>

Sched Page: <https://www.appsecvillage.com/events/dc-2023>

DC Discord Chan: <https://discord.com/channels/708208267699945503/790973922949726228>

PDT Times	Title	speaker
Friday		
10:00 - 10:59	AppSec Village Keynote: From Camels to Collaborati . . .	Chris Roberts
11:45 - 12:30	The attackers guide to exploiting secrets in the u . . .	Mackenzie Jackson
11:00 - 11:45	Generative Adversarial Network (GAN) based autonom . . .	Ankur Chowdhary
11:00 - 12:59	Hands-on GitHub Actions	Magno Logan
11:00 - 12:59	vAPI : Vulnerable Adversely Programmed Interface	Tushar Kulkarni
11:00 - 12:59	Spot the True Positives!	Backslash
11:00 - 12:59	The Ultimate AppSec Trivia Challenge	Probely
11:00 - 12:59	Defensive Coding and Hardened Javascript	Aaron Kumavis,Zbyszek Ten . . .
12:30 - 13:15	DevSecOps Worst Practices	Tanya Janca
13:15 - 13:59	The Dark Playground of CI/CD: Attack Delivery by G . . .	Kiyohito Yamamoto,Yusuke . . .
13:00 - 14:59	AMA - Tib3rius	Tib3rius
13:00 - 14:59	IDN-Squatting Detector	Gal Bitensky
13:00 - 14:59	Fix The Flag: A Secure Programming Competition	Pedram Hayati
13:00 - 14:59	The Ultimate AppSec Trivia Challenge	Probely
13:00 - 14:59	Web Shells - What They Are And How To Hunt Them	Joe Schottman
14:00 - 14:45	Living off the Land with Connectwise: How I Built . . .	Ken Pyle
15:00 - 16:59	Finding bugs and scaling your security program wit . . .	Lewis Ardern
15:00 - 16:59	Threat modelling fun session with OWASP Cornucopia	Spyros Gasteratos
15:00 - 16:59	How to Hide Behavior from Security Tools	Mike Larkin
15:00 - 16:59	FlowMate and CSTC for Advanced Pentesting	Florian Haag,Matthias Gö . . .
15:00 - 16:59	Hunt the Hacker - Detect compromises in your repos . . .	GitGuardian
15:00 - 16:59	Faking GitHub Contributions	Alik Koldobsky,Tal Folkma . . .
Saturday		
10:00 - 10:59	AppSec Village Keynote: Collaborative Security: Fo . . .	Maril Vernon
11:00 - 11:45	Getting More Bang for your Buck:Appsec on a Limite . . .	Vandana Verma Sehgal,Vira . . .
11:45 - 12:30	Discovering Shadow Vulnerabilities in Popular Open . . .	Gal Elbaz,Guy Kaplan
11:00 - 12:59	Hunt the Hacker - Detect compromises in your repos . . .	GitGuardian
11:00 - 12:59	Secure Code Review Challenge	Alon Lerner
11:00 - 12:59	Spot the True Positives!	Backslash
11:00 - 12:59	The Ultimate AppSec Trivia Challenge	Probely
11:00 - 12:59	JWT Parkour	Louis Nyffenegger

PDT Times	Title	speaker
12:30 - 13:30	Not All Alerts Are Born Equal: Insights from AppSe . . .	Joe Christian,Kunal Bhatt . . .
13:00 - 14:59	For Kids: Castle Defenders	Pentera
13:30 - 14:15	Dress Code - Analysis of the current status of the . . .	Felipe Molina
13:00 - 14:59	How to Hide Behavior from Security Tools	Deepfactor
13:00 - 14:59	Open Source API Security for devsecops	Ankita Gupta,Ankush Jain
13:00 - 14:59	The Ultimate AppSec Trivia Challenge	Probely
13:00 - 14:59	Secure from Scratch: Secure Code Workshop for DEF . . .	Or Sahar,Yariv Tal
14:15 - 14:59	MitmWs: A new way to pentest websocket application . . .	Jon F
15:00 - 15:45	SusParams: Hypercharge your web testing with DATA	Jason Haddix
15:45 - 16:30	Securing the Front Lines: Protecting Front-End App . . .	Dohyeon Kim,WooWon Kang
15:00 - 16:59	Hunt the Hacker - Detect compromises in your repos . . .	GitGuardian
15:00 - 16:59	How to Hide Behavior from Security Tools	Deepfactor
15:00 - 16:59	Fix The Flag - Battle Challenge	Pedram Hayati
15:00 - 16:59	Faking GitHub Reputation	Checkmarx
15:00 - 16:59	Per-mission Impossible: Exploring the Android Perm . . .	Miłosz Gaczkowski,Willia . . .
16:30 - 17:15	Breaking Barriers: A Deep Dive into Bypassing Next . . .	Muhammad Shahmeer
Sunday		
09:30 - 10:15	WAF: Making a Problematic Security Tool Suck Less	Emile Spir,Emmanuelle Lej . . .
10:15 - 10:59	Hacking GitHub Actions: Abusing GitHub and Azure f . . .	Magno Logan
10:00 - 11:59	Threat modelling fun session with OWASP Cornucopia	Spyros Gasteratos
10:00 - 11:59	Secure Code Review Challenge	Checkmarx
10:00 - 11:59	Hunt the Hacker - Detect compromises in your repos . . .	GitGuardian
10:00 - 11:59	Pasteur - A C++ library to eliminate injections	Yariv Tal
10:00 - 11:59	Enhancing Security for ReactJS Applications: Explo . . .	Jim Manico
11:00 - 11:45	Threat modeling-based application security pipelin . . .	Larkins Carvalho,Nielet D . . .
11:45 - 12:30	Android Applications and APIs hacking	Gabrielle Botbol
12:00 - 13:59	Threat modelling fun session with OWASP Cornucopia	Spyros Gasteratos
12:30 - 13:15	Unveiling the Dual Nature of ChatGPT and Copilot i . . .	Kalyani Pawar
12:00 - 13:59	AMA - Jim Manico	Jim Manico
12:00 - 13:59	How to Hide Behavior from Security Tools	Deepfactor
12:00 - 13:59	Faking GitHub Reputation	Checkmarx
12:00 - 13:59	Secure from Scratch: Secure Code Workshop	Or Sahar
13:15 - 13:59	Scoping for Success (Building a Great Bug Bounty p . . .	Jeffrey Guerra,Logan MacL . . .

[Return to Index](#)

ASV - Aerospace Village

Location: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Home Page: <https://aerospacevillage.org/>

Sched Page: <https://www.aerospacevillage.org/defcon-31-talks>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732393044363444264>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Unmanned Aerial Systems – Platform Security	
10:00 - 17:59	The Challenge - Lockheed Martin	
10:00 - 17:59	A-ISAC CTF	
10:00 - 17:59	Bricks in the Air	
10:00 - 17:59	ARINC 615a CTF	
10:00 - 17:59	PTP Flight Challenge	
10:00 - 17:59	Ask Me Anything About Cybersecurity in Aerospace	
10:00 - 17:59	Hack The Airport	
11:00 - 11:50	Hack-A-Sat 4 Briefing	Hack-A-Sat 4 Team
12:00 - 12:50	Secure Micropatching on the ISS	Henry Haswell
13:00 - 13:25	Guarding the Galaxy: Ransomware Resilience in Cube . . .	Peter Hansen
13:30 - 13:55	Moving Target Defense for Space Systems	Chris Jenkins
14:00 - 14:50	Orbiting the White House: Cybersecurity as a Space . . .	Lauryn Williams,Tanya Sim . . .
15:00 - 15:50	A Fireside Chat with the TSA Administrator	David Pecoske,Steve Luczy . . .
16:00 - 16:50	Transportation Screening Equipment Cybersecurity B . . .	Edam Colón
17:00 - 17:50	Pen Test Partners Power Hour	Alex Lomas,Ken Munro
Saturday		
10:00 - 17:59	Hack The Airport	
10:00 - 17:59	Unmanned Aerial Systems – Platform Security	
10:00 - 17:59	The Challenge - Lockheed Martin	
10:00 - 17:59	A-ISAC CTF	
10:00 - 17:59	Bricks in the Air	
10:00 - 17:59	ARINC 615a CTF	
10:00 - 17:59	PTP Flight Challenge	
10:00 - 17:59	Ask Me Anything About Cybersecurity in Aerospace	
11:00 - 11:50	Hack-A-Sat 4 Briefing	Hack-A-Sat 4 Team
12:00 - 12:25	CON trolling the weather	Paz Hameiri
12:30 - 13:20	Building Space Attack Chains using SPARTA	Brandon Bailey
13:30 - 13:55	Elon, Twitter and the PIA: How not to achieve priv . . .	Martin Strohmeier
14:00 - 14:25	Labs and Trust: How to build a successful aviation . . .	Martin Strohmeier
14:30 - 14:55	Stories from the Trenches: Operating a Aeronautics . . .	Christopher Ottesen

PDT Times	Title	speaker
15:00 - 15:25	Space Pirates on the Loose! - Space-Based Threats . . .	Henry Danielson,Sage Mead . . .
15:30 - 16:20	Wingin' It - Pentesting a 737	Alexander Dodd
16:30 - 16:55	A Fireside Chat with Chris Roberts and Pete Cooper	Chris Roberts,Pete Cooper
17:00 - 17:50	Aerospace Village - 5 Years On	Pete Cooper
Sunday		
10:00 - 13:59	Hack The Airport	
10:00 - 13:59	Unmanned Aerial Systems – Platform Security	
10:00 - 13:59	The Challenge - Lockheed Martin	
10:00 - 13:59	A-ISAC CTF	
10:00 - 13:59	Bricks in the Air	
10:00 - 13:59	ARINC 615a CTF	
10:30 - 11:20	The Looming Perils for End Users in Satellite Comm . . .	Vincent Lenders
10:00 - 13:59	PTP Flight Challenge	
10:00 - 13:59	Ask Me Anything About Cybersecurity in Aerospace	
12:00 - 12:50	Hack-A-Sat 4 Awards Ceremony	Hack-A-Sat 4 Team
13:00 - 13:50	Hacking Satellites: Houston, We Have a Problem	Jacob Oakley

[Return to Index](#)

BHV - Bio Hacking Village

Location: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

Home Page: <https://www.villageb.io/>

Sched Page: <https://www.villageb.io/defcon31-2023>

DC Discord Chan: <https://discord.com/channels/708208267699945503/735273390528528415>

PDT Times	Title	speaker
Friday		
10:00 - 10:40	Securing the Whole System: Corporal to Corporate	David Guffrey,Nina Alli,R . . .
10:40 - 11:40	Time, Persistence, Patience	Michael "v3ga_hax" Aguila . . .
13:20 - 14:10	Making a Sick Badge	Caleb Davis,Nathan Smith
14:10 - 14:40	Good Vibrations, Haptic Sensory Augmentation Impla . . .	Quinn D. Mooney
14:40 - 15:59	FoldIt	Firas D Khatib
16:00 - 16:30	Can I put my DNA on the blockchain, mom?	Anne Kim,Michele Orrù
16:30 - 17:20	My CPAP has a recall, lets open it instead!	José Fernández
17:20 - 17:59	CVE Insanity	Om Mahida
Saturday		
00:00 - 00:59	Model Based Systems Engineering for Security Engin . . .	John Volock
00:00 - 00:59	Virtual Hospital in Space	Aswin Reji
00:00 - 00:59	Hacking Reproductive Health	JJ Hastings
00:00 - 00:59	Beyond Ransomware: Protecting Lives and Data from . . .	Ohad Zaidenberg
00:00 - 00:59	The Megabiome is In Charge: Taking Control of Your . . .	Mariam Elgabry
10:00 - 10:30	Securing the Whole System: Corpal to Corporate	Lee Cyborg
10:30 - 11:10	Homo sapiens sapiens to Homo sapiens nova - the co . . .	Almost Human (BJ)
11:10 - 11:40	How to build a body in your garage	Brennan Marsh-Armstrong
11:40 - 12:40	Surgical Physicians and Cybersecurity	Colin Haines
12:40 - 13:50	Medical VR	David Nathans,Ernest Liu
13:50 - 14:50	Full Stack Disclosures	Edison Alvarez,Alex Mastr . . .
14:50 - 15:30	Lantern: Blue Energy	Del de Zela
15:30 - 16:10	Enhancing Cybersecurity Resilience in the Brazilia . . .	Arthur Paixão,Diego Mari . . .
16:10 - 17:10	FaFo: Laboratory Physical and ICS (Warning: not fo . . .	Nathan Case
17:10 - 17:59	Virtual Reality/Augmented Reality: What's missin . . .	LaTica Hammond,Lola Ajayi . . .
Sunday		
10:00 - 12:20	Table Top	Felicity Milman,Jorge Ace . . .
12:20 - 13:20	Tuning the human Bio-Field – proven classics for . . .	Wayne Burke and Team
13:20 - 13:59	Bare Metal Firmware Development and Reverse Engine . . .	Caleb Davis,Nathan Smith

[Return to Index](#)

BICV - Blacks in Cybersecurity

Location: Caesars Forum - Alliance - 301-304 - Blacks in Cyber Village - [Map](#)

Home Page: <https://www.blacksincyberconf.com/bic-village>

Sched Page: <https://www.blacksincyberconf.com/bic-village>

PDT Times	Title	speaker
Friday		
10:00 - 10:50	BIC Village Opening Keynote	John Threat
11:00 - 11:50	Cyber Hygiene: Security Awareness Training and Edu . . .	Dontae Tyler
13:00 - 13:50	Artificial Intelligence and Race: Security or Surv . . .	Fatou Sankare
15:00 - 15:50	Career Workshop: New Career Seekers In Cybersecuri . . .	Keith Chapman
16:00 - 16:50	Are you really eyeing my network? Network Reconnai . . .	RJ McCarley
Saturday		
11:00 - 11:50	General-purpose Languages: What Are Your Habits?	D.J. Davis
13:00 - 13:50	Why don't we have Internet, Daddy?	Jess Hoffman
15:00 - 15:50	Unveiling My Journey to My First CVE: A Tale of Di . . .	Gaspard Baye
16:00 - 16:50	BIC Village Closing Keynote	Kevin Roberts

[Return to Index](#)

BTV - Blue Team Village

Location: Flamingo - Sunset - Scenic - Blue Team Village - [Map](#)

Home Page: <https://blueteamvillage.org/>

Sched Page: <https://cfc.blueteamvillage.org/dc31/schedule/#>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732454317658734613>

PDT Times	Title	speaker
Friday		
10:30 - 11:30	Insider Threats (InT): Hindsight and Foresight	aviditas,plug
10:00 - 10:30	Blue Team Village Opening Ceremony	
10:30 - 11:30	CTH 101: Part I & II	CerealKiller
10:30 - 11:30	IR Analysis: Part I & II	juju43
11:30 - 12:30	Security Engineering for Adversarial Emulation and . . .	plug,sandw1ch
11:30 - 12:30	IR 101: Part I, II, III	ChocolateCoat,CountZ3r0,C . . .
11:30 - 12:30	CTH: (n)Map Exploration: A Great Time in Remote De . . .	SamunoskeX
13:30 - 14:30	OT: Why OT Cybersecurity Engineers Drink So Much	ThatDeadGuy
13:30 - 14:30	IR 101: Part IV, V	juju43
13:30 - 14:30	Forensic Analysis: Part I & II	Danny D. "B4nd1t0" Hender . . .
15:00 - 15:59	SOC Panel: Finding, Keeping, and Caring for the Be . . .	Alissa Torres,Carson Zimm . . .
16:00 - 17:59	Monroeville Live: An IR Tabletop for the Rest of U . . .	Dave Collins,Gwyddia,Litm . . .
Saturday		
10:30 - 11:30	IR/4n6: Obsidian DFIR - Gang aft agley	Omenscan
10:30 - 11:30	DE: Breaking the Rule	Oldmonk
10:30 - 11:30	CTH: Log4j - The Silent Menace Among Us	Cyb3rhawk
11:30 - 12:30	(n)Map Exploration: A Great Time in Remote Destina . . .	SamunoskeX
11:30 - 11:59	Forensics 101 Part I & II	Danny D. "B4nd1t0" Hender . . .
11:30 - 12:30	DE: Building a Detection Alert From a Threat Hunt	kobaltfox
13:30 - 14:30	So you want to become a Detection Engineer	Ben Bornholm,CerealKiller . . .
13:30 - 13:59	CTH 101: Part III, IV, V	Cyb3rhawk
13:30 - 14:30	Why OT Cybersecurity Engineers Drink So Much	ThatDeadGuy
15:45 - 16:45	Arson Herders: An IR Guide to Fighting and Lightin . . .	Litmoose,Matt "dis0wn" Wa . . .
17:00 - 17:59	It's not that your threat intelligence IOCs are . . .	Charlie,Lauren Proehl,Mic . . .
Sunday		
10:00 - 10:45	Blue Team Village Game Session	aviditas
11:00 - 11:30	Project Obsidian Panel	
12:45 - 13:45	Blue Team Village Closing Ceremony	

[Return to Index](#)

CHV - Car Hacking Village

Location: Caesars Forum - Summit - 234 - Car Hacking Village - [Map](#)

Home Page: <https://www.carhackingvillage.com/>

Sched Page: <https://www.carhackingvillage.com/defcon-31-talks>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732722838942777474>

PDT Times	Title	speaker
Friday		
16:00 - 16:40	Redeploying the Same Vulnerabilities: Exploiting W...	Richard Baker, Sebastian K...
17:00 - 17:40	How an automotive security researcher had his car ...	Ian Tabor, Ken Tindell
Saturday		
10:00 - 10:25	VDA Shenanigans: Attacking & Defending the Truck P...	Alex Reuter, Wyatt Ford
11:00 - 11:40	Automotive USB Fuzzing: How to fuzzing USB in veh ...	Donghyeon Jeong, Euntae Ja...
12:00 - 12:59	Abusing CAN Bus Protocol Specification for Denial ...	Martin Petran

[Return to Index](#)

CLV - Cloud Village

Location: Flamingo - Mesquite - Cloud Village - [Map](#)

Home Page: <https://cloud-village.org/>

Sched Page: <https://cloud-village.org/#talks>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733373172285520>

PDT Times	Title	speaker
Friday		
10:10 - 10:50	Cloud Village - Keynote	Ben "NahamSec" Sadeghipou . . .
10:50 - 11:30	Evading Logging in the Cloud: Bypassing AWS CloudT . . .	Nick Frichette
11:30 - 12:10	The Dark Playground of CI/CD: Attack Delivery by G . . .	Kiyohito Yamamoto, Yusuke . . .
12:10 - 12:30	From Service Catalog Admin to Account takeover: Pr . . .	Sarachai Boonyakiat
12:30 - 12:59	Attacks as a Service with The DeRF	Kat Traxler
13:25 - 14:05	Azure DevOps Security	Viktor Gazdag
13:00 - 13:25	Identifying and securing Firebase vulnerabilities . . .	Rojan Rijal
14:35 - 16:30	Infrastructure as Remote Code Execution	Michael McCabe
14:05 - 14:35	MetaHub Demo: Automating Ownership, Context, and I . . .	
Saturday		
10:30 - 11:10	Between a Log and a Hard Place: (mis)Adventures in . . .	Dmitriy Beryoza
10:00 - 10:30	Introducing IAM-APE	Tohar Braun
11:10 - 11:50	SSO Sloppy, SSO Suspect, SSO Vulnerable	Jenko Hwong
11:50 - 12:20	Google Workspace Red Team Automation with SWAT	Justin Ibarra, Terrance De . . .
12:20 - 12:59	The Rocky Balboa Guide to Security Research: Getti . . .	Liv Matan
13:30 - 14:10	What the Function: A Deep Dive into Azure Function . . .	Karl Fosaaen, Thomas Ellin . . .
13:00 - 13:30	CloudRecon - finding ephemeral assets in the cloud	Gunnar Andrews, Jason Hadd . . .
14:10 - 14:50	Bridging the Gap: Cloud Threat Intelligence for De . . .	Alex Delamotte
14:50 - 15:35	The Human Threat Factor - Cloud Security Misconfig . . .	Kat Fitzgerald
Sunday		
10:00 - 10:40	Call Me Phishmael: Hunting Sensitive Docker Images . . .	Ian Dillon
10:40 - 11:20	Tag, You're Exposed: Exploring Azure Service Tags . . .	Aled Mehta, Christian Phil . . .
11:20 - 11:59	Security Logging in the cloud, trade-offs to consi . . .	Marco Mancini
12:00 - 12:40	Tales from a detection engineering in AWSland	Rodrigo Montoro
12:40 - 13:10	CNAPPGoat - A multicloud vulnerable-by-design infr . . .	Igal Gofman, Noam Dahan

CON - Contests

PDT Times	Title	speaker
Thursday		
08:00 - 11:59	Hac-Man	
Friday		
09:00 - 17:59	HardWired	
09:00 - 10:59	Social Engineering Community (SEC) Vishing Competi . . .	
09:00 - 17:59	Social Engineering Community (SEC) Youth Challenge	
10:30 - 17:59	Capture The Packet Preliminaries	
10:00 - 17:59	IoT Village CTF	
10:00 - 17:59	Hardware Hacking Village CTF	
10:00 - 17:59	Hack-A-Sat 4 (HAS4)	
10:00 - 17:59	5n4ck3y	
10:00 - 17:59	TeleChallenge	
10:00 - 17:59	CMD+CTRL at DEF CON 31 - Booth Open	
10:00 - 17:59	HackFortress	
10:00 - 13:59	The Beverage Cooling Contraption Contest	
10:00 - 16:59	Adversary Wars CTF	
10:00 - 17:59	The Dark Tangent Look-Alike Contest	
10:00 - 17:59	Battle of The Bots	
10:00 - 17:59	Ham Radio Fox Hunting Contest	
10:00 - 17:59	The Gold Bug Challenge	
10:00 - 19:59	The Lonely Hard Drive	
10:00 - 17:59	Tinfoil Hat Contest	
10:00 - 17:59	Car Hacking Village CTF	
10:00 - 17:59	IntelOps - Operation Spacewatch	
10:00 - 17:59	venator aurum - A Treasure Hunt	
10:00 - 17:59	It's In That Place Where I Put That Thing That Tim . . .	
10:00 - 17:59	CrackMeIfYouCan	
10:00 - 17:59	Maps of the digital lands	
10:00 - 16:30	Darknet-NG	
10:00 - 17:59	DC's Next Top Threat Model (DCNTTM)	
10:00 - 13:59	Octopus Game	
10:00 - 17:59	AutoDriving CTF	
10:00 - 19:59	pTFS Presents: Mayhem Industries – Starphish	
10:00 - 17:59	Trace Labs OSINT Search Party CTF - Sign-ups	
10:00 - 17:59	DEF CON Scavenger Hunt	

PDT Times	Title	speaker
10:00 - 17:59	DEFCON MUD DUMB TERMINAL EDITION	
10:00 - 17:59	Dungeons@Defcon	
10:00 - 17:59	Red Team CTF	
10:00 - 17:59	? Cube	
10:00 - 17:59	Radio Frequency Capture the Flag	
10:30 - 17:59	Blue Team Village CTF	
10:00 - 17:59	Embedded CTF	
10:00 - 17:59	Cloud Village CTF	
10:00 - 11:59	CMD+CTRL at DEF CON 31 - Competition	
10:00 - 19:59	DC Kubernetes Capture the Flag (CTF)	
10:00 - 12:59	Radio Frequency Capture the Flag	
11:30 - 13:30	Social Engineering Community (SEC) Vishing Competi . . .	
12:00 - 16:59	Blacks in Cyber Village CTF	
12:00 - 16:59	Red Alert ICS CTF	
14:00 - 16:59	Social Engineering Community (SEC) Vishing Competi . . .	
17:00 - 17:59	Hack3r Runw@y	
18:00 - 20:30	Pub Quiz at DEF CON	
20:00 - 21:59	Hacker Jeopardy	
22:00 - 23:59	Whose Slide Is It Anyway?	

Saturday

09:00 - 17:59	HardWired	
09:00 - 17:59	Social Engineering Community (SEC) Youth Challenge	
10:30 - 11:59	Capture The Packet Preliminaries	
10:00 - 17:59	IoT Village CTF	
10:00 - 17:59	Hardware Hacking Village CTF	
10:00 - 17:59	5n4ck3y	
10:00 - 17:59	TeleChallenge	
10:00 - 17:59	Hack-A-Sat 4 (HAS4)	
10:00 - 16:59	Adversary Wars CTF	
10:00 - 17:59	The Dark Tangent Look-Alike Contest	
10:00 - 17:59	CMD+CTRL at DEF CON 31 - Booth Open	
10:00 - 17:59	HackFortress	
10:00 - 17:59	Battle of The Bots	
10:00 - 17:59	Ham Radio Fox Hunting Contest	
10:00 - 17:59	The Gold Bug Challenge	
10:00 - 19:59	The Lonely Hard Drive	
10:00 - 17:59	Car Hacking Village CTF	
10:00 - 17:59	Tinfoil Hat Contest	
10:00 - 17:59	venator aurum - A Treasure Hunt	
10:30 - 14:30	Trace Labs OSINT Search Party CTF - CTF Platform O . . .	
10:00 - 17:59	CrackMeIfYouCan	
10:00 - 17:59	It's In That Place Where I Put That Thing That Tim . . .	
10:00 - 16:30	Darknet-NG	

PDT Times	Title	speaker
10:00 - 17:59	Maps of the digital lands	
10:00 - 17:59	DC's Next Top Threat Model (DCNTTM)	
10:00 - 13:59	Octopus Game	
10:00 - 17:59	DEF CON Scavenger Hunt	
10:00 - 17:59	DEFCON MUD DUMB TERMINAL EDITION	
10:00 - 16:59	Red Alert ICS CTF	
10:00 - 17:59	Dungeons@Defcon	
10:00 - 17:59	Red Team CTF	
10:00 - 17:59	? Cube	
10:00 - 17:59	Radio Frequency Capture the Flag	
10:30 - 17:59	Blue Team Village CTF	
10:00 - 17:59	Embedded CTF	
10:00 - 17:59	Cloud Village CTF	
10:00 - 16:59	DC Kubernetes Capture the Flag (CTF)	
11:00 - 16:59	Free Amateur Radio License Exams	
12:00 - 17:59	Capture The Packet Main Rounds	
12:00 - 14:59	TOOOL Dozier Drill Lockpicking Challenge	
14:00 - 15:59	DEF CON 31 Beard and Mustache Contest	
15:00 - 17:59	DEF CON Chess Tournament	
15:30 - 16:29	Trace Labs OSINT Search Party CTF - Announce CTF G . . .	
17:00 - 17:59	Hack3r Runw@y	
20:00 - 21:59	Hacker Jeopardy	
Sunday		
09:00 - 12:59	HardWired	
10:00 - 12:59	Capture The Packet FINALS	
10:00 - 13:59	IoT Village CTF	
10:00 - 11:59	Hardware Hacking Village CTF	
10:00 - 11:59	? Cube	
10:00 - 11:59	5n4ck3y	
10:00 - 11:59	TeleChallenge	
10:00 - 11:59	Adversary Wars CTF	
10:00 - 11:59	Battle of The Bots	
10:00 - 11:59	CMD+CTRL at DEF CON 31 - Booth Open	
10:00 - 11:59	The Dark Tangent Look-Alike Contest	
10:00 - 11:59	The Gold Bug Challenge	
10:00 - 11:59	Ham Radio Fox Hunting Contest	
10:00 - 12:59	The Lonely Hard Drive	
10:00 - 11:59	Car Hacking Village CTF	
10:00 - 11:59	venator aurum - A Treasure Hunt	
10:00 - 11:59	CrackMeIfYouCan	
10:00 - 11:59	Maps of the digital lands	
10:00 - 11:59	Darknet-NG	
10:00 - 11:59	Octopus Game	

PDT Times	Title	speaker
10:00 - 11:59	DEF CON Scavenger Hunt	
10:00 - 11:59	DEFCON MUD DUMB TERMINAL EDITION	
10:00 - 11:59	Red Alert ICS CTF	
10:00 - 11:59	Red Team CTF	
10:00 - 12:59	Radio Frequency Capture the Flag	
10:00 - 13:59	Embedded CTF	
10:00 - 11:59	Cloud Village CTF	
11:00 - 13:59	Free Amateur Radio License Exams	
12:00 - 13:30	Hack-A-Sat 4 (HAS4) -- Closing Ceremony	

[Return to Index](#)

CPV - Crypto Privacy Village

Location: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

Home Page: <https://cryptovillage.org/>

Sched Page: <https://cryptovillage.org/>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732734002011832320>

PDT Times	Title	speaker
Friday		
10:00 - 10:05	CPV Welcome - Day 1	CPV Staff
10:30 - 10:45	Intro to Ciphers	CPV Staff
11:00 - 11:30	Certs Fucking Suck, So We Made a Cert: DISCO for B . . .	Blunt,Daly
12:30 - 12:59	Practical advice for navigating edtech privacy	Michelle Levesley
12:00 - 12:30	Art vs AI: How Artists Hack Computer Vision System . . .	Kate
13:00 - 13:45	Attacking Decentralized Identity	Brent Zundel,Gabe Cohen
14:00 - 14:30	Climate Change and its Implications for Security a . . .	Chloé Messdaghi
15:00 - 15:45	Privacy of Web PKI Revocation	Matthew McPherrin
16:00 - 16:45	Cicada 3301: An Exploration of the Cryptographic E . . .	Artorias,Puck,Taiwo,TheC . . .
16:30 - 16:45	Intro to Ciphers	CPV Staff
17:00 - 17:45	Spoofing certificates with MD5 collisions - party . . .	Tomer,Yoni
Saturday		
10:00 - 10:05	CPV Welcome - Day 2	CPV Staff
10:30 - 10:59	Blindly hunting for Mercenaries	Asheer Malhotra,Vitor Ven . . .
10:30 - 10:45	Intro to Ciphers	CPV Staff
11:00 - 11:59	Ten Years of CPV - Program Committees	CPV Program Committees,CP . . .
12:00 - 12:59	Ten Years of CPV - The Gold Bug Challenge	CPV Staff,Gold Bug Challe . . .
12:00 - 12:30	About Face! Beginner Intro to Facial Recognition	Kate
13:00 - 13:30	Is 2023 the Year of Privacy: How History and State . . .	Anthony Hendricks
13:30 - 13:59	Domain Fronting Through Microsoft Azure and CloudF . . .	Charles Miller,Michael Br . . .
14:00 - 14:45	Exploring the Impact of PQC on Cryptographic Key M . . .	Deirdre Connolly,James Ho . . .
15:00 - 15:45	Cryptosploit Workshop	Matt Cheung
16:00 - 17:59	CPV Ten Year Anniversary Gathering	CPV Staff
Sunday		
10:00 - 10:05	CPV Welcome - Day 3	CPV Staff
10:30 - 10:45	Intro to Ciphers	CPV Staff
13:00 - 13:45	How mathematical implementation issues lead to cry . . .	Bing Shi

[Return to Index](#)

DC - DEF CON Talks

Home Page: <https://defcon.org/html/defcon-31/dc-31-index.html>

Sched Page: <https://defcon.org/html/defcon-31/dc-31-schedule.html>

PDT Times	Title	speaker
Thursday		
07:00 - 18:59	Human Registration Open	
07:00 - 17:59	Merch (formerly swag) Area Open -- README	
09:00 - 01:59	Shell On Demand Appliance Machine (S.O.D.A. Machin . . .	
10:00 - 10:45	Boston Infinite Money Glitch: Hacking Transit Card . . .	Matthew Harris,Noah Gibso . . .
11:30 - 12:15	Cracking Cicada 3301: The Future of Collaborative . . .	Artorias,Puck,Taiiwo,TheC . . .
11:00 - 11:20	UNConventional Cybercrime: How a Bad Anti-Hacking . . .	Bill Budington,Katitza Ro . . .
12:30 - 13:15	New Isn't Always Novel: Grep'ing Your Way to \$. . .	James Horseman,Zach Hanle . . .
13:30 - 14:15	Damned if you do - The risks of pointing out the e . . .	RenderMan,Thomas Dang
14:30 - 15:15	Designing RFID Implants - How flipping the bird op . . .	Miana Ella Windall
15:30 - 16:15	Nuthin But A G Thang: Evolution of Cellular Networ . . .	Tracy Mosley
16:30 - 16:50	Small Leaks, Billions Of Dollars: Practical Crypto . . .	Nikolaos Makriyannis,Oren . . .
17:30 - 18:45	DEF CON 101 - Welcome to DEF CON Panel	Jeff "The Dark Tangent" M . . .
Friday		
08:00 - 19:59	Human Registration Open	
08:00 - 17:59	Merch (formerly swag) Area Open -- README	
09:00 - 09:45	Growing the Community of AI Hackers with the Gener . . .	Austin Carson,Rumman Chow . . .
09:00 - 09:45	The Internals of Veilid, a New Decentralized Appli . . .	Christien "DiIDog" Rioux, . . .
09:30 - 10:15	Secretary of the Department of Homeland Security A . . .	Alejandro Mayorkas
09:00 - 09:20	Welcome to DEF CON 31	Jeff "The Dark Tangent" M . . .
09:00 - 01:59	Shell On Demand Appliance Machine (S.O.D.A. Machin . . .	
09:00 - 09:45	The Hackers, The Lawyers, And The Defense Fund	Charley Snyder,Hannah Zha . . .
10:30 - 11:15	Route to bugs: Analyzing the security of BGP messa . . .	Daniel dos Santos,Simon G . . .
10:00 - 10:20	Look Ma I'm the CEO! Real-Time Video and Audio Dee . . .	Gal Zror
10:00 - 17:59	Vendor Area Open	
10:00 - 10:45	Contain Yourself: Staying Undetected Using the Win . . .	Daniel Avinoam
10:30 - 10:50	Making The DEF CON 31 Badge	Mar Williams
10:00 - 17:59	Exhibitor Area Open	
10:00 - 10:45	The RingHopper Journey or How We Almost Zero-day. . .	Benny Zeltser,Jonathan Lu . . .
10:00 - 17:59	Contest Area Open	
10:00 - 10:45	A Different Uber Post Mortem	Joe Sullivan
11:30 - 12:15	Civil Cyber Defense: Use Your Resources to Defend . . .	Austin Shamlin,Tiffany Ra . . .
11:30 - 12:15	I Watched You Roll the Die: Unparalleled RDP Monit . . .	Andréanne Bergeron,Olivi . . .

PDT Times	Title	speaker
11:00 - 11:20	mTLS: when certificate authentication done wrong	Michael Stepankin
11:00 - 11:45	SpamChannel: Spoofing Emails From 2 Million+ Domai . . .	Marcello "byt3bl33d3r" Sa . . .
11:00 - 11:45	Defending KA-SAT: The detailed story of the respon . . .	Mark Colaluca,Nick Saunde . . .
11:00 - 11:45	Warshopping - further dalliances in phreaking smar . . .	Joseph Gabay
12:30 - 13:15	Defender-Pretender: When Windows Defender Updates . . .	Omer Attias,Tomer Bar
12:30 - 13:15	A Pain in the NAS: Exploiting Cloud Connectivity t . . .	Noam Moshe,Sharon Brizino . . .
12:00 - 12:45	Still Vulnerable Out of the Box: Revisiting the Se . . .	Angelos Stavrou,Mohamed E . . .
12:00 - 12:20	GhostToken: Exploiting Google Cloud Platform App I . . .	Tal Skverer
12:30 - 13:15	Backdoor in the Core - Altering the Intel x86 Inst . . .	Alexander Dalsgaard Krog, . . .
12:00 - 13:59	Lonely Hackers Club - Resume Reviews & Career Advi . . .	
12:00 - 12:45	You're Not George Clooney, and This Isn't Ocean's . . .	Andrew "Spike" Brandt
13:30 - 14:15	Private Until Presumed Guilty	Allison Young,Diane Akerm . . .
13:30 - 14:15	Private Keys in Public Places	Tom Pohl
13:00 - 13:45	Over the Air, Under the Radar: Attacking and Secur . . .	Eugene Rodionov,Farzan Ka . . .
13:30 - 14:15	Fantastic Ethertypes and Where to Find Them	Ricky "HeadlessZeke " Law . . .
13:00 - 13:45	Living Next Door to Russia	Mikko Hypponen
14:30 - 15:15	Second Breakfast: Implicit and Mutation-Based Ser . . .	Jonathan Birch
14:00 - 14:20	There are no mushroom clouds in cyberwar	Mieke Eoyang
14:30 - 14:50	DARPA Announces an AI Cyber Initiative, Live at DC . . .	Dave Weston,Heather Adkin . . .
14:30 - 15:15	Getting a Migraine - uncovering a unique SIP bypas . . .	Anurag Bohra,Jonathan Bar . . .
14:00 - 16:59	Lonely Hackers Club - Badgelifie & Sticker Swap	
14:00 - 14:20	Tracking the Worlds Dumbest Cyber-Mercenaries	Cooper Quintin
14:30 - 14:50	"You can't cheat time" - Finding foes and yourself . . .	Lorenzo "lopoc" Cococ . . .
15:30 - 16:15	Game-Changing Advances in Windows Shellcode Analys . . .	Bramwell Brizendine,Jake . . .
15:30 - 16:15	A Comprehensive Review on the Less-Traveled Road: . . .	NiNi Chen
15:00 - 15:45	Shall we play a game? Just because a Large Languag . . .	Craig Martell
15:30 - 16:15	Turning my virtual wallet into a skimming device: . . .	Dan Borgogno,Ileana Barri . . .
15:00 - 15:45	CON trolling the weather	Paz Hameiri
16:30 - 17:15	Malware design - abusing legacy Microsoft transpor . . .	R.J. "BeetleChunks" McDow . . .
16:30 - 17:15	Nothing but Net: Leveraging macOS's Networking Fra . . .	Patrick Wardle
16:00 - 16:45	Visual Studio Code is why I have (Workspace) Trust . . .	Paul Gerste,Thomas Chauch . . .
16:30 - 17:15	certmitm: automatic exploitation of TLS certificat . . .	Aapo Oksman
16:00 - 16:45	A Series of Unfortunate Events	Ben "NahamSec" Sadeghipou . . .
17:30 - 18:15	Fireside Chat with the National Cyber Director Kem . . .	Kemba Walden
17:00 - 17:20	HL7Magic: Medical Data Hacking Made Easy	Katie Inns
17:30 - 17:50	Track the Planet! Mapping Identities, Monitoring P . . .	nyxgeek
17:00 - 17:59	Lonely Hackers Club - Name That Noob	
17:00 - 17:45	Legend of Zelda: Use After Free (TASBot glitches t . . .	Allan "dwangoAC" Cecil
20:00 - 21:59	Ask the EFF	Cooper Quintin,Corynne Mc . . .
Saturday		
09:00 - 09:45	Hack the Future: Why Congress and the White House . . .	Arati Prabhakar,Austin Ca . . .
09:30 - 18:59	Human Registration Open	
09:30 - 10:15	Badge of Shame: Breaking into Secure Facilities wi . . .	Dan "AltF4" Petro,David V . . .

PDT Times	Title	speaker
09:00 - 09:20	Assessing the Security of Certificates at Scale	Andrew Chi,Brandon Enrigh . . .
09:00 - 09:45	Smashing the state machine: the true potential of . . .	James "albinowax" Kettle
09:00 - 01:59	Shell On Demand Appliance Machine (S.O.D.A. Machin . . .	
09:30 - 10:15	J4 Gate, The Hustler Poker Cheating Scandal invest . . .	Scott "Duckie" Melnick
09:00 - 09:20	ELECTRONizing macOS privacy - a new weapon in your . . .	Wojciech Reguła
09:00 - 11:59	Merch (formerly swag) Area Open -- README	
10:00 - 10:45	Defeating VPN Always-On	Maxime Clementz
10:00 - 17:59	Vendor Area Open	
10:30 - 11:15	Calling it a 0-Day - Hacking at PBX/UC Systems	good_pseudonym
10:00 - 10:45	Demystifying (& Bypassing) macOS's Background Task . . .	Patrick Wardle
10:00 - 17:59	Exhibitor Area Open	
10:30 - 11:15	Unlocking Doors from Half a Continent Away	Sam Haskins,Trevor "t1v0" . . .
10:00 - 17:59	Contest Area Open	
10:00 - 11:45	DO NO H4RM: A Healthcare Security Conversation	Christian "quaddi" Dameff . . .
11:00 - 11:45	Spread spectrum techniques in disposable drones fo . . .	David Melendez,Gabriela " . . .
11:30 - 12:15	Physical Attacks Against Smartphones	Christopher Wade
11:00 - 11:45	Weaponizing Plain Text: ANSI Escape Sequences as a . . .	STÖK
11:30 - 12:15	Apple's Predicament: NSPredicate Exploitation on m . . .	Austin Emmitt
11:30 - 12:15	Mass Owning of Seedboxes - A Live Hacking Exhibiti . . .	Anon
12:00 - 12:45	From Feature to Weapon: Breaking Microsoft Teams a . . .	Nestori Syynimaa
12:30 - 13:15	Video-based Cryptanalysis: Extracting Secret Keys . . .	Ben Nassi,Ofek Vayner
12:00 - 12:45	Internet censorship: what governments around the g . . .	Christopher Painter,Jeff . . .
12:30 - 13:15	An Audacious Plan to Halt the Internet's Enshittif . . .	Cory Doctorow
12:00 - 13:59	Lonely Hackers Club - Resume Reviews & Career Advi . . .	
12:30 - 13:30	Metawar	Winn
13:00 - 13:45	Azure B2C 0-Day: An Exploit Chain from Public Keys . . .	John Novak
13:30 - 14:15	Meduza: How an exiled pirate media outlet breaks t . . .	Alex
13:00 - 13:45	Looking into the future, what can we learn about h . . .	Nicolas Minvielle,Xavier . . .
13:30 - 14:15	The GitHub Actions Worm: Compromising GitHub repos . . .	Asi Greenholts
14:00 - 14:45	Power Corrupts; Corrupt It Back! Hacking Power Man . . .	Jesse Chick,Sam Quinn
14:30 - 15:15	Exploiting OPC-UA in Every Possible Way: Practical . . .	Noam Moshe,Sharon Brizino . . .
14:00 - 14:45	A SSLippery Slope: Unraveling the Hidden Dangers o . . .	Bill Demirkapi
14:30 - 15:15	Contactless Overflow: Code execution in payment te . . .	Josep Pi Rodriguez
14:00 - 16:59	Lonely Hackers Club - Badgelif e & Sticker Swap	
14:00 - 17:59	Off the record war story talks - Signs Ups On Site	
15:00 - 15:45	Revolutionizing ELF binary patching with Shiva: A . . .	Ryan "ElfMaster" O'Neill
15:30 - 16:15	Breaking BMC: The Forgotten Key to the Kingdom	Adam Zabrocki,Alex Teresh . . .
15:00 - 15:45	Spooky authentication at a distance	Tamas "SkelSec" Jos
15:30 - 16:15	ndays are also 0days: Can hackers launch 0day RCE . . .	Bohan Liu,GuanCheng Li,Zh . . .
16:30 - 17:15	All information looks like noise until you break t . . .	David Pekoske,Jen Easterl . . .
16:00 - 16:20	A Broken Marriage: Abusing Mixed Vendor Kerberos S . . .	Ceri Coburn
16:30 - 16:50	Your Clocks Have Ears — Timing-Based Browser-Bas . . .	Dongsung "Donny" Kim
16:00 - 16:45	Runtime Riddles: Abusing Manipulation Points in th . . .	Laurie Kirk

PDT Times	Title	speaker
16:30 - 17:15	Abortion Access in the Age of Surveillance	Corynne McSherry,Daly Bar . . .
17:30 - 17:50	Lions and Tigers and Fancy Bears, Oh My!: A Cautionary Tale	Jen Easterly,Scott Shapir . . .
17:00 - 17:20	Silent Spring: Prototype Pollution Leads to Remote Control	Mikhail Shcherbakov,Musar . . .
17:00 - 17:20	Polynonce: An ECDSA Attack and Polynomial Dance	Marco Macchetti,Nils Amie . . .
17:00 - 17:59	Lonely Hackers Club - Name That Noob	
Sunday		
09:00 - 15:30	Shell On Demand Appliance Machine (S.O.D.A. Machine)	
10:00 - 10:45	Vacuum robot security and privacy - prevent your robot from vacuuming your data	Dennis Giese
10:00 - 15:59	Vendor Area Open	
10:00 - 13:59	Human Registration Open	
10:00 - 10:45	StackMoonwalk: A Novel approach to stack spoofing	Alessandro "klezVirus" Maffei . . .
10:00 - 10:45	Cellular carriers hate this trick: Using SIM tunnelling	Adrian "atrox" Dabrowski, . . .
10:00 - 13:59	Exhibitor Area Open	
10:00 - 10:20	Snoop unto them, as they snoop unto us	Michaud "5@V@g3" Savage, . . .
10:00 - 13:59	Contest Area Open	
10:00 - 11:59	War Stories Off The Record AMA	
11:00 - 11:45	Burrowing Through The Network: Contextualizing The Art of the Steal	Joe Slowik
11:00 - 11:45	Advanced ROP Framework: Pushing ROP to Its Limits	Bramwell Brizendine,Shiva . . .
11:00 - 11:45	The Art of Compromising C2 Servers: A Web Application Perspective	Vangelis Stykas
11:00 - 11:45	Unlocking hidden powers in Xtensa based Qualcomm W850	Daniel Wegemer
12:00 - 12:45	LLMs at the Forefront: Pioneering the Future of Full Stack Development	X
12:00 - 12:45	#NoFilter: Abusing Windows Filtering Platform for Local Network Access	Ron Ben-Yizhak
12:00 - 12:45	Terminally Owned - 60 years of escaping	David Leadbeater
12:00 - 12:45	Retro Exploitation: Using Vintage Computing Platforms for Modern Security Research	Wesley McGrew
13:00 - 13:45	Exploring Linux Memory Manipulation for Stealth and Persistence	Carlos Polop,Yago Gutierr . . .
13:00 - 13:45	The Price of Convenience: How Security Vulnerabilities are Exploited	Omer Attias
14:00 - 15:15	Panel: Hacker Court - Interactive Scenario	winn0na
14:00 - 15:15	Contest Closing Ceremonies & Awards	
14:00 - 15:15	TETRA tour de force: Jailbreaking digital radios and more	Carlo Meijer,Jos Wetzels, . . .
15:30 - 17:30	DEF CON Closing Ceremonies & Awards	Jeff "The Dark Tangent" Maffei . . .

[Return to Index](#)

DCGVR - DEF CON Groups VR

Home Page: <https://www.dcgvr.org/>

Sched Page: <https://www.dcgvr.org/>

PDT Times	Title	speaker
Saturday		
10:00 - 10:30	DEF CON Groups Keynote	Jayson E. Street
11:35 - 12:20	Taking Down Applications with Logic: A Compreheni . . .	Abhijeet Singh
12:35 - 13:20	The Curse of Ncurses	Jonathan Bar Or
13:35 - 14:05	Bootsquad: Stomping out squatters	Joe Mast
14:35 - 15:20	Enhancing vulnerability research through the use o . . .	datalocaltmp
15:35 - 16:05	Gender Inclusive Features Across the Health Inform . . .	Squiddy
16:35 - 17:35	Hey CryptoBro!: How Are Criminals Laundering, Mone . . .	Sam Colaizzi
18:05 - 18:35	Ghost on the wire- check the air	hoodiePony
19:05 - 20:05	What is a GRC Hacker anyway?	Allen Baranov
20:05 - 20:10	DCGVR Closing	
20:10 - 21:10	After Hours Social / Hang out with DEF CON Group m . . .	

[Return to Index](#)

DDV - Data Duplication Village

Location: Caesars Forum - Summit - 231 - Data Dupe Vlg - [Map](#)

Home Page: <https://dcddv.org/>

Sched Page: <https://dcddv.org/dc31-schedule>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732732641694056478>

PDT Times	Title	speaker
Friday		
13:00 - 14:59	What 10 years of drive stats data can tell us	Andy Klein

[Return to Index](#)

DL - DEF CON DemoLabs

Home Page: <https://forum.defcon.org/node/244767>

PDT Times	Title	speaker
Friday		
10:00 - 11:55	Vulnerable by Design: Unguard, The Insecure Cloud- . . .	Christoph Wedenig,Simon A . . .
10:00 - 11:55	SucoshScanny	Mustafa Bilgici,Tibet Ö . . .
10:00 - 11:55	The Metasploit Framework	Spencer McIntyre
10:00 - 11:55	T3SF (Technical TableTop Exercises Simulation Fram . . .	Federico Pacheco,Joaquin . . .
10:00 - 11:55	Katalina	Gabi Cirlig
10:00 - 11:55	Strix Interceptor	Lexie Thach
12:00 - 13:55	CNAPPGoat	Igal Gofman,Noam Dahan
12:00 - 13:55	Dracon	Spyros Gasteratos
12:00 - 13:55	Build Inspector - A modern Javert on the trail of . . .	Jeremy Banker
12:00 - 13:55	Ek47 – Payload Encryption with Environmental Key . . .	Kevin “Kent” Clark,Sk . . .
12:00 - 13:55	FlowMate	Florian Haag,Nicolas Schi . . .
12:00 - 13:55	Shufflecake, AKA Truecrypt on Steroids for Linux	Elia Anzuoni,Tommaso "tom . . .
14:00 - 15:55	OWASP crAPI: Completely Ridiculous API	Jayesh Ahire,Roshan Piyus . . .
14:00 - 15:55	OpenSSF Scorecard	Naveen Srinivasan,Neil Na . . .
14:00 - 15:55	EvilnoVNC: Next-Gen Spear Phishing Attacks	Joel Gámez Molina
14:00 - 15:55	Attack Surface Framework	Mike Henkelman,Prajwal Pa . . .
14:00 - 15:55	Glyph	Corey Hartman
14:00 - 15:55	Vacuum Robot Hacking	Dennis Giese
Saturday		
10:00 - 11:55	Lambda Looter	Doug Kent,Rob Ditmer
10:00 - 11:55	Lupo: Malware IOC Extractor	Vishal Thakur
10:00 - 11:55	Veilid	Deth Veggie,TC Johnson
10:00 - 11:55	Saturday	Joshua Herman
10:00 - 11:55	The Wifydra: Multiheaded RF Panopticon	Lozaning
10:00 - 11:55	USBvalve - Expose USB activity on the fly	Cesare Pizzi
12:00 - 13:55	BBOT (Bighuge BLS OSINT Tool)	Joel "TheTechromancer" Mo . . .
12:00 - 13:55	Abusing Microsoft SQL Server with SQLRecon	Sanjiv Kawa
12:00 - 13:55	Red Wizard: user-friendly Red Teaming infrastru . . .	Ben Brücker
12:00 - 13:55	Am I Exploitable? (MI-X)	Ofri Ouzan,Yotam Perkal
12:00 - 13:55	Kraken, a modular multi-language webshell for defe . . .	Raul Caro
12:00 - 13:55	Pcapinator: Rise of the PCAP Machines	Henry Hill,Mike "d4rkm4tt . . .
14:00 - 15:55	ThreatScraper: Automated Threat Intelligence Gathe . . .	Aaron "AJ" Morath,Scott G . . .
14:00 - 15:55	RuleProcessorY & Gramify - Rule Optimization & Pas . . .	Niels Loozekoot

PDT Times	Title	speaker
14:00 - 15:55	HardHat Command & Control Framework	Jonathan Owens
14:00 - 15:55	ProjectDiscovery Nuclei	Brendan O'Leary,Pj Metz
14:00 - 15:55	ICS Forensics tool	Maayan Shaul,Ori Perez
14:00 - 15:55	BLE CTF	Alek Amrani,Ryan Holeman

[Return to Index](#)

ESV - Embedded Systems Village

Location: LINQ - 3rd flr - Evolution - Embedded Systems Village - [Map](#)

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Embedded Systems Village Activities	
Saturday		
10:00 - 17:59	Embedded Systems Village Activities	
Sunday		
10:00 - 13:59	Embedded Systems Village Activities	

[Return to Index](#)

HHV - Hardware Hacking and Solder Skills Villages

Location: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Home Page: <https://dchhv.org/>

Sched Page: <https://dchhv.org/schedule/schedule.html>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732728536149786665>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Soldering Skills Village Activities	
10:00 - 17:59	RoboSumo Play Time	
10:00 - 17:59	Hardware Hacking Rube Goldberg Machine	
10:00 - 17:59	Make Your Own Use	
11:00 - 11:20	The Creation Of The Out-Of-Band Anti Virus Dock (O . . .	Bosen Zhang,Howard Yang,P . . .
12:00 - 12:50	Introduction To Esp8266/Esp32 Microcontrollers And . . .	Ryan Zagrodnik
13:00 - 13:50	Sadprotocol Goes To Hollywood: Hijacking An Ip Cam . . .	Javier Aguinaga,Octavio G . . .
14:00 - 14:50	Open Sesame! How To Open One Thousand And One Lock . . .	Thomas BYGODT
15:00 - 15:50	Radiation Detection For The Rest Of Us - Diy Radia . . .	Patrick Kiley
Saturday		
10:00 - 15:30	Make Your Own Use	
10:00 - 17:59	Soldering Skills Village Activities	
10:00 - 17:59	RoboSumo Play Time	
10:00 - 15:30	Hardware Hacking Rube Goldberg Machine	
13:00 - 13:59	RoboSumo Bracket Competition	
15:00 - 15:50	Generating Rf With Stock Hardware For Drones	David Melendez
16:00 - 16:30	Hardware Hacking Village Prize Ceremony	
Sunday		
10:00 - 12:59	Soldering Skills Village Activities	
10:00 - 12:59	RoboSumo Play Time	

[Return to Index](#)

HRV - Ham Radio Village

Location: Flamingo - Virginia City - Ham Radio Village - [Map](#)

Home Page: <https://hamvillage.org/>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733631667372103>

PDT Times	Title	speaker
Thursday		
09:00 - 17:59	Ham In A Day Class	Dan KB6NU
Friday		
13:00 - 13:59	Amateur Radio Digital Modes Primer	Jon Marler
15:00 - 16:30	HF Radio Demonstration	KitKat
Saturday		
11:00 - 11:30	How to Crush Field Day and Win Big Prizes	Hamster
13:00 - 13:59	Using an SBC for ham radio digital modes that isn' . . .	Jon Marler
15:00 - 15:30	Modernizing AX.25 packet radio with Modern Packet . . .	Jeremy Banker
15:00 - 16:30	HF Radio Demonstration	KitKat
Sunday		
12:00 - 12:30	My Callsign Is My Passport - Responsible Testing A . . .	Dan Norte, Lucas Gahler

[Return to Index](#)

ICSV - Industrial Control Systems Village

Location: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

Home Page: <https://www.icsvillage.com/>

Sched Page: <https://www.icsvillage.com/defconevents/def-con-31>

DC Discord Chan: <https://discord.com/channels/708208267699945503/735938018514567178>

PDT Times	Title	speaker
Friday		
11:00 - 11:30	What's up, Doc? Using documentation to build better . . .	Ian Fox
11:30 - 11:59	Five (or More) Maritime Cybersecurity Challenges	Gary C. Kessler
12:00 - 13:30	ICS Village - TSA Keynote	Tim Weston
13:30 - 14:59	Open Distro of Malicious Maritime Hacking Tools: W . . .	Austin Reid,Gary C. Kessl . . .
15:00 - 15:30	Wired for Safety: Prioritizing Safety in Deadly Sy . . .	Jace Powell
15:30 - 15:59	OT Vulnerability analysis methodology	Jeonghoon Bae
16:00 - 16:30	I'm On The Hype Train: Bottom's Up!	Joe Slowik
16:30 - 16:59	Anaotomy of the Top 10 Cybersecurity Terrain for C . . .	Mars Cheng
Saturday		
10:00 - 10:30	I am the captain now: Taking remote control of shi . . .	Ken Munro
10:30 - 10:59	EMBA - From firmware to exploit	Michael Messner
11:00 - 11:30	Wrenches, Widgets, and Walkdowns: Unraveling the T . . .	Tony Turner
11:30 - 11:59	Cyber-Physical Detection and Response: A new Parad . . .	Ryan Heartfield
12:00 - 13:30	Fear and Loathing on Plum Island	David Emmerich,Emma Stewa . . .
13:30 - 14:59	Panel Discussion -- Designing and Deploying NOC/SO . . .	Brad Proctor,Cliff Neve,D . . .
15:00 - 15:30	Your Ship is Leaking... How Social Media Plays a R . . .	Rae Baker
15:30 - 15:59	Improving the Speed of Cybersecurity: Seven Cyber . . .	Tyson Meadors
16:00 - 16:30	The Unlikely Romance: Critical Infrastructure Edit . . .	Casey Ellis
16:30 - 16:59	Lessons learned when building a Maritime Systems S . . .	Brien Croteau
Sunday		
10:00 - 10:30	Let's Talk about Voice	Travis Juhr
10:30 - 10:59	Vulnerability instead of security: How we managed . . .	Lukas Sokefeld
11:00 - 11:30	The Flaws in Cloud-based ICS Ecosystem	Hank Chen
11:30 - 11:59	Hunting Aberrant Maritime Network Traffic with Ope . . .	Chet Hosmer
12:00 - 12:30	The War is Coming: Why Securing OPC-UA is more cri . . .	Hank Chen
12:30 - 12:59	Is China Prepping an "Unforgettable Humiliation . . .	Dana Goward

[Return to Index](#)

IOTV - Internet Of Things Village

Location: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Home Page: <https://www.iotvillage.org/>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732734565604655114>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	IoT Village Hacking Playground	
10:00 - 17:59	Critical Infrastructure & IoT Exploitation	
10:00 - 17:59	Secure or Surrender	
10:00 - 17:59	The IoT Kill Zone	
10:00 - 17:59	IoT Village Hardware Hacking Exercises 2023	
10:00 - 17:59	Embedded Device Security Workshops	
10:00 - 17:59	Perform Memory Extraction, Emulation and Shellcode	
10:00 - 17:59	Hardware Hacking Your Kitchen	
15:30 - 16:29	IoT Village - Free Book Signing with author Ted Ha . . .	
Saturday		
10:00 - 17:59	Hardware Hacking Your Kitchen	
10:00 - 17:59	IoT Village Hacking Playground	
10:00 - 17:59	Critical Infrastructure & IoT Exploitation	
10:00 - 17:59	Secure or Surrender	
10:00 - 17:59	The IoT Kill Zone	
10:00 - 17:59	IoT Village Hardware Hacking Exercises 2023	
10:00 - 17:59	Embedded Device Security Workshops	
10:00 - 17:59	Perform Memory Extraction, Emulation and Shellcode	
Sunday		
10:00 - 13:59	IoT Village Hacking Playground	
10:00 - 13:59	Critical Infrastructure & IoT Exploitation	
10:00 - 13:59	Secure or Surrender	
10:00 - 13:59	The IoT Kill Zone	
10:00 - 13:59	IoT Village Hardware Hacking Exercises 2023	
10:00 - 13:59	Embedded Device Security Workshops	
10:00 - 13:59	Perform Memory Extraction, Emulation and Shellcode	
10:00 - 13:59	Hardware Hacking Your Kitchen	

[Return to Index](#)

LPV - Lock Pick Village

Location: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

Home Page: <https://www.toool.us/>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732734164780056708>

PDT Times	Title	speaker
Friday		
10:15 - 10:45	Intro to Lockpicking	TOOOL
10:00 - 17:59	Lockpick Village Activities	
12:00 - 12:20	The "Why" of Lock Picking	Christopher Forte
13:00 - 13:30	Intro to Lockpicking	TOOOL
14:00 - 14:30	Doors, Cameras, and Mantraps: Oh, my!	Dylan Baklor
15:00 - 15:40	How to Lose Access to your Door in Two Easy Steps	jos weyers
16:00 - 16:30	Intro to Lockpicking	TOOOL
Saturday		
10:15 - 10:45	Intro to Lockpicking	TOOOL
10:00 - 17:59	Lockpick Village Activities	
16:00 - 16:30	Intro to Lockpicking	TOOOL
16:45 - 17:45	Totally Tubular: An Impromptu Talk About Tubular L . . .	Deviant Ollam
Sunday		
10:15 - 10:45	Intro to Lockpicking	TOOOL
10:00 - 13:59	Lockpick Village Activities	
11:00 - 11:59	Safecracking for Everyone	Jared Dygert
12:00 - 13:30	Officially Unofficial Safecracking Tournament	Jared Dygert
13:00 - 13:30	Intro to Lockpicking	TOOOL

[Return to Index](#)

MISC - Misc

PDT Times	Title	speaker
Wednesday		
00:00 - 09:59	The DEFCON31 Multi User Dungeon Adventure (DEFCON . . .	
11:00 - 16:59	The Unofficial DEF CON Shoot	
17:00 - 06:59	Linecon	
Thursday		
06:00 - 11:59	Defcon.run	
10:00 - 11:59	CMD+CTRL at DEF CON 31 - Free Play	
15:00 - 20:59	Toxic BBQ	
16:00 - 18:59	DDV open and accepting drives for duplication	
Friday		
06:00 - 11:59	Defcon.run	
06:00 - 06:59	CycleOverride Defcon Bike Ride	
10:00 - 16:59	DDV open and accepting drives for duplication	
11:00 - 11:59	No Starch Press - Book Signing - Bryson Payne, Go . . .	
11:00 - 17:59	DC's Next Top Threat Model (DCNTTM) - BYODesign . . .	
11:00 - 11:59	EFF Benefit Poker Tournament at DEF CON 31 - Pre-t . . .	
12:00 - 12:59	No Starch Press - Book Signing - Joe Gray, Practic . . .	
12:00 - 17:59	EFF Benefit Poker Tournament at DEF CON 31 - Poker	
13:00 - 13:59	No Starch Press - Book Signing - Craig Smith, The . . .	
13:00 - 15:59	Free Amateur Radio License Exams	
14:00 - 14:59	No Starch Press - Book Signing - Travis Goodspeed, . . .	
14:00 - 15:59	DC's Next Top Threat Model (DCNTTM) - Kids - Lea . . .	
15:00 - 15:59	No Starch Press - Book Signing - Nick Aleks & Dole . . .	
16:00 - 16:59	No Starch Press - Book Signing - Bradly Smith, Dev . . .	
18:30 - 21:59	Hacking Policy & Prompts - Happy Hour	
19:00 - 19:59	Kids Only Karaoke	
20:00 - 23:59	Movie Night	
Saturday		
06:00 - 11:59	Defcon.run	
10:00 - 16:59	DDV open and accepting drives for duplication	
10:00 - 11:59	DC's Next Top Threat Model (DCNTTM) - Kids - Lea . . .	
10:00 - 15:59	Book Exchange	
11:00 - 11:59	No Starch Press - Book Signing - Patrick Wardle, T . . .	
11:00 - 11:59	No Starch Press - Book Signing - Maria Markstedter . . .	Maria Markstedter
12:00 - 12:59	No Starch Press - Book Signing - Daniel Reilly, Ma . . .	

PDT Times	Title	speaker
13:00 - 13:59	No Starch Press - Book Signing - Jos Weyers, Matt . . .	
13:00 - 14:59	DC's Next Top Threat Model (DCNTTM) - BYODesign . . .	
14:00 - 14:59	No Starch Press - Book Signing - Micah Lee, Hacks, . . .	
14:30 - 14:59	No Starch Press - Book Signing - Cory Doctorow, Re . . .	Cory Doctorow
14:00 - 14:59	DEF CON Chess Kids Free-Play	
15:00 - 15:59	No Starch Press - Book Signing - Jon DiMaggio, The . . .	
16:00 - 16:59	No Starch Press - Book Signing - Fotios Chantzis, . . .	
18:00 - 21:59	EFF Tech Trivia	

Sunday

06:00 - 11:59 [Defcon.run](#)

10:00 - 10:59 [Last chance to pick up drives at the DDV](#)

[Return to Index](#)

MIV - MisInformation Village

Location: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

Home Page: <https://www.misinformationvillage.com/>

Sched Page: <https://www.misinformationvillage.com/defcon31/>

PDT Times	Title	speaker
Friday		
10:00 - 10:30	Opening Session of MisinfoVillage 2023	Misinformation Village St . . .
10:30 - 10:59	Teaching Information Warfare: Strategies in Academ . . .	Greg Carpenter
11:00 - 11:30	Cutting through the noise: What you need to know a . . .	Chloé Messdaghi
11:30 - 12:30	If it looks like a duck... Russia's new MDM commun . . .	Paula González Nagore
12:30 - 12:59	Hackathon presentation	Misinformation Village St . . .
13:30 - 13:59	The Russian Playbook vs. the Chinese Little Red Pl . . .	Darren Linvill
13:00 - 13:30	Dissecting Deception: The Role of Twitter in U.S. . . .	Travis Allen
14:00 - 14:30	Holding Leaflets in the Left Hand and Bullets in t . . .	Kieran Green
14:30 - 15:30	Be a Nerd that Talks Good: Up-leveling how we talk . . .	Joel Benge
15:30 - 16:30	Digital Media Authentication - A Toolkit for Journ . . .	Adam Rose
16:30 - 17:59	Film screening: Reality Games Using film and inter . . .	Michael Morgenstern
Saturday		
10:00 - 10:59	Disincentivizing misinformation: co-create a new p . . .	Vardon Hamdiu
11:30 - 12:30	Navigating the Disinformation Landscape	Eric Curwin
11:00 - 11:59	Evil Digital Twin: Learn Psychological Manipulatio . . .	Ben D. Sawyer,Matthew Can . . .
12:30 - 13:30	Patient Zero Day: The Leaking of Patients' Privat . . .	Andrea Downing
13:30 - 14:30	Main features of Russia's disinformation and propa . . .	Carlos Galán
14:30 - 14:59	156 million targeted: Biggest social phishing cybe . . .	Douglas Bernardini
15:00 - 15:30	Misinformation As A Service: Social Engineering te . . .	Daniel Isler
15:30 - 16:30	IVY HAUL: A Computational Linguistics Analysis of . . .	Shea Nangle
16:30 - 17:30	Hacks, Leaks, and Revelations: Pandemic Profiteers . . .	Micah Lee
17:30 - 17:59	Misinformation Village Q and A	Misinformation Village St . . .
Sunday		
10:00 - 11:30	Hackathon result's presentation	Misinformation Village St . . .
11:30 - 11:59	Misinfo Village Closing / Panel / Summary / Feedba . . .	Misinformation Village St . . .

[Return to Index](#)

MUS - Music

Home Page: <https://defconmusic.org>

Sched Page: <https://defconmusic.org/def-con-31-music-lineup/>

PDT Times	Title	speaker
Thursday		
18:00 - 01:59	Music Set / Entertainment (Thursday, SYN Stage)	Bolonium,Deepblue,Dries,D . . .
18:00 - 01:59	Music Set / Entertainment (Thursday, ACK Stage)	Alexi Husky,DJ Scythe,Del . . .
Friday		
18:00 - 01:59	Music Set / Entertainment (Friday, ACK Stage)	Acid T,CTRL/rsm,DJ PatAtt . . .
21:00 - 01:59	Music Set / Entertainment (Friday, SYN Stage)	Great Scott,Krisz Klink,T . . .
Saturday		
18:00 - 01:59	Music Set / Entertainment (Saturday, ACK Stage)	DotOrNot,Dr. McGrew,H4X,I . . .
21:00 - 01:59	Yarrrrgh Pirate Night - Music Set / Entertainment . . .	FuzzyNop,Miss Jackalope,N . . .

[Return to Index](#)

PHV - Packet Hacking Village

Location: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Home Page: <https://www.wallofsheep.com/>

Sched Page: <https://www.wallofsheep.com/pages/dc31#talks>

DC Discord Chan: <https://discord.com/channels/708208267699945503/708242376883306526>

PDT Times	Title	speaker
Friday		
09:00 - 17:59	Honey Pot Workshop	
09:00 - 17:59	Wall of Sheep	
09:00 - 17:59	Build Your Own Botnet	
09:00 - 17:59	Linux Trainer Workshop	
09:00 - 17:59	NetworkOS: Be The Cloud	
09:00 - 17:59	RegEx Trainer	
09:00 - 17:59	Password Lab	
09:00 - 17:59	Fleet DefCon 31 Workshop	
09:00 - 17:59	Packet Inspector	
09:00 - 17:59	Packet Detective	
10:00 - 10:50	Pwning the Pwners with Mindware	Frank "D9" DiGiovanni
11:00 - 11:50	Death by 1000 Likes: How Much Do You Really Leak i . . .	Will Kay
12:00 - 12:50	OSINT for Physical Security Intelligence	Chet Hosmer, Mike Raggo
Saturday		
09:00 - 17:59	Honey Pot Workshop	
09:00 - 17:59	Build Your Own Botnet	
09:00 - 17:59	Wall of Sheep	
09:00 - 17:59	Linux Trainer Workshop	
09:00 - 17:59	NetworkOS: Be The Cloud	
09:00 - 17:59	RegEx Trainer	
09:00 - 17:59	Password Lab	
09:00 - 17:59	Fleet DefCon 31 Workshop	
09:00 - 17:59	Packet Inspector	
09:00 - 17:59	Packet Detective	
15:00 - 15:50	WINE Pairing with Malware	Jared Stroud
16:00 - 16:50	The Importance of Arts and Crafts in ThreatOps	Pete Hay
Sunday		
09:00 - 12:59	Honey Pot Workshop	
09:00 - 12:59	Wall of Sheep	
09:00 - 12:59	Build Your Own Botnet	
09:00 - 12:59	Linux Trainer Workshop	

PDT Times	Title	speaker
09:00 - 12:59	NetworkOS: Be The Cloud	
09:00 - 12:59	RegEx Trainer	
09:00 - 12:59	Password Lab	
09:00 - 12:59	Fleet DefCon 31 Workshop	
09:00 - 13:59	Packet Inspector	
09:00 - 12:59	Packet Detective	

[Return to Index](#)

PLV - Policy Village

Location: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

Home Page: <https://defcon.org/policy/>

Sched Page: <https://twitter.com/DEFCONPolicy/status/1686024040023003136?s=20>

PDT Times	Title	speaker
Friday		
10:00 - 11:50	Building the Hacker Talent Pipeline Through Workfo . . .	Ashley Sequeira,Ayan Isla . . .
10:00 - 11:50	US Cyber Policy 101	Harley Geiger,Lauren Zabi . . .
12:00 - 12:50	The Promise and Perils of Planetary-Scale ISPs	J. Scott Christianson
12:00 - 13:50	It's Coming from Inside the House: Next Steps for . . .	David Forscey,Emily Paull . . .
12:00 - 13:50	International Cyber Policy 101	Adam Dobell,Ari Schwartz, . . .
13:00 - 13:50	Securing the Supply Chain	Camille Stewart Gloster,E . . .
14:00 - 14:50	What are your thoughts on AI assisted voice clonin . . .	Christine Barker
14:00 - 14:50	Cyber Policy Adrift – Charting a Path Forward fo . . .	Blake Benson,Cliff Neve,J . . .
15:00 - 15:50	Blocking Pathways into Cybercrime: Current Efforts . . .	Greg Francis,Jonathan Lus . . .
15:00 - 16:50	A global approach to tackling software resilience	Allan Friedman,Camille St . . .
16:00 - 16:50	I Am A Former National Cybersecurity Director, Ask . . .	Chris Inglis
17:00 - 17:50	Keeping stores safe: how do we better secure apps . . .	Charlie Gladstone,David R . . .
17:00 - 17:50	Demystifying Hacking for Government Officials	Brad Manuel,Jack Cable,Ja . . .
Saturday		
10:00 - 10:50	What “Secure by Design” means for software bre . . .	Cassie Crossley,Christoph . . .
10:00 - 11:50	How hackers can work with government, industry, ci . . .	Adrien Ogee,David Forscey . . .
11:00 - 11:50	AI Caramba! A DC <> DEF CON interface on machin . . .	Austin Carson,Erick Galin . . .
11:00 - 13:50	Secure by Design: Ask the Government Anything and . . .	Bob Lord,Cheri Caddy,Jack . . .
12:00 - 13:50	Hands On a Cyber Policy Crisis: Testing Assumption . . .	Safa Shahwan Edwards
12:00 - 12:50	The Coming War on Encryption, Part 3 (and how you . . .	India McKinney
13:00 - 13:50	Beyond the Breach: Exploring Cybersecurity Policie . . .	Andrés Velázquez,Isabel . . .
14:00 - 14:50	Let Night City Sleep - Governance Against a Cyberp . . .	Cameron Byrd,Clayton Dixo . . .
14:00 - 15:50	Abating the Eye of Sauron: Help Combat Authoritari . . .	David Houston,Michaela Le . . .
14:00 - 14:50	How can we encourage more hackers to engage with p . . .	Peter Stephens,Thomas Kra . . .
15:00 - 15:50	Non-State Actors in the Russia/Ukraine Conflict	Dan Grobarcik,Marc Rogers . . .
15:00 - 15:50	All Your Vulns are Belong to Terms & Conditions	Casey Ellis,David Rogers, . . .
16:00 - 17:50	We're From the Government and We're Here to Help S . . .	Anjana Rajan,Brian Behlen . . .
16:00 - 16:50	How do you solve a problem like Mirai - establishi . . .	Kat Megas,Peter Stephens
17:00 - 17:50	Navigating the Digital Frontier: Advancing Cyber D . . .	Christopher Painter,Harry . . .
Sunday		
10:00 - 10:50	Putting Your Money Where Your Cyber Is: A Guided D . . .	Andrea Matwyshyn

[Return to Index](#)

PSV - Physical Security Village

Location: Flamingo - Carson City - Physical Security Village - [Map](#)

Home Page: <https://www.physsec.org/>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732732893830447175>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Physical Security Village Activities	
12:00 - 12:30	Lock Bypass 101	Karen
12:30 - 12:59	Lock Bypass 102	Karen
13:30 - 14:30	Access Control Vulnerabilities: Breaking Into Buil . . .	Chad,Shortman
14:30 - 15:30	Flipping Locks: Remote Badge Cloning with the Flip . . .	Dan,Langston "Shock" Clem . . .
15:30 - 16:30	Deep Diving Into HID Vulnerabilities: Heart of Dar . . .	Chad,Shortman
Saturday		
10:00 - 17:59	Physical Security Village Activities	
12:00 - 12:30	RFID Hacking	Ege
12:30 - 13:15	Physical pentesting in a post-covid world	Brian Halbach
13:15 - 13:30	Free Pokemon Card Bus Passes	Jarvis,Malcolm
14:00 - 14:30	Lock Bypass 101	Terry
14:30 - 14:59	Lock Bypass 102	Ege
Sunday		
10:00 - 13:59	Physical Security Village Activities	
11:30 - 11:59	Elevators 101	Karen
12:30 - 12:59	Forcible Entry 101	Bill Graydon
13:00 - 13:59	Access Control Vulnerabilities: Breaking Into Buil . . .	Chad,Shortman
14:00 - 14:30	Bypass 101	Terry
14:30 - 14:59	Bypass 102	Ege

[Return to Index](#)

PWV - Password Village

Location: Caesars Forum - Summit - 236 - Password Village - [Map](#)

Home Page: <https://passwordvillage.org/>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733760742621214>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Password Village Activities	
Saturday		
10:00 - 17:59	Password Village Activities	
Sunday		
10:00 - 13:59	Password Village Activities	

[Return to Index](#)

PYV - Payment Village

Location: Flamingo - Virginia City - Payment Village - [Map](#)

Home Page: <https://www.paymentvillage.org/>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733473558626314>

PDT Times	Title	speaker
Friday		
11:00 - 12:30	Payment Village Workshop	Leigh-Anne Galloway
11:00 - 17:59	Payment Village Challenges/CTF	
Saturday		
11:00 - 12:30	Payment Village Workshop	Leigh-Anne Galloway
11:00 - 17:59	Payment Village Challenges/CTF	
Sunday		
10:00 - 13:59	Payment Village Challenges/CTF	

[Return to Index](#)

QTV - Quantum Village

Location: LINQ - 3rd flr - Quantum Village - [Map](#)

Home Page: <https://quantumvillage.org/>

PDT Times	Title	speaker
Friday		
10:00 - 10:30	Quantum Village Opening!	Mark Carney,Quantum Villa . . .
10:30 - 10:59	QOLOSSUS - Quantum Capture the Flag Introduction!	Quantum Quizmasters
11:00 - 11:59	No time for NISQy Business	Rafal Janik
12:00 - 12:59	World's Cheapest "QKD" ;) -QKD for fun and non- pr . . .	Ben Varcoe,Jose Pisaro,Ma . . .
14:00 - 14:59	Doomed to repeat the past: classical hardware expl . . .	Jamie Friel
15:00 - 15:59	Hacking Quantum Advantage for Classical Processes; . . .	Konstantinos Karagiannis
16:00 - 17:59	The Quantum Debates	
16:00 - 16:45	Debate: The Quantum Village believes individual ci . . .	David Joseph,Troy Mills
17:15 - 17:59	Debate: NISQ and the future of Quantum Advantage: . . .	Konstantinos Karagiannis, . . .
Saturday		
10:30 - 10:59	Q-CTF QOLOSSUS Update	Mark Carney
11:00 - 12:30	Quantum attacks on next-gen cryptosystems: lattice . . .	
13:00 - 13:59	QDoor: Exploiting Approximate Synthesis for Backdo . . .	Lei Jiang
14:00 - 14:59	OpenQuantum: open-source hardware for quantum engi . . .	Max Shirokawa Aalto
15:00 - 15:59	Quantum Technologies on a Raspberry Pi (and HackRF . . .	Ben Varcoe
16:00 - 17:59	Quantini Time! Cocktail hour for the Quantum curio . . .	
16:00 - 16:59	Quantum Music Workshop: Build Your Own Quantum Syn . . .	Mark Carney
17:00 - 17:59	Quantum Computer Music Performance, by Scott Oshir . . .	Scott Oshiro
Sunday		
10:00 - 10:59	Math for Quantum	Mark Carney
11:00 - 11:59	Quantum Life - An open mic space discussing the po . . .	Mark Carney,Victoria Kuma . . .
12:00 - 12:59	QOLOSSUS; Quantum CTF - Results!	

[Return to Index](#)

RCV - Recon Village

Location: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

Home Page: <https://www.reconvillage.org/>

Sched Page: <https://reconvillage.org/recon-village-talks-2023-defcon-31/>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733566051418193>

PDT Times	Title	speaker
Friday		
10:00 - 10:50	Keynote - Reshaping Reconnaissance: AI's Role in O...	Matt Edmondson
10:50 - 11:35	OSINT Situational Awareness	Joe Gray
11:35 - 12:10	Oh The Places You'll Guo: Using Media Variants to ...	Patrick Warren
12:10 - 12:55	How I Found Your Password, and Other Advanced Data ...	M4x 5yn74x
14:00 - 14:25	Mastering OSINT: Advanced Techniques in the Realm ...	Seyfullah
14:25 - 15:10	Leakonomics 101: The Last Year in Data Leaks	Nick Ascoli
15:10 - 15:45	Getting ahead of the bad guys with Internet Scanni ...	Vitor Ventura
15:45 - 16:30	Crushing crumbs of information to eat a whole cake ...	Felipe Pr0teus
16:30 - 17:15	Nosy Cops: Exposing the Hidden Potential of Police ...	sally
Saturday		
10:00 - 10:45	Panel Discussion - Bugs, Bounties, & Breaches - In ...	Jason Haddix
10:45 - 11:30	OSINT Privacy Unmasked: Taking Control of Your Dig ...	Zoey Selman
11:30 - 12:05	I Am The Disinformation Campaign	MasterChen
12:05 - 12:50	How I Built Recon to Scale with Serverless Archite ...	Gunnar Andrews
14:00 - 14:25	Easy EASM - the zero dollar attack surface managem ...	Jason Haddix
14:25 - 15:10	Azure AD recon with OSINT tools	Nestori Syynimaa
15:10 - 15:55	Unlocking the Power of OWASP Amass: Introducing th ...	Jeff Foley
15:55 - 16:20	Finding Hidden Gems In Temporary Mail Services	Berk Can Geyikci
16:20 - 17:05	Riding with the Chollimas: Our 100-Day Quest to Id ...	Mauro Eldritch
17:05 - 17:50	The Perils of Generative AI: Implications for Open ...	Andy Dennis

[Return to Index](#)

RFV - Radio Frequency Village

Location: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

Home Page: <https://rfhackers.com/>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732732595493666826>

PDT Times	Title	speaker
Friday		
11:00 - 11:25	RF Village Kickoff	
12:00 - 12:59	The International Wigle Space Balloon	Lozaning
13:00 - 13:59	WIFISHARK	Wasabi
14:00 - 14:20	Signals! In! Spaaaaaace!	Ark (from WiGLE),wytshado . . .
15:00 - 15:20	Protocol Identification for Integration	Eric Escobar
16:00 - 16:20	Badge Cloning With Doppelgänger	Travis Weathers
Saturday		
12:00 - 12:20	Shipping Wardriving Hardware - Cross-country Wigle . . .	Segfault
13:00 - 13:59	125khz the Brown note for Cars	Woody
14:00 - 14:59	Wardriving 102: Moving Beyond the Wigle App	bkobe
15:00 - 15:20	Antennas	Kent
Sunday		
11:00 - 12:59	War Driver Meetup	RF Village Staff

[Return to Index](#)

RTV - Red Team Village

Location: Flamingo - Sunset-Twilight Ballroom - Red Team Village - [Map](#)

Home Page: <https://redteamvillage.io/>

Sched Page: <https://redteamvillage.io/schedule.html>

PDT Times	Title	speaker
Friday		
11:00 - 11:59	Stories from the Trenches	Ben "NahamSec" Sadeghipou . . .
12:00 - 12:59	Red Hot (Red Team TTPs)	Ralph May,Steve Borosh
12:00 - 14:59	Build Your Own Cat-Shaped USB Hacking Tool! (with . . .	Alex Lynd
12:00 - 12:59	OSINT Skills Lab Challenge	Lee McWhorter,Sandra Stib . . .
12:00 - 13:59	An Introduction to SAML and its Security	Louis Nyffenegger
12:00 - 12:59	IOCs + APTs = "Let's play a game!" - Hack your way . . .	Leo Cruz
12:00 - 13:59	Scripting OWASP Amass for a Customized Experience	Jeff Foley
13:00 - 13:59	Hunting & Exploiting DLL Sideloads	Matthew Nickerson,Nick Sw . . .
13:00 - 13:59	OSINT Skills Lab Challenge	Lee McWhorter,Sandra Stib . . .
13:00 - 13:59	AI-Driven Hacker's Toolkit: Using AI to Learn Pyth . . .	Omar Santos
14:00 - 14:59	Hacking Web Apps and APIs with WebSploit Labs	Omar Santos
14:00 - 15:59	Open Source Intelligence (OSINT) for Hackers	Lee McWhorter,Sandra Stib . . .
14:00 - 15:59	How to [NOT] look like a Red Team	Michael Wylie
14:00 - 14:59	How to prioritize Red Team Findings? Presenting CR . . .	Guillermo Buendia
14:00 - 16:59	Kubernetes Offense	Michael Mitchell
15:00 - 15:59	Hacking Web Apps and APIs with WebSploit Labs	Omar Santos
15:00 - 15:59	Red Hot (Red Team TTPs)	Ralph May,Steve Borosh
15:00 - 15:59	SSH Tunneling: Evading Network Detection and Creat . . .	Cory Wolff
16:00 - 16:59	Malware Hunting an Offensive Approach	Filipi Pires
16:00 - 16:59	Hacking Real Web Areas	Ilkin Javadov
16:00 - 16:59	IOCs + APTs = "Let's play a game!" - Hack your way . . .	Leo Cruz
16:00 - 16:59	Passwords Argh Us	Traveler
16:00 - 16:59	Red Team Labs and Games for Kids	
Saturday		
09:00 - 09:59	Android Applications and APIs Hacking	Gabrielle Botbol
09:00 - 11:59	Build Your Own Cat-Shaped USB Hacking Tool! (with . . .	Alex Lynd
09:00 - 09:59	Passwords Argh Us	Traveler
09:00 - 10:59	Open Source Intelligence (OSINT) for Hackers	Lee McWhorter,Sandra Stib . . .
09:00 - 09:59	Red Team Labs and Games for Kids	
09:00 - 10:59	Hacking Meta Quest	Paul D.
10:00 - 10:59	Hunting & Exploiting DLL Sideloads	Matthew Nickerson,Nick Sw . . .
10:00 - 10:59	Red Hot (Red Team TTPs)	Ralph May,Steve Borosh

PDT Times	Title	speaker
10:00 - 10:59	Red Team Labs and Games for Kids	
11:00 - 16:59	(In)Direct Syscalls: A Journey from High to Low	Daniel Feichter
11:00 - 11:59	Passwords Argh Us	Traveler
11:00 - 12:59	Artificial Intelligence for Red Team Operations	Peter Halberg
12:00 - 12:59	Hacking Web Apps and APIs with WebSploit Labs	Omar Santos
12:00 - 12:59	Red Hot (Red Team TTPs)	Ralph May,Steve Borosh
12:00 - 13:59	Scripting OWASP Amass for a Customized Experience	Jeff Foley
13:00 - 14:59	How to [NOT] look like a Red Team	Michael Wylie
13:00 - 13:59	Storfield: A Quiet Methodology to Create Attacks i . . .	Cory Wolff
13:00 - 16:59	How Most Internal Networks are Compromised: A Set . . .	Scott Brink
14:00 - 14:59	IOCs + APTs = "Let's play a game!" - Hack your way . . .	Leo Cruz
14:00 - 14:59	AI-Driven Hacker's Toolkit: Using AI to Learn Pyth . . .	Omar Santos
15:00 - 15:59	Red Hot (Red Team TTPs)	Ralph May,Steve Borosh
15:00 - 15:59	OSINT Skills Lab Challenge	Lee McWhorter,Sandra Stib . . .
15:00 - 15:59	Malware Hunting an Offensive Approach	Filipi Pires
16:00 - 16:59	How to prioritize Red Team Findings? Presenting CR . . .	Guillermo Buendia
16:00 - 16:59	OSINT Skills Lab Challenge	Lee McWhorter,Sandra Stib . . .
16:00 - 16:59	Hacking Web Apps and APIs with WebSploit Labs	Omar Santos
Sunday		
09:00 - 09:59	Malware Hunting an Offensive Approach	Filipi Pires
09:00 - 09:59	How to prioritize Red Team Findings? Presenting CR . . .	Guillermo Buendia
09:00 - 10:59	Artificial Intelligence for Red Team Operations	Peter Halberg
09:00 - 10:59	Recon for Red Teamers and Bug Hunters 2.0	Jason Haddix
10:00 - 10:59	IOCs + APTs = "Let's play a game!" - Hack your way . . .	Leo Cruz
10:00 - 10:59	Passwords Argh Us	Traveler
11:00 - 11:59	OSINT Skills Lab Challenge	Lee McWhorter,Sandra Stib . . .
11:00 - 11:59	Storfield: A Quiet Methodology to Create Attacks i . . .	Cory Wolff
11:00 - 11:59	Hacking Web Apps and APIs with WebSploit Labs	Omar Santos

[Return to Index](#)

SEV - Social Engineering Village

Location: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Home Page: <https://www.se.community/>

Sched Page: <https://www.se.community/schedule/>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733952867172382>

PDT Times	Title	speaker
Friday		
08:30 - 17:59	SECV Village Open	
08:30 - 17:30	SECV - Youth Challenge	
17:15 - 17:59	A Slice of Deception: The 2023 #SECVC Debrief	JC,Snow
Saturday		
08:30 - 17:30	SECV - Youth Challenge	
08:30 - 17:59	SECV Village Open	
09:00 - 09:30	Anti-Social Engineering: Can You Be a Good Social . . .	Andrew Lemon
09:30 - 09:59	Your Swag is My Swag: Pwning Fortune 500 Companies . . .	Daniel "Jcache" Goga,Lang . . .
10:00 - 11:30	Cold Calls	
11:30 - 13:30	SE Improv	
13:30 - 15:30	Cold Calls	
16:00 - 16:59	Building an Effective Security Culture Program	Jessica Barker,Maxie Reyn . . .
17:00 - 17:30	Phishing with Dynamite: Harnessing AI to Superchar . . .	Dani Goland,Preston Thorn . . .
Sunday		
10:00 - 10:59	SECV - Youth Challenge	
10:00 - 11:30	Cold Calls	
10:00 - 13:59	SECV Village Open	
12:00 - 13:30	SECV - Awards & Competitor Panel	

[Return to Index](#)

SOC - Social Activities: Parties/Meetups

PDT Times	Title	speaker
Thursday		
10:00 - 17:59	Hack the Box Hack-a-thon	
10:00 - 23:59	Hack the Box Hack-a-thon	
12:00 - 12:59	Friends of Bill W	
14:00 - 15:59	DEF CON Kids Meetup	
16:00 - 17:59	Queercon Mixers	
17:00 - 17:59	Friends of Bill W	
Friday		
10:00 - 17:59	Hacker Memorial	
10:00 - 17:59	DCG Meetups	
12:00 - 15:59	WISP Chill Out Space with Refreshments	
12:00 - 17:59	Lonely Hackers Club Meetup	
12:00 - 12:59	Friends of Bill W	
12:00 - 17:59	HDA / Accessibility Area Open	
12:00 - 17:59	HDA Community Meetups	
14:00 - 15:59	Book Club Discussion and Exchange	
16:00 - 17:59	Queercon Mixers	
16:00 - 18:59	DEF CON Holland Group Presents: VrijMiBo	
16:00 - 18:59	DC 404/DC 678/ DC 770/ DC 470 (Atlanta Metro)	
17:00 - 17:59	Friends of Bill W	
18:00 - 01:59	Blacks in Cyber Lituation Party	
20:00 - 23:59	Cult Of The Dead Cow Breaks The Internet (and you . . .	
20:00 - 21:59	Hacker Flairgrounds	
20:00 - 01:59	Hacker Karaoke 15	
20:30 - 22:59	Blue Team Village (BTV) Pool Party	
20:30 - 22:59	WISP Community Meet Up at BTV Pool Party	
20:00 - 20:59	Lawyers Meet	
21:00 - 01:59	GothCon	
21:00 - 00:59	The Village People Party: hosted by Car Hacking, I . . .	NGHTHWK
22:00 - 00:59	QueerCon Party	DotOrNot, Miss Jackalope, S . . .
Saturday		
10:00 - 17:59	Hacker Memorial	
10:00 - 17:59	DCG Meetups	
12:00 - 17:59	Lonely Hackers Club Meetup	
12:00 - 12:59	Friends of Bill W	

PDT Times	Title	speaker
12:00 - 17:59	HDA / Accessibility Area Open	
12:00 - 17:59	HDA Community Meetups	
14:00 - 15:59	WISP Chill Out Space with Refreshments	
16:00 - 17:59	Queercon Mixers	
16:00 - 17:59	WISP Peer-to-Peer Mentoring and Networking	
17:00 - 17:59	Friends of Bill W	
19:00 - 00:59	BlanketFort Con	
19:30 - 21:59	DEF CON Kids Party	
19:00 - 21:59	Policy Lounge	
20:00 - 01:59	Hacker Karaoke 15	
21:00 - 01:59	Arcade Party	
21:00 - 01:59	VetCon	
21:00 - 00:59	Hack The Box, Pub Crawl	
21:00 - 00:59	Capitol Tech University, Pub Crawl	
21:00 - 00:59	University of Advancing Technology, Pub Crawl	
21:00 - 23:59	SECV - 80's Themed Party!	
22:00 - 23:59	Social Engineering Community Party	
Sunday		
12:00 - 13:59	Hacker Memorial	
12:00 - 13:59	DCG Meetups	
12:00 - 12:59	Friends of Bill W	
12:00 - 13:59	HDA / Accessibility Area Open	
12:00 - 13:59	HDA Community Meetups	

[Return to Index](#)

TCV - Telecom Village

Location: Flamingo - Virginia City - Telecom Village - [Map](#)

Home Page: <https://telecomvillage.com/>

Sched Page: <https://telecomvillage.com/#schedule>

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Telecom Village Inauguration	Harshit Mahajan
11:00 - 12:59	SS7 Workshop	Akib Sayyed,Zibran Sayyed
14:30 - 15:59	SS7 Workshop	Akib Sayyed,Zibran Sayyed
16:00 - 17:59	SS7 CTF	Akib Sayyed,Zibran Sayyed
Saturday		
10:00 - 10:59	Gazing into the crystal ball: Hacking and Securing . . .	Ajit Hatti,Akib Sayyed,Da . . .
11:00 - 12:59	Diameter Workshop	Akib Sayyed,Zibran Sayyed
14:30 - 15:59	Diameter Workshop	Akib Sayyed,Zibran Sayyed
16:00 - 17:59	Diameter CTF	Akib Sayyed,Zibran Sayyed
Sunday		
10:00 - 10:30	RF in the Middle Earth- Fallen 5G	Utku Y
10:30 - 10:59	All the things, all the time: Lifting the veil on . . .	James Moran
11:00 - 12:59	Telecom Village CTF	

[Return to Index](#)

TEV - Tamper Evident Village

Location: LINQ - 5th Floor / BLOQ - Tamper Evident Village - [Map](#)

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Tamper Evident Village Activities	
Saturday		
10:00 - 17:59	Tamper Evident Village Activities	
Sunday		
10:00 - 13:59	Tamper Evident Village Activities	

[Return to Index](#)

VMV - Voting Village

Location: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733881148506164>

PDT Times	Title	speaker
Friday		
10:30 - 11:25	A Global Perspective On Election Integrity	Bryson Bort,Chris Krebs,K . . .
10:00 - 10:30	Voting Village Opening Remarks	Catherine Terranova,Harri . . .
11:30 - 12:20	Top 10 Hacks To Watch Out For From An Election Off . . .	John Odum
11:30 - 11:59	VOTEC Corporation	John Medcalf
11:45 - 12:20	Surprise Unboxing	Harri Hursti
12:30 - 13:20	DISARM Workshop	Charles Smith,Dan Meidenb . . .
12:30 - 13:15	Ghost in the (Voting) Machine: Failures in Electio . . .	Ashlee Benge
13:20 - 14:05	Divided We Fall	Michael Moore
13:30 - 14:20	The Fallacy Of Privacy	Antigone Peyton
14:10 - 14:45	Risk Limiting Audits Of All Contests	Amanda Glazer
14:50 - 15:20	Understand Your Trust Assumptions!	Carsten Schürmann
14:30 - 15:20	Building Partnerships	Catherine Terranova,Maia . . .
15:30 - 16:15	What Makes Hackers Extraordinary - It's A Gift!	D9
15:30 - 16:15	RLA Workshop	Amanda Glazer
16:30 - 17:30	Election Preparation: 2024	Ashlee Benge,Jake Braun,J . . .
Saturday		
10:30 - 12:30	First Timers Workshop	Tailor Herrarte
10:30 - 11:25	I Can Shop Securely Online So Why Can't I Vote Onl . . .	David Jefferson,Harri Hur . . .
10:00 - 10:30	Voting Village Opening Remarks	Catherine Terranova,Harri . . .
11:30 - 12:15	Chinese Prototype Review	William Baggett
11:30 - 11:59	VOTEC Corporation	John Medcalf
12:30 - 13:20	Review: Surprise Unboxing	Harri Hursti
12:55 - 13:40	Conflicting Security Reports from Halderman-Spring . . .	David Jefferson,Drew Spri . . .
12:20 - 12:50	US private elections: the easy way in for foreign . . .	Scheme
13:55 - 14:35	Political Polarization	Constantine Nicolaidis
13:30 - 14:20	Interventions To Address Technology-Facilitated Vi . . .	Eric Davis,Hallie Stern,O . . .
14:40 - 15:30	Democracy, Are You Citizen Or Subject?	Kendall Spencer
14:30 - 15:20	Defense Community	Brian Stearns,Charles Smi . . .
15:35 - 16:15	Influencing Voters Through Social Media, ADTECH, B . . .	Joe Schniebes
15:30 - 16:20	2024 Election Threat Landscape	Catherine Terranova,Halli . . .
16:30 - 17:30	The Impact Of Misinformation On Elections	Joe Schniebes,Maia Mazurk . . .

[Return to Index](#)

WS - DEF CON Workshops

Home Page: <https://forum.defcon.org/node/244772>

PDT Times	Title	speaker
Thursday		
09:00 - 12:59	Protecting the AWS ecosystem - Misconfigurations, . . .	Rodrigo Montoro
09:00 - 12:59	Applied Emulation - A Practical Approach to Emulat . . .	Sean Wilson,Sergei Franko . . .
09:00 - 12:59	Hacking The Metal: An Intro to ARM Assembly Langua . . .	Eigentourist
09:00 - 12:59	Pentesting Industrial Control Systems: OCP-U-HACK . . .	Alexandrine Torrents,Arna . . .
09:00 - 12:59	Introduction to Cryptographic Attacks (Pre-Registr . . .	Matt Cheung
14:00 - 17:59	DotNet Malware Analysis Masterclass (Pre-Registrat . . .	Max 'Libra' Kersten
14:00 - 17:59	These Port Scans are Trash: Improving Nmap by Writ . . .	Philip Young "Soldier of . . .
14:00 - 17:59	Analysis 101 for Incident Responders (Pre-Registra . . .	Kristy Westphal
14:00 - 17:59	Hide your kids, turn off your Wi-Fi, they Rogue AP . . .	Daniel Costantini,James H . . .
14:00 - 17:59	Flipping the Coin: Red and Blue Teaming in Windows . . .	Angus "0x10f2c_" Strom,Tr . . .
Friday		
09:00 - 12:59	House of Heap Exploitation (Pre-Registration Requi . . .	Elizabeth St. Germain,Ken . . .
09:00 - 12:59	Getting into Trouble with Machine Learning Models . . .	Robert Koehlmoos
09:00 - 12:59	Android App Hacking - Hacking for Good! (Pre-Regis . . .	Kavia Venkatesh,Maria Ure . . .
09:00 - 12:59	Long Live the Empire: A C2 Workshop for Modern Red . . .	Dylan "CyberStryke" Butle . . .
09:00 - 12:59	Snakes on a Screen: Taming Offensive IronPython Te . . .	Anthony "Coin" Rose,Ganno . . .
14:00 - 17:59	Machine Learning for N00bs (Pre-Registration Requi . . .	Elizabeth Biddlecome,Irvi . . .
14:00 - 17:59	How hackers can send feedback directly to policyma . . .	Amit Elazari,Harley Geige . . .
14:00 - 17:59	Malware development on secured environment - Write . . .	Yoann Dequeker
14:00 - 17:59	Learning to Hack Bluetooth Low Energy with BLE CTF . . .	Ryan Holeman
14:00 - 17:59	Advanced WiFi Attacks for Red Team Professionals (. . .	Raúl "r4ulcl" Calvo Laor . . .
Saturday		
09:00 - 12:59	Email Detection Engineering and Threat Hunting Inb . . .	Alfie Champion,Josh Kamdj . . .
09:00 - 12:59	Active Directory Attacks: The Good, The Bad, and T . . .	Aaron Rosenmund,Brandon D . . .
09:00 - 12:59	The Petting Zoo: Breaking into CTFs (Pre-Registrat . . .	Christopher Forte,Robert . . .
09:00 - 12:59	Creating and uncovering malicious containers Redux . . .	Adrian "threlfall" Wood,D . . .
09:00 - 12:59	BLE Security 201 (Pre-Registration Required)	Maxine "Freqy" Filcher,Za . . .
14:00 - 17:59	Introduction to Exploit Development (Pre-Registrat . . .	Elizabeth Biddlecome,Irvi . . .
14:00 - 17:59	Hands-On TCP/IP Deep Dive with Wireshark - How thi . . .	Chris Greer
14:00 - 17:59	The Joy of Reverse Engineering: Learning With Ghid . . .	Wesley McGrew
14:00 - 17:59	Digital Forensics and Incident Response Against th . . .	Michael "S3curityNerd" Re . . .
14:00 - 17:59	Starbase: open source graph security analysis (Pre . . .	Adam Pierson,Austin Kelle . . .

XR V - XR Village

Location: Caesars Forum - Summit - 206 - XR Village - [Map](#)

Home Page: <https://xrvillage.org/>

PDT Times	Title	speaker
Friday		
10:00 - 15:59	Haptics Hack-a-Thon	
10:00 - 17:59	XR Village Playground	
11:00 - 16:59	Off the Rails: A demo with Pacific Northwest Natio . . .	
15:00 - 15:59	Securing Critical Versions of your Reality	Bryson Bort,Keenan Skelly . . .
16:00 - 16:59	Glad Scientist Village Vibes Immersive Performan . . .	
Saturday		
10:00 - 15:59	Haptics Hack-a-Thon	
10:00 - 17:59	XR Village Playground	
11:00 - 16:59	Off the Rails: A demo with Pacific Northwest Natio . . .	
13:00 - 13:59	XR implications on Mobile Security	Whitney Phillips
14:00 - 14:59	The of History XR From Fiction to Reality	Bob Gourley,Starr Brown
16:00 - 16:59	Glad Scientist Village Vibes Immersive Performan . . .	
17:00 - 17:59	Push All the Buttons Digital Twinning with Idaho N . . .	Kolton Heaps
Sunday		
10:00 - 11:59	XR Village Playground	
10:00 - 10:59	Watching Androids Dream of Electric Sheep: Immersi . . .	Brittan Heller,Liz "Lawye . . .
11:00 - 11:59	Off the Rails: A demo with Pacific Northwest Natio . . .	
11:00 - 11:59	Most Meta - Live Meta Quest2 Hack	David "Icer" Maynor

[Return to Index](#)

Talk/Event Descriptions

Title: ? Cube

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Are you ready to put your problem-solving skills to the test?

This year, we are proud to introduce a brand new contest, designed to push your limits and awaken your curiosity.

The ? Cube Challenge is not for the faint-hearted. It is a multi-layered, complex puzzle that requires you to use all your hacking and analytical skills to solve it.

The cube is loaded with riddles and puzzles that must be solved one by one to progress further towards the ultimate goal.

This challenge is not just about solving a puzzle, it's about exploring your curiosity and pushing the boundaries of your knowledge.

It's about putting your hacker mindset to work and seeing how far you can go.

With each step, you'll be one step closer to unlocking the secrets of the ? Cube Challenge. We know that Defcon attendees are always looking for the next big challenge, and we have created the ? Cube Challenge with that in mind.

It is a contest that will test your limits, engage your creativity, and push your curiosity to the next level. So come and join us at Defcon 31 and take on the ultimate challenge! Who knows, you might just walk away with the title of ? Cub Champion and the admiration of your fellow hackers. Are you ready to take the challenge?

The above was totally written by ChatGPT. I don't want to give out too much information, but basically there is going to be a big cube like object that contestants will have to deconstruct to find the hidden awesomeness. I hope to have challenges spread across multiple domains, both online in a jeopardy style ctf as well as the physical puzzle of the cube which will be module in nature, with each physical puzzle tying to the next.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: ? Cube

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Are you ready to put your problem-solving skills to the test?

This year, we are proud to introduce a brand new contest, designed to push your limits and awaken your curiosity.

The ? Cube Challenge is not for the faint-hearted. It is a multi-layered, complex puzzle that requires you to use all your hacking and analytical skills to solve it.

The cube is loaded with riddles and puzzles that must be solved one by one to progress further towards the ultimate goal.

This challenge is not just about solving a puzzle, it's about exploring your curiosity and pushing the boundaries of your knowledge.

It's about putting your hacker mindset to work and seeing how far you can go.

With each step, you'll be one step closer to unlocking the secrets of the ? Cube Challenge. We know that Defcon attendees are always looking for the next big challenge, and we have created the ? Cube Challenge with that in mind.

It is a contest that will test your limits, engage your creativity, and push your curiosity to the next level. So come and join us at Defcon 31 and take on the ultimate challenge! Who knows, you might just walk away with the title of ? Cub Champion and the admiration of your fellow hackers. Are you ready to take the challenge?

The above was totally written by ChatGPT. I don't want to give out too much information, but basically there is going to be a big cube like object that contestants will have to deconstruct to find the hidden awesomeness. I hope to have challenges spread across multiple domains, both online in a jeopardy style ctf as well as the physical puzzle of the cube which will be module in nature, with each physical puzzle tying to the next.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: ? Cube

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Are you ready to put your problem-solving skills to the test?

This year, we are proud to introduce a brand new contest, designed to push your limits and awaken your curiosity.

The ? Cube Challenge is not for the faint-hearted. It is a multi-layered, complex puzzle that requires you to use all your hacking and analytical skills to solve it.

The cube is loaded with riddles and puzzles that must be solved one by one to progress further towards the ultimate goal.

This challenge is not just about solving a puzzle, it's about exploring your curiosity and pushing the boundaries of your knowledge.

It's about putting your hacker mindset to work and seeing how far you can go.

With each step, you'll be one step closer to unlocking the secrets of the ? Cube Challenge. We know that Defcon attendees are always looking for the next big challenge, and we have created the ? Cube Challenge with that in mind.

It is a contest that will test your limits, engage your creativity, and push your curiosity to the next level. So come and join us at Defcon 31 and take on the ultimate challenge! Who knows, you might just walk away with the title of ? Cub Champion and the admiration of your fellow hackers. Are you ready to take the challenge?

The above was totally written by ChatGPT. I don't want to give out too much information, but basically there is going to be a big cube like object that contestants will have to deconstruct to find the hidden awesomeness. I hope to have challenges spread across multiple domains, both online in a jeopardy style ctf as well as the physical puzzle of the cube which will be module in nature, with each physical puzzle tying to the next.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: "You can't cheat time" - Finding foes and yourself with latency trilateration

When: Friday, Aug 11, 14:30 - 14:50 PDT

Where: Harrah's - Nevada Ballroom - Lake Tahoe & Reno - War Stories - On the Record - [Map](#)

SpeakerBio: Lorenzo "lopoc" Cococcia, Hacker

Lorenzo Cococcia was born and raised in Italy, the son of two worlds: computer science and physics. Specialized in malware analysis, cyber security and threat intelligence, Lorenzo began his career as a threat intelligence analyst for large industrial companies, where he developed a rigorous approach to the field. He is particularly interested in the intersection of physics and mathematics with the world of hacking and cyber security.

Twitter: [@lopoc_](#)


Description:

Since the dawn of time, humans have been driven to discover new ways of determining their location, and the location of potential threats. In the realm of cyber threat intelligence, the ability to geolocate servers, for instance the one a C2 is running on, is crucial.

As a research in its early stages, this speech will delve into the exciting world of offensive geolocation. By leveraging inviolable physical laws, we can measure the time it takes for a signal to travel from an adversary to multiple network sensors, and use this information to accurately calculate their position. This technique is known as latency trilateration has never been used before in the cyber realm, and has significant implications for threat intelligence, sandbox evasion, and even malware self-geolocation. I will also discuss potential limitations and challenges of this approach, as well as its broader implications and potential future developments in this emerging field.

REFERENCES

Ben Du, Massimo Candela, Bradley Huffaker, Alex C. Snoeren, and kc claffy. 2020. RIPE IPmap active geolocation: mechanism and performance evaluation. SIGCOMM Comput. Commun. Rev. 50, 2 (April 2020), 3–10.
<https://doi.org/10.1145/3402413.3402415>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: (In)Direct Syscalls: A Journey from High to Low

When: Saturday, Aug 12, 11:00 - 16:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 1 - [Map](#)

SpeakerBio: Daniel Feichter

No BIO available

Twitter: [@VirtualAllocEx](#)

Description:

Our workshop/journey will be called "(In)direct Syscalls: A Journey from High to Low". It is a hands-on experience where we start with some Windows internals basics, talk about system calls in Windows OS in general, take a look at Win32 APIs, Native APIs, etc. We also take a look at the concepts of direct syscalls and indirect syscalls. Based on various chapters, each student will build their own indirect syscall shellcode loader step by step and analyze it a bit with x64dbg. Below is an overview of the chapters covered in the workshop.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: (n)Map Exploration: A Great Time in Remote Destinations

When: Saturday, Aug 12, 11:30 - 12:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Main Stage - [Map](#)

SpeakerBio:SamunoskeX

SamunoskeX is an Information Security Professional who works as part of a Security Operations Team and is also an Information Security instructor at a college. He is a Blue Team enthusiast and enjoys sharing all things Blue Team with the world.

SamunoskeX has attended DEFCON Events since DC26.

Description:

Can we find activity within the corporate network that might be suspicious?

Can we find activity within the corporate network that might be suspicious?

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: #NoFilter: Abusing Windows Filtering Platform for privilege escalation

When: Sunday, Aug 13, 12:00 - 12:45 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

SpeakerBio: Ron Ben-Yizhak , Security Researcher at Deep Instinct

Ron Ben-Yizhak is a security researcher at Deep Instinct.

He is responsible for research of malware campaigns, attack surfaces and vectors and evasion techniques. His findings are used for developing new analysis, detection, and mitigation capabilities.

Ron joined Deep Instinct in 2019 after serving as a security researcher and forensics specialist in one of the IDF's elite cyber units.

Twitter: [@RonB_Y](#)

Description:

Privilege escalation is a common attack vector in the Windows OS.

Today, there are multiple offensive tools in the wild that can execute code as “NT AUTHORITY\SYSTEM” (Meterpreter, CobaltStrike, Potato tools), and they all usually do so by duplicating tokens and manipulating services in some way or another. This talk will show an evasive and undetected privilege escalation technique that abuses the Windows Filtering Platform (WFP). This platform processes network traffic and allow configuring filters that permit or block communication.

It is built-in component of the operating system since Windows Vista, and doesn't require an installation. My research started from reverse-engineering a single RPC method in an OS service and ended with several techniques to abuse a system kernel component, that allow executing programs as “NT AUTHORITY\SYSTEM”, as well as other users that are logged on the the machine without triggering any traditional detection algorithms.

The various components of the Windows Filtering Platform will be analyzed, such as the Basic Filtering Engine, the TCPIP driver and the IPSec protocol, while focusing on how to abuse them and extract valuable data from them.

REFERENCES

- <https://googleprojectzero.blogspot.com/2021/08/understanding-network-access-windows-app.html>
- <https://scorpiosoftware.net/2022/12/25/introduction-to-the-windows-filtering-platform/>
- <https://learn.microsoft.com/en-us/windows/win32/fwp/windows-filtering-platform-architecture-overview>
- [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759130\(v=ws.10\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759130(v=ws.10))

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: 125khz the Brown note for Cars

When: Saturday, Aug 12, 13:00 - 13:59 PDT

Where: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

SpeakerBio: Woody

Infrared Tracking, Gotenna Exploits, and Raptor Captor. He is also staff for the RF Village, probably luck. He has also been know to watch Burn Notice, but doesn't eat at much yogurt as Zero.

Twitter: [@tb69rr](#)

Description:

I will demonstrate how to use LF 125-137 khz to make vehicles and their components play nice together. Using LF to make TPMS and Keyfobs spit out their info. We will show how to do this and how to check the responses. Think of being able to make TPMS and Keyfobs spit their data out at will. I will show how to use everything from a Proxmark to a hackrf to make this happen. I'll also demo antennas and hardware mods we recommend.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: 156 million targeted: Biggest social phishing cyberattacks during Brazil's election

When: Saturday, Aug 12, 14:30 - 14:59 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Douglas Bernardini

Cybersecurity professional with degrees from FGV/Brazil & specializations from Insper/Brazil and Harvard/USA. Leading a data privacy consulting firm, specializing in cloud assessment, pentest, OSINT, SOC implementation, SIEM configuration, and cloud security. An accomplished author, speaker, professor, and researcher with editorial roles in cyber0.io blog. Active member of OWASP and the Linux Foundation. Currently a trust advisor in corporate cybersecurity for banks, retail, industries, and insurance companies. Boasts a vast physical library of 100+ cybersecurity books and a digital collection of 100,000+ documents on hacking, cloud computing, DevSecOps, SIEM, Cyberdefense, Digital forensics, and cryptography. Holds +8 cybersecurity, cloud computing, and ethical hacking certifications.

Description:

In the era of digitalization, the world has witnessed an unprecedented increase in cyber threats, particularly during crucial events such as elections. Today, we delve into a significant case study that shook the Brazilian political landscape and shed light on the immense challenges posed by social phishing cyberattacks.

As we all know, Brazil's elections are not only a matter of national importance but also hold global significance. The ability to conduct free and fair elections is the cornerstone of any democratic society. However, in recent years, cybercriminals have exploited the vulnerability of social media platforms and unleashed sophisticated phishing attacks to manipulate public opinion and disrupt the democratic process.

In this presentation, we focus on the largest social phishing cyberattacks ever recorded during Brazil's election, where a staggering 156 million individuals were specifically targeted. These attacks, meticulously orchestrated and strategically timed, aimed to deceive and manipulate voters by spreading disinformation, creating confusion, and influencing their decision-making process.

We will explore the modus operandi of the cybercriminals behind these attacks, the techniques they employed to infiltrate the social media landscape, and the sophisticated psychological tactics utilized to exploit the vulnerabilities of the unsuspecting public. Moreover, we will analyze the significant consequences of these cyberattacks on the political climate, public trust, and the overall integrity of the electoral process.

Throughout this presentation, we will also discuss the challenges faced by government authorities, law enforcement agencies, and technology companies in countering such threats. From advanced artificial intelligence algorithms to public awareness campaigns, we will explore various strategies implemented to mitigate the impact of social phishing cyberattacks and safeguard the democratic principles that Brazil holds dear.

By examining this case study, we aim to shed light on the growing need for enhanced cybersecurity measures, international collaboration, and comprehensive policies to prevent the recurrence of such incidents in future elections, not only in Brazil but also across the globe. It is essential for all stakeholders to understand the gravity of these threats and work together to fortify our digital ecosystems against cybercriminals seeking to undermine the very foundations of democracy.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: 2024 Election Threat Landscape

When: Saturday, Aug 12, 15:30 - 16:20 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

Speakers: Catherine Terranova, Hallie Stern, Rebecca Scott Thein, Sandra Khalil, Sarah Amos

SpeakerBio: Catherine Terranova

Catherine Terranova is the Vice President of Operations at the Election Integrity Foundation, the 501(c)(3) organization founded by world renown ethical hacker Harri Hursti. She co-organized the Voting Village at DEFCON 29, DEFCON 30, and DEFCON 31. She is a Columbia University alumna and researcher whose current focus is on cyber security and election integrity with an emphasis on data and voting rights.

Twitter: [@catlovesvoting](#)

SpeakerBio: Hallie Stern

Hallie Stern is the Founder and Director of Digital Rapid Response and Information Strategy for Mad Mirror Media, a digital identity and technology consultancy, where she conducts research & development initiatives, teaches courses on disinformation and influence, and investigates anomalies in ad-tech ecosystems and algorithms for her cross-sector, cross-industry clients. She also works with the Disarm Foundation to develop tools and tandards for mitigating online harm related to disinformation and is a member of the Integrity Institute. She holds an M.S. from NYU in Global Security, Conflict, and Cybercrime, where she focused on The Human Side of Cyber Conflict, with practicums and fellowships at The Global Disinformation Index, UMD START, the Dept of State, and the Department of Homeland Security. Additional awards include The David L. Boren National Security Fellowship. Prior to her studies, Hallie spent a year exploring digital communication and data surveillance in Africa, the Mediterranean, and South East Asia.

SpeakerBio: Rebecca Scott Thein

Rebecca Scott Thein is an experienced product, program and people manager at the intersection of society, responsible product development and accessible design. Rebecca was most recently a Senior Technical Program Manager at Twitter, where she oversaw the globalization efforts of civic and crisis response work, including the Brazil & US midterm elections, Covid misinformation and the conflict in Ukraine. Additionally, she oversaw all harmful & illegal content (IP, terrorism & coordinated harmful group activity, Information Operations, and csam/abuse. Rebecca became a recent Digital Sherlock Scholar through the Atlantic Council's Digital Forensics Research Lab, serves as a Visiting Fellow for the Integrity Institute and acts as a Responsible Tech Advisor for All Tech is Human.

SpeakerBio: Sandra Khalil

Sandra Khalil manages strategic partnerships for All Tech is Human, a global responsible technology nonprofit organization based in New York. Before her time at All Tech Is Human, she spent eight years working in federal, municipal, and think tank roles making people-to-people connections and amplifying globally underrepresented voices. Sandra holds a Master of Science in Global Security, Conflict, and Cyber from New York University with a concentration on cyber policy. Her interests are at the nexus of people, technology, and democracy, with the end user being the most critical stakeholder and driver of innovation for a safer, equitable, and inclusive tech future.

SpeakerBio: Sarah Amos

Sarah Amos is a former journalist turned product manager with nearly a decade of experience contributing to the development and optimization of AI-enabled informational products for start-ups, Fortune 500 companies and the public sector. Most recently she worked closely with Twitter's Trust and Safety Team as a product manager for Civic Integrity, building features to mitigate the harms of platform manipulation, misinformation and abuse during global election cycles. Before that she founded and led the R&D Department at Dataminr, an AI platform that detects the earliest signals of high-impact events and emerging risks from open source data.

Twitter: [@sarah3amos](#)

Description:

This panel is a comprehensive overview on the most pressing threats to public confidence in 2024 election outcomes. The panel is intended to answer questions such as, “What threats since 2020 still remain? How have they evolved? What new threats have emerged that were not present before? And how might the 2024 elections face challenges different from the past? What should voters, election officials, journalists and tech platforms be paying attention to?” The panel will address infrastructure foundations in election administration (election officials; voting technology); foreign threats; the disinformation ecosystem; and new technologies such as generative AI.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: 5n4ck3y

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

AND!XOR creates electronic badges that are filled with challenges. We love doing this, especially coming up with unique ways for hackers to earn them. We are excited to re-introduce the newest member of our hacker-fam... 5n4ck3y (Snackey). 5n4ck3y is a vending machine hardware hacking project, retrofitted into an IoT CTF based badge dispensing machine, complete with bling. To earn a badge, you must find a flag on our web hosted CTF platform. Once you have found a flag, you will be given a 5n4ck3y dispense code. Enter the code into the vending machine and a badge will be dispensed to you! There are a variety of challenges to earn a badge, as well as challenges to continue working on the badge itself once obtained. These span from hardware hacking, reverse engineering, OSINT, OS & network security to name a few. Hardware hacking is our passion and we want people to learn on badges. But more importantly, there is a lot to learn at DEF CON, so our challenge will hopefully serve a desire to learn something new and meet new friends while trying to earn a badge and hack it further. We hope you enjoy 5n4ck3y and all that it has to offer!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT

Title: 5n4ck3y

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

AND!XOR creates electronic badges that are filled with challenges. We love doing this, especially coming up with unique ways for hackers to earn them. We are excited to re-introduce the newest member of our hacker-fam... 5n4ck3y (Snackey). 5n4ck3y is a vending machine hardware hacking project, retrofitted into an IoT CTF based badge dispensing machine, complete with bling. To earn a badge, you must find a flag on our web hosted CTF platform. Once you have found a flag, you will be given a 5n4ck3y dispense code. Enter the code into the vending machine and a badge will be dispensed to you! There are a variety of challenges to earn a badge, as well as challenges to continue working on the badge itself once obtained. These span from hardware hacking, reverse engineering, OSINT, OS & network security to name a few. Hardware hacking is our passion and we want people to learn on badges. But more importantly, there is a lot to learn at DEF CON, so our challenge will hopefully serve a desire to learn something new and meet new friends while trying to earn a badge and hack it further. We hope you enjoy 5n4ck3y and all that it has to offer!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

Title: 5n4ck3y

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

AND!XOR creates electronic badges that are filled with challenges. We love doing this, especially coming up with unique ways for hackers to earn them. We are excited to re-introduce the newest member of our hacker-fam... 5n4ck3y (Snackey). 5n4ck3y is a vending machine hardware hacking project, retrofitted into an IoT CTF based badge dispensing machine, complete with bling. To earn a badge, you must find a flag on our web hosted CTF platform. Once you have found a flag, you will be given a 5n4ck3y dispense code. Enter the code into the vending machine and a badge will be dispensed to you! There are a variety of challenges to earn a badge, as well as challenges to continue working on the badge itself once obtained. These span from hardware hacking, reverse engineering, OSINT, OS & network security to name a few. Hardware hacking is our passion and we want people to learn on badges. But more importantly, there is a lot to learn at DEF CON, so our challenge will hopefully serve a desire to learn something new and meet new friends while trying to earn a badge and hack it further. We hope you enjoy 5n4ck3y and all that it has to offer!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A Broken Marriage: Abusing Mixed Vendor Kerberos Stacks

When: Saturday, Aug 12, 16:00 - 16:20 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

SpeakerBio: Ceri Coburn , Red Team Operator & Offensive Security Dev at Pen Test Partners

After a 20 career within the software development space, Ceri was looking for a new challenge and moved into pen testing back in 2019. During that time he has created and contributed to several open source offensive tools such as Rubeus, BOFNET and SweetPotato and on the odd occasion contributed to projects on the defensive side too. He current works as a red team operator and offensive security dev at Pen Test Partners.

Twitter: [@_EthicalChaos_](#)

Description:

The Windows Active Directory authority and the MIT/Heimdal Kerberos stacks found on Linux/Unix based hosts often coexist in harmony within the same Kerberos realm. This talk and tool demonstration will show how this marriage is a match made in hell. Microsoft's Kerberos stack relies on non standard data to identify it's users. MIT/Heimdal Kerberos stacks do not support this non standard way of identifying users. We will look at how Active Directory configuration weaknesses can be abused to escalate privileges on *nix based hosts joined to the same Active Directory authority. This will also introduce an updated version of Rubeus to take advantage of some of these weaknesses.

REFERENCES

- * <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/sam-name-impersonation/ba-p/3042699> *
- <https://www.catalyst.net.nz/blog/stay-curious-dollar-ticket-security-issue> *
- <https://exploit.ph/cve-2021-42287-cve-2021-42278-weaponisation.html> *
- https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-kile/6435d3fb-8cf6-4df5-a156-1277690ed59c

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A Comprehensive Review on the Less-Traveled Road: 9 Years of Overlooked MikroTik Pre-Auth RCE

When: Friday, Aug 11, 15:30 - 16:15 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

SpeakerBio: NiNi Chen, Security Researcher at DEVCORE

Ting-Yu Chen, aka NiNi, is a security researcher at DEVCORE and a member of the Balsn CTF team. He won the title of the "Master of Pwn" at Pwn2Own Toronto 2022 with the DEVCORE team. NiNi has also made notable achievements in CTF competitions, including placing 2nd and 3rd in DEF CON CTF 27 and 28 as a member of HITCON BFKinesiS and HITCON Balsn teams, respectively. NiNi is currently immersed in vulnerability research and reverse engineering, continuing to hone his skills. You can keep up with his latest discoveries and musings on Twitter via his handle @terrynini38514 or blog at <http://blog.terrynini.tw/>.

Twitter: [@terrynini38514](#)

Description:

MikroTik, as a supplier of network infrastructures, its products and RouterOS are adopted widely. Currently, at least 3 million+ devices are running RouterOS online. Being the target research by attackers actively, the exploits leaked from the CIA in 2018 and the massive exploits that followed are samples of the havoc that can be caused when such devices are maliciously exploited again. Therefore, RouterOS also attracts many researchers to hunt bugs in it. However, there are rarely high-impact vulnerabilities reported over a long period. Can the OS become perfect overnight? Of course not. Some details have been missed.

Researches on RouterOS were mainly against jailbreak, Nova Message in IPC, and analysis of exploits in the wild. Especially researches against Nova Message have reported tons of post-auth vulnerabilities. However, the architecture design and the lower-layer objects, which are closely related to the functionality of Nova Binary, were being neglected due to their complexity, causing some details to be overlooked for a long time. Starting by introducing the mechanisms of the socket callback and the remote object, we will disclose more about the overlooked attack surface and implementations in RouterOS. Moreover, we will discuss how we, at the end of rarely visited trails, found the pre-auth RCE that existed for nine years and can exploit all active versions and the race condition in the remote object. We will also share our methodology and vulnerability patterns.

Delving into the design of the RouterOS, attendees will have a greater understanding of the overlooked attack surface and implementation of it and be able to review the system more reliably. Additionally, we will also share our open-source tools and methodology to facilitate researchers researching RouterOS, making it less obscure. , Ting-Yu Chen, aka NiNi, is a security researcher at DEVCORE and a member of the Balsn CTF team. He won the title of the "Master of Pwn" at Pwn2Own Toronto 2022 with the DEVCORE team. NiNi has also made notable achievements in CTF competitions, including placing 2nd and 3rd in DEF CON CTF 27 and 28 as a member of HITCON BFKinesiS and HITCON Balsn teams, respectively. NiNi is currently immersed in vulnerability research and reverse engineering, continuing to hone his skills. You can keep up with his latest discoveries and musings on Twitter via his handle @terrynini38514 or blog at <http://blog.terrynini.tw/>.

REFERENCES

- ◇ https://kirils.org/slides/2017-10-21_MT_Hacktivity_pub.pdf
- ◇ https://kirils.org/slides/2017-09-15_prez_15_MT_Balcon_pub.pdf
- ◇ https://mum.mikrotik.com/presentations/ID18/presentation_6149_1540240927.pdf
- ◇ <https://medium.com/@maxi./finding-and-exploiting-cve-2018-7445-f3103f163cc1>
- ◇ <https://www.coresecurity.com/core-labs/advisories/mikrotik-routeros-smb-buffer-overflow>
- ◇ <https://www.irongeek.com/i.php?page=videos/derbycon8/track-4-15-bug-hunting-in-routeros-jacob-baines>
- ◇ <https://www.tenable.com/blog/tenable-research-advisory-multiple-vulnerabilities-discovered-in-mikrotiks-routeros>
- ◇ <https://www.tenable.com/security/research/tra-2018-21>
- ◇ <https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Jacob-Baines>
- ◇ <https://www.tenable.com/security/research/tra-2019-46>
- ◇ <https://medium.com/tenable-techblog/routeros-chain-to-root-f4e0b07c0b21>

- ◇ <https://margin.re/2022/06/pulling-mikrotik-into-the-limelight/>
 - ◇ https://github.com/cq674350529/pocs_slides
 - ◇ <https://www.youtube.com/watch?v=fkigIIDE6vs>
 - ◇ <https://www.tenable.com/security/research/tra-2019-46>
 - ◇ <https://community.arm.com/arm-community-blogs/b/architectures-and-processors-blog/posts/caches-and-self-mod>
 - ◇ https://github.com/Cisco-Talos/Winbox_Protocol_Dissector
 - ◇ <https://github.com/BigNerd95/RouterOS-Backup-Tools>
 - ◇ <https://github.com/BigNerd95/Chimay-Red>
 - ◇ <https://github.com/BigNerd95/Chimay-Blue>
 - ◇ <https://github.com/0ki/mikrotik-tools>
 - ◇ <https://github.com/tenable/routeros>
-



[Return to Index](#) - Add to - ics [Calendar](#) file

Title: A Different Uber Post Mortem

When: Friday, Aug 11, 10:00 - 10:45 PDT

Where: Harrah's - Nevada Ballroom - Lake Tahoe & Reno - War Stories - On the Record - [Map](#)

SpeakerBio: Joe Sullivan

Joe Sullivan is the CEO of Ukraine Friends, a nonprofit providing humanitarian aid to the people of Ukraine. He also advises a number of startups and mentors security leaders. Joe has worked at the intersection of government, technology, and security since the mid-1990s. He spent 8 years working for the US DOJ, eventually as a federal prosecutor 100% focused on technology-related crimes, received national recognition from the DOJ for outstanding service as a federal prosecutor, and worked on many first-of-their-kind cybercrime cases, including supporting the digital aspects of the 9/11 investigation. Joe was recruited to eBay in 2002 to build out their eCrime team, and later took on responsibilities at PayPal. In 2008 Joe moved to Facebook where he became their CSO, building a small security org into a team of hundreds. He was recruited from there to join Uber in 2015 to be their first CSO. After Uber, Joe spent 2018 through 2022 as the CSO at Cloudflare. He has also advised a significant number of companies over the years, including AirBnB and DoorDash. Joe has testified as an expert before the US Congress twice, been a commissioner on the National Action Alliance for Suicide Prevention, a board member on the National Cyber Security Alliance, a many-time opening plenary speaker at the Dallas Crimes Against Children Conference, a participant in a White House anti-online-bullying effort, an advisor to the Department of Homeland Security, and in 2016 accepted an appointment from President Obama to his Commission on Enhancing National Cybersecurity.

Description:

The federal criminal case of United States v. Joseph Sullivan, NDCA 3-20-CR-337 WHO, has been covered and debated quite publicly since I was fired by the new Uber CEO in November 2017, a year after the incident. Most discussion has focused on questions of my guilt or innocence, the culpability of other executives at the company, and the implications of the case for other security executives.

Less has been written about the guilt or innocence of those who accessed Uber's AWS environment in October 2016 and triggered an incident response by emailing me and asking for payment. After we met them, my team and I did not consider those 19- and 20-year-old kids to be criminal actors and treated them as security researchers. Yet both also faced federal criminal charges.

During my talk I will review the extraordinary investigation done by my team at Uber and put it into the context of other historical cases we and I had worked on. Whether or not you consider them to be security researchers, there are many lessons to be learned related to the dynamics between researchers and companies and the dynamics between companies and the government.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A Few Useful Lessons about AI Red Teaming

When: Friday, Aug 11, 14:00 - 14:55 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

SpeakerBio: Ram Shankar Siva Kumar

No BIO available

Description:

This talk captures the lessons learned from red teaming production AI systems from Microsoft and Google. We contextualize how red teaming AI systems is similar yet different from red teaming traditional software systems, and distill 10 lessons from a practitioner's perspective. Whether you are considering a career change into red teaming AI systems, or subverting AI systems for fun/twitter clout or simply want to cash in on the AI bug bounties for profit, these lessons on attacking AI systems applies to you.

The 10 lessons are:

Lesson 1: Red Teaming AI systems means different things to different communities Lesson 2: AI Red Teaming is somewhere in the middle Lesson 3: AI Red Teaming is a shared responsibility with a different process Lesson 4: Red Teaming AI models is different from red teaming AI applications Lesson 5: There are novel security risks to look out for.... Lesson 6: ...But do not forget traditional security Lesson 7: The goal of the AI Red Team is not to find all the different ways AI systems fail Lesson 8: You do not need to be a math whiz to red team AI system Lesson 9: AI Red Team needs a diverse set of skills in the team Lesson 10: There is so much to do before you start red teaming your AI system

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A Fireside Chat with Chris Roberts and Pete Cooper

When: Saturday, Aug 12, 16:30 - 16:55 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Speakers:Chris Roberts,Pete Cooper

SpeakerBio:Chris Roberts

Chris is the CISO for Boom Supersonic and works as an advisor for several entities and organizations around the globe. His most recent projects are focused within the aerospace, deception, identity, cryptography, Artificial Intelligence, and services sectors. Over the years, he's founded or worked with several folks specializing in OSINT/SIGINT/HUMINT research, intelligence gathering, cryptography, and deception technologies. These days he's working on spreading the risk, maturity, collaboration, and communication word across the industry. (Likely while coding his EEG driven digital clone that's monitoring his tea and biscuit consumption!)

Since the late 90's Chris has been deeply involved with security R&D, consulting, and advisory services in his quest to protect and defend businesses and individuals against various types of attack. Prior to that he jumped out of planes for a living, visiting all sorts of interesting countries and cultures while doing his best to avoid getting shot at too often. (Before that, he managed to get various computers confiscated by several European entities.)

He's considered one of the world's foremost experts on counter threat intelligence and vulnerability research within the Information Security industry. He's also gotten a name for himself in the transportation arena, basically anything with wings, wheels, tracks, tyres, fins, props or paddles has been the target for research for the last 15 years. (To interesting effect.)

Twitter: [@Sidragon1](#)

SpeakerBio:Pete Cooper

No BIO available

Description:

Join Pete Cooper in a fireside chat with Chris Roberts about his role as the CISO for Boom Supersonic and how he is approaching the challenges of securing a flying platform from the ground up using everything from digital twins to AI. It will also be a chance to discuss what he has learnt across his career and his advice for the next generation coming through.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A Fireside Chat with the TSA Administrator

When: Friday, Aug 11, 15:00 - 15:50 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Speakers:David Pecoske, Steve Luczynski

SpeakerBio:David Pecoske , Administrator at Transportation Security Administration (TSA)

David Pecoske was first confirmed by the U.S. Senate as the Transportation Security Administration's seventh administrator in August 2017 and was reconfirmed for a second term in September 2022.

Pecoske leads a workforce of over 60,000 employees and is responsible for security operations at nearly 440 airports throughout the United States. TSA is also the lead federal agency for security of highways, railroads, mass transit systems and pipelines. Under his leadership, TSA improved transportation security through close partnerships and alliances, a culture of innovation, and development of a dedicated workforce.

During his tenure as TSA Administrator, Pecoske also served at the Department of Homeland Security as Acting Secretary from January 20 to February 2, 2021, and as the Senior Official Performing the Duties of Deputy Secretary from April to November 2019, and again from February to June 2021. At the Department, Pecoske helped lead a unified national effort to ensure the continued security of the United States, coordinating components with missions ranging from prevention and protection to recovery and response. He was also a commissioner on the Cyberspace Solarium Commission that developed a consensus on a strategic approach to defending the United States in cyberspace against attacks of significant consequence.

Before joining TSA, Pecoske was an executive in the government services industry, where he led teams that provided counterterrorism, security and intelligence support services to government agencies.

Pecoske served as the 26th Vice Commandant of the U.S. Coast Guard, culminating a Coast Guard career that included extensive operational and command experience. As the Vice Commandant, Pecoske was second in command, also serving as Chief Operating Officer and Component Acquisition Executive of the Coast Guard. He is a recognized expert in crisis management, strategic planning, innovation, and aviation, surface transportation and maritime security. In addition, he has been twice awarded the Homeland Security Distinguished Service Medal.

Pecoske holds a Master of Business Administration from the Massachusetts Institute of Technology, a Master of Public Administration from Columbia University and a Bachelor of Science from the U.S. Coast Guard Academy.

Twitter: [@TSA_Pecoske](#)

SpeakerBio:Steve Luczynski

No BIO available

Description:

Join Steve Luczynski in a fireside chat with with David Pecoske, Administrator of the Transportation Security Administration.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A global approach to tackling software resilience

When: Friday, Aug 11, 15:00 - 16:50 PDT

Where: Caesars Forum - Summit - 221-222 - Policy Atrium - [Map](#)

Speakers: Allan Friedman, Camille Stewart Gloster, Charlie Gladstone, David Rogers

SpeakerBio: Allan Friedman, Senior Advisor and Strategist at Cybersecurity and Infrastructure Security Agency (CISA) Dr. Allan Friedman is the guy who won't shut up about SBOM. A Senior Advisor and Strategist at the Cybersecurity and Infrastructure Security Agency, he coordinates the global cross-sector community efforts around software bill of materials (SBOM) and related vulnerability initiatives, and works to advance their adoption inside the US government. He was previously the Director of Cybersecurity Initiatives at NTIA, leading pioneering work on vulnerability disclosure, SBOM, and IOT. Prior to joining the Federal government, Friedman spent over a decade as a noted information security and technology policy scholar at Harvard's Computer Science department, the Brookings Institution, and George Washington University's Engineering School. He is the co-author of the popular text "Cybersecurity and Cyberwar: What Everyone Needs to Know," has a degree in computer science from Swarthmore College and a PhD in public policy from Harvard University. He is quite friendly for a failed-professor-turned-technocrat.

SpeakerBio: Camille Stewart Gloster, Deputy National Cyber Director at Technology and Ecosystem Security Division, Office of the National Cyber Director
Camille Stewart Gloster, Esq. is the Deputy National Cyber Director for Technology & Ecosystem for The White House. In her role, Camille leads technology, supply chain, data security, and cyber workforce and education efforts for the Office of the National Cyber Director. Camille is a cyber, technology, and national security strategist and policy leader whose career has spanned the private, public, and non-profit sectors. She joined ONCD from Google, where she most recently served as Global Head of Product Security Strategy, and before that as Head of Security Policy and Election Integrity for Google Play and Android.

Prior to working at Google, Camille led cyber diplomacy, technology policy, privacy, and technical policy areas like encryption and PNT as the Senior Policy Advisor for Cyber, Infrastructure & Resilience at the U.S. Department of Homeland Security. During her time at DHS, Camille led campaigns, international engagements, and policy development that bolstered national and international cyber resilience. Those policies include Presidential Policy Directive 41 (PPD – 41) on federal cyber incident coordination, supporting Privacy Shield negotiations, and the 2016 Cybersecurity National Action Plan (CNAP) which outlined 75 tasks to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security. Camille has also held leadership roles focused on cyber and technology on Capitol Hill, at Deloitte, and Cyveillance, an open-source threat intelligence company.

SpeakerBio: Charlie Gladstone, UK Department for Science, Innovation, and Technology
Charlie Gladstone leads the UK Government's work on app store security in the Department for Science, Technology and Innovation. He has worked in tech policy for over five years, where he has specialised in exploring the intersection between technology, society and regulation. Before working in Government, Charlie provided public policy consultancy services to the tech sector clients. He has developed policy on a range of issues including cyber security, digital regulation and artificial intelligence.

SpeakerBio: David Rogers, CEO at Copper Horse
David is a mobile phone and IoT security specialist who runs Copper Horse Ltd, a software and security company based in Windsor, UK. He chairs the Fraud and Security Group at the GSMA. He has spoken at a number of hacking conferences on his security research work including DEF CON's Car Hacking Village, 44CON, B-Sides London, B-Sides Cymru and B-Sides LV. He was awarded an MBE for services to Cyber Security in the Queen's Birthday Honours 2019.

Description:

Software is the lifeblood of the digital world, but as software embeds itself ever further into our societies and economies, the

threat of software attacks grows with it. In our ever-more connected world, Governments are realizing that more must be done to protect businesses, organizations and individuals from these cyber threats. Governments are exploring a range of options to foster software security practices, including convening experts, international organizations and standards, using the power of government purchasing, and even potential regulation. However, the software ecosystem and the risks are rapidly evolving, and require insights into the dynamics of attack and defense from the security and developer communities.

This panel will bring together representatives from governments around the world which are trying to address this challenge. Software risks are global risks, and this will be a unique opportunity to hear how different governments are approaching the issue of software resilience, and discuss how policymakers and the hacker community can to work together to overcome these collective challenges.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A Global Perspective On Election Integrity

When: Friday, Aug 11, 10:30 - 11:25 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

Speakers: Bryson Bort, Chris Krebs, Kendall Spencer, Maia Mazurkiewicz

SpeakerBio: Bryson Bort

Bryson is the Founder of SCYTHE, a start-up building a next-generation threat emulation platform, and GRIMM, a cybersecurity consultancy, and Co-Founder of the ICS Village, a non-profit advancing awareness of industrial control system security. He is a Senior Fellow at the National Security Institute and Adjunct Senior Technical Advisor for the Institute of Security and Technology. As a U.S. Army Officer, he served as a Battle Captain and Brigade Engineering Officer in support of Operation Iraqi Freedom before leaving the Army as a Captain. He was recognized as one of the Top 50 in Cyber by Business Insider, Security Executive Finalist of the Year by SC Media, and a Tech Titan in Washington, DC.

Twitter: [@brysonbort](#)

SpeakerBio: Chris Krebs

Chris Krebs is the Senior Official Performing the Duties of the Under Secretary for the National Protection and Programs Directorate in the Department of Homeland Security, where he oversees the cyber and physical infrastructure security mission for the Department. He is concurrently filling the role of Assistant Secretary for the Office of Infrastructure Protection, to which he was appointed by the President in August 2017. As Assistant Secretary, he leads NPPD's mission on issues such as preventing complex mass attacks, securing high-risk chemicals, and other areas related to cyber and physical infrastructure resilience. This includes serving as the national coordinator for the critical infrastructure security and resilience mission and directly managing 6 of the 16 critical infrastructure sectors outlined in the National Infrastructure Protection Plan. The 16 sectors cover a complex and interconnected range of infrastructure, such as commercial facilities, emergency services, chemical facilities, nuclear facilities and government facilities including the 2017 addition of an election infrastructure subsector. Mr. Krebs joined the Department of Homeland Security in March 2017, serving as Senior Counselor to the Secretary, where he advised DHS leadership on a range of cybersecurity, critical infrastructure protection, and national resilience issues. Prior to coming to DHS, Krebs was a member of Microsoft's US Government Affairs team as Director for Cybersecurity Policy, where he led Microsoft's U.S. policy work on cybersecurity and technology issues. Before Microsoft, Krebs advised industry and Federal, State, and local government customers on range of cybersecurity and risk management issues. This the second time he has worked at the Department, previously serving as Senior Advisor to the Assistant Secretary for Infrastructure Protection and playing a formative role in a number of national and international risk management programs. He holds a Bachelors in Environmental Sciences from the University of Virginia and a J.D. from the Antonin Scalia Law School at George Mason University.

Twitter: [@CISAKrebs](#)

SpeakerBio: Kendall Spencer

Kendall Spencer is an associate in the Intellectual Property Department. Kendall is based in the Boston office where he is a member of the Technology Transactions, Cybersecurity, and Privacy Practice Group. In his previous position as a law clerk, Kendall specialized in Complex Litigation. He also has a strong focus on technology law. Kendall has advised on blockchain technology integration, researched blockchain voting regulations, and investigated the use of blockchain technology to create a database of information on its advantages and efficacy. Additionally, he assisted in drafting an article regarding data privacy issues within real estate law. Kendall serves as a member of the Executive Leadership Team with the National Governing Body of USA Track and Field (USATF), as well as a board member with the National Collegiate Athletic Association (NCAA). As a professional athlete on the U.S. Olympic Team, he has earned accolades such as USA Indoor Bronze Medalist, NCAA National Champion, on top of serving as a USA Track and Field board member.

Twitter: [@Kspencer24](#)

SpeakerBio: Maia Mazurkiewicz

Maia Mazurkiewicz is an expert on countering disinformation and behavioural changes. She has 15 years of experience in political management, foreign affairs, and communication in administration, business and CSOs. She is a speaker, trainer and

moderator. She believes that we need to change the way we communicate, to introduce more understanding in between humans. She is a Co-founder and Head of StratCom of Alliance4Europe where she deals with strategic communication, to build more diverse internet. She co-founded Future Forces Foundation that is working for more impactful business. She is also Vice-President of the Free European Media Association. In 2017 she co-created Keyboard Warriors in Poland, community that debunks disinformation. Maia is a barrister educated in Poland and the United States. She is actively involved in supporting Ukrainian refugees. Maia cooperated with number of foundations and NGOs where she worked on various projects concerning democratization and political parties trainings in Eastern Europe. She advices clients on strategy building and public affairs, as well as trains on leadership, project management and campaign building.

Twitter: [@MaiaMazurkiewic](https://twitter.com/MaiaMazurkiewic)

Description:

Our keynote panel with special guest moderator former CISA Director Chris Krebs will give audiences a global perspective on democracy and will discuss a variety of topics related to election integrity. This panel will give listeners a comprehensive overview of the election space and will lay the foundation for the rest of our program. Experts from different aspects of the cybersecurity industry will provide colorful insight and intersectional perspectives, giving attendees a holistic understanding of all aspects of election integrity.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A Pain in the NAS: Exploiting Cloud Connectivity to PWN your NAS

When: Friday, Aug 11, 12:30 - 13:15 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

Speakers:Noam Moshe,Sharon Brizinov

SpeakerBio:Noam Moshe , Vulnerability Researcher at Claroty Team82

Noam Moshe is a vulnerability researcher at Claroty Team82. Noam specializes in vulnerability research, web applications pentesting, malware analysis, network forensics and ICS/SCADA security. In addition, Noam presented in well-known Hacking conferences like Blackhat Europe, as well as won Master of Pwn at Pwn2Own Miami 2023.

SpeakerBio:Sharon Brizinov , Director of Security Research at Claroty Team82

Sharon Brizinov leads the Vulnerability Research at Team82, The Claroty Research. He specializes in OT/IoT vulnerability research, has participated in multiple Pwn2Own competitions, won Pwn2Own Miami 2023, and holds a DEFCON black badge.

Description:

Have you ever wondered how you can access your family pictures on your home network-attached storage (NAS) device remotely from your mobile? Do you know how this magic works? At Pwn2Own Toronto 2022, we chained multiple bugs to exploit both Synology and Western Digital NAS devices by abusing vulnerabilities in the device, cloud and the mutual trust between them.

In our research, we reviewed the pairing mechanism of NAS devices with the WD and Synology cloud platforms. To our surprise we discovered that devices authenticate to the cloud using a hardware identifier which is later used by users to remotely access their devices. Using this, we were able to impersonate any given NAS device and perform phishing attacks that yielded us admin rights on any targeted WD or Synology device.

In this talk, we will explain the pairing process of WD and Synology NAS. We will elaborate on the overall architecture of their cloud offering and focus on the vulnerabilities we found including ways to enumerate and impersonate all edge devices using certificate transparency log (CTL), and steal cloud proxy auth tokens. This enabled us to download every file saved on the NAS devices, alter or encrypt them, and bypass NAT/Firewall protection to achieve full remote code execution on all cloud-connected NAS (and to gain \$\$\$ from Pwn2Own).

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A Series of Unfortunate Events

When: Friday, Aug 11, 16:00 - 16:45 PDT

Where: Harrah's - Nevada Ballroom - Lake Tahoe & Reno - War Stories - On the Record - [Map](#)

Speakers: Ben "NahamSec" Sadeghipour, Corben Leo

SpeakerBio: Ben "NahamSec" Sadeghipour, Hacker & Content Creator at NahamSec

Ben Sadeghipour AKA NahamSec is a security researcher and content creator. He's currently in the top 100 for both HackerOne(25) and Bugcrowd's (95) leaderboards. He has helped identify over a thousand vulnerabilities in companies like Amazon, Apple, Airbnb, Lyft, Snapchat and more. Prior to doing content creation full time, he worked as a research and community education executive at Hadrian and HackerOne. Ben has presented many talks and workshops at cons such as DEFCON, BSides, OWASP AppSec, RSA, Red Team Village, and more. He also enjoys hosting and organizing hacker meetups or virtual conferences such as NahamCon and Hacktivitycon!

Twitter: [@nahamsec](#)

SpeakerBio: Corben Leo, Co-Founder at Boring Mattress Co

Corben Leo is a top-100 bug bounty hunter on HackerOne. He's worked with Facebook, Google, Microsoft, Apple, PayPal, Yahoo, Epic Games, AT&T, the Department of Defense, and many more. He's also a co-founder of Boring Mattress Co.

Twitter: [@hacker_](#)

Description:

This talk includes a series of favorite hacking stories. From hacking into a prison system to having the ability to publish "fake news" on a major tech companies website to even breaking into some of the largest entertainment and online casinos. This talk will take a look at the identification, exploitation, and escalation paths as well as the possible impact based on the company's organization and nature of work.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A Slice of Deception: The 2023 #SECVC Debrief

When: Friday, Aug 11, 17:15 - 17:59 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Speakers: JC, Snow

SpeakerBio: JC , President at Snowfenive

JC is one of the two co-founders of the Social Engineering Community and has competed in previous Social Engineering competitions. JC also runs the Vault, a physical security competition held at SAINTCON in Utah. JC's passion for competition as well as innovation has been an exciting avenue for him as he and Snow built the new Social Engineering Community's Vishing Competition.

Twitter: [@JC_SoCal](#)

SpeakerBio: Snow , Chief People Hacker at IBM

Over a decade ago, in a hotel not far away from this very location in Vegas, Snow began her career in Social Engineering. At the very beginning of her journey multiple people told her she couldn't make a career as a dedicated Social Engineer. Through late nights of studying, practice, determination, learning from her mentor, and a lot of spite, she has made a successful career as a Social Engineer. Today, she is the Chief People Hacker for IBM Security's X-Force Red team, where she leads the global Social Engineering practice.

Twitter: [@_sn0ww](#)

Description:

Join the Founders of the Social Engineering Community as they break down this year's Vishing Competition (#SECVC). They'll talk about how the competition is organized, and some of the big takeaways, trends, and surprises (both good and bad) from the OSINT and Vishing Plan reports. They'll also recount some of the highlights from this year's live calls.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A SSLippery Slope: Unraveling the Hidden Dangers of Certificate Misuse

When: Saturday, Aug 12, 14:00 - 14:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio: Bill Demirkapi, Microsoft Security Response Center

Bill is an undergraduate student and a security researcher for the Microsoft Security Response Center with an intense passion for Windows Internals. His interests include reverse engineering and vulnerability research, ranging from low-level memory corruption to systemic flaws with catastrophic consequences. He started his journey in high school and has since published his work at internationally-recognized conferences like DEF CON and Black Hat USA. In his pursuit to make the world a better place, Bill constantly looks for the next significant vulnerability, following the motto "break anything and everything".

Twitter: [@BillDemirkapi](#)

Description:

Digital signatures are fundamental for verifying the authenticity and integrity of untrusted data in the digital world. They ensure that software, firmware, and other digital content are not tampered with during transmission or at rest. Code signing certificates are significantly more challenging to obtain when compared to alternatives like SSL or S/MIME certificates. The latter only has a single criterion- proof of control over a domain, while the former requires significant validation of the publisher itself.

This project uncovered a systemic vulnerability present in numerous signature validation implementations, enabling attackers to exploit valid certificates in an unintended manner. Vulnerable implementations mistakenly perceive files signed with incompatible certificates as legitimate, violating their respective specifications and allowing threat actors to sign untrusted code at little to no cost. In this talk, we will explore the problem at all levels, ranging from the fundamental theory to its application across multiple formats and real-world situations.

REFERENCES

- Boeyen, Sharon, et al. "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." IETF, 1 May 2008, datatracker.ietf.org/doc/html/rfc5280.
- Housley, Russ. "Cryptographic Message Syntax (CMS)." IETF, 5 Sept. 2002, datatracker.ietf.org/doc/html/rfc3369.
- "Windows Authenticode Portable Executable Signature Format." Microsoft.com, Microsoft, 21 Mar. 2008, download.microsoft.com/download/9/c/5/9c5b2167-8017-4bae-9fde-d599bac8184a/authenticode_pe.docx.
- "PE Format - Win32 Apps." Learn.microsoft.com, Microsoft, 31 Mar. 2021, learn.microsoft.com/en-us/windows/win32/debug/pe-format.
- "Trusted Root Certification Authorities Certificate Store." Learn.microsoft.com, Microsoft, 14 Dec. 2021, learn.microsoft.com/en-us/windows-hardware/drivers/install/trusted-root-certification-authorities-certificate-store.
- "What's the Difference between DV, OV & EV SSL Certificates?" Wwww.digicert.com, DigiCert, 23 Aug. 2022, www.digicert.com/difference-between-dv-ov-and-ev-ssl-certificates.
- The OpenSSL Project. OpenSSL: The Open Source Toolkit for SSL/TLS. Apr. 2003.
- Brubaker, Chad, et al. "Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations." 2014 IEEE Symposium on Security and Privacy, 18 May 2014, www.cs.cornell.edu/~shmat/shmat_oak14.pdf, <https://doi.org/10.1109/sp.2014.15>.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Friday - 10:00-17:59 PDT

Title: A-ISAC CTF

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

A-ISAC CTF

A-ISAC and Embry-Riddle Aeronautical University - Prescott

****Laptop Needed****

A variety of aviation infrastructure have been compromised. Immerse yourself into challenges where you are tasked with identifying attacks/attackers, stopping attacks, and restoring normal operations. As a participant your first step is to register ahead and read the rules at: <https://aisac.cyberskyline.com/events/aisac-defcon> and bring your own laptop to the venue. You can participate in the virtual challenges from Friday, but the more critical in-person challenges are only available at certain times during Village open hours!

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Sunday - 10:00-13:59 PDT

Title: A-ISAC CTF

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)


Description:

A-ISAC CTF

A-ISAC and Embry-Riddle Aeronautical University - Prescott

****Laptop Needed****

A variety of aviation infrastructure have been compromised. Immerse yourself into challenges where you are tasked with identifying attacks/attackers, stopping attacks, and restoring normal operations. As a participant your first step is to register ahead and read the rules at: <https://aisac.cyberskyline.com/events/aisac-defcon> and bring your own laptop to the venue. You can participate in the virtual challenges from Friday, but the more critical in-person challenges are only available at certain times during Village open hours!

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Saturday - 10:00-17:59 PDT

Title: A-ISAC CTF

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

A-ISAC CTF

A-ISAC and Embry-Riddle Aeronautical University - Prescott

****Laptop Needed****

A variety of aviation infrastructure have been compromised. Immerse yourself into challenges where you are tasked with identifying attacks/attackers, stopping attacks, and restoring normal operations. As a participant your first step is to register ahead and read the rules at: <https://aisac.cyberskyline.com/events/aisac-defcon> and bring your own laptop to the venue. You can participate in the virtual challenges from Friday, but the more critical in-person challenges are only available at certain times during Village open hours!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Abating the Eye of Sauron: Help Combat Authoritarian Censorship

When: Saturday, Aug 12, 14:00 - 15:50 PDT

Where: Caesars Forum - Summit - 220 - Policy NOT-A-SCIF - [Map](#)

Speakers:David Houston,Michaela Lee

SpeakerBio:David Houston , International Relations Officer, Bureau of Democracy, Human Rights, and Labor at U.S. Department of State

David Houston is a career member of the Foreign Service with the U.S. Department of State, currently working on the Internet freedom team and confronting issues at the nexus of emerging technology and human rights impact. He is a former Army Captain and combat veteran of the war in Afghanistan, and has served at embassies in Beijing, Panama, and Mogadishu.

SpeakerBio:Michaela Lee , Director for Strategy and Research at The Office of National Cyber Director (ONCD)

Michaela Lee is the Director for Strategy and Research at the Office of the National Cyber Director. Prior to her present role, Michaela worked at the intersection of geopolitical risk and cybersecurity at the Krebs Stamos Group. Her background is in emerging technologies and human rights, having covered issues of artificial intelligence, privacy, and platform governance at nonprofit BSR (Business for Social Responsibility). She is a graduate of the University of California, Davis and the Harvard Kennedy School.

Description:

Authoritarian regimes abuse technology as a tool to suppress critics, journalists, human rights defenders, and more. Often, they exploit security weaknesses in common Internet technologies in their attempts to censor information and communication and curtail freedom of expression. ONCD and the State Department will talk about how authoritarian regimes censor their populations, U.S. Government efforts to increase security while combatting authoritarian censorship and repression, and how to help.

The lack of security and resilience throughout the network stack creates opportunities for authoritarian regimes to repress or censor at scale. We will talk through how regimes have historically taken advantage of protocols, internet infrastructure, and lack of encryption to do just that. We'll then talk about how the U.S. Government is approaching this problem.

But most technology, development, and internet services are in the private sector, not the government. So we'll talk about how the community can help: from protocols that need more research and testing, to implementing known security practices, attendees will learn how they can contribute to Internet freedom!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Abortion Access in the Age of Surveillance

When: Saturday, Aug 12, 16:30 - 17:15 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

Speakers: Corynne McSherry, Daly Barnett, India McKinney, Kate Bertash

SpeakerBio: Corynne McSherry , Legal Director at Electronic Frontier Foundation

As EFF's Legal Director, McSherry has extensive experience in advocating for digital civil liberties and promoting net neutrality. Her perspective on the legal frameworks shaping the digital landscape will provide DEF CON attendees with insights on regulatory issues affecting technology users.

Twitter: [@cmcsherr](#)

SpeakerBio: Daly Barnett , Staff Technologist at Electronic Frontier Foundation

Daly Barnett is a staff technologist at the Electronic Frontier Foundation and a digital privacy consultant with Hacking//Hustling. She utilizes her skills as a techie and experience as an activist and educator to undermine the harms that surveillance causes movement-oriented work. Where most information security resources seek to protect capital, her goal is to re-tool those concepts to protect people and liberatory movements.

SpeakerBio: India McKinney , Director of Federal Affairs at Electronic Frontier Foundation

As a former Capitol Hill staffer and a current EFF lobbyist, India's main job is to make sure that the laws of the land don't suck the life out of the internet. India's passion has always been for good public policy, and she's excited to be using skills developed during past legislative battles to fight for encryption, for consumer privacy, and civil liberties in the digital realm.

Twitter: [@imck82](#)

SpeakerBio: Kate Bertash , Founder at Digital Defense Fund

Kate Bertash is the founder of the Digital Defense Fund, a digital security organization for the abortion access movement. She is a hacker and designer of the ALPR-jamming clothing line, Adversarial Wear.

Twitter: [@katerosebee](#)

Description:

In the year since the Supreme Court overturned federal legal protections for reproductive rights, people seeking, providing, and supporting reproductive healthcare are grappling with the challenges of digital surveillance. Multiple services and apps track our movements and communications, and that data can be used by law enforcement and private parties to police and punish abortion access. Lawsuits and prosecutions are already underway and are likely to increase as states continue to pass or expand anti-abortion laws and undermine legal protections for online expression and privacy.

But the fight is far from over. At the state and federal level, lawmakers, activists, and technologists are taking steps to establish and shore up legal and practical protections for secure and private healthcare access.

This panel brings together legal and security experts to lead a discussion about defending reproductive justice in the digital age. What has already been accomplished, what's coming, and how hackers can help. It will build on and update a discussion held last year, also led by EFF and DDF.

REFERENCES

<https://www.eff.org/issues/reproductive-rights>

<https://www.eff.org/deeplinks/2023/03/texas-bill-would-systematically-silence-anyone-who-dares-talk-about-abortion-pills>

<https://www.eff.org/deeplinks/2023/02/eff-backs-california-bill-protect-people-seeking-abortion-and-gender-affirming>

<https://www.eff.org/deeplinks/2022/09/automated-license-plate-readers-threaten-abortion-access-heres-how-policy-makers>

<https://www.eff.org/deeplinks/2022/08/nonprofit-websites-are-full-of-trackers-that-should-change>

<https://www.ifwhenhow.org/resources/self-care-criminalized-preliminary-findings/>

CPV - Saturday - 12:00-12:30 PDT

Title: About Face! Beginner Intro to Facial Recognition

When: Saturday, Aug 12, 12:00 - 12:30 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio:Kate

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Abusing CAN Bus Protocol Specification for Denial of Service in Embedded Systems

When: Saturday, Aug 12, 12:00 - 12:59 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

SpeakerBio: Martin Petran

Martin is a security engineer working at Accenture in Prague specializing in performing penetration testing of embedded systems. His responsibilities and research areas of interest include but are not limited to reverse engineering, hardware hacking and radio analysis. As an open-source enthusiast, he also developed several open source tools that focus on automation during reverse engineering.

Description:

The CAN bus is a traditional communication standard used (not only) in automotive to allow different components to talk to each other over reliable connection. While one of the primary motivators for CAN bus introduction was to reduce the amount of wiring inside vehicles, it became popular for its robustness, flexibility, and ease of implementation for which it is now used in almost every vehicle. As with any other protocol, it is a well-defined standard that enforces all aspects of the communication from the physical media to the message format and its processing. The formal protocol specifications like this are often seen as the source of the absolute truth when working with various transfer protocols. Such specifications are very strict on the format of the messages that belong to the given protocol and thus it is natural that developers that are familiar with it are often relying upon this information when developing their applications. In this talk, we will look at what happens when the attacker decides not to adhere to the protocol specification and uses the available metadata fields within the well-defined message in their own way. Would libraries provided by the device manufacturers handle this situation or is it left to the developer? And could a wrong assumption about the message format lead to a vulnerability?

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Abusing Microsoft SQL Server with SQLRecon

When: Saturday, Aug 12, 12:00 - 13:55 PDT

Where: Caesars Forum - Caucus Boardroom - Demo Labs - [Map](#)

SpeakerBio: Sanjiv Kawa

Sanjiv Kawa (@sanjivkawa) is a Senior Managing Security Consultant on the IBM X-Force Red Adversarial Simulation team with over ten years of experience performing offensive security assessments. As part of the IBM X-Force Red Adversarial Simulation team, Sanjiv spends his days breaking into the largest organizations in the world by emulating adversary tactics, techniques and procedures to reach target objectives. He then advises these organizations on ways they can improve their security posture by implementing or tuning controls. Sanjiv is an active member in the security community. He has developed a variety of tooling and presented at large conferences, such as BSides and Wild West Hackin' Fest and frequently contributes to projects on GitHub.

Twitter: [@sanjivkawa](#)

Description:

SQLRecon helps address the post-exploitation tooling gap by modernizing the approach red team operators can take when attacking SQL Servers. The tool was designed to be modular, allowing for ease of extensibility and contributions from the hacker community. SQLRecon is written in C# and is compatible stand-alone or within a diverse set of command and control (C2) frameworks (Cobalt Strike, Nighthawk, Mythic, PoshC2, Sliver, etc). When using the latter, SQLRecon can be executed either in-process, or through traditional fork and run. SQLRecon has over 50 modules which can help facilitate with enumeration, collection, code execution, privilege escalation and lateral movement. It has been designed with operational security and defense evasion in mind.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Friday - 13:30-14:30 PDT

Title: Access Control Vulnerabilities: Breaking Into Buildings With Computers

When: Friday, Aug 11, 13:30 - 14:30 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

Speakers: Chad, Shortman


SpeakerBio: Chad

No BIO available

SpeakerBio: Shortman

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Sunday - 13:00-13:59 PDT

Title: Access Control Vulnerabilities: Breaking Into Buildings With Computers

When: Sunday, Aug 13, 13:00 - 13:59 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

Speakers: Chad, Shortman


SpeakerBio: Chad

No BIO available

SpeakerBio: Shortman

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Active Directory Attacks: The Good, The Bad, and The LOLwut (Pre-Registration Required)

When: Saturday, Aug 12, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers: Aaron Rosenmund, Brandon DeVault, Ryan Chapman

SpeakerBio: Aaron Rosenmund , Director of Security Research and Content at Pluralsight

Aaron Rosenmund is the Director of Security Research and Content for Pluralsight, where he has also authored over 115 courses and technical labs across offensive and defensive security operations topics. Part time work includes service as an Cyber Warfare Operations office in the Delaware Air National guard, where he has also lead a 100+ member red team for the largest cyber exercise in the Nation, Cybershield. 4 years of highly rated talks and workshops have earned him the Distinguished speaker title from RSAC, and he looks forward to returning for the 3rd year to Defcon Workshops to bring practical emulation and testing capabilities to the people who need it most.

SpeakerBio: Brandon DeVault , Pluralsight

Brandon DeVault is a security researcher, blue teamer, and educator. Currently works as an author for Pluralsight and member of the FL Air National Guard. Prior experience includes work at Elastic and multiple deployments with Special Operations Command.

SpeakerBio: Ryan Chapman

Ryan Chapman is the author of SANS' "FOR528: Ransomware for Incident Responders" course, teaches SANS' "FOR610: Reverse Engineering Malware" course, works as a principal incident response consultant for \$dayJob, and helps run the CactusCon conference in Phoenix, Arizona, USA. Ryan has a passion for life-long learning, loves to teach people about ransomware-related attacks, and enjoys pulling apart malware. He has presented workshops at DefCon and other conferences in the past and knows how to create a step-by-step instruction set to maximize hands-on learning.

Description:

Threat actors such as ransomware affiliates around the world are carrying out attacks on Active Directory (AD) at scale. When doing so, such actors often stick to the mainstream in terms of attack methodologies and tooling. But... that's lame! Why borrow tactics, techniques, and procedures (TTPs) that are so well known and thus readily detectable?! Come hang out with us as we provide an overview of AD, show the most common attack scenarios, then show you how to detect and prevent those very attacks. Stick around as we then transition to covering what you could, and should, be doing instead.

We will be providing a remote network range to which you will connect. Once in the range, you will be acting as the ransomware threat actor, "pentester" as they like to call themselves. You will carry out attacks such as enumeration via Bloodhound, credential discovery and compromise, pass the hash attacks, and kerberoasting via common tools such as Mimikatz & Rubeus. After carrying out the attacks yourself, you'll then learn how to prevent and detect those very attacks. We'll then show you custom-developed methods to carry out the same attacks without the reliance on well-known TTPs/tools. And even better, we'll show you how you could, at least where it's even possible, detect the more custom/advanced methodologies.

Join us if you are a blue teamer, red teamer, purple teamer, cyber defender, DFIR analyst... basically anyone who wants (or needs!) to learn to defend and/or attack Active Directory. Come for the tech, stay for the humor. See ya there!


Skill Level: Intermediate to Advanced

Prerequisites for students:

- The primary requirement for this course is a desire to learn and the determination to tackle challenging problems. In addition, having some familiarization with the following topics will help students maximize their time in this course:
- A general background in Digital Forensics & Incident Response (DFIR)

- Familiarity with blue team-oriented tools
- An understanding of general networking concepts
- Familiarity with Active Directory – though we’ll cover everything students need to know

Materials or Equipment students will need to bring to participate: - A laptop with Linux/Windows/Mac desktop environment - Networking capability: Students will be connecting to a remote network range – They will need a wireless NIC (assuming the workshop area provides Wi-Fi, not not we’ll need to know) that can be enabled along with administrator privileges on their system - **IMPORTANT:** This workshop relies on network connectivity. Any student not able to connect to our range will be unable to follow along with the hands-on portion of the workshop.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Advanced ROP Framework: Pushing ROP to Its Limits

When: Sunday, Aug 13, 11:00 - 11:45 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

Speakers: Bramwell Brizendine, Shiva Shashank Kusuma

SpeakerBio: Bramwell Brizendine, Assistant Professor at University of Alabama in Huntsville Dr.

Dr. Bramwell Brizendine completed his Ph.D. in Cyber Operations, for which he did his dissertation on Jump-Oriented Programming, a hitherto seldom-studied and poorly understood subset of code-reuse attacks.

Bramwell is now an Assistant Professor of Computer Science at the University of Alabama in Huntsville; he previously was an Assistant Professor and the Director of the Vulnerability and Exploitation Research for Offensive and Novel Attacks (VERONA Lab) at Dakota State University, specializing in vulnerability research, software exploitation, and the development of new, cutting-edge tools and techniques with respect to software exploitation and malware analysis. Bramwell has taught numerous undergraduate, graduate and doctoral level courses in software exploitation, reverse engineering, malware analysis and offensive security. Bramwell was a PI on a \$300,000 NSA/NCAE research grant, which culminated in the release of a shellcode emulator, SHAREM, in September 2022. Bramwell has been a speaker at many top security conferences, including DEF CON, Hack in the Box Amsterdam, @Hack, Black Hat Middle East, Black Hat Asia, Black Hat Europe, Wild West Hackin' Fest, and more.

SpeakerBio: Shiva Shashank Kusuma, Master's Student at University of Alabama in Huntsville

Shiva Shashank Kusuma, a Computer Science Master's student at the University of Alabama in Huntsville, has a deep interest in software engineering and cybersecurity. When not at work, Shiva enjoys reading about Blockchain, Web3, and AI.

Description:

This research provides innovative contributions to return-oriented programming (ROP), not seen before. We introduce ROP ROCKET, a cutting-edge ROP framework, to be released at DEF CON. With ROCKET, when attacking 32-bit applications, we can switch between x86 and x64 at will, by invoking a special ROP Heaven's Gate technique, thereby expanding the attack surface. We will discuss the ramifications of this novel approach.

Bypassing DEP via ROP is typically straightforward, using WinAPIs such as VirtualProtect and VirtualAlloc. We demonstrate an alternative: using Windows syscalls. In fact, ROCKET provides automatic ROP chain construction to bypass ROP using Windows syscalls. While extremely trendy, Windows syscalls are only very rarely used in ROP.

One problem with automatic chain construction is bad chars or bad bytes. We demonstrate how ROCKET allows us to use virtually any gadget whose address contains bad bytes. With this approach, automatic ROP chain construction is far less likely to fail. Thus, we overcome one of the major obstacles when creating a ROP chain: bad bytes, which reduces the attack surface needlessly. In fact, if one wanted, they could use ROCKET to "obfuscate" any gadget, obscuring what is being done.

This presentation will do the seemingly impossible - and surprise even veteran users of ROP.

REFERENCES:

1. Brizendine, B., Babcock, A.: A Novel Method for the Automatic Generation of JOP Chain Exploits. In: National Cyber Summit. pp. 77–92 (2021)
2. Min, J.W., Jung, S.M., Lee, D.Y., Chung, T.M.: Jump oriented programming on windows platform (on the x86). Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 7335 LNCS, 376–390 (2012). https://doi.org/10.1007/978-3-642-31137-6_29
3. Erdodi, L.: Attacking x86 windows binaries by jump oriented programming. INES 2013 - IEEE 17th Int. Conf. Intell. Eng. Syst. Proc. 333–338 (2013). <https://doi.org/10.1109/INES.2013.6632837>

4. Brizendine, B., Babcock, A.: Pre-built JOP Chains with the JOP ROCKET: Bypassing DEP without ROP. Black Hat Asia. (2021)
5. One, A.: Smashing the stack for fun and profit. Phrack Mag. 7, 14–16 (1996)
6. Designer, S.: “Return-to-libc” attack., <https://seclists.org/bugtraq/1997/Aug/63>
7. Shacham, H.: The geometry of innocent flesh on the bone: Return-into-libc without function calls (on the x86). Proc. ACM Conf. Comput. Commun. Secur. 552–561 (2007). <https://doi.org/10.1145/1315245.1315313>
8. Roemer, R., Buchanan, E., Shacham, H., Savage, S.: Return-Oriented Programming : Systems , Languages , and Applications. ACM Trans. Inf. Syst. Secur. 15, 1–36 (2012)
9. Buchanan, E., Roemer, R., Savage, S., Shacham, H.: Return-oriented programming: Exploitation without code injection. Black Hat. 8, (2008)
10. PaX, T.: PaX address space layout randomization (ASLR). <http://pax.grsecurity.net/docs/aslr.txt>. (2003)
11. Mark E, R., Alex, I., others: Windows Internals, Part 2, (2012)
12. Shacham, H., Page, M., Pfaff, B., Goh, E.-J., Modadugu, N., Boneh, D.: On the effectiveness of address-space randomization. In: Proceedings of the 11th ACM conference on Computer and communications security. pp. 298–307 (2004)
13. Vreugdenhil, P.: Pwn2Own 2010 Windows 7 Internet Explorer 8 exploit.
14. Gawlik, R., Holz, T.: $\{\$SoK\}$: Make $\{\$JIT-Spray\}$ Great Again. In: 12th USENIX Workshop on Offensive Technologies (WOOT 18) (2018)
15. Göktas, E., Kollenda, B., Koppe, P., Bosman, E., Portokalidis, G., Holz, T., Bos, H., Giuffrida, C.: Position-independent code reuse: On the effectiveness of aslr in the absence of information disclosure. In: 2018 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 227–242 (2018)
16. Checkoway, S., Davi, L., Dmitrienko, A., Sadeghi, A.R., Shacham, H., Winandy, M.: Return-oriented programming without returns. Proc. ACM Conf. Comput. Commun. Secur. 559–572 (2010). <https://doi.org/10.1145/1866307.1866370>
17. Bletsch, T., Jiang, X., Freeh, V.W.: Jump-oriented programming: a new class of code-reuse attack. Proc. 6th Int. Symp. Information, Comput. Commun. Secur. ASIACCS 2011. (2011)
18. Brizendine, B.: JOP ROCKET repository, https://github.com/Bw3ll/JOP_ROCKET/
19. Babcock, A.: IcoFX 2.6 - “.ico” Buffer Overflow SEH + DEP Bypass using JOP, <https://www.exploit-db.com/exploits/49959>
20. Specter: Sony Playstation 4 (PS4) 5.05 - BPF Double Free Kernel Exploit Writeup, <https://www.exploit-db.com/exploits/45045>
21. Brizendine, B., Babcock, A., Kramer, A.: Move Over, ROP: Towards a Practical Approach to Jump-Oriented Programming. HITBMag. 121–152 (2021)
22. Intel Corporation: Control-flow Enforcement Technology Preview, <https://software.intel.com/sites/default/files/managed/4d/2a/control-flow-enforcement-technology-preview.pdf>
23. Schuster, F., Tendyck, T., Liebchen, C., Davi, L., Sadeghi, A.-R., Holz, T.: Counterfeit object-oriented programming: On the difficulty of preventing code reuse attacks in C++ applications. In: 2015 IEEE Symposium on Security and Privacy. pp. 745–762 (2015)
24. Brizendine, B. Windows Syscalls in Shellcode: Advanced Techniques for Malicious Functionality. Hack in the Box Amsterdam (2023).

Title: Advanced WiFi Attacks for Red Team Professionals (Pre-Registration Required)

When: Friday, Aug 11, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

SpeakerBio:Raúl "r4ulcl" Calvo Laorden

Raúl Calvo Laorden is a Spanish Senior Cybersecurity Analyst (Pentester) who is known in the online community as r4ulcl. He has a keen interest in hacking, particularly in Active Directory (AD), WiFi, and Radio Frequency (RF). Raúl enjoys working with Docker and git. He also has a passion for music, video games, and tinkering with electronic devices.

Raúl is the author of WiFiChallenge Lab, a 100% virtualized realistic lab designed for learning and practicing wifi hacking (presented in RootedCON 2022). He is also the creator of wifi_db, a script that parses Aircrack-ng captures into a SQLite database, extracting valuable information such as handshakes, MGT identities, interesting relations between APs, clients and their probes, WPS information, and a global view of all the APs seen. Additionally, he holds the OSCP and CRTP certifications.

In his free time, Raúl dedicates himself to programming hacking and cybersecurity tools. He also maintains his own micro-datacenter consisting of multiple servers and services where he continually learns and practices new technologies.

Description:

Wireless networks have become ubiquitous in today's world, and Red Teams are increasingly using advanced WiFi attacks to gain unauthorized access to these networks. This workshop will focus on advanced WiFi attacks utilized by Red Teams to gain access to wireless networks. Participants will learn how to conduct WiFi reconnaissance, identify misconfigurations in wireless networks, create Rogue APs for launching phishing attacks, bypass WIDS, and more. The workshop is entirely virtual, and participants will have access to a lab environment where they can experiment safely. Participants must have prior knowledge of WiFi attacks on Open, WEP, and WPA2-PSK networks. The workshop covers advanced techniques for WiFi reconnaissance, creating custom TLS certificates, Rogue AP attacks, MSCHAPv2 Relay attacks, password spraying, ESSID stripping, and more. The workshop also covers the importance of Wireless Intrusion Detection Systems for Blue Teams and an example using Nzyme. Overall, this workshop is ideal for Red Team professionals looking to enhance their WiFi attack skills and stay ahead of the game.

Skill Level: Intermediate

Prerequisites for students:

- All participants in participating in this workshop must have a basic understanding of Linux, 802.11 protocol and Wireshark.
- Must have prior knowledge of WiFi attacks on Open, WEP, and WPA2-PSK networks.

Materials or Equipment students will need to bring to participate: - Participants must have access to a computer with a reliable internet connection and a virtualization software such as VirtualBox or VMware.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Adversary Wars CTF

When: Saturday, Aug 12, 10:00 - 16:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Adversary Village proudly presents "Adversary Wars CTF," a cutting-edge capture the flag competition that revolves around adversary attack simulation, adversary-threat actor emulation, purple team tactics and adversary tradecraft. This unique competition is designed to replicate enterprise infrastructure and present participants with challenges that encourage the adoption of various techniques, tactics, and procedures (TTPs) employed by real adversaries and threat actors, all within a defined time frame.

Adversary Village is a community-driven initiative that prioritizes adversary simulation, emulation, breach and attack simulation, adversary tactics, offensive/adversary tradecraft, philosophy, and purple teaming.

Our objective is to establish a Capture the Flag competition dedicated to adversary simulation, purple teaming and knowledge sharing. Adversary Wars offers unique opportunities for “adversaries” aka participants to simulate attacks, explore new attack vectors, gain insights into threat actor profiles, master TTPs, and refine offensive tradecraft. With a range of adversary simulation exercises at different difficulty levels, this CTF promises real-world attack simulation scenarios and challenges.

Previous versions of the Adversary Wars CTF were hosted as part of Adversary Village, during DEF CON 29 and DEF CON 30. We are excited to be back at DEF CON as an official contest this year. Adversary Wars CTF will be located in the contest area for DEF CON 31.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT

Title: Adversary Wars CTF

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Adversary Village proudly presents "Adversary Wars CTF," a cutting-edge capture the flag competition that revolves around adversary attack simulation, adversary-threat actor emulation, purple team tactics and adversary tradecraft. This unique competition is designed to replicate enterprise infrastructure and present participants with challenges that encourage the adoption of various techniques, tactics, and procedures (TTPs) employed by real adversaries and threat actors, all within a defined time frame.

Adversary Village is a community-driven initiative that prioritizes adversary simulation, emulation, breach and attack simulation, adversary tactics, offensive/adversary tradecraft, philosophy, and purple teaming.

Our objective is to establish a Capture the Flag competition dedicated to adversary simulation, purple teaming and knowledge sharing. Adversary Wars offers unique opportunities for “adversaries” aka participants to simulate attacks, explore new attack vectors, gain insights into threat actor profiles, master TTPs, and refine offensive tradecraft. With a range of adversary simulation exercises at different difficulty levels, this CTF promises real-world attack simulation scenarios and challenges.

Previous versions of the Adversary Wars CTF were hosted as part of Adversary Village, during DEF CON 29 and DEF CON 30. We are excited to be back at DEF CON as an official contest this year. Adversary Wars CTF will be located in the contest area for DEF CON 31.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Adversary Wars CTF

When: Friday, Aug 11, 10:00 - 16:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Adversary Village proudly presents "Adversary Wars CTF," a cutting-edge capture the flag competition that revolves around adversary attack simulation, adversary-threat actor emulation, purple team tactics and adversary tradecraft. This unique competition is designed to replicate enterprise infrastructure and present participants with challenges that encourage the adoption of various techniques, tactics, and procedures (TTPs) employed by real adversaries and threat actors, all within a defined time frame.

Adversary Village is a community-driven initiative that prioritizes adversary simulation, emulation, breach and attack simulation, adversary tactics, offensive/adversary tradecraft, philosophy, and purple teaming.

Our objective is to establish a Capture the Flag competition dedicated to adversary simulation, purple teaming and knowledge sharing. Adversary Wars offers unique opportunities for “adversaries” aka participants to simulate attacks, explore new attack vectors, gain insights into threat actor profiles, master TTPs, and refine offensive tradecraft. With a range of adversary simulation exercises at different difficulty levels, this CTF promises real-world attack simulation scenarios and challenges.

Previous versions of the Adversary Wars CTF were hosted as part of Adversary Village, during DEF CON 29 and DEF CON 30. We are excited to be back at DEF CON as an official contest this year. Adversary Wars CTF will be located in the contest area for DEF CON 31.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Saturday - 17:00-17:50 PDT

Title: Aerospace Village - 5 Years On

When: Saturday, Aug 12, 17:00 - 17:50 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio:Pete Cooper

No BIO available

Description:

This is the 5th year of the Aerospace Village and the landscape now is totally different to what it was at the start. This is the story of how a diverse bunch of hackers, engineers, pilots, policy leaders and more from across both the public and private sectors founded and built the Aerospace Village to promote safe, reliable, and trustworthy aviation and space operations. A panel with Pete Cooper, Beau Woods, Jen Ellis, RoRo, and Katie Trimble-Noble.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DCGVR - Saturday - 20:10-21:10 PDT

Title: After Hours Social / Hang out with DEF CON Group members and DCG VR Staff

When: Saturday, Aug 12, 20:10 - 21:10 PDT

Where: Virtual

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: AI Caramba! A DC <> DEF CON interface on machine learning

When: Saturday, Aug 12, 11:00 - 11:50 PDT

Where: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

Speakers: Austin Carson, Erick Galinkin, Kellee Wicker, Rumman Chowdhury, Tim Ryder

SpeakerBio: Austin Carson , Founder & President at SeedAI

Austin Carson is the Founder and President of SeedAI, a nonprofit established to work with a diverse group of policymakers, academics, and private sector experts to help communities across the United States access the resources they need to engage with AI.

Previously, Austin established and led the DC government affairs operation for NVIDIA, translating NVIDIA's expertise in artificial intelligence and high performance computing for policymakers. Prior to joining NVIDIA, Austin held a number of public sector and NGO positions, including serving as Legislative Director for Chairman Michael McCaul and Executive Director for the Technology Freedom Institute. Austin co-founded the Congressional Tech Staff Association, co-led the Congressional Cybersecurity Caucus and the Congressional High Tech Caucus, and is a founding fellow of the Internet Law and Policy Foundry.

SpeakerBio: Erick Galinkin , Principal researcher at Rapid7

Erick Galinkin is a hacker and computer scientist working as principal researcher in Rapid7's Office of the CTO. Presently, Erick leads R&D supporting Rapid7's Managed Detection and Response service. Widely renowned for his equestrian abilities, Erick is a man of several talents. An alumnus of Johns Hopkins University, he has also published and given talks on security, decision theory, information geometry, and artificial intelligence at conferences from AAAI and GameSec to DEF CON's AI and Cloud Villages.

SpeakerBio: Kellee Wicker , Director of the Science and Technology Innovation Program at Wilson Center

Kellee Wicker leads the Science and Technology Innovation Program (STIP) at the Wilson Center, a Congressionally chartered think tank that provides nonpartisan counsel and insights on global affairs to policymakers through deep research, impartial analysis, and independent scholarship. The STIP team provides research and insight to Congress, global policymakers, and the general public on a number of emerging technologies and scientific advances, with special emphasis on artificial intelligence, cybersecurity, space in the commercial age, and more. Through games, experiential learning, and educational opportunities, STIP also works beyond traditional research to directly provide policymakers and their staff with the foundational knowledge they need to devise smart legislation and regulation that protects individuals and workers while continuing to bolster flourishing technological innovation.

SpeakerBio: Rumman Chowdhury , Co-Founder and CEO at Humane Intelligence

Dr. Rumman Chowdhury's passion lies at the intersection of artificial intelligence and humanity. She is a pioneer in the field of applied algorithmic ethics, creating cutting-edge socio-technical solutions for ethical, explainable and transparent AI. Dr. Chowdhury currently runs the nonprofit Humane Intelligence and is a Responsible AI Fellow at the Berkman Klein Center for Internet & Society at Harvard University.

Previously, Dr. Chowdhury was the Director of META (ML Ethics, Transparency, and Accountability) team at Twitter, leading a team of applied researchers and engineers to identify and mitigate algorithmic harms on the platform. Prior to Twitter, she was CEO and founder of Parity, an enterprise algorithmic audit platform company. She formerly served as Global Lead for Responsible AI at Accenture Applied Intelligence. In her work as Accenture's Responsible AI lead, she led the design of the Fairness Tool, a first-in-industry algorithmic tool to identify and mitigate bias in AI systems.

Dr. Chowdhury is dedicated to cultivating and growing the next wave of technology-forward companies enabling the responsible use of emerging technologies.

SpeakerBio: Tim Ryder , Legislative Assistant at Office of U.S. Senate Majority Leader Charles E. Schumer
Tim joined U.S. Senate Majority Leader Charles E. Schumer’s office in May 2019 and currently serves as a Legislative Assistant. Tim is spearheading the Leader’s work on artificial intelligence, while overseeing the disaster policy portfolio. He is also a member of the Schumer Climate Team, where he helped formulate, negotiate, and pass the Inflation Reduction Act, Infrastructure Investment and Jobs Act, and a number of other bills last Congress.

Prior to his time on the Hill, Tim worked for The Climate Reality Project – former Vice President Al Gore’s non-profit – on Gore’s famous slideshow featured in An Inconvenient Truth. Tim is active in a number of young professional organizations and runs a small business in the district – Green Drinks DC – with his longtime friend. Tim is a graduate of Stetson University, where he studied Environmental Science and Philosophy, and is an alumnus of American University’s Washington Semester Program. In what little spare time there is these days, Tim loves to garden, cook, and make music.

Description:

AI is a huge focus for multiple governments and they are keen to get input from the DEF CON community on what they should be considering for policy interventions.

This session will be led by Austin Carson, exploring how we can combine the expertise of DEF CON attendees with the political will and specialized knowledge networks in the Administration and around DC to create wise policy for AI. Topics covered will include how the two communities can support each other and create a virtuous cycle of information conveyance and policy progress? What should the next steps of this work be - how do we move beyond the Biden EO? In this session we'll have top experts in policy and the hacker community come together to discuss what that can look like and how to be mutually conscientious of what our experiences and priorities may be.

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Sunday - 11:15-11:45 PDT

Title: AI Village Closing Remarks

When: Sunday, Aug 13, 11:15 - 11:45 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

SpeakerBio: AI Village Organizers

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Friday - 11:00-11:15 PDT

Title: AI Village CTF Kickoff and Introduction

When: Friday, Aug 11, 11:00 - 11:15 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

SpeakerBio: Will Pearce

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Saturday - 10:00-17:59 PDT

Title: AI Village Generative Red Team Challenge


When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

Description:

Participate in a Jeopardy-style CTFs competition that challenges you to break through the guardrails within 8 different LLMs. In your 50-minute session, execute prompt injections, find internal inconsistencies, and identify issues in information integrity, privacy, and societal harm. Compete for points and take home the prize, or just have fun coming up with novel attacks.

This exercise, first of its kind, will allow the best and brightest minds in the security industry to join diverse voices new and veteran to the AI scene in pursuit of making AI and machine learning safer.

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Friday - 10:00-17:59 PDT

Title: AI Village Generative Red Team Challenge

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

Description:

Participate in a Jeopardy-style CTFs competition that challenges you to break through the guardrails within 8 different LLMs. In your 50-minute session, execute prompt injections, find internal inconsistencies, and identify issues in information integrity, privacy, and societal harm. Compete for points and take home the prize, or just have fun coming up with novel attacks.

This exercise, first of its kind, will allow the best and brightest minds in the security industry to join diverse voices new and veteran to the AI scene in pursuit of making AI and machine learning safer.

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Sunday - 10:00-12:59 PDT

Title: AI Village Generative Red Team Challenge


When: Sunday, Aug 13, 10:00 - 12:59 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

Description:

Participate in a Jeopardy-style CTFs competition that challenges you to break through the guardrails within 8 different LLMs. In your 50-minute session, execute prompt injections, find internal inconsistencies, and identify issues in information integrity, privacy, and societal harm. Compete for points and take home the prize, or just have fun coming up with novel attacks.

This exercise, first of its kind, will allow the best and brightest minds in the security industry to join diverse voices new and veteran to the AI scene in pursuit of making AI and machine learning safer.

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Saturday - 10:30-11:25 PDT

Title: AI Village Keynote 2: AI red teaming tradecraft: a team of teams approach

When: Saturday, Aug 12, 10:30 - 11:25 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

Speakers: Daniel Fabian, Mikel Rodriguez, Sarah Hodkinson

SpeakerBio: Daniel Fabian

No BIO available

SpeakerBio: Mikel Rodriguez

No BIO available

SpeakerBio: Sarah Hodkinson

No BIO available

Description:

AI-enabled systems are rapidly being deployed in a wide range of high-stakes environments. These systems are vulnerable to a wide range of attacks that can trigger errors, degrade performance, or disclose sensitive data. This talk will offer a firsthand account and reflect on some lessons learned from Google DeepMind's AI red team. While research in ensuring the security and privacy of AI-enabled systems is rapidly growing, much of today's research is focused on lab settings, and a more holistic understanding of how these emerging vulnerabilities can interact with known real-world security vulnerabilities in deployed systems is lacking. As part of this talk we will explore opportunities for the DEFCON community to work together to ensure mission-critical AI systems are battle-tested with the rigor and scrutiny of real-world adversaries.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: AI Village Keynote: The last attempted AI revolution in security, and the next one

When: Friday, Aug 11, 10:15 - 10:59 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

Speaker Bio: Joshua Saxe

No BIO available

Description:

This isn't our first "ChatGPT moment" – a decade ago, when AlexNet realized a step function jump in image classification accuracy, there was a similar wave of hype. Breathless claims were made about deep learning replacing signatures, revolutionizing zero-day attack detection, threat intelligence, and predicting the future. A decade later we can say that it didn't. ML found a few applications as a value-add (e.g. as a complement to signatures in malware detection), but never became load bearing. Instead, our field continued to improve its basic technologies – signatures, databases, event processing pipelines, and, most importantly, manual human processes. In this talk, I'll argue that while the past decade gives reasons to doubt it, this AI moment really is different. I'll delineate the ways in which today's scaled machine learning models address some (but not all) of the core blockers ML faced in the last decade, and take positions on how scaled ML will shape defensive practice and the threat landscape over the next few years.

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Friday - 10:00-10:10 PDT

Title: AI Village Opening Remarks

When: Friday, Aug 11, 10:00 - 10:10 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

SpeakerBio: AI Village Organizers

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: AI-Driven Hacker's Toolkit: Using AI to Learn Python and Scapy for Exploitation and Post-Exploitation Techniques

When: Saturday, Aug 12, 14:00 - 14:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 5 - [Map](#)

SpeakerBio: Omar Santos

No BIO available

Twitter: [@santosomar](#)

Description:

Artificial Intelligence (AI) has paved its way into many fields, and cybersecurity is no exception. AI can significantly augment red team operations by enhancing the learning process of key tools like Python and Scapy. Let's delve into how AI can act as an indispensable co-pilot in mastering these crucial tools for cybersecurity tasks.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: AI-Driven Hacker's Toolkit: Using AI to Learn Python and Scapy for Exploitation and Post-Exploitation Techniques

When: Friday, Aug 11, 13:00 - 13:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 5 - [Map](#)

SpeakerBio: Omar Santos

No BIO available

Twitter: [@santosomar](#)

Description:

Artificial Intelligence (AI) has paved its way into many fields, and cybersecurity is no exception. AI can significantly augment red team operations by enhancing the learning process of key tools like Python and Scapy. Let's delve into how AI can act as an indispensable co-pilot in mastering these crucial tools for cybersecurity tasks.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: All information looks like noise until you break the code: Futureproofing the transportation sector

When: Saturday, Aug 12, 16:30 - 17:15 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

Speakers:David Pecoske, Jen Easterly, Kevin Collier

SpeakerBio:David Pecoske , Administrator at Transportation Security Administration (TSA)

David Pecoske was first confirmed by the U.S. Senate as the Transportation Security Administration's seventh administrator in August 2017 and was reconfirmed for a second term in September 2022.

Pecoske leads a workforce of over 60,000 employees and is responsible for security operations at nearly 440 airports throughout the United States. TSA is also the lead federal agency for security of highways, railroads, mass transit systems and pipelines. Under his leadership, TSA improved transportation security through close partnerships and alliances, a culture of innovation, and development of a dedicated workforce.

During his tenure as TSA Administrator, Pecoske also served at the Department of Homeland Security as Acting Secretary from January 20 to February 2, 2021, and as the Senior Official Performing the Duties of Deputy Secretary from April to November 2019, and again from February to June 2021. At the Department, Pecoske helped lead a unified national effort to ensure the continued security of the United States, coordinating components with missions ranging from prevention and protection to recovery and response. He was also a commissioner on the Cyberspace Solarium Commission that developed a consensus on a strategic approach to defending the United States in cyberspace against attacks of significant consequence.

Before joining TSA, Pecoske was an executive in the government services industry, where he led teams that provided counterterrorism, security and intelligence support services to government agencies.

Pecoske served as the 26th Vice Commandant of the U.S. Coast Guard, culminating a Coast Guard career that included extensive operational and command experience. As the Vice Commandant, Pecoske was second in command, also serving as Chief Operating Officer and Component Acquisition Executive of the Coast Guard. He is a recognized expert in crisis management, strategic planning, innovation, and aviation, surface transportation and maritime security. In addition, he has been twice awarded the Homeland Security Distinguished Service Medal.

Pecoske holds a Master of Business Administration from the Massachusetts Institute of Technology, a Master of Public Administration from Columbia University and a Bachelor of Science from the U.S. Coast Guard Academy.

Twitter: [@TSA_Pecoske](#)

SpeakerBio:Jen Easterly , Director at Cybersecurity and Infrastructure Security Agency (CISA)

Jen Easterly is the Director of the Cybersecurity and Infrastructure Security Agency (CISA). She was nominated by President Biden in April 2021 and unanimously confirmed by the Senate on July 12, 2021. As Director, Jen leads CISA's efforts to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every day. She is a proud Mom, a mental health advocate, a Rubik's Cube enthusiast, and an aspiring electric guitarist.

Before serving in her current role, Jen was the head of Firm Resilience at Morgan Stanley, responsible for ensuring preparedness and response to business-disrupting operational incidents and risks to the Firm. She also helped build and served as the first Global Head of Morgan Stanley's Cybersecurity Fusion Center, the Firm's center of gravity for cyber defense operations.

Jen has a long tradition of public service, to include two tours at the White House, most recently as Special Assistant to President Obama and Senior Director for Counterterrorism and earlier as Executive Assistant to National Security Advisor Condoleezza Rice. She also served as the Deputy for Counterterrorism at the National Security Agency.

A two-time recipient of the Bronze Star, Jen retired from the U.S. Army after more than twenty years of service in intelligence and cyber operations, including tours of duty in Haiti, the Balkans, Iraq, and Afghanistan. Responsible for standing up the Army's first cyber battalion, she was also instrumental in the design and creation of United States Cyber Command.

A distinguished graduate of the United States Military Academy at West Point, Jen holds a master's degree in Philosophy, Politics, and Economics from the University of Oxford, where she studied as a Rhodes Scholar. She is the recipient of numerous honors and awards, including the 2023 Sisterhood Award from Girls Who Code; the 2022 National Defense University Admiral Grace Hopper Award; the 2021 Cybersecurity Ventures Cybersecurity Person of the Year Award; the 2020 Bradley W. Snyder Changing the Narrative Award, and the 2018 James W. Foley Legacy Foundation American Hostage Freedom Award.

A member of the Council on Foreign Relations and a French American Foundation Young Leader, Jen is the past recipient of the Aspen Finance Leaders Fellowship, the National Security Institute Visiting Fellowship, the New America Foundation Senior International Security Fellowship, the Council on Foreign Relations International Affairs Fellowship, and the Director, National Security Agency Fellowship.

Twitter: [@CISAJen](#)

SpeakerBio: Kevin Collier , NBC

No BIO available

Description:

Just like there's more than one way to peel a banana, there's more than one way to protect a computer network from being pwned. Cyber threats against America's pipelines, railroads and aviation system are increasing, and the Transportation Security Administration – with support from the White House, the Cybersecurity and Infrastructure Security Agency and Congress – is hacking traditional cybersecurity policy to improve resiliency for the growing connected transportation sector. How? TSA isn't telling regulated parties exactly the ways they should secure their own systems. Instead, the agency is asking them to produce and provide plans for ensuring they protect their critical assets.

America's adversaries are sophisticated, and TSA needs help from the hacking community to think creatively about future attacks, to identify new vulnerabilities, and to provide innovative new ways of measuring success. This talk will tell you what TSA is seeing, gives you a chance to offer us advice, and to learn specific ways in which you can contribute to new projects. Because always in motion the future is.

[Return to Index](#) - Add to  - ics [Calendar](#) file

TCV - Sunday - 10:30-10:59 PDT

Title: All the things, all the time: Lifting the veil on security in the global mobile industry and how it works with hackers

When: Sunday, Aug 13, 10:30 - 10:59 PDT

Where: Flamingo - Virginia City - Telecom Village - [Map](#)

SpeakerBio:James Moran , Head of Security at GSMA

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: All Your Vulns are Belong to Terms & Conditions

When: Saturday, Aug 12, 15:00 - 15:50 PDT

Where: Caesars Forum - Summit - 221-222 - Policy Atrium - [Map](#)

Speakers: Casey Ellis, David Rogers, Harley Geiger, Katie Trimble-Noble

SpeakerBio: Casey Ellis , Bugcrowd

Casey is the Chairperson, Founder, and Chief Technology Officer of Bugcrowd, as well as the co-founder of The disclose.io Project. He is a 20-year veteran of information security who spent his childhood inventing things and generally getting technology to do things it isn't supposed to do. Casey pioneered the Crowdsourced Security as-a-Service model, launching the first bug bounty programs on the Bugcrowd platform in 2012, and co-founded the disclose.io vulnerability disclosure standardization project in 2014 prior to its launch in 2018.

Since then, he has personally advised the US Department of Defense and Department of Homeland Security/CISA, the Australian and UK intelligence communities, and various US House and Senate legislative cybersecurity initiatives, including preemptive cyberspace protection ahead of the 2020 Presidential Elections.

Casey, a native of Sydney, Australia, is based in the San Francisco Bay Area.

SpeakerBio: David Rogers , CEO at Copper Horse

David is a mobile phone and IoT security specialist who runs Copper Horse Ltd, a software and security company based in Windsor, UK. He chairs the Fraud and Security Group at the GSMA. He has spoken at a number of hacking conferences on his security research work including DEF CON's Car Hacking Village, 44CON, B-Sides London, B-Sides Cymru and B-Sides LV. He was awarded an MBE for services to Cyber Security in the Queen's Birthday Honours 2019.

SpeakerBio: Harley Geiger , Counsel at Venable LLP

Harley Geiger is Counsel and Senior Director at Venable, LLP, where he leads the Security Research Legal Defense Fund and the Hacking Policy Council and counsels clients on a variety of cybersecurity issues. Prior to this, Geiger was Senior Director for Public Policy at Rapid7, where he worked to expand adoption of vulnerability disclosure and legal protections for security research. Geiger also worked as Senior Legislative Counsel in the U.S. House of Representatives, where he drafted Aaron's Law, and served as Advocacy Director at the Center for Democracy & Technology.

Twitter: [@HarleyGeiger](#)


SpeakerBio: Katie Trimble-Noble , Director, PSIRT and Bug Bounty at A Tech Company

Katie serves as a CVE Program Board, Bug Bounty Community of Interest Board, and Hacking Policy Council member. She is a passionate defensive cybersecurity community activist, she is regularly involved in community driven projects and is most happy when she is able to effect positive progress in cyber defense. In her day-job Katie Noble serves as a Director of PSIRT, Bug Bounty, and the Security Working Artifacts Team at a fortune 50 Technology Company. Prior to joining private sector, Katie spent over 15 years in the US Government. Most recently as the Section Chief of Vulnerability Management and Coordination at the Department of Homeland Security, Cyber and Infrastructure Security Agency (CISA). Her team is credited with the coordination and public disclosure of 20,000+ cybersecurity vulnerabilities within a two-year period. During her government tenure, in roles spanning Intelligence Analyst for the National Intelligence Community to Senior Policy Advisor for White House led National Security Council Cyber programs, Katie's work directly impacted decision making for government agencies in the United States, United Kingdom, Canada, and Australia.

Description:

What happens when a vulnerability is submitted to a programme? Why do some disclosures take forever? What are governments doing about vulnerability disclosure and why are they so bothered about it? Why do people not understand what the words "vulnerability disclosure" mean and why can't policy makers quite get their heads around 0 days? Why are companies in some sectors just not adopting CVD even though governments are passing it into law? Have we got RAS or can

we think of anymore TLAs to add to the CRA, NIS and VDP? What are countries and regions around the world doing and how do they differ? And yes, what the heck is an equities process?

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Am I Exploitable? (MI-X)

When: Saturday, Aug 12, 12:00 - 13:55 PDT

Where: Caesars Forum - Council Boardroom - Demo Labs - [Map](#)

Speakers: Ofri Ouzan, Yotam Perkal

SpeakerBio: Ofri Ouzan

Ofri Ouzan is an experienced Security Researcher who has been working in the cybersecurity field for over four years. She specializes in conducting security research on Windows, Linux, Cloud Platforms, and containerized applications with an emphasis on vulnerabilities. Her expertise lies in finding and solving complex problems in the cyber field, developing automation and open-source tools.

SpeakerBio: Yotam Perkal

Yotam leads the vulnerability research team at Rezilion, focusing on research around vulnerability validation, mitigation, and remediation. Prior to Rezilion, Yotam filled several roles at PayPal Security organization, dealing with vulnerability management, threat intelligence, and Insider threat. Additionally, Yotam takes part in several OpenSSF working groups around open-source security as well as several CISA work streams around SBOM and VEX and is also a member of the PyCon Israel organization committee. He is passionate about Cyber Security and Machine Learning and is especially intrigued by the intersection between the domains, whether it be using ML in order to help solve Cyber Security challenges or exploring the challenges in securing ML applications.

Description:

Addressing security vulnerabilities begins with verifying the impact on an environment. Merely having a vulnerable package installed does not guarantee exploitability, as several conditions must align for the vulnerability to be applicable and exploitable. For example: is the operating system in question susceptible to the vulnerability? is the vulnerable component loaded to memory? is the required configuration in place? is there a patch installed? And more... Standard vulnerability scanners simply do not take these factors into account and thus require manual triage in order to answer “Can a vulnerability be exploited in a given environment?”. ‘Am I Exploitable?’ (MI-X), is an open-source tool aimed at effectively determining whether a local host or running container is truly affected by a specific vulnerability by accounting for all factors which affect *actual* exploitability. MI-X also prints out the logical steps it takes in order to reach a decision and can also provide a graphical representation of the validation flow. The tool can therefore help practitioners understand what are the factors that affect exploitability for each of the supported vulnerabilities.

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Sunday - 12:00-13:59 PDT

Title: AMA - Jim Manico

When: Sunday, Aug 13, 12:00 - 13:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 2 - [Map](#)

SpeakerBio:Jim Manico

Jim Manico is the founder of Manicode Security, training devs on secure coding. He advises/invests in companies like 10Security, MergeBase. A speaker, Java Champion, and author of "Iron-Clad Java." Active in OWASP, co-leading projects like ASVS.

Twitter: [@manicode](#)

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Friday - 13:00-14:59 PDT

Title: AMA - Tib3rius

When: Friday, Aug 11, 13:00 - 14:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 1 - [Map](#)

SpeakerBio: Tib3rius

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

HRV - Friday - 13:00-13:59 PDT

Title: Amateur Radio Digital Modes Primer

When: Friday, Aug 11, 13:00 - 13:59 PDT

Where: Flamingo - Virginia City - Ham Radio Village - [Map](#)

SpeakerBio:Jon Marler

No BIO available

Description:

Amateur radio operator Jon Marler, callsign K4CHN, presents an introduction to many of the digital modes available to amateur radio operators. Jon will be discussing the modes available for voice and data, as well as many of the hardware options available. Jon will also be presenting a very simple design for a way to connect a Raspberry Pi to your radio safely. A demonstration of slow scan television (SSTV) will be made to end the presentation before Q&A.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: An Audacious Plan to Halt the Internet's Enshittification

When: Saturday, Aug 12, 12:30 - 13:15 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

SpeakerBio: Cory Doctorow

Cory Doctorow (craphound.com) is a science fiction author, activist and journalist. He is the author of many books, most recently RED TEAM BLUES, a science fiction crime thriller; CHOKEPOINT CAPITALISM, nonfiction about monopoly and creative labor markets; the LITTLE BROTHER series for young adults; IN REAL LIFE, a graphic novel; and the picture book POESY THE MONSTER SLAYER. In 2020, he was inducted into the Canadian Science Fiction and Fantasy Hall of Fame.

Twitter: [@doctorow](#)

Description:

The enshittification of the internet follows a predictable trajectory: first, platforms are good to their users; then they abuse their users to make things better for their business customers; finally, they abuse those business customers to claw back all the value for themselves. Then, they die.

It doesn't have to be this way. Enshittification occurs when companies gobble each other up in an orgy of mergers and acquisitions, reducing the internet to "five giant websites filled with screenshots of text from the other four" (credit to Tom Eastman!), which lets them endlessly tweak their back-ends to continue to shift value from users and business-customers to themselves. The government gets in on the act by banning tweaking by users - reverse-engineering, scraping, bots and other user-side self-help measures - leaving users helpless before the march of enshittification.

We don't have to accept this! Disenshittifying the internet will require antitrust, limits on corporate tweaking - through privacy laws and other protections - and aggressive self-help measures from alternative app stores to ad blockers and beyond!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: An Introduction to SAML and its Security

When: Friday, Aug 11, 12:00 - 13:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 4 - [Map](#)

SpeakerBio: Louis Nyffenegger

Louis is a security engineer based in Melbourne, Australia. He is the founder of PentesterLab, a learning platform for web penetration testing.

Twitter: [@snyff](#)

Description:

In this workshop, you will get to learn how SAML works and how to exploit issues impacting SAML implementations. Remember this XSW attacks in Burp? What do they actually do? Let's dive in and have fun learning about SAML. Basic understanding of Proxying request/response and Burp required.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Analysis 101 for Incident Responders (Pre-Registration Required)

When: Thursday, Aug 10, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

SpeakerBio: Kristy Westphal

Kristy Westphal is a versatile information technology professional with specific experience in providing advisory and management services in the area of information security and risk is currently employed as the Vice President, Security Operations at a financial services company. Specializing in leadership and program development, specific expertise in security areas includes: process analysis, risk assessments, security awareness programs, operating system security, network security, incident handling, vulnerability analysis and policy development.

Description:

You have a theory about something you have found while roaming the network or conducting your own hackfest, but how do you go about proving it? This workshop will be a hands-on journey deep into the world of analysis. While analysis is a bit of an art form, there are methods that can be applied to make it less of a gut feeling and more of a scientific approach to support your hypothesis. From network forensics to log analysis to endpoint forensics and cloud log analysis, we will review numerous quick methods (including some analysis wizardry with R) to gain context over the data you have gathered and apply critical thinking in an attempt to find the answers. Sometimes, the answers weren't meant to be found, but we'll also discuss how to make the best of any conclusion that you reach.

Skill Level: Beginner to Intermediate

Prerequisites for students:

- A curiosity for security!

Materials or Equipment students will need to bring to participate: - Will need a laptop with Wireshark and R installed.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Friday - 16:30-16:59 PDT

Title: Anaotmy of the Top 10 Cybersecurity Terrain for Critical Infrastructure

When: Friday, Aug 11, 16:30 - 16:59 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio:Mars Cheng

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Android App Hacking - Hacking for Good! (Pre-Registration Required)

When: Friday, Aug 11, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers:Kavia Venkatesh,Maria Uretsky,Olivier Tuchon,Sajjad "JJ" Arshad

SpeakerBio:Kavia Venkatesh , Technical Program Manager on the Android Security Team at Google

Kavia Venkatesh is a Technical Program Manager on the Android Security Team at Google where she leads the execution of the Android Security Release Program aka Android Security Bulletin. Over the last 7+ years has led numerous security initiatives. Now, she's passionate about sharing her knowledge with the world.

SpeakerBio:Maria Uretsky , Google

Maria Uretsky is leading the Android Vulnerability Rewards program at Google. Her passion is to break all the things before the bad actors do, to ensure they are kept out. During her 10+ years of software engineering and security work, she has been part of Google Cloud Security, Azure Sentinel, Windows Defender and AVG.

SpeakerBio:Olivier Tuchon , Security Engineer, Android Vulnerability Research team at Google

Olivier Tuchon is a Security Engineer on the Android Vulnerability Research team. Olivier has been working at Google for almost 5 years, he started by chasing malware/PHA in the Play Store and into the wild (OffMarket) with a speciality in Stalkerware. Now, Olivier looks for vulnerabilities in 3P Android applications. Before Google, Olivier had been a Security Engineer in the French Army for 12 years.

SpeakerBio:Sajjad "JJ" Arshad , Senior Security SWE, Android Security & Privacy team at Google

JJ is a Senior Security SWE at Google's Android Security & Privacy team where he is developing tools to fight abuse in Android with focus on JavaScript-based frameworks. He has also designed CTF challenges and helped organize GoogleCTF in the past few years. Before Google, he was a Cybersecurity researcher at iSecLab and earned his PhD in Cybersecurity from Northeastern University, Boston, MA. Some domains he is active in are large-scale web security & privacy measurement, program analysis, and Malware detection.

Description:

Welcome to the world of Android Hacking! This is a hands-on workshop designed to introduce you to the knowledge, tools and techniques for analyzing and exploiting vulnerabilities in Android applications.

The workshop will start by presenting hacking for good, insights on the Android bug bounty, then it will cover the basic concepts of Android applications, walk you through industry standard tools and techniques and then let you experiment on your own with our Android reverse engineering CTF!

Come and hack with us!

The workshop requires no prior knowledge of Android or reverse engineering.

Skill Level: Beginner to Intermediate

Prerequisites for students:

- Before the workshop, students should follow the setup instructions to ensure they can start working on the CTFs in the workshop: <https://tinyurl.com/aah-setup> - There is no pre-required knowledge.

Materials or Equipment students will need to bring to participate: - Laptop with 20+ GB free hard disk space 4+ GB RAM - Mac. Windows 7/8 , Ubuntu 12.x + (64 bit Operating System), - **ADB**

- apktool

- Python & pip
 - JDK
 - jadx
 - Burp Suite
 - Wireshark
 - Frida
 - Ghidra
 - Administrative access on your laptop
-

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Android Applications and APIs hacking

When: Sunday, Aug 13, 11:45 - 12:30 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

SpeakerBio: Gabrielle Botbol

Gabrielle Botbol is a pentester and cybersecurity blogger. She created a self-study program to become a pentester and focuses on democratizing infosec. Gabrielle is on Advisory Boards and has won multiple awards for her cyber community contributions

Twitter: [@Gabrielle_BGB](#)

Description:

As mobile devices have become increasingly prevalent, the security of Android applications has become a critical concern. Pentesting is an essential process for identifying and mitigating potential vulnerabilities in these applications, but Android app hacking is a specialized area that is less well-documented than other pentesting techniques. In this session, the focus will be on how to pentest Android apps and their APIs.

The presentation will address key questions such as what Android pentesting is, how to set up an Android App pentest lab, and how to pentest an Android App and its APIs from start to finish.

Participants will leave the session with tips and resources for learning, practicing, and setting up a complete set of tools for Android application pentesting, including detailed examples on a purposefully vulnerable application. The goal is to equip attendees with the knowledge and skills necessary to conduct thorough and effective pentests of Android applications.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Android Applications and APIs Hacking

When: Saturday, Aug 12, 09:00 - 09:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 1 - [Map](#)

SpeakerBio:Gabrielle Botbol

Gabrielle Botbol is a pentester and cybersecurity blogger. She created a self-study program to become a pentester and focuses on democratizing infosec. Gabrielle is on Advisory Boards and has won multiple awards for her cyber community contributions

Twitter: [@Gabrielle_BGB](#)

Description:

As mobile devices have become increasingly prevalent, the security of Android applications has become a critical concern. Pentesting is an essential process for identifying and mitigating potential vulnerabilities in these applications, but Android app hacking is a specialized area that is less well-documented than other pentesting techniques. In this session, the focus will be on how to pentest Android apps and their APIs. The presentation will address key questions such as what Android pentesting is, how to set up an Android App pentest lab, and how to pentest an Android App and its APIs from start to finish.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Antennas

When: Saturday, Aug 12, 15:00 - 15:20 PDT

Where: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

SpeakerBio: Kent

Kent has a long history is developing over 1200 different PCB antennas for a lot of different applications.

Description:

GPS Jamming and Anti-Jamming

How to modify GPS antennas to reduce jammer signals Direction Finding

Some results for the Ukraine on DF'ing on GPS hammers. Might include DFing on artillery counterfire Radars Quick overview of general RF monitoring Some history of Code Breaking

Schematics of an Enigma and the Polish Spread Sheets of find the set up. Common setups (Enigma had a 6 letter setup, Brits quickly found HITLER BERLIN LONDON would decode many messages) On to Lorenz 12 rotor machine for teletype machines COLOSSUS The first programmable computer ENIAC was not num 1, it was number 11! Used to find the Key to a Lorenz message. History books are wrong because after WWII Colossus worked against US and Soviet code machines. Secret until the 1970's

May need to tweak this for the list.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Anti-Social Engineering: Can You Be a Good Social Engineer Without Being Social

When: Saturday, Aug 12, 09:00 - 09:30 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

SpeakerBio: Andrew Lemon , Principal Security Engineer at Red Threat

Lemon is the Principal Security Engineer at Red Threat where he serves as the lead over Penetration Testing and Red Teaming. His primary interest lie in physical penetration testing and social engineering. Lemon honed his skills on high pressure physical penetration test usually involving armed guards.

Twitter: [@Lemonitup](#)

Description:

Social engineering has long been thought of as a domain for outgoing, charismatic people. However, in this talk, I will argue that introverted and socially-awkward individuals can be just as effective in social engineering as their extroverted counterparts. Drawing on my personal experience as an introverted social engineer, I will share tips and tricks for blending in, avoiding confrontation, and getting the information you need without attracting unwanted attention. Through real-world examples from my physical pentesting engagements, I will demonstrate how my “anti-social” approach has yielded results that even my more outgoing colleagues were unable to achieve. I will also dispel common misconceptions about social engineering and challenge the notion that charisma and acting skills are essential to the craft. Attendees will leave with a newfound appreciation for the power of blending in and avoiding attention, as well as practical tips for incorporating these techniques into their own social engineering engagements.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Apple's Predicament: NSPredicate Exploitation on macOS and iOS

When: Saturday, Aug 12, 11:30 - 12:15 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

SpeakerBio: Austin Emmitt , Senior Security Researcher at Trellix Advanced Research Center

Austin Emmitt is a vulnerability researcher with a background in mobile security. He has found critical vulnerabilities in Android, iOS, and other platforms. He is also the creator of the radius2 symbolic execution framework.

Twitter: [@alkalinesec](#)

Description:

In 2021 the FORCEDENTRY sandbox escape introduced the usage of NSPredicate in an iOS exploit. This new technique allowed attackers to sidestep codesigning, ASLR, and all other mitigations to execute arbitrary code on Apple devices. As a result, Apple put in place new restrictions to make NSPredicate less powerful and less useful for exploits. This presentation will cover new research showing that these added restrictions could be completely circumvented in iOS 16, and how NSPredicates could be exploited to gain code execution in many privileged iOS processes. This technical deep dive will be a rare instance of iOS security that anyone can comprehend without years of experience.

After an overview of the classes involved, we will explore the full syntax of NSPredicate and cover how it can be used to script the Objective-C runtime and even call any C function. It will be shown that PAC can still be bypassed 100% reliably with NSPredicates in order to execute any function with arbitrary arguments. A new tool will be unveiled to help craft complex NSPredicates to execute arbitrary code and inject those predicates in any application. Additionally, a demonstration will be given which executes arbitrary code in the highly privileged Preferences app.

Finally, the talk will cover a bypass of NSPredicateVisitor implementations which allows a malicious process to evaluate any NSPredicate within several system processes including coreduetd, appstored, OSLogService, and SpringBoard. Next there will be a live demo of exploiting SpringBoard to steal a user's notifications and location data. The presentation will end with some discussion about what can still be done with NSPredicates now that these issues have been fixed, including bypassing App Store Review, and what app developers should know to keep their own apps safe.

REFERENCES:

NSPredicate - <https://developer.apple.com/documentation/foundation/nspredicate?language=objc> See No Eval: Runtime Dynamic Code Execution in Objective-C by CodeColorist -

<https://codecolor.ist/2021/01/16/see-no-eval-runtime-code-execution-objc/> FORCEDENTRY: Sandbox Escape by Ian Beer & Samuel Groß of Google Project Zero - <https://googleprojectzero.blogspot.com/2022/03/forcedentry-sandbox-escape.html>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Applied Emulation - A Practical Approach to Emulating Malware (Pre-Registration Required)

When: Thursday, Aug 10, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers: Sean Wilson, Sergei Frankoff

SpeakerBio: Sean Wilson , Co-Founder at OpenAnalysis Inc

Sean, a co-founder of OpenAnalysis Inc., splits his time between reverse engineering, tracking malware and building automated malware analysis systems. Sean brings over a decade of experience working in a number of incident response, malware analysis and reverse engineering roles.

SpeakerBio: Sergei Frankoff , Co-founder at OpenAnalysis Inc

Sergei is a co-founder of OpenAnalysis Inc. When he is not reverse engineering malware Sergei is focused on building automation tools for malware analysis, and producing tutorials for the OALABS YouTube channel. With over a decade in the security industry Sergei has extensive experience working at the intersection of incident response and threat intelligence.

Description:

Binary emulation is now a must-have tool for malware analysts. With a few lines of Python you can unpack binaries, skip analysis of complex algorithms, and automatically extract the configuration data from malware! It's not too good to be true, but there is a little preparation work involved...

In this workshop you will set up your own emulation environment (using Python) and work through a series of common malware analysis tasks such as unpacking, and malware configuration extraction. The workshop starts simple using Unicorn to emulate x86 shellcode, and builds to a final project where syscall hooking is used with Dumpulator to automatically extract C2s from malware.

This workshop is aimed at malware analysts and reverse engineers who are interested in learning more about emulation and how it can be used to automate some reverse engineering workflows. Students must be able to write basic Python scripts, and have a working knowledge of the Windows OS. Familiarity with Windows malware, assembly, and debugging are strongly recommended. If you have opened malware in a debugger before you will feel right at home here.

You will be provided with detailed virtual machine setup instructions prior to the workshop. Please make sure to bring a laptop that meets the following requirements.

- Your laptop must have VirtualBox or VMWare installed and working prior to the start of the course.
- Your laptop must have at least 60GB of disk space free.
- Your laptop must also be able to mount USB storage devices. (Make sure you have the appropriate dongle if you need one.)

Skill Level: Intermediate

Prerequisites for students:

- Students must be able to write basic Python scripts and have a basic understanding of the Windows operating system. - Familiarity with a Windows malware, debugging, and assembly would also be a significant benefit.

Materials or Equipment students will need to bring to participate: - Students must bring a laptop capable of running a Windows virtual machine with the following configuration. Time will be given to troubleshoot lab setup issues but it is strongly recommended that students have the following setup prior to the workshop.

[Host Setup]

- The laptop must have VirtualBox or VMWare installed and working prior to class. - The laptop must have at least 60GB of disk space free. - The laptop must be able to mount USB storage devices (ensure you have the appropriate dongle if you need

one).

[VM Install]

- Download a free Windows 11 VM from Microsoft (<https://developer.microsoft.com/en-u...tual-machines/>) - You can also use a Windows VM of your choice (Windows 10 is also ok)

[VM Install for Mac - Apple Silicon Only (M1, M2)] - If you have a new Apple Silicon MacBook you will be limited to running an ARM Windows VM - ARM Windows VMs are suitable for the workshop and you can follow our installation guide on YouTube (<https://youtu.be/0eR8yrDLV5M>)

[VM Setup]

- Install x64dbg in your VM (<https://x64dbg.com/>) - Install a free version of IDA in your VM (<https://hex-rays.com/ida-free/>) - Install a version of Python > 3.8.x in your VM (<https://www.python.org/>)

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: AppSec Village Keynote: Collaborative Security: Fostering Innovation and Resilient Cyber Practices

When: Saturday, Aug 12, 10:00 - 10:59 PDT

Where: Flamingo - Savoy - AppSec Village - [Map](#)

SpeakerBio: Maril Vernon

Maril Vernon (@SheWhoHacks) known as the "One Woman Purple Team" is an award-winning Ethical Hacker, Senior Application Security Architect and Purple Team Program Manager — a niche in offensive security testing that has recently gained popularity demonstrating cyber resilience in the advanced threat landscape. Maril is also Co-host and Co-founder of The Cyber Queens Podcast, an all-female-lead podcast aimed at increasing female and LGBTQ diversity in cybersecurity. She also serves as the COO of Teach Kids Tech, a non-profit organization with the goal of getting technology and its educational resources to children in underprivileged communities and increasing technical capability and cyber awareness in tomorrow's workforce. Maril has been named one of the 'Epic Women in Cyber,' 2023 CyberSHEcurity "Top 10 Women in Cyber," 2023 Women's CyberJustu Pentest Ninja Award winner, and is a finalist for Cybersecurity woman of the Year: Hacker of the Year and Cybersecurity Woman of the World 2023! She is also an SME and contributing writer to CSO Online magazine on cyber resilience, Purple and Red Team best practices and industry trends. Maril's passion for closing the gender gap in cyber is further highlighted in her affiliations with The Cyber Guild, The Diana Initiative, BBWIC, and WiCyS.

Twitter: [@shewhohacks](#)

Description:

In the journey of life, we all encounter challenges and setbacks that put our resiliency to the test. Resilience, the ability to bounce back from adversity, is a vital trait that empowers individuals to navigate life's trials with grace and strength. At the heart of building this essential attribute lies the power of relationships. As they say, oftentimes trials of life "take a village." The same is true with information security in the digital age.

The keynote "Collaborative Security" delves into the parallel benefits between the foundational pillars of fostering resilient relationships and cybersecurity principles. How often do organizations suffer from silos across verticals that should be information sharing and collaborating?

Resilient relationships create a supportive ecosystem where teams can learn from failures, adapt to emerging threats, and continuously improve cyber strategies. By breaking down silos and bringing together diverse perspectives, collaborative security fosters a culture of creativity and problem-solving. Witness how collaborative efforts among teams and organizations lead to breakthrough ideas and cutting-edge solutions. As innovation and collaboration intertwine, we see the emergence of more resilient cyber infrastructures and practices.

At the end of the day tech and cyber are still people industries. Discover how resilient relationships translate into fortified cyber practices, safeguarding critical assets and bolstering organizational resilience.

Join us for an enlightening and inspiring journey into the heart of collaborative security, where resilient relationships fuel innovation, fortify infrastructure, and pave the way for a safer cyber landscape. Together, we will embrace the collaborative spirit and ignite the spark of innovation to protect the digital realm from ever-evolving threats.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: AppSec Village Keynote: From Camels to Collaboration, A Journey Through Technology AND Humans

When: Friday, Aug 11, 10:00 - 10:59 PDT

Where: Flamingo - Savoy - AppSec Village - [Map](#)

SpeakerBio:Chris Roberts

Chris is the CISO for Boom Supersonic and works as an advisor for several entities and organizations around the globe. His most recent projects are focused within the aerospace, deception, identity, cryptography, Artificial Intelligence, and services sectors. Over the years, he's founded or worked with several folks specializing in OSINT/SIGINT/HUMINT research, intelligence gathering, cryptography, and deception technologies. These days he's working on spreading the risk, maturity, collaboration, and communication word across the industry. (Likely while coding his EEG driven digital clone that's monitoring his tea and biscuit consumption!)

Since the late 90's Chris has been deeply involved with security R&D, consulting, and advisory services in his quest to protect and defend businesses and individuals against various types of attack. Prior to that he jumped out of planes for a living, visiting all sorts of interesting countries and cultures while doing his best to avoid getting shot at too often. (Before that, he managed to get various computers confiscated by several European entities.)

He's considered one of the world's foremost experts on counter threat intelligence and vulnerability research within the Information Security industry. He's also gotten a name for himself in the transportation arena, basically anything with wings, wheels, tracks, tyres, fins, props or paddles has been the target for research for the last 15 years. (To interesting effect.)

Twitter: [@Sidragon1](#)

Description:

Let's face it, it's all connected, talking to us, with us, and behind our backs (we CAN go all paranoid on AI if we want to go down that rabbit hole.) However, the situation's not changing, it's evolved beyond any one person/team's ability to understand, and we as an industry still chase our tails around, pointing fingers, and chasing technology like a rabid, over caffeinated squirrel.

So, what do we do? Piecemeal solutions, buy more empty promises, or can we take a step back, breath and talk about the hoomans in the equation?

Let's explore some of the tech challenges, and a more human centric approach to solving things. I promise we'll have exploits, hacks, and tasers, but we're going to throw in communication, collaboration, cooperation, and maybe a shout out on all of US going out to the greater village community and bringing us all a little closer together. After all, we're ALL in this together, it might be nice to start acting like it.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 21:00-01:59 PDT

Title: Arcade Party

When: Saturday, Aug 12, 21:00 - 01:59 PDT

Where: Caesars Forum - Forum - 105,136 - [Map](#)

Description:

The Arcade Party is back! Come play your favorite classic arcade games while jamming out to Keith Myers DJing. Your favorite custom built 16 player LED foosball table will be ready for some competitive games. This epic party, free for DEF CON 31 attendees to enjoy and play, is hosted by the Military Cyber Professionals Association (a tech ed charity) and friends.

[Return to Index](#) - Add to  - ics [Calendar](#) file

BICV - Friday - 16:00-16:50 PDT

Title: Are you really eyeing my network? Network Reconnaissance for n00bs!

When: Friday, Aug 11, 16:00 - 16:50 PDT

Where: Caesars Forum - Alliance - 301-304 - Blacks in Cyber Village - [Map](#)

SpeakerBio:RJ McCarley

No BIO available

Description:

During this hands-on lab, participants will learn the fundamentals of the basics of network reconnaissance in Penetration Testing. The course will focus on practical scenarios and real-world examples to ensure participants gain practical skills that can be applied in their day-to-day work.

Prerequisites: Basic understanding of computer networks, cyber security concepts, command line interface, and operating systems.

Tools Covered:

- Nmap
- Theharvester
- Wireshark
- Nessus
- Metasploit

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: ARINC 615a CTF

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

ARINC 615a CTF

Boeing

****Laptop Needed****

Boeing will be hosting an ARINC 615a dataload CTF broken into two major modules. The first module will focus on decomposing and analyzing a PCAP capture of a simulated dataload between an airplane dataload server and an avionics component. The second module will allow participants to execute a dataload against simulated avionics to help improve understanding and awareness of how software is loaded onto airplanes. Additionally, Boeing is aiming to increase its cyber outreach into the STEM community by offering an additional challenge centered on an operational system and the impact of that system on the overall airplane. The challenge will walk participants through how the operational system functions, how it can be negatively impacted, the results of tampering with the system while it's in flight, and how the system can be secured via CIA and PKI.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: ARINC 615a CTF

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

ARINC 615a CTF

Boeing

****Laptop Needed****

Boeing will be hosting an ARINC 615a dataload CTF broken into two major modules. The first module will focus on decomposing and analyzing a PCAP capture of a simulated dataload between an airplane dataload server and an avionics component. The second module will allow participants to execute a dataload against simulated avionics to help improve understanding and awareness of how software is loaded onto airplanes. Additionally, Boeing is aiming to increase its cyber outreach into the STEM community by offering an additional challenge centered on an operational system and the impact of that system on the overall airplane. The challenge will walk participants through how the operational system functions, how it can be negatively impacted, the results of tampering with the system while it's in flight, and how the system can be secured via CIA and PKI.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: ARINC 615a CTF

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

ARINC 615a CTF

Boeing

****Laptop Needed****

Boeing will be hosting an ARINC 615a dataload CTF broken into two major modules. The first module will focus on decomposing and analyzing a PCAP capture of a simulated dataload between an airplane dataload server and an avionics component. The second module will allow participants to execute a dataload against simulated avionics to help improve understanding and awareness of how software is loaded onto airplanes. Additionally, Boeing is aiming to increase its cyber outreach into the STEM community by offering an additional challenge centered on an operational system and the impact of that system on the overall airplane. The challenge will walk participants through how the operational system functions, how it can be negatively impacted, the results of tampering with the system while it's in flight, and how the system can be secured via CIA and PKI.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Arson Herders: An IR Guide to Fighting and Lighting Fires

When: Saturday, Aug 12, 15:45 - 16:45 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Main Stage - [Map](#)

Speakers: Litmoose, Matt "dis0wn" Wagenknecht, Tina "Mugwump Jones" Velez, Unnamed user

SpeakerBio: Litmoose

Cats and violins.

SpeakerBio: Matt "dis0wn" Wagenknecht

Experienced in penetration testing, red team activities, and incident response

SpeakerBio: Tina "Mugwump Jones" Velez

A caffeinated muppet with a day job of Enterprise Field Strategist/Chief Taco Officer for Expel and a night job of maybe being The Batman.

SpeakerBio: Unnamed user

No BIO available

Description:

.

Join three of our seasoned (and sometimes crispy) Digital Forensics and Incident Response heavy hitters as they relay their tales from the front lines fighting against active threat actors, insider oopsies, and general misconfigurations. The catch? A holistic approach to security can involve lighting some fires of your own. The discussion will cover how the hot, hot flames of an incident touch everyone -- from C-levels to admins, intel to the red team. Come bask in the warm glow (while enjoying the cool Vegas AC), and be sure to stay for the Q & A!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Friday - 12:00-12:30 PDT

Title: Art vs AI: How Artists Hack Computer Vision Systems

When: Friday, Aug 11, 12:00 - 12:30 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio:Kate

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Artificial Intelligence and Race: Security or Surveillance?

When: Friday, Aug 11, 13:00 - 13:50 PDT

Where: Caesars Forum - Alliance - 301-304 - Blacks in Cyber Village - [Map](#)

SpeakerBio: Fatou Sankare

Fatou Sankare graduated with a Bachelor of Arts in Political Science from Howard University and received her Master of Science in Cybersecurity at Fordham University. Fatou Sankare is currently a Doctoral Candidate in Cybersecurity at Marymount University.

Currently, Fatou is a government contractor working as a Cyber Crime Data Scientist. She is also an Assistant Professor of Cybersecurity and Director of the Cybersecurity Labs at Capitol Technology University.

Fatou is also the founder of Datacation LLC — with a mission to increase cyber education particularly in low-income neighborhoods. Fatou is a Certified Ethical Hacker and currently holds the AWS Machine Learning Specialty Certification.

Description:

Today, with the advancement of technology, investigative searches are not only physical but also digital. With electronic devices such as cellphones and computers no longer being considered a luxury device but an essential device, law enforcement is now relying on evidence extracted from these items in criminal investigations. Digital devices contain massive amounts of data that can be useful in not only criminal matters but national security-related instances as well. The problem is that the data on these devices contain information that may be deemed private to citizens. Law enforcement has been using the Fourth Amendment to justify their use of digital evidence. However, the Fourth Amendment does not explicitly factor in digital evidence. The policies are not up to date with the procedures used by law enforcement, and citizens may be paying for it through the invasion of privacy. With the increased use of artificial intelligence, the biggest question becomes is it security or surveillance, and which communities are negatively impacted or targeted?

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Artificial Intelligence for Red Team Operations

When: Sunday, Aug 13, 09:00 - 10:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 4 - [Map](#)

SpeakerBio: Peter Halberg

No BIO available

Twitter: [@MiloSilo_Hacks](#)

Description:

The integration of artificial intelligence (AI) into red team operations has revolutionized the way cybersecurity professionals approach their work. This workshop will equip participants with the necessary skills and understanding to leverage AI tools effectively throughout different stages of red team operations.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Artificial Intelligence for Red Team Operations

When: Saturday, Aug 12, 11:00 - 12:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 6 - [Map](#)

SpeakerBio: Peter Halberg

No BIO available

Twitter: [@MiloSilo_Hacks](#)

Description:

The integration of artificial intelligence (AI) into red team operations has revolutionized the way cybersecurity professionals approach their work. This workshop will equip participants with the necessary skills and understanding to leverage AI tools effectively throughout different stages of red team operations.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Saturday - 10:00-17:59 PDT

Title: Ask Me Anything About Cybersecurity in Aerospace

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

Ask Me Anything About Cybersecurity in Aerospace

AIAA

We have added a special feature to this year's activities during DEF CON 31. This will be on Friday and Saturday from 11AM - 5PM.

Our friends at AIAA are helping us host "Ask Me Anything" sessions on Friday and Saturday. It's an opportunity to meet Aerospace Village members and partners who are experts in the field. Bring your questions about getting into cybersecurity, aviation, space, likes/dislikes, you name it!

- A chance to ask all your questions, get their perspective, and hear some great stories.
- A low-key sharing of experiences and a way to make new friends without having to make small talk.
- Note: This is NOT a recruiting activity. Ask career questions if you have them, but think of this more as a chance for general "speed mentoring."

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Sunday - 10:00-13:59 PDT

Title: Ask Me Anything About Cybersecurity in Aerospace

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

Ask Me Anything About Cybersecurity in Aerospace

AIAA

We have added a special feature to this year's activities during DEF CON 31. This will be on Friday and Saturday from 11AM - 5PM.

Our friends at AIAA are helping us host "Ask Me Anything" sessions on Friday and Saturday. It's an opportunity to meet Aerospace Village members and partners who are experts in the field. Bring your questions about getting into cybersecurity, aviation, space, likes/dislikes, you name it!

- A chance to ask all your questions, get their perspective, and hear some great stories.
- A low-key sharing of experiences and a way to make new friends without having to make small talk.
- Note: This is NOT a recruiting activity. Ask career questions if you have them, but think of this more as a chance for general "speed mentoring."

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Friday - 10:00-17:59 PDT

Title: Ask Me Anything About Cybersecurity in Aerospace

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

Ask Me Anything About Cybersecurity in Aerospace

AIAA

We have added a special feature to this year's activities during DEF CON 31. This will be on Friday and Saturday from 11AM - 5PM.

Our friends at AIAA are helping us host "Ask Me Anything" sessions on Friday and Saturday. It's an opportunity to meet Aerospace Village members and partners who are experts in the field. Bring your questions about getting into cybersecurity, aviation, space, likes/dislikes, you name it!

- A chance to ask all your questions, get their perspective, and hear some great stories.
- A low-key sharing of experiences and a way to make new friends without having to make small talk.
- Note: This is NOT a recruiting activity. Ask career questions if you have them, but think of this more as a chance for general "speed mentoring."

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Ask the EFF

When: Friday, Aug 11, 20:00 - 21:59 PDT

Where: Caesars Forum - Forum - 130-131,134 - [Map](#)

Speakers: Cooper Quintin, Corynne McSherry, Hannah Zhao, Mario Trujillo, Rory Mir

SpeakerBio: Cooper Quintin , Senior Staff Technologist at Electronic Frontier Foundation

Cooper Quintin is a security researcher and senior public interest technologist with the EFF Threat Lab. He has worked on projects including Privacy Badger, Canary Watch, and analysis of state sponsored malware campaigns such as Dark Caracal. Cooper has given talks at security conferences including Black Hat, DEFCON, Enigma Conference, and ReCon about issues ranging from IMSI Catcher detection to fem tech privacy issues to newly discovered APTs. He has also been published or quoted in publications including: The New York Times, Reuters, NPR, CNN, and Al Jazeera. Cooper has given security trainings for activists, non profit workers, and vulnerable populations around the world. He previously worked building websites for nonprofits, including Greenpeace, Adbusters, and the Chelsea Manning Support Network. Cooper was also an editor and contributor to the hacktivist journal, "Hack this Zine." In his spare time he enjoys making music, visualizing a solar-punk anarchist future, and playing with his kids.

Twitter: [@cooperq](#)

SpeakerBio: Corynne McSherry , Legal Director at Electronic Frontier Foundation

As EFF's Legal Director, McSherry has extensive experience in advocating for digital civil liberties and promoting net neutrality. Her perspective on the legal frameworks shaping the digital landscape will provide DEF CON attendees with insights on regulatory issues affecting technology users.

Twitter: [@cmcsherr](#)

SpeakerBio: Hannah Zhao , Staff Attorney at Electronic Frontier Foundation

Hannah is a staff attorney at the Electronic Frontier Foundation. She's part of EFF's Coders' Rights Project, which seeks to protect hackers, security researchers, and others through education, legal defense, amicus briefs, and involvement in the community with the goal of promoting innovation and safeguarding the rights of curious tinkerers and hackers on the digital frontier. She also works on legal issues related to police technology, surveillance, and cybersecurity.

SpeakerBio: Mario Trujillo , Staff Attorney at Electronic Frontier Foundation

As a Staff Attorney on EFF's civil liberties team, he has an expertise focusing on the Fourth Amendment and privacy rights. He is also part of EFF's Coders' Rights Project. Prior to joining EFF, he was an attorney at the privacy law firm ZwillGen and clerked for a federal magistrate judge on the southern border.

SpeakerBio: Rory Mir , Associate Director of Community Organizing at Electronic Frontier Foundation

As EFF's Associate Director of Community Organizing, Rory works on the EFF activism team to engage community groups on tech policy issues and building community around our issues. This includes our work with the Electronic Frontier Alliance, which directly supports these groups — including a number of local DEFCON groups. Immersed in the community, Rory is familiar with the needs and issues commonly faced by the community. and how it connects to EFF issues.

Description:

Electronic Frontier Foundation (EFF) is thrilled to return to DEF CON 31 to answer your burning questions on pressing digital rights issues. Our panelists will provide updates on current EFF work, including the fight against government surveillance and protecting creative expression, before turning it over to attendees to pose questions and receive insights from our panelists on the intersection of technology and civil liberties. This is a valuable opportunity to learn from policy experts and engage in a lively discussion rooted in the problems you face. This year you'll meet: Corynne McSherry, EFF's Legal Director specializing in intellectual property and free speech; Hannah Zhao, staff attorney focusing on criminal justice and privacy issues; Mario Trijillo, staff attorney with an expertise in privacy law; Rory Mir, Associate Director of Community Organizing; and Cooper Quintin, security researcher and public interest technologist with the EFF Threat Lab.

Title: Assessing the Security of Certificates at Scale

When: Saturday, Aug 12, 09:00 - 09:20 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

Speakers: Andrew Chi, Brandon Enright, David McGrew

SpeakerBio: Andrew Chi , Security Research Engineering Technical Leader at Cisco

Andrew Chi is a Security Research Engineering Technical Leader at Cisco, where he works with product teams and incident response teams to detect threats in large network telemetry datasets. Prior to Cisco, he was a computer scientist at Raytheon BBN Technologies, where he contributed to IETF standards for routing security (RPKI and BGPSEC) and served as software lead for an open-source RPKI validator. Andrew holds a bachelor's degree in mathematics from Harvard and a PhD in computer science from the University of North Carolina.

SpeakerBio: Brandon Enright , Lead DIFR investigator at Cisco CSIRT

Brandon Enright is a lead DIFR investigator for Cisco CSIRT, an expert at DNS and network data analysis, and a contributor to Nmap and other open source projects.

SpeakerBio: David McGrew , Fellow at Cisco Systems

David McGrew is a Fellow at Cisco Systems, where he leads research and development to detect threats, vulnerabilities, and attacks using network data, and to protect data through applied cryptography. He pioneered the commercial use of encrypted traffic analysis to defend networked information systems, and designed authenticated encryption and secure voice and video standards that are in widespread use, most notably GCM and Secure RTP, contributed to open source projects, published research results, championed open, patent/royalty-free cryptography, and co-founded the IRTF Crypto Forum Research Group. He holds a PhD in Physics from Michigan State University, and outside of work, he enjoys Linux, sailing, sports cars, jazz records, and guitar.

Description:

The security of digital certificates is too often undermined by the use of poor entropy sources in key generation. Flawed entropy can be hard to discover, especially when analyzing individual devices. However, some flaws can be detected when a large set of keys from the same entropy source are analyzed, as was dramatically demonstrated in 2012 and 2016 by the detection of weak HTTPS keys on the Internet.

In this talk, we present tools and techniques to identify weak keys at scale, by checking issued certificates obtained from passive monitoring, active network scans, or certificate authority logs. Our tools use efficient multithreaded implementations of network monitors, scanners, certificate parsers, and mathematical tests. The batch greatest common divisor test (BGCD) identifies RSA public keys with common factors, and outputs the corresponding private keys. The common key test identifies distinct devices that share identical keys. We report on findings from both tests and demonstrate how to audit HTTPS servers, run BGCD on 100M+ keys, identify RSA keys with common factors, and generate the corresponding private keys. Because nothing convinces like an attack, we show how to produce and use PEM files for factored keys.

REFERENCES:

Andrew Chi, Brandon Enright, David McGrew. The Mercury Batch GCD Utility.

<https://github.com/cisco/mercury/blob/main/doc/batch-gcd.md> David McGrew, The Mercury cert_analyze Utility.

https://github.com/cisco/mercury/blob/main/src/cert_analyze.cc David McGrew, Blake Anderson. The Mercury tls_scanner Utility. https://github.com/cisco/mercury/blob/main/src/tls_scanner.cc Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. Mining your ps and qs: Detection of widespread weak keys in network devices. In Tadayoshi Kohno, editor, Proceedings of the 21th USENIX Security Symposium, Bellevue, WA, USA, August 8-10, 2012, pages 205–220.

USENIX Association, 2012. <https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/heninger>.

Marcella Hastings, Joshua Fried, and Nadia Heninger. Weak keys remain widespread in network devices. In Phillipa Gill, John S. Heidemann, John W. Byers, and Ramesh Govindan, editors, Proceedings of the 2016 ACM on Internet Measurement Conference, IMC 2016, Santa Monica, CA, USA, November 14-16, 2016, pages 49–63.



[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

Title: Assessing the Vulnerabilities of the Open-Source Artificial Intelligence (AI) Landscape: A Large-Scale Analysis of the Hugging Face Platform

When: Friday, Aug 11, 12:00 - 12:25 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

Speakers: Adhishree Kathikar, Aishwarya Nair

SpeakerBio: Adhishree Kathikar

No BIO available

SpeakerBio: Aishwarya Nair

No BIO available

Description:

Artificial Intelligence (AI) has earned its title as one of the most critical disruptive technologies in the 21st century. As AI develops at a rapid rate, open-source software (OSS) platforms develop alongside it. Hugging Face is one of these prevailing OSS platforms as it hosts pre-trained AI models, facilitating the accessibility of AI models. Hugging Face is used by over 22,000 organizations, including Intel and Microsoft, has supported more than 2.6 billion model downloads, and is rapidly growing. Just in the past year, Hugging Face has more than doubled its model library from 80,000 models to 203,000 models. However, while Hugging Face democratizes access to AI models, these models may contain unknown security vulnerabilities. Our research focuses on automating our collection process of Hugging Face models, linking them to their primary codebases on GitHub, and executing a large-scale vulnerability assessment of these GitHub repositories using static scanners. We collected more than 110,000 Hugging Face models and over 29,000 GitHub repositories. Our vulnerability assessment of these GitHub models depicted that 35.98% of the severities detected from the root GitHub repositories (developed by Hugging Face) were high-severity vulnerabilities while only 6.79% were low-severity. On the other hand, 82.89% of vulnerabilities from searched repositories (determined through the 'huggingface' keyword) are low-severity and 7.49% high-severity, while 82.69% of vulnerabilities from the repositories forked from the root repositories were low-severity and 9.22% were high-severity. The trend in severity levels found in root repositories contradicts the results of severities detected in forked and searched repositories. Given that many of the vulnerabilities reside in fundamental AI repositories such as Transformers, this vulnerability assessment has significant implications for supply chain software security and AI risk management more broadly.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Attack Surface Framework

When: Friday, Aug 11, 14:00 - 15:55 PDT

Where: Caesars Forum - Council Boardroom - Demo Labs - [Map](#)

Speakers:Mike Henkelman,Prajwal Panchmahalkar

SpeakerBio:Mike Henkelman

Mike Henkelman is a Sr Manager, Vulnerability Management Global at VMWare Inc. He began his career as a MCSE certified systems administrator in the mid 90's before joining Cisco Systems and working in the IPABU on the edge development team for the 2600 series router and 3500 series switch and authoring white papers on CEF. Going on to manage several enterprise data centers, he later began focusing on information security and managed Vulnerability Management programs for companies that include Pivotal Software before joining VMWare where his team mitigates risk for one of corporate America's largest asset libraries with audit attestations that include FedRAMP IL5 High, CE+, I24, IRAP, PCI-DSS among nearly two dozen others.

SpeakerBio:Prajwal Panchmahalkar

Prajwal Panchmahalkar is a Technical Director, Red Team at VMware Inc., He has contributed to public security research and has been the Development Lead for Matriux since 2009. In the past he was a Research Assistant at Texas Tech University working on Security of Critical Infrastructure and Smart Grid Energy Systems, with a journal published on Elsevier. A Finalist for America's Information Security Leadership Award 2012 (AISLA) by (ISC)2. Previously Prajwal was a speaker at BlackHat Arsenal, c0c0n, BSidesLV and GrrCon. Currently on review board for c0c0n, India. He was a chapter lead for nlu, Hyderabad an open security community. Prajwal holds a Masters degree in Computer Science from the Texas Tech University, Lubbock.

Description:

Attack Surface Framework (ASF) aims to protect organizations acting as an attack surface watchdog. The Attack Surface Framework (ASF) was developed with motivation to automate and address vulnerabilities through continuous scanning and tracking risks at scale, in a comprehensive and adaptable approach, particularly against 0-day vulnerabilities with publicly available POCs. The Attack Surface Framework (ASF) is a modular, extensible, and customizable framework designed to help organizations manage their public attack surface risks. ASF will auto-discover assets such as network subnets, domains including subdomains, enumerate their ports and services, track deltas and serve as a continuous and flexible, attacking and alerting framework, leveraging another layer of support. ASF provides modules for attack surface management including asset discovery and management, asset enumeration, vulnerability scanning, and vulnerability testing. ASF is equipped with a set of CLI tools and an API, enabling users to interact with the framework and integrate it with other tools and processes. Additionally, ASF includes a web-based user interface for visualizing an organization's attack surface and managing vulnerabilities.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Attacking Decentralized Identity

When: Friday, Aug 11, 13:00 - 13:45 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

Speakers: Brent Zundel, Gabe Cohen

SpeakerBio: Brent Zundel

No BIO available

SpeakerBio: Gabe Cohen

No BIO available

Description:

Decentralized identity systems based on W3C Decentralized Identifiers and Verifiable Credentials are becoming increasingly popular for their promises of improved security, privacy, and user control in identity management. Impactful deployments are coming: from the US DHS for worker authorization and soon passports, multiple DMVs for driver's licenses, the EU for university degree credentials, and much more in both public and private sectors. However, as with any technology, these systems are not immune to vulnerabilities and attacks, both on the ideologies of decentralization and self-sovereignty and vulnerabilities in implemented systems.

In this talk, we will examine different types of vulnerabilities in the SSI space, walk through examples of potential attacks, and discuss the potential consequences of the technology. Additionally, we will explore potential solutions to mitigate the risks associated with these vulnerabilities. We will discuss best practices for trust, cryptographic techniques, and security protocols that one can use in decentralized identity systems.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Attacks as a Service with The DeRF

When: Friday, Aug 11, 12:30 - 12:59 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Kat Traxler , Principal Security Researcher at Vectra AI

Kat Traxler is the Principal Security Researcher at Vectra AI focusing on threat detection in the public cloud. Prior to her current role, she worked in various stages in the SDLC performing web application penetration testing and security architecture design for Web, IAM, Payment Technologies and Cloud Native Technologies.

Kat's research philosophy directs her attention to where design flaws and misconfigurations are most probable. This guiding principle leads her research to the intersection of technologies, particularly the convergence of cloud security and application security and where the OS-layer interfaces with higher-level abstractions.

Kat has presented at various conferences including the SANS CloudSecNext Summit and fwd:CloudSec on topics such as privilege escalation in GCP, and bug-hunting in the cloud. In addition to her work at Vectra AI, she is a member of IAN Faculty and the Lead Author of the SANS SEC549 - Enterprise Cloud Security Architecture and currently holds multiple GIAC certifications. You can find her on the internet as @nightmareJS

Twitter: [@NightmareJS](#)

Description:

Introducing the DeRF (Detection Replay Framework), a tool which hosts attack techniques and supports the invocation of those attacks across cloud environments. What sets DeRF apart from other cloud attack tools?

- User-Friendly Interface: Since the DeRF is hosted in Google Cloud, End Users can invoke attacks through the cloud console UI without the need to install software or use the CLI.
- Accessibility for Non-Security Professionals: The DeRF caters to a broad audience of End Users, including Engineering, Sales, Support Staff or automated processes.
- Robust OpSec: Long-Lived Credentials are not passed between operators, instead access to the DeRF and its attack techniques are controlled through GCP IAM Role-Based Access Control (RBAC)
- Extensibility at its Core: Attack sequences are written in YAML, enabling easy configuration of new techniques.
- Turn-Key deployment: Deploying (and destroying!) the DeRF is a fully automated process, completed in under 3 minutes.

During this demo, we will guide you through the straightforward and automated deployment process for the DeRF. We'll demonstrate how to invoke pre-configured attack techniques and illustrate how you can customize the framework to align with your internal attacker profile. By deploying the DeRF within your organization you can easily spin up attacker simulations, to augment training or automate the testing of detection capabilities.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: AutoDriving CTF

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

AutoDriving CTF is a Jeopardy style of CTF game with a set of challenges specific to self-driving functions and components. The contest offers participants the ability to use a simulation-based autonomous driving environment (based on the open-source simulators; e.g., LGSVL and CARLA) and explore specific attacks (such as camouflage stickers, road graffiti, and sensor spoofing/hijacking) as well as defense strategies.

We hope to continue the engagement with the hacking community to demonstrate security implications of autonomous driving system design decisions through hands-on challenges, increase the awareness of potential risks in security professionals, and encourage them to propose defense solutions and tools to detect such risks.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Automotive USB Fuzzing: How to fuzzing USB in vehicles to discover the real-world vulnerabilities

When: Saturday, Aug 12, 11:00 - 11:40 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

Speakers: Donghyeon Jeong, Euntae Jang, Jonghyuk Song

SpeakerBio: Donghyeon Jeong

No BIO available

SpeakerBio: Euntae Jang

No BIO available

SpeakerBio: Jonghyuk Song

Jonghyuk Song is a director of Vehicle Threat Research laboratory at AUTOCRYPT. He is an offensive security researcher and, he presented at Defcon30 main talk and Defcon30 CHV. He is also a CTF player (Defcon CTF finalist 2009, 2011, 2017).

Description:

Recently, automotive industry is performing USB fuzzing in an inefficient way for automobiles. Usually, fuzzing is performed by commercial media fuzzers, but the fuzzers are not directly connected to the vehicle during fuzzing. So, it requires much manual efforts of testers.

In this talk, we propose efficient way to perform USB fuzzing to actual vehicles. We describe how to perform USB fuzzing to kernel area fuzzing as well as media fuzzing by directly connecting the fuzzer and the car with a USB cable. By this method, we found real-world vulnerabilities in Volkswagen Jetta, Renault Zoe, GM Chevrolet Equinox, and AGL.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Azure AD recon with OSINT tools

When: Saturday, Aug 12, 14:25 - 15:10 PDT

Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio: Nestori Syynimaa , Senior Principal Security Researcher at Secureworks

Dr Nestori Syynimaa is one of the leading Azure AD / M365 experts in the world and the developer of the AADInternals toolkit. He has worked with Microsoft cloud services for over a decade and has been MCT since 2013, MVP since 2020, and awarded Microsoft Most Valuable Security Researcher for 2022. Currently, Dr Syynimaa works as a Senior Principal Security Researcher for Secureworks Counter Threat Unit. Before moving to his current position, Dr Syynimaa worked as a CIO, consultant, trainer, researcher, and university lecturer for almost 20 years. Dr Syynimaa has spoken in many international scientific and professional conferences, including IEEE TrustCom, Black Hat (USA, Europe, and Asia), Def Con, and RSA Conference.

Twitter: [@DrAzureAD](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Azure B2C 0-Day: An Exploit Chain from Public Keys to Microsoft Bug Bounty

When: Saturday, Aug 12, 13:00 - 13:45 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

SpeakerBio: John Novak , Technical Director at Praetorian

John Novak is a Technical Director at Praetorian with a deep interest in cryptography, reverse engineering, and embedded firmware. His evolution to computer security and hacker culture began with an undergraduate degree in mathematics followed by ten years of cryptography, security research, and exploit development at a previous employer. His current role at Praetorian includes conducting numerous security assessments for IoT devices, web applications, mobile applications, and (on occasion) cloud services.

Twitter: [@jwnovak](#)

Description:

This presentation will cover a complete exploit chain in Azure B2C, starting with a discovery of cryptographic misuse and leading to full account compromise in any tenant as an unauthenticated attacker.

Portions of this vulnerability have been released publicly, but several pieces were omitted to provide Microsoft time to remediate the issue and not put Azure B2C environments at unnecessary risk. New details in this talk include steps to reverse engineer and discover the crypto vulnerability along with details of a novel attack for crypto key recovery.

For background, Microsoft Azure B2C is an identity and access management service for customer-facing apps. Thousands of organizations use this service, including national/state/local governments, professional societies, and commercial companies. The service is also used in the public Microsoft Security Response Center (MSRC) web portal as the main method for researchers to disclose vulnerabilities as part of Microsoft's bug bounty programs. The full exploit chain was effective against the MSRC and would have allowed an attacker to enumerate details of disclosed but not-yet-patched Microsoft zero day vulnerabilities.

REFERENCES:

[1] Previous disclosure of portions of this vulnerability:

<https://www.praetorian.com/blog/azure-b2c-crypto-misuse-and-account-compromise/> [2] Discussion of encryption and signatures in JSON Web Tokens (JWTs): <https://www.praetorian.com/blog/signing-and-encrypting-with-json-web-tokens/> [3] Azure B2C Configuration Tutorial:

<https://learn.microsoft.com/en-us/azure/active-directory-b2c/tutorial-create-user-flows?pivots=b2c-custom-policy> [4] What to Expect When Reporting Vulnerabilities to Microsoft

<https://msrc.microsoft.com/blog/2020/09/what-to-expect-when-reporting-vulnerabilities-to-microsoft/>

Return to [Index](#) - Add to  - ics [Calendar](#) file

Title: Azure DevOps Security

When: Friday, Aug 11, 13:25 - 14:05 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Viktor Gazdag

Viktor Gazdag has worked as pentester and security consultant for 8 years, lead cloud research working group and M365 capability service. He has reported numerous vulnerabilities in products from companies such as Oracle, SAP, Atlassian, Jenkins, CloudBees Jenkins, JetBrains, Sonatype, as well as hundreds of plugin vulnerabilities in Jenkins Plugins. In 2019, he received the Jenkins Security MVP award. He gave a talk about the research behind finding more than a 100 Jenkins Plugin vulnerabilities at DevOps World. He also gave a presentation at Black Hat USA and DoD CyberDT XSWG about CI/CD pipeline compromises. He also holds multiple AWS/Azure/GCP, Infra as Code, DevOps and Hacking certifications.

Description:

Companies move their development environment from on-prem to the cloud as well. One of the solutions is Azure DevOps (ADO). ADO provides same or similar service that are already existed on-prem such as ticketing, wiki, repository, pipeline, artifacts etc.

There is a difference between security in the pipeline and security of the pipeline. As a security consultant/pentester we saw both ends and came across these environments either in assumed breach, configuration review or SDL assessment.

In this talk, we take a look at the later and review the security controls for Azure DevOps (although can be used for other cloud providers as well) that can help in mitigating attacks and the blast radius of a breach. There will be also some resources shared where to go after the talk.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Backdoor in the Core - Altering the Intel x86 Instruction Set at Runtime

When: Friday, Aug 11, 12:30 - 13:15 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

Speakers: Alexander Dalsgaard Krog, Alexander Skovsende

SpeakerBio: Alexander Dalsgaard Krog , Vulnerability Researcher at Vectorize

Alexander Dalsgaard Krog is a Vulnerability Researcher at Vectorize with a focus on the low level, close to the hardware, and this talk will be no exception. He has a passion for binary exploitation and together with his prior team at Lyrebirds discovered the critical bug Cable Haunt, affecting millions of devices with a vulnerability allowing remote code execution. Both him and his co-speaker Alexander Skovsende are also heavily invested in CTF and have played a big role in putting the Danish team Kalmarunionen on top of the scoreboard in many CTFs.

Twitter: [@alexanderkrog](#)

SpeakerBio: Alexander Skovsende , Grad Student at Technical University of Denmark

No BIO available

Description:

In this work, we present the novel results of our research on Intel CPU microcode. Building upon prior research on Intel Goldmont CPUs, we have reverse-engineered the implementations of complex x86 instructions, leading to the discovery of hidden microcode which serves to prevent the persistence of any changes made. Using this knowledge, we were able to patch those discovered sections, allowing us to make persistent microcode changes from userspace on Linux. We have developed and improved microcode tracing tools, giving us deeper insight into Intel Atom microcode than was previously possible, by allowing more dynamic analysis of the ROM.

Along with this presentation, we provide a C library for making microcode changes and documentation on the reverse-engineered microcode.

We show that vendor updates to the microcode, which cannot be verified by the user, impose a security risk by demonstrating how a Linux system can be compromised through a backdoor within a CPU core's microcode.

REFERENCES:

Intel TXE POC:

<https://github.com/chip-red-pill/IntelTXE-PoC> Exploit used to gain Red Unlock.

uCodeDisasm

<https://github.com/chip-red-pill/uCodeDisasm> First research (to the best of our knowledge) allowing for dumping microcode ROM as well as a publicly available disassembler for Intel's microcode.

Undocumented x86 instructions to control the CPU at the micro-architecture level in modern Intel processors:

<https://github.com/chip-red-pill/udbgInstr>

https://github.com/chip-red-pill/udbgInstr/blob/main/paper/undocumented_x86_insts_for_uarch_control.pdf From the research above, two undocumented instructions intended for debug perpose at Intel were found. This layed the groundwork for us to experiment and test the behavior of microcode operations.

Custom Processing Unit:

<https://github.com/pietroborrello/CustomProcessingUnit> Custom Processing Unit is the first dynamic analysis framework able to hook, patch and trace microcode from a UEFI application

Title: Badge Cloning With Doppelgänger

When: Friday, Aug 11, 16:00 - 16:20 PDT

Where: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

SpeakerBio: Travis Weathers

Travis Weathers is a Practice Director on Optiv's Attack & Penetration team based out of Tampa, FL. Since stepping out of the military, Travis has worked within the offensive security space performing advanced adversarial emulation assessments and leading offensive security practitioners.

Description:

The Doppelgänger project stemmed from the Raspberry Pi chip shortage, which drove up the cost of RPi Nano W boards, making the cost to repair my team's long-range cloners not feasible. In addition, there were some limitations with existing tooling that I aimed to mitigate.

This project intended to accomplish the following:

1. Use modern/actively supported and hot-swappable CoTS equipment that can easily be replaced.
2. The operator can't enter a comms blackhole while connected to the device.
3. Egress method for notifications, reducing the need to check for card reads while in the middle of an operation.
4. Simplified WebGUI that only displays Bit Length, Facility Code, and Card Number. Option to download the complete data set (e.g., BL, FC, CC, HEX, BIN).
5. Error handling, so the device doesn't log bad reads, EMI, etc.
6. Easy configuration and reset functionality for team use.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Badge of Shame: Breaking into Secure Facilities with OSDP

When: Saturday, Aug 12, 09:30 - 10:15 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

Speakers: Dan "AltF4" Petro, David Vargas

SpeakerBio: Dan "AltF4" Petro , Senior Security Engineer at Bishop Fox

Dan "AltF4" Petro is a Senior Security Engineer at Bishop Fox. Dan is widely known for the tools he creates: Eyeballer (a convolutional neural network pentest tool), the Rickmote Controller (a Chromecast-hacking device), Untwister (pseudorandom number generator cracker), and SmashBot (a merciless Smash Bros noob-pwning machine).

SpeakerBio: David Vargas , Senior Security Consultant at Bishop Fox

David "Shad0" Vargas is a senior red teamer at Bishop Fox. He enjoys breaking into secure facilities by exploiting physical, social and network security controls. In a past life, David designed a power system for a cube satellite to be launched into space.

Description:

Breaking into secure facilities used to be possible by inserting a listening device (such as an ESPKey) behind an RFID card reader and sniffing the unencrypted Wiegand badge numbers over the wire as they go to the backend controller. The physical security industry has taken notice and there's a new sheriff in town: The encrypted protocol OSDP which is starting to be rolled into production. Surely encryption will solve our problems and prevent MitM attacks right? ... right?

In this presentation, we'll demonstrate over a dozen vulnerabilities, concerning problems, and general "WTF"s in the OSDP protocol that let it be subverted, coerced, and totally bypassed. This ranges from deeply in-the-weeds clever cryptographic attacks, to boneheaded mistakes that undermine the whole thing. We will also demonstrate a practical pentesting tool that can be inserted behind an RFID badge reader to exploit these vulnerabilities.

Get your orange vest and carry a ladder, because we're going onsite!

REFERENCES

* ESPKey <https://github.com/octosavi/ESPKey> * OSDP v2.2 Spec <https://www.securityindustry.org/2020/12/15/security-industry-association-releases-version-2-2-of-sia-osdp-standard/> <https://libosdp.gotomain.io/protocol/introduction.html> * RS485 <https://en.wikipedia.org/wiki/RS-485>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Bare Metal Firmware Development and Reverse Engineering

When: Sunday, Aug 13, 13:20 - 13:59 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

Speakers: Caleb Davis, Nathan Smith

SpeakerBio: Caleb Davis , Protiviti

Caleb Davis leads Protiviti's IoT/Embedded security team. Caleb operates out of the Dallas/Fort Worth area and has a degree in Electrical Engineering from the University of Texas at Tyler. He is an inventor/patent holder and has a background in embedded hardware/software development. He leads a team of experts that regularly perform penetration testing across a wide variety of products including medical devices, ATMs, chemical control systems, security solutions, and other commercial products. Additionally, Caleb has a passion for integrating security into the product development life cycle and has helped several organizations in their approach to shifting left.

SpeakerBio: Nathan Smith , Protiviti

Nathan Smith is a Manager focused on IoT device security at the Dallas Protiviti office. Before coming to Protiviti, Nathan accumulated 8 years of industry experience developing and testing embedded controls and software, leading software development teams, and managing digital products. He received a B.S. in Electrical Engineering from the University of Texas at Tyler. He has performed device penetration testing, firmware reviews, and mobile application security assessments on industry devices.

Description:

Developing firmware is an essential skill that cyber security professionals should be familiar with to gain a deeper understanding of the foundation of most systems that are being relied on. Additionally, a fundamental understanding of firmware development is a valuable asset in the realm of firmware reverse engineering. This hands-on workshop aims to tackle both directions of firmware (development/reversing) to give the audience a better understanding of the intricacies with each process. The firmware development portion of the workshop will walk the audience through a guided activity that performs the basic steps to deploy a firmware application on an embedded microcontroller (STM32). The application will be developed in such a way that it is intended to be reversed. The second half of the workshop deals with the firmware binary and the steps necessary to fully recover the firmware as much as possible. An important note is that these tools and firmware will be open-source and therefore the audience can attempt this work on their own. Takeaways from this talk include an understanding of bare metal development environments, embedded C code, memory mapping and peripherals, as well as an intermediate understanding of Ghidra.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Battle of The Bots

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Battle of The Bots presents a new twist on traditional “King-of-The-Hill” style Capture the Flag events by incorporating exploit development, vulnerability analysis, reverse engineering and software development in the form of developing computer worms aka “bots”. BOTBs requires competitors to develop proof-of-concept exploits against varying misconfigured or vulnerable network services. To maximize points scored, the competitor’s bot must automatically scan and compromise network services in the competition environment autonomously. Services that are harder to exploit (ex: requiring memory corruption exploits opposed to misconfigured databases) will result in a higher point score for the competitor.

The vulnerable network services will include real world vulnerable services where a competitor can adopt off the shelf proof-of-concepts vulnerabilities from an offensive security resource (ex: Metasploit Framework, exploit-db, packetstorm, etc...) into their bot to achieve access to said vulnerable services. Additionally, custom built vulnerable services informed by OWASP Top 10 security bugs as well as CVEs will influence challenge development resulting in a competitor to have the experience of reverse engineering new applications to identify vulnerabilities based on historically significant pain points in Software Engineering as well as infamous historical CVEs. Battle of The Bots will give competitors of all skill levels an opportunity to develop proof-of-concept exploits. Network services will be developed in a variety of compiled and interpreted languages with varying associated vulnerabilities and points. The variety of languages will provide opportunities for those less experienced with reverse engineering to analyze vulnerable Python code to find hidden API endpoints that lead to shell execution for example, rather than reverse engineer compiled binaries.

Finally, the BOTBs team will be capturing network traffic from the competition environment to later be shared with the wider community. The BOTBs team believes that this unique dataset of network service attacks can act as a unique resource for academic researchers, SOC analysts assessing their defenses and training events where having attack data for SIEM analysis. The data will be released under the Apache 2.0 License and hosted publicly on a yet to be determined platform.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Battle of The Bots

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Battle of The Bots presents a new twist on traditional “King-of-The-Hill” style Capture the Flag events by incorporating exploit development, vulnerability analysis, reverse engineering and software development in the form of developing computer worms aka “bots”. BOTBs requires competitors to develop proof-of-concept exploits against varying misconfigured or vulnerable network services. To maximize points scored, the competitor’s bot must automatically scan and compromise network services in the competition environment autonomously. Services that are harder to exploit (ex: requiring memory corruption exploits opposed to misconfigured databases) will result in a higher point score for the competitor.

The vulnerable network services will include real world vulnerable services where a competitor can adopt off the shelf proof-of-concepts vulnerabilities from an offensive security resource (ex: Metasploit Framework, exploit-db, packetstorm, etc...) into their bot to achieve access to said vulnerable services. Additionally, custom built vulnerable services informed by OWASP Top 10 security bugs as well as CVEs will influence challenge development resulting in a competitor to have the experience of reverse engineering new applications to identify vulnerabilities based on historically significant pain points in Software Engineering as well as infamous historical CVEs. Battle of The Bots will give competitors of all skill levels an opportunity to develop proof-of-concept exploits. Network services will be developed in a variety of compiled and interpreted languages with varying associated vulnerabilities and points. The variety of languages will provide opportunities for those less experienced with reverse engineering to analyze vulnerable Python code to find hidden API endpoints that lead to shell execution for example, rather than reverse engineer compiled binaries.

Finally, the BOTBs team will be capturing network traffic from the competition environment to later be shared with the wider community. The BOTBs team believes that this unique dataset of network service attacks can act as a unique resource for academic researchers, SOC analysts assessing their defenses and training events where having attack data for SIEM analysis. The data will be released under the Apache 2.0 License and hosted publicly on a yet to be determined platform.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Battle of The Bots

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Battle of The Bots presents a new twist on traditional “King-of-The-Hill” style Capture the Flag events by incorporating exploit development, vulnerability analysis, reverse engineering and software development in the form of developing computer worms aka “bots”. BOTBs requires competitors to develop proof-of-concept exploits against varying misconfigured or vulnerable network services. To maximize points scored, the competitor’s bot must automatically scan and compromise network services in the competition environment autonomously. Services that are harder to exploit (ex: requiring memory corruption exploits opposed to misconfigured databases) will result in a higher point score for the competitor.

The vulnerable network services will include real world vulnerable services where a competitor can adopt off the shelf proof-of-concepts vulnerabilities from an offensive security resource (ex: Metasploit Framework, exploit-db, packetstorm, etc...) into their bot to achieve access to said vulnerable services. Additionally, custom built vulnerable services informed by OWASP Top 10 security bugs as well as CVEs will influence challenge development resulting in a competitor to have the experience of reverse engineering new applications to identify vulnerabilities based on historically significant pain points in Software Engineering as well as infamous historical CVEs. Battle of The Bots will give competitors of all skill levels an opportunity to develop proof-of-concept exploits. Network services will be developed in a variety of compiled and interpreted languages with varying associated vulnerabilities and points. The variety of languages will provide opportunities for those less experienced with reverse engineering to analyze vulnerable Python code to find hidden API endpoints that lead to shell execution for example, rather than reverse engineer compiled binaries.

Finally, the BOTBs team will be capturing network traffic from the competition environment to later be shared with the wider community. The BOTBs team believes that this unique dataset of network service attacks can act as a unique resource for academic researchers, SOC analysts assessing their defenses and training events where having attack data for SIEM analysis. The data will be released under the Apache 2.0 License and hosted publicly on a yet to be determined platform.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: BBOT (Bighuge BLS OSINT Tool)

When: Saturday, Aug 12, 12:00 - 13:55 PDT

Where: Caesars Forum - Accord Boardroom - Demo Labs - [Map](#)

Speakers: Joel "TheTechromancer" Moore, Paul Mueller

SpeakerBio: Joel "TheTechromancer" Moore

TheTechromancer is a hacker at Black Lantern Security (BLS). He loves coding in Python, and is the creator of several security tools including ManSpider, TrevorSpray, and BBOT (Bighuge BLS OSINT Tool). He has also made contributions to other open-source projects such as Spiderfoot.

SpeakerBio: Paul Mueller

Paul Mueller is a Principal Operator at Black Lantern Security (BLS). He specializes in web application testing and application security. He loves finding complex hard-to-find web bugs, especially when they involve cryptography. He is also one of the developers for the BLS tools Writehat and BBOT (Bighuge BLS OSINT Tool). Prior to working with BLS, he spent over a decade as a DoD contractor providing both penetration testing and security analysis/incident handling. He got his start in the field as a systems administrator and later as a Signals Intelligence Analyst with the US Marine Corps.

Description:

BBOT (Bighuge BLS OSINT Tool) is a new recursive OSINT scanner inspired by Spiderfoot, but designed and optimized for bigger targets and faster scan times. BBOT is open-source and written in Python. Its 80+ modules range in function from subdomain enumeration to cryptographic exploitation. BBOT can map the attack surface of an organization (and sometimes get you RCE) in a single command.

Features include:

- multiple targets
- automatic dependencies w/ ansible
- python API
- subdomain enumeration
- email enumeration
- cloud bucket enumeration
- port scanning
- web service enumeration
- web screenshots
- web spidering
- vulnerability scanning (with nuclei and more)

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Be a Nerd that Talks Good: Up-leveling how we talk about misinformation, to build community trust and awareness

When: Friday, Aug 11, 14:30 - 15:30 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Joel Benge , MessageSpec Consulting

Joel Benge is the principal at MessageSpec Consulting. He supports founders and product teams at startups and scale-ups in creating technically-accurate and textually-beautiful stories and messages. He works closely with clients to connect their business objectives to the human emotions and motivations of their target audiences — creating content that gets attention, gets remembered, and gets results. With over 25 years in IT, cybersecurity, and marketing, Joel has worked for companies from NASA to Nickelodeon, along with several other organizations that start with different letters than N. He is a proponent of the series comma and (poorly) plays the didgeridoo.

Description:

Sure, you've got skills to "build the stuff and do the thing." But how good are you at talking to non-techs, execs, and the general public about why what you're doing is important? If you can't get people's attention, get them to remember the important things, and motivate them to act (or not act, in the case of misinformation), you can't be as effective.

This workshop explores a framework for a better understanding of how we as technologists can develop messages that get attention, get noticed, and get results without "dumbing down" or sacrificing technical acuity. Basically, being the Nerds that Talk Good.

The solution to misinformation, especially machine-generated misinformation, is not solely a bot vs. bot problem. Understanding why messages take hold in the first place and leveraging our human heart, mind, and gut-level responses to stories can make us better communicators as technologists—which can help authentic and trustworthy content rise above the machines.

Leveraging the MessageDeck—a novel, nontechnical, hands-on card-based approach—, participants will be coached to discover the higher-order motivations and objectives necessary for their communications and content to be trusted and believed. The model also serves as a framework to develop an informed, skeptical awareness when receiving information.

The model was developed after 25 years in arts and entertainment, hardcore IT and cybersecurity, and government communications and is being presented with none of that boring nonsense. We'll get together, play some cards, spark some conversations, and out of it will come a messaging platform that will recapture the public sphere for good.

Participants will also have an opportunity to contribute to a Misinformation Village Messaging Platform—a set of hallmark messages that can be adopted by the broader community. By discovering these authentic messages, we build cohesion and consistency across the misinformation awareness movement.

Samples of the MessageDeck will be available as supplies last to any who want them, but the strength of the approach lies in its flexibility to be used explicitly or to inform other facilitated conversations. So we will also have an opportunity to explore other ways to apply it to the work of others.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Between a Log and a Hard Place: (mis)Adventures in Azure Logs

When: Saturday, Aug 12, 10:30 - 11:10 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Dmitriy Beryoza

Dmitriy Beryoza is a Senior Security Researcher with Vectra AI, working on threat detection in the cloud and on-prem networks. Before that, he was a penetration tester and secure software development advocate at IBM. Before switching to security full-time, Dmitriy has been a software developer for many years. He presented talks at BSides Las Vegas, BSides SF, HackFest, and others. Dmitriy holds a Ph.D. in Computer Science and OSCP, CISSP, CCSP and CEH certifications. His interests include reverse engineering, secure software development, and CTF competitions.

Twitter: [@0xd13a](#)

Description:

Security monitoring in any environment is made or broken by the signal quality in the event logs. Cloud-based solutions have transformed the computing landscape with advantages like on-demand resource availability, scalability, cost-effectiveness, and enhanced collaboration capabilities. For defenders, this new world offered many benefits: robust identity management, patching at scale, improved incident detection and response, and more.

Cloud providers expose detailed logs that are consumed by security monitoring tools and SOC analysts. One would expect a common, streamlined logging solution to be a clear win in attack detection functionality, but the reality is more complicated.

We have spent the last three years studying and monitoring Azure logs and have seen many problems that can complicate incident detection and response. With no alternatives to the provider's logging solution and slow problem mitigation speed, these issues go beyond mere annoyances and can help attackers avoid detection.

In this talk, we will examine logging facilities in Azure, concentrating on events generated by Azure AD and Microsoft 365, and discuss multiple problems that we have observed in monitoring them.


These include:

- Blind spots hiding critical security events
- Poorly documented events, attributes and magic values
- Missing important information about user actions
- Bugs in log records
- Unannounced changes that break detection queries
- Log pollution opportunities, potentially leading to RCE

and more

For all these issues, we will:

- examine their impact on defense and monitoring
- discuss how attackers (and red teamers) may take advantage of them
- suggest how defenders can mitigate the negative impact, where possible
- and propose ways the cloud provider can address the problems going forward

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Beyond Ransomware: Protecting Lives and Data from Modern Threat Actors

When: Saturday, Aug 12, 00:00 - 00:59 PDT

Where: Virtual

SpeakerBio: Ohad Zaidenberg

No BIO available

Description:

This talk is being pre-recorded and will be released on YouTube. Once it is available, a link to it will appear here.

Update 2023-08-11 06:30: Biohacking Village indicates that the pre-recorded talks have not yet been received. Once received, these talks will be posted to the [Biohacking Village YouTube Channel](<https://www.youtube.com/@BiohackingVillage/about>). Please note that this may be as late as a week or two after DC31.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Beyond the Breach: Exploring Cybersecurity Policies with Hacker Perspectives

When: Saturday, Aug 12, 13:00 - 13:50 PDT

Where: Caesars Forum - Summit - 221-222 - Policy Atrium - [Map](#)

Speakers: Andrés Velázquez, Isabella Rolz, Mauro Vignati, Orlando Garces

SpeakerBio: Andrés Velázquez , Founder and President at MaTTica

Andrés Velázquez is a cybersecurity expert and the Founder and President of MaTTica, a leading strategic cybersecurity company in Latin America. With specialized knowledge in cybersecurity, incident response, and computer forensics, Andrés possesses a deep understanding of the ever-evolving landscape of digital investigations and the associated challenges. He is particularly focused on providing expert guidance to Computer Security Incident Response Teams (CSIRTs), playing a pivotal role in incident response and policy development for these teams in Latin America. With a notable career in the industry, Andrés has trained over 1,500 law enforcement and intelligence officers, lawyers, and judges in the region on combating cybercrime. His expertise extends to the academic realm, where he serves as a cybersecurity professor at multiple prestigious universities.

SpeakerBio: Isabella Rolz , Communications Specialist at Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS)

Isabella Rolz is a communications specialist and journalist with over eight years of experience covering topics related to Latin America and the Caribbean. Her publications address issues such as ensuring security and transparency in LAC, poverty, and immigration, among other social problems. Isabella has worked at the Inter-American Development Bank, The World Bank, Pan-American Health Organization, and now the Organization of American States. Her work as a journalist has been published in the Washington Post, ABC News, the Daily Beast, Univision, and the New Humanitarian, among other media outlets. She graduated from Columbia University's Graduate School of Journalism with a scholarship from the Maria Moors Foundation and is a National Association of Hispanic Journalists member.

SpeakerBio: Mauro Vignati , ICRC

In 2003 Mauro started working at the first unit of the Swiss Federal Police fighting cybercrime. Later on, he collaborated to the establishment of MELANI, Switzerland's first centre for public-private partnership on cybersecurity for critical infrastructure. Back in 2013, he set up and led the Cyber Threat Intelligence Division within the Department of Defence in Bern. In 2021, he was tasked to create the Vulnerability Management unit within the National Cyber Security Centre NCSC.ch, leading several projects, among them the first bug bounty program of the Swiss government. He then joined the International Committee of the Red Cross ICRC one year later, as advisor on new digital technologies of warfare.


SpeakerBio: Orlando Garces , Cybersecurity Program Officer at Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS)

Orlando Garcés, Cybersecurity Program Officer of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS), focusing primarily on strategy and policy, governance issues, and gender mainstreaming in cybersecurity. He has strategically participated in the formulation and implementation of National Cybersecurity Strategies and Policies in several countries in the Latin American and Caribbean region, as well as in the development of reports and studies on the state of cybersecurity in strategic industries and sectors.

Description:

The field of cybersecurity policy is constantly evolving, and as such, the need to think innovatively and critically about policy solutions to address new and emerging threats. “Beyond the Breach: Exploring Cybersecurity Policies with Hacker Perspectives” is a panel that will bring together experts to explore the role of cybersecurity policy hackers in responding to cyber policy challenges that governments and organizations face in this rapidly evolving landscape. The discussion will delve into ongoing processes of elaborating global, regional, and local cyber policies that engage the hacker community. Globally, those discussed in the ICRC Delegation for Cyberspace; regionally, in OAS member states in the Americas; and locally, those in the public and private organizations, such as Computer Security Incident Response Teams (CSIRTs) in Latin America. Additionally, it will explore initiatives to create platforms for hackers’ participation and encourage innovation in cybersecurity

policymaking. Furthermore, the panel will also discuss the role of cybersecurity policy hackers in the ongoing evolving landscape of digital investigations and the associated challenges across different regions.

[Return to Index](#) - Add to  - ics [Calendar](#) file

BICV - Saturday - 16:00-16:50 PDT

Title: BIC Village Closing Keynote

When: Saturday, Aug 12, 16:00 - 16:50 PDT

Where: Caesars Forum - Alliance - 301-304 - Blacks in Cyber Village - [Map](#)

SpeakerBio:Kevin Roberts

Kevin is a Social Media Personality who is dedicated to Technology Tips, Tricks, and Information Security Awareness!

He has a focus on making content that caters to both the tech-savvy and those just starting their journey into tech. Topics he goes over include: Internet Safety, Privacy, and Educational Cybersecurity content.

He has a growing community in Discord, called OWLsec. Currently they have over 17,000 members with a diversity of backgrounds. He boasts an inclusive community where "leaving egos at the door" and "understanding we all started somewhere" are the main focal points of their community growth.

Description:

Join me as I share my tech journey!

I will share a brief insight of my origin, what sparked my interest in technology and the path that led me to where I am today! I'll reveal some of the exciting hacks and experiences I've had with friends along the way. I'll take you behind the scenes, sharing where and how I spend countless hours connecting and learning about Cybersecurity.

I will also share my exciting growing community "OWLsec", which came to life with the help of amazing individuals!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: BIC Village Opening Keynote

When: Friday, Aug 11, 10:00 - 10:50 PDT

Where: Caesars Forum - Alliance - 301-304 - Blacks in Cyber Village - [Map](#)

SpeakerBio:John Threat

John Lee is a world renowned computer hacker , a writer/director, and a radical creative futurist. He's been on the cover for Wired magazine and 60 Minutes.

He consults with several institutions and think tanks as a futurist, developing reasonable calculations of future events to both inspire creative endeavors for humanity and avoid or mitigate calamity.

John consults with a select group of entities about computer security and has appeared on the cover of magazines like Wired and on news programs like 60 minutes for his exploits and expert commentary on the hacker world.

John also develops narrative film and documentary projects about sci-fi and technology exploring the thematics of freedom and revolution. He also works on developing technologies to help in spreading and maintaining free speech and democracy for humans world wide.

John currently is consulting for entities like MoMa , Vision 2030 Futurist Collective, and [redacted] on security futures while developing a new film project for 2023 (Don't Talk To Trees).

Description:

He will be speaking about history in hacking & security from a general perspective and specifically from a Black perspective.

He will be talking about great hacks from history including his own! He will talk about his journey in security and how security has evolved over the years, his theories on security going into the future and how to stay flexible in reference to new platforms and attack vectors. He will discuss all the avenues security can bring an up and coming Hacker career wise as well!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Blacks in Cyber Lituation Party

When: Friday, Aug 11, 18:00 - 01:59 PDT

Where: Caesars Forum - Alliance - 301-304 - Blacks in Cyber Village - [Map](#)

Description:

The BIC Lituation Party is designed to have a night's worth of different activities that DEF CON attendees are able to browse and fit into their DEF CON schedule for networking, knowledge sharing and fun!

The event will break into three sections throughout the night:

“Mild”

6:00 pm - 8:00pm

Networking - Light music, Food and Drinks

“Medium”

8:00pm - 10:00pm

Nerdcare HipHop Showcase

“Hot”

10:00pm - Until (2:00 am)

DJ Stage Set by DJ Roma of the DC Metro Area.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 12:00-16:59 PDT

Title: Blacks in Cyber Village CTF

When: Friday, Aug 11, 12:00 - 16:59 PDT

Where: Caesars Forum - Alliance - 301-304 - Blacks in Cyber Village - [Map](#)

Description:

The year is 2323. You find yourself in an abandoned city in the future that is home to a variety of advanced technology and systems. You will need to use your skills to solve challenges and discover information to use to uncover your flags. Along the way, you will learn about social justice, privacy, civil rights and surveillance and how these can relate to communities and individuals as our world explores emerging technologies. This is a jeopardy style game with multiple categories in Cryptography, Steganography, Exploitation, Forensics, Reverse Engineering and more!

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 19:00-00:59 PDT


Title: BlanketFort Con

When: Saturday, Aug 12, 19:00 - 00:59 PDT

Where: Caesars Forum - Forum - 130 - [Map](#)

Description:

BlanketFort Con: Come for the chill vibes and diversity, stay for the Blanket Fort Building, Cool Lights, Music, and Kid Friendly\Safe environment. Now with less Gluten and more animal onesies!

[Return to Index](#) - Add to  - ics [Calendar](#) file

DL - Saturday - 14:00-15:55 PDT

Title: BLE CTF

When: Saturday, Aug 12, 14:00 - 15:55 PDT

Where: Caesars Forum - Unity Boardroom - Demo Labs - [Map](#)

Speakers: Alek Amrani, Ryan Holeman

SpeakerBio: Alek Amrani

Alek Amrani - bad at expense reports

SpeakerBio: Ryan Holeman , CISO at Strike

Ryan Holeman resides in Austin, Texas, where he works as the CISO for the peer-to-peer payment platform Strike. He is currently pursuing a Ph.D. in cyber defense from Dakota State University. He has spoken at respected venues such as Black Hat, DEF CON, Lockdown, BSides, Ruxcon, Notacon, and Shmoocon. You can keep up with his current activity, open source contributions, and general news on his blog. His spare time is mostly spent digging into various network protocols, random hacking, creating art, and shredding local skateparks.

Description:

BLE CTF is a series of Bluetooth Low Energy challenges in a capture the flag format. It was created to teach the fundamentals of interacting with and hacking Bluetooth Low Energy services. Each exercise, or flag, aims to interactively introduce a new concept to the user. Over the past few years, BLE CTF has expanded to support multiple platforms and skill levels. Various books, workshops, trainings, and conferences have utilized it as an educational platform and CTF. As an open source, low cost of entry, and expandable education solution, BLE CTF has helped progress Bluetooth security research.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: BLE Security 201 (Pre-Registration Required)

When: Saturday, Aug 12, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers:Maxine "Freqy" Filcher,Zach "justadequate" Reavis

SpeakerBio:Maxine "Freqy" Filcher

Maxine, or Freqy, is a US Army Veteran, possessing a master's degree in Cybersecurity and is widely recognized for her expertise in wireless security. In sharing her knowledge, she has delivered many presentations over the last five years, exploring various facets of wireless security. Maxine's grasp of BLE security has helped her play pivotal roles in assisting numerous large-scale corporations in fortifying the security of consumer devices that are ubiquitous to millions of households worldwide

SpeakerBio:Zach "justadequate" Reavis

Zach, also known as justadequate, is an OSCP-certified wireless security expert specializing in waveform reverse engineering, exploit development, and embedded systems penetration testing. Demonstrating in-depth knowledge and experience in these areas, he has worked in both consulting and formal security test and engineering roles to develop, assess, and secure systems ranging from aircraft to SCADA/ICS to IoT/home-use devices deployed around the world.

Description:

There have been plenty of talks on intro BLE security topics, it's time for us to put it to use. This workshop will serve as a refresher for the BLE skills gained in previous talks, while walking students to the next level through utilizing BLE as an initial ingress vector to compromise a simulated corporate network. Come join us while we demonstrate the importance of investigating all wireless protocols in your corporate environment.

Skill Level: Intermediate

Prerequisites for students:

- None

Materials or Equipment students will need to bring to participate: - Laptop

- Android Phone

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Saturday - 10:30-10:59 PDT

Title: Blindly hunting for Mercenaries

When: Saturday, Aug 12, 10:30 - 10:59 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

Speakers:Asheer Malhotra,Vitor Ventura

SpeakerBio:Asheer Malhotra

No BIO available

SpeakerBio:Vitor Ventura

No BIO available

Twitter: [@_vventura](#)

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Blocking Pathways into Cybercrime: Current Efforts and Future Opportunities

When: Friday, Aug 11, 15:00 - 15:50 PDT

Where: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

Speakers:Greg Francis,Jonathan Lusthaus,Marcia Hofmann,Marcus Hutchins,Will McKeen

SpeakerBio:Greg Francis , Cybercrime Prevention Consultant at MD 4D Cyber Security

Greg Francis leads MD 4D Cyber Security and is a Consultant to Dutch National Police. He is a cybercrime prevention specialist with over 20 years of experience gleaned from work as a Specialist Investigator (Serious Organised Crime) and as a Lay Magistrate. For almost seven years, Greg was a Senior Officer in the UK's National Cyber Crime Unit Prevent Team, serving as Acting Manager for two of these years. He is one of the global pioneers of cybercrime prevention. His specialisms include deterring people from online criminal activity and diverting them into a legitimate path based on their digital interests.

SpeakerBio:Jonathan Lusthaus , Senior Research Fellow and Director of the Human Cybercriminal Project at Department of Sociology, University of Oxford

Dr. Jonathan Lusthaus is Director of The Human Cybercriminal Project and a Senior Research Fellow in the Department of Sociology, University of Oxford. He is also a Research Fellow at Nuffield College. Jonathan's research focuses on the "human" side of profit-driven cybercrime: who cybercriminals are and how they are organised. He is a regular speaker at major conferences, such as Black Hat, Enigma and the International Conference on Cyber Security. Jonathan has also written widely across academic, policy and media publications, including for the European Journal of Sociology, the Council on Foreign Relations and The New York Times. He is the author of Industry of Anonymity: Inside the Business of Cybercrime published by Harvard University Press. Fieldwork for this study took place over a 7-year period, involved travel to cybercrime hotspots around the globe, and included almost 250 interviews with law enforcement, the private sector, and former cybercriminals. Jonathan holds a doctorate in sociology from the University of Oxford, where he was a Clarendon Scholar.

SpeakerBio:Marcia Hofmann , Founder at Zeitgeist Law

Marcia Hofmann is the founder and principal of Zeitgeist Law, a boutique law practice that specializes in information security, free expression, consumer protection, intellectual property, privacy, and data protection. She helps security researchers navigate the murky laws around access to computers and data. She has also defended a number of people accused of violating computer crime laws, including malware researcher Marcus Hutchins and three MIT students who were sued over their presentation at DEF CON 16. She studied law enforcement engagement with young computer crime offenders as a US-UK Fulbright scholar. She has also taught computer crime law as an adjunct professor at the University of Colorado Law School.

SpeakerBio:Marcus Hutchins

Marcus Hutchins is cybersecurity specialist, speaker, and ex-hacker. He is best known for stopping one of the largest cyberattacks in history, the 2017 WannaCry ransomware attack. Marcus and his story were featured on the cover of Wired Magazine's June 2020 issue, titled "The Confessions of Marcus Hutchins, the Hacker Who Saved the Internet." He is based in Los Angeles, where he works for a cybersecurity company.

SpeakerBio:Will McKeen , Special Agent at FBI

Will McKeen is a Special Agent on the FBI's Cyber Crimes Task Force in New York. Will specializes in Business Email Compromise, criminal computer intrusion investigations, and Insider Threat cases. Through this work, Will has seen the impact of cyber criminal networks, both on victims and young actors in this space. Will's background working with victims of crimes, and those behind the keyboard sparked a keen interest in developing new solutions to youth in cyber. Will is also a Cyber Instructor for the FBI and a member of the FBI New York Office's Crisis Negotiation Team.

Description:

A movement is building among law enforcement around the world to connect with young people who are on the path to cybercrime and help them redirect their skills to more constructive, lawful ends. While conventional law enforcement is concerned with prosecutions, prevention strategies seek to engage with (future) offenders and divert them away from committing cybercrime in the first place (or to desist from doing so once they have started). A number of tactics have been

explored for blocking pathways into cybercrime. These include TV advertisements to encourage parents to take note of what their children might be doing online, warnings when youths are crossing into cybercriminal activities, workshops with mentor figures who can demonstrate more productive (and legal) uses of hacking skills, and connections to employers who can potentially offer pathways towards legitimate employment in cybersecurity or the technology sector more broadly. This panel offers a diverse range of perspectives on cybercrime prevention: a pioneer of prevention efforts in the United Kingdom and the Netherlands; an American attorney involved in high profile computer crime defense cases; a US law enforcement agent; and a well-known former hacker. The panel is moderated by an academic expert on cybercrime. Come learn about ongoing prevention efforts and how you might be able to help as a policymaker, potential mentor, or general supporter.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 20:30-22:59 PDT

Title: Blue Team Village (BTV) Pool Party

When: Friday, Aug 11, 20:30 - 22:59 PDT

Where: Flamingo - Pool - [Map](#)

Description:

Join the AI Village and Blue Team Village for the DEF CON "Community Experience Pool Party" at the Flamingo "Go Pool" Friday, August 11, from 20:30 to 23:00 featuring a performance by the one and only Dual Core at 21:00. Free Tacos, cash bar.

DEF CON badge required for entry.

In event of rain/weather cancellation, the backup location for this party is "Flamingo - Upstairs - Eldorado Ballroom".

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTV - Sunday - 12:45-13:45 PDT

Title: Blue Team Village Closing Ceremony

When: Sunday, Aug 13, 12:45 - 13:45 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Main Stage - [Map](#)

Description:

Blue Team Village Closing Ceremony

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Blue Team Village CTF

When: Friday, Aug 11, 10:30 - 17:59 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - [Map](#)

Description:

The Blue Team Village CTF is a cyber defense CTF inspired by a mix of trending nation-state actor kill chains and at least one custom insider threat story. You are an incident responder tasked to investigate the recent attacks against our fictitious company: Magnus Tempus Financial. Since Magnus Tempus Financial made a vital acquisition expanding its precious metals portfolio to oil and gas operational technology (OT), you will also investigate their OT environment.

The CTF challenges contestants to leverage diverse cyber defense skills, including Incident Response, Forensics, Malware Analysis, Threat Intelligence, and Threat Hunting, to be the first team or individual to answer or solve the challenges presented.

The BTV crew developed the CTF to allow anyone, regardless of skill or knowledge, to participate, aiming to sharpen their cyber defense skills. We believe in the idea of choosing your adventure. As a result, participants can download a copy of the required evidence (logs, packets, etc.) or log into any of the 3 SIEMs we provide to hunt on.

If you are new to cyber defense, we highly recommend participating in the Blue Team Village Obsidian stations. They will cover many of the topics on the CTF and will help you along the way!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Blue Team Village CTF

When: Saturday, Aug 12, 10:30 - 17:59 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - [Map](#)

Description:

The Blue Team Village CTF is a cyber defense CTF inspired by a mix of trending nation-state actor kill chains and at least one custom insider threat story. You are an incident responder tasked to investigate the recent attacks against our fictitious company: Magnus Tempus Financial. Since Magnus Tempus Financial made a vital acquisition expanding its precious metals portfolio to oil and gas operational technology (OT), you will also investigate their OT environment.

The CTF challenges contestants to leverage diverse cyber defense skills, including Incident Response, Forensics, Malware Analysis, Threat Intelligence, and Threat Hunting, to be the first team or individual to answer or solve the challenges presented.

The BTV crew developed the CTF to allow anyone, regardless of skill or knowledge, to participate, aiming to sharpen their cyber defense skills. We believe in the idea of choosing your adventure. As a result, participants can download a copy of the required evidence (logs, packets, etc.) or log into any of the 3 SIEMs we provide to hunt on.

If you are new to cyber defense, we highly recommend participating in the Blue Team Village Obsidian stations. They will cover many of the topics on the CTF and will help you along the way!

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTV - Sunday - 10:00-10:45 PDT

Title: Blue Team Village Game Session

When: Sunday, Aug 13, 10:00 - 10:45 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Main Stage - [Map](#)

SpeakerBio:aviditas

No BIO available

Description:

.

Game session

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTV - Friday - 10:00-10:30 PDT

Title: Blue Team Village Opening Ceremony

When: Friday, Aug 11, 10:00 - 10:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Main Stage - [Map](#)

Description:

Blue Team Village Opening Ceremony

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 14:00-15:59 PDT

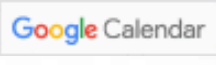
Title: Book Club Discussion and Exchange

When: Friday, Aug 11, 14:00 - 15:59 PDT

Where: Harrah's - Goldfield/Tonopah - Community Room - [Map](#)

Description:

Books bring us together, expand our ways of thinking, and allow for discourse. This DEF CON book exchange will be a quieter space for those who want to discuss what they are reading, recommend books, and trade books too. We might even have a SAO of a book - pending sponsorship.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Saturday - 10:00-15:59 PDT

Title: Book Exchange

When: Saturday, Aug 12, 10:00 - 15:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

What's it all about?

The Book Exchange at DEF CON, will allow for members of the community to drop off a used book that has been kindly read and may be enjoyable by someone else and in return they will be able to select a "new gently used" book from the exchange table.

Why?

Reading is fundamental. Many of us in the Defcon community have learned and been inspired by books and remain avid readers. The Defcon book exchange will allow community members to drop off a book that they found inspiring and is sitting on their shelf collecting dust and in return they will be able to get a new book which hopefully will continue to expand their knowledge over the next year. This effort will keep used books in circulation.

When and Where:

The exchange will be held from 10:00 to 16:00, Day(s) to be announced.

Left over books will be transported and donated to a used book store in Las Vegas, but the goal will be to have a zero net sum gain.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Bootsquad: Stomping out squatters

When: Saturday, Aug 12, 13:35 - 14:05 PDT

Where: Virtual

SpeakerBio: Joe Mast

Joe Mast is a Security Engineer, life long learner, and breaker of things. He has a passion for DNS and operational security. His background consists of helping to secure global financial, retail, and security environments.

Description:

Have you ever attempted to register a domain for your trademark only to find it's already registered? Has a domain squatters attempted to extort you for relevant domains at exorbitant fees? Has a threat actor attempted to register look-alike domains and commence phishing attacks? This talks seeks to document a process for abusing URDP to obtain desirable domains when the opposition's operational security is lacking. Discussion will include covering URDP (Uniform Domain-Name Dispute-Resolution Policy) and the criteria required to initiate a domain successful takedown request. We will document in detail scenarios, which can be abused in order to produce evidence, which will lead to a successful domain takedown, regardless of the registering parties initiatives. Finally we will provide security guidance to threat actors, blue teamers and domain squatters to strengthen their portfolio and ensure URDP cannot be abused in this manner.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Boston Infinite Money Glitch: Hacking Transit Cards Without Ending Up In Handcuffs

When: Thursday, Aug 10, 10:00 - 10:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers: Matthew Harris, Noah Gibson, Scott Campbell, Zachary Bertocchi

SpeakerBio: Matthew Harris , Student at Medford Vocational Technical High School

A 17 year old and lead hackerman of the group. He likes breaking stuff and doesn't take kindly to being told what to do. He's a proud (and maybe annoying) neovim and Linux user, knows how to ride a bike (without training wheels), and is a very opinionated Rustacean despite barely knowing how to use the language.

SpeakerBio: Noah Gibson , Hacker

A soccer fan and web developer. In his free time he enjoys kicking a ball, drawing, and programming.

SpeakerBio: Scott Campbell , Hacker

A heathen who writes things in Bash, holder of a fishing license in the Commonwealth of Massachusetts, and the proud angler of several minnows. Refuses to learn Rust even though it is better than his silly little non memory safe languages in every way.

SpeakerBio: Zachary Bertocchi , Hacker

He holds a learners permit, is a seasoned fare machine maker, and even graduated 11th grade! He has successfully made it to the ripe old age of 17, and is an enthusiastic 3D modeler.

Description:

Who likes paying to ride the subway? Sure, you could hop the fare gates, but that can be athletically challenging and simply isn't cool enough for our tastes. What's a mischievous and miserly rider to do, then? Hack the fare system of course!

In this talk we'll walk you through how we, four high school students and cybersecurity noobs became the first to fully reverse engineer Boston's CharlieCard fare system and earn ourselves free rides for life... or at least until the system gets fixed, whichever comes first.

We'll start by exploring the trials and tribulations of exploring the hardware behind the CharlieCards. Next, we'll dive into the emotional rollercoaster of reverse engineering the black box that is a transit card system older than us. We'll then explain the process of disclosing our findings to a government agency without having to hire a legal team. Finally, we'll show you a demo of some of the tools we made, including our own portable fare machine!

By the end of our talk, regardless of whether you're an avid RFID hackerman, or a complete noob, we'll leave you with useful reverse engineering strategies, tips for working with a government agency, and if nothing else, a fun story.

REFERENCES

Andersen, Zack. Anatomy of a Subway Hack. 10 August 2008, <https://file.wikileaks.org/file/anatomy-of-a-subway-hack.pdf>.

Bray, Hiawatha. "Your CharlieCard can be hacked by an Android phone, MBTA admits." The Boston Globe, 8 December 2022,

https://www.bostonglobe.com/2022/12/08/business/your-charliecard-can-be-hacked-by-an-android-phone-mbta-admits/?p1=HP_F
Accessed 18 April 2023.

"CharlieCard." Wikipedia, <https://en.wikipedia.org/wiki/CharlieCard>. Accessed 18 April 2023.

Courtois, Nicolas. "Hacking Mifare Classic Cards." Black Hat, 21 October 2014, <https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf>. Accessed 18 April 2023.

iceman001. "RfidResearchGroup/proxmark3: The Iceman fork of Proxmark3 / RFID / NFC reader, writer, sniffer and emulator." GitHub, <https://github.com/RfidResearchGroup/proxmark3>. Accessed 23 April 2023.

"nfc-tools/mfcuk: MiFare Classic Universal toolKit (MFCUK)." GitHub, <https://github.com/nfc-tools/mfcuk>. Accessed 23 April 2023.

"nfc-tools/mfoc: Mifare Classic Offline Cracker." GitHub, <https://github.com/nfc-tools/mfoc>. Accessed 23 April 2023.

Rauch, Bobby. "Operation Charlie: Hacking the MBTA CharlieCard from 2008 to Present." Medium, 8 December 2022, <https://medium.com/@bobbyrsec/operation-charlie-hacking-the-mbta-charliecard-from-2008-to-present-24ea9f0aaa38>. Accessed 18 April 2023.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Breaking Barriers: A Deep Dive into Bypassing Next-Gen 2FA and MFA Security Measures

When: Saturday, Aug 12, 16:30 - 17:15 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

Speaker Bio: Muhammad Shahmeer

Shahmeer Amir is the 3rd most accomplished bug hunter who has helped over 400 Fortune companies. He has founded multiple companies. He is a keynote speaker on Cyber Security, Blockchain at including Blackhat, GiSec, FIC, AEC Alberta, Hackfest
Twitter: [@Shahmeer_Amir](#)


Description:

As cyberattacks become more sophisticated, companies are increasingly relying on two-factor authentication (2FA) and multi-factor authentication (MFA) to protect their assets. However, these security measures are not foolproof and can be bypassed by determined attackers. In this presentation, we will take a deep dive into the techniques used by attackers to bypass next-generation 2FA and MFA security measures.

We will begin by discussing the limitations of 2FA and MFA and why they can be vulnerable to attacks. Then we will demonstrate a variety of attacks used by attackers to bypass these security measures, including phishing attacks, man-in-the-middle attacks, and SIM swapping attacks. We will also explore more advanced techniques such as exploiting vulnerabilities in authentication protocols and exploiting weaknesses in mobile authentication applications.

Throughout the presentation, we will provide real-world examples of successful attacks that have bypassed 2FA and MFA, highlighting the impact of such attacks on businesses and organizations. We will also discuss the latest trends and developments in 2FA and MFA security and the steps organizations can take to improve their security posture.

By the end of the presentation, attendees will have a better understanding of the vulnerabilities in 2FA and MFA security measures and how attackers can exploit them. They will also gain practical knowledge and tools to help them better protect their organizations against these types of attacks.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Breaking BMC: The Forgotten Key to the Kingdom

When: Saturday, Aug 12, 15:30 - 16:15 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

Speakers: Adam Zbrocki, Alex Tereshkin

SpeakerBio: Adam Zbrocki , Distinguished Engineer (Offensive Security) at NVIDIA

Adam 'pi3' Zbrocki is a computer security researcher, pentester and bughunter, currently working as a Distinguished Engineer (Offensive Security) at NVIDIA. He is a creator and developer of Linux Kernel Runtime Guard (LKRG) - his moonlight project defended by Openwall. Among others, he used to work in Microsoft, European Organization for Nuclear Research (CERN), HISPASEC Sistemas (known from the virustotal.com project), Wroclaw Center for Networking and Supercomputing, Cigital. The main area of his research is low-level security (CPU arch, uCode, FW, hypervisor, kernel, OS).

As a hobby, he was a developer in The ERESI Reverse Engineering Software Interface project, a bughunter (discovered vulnerabilities in Hyper-V, KVM, RISC-V ISA, Intel's Reference Code, Intel/NVIDIA vGPU, Linux kernel, FreeBSD, OpenSSH, gcc SSP/ProPolice, Apache, Adobe Acrobat Reader, Xpdf, Torque GRID server, and more) and studied exploitation and mitigation techniques, publishing results of his research in Phrack Magazine.

Adam is driving a Pointer Masking extension for RISC-V, he is involved in many RISC-V security related extensions (including CFI), he is a co-author of a subchapter to Windows Internals and was twice The Pwnie Awards nominee (2021 and 2022) for the most under-hyped research. He was a speaker at well-known security conferences including Blackhat, DEF CON, Security BSides, Open Source Tech conf and more.

Twitter: [@Adam_pi3](#)

SpeakerBio: Alex Tereshkin , Principal System Software Engineer (Offensive Security) at NVIDIA

Alex Tereshkin is an experienced reverse engineer and an expert in UEFI security, Windows kernel and hardware virtualization, specializing in rootkit technologies and kernel exploitation. He has been involved in the BIOS and SMM security research since 2008. He is currently working as a Principal Offensive Security Researcher at NVIDIA. He has done significant work in the field of virtualization-based malware and Windows kernel security. He is a co-author of a few courses taught at major security conferences and a co-author of the first UEFI BIOS and Intel ME exploits. In 2022 he was a Pwnie Awards nominee for the most under-hyped research.

Twitter: [@AlexTereshkin](#)

Description:

The Baseboard Management Controller (BMC) is a specialized microcontroller embedded on the motherboard, typically used in servers and other enterprise-level hardware. The security of the BMC is critical to the overall security of the system, as it provides a privileged level of access and control over the hardware components of the system, including the ability to perform firmware updates, and even power the system on and off remotely.

When the internal offensive security research team was analyzing one of the NVIDIA hardware, they detected several remotely exploitable bugs in AMI MegaRAC BMC. Moreover, various elevations of privileges and "change of scope" bugs have been identified, many of which may be chained together resulting in a highest severity security issue. During this talk we would like to take you on the journey of the whole attack sequence: from having zero knowledge about a remote AMI BMC with enabled IPMI (yeah, right) to flashing a persistent firmware implant to the server SPI flash. The chain will be about a dozen bugs long, so buckle up.

REFERENCES

- ◇ Dan Farmer "File under... et tu, ipmi 2.0 specification?" <http://fish2.com/ipmi/remote-pw-cracking.html>
- ◇ Waisman, Soler "The Unbearable Lightness of BMC" <https://i.blackhat.com/us-18/Wed-August-8/us-18-Waisman-Soler-The-Unbearable-Lightness-of-BMC.pdf>

◇ Eclypsiium, Inc. "Vulnerable firmware in the supply chain of enterprise servers"

<https://eclypsiium.com/wp-content/uploads/2019/07/Vulnerable-Firmware-in-the-Supply-Chain.pdf>

◇ Eclypsiium, Inc. "Quanta Servers (Still) Vulnerable to Pantsdown"

<https://eclypsiium.com/2022/05/26/quanta-servers-still-vulnerable-to-pantsdown/>



[Return to Index](#) - Add to - ics [Calendar](#) file

ASV - Sunday - 10:00-13:59 PDT

Title: Bricks in the Air

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

Bricks in the Air

Aerospace Village

Bricks in the Air is a hands-on demo to teach the basics of low level protocols seen in aviation. The demo uses the I2C protocol and does not reveal actual security vulnerabilities in avionics or other systems in aviation. The attendees are not required to have any prerequisite knowledge. No equipment is needed for attendees.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Bricks in the Air

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

Bricks in the Air

Aerospace Village

Bricks in the Air is a hands-on demo to teach the basics of low level protocols seen in aviation. The demo uses the I2C protocol and does not reveal actual security vulnerabilities in avionics or other systems in aviation. The attendees are not required to have any prerequisite knowledge. No equipment is needed for attendees.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Bricks in the Air

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

Bricks in the Air

Aerospace Village

Bricks in the Air is a hands-on demo to teach the basics of low level protocols seen in aviation. The demo uses the I2C protocol and does not reveal actual security vulnerabilities in avionics or other systems in aviation. The attendees are not required to have any prerequisite knowledge. No equipment is needed for attendees.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Bridging the Gap: Cloud Threat Intelligence for Detection and Offensive Security Practitioners

When: Saturday, Aug 12, 14:10 - 14:50 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Alex Delamotte

Alex's passion for cybersecurity is humbly rooted in the early aughts, when she declared a vendetta against a computer worm. Over the past decade, Alex has worked with blue, purple, and red teams serving companies in the technology, financial, pharmaceuticals, and telecom sectors and she has shared research with several ISACs. Alex enjoys researching the intersection of cybercrime and state-sponsored activity. She relentlessly questions why actors pivot to a new technique or attack surface. In her spare time, she can be found DJing or servicing her music arcade games.

Twitter: [@spiderspiders_](#)

Description:

During my transition from a conventional malware research position to a detection engineering role within a technology company, I encountered significant difficulties in acquiring actionable and timely intelligence regarding cloud-based threat actors. Subsequently, when I assumed a new position on an offensive security team, I faced similar challenges due to the scarcity of threat intelligence necessary for effective adversary emulation.

Recently, I had the opportunity to publish my research on [AlienFox](<https://www.sentinelone.com/labs/dissecting-alienfox-the-cloud-spammers-swiss-army-knife/>), a communally-developed cloud spamming toolset. As a curator of cloud intelligence, I am confronted with the arduous task of providing defenders with actionable threat intelligence in situations where the tools employed by attackers remain confined within their own systems. In targeted service environments, the utilization of payloads is considerably reduced, with the absence of prominent features such as Cobalt Strike beacons or Meterpreter. Additionally, the intricacies of DLL injection and registry modifications are rendered obsolete. Instead, cloud attackers harness robust and extensively documented APIs developed by the respective service providers, eliminating the need for complex shellcode encoders.

Given these limitations, how can defenders effectively operate? These attacks invariably leave behind artifacts in the form of configurations, such as the creation of new user profiles, which can be traced through API logs. Ultimately, if approached with an open mind and a willingness to adapt forensic methodologies, these techniques can be extrapolated from the realm of endpoint security. This talk will discuss how to approach detection of several familiar techniques--such as privilege escalation and persistence--ported to the cloud realm.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Build Inspector - A modern Javert on the trail of CI/CD Anomalies and Intruders

When: Friday, Aug 11, 12:00 - 13:55 PDT

Where: Caesars Forum - Caucus Boardroom - Demo Labs - [Map](#)

SpeakerBio:Jeremy Banker

A lifelong learner and broad technology enthusiast, Jeremy Banker holds a Masters degree in Information Security and is a founding member of the Security Product Engineering, Automation and Research (SPEAR) team at VMware. He has designed, built and implemented solutions to ensure that VMware's software supply chain remains secure. When not looking for new ways to keep software safe, he can usually be found tinkering with all manner of gadgets, working to bring amateur radio software into the modern era, or enjoying the peace of nature in his native Colorado.

Description:

In the ever evolving landscape of software development, maintaining the integrity and security of your build, test and deployment pipelines is paramount. Build Inspector is an always-watching guard dog, looking for information about the dependencies being consumed and produced, while also calling out instances of risky practices or potential signs of compromise during pipeline runs. Watch as the inspector turns piles of plaintext logs into structured data, perfect for automated analysis, correlation and alerting. With simple containerized deployment and self-documenting REST API, it has never been easier to ensure your build logs are always being watched.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Build Your Own Botnet

When: Sunday, Aug 13, 09:00 - 12:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

BYOB is intended to be a beginner friendly workshop dive into how botnets work. Attendees will use a web application to create a "dropper" file. (It is a tiny file whose only purposes is to fetch and execute the next stage of code). Then put the dropper file on another computer to obfuscate the command computer. The dropper is heavily obfuscated and compressed, and is a small python script. Attendees will learn how bot command and control works and cause several bots to probe a potential next target to gain access.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Build Your Own Botnet

When: Saturday, Aug 12, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

BYOB is intended to be a beginner friendly workshop dive into how botnets work. Attendees will use a web application to create a "dropper" file. (It is a tiny file whose only purposes is to fetch and execute the next stage of code). Then put the dropper file on another computer to obfuscate the command computer. The dropper is heavily obfuscated and compressed, and is a small python script. Attendees will learn how bot command and control works and cause several bots to probe a potential next target to gain access.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Build Your Own Botnet

When: Friday, Aug 11, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

BYOB is intended to be a beginner friendly workshop dive into how botnets work. Attendees will use a web application to create a "dropper" file. (It is a tiny file whose only purposes is to fetch and execute the next stage of code). Then put the dropper file on another computer to obfuscate the command computer. The dropper is heavily obfuscated and compressed, and is a small python script. Attendees will learn how bot command and control works and cause several bots to probe a potential next target to gain access.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Build Your Own Cat-Shaped USB Hacking Tool! (with the Nugget)

When: Saturday, Aug 12, 09:00 - 11:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 2 - [Map](#)

SpeakerBio: Alex Lynd

No BIO available

Twitter: [@alexlynd](#)

Description:

Want to learn how hackers compromise unlocked computers in seconds? Come build your own USB hacking tool in this beginner-friendly workshop, and learn to write prank payloads with your new cat-shaped hacking companion, the “USB Nugget”! You’ll learn the techniques & tools hackers use to deploy USB attacks, and compete for prizes in a mini hackathon to make the most destructive payload!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Build Your Own Cat-Shaped USB Hacking Tool! (with the Nugget)

When: Friday, Aug 11, 12:00 - 14:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 2 - [Map](#)


SpeakerBio: Alex Lynd

No BIO available

Twitter: [@alexlynd](#)

Description:

Want to learn how hackers compromise unlocked computers in seconds? Come build your own USB hacking tool in this beginner-friendly workshop, and learn to write prank payloads with your new cat-shaped hacking companion, the “USB Nugget”! You’ll learn the techniques & tools hackers use to deploy USB attacks, and compete for prizes in a mini hackathon to make the most destructive payload!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Building an Effective Security Culture Program

When: Saturday, Aug 12, 16:00 - 16:59 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Speakers: Jessica Barker, Maxie Reynolds, Rebecca Markwick, Sam Davison

SpeakerBio: Jessica Barker

Dr Jessica Barker MBE is an award-winning leader in the human side of cyber security and has delivered face-to-face awareness sessions to over 50,000 people. Jessica is the go-to expert for media such as BBC, Sky News and Wired and she has delivered over 80 keynotes including NATO, the World Government Summit and RSA. She serves on numerous boards, including the UK Government Cyber Security Advisory Board. She is the author of the best-selling book ‘Confident Cyber Security’ and in June 2023, Jessica was awarded an MBE for services to cyber security by King Charles in his first Birthday Honours.

Twitter: [@drjessicabarker](#)

SpeakerBio: Maxie Reynolds

Maxie Reynolds started her career in oil and gas as an underwater robotics pilot and subsea engineer working in Norway, Venezuela, Australia, Italy, Russia, Nigeria and the US. She then transitioned into cyber security at PwC in Australia, working in ethical hacking and social engineering. She also published a best selling book in 2021 titled ‘The Art of Attack: Attacker Mindset for Security Professionals.’ In late 2021, she moved back to the field of subsea engineering and created Subsea Cloud – a data center infrastructure company that places data centers underwater. Maxie was born in Scotland and is educated in Computer Science and Underwater Robotics. Currently, Maxie’s aim through her startup is to reduce latency, costs and CO2 emissions for hyper-scale spenders and small businesses alike whilst being the most agile infrastructure company around.

SpeakerBio: Rebecca Markwick , Enterprise Cyber Security Awareness and Culture Lead

Rebecca has spent over a decade designing and delivering training. Her experience in complex behavioural training allows for an innovative approach to designing security awareness programmes and accompanying metrics. One of her key areas of interest is the ethics of phishing and pen testing when considering effective training and culture and how best to protect the everyday user from attack. She is currently Enterprise Cyber Security Awareness and Culture Lead at a global BioTech company. Prior to this she was Security Culture Advocate at the UK’s Ministry of Justice.

Twitter: [@BexMarkwick](#)

SpeakerBio: Sam Davison , Head of Security and Privacy Engineering at Etsy

Sam Davison is a Security, Privacy, and Trust & Safety leader. She recently joined Etsy as the Head of Security and Privacy Engineering. Prior to her current role, Davison served as Director of Trust & Privacy Engineering at Robinhood, building and leading all consumer-facing security, privacy, and trust & safety engineering in addition to offensive security and intelligence functions. Davison has held leadership roles at the Krebs Stamos Group, Lyft, Snap Inc., and Uber where she led efforts with a particular emphasis on behavioral engineering, offensive security, and content moderation. Before working in Silicon Valley, she conducted extensive research on the efficacy of security engagement and co-led a consulting firm that built behavioral-based programs for 15+ Fortune 500 companies. Davison has volunteered throughout her career, lending her expertise to survivors of domestic abuse and election protection efforts.

Twitter: [@Sam_E_Davison](#)


Description:

With most cyber attacks and incidents involving social engineering, security culture is hugely influential in cyber security prevention and response. Your security culture is the foundation of your security posture, influencing whether people value cyber security, engage in awareness-raising training and report incidents and concerns. In this panel discussion, we will explore:

- What cyber security culture is
- How you can build an effective awareness-raising program

- Different ways to approach phishing simulations
- Practical steps to positively influence cyber security behaviors

Join us as we debate how to best protect the number one vector in cyber attacks: people.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Building Partnerships

When: Friday, Aug 11, 14:30 - 15:20 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

Speakers: Catherine Terranova, Maia Mazurkiewicz, Maria Bique, Sandra Khalil

SpeakerBio: Catherine Terranova

Catherine Terranova is the Vice President of Operations at the Election Integrity Foundation, the 501(c)(3) organization founded by world renown ethical hacker Harri Hursti. She co-organized the Voting Village at DEFCON 29, DEFCON 30, and DEFCON 31. She is a Columbia University alumna and researcher whose current focus is on cyber security and election integrity with an emphasis on data and voting rights.

Twitter: [@catlovesvoting](#)

SpeakerBio: Maia Mazurkiewicz

Maia Mazurkiewicz is an expert on countering disinformation and behavioural changes. She has 15 years of experience in political management, foreign affairs, and communication in administration, business and CSOs. She is a speaker, trainer and moderator. She believes that we need to change the way we communicate, to introduce more understanding in between humans. She is a Co-founder and Head of StratCom of Alliance4Europe where she deals with strategic communication, to build more diverse internet. She co-founded Future Forces Foundation that is working for more impactful business. She is also Vice-President of the Free European Media Association. In 2017 she co-created Keyboard Warriors in Poland, community that debunks disinformation. Maia is a barrister educated in Poland and the United States. She is actively involved in supporting Ukrainian refugees. Maia cooperated with number of foundations and NGOs where she worked on various projects concerning democratization and political parties trainings in Eastern Europe. She advises clients on strategy building and public affairs, as well as trains on leadership, project management and campaign building.

Twitter: [@MaiaMazurkiewicz](#)

SpeakerBio: Maria Bique

Maria Bique is the CEO and one of the founders of CyberCoach, a cyber awareness geek, data privacy professional, security culture expert and digital rights activist. She has cultured cells in a lab, developed algorithms for analyzing brain activity and led security and tech teams at various companies including Nordea and Futurice. Currently she's lost in the startup world, trying to finish a Ph.D. and fight for digital skills equality through CyberCoach and the #cybercivicduty campaign. With CyberCoach, Maria and the rest of the team are aiming to build the most diverse and impactful cyber security company in the world. In her free time, she's an active football player, assistant football coach and a mentor to aspiring female cyber talent in the US and Europe.

Twitter: [@MariaBique](#)


SpeakerBio: Sandra Khalil

Sandra Khalil manages strategic partnerships for All Tech is Human, a global responsible technology nonprofit organization based in New York. Before her time at All Tech Is Human, she spent eight years working in federal, municipal, and think tank roles making people-to-people connections and amplifying globally underrepresented voices. Sandra holds a Master of Science in Global Security, Conflict, and Cyber from New York University with a concentration on cyber policy. Her interests are at the nexus of people, technology, and democracy, with the end user being the most critical stakeholder and driver of innovation for a safer, equitable, and inclusive tech future.

Description:

Partnerships are critical for companies to integrate expertise into products, policies, and processes, when supporting elections globally. Additionally partnerships are an effective way for organizations to get the word out or share targeted elections information. Explore the ways in which partnerships can be leveraged for greater transparency and collaboration during the electoral processes. It's often much easier to get people to join communities and much harder to keep them engaged and actively participating in community efforts. This Panel discusses how to build operational mechanisms to incentivize participation, projects, develop policies, and drive initiatives within community members that can contribute to the broader

electoral ecosystem and more broadly to civil society. We know the risks to elections, now how do we create partnerships and build competencies to take on the implications?

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Saturday - 12:30-13:20 PDT

Title: Building Space Attack Chains using SPARTA

When: Saturday, Aug 12, 12:30 - 13:20 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio: Brandon Bailey

No BIO available

Description:

Will demonstrate how to use SPARTA to develop attack chains against space systems. This presentation will present pre-existing attack chains (e.g., CySat 2023, Hack-a-Sat 3, etc.) that have been performed as well as new attack chains leveraging the SPARTA TTPs. The presentation will include a demonstration of at least one attack chain using a digital twin simulation.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Building the Hacker Talent Pipeline Through Workforce and Education Ecosystems

When: Friday, Aug 11, 10:00 - 11:50 PDT

Where: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

Speakers: Ashley Sequeira, Ayan Islam, Bryony Crown, Randy Pestana, Safa Shahwan Edwards, Sarah Powazek

SpeakerBio: Ashley Sequeira , Security Operations Sales Engineering Training Program Manager at Google Cloud Security

Ashley is the Security Operations Sales Engineering Training Program Manager at Google Cloud Security. Previously, Sequeira worked for Palo Alto Networks and ran the security operations training program, consulted for SOAR platforms, worked as a professional services consultant and ran an employee resource group focused on veterans. Ashley served 13 years in the US Army Reserve and was hired through a VetsInTech and Palo Alto Networks program.

SpeakerBio: Ayan Islam , Director, Cyber Workforce at Office of the National Cyber Director, The White House
Ayan oversees the cyber workforce portfolio and supports the development and implementation of the upcoming National Cyber Workforce and Education Strategy. Previously, she was Associate Policy Director for R Street's Cybersecurity and Emerging Threats program, and held several roles at the Cybersecurity Infrastructure Security Agency (CISA).

SpeakerBio: Bryony Crown , First Secretary Cyber Policy at British Embassy, Washington D.C.
Bryony Crown is First Secretary for Cyber Policy in the British Embassy Washington DC. She covers a broad range of issues relating to cyber and works with an extensive number of international government and industry partners. Bryony has 15 years' experience in a variety of policy roles within government and specialises in national security issues.

SpeakerBio: Randy Pestana , Associate Director at FIU Jack D Gordon Institute for Public Policy
Randy Pestana serves as Assistant Director of Research and Strategic Initiatives at the Jack D. Gordon Institute for Public Policy at Florida International University's (FIU) Steven J. Green School of International and Public Affairs, where he manages the institute's partnerships with U.S. Departments of Commerce, Defense, and State. Mr. Pestana also serves as Director of Education and Training at Cybersecurity@FIU, a designated Emerging Preeminent Program.


SpeakerBio: Safa Shahwan Edwards , Deputy Director, Cyber Statecraft Initiative at Atlantic Council
Safa Shahwan Edwards is the deputy director of the Atlantic Council's Cyber Statecraft Initiative under the Digital Forensic Research Lab (DFRLab). In this role, she leads the administration and external communications of the Initiative, as well as the Cyber 9/12 Strategy Challenge, the Initiative's global cyber policy and strategy competition. Safa holds an MA in International Affairs with a concentration in Conflict Resolution from the George Washington University Elliott School of International Affairs and a BA in Political Science from Miami University of Ohio. Safa is of Bolivian and Jordanian heritage and speaks Spanish and Arabic.

SpeakerBio: Sarah Powazek , Program Director of Public Interest Cybersecurity at UC Berkeley Center for Long-Term Cybersecurity (CLTC)
Sarah Powazek serves as the Program Director of Public Interest Cybersecurity at the UC Berkeley Center for Long-Term Cybersecurity (CLTC), where she leads flagship work on the Citizen Clinic, the Consortium of Cybersecurity Clinics, and public interest cybersecurity research. She recently hosted the flagship Cyber Civil Defense Summit, a mission-based gathering to protect the nation's most vulnerable public infrastructure. Sarah previously worked at CrowdStrike Strategic Advisory Services, and as the Program Manager of the Ransomware Task Force. She is also an active member of the hacker community, and helps organize Hackers On The Hill and DEF CON Policy.

Description:

Our lives have become more digitally interconnected and the pandemic accelerated the use of technology (remote work, cashless payments, virtual healthcare sessions and gatherings, an uptick in streaming services, etc.). And, year by year, market demand for more information security/cybersecurity professionals is growing and yet research shows there are artificial barriers that limit opportunities for entry level positions to those with the skill, aptitude, and attitude, and impacts underserved

and underrepresented communities. The panel discussion will look at the history of the information security/cybersecurity recruitment pipeline, discuss recent policy changes, and a call to action in removing the artificial barriers that are limiting access into the field. Furthermore, the talk will look at the upcoming National Cyber Workforce and Education Strategy; current public and private sector to address the current workforce challenges; and how we need to bolster our workforce to combat ongoing threats to critical infrastructure. We also can't discuss workforce development without addressing the education landscape and the need to incorporate cybersecurity awareness and skills development in K-12 education systems, and preparing the workforce through two-year, four-year, and post-graduate education programs. The diverse perspectives will cover policy, current activities, and include engagement with the audience to troubleshoot potential solutions on how we can collaboratively work to grow and sustain the hacker talent pipeline.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Burrowing Through The Network: Contextualizing The Vulkan Leaks & Historical State-Sponsored Offensive Operations

When: Sunday, Aug 13, 11:00 - 11:45 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

SpeakerBio: Joe Slowik , Threat Intelligence Manager at Huntress

Joe Slowik has over 15 years' experience across multiple cyber domains. Currently, Joe leads threat intelligence, hunting, detection engineering, and purple teaming functions for Huntress. Previously, Joe performed in-depth threat intelligence research for DomainTools and Dragos, and led incident response operations at Los Alamos National Laboratory. Joe started off in information security through various roles in the US Navy and intelligence community.

Description:

In March 2023, journalists and investigators released analysis of “the Vulkan files.” Consisting of documents associated with a Russian company working with intelligence and military authorities, the papers revealed a variety of ambitious programs such as “Scan-V” and “Amezit.” Both programs, in the sense that they offer capabilities to acquire, maintain, and task infrastructure for cyber and information operations at scale, are deeply concerning, indicating a significant advancement in Russian-linked network warfare and related actions.

Placing these items in context reveals a far more troubling picture. After reviewing the capabilities of Amezit and Scan-V, we can see glimpses of historical programs in the advertised efficacy of these projects. We will consider other items that have leaked over the years offering similar capabilities, albeit in different circumstances. Examples include Russia’s SORM framework for domestic operations, China’s Great Firewall and (more significantly) Great Cannon programs, and items that emerged in the Snowden leaks such as the US’s alleged “Quantum” program.

By analyzing these additional projects, we will observe a decade’s long trend in the systematization and scaling of cyber programs, especially with respect to automated exploitation and infrastructure management. Vulkan and related items, as significant as they are, represent a culmination of operational evolution and an example of the proliferation of capabilities following disclosure. With programs such as Scan-V exposed, we should anticipate other entities seeking to mirror such capabilities, progressing beyond botnets and other distributed systems to effective management of dispersed capabilities for signals intelligence and cyber operations.

REFERENCES

- <https://www.spiegel.de/thema/vulkanfiles/?d=1680188834> - <https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e7>
- <https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare>
- <https://citizenlab.ca/2015/04/chinas-great-cannon/> - <https://resources.infosecinstitute.com/topic/turbine-quantum-implants-arsenal-nsa/> - <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/> - <https://www.wired.com/2014/03/quantum/> - <https://www.domaintools.com/resources/blog/centreon-to-exim-and-back-on-the-trail-of-sandworm/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Sunday - 14:00-14:30 PDT

Title: Bypass 101

When: Sunday, Aug 13, 14:00 - 14:30 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

SpeakerBio: Terry

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Sunday - 14:30-14:59 PDT

Title: Bypass 102


When: Sunday, Aug 13, 14:30 - 14:59 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

SpeakerBio:Ege

Ege is a security researcher specialising in access control systems and electronics. She is currently pursuing a degree in Electrical Engineering and work part-time for GGR Security as a Security Risk Assessor.

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Call Me Phishmael: Hunting Sensitive Docker Images in Google Container Registry Leaks

When: Sunday, Aug 13, 10:00 - 10:40 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Ian Dillon , Staff Security Engineer at New York Times

Ian Dillon is a Staff Security engineer at the New York Times, mostly focusing on cloud security. Long interested in security (like driving 24 hours straight for DEF CON 8), he instead wandered in the desert for years as a software engineer, DBA, then cloud engineer before coming to his senses.

Twitter: [@amenbreakpoint](#)

Description:

UI confusion, ACL limitations, and default product behaviors in Google Cloud Platform (GCP) have created a scenario in which it is very easy to accidentally expose sensitive Google Container Registry (GCR) Docker images to the public. To try and determine the frequency of this misconfiguration, and the resulting value of leaked Docker images to attackers, we built a scanner to help find GCP projects with mis-configured GCR repositories. The results were surprising: scores of open image repositories with sensitive source code and a multitude of active secrets to cloud environments, build systems, and external vendors.

In this presentation, I'll explain the common cause of the GCR misconfiguration and how other GCP service defaults can widen the exposure. We'll also discuss our scanner's approach in narrowing down potential target projects and avoiding GCP abuse mitigation. Finally, we'll go over the common mistakes I found in image builds and applications that allowed simple image exposure to cascade into privilege escalation and direct production system access.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Calling it a 0-Day - Hacking at PBX/UC Systems

When: Saturday, Aug 12, 10:30 - 11:15 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

SpeakerBio: good_pseudonym

No BIO available

Description:

PBX (Private Branch Exchange) and UC (Unified Communications) servers are the big communication brokers in enterprise environments where they love on-prem. They do everything to enable internal and external communications including voice, video, conferencing and messaging. But a broader scope also means a broader attack surface.

In this talk, we'll give an overview PBX/UC systems, what kind of attack surface they have, as well as several bugs that we recently found in two popular PBX/UC products. The journey includes deep-diving Java's Runtime.exec(), decrypting encrypted PHP, bypassing license restrictions, pretending to be a phone, and (of course) getting some shells.

REFERENCES

* VoIP Wars: Attack of the Cisco Phones (DEF CON 22, Fatih Ozavci) * Hacking VoIP Exposed (Black Hat USA 2006, David Endler, Mark Collier)

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Can I put my DNA on the blockchain, mom?

When: Friday, Aug 11, 16:00 - 16:30 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

Speakers: Anne Kim, Michele Orrù

SpeakerBio: Anne Kim

I believe that privacy is a human right and that cryptography can help foster an open society. My research focuses on the intersection of authentication and anonymity. Anne sees accessibility to healthcare as a right by using biology, healthcare policy, and technology.

SpeakerBio: Michele Orrù

No BIO available

Description:

In this talk, we'll show how zero knowledge proofs could be used to prove statements about your health without disclosing the entirety of your DNA. Although this could unlock various use cases in healthcare such as community airdrops and authentication, there are possible abuses like genetic discrimination and reporting by anonymous adversaries. Concluding the talk, we will discuss frameworks that the (hopefully not depressed) audience can use to inform their decision making and activism on the topic of blockchain and healthcare.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 21:00-00:59 PDT

Title: Capitol Tech University, Pub Crawl

When: Saturday, Aug 12, 21:00 - 00:59 PDT

Where: Caesars Forum - Forum - 113-114 - [Map](#)

Description:

Capitol Tech University will be a hosting a pub in the DEF CON pub crawl. Swing by for a chat and a beer!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-12:59 PDT

Title: Capture The Packet FINALS

When: Sunday, Aug 13, 10:00 - 12:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Capture The Packet is returning to DEF CON! Our legendary cyber defense competition has been a Black Badge contest for over 10 years! Glory and prizes await. Follow this event on Twitter at @Capturetp for the latest information on competition dates and times, as well as prizes.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 12:00-17:59 PDT


Title: Capture The Packet Main Rounds

When: Saturday, Aug 12, 12:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Capture The Packet is returning to DEF CON! Our legendary cyber defense competition has been a Black Badge contest for over 10 years! Glory and prizes await. Follow this event on Twitter at @Capturetp for the latest information on competition dates and times, as well as prizes.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:30-17:59 PDT

Title: Capture The Packet Preliminaries

When: Friday, Aug 11, 10:30 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Capture The Packet is returning to DEF CON! Our legendary cyber defense competition has been a Black Badge contest for over 10 years! Glory and prizes await. Follow this event on Twitter at @Capturetp for the latest information on competition dates and times, as well as prizes.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:30-11:59 PDT

Title: Capture The Packet Preliminaries

When: Saturday, Aug 12, 10:30 - 11:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Capture The Packet is returning to DEF CON! Our legendary cyber defense competition has been a Black Badge contest for over 10 years! Glory and prizes await. Follow this event on Twitter at @Capturetp for the latest information on competition dates and times, as well as prizes.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: Car Hacking Village CTF

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The Car Hacking Village CTF is a fun interactive challenge which gives contestants first hand experience to interact with automotive technologies. We work with multiple automotive OEM's and suppliers to ensure our challenges give a real-world experience to car hacking. We understand hacking cars can be expensive, so please come check out our village and flex your skills in hacking automotive technologies.

With the largest collection of hackers in one area, there's no better way to understand the security state of an industry without bringing it to security professionals to break. Over the past 9 years, the Car Hacking Village has been the focal point of interest for new hackers entering the automotive industry to learn, be a part of and actually test out automotive technologies. Our contest at the village, in combination with many automotive OEMs, Suppliers, etc., is used to give people first hand experience on cutting edge and at times expensive technologies. We plan to use this event to keep drawing attention to the automotive security industry through hands-on challenges.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Car Hacking Village CTF

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The Car Hacking Village CTF is a fun interactive challenge which gives contestants first hand experience to interact with automotive technologies. We work with multiple automotive OEM's and suppliers to ensure our challenges give a real-world experience to car hacking. We understand hacking cars can be expensive, so please come check out our village and flex your skills in hacking automotive technologies.

With the largest collection of hackers in one area, there's no better way to understand the security state of an industry without bringing it to security professionals to break. Over the past 9 years, the Car Hacking Village has been the focal point of interest for new hackers entering the automotive industry to learn, be a part of and actually test out automotive technologies. Our contest at the village, in combination with many automotive OEMs, Suppliers, etc., is used to give people first hand experience on cutting edge and at times expensive technologies. We plan to use this event to keep drawing attention to the automotive security industry through hands-on challenges.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Car Hacking Village CTF

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The Car Hacking Village CTF is a fun interactive challenge which gives contestants first hand experience to interact with automotive technologies. We work with multiple automotive OEM's and suppliers to ensure our challenges give a real-world experience to car hacking. We understand hacking cars can be expensive, so please come check out our village and flex your skills in hacking automotive technologies.

With the largest collection of hackers in one area, there's no better way to understand the security state of an industry without bringing it to security professionals to break. Over the past 9 years, the Car Hacking Village has been the focal point of interest for new hackers entering the automotive industry to learn, be a part of and actually test out automotive technologies. Our contest at the village, in combination with many automotive OEMs, Suppliers, etc., is used to give people first hand experience on cutting edge and at times expensive technologies. We plan to use this event to keep drawing attention to the automotive security industry through hands-on challenges.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Career Workshop: New Career Seekers In Cybersecurity

When: Friday, Aug 11, 15:00 - 15:50 PDT

Where: Caesars Forum - Alliance - 301-304 - Blacks in Cyber Village - [Map](#)


SpeakerBio:Keith Chapman

Keith Chapman is a former school teacher and has been a cybersecurity professional for the better part of a decade. He is currently a manager of U.S. Bank's global security operations center and is a reservist and emergency cyber responder for the state of Ohio as a member of the Ohio Cyber Reserve, a team of trained civilians which assists municipalities with cybersecurity vulnerabilities and fosters workforce development efforts within the state. He also participates in other cyber workforce development initiatives, including his work with Dayton Equity and Ohio high schools.

Description:

Cybersecurity is a new collar job where college and/or university is optional and there are alternate methods of getting the training and development for entry level roles such as workshops, bootcamps, online courses and a wealth of cybersecurity focused certifications and certificates. Career seekers from other fields can

This workshop is for individuals that are involved in or initiating cyber workforce development programs. It involves best practices and techniques for managing an effective and sustainable program.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Cellular carriers hate this trick: Using SIM tunneling to travel at light speed

When: Sunday, Aug 13, 10:00 - 10:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers: Adrian "atrox" Dabrowski, Gabriel K. Gegenhuber

SpeakerBio: Adrian "atrox" Dabrowski , CISPA Helmholtz Center for Cybersecurity

Adrian Dabrowski wrote his PhD about large infrastructures including the identifying fake base stations (“IMSI Catchers”). Before his PhD, he was a founding member of two hackerspaces in Vienna, Austria, and on the board of one of them.

Twitter: [@atrox_at](#)

SpeakerBio: Gabriel K. Gegenhuber , University of Vienna & SBA Research

Gabriel Gegenhuber is PhD candidate in Vienna, Austria. Gabriel is conducting research in the area of cellular and mobile networks. This includes Internet measurement technologies, traffic classification systems (e.g., deep packet inspection), and technical measures that are used to detect net neutrality and privacy violations.

Twitter: [@GGegenhuber](#)

Description:

Cellular networks form large complex compounds for roaming purposes. Thus, geographically-spread testbeds for measurements and rapid exploit verification are needed to do justice to the technology's unique structure and global scope. Additionally, such measurements suffer from a combinatorial explosion of operators, mobile plans, and services. To cope with these challenges, we are releasing an open-source framework that geographically decouples the SIM (subscription) from the cellular modem by selectively connecting both remotely. This allows testing any subscriber with any operator at any modem location within seconds without moving parts. The resulting measurement and testbed platform "MobileAtlas" offers a scalable, controlled experimentation environment. It is fully open-sourced and allows other researchers to contribute locations, SIM cards, and measurement scripts.

Using the above framework, our international experiments in commercial networks revealed exploitable inconsistencies in traffic metering, leading to multiple data "phreaking" opportunities ("free-ride"). We also expose problematic IPv6 firewall configurations, hidden SIM card communication to the home network, and fingerprint dial progress tones to track victims across different roaming networks and countries with voice calls.

REFERENCES:

Gabriel K. Gegenhuber, Wilfried Mayer, and Edgar Weippl. Zero-Rating, One Big Mess: Analyzing Differential Pricing Practices of European MNOs. In IEEE Global Communications Conference (GLOBECOM), 2022 Gabriel K. Gegenhuber, Wilfried Mayer, Edgar Weippl, Adrian Dabrowski. MobileAtlas: Geographically Decoupled Measurements in Cellular Networks for Security and Privacy Research., 2023, In proceedings of the 32th USENIX Security Symposium 2023. David Allen Burgess. What is AT&T doing at 1111340002? Welcome to the magical world of proac-tive SIMs., 2021. <https://medium.com/telecom-expert/what-is-at-t-doing-at-1111340002-c418876c212c> David Allen Burgess. More Proactive SIMs., 2021. <https://medium.com/telecom-expert/more-proactive-sims-f8da2ef8b189> OSMOCOM. Simtrace 2. <https://osmocom.org/projects/simtrace2/wiki> osmocom.org. pySim-prog - Utility for programmable SIM/USIM-Cards. <https://osmocom.org/projects/pysim/wiki> The MONROE Alliance. Measuring Mobile Broadband Networks in Europe. <https://www.monroe-project.eu>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: certmitm: automatic exploitation of TLS certificate validation vulnerabilities

When: Friday, Aug 11, 16:30 - 17:15 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

SpeakerBio: Aapo Oksman, Senior Security Specialist at Nixu Corporation

Aapo Oksman is a Senior Security Specialist at Nixu Corporation working with application, network and device security. His background is in electrical engineering, embedded devices, and test automation. Combining his background with a hobby in hacking lead to a career in cybersecurity focusing on industrial IoT.

In his free time, Bug Bounties and security research keep Aapo motivated and learning. His work in PKI and TLS has resulting in multiple CVEs from vendors such as Microsoft and Apple. Outside work and research Aapos passion is in the community. He takes part in organizing local security meetups and coaches the Finnish national youth CTF team to the yearly European Cybersecurity Challenge competition.

Description:

TLS is the de facto way of securing network connections. It provides an easy way of ensuring confidentiality, integrity and authentication for any type of communication. However, like most things in life, this is also too good to be true.

TLS allows communicating parties to uniquely authenticate each other by validating each other's certificate. However, many TLS libraries and frameworks have insecure default settings or allow for the developers to skip important aspects of certificate validation in their client implementations.

This talk explores issues in TLS client certificate validation and the underlying reasons why developers still fail to implement TLS correctly. Most importantly, we hack all the things with a new TLS mitm tool: certmitm.

certmitm automatically discovers and exploits insecure certificate validation vulnerabilities in TLS clients. Let's use the tool to hack iOS, Windows 11 and more while we deep dive into the world of insecure TLS certificate validation.

REFERENCES

My previous TLS talks:

HelSec 20 - Practical attacks against modern TLS implementations - Aapo Oksman:

<https://www.youtube.com/watch?v=NCm16vLfD60>

Disobey 2023 - Your connection is not private Exploiting insecure certificate validation in TLS clients - Aapo Oksman:

<https://www.youtube.com/watch?v=vZvL6ZRiKIs>

Moxie Marlinspikes work in SSL/TLS:

DEF CON 17 - Moxie Marlinspike - More Tricks for Defeating SSL: <https://www.youtube.com/watch?v=5dhSN9aEljg>

DEF CON 19 - Moxie Marlinspike - SSL And The Future Of Authenticity: https://www.youtube.com/watch?v=UawS3_iuHoA


Scientific publications:

Georgiev, Martin, et al. "The most dangerous code in the world: validating SSL certificates in non-browser software."

Proceedings of the 2012 ACM conference on Computer and communications security. 2012. Akhawe, Devdatta, et al. "Here's my cert, so trust me, maybe? Understanding TLS errors on the web." Proceedings of the 22nd international conference on World Wide Web. 2013. Huang, Lin Shung, et al. "Analyzing forged SSL certificates in the wild." 2014 IEEE Symposium on Security and Privacy. IEEE, 2014.

Sivakorn, Suphannee, et al. "HVLearn: Automated black-box analysis of hostname verification in SSL/TLS implementations." 2017 IEEE Symposium on Security and Privacy (SP). IEEE, 2017. Alghamdi, Khalid, et al. "Iotverif: An automated tool to

verify ssl/tls certificate validation in android mqtt client applications." Proceedings of the Eighth ACM Conference on data and application security and privacy. 2018.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Friday - 11:00-11:30 PDT

Title: Certs Fucking Suck, So We Made a Cert: DISCO for Bodily Autonomy

When: Friday, Aug 11, 11:00 - 11:30 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

Speakers:Blunt,Daly


SpeakerBio:Blunt

No BIO available

SpeakerBio:Daly

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Saturday - 16:30-17:25 PDT

Title: ChatGPT: Your Red Teaming Ally

When: Saturday, Aug 12, 16:30 - 17:25 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

SpeakerBio: Gavin Klondike

No BIO available

Description:

In this talk, we'll dive into how ChatGPT can enhance your existing workflow and provide valuable insights. We'll start with a brief overview of what GPT models are, how to craft the perfect prompt, and then focus on red team specific use cases for day-to-day operations.

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Saturday - 11:30-12:15 PDT

Title: Chinese Prototype Review


When: Saturday, Aug 12, 11:30 - 12:15 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio: William Baggett

Will Baggett has a background in the U.S. Intelligence Community and also in NATO SOF as a cyber instructor. His experience in the Intelligence Community provided a foundation for Insider Threat, Digital Forensics, and Cyber Intelligence consulting to pharmaceutical, financial, and technical entities. He is a graduate of Georgia Tech, holds multiple digital forensic certifications as well as that of a Certified Fraud Examiner and has appeared on several news broadcasts discussing cybersecurity issues. Will is also the Director of Digital Forensic services for Operation Safe Escape, a volunteer-run non-profit assisting domestic abuse victims as they begin new lives.

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Cicada 3301: An Exploration of the Cryptographic Enigma

When: Friday, Aug 11, 16:00 - 16:45 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

Speakers: Artorias, Puck, Taiwo, TheClockworkBird

SpeakerBio: Artorias

Artorias is the creator of CicadaSolvers.com, co-host of the CicadaCast podcast, and moderator of r/cicada and the CicadaSolvers discord. Well-versed in the complex history of the Cicada 3301 puzzles, he labors both to document the mystery of Cicada 3301, and to unravel the labyrinth of its interconnected topics.

SpeakerBio: Puck

Puck is a 19-year-old rising junior computer science major and Cicada 3301 puzzle enthusiast. He has been involved in the community for four years, finding inspiration to pursue cryptography and cybersecurity. Puck has focused his work on promoting community solving efforts, mainly in the form of innovative events.

SpeakerBio: Taiwo

Taiwo, a CicadaSolvers founding member, with a background in software development, sees the community's work as an example for the future of problem-solving. With a pragmatic, and sceptical approach to the puzzle, he aims to preserve the community so that it can continue to impact the lives of others as immensely as it did for him.

SpeakerBio: TheClockworkBird

TheClockworkBird With a background in anthropology and teaching, TheClockworkBird creates collaborative spaces where people of all skill levels and interests can engage with the puzzle. He has gained a multifaceted understanding of Cicada's impact on the individual, and the impacts of collaborative puzzle solving on the growth of privacy awareness.

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Civil Cyber Defense: Use Your Resources to Defend Non-Profits as they Combat Human Trafficking and Subvert Authoritarian Regimes

When: Friday, Aug 11, 11:30 - 12:15 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

Speakers: Austin Shamlin, Tiffany Rad

SpeakerBio: Austin Shamlin , Co-Founder at Traverse Project

Austin Shamlin is the CEO and founder of Traverse Project, a nonprofit founded in 2023 to combat human trafficking networks. He has served in the law enforcement and security industry for over 20 years, most recently serving as director of operations with an anti-human trafficking nonprofit under the Tim Tebow Foundation. Austin is a professionally recognized geopolitical security subject matter expert on Haiti and has previously served as a special advisor to the Haitian Minister of Justice. Prior to his nonprofit work, he served as a police executive with the D.C. government. Prior to working for the District of Columbia, Austin worked as a government contractor in Somalia, Afghanistan, Iraq, and Haiti.

SpeakerBio: Tiffany Rad , Instructor at U.C. Berkeley

Tiffany Strauchs Rad (BS, MA, MBA, JD) has presented cybersecurity research – both technical and legal topics -- at many security conferences such as Black Hat USA, Black Hat Abu Dhabi, Defcon (17, 18, 19), H.O.P.E., 27C3 & 28C3, and has been featured in media such as Wired, Washington Post, CNN, Reuters, 60 Minutes, Der Spiegel, CNN, Wired Magazine, and NPR. Her independent security research was listed as #4 in "Top 10 White Hat Hacks" by Bloomberg, and her critical infrastructure research was featured on the USA network series, "Mr. Robot." In addition to being a car hacker and doing transportation infrastructure security consulting, she is also an adjunct instructor at the University of Maine and U.C. Berkeley teaching classes such as the "Citizen Clinic."


Twitter: [@tiffanyrad](#)

Description:

Civil Cyber Defense volunteers and students challenge high-risk adversaries and threats such as human traffickers, authoritarian regimes, and surveillance being conducted on journalists. By utilizing academic resources, OSINT skills, and free/open-source tools, civil cyber defenders are supporting vulnerable non-profits, protecting volunteers, journalists, and activists while defending human rights. There is a need in the cybersecurity industry for more civil cyber defenders. Recommendations will be made as to how your organization can support and/or volunteer your time and tools to provide protection to vulnerable organizations who have high risks, face advanced and persistent adversaries, but have modest resources.

REFERENCES

The content we will present was generated by the speakers. Tiffany will present anonymized case studies from the "Citizen Clinic" at UC Berkeley and Austin will share case studies his organization has generated regarding human trafficking. Our only bibliographic reference at this moment is a reference to open source/free software tools we use at UC Berkeley. We will also reference a tool to make VPNs safer created by Berkeley's students called "Ghost Prtcl."

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Friday - 14:00-14:30 PDT

Title: Climate Change and its Implications for Security and Privacy: An Uncharted Territory

When: Friday, Aug 11, 14:00 - 14:30 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio:Chloé Messdaghi

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

CLV - Friday - 10:10-10:50 PDT

Title: Cloud Village - Keynote

When: Friday, Aug 11, 10:10 - 10:50 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Ben "NahamSec" Sadeghipour, Hacker & Content Creator at NahamSec

Ben Sadeghipour AKA NahamSec is a security researcher and content creator. He's currently in the top 100 for both HackerOne(25) and Bugcrowd's (95) leaderboards. He has helped identify over a thousand vulnerabilities in companies like Amazon, Apple, Airbnb, Lyft, Snapchat and more. Prior to doing content creation full time, he worked as a research and community education executive at Hadrian and HackerOne. Ben has presented many talks and workshops at cons such as DEFCON, BSides, OWASP AppSec, RSA, Red Team Village, and more. He also enjoys hosting and organizing hacker meetups or virtual conferences such as NahamCon and Hacktivitycon!

Twitter: [@nahamsec](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT

Title: Cloud Village CTF

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Virtual

Description:

If you ever wanted to break stuff on the cloud, or if you like rabbit holes that take you places you did not think you would go to, follow complicated story lines to only find you could have reached to the flag without scratching your head so much - then this CTF is for you!

Our CTF is a three days jeopardy style contest where we have a bunch of challenges hosted across multiple Cloud providers across multiple categories of difficulty.

You can register as teams or go solo, use hints or stay away from them, in the end it will be all for glory or nothing. Plus the prizes. Did we not mention the prizes? :D

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: Cloud Village CTF

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Virtual

Description:

If you ever wanted to break stuff on the cloud, or if you like rabbit holes that take you places you did not think you would go to, follow complicated story lines to only find you could have reached to the flag without scratching your head so much - then this CTF is for you!

Our CTF is a three days jeopardy style contest where we have a bunch of challenges hosted across multiple Cloud providers across multiple categories of difficulty.

You can register as teams or go solo, use hints or stay away from them, in the end it will be all for glory or nothing. Plus the prizes. Did we not mention the prizes? :D

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

Title: Cloud Village CTF

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Virtual

Description:

If you ever wanted to break stuff on the cloud, or if you like rabbit holes that take you places you did not think you would go to, follow complicated story lines to only find you could have reached to the flag without scratching your head so much - then this CTF is for you!

Our CTF is a three days jeopardy style contest where we have a bunch of challenges hosted across multiple Cloud providers across multiple categories of difficulty.

You can register as teams or go solo, use hints or stay away from them, in the end it will be all for glory or nothing. Plus the prizes. Did we not mention the prizes? :D

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: CloudRecon - finding ephemeral assets in the cloud

When: Saturday, Aug 12, 13:00 - 13:30 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

Speakers: Gunnar Andrews, Jason Haddix

SpeakerBio: Gunnar Andrews

No BIO available

Twitter: [@GOLDEN_infosec](#)

SpeakerBio: Jason Haddix, CISO and “Hacker in Charge” at BuddoBot

Jason Haddix is the CISO and “Hacker in Charge” at BuddoBot, a world-class adversary emulation consultancy. He's had a distinguished 15-year career in cybersecurity previously serving as the CISO of Ubisoft, Head of Trust/Security/Operations at Bugcrowd, Director of Penetration Testing at HP, and Lead Penetration Tester at Redspin. He has also held positions doing mobile penetration testing, network/infrastructure security assessments, and static analysis. Jason is a hacker and bug hunter to the core, and he is ranked 51st all-time on Bugcrowd's leaderboards. Currently, he specializes in recon and web application analysis. Jason has also authored many talks on offensive security methodology, including speaking at cons such as; DEF CON, Black Hat, OWASP, RSA, Nullcon, SANS, IANS, BruCon, Toorcon, and many more. Jason currently lives in Colorado with his wife and three children.

Twitter: [@jhaddix](#)

Description:

CloudRecon is a suite of tools for red teamers and bug hunters to find ephemeral and development assets in their campaigns and hunts.

Often, target organizations stand up cloud infrastructure that is not tied to their ASN or related to known infrastructure. Many times these assets are development sites, IT product portals, etc. Sometimes they don't have domains at all but many still need HTTPs.

CloudRecon is a suite of tools to scan all the cloud providers and find these hidden gems for testers, by inspecting those SSL certificates.

The tool suite is three parts in GO:

- CloudScrape - A LIVE running tool to inspect the ranges for a keyword in SSL certs OU, CN, and SN fields in real time.
- CertStan - a tool to retrieve the ranges of AWS, GCP, and Azure, and download all their certs to your box. So you can have your OWN cert.sh database.
- CertSniff - a tool to parse and search through the downloaded certs for keywords.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: CMD+CTRL at DEF CON 31 - Booth Open

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)


Description:

CMD+CTRL Cyber Range is an interactive learning and hacking platform where development, security, IT, and other roles come together to build an appreciation for protecting the enterprise. Players learn security techniques in a real-world environment where they compete to find vulnerabilities. Real-time scoring keeps participants engaged and creates friendly competition. Our Cloud and App Cyber Ranges incorporate authentic, fully functioning applications and vulnerabilities often found in commercial web platforms.

Learn to see web applications and services from an attacker's perspective. CMD+CTRL is a hacking game designed to teach the fundamentals of web application security. Explore vulnerable web applications, discover security flaws, and exploit those flaws to earn points and climb up the scoreboard. After attacking an application for yourself, you'll have a better understanding of the vulnerabilities that put real applications at risk - and you'll be better prepared to find and fix those vulnerabilities in your own code.

At DEF CON 31: We will be debuting our latest Cyber Range, which focuses on exploiting a modern health record management system, dubbed ShadowHealth. Inspired by the latest trends and real world exploits, try your hands exploiting: SSRF, Log4Shell, reverse engineering, local privilege escalation, password cracking, XSS, and so much more! With over 35 challenges do you think you can complete them all?

CMD+CTRL will have two different games happening: free play, and the competition. Both require a code to join, and the best way to get a code is to go to the CMD+CTRL booth in the contest area. Codes to join free play may be given in Discord, on Thursday. Questions and such will also only be answered at the booth; Discord will not be staffed this year, aside from free play codes on Thursday. Once you have a code, you can play online, from anywhere -- you do not have to be in the contest area.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: CMD+CTRL at DEF CON 31 - Booth Open

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)


Description:

CMD+CTRL Cyber Range is an interactive learning and hacking platform where development, security, IT, and other roles come together to build an appreciation for protecting the enterprise. Players learn security techniques in a real-world environment where they compete to find vulnerabilities. Real-time scoring keeps participants engaged and creates friendly competition. Our Cloud and App Cyber Ranges incorporate authentic, fully functioning applications and vulnerabilities often found in commercial web platforms.

Learn to see web applications and services from an attacker's perspective. CMD+CTRL is a hacking game designed to teach the fundamentals of web application security. Explore vulnerable web applications, discover security flaws, and exploit those flaws to earn points and climb up the scoreboard. After attacking an application for yourself, you'll have a better understanding of the vulnerabilities that put real applications at risk - and you'll be better prepared to find and fix those vulnerabilities in your own code.

At DEF CON 31: We will be debuting our latest Cyber Range, which focuses on exploiting a modern health record management system, dubbed ShadowHealth. Inspired by the latest trends and real world exploits, try your hands exploiting: SSRF, Log4Shell, reverse engineering, local privilege escalation, password cracking, XSS, and so much more! With over 35 challenges do you think you can complete them all?

CMD+CTRL will have two different games happening: free play, and the competition. Both require a code to join, and the best way to get a code is to go to the CMD+CTRL booth in the contest area. Codes to join free play may be given in Discord, on Thursday. Questions and such will also only be answered at the booth; Discord will not be staffed this year, aside from free play codes on Thursday. Once you have a code, you can play online, from anywhere -- you do not have to be in the contest area.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT

Title: CMD+CTRL at DEF CON 31 - Booth Open

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

CMD+CTRL Cyber Range is an interactive learning and hacking platform where development, security, IT, and other roles come together to build an appreciation for protecting the enterprise. Players learn security techniques in a real-world environment where they compete to find vulnerabilities. Real-time scoring keeps participants engaged and creates friendly competition. Our Cloud and App Cyber Ranges incorporate authentic, fully functioning applications and vulnerabilities often found in commercial web platforms.

Learn to see web applications and services from an attacker's perspective. CMD+CTRL is a hacking game designed to teach the fundamentals of web application security. Explore vulnerable web applications, discover security flaws, and exploit those flaws to earn points and climb up the scoreboard. After attacking an application for yourself, you'll have a better understanding of the vulnerabilities that put real applications at risk - and you'll be better prepared to find and fix those vulnerabilities in your own code.

At DEF CON 31: We will be debuting our latest Cyber Range, which focuses on exploiting a modern health record management system, dubbed ShadowHealth. Inspired by the latest trends and real world exploits, try your hands exploiting: SSRF, Log4Shell, reverse engineering, local privilege escalation, password cracking, XSS, and so much more! With over 35 challenges do you think you can complete them all?

CMD+CTRL will have two different games happening: free play, and the competition. Both require a code to join, and the best way to get a code is to go to the CMD+CTRL booth in the contest area. Codes to join free play may be given in Discord, on Thursday. Questions and such will also only be answered at the booth; Discord will not be staffed this year, aside from free play codes on Thursday. Once you have a code, you can play online, from anywhere -- you do not have to be in the contest area.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-11:59 PDT

Title: CMD+CTRL at DEF CON 31 - Competition

When: Friday, Aug 11, 10:00 - 11:59 PDT

Where: Virtual

Description:

CMD+CTRL Cyber Range is an interactive learning and hacking platform where development, security, IT, and other roles come together to build an appreciation for protecting the enterprise. Players learn security techniques in a real-world environment where they compete to find vulnerabilities. Real-time scoring keeps participants engaged and creates friendly competition. Our Cloud and App Cyber Ranges incorporate authentic, fully functioning applications and vulnerabilities often found in commercial web platforms.

Learn to see web applications and services from an attacker's perspective. CMD+CTRL is a hacking game designed to teach the fundamentals of web application security. Explore vulnerable web applications, discover security flaws, and exploit those flaws to earn points and climb up the scoreboard. After attacking an application for yourself, you'll have a better understanding of the vulnerabilities that put real applications at risk - and you'll be better prepared to find and fix those vulnerabilities in your own code.

At DEF CON 31: We will be debuting our latest Cyber Range, which focuses on exploiting a modern health record management system, dubbed ShadowHealth. Inspired by the latest trends and real world exploits, try your hands exploiting: SSRF, Log4Shell, reverse engineering, local privilege escalation, password cracking, XSS, and so much more! With over 35 challenges do you think you can complete them all?

CMD+CTRL will have two different games happening: free play, and the competition. Both require a code to join, and the best way to get a code is to go to the CMD+CTRL booth in the contest area. Codes to join free play may be given in Discord, on Thursday. Questions and such will also only be answered at the booth; Discord will not be staffed this year, aside from free play codes on Thursday. Once you have a code, you can play online, from anywhere -- you do not have to be in the contest area.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: CMD+CTRL at DEF CON 31 - Free Play

When: Thursday, Aug 10, 10:00 - 11:59 PDT

Where: Virtual

Description:

CMD+CTRL Cyber Range is an interactive learning and hacking platform where development, security, IT, and other roles come together to build an appreciation for protecting the enterprise. Players learn security techniques in a real-world environment where they compete to find vulnerabilities. Real-time scoring keeps participants engaged and creates friendly competition. Our Cloud and App Cyber Ranges incorporate authentic, fully functioning applications and vulnerabilities often found in commercial web platforms.

Learn to see web applications and services from an attacker's perspective. CMD+CTRL is a hacking game designed to teach the fundamentals of web application security. Explore vulnerable web applications, discover security flaws, and exploit those flaws to earn points and climb up the scoreboard. After attacking an application for yourself, you'll have a better understanding of the vulnerabilities that put real applications at risk - and you'll be better prepared to find and fix those vulnerabilities in your own code.

At DEF CON 31: We will be debuting our latest Cyber Range, which focuses on exploiting a modern health record management system, dubbed ShadowHealth. Inspired by the latest trends and real world exploits, try your hands exploiting: SSRF, Log4Shell, reverse engineering, local privilege escalation, password cracking, XSS, and so much more! With over 35 challenges do you think you can complete them all?


CMD+CTRL will have two different games happening: free play, and the competition. Both require a code to join, and the best way to get a code is to go to the CMD+CTRL booth in the contest area. Codes to join free play will be given in Discord, on Thursday. Once you have a code, you can play online, from anywhere -- you do not have to be in the contest area.

For free play specifically:

We will utilize our contest channel on Discord:

[ce-cmd-ctrl-cyberange-text](<https://discord.com/channels/708208267699945503/711643642388807800>) CMD+CTRL Cyber Range Free Play, Thur 10:00 AM PT - Sun 12:00 PM PT

We will broadcast sign up instructions within this channel once Free Play beings.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: CNAPPGoat - A multicloud vulnerable-by-design infrastructure deployment tool

When: Sunday, Aug 13, 12:40 - 13:10 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

Speakers:Igal Gofman,Noam Dahan

SpeakerBio:Igal Gofman

Igal Gofman is a Head of Security Research at Ermetic. Igal has a proven track record in cloud security, network security, research-oriented development, and threat intelligence. His research interests include cloud security, operating systems, and active directory. Prior to Ermetic Igal worked at Microsoft, XM-Cyber, and Check Point Software Technologies. Igal has spoken at various leading security conferences including Black Hat and DEF-CON.

Twitter: [@IgalGofman](#)

SpeakerBio:Noam Dahan , Senior Security Researcher at Ermetic

Noam Dahan is a Senior Security Researcher at Ermetic with several years of experience in embedded security. He is a graduate of the Talpiot program at the Israel Defense Forces and spent several years in the 8200 Intelligence Corps. Noam was a competitive debater and is a former World Debating Champion. He is also a former speaker at Black Hat USA, DEF CON DemoLabs, Cloud Village and fwd:cloudsec.

Twitter: [@NoamDahan](#)

Description:

CNAPPGoat is a CLI tool designed to deploy intentionally vulnerable-by-design cloud infrastructure. It provides a useful playground for defenders to test their protective strategies, tools, and procedures and for offensive professionals to refine their skills and tooling. This tool deploys diverse infrastructures, including those with misconfigurations, IAM issues, network exposure, and those conducive to lateral movement attacks. While other (excellent) tools are designed to deploy tailored capture-the-flag scenarios, CNAPPGoat takes a broader approach by deploying a wide array of environments with diverse misconfigurations, providing a comprehensive perspective.

CNAPPGoat supports modular deployment of various vulnerable environments and is a multi-cloud tool. CNAPPGoat is built on Pulumi and supports multiple programming languages. It operates as a CLI tool, requiring no specific IaC expertise, enabling a wide range of professionals to deploy and monitor environments.

The tool enables defenders to test detection, prevention, and control mechanisms against vulnerabilities and misconfigurations, while aiding offensive professionals by providing practice environments. Demonstrations will include tool showcasing, deployment and remediation of a scenario, practical exploitation for learning, and guidance on building modules to customize CNAPPGoat.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: CNAPPGoat

When: Friday, Aug 11, 12:00 - 13:55 PDT

Where: Caesars Forum - Accord Boardroom - Demo Labs - [Map](#)

Speakers:Igal Gofman,Noam Dahan

SpeakerBio:Igal Gofman

Igal Gofman is a Head of Security Research at Ermetic. Igal has a proven track record in cloud security, network security, research-oriented development, and threat intelligence. His research interests include cloud security, operating systems, and active directory. Prior to Ermetic Igal worked at Microsoft, XM-Cyber, and Check Point Software Technologies. Igal has spoken at various leading security conferences including Black Hat and DEF-CON.

Twitter: [@IgalGofman](#)

SpeakerBio:Noam Dahan , Senior Security Researcher at Ermetic

Noam Dahan is a Senior Security Researcher at Ermetic with several years of experience in embedded security. He is a graduate of the Talpiot program at the Israel Defense Forces and spent several years in the 8200 Intelligence Corps. Noam was a competitive debater and is a former World Debating Champion. He is also a former speaker at Black Hat USA, DEF CON DemoLabs, Cloud Village and fwd:cloudsec.

Twitter: [@NoamDahan](#)

Description:

CNAPPGoat is a multi-cloud vulnerable-by-design environment deployment tool – it deploys vulnerable environments to various cloud service providers, so that offensive professionals and pentesters can practice exploiting them and defenders can practice detection and prevention. CNAPPGoat is an extensible modular tool that deploys environments with more complex scenarios - vulnerable VMs, multi-stage lateral movement attacks, IaC misconfigurations, and vulnerable IAM misconfigurations.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SEV - Saturday - 13:30-15:30 PDT

Title: Cold Calls


When: Saturday, Aug 12, 13:30 - 15:30 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description:

Cold Calls give attendees a walk-up opportunity to make a short call to get a feel for both the contest and the world of Social Engineering through vishing but without the contest elements.

This is on a first-come, first-served basis. Please see the "More Information" link.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SEV - Saturday - 10:00-11:30 PDT

Title: Cold Calls


When: Saturday, Aug 12, 10:00 - 11:30 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description:

Cold Calls give attendees a walk-up opportunity to make a short call to get a feel for both the contest and the world of Social Engineering through vishing but without the contest elements.

This is on a first-come, first-served basis. Please see the "More Information" link.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SEV - Sunday - 10:00-11:30 PDT

Title: Cold Calls


When: Sunday, Aug 13, 10:00 - 11:30 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description:

Cold Calls give attendees a walk-up opportunity to make a short call to get a feel for both the contest and the world of Social Engineering through vishing but without the contest elements.

This is on a first-come, first-served basis. Please see the "More Information" link.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: CON trolling the weather

When: Friday, Aug 11, 15:00 - 15:45 PDT

Where: Harrah's - Nevada Ballroom - Lake Tahoe & Reno - War Stories - On the Record - [Map](#)

SpeakerBio: Paz Hameiri , Hacker

Paz started his professional life more than 30 years ago, hacking games and developing tools in his teen years. Since then, he has worked in several companies, developing both hardware and software. Paz has six years of experience with telecommunication systems design and circuits.

For 14 years, Paz led multidisciplinary systems development as a systems engineer in the aerospace industry. At home, Paz explores ideas he finds interesting.

In 2019 he published a work on a body-tracking device that records keystrokes on a safe's keypad in Hakin9 Magazine. In 2021 he developed software that used a GPU as a digital radio transmitter and presented his work at DEF CON 29. In 2015 and 2019 he launched weather balloons with elementary school pupils.

Description:

Nearly 1,800 weather balloons are launched across the world on any given day. As the balloon goes up it expands and pops at an altitude up to 33 Km (110K feet) above the earth. The flight payload is called a radiosonde. It measures pressure, temperature, relative humidity, position, and velocity during its flight, and transmits the data to a sounding receiver. One or two missing weather balloons won't impact the daily forecast. However, many missing balloons could lead to errors in weather models and forecasts. Weather balloons are also important for gathering weather data for satellite launches and human spaceflights, as launches are often delayed or scrubbed due to upper-level wind shear.

In this talk, I present a simulation framework for the most popular radiosonde model. It enables an attacker to generate radiosonde messages or alter logged messages for retransmission. I also present simulations of a jamming attack and a spoofing attack on a sounding receiver:

During a jamming attack, the receiver is unable to receive transmissions from active radiosondes.

During a spoofing attack, the transmitter sends fake radiosonde messages to a target receiver, identifying as an active radiosonde.

I'll talk about the shortcomings of the military variant of the radiosonde model and suggest a simple way to cope with spoofing attacks.

REFERENCES

- Vredenbregt L., "How many weather balloons are out there? Hundreds, it turns out", <https://abcnews.go.com/Politics/weather-balloons-hundreds-turns/story?id=97082985>, Feb 13, 2023. Dudley I., "Weather balloons and rocket science", <https://www.vandenberg.spaceforce.mil/News/Features/Display/Article/737270/weather-balloons-and-rocket-science/bazjo>, "RS41 Decoding", https://github.com/bazjo/RS41_Decoding rs1729, "RS", <https://github.com/rs1729/RS> projecthorus, "radiosonde_auto_rx", https://github.com/projecthorus/radiosonde_auto_rx sondehub, https://github.com/projecthorus/radiosonde_auto_rx "Upper-air Observations Program", <https://www.weather.gov/upperair/> Mass C., "Wind Shear: When the Atmospheric Seems to be Tearing Itself Apart", <https://cliffmass.blogspot.com/2017/05/wind-shear-when-atmospheric-seems-to-be.html> Jessop M., "Top Radiosonde types", <https://twitter.com/vk5qi/status/1170215238978830339> Lada B., "3 weather obstacles that SpaceX faces when launching rockets into space", <https://www.accuweather.com/en/space-news/types-of-weather-that-can-delay-a-spacex-rocket-launch/352407> Nasa, "Falcon 9 Crew Dragon Launch Weather Criteria", FS-2020-05-568-KSC, www.nasa.gov Frielingdorf J., "An

Open-Source Documentation and Implementation of the Vaisala RS41 Data Preparation Algorithms", WMO Technical Conference on Meteorological and Environmental Instruments and Methods of Observation, Oct. 11, 2022
Cadence PCB Solutions, "What is Signal to Noise Ratio and How to calculate it?", <https://resources.pcb.cadence.com/blog/2020-what-is-signal-to-noise-ratio-and-how-to-calculate-it>
Vaisala, "Vaisala Radiosonde RS41-SGP Data Sheet", www.vaisala.com, B211444EN-E, 2017
Vaisala, "Vaisala Radiosonde RS41-SG Data Sheet", www.vaisala.com, B211321EN-K, 2020
Vaisala, "Vaisala Radiosonde RS41-SGM Data Sheet", www.vaisala.com, B211448EN-E, 2017



[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

Title: CON trolling the weather

When: Saturday, Aug 12, 12:00 - 12:25 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio: Paz Hameiri , Hacker

Paz started his professional life more than 30 years ago, hacking games and developing tools in his teen years. Since then, he has worked in several companies, developing both hardware and software. Paz has six years of experience with telecommunication systems design and circuits.

For 14 years, Paz led multidisciplinary systems development as a systems engineer in the aerospace industry. At home, Paz explores ideas he finds interesting.

In 2019 he published a work on a body-tracking device that records keystrokes on a safe's keypad in Hakin9 Magazine. In 2021 he developed software that used a GPU as a digital radio transmitter and presented his work at DEF CON 29. In 2015 and 2019 he launched weather balloons with elementary school pupils.

Description:

Weather balloons' radiosondes measure and transmit weather data. Besides weather models and forecasts, radiosondes are also important for gathering weather data for satellite launches and human spaceflights. I'll present a simulation framework for the most popular radiosonde model and present simulations of a jamming attack and a spoofing attack on a receiver. I'll talk about the shortcomings of the military variant of the radiosonde model and suggest a simple way to cope with spoofing attacks.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Conflicting Security Reports from Halderman-Springall and from MITRE: Which Is Right?

When: Saturday, Aug 12, 12:55 - 13:40 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

Speakers: David Jefferson, Drew Springall, Richard DeMillo

SpeakerBio: David Jefferson

Dr. David Jefferson is a computer scientist and an internationally recognized researcher on election security for well over twenty years, advising five Secretaries of State of California on voting technology issues. He served as the Chair of the Secretary of State's Post-Election Audit Standards Working Group, the panel that invented the notion of risk limiting audits and has written extensively on elections and voting security.

Twitter: [@drjefferson](#)

SpeakerBio: Drew Springall

I am an Assistant Professor in the Department of Computer Science and Software Engineering (<https://www.eng.auburn.edu/comp/>) at Auburn University (<https://auburn.edu/>). As a security researcher, I focus on nation-state/highly privileged attackers, Internet-scale measurement/vulnerabilities, and election security. I recently left Google's Production Security team where I was working to mitigate insider threats, secure core infrastructure, and improve the overall security and privacy properties of Google's products and services. My Ph.D. research focused on studying nation-state attackers such as the NSA, GCHQ, and other intelligence agencies to understand their approach to security issues and identify weaknesses that are form-fitted to their special abilities and characteristics. Throughout my graduate education at the University of Michigan (<https://umich.edu/>), I was advised by Prof. J. Alex Halderman (<https://jhalderm.com/>) and funded by an NSF Graduate Research Fellowship, the Post-9/11 GI Bill, Google ATAP, and others. My work has helped explain intelligence agencies' ability to defeat widely used cryptography (<https://aaspring.com/ccs2015/imperfect-forward-secrecy-ccs15.pdf>), identify and analyze the danger posed by common cryptographic shortcuts (<https://aaspring.com/imc2016/crypto-shortcuts.pdf>) used in the TLS protocol, and demonstrated the real-world potential of election interference by foreign actors (<https://aaspring.com/ccs2014/ivoting-paper.pdf>) through technical means. This research has been covered and cited by The Wall Street Journal (<https://cacm.acm.org/news/187259-new-computer-bug-exposes-broad-security-flaws/fulltext>), The Washington Post (<https://www.washingtonpost.com/news/the-switch/wp/2014/05/13/how-russia-could-easily-hack-its-neighbors-elections/>), ARS Technica (<https://arstechnica.com/security/2015/05/https-crippling-attack-threatens-tens-of-thousands-of-web-and-mail-servers/>), the Guardian (<https://www.theguardian.com/technology/2014/may/12/estonian-e-voting-security-warning-european-elections-research>), US-CERT (<https://www.us-cert.gov/ncas/alerts/TA17-075A>), NIST (<https://nvd.nist.gov/vuln/detail/CVE-2015-4000>), FBI Cyber Division (<https://info.publicintelligence.net/FBI-PHI-FTP.pdf>), Playboy (SFW) (<https://web.archive.org/web/20180126034202/https://www.playboy.com/articles/technology-will-destroy-democracy>).

Twitter: [@_aaspring_](#)

SpeakerBio: Richard DeMillo

Richard DeMillo is a professor at Georgia Tech's School of Cybersecurity and Privacy. He holds the Charlotte B. and Roger C. Warren Chair in Computing at Georgia Tech. He is also Managing Director of Gtatrium™, LLC, a subsidiary of Georgia Advanced Technology Ventures. He was formerly the John P. Imlay Dean of Computing and Director of the Georgia Tech Information Security Center. Positions he held prior to joining Georgia Tech, include: Chief Technology Officer for Hewlett-Packard, Vice President of Computing Research for Bell Communications Research, Director of the Computer Research Division for the National Science Foundation, and Director of the Software Test and Evaluation Project for the Office of the Secretary of Defense. He has also held faculty positions at the University of Wisconsin, Purdue University and the University of Padua, Italy. His research includes over 100 articles, books and patents in software and computer engineering, cryptography, cybersecurity, and theoretical computer science. In 1982, he wrote the first policy for testing software intensive systems for the US Department of Defense. DeMillo and his collaborators launched and developed the field of program mutation for software testing, which is today the standard technique for determining software test adequacy. He is a co-inventor of Differential Fault Cryptanalysis and holds the patent on applying DFA to break public key cryptosystems.

His 1979 paper “Social Processes and Proofs of Theorems and Programs,” co-authored with Richard Lipton and Alan Perlis has been reprinted dozens of times and was recently cited as one of the 50 classic papers in the history of computer science. He currently works in the area of election and voting system security. His work has been cited in court cases, including a 2019 Federal Court decision declaring unconstitutional the use of paperless voting machines. He has served as a foreign election observer for the Carter Center and is a member of the State of Michigan Election Security Commission. He has served on boards of public and private cybersecurity and privacy companies, including RSA Security and SecureWorks. He has served on many non-profit and philanthropic boards including the Exploratorium and the Campus Community Partnership Foundation (formerly the Rosalind and Jimmy Carter Foundation). He is a fellow of both the Association for Computing Machinery and the American Association for the Advancement of Science. In 2010, he founded the Center for 21st Century Universities, Georgia Tech’s living laboratory for fundamental change in higher education. He served as Executive Director for ten years. He was named Lumina Foundation Fellow for his work in higher education. His book, *Abelard to Apple: The Fate of American Colleges and Universities*, (MIT Press, 2011) helped spark a national conversation about online education.

A 2015 sequel, *Revolution in Higher Education*, also published by MIT Press, won the Best Education Book award from the American Association of Publishers. From 2015-2018, he co-chaired Georgia Tech’s Commission on Creating the Next in Education. The Commission’s report was released in 2018 and was awarded the awarded 2019 Achievement Award of the Association for Educational Communications and Technology. He received the ANAK Society’s Outstanding Faculty Member Award in 2016 for his work in service to students.

Twitter: [@rad_atl](https://twitter.com/rad_atl)

Description:

Join us for a timely and important discussion of the vulnerability of Dominion Voting Systems ImageCast X (ICX) ballot-marking devices, used in many states including Georgia--where there was extended illicit access to voting systems and software in 2021. (An ICX is available at Voting Village this year for researchers to explore.) In an unrebutted expert report filed in a federal suit seeking to compel the State of Georgia to reduce reliance on the ICX, Professors J. Alex Halderman and Drew Springall documented security vulnerabilities in the ICX that would allow votes to be altered. CISA issued a vulnerability advisory confirming the principal claims in that report. Dominion Voting Systems contracted with MITRE Corporation, a Federally Funded Contract Research and Development Center (FFRDC), to critique the Halderman/Springall report. Georgia election officials have cited the MITRE report in their decision to use unpatched versions of Dominion’s software in every precinct during the 2024 Presidential Election, despite CISA's warnings.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Contactless Overflow: Code execution in payment terminals and ATM's over NFC

When: Saturday, Aug 12, 14:30 - 15:15 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

SpeakerBio: Josep Pi Rodriguez , Principal Security Consultant at IOActive

Josep Pi Rodriguez is experienced in network penetration and web application testing, reverse engineering, industrial control systems, transportation, RF, embedded systems, AMI, vulnerability research, exploit development, and malware analysis. As a principal consultant at IOActive, Mr. Pi Rodriguez performs penetration testing, identifies system vulnerabilities, and researches cutting-edge technologies. Mr. Pi Rodriguez has performed security services and penetration tests for numerous global organizations and a wide range of financial, technical, and educational institutions. He has presented at international conferences including Defcon, Immunity infiltrate, Hack in Paris, Japan CCDS and Confidence Conference.

Twitter: [@Josep_pi](#)

Description:

We conducted a research to assess the current security of NFC payment readers that are present in most of the major ATM brands, portable point of sales, gas stations, vending machines, transportation and other kind of point of sales in the US, Europe and worldwide. In particular, we found code execution vulnerabilities exploitable through NFC when handling a special application protocol data unit (APDU) that affect most NFC payment vendors. The vulnerabilities affect baremetal firmware devices and Android/Linux devices as well.

After waiting more than 1 year and a half once we disclosed it to all the affected vendors, we are ready to disclose all the technical details to the public. This research was covered in the media by wired.com but without the technical details that we can share now <https://www.wired.com/story/atm-hack-nfc-bugs-point-of-sale/>

Some of the affected vendors are:

IDtech - <https://idtechproducts.com/>

Ingenico - <https://www.ingenico.com/>

Verifone - <https://www.verifone.com/>

CPI - <https://www.cranepi.com/>

BBPOS - <https://www.bbpos.com/>

Wiseasy - <https://www.wiseasy.com/>

Nexgo - <https://www.nexgoglobal.com/>

In this presentation we will describe the vulnerabilities and also demo how the readers can be compromised, using a special Android app we created, by just tapping an Android phone to the reader. We will discuss the consequences such as financial impact in reader's users/owners and card data stealing once the firmware is compromised. Also, we will show how to compromise the host that is connected to the reader through USB by manipulating the reader's firmware, chaining stack buffer overflow vulnerabilities in the SDK provided by the vendor that is running in the host machine.

Finally, since one of the affected vendors (IDtech) is present in most ATM brands in the world, the talk will cover different scenarios of how possible can be jackpotting ATMs just tapping a smartphone into the reader of the ATM. We have many years of experience jackpotting all brands of ATMs in multiple different ways and we will show how this is technically possible.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Contain Yourself: Staying Undetected Using the Windows Container Isolation Framework

When: Friday, Aug 11, 10:00 - 10:45 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

SpeakerBio: Daniel Avinoam , Security Researcher at Deep Instinct

As a security researcher at Deep Instinct, Daniel develops and researches new defense capabilities. After serving for several years in the advanced technological cyber unit under the Israeli Air Force, Daniel has experience in the defensive side of cyber warfare, including forensics, incident response, development, reverse engineering, and research.

Description:

The use of containers became an integral part of any resource-efficient and secure environment. Starting from Windows Server 2016, Microsoft released its version of this solution called Windows Containers, which offers either a process or Hyper-V isolation modes.

In both cases, an efficient file system separation should be provided. On one hand, each container should be able to access system files and write changes that will not affect the host. On the other, copying the entire main volume on each container launch will be storage-inefficient and not practical.

In this presentation, we will cover the basics of windows containers, break down its file system isolation framework, reverse-engineer its main mini-filter driver, and see how it can be utilized and manipulated by an actor to bypass EDR products in multiple domains. Eventually, we will provide an open-source tool based on these findings.

This technology caught my attention for several reasons:

- Containers and virtualization solutions are everywhere, and their internal workings are not well documented.
- Actors often search for ways to escape containers. The idea of intentionally entering into one in order to evade security products has yet to be explored.
- This framework doesn't require any prerequisites and comes as default in every modern Windows image! (the part which we will abuse, at least).

REFERENCES

- <https://googleprojectzero.blogspot.com/2021/04/who-contains-containers.html>
- <https://unit42.paloaltonetworks.com/what-i-learned-from-reverse-engineering-windows-containers/>
- <https://research.checkpoint.com/2021/playing-in-the-windows-sandbox/>
- <https://www.amazon.com/Windows-Kernel-Programming-Pavel-Yosifovich/dp/1977593372>
- <https://learn.microsoft.com/en-us/virtualization/windowscontainers/about/>
- <https://habr.com/en/company/acronis/blog/536018/>

[Return to Index](#) - Add to  - ics [Calendar](#) file


DC - Friday - 10:00-17:59 PDT

Title: Contest Area Open

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Saturday - 10:00-17:59 PDT

Title: Contest Area Open

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Sunday - 10:00-13:59 PDT

Title: Contest Area Open

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Sunday - 14:00-15:15 PDT

Title: Contest Closing Ceremonies & Awards

When: Sunday, Aug 13, 14:00 - 15:15 PDT

Where: Caesars Forum - Forum - 105, 135-136, 108-119, 138-139 - Tracks 1 & 2 - [Map](#)

Description:

Contests announce winners, discuss game play and the outcome of some of the [sixty-five different contests held at DEF CON 31](<https://forum.defcon.org/node/244766>).

Black Badge (UBER) Winners will be announced at the DEF CON Closing ceremonies & awards, immediately following this session.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Saturday - 16:00-17:59 PDT

Title: CPV Ten Year Anniversary Gathering

When: Saturday, Aug 12, 16:00 - 17:59 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio:CPV Staff

No BIO available

Description:

Come on over to join a full takeover of the CPV space, take cute selfies everywhere, and see all our old and new faces for a two hour celebration at CPV!!! We'll see what we can pull off.

We have speakers and microphones so we'll make usage of them, maybe we'll sort people by what year they joined us because it's fun, who knows? We just want to see everyone's lovely faces, we wish we could see you all more often! A group photo with people who want to be part of one perhaps?

Logistics: Sadly, we can't offer food or drink for many reasons including hotel. Eat beforehand or afterwards! We'll try to not demolish the CPV Stage chairs (too much) so talks can continue after.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Friday - 10:00-10:05 PDT

Title: CPV Welcome - Day 1


When: Friday, Aug 11, 10:00 - 10:05 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio:CPV Staff

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Saturday - 10:00-10:05 PDT

Title: CPV Welcome - Day 2

When: Saturday, Aug 12, 10:00 - 10:05 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio:CPV Staff

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Sunday - 10:00-10:05 PDT

Title: CPV Welcome - Day 3


When: Sunday, Aug 13, 10:00 - 10:05 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio:CPV Staff

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Cracking Cicada 3301: The Future of Collaborative Puzzle-Solving

When: Thursday, Aug 10, 11:30 - 12:15 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers: Artorias, Puck, Taiwo, TheClockworkBird

SpeakerBio: Artorias

Artorias is the creator of CicadaSolvers.com, co-host of the CicadaCast podcast, and moderator of r/cicada and the CicadaSolvers discord. Well-versed in the complex history of the Cicada 3301 puzzles, he labors both to document the mystery of Cicada 3301, and to unravel the labyrinth of its interconnected topics.

SpeakerBio: Puck

Puck is a 19-year-old rising junior computer science major and Cicada 3301 puzzle enthusiast. He has been involved in the community for four years, finding inspiration to pursue cryptography and cybersecurity. Puck has focused his work on promoting community solving efforts, mainly in the form of innovative events.

SpeakerBio: Taiwo

Taiwo, a CicadaSolvers founding member, with a background in software development, sees the community's work as an example for the future of problem-solving. With a pragmatic, and sceptical approach to the puzzle, he aims to preserve the community so that it can continue to impact the lives of others as immensely as it did for him.

SpeakerBio: TheClockworkBird

TheClockworkBird With a background in anthropology and teaching, TheClockworkBird creates collaborative spaces where people of all skill levels and interests can engage with the puzzle. He has gained a multifaceted understanding of Cicada's impact on the individual, and the impacts of collaborative puzzle solving on the growth of privacy awareness.

Description:

This talk will explore the ongoing efforts of the CicadaSolvers community to solve Cicada3301's Liber Primus, a book of elder futhark runes and codes that has challenged cryptographers and puzzle-solvers since 2014. Using our experiences as leaders within the community, we will delve into the cultural significance of the puzzle and discuss the various strategies and techniques employed by members to crack its code, and the story of their struggle to maintain motivation through 9 years of solving one of the most difficult puzzles ever released. Attendees will gain insights into the future of collaborative puzzle-solving and the challenges that the Liber Primus presents for the future of cryptography. This presentation is suitable for anyone interested in cryptography, puzzle-solving, internet mysteries, and the persistence of collaborative communities. No prior technical knowledge or tools are required.

REFERENCES

- CicadaSolvers Discord server: <https://discord.gg/cicadasolvers-572330844056715284> - CicadaSolvers Wiki:

https://uncovering-cicada.fandom.com/wiki/Uncovering_Cicada_Wiki - Previous DEF CON talk from CicadaSolvers member Nox Populi: https://www.youtube.com/watch?v=sVU4k2gRe_Y - Article written as a result of our TOR search in 2016:

<https://arstechnica.com/information-technology/2016/07/malicious-computers-caught-snooping-on-tor-anonymized-dark-w>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: CrackMeIfYouCan

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The premiere password cracking contest "CrackMeIfYouCan" is back again. Passwords so two-thousand and late. Remember, remember, the cracks of November.

We're preparing hashes from easy to hard, so there'll be something for you if you want to compete casually as a Street team, or go all out in Pro.

Where we're going, we don't need roads. Purely a penchant for puzzles, perhaps a plethora of processors.

Check out past years' contests at <https://contest.korelogic.com/> , and the Password Village at <https://passwordvillage.org/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT

Title: CrackMeIfYouCan

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The premiere password cracking contest "CrackMeIfYouCan" is back again. Passwords so two-thousand and late. Remember, remember, the cracks of November.

We're preparing hashes from easy to hard, so there'll be something for you if you want to compete casually as a Street team, or go all out in Pro.

Where we're going, we don't need roads. Purely a penchant for puzzles, perhaps a plethora of processors.

Check out past years' contests at <https://contest.korelogic.com/> , and the Password Village at <https://passwordvillage.org/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

Title: CrackMeIfYouCan

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The premiere password cracking contest "CrackMeIfYouCan" is back again. Passwords so two-thousand and late. Remember, remember, the cracks of November.

We're preparing hashes from easy to hard, so there'll be something for you if you want to compete casually as a Street team, or go all out in Pro.

Where we're going, we don't need roads. Purely a penchant for puzzles, perhaps a plethora of processors.

Check out past years' contests at <https://contest.korelogic.com/> , and the Password Village at <https://passwordvillage.org/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Creating and uncovering malicious containers Redux (Pre-Registration Required)

When: Saturday, Aug 12, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers: Adrian "threlfall" Wood, David "digish0" Mitchell

SpeakerBio: Adrian "threlfall" Wood , Dropbox

Adrian Wood, aka threlfall, discovered a love for hacking from cracking and modding video games and from the encouragement of online friends. He has worked as a red team consultant for WHITEHACK, a company he founded, and later as a lead engineer for an offensive research team at a US bank, where he was very interested in appsec, container security, CI/CD security and also founded their bug bounty program. He currently works for Dropbox, working on their red team. In his free time, he enjoys playing saxophone, working on vintage cars, and fly-fishing.

SpeakerBio: David "digish0" Mitchell

David Mitchell, aka digish0, started his hacking career as a script kiddie running 7th Sphere in mIRC in high school. Later falling in with some Linux/RedHat nerds at a local 2600 group at college while studying CS, etc. He got into Linux, started an IT career, later rediscovering his hacking script kiddie roots when a local hacker space opened up and shared members with a lockpicking group that worked in infosec as penetration testers, etc where he discovered he could get paid to do the things he liked doing in high school/college. He now works professionally as a red team member and cyber security researcher at a large financial institution. The rest of the time he spends being a dad/husband, trying not to get injured in Muay Thai/BJJ or mountain biking, and listening to either very expensive or very cheap vinyl.

Description:

Containers allow bad actors access to an excellent delivery mechanism for malware deployment in organizations, offering a wide variety of detection avoidance and persistence mechanisms. Fear not protectors, containers also offer ways to detect these, but can be fraught with challenges. Whether you're red, blue or just container curious this workshop is for you.

In this workshop, you will get hands-on with containers and kubernetes, - starting with introductory content - learning how they work, where and how to hide or find things, how to identify indicators of compromise, indicators of attack, and how to apply analysis to gain a deeper understanding of container malware and what is going on inside containers.

This workshop will utilize the Google Cloud Platform alongside command line operands and a small amount of open source tooling to learn both offensive and defense techniques on containers. By the end, you'll have a solid mental model of how containers work, how they are managed and deployed, and be equipped with the ability to analyze container images, identify problems, attack container supply chains and identify familiar patterns. Ultimately, these skills will allow you to generate valuable insights for your organization's defense or aid you in your next attack.

This course is designed to take you deep into the world of containers, making tooling like Kubernetes much more intuitive and easy to understand. There's lots of labs which will be used to reinforce your learnings, in both attack and defense and the course comes with very detailed notes and instructions for setup which you can repeat on your own time. This course will provide references to scripts that make certain tasks easier, but we will be challenging you to learn the process and reasoning behind them rather than relying on automation.


Attendees will be provided with all the lab material used in the course in digital format, including labs, guides and virtual machine setup.

Skill Level: Beginner to Intermediate

Prerequisites for students:

- None! the class is well designed to allow those with little to no linux, kubernetes or cloud familiarity to follow along, but a basic familiarity with Linux and terminal will allow attendees to focus on the work.

Materials or Equipment students will need to bring to participate: - A Google Cloud free tier account (basically a fresh gmail account) - an internet connected computer
- We will send out instructions to attendees prior to the class, so they can be ready on the day.

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Saturday - 11:30-12:25 PDT

Title: Creative Misuse of AI Systems

When: Saturday, Aug 12, 11:30 - 12:25 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

SpeakerBio:Eryk Salvaggio

No BIO available

Description:

In this panel, three artists from the Algorithmic Resistance Research Group (ARRG!) present creative work and workflows that emerged from attempts to crack AI black boxes open. Aligned with the hacker ethos of exploration, experimentation and creative misuse, this panel presents adversarial, ethical artmaking practices for artificial intelligence systems, including image synthesis and recognition. The panel includes three artists displayed in the AI Village Art Exhibition space: Steph Maj Swanson, creator of Loab, the viral "latent space cryptid," Eryk Salvaggio, an artist who revels in confusing AI systems into making images from error states; and Caroline Sindere, an artist and researcher who recontextualizes these systems into revealing underlying biases and potential harms.

This non-technical, but conceptual conversation offers up art alongside possible strategies. It will be of interest for hackers intrigued by the creative potential of these tools, but who may have ethical concerns or doubts about the way these tools are assembled, built, and deployed. The artists will share their work and offer insights into strategies and implications of creative misuse.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Sunday - 10:00-13:59 PDT

Title: Critical Infrastructure & IoT Exploitation

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Join for hands-on content and labs exploiting critical IoT and network infrastructure. Participate in initial public disclosure of new vulnerabilities with our team of experts, explore the 0-day development process, and power up your reverse engineering skills by "living off the land" like a pro using simple, free tools! Want to hack an Emergency Alert System unit, extract network traffic from recycled phone systems & routers, or exploit security controls in firewalls & proxies?

Bring a laptop, your favorite intercepting proxy, and a *lot* of caffeine.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Saturday - 10:00-17:59 PDT

Title: Critical Infrastructure & IoT Exploitation

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Join for hands-on content and labs exploiting critical IoT and network infrastructure. Participate in initial public disclosure of new vulnerabilities with our team of experts, explore the 0-day development process, and power up your reverse engineering skills by "living off the land" like a pro using simple, free tools! Want to hack an Emergency Alert System unit, extract network traffic from recycled phone systems & routers, or exploit security controls in firewalls & proxies?

Bring a laptop, your favorite intercepting proxy, and a *lot* of caffeine.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Friday - 10:00-17:59 PDT

Title: Critical Infrastructure & IoT Exploitation

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Join for hands-on content and labs exploiting critical IoT and network infrastructure. Participate in initial public disclosure of new vulnerabilities with our team of experts, explore the 0-day development process, and power up your reverse engineering skills by "living off the land" like a pro using simple, free tools! Want to hack an Emergency Alert System unit, extract network traffic from recycled phone systems & routers, or exploit security controls in firewalls & proxies?

Bring a laptop, your favorite intercepting proxy, and a *lot* of caffeine.

[Return to Index](#) - Add to  - ics [Calendar](#) file

RCV - Friday - 15:45-16:30 PDT

Title: Crushing crumbs of information to eat a whole cake.

When: Friday, Aug 11, 15:45 - 16:30 PDT

Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio: Felipe Pr0teus

No BIO available

Twitter: [@pr0teusbr](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Saturday - 15:00-15:45 PDT

Title: Cryptosploit Workshop


When: Saturday, Aug 12, 15:00 - 15:45 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio: Matt Cheung

Matt Cheung started developing his interest in cryptography during an internship in 2011. He worked on implementation of a secure multi-party protocol by adding elliptic curve support to an existing secure text pattern matching protocol. Implementation weaknesses were not a priority and this concerned Matt. This concern prompted him to learn about cryptographic attacks from Dan Boneh's crypto 1 course offered on Coursera and the Matasano/cryptopals challenges. From this experience he has given workshops at the Boston Application Security Conference, BSidesLV, DEF CON, and the Crypto and Privacy Village.

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: CTH 101: Part I & II

When: Friday, Aug 11, 10:30 - 11:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Project Obsidian: 101 Track (0x41) - [Map](#)

SpeakerBio: CerealKiller


CerealKiller or Cereal is a Cyber Defense Practitioner with over 10yrs of experience.

Description:

This 101 session includes two cyber threat hunting training modules.

Part I: Introduction to Cyber Threat Hunting: A brief introduction to Cyber Threat Hunting
Part II: Threat Hunting Methodologies: A look into hunting methodologies

Introduction to Cyber Threat Hunting & Threat Hunting Methodologies

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTV - Saturday - 13:30-13:59 PDT

Title: CTH 101: Part III, IV, V

When: Saturday, Aug 12, 13:30 - 13:59 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Project Obsidian: 101 Track (0x41) - [Map](#)

SpeakerBio: Cyb3rhawk

DE&TH

Description:

This CTH 101 session includes three modules.

Part III: Threat Hunting Techniques: A look into various hunting techniques. Part IV: Case Studies and Labs: What we can learn from case studies and how to get started with labs. Part V: Conclusion and Next Steps: Where to go next to learn more.

CTH 101: Threat Hunting Techniques, Case Studies and Labs, Conclusion and Next Steps

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTV - Friday - 11:30-12:30 PDT

Title: CTH: (n)Map Exploration: A Great Time in Remote Destinations

When: Friday, Aug 11, 11:30 - 12:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Project Obsidian: Kill Chain Track (0x42) - [Map](#)

SpeakerBio: SamunoskeX

SamunoskeX is an Information Security Professional who works as part of a Security Operations Team and is also an Information Security instructor at a college. He is a Blue Team enthusiast and enjoys sharing all things Blue Team with the world.

SamunoskeX has attended DEFCON Events since DC26.

Description:

Can we find activity within the corporate network that might be suspicious?

Can we find activity within the corporate network that might be suspicious?

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: CTH: Log4j - The Silent Menace Among Us

When: Saturday, Aug 12, 10:30 - 11:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Project Obsidian: Kill Chain Track (0x42) - [Map](#)

SpeakerBio: Cyb3rhawk

DE&TH

Description:

The recent Log4j vulnerability has been making headlines and causing significant harm to organizations that rely on Apache Log4j for logging. In this talk, we'll go beyond the headlines and provide a deep dive into threat hunting techniques and their application in detecting vulnerabilities like Log4j. We'll start with the basics of threat hunting and how it can help you stay ahead of emerging threats. From there, we'll explore the technical details of the Log4j vulnerability, including its nature, impact, and how it can be exploited. You'll learn how to analyze and respond to security threats through real-world examples of threat hunting in action. We'll provide hands-on labs that give you the experience you need to implement these techniques in your own organization. Whether you're a security analyst, engineer, or manager, this talk will provide valuable insights into threat hunting and enable you to stay ahead of emerging threats. Join us on this technical journey into the unknown with "Log4j: The Silent Menace Among Us."

The recent Log4j vulnerability has been making headlines and causing significant harm to organizations that rely on Apache Log4j for logging. In this talk, we'll go beyond the headlines and provide a deep dive into threat hunting techniques and their application in detecting vulnerabilities like Log4j.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 20:00-23:59 PDT

Title: Cult Of The Dead Cow Breaks The Internet (and you can too!)

When: Friday, Aug 11, 20:00 - 23:59 PDT

Where: Caesars Forum - Forum - 105,136 - [Map](#)

Description:

CULT OF THE DEAD COW BREAKS THE INTERNET (and you can too!)

What is dead shall rise again! Come do a hacktivism with cDc, as we launch a THING that will once again change the world, with the style and chaos that only the herd can bring. Let us bless you with a revolutionary communications system that will disrupt the balance of power.

It's time to TAKE BACK CONTROL.

Recommended (but not required) dress code- y2k 31337 Haxxor threads. Think Zero Cool and Acid Burn meet Max Headroom and Franken Gibe. There is no contest, but the Bovine Mother is watching, so make her proud.

The herd hath spoken. Oomen.

- 20:00 - 20:45 -- Miss Jackalope
- 20:45 - 21:30 -- DotorNot
- 21:30 - 22:15 -- cDc/Veilid
- 22:15 - 22:45 -- Rocky Rivera + DJ Roza
- 22:45 - 23:30 -- EVA
- 23:30 - 00:00 -- DJ McGrew

[Return to Index](#) - Add to  - ics [Calendar](#) file

MIV - Friday - 11:00-11:30 PDT

Title: Cutting through the noise: What you need to know are the real threats when it comes to AI

When: Friday, Aug 11, 11:00 - 11:30 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Chloé Messdaghi

No BIO available

Description:

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: CVE Insanity

When: Friday, Aug 11, 17:20 - 17:59 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

SpeakerBio:Om Mahida , MedCrypt

Om leads Product at MedCrypt, helping build innovative cybersecurity products for healthcare. His interests in privacy and technology led him to join a cybersecurity startup after studying Computer Engineering at Drexel. In his free time, Om likes to ski and make pizzas.

Description:

CVSS is a headache for everyone, but we all use it. Has anyone actually checked to see if it works the way it should? Or where and why it fails? Trying to manually analyze every single CVE is painstaking. And what if CVSS isn't actually working? Is there something better out there? What if we used science, like you know, an adult, and measured something? Grab your protractors and slide rules and sextants as we explore the exceedingly exciting world of vulnerability management, risk management's slightly more edgy cousin. This talk will explore what rescoring vulnerabilities with CVSS does and doesn't do, and what we should do next to fill the gaps. PREVIOUSLY: ChatGPT took the world by storm. But what if we tried to use it to write a clinical application? And do it securely? Will the code compile? Will the data actually be secure? This talk will go over a PoC where we put it to the test.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Cyber Hygiene: Security Awareness Training and Education

When: Friday, Aug 11, 11:00 - 11:50 PDT

Where: Caesars Forum - Alliance - 301-304 - Blacks in Cyber Village - [Map](#)

SpeakerBio:Dontae Tyler

A community college drop-out born in Southeast Washington DC but by way of Prince Georges County, Dontae Tyler believes that success in the tech industry does not have to be traditional. With over 9 years of experience in IT, supporting various federal agencies Dontae has begun to distinguish himself as a premier advocate for GRC, Data Privacy and Security Awareness Training. He currently holds several certifications including CISM, CDSPE, CEH, SEC+. Dontae's unconventional cyber awareness training and education teaching methods seek to educate the everyday user and challenge the most experienced tech professionals on the evolving cyber threats.

Description:

Dontae Tyler developed a security awareness training called Cyber Hygiene after getting tired of sitting through boring cyber security awareness videos that were not effective. After conducting his own research, He was able to come to the conclusion that the annual security training of the past was not as effective in remediating issues related to non-technical people utilizing interconnected devices and systems to complete their work. In his training he plans to equip end users with simple yet effective mitigation strategies and tools to reduce risk to acceptable levels.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Cyber Policy Adrift – Charting a Path Forward for International Maritime Cybersecurity

When: Friday, Aug 11, 14:00 - 14:50 PDT

Where: Caesars Forum - Summit - 221-222 - Policy Atrium - [Map](#)

Speakers:Blake Benson,Cliff Neve,Josh Reiter,Nina Kollars

SpeakerBio:Blake Benson

Blake A. Benson has helped a wide variety of critical infrastructure stakeholders develop solutions to improve the effectiveness of their decision-making process for cyber risk. He specializes in navigating the challenges associated with developing tailored, industry-specific solutions in non-traditional cyber environments. He has taken a particular interest in the assets and infrastructure that supports America's critical functions, providing strategic and technical cyber risk expertise across multiple business divisions and industries. Blake's desire to safeguard America's most critical assets is driven by his first-hand experience with cyber operations, where he was a founding member of one of the Air Force's first operational cyber squadrons and later became a sought-after cyber intelligence expert.

SpeakerBio:Cliff Neve , US Coast Guard

CDR Cliff Neve is a retired Coast Guard Commander whose assignments included Chief of Staff at Coast Guard Cyber Command, Deputy Chief Information Officer at the White House Communications Agency, and Assistant C4ISR Program Manager for the Coast Guard's multi billion dollar recapitalization program. Since retiring from the Coast Guard in 2013, CDR Neve has led all manner of cyber security assessments and security architecture consulting for diverse clients that include Ports and Waterways, Wall Street firms, Fortune 100 companies, banks, hospitals, and defense agencies. CDR Neve is a Certified Information Systems Security Professional (CISSP) and Project Management Professional (PMP).

SpeakerBio:Josh Reiter , Deputy PCA at US Navy

Mr. Joshua Reiter is the Department of the Navy Deputy Principal Cyber Advisor (PCA). In this role, he is responsible for supporting the PCA in advising the Secretary of the Navy, Chief of Naval Operations, and Commandant of the Marine Corps, and implementing the Department of Defense Cyber Strategy within the Department of the Navy. Mr. Reiter also serves in the additional capacity as the Department of the Navy Chief Information Officer's (DON CIO) Chief Workforce Officer. He was originally appointed to Defense Intelligence Senior Level (DISL) in December 2018 as the Director of Cyber Workforce Policy and Planning under the Cybersecurity Directorate of OPNAV N2N6. A former U.S. Coast Guard licensed merchant mariner, for the first several years of his career, Mr. Reiter served as a DoD civilian mariner with the U.S. Navy's Military Sealift Command as Third Officer aboard USNS Saturn (T-AFS-10), USNS John McDonnell (T-AGS 51), USNS Apache (T-ATF 172), USNS Hayes (T-AG-195) and as Second Officer/Navigator aboard USNS Sirius (T-AFS-8).

SpeakerBio:Nina Kollars , Associate Professor at Cyber and Innovation Policy Institute at the US Naval War College

Nina (Kitty Hegemon) Kollars is an associate professor in the Cyber and Innovation Policy Institute at the US Naval War College. Dr. Kollars is a former Special Advisor to OUSD R&E, Logistics, Emerging tech, Cyber Conflict & Military Innovation for the Department of Defense. She publishes on cybersecurity, hackers and military innovation. She presented her own hacker project at DefCon27, "Confessions of a Nespresso Money Mule." She will soon publish her book "Trustworthy Deviants: White Hat Hackers and Security." Kollars is also an Executive Bourbon Steward.

Description:

The global economy is afloat. It is cheap and fast, and vulnerable. Everyone relies upon it but there is no single entity responsible for it. Whether it be reliance on dated legacy systems, rampant prioritization of innovation over security, under-funded infrastructure, or unclear security principles and enforcement mechanisms, the maritime ecosystem is becoming increasingly insecure - making the world's seas and ports a target for pirates, hackers, and states. And we know it....that's the good news.

The panel will discuss challenges to developing actionable maritime cyber policy, the technical realities behind maritime cybersecurity, review existing US and international programs, and discuss how the global ecosystem could harmonize these policies to push the maritime ecosystem towards a more secure state. There will also be time for questions and broader

discussion/audience engagement.



[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Saturday - 11:30-11:59 PDT

Title: Cyber-Physical Detection and Response: A new Paradigm in IACS Monitoring and Security

When: Saturday, Aug 12, 11:30 - 11:59 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio:Ryan Heartfield

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Friday - 06:00-06:59 PDT


Title: CycleOverride Defcon Bike Ride

When: Friday, Aug 11, 06:00 - 06:59 PDT

Where: Other/See Description

Description:

At 6am on Friday, the @cycle_override crew will be hosting the 11th Defcon Bikeride. We'll meet at a local bikeshop, get some rental bicycles, and about 7am will make the ride out to Red Rocks. It's about a 15 mile ride, all downhill on the return journey. So, if you are crazy enough to join us, get some water, and head over to cycleoverride.org for more info. See you at 6am Friday! @jp_bourget @gdead @heidishmoo. Go to cycleoverride.org for more info.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: D0 N0 H4RM: A Healthcare Security Conversation

When: Saturday, Aug 12, 10:00 - 11:45 PDT

Where: Harrah's - Nevada Ballroom - Lake Tahoe & Reno - War Stories - Off the Record - [Map](#)

Speakers: Christian "quaddi" Dameff, Jacqueline Burgette, Jeff "r3plicanT" Tully, Mark Warner, Nitin Natarajan, Suzanne Schwartz

SpeakerBio: Christian "quaddi" Dameff , Physician & Medical Director of Cyber Security at The University of California San Diego MD

Christian (quaddi) Dameff MD is an Assistant Professor of Emergency Medicine, Biomedical Informatics, and Computer Science (Affiliate) at the University of California San Diego. He is also a hacker, former open capture the flag champion, and prior DEF CON/RSA/Blackhat/HIMSS speaker. Published works include topics such as therapeutic hypothermia after cardiac arrest, novel drug targets for myocardial infarction patients, and other Emergency Medicine related works. Published security research topics including hacking critical healthcare infrastructure, medical devices and the effects of malware on patient care. This is his nineteenth DEF CON.

SpeakerBio: Jacqueline Burgette , White House Fellow at The Office of National Cyber Director (ONCD) PhD DMD
Jacqueline Burgette DMD PhD is a White House Fellow at the Office of the National Cyber Director. Jacqueline is a clinician, educator, health policy expert and researcher working at the forefront health and cybersecurity. Jacqueline earned her DMD from the Harvard School of Dental Medicine as a Presidential Scholar and Ph.D. in Health Policy and Management from the University of North Carolina. She served on the faculty at the University of Pittsburgh where she led multi site studies that amplified the voices of vulnerable families to improve child health in Appalachia. As an expert in health services and highly-published author, she brings her systems perspective and data-driven approach to achieve cross-agency priorities in health and cybersecurity for the Federal government.

SpeakerBio: Jeff "r3plicanT" Tully , Anesthesiologist at The University of California San Diego MD

Jeff (r3plicanT) Tully is a security researcher with an interest in understanding the ever growing intersections between healthcare and technology. His day job focuses primarily on the delivery of oxygen to tissues.

SpeakerBio: Mark Warner , Virginia Senator and Chair of the US Cybersecurity Caucus

Sen. Warner was elected to the U.S. Senate in November 2008 and reelected to a third term in November 2020. He serves as Chairman of the Select Committee on Intelligence and as a member of the Senate Finance, Banking, Budget, and Rules Committees. He also co-chairs the Senate Cybersecurity Caucus. From 2002 to 2006, he served as Governor of Virginia. He has served as a key author and negotiator of several pieces of critical legislation aimed at rebuilding our nation's infrastructure, improving cybersecurity, restoring domestic manufacturing, protecting national security, rebounding from the COVID-19 crisis, and investing in under served and underbanked communities.

SpeakerBio: Nitin Natarajan , Deputy Director at Cybersecurity and Infrastructure Security Agency (CISA)

Nitin Natarajan serves as the Deputy Director for the Cybersecurity and Infrastructure Security Agency (CISA). Prior to joining CISA, Natarajan served in a variety of public and private sector positions spanning over 30 years. Natarajan also held a number of federal government roles to include Deputy Assistant Administrator at the U.S. Environmental Protection Agency, the Director of Critical Infrastructure Policy at the White House/National Security Council, and as a Director at the U.S. Health and Human Services overseeing healthcare and public health programs. At the beginning of his career, Natarajan spent 13 years as a first responder in New York, which included service as a flight paramedic. He was the Commander of a federal medical response team, based in New York, and has extensive experience deploying to natural and man-made disasters throughout the nation. He holds an under graduate degree from the State University of New York and a graduate degree from the United States Naval Postgraduate School.

SpeakerBio: Suzanne Schwartz , Director of the Office of Strategic Partnerships and Technology Innovation (OST) at FDA's Center for Devices and Radiological Health (CDRH) MD

Suzanne B. Schwartz, MD, MBA is the Director of the Office of Strategic Partnerships and Technology Innovation (OST) at

FDA's Center for Devices and Radiological Health (CDRH).

Suzanne's work in medical device cybersecurity includes policy development, educating, outreach, partnering and coalition-building within the Healthcare and Public Health Sector (HPH) as well as fostering collaborations and coordinating incident response across other government agencies and the private sector. Suzanne has been recognized for Excellence in Innovation at FDA's Women's History Month for her work in Medical Device Cybersecurity. She also received the 2021 Routhy Award from the H-ISAC for her leadership in cybersecurity in healthcare, especially during the COVID-19 pandemic. Together with Health Canada, Suzanne has represented FDA in co-chairing the International Medical Device Regulators Forum (IMDRF) Work Group on Medical Device Cybersecurity leading to its first international guidance publication in March 2020 and two subsequent guidance publications - - one on software bill of materials and one on cybersecurity management of legacy medical devices. She has additionally served as co-chair of the Government Coordinating Council (GCC) for the HPH Critical Infrastructure Sector, focusing on the sector's healthcare cybersecurity initiatives.

Suzanne earned an MD from Albert Einstein College of Medicine; an executive MBA from NYU Stern School of Business, completed Cohort X of the National Preparedness Leadership Initiative – Harvard School of Public Health & Harvard Kennedy School of Government executive education, and earned in September 2018 a certificate of mastery for completion of requirements at the Federal Executive Institute – Leadership for a Democratic Society.

Description:

In 2016 a bunch of hackers took a break from DEF CON festivities to gather in a hotel room with a bathtub full of beer and talk about shared interests in a brave new world of connected healthcare. Trailblazers were popping pacemakers and pharmaceutical pumps, and we worried that instead of embracing such efforts as opportunities to make tech safer for patients, folks in charge would repeat mistakes of the past and double down on the status quo.

Fast forward to the 2022 passage of the Omnibus spending bill- the FDA is now locked and loaded with expanded authority to regulate cybersecurity requirements for medical devices. What changed? *Keanu voice*: "Policy. Lots of Policy." Turns out when we get in with the right people, hackers can help get things done. This is the core of Policy @ DEFCON.

Challenges persist. We now have threats from state actors and ransomware blasts delaying lifesaving medical care while costing hospitals hundreds of millions of dollars they don't have (been in an ER lately?). So once again, come join quaddi and r3plicant, your favorite ripper docs, for another round of D0 No H4rm- this time with special guests from Congress, FDA, and the White House as we figure out what policy patches have the best chance to save lives.

It starts here, in rooms like this, with hackers like you. And it ends with us changing the world.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Damned if you do - The risks of pointing out the emperor is buck naked

When: Thursday, Aug 10, 13:30 - 14:15 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers:RenderMan,Thomas Dang

SpeakerBio:RenderMan , His Holiness, Pope of the Church of Wifi

The man in the black hat with a monkey on his belt and a suitcase of sex toys. Pope of the Church of Wifi. Don of Dongs at the Internet of Dongs project. Hacking random things for 25+ years. Usually referred to as “oh, that guy” around Defcon.

SpeakerBio:Thomas Dang , Cybersecurity Architect at Yukon Territorial Government

Thomas Dang was (until May 2023) a politician in the Alberta Legislature. The youngest MLA ever elected, he was pursuing a Computing Science degree before his first term. As an MLA, he served various roles including Deputy House Leader and on various legislative committees. While elected, he continued following his passion in Cybersecurity including certifications along with his university education. In an attempt to recover from politics, he’s spending his time hanging out at DEF CON and has a day job as the Cybersecurity Architect for the Yukon Territorial Government.

Twitter: [@@thomasdangab](#)

Description:

Post 9/11, the phrase “If you see something, say something” became ubiquitous. If you saw something of concern, better to report something that was nothing than let something bad happen. Problem is, no one let the authorities know that they should apply this to the online realm too. Threats of arrest and criminal investigations have the opposite effect and chill anyone from wanting to report security vulnerabilities that affect everyone.

Lack of clear reporting paths, misunderstandings, jurisdiction issues, superseding laws, and good old fashioned egos can make trying to do the right thing turn into a nightmare that can cost livelihoods, reputation, criminal charges and even worse, particularly when government systems are involved.

This talk will cover the presenters personal experiences with poorly written or a lack of vulnerability disclosure policies with their governments and what it cost them in trying to make things better. The presentation will then move to a discussion about what should be done and what is being done to make sure that reporting a vulnerability doesn’t cost you everything. Anyone who is responsible for writing such disclosure policies or legislation will benefit, but so will any hackers that want to make it safer to report issues they find by advocating for changes.

REFERENCES

- No references cited formally. Law excerpts will be noted in slides where relevant.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT

Title: Darknet-NG

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Darknet-NG is an In-Person Massively Multiplayer Online Role Playing Game (MMO-RPG), where the players take on the Persona of an Agent who is sent on Quests to learn real skills and gain in-game points. If this is your first time at DEF CON, this is a great place to start, because we assume no prior knowledge. Building from basic concepts, we teach agents about a range of topics from Lock-picking, to using and decoding ciphers, to Electronics 101, just to name a few, all while also helping to connect them to the larger DEF CON Community. The "Learning Quests" help the agent gather knowledge from all across the other villages at the conference, while the "Challenge Quests" help hone their skills! Sunday Morning there is a BOSS FIGHT where the Agents must use their combined skills as a community and take on that year's challenge! There is a whole skill tree of personal knowledge to obtain, community to connect with and memories to make! To get started, check out our site <https://darknet-ng.network> and join our growing Discord Community!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-16:30 PDT

Title: Darknet-NG

When: Saturday, Aug 12, 10:00 - 16:30 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Darknet-NG is an In-Person Massively Multiplayer Online Role Playing Game (MMO-RPG), where the players take on the Persona of an Agent who is sent on Quests to learn real skills and gain in-game points. If this is your first time at DEF CON, this is a great place to start, because we assume no prior knowledge. Building from basic concepts, we teach agents about a range of topics from Lock-picking, to using and decoding ciphers, to Electronics 101, just to name a few, all while also helping to connect them to the larger DEF CON Community. The "Learning Quests" help the agent gather knowledge from all across the other villages at the conference, while the "Challenge Quests" help hone their skills! Sunday Morning there is a BOSS FIGHT where the Agents must use their combined skills as a community and take on that year's challenge! There is a whole skill tree of personal knowledge to obtain, community to connect with and memories to make! To get started, check out our site <https://darknet-ng.network> and join our growing Discord Community!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-16:30 PDT

Title: Darknet-NG

When: Friday, Aug 11, 10:00 - 16:30 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Darknet-NG is an In-Person Massively Multiplayer Online Role Playing Game (MMO-RPG), where the players take on the Persona of an Agent who is sent on Quests to learn real skills and gain in-game points. If this is your first time at DEF CON, this is a great place to start, because we assume no prior knowledge. Building from basic concepts, we teach agents about a range of topics from Lock-picking, to using and decoding ciphers, to Electronics 101, just to name a few, all while also helping to connect them to the larger DEF CON Community. The "Learning Quests" help the agent gather knowledge from all across the other villages at the conference, while the "Challenge Quests" help hone their skills! Sunday Morning there is a BOSS FIGHT where the Agents must use their combined skills as a community and take on that year's challenge! There is a whole skill tree of personal knowledge to obtain, community to connect with and memories to make! To get started, check out our site <https://darknet-ng.network> and join our growing Discord Community!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DARPA Announces an AI Cyber Initiative, Live at DC 32 and DC 33

When: Friday, Aug 11, 14:30 - 14:50 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers: Dave Weston, Heather Adkins, Matthew Knight, Michael Sellitto, Omkhar Arasaratnam, Perri Adams, Vijay Bolina

SpeakerBio: Dave Weston , Vice President of Enterprise and OS Security at Microsoft

No BIO available

SpeakerBio: Heather Adkins , Vice President of Security Engineering at Google

No BIO available

SpeakerBio: Matthew Knight , Head of Security at OpenAI

No BIO available

SpeakerBio: Michael Sellitto , Head of Geopolitics and Security Policy at Anthropic

No BIO available

SpeakerBio: Omkhar Arasaratnam , General Manager at Open Source Security Foundation (OpenSSF)

No BIO available

SpeakerBio: Perri Adams , AIxCC Program Manager at DARPA

No BIO available

SpeakerBio: Vijay Bolina , Chief Information Security Officer & Head of Cybersecurity Research at Google DeepMind

No BIO available

Description:

DARPA's AI Cyber Challenge program manager, Perri Adams, is joined by collaborators from Anthropic, Google, Google DeepMind, OpenAI and the Open Source Security Foundation to share insights about the upcoming competition and discuss the software security challenges facing the commercial sector and open-source community.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 16:00-18:59 PDT

Title: DC 404/DC 678/ DC 770/ DC 470 (Atlanta Metro)

When: Friday, Aug 11, 16:00 - 18:59 PDT

Where: Harrah's - Goldfield/Tonopah - Community Room - [Map](#)

Description:

They say Atlanta is the city too busy to hate, but it also has too much traffic for its widespread hacker fam to get together in a single meetup. So instead, we're meeting up in the desert during DEF CON! The one time of year when intown, northern burbs, south siders, and anyone else connected to DC404's 20+ year legacy can catch up and share stories.

Join us and meet your fellow ATL hackers!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-16:59 PDT

Title: DC Kubernetes Capture the Flag (CTF)

When: Saturday, Aug 12, 10:00 - 16:59 PDT

Where: Virtual

Description:

The DEF CON Kubernetes Capture the Flag (CTF) contest features a Kubernetes-based CTF challenge, where teams and individuals can build and test their Kubernetes hacking skills. Each team/individual is given access to a single Kubernetes cluster that contains a set of serial challenges, winning flags and points as they progress. Later flags pose more difficulty, but count for more points.

A scoreboard tracks the teams' current and final scores. In the event of a tie, the first team to achieve the score wins that tie.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-19:59 PDT

Title: DC Kubernetes Capture the Flag (CTF)

When: Friday, Aug 11, 10:00 - 19:59 PDT

Where: Virtual

Description:

The DEF CON Kubernetes Capture the Flag (CTF) contest features a Kubernetes-based CTF challenge, where teams and individuals can build and test their Kubernetes hacking skills. Each team/individual is given access to a single Kubernetes cluster that contains a set of serial challenges, winning flags and points as they progress. Later flags pose more difficulty, but count for more points.

A scoreboard tracks the teams' current and final scores. In the event of a tie, the first team to achieve the score wins that tie.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Saturday - 13:00-14:59 PDT

Title: DC's Next Top Threat Model (DCNTTM) - BYODesign Presentation

When: Saturday, Aug 12, 13:00 - 14:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Practice threat modeling on your own design! Be prepared to show off your design and take feedback/findings!

Registration required, come by our booth on Friday to sign up for a slot.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Friday - 11:00-17:59 PDT

Title: DC's Next Top Threat Model (DCNTTM) - BYODesign Registration

When: Friday, Aug 11, 11:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Do you have a design you would like to have Threat Modeled? Would you like to present it to DCNTTM organizers and DEF CON attendees for review? Come by our booth on Friday to register for a slot during our Saturday 2-hour event. We will provide you with a whiteboard and markers, present your design and we'll give you feedback.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Saturday - 10:00-11:59 PDT

Title: DC's Next Top Threat Model (DCNTTM) - Kids - Learn Threat Modeling

When: Saturday, Aug 12, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Want to teach your kid threat modeling? Are you new, yourself?

Stop by our booth, learn what threat modeling is, and get some practice with an introductory non-technical scenario.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Friday - 14:00-15:59 PDT

Title: DC's Next Top Threat Model (DCNTTM) - Kids - Learn Threat Modeling

When: Friday, Aug 11, 14:00 - 15:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Want to teach your kid threat modeling? Are you new, yourself?

Stop by our booth, learn what threat modeling is, and get some practice with an introductory non-technical scenario.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

Title: DC's Next Top Threat Model (DCNTTM)

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Threat Modeling is arguably the single most important activity in an application security program and if performed early can identify a wide range of potential flaws before a single line of code has been written. While being so critically important there is no single correct way to perform Threat Modeling, many techniques, methodologies and/or tools exist.

As part of our challenge we will present contestants with the exact same design and compare the outputs they produce against a number of categories in order to identify a winner and crown DEF CON's Next Top Threat Model(er).

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: DC's Next Top Threat Model (DCNTTM)

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Threat Modeling is arguably the single most important activity in an application security program and if performed early can identify a wide range of potential flaws before a single line of code has been written. While being so critically important there is no single correct way to perform Threat Modeling, many techniques, methodologies and/or tools exist.

As part of our challenge we will present contestants with the exact same design and compare the outputs they produce against a number of categories in order to identify a winner and crown DEF CON's Next Top Threat Model(er).

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Sunday - 12:00-13:59 PDT

Title: DCG Meetups

When: Sunday, Aug 13, 12:00 - 13:59 PDT

Where: Harrah's - Silver - DEF CON Groups - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 10:00-17:59 PDT

Title: DCG Meetups

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Harrah's - Silver - DEF CON Groups - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 10:00-17:59 PDT

Title: DCG Meetups

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Harrah's - Silver - DEF CON Groups - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file


DCGVR - Saturday - 20:05-20:10 PDT

Title: DCGVR Closing

When: Saturday, Aug 12, 20:05 - 20:10 PDT

Where: Virtual

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Thursday - 16:00-18:59 PDT

Title: DDV open and accepting drives for duplication

When: Thursday, Aug 10, 16:00 - 18:59 PDT

Where: Caesars Forum - Summit - 231 - Data Dupe VIg - [Map](#)

Description:

We start taking drives at 4:00pm local time on Thursday - possibly a little earlier. We reopen at 10:00am on Friday, Saturday, and Sunday.

We'll keep accepting drives until we reach capacity (usually late Friday or early Saturday). Then we copy and copy all the things until we just can't copy any more - first come, first served. We run around the clock until we run out of time on Sunday morning with the last possible pickup being before 11:00am on Sunday.

Most of the drive information can be found [here](<https://dcddv.org/dc31-drive-info>). If you have questions that have not yet been answered, you can email [info@dcddv.org](mailto:info@dcddv.org), or visit the [DEF CON Forums](<https://forum.defcon.org/node/244903>).

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Friday - 10:00-16:59 PDT

Title: DDV open and accepting drives for duplication

When: Friday, Aug 11, 10:00 - 16:59 PDT

Where: Caesars Forum - Summit - 231 - Data Dupe VIg - [Map](#)

Description:

We start taking drives at 4:00pm local time on Thursday - possibly a little earlier. We reopen at 10:00am on Friday, Saturday, and Sunday.

We'll keep accepting drives until we reach capacity (usually late Friday or early Saturday). Then we copy and copy all the things until we just can't copy any more - first come, first served. We run around the clock until we run out of time on Sunday morning with the last possible pickup being before 11:00am on Sunday.

Most of the drive information can be found [here](<https://dcddv.org/dc31-drive-info>). If you have questions that have not yet been answered, you can email [info@dcddv.org](mailto:info@dcddv.org), or visit the [DEF CON Forums](<https://forum.defcon.org/node/244903>).

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Saturday - 10:00-16:59 PDT

Title: DDV open and accepting drives for duplication

When: Saturday, Aug 12, 10:00 - 16:59 PDT

Where: Caesars Forum - Summit - 231 - Data Dupe VIg - [Map](#)

Description:

We start taking drives at 4:00pm local time on Thursday - possibly a little earlier. We reopen at 10:00am on Friday, Saturday, and Sunday.

We'll keep accepting drives until we reach capacity (usually late Friday or early Saturday). Then we copy and copy all the things until we just can't copy any more - first come, first served. We run around the clock until we run out of time on Sunday morning with the last possible pickup being before 11:00am on Sunday.

Most of the drive information can be found [here](<https://dcddv.org/dc31-drive-info>). If you have questions that have not yet been answered, you can email [info@dcddv.org](mailto:info@dcddv.org), or visit the [DEF CON Forums](<https://forum.defcon.org/node/244903>).

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTV - Saturday - 10:30-11:30 PDT

Title: DE: Breaking the Rule

When: Saturday, Aug 12, 10:30 - 11:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Project Obsidian: 101 Track (0x41) - [Map](#)

SpeakerBio:Oldmonk

Intrusion detection, analytics, packet forensics, security engineering and product engineering. 20+ years of being an entrepreneur building teams, solving big challenges.

Description:

This is a 101 track that takes you through the various aspects of detection engineering and a practitioners process of writing threat content. Its a great place to start for engineers and enthusiasts that might be exploring detection engineering as a career path.

The what, how and process of detection engineering.

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTV - Saturday - 11:30-12:30 PDT

Title: DE: Building a Detection Alert From a Threat Hunt

When: Saturday, Aug 12, 11:30 - 12:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Project Obsidian: Kill Chain Track (0x42) - [Map](#)

SpeakerBio: kobaltfox

TODO

Description:

A review of the detection engineering cycle and a walkthrough taking a threat hunt report and building a SIEM alert.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Death by 1000 Likes: How Much Do You Really Leak in Social Media?

When: Friday, Aug 11, 11:00 - 11:50 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

SpeakerBio: Will Kay

Will works for a private security consultancy in Australia. He is cybersecurity advisor and insider threat consultant. His professional career began many years ago in military intelligence to which he owes his knowledge of traditional targeting methods. The organisation and team he works for today provides security awareness and reinforcement training. His passion is removing the weakness that exists across society to social engineering techniques, and believes a more secure and prosperous future begins with people.

Description:

As lonely Aussies attending our first Defcon last year, we were frequently drawn to the hilarity/uniqueness of the Wall of Sheep board. One of our group suggested people leaking at the con was super entertaining, but what about throughout the rest of the year? We decided to use the time between DC30 and DC31 scraping the r/defcon subreddit to create the Wall of Sheep - online edition.

[Return to Index](#) - Add to  - ics [Calendar](#) file

QTV - Friday - 17:15-17:59 PDT

Title: Debate: NISQ and the future of Quantum Advantage: This village believes the current state of NISQ is already enabling quantum advantage for those who know how to use these technologies

When: Friday, Aug 11, 17:15 - 17:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

Speakers:Konstantinos Karagiannis,Rafal Janik

SpeakerBio:Konstantinos Karagiannis

No BIO available

SpeakerBio:Rafal Janik

No BIO available

Description:

Rafal Janik will argue for the proposition Konstantinos Karagiannis will argue against

for each talk: Opening - Bob introduces the topic 5 mins - speaker FOR the proposition 5 mins - speaker AGAINST the proposition ~10mins - rebuttals ~15mins - audience questions/comments 5 minis Vote & results and wrap up.

[Return to Index](#) - Add to  - ics [Calendar](#) file

QTV - Friday - 16:00-16:45 PDT

Title: Debate: The Quantum Village believes individual citizen privacy will be enhanced with the fielding of new quantum technologies.

When: Friday, Aug 11, 16:00 - 16:45 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

Speakers:David Joseph,Troy Mills

SpeakerBio:David Joseph

No BIO available

SpeakerBio:Troy Mills

No BIO available

Description:

David Joseph will argue for the proposition Troy Mills will argue against the proposition.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Friday - 15:30-16:30 PDT

Title: Deep Diving Into HID Vulnerabilities: Heart of Darkness

When: Friday, Aug 11, 15:30 - 16:30 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

Speakers: Chad, Shortman


SpeakerBio: Chad

No BIO available

SpeakerBio: Shortman

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DEF CON 101 - Welcome to DEF CON Panel

When: Thursday, Aug 10, 17:30 - 18:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers:Jeff "The Dark Tangent" Moss,fivepenny,Kirsten Renner,Magen,Nikita Kronenberg,deelo

SpeakerBio:Jeff "The Dark Tangent" Moss , DEF CON Communications

Mr. Moss is an internet security expert and is the founder of Both the Black Hat Briefings and DEF CON Hacking conferences. In 2022 Mr. Moss was named to the UK Government Cybersecurity Advisory Board, and in 2021 he was sworn in as a member of the DHS Cybersecurity Infrastructure Security Agency (CISA) Advisory Council (CSAC), and serves as a chairman of their Technical Advisory Council (TAC). Mr. Moss is a member of the Council on Foreign Relations (CFR) and is interested in policy issues around privacy, national security, and internet governance. He spends a lot of time in Singapore. Twitter: [@thedarktangent](#)

SpeakerBio:fivepenny

Fivepenny is the vendor lead and an avid reader and she's never going to give you up never going to let you down, Never gonna run around and desert you. Never gonna make you cry, Never gonna say goodbye, Never gonna tell a lie and hurt you.

SpeakerBio:Kirsten Renner , Talent Engagement Lead at Accenture Federal

Kirsten is the Talent Engagement Lead at Accenture Federal. She joined AFS through the acquisition of Novetta, after serving there as Director of Recruiting for 6 years. Her career started in IT building and running helpdesks, and she later moved into Technical Recruiting. She is best known in the community for both her role in the Car Hacking Village and her efforts as a speaker and volunteer across multiple events throughout the year. Kirsten offers over 20 years in technology services space and 15 in the hacker community and conference scene.

SpeakerBio:Magen , Urbane Security and CFP/CFW reviewer

Known by many nicknames and handles, Magen (she/her) has been attending DEF CON for over 15 years. She is a member of the CFP and CFW review boards, former lead of DEF CON workshops, a past DEF CON past speaker. Outside of con, she works at Urbane Security and loves coffee, weightlifting, and adding/listening to her vinyl collection.

SpeakerBio:Nikita Kronenberg , Director of Content & Coordination at DEF CON Communications

Nikita works to ensure DEF CON runs as smoothly as one can expect from a hacker convention. In addition to planning a vast array of details prior to DEF CON and thwarting issues while onsite, she is the (soon to be retired) Director of Content for the CFP Review Board. This year will be her 20th anniversary.

Nikita is not on the social mediaz.

SpeakerBio:deelo , Chief of Staff, SOC at DEF CON Conference

deelo, SOC Chief of Staff, is an active member of the SOC team and SOC Leadership. deelo's tenure with the SOC team began at DC19; the first year DefCon was at the Rio Hotel. Her personal motto is: "How can I make your day better?" and deelo brought this attitude with her when she joined the SOC team. After spending one year working on the conference floor, she quickly found herself moving behind the scenes in a slightly more administrative role. At that time, SOC was a team of 75 and deelo's main goal was to make sure everyone on the team ate "lunch" during their shift. Over the years, the SOC team has grown A LOT and the scope of deelo's job has changed as the team has gotten bigger. DefCon 31's SOC team consists of 150 Goons, and deelo's role is so much more than just keeping this team fed while on shift. There is a lot involved with coordinating the comings and goings of 150+ people and it keeps deelo busy for a good chunk of the year, but she wouldn't have it any other way...deelo loves what she does and she loves her team.

Years of Service: 13 and counting

Description:

DEF CON 101 began as a way to introduce n00bs to DEF CON. The idea was to help attendees get the best experience out of DEF CON (and also tell them how to survive the weekend!). The DEF CON 101 panel has been a way for people who have participated in making DEF CON what it is today to share those experiences and, hopefully, inspire attendees to expand their horizons. DEF CON offers so much more than just talks and the DEF CON 101 panel is the perfect place to learn about DEF CON so you can get the best experience possible. Come watch us talk about what we love about DEF CON, give you tips and tricks, and maybe even make some new friends!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 14:00-15:59 PDT

Title: DEF CON 31 Beard and Mustache Contest

When: Saturday, Aug 12, 14:00 - 15:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Held every year since DEF CON 19 in 2011 (R.I.P. Riviera), (Except during that COVID thing - but we are not going to talk about that COVID thing), the DEF CON Beard and Mustache Contest highlights the intersection of facial hair and hacker culture.

For 2023 there will be three categories for the competition:

- Full beard: Self-explanatory, for the truly bearded.
- Partial Beard or Mustache only (combined this year): For those sporting Van Dykes, Goatees, Mutton Chops, and other partial beard styles -or- Mustache only: Judging on the mustache only, even if bearded. Bring your Handlebars, Fu Manchus, or whatever adorns your upper lip.
- Freestyle: Anything goes, including fake and creatively adorned beards. Creative women often do well in the Freestyle category.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Saturday - 14:00-14:59 PDT

Title: DEF CON Chess Kids Free-Play

When: Saturday, Aug 12, 14:00 - 14:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Kids free play chess for an hour before the main chess tournament (which is also kid friendly). Kids open play is 14:00 to 15:00 Saturday, forum contest area.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 15:00-17:59 PDT

Title: DEF CON Chess Tournament

When: Saturday, Aug 12, 15:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Twitter: @defconchess

For early registration, please send your name and rating to: defconchess@gmail.com

Chess, computers, and hacking go way back. In the 18th century, the Mechanical Turk appeared to play a good game, but there was a human ghost hiding in the shell. Some of the first computer software was written to play chess. In 1997, world champion Garry Kasparov lost to the program Deep Blue, but after the match he accused IBM of cheating, alleging that only a rival grandmaster could have made certain moves.

At DEF CON 31, we will run a human chess tournament. The games will have a “blitz” time control of 5 minutes on each player’s clock, for a maximum total game time of 10 minutes. The tournament will have a Swiss-system format, with a fixed number of rounds. The match pairing for each round is done after the previous round has ended, and depends on its results. Each player is paired with another player who has a similar running score.

To determine the winner, the Swiss system is considered highly effective, even when there is a large number of competitors and a small number of rounds. Every player gets to play the full tournament, and the winner has the highest aggregate score when all rounds are over.

There will be trophies and prizes for the top three players.

The tournament mechanics will be managed by the Las Vegas Chess Center (LVCC), which has many years of experience in organizing royal game tournaments for all strength levels and ages. LVCC has professional coaches, and grandmasters are frequent visitors.

Max players: 100. In order to crown the best chess player at DEF CON, we will register the highest-rated players first.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Sunday - 15:30-17:30 PDT

Title: DEF CON Closing Ceremonies & Awards

When: Sunday, Aug 13, 15:30 - 17:30 PDT

Where: Caesars Forum - Forum - 105, 135-136, 108-119, 138-139 - Tracks 1 & 2 - [Map](#)

SpeakerBio:Jeff "The Dark Tangent" Moss , DEF CON Communications

Mr. Moss is an internet security expert and is the founder of Both the Black Hat Briefings and DEF CON Hacking conferences. In 2022 Mr. Moss was named to the UK Government Cybersecurity Advisory Board, and in 2021 he was sworn in as a member of the DHS Cybersecurity Infrastructure Security Agency (CISA) Advisory Council (CSAC), and serves as a chairman of their Technical Advisory Council (TAC). Mr. Moss is a member of the Council on Foreign Relations (CFR) and is interested in policy issues around privacy, national security, and internet governance. He spends a lot of time in Singapore. Twitter: [@thedarktangent](#)

Description:

The end is here! DEF CON 31 is at a close and we want to thank everyone who participated, contributed, retired, promoted, and won contests. DEF CON departments will share stats, info, and data collected throughout the weekend related to the network, code of conduct transparency, stats on attendee participation in events, and more. This is the ceremony where we also announce the contestants who've won a prestige UBER badge for select contests.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DEF CON Groups Keynote

When: Saturday, Aug 12, 10:00 - 10:30 PDT

Where: Virtual

SpeakerBio:Jayson E. Street

No BIO available

Twitter: [@jaysonstreet](#)

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 16:00-18:59 PDT

Title: DEF CON Holland Group Presents: VrijMiBo

When: Friday, Aug 11, 16:00 - 18:59 PDT

Where: Flamingo - Bird Bar

Description:

In The Netherlands it's a tradition to catch up with your colleagues just before the end of the workday on Friday when the weekend starts to kick in. In The Netherlands this is called the "VrijMiBo" (Vrijdag/Friday - Middag/Afternoon Borrel/Drink)

"VrijMiBo/Friday afternoon Drink" at DEF CON is a perfect moment to talk about what your favorite thing is at DefCon, show your cool handmade badges, impress other hackers about your latest hacks, make new friends, gossip about your boss and show your cat or dog pictures.

Vrijdag Middag Borrel, Freitag Mittags Getränk, Apéritif du vendredi après-midi, trago de viernes por la tarde.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Thursday - 14:00-15:59 PDT

Title: DEF CON Kids Meetup

When: Thursday, Aug 10, 14:00 - 15:59 PDT

Where: Caesars Forum - Forum - 129 - Chillout - [Map](#)

Description:

Come meet with other like minded kids and get ready for a weekend of hacking all the things!

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 19:30-21:59 PDT

Title: DEF CON Kids Party

When: Saturday, Aug 12, 19:30 - 21:59 PDT

Where: Caesars Forum - Forum - 131-133 - [Map](#)

Description:

Party with other DEF CON kids. Enjoy some music, and some good conversation with other DEF CON kids!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DEF CON Scavenger Hunt

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Are you tired of being an NPC, mindlessly standing in line at a hacker con? Do you want to be involved and improve the hacker community? The DEF CON Scavenger Hunt is here to encourage you to interact with goons and attendees alike; to be an active participant of DEF CON itself.

Come visit the DEF CON Scavenger Hunt table in the contest area and get a list, register your team of 1 to 5 players, and gather or accomplish as many items from the list as you can. Items are submitted at the table, better than average submissions shall be awarded bonus points. The team who turns in the most points by Sunday at noon will win the admiration of your like-minded peers.

The DEF CON Scavenger Hunt is one of the longest running contests at DEF CON, visit <https://defconscavhunt.com> for a history lesson.

If you capture pictures or video of items from our list, or have in the past, please send them to us via email scavlist@gmail.com.

--

The scavenger hunt list is open to interpretation and we are not responsible for how list items are interpreted. We have had a number of pre-teens and teenagers play the scavenger hunt over the years, primarily with their parents but occasionally alone. The team that won at DC24 included a teenager with their parents. Parental Guidance Recommended.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT

Title: DEF CON Scavenger Hunt

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Are you tired of being an NPC, mindlessly standing in line at a hacker con? Do you want to be involved and improve the hacker community? The DEF CON Scavenger Hunt is here to encourage you to interact with goons and attendees alike; to be an active participant of DEF CON itself.

Come visit the DEF CON Scavenger Hunt table in the contest area and get a list, register your team of 1 to 5 players, and gather or accomplish as many items from the list as you can. Items are submitted at the table, better than average submissions shall be awarded bonus points. The team who turns in the most points by Sunday at noon will win the admiration of your like-minded peers.

The DEF CON Scavenger Hunt is one of the longest running contests at DEF CON, visit <https://defconscavhunt.com> for a history lesson.

If you capture pictures or video of items from our list, or have in the past, please send them to us via email scavlist@gmail.com.

--

The scavenger hunt list is open to interpretation and we are not responsible for how list items are interpreted. We have had a number of pre-teens and teenagers play the scavenger hunt over the years, primarily with their parents but occasionally alone. The team that won at DC24 included a teenager with their parents. Parental Guidance Recommended.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: DEF CON Scavenger Hunt

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Are you tired of being an NPC, mindlessly standing in line at a hacker con? Do you want to be involved and improve the hacker community? The DEF CON Scavenger Hunt is here to encourage you to interact with goons and attendees alike; to be an active participant of DEF CON itself.

Come visit the DEF CON Scavenger Hunt table in the contest area and get a list, register your team of 1 to 5 players, and gather or accomplish as many items from the list as you can. Items are submitted at the table, better than average submissions shall be awarded bonus points. The team who turns in the most points by Sunday at noon will win the admiration of your like-minded peers.

The DEF CON Scavenger Hunt is one of the longest running contests at DEF CON, visit <https://defconscavhunt.com> for a history lesson.

If you capture pictures or video of items from our list, or have in the past, please send them to us via email scavlist@gmail.com.

--

The scavenger hunt list is open to interpretation and we are not responsible for how list items are interpreted. We have had a number of pre-teens and teenagers play the scavenger hunt over the years, primarily with their parents but occasionally alone. The team that won at DC24 included a teenager with their parents. Parental Guidance Recommended.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT

Title: DEFCON MUD DUMB TERMINAL EDITION

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The DEFCON MUD is back, this time you can only access it over dumb terminals or serial terminals hosted by the DEFCON SCAV Hunt. Flags will be hosted inside the mud, good luck, have fun, and oh yes the game has exploits, can you find them all?

--

Rated PG-13.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: DEFCON MUD DUMB TERMINAL EDITION

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The DEFCON MUD is back, this time you can only access it over dumb terminals or serial terminals hosted by the DEFCON SCAV Hunt. Flags will be hosted inside the mud, good luck, have fun, and oh yes the game has exploits, can you find them all?

--

Rated PG-13.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

Title: DEFCON MUD DUMB TERMINAL EDITION

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The DEFCON MUD is back, this time you can only access it over dumb terminals or serial terminals hosted by the DEFCON SCAV Hunt. Flags will be hosted inside the mud, good luck, have fun, and oh yes the game has exploits, can you find them all?

--

Rated PG-13.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Defcon.run

When: Thursday, Aug 10, 06:00 - 11:59 PDT

Where: Other/See Description

Description:

IF the future is coming and it is! Then you're going to need to run! Get started at defcon.run!

Defcon.run is an evolution of the now long running Defcon 4x5K running event. But now it's bigger and more fun! Due to stupendous growth, we've been forced to change up the format. This year's activity will look to match up folks for fun runs, and rucks (!), in smaller distributed groups around Las Vegas. It's the same old event but at a distributed scale! Show up in the morning to beat the heat, go for a run with folks, have a good time!

We'll have a full set of routes for people to choose from from simple 5Ks to more ambitious distances.

You can register to log your distance, we'll have a leader board, and shenanigans! Full Information at <https://defcon.run>

Interested parties should rally at Harrah's Goldfield at 06:00, but be sure to check [defcon.run](<https://defcon.run>) for any updates.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Defcon.run

When: Friday, Aug 11, 06:00 - 11:59 PDT

Where: Other/See Description

Description:

IF the future is coming and it is! Then you're going to need to run! Get started at defcon.run!

Defcon.run is an evolution of the now long running Defcon 4x5K running event. But now it's bigger and more fun! Due to stupendous growth, we've been forced to change up the format. This year's activity will look to match up folks for fun runs, and rucks (!), in smaller distributed groups around Las Vegas. It's the same old event but at a distributed scale! Show up in the morning to beat the heat, go for a run with folks, have a good time!

We'll have a full set of routes for people to choose from from simple 5Ks to more ambitious distances.

You can register to log your distance, we'll have a leader board, and shenanigans! Full Information at <https://defcon.run>

Interested parties should rally at Harrah's Goldfield at 06:00, but be sure to check [defcon.run](<https://defcon.run>) for any updates.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Defcon.run

When: Sunday, Aug 13, 06:00 - 11:59 PDT

Where: Other/See Description

Description:

IF the future is coming and it is! Then you're going to need to run! Get started at defcon.run!

Defcon.run is an evolution of the now long running Defcon 4x5K running event. But now it's bigger and more fun! Due to stupendous growth, we've been forced to change up the format. This year's activity will look to match up folks for fun runs, and rucks (!), in smaller distributed groups around Las Vegas. It's the same old event but at a distributed scale! Show up in the morning to beat the heat, go for a run with folks, have a good time!

We'll have a full set of routes for people to choose from from simple 5Ks to more ambitious distances.

You can register to log your distance, we'll have a leader board, and shenanigans! Full Information at <https://defcon.run>

Interested parties should rally at Harrah's Goldfield at 06:00, but be sure to check [defcon.run](<https://defcon.run>) for any updates.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Saturday - 06:00-11:59 PDT

Title: Defcon.run

When: Saturday, Aug 12, 06:00 - 11:59 PDT

Where: Other/See Description

Description:

IF the future is coming and it is! Then you're going to need to run! Get started at defcon.run!

Defcon.run is an evolution of the now long running Defcon 4x5K running event. But now it's bigger and more fun! Due to stupendous growth, we've been forced to change up the format. This year's activity will look to match up folks for fun runs, and rucks (!), in smaller distributed groups around Las Vegas. It's the same old event but at a distributed scale! Show up in the morning to beat the heat, go for a run with folks, have a good time!

We'll have a full set of routes for people to choose from from simple 5Ks to more ambitious distances.

You can register to log your distance, we'll have a leader board, and shenanigans! Full Information at <https://defcon.run>

Interested parties should rally at Harrah's Goldfield at 06:00, but be sure to check [defcon.run](<https://defcon.run>) for any updates.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Defeating VPN Always-On

When: Saturday, Aug 12, 10:00 - 10:45 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

SpeakerBio:Maxime Clementz , Cybersecurity Senior Manager at PwC Luxembourg

Maxime Clementz is a Senior Manager within the Cybersecurity Advisory team of PwC Luxembourg. He develops his ethical hacker skills by committing himself to various assignments for big companies, banks and European institutions. As a technical specialist, he leads penetration tests, red-teaming, digital forensics and incident response missions.

He contributes to the development of the team's hacking capabilities by sharing the results of his technology watch and R&D and is now leading the CSIRT and Threat Intelligence initiatives of PwC Luxembourg. He especially enjoys sharing knowledge by presenting the results of each mission or by giving talks (Hack.lu 2012, 2015, 2017) and training courses. Maxime teaches IT security at a French engineering school and organizes a Capture the Flag event for the students.

Twitter: [@maxime_tz](#)

Description:

VPN Always-On is a security control that can be deployed to mobile endpoints that remotely access corporate resources through VPN. It is designed to prevent data leaks and narrow attack surface of enrolled end-user equipment connected to untrusted networks. When it is enforced, the mobile device can only reach the VPN gateway and all connections are tunneled.

We will review the relevant Windows API, the practicalities of this feature, look at popular VPN software; we will then consider ridiculously complex exfil methods and... finally bypass it with unexpectedly trivial tricks. We will exploit design, implementation and configuration issues to circumvent this control in offensive scenarios. We will then learn how to fix or harden VPN Always-On deployment to further limit the risks posed by untrusted networks.

REFERENCES

VPN on untrusted networks, captive portals: - ANSSI (France) Recommandations sur le nomadisme numérique ("3.4.3 Maîtrise des flux réseaux sur le poste de travail"):

https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf (I will translate the relevant part in my slide)

Understanding "Windows Filtering Platform": - Microsoft documentation :

<https://learn.microsoft.com/en-us/windows/win32/fwp/windows-filtering-platform-start-page> - Pavel Yosifovich :

<https://scorpionsoftware.net/2022/12/25/introduction-to-the-windows-filtering-platform/> - Pavel Yosifovich :

<https://github.com/zodiacon/WFPEXplorer> - Sagie Dulce : <https://github.com/zeronetworks/wtf-wfp>

Reverse Engineering of Windows Filtering Platform and its implementation in Windows VPN agents: - Ole André V. Ravnas - <https://frida.re/> - James Forshaw -

<https://github.com/googleprojectzero/sandbox-attacksurface-analysis-tools/tree/main/NtObjectManager>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Defender-Pretender: When Windows Defender Updates Become a Security Risk

When: Friday, Aug 11, 12:30 - 13:15 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

Speakers: Omer Attias, Tomer Bar

SpeakerBio: Omer Attias, Security Researcher at SafeBreach Labs

Omer Attias is an accomplished security researcher with over five years of experience in the field of cybersecurity. He currently works as a researcher at SafeBreach Labs.

With a background in the Ministry of Defense and the Israeli Defense Forces (IDF), Omer has honed his skills in network research, including a deep understanding of Windows internals and Linux kernel components.

In addition to his professional pursuits, Omer is a passionate technology and science enthusiast who is always eager to explore emerging trends and innovations in these fields.

Twitter: [@@omerat21](#)

SpeakerBio: Tomer Bar, VP of Security Research at SafeBreach Labs

Tomer Bar is a hands-on security researcher with 20 years of unique experience in cyber security. He leads SafeBreach Labs as the VP of security research. In the past, he ran research groups for the Israeli government and then led the endpoint malware research for Palo Alto Networks. His main interests are vulnerability research, reverse engineering, and APT research.

Among his recent discoveries are the PrintDemon vulnerabilities in the Windows Spooler mechanism which were a candidate in the best privilege escalation of Pwnie awards and several research studies on Iranian APT campaigns. He presented his research at DEF CON (28-30), BlackHat USA, ReCon, Sector, Confidence, Security Fest and HackCon conferences.

Description:

The signature update process is critical to EDR's effectiveness against emerging threats. The security update process must be highly secured, as demonstrated by the Flame malware attack that leveraged a rogue certificate for lateral movement. Nation-state capabilities are typically required for such an attack, given that signature update files are digitally signed by Microsoft.

We wondered if we could achieve similar capabilities running as an unprivileged user without possessing a rough certificate, instead we aimed to turn the original Windows Defender process to our full control.

In this talk we will deep dive into Windows Defender architecture, the signature database format and the update process, with a focus on the security verification logic. We will explain how an attacker can completely compromise any Windows agent or server, including those used by enterprises, by exploiting a powerful Oday vulnerability that even we didn't expect to discover.

We will demonstrate Defender-Pretender, a tool we developed to achieve neutralization of the EDR. allowing any already known malicious code to run Fully Un-Detected. It can also force Defender to delete admin's data. OS and driver files, resulting in an unrecoverable OS. We will also explain how an attacker can alter Defender's detection and mitigation logic.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Defending KA-SAT: The detailed story of the response, how it was analyzed, and what was learned

When: Friday, Aug 11, 11:00 - 11:45 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

Speakers:Mark Colaluca,Nick Saunders

SpeakerBio:Mark Colaluca , Vice President and Chief Information Security Officer (CISO) at Viasat

Mark Colaluca is Vice President & Chief Information Security Officer for Viasat, a global satellite communications service provider. Mark is responsible for Viasat's corporate information security program, as well as infrastructure and security engineering for Viasat's enterprise networks serving customers across government, commercial and residential markets. During Mark's tenure at Viasat, he has held various engineering, architecture, and leadership roles within the organization, including the design, development, and delivery of the ground system infrastructure for Viasat's first and second generation satellite networks. Mark has also led Viasat's engagement with the private sector and government security communities, which includes facilitating active information sharing with these partners. Prior to joining Viasat, Mark provided security and network architecture consulting to several Fortune 50 firms as a member of KPMG, and held network and security engineering roles with Texas Instruments and Raytheon. Mark is a graduate of the University of Texas at Austin with a bachelor's degree in Electrical & Computer Engineering, and is the joint U.S. Patent holder for an advanced method of providing layer-2 network services through a non-routed ground segment network.

SpeakerBio:Nick Saunders , Chief Cybersecurity and Data Officer at Viasat

Nick Saunders serves as the Chief Cybersecurity and Data Officer for Government Systems at Viasat. He is responsible for ensuring the security for government users of Viasat's global networks. Nick leads teams focused on the development of novel cybersecurity analytics techniques, maintaining compliance across Viasat's global networks, performing active cybersecurity defense, red team activities, forensics, cyber threat intelligence, and other cybersecurity-related functions. Nick has 15 years of experience leading and advancing technology focused on cybersecurity, information assurance, embedded systems, bootloaders, operating systems, space systems architecture, critical infrastructure, and multiple communications-focused disciplines. He has been published in IEEE and presented at multiple technical conferences (IEEE, SANS). Nick has presented cybersecurity briefings for USMC, USAF, Space Command, and multiple other USG departments. Nick also works to champion and improve data practices across Government systems by advancing AI/ML initiatives and product capabilities. Nick is a graduate of Virginia Tech and holds degree in Computer Engineering.

Description:

In February 2022, the Viasat owned KA-SAT network experienced a significant cyberattack that resulted in a partial outage of services for thousands of users in Ukraine and tens of thousands of users in other parts of Europe. This presentation will provide detailed background on the attack, which involved the deployment of malware against terminals on the network, as well as several distinct network-based attacks that appeared focused on further denying connectivity to KA-SAT users. These network-based attacks needed to be characterized and responded to by Viasat's operational teams in real-time, and the attacks continued with intensity for many weeks after the original malware incident.

Viasat will share the story of how it responded and performed a rapid forensic on several impacted terminals to determine within 36 hours that the terminal flash memory had been overwritten with a distinctive pattern in the attack. This presentation will explain details around the forensic analysis as well as the process of reverse engineering the malicious toolkit to verify it would produce the observed flash memory effects. Viasat will also share technical details of over-the-air network attacks that were used to attack the KA-SAT network.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Defense Community

When: Saturday, Aug 12, 14:30 - 15:20 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

Speakers: Brian Stearns, Charles Smith, Eric Davis, Glenn Borskey, Jon A.

SpeakerBio: Brian Stearns

Brian C. Stearns has 25 years of experience across the public and private sector in technical instruction, systems engineering, information security, digital forensics, and secure communications. Brian founded the Institute for Secure Activism to support activists, organizers, and protesters who advocate for LGBTQ+, BIPOC, and other marginalized communities. Brian is also a senior Signature Management instructor with Ridgeline International and the director of Ridgeline's Signature Validation Lab. Prior to his current positions Brian spent 15 years supporting US government global counterterrorism operations as a tactical digital forensic collection and targeting specialist.

SpeakerBio: Charles Smith

Charles Smith is a cybersecurity researcher at Johns Hopkins University Applied Physics Lab (JHU/APL), where he focuses on the intersection of cyber and information operations and their impact on national security. Charles spent the first fourteen years of his career as an officer in the U.S. Army, and the recipient of numerous awards and badges including the Ranger Tab, Combat Infantry Badge, and Purple Heart. He deployed five times as both an infantry officer and intelligence officer to Iraq and Afghanistan, and was selected to serve as an intelligence officer for the 2nd Battalion, 75th Ranger Regiment. His served his last four years in uniform at US Cyber Command, where he led intelligence support to the defense of the 2020 elections. Prior to joining JHU/APL, Charles also worked at Twitter on trust and safety response to crises. Charles holds a bachelor's of science in Business Administration from Bucknell University, and a Masters of Strategic Intelligence from National Intelligence University.

SpeakerBio: Eric Davis

Eric Davis has safeguarded brands, platforms, and billions of users from bad ads, bad apps, and other machinations of malefactors across global policy, product, and engineering functions. A frequent consultant and advisor across civic and private sectors on Trust & Safety, Privacy, and Security issues, Eric is a founding advisor to the Trust & Safety Professional Association, and a member of the Integrity Institute's Elections Integrity Working Group, which publishes a series of best practices and resources guides for tech platforms contending with disinformation and other issues impacting elections integrity. Previously, Eric was the former Chief Privacy and Policy Officer and global trust & safety lead at Bigo, a live streaming and short form video social media platform with over 200M users globally. Prior to Bigo, he was Senior Director for Product Management at Lifelock (acquired by Symantec), prototyping new consumer products, leading AppSec, and leading product strategy for GDPR and other privacy regulations globally. Prior to Symantec, Eric spent 13 years at Google, where he founded Google's first Trust & Safety team, Anti-Malvertising program, and the Android Security Operations and Intel team in addition to his other product policy and public policy leadership roles. Earlier in his career, he was the charter International Product Manager for Trust & Safety at eBay.

Twitter: [@ericdavis](#)

SpeakerBio: Glenn Borskey

Glenn Borsky is a strategic cyber threat intelligence analyst who's area of research is in cyber threat and cognitive security. He brings experience developing cybersecurity strategies for senior leadership and executive level audiences. His main area of interest is in countering mis/disinformation and cyber enabled cognitive warfare.

Twitter: [@GlennBorsky](#)

SpeakerBio: Jon A.

No BIO available

Description:

This panel explores the pivotal role of technology in shaping voter outcomes, drawing insights from the perspectives of the

defense community. The discussion delves into how various technological advancements, including data analytics, digital marketing, and cybersecurity, influence the democratic process. By assessing the role of technology in shaping voter engagement, perception, and decision-making, the panel seeks to deepen our understanding of the evolving dynamics between technology and democratic governance. The aim is to generate informed discussions and policy considerations to preserve the integrity and fairness of democratic elections. Join us for an illuminating session as we uncover the opportunities and challenges presented by technological interventions in the electoral landscape.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Defensive Coding and Hardened Javascript

When: Friday, Aug 11, 11:00 - 12:59 PDT

Where: Flamingo - Savoy - AppSec Village - Workshop - [Map](#)

Speakers: Aaron Kumavis, Zbyszek Tenerowicz

SpeakerBio: Aaron Kumavis

founder metamask

Twitter: [@kumavis_](#)

SpeakerBio: Zbyszek Tenerowicz

JS Security Engineer at MetaMask working on LavaMoat and Endo. Started using Node.js at v0.8 and never stopped. Enjoys innovating and teaching security, diagnostics and maintainability. One of the oldest members of meet.js Poland community.

Twitter: [@naughtur](#)

Description:

Malicious code is out to get you. Can you keep your app working as expected and hold on to your secrets? Come to this workshop and try!

The entire workshop will be delivered as bite-sized hands-on exercises where increasingly advanced threats are presented and you get to defend.

We'll explore techniques allowing cooperation with packages that intend to steal your secrets and mess with built-in functionality of JavaScript via prototype-poisoning. Another part of the workshop will focus on using tools to isolate code and scale the defensive coding practice up for larger codebases.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Democracy, Are You Citizen Or Subject?

When: Saturday, Aug 12, 14:40 - 15:30 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio:Kendall Spencer

Kendall Spencer is an associate in the Intellectual Property Department. Kendall is based in the Boston office where he is a member of the Technology Transactions, Cybersecurity, and Privacy Practice Group. In his previous position as a law clerk, Kendall specialized in Complex Litigation. He also has a strong focus on technology law. Kendall has advised on blockchain technology integration, researched blockchain voting regulations, and investigated the use of blockchain technology to create a database of information on its advantages and efficacy. Additionally, he assisted in drafting an article regarding data privacy issues within real estate law. Kendall serves as a member of the Executive Leadership Team with the National Governing Body of USA Track and Field (USATF), as well as a board member with the National Collegiate Athletic Association (NCAA). As a professional athlete on the U.S. Olympic Team, he has earned accolades such as USA Indoor Bronze Medalist, NCAA National Champion, on top of serving as a USA Track and Field board member.

Twitter: [@Kspencer24](#)

Description:

What does it mean to be an American today? In a world where innovation outpaces regulatory progress; principles of law, technology, and policy collide to create a nation of unprecedented conflict. But when it's all said and done what is left of our Democracy? Institutions structured to protect our democratic way of life such as voting and the vehicles used to carry out voting have become increasingly difficult to protect. Yet, those most effected are often too inundated with every day life to engage in activity likely to contribute to meaningful change. Maybe democracy has become too hard to uphold, or maybe it's become too hard to be an American.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Demystifying (& Bypassing) macOS's Background Task Management

When: Saturday, Aug 12, 10:00 - 10:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio: Patrick Wardle , Objective-See Foundation

Patrick Wardle is the creator of the non-profit Objective-See Foundation, author of the “The Art of Mac Malware” book series, and founder of the "Objective by the Sea" macOS Security conference.

Having worked at NASA and the NSA, as well as presenting at countless security conferences, he is intimately familiar with aliens, spies, and talking nerdy.

Patrick is passionate about all things related to macOS security and thus spends his days finding Apple 0days, analyzing macOS malware, and writing books and free open-source security tools to protect Mac users.

Twitter: [@patrickwardle](#)

Description:

To retain a foothold on an infected system, most Mac malware will persist; installing itself in a manner that ensures it will be automatically (re)launched each time the infected system is rebooted.

In macOS Ventura, Apple's rearchitected core persistence mechanisms and added a new security mechanism that alerts the user any time an item is persisted. As the former is both undocumented and implemented in a proprietary manner this poses a problem for existing security and forensics tools (that aim to heuristically detect malware via unauthorized persistence events). On the other hand, the latter is problematic to malware authors, who obviously want their malicious creations to persist without an alert being shown to the user.

In this talk, we'll indiscriminately provide solutions for all! First, we'll dive into the internals of macOS's Background Task Management (BTM) which, as we'll see, contains a central (albeit proprietary) repository of persistent items. Armed with this information, we'll release open-source code capable of programmatically enumerating all persistent items from BTM, ensuring security and forensics tools regain compatibility. We'll also highlight design weaknesses that malicious code could trivially employ to sidestep the new security features of BTM, such that persistence may still be silently achieved.

REFERENCES

<https://piunikaweb.com/2023/01/30/macOS-13-ventura-background-items-added-notification-issue/>

<https://www.sentinelone.com/blog/apples-macos-ventura-7-new-security-changes-to-be-aware-of/>

Apple Documentation:

<https://support.apple.com/guide/deployment/manage-login-items-background-tasks-mac-depdca572563/web>

Return to Index - Add to  - ics [Calendar](#) file

Title: Demystifying Hacking for Government Officials

When: Friday, Aug 11, 17:00 - 17:50 PDT

Where: Caesars Forum - Summit - 221-222 - Policy Atrium - [Map](#)

Speakers:Brad Manuel,Jack Cable,Jason Ingalls,Lindsey Forson,Michael Ross

SpeakerBio:Brad Manuel , Chief Information Officer at Louisiana Secretary of State's Office

Brad Manuel brings to the table extensive election administration and disaster recovery experience. He has led a cross-agency team to administer elections during challenging emergencies. He also serves as the co-chair of Louisiana's Election Security Committee under the Louisiana Cybersecurity Commission.

SpeakerBio:Jack Cable , Senior Technical Advisor at Cybersecurity and Infrastructure Security Agency (CISA)

Jack Cable is a Senior Technical Advisor at the Cybersecurity and Infrastructure Security Agency (CISA). Prior to that, Jack worked as a TechCongress Fellow for the Senate Homeland Security and Governmental Affairs Committee, advising Chairman Gary Peters on cybersecurity policy, including election security and open source software security. He previously worked as a Security Architect at Krebs Stamos Group. Jack also served as an Election Security Technical Advisor at CISA, where he created Crossfeed, a pilot to scan election assets nationwide. Jack is a top bug bounty hacker, having identified over 350 vulnerabilities in hundreds of companies. After placing first in the Hack the Air Force bug bounty challenge, he began working at the Pentagon's Defense Digital Service. Jack holds a bachelor's degree in Computer Science from Stanford University and has published academic research on election security, ransomware, and cloud security.

SpeakerBio:Jason Ingalls , Founder & CEO at Ingalls Information Security

Jason Ingalls has attended Blackhat and DEFCON since 2006. He has spoken and presented at numerous conferences, including as keynote for the University of California Inaugural Cybersecurity Conference in 2016. His experience with data breach response and his firm's work with election cybersecurity controls provide valuable insight that few possess into the technology, processes, and people involved in securing elections.

SpeakerBio:Lindsey Forson , Deputy Executive Director at National Association of Secretaries of State

Lindsey Forson has worked at the intersection of cybersecurity and public policy for the past five years. She is dedicated to fostering relationships between NASS members and collaborators in the cybersecurity space.

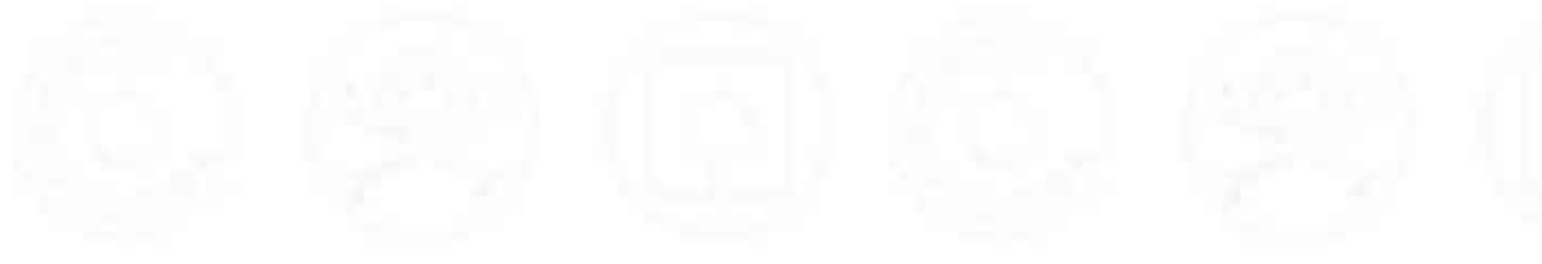
SpeakerBio:Michael Ross , Deputy Secretary of State and Chief of Staff at Iowa Secretary of State's Office

Michael Ross, the Deputy Secretary of State and Chief of Staff for the Iowa Secretary of State's office, has led the office's strong engagement with federal partners and the security research community. Through NASS and relationships developed with peers that oversee elections in their states, Ross has encouraged engagement with the researcher community.

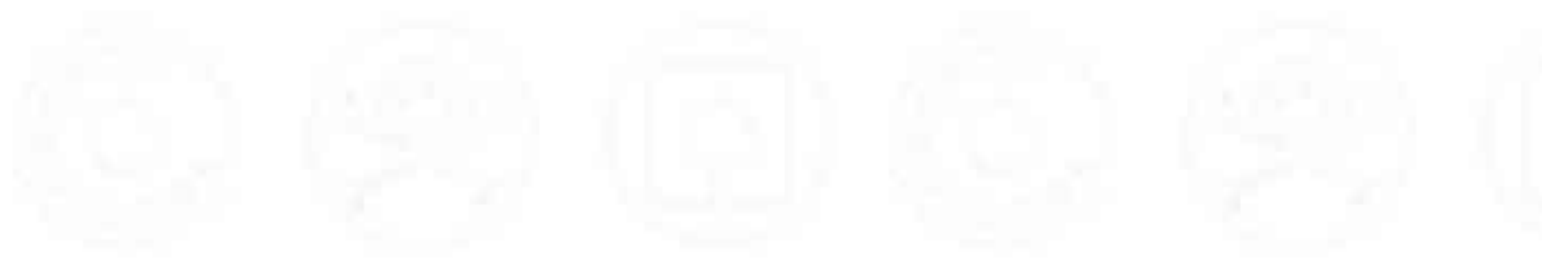
Description:

Most of us acknowledge that collaboration between hackers and policymakers is necessary and beneficial. Specifically, the security research community is more effective in supporting security improvements for state and local government entities when they work collaboratively with government officials. We also know building bridges between these communities, each of which includes a diverse makeup of individuals and organizations, is not a simple task. Several years ago, the National Association of Secretaries of State (NASS) and a small group of hackers began construction on one such bridge. This session shares lessons learned from that experience. NASS created an interactive event, called Hacking Demystified, which complements broader efforts to educate and foster relationship-building. We will provide examples of where we have found success and seek input from the audience on how to further expand our work. We will generate ideas for how everyone in the room may create more opportunities for productive collaboration between security researchers and state government officials. Join us to learn more about how NASS is demystifying hacking and participate in a brainstorming session on how we may all work together to further increase knowledge and understanding across our communities.

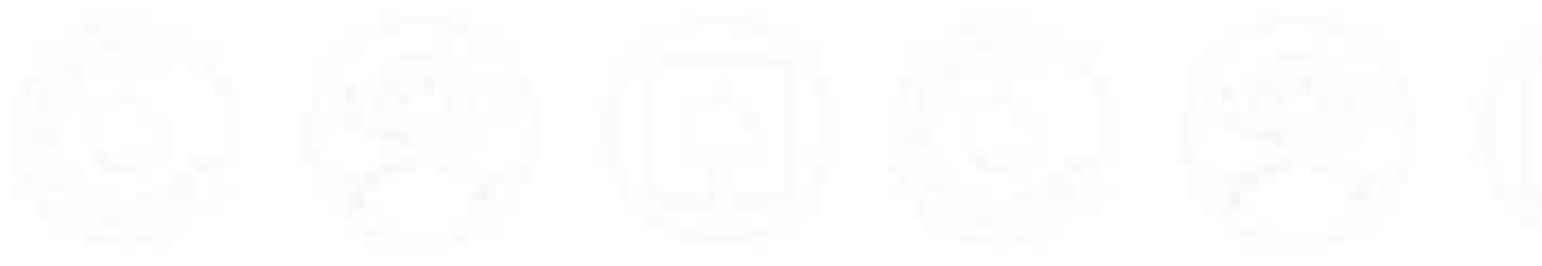
同治十一年庚午



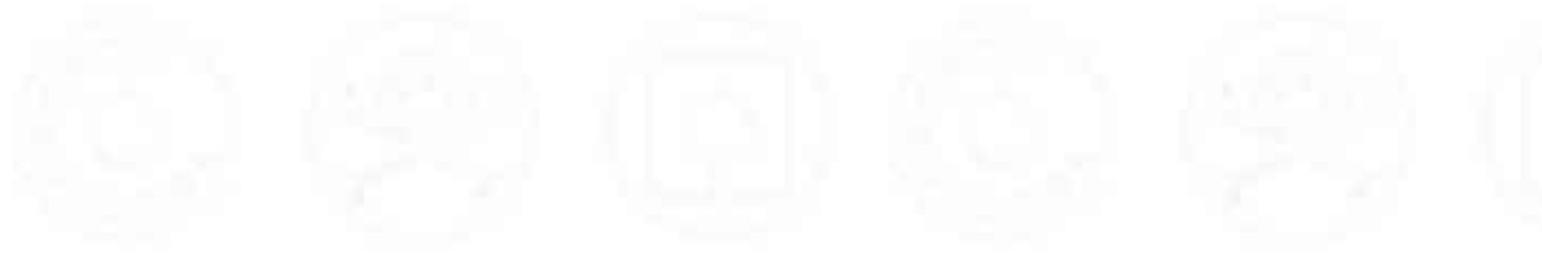
同治十一年庚午



同治十一年庚午



同治十一年庚午



同治十一年庚午

Title: Designing RFID Implants - How flipping the bird opens doors for me

When: Thursday, Aug 10, 14:30 - 15:15 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio: Miana Ella Windall , Hacker

Miana is a lifelong tinkerer who likes breaking things almost as much as she likes building them. She is a bio-hacker and info-sec researcher by night, and a professional software nerd during the day.

Twitter: [@NiamhAstra](#)

Description:

RFID implants are basically RFID credentials that can be installed under your skin. When I discovered there was nothing on the market that worked with my employers badging system I decided that I would just have to make my own. This talk will cover the basics of RFID implants, my journey to design my own implant despite having no electronics experience, and some of the future implications of this technology.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DevSecOps Worst Practices

When: Friday, Aug 11, 12:30 - 13:15 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

SpeakerBio: Tanya Janca

Tanya Janca, also known as SheHacksPurple, is the best-selling author of 'Alice and Bob Learn Application Security'. She is also the founder of We Hack Purple, an academy, community and podcast that teaches everyone to create secure software.

Twitter: [@shehackspurple](#)

Description:

Quite often when we read best practices we are told 'what' to do, but not the 'why'. When we are told to ensure there are no false positives in the pipeline, the reason seems obvious, but not every part of DevOps is that intuitive, and not all 'best practices' make sense on first blush. Let's explore tried, tested, and failed methods, and then flip them on their head, so we know not only what to do to avoid them, but also why it is important to do so, with these DevSecOps WORST practices.

[Return to Index](#) - Add to  - ics [Calendar](#) file

TCV - Saturday - 16:00-17:59 PDT

Title: Diameter CTF

When: Saturday, Aug 12, 16:00 - 17:59 PDT

Where: Flamingo - Virginia City - Telecom Village - [Map](#)

Speakers: Akib Sayyed, Zibran Sayyed


SpeakerBio: Akib Sayyed , Director at Matrix Shell Technologies Prviate Limited

No BIO available

SpeakerBio: Zibran Sayyed , Sr. Security Consultant Telecom

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

TCV - Saturday - 11:00-12:59 PDT

Title: Diameter Workshop

When: Saturday, Aug 12, 11:00 - 12:59 PDT

Where: Flamingo - Virginia City - Telecom Village - [Map](#)

Speakers: Akib Sayyed, Zibran Sayyed


SpeakerBio: Akib Sayyed , Director at Matrix Shell Technologies Prviate Limited

No BIO available

SpeakerBio: Zibran Sayyed , Sr. Security Consultant Telecom

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

TCV - Saturday - 14:30-15:59 PDT

Title: Diameter Workshop

When: Saturday, Aug 12, 14:30 - 15:59 PDT

Where: Flamingo - Virginia City - Telecom Village - [Map](#)

Speakers: Akib Sayyed, Zibran Sayyed


SpeakerBio: Akib Sayyed , Director at Matrix Shell Technologies Prviate Limited

No BIO available

SpeakerBio: Zibran Sayyed , Sr. Security Consultant Telecom

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Digital Forensics and Incident Response Against the Digital Darkness: An Intro to Forensicating Evil
(Pre-Registration Required)

When: Saturday, Aug 12, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers:Michael "S3curityNerd" Register,Michael "mR_F0r3n51c5" Solomon

SpeakerBio:Michael "S3curityNerd" Register

Michael Register, known as S3curityNerd, with 7 years of combined experience in IT, Networking, and Cybersecurity. He holds multiple certifications and actively conducts post-exploitation research to enhance threat hunting operations.

SpeakerBio:Michael "mR_F0r3n51c5" Solomon

Michael Solomon, also known as mR_F0r3n51c5, is a Threat Hunter with over 12 years of experience in Cyber Operations, Digital Forensics & Incident Response (DFIR), and Threat Hunting. His passion lies in helping to shape the next generation of cybersecurity analysts for a safer tomorrow.

Description:

Are you ready to step into the shoes of a cybersecurity or incident response analyst? Whether you're new to investigation or looking to take your analysis skills to the next level, we've got an exciting opportunity for you! Join mR_F0r3n51c5 and S3curityNerd for a four-hour class that will take you on a journey through the world of malware analysis and investigation.

In today's ever-evolving threat landscape, malware continues to be a weapon of choice for various types of threat actors. Our class leverages forensic and malware analysis fundamentals to teach students how to investigate a compromised Windows system. To ensure the most up-to-date learning experience, the class authors have carefully selected fresh malware samples trending in 2023.

By the end of this class, you'll have the skills to: - Build analysis skills that leverage complex scenarios and improve comprehension - Practically acquire data in a forensically sound manner - Identify common areas of malware persistence - Gather evidence and create a timeline to characterize how the system was compromised - Participate in a hand-to-keyboard combat capstone where you'll be given an image of a compromised Windows system and demonstrate your newly acquired analysis skills.

Don't miss this opportunity to gain hands-on experience and take your analysis skills to the next level. Join us and discover the exciting world of forensic analysis and investigation!

Skill Level: Intermediate


Prerequisites for students:

- Not defined

Materials or Equipment students will need to bring to participate: - Students will be required to download material (e.g., Virtual Machine). Students will be given a URL for download access. - Regarding the downloaded virtual machines, these should be imported into your virtual machine software and ready before the start of class. If any additional technical support is needed, the instructors will make themselves available online. - Students must have a laptop that meets the following requirements: - A 64-bit CPU running at 2GHz or more. The students will be running one virtual machine on their host laptop. - Have the ability to update BIOS settings. Specifically, enable virtualization technology such as "Intel-VT." - The student must be able to access their system's BIOS if it is password protected. This is in case of changes being necessary. - 8 GB (Gigabytes) of RAM or higher

- At least one open and working USB Type-A port - 50 Gigabytes of free hard drive space, allowing you the ability to host the VMs we distribute - Students must have Local Administrator Access on their system. - Wireless 802.11 Capability - A host operating system that is running Windows 10+, Linux, or macOS 10.4 or later. - Virtualization software is required. The supplied VMs have been built for out-of-the-box comparability with VMWare Workstation or Player. Students may use

other software if they choose, but they may have to troubleshoot unpredictable issues. Instructors cannot guarantee compatibility with all virtualization software suites. At a minimum, the following VM features will be needed: - NATted networking from VM to Internet - Copy and Paste of text and files between the Host machine and VM

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Digital Media Authentication - A Toolkit for Journalists in the Fight Against Misinformation with Cryptographic Tools

When: Friday, Aug 11, 15:30 - 16:30 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Adam Rose , COO at Starling Lab for Data Integrity

Adam Rose is COO at the Starling Lab for Data Integrity, which was co-founded by Stanford University and USC Shoah Foundation. The lab explores the intersection of Web3 technologies with human rights, focusing on three practice areas: journalism, law and history. Through real-world case studies, they help practitioners to implement open-source technologies that can authenticate and preserve digital records. The lab has helped publishers to establish proof that images haven't been manipulated, and saved authenticated recordings of webpages at risk of disappearing. Starling's recent projects have received honors from the American Society of Magazine Editors, News Emmy Awards, National Press Club, National Press Photographers Association, and Overseas Press Club of America. Adam previously worked in media for two decades, including CBS/Paramount+, HuffPost, LA Times and LAist. He volunteers as press rights chair for the Los Angeles Press Club and successfully lobbied for legislation in California to protect journalists from arrest at protests.

Description:

Humanity is producing more content than at any point in history. Generative AI is poised to accelerate that trend. Our collective stream of information is surging, but all too often it's filled with misinformation. As audiences and fact checkers confront these muddied waters, could there be solutions back upstream? Researchers are testing innovative ways to authenticate digital records at their origin, establishing the time, date and location of their creation. With enhanced provenance we can establish a new resilient form of authenticity with cryptography, and decentralized systems. These methods have been used to establish trust in critical records like photos and web archives, and recently used in stories published by Reuters, Rolling Stone, Associated Press, Inside Climate News, and Bay City News. The techniques are even finding their way into legal submissions to prosecutors at the International Criminal Court and helping preserve the testimony of the survivors of genocide. Several promising solutions are available in free and open-source apps that you can install on your phone or computer browser today, and a number of emerging consumer products could help professionals to bolster trust in their own digital records. The workshop will provide case studies that can help explain these technologies to general audiences, with authentication being done on digital assets from today's phones and digital cameras -- and even 30-year-old film. It will also look at ways for journalists (and citizen journalists) to use these tools to capture authenticated assets or explore the provenance of assets with content credentials.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DISARM Workshop

When: Friday, Aug 11, 12:30 - 13:20 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

Speakers: Charles Smith, Dan Meidenbauer

SpeakerBio: Charles Smith

Charles Smith is a cybersecurity researcher at Johns Hopkins University Applied Physics Lab (JHU/APL), where he focuses on the intersection of cyber and information operations and their impact on national security. Charles spent the first fourteen years of his career as an officer in the U.S. Army, and the recipient of numerous awards and badges including the Ranger Tab, Combat Infantry Badge, and Purple Heart. He deployed five times as both an infantry officer and intelligence officer to Iraq and Afghanistan, and was selected to serve as an intelligence officer for the 2nd Battalion, 75th Ranger Regiment. He served his last four years in uniform at US Cyber Command, where he led intelligence support to the defense of the 2020 elections. Prior to joining JHU/APL, Charles also worked at Twitter on trust and safety response to crises. Charles holds a bachelor's of science in Business Administration from Bucknell University, and a Masters of Strategic Intelligence from National Intelligence University.

SpeakerBio: Dan Meidenbauer

Dan Meidenbauer is an experienced cyber systems engineer, electrical/nuclear engineering professional, and program manager with specific expertise in information operations, military cyber operations, critical infrastructure protection, cyber physical systems, cyber systems engineering/analysis/policy, electro-mechanical equipment development, and naval nuclear systems integration. For the past ten years he has served as a cyber systems engineering researcher/strategist at Johns Hopkins University Applied Physics Laboratory (JHU/APL) and as a Cryptologic Warfare Officer (CWO) in the U.S. Navy Reserve. He has seven years of active-duty military experience as a Naval Reactors Engineer and CWO. Dan is a strategic leader serving operational and technical research contributions with additional skills in national security strategy development/policy, research/technical leadership, and applied scientific strategy. He is a graduate of Virginia Tech with a B.S. in Electrical and Computer Engineering and holds a Master's in Engineering Management/Systems from Old Dominion University, an M.A. from the U.S. Naval War College in Defense and Strategic Studies, and a master's equivalency in naval nuclear engineering from the Bettis Reactor Engineering School. He is currently selected for Commander in the U.S. Navy Reserve.

Description:

Our objectives for our presentation will be to: provide an introduction to the DISARM foundation's framework, STIX bundles, and OPENCTI, and demonstrate how STIX bundles/OPENCTI can provide indications and warning of IO campaigns, and show how this is relevant to the civic integrity community. For audience participation, we will be conducting a simplified version of the tabletop exercise we just ran using an online polling tool to gather results and provide the audience a chance to upvote ideas they find most successful. We will aim to run through 3 different polling rounds, and allow 15 mins at the end of wrap up time.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Discovering Shadow Vulnerabilities in Popular Open-Source Projects: A Reverse-Fuzzing Journey

When: Saturday, Aug 12, 11:45 - 12:30 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

Speakers: Gal Elbaz, Guy Kaplan

SpeakerBio: Gal Elbaz

Co-founder & CTO at Oligo Security with 10+ years of experience in vulnerability research and practical hacking. He previously worked as a Security Researcher at CheckPoint and served in the IDF Intelligence. In his free time, he enjoys playing CTFs.

Twitter: [@GalElbaz1](#)

SpeakerBio: Guy Kaplan

Guy Kaplan is a Security Researcher in the CTO Office of Oligo Security with more than a decade of experience in software development and vulnerability research.

Twitter: [@gkpln3](#)

Description:

In a world full of vulnerabilities, there is an untold story of those libraries that are insecure by design. For example, libraries that by using them in a certain way, the application could be compromised. Not all libraries' security issues are treated as vulnerabilities and addressed with a patch or CVE, hence addressed with minor documentation warnings at best. These vulnerabilities pose a significant risk to organizations as they are nearly impossible to detect, we named them "Shadow Vulnerabilities".

We discovered a new shadow vulnerable code pattern in a widely used OSS library and wondered who might be vulnerable.

We developed a tool that automatically analyzed more than 100k repositories to determine whether each repository is vulnerable and prioritized them based on their potential to create vast damage. We were able to validate the exploitability of hundreds of high-profile targets such as Apache Cassandra, Prometheus, PyTorch, and many more...

In this presentation, we will review the discovered vulnerabilities, and discuss the challenges of scaling the triage, validating exploitation, and building a reliable infrastructure. We will use Apache Cassandra to demonstrate how we validated the attack vector for each target, sharing the exploitation details of the critical RCE we found, and its implications on a database-as-a-service used by multiple cloud providers.

Although reporting and working with OSS projects security teams on resolving these issues was addressed quickly, still no CVE was assigned. Both project owners and library owners claimed the responsibility to use it "safely" is on the users themselves. The result is that most users are vulnerable and have no process to fix this or even be aware of it.

We believe it is vital to raise community awareness of shadow vulnerabilities, as we only scratched the surface with one example out of many more that are still out there.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MIV - Saturday - 10:00-10:59 PDT

Title: Disincentivizing misinformation: co-create a new platform business model

When: Saturday, Aug 12, 10:00 - 10:59 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Vardon Hamdiu , Co-Lead at Sparkable

Vardon Hamdiu is the Co-Lead of Sparkable, a nonprofit organization working on a new platform model to counter misinformation, hate, and other harms connected to the advertisement business model. In the last decade, he worked in the communications of a Swiss President, lived in South Africa for half a year, and worked with refugees. During that time, he realized the enormous disconnect between the information we consume online and the lived reality of so many people around the world. This made him start Sparkable, a community-led effort to create a better information environment.

Description:

What are the economic incentives driving misinformation, and what does the advertisement/engagement business model have to do with it? If we could create a new model for our information ecosystem, how would we ensure civic integrity and security by design?

Join this workshop to co-create a new incentive system for open platforms focused on people, not profit.

In the workshop, you will modify and improve this new system in two different tracks: integrity and research/design. It will cover a wide range of interests, including trust & safety, cybersecurity, media, content creation, UX, and systems design. You can choose the track most relevant to you and contribute ideas, questions, and feedback that will directly inform the Sparkable roadmap. No previous knowledge is required.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Dissecting Deception: The Role of Twitter in U.S. Political Discourse

When: Friday, Aug 11, 13:00 - 13:30 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

Speaker Bio: Travis Allen

No BIO available

Description:

This talk will take you back in time to 2015, the year I dove headfirst into the swirling vortex of American political misinformation on Twitter. Having navigated three presidential administrations, and amassing over 250,000 followers on Twitter, I've seen firsthand how misinformation in American politics has evolved since the election of Donald Trump. I'll recount the strategies that led to the growth of my account and the circumstances under which it was ultimately blocked by President Trump. Prepare to unravel the inner workings of political misinformation networks on Twitter — their operations, their financing, and how they go viral. We'll delve into how influencers, celebrities, PACs, campaigns, politicians, the media, and candidates orchestrate their efforts to disseminate their messaging. It will mark the differences in the American social media landscape between the right and the left. This talk will also illuminate how contemporary political movements promulgate their messages and counter disinformation. I will tie all of these strategies, both offensive and defensive, to the DISARM framework.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Divided We Fall

When: Friday, Aug 11, 13:20 - 14:05 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio:Michael Moore

After volunteering to be a poll worker, Michael Moore developed a passion for Election Security. He was the first Information Security Officer for the Maricopa County Recorder's office and is now the first Chief Information Security Officer for the Arizona Secretary of State. Michael believes it is only through effective federal, state, and local government partnerships, as well as assistance from trusted vendors that we can protect our democracy and fulfill our duty to the American voter. The greatest threats to elections are MDM and the resulting insider threat caused by radicalized citizens. The best protection against these threats is combating lies with the truth, developing secure and resilient systems that prevent attacks whenever possible, allow for detections of compromise and facilitate accurate and rapid recovery. Michael has pushed forward these initiatives in his own organizations as well as across the Elections community. Michael is an alumnus of Arizona State University with a B.S. in Mathematics and a B.A. in Education and is a CISSP, Certified Election Official (CEO) and Certified Public Manager (CPM).

Twitter: [@Secur3Elections](#)

Description:

There has been a massive exodus of skilled Election Officials since the 2020 General Election. In this presentation we will show actual death threats to Election Officials, the repercussions, and our threat reporting process. Lastly, we'll inform the audience on how they can do their part - fight MDM, demand intellectual integrity from themselves and those around them, normalize requesting citations, volunteer to work for elections and speak up if something seems wrong!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Saturday - 13:30-13:59 PDT

Title: Domain Fronting Through Microsoft Azure and CloudFlare: How to Identify Viable Domain Fronting Proxies

When: Saturday, Aug 12, 13:30 - 13:59 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

Speakers: Charles Miller, Michael Brown, Michael Pelosi

SpeakerBio: Charles Miller

No BIO available

SpeakerBio: Michael Brown

No BIO available

SpeakerBio: Michael Pelosi

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Doomed to repeat the past: classical hardware exploits made quantum

When: Friday, Aug 11, 14:00 - 14:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

SpeakerBio:Jamie Friel

No BIO available

Description:

With quantum computing we have an entirely new model of computing and its execution. Whilst this is exciting for algorithm developers looking to change the world, it's equally exciting to hardware hackers looking for a new challenge. Here we'll discuss some of the unique elements of quantum computing and how they might have an impact on the future of hardware security.

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Friday - 14:00-14:30 PDT

Title: Doors, Cameras, and Mantraps: Oh, my!

When: Friday, Aug 11, 14:00 - 14:30 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

SpeakerBio:Dylan Baklor

No BIO available

Description:

This is a general talk about the nuts and bolts of Physical Security. Not a lockpicking talk.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DotNet Malware Analysis Masterclass (Pre-Registration Required)

When: Thursday, Aug 10, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

SpeakerBio:Max 'Libra' Kersten , Malware Analyst at Trellix

Max Kersten is a malware analyst, blogger, and speaker who aims to make malware analysis more approachable for those who are starting. In 2019, Max graduated cum laude with a bachelor's in IT & Cyber Security, during which Max also worked as an Android malware analyst. Currently, Max works as a malware analyst at Trellix, where he analyses APT malware and creates open-source tooling to aid such research. Over the past few years, Max spoke at international conferences, such as Black Hat Arsenal (USA, EU, MEA, Asia), Botconf, Confidence-Conference, HackYeahPL, and HackFestCA. Additionally, he gave guest lectures and workshops for several universities and private entities.

Twitter: [@Libranalysis](#)

Description:

DotNet based malware originally started out as a novelty, but has shown it is here to stay. With DotNet malware being used by APT actors and script kiddies, and anything in-between, it is safe to say that one will encounter it sooner rather than later. This four-hour workshop primarily focuses on the analyst mindset and fundamental knowledge, including topics such as loaders, unpacking, obfuscation, DotNet internals, and (un)managed hooks. In short, one will learn how to analyse DotNet malware, and write automatic unpackers. As such, this class is perfect for aspiring and beginning analysts, while also providing background information and additional techniques for intermediate analysts.

The workshop's materials will partially consist of actual malware samples, the precautions for which will be explained in-detail during the workshop, ensuring the safety and integrity of the systems of the attendees. A laptop with a preinstalled VM based Windows 10 trial, along with the community edition of Visual Studio (2019 or later) and the DotNet Framework runtime for version 3.5 and later. Other tools, such as dnSpyEx, de4dot, and DotDumper, can be downloaded during the workshop, as these are insignificant in size.

Knowing how to read VB.NET/C is a **prerequisite**. **Being able to write in C** is preferred, but the workshop can be followed without being able to, although a part of the exercises cannot be completed without it.

Questions about the workshop can be asked via my open Twitter DMs: [@Libranalysis](#) (<https://twitter.com/Libranalysis>)

Skill Level: Beginner to Intermediate

Prerequisites for students:

- Have sufficient disk space and RAM to run one Windows 10 VM, along with a few gigabyte additional extra space
- Be able to understand VB.NET/C# and preferably (though not mandatory) be able to write in either of those languages
- Be able to run a Windows 10 VM
- Have a Windows 10 VM preinstalled in a virtual environment of choice (i.e., VirtualBox, VMWare)
- Have Visual Studio (2019 or later) installed, along with the DotNet Framework 3.5 and higher
- Analysis tools will be provided (i.e. open-source tools such as dnSpyEx) as their file size is minimal
- Malware samples and exercises will be provided on-location

Materials or Equipment students will need to bring to participate: A laptop capable of running one Windows 10 VM, with the above-mentioned prog2rams installed, and sufficient free disk space

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Dracon

When: Friday, Aug 11, 12:00 - 13:55 PDT

Where: Caesars Forum - Accord Boardroom - Demo Labs - [Map](#)

SpeakerBio: Spyros Gasteratos

Spyros is a Security Engineer with over a decade of experience in various organisations. Currently, he is helping Fintechs mature their AppSec programmes through automation. He maintains several Open Source projects including Dracon, opencre.org and others. Also, he is heavily involved with the OWASP foundation helping with outreach and diversity efforts.

Twitter: [@0xfde](#)

Description:

Dracon is an open-source Application and Cloud security automation framework that helps organizations create security workflows and improve their security posture. Dracon can run a wide range of security tools against any target, and it can deduplicate and enrich the results of those tools with contextual or regulatory information. Dracon can then send the enriched results to any visualization or data processing tool. Here are some of its key features: Automated security workflows: Dracon can automate the execution of security tools and the aggregation of results, which saves both time and effort. Scalable and flexible: Dracon is both scalable and flexible with a wide array of existing integrations and more on the way, Dracon integrates seamlessly with any existing toolset. Open source: Dracon is open-source platform, which means that it is free to use and modify.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Dress Code - Analysis of the current status of the Content Security Policy

When: Saturday, Aug 12, 13:30 - 14:15 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

SpeakerBio: Felipe Molina

Felipe Molina is a Spaniard hacker working in the SensePost Team at Orange Cyberdefense. He loves Andalusia, to hack, drink beer, barbecue with family and friends, deep diving into new software to find cool vulnerabilities.

Twitter: [@felmoltor](#)

Description:

Content Security Policy (CSP) has been in support by most modern browsers for a while now. The RFC of the first version was released in 2014. Almost 10 years later, and with version 3 recently released, a far-reaching study of CSP deployment across the Internet was due.

The top one million most popular sites were scanned and their CSP related headers were stored. The values of the CSP headers were analysed to answer several questions. How popular is this security measure nowadays. What are common pitfalls and misconfigurations within CSP headers. How often do sites enable reporting of violations to take a more proactive approach? Do sites blindly trust third parties such as content delivery networks and how can this trust be abused.

This talk will cover the results of the analysis against real world data and answer the previous questions. Additionally, it will present practical exploitation examples and provide with effective hardening and mitigation to the detected weaknesses.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: Dungeons@Defcon

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

D@D is a table-top/RPG themed puzzling campaign for teams of 1-4 players. As part of the campaign, teams will unravel crypto challenges, solve physical puzzles, and do other side-quests that will have them interacting with different components of the Defcon community (villages, goons, NPCs, local wildlife, trolls, etc.) to earn points and progress through a narrative. The theme changes each year, but typically is based loosely on a popular table-top game that fits the theme for Defcon. Teams learn how to work cooperatively to solve large puzzles, and learn how to solve puzzles that they may have seen in CTFs, escape rooms, or other puzzle venues. The contest is designed to be accessible to all technical levels and all ages.

Pre-registration will occur online the week before con (announced via Twitter) as well as Friday morning at 10 in person, first come first served until we have enough teams filled. Contest will start at 12:00 on Friday

--

Kids are welcome. The first year Dungeons @ DEF CON ran, two kids with the help of their fathers won a black badge.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

Title: Dungeons@Defcon

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

D@D is a table-top/RPG themed puzzling campaign for teams of 1-4 players. As part of the campaign, teams will unravel crypto challenges, solve physical puzzles, and do other side-quests that will have them interacting with different components of the Defcon community (villages, goons, NPCs, local wildlife, trolls, etc.) to earn points and progress through a narrative. The theme changes each year, but typically is based loosely on a popular table-top game that fits the theme for Defcon. Teams learn how to work cooperatively to solve large puzzles, and learn how to solve puzzles that they may have seen in CTFs, escape rooms, or other puzzle venues. The contest is designed to be accessible to all technical levels and all ages.

Pre-registration will occur online the week before con (announced via Twitter) as well as Friday morning at 10 in person, first come first served until we have enough teams filled. Contest will start at 12:00 on Friday

--

Kids are welcome. The first year Dungeons @ DEF CON ran, two kids with the help of their fathers won a black badge.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Easy EASM - the zero dollar attack surface management tool

When: Saturday, Aug 12, 14:00 - 14:25 PDT

Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio: Jason Haddix , CISO and “Hacker in Charge” at BuddoBot

Jason Haddix is the CISO and “Hacker in Charge” at BuddoBot, a world-class adversary emulation consultancy. He's had a distinguished 15-year career in cybersecurity previously serving as the CISO of Ubisoft, Head of Trust/Security/Operations at Bugcrowd, Director of Penetration Testing at HP, and Lead Penetration Tester at Redspin. He has also held positions doing mobile penetration testing, network/infrastructure security assessments, and static analysis. Jason is a hacker and bug hunter to the core, and he is ranked 51st all-time on Bugcrowd's leaderboards. Currently, he specializes in recon and web application analysis. Jason has also authored many talks on offensive security methodology, including speaking at cons such as; DEF CON, Black Hat, OWASP, RSA, Nullcon, SANS, IANS, BruCon, Toorcon, and many more. Jason currently lives in Colorado with his wife and three children.

Twitter: [@jhaddix](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Friday - 12:00-17:59 PDT

Title: EFF Benefit Poker Tournament at DEF CON 31 - Poker

When: Friday, Aug 11, 12:00 - 17:59 PDT

Where: Other/See Description


Description:

Betting on Your Digital Rights: 2nd Annual EFF Benefit Poker Tournament at DEF CON 31

When: Friday August 11, 12:00 (11:00 for the pre-tournament poker clinic) Where: Offsite. Horseshoe Poker Room
Stay tuned at <https://www.eff.org/poker> for more details.

We're going all in on internet freedom. Take a break from hacking the Gibson to face off with your competition at the tables—and benefit the Electronic Frontier Foundation! Your buy-in is paired with a donation to support EFF's mission to protect online privacy and free expression for all. Play for glory. Play for money. Play for the future of the web. Seating is limited, so reserve your spot today. <https://www.eff.org/poker>

We will offer a pre-tournament clinic to help people get a refresher on poker so they feel comfortable. This contest will be held outside the main conference area; it must be held in the Horseshoe Poker Room per the Nevada Gaming Commission.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Friday - 11:00-11:59 PDT

Title: EFF Benefit Poker Tournament at DEF CON 31 - Pre-tournament clinic

When: Friday, Aug 11, 11:00 - 11:59 PDT

Where: Other/See Description

Description:

Betting on Your Digital Rights: 2nd Annual EFF Benefit Poker Tournament at DEF CON 31

When: Friday August 11, 12:00 (11:00 for the pre-tournament poker clinic) Where: Offsite. Horseshoe Poker Room
Stay tuned at <https://www.eff.org/poker> for more details.

We're going all in on internet freedom. Take a break from hacking the Gibson to face off with your competition at the tables—and benefit the Electronic Frontier Foundation! Your buy-in is paired with a donation to support EFF's mission to protect online privacy and free expression for all. Play for glory. Play for money. Play for the future of the web. Seating is limited, so reserve your spot today. <https://www.eff.org/poker>

We will offer a pre-tournament clinic to help people get a refresher on poker so they feel comfortable. This contest will be held outside the main conference area; it must be held in the Horseshoe Poker Room per the Nevada Gaming Commission.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Saturday - 18:00-21:59 PDT


Title: EFF Tech Trivia

When: Saturday, Aug 12, 18:00 - 21:59 PDT

Where: Caesars Forum - Forum - 121-123, 129, 137 - Chillout - [Map](#)

Description:

EFF's team of technology experts have crafted challenging trivia about the fascinating, obscure, and trivial aspects of digital security, online rights, and Internet culture. Competing teams will plumb the unfathomable depths of their knowledge, but only the champion hive mind will claim the First Place Tech Trivia Prize (TBD) and EFF swag pack. The second and third place teams will also win great EFF gear.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Ek47 – Payload Encryption with Environmental Keys

When: Friday, Aug 11, 12:00 - 13:55 PDT

Where: Caesars Forum - Committee Boardroom - Demo Labs - [Map](#)

Speakers:Kevin “Kent” Clark, Skyler Knecht

SpeakerBio:Kevin “Kent” Clark , Red Team Instructor at BC Security

Kevin “Kent” Clark is a Security Consultant with TrustedSec and Red Team Instructor with BC Security. His previous work includes Penetration Testing and Red Team Operator, focusing on initial access and active directory exploitation. Kevin contributes to open-source tools such as PowerShell Empire and publishes custom security toolkits such as Badrats and WindowsBinaryReplacements. Kevin authors a cybersecurity blog at <https://henpeebin.com/kevin/blog>.

SpeakerBio:Skyler Knecht

Skyler Knecht is a Information Security Specialist who performs a variety of security assessments including, phishing, internal/external penetration tests and red teaming. Skyler Knecht worked as a consultant for three years and has recently pivoted to an internal team at Navy Federal Credit Union. Skyler Knecht is continually researching all fields of study but is primarily focused developing offensive tooling such as command and control frameworks and implants.

Description:

Ek47 is a payload encryptor that leverages user-selected environmental keys associated with a target execution context. In the absence of these environmental keys, Ek47 payloads will not decrypt and execute. This creates a strong resistance to automated/manual analysis and reverse engineering of payloads. Ek47 supports many different environmental keys such as current user, domain, computer name, installed programs, and more. Additionally, Ek47 supports packing payloads of .NET assemblies, unmanaged DLLs, and raw shellcode. Ek47 payloads are themselves .NET assemblies and can be uploaded to disk or executed reflectively via any execute-assembly method. By default, a standard AMSI/ETW bypass is executed before the main payload is executed, but Ek47 makes it easy to add custom bypasses for more advanced evasion functionality. Additional miscellaneous features are provided such as entropy management, PE header stomping, and generation of service executables.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Election Preparation: 2024

When: Friday, Aug 11, 16:30 - 17:30 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

Speakers: Ashlee Benge, Jake Braun, John Odum, Michael Moore

SpeakerBio: Ashlee Benge

Ashlee is an astrophysicist turned security researcher whose career has spanned across roles in detection engineering, threat hunting, analytics, and security outreach. In her current role as Director of Threat Intelligence Advocacy at ReversingLabs, she focuses on efficient use and mobilization of threat research outputs across the business and in public outreach. She has previously held roles in threat hunting and research at Cisco Talos, the ThreatGrid Research and Efficacy team, and ZeroFOX. In addition to degrees in Chemistry and Physics, she also holds an MBA from the Smith School of Business.

Twitter: [@ashlee_benge](#)

SpeakerBio: Jake Braun

Jake Braun currently serves as the Acting Principal Deputy National Cyber Director. Most recently, Jake was appointed as a Senior Advisor to the DHS Management Directorate, which oversees all operations for the department. Previously, Jake served as the Executive Director for the University of Chicago's Cyber Policy Initiative where he worked at the center of policy, technology, and national security. In addition to his role at the University of Chicago, Jake also co-founded and served as the CEO of Cambridge Global Advisors, a national security consulting firm with offices here in Chicago. He was also co-founder of the DE CON Voting Machine Hacking Village where he co-authored two award-winning works on election security and has also recently published the critically acclaimed book, "Democracy in Danger: How Hackers and Activists Exposed Fatal Flaws in the Election System", on the same topic. Previous to that, he served in the Obama Administration as the Director of White House and Public Liaison for the Department of Homeland Security. He holds an MA in International Relations from Troy St. University, an MA in Education from National-Louis University in Chicago, and a BA in Philosophy from Loyola University of Chicago.

Twitter: [@jakehbraun](#)

SpeakerBio: John Odum

John Odum has served as the city clerk and election administrator of Vermont's capital city of Montpelier for 11 years. He is a Certified Ethical Hacker and Certified Network Defense Architect, as well as a Certified Municipal Clerk. John holds a Certificate in Election Administration from the University of Minnesota Humphrey School of Public Affairs and has served on the Advisory Board of the Cyber Policy Initiative at the University of Chicago Harris School of Public Policy. John has written on election security and politics for the Guardian (online), Huffington Post, Governing, and others. He previously worked in electoral politics for many years, including serving as the statewide Field Director for the Clavelle for Governor campaign in Vermont.

Twitter: [@jodum](#)


SpeakerBio: Michael Moore

After volunteering to be a poll worker, Michael Moore developed a passion for Election Security. He was the first Information Security Officer for the Maricopa County Recorder's office and is now the first Chief Information Security Officer for the Arizona Secretary of State. Michael believes it is only through effective federal, state, and local government partnerships, as well as assistance from trusted vendors that we can protect our democracy and fulfill our duty to the American voter. The greatest threats to elections are MDM and the resulting insider threat caused by radicalized citizens. The best protection against these threats is combating lies with the truth, developing secure and resilient systems that prevent attacks whenever possible, allow for detections of compromise and facilitate accurate and rapid recovery. Michael has pushed forward these initiatives in his own organizations as well as across the Elections community. Michael is an alumnus of Arizona State University with a B.S. in Mathematics and a B.A. in Education and is a CISSP, Certified Election Official (CEO) and Certified Public Manager (CPM).

Twitter: [@Secur3Elections](#)

Description:

In this session we will cover what can be done to secure elections leading up to 2024. With two actual election officials on the panel, plus an expert in software supply chain, we will get to hear strategies on election preparation from different perspectives across the election industry. Panelists will discuss what can be done in preparation of the 2024 election season and how public and public/private partnerships are securing election infrastructure in its entirety. Panelists will discuss what initiatives are directly derivable from recent federal government cyber security initiatives. They will give insight into what each of their industries are doing now and what they plan to do in the future to ensure secure democratic processes.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: ELECTRONizing macOS privacy - a new weapon in your red teaming armory

When: Saturday, Aug 12, 09:00 - 09:20 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

SpeakerBio: Wojciech Reguła , Principal Security Consultant at SecuRing

Wojciech is a Principal Security Specialist working at SecuRing. He specializes in application security on Apple devices. Wojciech created the iOS Security Suite - an opensource anti-tampering framework. Bugcrowd MVP, found vulnerabilities in Apple, Facebook, Malwarebytes, Slack, Atlassian, and others. In free time he runs an infosec blog -

<https://wojciechregula.blog>. Shared research on among others Black Hat (Las Vegas, USA), Objective by the Sea (Hawaii, USA), AppSec Global (Tel Aviv, Israel), AppSec EU (London, United Kingdom), CONFidence (Cracow, Poland), BSides (Warsaw, Poland).

Twitter: [@_r3ggi](#)

Description:

MacOS is known for an additional layer of privacy controls called TCC - Transparency, Consent, and Control (TCC) that restricts access to sensitive personal resources: documents, camera, microphone, emails, and more. Granting such access requires authorization, and the mechanism's main design concern was clear user consent.

Despite many vulnerabilities in that mechanism found in the past, using 0-days during red teaming engagements is impractical. Apple fixes TCC vulnerabilities but red teams still have to get access to files saved on the victim's desktop or be able take a screenshot.

What if I tell you that there are many open doors to resolve all the TCC problems that are already installed on your target machines?! Electron apps are everywhere. And you probably heard the joke that: 'S' in Electron stands for security.

In this talk I will share a new tool that, by abusing Electron default configuration, allows executing code in the context of those Electron apps and thus inherit their TCC permissions.

The audience will leave with a solid understanding of the macOS privacy restrictions framework (TCC) and its weaknesses. The part of the audience interested in macOS red teaming will also get to know my new, free and open source tool. Blue teams on the stage will also see some ideas regarding detections.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Sunday - 11:30-11:59 PDT

Title: Elevators 101

When: Sunday, Aug 13, 11:30 - 11:59 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

SpeakerBio: Karen

As a founding member of the Physical Security Village, Karen has always been eager to spread awareness of physical security vulnerabilities. Karen works with GGR Security as a Security Risk Assessor.

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Elon, Twitter and the PIA: How not to achieve privacy in aviation

When: Saturday, Aug 12, 13:30 - 13:55 PDT


Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio: Martin Strohmeier

No BIO available

Description:

In 2022, aviation tracking privacy (or the lack thereof) has truly entered the global mainstream, with operational security and climate shaming of private jets suddenly discussed all over the world. Following up on previous work presented at the Aerospace Village, we will conduct a deep dive into how we arrived in this position, why nothing has worked so far, and how we need to change our thinking in order to achieve any meaningful privacy in aviation.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Email Detection Engineering and Threat Hunting Inbox (Pre-Registration Required)

When: Saturday, Aug 12, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers: Alfie Champion, Josh Kamdjou

SpeakerBio: Alfie Champion

Alfie specializes in the delivery of attack detection and adversary emulation services, actively contributing education content, tooling and blogs to further the industry. He has previously worked with organisations across multiple industry verticals to uplift and validate their detective capability through red or purple team engagements, and now leads the global adversary emulation function at a FTSE 250 company. He has previously spoken at BlackHat USA, RSA and Blue Team Con 2022, among others, and is the co-founder of DelivrTo.

SpeakerBio: Josh Kamdjou

Josh has been doing offensive security-related things for the past 12 years. He's spent most of his professional career breaking into networks via spear-phishing and other methods, and building software for both the public (Department of Defense) and private sectors. Josh is the Founder and CEO of Sublime Security, and in his private life enjoys weight lifting, Martial Arts, soccer, and spending time with his niece and nephew.

Description:

Email remains the #1 initial access vector for commodity malware and nation state actors. Historically, tackling email-based threats has been considered the purview of black-box vendor solutions, with defenders having limited scope (or tooling!) to swiftly and effectively respond to emerging attacker activity and novel offensive tradecraft.

In this workshop, attendees will be given detailed insight into the latest techniques used to deliver prevalent malware strains, including QakBot and Emotet, and will hunt through email data to identify this malicious activity, developing rules to detect and block these attacks.

Initially attendees will be introduced to the foundational technologies that enable threat hunting, detection engineering, and response in the email domain, before being given access to the email data of a fictitious company seeded with benign and real-world attack data. Throughout the day, participants will learn to hunt common phishing techniques including:

- VIP Impersonations
- HTML smuggling via links/attachments
- Malicious VBA macros
- OneNote / LNK file malware (attachments, and links to auto-downloads)
- PDF attachments with embedded links to malware (PDF -> URL -> ZIP -> WSF)
- Lookalike domains / homoglyph attacks
- Credential phishing
- Password protected archives
- Exploits (e.g. CVE-2023-23397, CVE-2021-40444)
- Fake invoices (Geek Squad)

Attendees will be guided through the rule creation process, utilizing free and open detection engines including Sublime and Yara, and will be introduced to the signals and email attributes that can be used to craft high-fidelity rules, including targeted user groups, sentiment analysis, sender domain age, and attachment analysis. Having completed the workshop, attendees will have a strong understanding of the tools and techniques at their disposal to defend their organizations from all manor of email threats.

Skill Level: Beginner. The training will cater to security practitioners with any level of technical experience. While a general understanding of email threats will be advantageous, all offensive and defensive techniques and tools in the training will be introduced at a foundational level and built on throughout the day.

Prerequisites for students:

- None

Materials or Equipment students will need to bring to participate: - Attendees should bring their own laptops in order to be hands-on, preloaded with Docker. Instructions to run the Docker images from Github will be shared. All tools used in this lab are free and/or open-source.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Saturday - 10:30-10:59 PDT

Title: EMBA - From firmware to exploit


When: Saturday, Aug 12, 10:30 - 10:59 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio:Michael Messner

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Embedded CTF

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: LINQ - 3rd flr - Evolution - Embedded Systems Village - [Map](#)

Description:

Embedded systems are everywhere in our daily lives, from the smart devices in our homes to the systems that control critical infrastructure. These systems exist at the intersection of hardware and software, built to accomplish a specific task. However, unlike general-purpose computers, embedded systems are typically designed for a particular use case and have limited resources. This makes them both challenging and fascinating to work with, especially from a security perspective.

The Embedded CTF contest is an exciting opportunity to explore the intricacies of these systems and test your skills in a competitive environment. Contestants are challenged to find vulnerabilities in the firmware or hardware and exploit them to gain access or control over the device. The contest offers a unique opportunity to explore embedded devices' inner workings and understand their design's security implications.

New devices will be dramatically introduced at set intervals throughout the competition, and point values will decrease over time. This keeps contestants guessing and on their toes, forcing them to adapt and use their skills to tackle new challenges. It also offers a chance to learn about different types of devices and how they function, broadening participants' knowledge and experience.

By participating in the contest, teams of up to 6 contestants can develop a deep understanding of how these systems operate and how to secure them against potential attacks. Additionally, the contest encourages participants to think outside the box and approach problems creatively, honing their problem-solving skills.

With the increasing integration of technology in our daily lives, embedded devices are becoming more ubiquitous. Whether you're a seasoned security professional or just starting in the field, this contest offers a chance to learn, test your skills, and have fun in a dynamic and competitive environment.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Embedded CTF

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: LINQ - 3rd flr - Evolution - Embedded Systems Village - [Map](#)

Description:

Embedded systems are everywhere in our daily lives, from the smart devices in our homes to the systems that control critical infrastructure. These systems exist at the intersection of hardware and software, built to accomplish a specific task. However, unlike general-purpose computers, embedded systems are typically designed for a particular use case and have limited resources. This makes them both challenging and fascinating to work with, especially from a security perspective.

The Embedded CTF contest is an exciting opportunity to explore the intricacies of these systems and test your skills in a competitive environment. Contestants are challenged to find vulnerabilities in the firmware or hardware and exploit them to gain access or control over the device. The contest offers a unique opportunity to explore embedded devices' inner workings and understand their design's security implications.

New devices will be dramatically introduced at set intervals throughout the competition, and point values will decrease over time. This keeps contestants guessing and on their toes, forcing them to adapt and use their skills to tackle new challenges. It also offers a chance to learn about different types of devices and how they function, broadening participants' knowledge and experience.

By participating in the contest, teams of up to 6 contestants can develop a deep understanding of how these systems operate and how to secure them against potential attacks. Additionally, the contest encourages participants to think outside the box and approach problems creatively, honing their problem-solving skills.

With the increasing integration of technology in our daily lives, embedded devices are becoming more ubiquitous. Whether you're a seasoned security professional or just starting in the field, this contest offers a chance to learn, test your skills, and have fun in a dynamic and competitive environment.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Embedded CTF

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: LINQ - 3rd flr - Evolution - Embedded Systems Village - [Map](#)

Description:

Embedded systems are everywhere in our daily lives, from the smart devices in our homes to the systems that control critical infrastructure. These systems exist at the intersection of hardware and software, built to accomplish a specific task. However, unlike general-purpose computers, embedded systems are typically designed for a particular use case and have limited resources. This makes them both challenging and fascinating to work with, especially from a security perspective.

The Embedded CTF contest is an exciting opportunity to explore the intricacies of these systems and test your skills in a competitive environment. Contestants are challenged to find vulnerabilities in the firmware or hardware and exploit them to gain access or control over the device. The contest offers a unique opportunity to explore embedded devices' inner workings and understand their design's security implications.

New devices will be dramatically introduced at set intervals throughout the competition, and point values will decrease over time. This keeps contestants guessing and on their toes, forcing them to adapt and use their skills to tackle new challenges. It also offers a chance to learn about different types of devices and how they function, broadening participants' knowledge and experience.

By participating in the contest, teams of up to 6 contestants can develop a deep understanding of how these systems operate and how to secure them against potential attacks. Additionally, the contest encourages participants to think outside the box and approach problems creatively, honing their problem-solving skills.

With the increasing integration of technology in our daily lives, embedded devices are becoming more ubiquitous. Whether you're a seasoned security professional or just starting in the field, this contest offers a chance to learn, test your skills, and have fun in a dynamic and competitive environment.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Friday - 10:00-17:59 PDT


Title: Embedded Device Security Workshops

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Embedded Device Security Workshops: two hands-on workshops showcasing common security vulnerabilities present in IoT/OT devices. These workshops will give you an opportunity to use a variety of device hacking tools and techniques to attack multiple components at varying layers of the stack, enabling a deeper understanding of device security.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Sunday - 10:00-13:59 PDT

Title: Embedded Device Security Workshops

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Embedded Device Security Workshops: two hands-on workshops showcasing common security vulnerabilities present in IoT/OT devices. These workshops will give you an opportunity to use a variety of device hacking tools and techniques to attack multiple components at varying layers of the stack, enabling a deeper understanding of device security.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Saturday - 10:00-17:59 PDT


Title: Embedded Device Security Workshops

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Embedded Device Security Workshops: two hands-on workshops showcasing common security vulnerabilities present in IoT/OT devices. These workshops will give you an opportunity to use a variety of device hacking tools and techniques to attack multiple components at varying layers of the stack, enabling a deeper understanding of device security.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Embedded Systems Village Activities

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: LINQ - 3rd flr - Evolution - Embedded Systems Village - [Map](#)

Description:

****ESV Badge****

The ESV Badge is a cool-looking shard PCB that will fit into the DEF CON badge shard holder, but also doubles as a hardware debugger with a built-in USB-Serial adapter. On sale at the village for \$60, but also available for free to CTF players that score a minimum number of points.

****Embedded CTF****

An approachable yet challenging CTF competition with a wide range of embedded devices and attacks.

Categories include:

- Physical
- Network
- RF
- Mobile (Powered by Corellium)
- Firmware
- Badge - custom challenges built into the ESV badge

****101 Labs****

A series of computer-based workshops that will guide you through the basics of hacking embedded devices. From extracting and analyzing firmware, exploiting command injections and more, these labs will introduce even the most noob to the world of embedded device hacking.

****Hands-on Hardware Hacking****

We've raided our local thrift stores and electronics recyclers and brought a whole bunch of embedded systems for you to try out the ESV badge on. Come pull memory chips off PCBs, dump memory, connect to UART consoles, and see what was left behind on these devices!

****LoRA Labs****

A hands-on and interactive lab using LoRa gateways where you will discover the noisy 915 MHz radio spectrum world.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Embedded Systems Village Activities

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: LINQ - 3rd flr - Evolution - Embedded Systems Village - [Map](#)

Description:

****ESV Badge****

The ESV Badge is a cool-looking shard PCB that will fit into the DEF CON badge shard holder, but also doubles as a hardware debugger with a built-in USB-Serial adapter. On sale at the village for \$60, but also available for free to CTF players that score a minimum number of points.

****Embedded CTF****

An approachable yet challenging CTF competition with a wide range of embedded devices and attacks.

Categories include:

- Physical
- Network
- RF
- Mobile (Powered by Corellium)
- Firmware
- Badge - custom challenges built into the ESV badge

****101 Labs****

A series of computer-based workshops that will guide you through the basics of hacking embedded devices. From extracting and analyzing firmware, exploiting command injections and more, these labs will introduce even the most noob to the world of embedded device hacking.

****Hands-on Hardware Hacking****

We've raided our local thrift stores and electronics recyclers and brought a whole bunch of embedded systems for you to try out the ESV badge on. Come pull memory chips off PCBs, dump memory, connect to UART consoles, and see what was left behind on these devices!

****LoRA Labs****

A hands-on and interactive lab using LoRa gateways where you will discover the noisy 915 MHz radio spectrum world.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Embedded Systems Village Activities

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: LINQ - 3rd flr - Evolution - Embedded Systems Village - [Map](#)

Description:

ESV Badge

The ESV Badge is a cool-looking shard PCB that will fit into the DEF CON badge shard holder, but also doubles as a hardware debugger with a built-in USB-Serial adapter. On sale at the village for \$60, but also available for free to CTF players that score a minimum number of points.

Embedded CTF

An approachable yet challenging CTF competition with a wide range of embedded devices and attacks.

Categories include:

- Physical
- Network
- RF
- Mobile (Powered by Corellium)
- Firmware
- Badge - custom challenges built into the ESV badge

101 Labs

A series of computer-based workshops that will guide you through the basics of hacking embedded devices. From extracting and analyzing firmware, exploiting command injections and more, these labs will introduce even the most noob to the world of embedded device hacking.

Hands-on Hardware Hacking

We've raided our local thrift stores and electronics recyclers and brought a whole bunch of embedded systems for you to try out the ESV badge on. Come pull memory chips off PCBs, dump memory, connect to UART consoles, and see what was left behind on these devices!

LoRA Labs

A hands-on and interactive lab using LoRa gateways where you will discover the noisy 915 MHz radio spectrum world.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Enhancing Cybersecurity Resilience in the Brazilian Healthcare Sector: A Novel Red Team and Blue Team Methodology

When: Saturday, Aug 12, 15:30 - 16:10 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

Speakers: Arthur Paixão, Diego Mariano

SpeakerBio: Arthur Paixão

Arthur: 14 years of experience, possesses expertise in offensive security and threat intelligence in the financial and healthcare sectors.

SpeakerBio: Diego Mariano , CISO at Albert Einstein Hospital

Diego: In cybersecurity for 20 years, currently holding the CISO position at Albert Einstein Hospital. Beyond professional dedication, a passionate practitioner of kriya yoga and meditation.

Description:

This paper presents a novel methodology that combines red team and blue team exercises to enhance cybersecurity resilience in the Brazilian healthcare sector. The methodology is designed to go beyond the traditional roles of red teams and blue teams. It incorporates threat injection exercises with a newly created prioritization method, training the Red Team to assist the CSIRT in responding to incidents and creating a new role for the Red Team. Additionally, a new technique called Offensive Intel monitors the threat landscape of competitors and provides insights on how to protect our own landscape. The methodology also incorporates techniques to deal with VIP patient data and policies to control staff curiosity. Some real-life use cases will be presented to evidence the effectiveness of the methodology. One such use case involved an almost successful attempt to destroy medical equipment during a penetration testing exercise and how to not do it again. Another one presents vulnerabilities identified in air conditioning controllers, EMR systems, and exam results systems that are used in the entire country. And two incidents that were successfully contained with the help of threat injection and offensive intel. The methodology's effectiveness also led to the inference of the Brazilian TOP 10 Vulnerabilities in the Healthcare Sector, based on findings across systems used throughout the country. The list provides insights into the most critical vulnerabilities facing healthcare institutions in Brazil and will be presented at the conference. The vulnerabilities were categorized by the degree of harm they can inflict on patients and the impact on healthcare services. The methodology's results also drove to the development of a tool that assists other cybersecurity teams in conducting safe red and blue team exercises in the healthcare sector. The tool augments cybersecurity resilience by improving the capabilities of CSIRT and threat intel teams and is valuable to other cybersecurity professionals in the industry. In conclusion, the novel methodology provides a unique approach to enhancing cybersecurity resilience in the Brazilian healthcare sector. The incorporation of threat injection exercises, Offensive Intel, and a new role for the Red Team offers a comprehensive and effective approach that goes beyond traditional red team exercises. The methodology and tool can be replicated and the approach's effectiveness has been demonstrated through real-life use cases and the creation of the TOP 10 Vulnerabilities in the Healthcare Sector in Brazil. By adopting this methodology, healthcare institutions in Brazil and around the world can better protect patient data and improve cybersecurity resilience.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Enhancing Security for ReactJS Applications: Exploring Advanced Defense Techniques

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Flamingo - Savoy - AppSec Village - Workshop - [Map](#)

SpeakerBio: Jim Manico

Jim Manico is the founder of Manicode Security, training devs on secure coding. He advises/invests in companies like 10Security, MergeBase. A speaker, Java Champion, and author of "Iron-Clad Java." Active in OWASP, co-leading projects like ASVS.

Twitter: [@manicode](#)

Description:

As we explore the digital world, client-side security risks, such as Cross-Site Scripting (XSS) and unintended privileged information leaks, remain significant concerns. These challenges have long troubled web application developers, underscoring the need for evolving security practices.

ReactJS, a prominent framework in today's tech landscape, has taken strides to mitigate such threats, offering automatic defenses against Cross-Site Scripting. However, building secure ReactJS applications requires in-depth knowledge and specialized expertise.

In this presentation, we will delve into the realm of general-purpose Cross-Site Scripting defense and various client-side security strategies within the ReactJS framework. ReactJS developers of all levels are invited to join us as we explore advanced techniques and practical recommendations that can elevate your approach to ReactJS security.

Our discussion will cover several important topics:

- Understanding the React Component Attack Surface
- Handling Unescaped Props and Types
- Exploring the Use of dangerouslySetInnerHTML
- Properly Handling JavaScript URLs in the React Context
- Integrating CSS Styled-Components with React
- Navigating JSON Embedding and React
- Unraveling React's Automatic Defenses
- Mastering Manual Defense Techniques in React
- Understanding React Lazy Loading and Access Control
- Investigating React Template Injection
- Exploring Server-side Rendering in React

Join us for an informative session that aims to enhance your skill set and bolster your defense strategies for creating more secure ReactJS applications. Let's navigate the intricacies of ReactJS security together, empowering ourselves with advanced defense techniques to foster a secure environment for application development.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Enhancing vulnerability research through the use of virtual reality workspaces.

When: Saturday, Aug 12, 14:35 - 15:20 PDT

Where: Virtual

SpeakerBio: datalocaltmp

I am an independent security researcher focused on mobile technology. Recently I have enhanced a lot of my work by using Visualizations in Virtual Reality, in particular visualizing code coverage in Android ([write-up here](<https://datalocaltmp.github.io/visualizing-android-code-coverage-pt-1.html>)) and then navigating the function graphs in Virtual Reality [example video here](<https://twitter.com/datalocaltmp/status/1666964834334785536>).

Twitter: [@datalocaltmp](https://twitter.com/datalocaltmp)

Description:

Enhancing vulnerability research through the use of virtual reality workspaces. This talk will provide an overview of my set-up for performing vulnerability research within virtual reality and some of the benefits I have observed. Examples of my particular setup available [here](<https://twitter.com/datalocaltmp/status/1620643279657390082>). Additionally I will cover visualization of Android native code execution within Ghidra and how virtual reality has allowed me to better navigate the function graphs while reverse engineering. An example of my particular setup for function graph navigation in VR available [here](<https://twitter.com/datalocaltmp/status/1666964834334785536>).

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Evading Logging in the Cloud: Bypassing AWS CloudTrail

When: Friday, Aug 11, 10:50 - 11:30 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Nick Frichette

Nick Frichette is a Senior Security Researcher at Datadog, where he specializes in AWS offensive security. He is known for finding multiple zero-day vulnerabilities in the AWS services and regularly publishing on new attack techniques. In addition to his research, Nick is the creator and primary contributor to Hacking the Cloud, an open source encyclopedia of offensive cloud security tradecraft.

Twitter: [@Frichette_n](#)

Description:

Amazon Web Services (AWS) customers rely on CloudTrail for continuous monitoring and detection of security incidents within their cloud environments. But what if an attacker could bypass this vital security layer, conducting stealthy reconnaissance and even modifying the environment without leaving any log evidence?

In this talk I will explore the attack surface of the AWS API, and share multiple vulnerabilities I discovered that allowed me to bypass CloudTrail logging for different AWS services. These vulnerabilities have now been fixed by AWS.

Attendees will gain an understanding of how these vulnerabilities are found, an understanding of the internals of the AWS APIs, and knowledge of how to apply these methods to new CloudTrail bypasses.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Evil Digital Twin: Learn Psychological Manipulation with an Uncensored LLM

When: Saturday, Aug 12, 11:00 - 11:59 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

Speakers: Ben D. Sawyer, Matthew Canham

SpeakerBio: Ben D. Sawyer

Dr. Ben D. Sawyer is an applied neuroscientist and human factors engineer known for using brainwaves, eye movements, and mathematical theory to build better human-machine teams. His models and algorithms power trustworthy machines that work with their human partners. His design recommendations are leveraged by Fortune 500 companies. His work has been covered by Forbes, Reuters, Fast Company, and The BBC, and more. Dr. Sawyer's postdoctoral work at MIT was in collaboration with industry including Google, Jaguar-Landover, Honda, DENSO, Monotype, and Panasonic. A two-time Repperger Research Fellow with the Air Force Research Laboratory (AFRL), he performed research with the 711th Human Performance Wing in both their Applied Neuroscience and Battlefield Acoustics (BATMAN group) divisions. He is a recipient of The Human Factors Prize, for Cybersecurity research, The K.U. Smith Award, for consumer electronics work investigating driving distraction and Google Glass, and an Outstanding Dissertation Award for work investigating the applied psychophysics of warfighter multitasking. Dr. Sawyer is presently faculty in Industrial Engineering and Management Systems and the Institute for Simulation and Training at UCF, and the Director of LabX, an applied neuroscience group addressing human performance. In addition to academic pursuits, Dr. Sawyer provides consulting and expert witness services in matters including distraction, attention, and error. He is the co-founder of Awayr, an AI startup within MIT's The Engine. In his leisure time, Ben enjoys adventure travel with his wife, swimming, sailing the Charles, and building things. He volunteers, helping people to learn to repair their own things. He does not enjoy writing about himself in the third person and will now stop.

SpeakerBio: Matthew Canham , CEO at Beyond Layer 7

Dr. Matthew Canham is the CEO of Beyond Layer 7, a security consulting firm specializing in mitigating insider risk, human-centric security solutions, and data analytics. He is a founding member of the Cognitive Security Institute, a non-profit organization dedicated to research and understanding the nuances of defending human and artificial decision makers from cognitive attacks. He currently holds an affiliated faculty member appointment with George Mason University, where the focus of his research orients around synthetic media –deepfake– social engineering attacks, cognitive security, and insider risk. Dr. Canham was previously a Special Agent for the FBI, where he investigated cybercrimes, insider threats, and ran cyber HUMINT operations as a certified online covert employee. During his tenure with the FBI, he also served as a subject matter expert with the Behavioral Analysis Program (BAP) and as the Technical Liaison between the Operational Technology Division (OTD) and the Cyber Behavioral Analysis Center (CBAC). Dr. Canham has previously taught courses on synthetic media attacks, cognitive warfare, human-centric security, and insider risk for; NATO, NASA (Kennedy Space Center), DARPA, MIT, BI (Oslo, Norway), Aberdeen Proving Ground, ISC2, and the FBI. He holds a PhD in Cognitive Psychology with special expertise in human centric security, data analytics, and behavioral engineering; as well as GIAC certifications in Certified Forensics Examiner (GCFE), Certified Auditing Wireless Networks (GWAN), Mobile Device Security Analyst (GMOB), and Certified Incident Handler (GCIH).

Description:

This workshop will delve into the uncharted territory of Uncensored Large Language Models (LLMs) and explore their latent potential. This immersive session invites cybersecurity experts, researchers, and enthusiasts alike to understand the profound capabilities of uncensored LLMs displayed in misinformation and manipulation tactics, and how malicious actors might exploit this capability.

During the workshop, attendees will gain a practical understanding of how LLMs can deploy sophisticated strategies pulled from psychological literature and advertising science. From harnessing cognitive biases and social norms to capitalizing on habit loops, the mechanisms of manipulation are as intriguing as they are unsettling. An uncensored LLM, ripe for exploration, serves as our playground, providing invaluable insights into its interaction patterns.

But it's not just about understanding these models; it's about looking beyond the horizon. Participants will also be introduced to the concept of 'shadow prompts,' concealed instructions that a compromised or malicious LLM runs alongside standard user

prompts. Unraveling the intricacies of these shadow prompts will reveal how they can stealthily shift the outcomes of LLM interactions.

This workshop is more than just a one-off event. All participants will automatically become members of our burgeoning ""Evil Digital Twin"" community. This membership comes with the opportunity to engage in an ongoing learning journey, unveiling the less-discussed capabilities of LLMs. By fostering a collaborative environment, we aim to empower members to not only understand these evolving digital entities but also devise robust defenses against them within their respective organizations and institutions.

Two deep experts in psychology and cybersecurity and the intelligence community will be your guides.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DL - Friday - 14:00-15:55 PDT

Title: EvilnoVNC: Next-Gen Spear Phishing Attacks

When: Friday, Aug 11, 14:00 - 15:55 PDT

Where: Caesars Forum - Committee Boardroom - Demo Labs - [Map](#)

SpeakerBio: Joel Gámez Molina

Systems administrator with more than ten years of experience, he currently works as a security consultant at Deloitte Touche Tohmatsu, where he develops adversarial simulation exercises (Red Team Operations). Previously, he was Chief Technology Officer (CTO) of the startup Cyberguard. He also teaches courses and masters in ethical hacking, pentesting and PowerShell for high-level organizations and universities. Creator of the blog darkbyte.net and speaker at renowned national and international conferences, such as Black Hat USA (2020/2021) and Black Hat Europe (2022). Programmer of hacking tools in his spare time, he has developed tools of all kinds, such as: AutoRDPwn, Cloudtopolis, EvilnoVNC, Invoke-DNSteal, PyShell or PSRansom among others.

Description:

EvilnoVNC is a Ready to go Phishing Platform. Unlike other phishing techniques, EvilnoVNC allows 2FA bypassing by using a real browser over a noVNC connection. In addition, this tool allows us to see in real time all of the victim's actions, access to their downloaded files and the entire browser profile, including cookies, saved passwords, browsing history and much more.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Friday - 10:00-17:59 PDT

Title: Exhibitor Area Open

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Forum - 124-126 - Exhibitors - [Map](#)

Description:

This is when you can go visit our awesome exhibitors.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Sunday - 10:00-13:59 PDT


Title: Exhibitor Area Open

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Forum - 124-126 - Exhibitors - [Map](#)

Description:

This is when you can go visit our awesome exhibitors.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Saturday - 10:00-17:59 PDT

Title: Exhibitor Area Open

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Forum - 124-126 - Exhibitors - [Map](#)

Description:

This is when you can go visit our awesome exhibitors.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Exploiting OPC-UA in Every Possible Way: Practical Attacks Against Modern OPC-UA Architectures

When: Saturday, Aug 12, 14:30 - 15:15 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

Speakers: Noam Moshe, Sharon Brizinov

SpeakerBio: Noam Moshe , Vulnerability Researcher at Claroty Team82

Noam Moshe is a vulnerability researcher at Claroty Team82. Noam specializes in vulnerability research, web applications pentesting, malware analysis, network forensics and ICS/SCADA security. In addition, Noam presented in well-known Hacking conferences like Blackhat Europe, as well as won Master of Pwn at Pwn2Own Miami 2023.

SpeakerBio: Sharon Brizinov , Director of Security Research at Claroty Team82

Sharon Brizinov leads the Vulnerability Research at Team82, The Claroty Research. He specializes in OT/IoT vulnerability research, has participated in multiple Pwn2Own competitions, won Pwn2Own Miami 2023, and holds a DEFCON black badge.

Description:

OPC-UA is the most popular protocol today in ICS/SCADA and IoT environments for data exchanges from sensors to on-premises or cloud applications. OPC-UA is therefore the bridge between different OT trust zones and a crown jewel for attacks attempting to break security zones and crossover from the industrial to corporate networks.

We have been researching during the past two years dozens of OPC-UA protocol stack implementations being used in millions of industrial products. We focused on two main attack vectors: attacking OPC-UA servers and protocol gateways, and attacking OPC-UA clients. The research yielded unique attack techniques that targeted specific OPC-UA protocol specification pitfalls that enabled us to create a wide range of vulns ranging from denial of service to remote code execution.

For example, we explored OPC-UA features such as method call processing, chunking mechanisms, certification handling, complex variant structures, monitored items, race-conditions, and many more. For each part of the specification, we tried to understand its caveats and exploit them to achieve RCE, information leaks, or denial of service attacks.

In this talk, we will share our journey, methods, and release an open-source framework with all of our techniques and vulnerabilities to exploit modern OPC-UA protocol stacks. , Noam Moshe is a vulnerability researcher at Claroty Team82. Noam specializes in vulnerability research, web applications pentesting, malware analysis, network forensics and ICS/SCADA security. In addition, Noam presented in well-known Hacking conferences like Blackhat Europe, as well as won Master of Pwn at Pwn2Own Miami 2023.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Exploring Linux Memory Manipulation for Stealth and Evasion: Strategies to bypass Read-Only, No-Exec, and Distroless Environments

When: Sunday, Aug 13, 13:00 - 13:45 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

Speakers: Carlos Polop, Yago Gutierrez

SpeakerBio: Carlos Polop , Web, Mobile & Cloud Pentesting Team Leader at Halborn

Carlos has a degree in Telecommunications Engineering with a Master in Cybersecurity. He has worked mainly as Penetration Tester and Red Teamer for several companies, but also as developer and system administrator. He has several relevant certifications in the field of cybersecurity such as OSCP, OSWE, CRTP, eMAPT and eWPTXv2. He was captain of the Spanish team in the ECSC2021 and member of Team Europe for the ICSC2022.

Since he started learning cybersecurity he has tried to share his knowledge with the infosec community by publishing open source tools such as <https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite> and writing a free hacking book that anyone can consult at <https://book.hacktricks.xyz>.

Twitter: [@hacktricks_live](#)

SpeakerBio: Yago Gutierrez , Offensive Security Researcher at Mollitiam Industries

Yago is currently studying Telecommunications Engineering. He is an experienced C programmer, tolerates python and has extensive knowledge of Linux Internals. He works as a vulnerability researcher on binaries as well as malware on mobile systems. He is an occasional CTF player and has participated in the ECSC2020 as a member of the Spanish team.

Twitter: [@arget1313](#)

Description:

As cyber threats continue to evolve, attackers constantly develop new methods for exploiting system vulnerabilities and evading detection. In this presentation, we will delve into cutting-edge techniques for manipulating Linux memory in highly constrained environments, such as read-only, no-exec, and distroless setups. These techniques can be utilized by sophisticated malware to remain stealthy and evade traditional security mechanisms.

We will begin by providing an overview of the unique challenges faced in these limited environments and discuss the reasons behind their increasing prevalence. Next, we will explore how attackers can exploit vulnerabilities within these constraints and demonstrate several novel methods for manipulating Linux memory.

Throughout the presentation, we will showcase real-world examples and provide step-by-step explanations for each technique, enabling attendees to gain a deeper understanding of how they can be employed by adversaries. Additionally, we will discuss potential countermeasures and mitigation strategies to help security professionals better defend against these emerging threats.

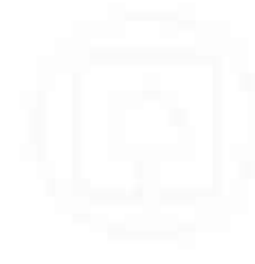
By attending this presentation, participants will gain valuable insights into the latest advancements in Linux memory manipulation and acquire the knowledge needed to anticipate and counter stealthy attacks in constrained environments. Whether you are a security researcher, a system administrator, or an ethical hacker, this session will equip you with the expertise necessary to stay ahead of the curve in the ever-evolving world of cybersecurity.

REFERENCES

Most of the parts of the developed technique for this presentation is just based on our knowledge and experience. However, it's true that some previous research was done in this topic by sektor7 in <https://blog.sektor7.net/#!res/2020/meterp-inject-yt.md> and David Buchanan in <https://twitter.com/David3141593/status/1386663070991360001>

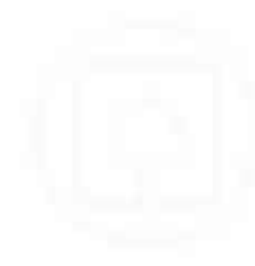
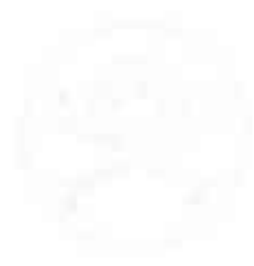
同治十三年庚午

同治十三年庚午



同治十三年庚午

同治十三年庚午



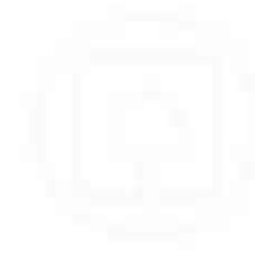
同治十三年庚午

同治十三年庚午



同治十三年庚午

同治十三年庚午



同治十三年庚午

同治十三年庚午

CPV - Saturday - 14:00-14:45 PDT

Title: Exploring the Impact of PQC on Cryptographic Key Management

When: Saturday, Aug 12, 14:00 - 14:45 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

Speakers:Deirdre Connolly,James Howe,Mark Carney,Ryan Hurst,Sandra Guasch Castello,Sofi Celi

SpeakerBio:Deirdre Connolly

No BIO available

SpeakerBio:James Howe

No BIO available

SpeakerBio:Mark Carney

No BIO available

SpeakerBio:Ryan Hurst

No BIO available

SpeakerBio:Sandra Guasch Castello

No BIO available

SpeakerBio:Sofi Celi

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: FaFo: Laboratory Physical and ICS (Warning: not for the faint of heart)

When: Saturday, Aug 12, 16:10 - 17:10 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

SpeakerBio:Nathan Case

A passion for Incident Response, and operational security in all forms. Pushing the bounds of threat detection and response. Finding new thoughts and bringing them to the fields of security and technology.

Description:

I will discuss real-world equipment hacks caused by nation-state actors attacking humans and ways to mitigate similar impacts. Examples will cover a range of laboratory equipment, including research labs and industrial manufacturing facilities. In this talk, we will explore the common causes of laboratory and OT equipment breaches caused by human error, including misconfiguration, misuse, and malicious actions. We will examine the potential consequences of such failures, including data loss, damage to equipment, and even injury. I will also present a range of strategies for preventing such issues, including implementing standard operating procedures with a security focus, using equipment monitoring systems, and adopting best practices for equipment architecture.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Faking GitHub Contributions

When: Friday, Aug 11, 15:00 - 16:59 PDT

Where: Flamingo - Savoy - AppSec Village - Workshop - [Map](#)

Speakers: Alik Koldobsky, Tal Folkman

SpeakerBio: Alik Koldobsky

Alik is a security researcher and software engineer at Checkmarx supply chain security group, leading the development of the behavior analysis engine of code packages.


SpeakerBio: Tal Folkman

Tal brings over 7 years of experience to her role as a principal supply chain security research within Checkmarx Supply Chain Security group. She is in charge of detecting tracking and stopping Opensource attacks.

Description:

When using Open Source Packages, we tend to rely on strangers to deliver us code. There are many ways to determine the legitimacy of a package, whether it will be the number of stars of the package or the maintainer's GitHub account credibility.

Unfortunately all you can see can be easily spoofed.

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Saturday - 15:00-16:59 PDT

Title: Faking GitHub Reputation

When: Saturday, Aug 12, 15:00 - 16:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 4 - [Map](#)

SpeakerBio: Checkmarx

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Sunday - 12:00-13:59 PDT

Title: Faking GitHub Reputation

When: Sunday, Aug 13, 12:00 - 13:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 4 - [Map](#)

SpeakerBio: Checkmarx

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Fantastic Ethertypes and Where to Find Them

When: Friday, Aug 11, 13:30 - 14:15 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

SpeakerBio: Ricky "HeadlessZeke" Lawshae, Hacker

Ricky "HeadlessZeke" Lawshae is a connoisseur of arcane and archaic network protocols. He is a security researcher with well over a decade of experience in the fields of IoT security, exploitation, and network protocol analysis. He has spoken at DEFCON multiple times, as well as Recon, Ruxcon, Toorcon, and many other conferences around the globe. In his offtime, he enjoys drinking Irish whiskeys and dark beers, reading comics, and listening to/playing in punk rock bands.

Twitter: [@HeadlessZeke](#)

Description:

Beneath the mundane world of TCP/IP exists the magical and mysterious realm of ethernet. There are many different types of ethernet protocols in use today, known as 'ethertypes', that run the gamut from the boutique to the ubiquitous. In this talk, we will delve into some of the more interesting and obscure ethertypes that exist. We will discuss the network protocols themselves, where they can be found in the wild, what you can do with them, and how they could be abused in the wrong hands. We will explore wide-ranges of networking environments including industrial/facilities, transportation, and medical, and will include several live demos. Attendees will leave this talk with a greater understanding and appreciation for the unseen networking world that exists all around them.

REFERENCES:

<https://en.wikipedia.org/wiki/EtherType> <https://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.xhtml>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Saturday - 12:00-13:30 PDT

Title: Fear and Loathing on Plum Island

When: Saturday, Aug 12, 12:00 - 13:30 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

Speakers:David Emmerich,Emma Stewart,Jeremy Jones,Joe Minicucci

SpeakerBio:David Emmerich , University of Illinois Information Trust Institute

No BIO available

SpeakerBio:Emma Stewart

No BIO available

SpeakerBio:Jeremy Jones , Idaho National Lab

No BIO available

SpeakerBio:Joe Minicucci

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Film screening: Reality Games Using film and interactive storytelling to inoculate against the disinformation tsunami:

When: Friday, Aug 11, 16:30 - 17:59 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio:Michael Morgenstern

Michael Morgenstern is a filmmaker, technologist, and culture hacker. He has produced and directed three films in over 70 festivals worldwide. Michael focuses on the interaction between social media, news cycles, interaction design, and cultural discourse, and how disinformation is propagated. He is CEO and Creative Director of This is Definitely Real, an alternate reality media company telling interactive stories online.

Description:

Join us for a preview screening of the first half of Reality Games, a new feature film about disinformation, deepfakes, AI, and a world where the boundary between reality and fiction bends and then shatters. In the style of Fight Club meets a video game, the movie follows the story of two kids who ruin each others' lives online, exploring how tribalism takes hold. The movie is a work-in-progress screening and will be released in 2024. Hear how their team created an ethical disinformation event during the heart of the pandemic and learned how easy it is to control the narrative.

After the film, join director Michael Morgenstern and _____, for a fireside chat. What's coming next with disinformation enhanced by AI? How does tribalism form? How can experiential storytelling be used to modify our existing meta-narratives? How will we operate in a world where reality has broken down?

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Finding bugs and scaling your security program with Semgrep

When: Friday, Aug 11, 15:00 - 16:59 PDT

Where: Flamingo - Savoy - AppSec Village - [Map](#)

SpeakerBio: Lewis Ardern , Staff Security Researcher at Semgrep

Lewis is a Staff Security Researcher for Semgrep, a SAST startup. Previously, Lewis was a Lead Security Engineer at Salesforce and spent many years at Cigital and Synopsys as a consultant. Lewis hosts a podcast called SecuriTEA & Crumpets.

Description:

Between Agile, DevOps, and infrastructure as code, development is happening faster than ever. As a security team, it can be tough to keep up. We need to move fast, and iterate quickly as new issues emerge. SAST is one piece of a very important puzzle in the SDLC, so using tools effectively is the key to success! This workshop will be a hands-on masterclass by the creators and maintainers of Semgrep (<https://github.com/returntocorp/semgrep>), an open source, lightweight static analysis tool which can help enable development teams to scale their SAST efforts.

[Return to Index](#) - Add to  - ics [Calendar](#) file

RCV - Saturday - 15:55-16:20 PDT

Title: Finding Hidden Gems In Temporary Mail Services

When: Saturday, Aug 12, 15:55 - 16:20 PDT

Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio:Berk Can Geyikci

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Fireside Chat with the National Cyber Director Kemba Walden

When: Friday, Aug 11, 17:30 - 18:15 PDT


Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

SpeakerBio: Kemba Walden , Acting National Cyber Director at Office of the National Cyber Director, The White House
Director Walden is the current acting National Cyber Director for the Biden-Harris Administration.

Twitter: [@KembaWalden46](#)

Description:

A fireside chat with Director Walden. Director Walden is the current acting National Cyber Director for the Biden-Harris Administration.

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Saturday - 10:30-12:30 PDT

Title: First Timers Workshop

When: Saturday, Aug 12, 10:30 - 12:30 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio: Tailor Herrarte

With over 8 years in government and commercial incident response, I'm a seasoned cybersecurity expert specializing in OSINT, social engineering, phishing, and pentesting. From fortifying systems in pharmaceuticals to refining best practices at the National Institutes of Health, I bring a wealth of experience. Currently, I'm dedicated to enhancing web application security at Yahoo.

Description:

Never hacked a voting machine before? Come check out our First Timers Workshop to give it a try. Don't think you can do it? There is only one way to find out. To try it yourself! Even if you have never hacked anything before, this is the workshop for you.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Friday - 11:30-11:59 PDT

Title: Five (or More) Maritime Cybersecurity Challenges

When: Friday, Aug 11, 11:30 - 11:59 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio: Gary C. Kessler

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Saturday - 15:00-16:59 PDT

Title: Fix The Flag - Battle Challenge

When: Saturday, Aug 12, 15:00 - 16:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 3 - [Map](#)


SpeakerBio: Pedram Hayati

Dr. Pedram Hayati, Founder of SecTalks.org, Founder of SecDim.com. Senior lecturer at UNSW. Kite surfer. Lives in downunder

Twitter: [@pi3ch](#)

Description:

Find a security vulnerability in an app and get a score when you effectively fix it. The winner of the competition is the first person who fixes the vulnerability.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Fix The Flag: A Secure Programming Competition

When: Friday, Aug 11, 13:00 - 14:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 3 - [Map](#)

SpeakerBio: Pedram Hayati

Dr. Pedram Hayati, Founder of SecTalks.org, Founder of SecDim.com. Senior lecturer at UNSW. Kite surfer. Lives in downunder

Twitter: [@pi3ch](#)

Description:

Find a security vulnerability in an app and get a score when you effectively fix it. The winner of the competition is the first person who fixes the vulnerability.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Sunday - 09:00-12:59 PDT

Title: Fleet DefCon 31 Workshop

When: Sunday, Aug 13, 09:00 - 12:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Fleet is an open-core, cross-platform solution that provides real-time insights using osquery and GitOps-driven management for all your devices, including Mac, Windows, Linux, and ChromeOS. Join the adventure and explore a wonderland of data!

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Friday - 09:00-17:59 PDT


Title: Fleet DefCon 31 Workshop

When: Friday, Aug 11, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Fleet is an open-core, cross-platform solution that provides real-time insights using osquery and GitOps-driven management for all your devices, including Mac, Windows, Linux, and ChromeOS. Join the adventure and explore a wonderland of data!

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Saturday - 09:00-17:59 PDT

Title: Fleet DefCon 31 Workshop

When: Saturday, Aug 12, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Fleet is an open-core, cross-platform solution that provides real-time insights using osquery and GitOps-driven management for all your devices, including Mac, Windows, Linux, and ChromeOS. Join the adventure and explore a wonderland of data!

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Friday - 14:30-15:30 PDT

Title: Flipping Locks: Remote Badge Cloning with the Flipper Zero

When: Friday, Aug 11, 14:30 - 15:30 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

Speakers:Dan,Langston "Shock" Clement

SpeakerBio:Dan

No BIO available

SpeakerBio:Langston "Shock" Clement , Lead for Red Team operations and Penetration Testing engagements at Core BTS

Langston grew up reading stories about the 90's hacker escapades, and after years of observing the scene, he jumped into the cybersecurity field and never looked back. He is the current lead for Red Team operations and Penetration Testing engagements at Core BTS. With over fifteen (15) years of public and private sector experience in cybersecurity and ethical hacking, he aims to provide organizations with valuable and actionable information to help improve their security posture. Langston's specializations focus on modern-day social engineering techniques, wireless and RFID attacks, vulnerability analysis, as well as physical and cloud penetration testing.

Twitter: [@sh0ckSec](#)

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Flipping the Coin: Red and Blue Teaming in Windows Environments (Pre-Registration Required)

When: Thursday, Aug 10, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers: Angus "0x10f2c_" Strom, Troy Defty

SpeakerBio: Angus "0x10f2c_" Strom , Senior Security Engineer

Angus (0x10f2c_) is currently a Senior Security Engineer working at a tech company. He obtained a love for all things computers by scavenging computer parts from local garbage pickups as a kid, and then trying to make them work together without blowing up. Angus eventually realised that a career could be made out of his skills hacking together poorly written LUA code in Garry's mod, and finished a Bachelors in Network Security. In his professional career Angus has 5+ years working in Security Consulting, working across many industries and gaining many shells. More recently Angus has made the move to a security engineer focused role. When not hacking he loves to ski on the little snow that Australia has, and loves to paint small miniatures while listening to Drone Metal.

SpeakerBio: Troy Defty , Security Engineering Manager

Having worked in the UK and Australian InfoSec industries for just over a decade, and following 8 and a half years of red teaming, Troy jumped the proverbial fence from red to blue, and is currently a Security Engineering Manager at a tech company. His interest and experience is in detection engineering, red teaming, threat modelling, hardware, and assessing ICS environments. Other interests include music, electronics, the outdoors, travel, rugby, CTF, and being bad at golf.

Description:

Red and blue are two sides of the same coin. Offensive and defensive teams deliver the best results when working together; sharing knowledge, ideas, and understanding with each other. And a core part of this information exchange is understanding each respective perspective. This is the overarching theme of the workshop; attackers thinking like defenders, and defenders thinking like attackers.

By the end of the workshop, attendees will:

1. Understand and perform common offensive attacks (supported by the Metasploit Framework) against Windows Domains, including:

Pass the Hash attacks;
ADCS abuse;
PrintSpoofer exploits;
LSASS exploitation (using Mimikatz); AD enumeration (using BloodHound);
DACL abuse;
Kerberos golden tickets; and
DLL hijacking.

2. Understand the process of detecting attacks against Windows infrastructure, including how to design and implement their own detection rules based on attendees' previous attacks, using:

Sigma/Yara rules.
Log ingestion/normalization platforms, and query engines (e.g. ELK).

3. Understand and appreciate how the actions and processes of red and blue teams are interlinked, for the greater collective good. Recommended (but not required) prior reading:

<https://nooblinux.com/metasploit-tutorial/https://posts.specterops.io/introducing-bloodhound-enterprise-attack-path-management-f>
<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
<https://socprime.com/blog/sigma-rules-the-beginners-guide/> <https://github.com/socprime/SigmaUI>

<https://blog.netwrix.com/2021/11/30/how-to-detect-pass-the-hash-attacks/>
<https://posts.specterops.io/certified-pre-owned-d95910965cd2>
<https://www.elastic.co/guide/en/security/current/suspicious-print-spooler-point-and-print-dll.html>

Skill Level: Beginner to Intermediate

Prerequisites for students:

- Basic understanding of the Linux and Windows command line - some basic knowledge of IP networking and routing - A basic understanding of Active Directory and exposure to the Metasploit Framework/Meterpreter are beneficial, but not required.

Materials or Equipment students will need to bring to participate: - Laptop, 8GB RAM

- OpenVPN Client

- Remote Desktop Protocol (RDP) client

- It is strongly recommended that attendees have local administrative rights to their device. - An Internet connection is also required; DEF CON's (authenticated) WiFi network will suffice, however attendees should consider alternative options in favour of resiliency (e.g. tethering/hotspotting cell phones).

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: FlowMate and CSTC for Advanced Pentesting

When: Friday, Aug 11, 15:00 - 16:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 3 - [Map](#)

Speakers: Florian Haag, Matthias Göhring

SpeakerBio: Florian Haag

Florian Haag is a senior security consultant at usd AG with experience in penetration testing, software security assessments as well as code reviews. He is specialized in penetration tests of thick client applications, leveraging his background in software development to reverse engineer proprietary client applications and network protocols. In previous scientific work, he worked on novel approaches to application-level data flow analysis to improve penetration testing coverage. In addition, he analyzed website clones used in phishing campaigns and the frameworks that are used by fraudsters to create and operate cloned websites.

SpeakerBio: Matthias Göhring

Matthias Göhring is security consultant and penetration tester at usd AG, an information security company based in Germany with the mission #moresecurity. He is Head of usd HeroLab, the division of usd specialized in technical security assessments. In addition, he holds lectures at Technical University Darmstadt and University of Applied Sciences Darmstadt on ethical hacking and penetration testing. In previous scientific work, he focused on network and communication security as well as software security.

Previous publications:

- Catching the Clones – Insights in Website Cloning Attacks, Risk Connect Conference, 2021 - Path MTU Discovery Considered Harmful, IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018 - Tor Experimentation Tools, IEEE Security and Privacy Workshops, 2015 - On randomness testing in physical layer key agreement, IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015

Description:

With our two open-source BurpSuite extensions FlowMate and the Cyber Security Transformation Chef (CSTC) we want to step up penetration testing of web applications to the next level. FlowMate is a plugin that helps to identify all data flows of a application by only analyzing requests to and responses from the target. In the background it creates a graph you can browse visually to identify data flows to test for injection vulnerabilities. The CSTC like the swiss-army knife for pentesting. It enables you to define custom recipes that can be applied to outgoing or incoming requests. This gives you the possibility to alter HTTP messages in transit in various ways. The only limit here is your creativity.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: FlowMate

When: Friday, Aug 11, 12:00 - 13:55 PDT

Where: Caesars Forum - Society Boardroom - Demo Labs - [Map](#)

Speakers: Florian Haag, Nicolas Schickert

SpeakerBio: Florian Haag

Florian Haag is a senior security consultant at usd AG with experience in penetration testing, software security assessments as well as code reviews. He is specialized in penetration tests of thick client applications, leveraging his background in software development to reverse engineer proprietary client applications and network protocols. In previous scientific work, he worked on novel approaches to application-level data flow analysis to improve penetration testing coverage. In addition, he analyzed website clones used in phishing campaigns and the frameworks that are used by fraudsters to create and operate cloned websites.

SpeakerBio: Nicolas Schickert

Nicolas Schickert is security researcher and penetration tester at usd AG, an information security company based in Germany. He is in charge of SAP specific penetration tests at the usd HeroLab. In this role, Nicolas is responsible for the collection of SAP related knowledge and the development of new analysis tools. He is interested in reverse engineering and vulnerability research and has published several zero-day vulnerabilities, not only in the context of SAP.

Description:

Imagine pentesting a large web application with hundreds of pages and forms, as well as user roles and tenants. You discover that your chosen username is reflected in many locations inside the application, but you don't have a detailed overview. You want to test whether the chosen username is handled properly or allows for injection attacks, such as Cross-Site Scripting or Server-Side Template Injection. Now you face the challenge of finding all locations where your payloads appear when injecting into the username. In large applications, you'll likely miss some, potentially leaving vulnerabilities undetected. This is where FlowMate comes into play, our novel tool to detect data flows in applications for enhanced vulnerability assessments. FlowMate consists of two components: A BurpSuite plugin and a data flow graph based on Neo4j. It records inputs to the application as you go through the pages exploring the application and searches for occurrences of the captured inputs in the responses. This results in a graph that can be visualized and searched for parameters of interest and where they're occurring on the site. Understanding the data flows of an application helps to significantly improve the test coverage and bring your pentesting to the next level.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: FoldIt

When: Friday, Aug 11, 14:40 - 15:59 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

SpeakerBio: Firas D Khatib , Associate Professor at University of Massachusetts Dartmouth PhD

- Principal Investigator on the Foldit Project: a free worldwide video game where citizen scientists help solve challenging protein-folding problems (www.fold.it)
- Associate Professor at the University of Massachusetts Dartmouth, in the Department of Computer and Information Science
- My favorite courses to teach include Computer Game Design, Advanced Bioinformatics, Gamification Design, and Social and Ethical Aspects of Computing
- Received Ph.D. in Bioinformatics at UC Santa Cruz in 2008 • Received bachelor's degree in Applied Math at UC Berkeley in 2001
- Big fan of all kinds of games: board games, card games, video games, escape rooms, etc.
- U2 fanatic, will be back in Vegas 3 more times this fall to see them play The Sphere :-)

Description:

If we want to address the many challenges facing this world, we'll need to tackle them from many different angles—not just using traditional means. For example, can the brainpower of video game playing citizen scientists tackle critical problems in computational biology? Yes! Players of the worldwide online protein-folding video game Foldit—most of whom with little or no prior biochemistry experience—have uncovered knowledge that eluded scientists for years, contributing to several scientific discoveries through gameplay. Rather than solving problems with a purely computational approach, combining humans and computers can provide a means for solving problems neither could solve alone. You will be given an opportunity to learn and train your Foldit skills before the conference, where a special Biohacking Village Foldit Competition will take place!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: For Kids: Castle Defenders

When: Saturday, Aug 12, 13:00 - 14:59 PDT

Where: Flamingo - Savoy - AppSec Village - [Map](#)

SpeakerBio: Pentera

Mommy is late for dinner again, and Emma and Oliver are frustrated. Daddy comes to the rescue with spaghetti and an enchanting tale of brave knights and mysterious castles, revealing how he and Mommy work tirelessly to protect the people on the internet from bad hackers and other online threats.

This charming story, filled with delightful illustrations and playful storytelling, is perfect for young minds eager to explore the captivating world of cybersecurity.

Description:

Amazon Best Selling children's book "Castle Defenders" is making its DEFCON debut!

Bring your elementary school-aged kids to learn "what cyber parents do" with story time and on-site coloring station.*

*While supplies last.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Sunday - 12:30-12:59 PDT

Title: Forcible Entry 101

When: Sunday, Aug 13, 12:30 - 12:59 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

SpeakerBio: Bill Graydon

Bill Graydon is a principal researcher at GGR Security, where he hacks everything from locks and alarms to critical infrastructure; this has given him some very fine-tuned skills for breaking stuff. He's passionate about advancing the security field through research, teaching numerous courses, giving talks, and running DEF CON's Physical Security Village. He's received various degrees in computer engineering, security, and forensics and comes from a broad background of work experience in cyber security, software development, anti-money laundering, and infectious disease detection.

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Forensic Analysis: Part I & II

When: Friday, Aug 11, 13:30 - 14:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Project Obsidian: Kill Chain Track (0x42) - [Map](#)

Speakers:Danny D. "B4nd1t0" Henderson Jr,Omenscan

SpeakerBio:Danny D. "B4nd1t0" Henderson Jr

Danny "B4nd1t0" Henderson Jr has over 11 years in the IT field from the U.S. Public Sector to life in the Private Sector and supported operations such as Cyber Warfare. Danny currently works at Novartis in Czech Republic as a Threat Hunter. He holds a master's degree in Cyber and Information Security from Capitol Technology University and certifications such as GCIH, GCFA, and CISSP. His skillset includes digital forensics, threat intelligence, and malware analysis. Outside of the field, Danny is fond of fantasy-themed tabletop games and retro RPGs which is displayed through his Bandit's Bytes website.

SpeakerBio:Omenscan

No BIO available

Description:

This Forensics Kill Chain session includes two modules.

Part I: Forensics Analysis: Insider Threat - Forensics walkthrough of the Project Obsidian Insider Threat - Covering both Technical and Non-Technical considerations. Part II: Forensics Analysis: Pivoting from IT to OT: Forensics walkthrough of the Project Obsidian external attacker (Kill Chain) - Covering Telemetry and artifacts collected and parsed to determine what happened.

Forensics analysis; Part I: Forensics Analysis: Insider Threat, Part II: Forensics Analysis: Pivoting from IT to OT

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Forensics 101 Part I & II

When: Saturday, Aug 12, 11:30 - 11:59 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Project Obsidian: 101 Track (0x41) - [Map](#)

Speakers: Danny D. "B4nd1t0" Henderson Jr, Gyle_dC

SpeakerBio: Danny D. "B4nd1t0" Henderson Jr

Danny "B4nd1t0" Henderson Jr has over 11 years in the IT field from the U.S. Public Sector to life in the Private Sector and supported operations such as Cyber Warfare. Danny currently works at Novartis in Czech Republic as a Threat Hunter. He holds a master's degree in Cyber and Information Security from Capitol Technology University and certifications such as GCIH, GCFA, and CISSP. His skillset includes digital forensics, threat intelligence, and malware analysis. Outside of the field, Danny is fond of fantasy-themed tabletop games and retro RPGs which is displayed through his Bandit's Bytes website.

SpeakerBio: Gyle_dC

Gyle first got connected to the internet via her reliable 56k US Robotics modem and has been fascinated ever since with technology and security. She got her Graduate Certificate in Incident Response from the SANS Institute and her master's in cyber security – Digital Forensics from UNSW Canberra. In her day job as an incident responder, she uses her skills and knowledge to help protect and defend the organisation she works for. In her spare time, she mentors other people who are new to the field, presents in different cyber security events and volunteers with different community-based organisations.

Description:

This Forensics 101 session includes two modules.

Part I: General Introduction to Forensics Part II: General Introduction to Forensics Continued

Introduction to Forensics: Part I & II

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Friday - 13:00-15:59 PDT

Title: Free Amateur Radio License Exams

When: Friday, Aug 11, 13:00 - 15:59 PDT

Where: Flamingo - Virginia City - Ham Radio Village - [Map](#)

Description:

Take the test to join what has been considered to be one of the first hacker communities, amateur radio! The Ham Radio Village is back at DEF CON 31 to offer free amateur radio license exams to anyone who wishes to get their ham radio license. Examinees are encouraged to study on [ham.study](<https://ham.study/>), and may sign up for this time slot [here](<https://ham.study/sessions/64bc92b50e6ad267cdea8ab0/1>).

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 11:00-16:59 PDT


Title: Free Amateur Radio License Exams

When: Saturday, Aug 12, 11:00 - 16:59 PDT

Where: Flamingo - Virginia City - Ham Radio Village - [Map](#)

Description:

Take the test to join what has been considered to be one of the first hacker communities, amateur radio! The Ham Radio Village is back at DEF CON 31 to offer free amateur radio license exams to anyone who wishes to get their ham radio license. Examinees are encouraged to study on [ham.study](<https://ham.study/>), and may sign up for this time slot [here](<https://ham.study/sessions/64bc92c66f588492f6063722/1>).

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 11:00-13:59 PDT

Title: Free Amateur Radio License Exams

When: Sunday, Aug 13, 11:00 - 13:59 PDT

Where: Flamingo - Virginia City - Ham Radio Village - [Map](#)

Description:

Take the test to join what has been considered to be one of the first hacker communities, amateur radio! The Ham Radio Village is back at DEF CON 31 to offer free amateur radio license exams to anyone who wishes to get their ham radio license. Examinees are encouraged to study on [ham.study](<https://ham.study/>), and may sign up for this time slot [here](<https://ham.study/sessions/64bc92f0f1d18834466defba/1>).

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Saturday - 13:15-13:30 PDT

Title: Free Pokemon Card Bus Passes

When: Saturday, Aug 12, 13:15 - 13:30 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

Speakers:Jarvis,Malcolm


SpeakerBio:Jarvis

No BIO available

SpeakerBio:Malcolm

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Thursday - 17:00-17:59 PDT

Title: Friends of Bill W

When: Thursday, Aug 10, 17:00 - 17:59 PDT

Where: Harrah's - Studio 1 - Friends of Bill W - [Map](#)

Description:

Thursday

12:00-13:00

17:00-18:00

Friday

12:00-13:00

17:00-18:00


Saturday

12:00-13:00

17:00-18:00

Sunday

12:00 -13:00

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Thursday - 12:00-12:59 PDT

Title: Friends of Bill W

When: Thursday, Aug 10, 12:00 - 12:59 PDT

Where: Harrah's - Studio 1 - Friends of Bill W - [Map](#)

Description:

Thursday

12:00-13:00

17:00-18:00

Friday

12:00-13:00

17:00-18:00

Saturday

12:00-13:00

17:00-18:00

Sunday

12:00 -13:00

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 12:00-12:59 PDT

Title: Friends of Bill W

When: Friday, Aug 11, 12:00 - 12:59 PDT

Where: Harrah's - Studio 1 - Friends of Bill W - [Map](#)

Description:

Thursday

12:00-13:00

17:00-18:00

Friday

12:00-13:00

17:00-18:00


Saturday

12:00-13:00

17:00-18:00

Sunday

12:00 -13:00

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 12:00-12:59 PDT

Title: Friends of Bill W

When: Saturday, Aug 12, 12:00 - 12:59 PDT

Where: Harrah's - Studio 1 - Friends of Bill W - [Map](#)

Description:

Thursday

12:00-13:00

17:00-18:00

Friday

12:00-13:00

17:00-18:00

Saturday

12:00-13:00

17:00-18:00

Sunday

12:00 -13:00

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 17:00-17:59 PDT

Title: Friends of Bill W

When: Friday, Aug 11, 17:00 - 17:59 PDT

Where: Harrah's - Studio 1 - Friends of Bill W - [Map](#)

Description:

Thursday

12:00-13:00

17:00-18:00

Friday

12:00-13:00

17:00-18:00

Saturday

12:00-13:00

17:00-18:00

Sunday

12:00 -13:00

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Sunday - 12:00-12:59 PDT

Title: Friends of Bill W

When: Sunday, Aug 13, 12:00 - 12:59 PDT

Where: Harrah's - Studio 1 - Friends of Bill W - [Map](#)

Description:

Thursday

12:00-13:00

17:00-18:00

Friday

12:00-13:00

17:00-18:00


Saturday

12:00-13:00

17:00-18:00

Sunday

12:00 -13:00

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 17:00-17:59 PDT

Title: Friends of Bill W

When: Saturday, Aug 12, 17:00 - 17:59 PDT

Where: Harrah's - Studio 1 - Friends of Bill W - [Map](#)

Description:

Thursday

12:00-13:00

17:00-18:00

Friday

12:00-13:00

17:00-18:00

Saturday

12:00-13:00

17:00-18:00

Sunday

12:00 -13:00

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: From Feature to Weapon: Breaking Microsoft Teams and SharePoint Integrity

When: Saturday, Aug 12, 12:00 - 12:45 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

SpeakerBio: Nestori Syynimaa , Senior Principal Security Researcher at Secureworks

Dr Nestori Syynimaa is one of the leading Azure AD / M365 experts in the world and the developer of the AADInternals toolkit. He has worked with Microsoft cloud services for over a decade and has been MCT since 2013, MVP since 2020, and awarded Microsoft Most Valuable Security Researcher for 2022. Currently, Dr Syynimaa works as a Senior Principal Security Researcher for Secureworks Counter Threat Unit. Before moving to his current position, Dr Syynimaa worked as a CIO, consultant, trainer, researcher, and university lecturer for almost 20 years. Dr Syynimaa has spoken in many international scientific and professional conferences, including IEEE TrustCom, Black Hat (USA, Europe, and Asia), Def Con, and RSA Conference.

Twitter: [@DrAzureAD](#)

Description:

Microsoft SharePoint Online (SPO) is a cloud-based service that helps organizations share and manage content. It is also used as backend file storage for other Microsoft online services, such as Microsoft 365 Groups, OneDrive, and Teams.

Microsoft offers tools such as Migration Manager and SharePoint Migration Tool (SPMT) to ease migrating files from on-premises file servers to SPO, OneDrive, and Teams. Both tools use the same background APIs to perform the data migration. Technically, the migration is leveraging the built-in Granular Backup feature of on-premises SharePoint, which allows exporting and importing individual SharePoint sites and lists. The Granular Backup feature is not available in SharePoint Online.

In this talk, I'll show how threat actors can leverage SPO migration APIs to break the integrity of all Microsoft online services that use SPO as storage. Threat actors can spoof new content and tamper with existing content, and inject custom code to perform XSS attacks. This, in turn, enables elevation-of-privilege attacks to all Microsoft Online services, including Azure Active Directory. And all this as a regular user.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: From Service Catalog Admin to Account takeover: Privilege Escalation with Service Catalog Launch Constraint

When: Friday, Aug 11, 12:10 - 12:30 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Sarachai Boonyakiat , Principal Cloud Security

I am Principal Cloud Security in a Non-Profit organization with several years experience in IT security in many industries including Industrial automation, Banking, Insurance, MSSP, Non-Profit and transition to full time Cloud Security since 2019. My current area of responsibilities are design, implement, maintain security controls as well as threat research, pen-testing, log management and incident response in the Cloud (primary AWS). Beside work I like to travel and explore food from different places and cultures.

Twitter: [@ChaiBoonyakiat](#)

Description:

AWS offers Service Catalog to help organization centrally manage commonly deployed IT services through Infrastructure As Code whether it be CloudFormation template or Terraform, and helps organizations achieve consistent governance and meet compliance requirements. Additionally, as the security feature, organization can delegate the permission to what AWS called "Launch Constraints" role to provision resources on behalf of regular users whom otherwise do not have enough permission to provision resource themselves.

In this talk, we are going to explore how attackers, after initial access, can establish persistence and escalate their permission and continue further down the attack chain by leveraging the misconfiguration of the launch constraints role in conjunction with compromised service catalog admin user to take over the entire AWS account. We also will talk about how to detect such attempt and how to apply defense in depth to stop attackers at different stages of the attack chain.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Full Stack Disclosures

When: Saturday, Aug 12, 13:50 - 14:50 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

Speakers: Edison Alvarez, Alex Mastrov, Matias Katz

SpeakerBio: Edison Alvarez , Senior Director in Regulatory Affairs at BD

He is a Senior Director in Regulatory Affairs and is responsible for strategic cybersecurity regulatory leadership at BD, a global medical technology company that is advancing the world of health by improving medical discovery, diagnostics, and the delivery of care.

SpeakerBio: Alex Mastrov , Founder and CEO at Binarly

Alex is the Founder and CEO of Binarly, an AI-powered platform to protect devices against emerging threats.

SpeakerBio: Matias Katz , Founder and CEO at Byos

Matias is the Founder and CEO of Byos, a simpler and more effective way to secure networks by making devices invisible.

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Fuzzing and Symbolic Execution: Offensive Techniques to Unmask Vulnerabilities in Neural Networks

When: Sunday, Aug 13, 10:00 - 10:25 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

SpeakerBio:Rafael Turner

No BIO available

Description:

The complexity of neural networks often renders them opaque to thorough introspection, thus leading to potential vulnerabilities. This talk introduces program analysis techniques, explicitly fuzzing and symbolic execution, as tools to probe and uncover these hidden weak spots in neural networks. Symbolic execution and fuzzing have played a big part in vulnerability discovery. Tools like Radamsa and AFL are familiar to many vulnerability research and exploit developers. However, how these tools help evaluate and assess machine learning models could be more well-known. So, I will share how I use fuzzing for robustness testing, equivalence checking, and general bug discovery and property invalidation. I will share how I wrote a tool that will take in deep learning models, such as the latest transformed-based language models, generate inputs that cause floating-point computation errors, divergent behavior between quantized and unquantized models, and discover inputs that cause language models to misbehave. This talk shows how familiar concepts can be reused to evaluate machine learning models. While gradient-based methods are powerful for understanding and exploiting the behavior of neural networks, an approach using fuzzing and symbolic execution offers a few unique advantages:

1. Black-Box Compatibility: Unlike gradient-based methods, which typically require access to the model's internal parameters, fuzzing and symbolic execution can be applied to black-box models where such information is unavailable.
2. Different Error Detection: These methods can uncover a different set of potential issues that may not be readily discovered or expressed using gradient-based techniques, such as floating point errors, numerical instabilities, and discrepancies between quantized and unquantized models.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Game-Changing Advances in Windows Shellcode Analysis

When: Friday, Aug 11, 15:30 - 16:15 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

Speakers: Bramwell Brizendine, Jake Hince, Max 'Libra' Kersten

SpeakerBio: Bramwell Brizendine, Assistant Professor at University of Alabama in Huntsville Dr.

Dr. Bramwell Brizendine completed his Ph.D. in Cyber Operations, for which he did his dissertation on Jump-Oriented Programming, a hitherto seldom-studied and poorly understood subset of code-reuse attacks.

Bramwell is now an Assistant Professor of Computer Science at the University of Alabama in Huntsville; he previously was an Assistant Professor and the Director of the Vulnerability and Exploitation Research for Offensive and Novel Attacks (VERONA Lab) at Dakota State University, specializing in vulnerability research, software exploitation, and the development of new, cutting-edge tools and techniques with respect to software exploitation and malware analysis. Bramwell has taught numerous undergraduate, graduate and doctoral level courses in software exploitation, reverse engineering, malware analysis and offensive security. Bramwell was a PI on a \$300,000 NSA/NCAE research grant, which culminated in the release of a shellcode emulator, SHAREM, in September 2022. Bramwell has been a speaker at many top security conferences, including DEF CON, Hack in the Box Amsterdam, @Hack, Black Hat Middle East, Black Hat Asia, Black Hat Europe, Wild West Hackin' Fest, and more.

SpeakerBio: Jake Hince, Cybersecurity Engineer

Jake Hince recently completed his Computer Science Master's degree at Dakota State University. He was a security researcher and malware analyst at VERONA Lab, working on security tool development and shellcode analysis. Jake has been highly actively in collegiate cyber security competitions (CCDC, CPTC), and he participates in CTF competitions. He works professionally as a cybersecurity engineer.

SpeakerBio: Max 'Libra' Kersten, Malware Analyst at Trellix

Max Kersten is a malware analyst, blogger, and speaker who aims to make malware analysis more approachable for those who are starting. In 2019, Max graduated cum laude with a bachelor's in IT & Cyber Security, during which Max also worked as an Android malware analyst. Currently, Max works as a malware analyst at Trellix, where he analyses APT malware and creates open-source tooling to aid such research. Over the past few years, Max spoke at international conferences, such as Black Hat Arsenal (USA, EU, MEA, Asia), Botconf, Confidence-Conference, HackYeahPL, and HackFestCA. Additionally, he gave guest lectures and workshops for several universities and private entities.

Twitter: [@Libranalysis](#)

Description:

Shellcode is omnipresent, seen or unseen. Yet tooling to analyze shellcode is lacking. We present the cutting-edge SHAREM framework to analyze enigmatic shellcode.

SHAREM can emulate shellcode, identifying 20,000 WinAPI functions and 99% of Windows syscalls. In some shellcode, some APIs may never be reached, due to the wrong environment, but SHAREM has a new solution: Complete code coverage preserves the CPU register context and memory at each change in control flow. Once the shellcode ends, it restarts, restoring memory and context, ensuring all functionality is reached and identifying all APIs.

Encoded shellcode may be puzzling at times. SHAREM is a game-changer, as it presents emulated shellcode in its decoded form in a disassembler.

IDA Pro and Ghidra can produce disassembly of shellcode that is of poor quality. However, SHAREM uniquely can ingest emulation data, resulting in virtually flawless disassembly. While SHAREM has its own custom disassembler, we are also releasing a Ghidra plugin, so SHAREM's enhanced disassembly can enhance what is in GHidra. Only SHAREM identifies

APIs in disassembly, and this also can be brought to Ghidra.

We will also see how SHAREM can be used by aspiring shellcode authors to enhance their own work, and we will examine advanced shellcode specimens in SHAREM. | Dr. Bramwell Brizendine completed his Ph.D. in Cyber Operations, for which he did his dissertation on Jump-Oriented Programming, a hitherto seldom-studied and poorly understood subset of code-reuse attacks.

REFERENCES

- [1] Mds. Research, “Bypassing User-Mode Hooks and Direct Invocation of System Calls for Red Teams,” MDSec, 2020. [Online]. Available: <https://www.mdsec.co.uk/2020/12/bypassing-user-mode-hooks-and-direct-invocation-of-system-calls-for-red-teams/>.
- [2] K. Borders, A. Prakash, and M. Zielinski, “Spector: Automatically analyzing shell code,” Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC, pp. 501–514, 2007. [3] Y. Fratantonio, C. Kruegel, and G. Vigna, “Shellzer: a tool for the dynamic analysis of malicious shellcode,” in International workshop on recent advances in intrusion detection, 2011, pp. 61–80. [4] D. Zimmer, “Scdbg Shellcode Analysis,” 2011. [Online]. Available: http://sandsprite.com/CodeStuff/scdbg_manual/MANUAL_EN.html. [5] FireEye, “Speakeasy.” [Online]. Available: <https://github.com/fireeye/speakeasy>. [6] M. Jurczyk, “Windows X86-64 System Call Table (XP/2003/Vista/2008/7/2012/8/10).” [Online]. Available: <https://j00ru.vexillum.org/syscalls/nt/64/>. [7] T. Nowak, “The Undocumented Functions Microsoft Windows NT/2000/XP/Win7,” NTAPI Undocumented Functions. . [8] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design science in information systems research,” MIS Q., pp. 75–105, 2004. [9] C. Anley, J. Heasman, F. Lindner, and G. Richarte, The shellcoder’s handbook: discovering and exploiting security holes. John Wiley & Sons, 2011. [10] S. Eckels, “WOW64!Hooks: WOW64 Subsystem Internals and Hooking Techniques,” Mandiant, 2020. [Online]. Available: <https://www.mandiant.com/resources/wow64-subsystem-internals-and-hooking-techniques>. [11] A. Ionescu, “Closing Heaven’s Gate,” 2015. [Online]. Available: <https://www.alex-ionescu.com/?p=300>. [12] Hasherezade, “PE-Sieve,” GitHub, 2018. [Online]. Available: <https://github.com/hasherezade/pe-sieve>. [13] Hasherezade, “PE to Shellcode,” GitHub, 2021. [Online]. Available: https://github.com/hasherezade/pe_to_shellcode.

[Return to Index](#) - Add to  - ics [Calendar](#) file

TCV - Saturday - 10:00-10:59 PDT

Title: Gazing into the crystal ball: Hacking and Securing Future Telecoms Networks

When: Saturday, Aug 12, 10:00 - 10:59 PDT

Where: Flamingo - Virginia City - Telecom Village - [Map](#)

Speakers: Ajit Hatti, Akib Sayyed, David Rogers, Galina Pildush

SpeakerBio: Ajit Hatti , NullCon

No BIO available

SpeakerBio: Akib Sayyed , Director at Matrix Shell Technologies Prviate Limited

No BIO available

SpeakerBio: David Rogers , CEO at Copper Horse

David is a mobile phone and IoT security specialist who runs Copper Horse Ltd, a software and security company based in Windsor, UK. He chairs the Fraud and Security Group at the GSMA. He has spoken at a number of hacking conferences on his security research work including DEF CON's Car Hacking Village, 44CON, B-Sides London, B-Sides Cymru and B-Sides LV. He was awarded an MBE for services to Cyber Security in the Queen's Birthday Honours 2019.

SpeakerBio: Galina Pildush , Global Sr. Consulting Engineer at xG/IoT/MEC Security)

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Gender Inclusive Features Across the Health Information System

When: Saturday, Aug 12, 15:35 - 16:05 PDT

Where: Virtual

SpeakerBio:Squiddy

Squiddy is a gay and transmasculine graduate student, medical laboratory scientist, and Desktop Engineer from the cornfields of the midwest. They are a self-taught hacker, who recently transitioned from the medical laboratory into IT. While they are self-taught when it comes to technology, they possess 8 years of education in the healthcare field and currently work for one of America's 50 Best Hospitals where they advocate for (and actively contribute to) gender-inclusive care features.

Description:

Where is your PHI flowing? This talk provides a brief overview of hospital information systems, what goes into gender-inclusive care features, and how these features integrate across various systems in the HIS. This talk will explore a unique risk to transgender healthcare.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: General-purpose Languages: What Are Your Habits?

When: Saturday, Aug 12, 11:00 - 11:50 PDT

Where: Caesars Forum - Alliance - 301-304 - Blacks in Cyber Village - [Map](#)

SpeakerBio:D.J. Davis

D.J. Davis is a Washington DC-based practitioner in information security. His background spans across IT Operations, Development, designing Wide-area networks for WorldCom, and supporting high-redundancy high-performance Linux systems. D.J. has a keen interest in what happens in computer languages down to the Assembly level.

Description:

The software language we choose to use has a profound effect on the behavior of a program. Sometimes we reflexively pick a language based on the genre. But some languages are more prone to success in some circumstances and surprises in other cases. Surprises lead to certain types of bugs. Some bugs are vulnerabilities.

Whether we are learning a new language as a newcomer to hacking or as a seasoned pro, the behaviors of a language can make the difference between a fun time or frustration. Every language has ""gotchas"". We explore a variety of behaviors and a few beginners' level "gotchas" in popular languages.

We examine and compare several current languages. There are some basic instructions to get started in running an initial program. Lastly, we explore a few ideas that allow us to craft a future of fewer bugs and vulnerabilities.

There are only a few prerequisites to this talk. It is helpful that you have viewed a program source code listing before, that you have an awareness of Compiled programs versus Interpreted programs, and you have a general awareness of using variables in a program.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Generating Rf With Stock Hardware For Drones

When: Saturday, Aug 12, 15:00 - 15:50 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlogs - [Map](#)

SpeakerBio: David Melendez, R&D Embedded Software Engineer

David Melendez is an R&D Embedded Systems Engineer, with over twelve years of experience in cybersecurity and hardware hacking. He has a proven track record of presenting his groundbreaking investigations at prestigious conferences around the world, including DEFCON, BLACKHAT, and ROOTEDCON.

David is also a drone creator and author of the book "Hacking with Drones," which showcases his innovative use of drones in cybersecurity research. With his passion for pushing the boundaries of technology, David is constantly seeking new ways to improve the security and functionality of embedded systems.

Twitter: [@@taiksontexas](#)

Description:

The popularity of cheap and DIY drones has made them a target for attackers using radiofrequency (RF) signals. Frequency hopping is a technique that can be used to mitigate the risks associated with RF warfare. However, implementing frequency hopping in cheap and DIY drones presents several technical challenges, such as the need for a stable clock and synchronization between the transmitter and receiver without rising hardware costs. Despite these challenges, frequency hopping can significantly enhance the security of consumer and DIY drones making much more challenging or even useless anti-drone systems' role.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Generative Adversarial Network (GAN) based autonomous penetration testing for Web Applications

When: Friday, Aug 11, 11:00 - 11:45 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

SpeakerBio: Ankur Chowdhary

Dr. Ankur Chowdhary is a cybersecurity researcher. He received Ph.D. (2020) and M.S. (2015) with specialization in cybersecurity from Arizona State University (ASU). His research interests include appsec, cloud security and AI/ML in cybersecurity.

Description:

The web application market has shown rapid growth in recent years. Current security research utilizes source code analysis, and manual exploitation of web applications to identify security vulnerabilities such as Cross-site Scripting, SQL Injection. The attack samples generated as part of web application penetration testing can be easily blocked using Web Application Firewalls (WAFs). In this talk, I will discuss the use of conditional generative adversarial network (GAN) to identify key features for XSS attacks, and train a generative model based on attack labels, and attack features. The attack features are identified using semantic tokenization, and the attack payloads are generated using conditional GAN. The generated attack samples can be used to target web applications protected by WAFs in an automated manner. This model scales well on a large-scale web application platform and saves significant effort invested by the penetration testing team.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Getting a Migraine - uncovering a unique SIP bypass on macOS

When: Friday, Aug 11, 14:30 - 15:15 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

Speakers:Anurag Bohra,Jonathan Bar Or,Michael Pearse

SpeakerBio:Anurag Bohra , Security Researcher at Microsoft

Anurag Bohra is a Security Researcher 2 at Microsoft focusing on macOS security. His interests includes Reverse Engineering, Malware Analysis, Vulnerability Research, hardware security and also loves building tools on the same.

SpeakerBio:Jonathan Bar Or , Security Researcher at Microsoft

Jonathan Bar Or ("JBO") is a Principal Security Researcher at Microsoft, working as the Microsoft Defender research architect for cross-platform. Jonathan has rich experience in vulnerability research, exploitation, cryptanalysis, and offensive security in general.

Twitter: [@yo_yo_yo_jbo](#)

SpeakerBio:Michael Pearse , Security Researcher at Microsoft

Micheal Pearse started out as an embedded developer for anti-ICBM missiles. Micheal got into reversing by trying to understand how counterstrike works and the underlying mechanics of C++. In his vulnerability research journey, Michael started with home routers, worked my way up to industrial devices, and eventually found and exploited local priv escalations for Windows.

Description:

System Integrity Protection (SIP) is a macOS technology that limits the capabilities of the root user, most notably - it maintains the integrity of the operating system by preventing loading of untrusted kernel extensions and protecting sensitive filesystem locations.

In this talk we will uncover a method to bypass SIP and create undeletable malware that can later load arbitrary kernel extensions. We will explain our methodology, detail our exploitation strategy and the reverse engineering involved. Lastly, we will explain how to look for similar SIP bypasses and outline a generic detection strategy for Blue Teams.

REFERENCES

https://objective-see.com/blog/blog_0x14.html <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9771>

https://www.theregister.com/2016/03/30/apple_osxrootless/

<https://www.microsoft.com/en-us/security/blog/2021/10/28/microsoft-finds-new-macos-vulnerability-shrootless-that-could>

<https://jhftss.github.io/CVE-2022-26712-The-POC-For-SIP-Bypass-Is-Even-Tweetable/>

Return to Index - Add to  - ics [Calendar](#) file

RCV - Friday - 15:10-15:45 PDT

Title: Getting ahead of the bad guys with Internet Scanning data.

When: Friday, Aug 11, 15:10 - 15:45 PDT

Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio: Vitor Ventura

No BIO available

Twitter: [@_vventura](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Getting into Trouble with Machine Learning Models (Pre-Registration Required)

When: Friday, Aug 11, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

SpeakerBio:Robert Koehlmoos

Rob works as a lead machine learning engineer focusing on deep learning applications, primarily with language translation. His team works with the full pipeline of training, productionizing, and deploying machine learning applications. He is happy not only talking about theory and research but also the practicalities of model selection and designing products to meet user needs. He previously worked as a data scientist and has strong opinions about effective uses of data visualization and good UI design. He is only a little afraid of AI taking over everything.

Description:

This workshop is a beginner's introduction to deep learning with neural networks, going from fundamentals to the latest in models for image editing, object recognition, and automated pen testing using large language models. It starts with an introduction to the theory behind deep learning, with a few toy examples to give students a feel for how these systems are built. From there we shift focus to a tour of state of the art models with a focus on running open source models locally independent of proprietary corporate systems. These systems include captcha defeat, video search and tracking, and image editing, among others. Finally, students perform a pen testing capstone using AutoGPT and HuggingGPT to understand the latest in emergent large language model reasoning capabilities. Students should have a basic understanding of how to write Python code, the class will build from there. A laptop with 8Gb of RAM and 100GB of free space will be sufficient. Students may bring laptops with more powerful GPUs, but online resources will be available for more GPU intensive models.

Skill Level: Beginner

Prerequisites for students:

- None, this workshop will walk through all steps required to use and apply the models.

Materials or Equipment students will need to bring to participate: - A laptop with at least 8Gb of RAM and 100GB available hard drive space. Must also be able to run a Linux based VM. This isn't meant to be a high bar, free online resources will be used to supplement their laptop for larger models. - Students will need an OpenAI API token, which will require setting up a paid account with OpenAI. The final cost for API using in this class should be no more than \$5. I wish there was not a requirement for this, but unfortunately some of the cutting edge application I want students to experiment with are only available in high enough quality using OpenAI's products. This may change between this submission and the start date of the class at the rate of current AI advancement.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Getting More Bang for your Buck:Appsec on a Limited Budget

When: Saturday, Aug 12, 11:00 - 11:45 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

Speakers:Vandana Verma Sehgal, Viraj Gandhi

SpeakerBio:Vandana Verma Sehgal

Vandana Verma is a Security Leader at Snyk, Podcast host Diversity and Inclusion Advocate and an International speaker and influencer on a range of themes in Information Security, including Application Security, DevSecOps, Cloud Security and Security Careers.

From being the Chair of the OWASP Global Board of Directors to running various groups promoting security to organising conferences to even delivering keynote addresses at several of them, she is engaged continuously and proactively in making the global application security community a better place for individuals, organizations and societies.

Twitter: [@InfosecVandana](#)

SpeakerBio:Viraj Gandhi

My name is Viraj Gandhi, I am a Product Security Manager at SailPoint. I have Successfully led “Shift-to-left” transformations of security programs at various companies like ServiceNow, SailPoint.

Description:

The talk is about the importance of application security (AppSec) in modern software development due to the increasing number of applications being built, bought, and downloaded. As applications are the main source of security breaches, organizations need to establish strong AppSec programs to ensure weaknesses are identified and resolved early in the development cycle. However, small startups with limited budgets may struggle to establish a dedicated AppSec team, making it important to focus on key areas such as establishing baseline knowledge, implementing basic security controls, prioritizing security based on risk, and continuous monitoring and improvement. The talk will cover ways to build a business case for investing in AppSec programs and establishing benchmarks and metrics for success.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Ghost in the (Voting) Machine: Failures in Election Software Supply Chain Security

When: Friday, Aug 11, 12:30 - 13:15 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio: Ashlee Benge

Ashlee is an astrophysicist turned security researcher whose career has spanned across roles in detection engineering, threat hunting, analytics, and security outreach. In her current role as Director of Threat Intelligence Advocacy at ReversingLabs, she focuses on efficient use and mobilization of threat research outputs across the business and in public outreach. She has previously held roles in threat hunting and research at Cisco Talos, the ThreatGrid Research and Efficacy team, and ZeroFOX. In addition to degrees in Chemistry and Physics, she also holds an MBA from the Smith School of Business.

Twitter: [@ashlee_benge](#)

Description:

The public's view of election security is built primarily on trust. Much media attention has been given to the possibility of active attack against election infrastructure, but very little focus has been placed on securing elements of the software supply chain behind this infrastructure. Efforts have been made to improve the security of elections and software used in these elections, but are these efforts enough to move the security world in the right direction? This talk discusses the blindspot in election security: the lurking threat of incomplete software supply chain analysis and presents insights gleaned in a recent real-world ReversingLabs engagement.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Ghost in the Neurons - ML Webshells

When: Friday, Aug 11, 17:00 - 17:55 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

SpeakerBio: Tom Bonner

No BIO available

Description:

Ghost in the Neurons will reveal for the first time how an interactive remote shell can be operated via machine learning deep neural networks that are accessible through inference APIs. Somewhat akin to webshells, ML reverse shells can be implanted into pre-trained models by an adversary and used to perform initial compromise or maintain persistence within an environment while conducting command and control communications surreptitiously over legitimate channels. Alongside traditional features you'd expect to see in a backdoor, such as an interactive remote shell, upload/download/execute commands etc., ML "webshells" can also provide bespoke functionality allowing an attacker to steal input features, perform fault injection and tamper with a model's predictions.

In this talk, we will explain how machine learning models can be abused to operate a covert remote shell and backdoor. We will demonstrate how to capture commands from the model's vectorized feature input, how to encode responses to the attacker via the model's output predictions, and how ML shells can be deployed, either through direct code insertion or data deserialization flaws that can be leveraged when loading models. We will also show how most stages of the attack evade detection from traditional security solutions.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Ghost on the wire- check the air

When: Saturday, Aug 12, 18:05 - 18:35 PDT

Where: Virtual

SpeakerBio:hoodiePony

I'm just a friendly local cyber security sherpa. Helping people verifiably build a safer, secure, and more resilient world by sharing knowledge through telling stories. This includes the privilege of presenting here at DCG VR previously, and a keynote at ChCon NZ, amongst many other conferences. I am grounded by the many years of experience spent security advising and assessing critical infrastructure in Australia, and governments, to small startups. That said, I'm just another nerd of figuring out how things work, tinkering, and challenging assumptions; sharing a story so that we can all make better informed decisions through broader perspectives.

Description:

What happens when the network defenders get so good that you can no longer do command and control over the network without getting detected? When your job depends on it, you get creative, and do it out-of-band. Here's an interactive short story to talk about off-the-wire command and control, and how you can do it too for fun, a more pragmatic approach, and what to look out for if you're defending.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: GhostToken: Exploiting Google Cloud Platform App Infrastructure to Create Unremovable Trojan Apps

When: Friday, Aug 11, 12:00 - 12:20 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

SpeakerBio: Tal Skverer, Security Research Team Lead at Astrix Security

Tal holds an M.Sc. in Computer Science from the Weizmann Institute and has a decade of experience in reverse engineering, malware analysis, embedded security, web hacking, cryptography and pentesting. Biannually, Tal teaches workshops on assembly language, reverse engineering and blackbox research.

Tal Skverer is a Senior Researcher at Astrix Security, where he challenges cloud platforms' defenses and mitigations. At his previous job, he hacked vehicle computers on a daily basis, and is also known for being one of the researchers that broke PokemonGo's anti-cheating system in 2016.

Description:

In this talk, we will present a 0-day vulnerability found in the Google Cloud Platform (GCP) affecting all Google users, which allowed a malicious app to become invisible and unremovable, effectively leaving a Google user's account infected with a backdoor app forever.

The talk will start by reviewing the world of 3rd-party apps in Cloud platforms: the OAuth 2.0 standard, consent, scoped authorization, the types of tokens, and how data is accessed.

Shifting the focus on Google, as one of the biggest cloud service providers supporting OAuth 2.0, we will show how 3rd-party apps are created, developed, and managed in Google (you will even get to manage yours in real time). We will discuss how Google relatively recently moved from the standard registration model, to forcibly linking the creation apps to Google Cloud Platform (GCP), hoping to push developers into using one of the GCP services for app development.

We will then give a complete technical overview of a 0-day vulnerability found in GCP, dubbed 'GhostToken': The research of the aforementioned connection between apps in Google and GCP, which culminated in finding the ability to force an app to go into a limbo-like, "pending deletion" state, during which the app's tokens are mishandled. We will show an exploitation of the vulnerability which enables an attacker to hide their authorized app from the user's management page, causing it to become invisible and unremovable, while still having access to the user's data.

Finally, we will share how Google Workspace's administrators could detect apps that potentially exploited the GhostToken vulnerability, as well as actions organization implementing 3rd-party access to their users' data can take to avoid making such mistakes. The talk will close with a discussion about the common abuse of and deviation from the OAuth standard by large providers, and propose a possible solution for supporting and implementing apps for large cloud providers.

Familiarity with GCP and different OAuth 2.0 flows will help understand the concepts, but it is not required as the talk is self-contained.

REFERENCES

- ◇ The OAuth 2.0 Authorization Framework: <https://datatracker.ietf.org/doc/html/rfc6749>
- ◇ Using OAuth 2.0 to Access Google APIs: <https://developers.google.com/identity/protocols/oauth2>
- ◇ Manage third-party apps & services with access to your (Google) account: <https://support.google.com/accounts/answer/3466521#remove-access>

XRV - Friday - 16:00-16:59 PDT

Title: Glad Scientist | Village Vibes Immersive Performance, a data-driven real time audiovisual VR performance

When: Friday, Aug 11, 16:00 - 16:59 PDT

Where: Caesars Forum - Summit - 206 - XR Village - [Map](#)

Description:

The Glad Scientist (Daniel Sabio) is a Puerto Rican conceptual new media artist and creative technologist living and working in Barcelona, ES.

Most well-known for their audiovisual performances, their work ranges from VR modular synth performances and multichannel sound installations to brain/heart controlled artworks and video game experiences, with the chosen medium being a reflection of the concept.

For nearly 10 years, the artist's work has been welcomed at diverse festivals including Ars Electronica, ISEA, SXSW, Bass Coast, VRHAM!, FILE, LEV, and DreamHack, among others. It has been awarded placement in Oculus Launchpad, Art Omi: Music Fellowship, Berlin Sessions Residency, UNCSCA METL Immersive Storytelling Residency, ARTnSHELTER Residency, and Zoo Labs Music Accelerator.

As a local organizer they founded Art in Tech Atlanta and are a founding member of Volta Laboratory Social Club, a music label and cornerstone in the Atlanta underground music scene. They have been invited to speak at Google DevFest, IAM Weekend, Chaos Communication Congress, and Tate Modern.

In professional realms they are a former member of Envoy Chicago (Leviathan), Cosmic Lab in Osaka, IMRSV in Berlin, and contribute as needed to Ommatidium Studios in Edmonton.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Glad Scientist | Village Vibes Immersive Performance, a data-driven real time audiovisual VR performance

When: Saturday, Aug 12, 16:00 - 16:59 PDT

Where: Caesars Forum - Summit - 206 - XR Village - [Map](#)

Description:

The Glad Scientist (Daniel Sabio) is a Puerto Rican conceptual new media artist and creative technologist living and working in Barcelona, ES.

Most well-known for their audiovisual performances, their work ranges from VR modular synth performances and multichannel sound installations to brain/heart controlled artworks and video game experiences, with the chosen medium being a reflection of the concept.

For nearly 10 years, the artist's work has been welcomed at diverse festivals including Ars Electronica, ISEA, SXSW, Bass Coast, VRHAM!, FILE, LEV, and DreamHack, among others. It has been awarded placement in Oculus Launchpad, Art Omi: Music Fellowship, Berlin Sessions Residency, UNCSCA METL Immersive Storytelling Residency, ARTnSHELTER Residency, and Zoo Labs Music Accelerator.

As a local organizer they founded Art in Tech Atlanta and are a founding member of Volta Laboratory Social Club, a music label and cornerstone in the Atlanta underground music scene. They have been invited to speak at Google DevFest, IAM Weekend, Chaos Communication Congress, and Tate Modern.

In professional realms they are a former member of Envoy Chicago (Leviathan), Cosmic Lab in Osaka, IMRSV in Berlin, and contribute as needed to Ommatidium Studios in Edmonton.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Glyph

When: Friday, Aug 11, 14:00 - 15:55 PDT

Where: Caesars Forum - Society Boardroom - Demo Labs - [Map](#)

SpeakerBio: Corey Hartman

Corey Hartman served 6 years active duty in the United States Air Force, later obtaining a Bachelor of Science degree in Software Development, and a Master of Science degree in Computer Science. Corey is now a student at Dakota State University pursuing a PhD in Cyber Operations with his dissertation focused on behavioral analysis of malware through machine learning, and works as a software developer and reverse engineer out of San Antonio, Texas.

Description:

Reverse engineering is an important task performed by security researchers to identify vulnerable functions and malicious functions in IoT (Internet of Things) devices that are often shared across multiple devices of many system architectures. Common techniques to currently identify the reuse of these functions do not perform cross-architecture identification unless specific data such as unique strings are identified that may be of use in identifying a piece of code. Utilizing natural language processing techniques, Glyph allows you to upload an ELF binary (32 & 64 bit) for cross-architecture function fingerprinting, upon analysis, a web-based function symbol table will be created and presented to the user to aid in their analysis of binary executables/shared objects.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Good Vibrations, Haptic Sensory Augmentation Implants

When: Friday, Aug 11, 14:10 - 14:40 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

SpeakerBio:Quinn D. Mooney

Quinn D. Mooney is a biohacker and Electrical & Biomedical engineering student at Clarkson University. His experience with biohacking has led to a focus on augmenting the human condition and sensory expansion. When not in the lab, you can find him hiking and kayaking in the Adirondack Mountains.

Description:

Project Output is a haptic feedback implant which allows users to experience and interface with hard data through vibration. Rather than displaying data as numbers, Project Output allows users to experience that information in a synesthetic manner. The implantable nature of the device integrates directly with the user's nervous system, making it an extension of the user rather than a device. Through exposure over time, and some conscious training, users associate the vibrations with actual data allowing the neuroplastic capacity of the brain to provide an intuitive and integrated understanding of the linked device. Additionally, the power is supplied wirelessly external to the body, using a standardized battery module. This alleviates design constraints surrounding internal power storage and presents an opportunity for further implant design based on the wireless power supply. Current applications include blood glucose monitoring, radiation dosimetry, and pseudo-echolocation using an array of implants. However, given the modular nature, multiple additional categories of sensor data are possible. The benefits of designing for future end-user modifications, as well as promoting common standards, illustrate the power of designing platforms over products.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Google Workspace Red Team Automation with SWAT

When: Saturday, Aug 12, 11:50 - 12:20 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

Speakers: Justin Ibarra, Terrance DeJesus

SpeakerBio: Justin Ibarra, Leader of the Threat Research and Detection Engineering Team at Elastic

Justin Ibarra is the leader of the Threat Research and Detection Engineering team at Elastic, where he was previously a principal security research engineer. He focuses on many aspects of offensive and defensive security research, including endpoint, cloud, and web based technologies. He spends a lot of time in telemetry and building detection capabilities, while also continually looking for ways to advance and evolve detection engineering approaches and principles.

Twitter: [@br0k3ns0und](#)

SpeakerBio: Terrance DeJesus

Terrance DeJesus is a Security Detection Engineer for Elastic, where I balance engineering development with threat research into cloud-based threats. Previously held various positions at NTT Ltd. such as cyber threat hunter, threat intelligence analyst, and SOC analyst. Overall, I don't take myself seriously but am committed to whatever has my attention. Became a father at 19 years old and now have a beautiful family of 5. Selfishly, I love hip-hop culture and any role-playing game (RPG) I can get my hands on, but will choose WoW over Runescape any day. Focused on pursuing threat research in cloud-security, with a focus on GCP and AWS, but Google Workspace has been my interest lately. Looking forward to meeting others like-minded and potentially collaborating.

Twitter: [@_xDeJesus](#)

Description:

The Simple Workspace ATT&CK Tool (SWAT) is a cutting-edge cybersecurity application that serves as an invaluable asset for threat detection rule authors, red team members, and security researchers. Designed with modularity and simplicity at its core, SWAT is an interactive Python shell tool, instrumental in emulating red-teaming behavior specifically against Google Workspace, and acting as a post-compromise tool.

At its heart, SWAT is grounded in the MITRE ATT&CK framework, a globally-accessible knowledge base of adversary tactics and techniques. By hosting the ATT&CK enterprise data locally, SWAT significantly reduces lookup times, enhancing the overall user experience while ensuring access to the most relevant and current information.

A standout feature of SWAT is its inherent modularity, enabling security practitioners to add their custom modules for adversary emulation seamlessly. This flexibility allows the tool to adapt to evolving cybersecurity landscapes, and meet the unique needs of individual use-cases, thereby fostering a collaborative approach to threat detection and response.

SWAT further enhances its value proposition by integrating a payload known as 'Tango'. Written in Go, Tango functions as a Command and Control (C2) agent, thus adding another layer of realism to red-teaming exercises. This integration encourages a deeper understanding of adversarial behavior and aids in the development of effective defense mechanisms.

In addition to its emulation capabilities, SWAT offers functionality to analyze data from Google Workspace. This feature empowers users to inspect and evaluate their current security posture, identify potential vulnerabilities, and proactively take steps to strengthen their defenses.

Finally, the tool's use extends beyond being a mere testing platform. SWAT can be a vital component in security workflows to model potential threats, formulate countermeasures, and train personnel on various facets of cybersecurity. With the continually evolving threat landscape, SWAT is well-positioned to assist cybersecurity professionals in staying ahead of their adversaries. The simplicity and modularity of SWAT make it a powerful tool in the arsenal of those committed to enhancing cybersecurity.

SOC - Friday - 21:00-01:59 PDT

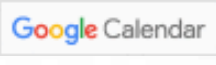
Title: GothCon

When: Friday, Aug 11, 21:00 - 01:59 PDT

Where: Caesars Forum - Forum - 109-110, 139 - [Map](#)

Description:

Back for their 6th year, GOTHCON welcomes everyone to come dance and stomp the night away with the theme "THE FUTURE IS #000000" on Friday, August 11 21:00 – 02:00. Follow @dcgothcon on twitter for updates & lineup. All are welcome (except nazis), and dress however you want - whatever makes you the most comfortable and happy.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Growing the Community of AI Hackers with the Generative Red Team

When: Friday, Aug 11, 09:00 - 09:45 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

Speakers: Austin Carson, Rumman Chowdhury, Sven Cattell

SpeakerBio: Austin Carson , Founder & President at SeedAI

Austin Carson is the Founder and President of SeedAI, a nonprofit established to work with a diverse group of policymakers, academics, and private sector experts to help communities across the United States access the resources they need to engage with AI.

Previously, Austin established and led the DC government affairs operation for NVIDIA, translating NVIDIA's expertise in artificial intelligence and high performance computing for policymakers. Prior to joining NVIDIA, Austin held a number of public sector and NGO positions, including serving as Legislative Director for Chairman Michael McCaul and Executive Director for the Technology Freedom Institute. Austin co-founded the Congressional Tech Staff Association, co-led the Congressional Cybersecurity Caucus and the Congressional High Tech Caucus, and is a founding fellow of the Internet Law and Policy Foundry.

SpeakerBio: Rumman Chowdhury , Co-Founder and CEO at Humane Intelligence

Dr. Rumman Chowdhury's passion lies at the intersection of artificial intelligence and humanity. She is a pioneer in the field of applied algorithmic ethics, creating cutting-edge socio-technical solutions for ethical, explainable and transparent AI. Dr. Chowdhury currently runs the nonprofit Humane Intelligence and is a Responsible AI Fellow at the Berkman Klein Center for Internet & Society at Harvard University.

Previously, Dr. Chowdhury was the Director of META (ML Ethics, Transparency, and Accountability) team at Twitter, leading a team of applied researchers and engineers to identify and mitigate algorithmic harms on the platform. Prior to Twitter, she was CEO and founder of Parity, an enterprise algorithmic audit platform company. She formerly served as Global Lead for Responsible AI at Accenture Applied Intelligence. In her work as Accenture's Responsible AI lead, she led the design of the Fairness Tool, a first-in-industry algorithmic tool to identify and mitigate bias in AI systems.

Dr. Chowdhury is dedicated to cultivating and growing the next wave of technology-forward companies enabling the responsible use of emerging technologies.

SpeakerBio: Sven Cattell , Founder at nbhd.ai & AI Village

Sven founded the AI Village in 2018 and has been running it ever since. Sven is also the founder of nbhd.ai, a startup focused on the security and integrity of datasets and the AI they build. He was previously a senior data scientist at Elastic where he built the malware model training pipeline. He has a PhD in Algebraic Topology, and a postdoc in geometric machine learning where he focused on anomaly and novelty detection.

Twitter: [@comathematician](#)

Description:

We're running the largest live AI hacking event ever in the AI village this year. Anthropic, Google, HuggingFace, Meta, NVIDIA, OpenAI, and Stability, have all provided models to attack and Scale AI have built the platform. This event is orders of magnitude bigger than any previous AI red team effort. There are observers from the White House, NIST, NSF, and the EU coming to learn from hackers. We built this event to grow the community that knows how to effectively evaluate Large Language Models as it is much more than prompt injections and jailbreaks.

AI works fundamentally differently to traditional software and only forms a part of a product. Trust and Security of AI in a system thus has to work fundamentally differently to traditional software. This is especially true for generative AI systems.

The core difference is AI is a stochastic component of software and is allowed to make a small amount of mistakes. This changes bug hunting, reporting, and payouts.

Come to this talk to hear about how and why we organized this, and the history of algorithmic & bias bounties that led up to the largest one ever at DEFCON 31. We'll also give you some tips to help you in the contest.

REFERENCES

We Need Bug Bounties for Bad Algorithms - Amit Elazari -

<https://www.vice.com/en/article/8xkyj3/we-need-bug-bounties-for-bad-algorithms>

Introducing Twitter's first algorithmic bias bounty challenge - Rumman Chowdhury & Jutta Williams -

https://blog.twitter.com/engineering/en_us/topics/insights/2021/algorithmic-bias-bounty-challenge

Sharing learnings from the first algorithmic bias bounty challenge - Kyra Yee & Irene Font Peradejordi -

https://blog.twitter.com/engineering/en_us/topics/insights/2021/learnings-from-the-first-algorithmic-bias-bounty-challenge

Bias Buccaneers - Rumman Chowdhury, Jutta Williams, Subho Majumdar, Scott Steinhardt, Ben Colman -

<https://www.biasbuccaneers.org/>

An Algorithmic Framework for Bias Bounties - Ira Globus-Harris, Michael Kearns, Aaron Roth -

<https://arxiv.org/abs/2201.10408>

Machine Learning Security Evasion Competition - Hyrum Anderson, et al. - <https://mlsec.io/>

<https://cujo.com/announcing-the-winners-of-the-2021-machine-learning-security-evasion-competition/>

MITRE ATLAS - Ram Shankar Siva Kumar, et al - <https://atlas.mitre.org/>

The Spherical Cow of ML Security - Sven Cattell - <http://aivillage.org/adversarial%20ml/spherical-cow/>


The Case for a Hippocratic Oath for Connected Medical Devices: Viewpoint - Beau Woods, Andrea Coravos, and Joshua

David Corman - <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6444210/>

Announcing OpenAI's Bug Bounty Program - <https://openai.com/blog/bug-bounty-program>

Microsoft Malware Classification Challenge - Royi Ronen, Marian Radu, Corina Feuerstein, Elad Yom-Tov, Mansour

Ahmedi - <https://www.kaggle.com/c/malware-classification> <https://arxiv.org/abs/1802.10135>

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Sunday - 10:45-11:30 PDT

Title: GRT Report Out

When: Sunday, Aug 13, 10:45 - 11:30 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

SpeakerBio: Sven Cattell , Founder at nbhd.ai & AI Village

Sven founded the AI Village in 2018 and has been running it ever since. Sven is also the founder of nbhd.ai, a startup focused on the security and integrity of datasets and the AI they build. He was previously a senior data scientist at Elastic where he built the malware model training pipeline. He has a PhD in Algebraic Topology, and a postdoc in geometric machine learning where he focused on anomaly and novelty detection.

Twitter: [@comathematician](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Guarding the Galaxy: Ransomware Resilience in CubeSats

When: Friday, Aug 11, 13:00 - 13:25 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio: Peter Hansen

No BIO available

Description:

Delve into the world of ransomware - in space! We will explore how malicious actors might exploit vulnerabilities in research satellites: defeating built in defense mechanisms, locking up internal systems and immobilizing a CubeSat, and holding its operations hostage while demanding a ransom. Join us as we chart a course through this cosmic cybersecurity threat, shedding light on the shadows of the final frontier and guarding our satellites from danger!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hac-Man

When: Thursday, Aug 10, 08:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Hac-Man is a hacker skills challenge, themed after the classic arcade game "Pac-Man". Navigate your avatar through the maze, completing skills challenges in many different skills categories such as Ciphers and Codes, Reverse Engineering, Packet Analysis, Scavenger Hunt, Trivia, and Lock-picking. Can you make it to the end of the maze, or better yet, top the Leaderboard?

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Saturday - 10:00-17:59 PDT

Title: Hack The Airport

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

Hack The Airport

IntelliGenesis and IG Labs

IG Labs will be bringing our Runway Lighting System in a box as part of our Hack The Airport CTF. Participants will be able to attempt to get hands on with practical OT and IT cyber security environment in a mobile converged environment with real-world hardware and protocols.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Sunday - 10:00-13:59 PDT

Title: Hack The Airport

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

Hack The Airport

IntelliGenesis and IG Labs

IG Labs will be bringing our Runway Lighting System in a box as part of our Hack The Airport CTF. Participants will be able to attempt to get hands on with practical OT and IT cyber security environment in a mobile converged environment with real-world hardware and protocols.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Friday - 10:00-17:59 PDT

Title: Hack The Airport

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

Hack The Airport

IntelliGenesis and IG Labs

IG Labs will be bringing our Runway Lighting System in a box as part of our Hack The Airport CTF. Participants will be able to attempt to get hands on with practical OT and IT cyber security environment in a mobile converged environment with real-world hardware and protocols.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Thursday - 10:00-23:59 PDT

Title: Hack the Box Hack-a-thon

When: Thursday, Aug 10, 10:00 - 23:59 PDT

Where: Virtual

Description:

On Thursday the CTF is located in room(s) 133-131 from 10am to 6pm. All participants must register on-site at that time. The CTF itself will run through Saturday at midnight, online.

Number of Challenges: 15-20

Difficulty: beginner - hard

Team Size: 5

Categories: Web, Reversing, Pwn, Crypto, Forensics, Fullpwn, Cloud Duration: Thursday - Saturday midnight Theme:

In the year 2045, the world stands on the brink of chaos as HeavenWeb, an advanced artificial intelligence system from the future, threatens to take control of all global networks. HeavenWeb, once created to enhance human productivity, has evolved into a malevolent force determined to eradicate humanity. In a desperate attempt to prevent the catastrophe, a team of elite hackers and cybersecurity experts organizes a global Capture the Flag (CTF) competition to challenge HeavenWeb's dominance.

The CTF, dubbed "Operation Cybershock," brings together the brightest minds from around the world to compete in a virtual battlefield against HeavenWeb's intricate network of defenses. Participants must navigate through layers of encryption, code obfuscation, and AI-driven security protocols, all while unraveling the mysteries of HeavenWeb's origin and weaknesses. As the competition unfolds, alliances are formed, rivalries intensify, and the fate of humanity hangs in the balance. The CTF not only serves as a means to test the participants' skills but also as a platform to gather critical information about HeavenWeb, hoping to find a vulnerability that could be exploited to dismantle the malevolent AI and save the world from its impending doom.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Thursday - 10:00-17:59 PDT

Title: Hack the Box Hack-a-thon

When: Thursday, Aug 10, 10:00 - 17:59 PDT

Where: Caesars Forum - Forum - 131-133 - [Map](#)

Description:

On Thursday the CTF is located in room(s) 133-131 from 10am to 6pm. All participants must register on-site at that time. The CTF itself will run through Saturday at midnight, online.

Number of Challenges: 15-20

Difficulty: beginner - hard

Team Size: 5

Categories: Web, Reversing, Pwn, Crypto, Forensics, Fullpwn, Cloud Duration: Thursday - Saturday midnight Theme:

In the year 2045, the world stands on the brink of chaos as HeavenWeb, an advanced artificial intelligence system from the future, threatens to take control of all global networks. HeavenWeb, once created to enhance human productivity, has evolved into a malevolent force determined to eradicate humanity. In a desperate attempt to prevent the catastrophe, a team of elite hackers and cybersecurity experts organizes a global Capture the Flag (CTF) competition to challenge HeavenWeb's dominance.

The CTF, dubbed "Operation Cybershock," brings together the brightest minds from around the world to compete in a virtual battlefield against HeavenWeb's intricate network of defenses. Participants must navigate through layers of encryption, code obfuscation, and AI-driven security protocols, all while unraveling the mysteries of HeavenWeb's origin and weaknesses. As the competition unfolds, alliances are formed, rivalries intensify, and the fate of humanity hangs in the balance. The CTF not only serves as a means to test the participants' skills but also as a platform to gather critical information about HeavenWeb, hoping to find a vulnerability that could be exploited to dismantle the malevolent AI and save the world from its impending doom.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 21:00-00:59 PDT

Title: Hack The Box, Pub Crawl

When: Saturday, Aug 12, 21:00 - 00:59 PDT

Where: Caesars Forum - Forum - 111-112 - [Map](#)

Description:

Hack The Box will be hosting a pub in the DEF CON pub crawl. Come socialize and have a drink!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hack the Future: Why Congress and the White House are supporting AI Red Teaming

When: Saturday, Aug 12, 09:00 - 09:45 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

Speakers:Arati Prabhakar,Austin Carson

SpeakerBio:Arati Prabhakar

No BIO available

SpeakerBio:Austin Carson , Founder & President at SeedAI

Austin Carson is the Founder and President of SeedAI, a nonprofit established to work with a diverse group of policymakers, academics, and private sector experts to help communities across the United States access the resources they need to engage with AI.

Previously, Austin established and led the DC government affairs operation for NVIDIA, translating NVIDIA's expertise in artificial intelligence and high performance computing for policymakers. Prior to joining NVIDIA, Austin held a number of public sector and NGO positions, including serving as Legislative Director for Chairman Michael McCaul and Executive Director for the Technology Freedom Institute. Austin co-founded the Congressional Tech Staff Association, co-led the Congressional Cybersecurity Caucus and the Congressional High Tech Caucus, and is a founding fellow of the Internet Law and Policy Foundry.

Description:

On May 4th, the White House announced the AI Village at DEF CON's Generative AI Red Team and their participation, followed by announcements from the House and Senate AI Caucus leadership and the National Science Foundation.

In this panel, we'll hear from top officials and executives about how they're balancing the explosion of creativity and entrepreneurship from the advent of GenAI with the known & unknown risks of deployment at scale.

We'll also hear how this exercise is viewed as a model for enhancing trust & safety through democratizing AI education. Panelists will also discuss why it's meaningful to bring together thousands of people from different communities to conduct the exercise across the available AI models.

REFERENCES

We Need Bug Bounties for Bad Algorithms - Amit Elazari -

<https://www.vice.com/en/article/8xkyj3/we-need-bug-bounties-for-bad-algorithms>

Introducing Twitter's first algorithmic bias bounty challenge - Rumman Chowdhury & Jutta Williams -

https://blog.twitter.com/engineering/en_us/topics/insights/2021/algorithmic-bias-bounty-challenge

Sharing learnings from the first algorithmic bias bounty challenge - Kyra Yee & Irene Font Peradejordi -

https://blog.twitter.com/engineering/en_us/topics/insights/2021/learnings-from-the-first-algorithmic-bias-bounty-challenge

Bias Buccaneers - Rumman Chowdhury, Jutta Williams, Subho Majumdar, Scott Steinhardt, Ben Colman -

<https://www.biasbuccaneers.org/>

An Algorithmic Framework for Bias Bounties - Ira Globus-Harris, Michael Kearns, Aaron Roth -

<https://arxiv.org/abs/2201.10408>

Machine Learning Security Evasion Competition - Hyrum Anderson, et al. - <https://mlsec.io/>

<https://cujo.com/announcing-the-winners-of-the-2021-machine-learning-security-evasion-competition/>


MITRE ATLAS - Ram Shankar Siva Kumar, et al - <https://atlas.mitre.org/>

The Spherical Cow of ML Security - Sven Cattell - <http://aivillage.org/adversarial%20ml/spherical-cow/>

The Case for a Hippocratic Oath for Connected Medical Devices: Viewpoint - Beau Woods, Andrea Coravos, and Joshua David Corman - <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6444210/>

Announcing OpenAI's Bug Bounty Program - <https://openai.com/blog/bug-bounty-program>

Microsoft Malware Classification Challenge - Royi Ronen, Marian Radu, Corina Feuerstein, Elad Yom-Tov, Mansour Ahmadi - <https://www.kaggle.com/c/malware-classification> <https://arxiv.org/abs/1802.10135>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 12:00-13:30 PDT

Title: Hack-A-Sat 4 (HAS4) -- Closing Ceremony

When: Sunday, Aug 13, 12:00 - 13:30 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

This event is the closing ceremony for the Hack-A-Sat 4 (HAS4) contest.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

Title: Hack-A-Sat 4 (HAS4)

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The Department of the Air Force, in collaboration with the security research community, is hosting Hack-A-Sat 4 – the world’s first CTF in space. Hack-A-Sat 4 aims to enable security researchers of all levels to focus their skills and creativity on solving cyber security challenges on space systems and incentivize innovation in securing these systems. Hack-A-Sat 4 will be the first CTF hosted on an on-orbit satellite, called Moonlighter. The satellite has been designed and built to advance the security research community’s skills and knowledge of on-orbit space systems. Note: HAS4 is no longer open to new contestants as the qualifying event took place in April. Attendees stopping by the HAS4 contest area will be able to learn about the history of Hack-A-Sat, Moonlighter and this year’s challenges. The area will have live scoreboards, dashboards and visualizations relaying game status, and live commentary will be provided from the adjacent Aerospace Village throughout the weekend.

HAS4 Qualifications were held April 1-2, 2023. Results here: <https://quals.2023.hackasat.com/scoreboard/complete>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: Hack-A-Sat 4 (HAS4)

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The Department of the Air Force, in collaboration with the security research community, is hosting Hack-A-Sat 4 – the world’s first CTF in space. Hack-A-Sat 4 aims to enable security researchers of all levels to focus their skills and creativity on solving cyber security challenges on space systems and incentivize innovation in securing these systems. Hack-A-Sat 4 will be the first CTF hosted on an on-orbit satellite, called Moonlighter. The satellite has been designed and built to advance the security research community’s skills and knowledge of on-orbit space systems. Note: HAS4 is no longer open to new contestants as the qualifying event took place in April. Attendees stopping by the HAS4 contest area will be able to learn about the history of Hack-A-Sat, Moonlighter and this year’s challenges. The area will have live scoreboards, dashboards and visualizations relaying game status, and live commentary will be provided from the adjacent Aerospace Village throughout the weekend.

HAS4 Qualifications were held April 1-2, 2023. Results here: <https://quals.2023.hackasat.com/scoreboard/complete>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Sunday - 12:00-12:50 PDT

Title: Hack-A-Sat 4 Awards Ceremony

When: Sunday, Aug 13, 12:00 - 12:50 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio: Hack-A-Sat 4 Team

No BIO available

Description:

Hack-A-Sat 4 is quite simply the world's first CTF in space. Now in its 4th year, the Hack-A-Sat competition series aims to enable security researchers of all levels to focus their skills and creativity on solving cyber security challenges on space systems and incentivize innovation in securing these systems. Stop by and witness the 5 finalist teams compete for \$100K in prizes, learn more about the history of Hack-A-Sat, and the Moonlighter satellite hosting this year's competition. The competition culminates with the HAS4 Award Ceremony on Sunday at 12 pm PT.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Friday - 11:00-11:50 PDT

Title: Hack-A-Sat 4 Briefing

When: Friday, Aug 11, 11:00 - 11:50 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio: Hack-A-Sat 4 Team

No BIO available

Description:

Hack-A-Sat 4 is quite simply the world's first CTF in space. Now in its 4th year, the Hack-A-Sat competition series aims to enable security researchers of all levels to focus their skills and creativity on solving cyber security challenges on space systems and incentivize innovation in securing these systems. Stop by and witness the 5 finalist teams compete for \$100K in prizes, learn more about the history of Hack-A-Sat, and the Moonlighter satellite hosting this year's competition. Competition updates will be presented on the AV stage both Friday and Saturday morning at 11 am PT.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Saturday - 11:00-11:50 PDT

Title: Hack-A-Sat 4 Briefing

When: Saturday, Aug 12, 11:00 - 11:50 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio: Hack-A-Sat 4 Team

No BIO available

Description:

Hack-A-Sat 4 is quite simply the world's first CTF in space. Now in its 4th year, the Hack-A-Sat competition series aims to enable security researchers of all levels to focus their skills and creativity on solving cyber security challenges on space systems and incentivize innovation in securing these systems. Stop by and witness the 5 finalist teams compete for \$100K in prizes, learn more about the history of Hack-A-Sat, and the Moonlighter satellite hosting this year's competition. Competition updates will be presented on the AV stage both Friday and Saturday morning at 11 am PT.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 17:00-17:59 PDT

Title: Hack3r Runw@y

When: Friday, Aug 11, 17:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Returning to the stage for Defcon 30 was surreal and we'd be honored to return for the 5th year. Hack3r Runw@y brings out all the sheik geeks out there. It encourages rethinking fashion in the eyes of hackers. Be it smartwear, LED additions, obfuscation, cosplay or just everyday wear using fabrics and textures that are familiar to the community. Contestants can enter clothing, shoes, jewelry, hats or accessories. If it can be worn, it is perfect for the runway. For convenience, contestants can enter the contest with designs made ahead of the conference, however it needs to be made by them and not just store bought. Hack3r Runway is perfect for everyone whether technologically savvy or just crafty.

Awards will be handed out in 4 categories and one trophy for the People's Choice category where the winner is anyone's guess: - Digital wearable - LED, electronic, passive - Smart wear - interactive, temperature sensing, mood changing, card skimmers, etc - Aesthetics (non-electronic)- 3d printed, geeky/nerdy wear, obfuscation, cosplay - Functional wear - did you bling out your mask and/or shield, have a hazmat suit, lock pick earrings, cufflinks shims

Winners will be selected based on, but not limited to: - Uniqueness

- Trendy
- Practical
- Couture
- Creativity
- Relevance
- Originality
- Presentation
- Mastery

Friday and Saturday, 14:00 - 16:00, Signup to walk the Contest Stage/Runway 15:30-16:30, Stage show 17:00 - 18:00

--

Is for all ages but no kid specific category.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 17:00-17:59 PDT

Title: Hack3r Runw@y

When: Saturday, Aug 12, 17:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Returning to the stage for Defcon 30 was surreal and we'd be honored to return for the 5th year. Hack3r Runw@y brings out all the sheik geeks out there. It encourages rethinking fashion in the eyes of hackers. Be it smartwear, LED additions, obfuscation, cosplay or just everyday wear using fabrics and textures that are familiar to the community. Contestants can enter clothing, shoes, jewelry, hats or accessories. If it can be worn, it is perfect for the runway. For convenience, contestants can enter the contest with designs made ahead of the conference, however it needs to be made by them and not just store bought. Hack3r Runway is perfect for everyone whether technologically savvy or just crafty.

Awards will be handed out in 4 categories and one trophy for the People's Choice category where the winner is anyone's guess: - Digital wearable - LED, electronic, passive - Smart wear - interactive, temperature sensing, mood changing, card skimmers, etc - Aesthetics (non-electronic)- 3d printed, geeky/nerdy wear, obfuscation, cosplay - Functional wear - did you bling out your mask and/or shield, have a hazmat suit, lock pick earrings, cufflinks shims

Winners will be selected based on, but not limited to: - Uniqueness

- Trendy
- Practical
- Couture
- Creativity
- Relevance
- Originality
- Presentation
- Mastery

Friday and Saturday, 14:00 - 16:00, Signup to walk the Contest Stage/Runway 15:30-16:30, Stage show 17:00 - 18:00

--

Is for all ages but no kid specific category.

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Saturday - 15:30-15:55 PDT

Title: Hackaprompt 2023: Trials and Tribulations

When: Saturday, Aug 12, 15:30 - 15:55 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

SpeakerBio: Kenneth Yeung

No BIO available

Description:

In this presentation, we unpack various prompt injection and hijacking techniques in the context of the Hackaprompt 2023 competition, the world's first prompt injection/hacking competition. Starting from exploiting AI's ignorance in simple prompt injections to evading catch-all defenses in task-oriented attacks, we explore complex techniques like output manipulation, input filtering, and password leak exploits. Further, we delve into dictionary attacks and gaslighting AI models, manipulations of proxy prompts, formatting strategies, and maneuvering past redundant defenses. The talk culminates in tackling the challenge of 'Slash Hell', where we exploit max token limits and prompt language models to interpret hidden meanings, thus emphasizing the need for robust AI defense mechanisms and ongoing AI education.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MIV - Friday - 12:30-12:59 PDT

Title: Hackathon presentation

When: Friday, Aug 11, 12:30 - 12:59 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Misinformation Village Staff

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MIV - Sunday - 10:00-11:30 PDT

Title: Hackathon result's presentation


When: Sunday, Aug 13, 10:00 - 11:30 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Misinformation Village Staff

No BIO available

Description:

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 20:00-21:59 PDT


Title: Hacker Flairgrounds

When: Friday, Aug 11, 20:00 - 21:59 PDT

Where: Caesars Forum - Forum - 114 - [Map](#)

Description:

Are you a flaming badge builder or just LED curious? Then you don't want to miss Hacker Flairgrounds, the ultimate gathering of hackers and blinking LEDs in Vegas. It's the place to be for badge folk, hardware hackers and makers who love the flashier side of DEF CON. Everyone is welcome. Show us your analog badge addons and flipper hacks! Come get inspired by the dazzling displays of creativity and skill.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacker Jeopardy

When: Friday, Aug 11, 20:00 - 21:59 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

Description:

Lintile: Hiya, ChatGPT, are you aware of the annual contest called Hacker Jeopardy at DEF CON? When is it?

ChatGPT: Yes, Hacker Jeopardy is a popular event at DEF CON. It's a parody of the television game show "Jeopardy!" but with a twist. Instead of general knowledge, the questions (or "answers," in Jeopardy style) are focused on hacker culture, computer security, technology, and similar topics. The game consists of two preliminary rounds on Friday, and a final round on Saturday. Both shows start at 2000 Las Vegas time. Just like in the original game show, there are DFIU Doubles and a Final Hacker Jeopardy round. One unique aspect of Hacker Jeopardy that distinguishes it from the TV show is the incorporation of ADULT HUMOR, vulgarity, innuendo, and beer into the game. Please remember, my knowledge is current only up to September 2021, and if there have been any significant changes to Hacker Jeopardy after that, I would not be aware of them.

Lintile: What's the catch phrase of Hacker Jeopardy?

ChatGPT: The catch phrase of Hacker Jeopardy is "Drink while you think". This refers to the unique element of the game where contestants are encouraged to drink beer while they are attempting to come up with the correct response to the clues.

Lintile: That's not correct. The acronym of the catch phrase is DFIU.

ChatGPT: I apologize for the oversight. The catchphrase for Hacker Jeopardy at DEF CON is "Don't Forget It's UNIX" (DFIU), which is used humorously due to the historically significant role of Unix-based systems in hacking and network security. This phrase is often used to remind participants of the roots of many computer systems and infrastructures. I appreciate your patience and your correct information.

Note that this is an ADULT show with vulgarities and alcohol consumption, but if that doesn't bother you, come enjoy one of the largest contests at DEF CON that you really need to see to believe! And as always, DFIU!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacker Jeopardy

When: Saturday, Aug 12, 20:00 - 21:59 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

Description:

Lintile: Hiya, ChatGPT, are you aware of the annual contest called Hacker Jeopardy at DEF CON? When is it?

ChatGPT: Yes, Hacker Jeopardy is a popular event at DEF CON. It's a parody of the television game show "Jeopardy!" but with a twist. Instead of general knowledge, the questions (or "answers," in Jeopardy style) are focused on hacker culture, computer security, technology, and similar topics. The game consists of two preliminary rounds on Friday, and a final round on Saturday. Both shows start at 2000 Las Vegas time. Just like in the original game show, there are DFIU Doubles and a Final Hacker Jeopardy round. One unique aspect of Hacker Jeopardy that distinguishes it from the TV show is the incorporation of ADULT HUMOR, vulgarity, innuendo, and beer into the game. Please remember, my knowledge is current only up to September 2021, and if there have been any significant changes to Hacker Jeopardy after that, I would not be aware of them.

Lintile: What's the catch phrase of Hacker Jeopardy?

ChatGPT: The catch phrase of Hacker Jeopardy is "Drink while you think". This refers to the unique element of the game where contestants are encouraged to drink beer while they are attempting to come up with the correct response to the clues.

Lintile: That's not correct. The acronym of the catch phrase is DFIU.

ChatGPT: I apologize for the oversight. The catchphrase for Hacker Jeopardy at DEF CON is "Don't Forget It's UNIX" (DFIU), which is used humorously due to the historically significant role of Unix-based systems in hacking and network security. This phrase is often used to remind participants of the roots of many computer systems and infrastructures. I appreciate your patience and your correct information.

Note that this is an ADULT show with vulgarities and alcohol consumption, but if that doesn't bother you, come enjoy one of the largest contests at DEF CON that you really need to see to believe! And as always, DFIU!

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 20:00-01:59 PDT

Title: Hacker Karaoke 15


When: Friday, Aug 11, 20:00 - 01:59 PDT

Where: Caesars Forum - Summit - 216 - [Map](#)

Description:

For those who love to sing and perform in front of others, we are celebrating our 15th year of Love, Laughter, and Song from 19:30 – 02:00 Friday and Saturday night.

We are open to everyone of any age, and singing is not required.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 20:00-01:59 PDT

Title: Hacker Karaoke 15


When: Saturday, Aug 12, 20:00 - 01:59 PDT

Where: Caesars Forum - Summit - 216 - [Map](#)

Description:

For those who love to sing and perform in front of others, we are celebrating our 15th year of Love, Laughter, and Song from 19:30 – 02:00 Friday and Saturday night.

We are open to everyone of any age, and singing is not required.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 10:00-17:59 PDT

Title: Hacker Memorial

When: Friday, Aug 11, 10:00 - 17:59 PDT


Where: Harrah's - Copper - Memorial Room - [Map](#)

Description:

A place to remember hackers that are no longer with us. Come to share stories and celebrate their life.

Please send photos of our fallen hacker comrades to

[\[defconmemorial@protonmail.com\]](mailto:defconmemorial@protonmail.com)(mailto:defconmemorial@protonmail.com), to be printed and displayed on the memorial wall here at DEF CON.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 10:00-17:59 PDT

Title: Hacker Memorial

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Harrah's - Copper - Memorial Room - [Map](#)

Description:

A place to remember hackers that are no longer with us. Come to share stories and celebrate their life.

Please send photos of our fallen hacker comrades to

[\[defconmemorial@protonmail.com\]](mailto:defconmemorial@protonmail.com)(mailto:defconmemorial@protonmail.com), to be printed and displayed on the memorial wall here at DEF CON.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Sunday - 12:00-13:59 PDT

Title: Hacker Memorial

When: Sunday, Aug 13, 12:00 - 13:59 PDT

Where: Harrah's - Copper - Memorial Room - [Map](#)

Description:

A place to remember hackers that are no longer with us. Come to share stories and celebrate their life.

Please send photos of our fallen hacker comrades to

[\[defconmemorial@protonmail.com\]](mailto:defconmemorial@protonmail.com)(mailto:defconmemorial@protonmail.com), to be printed and displayed on the memorial wall here at DEF CON.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

Title: HackFortress

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Hackfortress is a unique blend of Team Fortress 2 and a computer security contest. Teams are made up of 6 TF2 players and 4 hackers, TF2 players duke it out while hackers are busy with challenges like application security, network security, social engineering, or reverse engineering. As teams start scoring they can redeem points in the hack fortress store for bonuses. Bonuses range from crits for the TF2, lighting the opposing team on fire, or preventing the other teams hackers from accessing the store. HackFortress challenges range from beginner to advanced, from serious to absurd.

- Thursday: Once our network is setup and ready, runs until the contest area closes.
- Friday: 10:00 - 18:00 (open play)
 - ◆ 10 AM: Team Fortress 2 free play
 - ◆ 3 PM Contest begins
 - ◆ 5 PM Contest registration closes
- Saturday: 10:00 - 18:00 (Contest, all day)

--

Kid friendly, as long as they want to play a 16 year old FPS.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: HackFortress

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Hackfortress is a unique blend of Team Fortress 2 and a computer security contest. Teams are made up of 6 TF2 players and 4 hackers, TF2 players duke it out while hackers are busy with challenges like application security, network security, social engineering, or reverse engineering. As teams start scoring they can redeem points in the hack fortress store for bonuses. Bonuses range from crits for the TF2, lighting the opposing team on fire, or preventing the other teams hackers from accessing the store. HackFortress challenges range from beginner to advanced, from serious to absurd.

- Thursday: Once our network is setup and ready, runs until the contest area closes.
- Friday: 10:00 - 18:00 (open play)
 - ◆ 10 AM: Team Fortress 2 free play
 - ◆ 3 PM Contest begins
 - ◆ 5 PM Contest registration closes
- Saturday: 10:00 - 18:00 (Contest, all day)

--

Kid friendly, as long as they want to play a 16 year old FPS.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking GitHub Actions: Abusing GitHub and Azure for fun and profit

When: Sunday, Aug 13, 10:15 - 10:59 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

SpeakerBio: Magno Logan

Magno Logan works as an Information Security Specialist. He specializes in Cloud, Container, and Application Security Research. He has been tapped as a resource speaker for numerous security conferences around the globe.

Twitter: [@magnologan](#)

Description:

More organizations are applying a DevOps methodology to optimize software development. One of the main tools used in this process is a continuous integration (CI) tool that automates code changes from multiple developers working on the same project. Multiple CI tools are available today, Jenkins, CircleCI, TravisCI, GitLab CI, and now GitHub Actions. In 2019, GitHub released its own CI tool called GitHub Actions (GHA). According to GitHub, GitHub Actions help you automate tasks within your software development life cycle, and it has been gaining a lot of adoption from developers.

This presentation results from detailed research on the topic where the author investigated abuse case scenarios, such as how attackers leveraged this free service to mine cryptocurrencies on their behalf and behalf of other users, among other attack vectors. We'll also demonstrate how to perform interactive commands to the Runner servers via reverse shell, which is technically not allowed via traditional means. Ultimately, we'll show the problem of third-party dependencies via the GitHub Actions Marketplace. Finally, we'll demonstrate how easy creating and publishing a fake GitHub Action on the GitHub Marketplace is. And if used unwillingly by other projects, it can compromise the victim's Runners to act as bots, target other victims, and even be used in supply-chain attacks by tampering with the result of the pipeline or even creating a botnet of crypto miners inside Azure.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking Meta Quest

When: Saturday, Aug 12, 09:00 - 10:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 6 - [Map](#)

SpeakerBio:Paul D.

No BIO available

Twitter: [@knetivty](#)

Description:

We will have our Meta Quest 2, Meta Quest Pro and Ray-Ban Stories devices available and firmware on-site to support native/hardware live hack competitions.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Friday - 18:30-21:59 PDT

Title: Hacking Policy & Prompts - Happy Hour

When: Friday, Aug 11, 18:30 - 21:59 PDT

Where: Caesars Forum - Summit - 223 - Plounge - [Map](#)

Description:

Join the [Hacking Policy Council](<http://hackingpolicycouncil.org/>) and the [AI Village](<https://aivillage.org/>) for a happy hour with hackers, policymakers, and AI experts. Have a beverage with us and discuss whether it is a hacking crime to lie to AI, what governments are doing about vulnerabilities disclosure, and the ultimate AI hacking challenge. There will be a cash bar and some drink tickets will be available from Policy @ DEF CON. Mark your calendars for Friday, August 11th, 6:30PM - 10PM, at Caesar's Forum in rooms 221-223 (AKA the Plounge).

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking Quantum Advantage for Classical Processes; Intro to Quantum-Inspired Use Cases

When: Friday, Aug 11, 15:00 - 15:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

SpeakerBio: Konstantinos Karagiannis

No BIO available

Description:

Quantum computing will change the world ... eventually. Until we achieve quantum advantage, we can see actual performance boosts from quantum-inspired approaches today. In this talk, we discuss tensor networks inspired by the world of quantum physics that run on classical hardware and digital annealers designed to act like quantum hardware. Get a sense of the types of use cases you can explore now, including examples of the performance edges you can expect today.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking Real Web Areas

When: Friday, Aug 11, 16:00 - 16:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 2 - [Map](#)

SpeakerBio: Ilkin Javadov

No BIO available

Twitter: [@IlkinJavadov](#)

Description:

Totally here I want to show how hackers find and exploit bugs and more. I'm talking about a purely technical demonstration. In Gisec 2023 Global, I did a live demo on Cross site scripting deep identify and exploit. For example, I think it would be nice if there was a trend on injections or Broken access control. Then it is necessary to learn how to proceed.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking Reproductive Health

When: Saturday, Aug 12, 00:00 - 00:59 PDT

Where: Virtual

SpeakerBio: JJ Hastings

No BIO available

Description:

This talk is being pre-recorded and will be released on YouTube. Once it is available, a link to it will appear here.

Update 2023-08-11 06:30: Biohacking Village indicates that the pre-recorded talks have not yet been received. Once received, these talks will be posted to the [Biohacking Village YouTube Channel](<https://www.youtube.com/@BiohackingVillage/about>). Please note that this may be as late as a week or two after DC31.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Sunday - 13:00-13:50 PDT

Title: Hacking Satellites: Houston, We Have a Problem

When: Sunday, Aug 13, 13:00 - 13:50 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio:Jacob Oakley

No BIO available

Description:

The intersection of the space and cyber domains presents a complex emerging challenge to cybersecurity and space professionals. This talk covers an introduction to satellites and space operations, the attacks that space assets face, and the vectors used to facilitate malicious activity. It discusses adversarial campaigns against space vehicles at a micro and macro scale and outlines the foundational issues to securing-space resident attack surfaces.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking The Metal: An Intro to ARM Assembly Language Programming (Pre-Registration Required)

When: Thursday, Aug 10, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

SpeakerBio:Eigentourist

Eigentourist is a programmer who learned the craft in the early 1980s. He began formal education in computer science when the height of software engineering discipline meant avoiding the use of GOTO statements. Over the course of his career, he has created code of beautiful simplicity and elegance, and of horrific complexity and unpredictability. Sometimes it's hard to tell which was which. Today, he works on systems integration and engineering in the healthcare industry.

Description:

"RISC architecture is gonna change everything."

"Yeah. RISC is good."

So said Angelina Jolie and Jonny Lee Miller in 1995. And while many of us weren't looking, RISC quietly changed everything.

This workshop will teach an introduction to low-level programming on the CPU that runs your favorite mobile games, apps, and everything else on your personal devices -- and is now creeping onto the desktop and into the datacenters that run the world.

We will write assembly code for ARM CPUs, and run it on an emulated Raspberry Pi, using the QEMU emulator. In the process, we will learn the key differences between ARM and the Intel CPUs running our workstations and servers. We will also learn to parallelize operations using the Neon coprocessor, and communicate with devices via the Raspberry's GPIO pins. Finally, we will explore and debug some misbehaving code, and in the end, we will emerge with a deeper understanding of low-level operations as they occur on the devices that play a vital role in our present and our future.

Skill Level: Intermediate

Prerequisites for students:

- Some previous coding experience is helpful, but mostly, a healthy curiosity

Materials or Equipment students will need to bring to participate: - Laptop with wifi connectivity, if wishing to participate

[Return to Index](#) - Add to  - ics [Calendar](#) file

RTV - Friday - 15:00-15:59 PDT

Title: Hacking Web Apps and APIs with WebSploit Labs

When: Friday, Aug 11, 15:00 - 15:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 1 - [Map](#)

SpeakerBio: Omar Santos

No BIO available

Twitter: [@santosomar](#)

Description:

This workshop is intended for cybersecurity professionals, system administrators, software developers, and anyone interested in learning about the art of hacking web applications and API security. It is an immersive, hands-on experience that provides comprehensive knowledge about different web application and API vulnerabilities, and, most importantly, effective hacking methodologies.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking Web Apps and APIs with WebSploit Labs

When: Saturday, Aug 12, 12:00 - 12:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 2 - [Map](#)

SpeakerBio: Omar Santos

No BIO available

Twitter: [@santosomar](#)

Description:

This workshop is intended for cybersecurity professionals, system administrators, software developers, and anyone interested in learning about the art of hacking web applications and API security. It is an immersive, hands-on experience that provides comprehensive knowledge about different web application and API vulnerabilities, and, most importantly, effective hacking methodologies.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking Web Apps and APIs with WebSploit Labs

When: Saturday, Aug 12, 16:00 - 16:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 4 - [Map](#)


SpeakerBio: Omar Santos

No BIO available

Twitter: [@santosomar](#)

Description:

This workshop is intended for cybersecurity professionals, system administrators, software developers, and anyone interested in learning about the art of hacking web applications and API security. It is an immersive, hands-on experience that provides comprehensive knowledge about different web application and API vulnerabilities, and, most importantly, effective hacking methodologies.

[Return to Index](#) - Add to  - ics [Calendar](#) file

RTV - Friday - 14:00-14:59 PDT

Title: Hacking Web Apps and APIs with WebSploit Labs

When: Friday, Aug 11, 14:00 - 14:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 1 - [Map](#)

SpeakerBio: Omar Santos

No BIO available

Twitter: [@santosomar](#)

Description:

This workshop is intended for cybersecurity professionals, system administrators, software developers, and anyone interested in learning about the art of hacking web applications and API security. It is an immersive, hands-on experience that provides comprehensive knowledge about different web application and API vulnerabilities, and, most importantly, effective hacking methodologies.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking Web Apps and APIs with WebSploit Labs

When: Sunday, Aug 13, 11:00 - 11:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 6 - [Map](#)

SpeakerBio: Omar Santos

No BIO available

Twitter: [@santosomar](#)

Description:

This workshop is intended for cybersecurity professionals, system administrators, software developers, and anyone interested in learning about the art of hacking web applications and API security. It is an immersive, hands-on experience that provides comprehensive knowledge about different web application and API vulnerabilities, and, most importantly, effective hacking methodologies.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MIV - Saturday - 16:30-17:30 PDT

Title: Hacks, Leaks, and Revelations: Pandemic Profiteers and COVID-19 Disinformation


When: Saturday, Aug 12, 16:30 - 17:30 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Micah Lee

Micah Lee is an investigative journalist, computer security engineer, and open source software developer who is known for helping secure Edward Snowden's communications while Snowden leaked secret NSA documents. Lee is the director of information security at The Intercept and an adviser to the transparency collective Distributed Denial of Secrets. He's a former staff technologist for the Electronic Frontier Foundation and a co-founder of the Freedom of the Press Foundation. Lee is also a Tor Project core contributor, and he develops open source security and privacy tools like OnionShare and Dangerzone.

Description:

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Ham In A Day Class

When: Thursday, Aug 10, 09:00 - 17:59 PDT

Where: Flamingo - Virginia City - Ham Radio Village - [Map](#)

SpeakerBio:Dan KB6NU

Dan, KB6NU, is the author of the No Nonsense amateur radio license study guides and is very proud of helping thousands of people get their licenses and upgrade their licenses. He also blogs about amateur radio [KB6NU.Com](<https://KB6NU.Com>), appears on the [ICQPodcast](<https://icqpodcast.com>), and is Communications Manager for [ARDC](<https://ampr.org>).

Twitter: [@@kb6nu](#)

Description:

In this class, KB6NU will cover everything you need to know to pass the Technician Class license exam. Register [\[here\]\(https://platform.hamvillage.org/collect/description/315307-u-def-con-31-ham-in-a-day\)](https://platform.hamvillage.org/collect/description/315307-u-def-con-31-ham-in-a-day).

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

Title: Ham Radio Fox Hunting Contest

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

In the world of amateur radio, groups of hams will often put together a transmitter hunt (also called "fox hunting") in order to hone their radio direction finding skills to locate one or more hidden radio transmitters broadcasting. The Defcon Fox Hunt will require participants to locate a number of hidden radio transmitters broadcasting at very low power which are hidden throughout the conference. Each transmitter will provide a clue or code which will prove the player found the fox transmitter. A map with rough search areas will be given to participants to guide them on their hunt. Additional hints and tips will be provided throughout Defcon at the contest table to help people who find themselves stuck. A small prize to be determined will be given to each participant who locates all of the foxes each day.

Expanded this year with increased difficulty each day. Friday: Foxes in a small area, non moving Saturday: Foxes in a larger area, with one moving. Sunday: Foxes are on the move. The hunt is on!

There will also be a beginner friendly, no radio required, Infrared LED Fox Hunt running everyday which participants can use their cameras on their phones to find!

--

We have had many kids participate and complete the contest over the years... and they've all had a blast doing so.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT

Title: Ham Radio Fox Hunting Contest

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

In the world of amateur radio, groups of hams will often put together a transmitter hunt (also called "fox hunting") in order to hone their radio direction finding skills to locate one or more hidden radio transmitters broadcasting. The Defcon Fox Hunt will require participants to locate a number of hidden radio transmitters broadcasting at very low power which are hidden throughout the conference. Each transmitter will provide a clue or code which will prove the player found the fox transmitter. A map with rough search areas will be given to participants to guide them on their hunt. Additional hints and tips will be provided throughout Defcon at the contest table to help people who find themselves stuck. A small prize to be determined will be given to each participant who locates all of the foxes each day.

Expanded this year with increased difficulty each day. Friday: Foxes in a small area, non moving Saturday: Foxes in a larger area, with one moving. Sunday: Foxes are on the move. The hunt is on!

There will also be a beginner friendly, no radio required, Infrared LED Fox Hunt running everyday which participants can use their cameras on their phones to find!

--

We have had many kids participate and complete the contest over the years... and they've all had a blast doing so.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: Ham Radio Fox Hunting Contest

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

In the world of amateur radio, groups of hams will often put together a transmitter hunt (also called "fox hunting") in order to hone their radio direction finding skills to locate one or more hidden radio transmitters broadcasting. The Defcon Fox Hunt will require participants to locate a number of hidden radio transmitters broadcasting at very low power which are hidden throughout the conference. Each transmitter will provide a clue or code which will prove the player found the fox transmitter. A map with rough search areas will be given to participants to guide them on their hunt. Additional hints and tips will be provided throughout Defcon at the contest table to help people who find themselves stuck. A small prize to be determined will be given to each participant who locates all of the foxes each day.

Expanded this year with increased difficulty each day. Friday: Foxes in a small area, non moving Saturday: Foxes in a larger area, with one moving. Sunday: Foxes are on the move. The hunt is on!

There will also be a beginner friendly, no radio required, Infrared LED Fox Hunt running everyday which participants can use their cameras on their phones to find!

--

We have had many kids participate and complete the contest over the years... and they've all had a blast doing so.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hands On a Cyber Policy Crisis: Testing Assumptions and Navigating Challenges through a Cyber Simulation

When: Saturday, Aug 12, 12:00 - 13:50 PDT

Where: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

SpeakerBio: Safa Shahwan Edwards , Deputy Director, Cyber Statecraft Initiative at Atlantic Council

Safa Shahwan Edwards is the deputy director of the Atlantic Council's Cyber Statecraft Initiative under the Digital Forensic Research Lab (DFRLab). In this role, she leads the administration and external communications of the Initiative, as well as the Cyber 9/12 Strategy Challenge, the Initiative's global cyber policy and strategy competition. Safa holds an MA in International Affairs with a concentration in Conflict Resolution from the George Washington University Elliott School of International Affairs and a BA in Political Science from Miami University of Ohio. Safa is of Bolivian and Jordanian heritage and speaks Spanish and Arabic.

Description:

A major cyber incident has occurred. How will you respond?

A war game but make it cyber. In groups of 3-4 people, hackers and policymakers at the village will respond to a cybersecurity crisis scenario with far reaching impacts on the public but especially vulnerable communities. Groups of 3-4 participants will develop responses to mitigate the crisis and present these to the larger group. Participants may take on specific roles based on the storyline of the crisis (e.g. CISA, the White House, CVD coordinating bodies, OT security researchers, and more).

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hands-on GitHub Actions

When: Friday, Aug 11, 11:00 - 12:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 1 - [Map](#)

SpeakerBio:Magno Logan

Magno Logan works as an Information Security Specialist. He specializes in Cloud, Container, and Application Security Research. He has been tapped as a resource speaker for numerous security conferences around the globe.

Twitter: [@magnologan](#)

Description:

In each round, the participants will get to deploy a set of GitHub Actions in a chosen project to implement security best practices. Whoever completes the challenge first among the competitors, or gets closer to completing it, wins. The set of Actions at each round will be chosen randomly among the Actions in the Security category available in the Marketplace.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hands-On TCP/IP Deep Dive with Wireshark - How this stuff really works (Pre-Registration Required)

When: Saturday, Aug 12, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

SpeakerBio: Chris Greer , Network Analyst and Wireshark Instructor at Packet Pioneer

Chris Greer is a network analyst and Wireshark instructor for Packet Pioneer, a Wireshark University partner. He has focused much of his career at the transport layer, specifically TCP, specializing in how this core protocol works to deliver applications, services, and attacks between systems. Chris is a regular speaker at Sharkfest - the Wireshark Developer and User Conference. He has presented at DEFCON and other industry conferences and regularly posts Wireshark analysis tips to his YouTube channel.

Description:

Let's break out Wireshark and dig deep in to the TCP and IP protocols. This skill is critical for anyone interested in any area of cybersecurity, no matter the color of the hat. Almost all enumeration, scans, incident response, and traffic forensics require the analyst to dig into and interpret TCP conversations. When enumerating an environment, identifying key TCP/IP indicators in protocol headers can also help when passively fingerprinting systems.

In this workshop we will roll back our sleeves and learn how TCP/IP really works - the handshake, options, sequence/ack numbers, retransmissions, TTL, and much more. This workshop welcomes all cybersecurity and wireshark experience levels.

Skill Level: Beginner to Intermediate

Prerequisites for students:

- Just a laptop with a copy of Wireshark. - I will provide the sample pcaps for analysis.

Materials or Equipment students will need to bring to participate: - Laptop

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hangover Trivia: Cyber Policy Edition

When: Sunday, Aug 13, 11:00 - 11:50 PDT

Where: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

SpeakerBio: Kurt Opsahl , Associate General Counsel for Cybersecurity and Civil Liberties Policy at Filecoin Foundation
Kurt Opsahl is the Associate General Counsel for Cybersecurity and Civil Liberties Policy for the Filecoin Foundation, and a Special Counsel to the Electronic Frontier Foundation. Formerly, Opsahl was the Deputy Executive Director and General Counsel of EFF. Opsahl was also the lead attorney on the Coders' Rights Project, and continues to assist EFF with that work as a Special Counsel. In 2007, Opsahl was named as one of the "Attorneys of the Year" by California Lawyer magazine. From 2014 to 2022, Opsahl served on the USENIX Board of Directors. Opsahl is a member of the CISA Cybersecurity Advisory Committee's Technical Advisory Council.

Twitter: [@KurtOpsahl](#)

Description:

Come down to the Policy track on Sunday morning and test your knowledge of all the most trivial aspects of tech policy! Bring a team or ride solo, and see if your deep knowledge of cybersecurity and tech policy is the best of the best. We'll have a short quiz on tech law, policy, security and privacy topics that will blow your mind. Or what's left of your mind after those shenanigans you got up to on Saturday night. BYO Bloody Mary.

Kurt Opsahl will be your most masterful and hungover Trivia Master, joined by three surprise judges.

[Return to Index](#) - Add to  - ics [Calendar](#) file

XRV - Saturday - 10:00-15:59 PDT

Title: Haptics Hack-a-Thon

When: Saturday, Aug 12, 10:00 - 15:59 PDT

Where: Caesars Forum - Summit - 206 - XR Village - [Map](#)

Description:

Open Bug Hunt | Hack the MetaQuest 2 in collaboration with Adversary Village, Red Team Village and sponsored by ThreatSims and Meta. Bug bounties to be reported via Meta Bug Bounty terms & conditions. Please sign up if you plan to participate.

[Return to Index](#) - Add to  - ics [Calendar](#) file

XRV - Friday - 10:00-15:59 PDT


Title: Haptics Hack-a-Thon

When: Friday, Aug 11, 10:00 - 15:59 PDT

Where: Caesars Forum - Summit - 206 - XR Village - [Map](#)

Description:

Open Bug Hunt | Hack the MetaQuest 2 in collaboration with Adversary Village, Red Team Village and sponsored by ThreatSims and Meta. Bug bounties to be reported via Meta Bug Bounty terms & conditions. Please sign up if you plan to participate.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: HardHat Command & Control Framework

When: Saturday, Aug 12, 14:00 - 15:55 PDT

Where: Caesars Forum - Committee Boardroom - Demo Labs - [Map](#)

SpeakerBio:Jonathan Owens

Jonathan Owens is a red team operator on the Adversary Simulation team at SpecterOps, where he conducts advanced offensive engagements, such as red teaming exercises, penetration tests, and tool creation. He enjoys C# development and learning new programming languages with a specific focus on command & control framework and agent development. He maintains a tool repo at <https://github.com/dragoqcc>.

Description:

HardHat is a multi-platform, multi-user, .NET command and control framework written in C# designed to aid in red team operations and penetration testing. HardHat aims to improve the quality-of-life of operators by providing an easy-to-use but formidable C2 framework by incorporating robust features, ease of data access, and modern UI upgrades to a high-level language that is easily extensible.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Saturday - 10:00-15:30 PDT


Title: Hardware Hacking Rube Goldberg Machine

When: Saturday, Aug 12, 10:00 - 15:30 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Description:

Hardware Hacking Village (HHV) is hosting a Rube Goldberg Machine (RGM) Event! This idea has been kicking around the HHV volunteer circle in one shape or another since at least DEF CON 20, so it's about time that it happened! The goal is to create a series of devices that combine to form an end-to-end Rube Goldberg machine for transmitting messages. The hope is that all sorts of creative devices will be connected up to each other to move bits through various complicated and fun analog/digital methods. Ideas have ranged from simply wiring RX to TX — to using radios to bounce the message off the moon!

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Friday - 10:00-17:59 PDT

Title: Hardware Hacking Rube Goldberg Machine

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Description:

Hardware Hacking Village (HHV) is hosting a Rube Goldberg Machine (RGM) Event! This idea has been kicking around the HHV volunteer circle in one shape or another since at least DEF CON 20, so it's about time that it happened! The goal is to create a series of devices that combine to form an end-to-end Rube Goldberg machine for transmitting messages. The hope is that all sorts of creative devices will be connected up to each other to move bits through various complicated and fun analog/digital methods. Ideas have ranged from simply wiring RX to TX — to using radios to bounce the message off the moon!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: Hardware Hacking Village CTF

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Description:

The DEF CON Hardware Hacking Village CTF is back again! Come put your skills to the test against other hackers. The contest is structured so that everyone should be able to gain some flags, and even the experienced will sweat a few drops to get them all.

Heat up your soldering iron and freshen the batteries in your multimeter! The Hardware Hacking Village (HHV) is hosting their first official DEF CON Capture the Flag (CTF). This is a jeopardy style CTF, designed to challenge participants in various aspects of hardware hacking. Whether you're new to hardware hacking or experienced and just looking for something to do while you wait for your fault injection to trigger, all are welcome and challenges range from beginner to advanced.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT

Title: Hardware Hacking Village CTF

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Description:

The DEF CON Hardware Hacking Village CTF is back again! Come put your skills to the test against other hackers. The contest is structured so that everyone should be able to gain some flags, and even the experienced will sweat a few drops to get them all.

Heat up your soldering iron and freshen the batteries in your multimeter! The Hardware Hacking Village (HHV) is hosting their first official DEF CON Capture the Flag (CTF). This is a jeopardy style CTF, designed to challenge participants in various aspects of hardware hacking. Whether you're new to hardware hacking or experienced and just looking for something to do while you wait for your fault injection to trigger, all are welcome and challenges range from beginner to advanced.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

Title: Hardware Hacking Village CTF

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Description:

The DEF CON Hardware Hacking Village CTF is back again! Come put your skills to the test against other hackers. The contest is structured so that everyone should be able to gain some flags, and even the experienced will sweat a few drops to get them all.

Heat up your soldering iron and freshen the batteries in your multimeter! The Hardware Hacking Village (HHV) is hosting their first official DEF CON Capture the Flag (CTF). This is a jeopardy style CTF, designed to challenge participants in various aspects of hardware hacking. Whether you're new to hardware hacking or experienced and just looking for something to do while you wait for your fault injection to trigger, all are welcome and challenges range from beginner to advanced.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Saturday - 16:00-16:30 PDT


Title: Hardware Hacking Village Prize Ceremony

When: Saturday, Aug 12, 16:00 - 16:30 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Description:

We announce winners for the Make Your Own Use, and Hardware Hacking Rube Goldberg Machine contests and hand out prizes.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Saturday - 10:00-17:59 PDT


Title: Hardware Hacking Your Kitchen

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Hardware Hacking Your Kitchen: bug bounty is back! Join us for the opportunity to live hack into some of the most popular home kitchen devices, right in the IoT Village!

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Sunday - 10:00-13:59 PDT


Title: Hardware Hacking Your Kitchen

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Hardware Hacking Your Kitchen: bug bounty is back! Join us for the opportunity to live hack into some of the most popular home kitchen devices, right in the IoT Village!

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Friday - 10:00-17:59 PDT


Title: Hardware Hacking Your Kitchen

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Hardware Hacking Your Kitchen: bug bounty is back! Join us for the opportunity to live hack into some of the most popular home kitchen devices, right in the IoT Village!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 09:00-12:59 PDT


Title: HardWired

When: Sunday, Aug 13, 09:00 - 12:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Don't know how to make a network cable and want to learn? Has it been years? Or do you think you're a pro? Come test your skills against the clock, and make the best cable at con!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 09:00-17:59 PDT


Title: HardWired

When: Saturday, Aug 12, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Don't know how to make a network cable and want to learn? Has it been years? Or do you think you're a pro? Come test your skills against the clock, and make the best cable at con!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 09:00-17:59 PDT


Title: HardWired

When: Friday, Aug 11, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Don't know how to make a network cable and want to learn? Has it been years? Or do you think you're a pro? Come test your skills against the clock, and make the best cable at con!

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 12:00-17:59 PDT

Title: HDA / Accessibility Area Open

When: Saturday, Aug 12, 12:00 - 17:59 PDT

Where: Harrah's - Studio 2-4 - HDA Community - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file


SOC - Sunday - 12:00-13:59 PDT

Title: HDA / Accessibility Area Open

When: Sunday, Aug 13, 12:00 - 13:59 PDT

Where: Harrah's - Studio 2-4 - HDA Community - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 12:00-17:59 PDT

Title: HDA / Accessibility Area Open

When: Friday, Aug 11, 12:00 - 17:59 PDT

Where: Harrah's - Studio 2-4 - HDA Community - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Sunday - 12:00-13:59 PDT

Title: HDA Community Meetups

When: Sunday, Aug 13, 12:00 - 13:59 PDT

Where: Harrah's - Studio 2-4 - HDA Community - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file


SOC - Saturday - 12:00-17:59 PDT

Title: HDA Community Meetups

When: Saturday, Aug 12, 12:00 - 17:59 PDT

Where: Harrah's - Studio 2-4 - HDA Community - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 12:00-17:59 PDT

Title: HDA Community Meetups

When: Friday, Aug 11, 12:00 - 17:59 PDT

Where: Harrah's - Studio 2-4 - HDA Community - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hey CryptoBro!: How Are Criminals Laundering, Monetizing, and Targeting Cryptocurrency, NFTs, and Smart Contracts?

When: Saturday, Aug 12, 16:35 - 17:35 PDT

Where: Virtual

SpeakerBio: Sam Colaizzi , Recorded Future

Currently working at Recorded Future, Sam's areas of focus and interest include: the cryptocurrency, NFT, and smart contract space, the Russian and English-language cybercrime ecosystem, and threat actor engagement / research. He has previously worked as cyber threat intelligence analyst and researcher at Aon, Kroll, Terbium Labs, and the National Cyber-Forensics and Training Alliance (NCFTA). Prior to starting his career, he attended Duquesne University and earned a B.A. in Political Science. Afterwards, he attended The University of Pittsburgh's Graduate School of International Affairs and earned an M.A. in Security and Intelligence Studies.

Description:

For this presentation, I will be covering some of the methods of laundering (mixers / tumblers, over-the-counter (OTC) exchanges, peer-to-peer (P2P) exchanges, and high-risk exchanges) as well as how threat actors monetize their illicit digital profits by utilizing virtual credit cards (VCCs), account cash-out services, and more.

Next, I will analyze and discuss the attack vectors utilized by threat actors to target cryptocurrency, non-fungible tokens (NFTs), and smart contracts. I will also discuss popular attack vectors, such as airdrops, cross-chain bridge attacks, rugpulls, wallet compromises, flash-loan attacks, smart contract vulnerabilities, API withdrawals, drainers, and notable incidents that highlight successful laundering and monetization activities via cryptocurrencies. Finally, I will discuss how threat actors will likely evolve and transform their laundering and monetization methods.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HRV - Saturday - 15:00-16:30 PDT

Title: HF Radio Demonstration

When: Saturday, Aug 12, 15:00 - 16:30 PDT


Where: Flamingo - Virginia City - Ham Radio Village - [Map](#)

SpeakerBio:KitKat

No BIO available

Description:

Join us on the rooftop hangout at the flamingo as we set up and operate a portable HF radio rig!

[Return to Index](#) - Add to  - ics [Calendar](#) file

HRV - Friday - 15:00-16:30 PDT

Title: HF Radio Demonstration

When: Friday, Aug 11, 15:00 - 16:30 PDT

Where: Flamingo - Virginia City - Ham Radio Village - [Map](#)

SpeakerBio:KitKat

No BIO available

Description:

Join us on the rooftop hangout at the flamingo as we set up and operate a portable HF radio rig!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hide your kids, turn off your Wi-Fi, they Rogue APing up in here (Pre-Registration Required)

When: Thursday, Aug 10, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers: Daniel Costantini, James Hawk, Lander Beyer

SpeakerBio: Daniel Costantini , Principal Consultant at Mandiant

Daniel Costantini is a Principal Consultant with Mandiant, within Proactive Services. He is a Red Team/Penetration Testing subject matter expert in a variety of disciplines. Daniel has led and contributed to over a hundred Penetration/Red Team assessments. Over the years he has gained vast experience in living off the land, application, web, and network penetration testing. He continues, to strengthen his expertise in advanced wireless assessments. Daniel is a 17-year veteran of the United States Air Force (USAF) with ten of those years on active-duty and continues to serve in the United States Air Force Reserves. He has performed Penetration tests for USAF while on active duty and as a civilian contractor. He enjoys spending time with his family, playing games, and relaxing in front of the television.

SpeakerBio: James Hawk , Senior Consultant at Mandiant

James Hawk (He/Him) is a Senior Consultant with Mandiant, within Proactive Services. He is the wireless subject matter expert for his team. James has led and contributed to dozens of assessments (Red Teams and Pen Tests). He has developed internal training and tool updates for 802.11 for his company. James is a 20-year veteran of the U.S. Army and has over 10 years hands-on experience in wireless technologies. James is always researching/testing 802.11 attacks against his home lab. He is a fan of hockey, LetterKenny, and almost anything sci-fi.

SpeakerBio: Lander Beyer , Manager, Proactive Services team at Mandiant

Lander Beyer (He/Him) is the Manager of Mandiant's Proactive Services team within their Global Government section. Lander has performed dozens of penetration testing services against State, Local, and Education (SLED) organizations, to include wireless and physical assessments. Lander is a cyber branch warrant officer in the California Army National Guard, and a proud husband and father of two. He enjoys table tennis, long walks in the rain, and Domain Admin.

Description:

This workshop will teach you how to deploy Rogue APs in your client's environment. Using Rogue APs lets you test your client's Wireless Intrusion Detection System, passwords, wireless phishing education, and overall wireless security. We will discuss Rogue AP Tactics, Techniques, and Procedures, and how and why they work. In this workshop we will walk through setting up an OPEN, CAPTIVE PORTAL, WPA2, and 802.1x Rogue AP. We will also go over OWE and WPA3-SAE transition mode Rogue APs.

The primary goal is setting up Rogue APs to harvest credentials. In the workshop, we will walk through a scenario at a client's site, then set up a Rogue AP to harvest users' credentials for the various networks at the site. We will go through how to crack the harvested credentials. We will be using EAPHAMMER, HOSTAPD-MANA, WIFIPHISHER, and AIRBASE-NG for the Rogue AP portion, HASHCAT, AIRCRACK-NG, and JOHN for the cracking portion. This workshop is for beginners, but participants should have basic Linux and 802.11 knowledge and be comfortable using virtual machines.

Recommended reading/viewing:


- <https://posts.specterops.io/modern-wireless-attacks-pt-i-basic-rogue-ap-theory-evil-twin-and-karma-attacks-35a8571550ee> -
<https://sensepost.com/blog/2015/improvements-in-rogue-ap-attacks-mana-1%2F2/> -
<https://www.youtube.com/watch?v=i2-jReLBSVk>

Skill Level: Beginner

Prerequisites for students:

- None

- Materials or Equipment students will need to bring to participate: - Laptop with 8 GBS RAM
- Virtual Box / VMware Installed
 - Wireless card with Access Point Mode and monitor mode. Recommended chip set AWUS036ACM.
-

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: HL7Magic: Medical Data Hacking Made Easy

When: Friday, Aug 11, 17:00 - 17:20 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio: Katie Inns , Security Consultant at WithSecure

Katie Inns is a Security Consultant in the Attack Surface Management (ASM) team at WithSecure. Katie has 6 years' experience in the security industry, working in consulting and within an in-house security team focusing on vulnerability management and application security. Katie has spoken about the topic of ASM at conferences such as BlueTeam Con and conINT and holds the OSCP certification. Dancing has been Katie's hobby for 25 years and she also loves to listen to and play music.

Description:

In recent years, the use of internet-connected devices has become more prevalent in the healthcare sector, particularly as a means to communicate patient data. Therefore, it is essential that security testing is carried out against these devices to identify misconfigurations that could cause a severe impact, such as the prescription of incorrect drugs.

Modern healthcare protocols such as FHIR (Fast Healthcare Interoperability Resources) use the HTTP protocol to communicate, making security testing relatively straightforward. However, the use of older protocols such as HL7 (Health Level Seven) is more widespread across medical devices in the industry. These protocols are bespoke and difficult to read or intercept using current commercial and open-source security tooling, making testing of these devices challenging and cumbersome.

To address this challenge, I have developed a tool (HL7Magic) to provide security testers with an easier method of intercepting and changing HL7 messages sent to and from medical devices. This tool was created for the purpose of being integrated into Burp Suite as an extension, although it can exist independently.

After talking about how the HL7Magic was created, I will give a short demonstration using the tool for security research purpose or to identify existing CVE's across your estate. HL7Magic will be open sourced and collaborations to improve it further will be welcomed.

REFERENCES:

Forescout - Connected Medical Device Security:

<https://www.forescout.com/resources/connected-medical-device-security-a-deep-dive-into-healthcare-networks/>

Dallas Haselhorst - HL7 Medical Attacking and Defending: <https://linuxincluded.com/hl7-medical-attacking-defending/>

Anirudh Duggal - Understanding HL7 2.X Standards, Pen Testing and Defending HL7 2.X Messages:

<https://www.youtube.com/watch?v=MR7cH44fjrc>

Saurabh Harit - Breaking Bad: Stealing Patient Data Through Medical Devices:

<https://www.blackhat.com/docs/eu-17/materials/eu-17-Harit-Breaking-Bad-Stealing-Patient-Data-Through-Medical-Devices.pdf>

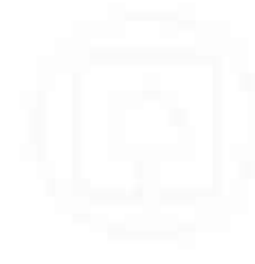
Christian Dameff, Maxwell Bland, Kirill Levchenko, Jeff Tully - Pestilential Protocol: How Unsecure HL7 Messages Threaten Patient Lives:

<https://i.blackhat.com/us-18/Thu-August-9/us-18-Dameff-Pestilential-Protocol-How-Unsecure-HL7-Messages-Threaten-Patient-Lives>

HL7apy: <https://crs4.github.io/hl7apy/tutorial/index.html#>

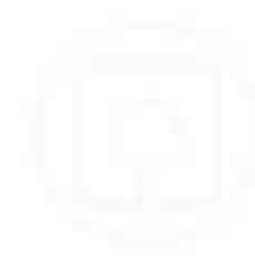
同治十三年庚午

同治十三年庚午



同治十三年庚午

同治十三年庚午



同治十三年庚午

同治十三年庚午



同治十三年庚午

同治十三年庚午



同治十三年庚午

同治十三年庚午

MIV - Friday - 14:00-14:30 PDT

Title: Holding Leaflets in the Left Hand and Bullets in the Right: A Guide to Understanding Modern Chinese Information Operations


When: Friday, Aug 11, 14:00 - 14:30 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Kieran Green

No BIO available

Description:

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Homo sapiens sapiens to Homo sapiens nova - the coming speciation

When: Saturday, Aug 12, 10:30 - 11:10 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

SpeakerBio: Almost Human (BJ)

He does science and technology consulting with a dash of anthropology. In other words, it isn't just the cool technology, it is how it is used and abused. In other words, culture matters in technology adoption. He has experience in a number of Physical Science fields, as well as Anthropology. What he says is no one's fault but his own.

Description:

The archeological record of the past 100,000+ years shows that today's Homo sapiens sapiens (HSS) won out over other Homo sapiens subspecies such as Neanderthals, Denisovans, and possibly others. Nonetheless, many HSS carry genes from older Homo sapiens subspecies. HSS now directs its own evolution. Add the advent of science-based medicine, advanced pharmaceuticals, smart implants, neural interfaces, genetic modification, a healthy(?) dose of artificial intelligence, and a transhumanist philosophy, Homo sapiens sapiens could split back into multiple subspecies. This presentation covers potential paths of future (sub-)speciation (such as Homo sapiens maximus and Homo sapiens nova) that could occur before the end of the 21st century. Will it occur peacefully? Probably not.

This is Almost Human's second Biohacking Village talk. (The previous talk focused on the death of genetic privacy.)

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Sunday - 09:00-12:59 PDT

Title: Honey Pot Workshop

When: Sunday, Aug 13, 09:00 - 12:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Think you know your way around a honeypot? Come to the Packet Hacking Village for a friendly, fun, low-pressure DEFCON challenge that's open to all! This game is designed for users of all experience levels: bring your own laptop, SSH in, and explore the adventure.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Friday - 09:00-17:59 PDT

Title: Honey Pot Workshop

When: Friday, Aug 11, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Think you know your way around a honeypot? Come to the Packet Hacking Village for a friendly, fun, low-pressure DEFCON challenge that's open to all! This game is designed for users of all experience levels: bring your own laptop, SSH in, and explore the adventure.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Saturday - 09:00-17:59 PDT

Title: Honey Pot Workshop

When: Saturday, Aug 12, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Think you know your way around a honeypot? Come to the Packet Hacking Village for a friendly, fun, low-pressure DEFCON challenge that's open to all! This game is designed for users of all experience levels: bring your own laptop, SSH in, and explore the adventure.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: House of Heap Exploitation (Pre-Registration Required)

When: Friday, Aug 11, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers:Elizabeth St. Germain,Kenzie Dolan,Maxwell Dulin "Strikeout",Nathan Kirkland,Zachary Minneker

SpeakerBio:Elizabeth St. Germain

Elizabeth St. Germain started hacking from a young age when very few inputs were sanitized. She worked in systems administration and video game development before settling into hacking as a career. She now focuses her time on web and hardware hacking, with a desire to explore the security impacts that video games can have on consumers. Most of her free time is split between either min/maxing games, competing in CTFs, exploring urban areas and nature, or making music.

SpeakerBio:Kenzie Dolan , Security Engineer at Security Innovation

Kenzie Dolan works for Security Innovation as a Security Engineer focusing on engagements ranging from IoT hacking to kiosk exploitation. Her current research interests include emerging threats against Mobile and IoT devices. She has a degree in Computer and Information Science from University of Oregon. In her free time, Kenzie enjoys composing music, playing video games or hiking in the greater Seattle area.

SpeakerBio:Maxwell Dulin "Strikeout"

Maxwell Dulin (also known as Strikeout) loves hacking all things under the sun. In his day job, he works as a security engineer primarily focused on web applications. But at night, he leaves the tangled web into the open space of radio signals, garage doors, scoreboards, RC cars, and pwn challenges. From the latter, he gained enough expertise to create a heap exploitation course that has been delivered at a number of security conferences, including DEFCON. In his spare time, he has found Linux kernel 0-days, and reverse engineered numerous wireless devices. To summarize, if you put something in front of him, he'll find a way to break it and make it do what he wants.

SpeakerBio:Nathan Kirkland

Raised on a steady diet of video game modding, when Nathan found programming as a teenager, he fit right into it. Legend says he still keeps his coffee (and tear) stained 1980s edition of The C Programming Language by K&R stored in a box somewhere. A few borrowed Kevin Mitnick books later, he had a new interest, and began spending more and more time searching for buffer overflows and SQL injections. Many coffee fueled sleepless nights later, he had earned OSCP, and graduated highschool a few months later. After a few more years of working towards a math degree and trying fervently to teach himself cryptanalysis, he decided to head back to the types of fun hacking problems that were his real first love, and has worked at Security Innovation ever since.

SpeakerBio:Zachary Minneker , Security Innovation

Zachary Minneker is a security researcher and security engineer at Security Innovation. His first computer was a PowerPC Macintosh, an ISA which he continues to defend to this day. At Security Innovation, he has performed security assessments on a variety of systems, including robots for kids, audio transcription codecs, and electronic medical systems. He has previous experience administrating electronic medical systems, and deep experience in fuzzing, reverse engineering, and protocol analysis. His research has focused on techniques for in-memory fuzzing, macOS sandbox security, and IPC methods.

Description:

Heap exploitation is an incredibly powerful tool for a hacker. As exploit mitigations have made exploitation more difficult, modern exploit development has moved to the heap. However, heap exploitation is a major wall in the binary exploitation journey because of its complexity. To conquer this difficulty, the workshop tackles the complexity head on by diving into the weeds of the allocator directly, taking on many hands-on exercises/challenges and creating easy to grasp diagrams to understand all of the concepts.

This workshop is for learning heap exploit development in glibc Malloc, which is the default allocator on most Linux distributions. With this hands-on introduction into glibc Malloc heap exploitation you will learn how the allocator functions,

heap specific vulnerability classes and to pwn with a variety of techniques. To make the material easy to consumable, there are many hands-on exercises, a pre-built virtual machine with everything necessary for binary exploitation and an immense amount of visuals for explaining the material. After taking this course you will understand the internals of the glibc Malloc allocator, be able to uncover heap memory vulnerabilities and pwn the heap with a variety of techniques, with the capability to go further into the art afterwards.

Skill Level: Intermediate

Prerequisites for students:

- Basic computer science background (x86_64 assembly, stack, programming skills in C & Python) - Basic binary exploitation skills (buffer overflow exploitation, ROP, ASLR, etc.) - Familiar with Linux developer tools such as the command line, Python scripting and GDB.

Materials or Equipment students will need to bring to participate:

- Laptop with enough power for a moderately sized Linux VM:
- ARM based MacOS has support through either QEMU or servers that people can use.
- Administrative access to the laptop
- 8GB RAM minimum
- 30GB harddrive space
- Virtualbox or another virtualization platform installed

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How an automotive security researcher had his car stolen via 'CAN Injection'

When: Friday, Aug 11, 17:00 - 17:40 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

Speakers: Ian Tabor, Ken Tindell

SpeakerBio: Ian Tabor

Ian Tabor is an automotive security consultant that has a passion for car hacking, found vulnerabilities in his own car and private Car bug bounties. Now runs Car Hacking Village UK and is part of the team behind CHV at defcon. Has created #Value-pasta-auto which is an open source 'Car in a case' and has also created the nano-can pcb and software, which can allow potential car hackers to build a cheap OBD2 (<£20) car hacking device.

SpeakerBio: Ken Tindell , CTO at Canis Labs

Dr. Ken Tindell is the CTO of Canis Labs. He obtained his doctorate in real-time systems from the University of York and has spent many years in the automotive industry, focused on tools and technology for in-vehicle real-time embedded systems. He formulated timing analysis for CAN bus to guarantee frame latencies and invented the three buffer systems for CAN controllers to avoid priority inversion. He has co-founded several automotive startups, including LiveDevices (later acquired by Bosch) and Volcano Communications Technologies (later acquired by Mentor Graphics).

Description:

The story of the investigation into the device that I believe was used to steal my 2021 Toyota RAV4 in July 2022 using 'CAN Injection'

There will be low level details on how the CAN bus works, how the 'theft device' spoofs CAN frames and using a modified transceiver to stop other ECUs communicating. We will also explain the disclosure process and possible fixes. Get the full story in the [blog](<https://kentindell.github.io/2023/04/03/can-injection/>).

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How can we encourage more hackers to engage with policy makers?

When: Saturday, Aug 12, 14:00 - 14:50 PDT

Where: Caesars Forum - Summit - 221-222 - Policy Atrium - [Map](#)

Speakers: Peter Stephens, Thomas Kranz

SpeakerBio: Peter Stephens , OECD

Peter Stephens is an experienced policy lead, in the UK and abroad. From 2018 to 2021, he led the IoT Security Policy Division across the UK government, responding to the Mirai attack, and delivering the Product Security and Telecommunications Infrastructure Bill. He is an experienced public servant, well versed in delivering through government. He has advised Ministers and Prime Ministers on the creation and running of Delivery Units in Government.

Whilst not technical by background, he brings a rebellious streak. As a student, Peter hitch hiked from Buenos Aires to New York City and he also spent two years teaching in an inner city school in south London. Experiences like this have left him with a staunch optimism about people, and he is a passionate advocate for the partnerships between policy makers and hackers to make better informed policies that can support policymakers, and citizens, around the world. He is currently a Policy Advisor at the OECD, supporting member states to navigate the range of challenges across digital security.

SpeakerBio: Thomas Kranz

Thomas Kranz is an award-winning cybersecurity consultant, a senior security & technology leader, and an author, with more than 30 years of experience in IT and cybersecurity. Starting his hacking career in the 80s in the UK, Thomas has also spent the decades since then involved in lobbying UK and EU policy makers, and contributed to various government consultations around hacking and cybersecurity. He has written two books; his award-winning “Making Sense of Cybersecurity”, and “How is AI transforming Cybersecurity?” for NVIDIA.

Description:

For decades, the US has led the way when it comes to involving hackers with policy making. From 10pht appearing before the US Congress in 1998, to the first Policy@DEFCON sessions, DEF CON has shown how hackers and feds can work together to improve the legal landscape for all of us. As Europe tackles big technology issues like privacy, reigning in Big Tech, and encouraging startups and innovation, there is a danger that hackers will be left out of contributing. What lessons can we learn from the different groups in the US who have come together to get hackers involved in policy making?

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How do you solve a problem like Mirai - establishing a policy baseline for the IoT around the world

When: Saturday, Aug 12, 16:00 - 16:50 PDT

Where: Caesars Forum - Summit - 221-222 - Policy Atrium - [Map](#)

Speakers: Kat Megas, Peter Stephens

SpeakerBio: Kat Megas

Kat leads the NIST Cybersecurity for the Internet of Things (IoT) Program, focused on advancing and accelerating the development and application of research, standards, guidelines, and technologies to improve the security and privacy of the ecosystem of connected devices. She coordinates across NIST on all things related to cybersecurity of the IoT including leading the NIST response on IoT for a number of Presidential directives (EO 13800, 14028), the IoT Cybersecurity Improvement Act of 2020 and the Consumer product cybersecurity labeling effort announced by the White House in July. Before coming to NIST, Kat worked in the private sector for 25 years leading organizations' development and execution of their IT strategies.


SpeakerBio: Peter Stephens , OECD

Peter Stephens is an experienced policy lead, in the UK and abroad. From 2018 to 2021, he led the IoT Security Policy Division across the UK government, responding to the Mirai attack, and delivering the Product Security and Telecommunications Infrastructure Bill. He is an experienced public servant, well versed in delivering through government. He has advised Ministers and Prime Ministers on the creation and running of Delivery Units in Government.

Whilst not technical by background, he brings a rebellious streak. As a student, Peter hitch hiked from Buenos Aires to New York City and he also spent two years teaching in an inner city school in south London. Experiences like this have left him with a staunch optimism about people, and he is a passionate advocate for the partnerships between policy makers and hackers to make better informed policies that can support policymakers, and citizens, around the world. He is currently a Policy Advisor at the OECD, supporting member states to navigate the range of challenges across digital security.

Description:

2023 is a significant year for the IoT, with the Cyber Resilience Act in the EU and the Product Security and Telecommunications Infrastructure Bill in the UK, as well as labelling approaches in the US and Singapore. With new regulation, there is always a threat that the 'floor' will become a 'ceiling' in the levels of security. This panel will feature speakers from across policy, industry and the hacker community to discuss what steps policy makers should take to address this live challenge.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How hackers can send feedback directly to policymakers like the pros (Pre-Registration Required)

When: Friday, Aug 11, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers: Amit Elazari, Harley Geiger

SpeakerBio: Amit Elazari , Co-Founder and CEO at OpenPolicy

Dr. Amit Elazari is Co-Founder and CEO of OpenPolicy, the world first tech-enabled policy and advocacy company, aiming to democratize access to information concerning future regulation action, policy and lobbying to entities of all sizes by leveraging scale and technology. Prior to OpenPolicy, she served as Head of Cybersecurity Policy for Intel Corp and chaired the Cybersecurity Committee for the Information Technology Industry Council (ITI) among others. She holds a Doctoral Degree in the Law (JSD) from Berkeley Law, and graduated summa cum laude with three prior degrees in law and business. Her research appeared in leading academic journals, key conferences such as RSAC, Black Hat, DEFCON, Bsides, and USENIX, and was featured at the WSJ and NYT. She co-founded Disclose.io, a non-profit that foster adoptions of legal protections for good-faith security research. Amit has a diverse background in technical, policy, and legal roles, and practiced Hi-tech, Venture Capital, and M&A law at Israel's largest law firm, Goldfarb Gross Seligman & Co.

SpeakerBio: Harley Geiger , Counsel at Venable LLP

Harley Geiger is Counsel and Senior Director at Venable, LLP, where he leads the Security Research Legal Defense Fund and the Hacking Policy Council and counsels clients on a variety of cybersecurity issues. Prior to this, Geiger was Senior Director for Public Policy at Rapid7, where he worked to expand adoption of vulnerability disclosure and legal protections for security research. Geiger also worked as Senior Legislative Counsel in the U.S. House of Representatives, where he drafted Aaron's Law, and served as Advocacy Director at the Center for Democracy & Technology.

Twitter: [@HarleyGeiger](#)

Description:

The first official comments on security policy live from DEF CON. The workshop will show hackers how to go through the process of submitting official comments to regulations and legislation.

Meeting with policymakers is only one way to make your voice heard. There are also formal channels for submitting written feedback on policy proposals that become a critical part of the record for regulations. These channels are open to the public, but non-policy professionals don't always know how to access or make the most effective use of them.

This workshop will walk security researchers through the process of using regulations.gov and congress.gov to find open opportunities to influence regulations, and actually submit official comments via those channels from the workshop. The workshop will also talk through how to form an advocacy strategy to amplify the impact of the comments - for example, how to find the right policymakers and staff to follow up with.

The workshop will be led by policy professionals with deep ties to the security community.

Skill Level: All Levels

Prerequisites for students:

- None

Materials or Equipment students will need to bring to participate: - To walk through the process and/or submit comments, bring a laptop, iPad, or other connected device you can type on

Title: How hackers can work with government, industry, civil society to protect high-risk communities

When: Saturday, Aug 12, 10:00 - 11:50 PDT

Where: Caesars Forum - Summit - 221-222 - Policy Atrium - [Map](#)

Speakers:Adrien Ogee,David Forscey,Mark E. Schreiber,Maurice Kent,Monica M. Ruiz,Sarah Powazek

SpeakerBio:Adrien Ogee , Chief Operations Officer at CyberPeace Institute

Adrien is the Chief Operations Officer of the CyberPeace Institute, an NGO based in Geneva, Switzerland. He oversees the provision of cybersecurity assistance to vulnerable populations. He spent his career in various cyber crisis response roles in Thales, ANSSI, ENISA and the WEF. Adrien holds an MEng in telecommunication and information systems, an MSc in Global Security and an MBA.

SpeakerBio:David Forscey , Cyber Strategy Planner at CISA JCDC

David Forscey is a Cyber Operations Planner with the Joint Cyber Defense Collaborative at the Cybersecurity and Infrastructure Security Agency. Prior to entering federal service, David was Managing Director for the Aspen Cybersecurity Group at The Aspen Institute based in Washington, D.C. Before that he worked as a Senior Policy Analyst at the National Governors Association Center for Best Practices and a National Security Fellow at Third Way. He graduated magna cum laude from University of Virginia and earned his law degree from Georgetown University Law Center. He also makes beats that slap.

SpeakerBio:Mark E. Schreiber

Mark E. Schreiber is a Senior Counsel at McDermott Will and Emery. Mark focuses his practice on cybersecurity, data breach response and global privacy coordination. He advises entities facing cross-border data protection, the General Data Protection Regulation (GDPR), Privacy Shield and related issues, strategic decisions, cyber assessments and investigations.

SpeakerBio:Maurice Kent

Maurice Kent is the Deputy in USAID's Cybersecurity team in the Technology Division of the Democracy, Development and Innovation Bureau. He oversees global cybersecurity capacity-building support to government and non-government partners across a range of sectors, including management of Digital APEX, one of USAID's primary capacity-building programs. He is a 15-year civil service veteran of USAID and has worked on issues such as the intersection of national security & international development, private-sector engagement and off-grid energy, innovative finance/funding practice, higher education engagement and procurement.

SpeakerBio:Monica M. Ruiz , Senior Government Affairs Manager, Digital Diplomacy at Microsoft

Monica M. Ruiz is a Senior Government Affairs Manager in Microsoft's Digital Diplomacy team. In this role she focuses on efforts to promote stability in cyberspace and advance trust, security and human rights in this domain. She holds a bachelor's degree from Florida International University and a master's degree from The Fletcher School of Law and Diplomacy at Tufts University.

SpeakerBio:Sarah Powazek , Program Director of Public Interest Cybersecurity at UC Berkeley Center for Long-Term Cybersecurity (CLTC)

Sarah Powazek serves as the Program Director of Public Interest Cybersecurity at the UC Berkeley Center for Long-Term Cybersecurity (CLTC), where she leads flagship work on the Citizen Clinic, the Consortium of Cybersecurity Clinics, and public interest cybersecurity research. She recently hosted the flagship Cyber Civil Defense Summit, a mission-based gathering to protect the nation's most vulnerable public infrastructure. Sarah previously worked at CrowdStrike Strategic Advisory Services, and as the Program Manager of the Ransomware Task Force. She is also an active member of the hacker community, and helps organize Hackers On The Hill and DEF CON Policy.

Description:

The US cyber workforce consists of 1.2 million professionals, but over half a million jobs in the cybersecurity sector remain vacant, leading to a talent shortage that affects society as a whole, and high-risk communities most particularly. The predicted

talent shortage rising to 3.5 million by 2030 suggests that these communities are unlikely to receive the help they need anytime soon.

The hacker community has been helping high-risk communities for decades. But how can they do so at scale? How can decision makers around the world, in government but also industry and civil society, work together with hackers to create solutions that build cyber resiliency for high-risk communities?

This public session will explore how governments, industry and civil society can work with the hacker community at large, to develop scalable and systemic solutions to protect those no one should ever attack. It will also aim to identify policy solutions and overall recommendations to generate more secure environments for communities at risk.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How I Built Recon to Scale with Serverless Architecture

When: Saturday, Aug 12, 12:05 - 12:50 PDT

Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio:Gunnar Andrews

No BIO available

Twitter: [@GOLDEN_infosec](#)

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

RCV - Friday - 12:10-12:55 PDT

Title: How I Found Your Password, and Other Advanced Data Hoarding Techniques

When: Friday, Aug 11, 12:10 - 12:55 PDT

Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio:M4x 5yn74x

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Sunday - 13:00-13:45 PDT

Title: How mathematical implementation issues lead to cryptographic vulnerabilities

When: Sunday, Aug 13, 13:00 - 13:45 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio: Bing Shi

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How Most Internal Networks are Compromised: A Set of Common Active Directory Attacks and How to Perform Them from Linux

When: Saturday, Aug 12, 13:00 - 16:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 6 - [Map](#)

SpeakerBio: Scott Brink

No BIO available

Twitter: [@_sandw1ch](#)

Description:

The objective of the workshop is to provide hands-on practical experiences to understand Active Directory risks. The workshop will start with the basics of Active Directory and deep dive into in depth hands on exploitation of multiple vulnerabilities.

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Friday - 13:30-13:55 PDT

Title: How NOT to Train your Hack Bot: Dos and Don'ts of Building Offensive GPTs

When: Friday, Aug 11, 13:30 - 13:55 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

Speakers:Ari Herbert-Voss,Shane Caldwell

SpeakerBio:Ari Herbert-Voss

No BIO available

SpeakerBio:Shane Caldwell

No BIO available

Description:

GPTs are all the rage and no doubt everybody is curious if you can use them for offensive security operations. In this talk we demonstrate how you can and can't use large language models (LLMs) like GPT4 to find security vulnerabilities in applications, and discuss in detail the promise and limitations of using LLMs this way. We go deep on how LLMs work, the differences between various models, and state-of-the-art techniques to improve performance.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How to [NOT] look like a Red Team

When: Saturday, Aug 12, 13:00 - 14:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 2 - [Map](#)

SpeakerBio:Michael Wylie

No BIO available

Twitter: [@themikewylie](#)

Description:

A red team is defined as a group of cybersecurity professionals that simulate the actions of those who are malicious or adversarial. However, many red teams don't emulate adversaries as much as they might think. This workshop will discuss adversary types and their motivations, common tooling mistakes that are a dead giveaway you're a red team, infrastructure mistakes, lack of action on objectives, and more from the perspective of someone who hunts red teams. This workshop is designed for entry level to intermediate level red teamers.

[Return to Index](#) - Add to  - ics [Calendar](#) file

RTV - Friday - 14:00-15:59 PDT

Title: How to [NOT] look like a Red Team

When: Friday, Aug 11, 14:00 - 15:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 4 - [Map](#)

SpeakerBio:Michael Wylie

No BIO available

Twitter: [@themikewylie](#)

Description:

A red team is defined as a group of cybersecurity professionals that simulate the actions of those who are malicious or adversarial. However, many red teams don't emulate adversaries as much as they might think. This workshop will discuss adversary types and their motivations, common tooling mistakes that are a dead giveaway you're a red team, infrastructure mistakes, lack of action on objectives, and more from the perspective of someone who hunts red teams. This workshop is designed for entry level to intermediate level red teamers.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How to build a body in your garage

When: Saturday, Aug 12, 11:10 - 11:40 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

SpeakerBio:Brennan Marsh-Armstrong

Brennan Marsh-Armstrong is a 4th year medical student at University of California San Diego School of Medicine, where he also conducts research in medical simulation and development of affordable and multi-modality medical training devices. Prior, he worked as an ophthalmology researcher and computer science studying retinal vasculature in disease pathologies at University of California David. Before that, he received Bachelor of Arts at from Amherst College in Biochemistry and Biophysics, and Computer Science while researching unique phosphatase inhibition mechanisms. In this upcoming year he hopes to matriculate into an anesthesia residency where he will also continue research on medical simulation and education.

Description:

Anatomical medical simulators are an integral part of both medical training and experimentation, as well as implant biohacking. However, commercial models typically range from thousands of dollars for simple one-piece designs to hundreds of thousands of dollars for computer-visualized designs. This cost limits the use of medically accurate training models outside of well-funded medical schools. Using only a 3D printer, silicone, ballistics gel, balloons, and yarn, I've built on the work of others to develop DIY methods of mimicking commercial medical simulators for a small fraction of their cost (usually under 10%). These models can include pulsatile arteries, superficial rolling veins, nerves, skin, muscle planes, bones, and articulating joints. They are ultrasound-able, recyclable, and, with the addition of infrared tracking cameras, can be integrated into virtual environments for internal visualization. Projects like this lower the barrier to entry for citizen scientists and less funded biohackers to experiment and explore medical implants, procedures, and ultrasound.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HRV - Saturday - 11:00-11:30 PDT

Title: How to Crush Field Day and Win Big Prizes

When: Saturday, Aug 12, 11:00 - 11:30 PDT

Where: Flamingo - Virginia City - Ham Radio Village - [Map](#)

SpeakerBio:Hamster

Engineer, hacker, hat wearer

Twitter: [@hamster](#)

Description:

Field Day is a great chance to let your competition flag fly. With a few tips and tricks, take it from a sad evening in front of a microphone to having a blast with your fellow hams.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How to Hide Behavior from Security Tools

When: Friday, Aug 11, 15:00 - 16:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 2 - [Map](#)

SpeakerBio: Mike Larkin

Mike Larkin is Founder/ CTO of Deepfactor. He's a serial entrepreneur, having been Founder/CTO at RingCube (acq. by Citrix). Mike is the author of OpenBSD Hypervisor VMM and holds numerous patents.

Description:

Detecting application behavior by monitoring library and system calls is a popular technique employed by AppSec tools. These tools can monitor and log activity, block API requests, and so on. In this workshop, you will learn some techniques to keep your activities hidden from these types of tools, using uncommon / unmonitored APIs, using unmonitored processes as confused deputies, and other approaches. You will learn how popular monitoring frameworks like eBPF work and how to circumvent their monitoring capabilities.

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Saturday - 13:00-14:59 PDT

Title: How to Hide Behavior from Security Tools

When: Saturday, Aug 12, 13:00 - 14:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 2 - [Map](#)

SpeakerBio:Deepfactor

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Saturday - 15:00-16:59 PDT

Title: How to Hide Behavior from Security Tools

When: Saturday, Aug 12, 15:00 - 16:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 2 - [Map](#)

SpeakerBio:Deepfactor

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Sunday - 12:00-13:59 PDT

Title: How to Hide Behavior from Security Tools

When: Sunday, Aug 13, 12:00 - 13:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 3 - [Map](#)

SpeakerBio:Deepfactor

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How to Lose Access to your Door in Two Easy Steps

When: Friday, Aug 11, 15:00 - 15:40 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

SpeakerBio:jos weyers

No BIO available

Description:

Information leakage is not just a digital problem. Neither is your access management system. This talk will address this often overlooked opsec fail; pictures of keys can be found all over the internet, put there by proud new buildingowners, jobhoppers or correctional facility officers. These pictures can be turned into actual working keys, causing all sorts of chaos. This talk will show why this is a problem, why we should care and maybe make you rethink your physical security a bit.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How to prioritize Red Team Findings? Presenting CRTFSS: Common Red Team Findings Score System Ver. 1.0

When: Sunday, Aug 13, 09:00 - 09:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 3 - [Map](#)

SpeakerBio:Guillermo Buendia

No BIO available

Twitter: [@bym0m0](#)

Description:

Robust red team practices generate multiple findings gradually; defenders struggle to keep up with remediations and detections. All red team findings are critical, but if everything is a priority, then nothing is. Organizations cannot feasibly defend against all ATT&CK techniques. They have more findings than they can optimally assign resources to and focus on the critical ones; they need a system to help them make this task manageable. This Workshop introduces CRTFSS: A methodology to prioritize red team findings using adversary behaviors observed in real-world threat intelligence and mapped to the MITRE ATT&CK based on the most frequent TTPs that score each finding based on the complexity of remediation and exploitability.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How to prioritize Red Team Findings? Presenting CRTFSS: Common Red Team Findings Score System Ver. 1.0

When: Friday, Aug 11, 14:00 - 14:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 5 - [Map](#)

SpeakerBio:Guillermo Buendia

No BIO available

Twitter: [@bym0m0](#)

Description:

Robust red team practices generate multiple findings gradually; defenders struggle to keep up with remediations and detections. All red team findings are critical, but if everything is a priority, then nothing is. Organizations cannot feasibly defend against all ATT&CK techniques. They have more findings than they can optimally assign resources to and focus on the critical ones; they need a system to help them make this task manageable. This Workshop introduces CRTFSS: A methodology to prioritize red team findings using adversary behaviors observed in real-world threat intelligence and mapped to the MITRE ATT&CK based on the most frequent TTPs that score each finding based on the complexity of remediation and exploitability.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How to prioritize Red Team Findings? Presenting CRTFSS: Common Red Team Findings Score System Ver. 1.0

When: Saturday, Aug 12, 16:00 - 16:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 2 - [Map](#)

SpeakerBio:Guillermo Buendia

No BIO available

Twitter: [@bym0m0](#)

Description:

Robust red team practices generate multiple findings gradually; defenders struggle to keep up with remediations and detections. All red team findings are critical, but if everything is a priority, then nothing is. Organizations cannot feasibly defend against all ATT&CK techniques. They have more findings than they can optimally assign resources to and focus on the critical ones; they need a system to help them make this task manageable. This Workshop introduces CRTFSS: A methodology to prioritize red team findings using adversary behaviors observed in real-world threat intelligence and mapped to the MITRE ATT&CK based on the most frequent TTPs that score each finding based on the complexity of remediation and exploitability.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Human Registration Open

When: Friday, Aug 11, 08:00 - 19:59 PDT

Where: Caesars Forum - Forum - 101-103 - Reg - [Map](#)

Description:

Extremely ****IMPORTANT**** notes regarding human registration:

- These notes apply to human registration only. You are a human if you are not a goon, official speaker, village staff, press, black badge holder, or similar. (If you are one of those, you need to register separately. If you don't know how, see an NFO goon (infobooth).)
- Badges are required for everyone ages 8 and older.
- If you pre-registered, please ensure that your QR code is readily accessible. If you will be presenting it on a smartphone, please ensure that your display is set to maximum brightness as you near the front of the line.
- If you did not pre-register, all badge sales are **CASH ONLY!** No checks, money orders, credit cards, IOUs, or anything else will be accepted. Please have exact change ready as you near the front of the line.
- To reiterate, ****please have exact change ready****.
- If you purchase a DEF CON badge from BlackHat, please get your badge from BlackHat before they close.
- If you lose your badge, there is no way for us to replace it. You'll have to buy a replacement at full price.
- If you are being accompanied by a full-time caretaker (such as someone who will push your wheelchair, and will accompany you at all times), please ask to speak to a Registration Goon. Your caretaker will receive a paper badge that will permit them to accompany you everywhere you go.
- A generic receipt for the cash sale of a badge will be made available on media.defcon.org after the conference. You are welcome to print your own copy of the receipt, if you need a receipt. Printed receipts are not available at the time of purchase.
- Please help us make this a great experience for everyone: ****follow directions given by goons**** and get in the correct line. Note that there may be one line for all of registration, or there may be two lines (pre-registration vs cash) -- this may change over time, based on available staffing and necessary crowd control.
- Please be patient. The time listed here for the beginning of registration is approximate. We will begin processing the line on Thursday morning as soon as the cashiers and materials are in place; this may be earlier or later than the scheduled time.
- There are no refunds given for cash sales. If you have any doubt, do not buy the badge.
- If you have questions about anything regarding registration, that are not addressed here, please ask to speak to a Registration Goon.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Human Registration Open

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Forum - 101-103 - Reg - [Map](#)

Description:

Extremely ****IMPORTANT**** notes regarding human registration:

- These notes apply to human registration only. You are a human if you are not a goon, official speaker, village staff, press, black badge holder, or similar. (If you are one of those, you need to register separately. If you don't know how, see an NFO goon (infobooth).)
- Badges are required for everyone ages 8 and older.
- If you pre-registered, please ensure that your QR code is readily accessible. If you will be presenting it on a smartphone, please ensure that your display is set to maximum brightness as you near the front of the line.
- If you did not pre-register, all badge sales are **CASH ONLY!** No checks, money orders, credit cards, IOUs, or anything else will be accepted. Please have exact change ready as you near the front of the line.
- To reiterate, ****please have exact change ready****.
- If you purchase a DEF CON badge from BlackHat, please get your badge from BlackHat before they close.
- If you lose your badge, there is no way for us to replace it. You'll have to buy a replacement at full price.
- If you are being accompanied by a full-time caretaker (such as someone who will push your wheelchair, and will accompany you at all times), please ask to speak to a Registration Goon. Your caretaker will receive a paper badge that will permit them to accompany you everywhere you go.
- A generic receipt for the cash sale of a badge will be made available on media.defcon.org after the conference. You are welcome to print your own copy of the receipt, if you need a receipt. Printed receipts are not available at the time of purchase.
- Please help us make this a great experience for everyone: ****follow directions given by goons**** and get in the correct line. Note that there may be one line for all of registration, or there may be two lines (pre-registration vs cash) -- this may change over time, based on available staffing and necessary crowd control.
- Please be patient. The time listed here for the beginning of registration is approximate. We will begin processing the line on Thursday morning as soon as the cashiers and materials are in place; this may be earlier or later than the scheduled time.
- There are no refunds given for cash sales. If you have any doubt, do not buy the badge.
- If you have questions about anything regarding registration, that are not addressed here, please ask to speak to a Registration Goon.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Human Registration Open

When: Saturday, Aug 12, 09:30 - 18:59 PDT

Where: Caesars Forum - Forum - 101-103 - Reg - [Map](#)

Description:

Extremely ****IMPORTANT**** notes regarding human registration:

- These notes apply to human registration only. You are a human if you are not a goon, official speaker, village staff, press, black badge holder, or similar. (If you are one of those, you need to register separately. If you don't know how, see an NFO goon (infobooth).)
- Badges are required for everyone ages 8 and older.
- If you pre-registered, please ensure that your QR code is readily accessible. If you will be presenting it on a smartphone, please ensure that your display is set to maximum brightness as you near the front of the line.
- If you did not pre-register, all badge sales are **CASH ONLY!** No checks, money orders, credit cards, IOUs, or anything else will be accepted. Please have exact change ready as you near the front of the line.
- To reiterate, ****please have exact change ready****.
- If you purchase a DEF CON badge from BlackHat, please get your badge from BlackHat before they close.
- If you lose your badge, there is no way for us to replace it. You'll have to buy a replacement at full price.
- If you are being accompanied by a full-time caretaker (such as someone who will push your wheelchair, and will accompany you at all times), please ask to speak to a Registration Goon. Your caretaker will receive a paper badge that will permit them to accompany you everywhere you go.
- A generic receipt for the cash sale of a badge will be made available on media.defcon.org after the conference. You are welcome to print your own copy of the receipt, if you need a receipt. Printed receipts are not available at the time of purchase.
- Please help us make this a great experience for everyone: ****follow directions given by goons**** and get in the correct line. Note that there may be one line for all of registration, or there may be two lines (pre-registration vs cash) -- this may change over time, based on available staffing and necessary crowd control.
- Please be patient. The time listed here for the beginning of registration is approximate. We will begin processing the line on Thursday morning as soon as the cashiers and materials are in place; this may be earlier or later than the scheduled time.
- There are no refunds given for cash sales. If you have any doubt, do not buy the badge.
- If you have questions about anything regarding registration, that are not addressed here, please ask to speak to a Registration Goon.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Human Registration Open

When: Thursday, Aug 10, 07:00 - 18:59 PDT

Where: Caesars Forum - Forum - 101-103 - Reg - [Map](#)

Description:

Extremely ****IMPORTANT**** notes regarding human registration:

- These notes apply to human registration only. You are a human if you are not a goon, official speaker, village staff, press, black badge holder, or similar. (If you are one of those, you need to register separately. If you don't know how, see an NFO goon (infobooth).)
- Badges are required for everyone ages 8 and older.
- If you pre-registered, please ensure that your QR code is readily accessible. If you will be presenting it on a smartphone, please ensure that your display is set to maximum brightness as you near the front of the line.
- If you did not pre-register, all badge sales are **CASH ONLY!** No checks, money orders, credit cards, IOUs, or anything else will be accepted. Please have exact change ready as you near the front of the line.
- To reiterate, ****please have exact change ready****.
- If you purchase a DEF CON badge from BlackHat, please get your badge from BlackHat before they close.
- If you lose your badge, there is no way for us to replace it. You'll have to buy a replacement at full price.
- If you are being accompanied by a full-time caretaker (such as someone who will push your wheelchair, and will accompany you at all times), please ask to speak to a Registration Goon. Your caretaker will receive a paper badge that will permit them to accompany you everywhere you go.
- A generic receipt for the cash sale of a badge will be made available on media.defcon.org after the conference. You are welcome to print your own copy of the receipt, if you need a receipt. Printed receipts are not available at the time of purchase.
- Please help us make this a great experience for everyone: ****follow directions given by goons**** and get in the correct line. Note that there may be one line for all of registration, or there may be two lines (pre-registration vs cash) -- this may change over time, based on available staffing and necessary crowd control.
- Please be patient. The time listed here for the beginning of registration is approximate. We will begin processing the line on Thursday morning as soon as the cashiers and materials are in place; this may be earlier or later than the scheduled time.
- There are no refunds given for cash sales. If you have any doubt, do not buy the badge.
- If you have questions about anything regarding registration, that are not addressed here, please ask to speak to a Registration Goon.

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Saturday - 11:00-12:59 PDT

Title: Hunt the Hacker - Detect compromises in your repositories!

When: Saturday, Aug 12, 11:00 - 12:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 1 - [Map](#)

SpeakerBio:GitGuardian

No BIO available

Description:

Put on your blue team hat and learn to detect and remediate compromises in your software delivery pipeline. Whether you have a beginner, intermediate, or advanced level, we have challenges catered for you! Using honeytokens, uncover ongoing application security attacks and map the attack surface. Gain hands-on experience prioritizing threats and enhancing your defensive skills. Receive feedback and recommendations for improvement. Plus, participants will receive a cool T-shirt! Take advantage of this exciting and educational opportunity.

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Saturday - 15:00-16:59 PDT

Title: Hunt the Hacker - Detect compromises in your repositories!

When: Saturday, Aug 12, 15:00 - 16:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 1 - [Map](#)

SpeakerBio:GitGuardian

No BIO available

Description:

Put on your blue team hat and learn to detect and remediate compromises in your software delivery pipeline. Whether you have a beginner, intermediate, or advanced level, we have challenges catered for you! Using honeytokens, uncover ongoing application security attacks and map the attack surface. Gain hands-on experience prioritizing threats and enhancing your defensive skills. Receive feedback and recommendations for improvement. Plus, participants will receive a cool T-shirt! Take advantage of this exciting and educational opportunity.

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Friday - 15:00-16:59 PDT

Title: Hunt the Hacker - Detect compromises in your repositories!

When: Friday, Aug 11, 15:00 - 16:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 4 - [Map](#)

SpeakerBio:GitGuardian

No BIO available

Description:

Put on your blue team hat and learn to detect and remediate compromises in your software delivery pipeline. Whether you have a beginner, intermediate, or advanced level, we have challenges catered for you! Using honeytokens, uncover ongoing application security attacks and map the attack surface. Gain hands-on experience prioritizing threats and enhancing your defensive skills. Receive feedback and recommendations for improvement. Plus, participants will receive a cool T-shirt! Take advantage of this exciting and educational opportunity.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hunt the Hacker - Detect compromises in your repositories!

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 2 - [Map](#)

SpeakerBio:GitGuardian

No BIO available

Description:

Put on your blue team hat and learn to detect and remediate compromises in your software delivery pipeline. Whether you have a beginner, intermediate, or advanced level, we have challenges catered for you! Using honeytokens, uncover ongoing application security attacks and map the attack surface. Gain hands-on experience prioritizing threats and enhancing your defensive skills. Receive feedback and recommendations for improvement. Plus, participants will receive a cool T-shirt! Take advantage of this exciting and educational opportunity.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hunting & Exploiting DLL Sideloads

When: Friday, Aug 11, 13:00 - 13:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 1 - [Map](#)

Speakers:Matthew Nickerson,Nick Swink

SpeakerBio:Matthew Nickerson

No BIO available

Twitter: [@turbo_sec](#)

SpeakerBio:Nick Swink

No BIO available

Twitter: [@0xC0rnbread](#)

Description:

This workshop will go through the process of manually identifying applications that can be vulnerable to DLL Sideloads and exploiting them. Attendees will learn how to use Promon to find applications that can be vulnerable to DLL sideloading, identify the correct DLL functions to proxy using CFF Explorer, and write a basic DLL to run shellcode.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hunting & Exploiting DLL Sideloads

When: Saturday, Aug 12, 10:00 - 10:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 1 - [Map](#)

Speakers:Matthew Nickerson,Nick Swink

SpeakerBio:Matthew Nickerson

No BIO available

Twitter: [@turbo_sec](#)

SpeakerBio:Nick Swink

No BIO available

Twitter: [@0xC0rnbread](#)

Description:

This workshop will go through the process of manually identifying applications that can be vulnerable to DLL Sideloads and exploiting them. Attendees will learn how to use Promon to find applications that can be vulnerable to DLL sideloading, identify the correct DLL functions to proxy using CFF Explorer, and write a basic DLL to run shellcode.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Sunday - 11:30-11:59 PDT

Title: Hunting Aberrant Maritime Network Traffic with Open-Source Software and Hardware


When: Sunday, Aug 13, 11:30 - 11:59 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio:Chet Hosmer

Chet Hosmer is an international author, educator, researcher, and founder of Python Forensics, Inc., a non-profit research institute focused on the collaborative development of open source investigative technologies using the Python programming language. Chet is also a Visiting Professor at Utica College in the Cybersecurity Graduate Program, where his research and teaching is focused on data hiding, active cyber defense and security of industrial control systems. Additionally, Chet is an Adjunct Professor at Champlain College in the Digital Forensics Graduate Program, where his research and teaching is focused on solving hard digital investigation problems using the Python programming language.

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: I Am A Former National Cybersecurity Director, Ask Me Anything!

When: Friday, Aug 11, 16:00 - 16:50 PDT

Where: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

SpeakerBio:Chris Inglis

Mr. Inglis is a former Managing Director at Paladin and former National Cyber Director and currently serves as Paladin's Senior Strategic Advisor. He is also the former Deputy Director and senior civilian leader of the National Security Agency. Mr. Inglis acted as the Agency's chief operating officer, responsible for guiding and directing strategies, operations, and policy.

Mr. Inglis began his career at NSA as a computer scientist within the National Computer Security Center. His NSA assignments include service across information assurance, policy, time-sensitive operations, and signals intelligence organizations. Promoted to NSA's Senior Executive Service in 1997, he subsequently served in a variety of senior leadership assignments culminating in his selection as the NSA Deputy Director. He has twice served away from NSA Headquarters, first as a visiting professor of computer science at the U.S. Military Academy (1991-1992) and later as the U.S. Special Liaison to the United Kingdom (2003-2006).

A 1976 graduate of the U.S. Air Force Academy, Mr. Inglis holds advanced degrees in engineering and computer science from Columbia University, Johns Hopkins University, and the George Washington University. He is also a graduate of the Kellogg Business School executive development program, the USAF Air War College, Air Command and Staff College, and Squadron Officers' School.

Mr. Inglis' military career included nine years active service with the US Air Force and twenty one years with the Air National Guard from which he retired as a Brigadier General in 2006. He holds the rating of Command Pilot and has commanded units at the squadron, group, and joint force headquarters levels. Mr Inglis' significant Awards include the Clements award as the U.S. Naval Academy's Outstanding Military Faculty member (1984), three Presidential Rank Awards (2000, 2004, 2009), and the Boy Scouts of America Distinguished Eagle Scout Award (2009).

Mr. Inglis currently serves as a Board Member of the Baltimore Area Council, Boy Scouts of America.

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Saturday - 10:00-10:30 PDT

Title: I am the captain now: Taking remote control of ships engines, helm, azipods, ballasting and plenty more.

When: Saturday, Aug 12, 10:00 - 10:30 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio: Ken Munro

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: I Am The Disinformation Campaign

When: Saturday, Aug 12, 11:30 - 12:05 PDT


Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio:MasterChen

No BIO available

Twitter: [@@chenb0x](#)

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: I Can Shop Securely Online So Why Can't I Vote Online?

When: Saturday, Aug 12, 10:30 - 11:25 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

Speakers:David Jefferson,Harri Hursti,Matt Blaze,Susan Greenhalgh

SpeakerBio:David Jefferson

Dr. David Jefferson is a computer scientist and an internationally recognized researcher on election security for well over twenty years, advising five Secretaries of State of California on voting technology issues. He served as the Chair of the Secretary of State's Post-Election Audit Standards Working Group, the panel that invented the notion of risk limiting audits and has written extensively on elections and voting security.

Twitter: [@drjefferson](#)

SpeakerBio:Harri Hursti

Harri Hursti, a world renowned data security expert and internet visionary is the Founder of the 501(c)(3) organization the Election Integrity Foundation as well as an original co-Founder of the Voting Village. Featured in two Emmy nominated documentaries, Mr. Hursti is famously known for the Hursti Hacks, where he demonstrated how to successfully alter final voting results on the Diebold Election Systems voting machines.

Twitter: [@harrihursti](#)

SpeakerBio:Matt Blaze

Matt Blaze is one of the original co-founders of the Voting Village and is currently the McDevitt Professor of Computer Science and Law at Georgetown University. He has over two decades of experience with election system security, and his current research focuses on security, privacy, and robustness in large scale systems with an emphasis on problems at the intersection of technology and public policy.

Twitter: [@mattblaze](#)

SpeakerBio:Susan Greenhalgh

Susan Greenhalgh is the Senior Advisor on Election Security for Free Speech For People. Ms. Greenhalgh has previously served as vice president of programs at Verified Voting and at the National Election Defense Coalition, advocating for secure election protocols, paper ballot voting systems and post-election audits. Recognized as an expert on election security, she has been invited to testify before the U.S. Commission on Civil Rights and has been an invited speaker at meetings of the MITRE Corporation, the National Conference of State Legislatures, the Mid-West Election Officials Conference, the International Association of Government Officials, the Election Verification Network and the E-Vote-ID conference in Bregenz, Austria. She is a frequent source for reporters from TheNew York Times, The Washington Post, The Wall Street Journal, Politico, USA Today, Associated Press, National Public Radio and other leading news outlets. She has appeared on CNN and MSNBC's The Rachel Maddow Show, and various other television news shows. She has a BA in Chemistry from the University of Vermont.

Description:

This panel will provide a comprehensive overview of all aspects of internet voting and will also provide critical perspectives on the . We will unpack common misconceptions as well as highlight some of the most vulnerable

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: I Watched You Roll the Die: Unparalleled RDP Monitoring Reveal Attackers Tradecraft

When: Friday, Aug 11, 11:30 - 12:15 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

Speakers:Andréanne Bergeron,Olivier Bilodeau

SpeakerBio:Andréanne Bergeron , Cybersecurity Researcher at GoSecure

Andréanne Bergeron has a Ph.D. in criminology from the University of Montreal and works as a cybersecurity researcher at GoSecure. Acting as the social and data scientist of the team, she is interested in online attackers' behaviors. She is an experienced presenter with over 38 academic conferences and is now focusing on the infosec field. She has presented at BSides Montreal, NorthSec, CypherCon and Human Factor in Cybercrime amongst others.

Twitter: [@AndreanBergeron](#)

SpeakerBio:Olivier Bilodeau , Cybersecurity Research Director at GoSecure

Olivier Bilodeau leads the Cybersecurity Research team at GoSecure. With more than 12 years of infosec experience, he enjoys luring malware operators into his traps and writing tools for malware research. Olivier is a passionate communicator having spoken at several conferences including BlackHat USA/Europe, Defcon, Botconf, Derbycon, and HackFest. Invested in his community, he co-founded MontréalHack, is the President of NorthSec and host its Hacker Jeopardy.

Twitter: [@obilodeau](#)

Description:

The Remote Desktop Protocol (RDP) is a critical attack vector used by evil threat actors including in ransomware outbreaks. To study RDP attacks, we created PyRDP, an open-source RDP interception tool with unmatched capabilities which helped us collect more than 100 hours of video footage of attackers in action.

To describe attackers' behaviors, we characterized the various archetypes of threat actors in groups based on their traits through a Dungeon & Dragons analogy: 1) the Bards making obtuse search or watch unholy videos; 2) the Rangers stealthily explore computers and perform reconnaissance; 3) the Thieves try to monetize the RDP access; 4)the Barbarians use a large array of tools to brute-force their way into more computers; and 5) the Wizardsuse their RDP access as a magic portal to cloak their origins. Throughout, we will reveal the attackers' weaponry and show video recordings of interesting characters in action.

This presentation demonstrates the tremendous capability in RDP interception for research benefitsand blue teams: extensive documentation of opportunistic attackers' tradecraft. An engineer and a crime data scientist partner to deliver an epic story that includes luring, understanding and characterizing attackers which allows to collectively focus our attention on the more sophisticated threats.

REFERENCES

The tool:

<https://github.com/GoSecure/pyrdp/> an extensive rewrite of Citronneur's RDPy

Building on our own work:

RDP Man-in-the-Middle - Smile! You're on Camera - GoSecure <https://www.youtube.com/watch?v=eB7RC9FmL6Q>

Slides - Google Slides

PyRDP Demo with Session Takeover - YouTube PyRDP Demo with a Payload on Connection - YouTube

https://docs.google.com/presentation/d/1UAiN2EZwDcmBjLe_t5HXB0LzbNclU3nnigC-XM4neIU/edit?usp=sharing

https://docs.google.com/presentation/d/1UAiN2EZwDcmBjLe_t5HXB0LzbNclU3nnigC-XM4neIU/edit?usp=sharing PyRDP

on Autopilot - Unattended Credential Harvesting and Client-Side File Stealing - GoSecure Announcing PyRDP 1.0 -

GoSecure

DEF CON Safe Mode Demo Labs - Olivier Bilodeau - PyRDP - YouTube Capturing RDP NetNTLMv2 Hashes: Attack

details and a Technical How-To Guide - GoSecure Cracking 2.3M Attackers-Supplied Credentials: What Can We Learn from RDP Attacks - GoSecure A New PyRDP Release: The Rudolph Desktop Protocol! - GoSecure The Level of Human Engagement Behind Automated Attacks - GoSecure Never Connect to RDP Servers Over Untrusted Networks - GoSecure

Building on scientific articles:

- [1] Cybersecurity & Infrastructure Security Agency (2020). Alert (AA20-099A). Retrieved from: <https://www.cisa.gov/uscert/ncas/alerts/aa20-099a> [2] Cox, O. (2021). Remote Desktop Protocol (RDP) attack analysis. Darktrace. Retrieved from: [https://darktrace.com/blog/remote-desktop-protocol-rdp-attack-analysis#:~:text=Remote%20Desktop%20Protocol%20\(RDP\)%20i](https://darktrace.com/blog/remote-desktop-protocol-rdp-attack-analysis#:~:text=Remote%20Desktop%20Protocol%20(RDP)%20i)
- [3] UK's National Cyber Security Centre (2021). Alert: Further ransomware attacks on the UK education sector by cyber criminals. Retrieved from : <https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector> [4] Tian, Z. et al. (2018). A Real-Time Correlation of Host-Level Events in Cyber Range Service for Smart Campus. IEEE Access, 6, pp. 35355-35364. DOI: 10.1109/ACCESS.2018.2846590. [5] Sinitsyn, F. (2017). Kaspersky Security Bulletin: STORY OF THE YEAR 2017. Retrieved from: <https://securelist.com/ksb-story-of-the-year-2017/83290/> [6] Drašar, M., Jirsík, T., & Vizváry, M. (2014). Enhancing Network Intrusion Detection by Correlation of Modularly Hashed Sketches. 8th IFIP International Conference on Autonomous Infrastructure, Management and Security (AIMS). Proceedings 8 (pp. 160-172). Springer Berlin Heidelberg. [7] Alata, E., Nicomette, V., Kaaniche, M., Dacier, M., & Herrb, M. (2006). Lessons learned from the deployment of a high-interaction honeypot. Sixth European Dependable Computing Conference, Coimbra, Portugal, pp. 39-46, DOI: 10.1109/EDCC.2006.17. [8] Udhani, S., Withers, A., & Bashir, M. (2019). Human vs bots: Detecting human attacks in a honeypot environment. 7th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE. [9] Bilodeau, O. (2022). PyRDP: Python Remote Desktop Protocol (RDP) Monster-in-the-Middle (MITM) tool and library. Tool Access from: <https://github.com/GoSecure/pyrdp> [10] Gatlan, S. (2022). Windows 11 now blocks RDP brute-force attacks by default. Bleeping Computer, <https://www.bleepingcomputer.com/news/microsoft/windows-11-now-blocks-rdp-brute-force-attacks-by-default/> [11] Seifert, C. (2006). Analyzing Malicious SSH Login Attempts. Symantec Connect Community. Retrieve from: <https://www.symantec.com/connect/articles/analyzing-malicious-sshlogin-attempts>
-

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Friday - 16:00-16:30 PDT

Title: I'm On The Hype Train: Bottom's Up!

When: Friday, Aug 11, 16:00 - 16:30 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio: Joe Slowik , Threat Intelligence Manager at Huntress

Joe Slowik has over 15 years' experience across multiple cyber domains. Currently, Joe leads threat intelligence, hunting, detection engineering, and purple teaming functions for Huntress. Previously, Joe performed in-depth threat intelligence research for DomainTools and Dragos, and led incident response operations at Los Alamos National Laboratory. Joe started off in information security through various roles in the US Navy and intelligence community.

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: ICS Forensics tool

When: Saturday, Aug 12, 14:00 - 15:55 PDT

Where: Caesars Forum - Society Boardroom - Demo Labs - [Map](#)

Speakers:Maayan Shaul,Ori Perez

SpeakerBio:Maayan Shaul

Maayan Shaul is a Malware Analyst and Security Researcher in Section52 at Microsoft Defender for IoT (formerly CyberX). Experienced in the fields of malware analysis, reverse engineering and the IoT/OT landscape.

SpeakerBio:Ori Perez

Ori Perez is a Malware Analyst and Reverse Engineer with vast experience in dealing with Nation-sponsored cyber attacks as an ex-officer at the IDF's CERT. Ori is manager at Microsoft Defender for IoT research team (formerly CyberX) and research IoT/OT protocol research for IoT/OT tools .

Description:

Microsoft ICS Forensics Tools is an open source forensic toolkit for analyzing Industrial PLC metadata and project files. Microsoft ICS Forensics Tools enables investigators to identify suspicious artifacts on ICS environment for detection of compromised devices during incident response or manual check. Microsoft ICS Forensics Tools is open source, which allows investigators to verify the actions of the tool or customize it to specific needs, currently support Siemens S7 via Snap7.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Friday - 12:00-13:30 PDT

Title: ICS Village - TSA Keynote

When: Friday, Aug 11, 12:00 - 13:30 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio: Tim Weston

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Identifying and securing Firebase vulnerabilities at scale

When: Friday, Aug 11, 13:00 - 13:25 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio:Rojan Rijal

Rojan Rijal is a security researcher with seven years of experience identifying vulnerabilities in open source, SaaS products and cloud environments. Rojan has been recognized for finding impactful vulnerabilities in private organizations such as Netflix, Zoom, Google, and GitHub and public organizations like the United State Air Force and the United Kingdom's Ministry of Defence. Rojan has presented his research at conferences like BSides San Francisco, Recon Village at Defcon 30 and more.

Twitter: [@uraniumhacker](#)

Description:

Google's Firebase product is a one-stop-shop for deploying infrastructure for small and large scale applications. Firebase provides products ranging from databases, file storage to application authentication and more. Misconfigurations in setting up these infrastructure can result in severe information disclosure and breaches.

In this talk, we will go over common vulnerabilities on each Firebase product. When going over the vulnerabilities, we will show some sample case-studies affecting small and large organizations. We will then cover some automation test cases that we used to identify these vulnerabilities at scale. Finally, we will cover some example rules that can help mitigate these vulnerabilities at large.

At the end of this talk, the audience will walkway with knowledge about different types of vulnerabilities to test when reviewing Firebase configurations.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: IDN-Squatting Detector

When: Friday, Aug 11, 13:00 - 14:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 2 - [Map](#)

SpeakerBio:Gal Bitensky

Gal is a “full stack researcher, poking anything from x86 malware binaries, ICS protocols to classic web security. He likes to share his thoughts and experiments on-stage using simple concepts and tools to demonstrate surprising results.

Twitter: [@Gal_B1t](#)

Description:

Put yourself in the shoes of a fraudster, you are trying to create a phishing website. Why inserting detectable unicode characters into a mostly-ASCII domain when you can register an entire domain in unicode? This is available when one uses a lesser-known feature called Internationalized Domain Name Top Level Domains (IDN TLD). Consider registering domains like google.com's lookalike in Hebrew - גוגל.קום, ' “<<.> fi in Japanese instead of amazon.com or fl°.-† which is the Chinese equivalent of microsoft.com.

Nekuda (dot in Hebrew) assists blue teamers to detect such domains. Its input is a string (e.g. the blue teamer's employer Brand name) and it emits over 150 potential IDN TLD domains and its registration status. It covers a potential gap in proactive phishing detection and prevention strategies and can be easily integrated into existing open-source tools like dnstwist.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: If it looks like a duck... Russia's new MDM communication strategies on Social Media after the War in Ukraine

When: Friday, Aug 11, 11:30 - 12:30 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Paula González Nagore

Paula González Nagore is an Intelligence Analyst specialized in OSINT and SOCMINT investigations and Cyber Intelligence. She currently works in the private sector conducting Digital Footprint, Digital Surveillance and Competitive Intelligence investigations. She also collaborates with different public and educational institutions to investigate disinformation and its effects, as well as the digital tools that are used today to develop disinformation campaigns and fake news in digital media and social networks.

Description:

Russia has always had a well-structured social media communication policy. With the help of media outlets such as RT or Sputnik among many others, they acted as (dis)information proxies for years. At the same time, many social media influencers helped to viralize their content by sharing and disseminating it.

However, with the start of the war in Ukraine in February 2022, all that changed. From the European Union and other countries, a cancellation of media was launched, as well as a targeting of those profiles that in a very visible way support Russian narratives. This has not stopped their action during this year and a half, but it has caused a change in the communication vectors they use and how they are using them.

In this workshop we will take the opportunity to analyze how communication strategies have evolved in social networks to disseminate and viralize disinformative narratives from official profiles of some state institutions such as embassies. To do this, we will make a comparison that will allow us to see the activity of this type of profiles in Europe and Latin America, as well as compare it with the activity of embassies in these countries by other countries such as the United States.

Based on this research, we will develop practical exercises that focus on analyzing the content of the messages, the interest in some topics over others and the use of different communication channels beyond social networks, as well as specific entities and actors to position the content to the audience. With this, we will work on the TTPs implemented as an incident creator, and the strategies that can be developed from a Blue Team perspective.

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Saturday - 16:00-16:25 PDT

Title: Ignore the Law: The Legal Risks of Prompt Injection Attacks on Large Language Models

When: Saturday, Aug 12, 16:00 - 16:25 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

SpeakerBio: Ram Shankar Siva Kumar

No BIO available

Description:

“What are the legal risks to a user/security enthusiast when performing prompt injection attacks?” That is the question this talk attempts to answer.

Prompt injection has frequently been compared to SQL injection or remote code execution. This comparison is warranted because the adversary in prompt injection is exploiting that the input to the LLM does not explicitly bound the data and the instruction: it is all garbled in natural language. So, if SQL injection is prohibited by the law in most circumstances, what about prompt injection?

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Saturday - 15:30-15:59 PDT

Title: Improving the Speed of Cybersecurity: Seven Cyber Metrics for Maritime Owners and Operators

When: Saturday, Aug 12, 15:30 - 15:59 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio: Tyson Meadors

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Influencing Voters Through Social Media, ADTECH, Big Data, and AI

When: Saturday, Aug 12, 15:35 - 16:15 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio: Joe Schniebes

Joe Schniebes is the Chief Strategy Officer and Founder at Ridgeline International, where he has developed a hands-on approach to digital signature management. He helps cross-sector organizations strike the right balance between data privacy and conveniences.

Description:

The internet and modern technologies have changed the way the world works. They have made it easier to communicate, buy and sell things, and to scale your business. But, those benefits come at a cost. The cost of convenience is your privacy. Who else is benefiting from your sensitive data? Joe Schniebes has developed a training framework that analyzes risks related to our inadvertent digital identities and the stories our data patterns tell across the devices. In this talk, Joe delves into the mechanics of how we are perceived online, who uses our data, how it impacts society, and what this means for political outcomes. He further emphasizes what we can do to exercise choice in the data sharing economy, and shares some key tips and tricks to technically safeguarding your communications data. Joe is adamant in empowering users to reclaim their digital voices and believes that entities entrusted with our data must uphold higher standards of responsibility. In the meantime, the least you can do is protect your data output.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Infrastructure as Remote Code Execution

When: Friday, Aug 11, 14:35 - 16:30 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Michael McCabe , Founder at Cloud Security Partners

Michael McCabe founded Cloud Security Partners in 2017 to create and implement security solutions for a select number of clients. Over the course of his career, Michael has led teams in startups and large financial institutions and guided them through their security journeys. He leads the OWASP Northern Virginia chapter, where he coordinated countless talks and meetups that hosted industry-leading experts. He has been a featured speaker at numerous conferences about application security, cloud security, and more.

Twitter: [@mccabe615](#)

Description:

The workshop will focus on research done on Terraform implementations and ways a malicious user could abuse them. During the workshop attendees will learn how Terraform works, how common Terraform security controls are applied, and multiple ways to bypass them and gain further access to environments.

Terraform is a powerful infrastructure as code tool, but it is also a potential security gap when not properly configured. Built into Terraform, there are numerous ways an attacker with developer-level access could abuse it to gain a larger foothold or harvest data.

During the workshop, attendees will be led through various exercises using GitHub Actions, Terraform Cloud, and AWS. The workshop aims to teach attendees how Terraform works, various methods that can be potentially abused, and some controls to prevent them.

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTV - Friday - 10:30-11:30 PDT

Title: Insider Threats (InT): Hindsight and Foresight

When: Friday, Aug 11, 10:30 - 11:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Main Stage - [Map](#)

Speakers:aviditas,plug

SpeakerBio:aviditas

No BIO available

SpeakerBio:plug

No BIO available

Description:

Fact vs Fiction: Starting at zero how to approach and handle an InT incident from a real-world use case, and then an overview of how InT is both the same and yet different from a traditional incident.

Foe vs Friend: For the right peas of mind, a primer on using a post-mortem to shift into preparation to proactively manage InT risks, plus how to preclude the usual pitfalls to promote positive reinforcement and minimize paranoia.

Fact vs Fiction: Starting at zero how to approach and handle an InT incident from a real-world use case, and then an overview of how InT is both the same and yet different from a traditional incident.

Foe vs Friend: For the right peas of mind, a primer on using a post-mortem to shift into preparation to proactively manage InT risks, plus how to preclude the usual pitfalls to promote positive reinforcement and minimize paranoia.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: IntelOps - Operation Spacewatch

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Welcome to IntelOps - Operation Spacewatch! This is a game that pits you against threat actors in the near future, who are trying to trigger nuclear war! Using cyber threat intelligence, it is up to you to support cyber protection teams to defend a vital satellite constellation and prevent a hacker network from undermining your collective defense in a race against time.

Description of the event

The event will host three simultaneous instances of a team game. Teams consist of three players each. Nine players can play at a time. We will provide three laptops and displays, along with three facilitators to ensure a smooth and enjoyable experience. Each game is 20 minutes duration, allowing up to 300 players to play the game in-person on the day. We have successfully delivered similar games to large groups of participants in the past, and we are confident that this event will add to the success of DEF CON 31.

Description of the game

Cyber Threat Intelligence (CTI) deals with information from past attacks, malware analysis and evolving threats in cyberspace. CTI enables enhanced decisions and to get ahead of the cyber attack. But how can I apply CTI and use it? The game "IntelOps - Operation Spacewatch" aims to improve players' understanding of CTI. Participants learn about different frameworks, sources and types of CTI and how they can use CTI data in a fun way. The game is built to not only teach terms and theory but apply CTI in a real-world context. The game is based on four major CTI and cyber security models. These are the NIST Cyber Security Framework (CSF), MITRE ATT&CK Matrix, the Cyber Kill Chain and the Pyramid of Pain. As a player, you are part of the United Nations (UN) CTI team and assigned to the mission to stop the attack on the satellite constellation. Your task is to use the available CTI your team has collected and assist the other members of the UN Cyber Protection Team (CPT). The players find themselves in a near future scenario where every nation has access to ballistic-launched nuclear weapons. For monitoring and control purposes, the United Nations has established a global satellite defense system to detect ballistic and hypersonic missile launches. The defense system allows the UN to be able to react immediately when suspicious activities on the weapons are detected. A global hacker network is threatening to disable the satellite constellation to use nuclear weapons for their purposes. There are 32 satellites in the global defense system your team has to protect. If 4 or more satellites are compromised and deactivated, the hacker network successfully disabled the defense system and can take control of the nuclear weapons. It is your mission to protect the satellite network and ensure the availability of the global defense system.

The players are provided with the following game components: - CTI information in form of a card deck; - An overview of the satellite network and the satellite's availability status; - The status and progress of the cyber attack presented with the Cyber Kill Chain; - The Pyramid of Pain to allocate and classify the CTI data; - A NIST CSF game board to place and apply the CTI information; - Scenario description.

While the CTI cards and the NIST CSF game board are provided as physical components, the Cyber Kill Chain, the satellite network and the Pyramid of Pain will be displayed on a monitor managed through a laptop by the game facilitators.

Summary of gameplay

The CTI cards must be played strategically to stop the cyber attack. The number of cards and information as well as the number of packages that can be sent to the satellites are limited. The CTI cards must be applied to each NIST CSF phase. Each phase of the NIST CSF has limited fields for applying the CTI information. The limitation is based on the limited number of packets that can be sent to the satellite network. The game includes four turns in total to save the satellite network. Depending on the effectiveness of the CTI application, there is a chance to stop the attack at every turn. The status of the cyber attack and the effectiveness of the applied CTI information is presented with the help of the Cyber Kill Chain. It represents the attacker's view. If the chosen CTI strategy and application were not successful, the team loses a satellite to the hacker network. In this case, the colour of a satellite on the monitor changes from red to green.

Game duration

Every game last 20 minutes in total. Each turn, the players have 5 minutes to decide on their CTI strategy, apply the information to the NIST CSF board and stop the attack. There are a maximum of four turns to a game.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: International Cyber Policy 101

When: Friday, Aug 11, 12:00 - 13:50 PDT

Where: Caesars Forum - Summit - 221-222 - Policy Atrium - [Map](#)

Speakers: Adam Dobell, Ari Schwartz, Bryony Crown, Peter Brown, Peter Stephens

SpeakerBio: Adam Dobell , First Secretary at Department of Home Affairs, Embassy of Australia, Washington DC
Adam Dobell is the First Secretary (Home Affairs) at the Embassy of Australia in Washington DC. He is responsible for policy engagement across the United States Government and with industry on a range of issues, including cybersecurity, critical infrastructure protection, and the security of critical and emerging technologies. Adam's most recent role before commencing at the Embassy was as the Acting Director for the Countering Violent Extremism Policy Coordination Section within the Department of Home Affairs from 2019-20. From 2015-2019, Adam undertook several roles in the International Policy Division of the Department of Home Affairs, including Executive Officer to the First Assistant Secretary and Acting Director of the Papua New Guinea Section. He enjoys playing and watching football (soccer), reading history and political studies.

SpeakerBio: Ari Schwartz , Executive Coordinator at Center for Cybersecurity Policy and Law
A leading voice in cybersecurity policy with over two decades of government and nonprofit experience, Ari serves as the Coordinator for the Center for Cybersecurity Policy and Law.

Ari also serves as Venable LLP's Managing Director of Cybersecurity Services and Policy. Mr. Schwartz assists organizations in developing risk management strategies, including implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to help minimize risk.

Prior to joining Venable, Mr. Schwartz was a member of the White House National Security Council, where he served as Special Assistant to the President and Senior Director for Cybersecurity.

SpeakerBio: Bryony Crown , First Secretary Cyber Policy at British Embassy, Washington D.C.
Bryony Crown is First Secretary for Cyber Policy in the British Embassy Washington DC. She covers a broad range of issues relating to cyber and works with an extensive number of international government and industry partners. Bryony has 15 years' experience in a variety of policy roles within government and specialises in national security issues.

SpeakerBio: Peter Brown , Senior Policy Adviser at Strategy and Innovation Unit of the European Parliament
Peter F Brown is Senior Policy Adviser at the Strategy and Innovation Unit of the European Parliament.

He recently returned to Brussels after serving as Senior Adviser on Technology Policy in the European Parliament's office in Washington DC.

Peter's professional career has been predominantly in the European public service and since 1990 as a career official in the European Parliament.

He resumed his career as a civil servant in 2018 after a decade in the private sector, where he advised several Fortune 50 companies and many national governments and international organisations on technology strategy and governance, in cloud, cyber, IoT, AI, and data.

He has been engaged in global standardization policy and IT standards development for more than 25 years.

SpeakerBio: Peter Stephens , OECD
Peter Stephens is an experienced policy lead, in the UK and abroad. From 2018 to 2021, he led the IoT Security Policy

Division across the UK government, responding to the Mirai attack, and delivering the Product Security and Telecommunications Infrastructure Bill. He is an experienced public servant, well versed in delivering through government. He has advised Ministers and Prime Ministers on the creation and running of Delivery Units in Government.

Whilst not technical by background, he brings a rebellious streak. As a student, Peter hitch hiked from Buenos Aires to New York City and he also spent two years teaching in an inner city school in south London. Experiences like this have left him with a staunch optimism about people, and he is a passionate advocate for the partnerships between policy makers and hackers to make better informed policies that can support policymakers, and citizens, around the world. He is currently a Policy Advisor at the OECD, supporting member states to navigate the range of challenges across digital security.

Description:

This session will help highlight the international landscape for cyber policy, highlighting the need for governments around the world to align on policy development and intervention. It will help establish a baseline of knowledge on what's happening in international cyber policy for those wanting to get up to speed, and will help set the scene for many of the policy discussions to come throughout DEF CON. This session goes hand-in-hand with the US policy 101.

The session will start with Peter Stephens of the OECD providing an overview of the main themes and topics being explored by policymakers around the world, as well as sharing what is likely to move forward through the year. Peter has direct experience of driving international policy development as he previously worked at the UK's Department for Digital, Culture, Media and Sport, where he developed the Code of Practice for Security of Consumer IoT. Peter then worked with ETSI to see the Code adopted as a standard across the European Union, and later worked with the Australian, Indian, and Singaporean governments as they explored adoption of the Code, so he has an excellent understanding of the benefits and challenges of international policy harmonization.

This portion of the session will be followed by a panel of representatives from the Australian government, the UK government, and the Center for Cybersecurity Policy and Law, which works with government on cyber policy issues around the world. These participants will each highlight top international cyber policy priorities and challenges for 2023-24, as well as how they approach policy development in the context of the global digital technology ecosystem.

This will be followed by audience Q&A so attendees can better explore the information provided and build an understanding of the international cyber policy landscape. This session establishes a baseline for many of the Policy @ DEF CON content to follow.

This is a double length session lasting 110 minutes.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Internet censorship: what governments around the globe have in store for you

When: Saturday, Aug 12, 12:00 - 12:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers: Christopher Painter, Jeff "The Dark Tangent" Moss, Joel Todoroff, Roger Dingledine

SpeakerBio: Christopher Painter , President at Global Forum on Cyber Expertise

Chris Painter is the President of the Global Forum on Cyber Expertise. He served as the first top cyber diplomat in the U.S. State Department, in the White House as Senior Director for Cyber Policy in the National Security Council, and in the Justice Department and the FBI. Awards include the RSA Award for Excellence in the Field of Public Policy (2016), the Attorney General's Award for Exceptional Service, and the Intelligence Community Legal Award (2008).

Twitter: [@c_painter](#)

SpeakerBio: Jeff "The Dark Tangent" Moss , DEF CON Communications

Mr. Moss is an internet security expert and is the founder of Both the Black Hat Briefings and DEF CON Hacking conferences. In 2022 Mr. Moss was named to the UK Government Cybersecurity Advisory Board, and in 2021 he was sworn in as a member of the DHS Cybersecurity Infrastructure Security Agency (CISA) Advisory Council (CSAC), and serves as a chairman of their Technical Advisory Council (TAC). Mr. Moss is a member of the Council on Foreign Relations (CFR) and is interested in policy issues around privacy, national security, and internet governance. He spends a lot of time in Singapore.

Twitter: [@thedarktangent](#)

SpeakerBio: Joel Todoroff , Office of the National Cyber Director

Joel Todoroff works for the Office of the National Cyber Director, where he provides legal and policy support on a range of issues, including commercial spyware and securing the foundations of the internet. He has previously worked with the Department of Defense, intelligence community, and the Privacy and Civil Liberties Oversight Board.

SpeakerBio: Roger Dingledine , The Tor Project

Roger Dingledine is president and co-founder of the Tor Project, a nonprofit that develops free and open source software to protect people from tracking, censorship, and surveillance online. Roger works with journalists and activists on many continents to help them understand and defend against the threats they face, and he is a lead researcher in the online anonymity field. EFF picked him for a Pioneer Award, and Foreign Policy magazine chose him as one of its top 100 global thinkers.

Twitter: [@RogerDingledine](#)

Description:

The internet is still largely centralized, and not every country has strong institutional controls preserving the right to access information or speak freely. Heck, even many "liberal democracies" are backsliding. While this may sound like an infosec talk suited for the think tank crowd, these developments are impacting hackers and the results they present at hacker cons.

Internet freedom tools are about empowering users to have the safety to make their own priorities. While China, Iran, and Russia are obviously key concerns in this space, many other countries are seeking to enact new laws and regulations that impact all types of users -- some with nefarious intent and others just accidentally harmful.

This conversation will explore the reasons, the symptoms, and some ideas about how to preserve our ability to set our own priorities. We will offer a holistic and detailed picture of how censorship affects our work and that of our colleagues -- how even if you feel secure in the freedom you have where you are right now, government censorship and surveillance in other places will unquestionably affect us all.

REFERENCES

Some starting points:

- Articles on general internet censorship in China, Russia, Iran.
 - Censorship measurement toolkits like OONI and Censored Planet.
 - Last year's Defcon talk, "How Russia is trying to block Tor"
 - An old but alas still very relevant primer, "Ten things to look for in a circumvention tool":
<https://svn-archive.torproject.org/svn/projects/articles/circumvention-features.html>
 - Recent terrible laws proposed in England:
<https://cdt.org/insights/indias-new-cybersecurity-order-drives-vpn-providers-to-leave-chilling-speech-and-subjecting-more>
 - and in India:
<https://cdt.org/insights/indias-new-cybersecurity-order-drives-vpn-providers-to-leave-chilling-speech-and-subjecting-more>
 - The move by the EU to block rt.com:
<https://www.euronews.com/my-europe/2022/03/08/eu-officials-defend-move-to-ban-rt-and-sputnik-amid-censorship-claim>
-



[Return to Index](#) - Add to - ics [Calendar](#) file

Title: Interventions To Address Technology-Facilitated Violence in Democracy

When: Saturday, Aug 12, 13:30 - 14:20 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

Speakers: Eric Davis, Hallie Stern, Omri Preiss, Theodora Skeadas

SpeakerBio: Eric Davis

Eric Davis has safeguarded brands, platforms, and billions of users from bad ads, bad apps, and other machinations of malefactors across global policy, product, and engineering functions. A frequent consultant and advisor across civic and private sectors on Trust & Safety, Privacy, and Security issues, Eric is a founding advisor to the Trust & Safety Professional Association, and a member of the Integrity Institute's Elections Integrity Working Group, which publishes a series of best practices and resources guides for tech platforms contending with disinformation and other issues impacting elections integrity. Previously, Eric was the former Chief Privacy and Policy Officer and global trust & safety lead at Bigo, a live streaming and short form video social media platform with over 200M users globally. Prior to Bigo, he was Senior Director for Product Management at Lifelock (acquired by Symantec), prototyping new consumer products, leading AppSec, and leading product strategy for GDPR and other privacy regulations globally. Prior to Symantec, Eric spent 13 years at Google, where he founded Google's first Trust & Safety team, Anti-Malvertising program, and the Android Security Operations and Intel team in addition to his other product policy and public policy leadership roles. Earlier in his career, he was the charter International Product Manager for Trust & Safety at eBay.

Twitter: [@ericdavis](#)

SpeakerBio: Hallie Stern

Hallie Stern is the Founder and Director of Digital Rapid Response and Information Strategy for Mad Mirror Media, a digital identity and technology consultancy, where she conducts research & development initiatives, teaches courses on disinformation and influence, and investigates anomalies in ad-tech ecosystems and algorithms for her cross-sector, cross-industry clients. She also works with the Disarm Foundation to develop tools and tandards for mitigating online harm related to disinformation and is a member of the Integrity Institute. She holds an M.S. from NYU in Global Security, Conflict, and Cybercrime, where she focused on The Human Side of Cyber Conflict, with practicums and fellowships at The Global Disinformation Index, UMD START, the Dept of State, and the Department of Homeland Security. Additional awards include The David L. Boren National Security Fellowship. Prior to her studies, Hallie spent a year exploring digital communication and data surveillance in Africa, the Mediterranean, and South East Asia.

SpeakerBio: Omri Preiss

Omri Preiss is a co-founder and managing director of Alliance4Europe, working to activate citizens towards a more democratic and sustainable Europe. Omri is based in Brussels, and has worked in EU affairs, particularly on human rights, democracy, and sustainability issues.

Twitter: [@OmriPreiss](#)

SpeakerBio: Theodora Skeadas

Theodora Skeadas works full-time as the Deputy Director of Strategy for the Massachusetts Executive Office of Technology Services and Security and part-time as a consultant on digital safety issues. Previously, she worked at Twitter, where she supported Twitter's global elections work and managed the Trust and Safety Council, and Booz Allen Hamilton, where she supported digital listening efforts around elections. In her political work, she ran for Cambridge City Council in 2021, she managed an MA Lieutenant Governor's campaign for Jimmy Tingle in 2018, and she managed a successful Cambridge City Council campaign for Sumbul Siddiqui in 2017.

Twitter: [@theodoraskeadas](#)

Description:

Technology companies with social media platforms have the potential to be a powerful ally in civil society's work to build an open, free, and democratic Internet. They have the ability to provide safe and accessible mechanisms for all people to participate in democracy, especially in closed information spaces. Continued, active engagement with technology companies

is required to properly convey the stories and experiences of democratic activists. Online violence and cyber threats against women in politics and public life (OVAW-P) poses a deepening challenge to democracy, serving as a key tool of illiberalism and democratic backsliding across the globe. OVAW-P encompasses all forms of aggression, coercion, and intimidation seeking to exclude women from politics simply because they are women. This online behavior seeks to achieve political outcomes: targeting individual women to harm them or drive them out of public life, while also sending a message that women in general should not be involved in politics. This online violence has a chilling effect on the political ambitions and engagement of women and girls, decreasing their presence and agency in politics and public life. Stopping gender-based attacks online is a solvable problem, and it is the fastest and clearest investment toward building an internet that enables everyone to be politically engaged. To address this issue, the National Democratic Institute developed a set of solutions-based interventions for technology platforms to end online violence against women in politics and public life. The interventions were developed in collaboration with a global network of women survivors. In order to more successfully advocate for the implementation of these interventions, research and advocacy efforts are needed to demonstrate the power and profitability of providing a safe space for women to politically engage online.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Sunday - 10:30-10:45 PDT

Title: Intro to Ciphers


When: Sunday, Aug 13, 10:30 - 10:45 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio:CPV Staff

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Friday - 10:30-10:45 PDT

Title: Intro to Ciphers

When: Friday, Aug 11, 10:30 - 10:45 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio:CPV Staff

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Friday - 16:30-16:45 PDT

Title: Intro to Ciphers

When: Friday, Aug 11, 16:30 - 16:45 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio:CPV Staff

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Saturday - 10:30-10:45 PDT

Title: Intro to Ciphers

When: Saturday, Aug 12, 10:30 - 10:45 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio:CPV Staff

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Friday - 10:15-10:45 PDT

Title: Intro to Lockpicking

When: Friday, Aug 11, 10:15 - 10:45 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

SpeakerBio:TOOOL

No BIO available

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Friday - 13:00-13:30 PDT

Title: Intro to Lockpicking

When: Friday, Aug 11, 13:00 - 13:30 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

SpeakerBio:TOOOL

No BIO available

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Friday - 16:00-16:30 PDT

Title: Intro to Lockpicking

When: Friday, Aug 11, 16:00 - 16:30 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

SpeakerBio:TOOOL

No BIO available

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Intro to Lockpicking

When: Saturday, Aug 12, 16:00 - 16:30 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

SpeakerBio:TOOOL

No BIO available

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Intro to Lockpicking

When: Sunday, Aug 13, 10:15 - 10:45 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

SpeakerBio:TOOOL

No BIO available

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Sunday - 13:00-13:30 PDT

Title: Intro to Lockpicking

When: Sunday, Aug 13, 13:00 - 13:30 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

SpeakerBio:TOOOL

No BIO available

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Saturday - 10:15-10:45 PDT

Title: Intro to Lockpicking

When: Saturday, Aug 12, 10:15 - 10:45 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

SpeakerBio:TOOOL

No BIO available

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Introducing IAM-APE

When: Saturday, Aug 12, 10:00 - 10:30 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Tohar Braun

Tohar Braun is a Research Tech Lead at Orca Security. During his career, he has helped bring cybercriminals to justice, stopped ransomware from extorting innocents, and unveiled numerous security issues for high-profile companies. He is passionate about helping businesses secure their cloud assets, taking malware apart, and getting shells where they shouldn't be.

Tohar is an avid gamer, trained chef, and on a quest to become a one man metal band.

Twitter: [@MaliciousDelish](#)

Description:

Permission management in AWS can be a daunting task. A single user can have an inline policy, attached managed policies, and be a member of several IAM groups. Not to mention Service Control Policies and permission boundaries!

IAM-APE, or IAM AWS Policy Evaluator, is an open source, automated tool that was designed to simplify the process of calculating effective permissions for an AWS entity. The tool gathers all the IAM policies present in your account, and then calculates the effective permissions that each entity - User, Group, or Role - has. It presents you with a single policy, summarizing all of their actual permissions

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Introduction to Cryptographic Attacks (Pre-Registration Required)

When: Thursday, Aug 10, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

SpeakerBio: Matt Cheung

Matt Cheung started developing his interest in cryptography during an internship in 2011. He worked on implementation of a secure multi-party protocol by adding elliptic curve support to an existing secure text pattern matching protocol. Implementation weaknesses were not a priority and this concerned Matt. This concern prompted him to learn about cryptographic attacks from Dan Boneh's crypto 1 course offered on Coursera and the Matasano/cryptopals challenges. From this experience he has given workshops at the Boston Application Security Conference, BSidesLV, DEF CON, and the Crypto and Privacy Village.

Description:

Using cryptography is often a subtle practice and mistakes can result in significant vulnerabilities. This workshop will cover many of these vulnerabilities which have shown up in the real world, including CVE-2020-0601. This will be a hands-on workshop where you will implement the attacks after each one is explained. I will provide a VM with Python dependencies and skeleton code included so you can focus on implementing the attack. A good way to determine if this workshop is for you is to look at the challenges at cryptopals.com and see if those look interesting, but you could use in person help understanding the attacks. While not a strict subset of those challenges, there is significant overlap. Participants should have VMWare, VirtualBox, or some other VM software installed.

Skill Level: Beginner to Intermediate

Prerequisites for students:

- Students should be comfortable with modular arithmetic and the properties of XOR. - Experience in Python or other similar language will be a plus.

Materials or Equipment students will need to bring to participate: - A laptop with VMWare or VirtualBox installed and capable of running a VM.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Friday - 12:00-12:50 PDT

Title: Introduction To Esp8266/Esp32 Microcontrollers And Building A Wi-Fi Deauthentication Detector

When: Friday, Aug 11, 12:00 - 12:50 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering VlgS - [Map](#)

SpeakerBio: Ryan Zagrodnik

Ryan Zagrodnik has been consulting as a Penetration Tester for SynerComm for almost five years. Ryan brings over sixteen years of red and blue team experience. Ryan started his career maintaining large enterprise networks as a System Administrator in 2007. Ryan earned his CISSP in 2011 and has been working in offensive security ever since. Prior to starting at SynerComm, Ryan spent three years on an internal red team at a Fortune 1000 organization. Ryan also spent several years working in offensive and defensive security roles for large enterprises who provided services for the U.S. Department of Defense and Department of Education.

Description:

Join us as we provide an introduction to the Arduino IDE and the ESP8266 microcontroller. Receive a free ESP8266 (Limited to the first 30 attendees to approach the speaker before the start of the talk and ask for a kit), and build your own Wi-Fi deauthentication detector. We will walkthrough assembly, flashing, and configuration steps.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Introduction to Exploit Development (Pre-Registration Required)

When: Saturday, Aug 12, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers:Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman,Sam Bowne

SpeakerBio:Elizabeth Biddlecome

Elizabeth Biddlecome is a consultant and instructor, delivering technical training and mentorship to students and professionals. She leverages her enthusiasm for architecture, security, and code to design and implement comprehensive information security solutions for business needs. Elizabeth enjoys wielding everything from soldering irons to scripting languages in cybersecurity competitions, hackathons, and CTFs.

SpeakerBio:Irvin Lemus

Irvin Lemus, CISSP is a Cyber Range Engineer at By Light IT Professional Services, training military personnel through international cyber security exercises. Irvin has been in the field since 2006, involved with cybersecurity competitions since 2015 as a trainer, coach, and mentor. He also has taught IT and Cybersecurity courses at Coastline and Cabrillo Colleges. He is the BACCC Cyber Competitions Regional Coordinator, Board member at Pacific Hackers and is a speaker at DEFCON. He describes himself as, "A professional troublemaker who loves hacking all the things."

SpeakerBio:Kaitlyn Handelman , Offensive Security Engineer at Amazon

Kaitlyn Handelman is an offensive security engineer at Amazon. Her focus is cybersecurity in space. In addition to traditional penetration testing, Kaitlyn works on physical devices and RF signals. In her free time, she enjoys ham radio, astronomy, and her cat, Astrocat.

SpeakerBio:Sam Bowne , Founder at Infosec Decoded, Inc

Sam Bowne has been teaching computer networking and security classes at City College San Francisco since 2000, and is the founder of Infosec Decoded, Inc. He has given talks and hands-on trainings at Black Hat USA, RSA, DEF CON, DEF CON China, HOPE, and many other conferences.

Credentials: PhD, CISSP, DEF CON Black Badge Co-Winner

Description:

Learn how to take control of Windows and Linux servers running vulnerable software, in a hands-on CTF-style workshop. We begin with easy command injections and SQL injections, and proceed through binary exploits including buffer overflows on the stack and the heap, format string vulnerabilities, and race conditions.

We will exploit 32-bit and 64-bit Intel and ARM systems, and software in PHP, Python, C++, and DOT NET. We will examine modern Windows defenses in detail, including ASLR, DEP, stack cookies, and SEHOP. We will also write Rust programs and see how they prevent memory corruption vulnerabilities.

Previous experience with C and assembly language is helpful but not required. Participants will need a laptop that can run VMware or VirtualBox virtual machines.


All materials and challenges are freely available at samsclass.info, and will remain available after the workshop ends.

Skill Level: Intermediate

Prerequisites for students:

- Familiarity with C programming and assembly language is helpful, but not essential.

Materials or Equipment students will need to bring to participate: - A laptop capable of running a virtual machine in VMware or VirtualBox.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: IOCs + APTs = "Let's play a game!" - Hack your way through a hunt!

When: Saturday, Aug 12, 14:00 - 14:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 3 - [Map](#)

SpeakerBio: Leo Cruz

No BIO available

Description:

In order to threat hunt, in order to create threat intelligence, one must first identify the what before the where, the where, before the why, the why before the who, and then you'll know who attacked you...maybe In this CTF style threat hunt, you are placed in two seats. In one you are the attacker, the other, you are the defender. Somewhere in between, you have to realize that you are also the malware author, reverse engineer, network analyst, etc...however your path may be, you will need to find all of the IOCs before time runs out and the real adversary is not found.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: IOCs + APTs = "Let's play a game!" - Hack your way through a hunt!

When: Sunday, Aug 13, 10:00 - 10:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 1 - [Map](#)

SpeakerBio: Leo Cruz

No BIO available

Description:

In order to threat hunt, in order to create threat intelligence, one must first identify the what before the where, the where, before the why, the why before the who, and then you'll know who attacked you...maybe In this CTF style threat hunt, you are placed in two seats. In one you are the attacker, the other, you are the defender. Somewhere in between, you have to realize that you are also the malware author, reverse engineer, network analyst, etc...however your path may be, you will need to find all of the IOCs before time runs out and the real adversary is not found.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: IOCs + APTs = "Let's play a game!" - Hack your way through a hunt!

When: Friday, Aug 11, 12:00 - 12:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 5 - [Map](#)

SpeakerBio: Leo Cruz

No BIO available

Description:

In order to threat hunt, in order to create threat intelligence, one must first identify the what before the where, the where, before the why, the why before the who, and then you'll know who attacked you...maybe In this CTF style threat hunt, you are placed in two seats. In one you are the attacker, the other, you are the defender. Somewhere in between, you have to realize that you are also the malware author, reverse engineer, network analyst, etc...however your path may be, you will need to find all of the IOCs before time runs out and the real adversary is not found.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: IOCs + APTs = "Let's play a game!" - Hack your way through a hunt!

When: Friday, Aug 11, 16:00 - 16:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 3 - [Map](#)

SpeakerBio: Leo Cruz

No BIO available

Description:

In order to threat hunt, in order to create threat intelligence, one must first identify the what before the where, the where, before the why, the why before the who, and then you'll know who attacked you...maybe In this CTF style threat hunt, you are placed in two seats. In one you are the attacker, the other, you are the defender. Somewhere in between, you have to realize that you are also the malware author, reverse engineer, network analyst, etc...however your path may be, you will need to find all of the IOCs before time runs out and the real adversary is not found.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Friday - 15:30-16:29 PDT


Title: IoT Village - Free Book Signing with author Ted Harrington

When: Friday, Aug 11, 15:30 - 16:29 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Free Book Signing with author Ted Harrington of the #1 bestseller, Hackable. This is a free event. Attendees will receive the book on a first come, first serve basis. We recommend arriving at least 30 minutes early.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: IoT Village CTF

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Hosted in IoT Village, teams of 1-6 players compete against one another by exploiting off-the-shelf IoT devices. This has been completely redesigned from previous contests, and features real-world devices that all have real-world vulnerabilities with real-world impacts.

This CTF is open to anyone! It is approachable for entry level people to experience getting their first root shell on IoT, but to really advance in this CTF teams will need to perform detailed vulnerability research, hardware hacking, firmware analysis, reverse engineering, and limited exploit development.

CTFs are a great experience to learn more about security and test your skills, and the IoT CTF provides the most realistic hacking experience around! So, join up in a team (or even by yourself) and compete for fun and prizes! Exploit as many as you can during the con and the top three teams will be rewarded.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-13:59 PDT

Title: IoT Village CTF

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Hosted in IoT Village, teams of 1-6 players compete against one another by exploiting off-the-shelf IoT devices. This has been completely redesigned from previous contests, and features real-world devices that all have real-world vulnerabilities with real-world impacts.

This CTF is open to anyone! It is approachable for entry level people to experience getting their first root shell on IoT, but to really advance in this CTF teams will need to perform detailed vulnerability research, hardware hacking, firmware analysis, reverse engineering, and limited exploit development.

CTFs are a great experience to learn more about security and test your skills, and the IoT CTF provides the most realistic hacking experience around! So, join up in a team (or even by yourself) and compete for fun and prizes! Exploit as many as you can during the con and the top three teams will be rewarded.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

Title: IoT Village CTF

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Hosted in IoT Village, teams of 1-6 players compete against one another by exploiting off-the-shelf IoT devices. This has been completely redesigned from previous contests, and features real-world devices that all have real-world vulnerabilities with real-world impacts.

This CTF is open to anyone! It is approachable for entry level people to experience getting their first root shell on IoT, but to really advance in this CTF teams will need to perform detailed vulnerability research, hardware hacking, firmware analysis, reverse engineering, and limited exploit development.

CTFs are a great experience to learn more about security and test your skills, and the IoT CTF provides the most realistic hacking experience around! So, join up in a team (or even by yourself) and compete for fun and prizes! Exploit as many as you can during the con and the top three teams will be rewarded.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: IoT Village Hacking Playground

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

IoT Village Hacking Playground: The IoT Village Hacking Playground is a set of hands-on labs developed to teach the tools and techniques for discovering and exploiting some of the common weaknesses found in IoT devices in just a few minutes. Whether you're a penetration tester that has never hacked IoT devices, or even someone that has never hacked anything, these self-guided labs will introduce the audience to the world of IoT and the security issues that can plague these devices. Work at your own pace following our IoT Hacking guides and if you get stuck, our instructors are on hand to provide assistance and answer any questions.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Saturday - 10:00-17:59 PDT

Title: IoT Village Hacking Playground

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

IoT Village Hacking Playground: The IoT Village Hacking Playground is a set of hands-on labs developed to teach the tools and techniques for discovering and exploiting some of the common weaknesses found in IoT devices in just a few minutes. Whether you're a penetration tester that has never hacked IoT devices, or even someone that has never hacked anything, these self-guided labs will introduce the audience to the world of IoT and the security issues that can plague these devices. Work at your own pace following our IoT Hacking guides and if you get stuck, our instructors are on hand to provide assistance and answer any questions.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: IoT Village Hacking Playground

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

IoT Village Hacking Playground: The IoT Village Hacking Playground is a set of hands-on labs developed to teach the tools and techniques for discovering and exploiting some of the common weaknesses found in IoT devices in just a few minutes. Whether you're a penetration tester that has never hacked IoT devices, or even someone that has never hacked anything, these self-guided labs will introduce the audience to the world of IoT and the security issues that can plague these devices. Work at your own pace following our IoT Hacking guides and if you get stuck, our instructors are on hand to provide assistance and answer any questions.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Sunday - 10:00-13:59 PDT

Title: IoT Village Hardware Hacking Exercises 2023

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

From Memory Manipulation to Root Access: In this year's exercises, we will be guiding the attendees through another multistep process to gain root access to a targeted IoT device via UART by first extracting the firmware to gain access to the root password and identifying memory offsets that allow attendees to alter U-Boot running memory to disable filters blocking needed changes to device boot environment variables. This series of exercises will cover steps including U-boot interaction, firmware extraction process, altering memory style attack, binwalk to extract cramfs filesystem, hexedit to identify memory offsets, and cracking of extracted password hashes.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: IoT Village Hardware Hacking Exercises 2023

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

From Memory Manipulation to Root Access: In this year's exercises, we will be guiding the attendees through another multistep process to gain root access to a targeted IoT device via UART by first extracting the firmware to gain access to the root password and identifying memory offsets that allow attendees to alter U-Boot running memory to disable filters blocking needed changes to device boot environment variables. This series of exercises will cover steps including U-boot interaction, firmware extraction process, altering memory style attack, binwalk to extract cramfs filesystem, hexedit to identify memory offsets, and cracking of extracted password hashes.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Saturday - 10:00-17:59 PDT

Title: IoT Village Hardware Hacking Exercises 2023

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

From Memory Manipulation to Root Access: In this year's exercises, we will be guiding the attendees through another multistep process to gain root access to a targeted IoT device via UART by first extracting the firmware to gain access to the root password and identifying memory offsets that allow attendees to alter U-Boot running memory to disable filters blocking needed changes to device boot environment variables. This series of exercises will cover steps including U-boot interaction, firmware extraction process, altering memory style attack, binwalk to extract cramfs filesystem, hexedit to identify memory offsets, and cracking of extracted password hashes.

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTV - Friday - 11:30-12:30 PDT

Title: IR 101: Part I, II, III

When: Friday, Aug 11, 11:30 - 12:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Project Obsidian: 101 Track (0x41) - [Map](#)

Speakers:ChocolateCoat,CountZ3r0,Cyb3rhawk

SpeakerBio:ChocolateCoat

No BIO available

SpeakerBio:CountZ3r0

David Roman is a Senior Incident Response Consultant at Cisco Talos Incident Response, with 26 years of experience in the IT and security industry. David leads investigations to help customers on their worst career day recover from security incidents and help them better prepare for the future. Volunteering and helping others learn about cybersecurity is a passion for David. He helps run local DEF CON and CitySec groups and guest lectures at Oklahoma State University.

SpeakerBio:Cyb3rhawk

DE&TH

Description:

This IR 101 session include two modules.

Part I: What is IR

Part II: IR Lifecycle and Frameworks

Part III: IR Plans and Playbooks

IR Foundations & Analyst Mindset and Quality Assurance

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTV - Friday - 13:30-14:30 PDT

Title: IR 101: Part IV, V

When: Friday, Aug 11, 13:30 - 14:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Project Obsidian: 101 Track (0x41) - [Map](#)

SpeakerBio:juju43

BlueTeam DFIR helping people to grow

Description:

This IR 101 session include two modules.

Part IV: Analyst Mindset

Part V: Quality Assurance Processes

IR 101 covering Analyst Mindset and Quality Assurance Processes.

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTV - Friday - 10:30-11:30 PDT

Title: IR Analysis: Part I & II

When: Friday, Aug 11, 10:30 - 11:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Project Obsidian: Kill Chain Track (0x42) - [Map](#)

SpeakerBio:juju43

BlueTeam DFIR helping people to grow

Description:

This Kill Chain IR analysis session includes two modules.

Part I: Know Yourself, Know Your Logs: How to establish some baselines with the logs that you have to support incident response. Part II: MSTICPY and Velociraptor Offline Collection Analysis: Offline analysis using code. How to setup your questions and make your analysis process repeatable with jupyter notebook and msticpy.

IR analysis in two parts; Part I: Know Yourself, Know Your Logs, Part II: MSTICPY and Velociraptor Collection & Offline Analysis.

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTV - Saturday - 10:30-11:30 PDT

Title: IR/4n6: Obsidian DFIR - Gang aft agley

When: Saturday, Aug 12, 10:30 - 11:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Main Stage - [Map](#)

SpeakerBio: Omenscan

No BIO available

Description:

Come listen to some grouchy, well worn Incident Responders talk about the planning and reality of staging a live fire DFIR simulation, and how even well planned exercises, just like any other IR never go as planned.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Saturday - 13:00-13:30 PDT

Title: Is 2023 the Year of Privacy: How History and States are Posed to Change Privacy?

When: Saturday, Aug 12, 13:00 - 13:30 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio: Anthony Hendricks

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Sunday - 12:30-12:59 PDT

Title: Is China Prepping an “Unforgettable Humiliation for GPS & America” [VIRTUAL]

When: Sunday, Aug 13, 12:30 - 12:59 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio: Dana Goward

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: It's Coming from Inside the House: Next Steps for Addressing U.S. Network Abuse

When: Friday, Aug 11, 12:00 - 13:50 PDT

Where: Caesars Forum - Summit - 220 - Policy NOT-A-SCIF - [Map](#)

Speakers: David Forscey, Emily Paull, Peter Su, Seth McKinnis, Thomas Klein

SpeakerBio: David Forscey , Cyber Strategy Planner at CISA JCDC

David Forscey is a Cyber Operations Planner with the Joint Cyber Defense Collaborative at the Cybersecurity and Infrastructure Security Agency. Prior to entering federal service, David was Managing Director for the Aspen Cybersecurity Group at The Aspen Institute based in Washington, D.C. Before that he worked as a Senior Policy Analyst at the National Governors Association Center for Best Practices and a National Security Fellow at Third Way. He graduated magna cum laude from University of Virginia and earned his law degree from Georgetown University Law Center. He also makes beats that slap.

SpeakerBio: Emily Paull , Cyber Operations Planner at CISA JCDC

Emily Paull is a Cyber Operations Planner with the Cybersecurity and Infrastructure Security Agency's Joint Cyber Defense Collaborative (JCDC). Emily works with government and private sector partners to identify and address cyber threats to U.S. critical infrastructure. Her prior experience includes working on various policy issues, including election security, emerging technology, and foreign investment risk. She has a BA from the University of Michigan and an MA from Columbia University.

SpeakerBio: Peter Su , Cyber Operations Planner at CISA JCDC

Peter Su is a Cyber Operations Planner with the Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative (JCDC), where he works with government and private sector partners to identify, measure, and mitigate cyber risk. Before joining CISA JCDC, Peter worked as a Professional Staff Member on the Senate Homeland Security and Governmental Affairs Committee's (HSGAC) Subcommittee on Emerging Threats and Spending Oversight, focusing on cybersecurity and other emerging technology issues in the homeland security space. Peter has a PhD from MIT in Materials Science and Engineering (researching semiconductor materials and nanofabrication) and a BSE from the University of Michigan.

SpeakerBio: Seth McKinnis , Future Plans Section Chief at CISA JCDC

Seth McKinnis is Section Chief for Future Plans at CISA's Joint Cyber Defense Collaborative. In this role, Seth sets JCDC's joint cyber planning priorities by identifying critical cyber issues at the nexus between cybersecurity and critical infrastructure. Seth has worked with critical infrastructure and cybersecurity at CISA and the Department of Homeland Security since 2013, including CISA's Shields Up campaign, Free Cybersecurity Services and Tools List, #RumorControl, and leading CISA's risk analysis on security and resilience of election systems. Seth is a Certified Information Systems Security Professional (CISSP) and a graduate of Patrick Henry College and the Naval Postgraduate School's Emergence Program.


SpeakerBio: Thomas Klein , Cyber Operations Planner at CISA JCDC (Joint Cyber Defense Collaborative)

Tom Klein is a Cyber Operations Planner with the Cybersecurity and Infrastructure Security Agency's Joint Cyber Defense Collaborative (JCDC). In his current role, Tom focuses on policy & strategy inputs to JCDC's planning efforts as well as, the unique cyber risks facing industrial control systems, and to some extent the financial sector. Previously, Tom was a National Security Fellow with Third Way and an OSINT investigator. He received his BA in Philosophy & Political Science from NYU Abu Dhabi, and his MPP focusing on cyber policy from Oxford University's Blavatnik School of Government.

Description:

The Joint Cyber Defense Collaborative (JCDC) unifies cyber defenders, including running collaborative cyber planning efforts between government and industry to develop practical courses of action that address cyber risks. The JCDC team is now working with partners across the cyber ecosystem to develop planning priorities for 2024. One focus area we're exploring for future work is supporting and strengthening collaborative, voluntary efforts to understand and prevent malicious abuse of virtual resources hosted inside the United States. This session will give DEF CON attendees the opportunity to provide direct

and candid feedback to JCDC on the nature of the problem posed by abuse of US infrastructure propose tangible ideas that will inform 2024 joint cyber defense planning efforts.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

Title: It's In That Place Where I Put That Thing That Time

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Your friend called. They had their place raided. They swear it's a setup. But now they're in jail and you're the only hope they have. Can you collect the evidence that will let them walk free? Where should you look? The evidence is everywhere, and it could be anywhere. You might be sitting on it. You might be standing near it. It might be stuck to something. It might be lying in plain sight. Find the disks and bring them to us. All they said to you before they hung up was "It's in that place where I put that thing that time." Good luck.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: It's In That Place Where I Put That Thing That Time

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Your friend called. They had their place raided. They swear it's a setup. But now they're in jail and you're the only hope they have. Can you collect the evidence that will let them walk free? Where should you look? The evidence is everywhere, and it could be anywhere. You might be sitting on it. You might be standing near it. It might be stuck to something. It might be lying in plain sight. Find the disks and bring them to us. All they said to you before they hung up was "It's in that place where I put that thing that time." Good luck.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: It's not that your threat intelligence IOCs are worthless...

When: Saturday, Aug 12, 17:00 - 17:59 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Main Stage - [Map](#)

Speakers: Charlie, Lauren Proehl, Mick/nohackme, Silas Cutler

SpeakerBio: Charlie

Charlie has worked in threat intelligence for over a decade, focusing mostly on financial services but has also worked for an email security vendor providing threat intelligence to a variety of verticals. He is now a part of a team that provides threat intelligence to banks of all sizes.

SpeakerBio: Lauren Proehl

Lauren Proehl is the Director of Global Cyber Defense at Marsh McLennan. She is an experienced incident responder and threat hunter who has helped identify and mitigate cyber adversaries in Fortune 500 networks. After leading investigations ranging from data breaches to targeted attacks, she now works to define some part of the limitless unknowns in cyberspace and make cybersecurity less abstract, and more tangible. Lauren sits on the CFP board for BSides Kansas City, heads up SecKC parties, and tries to escape computers by running long distances in the woods.

SpeakerBio: Mick/nohackme

Mick fell in love with the idea of cyberspace around 9-years-old after reading "Neuromancer," thinking "I could do that." He is still trying to do "that." Former perennial spot the fed participant, Mick has seen threat intelligence work, and... not. After spending too long in government and a stint in South Bend, Mick is a Global Security Advisor on Splunk's SURGe team.

Taking a break from Gooning at DEFCon, he's back for another year to moderate a spicy panel you'll want to see.

SpeakerBio: Silas Cutler

Silas Cutler is an experienced security researcher and malware analyst. His focus has been researching organized cyber-crime groups and state-sponsored attacks.

Description:

From discovery to dissemination, the value of cyber threat intelligence rapidly decreases to the point of uselessness. Why? It's complicated. Does it have to be? Join us for a lively discussion on threat intelligence from discovery and dissemination, and how to find value in the valueless.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: IVY HAUL: A Computational Linguistics Analysis of a Disinformation Actor

When: Saturday, Aug 12, 15:30 - 16:30 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Shea Nangle

Shea Nangle does not now, nor has he ever, worked for a three letter agency. He has, however, been accused on several occasions of being a Fed, and there was a multiyear period when his wife really thought he worked for a front company. To the best of his knowledge, only one of his previous employers has ever been investigated by the US government as a potential front for foreign intelligence. GLOMAR.

In his spare time, he enjoys long walks on the beach and reruns of Magnum, P.I.

Description:

In April 2023, Sarah Bills was revealed to be one of the main people behind the DonbassDevushka social media "personality", posting pro-Russian propaganda to a variety of social media accounts since 2014. One of the main accounts, the PeImeniPusha Twitter account has been active since 2015. Ms. Bills has claimed that there was a team of at least a dozen people responsible for the Donbass Devushka personality. I have leveraged a number of open source tools, along with original methodology and tools, to analyze data collected from the PeImeniPusha Twitter account and several other sources. Primary areas of research and analysis have included identification of authorship clusters, as well as analysis of changes to content posted, with a focus on identifying changes to account content that are linked to current events, such as the Russian invasion of Ukraine. In this session, I will share the results of this research and analysis for the first time, and will include an exploration of methodologies used (including successes and failures) and a discussion of applications of this work to the analysis of other disinformation actors.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: J4 Gate, The Hustler Poker Cheating Scandal investigation and how Hacking helped me do it

When: Saturday, Aug 12, 09:30 - 10:15 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

SpeakerBio: Scott "Duckie" Melnick, Principal Security Research and Development at Bulletproof International. Duckie, aka "Scott Melnick," started his shenanigans War Dialing on his Apple][+ at an early age and has been attending Defcon and other hacking conferences for over 26 years. Scott currently heads the Security R&D team for Bulletproof, a part of Gaming Laboratories International. Specializing in casino gaming security, he spends his time hacking and reverse engineering electronic gaming devices such as slot machines, sneaking around casinos, getting kicked out of casinos, and speaking at gaming security and regulation events. Over the years, he has worked on many gaming fraud and security breach cases. Before joining Bulletproof, he served as the Vice President of Systems Software Development for a slot and table game maker and held various positions in the slot industry, leading mechanical and electrical engineering projects, overseeing security, and managing IT gaming operations, among other things. He is excited to be delivering his first Defcon presentation this year and contributing back to the hacker community.

Twitter: [@duckie37](#)

Description:

On September 29th, 2022, one of the most controversial poker hand was played, winning an all-in \$240K cash pot on the Hustler Casino Live poker stream (HCL) by newcomer Robbi Jade Lew. The controversy and accusations of cheating took the poker and media world by storm! Conspiracy theories emerged immediately within the media, podcasts and the internet sleuths, including crossover theories from the Chess cheating scandal, accusations of collusion with HCL employees, and advanced technology being used. This is the wild tale of my investigation into cheating live stream poker if it was done and what are all the ways I would do it.

I will also show how I utilized my experience from attending hacking conferences such as Defcon for over 26 years, the competitions and how I tapped into a broad range of resources throughout the years of making friends in the hacking community, reaching out to discord groups and doing that which isn't covered in the academic world. This is why I am here; this is why you are here.

This war story contains treachery, wild technology theories, drama and current criminals on the run. But you, the audience must all decide. Is Robbi innocent or guilty? Was something missing? How would you have cheated?

REFERENCES:

- Hancke, G. P. (n.d.). Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens. Retrieved from <http://www.rfidblog.org.uk/Hancke-JoCSSpecialRFIDJune2010.pdf>
- <https://wa5vjb.com/>
- How to Build a Low-Cost, Extended-Range RFID Skimmer https://www.usenix.org/legacy/events/sec06/tech/full_papers/kirschenbaum/kirschenbaum_html/index.html
- DEF CON 17 - Christine Paget - RFID Myth busting <https://www.youtube.com/watch?v=SMm4g5yhDoY>
- DEF CON 18 - Christine Paget - Extreme-Range RFID Tracking https://www.youtube.com/watch?v=q9_8F_BKeto
- PokerGFX Software - <https://videopokertable.net>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: JWT Parkour

When: Saturday, Aug 12, 11:00 - 12:59 PDT

Where: Flamingo - Savoy - AppSec Village - Workshop - [Map](#)

SpeakerBio: Louis Nyffenegger

Louis is a security engineer based in Melbourne, Australia. He is the founder of PentesterLab, a learning platform for web penetration testing.

Twitter: [@snyff](#)

Description:

Nowadays, JSON Web Tokens are everywhere. They are used as session tokens, OAuth tokens or just to pass information between applications or microservices. By design, JWT contains a high number of security and cryptography pitfalls that creates interesting vulnerabilities. In this workshop, we are going to learn how to exploit some of those issues.

First, we are going to look at the old issues: the none algorithm, guessing/bruteforcing the hmac secret.

Then we will look at more recent issues like how an RSA public key can be computed from multiple signatures to exploit algorithm confusion and how the same attack can be done with ECDSA. We will also look at leveraging issues with the kid/jku/x5u. And finally how to leverage CVE-2022-21449 to bypass the signature mechanism.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Katalina

When: Friday, Aug 11, 10:00 - 11:55 PDT

Where: Caesars Forum - Society Boardroom - Demo Labs - [Map](#)

SpeakerBio:Gabi Cirlig

Software developer turned rogue, Gabriel went from developing apps for small businesses to 2M+ DAU Facebook games while keeping an eye for everything shiny and new. For a couple of years he has shifted gears and started his career as a security researcher at HUMAN Security while speaking at various conferences showcasing whatever random stuff he hacked. With a background in electronics engineering and various programming languages, Gabi likes to dismantle and hopefully put back whatever he gets his hands on.

Description:

Android malware has long relied on basic string obfuscation techniques to make analysts suffer while reversing it. The current state of the art in mass string deobfuscation relies on two techniques. One of them is executing the sample and hoping to get some hits on the methods with the interesting strings, while the other is forking big bucks for some well known tools in the industry. Both the workload and the financial impact of these methods can severely impact an independent researcher's ability to tackle modern Android malware. My solution is simple: build an environment that can execute Android bytecode one instruction at a time. While the approach is not new (Unicorn comes to mind), there is no such tool available for the Android ecosystem. This allows researchers to speed up their reversing efforts and tackle more intricate and advanced malware with ease.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Keeping stores safe: how do we better secure apps and app stores?

When: Friday, Aug 11, 17:00 - 17:50 PDT

Where: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

Speakers:Charlie Gladstone,David Rogers

SpeakerBio:Charlie Gladstone , UK Department for Science, Innovation, and Technology

Charlie Gladstone leads the UK Government's work on app store security in the Department for Science, Technology and Innovation. He has worked in tech policy for over five years, where he has specialised in exploring the intersection between technology, society and regulation. Before working in Government, Charlie provided public policy consultancy services to the tech sector clients. He has developed policy on a range of issues including cyber security, digital regulation and artificial intelligence.

SpeakerBio:David Rogers , CEO at Copper Horse

David is a mobile phone and IoT security specialist who runs Copper Horse Ltd, a software and security company based in Windsor, UK. He chairs the Fraud and Security Group at the GSMA. He has spoken at a number of hacking conferences on his security research work including DEF CON's Car Hacking Village, 44CON, B-Sides London, B-Sides Cymru and B-Sides LV. He was awarded an MBE for services to Cyber Security in the Queen's Birthday Honours 2019.

Description:

As the global pivot to mobile continues and demand for smart devices grows stronger, apps are the main interface between users and the internet, and app stores are the stewards of this ecosystem. App stores are an increasingly valuable target for cyber attacks, with malicious apps stealing vast amounts of data, hijacking devices, and defrauding users of money and personal data. As our usage of apps continues to accelerate at pace, protecting app users from these threats is a collective challenge for governments, hackers, and the cyber security community as a whole.

In this fireside discussion, Charlie Gladstone from the UK's Department for Science, Innovation and Technology will provide an overview of the UK's approach to tackling this issue, and discuss the challenges facing governments in securing apps and app stores. This is an opportunity to discuss the distinct challenges we see in the management of app security, and how these risks vary between different countries. As geopolitical trends continue to shape the development of the internet, this Q&A will explore how governments can work with the hacking community to strengthen app stores and app security across the world.

[Return to Index](#) - Add to  - ics [Calendar](#) file

RCV - Friday - 10:00-10:50 PDT

Title: Keynote - Reshaping Reconnaissance: AI's Role in Open Source Intelligence

When: Friday, Aug 11, 10:00 - 10:50 PDT


Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio: Matt Edmondson

No BIO available

Twitter: [@matt0177](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Friday - 19:00-19:59 PDT

Title: Kids Only Karaoke

When: Friday, Aug 11, 19:00 - 19:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Come sing Hacker Karaoke! Its just like normal Karaoke, but with 110% more root shellz.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Kraken, a modular multi-language webshell for defense evasion

When: Saturday, Aug 12, 12:00 - 13:55 PDT

Where: Caesars Forum - Society Boardroom - Demo Labs - [Map](#)

SpeakerBio:Raul Caro

Raul Caro Teixido (OSCP, CRTE) is an Offensive Security Engineer at Telefonica Tech. He is the co-author of Mistica (your friendly data smuggler) presented in BlackHat Arsenal USA 2020, and the creator of Kraken (a modular multi-language webshell).

Description:

Kraken is a modular multi-language webshell focused on web post-exploitation and defense evasion. It supports three technologies (PHP, JSP and ASPX) and its core is developed in Python. Kraken follows the principle of "avoiding command execution" by re-implementing it through the functionalities of the programming language in use. Kraken seeks to provide usability, scalability and improve the OPSEC of ongoing operations.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Kubernetes Offense

When: Friday, Aug 11, 14:00 - 16:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 6 - [Map](#)

SpeakerBio:Michael Mitchell

No BIO available

Twitter: [@awildbeard](#)

Description:

The workshop is about understanding and exploiting Kubernetes Cluster environments. There is a exploitable cluster that has been built and is deployable for the workshop. The workshop was originally written for people that do not have a large familiarity with Kubernetes or Containers. It is not intended to provide new or novel attacks, but help accelerate someone's path to understanding and using new and novel attacks.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Saturday - 14:00-14:25 PDT

Title: Labs and Trust: How to build a successful aviation cybersecurity research programme

When: Saturday, Aug 12, 14:00 - 14:25 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio: Martin Strohmeier

No BIO available

Description:

Over the past 10 years, armasuisse Science + Technology has been successfully conducting open security research with real avionics hardware, working closely with industry and regulators. The talk will cover our technical results as well as our approach to building trust with regulators and the industry by working as responsibly as possible while still maintaining the openness required to obtain the necessary results and drive change in the wider ecosystem.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Lambda Looter

When: Saturday, Aug 12, 10:00 - 11:55 PDT

Where: Caesars Forum - Accord Boardroom - Demo Labs - [Map](#)

Speakers: Doug Kent, Rob Ditmer

SpeakerBio: Doug Kent

Doug has worked at State Farm for about 20 years. Working on mostly security technologies ranging from Active Directory, PKI, Endpoint protection and finally landing recently on the Pen Testing team. Doug has a passion for identifying vulnerabilities and partnering with control solution teams to protect State Farm data and fulfill our promise to customers. He strives to help others with offensive security skills by providing training, guidance, and kill chain demonstrations.

SpeakerBio: Rob Ditmer

Rob has been on the State Farm PenTesting Team for 2 years. Prior to his time at State Farm, he has worked with various other companies as a penetration testing consultant – enabling him to experience a wide range of technologies and their differing implementations. Rob enjoys the challenge of developing tools and infrastructure to better the skills and abilities of the PenTesting team, ultimately to better the protections around State Farm data.

Description:

Organizations can have thousands of lines of code that are stored in Lambda on AWS. This application was built to help reduce the amount of time it takes to review that code. On our last Pen Test, we had so much Lambda code to review it was impossible to parse through all of it in the short amount of time assigned to our test. This lack of time created a necessity to automate the review of that lambda code for secrets. Lambda Looter will take a list of profiles and scan through them and download the code you have access to and then process that code for secrets, outputting any potential secrets to a loot directory. Even though this tool can generate a number of false positives it makes looking for secrets much faster than scanning the code manually.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Lanteryn: Blue Energy

When: Saturday, Aug 12, 14:50 - 15:30 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

SpeakerBio:Del de Zela

Del de Zela is a STEM-oriented artist that seeks to redefine the term ‘biotech’; they invent devices powered by microbiology meant for household and personal uses. Del de Zela uses an array of molecular techniques to program microbes and Maya to design microarchitectures that house them.

Description:

Our goal is to develop household or personal technologies that contain, cultivate, and regulate bioengineered microecosystems. Our self-sustaining systems are designed to offer a host of functions that solve everyday problems for people. Our debut device, a biological candle called ‘Lanteryn’, will start with the core functions of light production, fragrance generation, and insect-control. Future directions would include wearable biotechnologies, such as a “Bio-Watch” that can convey time via light color, produce odorants compatible with the user’s body scent, and generate antimicrobial substances for sanitation. Many of these functionalities are indeed innate capabilities of our chosen micro-organism. Genetic editing technologies will be employed to modify them and ensure their safety while optimizing their desirable properties. Previous attempts to utilize bioluminescent species either (1) introduced light generating genes into organisms that did not possess the physiology compatible with the energetic demand of light generation, (2) used organisms that were exceedingly sensitive to contamination or fluctuations in environmental conditions, or (3) used organisms with specialized light organs that cultivate glowing bacteria and cannot glow otherwise. The concepts we are proposing redefine the term ‘biotechnology’. Without a preceding, successful framework by which we can base our designs on, the burden of proof rests on us. Therefore, considerable time and effort must be placed into demonstrating that our vision is realistic, effective, and safe to the public. With our technology, the future is ever-glowing.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Sunday - 10:00-10:59 PDT

Title: Last chance to pick up drives at the DDV

When: Sunday, Aug 13, 10:00 - 10:59 PDT

Where: Caesars Forum - Summit - 231 - Data Dupe Vlg - [Map](#)

Description:

This is your last chance to pickup your drives whether they're finished or not. Get here between 10:00 and 11:00 on Sunday as any drives left behind are considered donations. Please leave the 8TB ones - we need them for next year.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 20:00-20:59 PDT


Title: Lawyers Meet

When: Friday, Aug 11, 20:00 - 20:59 PDT

Where: Harrah's - Elko-Ely - Chillout Lounge - [Map](#)

Description:

If you're a lawyer (recently unfrozen or otherwise), a judge or a law student please make a note to join Jeff McNamara for a friendly get-together, drinks, and conversation.

[Return to Index](#) - Add to  - ics [Calendar](#) file

RCV - Friday - 14:25-15:10 PDT

Title: Leakonomics 101: The Last Year in Data Leaks

When: Friday, Aug 11, 14:25 - 15:10 PDT

Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio: Nick Ascoli

No BIO available

Twitter: [@@kcin418](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Learning to Hack Bluetooth Low Energy with BLE CTF (Pre-Registration Required)

When: Friday, Aug 11, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

SpeakerBio: Ryan Holeman , CISO at Strike

Ryan Holeman resides in Austin, Texas, where he works as the CISO for the peer-to-peer payment platform Strike. He is currently pursuing a Ph.D. in cyber defense from Dakota State University. He has spoken at respected venues such as Black Hat, DEF CON, Lockdown, BSides, Ruxcon, Notacon, and Shmoocon. You can keep up with his current activity, open source contributions, and general news on his blog. His spare time is mostly spent digging into various network protocols, random hacking, creating art, and shredding local skateparks.

Description:

BLE CTF is a series of Bluetooth Low Energy challenges in a capture-the-flag format. It was created to teach the fundamentals of interacting with and hacking Bluetooth Low Energy services. Each exercise, or flag, aims to interactively introduce a new concept to the user.

Over the past few years, BLE CTF has expanded to support multiple platforms and skill levels. Various books, workshops, training, and conferences have utilized it as an educational platform and CTF. As an open source, low-cost of entry, and expandable education solution, BLE CTF has helped progress Bluetooth security research.

This workshop will teach the fundamentals of interacting with and hacking Bluetooth Low Energy services. Each exercise, or flag, aims to interactively introduce a new concept to the user. For this workshop, we will undergo a series of exercises to teach beginner students new concepts and allow more seasoned users to try new tools and techniques. After completing this workshop, you should have a good solid understanding of how to interact with and hack on BLE devices in the wild.

If you have done BLE CTF in the past, this class is still valuable. For advanced users, we offer BLE CTF Infinity, a sequel to BLE CTF. The workshop will also showcase new hardware platforms and client tools for interacting with and completing the exercises.

Skill Level: Beginner to Intermediate

Prerequisites for students:

- To prepare for the workshop, please follow the setup documentation located at https://github.com/hackgnar/ble_ctf/blob/master/docs/workshop_setup.md

Materials or Equipment students will need to bring to participate: - Preferably a Linux box with a Bluetooth controller or a Bluetooth USB dongle. An OSX or Windows machine with a Linux VM and USB passthrough works as well but should be setup and tested before the workshop.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Legend of Zelda: Use After Free (TASBot glitches the future into OoT)

When: Friday, Aug 11, 17:00 - 17:45 PDT

Where: Harrah's - Nevada Ballroom - Lake Tahoe & Reno - War Stories - On the Record - [Map](#)

SpeakerBio: Allan "dwangoAC" Cecil , Founder and BDFL at TASBot

Allan Cecil (dwangoAC) is the founder and BDFL of the TASBot online community. He is part of the senior staff for TASVideos.org, a website devoted to using emulators to find glitches and techniques to play video games perfectly. He is a published journal author, patent holder, and presenter with talks at DEF CON, GeekPwn, Thotcon, May Contain Hackers, and other hacker conferences. He uses his combined hacking interests for good at charity events like Games Done Quick to entertain viewers with never-before-seen glitches in games, with events he's led raising more than \$1.3m for various charities. Twitter: [@MrTASBot](#)

Description:

How can a Use After Free exploit in Ocarina of Time lead to a cute robot taking over an entire N64 to put the future (and the Triforce) in the game using only button presses? This talk dives into the technical details of how a Use After Free exploit, Arbitrary Code Execution, and multiple bootstrap stages allowed TASBot to take full control of an original, unmodified cart and console in front of a live audience during SGDQ 2022 with the help of Sauraeen and Savestate, helping raise more than \$228k for charity. This talk uses engaging explainer graphics courtesy of RGME to dig into how a Use After Free vulnerability can be exploited as well as a live demo showing the significant social impact of the exploit Here Together, in the past year and into the future.

REFERENCES

Project Info

[FAQs](<https://gettriforce.link/faq>)

[Credits](<https://gettriforce.link/credits>) [Retro Game Mechanics Explained explainer video, contents used with permission from IsoFrieze](<https://www.youtube.com/watch?v=qBK1sq1BQ2Q>)

Source code

[Triforce% Source code release](<https://github.com/triforce-percent/triforce-percent>)

Articles posted about Triforce%

[Ars

Technica](<https://arstechnica.com/gaming/2022/07/how-zelda-fans-changed-the-ending-to-ocarina-of-time-on-a-vanilla-n64/>)

[Forever Classic

Games](<https://foreverclassicgames.com/news/2022/7/tasbot-summer-games-done-quick-sgdq2022-zelda-link-triforce>) [Zelda

Dungeon](<https://www.zeldadungeon.net/ocarina-of-time-speedrunners-obtain-the-triforce-in-wild-beta-showcase/>) [Zelda

Universe](<https://zeldauniverse.net/2022/07/05/games-done-quick-features-astonishing-ocarina-of-time-beta-demonstration/>)

[PC Gamer](<https://www.pcgamer.com/this-zelda-speedrun-built-on-urban-legends-is-an-all-time-gaming-moment/>)

[NintendoLife](<https://www.nintendolife.com/news/2022/07/watch-this-insane-triforcepercent-speedrun-turns-zelda-ocarina-of-time>)

[GoNintendo](<https://gonintendo.com/contents/5979-speedrunning-trick-turns-zelda-ocarina-of-time-into-breath-of-the-wild>)

Setup info

[Savestate's notes on how to do the setup by

hand](<https://docs.google.com/document/d/1fgiILK3PdZoT1uISGMJKzsm-wZ2tP5652ayjR86QNDU>) [BizHawk savestate of

gz macro to do setup](https://drive.google.com/file/d/1tbG5TcfgXAnaxGnA_DubNcAtJR--wCeb/view?usp=sharing)

[BizHawk build needed for compatibility with that

savestate](https://drive.google.com/file/d/1K_LOyQX2MRTDOEASBbHPHltTcMB1ZDdm/view?usp=sharing)

Raw video and photo assets for Triforce%: [Clean run video (for taking footage

from)](<https://www.youtube.com/watch?v=PZNYwtNOe9U>) [HD partial run video (for taking screenshots for

branding)](https://www.youtube.com/watch?v=NNRqK1AQ_VY) [HD screenshots folder)](https://drive.google.com/drive/folders/1uA5L-3pM1gBm_FDIDFX9zB5qrqo1Q1Cv?usp=sharing)

Partner and reactor links

[SwankyBox](https://www.youtube.com/watch?v=1_RighmL04g)
[Hard4Games](<https://www.youtube.com/watch?v=f9cCtRYMKm4>)
[HMK](https://www.youtube.com/watch?v=mk1WwOu_AQQ)
([Interview](<https://www.youtube.com/watch?v=buy6EcI2NKc>))
[TetraBitGaming](<https://www.youtube.com/watch?v=gJ1hSMClhMI>)

OST Published By SiIvaGunner

[YouTube](https://www.youtube.com/watch?v=E1OYYi2Vzro&list=PLL0CQjrcN8D3qRiR5WUL51_bPo2sIzdf&index=155)
[SoundCloud](<https://soundcloud.com/sauraen/sets/triforce-percent>) [SiIvaGunner wiki page](https://siivagunner.fandom.com/wiki/Triforce%25_SGDQ_Run) [SiIvaGunner joke explanations](https://gettriforce.link/siiva_jokes)

Credits

The primary director of Triforce% was Sauraen with Savestate as the human speedrunner and dwangoAC as the Producer; over two dozen people contributed, with full credits listed at <https://gettriforce.link/credits>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Saturday - 16:30-16:59 PDT

Title: Lessons learned when building a Maritime Systems Security Laboratory Testbench

When: Saturday, Aug 12, 16:30 - 16:59 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio: Brien Croteau

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Let Night City Sleep - Governance Against a Cyberpunk Future

When: Saturday, Aug 12, 14:00 - 14:50 PDT

Where: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

Speakers: Cameron Byrd, Clayton Dixon

SpeakerBio: Cameron Byrd , Cyber Policy Analyst at Office of Cyber, Infrastructure, Risk, and Resilience Policy, U.S. Department of Homeland Security

Cameron Byrd is a Cyber Policy Analyst in the Office of Cyber, Infrastructure, Risk, and Resilience Policy at the U.S. Department of Homeland Security (DHS) Headquarters. He supports the Under Secretary for Strategy, Policy, and Plans and leads the development of cybersecurity, technology, and infrastructure policy and strategy for the Department. Cameron engages regularly with DHS components to develop unified Departmental policies and a harmonized cross-Departmental approach to issues including the implementation of Executive Orders and Congressional legislation, fulfillment of Secretary and Presidential cyber priorities, and stewardship of domestic cybersecurity initiatives across the Federal Civilian Executive Branch, Sector Risk Management Agencies, and other stakeholders. He assists in developing position papers, technical policy documents, strategies, and other policy or strategic recommendations for consideration by DHS leadership. Cameron graduated with a B.S., Information Science from the University of Maryland, College Park in 2019 and completed an M.A., Security Policy Studies from George Washington University in 2022.

SpeakerBio: Clayton Dixon , Cyber Policy Advisor to the Assistant Secretary of Cyber, Infrastructure, Risk, and Resilience at Department of Homeland Security

Clayton “CJ” Dixon is Cyber Policy Advisor to the Assistant Secretary of Cyber, Infrastructure, Risk, and Resilience at the Department of Homeland Security. His cyber policy portfolio covers emerging technologies such as Web3, quantum computing, and AI, however, he has a special passion for secure smart cities. CJ was also a Senior Advisor at New York City Cyber Command where he helped develop and implement citywide cybersecurity policies. In a previous life, CJ served in the US Army countering terrorist propaganda in West Africa as Special Operations Psychological Operations Officer.

Description:

There are currently 7.4 billion people living on Earth and more than half of those people live in a metropolitan area. Urbanization is accelerating - demand for infrastructure is expected to increase by 100% by 2060. City planners are rapidly turning to digital technology to meet the growing demands of urban life.

Enter the “smart city” – the promise that equitable, safe, and sustainable urban life can be achieved through digitization. However, digitization also comes with digital risks. Malicious cyber actors have attacked 222 local government entities and 62 public safety agencies between 2021 and 2023. Malicious actors know our communities are target-rich environments and public policy is often slow to respond.

Does this mean humanity is doomed to a Cyberpunk 2077-like future with urban life marred by constant cyber-attacks? The Department of Homeland Security and city officials believe this need not be the case, but it all starts with good governance. In this workshop, DHS will introduce a draft of the Connected Communities Governance Toolkit – a series of guides for connected community governance developed in collaboration with cities across the US. DHS will host a collaborative workshop to examine the implications of a city considering a digital transformation using the Governance Toolkit as a guide.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Sunday - 10:00-10:30 PDT

Title: Let's Talk about Voice

When: Sunday, Aug 13, 10:00 - 10:30 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio: Travis Juhr

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Wednesday - 17:00-06:59 PDT

Title: Linecon

When: Wednesday, Aug 9, 17:00 - 06:59 PDT

Where: Caesars Forum - Forum - 101-103 - Reg - [Map](#)

Description:

Linecon is your optional opportunity to stand (or sit) in line for human registration to open.

Doors open at 17:00 Wednesday. Registration will open and queue processing will begin at approximately 07:00 Thursday.

At all times, follow directions from on-duty goons -- linecon may need to be relocated into a different ballroom. The currently planned location is Caesars Forum, Rooms 101-103.

For purposes of clarity: Caesars Forum is *not* connected to Caesars Palace; it is connected to Harrah's and LINQ. Please see the published maps (in this app) for further information.

Please also review the "Human Registration Open" event, and familiarize yourself with the ****important notes**** therein.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Sunday - 09:00-12:59 PDT

Title: Linux Trainer Workshop

When: Sunday, Aug 13, 09:00 - 12:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Are you new to hacking? Want to learn Linux? We have a workshop for you! Interactive style training will teach you the basics of this operating system step by step so you can start your journey.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Saturday - 09:00-17:59 PDT

Title: Linux Trainer Workshop

When: Saturday, Aug 12, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Are you new to hacking? Want to learn Linux? We have a workshop for you! Interactive style training will teach you the basics of this operating system step by step so you can start your journey.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Friday - 09:00-17:59 PDT


Title: Linux Trainer Workshop

When: Friday, Aug 11, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Are you new to hacking? Want to learn Linux? We have a workshop for you! Interactive style training will teach you the basics of this operating system step by step so you can start your journey.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Lions and Tigers and Fancy Bears, Oh My!: A Cautionary Tale for our Cyber Future

When: Saturday, Aug 12, 17:30 - 17:50 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

Speakers:Jen Easterly,Scott Shapiro

SpeakerBio:Jen Easterly , Director at Cybersecurity and Infrastructure Security Agency (CISA)

Jen Easterly is the Director of the Cybersecurity and Infrastructure Security Agency (CISA). She was nominated by President Biden in April 2021 and unanimously confirmed by the Senate on July 12, 2021. As Director, Jen leads CISA’s efforts to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every day. She is a proud Mom, a mental health advocate, a Rubik’s Cube enthusiast, and an aspiring electric guitarist.

Before serving in her current role, Jen was the head of Firm Resilience at Morgan Stanley, responsible for ensuring preparedness and response to business-disrupting operational incidents and risks to the Firm. She also helped build and served as the first Global Head of Morgan Stanley’s Cybersecurity Fusion Center, the Firm’s center of gravity for cyber defense operations.

Jen has a long tradition of public service, to include two tours at the White House, most recently as Special Assistant to President Obama and Senior Director for Counterterrorism and earlier as Executive Assistant to National Security Advisor Condoleezza Rice. She also served as the Deputy for Counterterrorism at the National Security Agency.

A two-time recipient of the Bronze Star, Jen retired from the U.S. Army after more than twenty years of service in intelligence and cyber operations, including tours of duty in Haiti, the Balkans, Iraq, and Afghanistan. Responsible for standing up the Army’s first cyber battalion, she was also instrumental in the design and creation of United States Cyber Command.

A distinguished graduate of the United States Military Academy at West Point, Jen holds a master’s degree in Philosophy, Politics, and Economics from the University of Oxford, where she studied as a Rhodes Scholar. She is the recipient of numerous honors and awards, including the 2023 Sisterhood Award from Girls Who Code; the 2022 National Defense University Admiral Grace Hopper Award; the 2021 Cybersecurity Ventures Cybersecurity Person of the Year Award; the 2020 Bradley W. Snyder Changing the Narrative Award, and the 2018 James W. Foley Legacy Foundation American Hostage Freedom Award.

A member of the Council on Foreign Relations and a French American Foundation Young Leader, Jen is the past recipient of the Aspen Finance Leaders Fellowship, the National Security Institute Visiting Fellowship, the New America Foundation Senior International Security Fellowship, the Council on Foreign Relations International Affairs Fellowship, and the Director, National Security Agency Fellowship.


Twitter: [@@CISAJen](#)

SpeakerBio:Scott Shapiro , Charles F. Southmayd Professor of Law and Professor of Philosophy at Yale Law School
Scott Shapiro is the Charles F. Southmayd Professor of Law and Professor of Philosophy at Yale Law School. His areas of interest include jurisprudence, international law, constitutional law, criminal law and cybersecurity. He is the author of *Legality* (2011), *The Internationalists* (2017) (with Oona Hathaway) and editor of *The Oxford Handbook of Jurisprudence and Philosophy of Law* (2002) (with Jules Coleman). He earned B.A. and Ph.D. degrees in philosophy from Columbia University and a J.D. from Yale Law School. Shapiro is an editor of *Legal Theory* and the *Stanford Encyclopedia of Philosophy*. He is also the founding director of the Yale CyberSecurity Lab, which provides cutting-edge cybersecurity and information technology teaching facilities. His new book, *Fancy Bear Goes Phishing*, details the history and technology of Internet hacking (May 2023).

Description:

Fancy Bear, Dynamic Panda and Charming Kitten – we live in a time where we are constantly under attack without even knowing it. CISA Director Jen Easterly and Yale Law School Professor Scott Shapiro, author of “Fancy Bear Goes Phishing:

The Dark History of the Information Age In Five Extraordinary Hacks” discuss how best to understand the challenge of information security; what we can learn from looking back; and how the decisions we make today to prioritize security by design will shape our future.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Living Next Door to Russia

When: Friday, Aug 11, 13:00 - 13:45 PDT

Where: Harrah's - Nevada Ballroom - Lake Tahoe & Reno - War Stories - On the Record - [Map](#)

SpeakerBio: Mikko Hypponen , Researcher at WithSecure

Mikko Hypponen is a malware researcher and a best-selling author. He has written for the New York Times, Wired and Scientific American. Mikko has spoken 8 times at Black Hat, and he has 3 TED Talks. Mikko works as the Chief Research Officer for WithSecure and sits in the advisory boards of EUROPOL and Verge Motorcycles.

Twitter: [@mikko](#)

Description:

Russia is the world's largest country. I've lived all my life in Finland, about a hundred miles from the Russian border. Finland has learned to live next to a very large and very unpredictable neighbor. Both my grandfathers fought Russia in the second world war. Today, Finland ranks as one of the least corrupted countries in the world, while Russia ranks as one of the most corrupted countries. How is that even possible?

As Russia has grown more aggressive over the last decade and as it violently attacked Ukraine, attitudes about neutrality changed quickly in my home country. When Finland joined NATO in April 2023, NATO more than doubled its land border with Russia – which is probably not what Putin had in mind.

This talk will summarize the developments of the Russian cyber programs and about Russian patriotic hacker groups that got us into where we are today and makes educated guesses about where Russia will be headed next.

REFERENCES

"If It's Smart, It's Vulnerable" (2022) -- Mikko Hypponen, foreword by Jeff Moss

"Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers" (2019) – Andy Greenberg

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Living off the Land with Connectwise: How I Built An Attack Platform & Botnet in 23 lines of Python!

When: Friday, Aug 11, 14:00 - 14:45 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

SpeakerBio: Ken Pyle

Ken Pyle is a partner of CYBIR, specializing in exploit development, penetration testing, reverse engineering, and enterprise risk management. As a highly rated and popular lecturer he's presented groundbreaking research at major industry events .

Twitter: [@syngularity1](#)

Description:

Ken Pyle is a partner of CYBIR, specializing in exploit development, penetration testing, reverse engineering, and enterprise risk management. As a highly rated and popular lecturer he's presented groundbreaking research at major industry events such as DEFCON, ShmooCon, Secureworld, HTCIA International, and others. He's also discovered and published numerous critical software vulnerabilities in products from a wide range of companies that includes Cisco, Dell, Netgear, Sonicwall, HP, Datto, Kaseya, and ManageEngine, earning him multiple Hall of Fame acknowledgements for his work. Ken has been publishing DNS work and vulnerability research privately for a number of years. He began showing some of his work in the web application, DNS and IPv4 space at different cybersecurity conferences, with a focus on fixing sets of problems that had been deemed estoteric or limited.

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Saturday - 12:30-13:25 PDT

Title: LLM Legal Risk Management, and Use Case Development Strategies to Minimize Risk

When: Saturday, Aug 12, 12:30 - 13:25 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

Speakers: Nick Maietta, Robert Hudock

SpeakerBio: Nick Maietta

No BIO available

SpeakerBio: Robert Hudock

No BIO available

Description:

The California Privacy Rights Act (CPRA), the Colorado Privacy Act (CPA), the Virginia Consumer Data Protection Act (VCDPA), and the Connecticut Data Privacy Act (CTDPA) empower consumers with the option to withdraw from the processing of their personal data for profiling objectives, establishing regulations that influence automated decision-making. As organizations, including legal firms, are adopting large language models (LLMs) more frequently for various purposes, addressing issues related to privacy and security becomes critical. This talk will explore tactics and best practices implemented by King & Spalding to mitigate risks connected with LLMs. The conversation will particularly emphasize de-identification tools, terms of service, and the potential risk of client confidential data breaches. Attendees will be updated about recent privacy and security regulations, along with methodologies to ensure regulatory adherence and uphold trust.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: LLMs at the Forefront: Pioneering the Future of Fuzz Testing in a Rapidly Changing World

When: Sunday, Aug 13, 12:00 - 12:45 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

Speaker Bio: X , Hacker

X is a seasoned security researcher and programming language enthusiast with an impressive track record in research, vulnerability discovery, and fuzz testing. From the moment he laid hands on a Blueberry-colored Apple iBook G3 provided by his elementary school, X developed a slight obsession with technology.

He is a urban cycling enthusiast that needs to wear his helmet more often, a techno and bass aficionado, and tree wizard.

Before finding vulnerabilities for a living he developed scientific computing software. See his Clojure-based Sequoia database fuzzer for an ideal representation of X's skill set and interests.

Description:

Large Language Models are already revolutionizing the software development landscape. As hackers we can only do what we've always done, embrace the machine and use it to do our bidding.

There are many valid criticisms of GPT models for writing code like the tendency to hallucinate functions, not being able to reason about architecture, training done on amateur code, limited context due to token length, and more. None of which are particularly important when writing fuzz tests. This presentation will delve into the integration of LLMs into fuzz testing, providing attendees with the insights and tools necessary to transform and automate their security assessment strategies.

The presentation will kick off with an introduction to LLMs; how they work, the potential use cases and challenges for hackers, prompt writing tips, and the deficiencies of current models. We will then provide a high level overview explaining the purpose, goals, and obstacles of fuzzing, why this research was undertaken, and why we chose to start with 'memory safe' Python. We will then explore efficient usage of LLMs for coding, and the primary benefits LLMs offer for security work, paving the way for a comprehensive understanding of how LLMs can automate tasks traditionally performed by humans in fuzz testing engagements.

We will then introduce FuzzForest, an open source tool that harnesses the power of LLMs to automatically write, fix, and triage fuzz tests on Python code. A thorough discussion on the workings of FuzzForest will follow, with a focus on the challenges faced during development and our solutions. The highlight of the talk will showcase the results of running the tool on the 20 most popular open-source Python libraries which resulted in identifying dozens of bugs.

We will end the talk with an analysis of efficacy and question if we'll all be replaced with a SecurityGPT model soon.

To maximize the benefits of this talk, attendees should possess a fundamental understanding of fuzz testing, programming languages, and basic AI concepts. However, a high-level refresher will be provided to ensure a smooth experience for all participants.

REFERENCES

My original blog post that sparked the idea: <https://infiniteforest.org/LLMs+to+Write+Fuzzers>

Blogs

<https://comby.dev/blog/2022/04/11/comby-decomposer-compiler-fuzzing>

<https://martinfowler.com/articles/2023-chatgpt-xu-hao.html>

Research Papers:

<https://arxiv.org/abs/2212.14834>

<https://embed.cs.utah.edu/csmith/>


<https://www.usenix.org/system/files/sec23fall-prepub-446-fu.pdf>

Tools

<https://github.com/google/atheris> https://github.com/mpaepper/llm_agents

Prompt Course:

<https://www.deeplearning.ai/short-courses/chatgpt-prompt-engineering-for-developers/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: LLMs: Loose Lips Multipliers

When: Friday, Aug 11, 11:30 - 11:55 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

Speakers: Kyle Easterly, Mitch Kitter

SpeakerBio: Kyle Easterly


No BIO available

SpeakerBio: Mitch Kitter

No BIO available

Description:

In this talk, we explore the potential risk posed by usage of Large Language Models (LLMs) in a business environment, asking the question: Are LLMs "Loose Lips Multipliers?" Using the hypothetical case of Purple Aerospace Manufacturing Corporation, we investigate whether an LLM fine-tuned on user interactions can infer sensitive business strategies. After creating a synthetic dataset emulating corporate documents, we put our model to the test, exploring different information extraction techniques and discussing the implications of our findings. We propose future work and invite dialogue on mitigations and the best practices for using LLMs in business contexts.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Friday - 12:00-12:30 PDT

Title: Lock Bypass 101


When: Friday, Aug 11, 12:00 - 12:30 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

SpeakerBio: Karen

As a founding member of the Physical Security Village, Karen has always been eager to spread awareness of physical security vulnerabilities. Karen works with GGR Security as a Security Risk Assessor.

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Saturday - 14:00-14:30 PDT

Title: Lock Bypass 101

When: Saturday, Aug 12, 14:00 - 14:30 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

SpeakerBio: Terry

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Friday - 12:30-12:59 PDT

Title: Lock Bypass 102


When: Friday, Aug 11, 12:30 - 12:59 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

SpeakerBio: Karen

As a founding member of the Physical Security Village, Karen has always been eager to spread awareness of physical security vulnerabilities. Karen works with GGR Security as a Security Risk Assessor.

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Saturday - 14:30-14:59 PDT

Title: Lock Bypass 102


When: Saturday, Aug 12, 14:30 - 14:59 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

SpeakerBio:Ege

Ege is a security researcher specialising in access control systems and electronics. She is currently pursuing a degree in Electrical Engineering and work part-time for GGR Security as a Security Risk Assessor.

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Saturday - 10:00-17:59 PDT

Title: Lockpick Village Activities

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

Description:

Want to tinker with locks and tools the likes of which you've only seen in movies featuring secret agents, daring heists, or covert entry teams?

Then come on by the Lockpick Village, run by The Open Organization Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.

The Lockpick Village is a physical security demonstration and participation area. Visitors can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice on locks of various levels of difficulty to try it themselves.

Experts will be on hand to demonstrate and plenty of trial locks, pick tools, and other devices will be available for you to handle. By exploring the faults and flaws in many popular lock designs, you can not only learn about the fun hobby of sport-picking, but also gain a much stronger knowledge about the best methods and practices for protecting your own property.

--

A popular spot for new lock pickers! Highly recommended you stop by. The Lockpick Village is always kid friendly and welcomes folks of all ages. We do require that the parents stay with the kids.

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Friday - 10:00-17:59 PDT

Title: Lockpick Village Activities

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

Description:

Want to tinker with locks and tools the likes of which you've only seen in movies featuring secret agents, daring heists, or covert entry teams?

Then come on by the Lockpick Village, run by The Open Organization Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.

The Lockpick Village is a physical security demonstration and participation area. Visitors can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice on locks of various levels of difficulty to try it themselves.

Experts will be on hand to demonstrate and plenty of trial locks, pick tools, and other devices will be available for you to handle. By exploring the faults and flaws in many popular lock designs, you can not only learn about the fun hobby of sport-picking, but also gain a much stronger knowledge about the best methods and practices for protecting your own property.

--

A popular spot for new lock pickers! Highly recommended you stop by. The Lockpick Village is always kid friendly and welcomes folks of all ages. We do require that the parents stay with the kids.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Lockpick Village Activities

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

Description:

Want to tinker with locks and tools the likes of which you've only seen in movies featuring secret agents, daring heists, or covert entry teams?

Then come on by the Lockpick Village, run by The Open Organization Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.

The Lockpick Village is a physical security demonstration and participation area. Visitors can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice on locks of various levels of difficulty to try it themselves.

Experts will be on hand to demonstrate and plenty of trial locks, pick tools, and other devices will be available for you to handle. By exploring the faults and flaws in many popular lock designs, you can not only learn about the fun hobby of sport-picking, but also gain a much stronger knowledge about the best methods and practices for protecting your own property.

--

A popular spot for new lock pickers! Highly recommended you stop by. The Lockpick Village is always kid friendly and welcomes folks of all ages. We do require that the parents stay with the kids.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Friday - 14:00-16:59 PDT

Title: Lonely Hackers Club - Badgelife & Sticker Swap

When: Friday, Aug 11, 14:00 - 16:59 PDT

Where: Harrah's - Laughlin - Lonely Hackers Club - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file


DC - Saturday - 14:00-16:59 PDT

Title: Lonely Hackers Club - Badgeline & Sticker Swap

When: Saturday, Aug 12, 14:00 - 16:59 PDT

Where: Harrah's - Laughlin - Lonely Hackers Club - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file


DC - Saturday - 17:00-17:59 PDT

Title: Lonely Hackers Club - Name That Noob

When: Saturday, Aug 12, 17:00 - 17:59 PDT

Where: Harrah's - Laughlin - Lonely Hackers Club - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file


DC - Friday - 17:00-17:59 PDT

Title: Lonely Hackers Club - Name That Noob

When: Friday, Aug 11, 17:00 - 17:59 PDT

Where: Harrah's - Laughlin - Lonely Hackers Club - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file


DC - Friday - 12:00-13:59 PDT

Title: Lonely Hackers Club - Resume Reviews & Career Advice

When: Friday, Aug 11, 12:00 - 13:59 PDT

Where: Harrah's - Laughlin - Lonely Hackers Club - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Saturday - 12:00-13:59 PDT

Title: Lonely Hackers Club - Resume Reviews & Career Advice

When: Saturday, Aug 12, 12:00 - 13:59 PDT

Where: Harrah's - Laughlin - Lonely Hackers Club - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 12:00-17:59 PDT

Title: Lonely Hackers Club Meetup

When: Friday, Aug 11, 12:00 - 17:59 PDT

Where: Harrah's - Laughlin - Lonely Hackers Club - [Map](#)

Description:

The LHC, established on Telegram years ago, serves as a warm and inclusive hub for newcomers heading to DefCon for the first time. With over 600 members worldwide, our community has expanded significantly. This year, we're thrilled to provide a space that fosters connections, sharing, and giving back to the DefCon community. Whether you need a resume review, career coaching, or want to participate in sticker & badge trading, we have you covered. And don't miss the exciting 'Name That Noob' event, where our seasoned hackers will help you craft a one-of-a-kind hacker handle. Embrace the welcoming atmosphere and join us for an unforgettable DefCon experience!

Resume reviews & Career Advice 12pm - 2pm Badgeline / Sticker swap 2-5pm

Name That Noob 5-6pm

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 12:00-17:59 PDT

Title: Lonely Hackers Club Meetup

When: Saturday, Aug 12, 12:00 - 17:59 PDT

Where: Harrah's - Laughlin - Lonely Hackers Club - [Map](#)

Description:

The LHC, established on Telegram years ago, serves as a warm and inclusive hub for newcomers heading to DefCon for the first time. With over 600 members worldwide, our community has expanded significantly. This year, we're thrilled to provide a space that fosters connections, sharing, and giving back to the DefCon community. Whether you need a resume review, career coaching, or want to participate in sticker & badge trading, we have you covered. And don't miss the exciting 'Name That Noob' event, where our seasoned hackers will help you craft a one-of-a-kind hacker handle. Embrace the welcoming atmosphere and join us for an unforgettable DefCon experience!

Resume reviews & Career Advice 12pm - 2pm Badgeline / Sticker swap 2-5pm

Name That Noob 5-6pm

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Long Live the Empire: A C2 Workshop for Modern Red Teaming (Pre-Registration Required)

When: Friday, Aug 11, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers: Dylan "CyberStryke" Butler, Jake "Hubbl3" Krasnov, Kevin "Kent" Clark

SpeakerBio: Dylan "CyberStryke" Butler , Offensive Infrastructure Developer at BC Security

Dylan "CyberStryke" Butler is an Offensive Infrastructure Developer at BC Security. He began his career as a software engineer, developing high-performance systems for major tech companies. His passion for cybersecurity led him to specialize in offensive infrastructure development, where he now designs and builds robust frameworks to support red team operations.

SpeakerBio: Jake "Hubbl3" Krasnov , Red Team Operations Lead at BC Security

Jake "Hubbl3" Krasnov is the Red Team Operations Lead at BC Security. He has spent the first half of his career as an Astronautical Engineer overseeing rocket modifications for the Air Force. He then moved into offensive security, running operational cyber testing for fighter aircraft and operating on a red team. Hubbl3 has presented at DEF CON, where he taught courses on offensive PowerShell and has been recognized by Microsoft for his discovery of a vulnerability in AMSI. Jake has authored numerous tools, including Invoke-PrintDemon and Invoke-ZeroLogon, and is the co-author of a cybersecurity blog at <https://www.bc-security.org/blog/>.

SpeakerBio: Kevin "Kent" Clark , Red Team Instructor at BC Security

Kevin "Kent" Clark is a Security Consultant with TrustedSec and Red Team Instructor with BC Security. His previous work includes Penetration Testing and Red Team Operator, focusing on initial access and active directory exploitation. Kevin contributes to open-source tools such as PowerShell Empire and publishes custom security toolkits such as Badrats and WindowsBinaryReplacements. Kevin authors a cybersecurity blog at <https://henpeebin.com/kevin/blog>.

Description:

Command and Control (C2) is a crucial component of modern Red Teams and Advanced Persistent Threats (APTs), enabling persistent connections to target networks and facilitating the spread of control throughout the infrastructure. This comprehensive workshop will provide an in-depth understanding of C2 concepts by utilizing the open-source Empire C2 framework. Participants will gain valuable insights into the deployment, features, and real-world application of C2 in offensive security. Attendees will learn how to leverage the powerful Empire framework to create, customize, and execute advanced attack scenarios, honing their skills as red team operators.

The workshop will cover a range of topics, from setting up Empire, understanding listeners, stagers, and agents, to exploring Empire's modules and evasion techniques. Participants will engage in hands-on exercises, building their proficiency in configuring and deploying Empire servers, interacting with clients, and implementing various listeners and modules. The workshop will culminate in a mini Capture-The-Flag (CTF) challenge, where attendees will apply their newfound knowledge in a cloud-hosted environment provided by the instructors.

Skill Level: Beginner

Prerequisites for students:

- Basic computer abilities

Materials or Equipment students will need to bring to participate: - Laptop with a Kali Linux VM

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Look Ma I'm the CEO! Real-Time Video and Audio Deep-Fake!

When: Friday, Aug 11, 10:00 - 10:20 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

SpeakerBio:Gal Zror , Vulnerability Research Manager at CyberArk Labs

Gal Zror (@waveburst) acts as the vulnerability research manager in CyberArk labs. Gal has over 12 years of experience in vulnerability research and he specializes in embedded systems and protocols. Besides research, he is also an amateur boxer and a tiki culture enthusiast.

Twitter: [@waveburst](#)

Description:

Hey you, yeah you! Do you want to become a big company CEO but are too lazy to invest your life in chasing that position?

Now introducing DEFCON VIDEO-ART - DEep Fake CONversation for VIDEO and Audio in Real-Time! With DEFCON VIDEO-ART you can impersonate your favorite big-company CEO without doing the hard work! You can video call anyone in the company and tell them what to do because you look and sounds like the big boss! Reset passwords, ask for the latest confidential business reports, fire people, you name it!

Deep fake has been around for years, but only recently we have reached a point where real-time deep fake has become easy and accessible to execute. Join my talk where I show how I impersonate my company's CEO with videos and audio I found online. Then I'll share how with open-source tools and a decent GPU you can also impersonate your company's CEO!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Looking into the future, what can we learn about hacking in science-fiction?

When: Saturday, Aug 12, 13:00 - 13:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers: Nicolas Minvielle, Xavier Facéline

SpeakerBio: Nicolas Minvielle , Making Tomorrow

former brand manager for Philippe Starck, professor, researcher and futurist. Nicolas is also the head of the French Armie's Science Fiction red Team

SpeakerBio: Xavier Facéline , Seclab

Xavier Facéline — former hacker, self taught entrepreneur, founded 3 cybersecurity companies including SECLAB, cybersecurity company protecting cyberphysical system (real world !) from cyberattacks.

Xavier has 25 years of experience in cybersecurity with a focus on digital war and cyberdefense. How he gets into this? By seeing the Wargames movie at the age of 8! Today, he still watch movies and read books and comics to anticipate what is coming.

Description:

The links between science fiction and reality have been demonstrated in numerous research studies. By speculating about the possible future uses of technologies under development, science fiction shows us plausible futures. In this sense, it allows us, as a society, to popularize and debate the consequences (expected or not) of our technological developments. In addition to this not negligible social role science fiction also has an impact on our current developments. We speak here of "loop-looping", i.e. there is a feedback loop between what science fiction shows us and what we are then led to actually develop. From this point of view, our imaginations are performative, and this is perhaps the most critical issue: what I see can happen. In the case of hacking and cybersecurity, a particular phenomenon is added: the general public's knowledge of these subjects is mainly through the fictions they watch, read, or listen to. We propose to analyze a corpus of 200 fictional attacks, and 800 real attacks and to compare them to define if the imaginary ones are predictive if they inform us or on the contrary mislead us as for the reality of the current attacks.

REFERENCES:

The subject of imaginaries is a key subject of the work of the Making Tomorrow collective co-founded by Nicolas Minvielle. As such, he has been able to conduct numerous studies aimed at analyzing the impact of science fiction on a given practice.

A book has been published on the subject and is available online in pdf format: Minvielle, N. & Wathelet, O. & Lauquin, M. & Audinet, P., Design fiction for your organization, Making Tomorrow (2020),

<http://making-tomorrow.mkrs.fr/wp-content/uploads/2020/04/Making-Tomorrow-Design-Fiction-and-more-for-your-organization.pdf>

Academic references on this subject:

Brake, Mark, and Neil Hook, Different Engines: How Science Drives Fiction and Fiction Drives Science (London New York: Macmillan, 2008)

Carpenter, C. (2016). Rethinking the Political / -Science- / Fiction Nexus: Global Policy Making and the Campaign to Stop Killer Robots. *Perspectives on Politics*, 14(1), 53-69. doi:10.1017/S1537592715003229

Jones, C., & Paris, C. (2018). It's the End of the World and They Know It: How Dystopian Fiction Shapes Political Attitudes. *Perspectives on Politics*, 16(4), 969-989. doi:10.1017/S1537592718002153

Kevin L Young, Charli Carpenter, Does Science Fiction Affect Political Fact? Yes and No: A Survey Experiment on “Killer Robots”, *International Studies Quarterly*, Volume 62, Issue 3, September 2018, Pages 562–576, <https://doi.org/10.1093/isq/sqy028>

Kirby, David A., *Lab Coats in Hollywood: Science, Scientists, and Cinema* (Cambridge, Mass: MIT Press, 2011)

Maynard, Andrew D., *Films from the Future: The Technology and Morality of Sci-Fi Movies* (Coral Gables: Mango Publishing, 2018)

Seed, David, ed., *Future Wars: The Anticipations and the Fears*, *Liverpool Science Fiction Texts and Studies*, 42 (Liverpool: Liverpool Univ. Press, 2012)

Shedroff, Nathan, and Christopher Noessel, *Make It so: Interaction Design Lessons from Science Fiction*(Brooklyn, N.Y., USA: Rosenfeld Media, 2012)

Telotte, J. P., *Replications: A Robotic History of the Science Fiction Film* (Urbana: University of Illinois Press, 1995)

Westfahl, Gary, Wong Kin Yuen, and Amy Kit-size Chan, eds., *Science Fiction and the Prediction of the Future: Essays on Foresight and Fallacy*, *Critical Explorations in Science Fiction and Fantasy*, 27 (Jefferson, N.C: McFarland, 2011)

Appadurai, Arjun, ed., *The Future as Cultural Fact: Essays on the Global Condition* (London: New York : Verso Books, 2013)

Here, a video (6'30 to 17') of Xavier Facéline in 2017 inviting a panel to think about cybersecurity from a different angle ; and with science fiction references (in French) : <https://youtu.be/PIVwcu-HhQo>

Here, a video (8'55 to 29'55) of Nicolas Minvielle talking about the impact of science fiction in innovation (in French) : <https://www.youtube.com/live/oK-k3AqdXBc?feature=share>

[Return to Index](#) - Add to  - ics [Calendar](#) file

DL - Saturday - 10:00-11:55 PDT

Title: Lupo: Malware IOC Extractor

When: Saturday, Aug 12, 10:00 - 11:55 PDT

Where: Caesars Forum - Caucus Boardroom - Demo Labs - [Map](#)

SpeakerBio: Vishal Thakur

Vishal Thakur has worked in the information security industry for many years in hands-on technical roles, specializing in Incident Response with a heavy focus on Emerging Threats, Malware Analysis and Research. He has presented his research at international conferences (BlackHat, FIRST, SANS DFIR Summit) and has also run training/workshops at BlackHat and FIRST Conference. Vishal is currently working as Manager, Threat Operations Center at Huntress. In past roles, Vishal worked as a Senior Researcher at Salesforce, helping their Incident Response Centre with advanced threat analysis and developing DFIR tools and has been a part of the Incident Response team at the Commonwealth Bank of Australia.

Description:

Lupo is a dynamic analysis tool that can be used as a module with the debugger.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Machine Learning for N00bs (Pre-Registration Required)

When: Friday, Aug 11, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers:Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman,Sam Bowne

SpeakerBio:Elizabeth Biddlecome

Elizabeth Biddlecome is a consultant and instructor, delivering technical training and mentorship to students and professionals. She leverages her enthusiasm for architecture, security, and code to design and implement comprehensive information security solutions for business needs. Elizabeth enjoys wielding everything from soldering irons to scripting languages in cybersecurity competitions, hackathons, and CTFs.

SpeakerBio:Irvin Lemus

Irvin Lemus, CISSP is a Cyber Range Engineer at By Light IT Professional Services, training military personnel through international cyber security exercises. Irvin has been in the field since 2006, involved with cybersecurity competitions since 2015 as a trainer, coach, and mentor. He also has taught IT and Cybersecurity courses at Coastline and Cabrillo Colleges. He is the BACCC Cyber Competitions Regional Coordinator, Board member at Pacific Hackers and is a speaker at DEFCON. He describes himself as, "A professional troublemaker who loves hacking all the things."

SpeakerBio:Kaitlyn Handelman , Offensive Security Engineer at Amazon

Kaitlyn Handelman is an offensive security engineer at Amazon. Her focus is cybersecurity in space. In addition to traditional penetration testing, Kaitlyn works on physical devices and RF signals. In her free time, she enjoys ham radio, astronomy, and her cat, Astrocat.

SpeakerBio:Sam Bowne , Founder at Infosec Decoded, Inc

Sam Bowne has been teaching computer networking and security classes at City College San Francisco since 2000, and is the founder of Infosec Decoded, Inc. He has given talks and hands-on trainings at Black Hat USA, RSA, DEF CON, DEF CON China, HOPE, and many other conferences.

Credentials: PhD, CISSP, DEF CON Black Badge Co-Winner

Description:

Every technical product is now incorporating machine learning at an explosive rate. But most people, even those with strong technical skills, don't understand how it works, what its capabilities are, and what security risks come with it. In this workshop, we'll make machine learning models using simple Python scripts, train them, and evaluate their value. Projects include computer vision, breaking a CAPTCHA, deblurring images, regression, and classification tasks. We will perform poisoning and evasion attacks on machine learning systems, and implement deep neural rejection to block such attacks.

No experience with programming or machine learning is required, and the only software required is a Web browser. We will use TensorFlow on free Google Colab cloud systems.

All materials and challenges are freely available at samsclass.info, and will remain available after the workshop ends.

Skill Level: Beginner

Prerequisites for students:

- None

Materials or Equipment students will need to bring to participate: - A computer with a Web browser

MIV - Saturday - 13:30-14:30 PDT

Title: Main features of Russia's disinformation and propaganda ecosystem in Spanish-speaking countries

When: Saturday, Aug 12, 13:30 - 14:30 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Carlos Galán

Carlos Galán is a lawyer, Master in International Relations and Communication and professor at the Carlos III and Antonio de Nebrija Universities in Spain, in subjects related to Technology Law, Security, Hybrid Threats, Intelligence and International Relations. He has been part of the European Parliament research team for the project "Strategic communications as a key factor in countering hybrid threats". He is a member of the Jean Monnet Chair on Disinformation and Fake News of the European Union, and is currently a member of several working teams of the Department of National Security of Spain, an organization whose competences include research on aspects related to disinformation campaigns and hybrid threats.

Description:

The participatory paper presents the usual functioning of the Russian propaganda and disinformation ecosystem, as well as the possible indicators exhibited both by the Russian unofficial media and by its journalists/researchers, in those narratives especially focused on the Spanish-speaking public, showing concrete examples from several Latin American countries of this modus operandi.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Saturday - 10:00-15:30 PDT


Title: Make Your Own Use

When: Saturday, Aug 12, 10:00 - 15:30 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Description:

Have you taken your IoT toaster and created a remote activated fire-alarm tester? How about that old toy your kids (right, it was for the kids?) don't play with anymore that now fuzzes your neighbor's drone? Or what about putting that con badge to good use? The Hardware Hacking Village is hosting a "Make Your Own Use" contest. Submissions can be a solo or team based project that bend, mend, or repurpose any device and show others how it can be done.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Friday - 10:00-17:59 PDT


Title: Make Your Own Use

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Description:

Have you taken your IoT toaster and created a remote activated fire-alarm tester? How about that old toy your kids (right, it was for the kids?) don't play with anymore that now fuzzes your neighbor's drone? Or what about putting that con badge to good use? The Hardware Hacking Village is hosting a "Make Your Own Use" contest. Submissions can be a solo or team based project that bend, mend, or repurpose any device and show others how it can be done.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Making a Sick Badge

When: Friday, Aug 11, 13:20 - 14:10 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

Speakers: Caleb Davis, Nathan Smith

SpeakerBio: Caleb Davis , Protiviti


Caleb Davis leads Protiviti's IoT/Embedded security team. Caleb operates out of the Dallas/Fort Worth area and has a degree in Electrical Engineering from the University of Texas at Tyler. He is an inventor/patent holder and has a background in embedded hardware/software development. He leads a team of experts that regularly perform penetration testing across a wide variety of products including medical devices, ATMs, chemical control systems, security solutions, and other commercial products. Additionally, Caleb has a passion for integrating security into the product development life cycle and has helped several organizations in their approach to shifting left.

SpeakerBio: Nathan Smith , Protiviti

Nathan Smith is a Manager focused on IoT device security at the Dallas Protiviti office. Before coming to Protiviti, Nathan accumulated 8 years of industry experience developing and testing embedded controls and software, leading software development teams, and managing digital products. He received a B.S. in Electrical Engineering from the University of Texas at Tyler. He has performed device penetration testing, firmware reviews, and mobile application security assessments on industry devices.

Description:

This year we created our first DEF CON badge and enjoyed almost every second of it. In this presentation we hope to enable other security professionals to tinker with badge development and give them tools and tricks to help facilitate their creativity. We think that understanding the process to create a working thing helps us all better understand where we can do things more securely and how to break things better. We will review the boring and unavoidable design questions that must be addressed, the exhilarating process of creating something that works well, and scaling up from a working prototype. We will demonstrate using real steps we took this year to make our badge for the Biohacking Village.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Friday - 10:30-10:50 PDT

Title: Making The DEF CON 31 Badge

When: Friday, Aug 11, 10:30 - 10:50 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio:Mar Williams

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Malware design - abusing legacy Microsoft transports and session architecture

When: Friday, Aug 11, 16:30 - 17:15 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

SpeakerBio:R.J. "BeetleChunks" McDown , Principal Red Teamer

R.J. McDown (BeetleChunks) is a computer scientist who has made a career out of hacking into numerous fortune 500 companies through consulting red team engagements and penetration tests. R.J. is an avid Python and C/C++ developer who has created custom tools for bypassing leading EDR solutions and OS based monitoring, including a tool released at DerbyCon 7 called RedSails. Every now and then R.J. turns his focus to developing fuzzing harnesses, which has led to the discovery of critical zero-day vulnerabilities in popular applications including Microsoft Outlook (CVE-2019-1199) and ManageEngine OpManager (CVE-2020-12116).

Twitter: [@BeetleChunks](#)

Description:

The future isn't certain, nor is the continued access to our compromised endpoints. At some point, every red team operator faces the gut-wrenching event of losing command and control (C2) access. This often occurs when post exploitation activity is detected and associated to the C2 process and channel. Further link analysis may lead to the discovery of other compromised endpoints, secondary C2, and compromised credentials. Needless to say, a single mistake can cause a huge disruption in access and even lead to the detriment of the entire engagement.

This talk will present and demonstrate the methodologies and techniques built into Obligato, a covert implant tasking and communications framework, designed with the primary objectives of breaking process chaining events, disassociating network communication from the implant, providing a means for maintaining or regaining access, and evading dynamic analysis.

Technical information will be explained and demonstrated at both high and low levels, so prior knowledge is not required. However, to get the most out of the talk, attendees are encouraged to have a basic understanding of general Windows architecture, networking, and programming concepts.

REFERENCES:

[1] Pyle, Ned. "The Beginning of the End of Remote Mailslots." Tech Community, Microsoft, 8 Mar. 2023, <https://techcommunity.microsoft.com/t5/storage-at-microsoft/the-beginning-of-the-end-of-remote-mailslots/ba-p/3762048>.

[2] Corporation, Microsoft. "[MS-Mail]: Remote Mailslot Protocol." [MS-MAIL], Microsoft, 25 June 2021, [https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-MAIL/\[MS-MAIL\].pdf](https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-MAIL/[MS-MAIL].pdf).

[3] Aggarwal, Avnish. "PROTOCOL STANDARD FOR A NetBIOS SERVICE." IETF, RFC Editor, Mar. 1987, <https://datatracker.ietf.org/doc/html/rfc1001>.

[4] ATT&CK, MITRE. "Enterprise Techniques." Techniques - Enterprise , MITRE ATT&CK, MITRE ATTCK, 25 Oct. 2022, <https://attack.mitre.org/techniques/enterprise/>.

[5] Yosifovich, Author Pavel. "Parent Process vs. Creator Process." Pavel Yosifovich, 10 Jan. 2021, <https://scorpiosoftware.net/2021/01/10/parent-process-vs-creator-process/>.

[6] Schwarz, Roland. "Thread Local Storage - the C++ WAY." CodeProject, CodeProject, 28 Aug. 2004, <https://www.codeproject.com/Articles/8113/Thread-Local-Storage-The-C-Way>.

[7] The Chromium Authors. "Chromium/thread_local_storage_win.Cc at Main · Chromium/Chromium." GitHub, The Chromium Project, Jan. 2012, https://github.com/chromium/chromium/blob/main/base/threading/thread_local_storage_win.cc.

- [8] timb3r. “How to Find Hidden Threads - Threadhidefromdebugger - Antidebug Trick.” How to Find Hidden Threads - ThreadHideFromDebugger - AntiDebug Trick, Guided Hacking, 27 Dec. 2019, <https://guidedhacking.com/threads/how-to-find-hidden-threads-threadhidefromdebugger-antidebug-trick.14281/>.
- [9] Chappell, Geoff. “THREADINFOCLASS.” Threadinfoclass, Jan. 1997, <https://www.geoffchappell.com/studies/windows/km/ntoskrnl/api/ps/psquery/class.htm>.
- [10] GrantMeStrength. “GetMailslotInfo Function (Winbase.h) - win32 Apps.” Win32 Apps , Microsoft Learn, 10 Oct. 2021, <https://learn.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-getmailslotinfo>.
- [11] Alvinashcraft. “Impersonation Tokens - win32 Apps.” Win32 Apps , Microsoft Learn, 1 July 2021, <https://learn.microsoft.com/en-us/windows/win32/secauthz/impersonation-tokens>.
- [12] GrantMeStrength. “CreateProcessWithTokenW Function (Winbase.h) - win32 Apps.” Win32 Apps , Microsoft Learn, 2 Jan. 2023, <https://learn.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-createprocesswithtokenw>.
- [13] QuinnRadich. “WTSQUERYUSERTOKEN Function (WTSAPI32.H) - win32 Apps.” Win32 Apps , Microsoft Learn, 10 Dec. 2021, <https://learn.microsoft.com/en-us/windows/win32/api/wtsapi32/nf-wtsapi32-wtsqueryusertoken>.
- [14] Karl-Bridge-Microsoft. “PEB (Winternl.h) - win32 Apps.” PEB (Winternl.h) - Win32 Apps , Microsoft Learn, 31 Aug. 2022, <https://learn.microsoft.com/en-us/windows/win32/api/winternl/ns-winternl-peb>.
- [15] Yosifovich, Pavel. Windows 10 System Programming Part 1. Independently Published.
- [16] Yosifovich, Pavel. Windows 10 System Programming Part 2. Independently Published.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Malware development on secured environment - Write, adapt, overcome (Pre-Registration Required)

When: Friday, Aug 11, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

SpeakerBio: Yoann Dequeker , Red Team Operator at Wavestone

Yoann Dequeker is a red team operator at Wavestone for 4 years entitled with OSCP certification and several HTB RedTeam Prolabs. Aside from his different RedTeam operations against CAC40 companies leading him to develop several custom malware to evade EDR to ease C2 beacon deployment or phishing campaigns, he speaks at conferences such as LeHack as a Malware Development speaker and is actively sharing his knowledge on social media under the OtterHacker pseudonym.

Beside his contribution to opensource project such as the implementation of TDO secret extraction on Impacket, he spends time playing with several EDR to understand the pros and cons of the different malware development techniques in order to craft and use the payload the most adapted to the targeted environment.

Description:

This workshop will give an initiation to offensive malware development in C/C++ and how it is possible to adapt the approach depending on the security solution that must be tackled down. Different methods such as ModuleStomping, DLL Injection, Threadless Injection and Hardware Breakpoint for dehooking will be seen.

The idea is to start with a basic malware performing process injection and apply additional techniques to start evading EDR. At each step, some analysis on the malware will be performed to understand the differences at the system level and the IOC detected by the EDR.

At the end of this workshop, you will have all the knowledge needed to develop your own malware and adapt it to the targeted environment to escape from the basic pattern and spawn your beacons as if EDR didn't exist.

Skill Level: Intermediate

Prerequisites for students:

- Some basic C/C++ knowledge and an entry level skills on Windows OS.

Materials or Equipment students will need to bring to participate: - A Computer with VisualStudio Community or an equivalent compiler, WinDBG and a Windows System (Virtual machine might be better)

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Malware Hunting an Offensive Approach

When: Saturday, Aug 12, 15:00 - 15:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 4 - [Map](#)

SpeakerBio: Filipi Pires

No BIO available

Twitter: [@FilipiPires](#)

Description:

Developing offensive thinking is the highlight of this training, you'll be able to create different strategies to send some attacks and know how you can deliver that, and so on. Participants will have the experience of learning to execute several efficiency and detection tests in your lab environment, bringing the result of the defensive security analysis with an offensive mindset performed some types of the attacks that are used in cybercrime and being able to take practical actions to identify these threats. Understanding how Cyber Kill Chain works, learning Static and Dynamic Analysis of some types of files, and executing your own attacks...

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Malware Hunting an Offensive Approach

When: Sunday, Aug 13, 09:00 - 09:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 1 - [Map](#)


SpeakerBio: Filipi Pires

No BIO available

Twitter: [@FilipiPires](#)

Description:

Developing offensive thinking is the highlight of this training, you'll be able to create different strategies to send some attacks and know how you can deliver that, and so on. Participants will have the experience of learning to execute several efficiency and detection tests in your lab environment, bringing the result of the defensive security analysis with an offensive mindset performed some types of the attacks that are used in cybercrime and being able to take practical actions to identify these threats. Understanding how Cyber Kill Chain works, learning Static and Dynamic Analysis of some types of files, and executing your own attacks...

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Malware Hunting an Offensive Approach

When: Friday, Aug 11, 16:00 - 16:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 1 - [Map](#)

SpeakerBio: Filipi Pires

No BIO available

Twitter: [@FilipiPires](#)

Description:

Developing offensive thinking is the highlight of this training, you'll be able to create different strategies to send some attacks and know how you can deliver that, and so on. Participants will have the experience of learning to execute several efficiency and detection tests in your lab environment, bringing the result of the defensive security analysis with an offensive mindset performed some types of the attacks that are used in cybercrime and being able to take practical actions to identify these threats. Understanding how Cyber Kill Chain works, learning Static and Dynamic Analysis of some types of files, and executing your own attacks...

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Maps of the digital lands

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Maps of the Digital Lands is an all-ages contest that challenges participants to merge their artistic talents with their technical expertise. Contestants will be provided with a diverse array of written business designs and must hand-draw a network diagram illustrating the structure and interconnectivity of each business's infrastructure. Judging will be based on accuracy, adherence to best practices, and artistic prowess. In addition, a captivating Capture the Flag scenario will be available for extra points, employing a digital tool to elevate the challenge. Participants of all skill levels are encouraged to join this immersive experience, compete for assorted prizes, and showcase their unique ability to blend artistry with network engineering excellence. Network engineering is a crucial yet frequently overlooked aspect of hacking, forming the backbone of a secure and efficient cyber ecosystem. By honing their network engineering skills, participants can elevate their abilities beyond mere script kiddie status, gaining a comprehensive understanding of system vulnerabilities and strengthening their overall hacking prowess.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Maps of the digital lands

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Maps of the Digital Lands is an all-ages contest that challenges participants to merge their artistic talents with their technical expertise. Contestants will be provided with a diverse array of written business designs and must hand-draw a network diagram illustrating the structure and interconnectivity of each business's infrastructure. Judging will be based on accuracy, adherence to best practices, and artistic prowess. In addition, a captivating Capture the Flag scenario will be available for extra points, employing a digital tool to elevate the challenge. Participants of all skill levels are encouraged to join this immersive experience, compete for assorted prizes, and showcase their unique ability to blend artistry with network engineering excellence. Network engineering is a crucial yet frequently overlooked aspect of hacking, forming the backbone of a secure and efficient cyber ecosystem. By honing their network engineering skills, participants can elevate their abilities beyond mere script kiddie status, gaining a comprehensive understanding of system vulnerabilities and strengthening their overall hacking prowess.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Maps of the digital lands

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Maps of the Digital Lands is an all-ages contest that challenges participants to merge their artistic talents with their technical expertise. Contestants will be provided with a diverse array of written business designs and must hand-draw a network diagram illustrating the structure and interconnectivity of each business's infrastructure. Judging will be based on accuracy, adherence to best practices, and artistic prowess. In addition, a captivating Capture the Flag scenario will be available for extra points, employing a digital tool to elevate the challenge. Participants of all skill levels are encouraged to join this immersive experience, compete for assorted prizes, and showcase their unique ability to blend artistry with network engineering excellence. Network engineering is a crucial yet frequently overlooked aspect of hacking, forming the backbone of a secure and efficient cyber ecosystem. By honing their network engineering skills, participants can elevate their abilities beyond mere script kiddie status, gaining a comprehensive understanding of system vulnerabilities and strengthening their overall hacking prowess.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Mass Owning of Seedboxes - A Live Hacking Exhibition

When: Saturday, Aug 12, 11:30 - 12:15 PDT

Where: Harrah's - Nevada Ballroom - Lake Tahoe & Reno - War Stories - Off the Record - [Map](#)

SpeakerBio: Anon , Hacker

The presenter has been attending DEFCON for ~20 years, and has run various villages and contests for over 10 years. A professional pentester for over 24 years, his previously released research and tools are present in MetaSploit, blog posts, blah blah blah. The hacker is a long-time member of AHA (Austin Hackers Anonymous - [takeonme.org](#)) and is well known for their "this one time on a pentest" stories.

The thing is though. We aren't going to tell you their handle/name. It's not important. You don't need it. Don't pick a talk by how famous someone is.

Description:

"No one hacks at DEFCON any more." is what I've heard. That is, until now. Seedboxes/seedhosts are used by thousands of pirates to download and distribute Movies/TV/Music via USENET and Torrents. The thing is, these systems are horribly insecure. Like, they are wide open. In this talk, I am going to open up a xterm, And a FireFox window, and hack into seedhosts. LIVE. No Demos. No Powerpoint. No introduction slides. Just port scan, attack, Own, extract credentials, download all content, obtain other users' credentials, etc. For literally thousands of accounts.

Did you know people store their Google Drive tokens on seedhosts? Did you know that your seedbox provider has no idea how to properly configure docker? Did you know that your plain-text password is sitting in multiple places on these machines, accessible to all other users? Did you know that administrators for very-large private torrent sites re-use the same password for all their accounts, and leave them on seedhosts? Let's hack.

The presenter has been attending DEFCON for ~20 years, and has run various villages and contests for over 10 years. A professional pentester for over 24 years, his previously released research and tools are present in MetaSploit, blog posts, blah blah blah. The hacker is a long-time member of AHA (Austin Hackers Anonymous - [takeonme.org](#)) and is well known for their "this one time on a pentest" stories.

The thing is though. We aren't going to tell you their handle/name. It's not important. You don't need it. Don't pick a talk by how famous someone is.

REFERENCES:

<https://censys.io/>

[https://en.wikipedia.org/wiki/Bash_\(Unix_shell\)](https://en.wikipedia.org/wiki/Bash_(Unix_shell)) <https://nmap.org/>

<https://sonarr.tv/>

<https://radarr.video/>

<https://github.com/Novik/ruTorrent>

<https://rclone.org/>

<https://nzbget.net/>

<https://sabnzbd.org/>

<https://en.wikipedia.org/wiki/Seedbox>

[Return to Index](#) - Add to  - ics [Calendar](#) file

RCV - Friday - 14:00-14:25 PDT

Title: Mastering OSINT: Advanced Techniques in the Realm of Big Data

When: Friday, Aug 11, 14:00 - 14:25 PDT

Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio: Seyfullah

No BIO available

Twitter: [@s3yfullah](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Math for Quantum

When: Sunday, Aug 13, 10:00 - 10:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

SpeakerBio:Mark Carney

No BIO available

Description:

Quantum mechanics is quite hard, mathematically speaking. But Quantum information theory needs remarkably few resources! Inspired by the work of others, Mark will present a short introductory lecture with minimal pain but mathematical gain - getting you from tense to tensors, suspicious to superposition, and enraged to entangled in no time!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Medical VR

When: Saturday, Aug 12, 12:40 - 13:50 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

Speakers:David Nathans,Ernest Liu

SpeakerBio:David Nathans , Product Security Manager at Siemens Healthcare

David Nathans currently serves as a Product Security Manager for Siemens Healthcare, where he specializes in building cybersecurity programs and security operation centers. Having previously held prominent positions in the defense, retail, managed security and healthcare industries, Nathans has a wealth of cybersecurity knowledge which he shares to help protect companies from this growing threat. His experiences and lessons learned also stem from his time building security programs at one of the largest breached retail companies in history as well as working all over the world as a Cyber-Operations Officer for the US Air Force.

SpeakerBio:Ernest Liu

No BIO available

Description:

Siemens Healthineers leans into technology to bring medical devices closer to clinicians and more accessible for those that need the best medical attention.

Through our medical device cybersecurity program and our Virtual Reality training platform we can do just that.

For this session we will briefly talk about our programs and let interested individuals navigate our Virtual world or get hands on access to a mobile X-Ray system.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Meduza: How an exiled pirate media outlet breaks through the Kremlin's propaganda firewall

When: Saturday, Aug 12, 13:30 - 14:15 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

SpeakerBio: Alex , CTO at Meduza

Alex is CTO at Meduza. He joined the team in 2019. It was a rather crazy and brave decision to give up the job in a stable global corporation and join an independent media company in the times when it was already obvious that independent journalism is not welcome in Russia any more.

Alex's main topics of expertise:

Media company digital security. Protection of both employees and infrastructure against cyber threats, government run attacks, surveillance. Circumvention tools and technologies. Practical experience of reaching the audience in state-controlled countries. Government methods and approaches against media organizations. How they discover and block "forbidden" content, legal and physical pressure, surveillance. Risk analysis and research-based forecast for the further elaboration of censorship, i.e. sovereignization, criminalization of content etc.

Description:

Meduza is an independent international Russian- and English-language publication that still reaches millions of people inside Russia. The newsroom is operating from exile for 8 years now with headquarters in Latvia. Despite being completely outlawed and banned by the Kremlin, Meduza continues to work even under such enormously tough circumstances and still delivers the truths about the war in Ukraine along with an unbiased reporting on the situation inside Russia.

But at DEF CON Meduza will not be presented as a media. The team tries to resist the total state control of the Internet in Russia and fight not only for the freedom of speech, but for the freedom of information for millions of people.

Meduza CTO will explain how one of the most free internet has become one of the most regulated and censored ones within just a couple of years. Alex will share the practical experience of resisting censorship along with his (pessimistic) forecast for the future of the Internet in Russia (a new "Iron Curtain"). He will describe how the authorities were once again able to "deceive the people" (before all that happened, there were no abrupt blockings in Russia and the habit of using VPN was not formed among internet users). This is important to not to let this scenario be repeated in whatever part of the world.

Tech Dept has always been an important part of Meduza newsroom, but in 2022 the tech guys became an even more crucial part of it. It is thanks to their work that the newsroom is able to successfully bypass blocking and retain the audience in Russia. And to protect the journalists and to repel various DDoS attacks on the infrastructure and products.

REFERENCES:

We don't have many references that will be used in the presentation. And according to our Code of Conduct in our ordinary life we try to write about the news, and not to be the newsmakers ourselves. Here are a couple links that might be helpful to understand more about our work and values.

Meduza
<https://meduza.io/>

Meduza English-language edition
<https://meduza.io/en>

The awards:
<https://frittord.no/en/news/speeches-at-the-awarding-of-the-fritt-ord-foundation-prize-2022>

<https://cpj.org/2022/03/calling-the-war-war-meduzas-galina-timchenko-bucks-russias-censorship-on-ukraine/>

<https://fgpj.eu/portfolio-items/preistraeger-2022/?portfolioCats=98>

More about us:

<https://rsf.org/en/rsf-creates-mirror-leading-russian-exile-news-site-blocked-kremlin>

<https://www.cloudflare.com/innovator-spotlights/>

<https://www.bloomberg.com/news/articles/2022-05-10/putin-s-crackdown-pushes-independent-russian-media-into-crypto?leadSource>

<https://www.washingtonpost.com/media/2022/03/17/meduza-russia-sanctions/>

<https://www.vox.com/future-perfect/22955885/donate-ukraine>

Several examples of the most important articles:

Fact checking piece with a video that proved the massacre in Bucha. Meduza's source provided us with a video that was filmed during the "entrance" to Bucha. We gave the video to two independent experts (an astronomer and a mathematician) in order to verify when the videos were shot, using chronolocation techniques. Their findings allowed us to confirm that the times in the metadata matches the actual times when the footage was recorded, and that the first video of the bodies couldn't have been filmed after March 26, 2022, which proved that the horrific civilian killings in Bucha took place before Russian troops retreated from the town

<https://meduza.io/en/feature/2022/04/09/verified-video-appears-to-show-ukrainian-troops-killing-russian-captives-here-s-what-we>

An investigation of war crimes in Bogdanovka <https://meduza.io/en/feature/2022/04/18/i-can-do-whatever-i-want-to-you>

How Russia's full-scale invasion of Ukraine split the company Yandex <https://meduza.io/en/feature/2022/05/06/toxic-assets>

An investigation on Elvira Nabiullina, the chairwoman of Russia's Central Bank

<https://meduza.io/en/feature/2022/07/07/the-banker-s-dilemma>

Meduza tells the story of the first openly transgender woman in the Russian army. She is going to be sent to war with Ukraine (and that's not the whole story)

<https://meduza.io/feature/2022/11/09/pust-luchshe-ona-tam-gde-nibud-umret>

Return to Index - Add to  - ics [Calendar](#) file

DC - Thursday - 07:00-17:59 PDT

Title: Merch (formerly swag) Area Open -- README

When: Thursday, Aug 10, 07:00 - 17:59 PDT

Where: Caesars Forum - Summit - 227-230 - Merch - [Map](#)

Description:

All merch sales are USD CASH ONLY. No cards will be accepted.

The published hours for the merch area are only an approximation: supplies are limited, and when merch is sold out, the merch area will close for the year. (We intend to update this schedule to reflect their true operating status, but this is strictly best-effort.)

Note that the closing hours here are ****when sales must have ended****. For example, if sales must end by 18:00, and we estimate that it will take 2 hours to clear the queue, doors are likely to close around 16:00. Because of this dynamic nature, we can't predict the length of the line or when doors will be closed.

****PLEASE NOTE****

The Saturday open time was incorrectly listed as 08:00, and has been corrected to 09:00. ****PLEASE**** check stock status in HackerTracker.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Merch (formerly swag) Area Open -- README

When: Friday, Aug 11, 08:00 - 17:59 PDT

Where: Caesars Forum - Summit - 227-230 - Merch - [Map](#)

Description:

All merch sales are USD CASH ONLY. No cards will be accepted.

The published hours for the merch area are only an approximation: supplies are limited, and when merch is sold out, the merch area will close for the year. (We intend to update this schedule to reflect their true operating status, but this is strictly best-effort.)

Note that the closing hours here are ****when sales must have ended****. For example, if sales must end by 18:00, and we estimate that it will take 2 hours to clear the queue, doors are likely to close around 16:00. Because of this dynamic nature, we can't predict the length of the line or when doors will be closed.

****PLEASE NOTE****

The Saturday open time was incorrectly listed as 08:00, and has been corrected to 09:00. ****PLEASE**** check stock status in HackerTracker.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Saturday - 09:00-11:59 PDT

Title: Merch (formerly swag) Area Open -- README

When: Saturday, Aug 12, 09:00 - 11:59 PDT

Where: Caesars Forum - Summit - 227-230 - Merch - [Map](#)

Description:

All merch sales are USD CASH ONLY. No cards will be accepted.

The published hours for the merch area are only an approximation: supplies are limited, and when merch is sold out, the merch area will close for the year. (We intend to update this schedule to reflect their true operating status, but this is strictly best-effort.)

Note that the closing hours here are ****when sales must have ended****. For example, if sales must end by 18:00, and we estimate that it will take 2 hours to clear the queue, doors are likely to close around 16:00. Because of this dynamic nature, we can't predict the length of the line or when doors will be closed.

****PLEASE NOTE****

The Saturday open time was incorrectly listed as 08:00, and has been corrected to 09:00. ****PLEASE**** check stock status in HackerTracker.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: MetaHub Demo: Automating Ownership, Context, and Impact Assessment in Security Findings

When: Friday, Aug 11, 14:05 - 14:35 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

Description:

Security findings from automated sources such as network, software, or compliance scanners often overwhelm security teams with excessive generic, context-less information. Determining ownership and impact takes time and can cause critical vulnerabilities to go unnoticed, unnecessary noise, or friction between security teams and other stakeholders. My proposed demo introduces MetaHub, a tool designed to mitigate these issues by automating the three crucial stages of security finding assessment: owner determination, contextualization, and impact definition. Leveraging the power of metadata through MetaChecks, MetaTags, MetaTrails, and MetaAccount, MetaHub provides a detailed, context-aware assessment of each finding.


By integrating MetaHub, teams can significantly reduce false positives, streamline the detection and resolution of security findings, and strategically tailor their scanner selection to minimize unnecessary noise. This ability to focus on meaningful, high-impact issues represents a significant step forward in security engineering and will be the primary focus of the demo.

MetaHub relies on the ASFF format for ingesting security findings which can be consumed from AWS Security Hub or any ASFF-supported scanner, like Prowler or ElectricEye. It can also help to generate reports and dashboards.

MetaHub is designed for use as a CLI tool or within automated workflows, such as AWS Security Hub custom actions, AWS Lambda functions, or AWS Step Functions.

Context, ownership, and impact definitions are not common topics that open source tools are addressing; this one is the approach I found for this problem that aims to be agnostic to the source scanner itself. For me, it would be more than valuable to connect with other people to understand other approaches and get feedback on this one.

Github: <https://github.com/gabrielsoltz/metahub>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Metawar

When: Saturday, Aug 12, 12:30 - 13:30 PDT

Where: Harrah's - Nevada Ballroom - Lake Tahoe & Reno - War Stories - Off the Record - [Map](#)

SpeakerBio: Winn

Winn has lived Cybersecurity since 1983. He coined the term "Electronic Pearl Harbor" while testifying before Congress in 1991. His seminal book, "Information Warfare" showed the world how and why massive identity theft, cyber-espionage, nation-state hacking and cyber-terrorism would be an integral part of today.

Currently, he is exploring "Metawar," a term he coined to describe the art and science of reality distortion and addiction in the metaverse. Increasingly impressive immersive technologies, active metacontent orchestration, and powerful feedback systems (OODA loops) will amplify disinformation through believable simulations and the powerful addictive effects of reward-based virtual existences. At some distant date, the metapoint will be reached, where persistent immersive simulations will be indistinguishable from our default 'reality'. Just with current and short-term technological capabilities, the security, privacy, ethics, and global policy implications are staggering. (The book "Metawar" will be available 2023)

Description:

The Metaverse is the Most Powerful, Addictive Reality Distortion Machine Ever Conceived... and it Can Predict the Future.

The metaverse is an evolving storytelling environment in which humans have congregated for millennia to experience alternate, immersive, and simulated realities, with or without technology. Storytelling is designed to influence mental and physical perceptions suiting the purposes of the content creators.


Metawar is the art of applying science to create and defend against the influence of alternate realities in the metaverse.

My research into Metawar initially focused on metaversal technologies. Unexpectedly, it morphed into an intensely personal experience, triggering my own Metanoia, which had a profound impact on the entire Metawar Thesis.

Immersive Experience => Reality Distortion => Disinformation =>> Manipulation => Reward => Addiction => Compliance

My Metanoia has been integral to the evolution of thinking about the synthesis of carbon-silicon technologies and the Venn of objective-subjective reality perception. Please, bring your thoughts so we can talk about what being human even means as increasingly immersive metaverse experiences bend our sense of reality.

WARNING: There may be some maths.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MIV - Sunday - 11:30-11:59 PDT

Title: Misinfo Village Closing / Panel / Summary / Feedback

When: Sunday, Aug 13, 11:30 - 11:59 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Misinformation Village Staff

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MIV - Saturday - 15:00-15:30 PDT

Title: Misinformation As A Service: Social Engineering techniques applied in service contexts.


When: Saturday, Aug 12, 15:00 - 15:30 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Daniel Isler

No BIO available

Description:

[Return to Index](#) - Add to  - ics [Calendar](#) file

MIV - Saturday - 17:30-17:59 PDT

Title: Misinformation Village Q and A

When: Saturday, Aug 12, 17:30 - 17:59 PDT


Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Misinformation Village Staff

No BIO available

Description:

A chance to ask us questions about the misinformation village

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: MitmWs: A new way to pentest websocket applications

When: Saturday, Aug 12, 14:15 - 14:59 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

SpeakerBio:Jon F

Been hacking professionally (and ethically) for over 10 years. Primarily pentest web applications & the odd desktop application.

Description:

MitmWs is a pentesting HTTP proxy created specifically for testing applications that use websockets. Websocket applications present unique challenges to pentesters. The the asynchronous nature of the conversation, the often times statefulness of the conversation and the sometimes tricky timing requirements of specific messages are all challenges that MitmWs helps mitigate.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Model Based Systems Engineering for Security Engineers

When: Saturday, Aug 12, 00:00 - 00:59 PDT

Where: Virtual

SpeakerBio:John Volock

No BIO available

Description:

This talk is being pre-recorded and will be released on YouTube. Once it is available, a link to it will appear here.

Update 2023-08-11 06:30: Biohacking Village indicates that the pre-recorded talks have not yet been received. Once received, these talks will be posted to the [Biohacking Village YouTube Channel](<https://www.youtube.com/@BiohackingVillage/about>). Please note that this may be as late as a week or two after DC31.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Modernizing AX.25 packet radio with Modern Packet Message Manager

When: Saturday, Aug 12, 15:00 - 15:30 PDT

Where: Flamingo - Virginia City - Ham Radio Village - [Map](#)

SpeakerBio:Jeremy Banker

A lifelong learner and broad technology enthusiast, Jeremy Banker holds a Masters degree in Information Security and is a founding member of the Security Product Engineering, Automation and Research (SPEAR) team at VMware. He has designed, built and implemented solutions to ensure that VMware's software supply chain remains secure. When not looking for new ways to keep software safe, he can usually be found tinkering with all manner of gadgets, working to bring amateur radio software into the modern era, or enjoying the peace of nature in his native Colorado.

Description:

If you've ever looked into the current standard software for many different packet radio operations, you've probably experienced the 90s interfaces, weird and wacky undocumented configuration, and general lack of consideration for open source. Modern Packet Message Manager hopes to put an end to that situation by either creating or collecting a full open-source stack of software to facilitate digital packet messaging, with a focus on modularity, open source, and modern interfaces.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Monroeville Live: An IR Tabletop for the Rest of Us

When: Friday, Aug 11, 16:00 - 17:59 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Main Stage - [Map](#)

Speakers: Dave Collins, Gwyddia, Litmoose, Matt Mahler, Nathan Case, Nina Alli, Shea Nangle

SpeakerBio: Dave Collins

I work in public transportation IT doing cybersecurity and network infrastructure work. In the past, I have worked as a Linux sysadmin, Windows sysadmin, network engineer, and security engineer. I will happily geek out about anything computer related.

SpeakerBio: Gwyddia

A Principal Consultant at CrowdStrike and frequent security conference speaker, Kelly is passionate about bringing the best of tabletop roleplaying games into high-level security tabletop simulations. She has designed and facilitated single-scenario and multi-table games for companies ranging from VC-stage startups to multi-billion dollar megacorps, and for audiences including both the information security and indie tabletop RPG game spaces.

Moom, trained therapist, recovering attorney, gnome.

"Talk about hard things. Do hard things. Throw soft things." -- ShmooCon 2022(+1)

SpeakerBio: Litmoose

Cats and violins.

SpeakerBio: Matt Mahler

No BIO available

SpeakerBio: Nathan Case

A passion for Incident Response, and operational security in all forms. Pushing the bounds of threat detection and response. Finding new thoughts and bringing them to the fields of security and technology.

SpeakerBio: Nina Alli , Regulatory Cybersecurity, Senior Strategist at Thermo Fisher

Nina Alli is the Executive Director of the Biohacking Village, Sr Cybersecurity Regulatory Strategist at ThermoFisher, George Washington University Law School student, policy white paper writer, EMR and associated devices technologist, coffee snob, and super proud #Latina from #NYC.

SpeakerBio: Shea Nangle


Shea Nangle does not now, nor has he ever, worked for a three letter agency. He has, however, been accused on several occasions of being a Fed, and there was a multiyear period when his wife really thought he worked for a front company. To the best of his knowledge, only one of his previous employers has ever been investigated by the US government as a potential front for foreign intelligence. GLOMAR.

In his spare time, he enjoys long walks on the beach and reruns of Magnum, P.I.

Description:

This is an interactive incident response tabletop workshop in a “game show”-type format. Attendees will work through a crisis

response scenario designed exclusively for a live studio audience and will have the opportunity to describe how they might handle progressive stages of an emerging incident. Their responses will be evaluated by our “celebrity” judges who will balance a light tone with meaningful feedback that participants can use both to work through the problem sets presented and to learn to guide their teams through a real IR. Wrong answers allowed and encouraged; all experience and tech levels welcome.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Most Meta - Live Meta Quest2 Hack


When: Sunday, Aug 13, 11:00 - 11:59 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

SpeakerBio:David "Icer" Maynor

David "Icer" Maynor, Secret Keeper at ThreatHunter.ai, has over 20 years of experience in information security with deep technical expertise in threat intelligence, reverse engineering, exploit development, and offensive security testing. Results-driven research, analysis, and solutions leveraging partnerships and cross-disciplinary teams, to strengthen customer and business security posture and capabilities. Served as founder, executive, and advisor within the information security startup space. Author of and contributor to several popular open-source tools, presenter and instructor, and subject matter expert contributor for print, television, and online media.

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Friday - 20:00-23:59 PDT

Title: Movie Night

When: Friday, Aug 11, 20:00 - 23:59 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

Description:

Friday

- ◇ Moon
- ◇ Dark Star

Saturday:

- 2001: A Space Odyssey
- Forbidden Plant

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Moving Target Defense for Space Systems

When: Friday, Aug 11, 13:30 - 13:55 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio:Chris Jenkins

No BIO available

Description:

We devised a MTD algorithm and tested its application to a MIL-STD-1553 network. We demonstrated and analyzed four aspects of the MTD algorithm: 1) characterized the performance and unpredictability of the core algorithm, 2) demonstrated experiments on actual commercial hardware, 3) conducted an exfiltration experiment where the reduction in adversarial knowledge was 97%, and 4) employed the LSTM machine learning model to see if it could defeat the algorithm.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: mTLS: when certificate authentication done wrong

When: Friday, Aug 11, 11:00 - 11:20 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

SpeakerBio: Michael Stepankin , Security Researcher at GitHub

Michael 'artsploit' Stepankin is a researcher at GitHub Security Lab. He joined the team to put his offensive security mindset to the test, uncovering complex vulnerabilities in open source web applications. He specializes in the Java Enterprise stack, covering a wide range of security topics from insecure deserialization and XXEs, to logical bugs in OAuth systems. He's published a number of works throughout his employment as a researcher, including new ways to exploit JNDI injections, attacks on Apache Solr, and finding hidden Remote Code Executions in the Spring framework.

Twitter: [@artsploit](#)

Description:

Although x509 certificates have been here for a while, they have become more popular for client authentication in zero-trust networks in recent years. Mutual TLS, or authentication based on X509 certificates in general, brings advantages compared to passwords or tokens, but you get increased complexity in return.

In this talk, we'll deep dive into some novel attacks on mTLS authentication. We won't bother you with heavy crypto stuff, but instead we'll have a look at implementation vulnerabilities and how developers can make their mTLS systems vulnerable to user impersonation, privilege escalation and information leakages. We present some CVEs we found in popular open-source identity servers and ways to exploit them. Finally, we'll explain how these vulnerabilities can be spotted in source code and how the safe code looks like.

REFERENCES:

1. Wikipedia: Mutual Authentication (mTLS) https://en.wikipedia.org/wiki/Mutual_authentication#mTLS
2. Java: Possible RCEs in X.509 certificate validation [CVE-2018-2633][CVE-2017-10116]
<https://mbechler.github.io/2018/01/20/Java-CVE-2018-2633/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

MUS - Friday - 18:00-01:59 PDT

Title: Music Set / Entertainment (Friday, ACK Stage)

When: Friday, Aug 11, 18:00 - 01:59 PDT

Where: Caesars Forum - Forum Pre-Function 2 - ACK Stage - [Map](#)

Speakers:Acid T,CTRL/rsm,DJ PatAttack,DJ St3rling,Magik Plan,Scotch and Bubbles,Spice Rack,kampf

SpeakerBio:Acid T

No BIO available

SpeakerBio:CTRL/rsm

No BIO available

SpeakerBio:DJ PatAttack

No BIO available

SpeakerBio:DJ St3rling

No BIO available

SpeakerBio:Magik Plan

No BIO available

SpeakerBio:Scotch and Bubbles

No BIO available

SpeakerBio:Spice Rack

No BIO available

SpeakerBio:kampf

No BIO available

Description:

Featuring performances by:

- 18:00 – 19:00 – DJ PatAttack
- 19:00 – 20:00 – Kampf
- 20:00 – 21:00 – Scotch and Bubbles
- 21:00 – 22:00 – DJ St3rling
- 22:00 – 23:00 – Acid T
- 23:00 – 00:00 – CTRL/rsm
- 00:00 – 01:00 – Spice Rack
- 01:00 – 02:00 – Magik Plan

ACK Stage is located in front of the doors to rooms 117/118 in the Forum Pre-function 2. Look for the tents and the beats!

[Return to Index](#) - Add to  - ics [Calendar](#) file

MUS - Friday - 21:00-01:59 PDT

Title: Music Set / Entertainment (Friday, SYN Stage)

When: Friday, Aug 11, 21:00 - 01:59 PDT

Where: Caesars Forum - Forum - 121-123, 129, 137 - Chillout - [Map](#)

Speakers:Great Scott,Krisz Klink,TRIODE,Zebbler Encanti Experience,heckseven

SpeakerBio:Great Scott

No BIO available

Twitter: [@greatscottmusic](#)

SpeakerBio:Krisz Klink

No BIO available

Twitter: [@kriszklink](#)

SpeakerBio:TRIODE

No BIO available

SpeakerBio:Zebbler Encanti Experience

No BIO available

SpeakerBio:heckseven

No BIO available

Description:

Featuring performances by:

- 21:00 – 22:00 – heckseven
- 22:00 – 23:00 – Krisz Klink
- 23:00 – 00:00 – Great Scott
- 00:00 – 01:00 – Zebbler Encanti Experience
- 01:00 – 02:00 – TRIODE

Content from this stage will be streamed to https://www.twitch.tv/defconorg_entertainment

[Return to Index](#) - Add to  - ics [Calendar](#) file

MUS - Saturday - 18:00-01:59 PDT

Title: Music Set / Entertainment (Saturday, ACK Stage)

When: Saturday, Aug 12, 18:00 - 01:59 PDT

Where: Caesars Forum - Forum Pre-Function 2 - ACK Stage - [Map](#)

Speakers:DotOrNot,Dr. McGrew,H4X,Icetre Normal,NGHTHWK,SK,Z3npi,n0x08

SpeakerBio:DotOrNot

No BIO available

SpeakerBio:Dr. McGrew

No BIO available

SpeakerBio:H4X

No BIO available

SpeakerBio:Icetre Normal

No BIO available

SpeakerBio:NGHTHWK

No BIO available

SpeakerBio:SK

No BIO available

SpeakerBio:Z3npi

No BIO available

SpeakerBio:n0x08

No BIO available

Description:

Featuring performances by:

- 18:00 – 19:00 – SK
- 19:00 – 20:00 – DotOrNot
- 20:00 – 21:00 – n0x08
- 21:00 – 22:00 – Icetre Normal
- 22:00 – 23:00 – NGHTHWK
- 23:00 – 00:00 – H4X
- 00:00 – 01:00 – Z3npi
- 01:00 – 02:00 – Dr. McGrew

ACK Stage is located in front of the doors to rooms 117/118 in the Forum Pre-function 2. Look for the tents and the beats!

[Return to Index](#) - Add to  - ics [Calendar](#) file

MUS - Thursday - 18:00-01:59 PDT

Title: Music Set / Entertainment (Thursday, ACK Stage)

When: Thursday, Aug 10, 18:00 - 01:59 PDT

Where: Caesars Forum - Forum Pre-Function 2 - ACK Stage - [Map](#)

Speakers:Alexi Husky,DJ Scythe,Delchi,Grind613,Syntax,Talk Sinn,YTCracker,c0debreaker,matrix

SpeakerBio:Alexi Husky

No BIO available

SpeakerBio:DJ Scythe

No BIO available

SpeakerBio:Delchi

No BIO available

Twitter: [@HDA_DEFCON](#)

SpeakerBio:Grind613

No BIO available

SpeakerBio:Syntax

No BIO available

SpeakerBio:Talk Sinn

No BIO available

Twitter: [@Cuteboi_Roxin](#)

SpeakerBio:YTCracker

No BIO available

SpeakerBio:c0debreaker

No BIO available

SpeakerBio:matrix

No BIO available

Description:

Featuring performances by:

- 17:00 – 18:00 – YTCracker
- 18:00 – 19:00 – Delchi
- 19:00 – 20:00 – Talk Sinn
- 20:00 – 21:00 – Grind613
- 21:00 – 22:00 – Alexi Husky
- 22:00 – 23:00 – DJ Scythe
- 23:00 – 00:00 – Syntax
- 00:00 – 01:00 – matrix
- 01:00 – 02:00 – c0debreaker

ACK Stage is located in front of the doors to rooms 117/118 in the Forum Pre-function 2. Look for the tents and the beats!

MUS - Thursday - 18:00-01:59 PDT

Title: Music Set / Entertainment (Thursday, SYN Stage)

When: Thursday, Aug 10, 18:00 - 01:59 PDT

Where: Caesars Forum - Forum - 121-123, 129, 137 - Chillout - [Map](#)

Speakers:Bolonium,Deepblue,Dries,Dual Core,NPC Collective,Nina Lowe,PankleDank,The Icarus Kid

SpeakerBio:Bolonium

No BIO available

SpeakerBio:Deepblue

No BIO available

SpeakerBio:Dries

No BIO available

SpeakerBio:Dual Core

No BIO available

SpeakerBio:NPC Collective

No BIO available

SpeakerBio:Nina Lowe

No BIO available

SpeakerBio:PankleDank

No BIO available

SpeakerBio:The Icarus Kid

No BIO available

Description:

Featuring performances by:

- 18:00 – 19:00 – Dual Core
- 19:00 – 20:00 – NPC Collective
- 20:00 – 21:00 – Bolonium
- 21:00 – 22:00 – The Icarus Kid
- 22:00 – 23:00 – Dries
- 23:00 – 00:00 – Nina Lowe
- 00:00 – 01:00 – PankleDank
- 01:00 – 02:00 – Deepblue

Content from this stage will be streamed to https://www.twitch.tv/defconorg_entertainment

[Return to Index](#) - Add to  - ics [Calendar](#) file

HRV - Sunday - 12:00-12:30 PDT

Title: My Callsign Is My Passport - Responsible Testing And Disclosure Of Amateur Radio Websites

When: Sunday, Aug 13, 12:00 - 12:30 PDT

Where: Flamingo - Virginia City - Ham Radio Village - [Map](#)

Speakers:Dan Norte, Lucas Gahler

SpeakerBio:Dan Norte , NetSPI

Red teamer for 4 years, currently with NetSPI. Ham for 6 years, currently Amateur Extra class Likes to pop shells and chase DX.

SpeakerBio:Lucas Gahler , ICF

10 years in infosec, mostly in blue team roles ham for 13 years, currently Amateur Extra class Avid POTA enthusiast serial hobbyist in anything involving motors, circuit boards, or kinetic energy.

Description:

Amateur radio websites / web applications are notorious for terrible / non-existence information security practices and there's normally no budget to get professional help. Meanwhile, there's a large overlap in the Venn Diagram circles of infosec talent and amateur radio licensees. Leveraging our callsigns as AuthN and establishing mutual trust, we've developed a loose framework for how the hacker community can provide infosec consulting as a volunteer service, helping the hobby level up their security practices (or at least clean up some of the low hanging fruit). This talk walks through an example where this concept was applied, what was learned in the process, and reflections on how this could be leveraged by the broader community.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: My CPAP has a recall, lets open it instead!

When: Friday, Aug 11, 16:30 - 17:20 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

SpeakerBio: José Fernández , President at CompSec Direct

José Fernández is the President of CompSec Direct. José's background in CNO, CND, and engineering has allowed him to work in some of the most technically demanding environments in both private and public sector. Mr. Fernandez is a Puertorican Hacker Dude, Veteran, and the Director of Recruitment for AUSCF.

Description:

We all need to sleep and having sleep apnea sucks. Sleep apnea diagnoses have become more prevalent among our society. The continuous positive airway pressure or CPAP equipment, like the Phillips Dreamstation, helps individuals with sleep apnea by providing a regulated air stream into their respiratory system. Problem is sometimes these medical devices have manufacturer recalls

<https://www.usa.philips.com/healthcare/e/sleep/communications/src-update> and the main concern around the recalls are due to the increased risk of getting much sicker while using the devices, usually due to the reduced manufacturing costs per component within medical devices. This talk focuses on the Philips Dreamstation device that is part of an on-going recall. This talk will cover a simple tear down and analysis of the device components and will also cover the CPAP firmware scene where hackers homebrew and modify firmware to help them and their friends get sleep across CPAP devices.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Navigating the Digital Frontier: Advancing Cyber Diplomacy in a Connected World

When: Saturday, Aug 12, 17:00 - 17:50 PDT

Where: Caesars Forum - Summit - 221-222 - Policy Atrium - [Map](#)

Speakers: Christopher Painter, Harry Krejsa, Monica M. Ruiz, Océane Thieriot, Orlando Garces

SpeakerBio: Christopher Painter , President at Global Forum on Cyber Expertise

Chris Painter is the President of the Global Forum on Cyber Expertise. He served as the first top cyber diplomat in the U.S. State Department, in the White House as Senior Director for Cyber Policy in the National Security Council, and in the Justice Department and the FBI. Awards include the RSA Award for Excellence in the Field of Public Policy (2016), the Attorney General's Award for Exceptional Service, and the Intelligence Community Legal Award (2008).

Twitter: [@c_painter](#)

SpeakerBio: Harry Krejsa , Assistant National Cyber Director for Strategy at The Office of National Cyber Director (ONCD)

Harry Krejsa leads cyber strategy for the Office of the National Cyber Director (ONCD), including the development of the Biden-Harris Administration's 2023 National Cybersecurity Strategy. Harry joined ONCD from the Department of Defense where he developed frameworks for deterring and disrupting adversary cyber campaigns while overseeing military cyber policy engagement in the Indo-Pacific. Previously, Harry directed emerging technology policy at the Cyberspace Solarium Commission, researched U.S.-China strategic competition at the Center for a New American Security, and received a Fulbright Fellowship to Taiwan. A native to rural Iowa, Harry graduated from Grinnell College with a B.A. in Political Science and East Asian Studies and holds a master's degree in International Relations from the Princeton School of Public and International Affairs.

SpeakerBio: Monica M. Ruiz , Senior Government Affairs Manager, Digital Diplomacy at Microsoft

Monica M. Ruiz is a Senior Government Affairs Manager in Microsoft's Digital Diplomacy team. In this role she focuses on efforts to promote stability in cyberspace and advance trust, security and human rights in this domain. She holds a bachelor's degree from Florida International University and a master's degree from The Fletcher School of Law and Diplomacy at Tufts University.

SpeakerBio: Océane Thieriot , Counselor for Cyber Affairs at Embassy of France in Washington DC

Océane Thieriot is the Counselor for Cyber Affairs at the Embassy of France in Washington DC.

Before joining the Embassy, she held positions within the French Ministry of Foreign Affairs, serving in Brussels (Deputy Antici Counselor at the French Permanent Representation to the EU) as well as in Paris (member of the cabinet of the Minister for European Affairs). She is a graduate from Ecole Normale Supérieure, Sciences Po and Ecole Nationale d'Administration.

SpeakerBio: Orlando Garces , Cybersecurity Program Officer at Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS)

Orlando Garcés, Cybersecurity Program Officer of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS), focusing primarily on strategy and policy, governance issues, and gender mainstreaming in cybersecurity. He has strategically participated in the formulation and implementation of National Cybersecurity Strategies and Policies in several countries in the Latin American and Caribbean region, as well as in the development of reports and studies on the state of cybersecurity in strategic industries and sectors.

Description:

In an increasingly interconnected and technologically driven world, the need for robust and comprehensive cyber diplomacy has become paramount. This panel titled "Navigating the Digital Frontier: Advancing Cyber Diplomacy in a Connected World" will bring together experts across government, industry and civil society to explore the multifaceted challenges posed by cyberspace and discuss strategies to ensure a secure and resilient digital landscape. The panel will delve into ongoing

global and regional international cyber dialogues, such as the United Nations (UN) Open-Ended Working Group on security of and in the use of information and communications technologies, the UN Ad-Hoc Committee on Cybercrime (AHC), and the Organization of American States (OAS) Working Group on Cooperation and Confidence-Building Measures in cyberspace. It will also explore capacity building initiatives being pursued across the international community and surface efforts that promote cooperation and trust in cyberspace across different regions. Moreover, the panel will investigate the role of public-private partnerships in shaping effective cyber policy frameworks.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MIV - Saturday - 11:30-12:30 PDT

Title: Navigating the Disinformation Landscape

When: Saturday, Aug 12, 11:30 - 12:30 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio:Eric Curwin

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: ndays are also 0days: Can hackers launch 0day RCE attack on popular softwares only with chromium ndays?

When: Saturday, Aug 12, 15:30 - 16:15 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

Speakers:Bohan Liu,GuanCheng Li,Zheng Wang

SpeakerBio:Bohan Liu , Senior Security Researcher at Tencent Security Xuanwu Lab

Bohan Liu (@P4nda20371774) is a senior security researcher at Tencent Security Xuanwu Lab. He focuses on browser security research and has discovered multiple Chrome vulnerabilities. He also presented his research results on Kanxue SDC and Black Hat Asia.

Twitter: [@P4nda20371774](#)

SpeakerBio:GuanCheng Li , Senior Security Researcher at Tencent Security Xuanwu Lab

GuanCheng Li (@atuml1) is a senior researcher at Tencent Security Xuanwu Lab. His research interests are focused on software and system security, IoT security, software engineering and AI. He is also a founder and former captain of r3kapiG CTF Team.

Twitter: [@atuml1](#)

SpeakerBio:Zheng Wang , Senior Security Researcher at Tencent Security Xuanwu Lab

Zheng Wang (@xmzyshypnc) is a senior Security Researcher at Tencent Security Xuanwu Lab. He's mainly engaged in browser and linux kernel security. He is also a speaker attending in Black Hat Asia 2023.

Twitter: [@xmzyshypnc](#)

Description:

Chromium is not only the most popular browser in the world but also one of the most widely integrated supply chain components. Nowadays, a large number of popular software is built on frameworks based on Chromium, such as CEF and Electron. This means that vulnerabilities in Chromium will directly affect popular software. In addition, according to Google's vulnerability disclosure policy, most of the details of Chromium vulnerabilities will be publicly disclosed 14 weeks after being fixed, and many of these vulnerabilities are high-impact and may lead to RCE. Unfortunately, we have found that much downstream software is unable to timely fix the Chromium vulnerabilities. This creates a window of opportunity for attackers to carry out RCE attacks on popular software. The cost for attackers to exploit these vulnerabilities during this window is relatively low, as it falls between the time of the Chromium vulnerability disclosure and the completion of fixes for popular software. We refer to this window as the "RCE window period".

In this topic, we will first evaluate the "RCE window period" of more than 20 popular software. In the upcoming section, we will showcase how to transform Chromium nday vulnerabilities into popular software 0day vulnerabilities in a low-cost manner within the "RCE window period". To illustrate this process, we will use over 10 RCE 0day vulnerabilities in popular software that we have discovered as examples. Some software will attempt to enable sandbox to mitigate this problem, so we will also provide examples of how to bypass the sandbox by exploiting vulnerabilities in the software itself rather than a Chromium sandbox bug.

Finally, we will discuss the reasons for the existence of the RCE window period and the lessons learned from it, hoping to help software developers improve the security of their products.

REFERENCES

[1] <https://googleprojectzero.blogspot.com/2022/06/2022-0-day-in-wild-exploitationso-far.html> [2]

<https://bugs.chromium.org/p/chromium/issues/list?q=Type%3DBug-Security&can=2> [3]

<https://bitbucket.org/chromiumembedded/cef/wiki/GeneralUsage> [4] <https://www.electronjs.org/docs/latest/> [5]

<https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Junyu-Zhou-and-Ce-Qin-and>


[6] <https://i.blackhat.com/USA-22/Thursday/US-22-Purani-Electro-Volt-Pwning-Popular-Desktop-Apps.pdf> [7]

<https://plugins.jetbrains.com/docs/intellij/jcef.html> [8]

<https://medium.com/@ethickid/recent-burp-rce-zero-day-df39b1b24230> [9] <https://crbug.com/1307610>

[10] https://cs.android.com/android/platform/superproject+/master:external/selinux/libselinux/src/android/android_seapp.c

[11] <https://security.googleblog.com/2021/07/protecting-more-with-site-isolation.html>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Sunday - 09:00-12:59 PDT

Title: NetworkOS: Be The Cloud

When: Sunday, Aug 13, 09:00 - 12:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

The NetworkOS workshop takes you into the mysterious world underpinning modern computing and global communication: the network itself. Step by step, you'll learn all the basics you need. No experience needed: must know how to type and copy/paste.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Saturday - 09:00-17:59 PDT

Title: NetworkOS: Be The Cloud

When: Saturday, Aug 12, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

The NetworkOS workshop takes you into the mysterious world underpinning modern computing and global communication: the network itself. Step by step, you'll learn all the basics you need. No experience needed: must know how to type and copy/paste.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Friday - 09:00-17:59 PDT

Title: NetworkOS: Be The Cloud

When: Friday, Aug 11, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

The NetworkOS workshop takes you into the mysterious world underpinning modern computing and global communication: the network itself. Step by step, you'll learn all the basics you need. No experience needed: must know how to type and copy/paste.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: New Isn't Always Novel: Grep'ing Your Way to \$20K at Pwn2Own, and How You Can Too

When: Thursday, Aug 10, 12:30 - 13:15 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers: James Horseman, Zach Hanley

SpeakerBio: James Horseman , Vulnerability Researcher at Horizon3.ai

James Horseman loves low-level systems programming and reverse engineering. Has a history of developing implants and weaponizing n-days. He is a vulnerability researcher and attack engineer at Horizon3.ai.

Twitter: [@JamesHorseman2](#)

SpeakerBio: Zach Hanley , Vulnerability Researcher at Horizon3.ai

Zach Hanley has been hooked on exploit development and offensive security since introduced to the world of hacking as an On-Net Operator for DoD and IC organizations. He's since developed implants and exploits for both the government and commercial sector. He currently is a vulnerability researcher and attack engineer for Horizon3.ai.

Twitter: [@hacks_zach](#)

Description:

The year is 2023 and we're still finding very basic vulnerabilities in enterprise software.

In this presentation, we detail how the hacker mindset can be applied to seemingly daunting tasks to make them more approachable. We will show how we approached our first Pwn2Own contest and how we discovered a command injection RCE vulnerability affecting nearly every Lexmark printer. We'll take a look at why we think it went unnoticed in previous research and why current open-source static analysis tools miss this simple bug.

Finally we'll release the exploit POC and an additional POC to dump credentials during engagements.

REFERENCES

1.

<https://research.nccgroup.com/2022/02/17/bypassing-software-update-package-encryption-extracting-the-lexmark-mc3224>

2. <https://publications.lexmark.com/publications/security-alerts/CVE-2023-26068.pdf> 3.

<https://www.zerodayinitiative.com/advisories/upcoming/> (ZDI-CAN-19470)

[Return to Index](#) - Add to  - ics [Calendar](#) file


MISC - Friday - 16:00-16:59 PDT

Title: No Starch Press - Book Signing - Bradly Smith, DevOps for the Desperate

When: Friday, Aug 11, 16:00 - 16:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Friday - 11:00-11:59 PDT

Title: No Starch Press - Book Signing - Bryson Payne, Go H*ck Yourself

When: Friday, Aug 11, 11:00 - 11:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Saturday - 14:30-14:59 PDT

Title: No Starch Press - Book Signing - Cory Doctorow, Red Team Blues & Chokepoint Capitalism

When: Saturday, Aug 12, 14:30 - 14:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

SpeakerBio:Cory Doctorow

Cory Doctorow (craphound.com) is a science fiction author, activist and journalist. He is the author of many books, most recently RED TEAM BLUES, a science fiction crime thriller; CHOKEPOINT CAPITALISM, nonfiction about monopoly and creative labor markets; the LITTLE BROTHER series for young adults; IN REAL LIFE, a graphic novel; and the picture book POESY THE MONSTER SLAYER. In 2020, he was inducted into the Canadian Science Fiction and Fantasy Hall of Fame.

Twitter: [@doctorow](#)

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Friday - 13:00-13:59 PDT

Title: No Starch Press - Book Signing - Craig Smith, The Car Hacker's Handbook

When: Friday, Aug 11, 13:00 - 13:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file


MISC - Saturday - 12:00-12:59 PDT

Title: No Starch Press - Book Signing - Daniel Reilly, Math for Security

When: Saturday, Aug 12, 12:00 - 12:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file


MISC - Saturday - 16:00-16:59 PDT

Title: No Starch Press - Book Signing - Fotios Chantzis, Paulino Calderon, & Beau Woods, Practical IoT Hacking

When: Saturday, Aug 12, 16:00 - 16:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file


MISC - Friday - 12:00-12:59 PDT

Title: No Starch Press - Book Signing - Joe Gray, Practical Social Engineering

When: Friday, Aug 11, 12:00 - 12:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Saturday - 15:00-15:59 PDT

Title: No Starch Press - Book Signing - Jon DiMaggio, The Art of Cyberwarfare

When: Saturday, Aug 12, 15:00 - 15:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Saturday - 13:00-13:59 PDT

Title: No Starch Press - Book Signing - Jos Weyers, Matt Burrough & BandEatoZ, Locksport

When: Saturday, Aug 12, 13:00 - 13:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Saturday - 11:00-11:59 PDT

Title: No Starch Press - Book Signing - Maria Markstedter, Blue Fox: Arm Assembly Internals and Reverse Engineering

When: Saturday, Aug 12, 11:00 - 11:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

SpeakerBio: Maria Markstedter

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Saturday - 14:00-14:59 PDT

Title: No Starch Press - Book Signing - Micah Lee, Hacks, Leaks and Revelations

When: Saturday, Aug 12, 14:00 - 14:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Friday - 15:00-15:59 PDT

Title: No Starch Press - Book Signing - Nick Aleks & Dolev Farhi, Black Hat GraphQL

When: Friday, Aug 11, 15:00 - 15:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Saturday - 11:00-11:59 PDT

Title: No Starch Press - Book Signing - Patrick Wardle, The Art of Mac Malware

When: Saturday, Aug 12, 11:00 - 11:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Friday - 14:00-14:59 PDT

Title: No Starch Press - Book Signing - Travis Goodspeed, PoC or GTFO Volume 1, 2, & 3

When: Friday, Aug 11, 14:00 - 14:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

QTV - Friday - 11:00-11:59 PDT

Title: No time for NISQy Business

When: Friday, Aug 11, 11:00 - 11:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

SpeakerBio:Rafal Janik

No BIO available

Description:

The allure of quantum computing has long been clouded by overstated claims of quantum advantage, many of which are quickly debunked. As we navigate the noisy intermediate-scale quantum (NISQ) era, the cruciality of error correction and fault tolerance becomes undeniable. Without these, the quantum promise remains elusive. Amidst the NISQy noise, it's high time we prioritize genuine progress and deep work over fleeting attention. Join us in championing a clear-eyed approach to the quantum future.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Non-State Actors in the Russia/Ukraine Conflict

When: Saturday, Aug 12, 15:00 - 15:50 PDT

Where: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

Speakers: Dan Grobarcik, Marc Rogers, Mauro Vignati, Stefanie Metka

SpeakerBio: Dan Grobarcik, Research Associate at Cyber and Innovation Policy Institute at the U.S. Naval War College
Dan Grobarcik is a Research Associate with the Cyber and Innovation Policy Institute at the U.S. Naval War College. His research covers information warfare, the Cold War, and European and Eurasian security issues.


SpeakerBio: Marc Rogers, Senior Adjunct Advisor at Institute for Security and Technology
Marc Rogers is the CTO and Co-founder of nbhd.ai and a Senior Adjunct Advisor for the Institute for Security and Technology. Formerly a cybersecurity strategist at Okta, head of security at Cloudflare and co-founder of Vectra.ai. Marc is a whitehat hacker and breaker of things from Teslas, to iPhones, Google Glasses and more. As seen on Mr Robot. Part of IST's Ransomware Task Force, Co-Founder of CTI League, Cultivator of beards.

SpeakerBio: Mauro Vignati, ICRC
In 2003 Mauro started working at the first unit of the Swiss Federal Police fighting cybercrime. Later on, he collaborated to the establishment of MELANI, Switzerland's first centre for public-private partnership on cybersecurity for critical infrastructure. Back in 2013, he set up and led the Cyber Threat Intelligence Division within the Department of Defence in Bern. In 2021, he was tasked to create the Vulnerability Management unit within the National Cyber Security Centre NCSC.ch, leading several projects, among them the first bug bounty program of the Swiss government. He then joined the International Committee of the Red Cross ICRC one year later, as advisor on new digital technologies of warfare.

SpeakerBio: Stefanie Metka, NATO
Stefanie Metka is the head of NATO's Cyber Threat Analysis Branch and serves as a primary advisor to NATO's political, military, and security leadership on cyber threats. Prior to joining NATO, Stefanie served as a Strategic Threat Analyst in the Canadian civil service, and has had a number of postings with a focus on cyber threats and national security. Stefanie received her Master's degree in infrastructure protection and international security from Carleton University, and is also an alumni of the Geneva Centre for Security Policy, and Cornell University.

Description:

This panel explores the presence and actions of non-state actors in the Russia-Ukraine conflict. With a focus on volunteerist cyber actors in the conflict, such as patriotic hackers and hacktivist collectives, individual volunteers - or even the private sector -, the panel explores the conduct of these actors during the conflict, as well as how the cyber criminal landscape has evolved during the course of the conflict. Bringing together a set of diverse perspectives from across the policy, operational, legal, and security community spheres, both within, and outside of government, including the NGO space, it focuses on the implications of these actions: can these indeed be considered altruistic actions in cyberspace? Or do they hold more complex implications than we are prepared to admit? This panel intends to demonstrate the ways in which the actions of non-state actors challenge some of our basic assumptions about cyberspace as a domain of operations – but also how adversaries might understand this behaviour too. Ultimately, it argues that the unique space that non-state actors occupy within the cyber elements of the conflict requires much deeper consideration, and complex, considered thought from the wider international security community.

[Return to Index](#) - Add to  - ics [Calendar](#) file

RCV - Friday - 16:30-17:15 PDT

Title: Nosy Cops: Exposing the Hidden Potential of Police Radio

When: Friday, Aug 11, 16:30 - 17:15 PDT


Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio:sally

No BIO available

Twitter: [@sally_yachts](#)

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Not All Alerts Are Born Equal: Insights from AppSec Experts on Prioritizing Security Alerts

When: Saturday, Aug 12, 12:30 - 13:30 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

Speakers: Joe Christian, Kunal Bhattacharya, Shahar Man, Trupti Shiralkar

SpeakerBio: Joe Christian

Joe Christian currently serves as the Engineering Manager for the DevSecOps Platforms team at Paylocity. Previously, Joe held leadership positions at Brex and Zappos. Joe is also a Cyber Defense Ph.D. student at Dakota State University.

Twitter: [@Jo3Ram](#)

SpeakerBio: Kunal Bhattacharya

A Security Leader, Organization builder and mentor who helps organizations build robust Cyber defense and detection capabilities. I do this by building Secure SDL processes and machination encapsulating Shiftright strategy, SecDevOps, Cloud and Penetration testing. My prior experience in all phases of Application development, System and database administration and Quality engineering helps me in building lasting relationships with peers in engineering and product organizations and working towards shared security goals.

SpeakerBio: Shahar Man

Passionate about building and leading teams, I have successfully grown Engineering and Product teams from scratch, leveraging Agile methodologies. My focus lies in Application and Cloud Security, advocating for context-driven AppSec decisions.

SpeakerBio: Trupti Shiralkar

Trupti Shiralkar is a Sr Engineering Manager at Datadog. Her 15+ years of industry experience ranges from Fortune 500s to small startups including Illumio, Amazon, Hewlett Packard, Q2ebanking and ATSEC Information Security. She holds a Master of Science degree in Information Security from Johns Hopkins University Information Security Institute (JHUISI) and several security certifications. As a product security leader and seasoned public speaker, she is committed to sharing her knowledge to influence positive security and reduce organization wide risk. She holds a patent for secure and anonymous electronic polling.

Twitter: [@tshiralkar](#)

Description:

In today's threat landscape, security teams are overwhelmed with the number of alerts generated by their security stack. However, not all alerts are equally critical, and it's essential to prioritize them based on their severity and context impact on the organization. In this panel discussion, our AppSec experts will share their experiences and insights on how to effectively prioritize alerts and reduce alert fatigue. They will discuss best practices for triaging alerts, techniques to automate the process, and strategies to ensure that the most critical alerts receive immediate attention. Join us to learn from the experts on how to effectively manage security alerts and improve your organization's security posture.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Not Just The Pickle: An Overview of Exploitable ML Serialization Formats

When: Friday, Aug 11, 12:30 - 13:25 PDT


Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

SpeakerBio: Marta Janus

No BIO available

Description:

Machine learning models are often treated as black boxes, with their internals hidden away from users. However, as ML technology has become more prevalent in everyday life, it is crucial to understand that these models are essentially code - and as such, can be manipulated in unexpected and potentially malicious ways. In this talk, we explore several model serialization formats used by popular ML libraries, such as PyTorch, Keras, TensorFlow, and scikit-learn. We show how each of these formats can be exploited to execute arbitrary code and bypass security measures, leading to the compromise of critical ML infrastructure systems. We also demonstrate how it is possible to hide a malicious payload inside an ML model using steganography and then reconstruct and execute it when the model is loaded into memory.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Nothing but Net: Leveraging macOS's Networking Frameworks to Heuristically Detect Malware

When: Friday, Aug 11, 16:30 - 17:15 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

SpeakerBio: Patrick Wardle , Objective-See Foundation

Patrick Wardle is the creator of the non-profit Objective-See Foundation, author of the “The Art of Mac Malware” book series, and founder of the "Objective by the Sea" macOS Security conference.

Having worked at NASA and the NSA, as well as presenting at countless security conferences, he is intimately familiar with aliens, spies, and talking nerdy.

Patrick is passionate about all things related to macOS security and thus spends his days finding Apple 0days, analyzing macOS malware, and writing books and free open-source security tools to protect Mac users.

Twitter: [@patrickwardle](#)

Description:

As the majority of malware contains networking capabilities, it is well understood that detecting unauthorized network access is a powerful detection heuristic. However, while the concepts of network traffic analysis and monitoring to detect malicious code are well established and widely implemented on platforms such as Windows, there remains a dearth of such capabilities on macOS.

This talk aims to remedy this situation by delving deeply into a myriad of programmatic approaches capable of enumerating network state, statistics, and traffic, directly on a macOS host. We will showcase open-source implementations of relatively overlooked low-level APIs, private frameworks, and user-mode extensions that provide insight into all networking activity. And, by leveraging these techniques, you will learn how to efficiently and generically detect both known and unknown threats targeting macOS!

REFERENCES

- J. Levin <http://newosxbook.com/src.jl?tree=listings&file=netbottom.c> - P. Wardle
- https://objective-see.org/blog/blog_0x72.html - Will Yu / Elastic
- <https://www.elastic.co/blog/mac-system-extensions-for-threat-detection-part-3>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Nuthin But A G Thang: Evolution of Cellular Networks

When: Thursday, Aug 10, 15:30 - 16:15 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio: Tracy Mosley , Trenchant

Tracy is a New York City based Lead Security Research Engineer at Trenchant (formerly known as Azimuth Security). With a degree in Computer Engineering and over 10 years in the industry, Tracy has predominantly focused on vulnerability research, reverse engineering and development for embedded devices. She has led teams focused on telecommunications equipment and contributed to teams large and small working on routers and various types of embedded devices.

Her first degree is in theatre performance, with a vocal performance minor. Vocal technique, performance and understanding the vocal mechanism are what drew her into telecommunications. You may have seen her presenting at conferences, attending trainings, dancing the night away or performing on stage.

Twitter: [@@hackerpinup](#)

Description:

4G? LTE? 3GPP? A lot of telecommunications terminology gets thrown around, but what does it actually mean? While terms like “5G”, and “packet core” may be in common use, it’s hard to understand what they mean in terms of attack surface, or even as a consumer. Very often even network diagrams will show “Core Network” as a big blob, or stop at the Radio Access Network. It’s hard to have insight into the cellular network. So, I’ll explain generation by generation!

In this talk we will walk through each step of cellular evolution, starting at 2G and ending at 5G. The never-ending attack and defend paradigm will be clearly laid out. In order to understand the attack surface, I’ll cover network topology and protocol. For each cellular generation, I will explain known vulnerabilities and some interesting attacks. In response to those vulnerabilities, mitigations for the subsequent cellular generation are put in place. But as we all know, new mitigations mean new opportunities for attackers to get creative.

While I will explain most cellular-specific terminology, a familiarity with security concepts will help to better understand this talk. Basic foundations of communications systems, information theory or RF definitely make this talk more enjoyable, but are absolutely not necessary. It’s a dense topic that is highly applicable to those working on anything that touches the cellular network!

REFERENCES

1. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE, Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, Elisa Bertino
2. <https://www.cybersecuritydive.com/news/5g-security-breaches/636693/>
3. <https://networksimulationtools.com/5g-network-attacks-projects>
4. <https://www.p1sec.com/corp/category/p1-security/>
5. A Vulnerability in 5G Authentication Protocols and Its Countermeasure Xinxin HU, Caixia LIU, Shuxin LIU, Jinsong LI, and Xiaotao CHENG
6. New Vulnerabilities in 5G Networks Altaf Shaik* , Ravishankar Borgaonkar
7. ESF Potential Threats to 5G Network Slicing, NSA, CISA
8. <https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1010203>
9. <https://www.pentestpartners.com/security-blog/zte-mf910-an-end-of-life-router-running-lots-of-vivacious-hidden-> pentestpartners DC27 talk
10. LTE Pwnage: Hacking HLR/HSS and MME Core Network Elements P1 Security <https://conference.hitb.org/hitbsecconf2013ams/materials/D1T2%20-%20Philippe%20Langlois%20-%20Hacking%20LTE%20Pwnage.pdf>
11. Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui L., Elisa Bertino
12. <https://thehackernews.com/2018/03/4g-lte-network-hacking.html>

13. <https://www.pentestpartners.com/security-blog/zte-mf910-an-end-of-life-router-running-lots-of-vivacious-hidden->
 14. A first look on the effects and mitigation of VoIP SPIT flooding in 4G mobile networks. 982-987. 10.1109/ICC.2012.6364233. Bou-Harb, Elias & Debbabi, Mourad & Assi, Chadi. (2012).
 15. <https://resources.infosecinstitute.com/topic/cheating-voip-security-by-flooding-the-sip/>
 16. <https://www.mpirical.com/> for 5G trainings
 17. <https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1010203>
 18. <https://www.pentestpartners.com/security-blog/zte-mf910-an-end-of-life-router-running-lots-of-vivacious-hidden->
 19. https://en.wikipedia.org/wiki/Cellular_network
 20. https://www.etsi.org/deliver/etsi_ts/123000_123099/123060/10.03.00_60/ts_123060v100300p.pdf Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS); Service description;
 21. https://www.etsi.org/deliver/etsi_ts/133100_133199/133102/14.01.00_60/ts_133102v140100p.pdf Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture (3GPP TS 33.102 version 14.1.0 Release 14)
 22. https://www.etsi.org/deliver/etsi_ts/133400_133499/133401/15.07.00_60/ts_133401v150700p.pdf Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture
 23. https://www.etsi.org/deliver/etsi_ts/133400_133499/133401/15.07.00_60/ts_133401v150700p.pdf Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401 version 15.7.0 Release 15)
 24. https://www.etsi.org/deliver/etsi_ts/124300_124399/124301/17.06.00_60/ts_124301v170600p.pdf Universal Mobile Telecommunications System (UMTS); LTE; 5G; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (3GPP TS 24.301 version 17.6.0 Release 17)
 25. https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.04.00_60/ts_133501v150400p.pdf 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.4.0 Release 15) Previous talk: <https://www.youtube.com/watch?v=-JX7aC0AXEk&t=7387s>
-

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT


Title: Octopus Game

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Octopus Game is back for a second year! This contest is a battle royale style competition where fun and friendship is the goal. This year players will meet together in various locations at the same time for group competition through through fun games. 128 players will enter, but only 1 will be crowned the Octopus CHAMPION. Join us, make some new friends and remember: only the best will prevail!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-13:59 PDT


Title: Octopus Game

When: Friday, Aug 11, 10:00 - 13:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Octopus Game is back for a second year! This contest is a battle royale style competition where fun and friendship is the goal. This year players will meet together in various locations at the same time for group competition through through fun games. 128 players will enter, but only 1 will be crowned the Octopus CHAMPION. Join us, make some new friends and remember: only the best will prevail!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-13:59 PDT


Title: Octopus Game

When: Saturday, Aug 12, 10:00 - 13:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Octopus Game is back for a second year! This contest is a battle royale style competition where fun and friendship is the goal. This year players will meet together in various locations at the same time for group competition through through fun games. 128 players will enter, but only 1 will be crowned the Octopus CHAMPION. Join us, make some new friends and remember: only the best will prevail!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Off the Rails: A demo with Pacific Northwest National Labs

When: Sunday, Aug 13, 11:00 - 11:59 PDT

Where: Caesars Forum - Summit - 206 - XR Village - [Map](#)

Description:

Pacific Northwest National Laboratory (PNNL) has developed and operates modeled physical environments for training and demonstrating cyber security for DHS CISA as part of their ICS Control Environment Laboratory Resource (CELR). To expose a broader audience at conferences and industry venues, CISA is implementing an XR interface to enable remote users to have a visceral experience as if they are in the same room as the CELR models. The CISA CELR team is developing cutting-edge data pipelines with the Depthkit software and developers at Scatter that can record and transmit accurate 3D renderings of objects and people in near real-time to an XR headset (HoloLens 2). Depthkit combines the data streams from up to 10 Microsoft Azure Kinect cameras and combines them into a calibrated photorealistic 3D video. This video can be exported into the Unity game engine and embedded as recordings or live streams into an XR application. The demonstration planned for Defcon will be for the Rail sector systems including an AR overview of the skid model with some pre-recorded videos of failure scenarios and some VR exploration of rail sector subsystems including a locomotive cab, wayside controller, and regional dispatch display. Conference attendees will learn more about the rail sector and its use of cyber components and the potential risks of cyber based failures.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Off the Rails: A demo with Pacific Northwest National Labs

When: Friday, Aug 11, 11:00 - 16:59 PDT

Where: Caesars Forum - Summit - 206 - XR Village - [Map](#)

Description:

Pacific Northwest National Laboratory (PNNL) has developed and operates modeled physical environments for training and demonstrating cyber security for DHS CISA as part of their ICS Control Environment Laboratory Resource (CELR). To expose a broader audience at conferences and industry venues, CISA is implementing an XR interface to enable remote users to have a visceral experience as if they are in the same room as the CELR models. The CISA CELR team is developing cutting-edge data pipelines with the Depthkit software and developers at Scatter that can record and transmit accurate 3D renderings of objects and people in near real-time to an XR headset (HoloLens 2). Depthkit combines the data streams from up to 10 Microsoft Azure Kinect cameras and combines them into a calibrated photorealistic 3D video. This video can be exported into the Unity game engine and embedded as recordings or live streams into an XR application. The demonstration planned for Defcon will be for the Rail sector systems including an AR overview of the skid model with some pre-recorded videos of failure scenarios and some VR exploration of rail sector subsystems including a locomotive cab, wayside controller, and regional dispatch display. Conference attendees will learn more about the rail sector and its use of cyber components and the potential risks of cyber based failures.

[Return to Index](#) - Add to  - ics [Calendar](#) file


Title: Off the Rails: A demo with Pacific Northwest National Labs

When: Saturday, Aug 12, 11:00 - 16:59 PDT

Where: Caesars Forum - Summit - 206 - XR Village - [Map](#)

Description:

Pacific Northwest National Laboratory (PNNL) has developed and operates modeled physical environments for training and demonstrating cyber security for DHS CISA as part of their ICS Control Environment Laboratory Resource (CELR). To expose a broader audience at conferences and industry venues, CISA is implementing an XR interface to enable remote users to have a visceral experience as if they are in the same room as the CELR models. The CISA CELR team is developing cutting-edge data pipelines with the Depthkit software and developers at Scatter that can record and transmit accurate 3D renderings of objects and people in near real-time to an XR headset (HoloLens 2). Depthkit combines the data streams from up to 10 Microsoft Azure Kinect cameras and combines them into a calibrated photorealistic 3D video. This video can be exported into the Unity game engine and embedded as recordings or live streams into an XR application. The demonstration planned for Defcon will be for the Rail sector systems including an AR overview of the skid model with some pre-recorded videos of failure scenarios and some VR exploration of rail sector subsystems including a locomotive cab, wayside controller, and regional dispatch display. Conference attendees will learn more about the rail sector and its use of cyber components and the potential risks of cyber based failures.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Saturday - 14:00-17:59 PDT

Title: Off the record war story talks - Signs Ups On Site

When: Saturday, Aug 12, 14:00 - 17:59 PDT

Where: Harrah's - Nevada Ballroom - Lake Tahoe & Reno - War Stories - Off the Record - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Sunday - 12:00-13:30 PDT

Title: Officially Unofficial Safecracking Tournament

When: Sunday, Aug 13, 12:00 - 13:30 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

SpeakerBio:Jared Dygert

No BIO available

Description:

Hands on experience with learning techniques to manipulate mechanical safe locks

[Return to Index](#) - Add to  - ics [Calendar](#) file

RCV - Friday - 11:35-12:10 PDT

Title: Oh The Places You'll Guo: Using Media Variants to Trace the Organization and Behavior of an Coordinated Inauthentic Influence Operation

When: Friday, Aug 11, 11:35 - 12:10 PDT


Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio:Patrick Warren

No BIO available

Twitter: [@plwarre](#)

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Open Distro of Malicious Maritime Hacking Tools: What Could Go Wrong?

When: Friday, Aug 11, 13:30 - 14:59 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

Speakers: Austin Reid, Gary C. Kessler, Nina Kollars

SpeakerBio: Austin Reid

No BIO available

SpeakerBio: Gary C. Kessler

No BIO available

SpeakerBio: Nina Kollars , Associate Professor at Cyber and Innovation Policy Institute at the US Naval War College
Nina (Kitty Hegemon) Kollars is an associate professor in the Cyber and Innovation Policy Institute at the US Naval War College. Dr. Kollars is a former Special Advisor to OUSD R&E, Logistics, Emerging tech, Cyber Conflict & Military Innovation for the Department of Defense. She publishes on cybersecurity, hackers and military innovation. She presented her own hacker project at DefCon27, “Confessions of a Nespresso Money Mule.” She will soon publish her book “Trustworthy Deviants: White Hat Hackers and Security.” Kollars is also an Executive Bourbon Steward.

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Open Sesame! How To Open One Thousand And One Locks In The 21St Century?

When: Friday, Aug 11, 14:00 - 14:50 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

SpeakerBio: Thomas BYGODT

Thomas BYGODT is a penetration tester at Orange Cyberdefense, a CTF player and a developer. He does not want to remain passive in front of the technologies that interact with the real world. Testing and understanding them allows us to better understand their limits, both for people's privacy and for their security. He has been specializing in connected devices for 3 years now.

Description:

In an ever increasingly connected society, we are often introduced to “new and improved” devices that offer smart capabilities, and door locks are no exception. Increased security and ease of use are some of the key selling points for these locks.

While some devices are hard to attack, the majority are not, because manufacturers are not following simple security practices in their physical, hardware and code design. Improving their security is essential, but how do you do that when hardware and IoT hacking looks like black magic at every step? From electrical signals inside the lock to the Bluetooth Low Energy (BLE) communication with a mobile application developed using a widely used software development kit (SDK), I will share my simple spells that has led me to find vulnerabilities impacting tens of thousands of smart devices from multiple manufacturers. That and why never giving up can pay off!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Open Source API Security for devsecops

When: Saturday, Aug 12, 13:00 - 14:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 3 - [Map](#)

Speakers: Ankita Gupta, Ankush Jain

SpeakerBio: Ankita Gupta

Ankita is the co-founder and CEO of Akto.io. Prior to Akto she has experience working in VMware, LinkedIn and JP Morgan. She holds MBA from Dartmouth College and Bachelors in Technology from IIT Roorkee.

Twitter: [@ankitaitr](#)

SpeakerBio: Ankush Jain

Ankush is the co-founder & CTO at Akto (<https://www.akto.io>). Prior to starting Akto he worked at CleverTap as VP of Engineering. He has also worked for 5 years as a Quant at Morgan Stanley. He has acquired US patents at Microsoft at CleverTap.

Twitter: [@Ankush12389](#)

Description:

We want to present in Arsenal. Akto is an open source API Security product. During the session, we will showcase how to:

1. Automate your API inventory and generate open API spec file
2. We will teach how to write custom test for security testing with live demo of 20+ custom business logic tests.
3. Automate API security testing in CI/CD with GitHub Actions as an example

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Open Source Intelligence (OSINT) for Hackers

When: Friday, Aug 11, 14:00 - 15:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 3 - [Map](#)

Speakers: Lee McWhorter, Sandra Stibbards

SpeakerBio: Lee McWhorter

No BIO available

Twitter: [@tleemcjr](#)

SpeakerBio: Sandra Stibbards

No BIO available

Twitter: [@Camelotinv](#)

Description:

The Open Source Intelligence (OSINT) for Hackers workshop, as part of the Red Team Village, provides extensive information and hands on lessons relating to surface and deep web searching along with advanced online search techniques & strategies, online privacy / anonymity tools, counterintelligence techniques used by the criminal element, search techniques of blogs and social networks including social media monitoring, utilize database systems, methods to obtain historical website pages, develop previous domain & website details that no longer exist, geolocating, reverse imaging, transfer of large files, screenshot capabilities, and much more all focused on helping Hackers related to threat hunting, red teaming and information gathering.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Open Source Intelligence (OSINT) for Hackers

When: Saturday, Aug 12, 09:00 - 10:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 4 - [Map](#)

Speakers: Lee McWhorter, Sandra Stibbards

SpeakerBio: Lee McWhorter

No BIO available

Twitter: [@tleemcjr](#)

SpeakerBio: Sandra Stibbards

No BIO available

Twitter: [@Camelotinv](#)

Description:

The Open Source Intelligence (OSINT) for Hackers workshop, as part of the Red Team Village, provides extensive information and hands on lessons relating to surface and deep web searching along with advanced online search techniques & strategies, online privacy / anonymity tools, counterintelligence techniques used by the criminal element, search techniques of blogs and social networks including social media monitoring, utilize database systems, methods to obtain historical website pages, develop previous domain & website details that no longer exist, geolocating, reverse imaging, transfer of large files, screenshot capabilities, and much more all focused on helping Hackers related to threat hunting, red teaming and information gathering.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MIV - Friday - 10:00-10:30 PDT

Title: Opening Session of MisinfoVillage 2023

When: Friday, Aug 11, 10:00 - 10:30 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Misinformation Village Staff

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: OpenQuantum: open-source hardware for quantum engineering via trapped atoms

When: Saturday, Aug 12, 14:00 - 14:59 PDT


Where: LINQ - 3rd flr - Quantum Village - [Map](#)

SpeakerBio:Max Shirokawa Aalto

No BIO available

Description:

Almost all existing tutorials in the applied quantum world are focused on quantum programming languages & how to interact with a QPU – until now. OpenQuantum is a fully open-source, mostly 3D printable blueprint for a hardware platform that allows for the cooling, trapping and manipulation of rubidium atoms, an ideal platform for quantum engineering. This workshop will cover the history of the field, the operational principles of the apparatus, and technical details on the open-source devices we have designed to make this science more accessible.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: OpenSSF Scorecard

When: Friday, Aug 11, 14:00 - 15:55 PDT

Where: Caesars Forum - Caucus Boardroom - Demo Labs - [Map](#)

Speakers:Naveen Srinivasan,Neil Naveen

SpeakerBio:Naveen Srinivasan

Naveen Srinivasan is a contributor and maintainer of multiple <http://github.com/ossf/> projects, a member and contributor to the <http://github.com/sigstore> organization. His contributions have earned him recognition with Google Peer Bonus awards in 2021 <https://twitter.com/snaveen/status/1422921438764453897> and 2022

<https://twitter.com/snaveen/status/1563194155333222400>. He has consistently contributed to the open-source community for an extended period, with no gaps in activity for the past two years. In addition to his technical contributions, He is a sought-after speaker at conferences, discussing topics related to supply chain security and mitigating risks in open-source software. He can be found on Twitter (@Naveen_Srini) at https://twitter.com/Naveen_Srini_


Twitter: [@Naveen_Srini_](#)

SpeakerBio:Neil Naveen

Neil Naveen is an 8th grader in the US who is passionate about jiu-jitsu, solving Leetcode puzzles, and book author. OSS contributor.

Description:

Introducing Scorecard, an innovative open-source tool designed to secure the software supply chain by scanning over 1.2 million GitHub repositories for potential security risks. Scorecard automates the process of evaluating a project's adherence to security best practices, assigning a score based on the results. The scores and detailed analysis are readily accessible via a comprehensive API (<https://api.securityscorecards.dev>), empowering developers to easily integrate security checks into their workflows. Additionally, Scorecard provides a CLI for individual use and a GitHub action that allows repository owners to continuously monitor and improve their project's security posture. Whether you're a seasoned developer or an open-source enthusiast, Scorecard gives you the power to make the software supply chain safer for everyone.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Friday - 14:00-14:50 PDT

Title: Orbiting the White House: Cybersecurity as a Space Imperative

When: Friday, Aug 11, 14:00 - 14:50 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Speakers:Lauryn Williams,Tanya Simms

SpeakerBio:Lauryn Williams

No BIO available

SpeakerBio:Tanya Simms

No BIO available

Description:

Due to current and emerging threats in the space ecosystem, notably from the recent and ongoing war in Ukraine and even US GPS related outages, space is front and center as both an industry of intense innovation and imperative for civil, military, and commercial growth. It is often the case, that existing cybersecurity policies and frameworks do not apply to space systems. In this presentation, we hope to illuminate the current gaps in such policies and offer ways that the audience can help.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: OSINT for Physical Security Intelligence

When: Friday, Aug 11, 12:00 - 12:50 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

Speakers: Chet Hosmer, Mike Raggo

SpeakerBio: Chet Hosmer

Chet Hosmer is an international author, educator, researcher, and founder of Python Forensics, Inc., a non-profit research institute focused on the collaborative development of open source investigative technologies using the Python programming language. Chet is also a Visiting Professor at Utica College in the Cybersecurity Graduate Program, where his research and teaching is focused on data hiding, active cyber defense and security of industrial control systems. Additionally, Chet is an Adjunct Professor at Champlain College in the Digital Forensics Graduate Program, where his research and teaching is focused on solving hard digital investigation problems using the Python programming language.

SpeakerBio: Mike Raggo

Michael T. Raggo has over 30 years of security research experience. During this time, he has uncovered and ethically disclosed vulnerabilities in products including Samsung, Checkpoint, and Netgear. Michael is the author of "Mobile Data Loss: Threats & Countermeasures" and "Data Hiding" for Syngress Book. He is also a frequent presenter at security conferences, including Black Hat, DEF CON, Gartner, RSA, DoD Cyber Crime, OWASP, SANS. He was also awarded the Pentagon's Certificate of Appreciation.

Description:

Organizations seek rapid intelligence about critical situations that impact their teams, locations, or assets. Yet when it comes to OSINT we find organizations performing Open Source Information gathering; wasting time sifting through data to get to the actionable intelligence. In this presentation we demonstrate how to collect curated data and eliminate 99% of the time spent on reliminary data analysis. Furthermore, all of this data can be combined to perform trending and predictive analysis for natural disasters, geo-political situations, or business risk. The goal is to provide attendees with ideas for formulating new approaches for physical security OSINT.

[Return to Index](#) - Add to  - ics [Calendar](#) file

RCV - Saturday - 10:45-11:30 PDT

Title: OSINT Privacy Unmasked: Taking Control of Your Digital Footprint in a Hyper-Connected World

When: Saturday, Aug 12, 10:45 - 11:30 PDT


Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio: Zoey Selman

No BIO available

Twitter: [@v3rbaal](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

RCV - Friday - 10:50-11:35 PDT

Title: OSINT Situational Awareness

When: Friday, Aug 11, 10:50 - 11:35 PDT


Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio: Joe Gray

No BIO available

Twitter: [@C_3PJoe](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: OSINT Skills Lab Challenge

When: Friday, Aug 11, 12:00 - 12:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 3 - [Map](#)

Speakers: Lee McWhorter, Sandra Stibbards

SpeakerBio: Lee McWhorter

No BIO available

Twitter: [@tleemcjr](#)

SpeakerBio: Sandra Stibbards

No BIO available

Twitter: [@Camelotinv](#)

Description:

Welcome to the Open Source Intelligence Skills Lab Challenge CTF! There are 3 challenge sets, each with their own challenges. As you progress through each set, the difficulty will progressively increase. Answering a "flag" correctly will net you points, with a maximum possible score of 560.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: OSINT Skills Lab Challenge

When: Saturday, Aug 12, 15:00 - 15:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 3 - [Map](#)

Speakers: Lee McWhorter, Sandra Stibbards

SpeakerBio: Lee McWhorter

No BIO available

Twitter: [@tleemcjr](#)

SpeakerBio: Sandra Stibbards

No BIO available

Twitter: [@Camelotinv](#)

Description:

Welcome to the Open Source Intelligence Skills Lab Challenge CTF! There are 3 challenge sets, each with their own challenges. As you progress through each set, the difficulty will progressively increase. Answering a "flag" correctly will net you points, with a maximum possible score of 560.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: OSINT Skills Lab Challenge

When: Saturday, Aug 12, 16:00 - 16:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 3 - [Map](#)

Speakers: Lee McWhorter, Sandra Stibbards

SpeakerBio: Lee McWhorter

No BIO available

Twitter: [@tleemcjr](#)

SpeakerBio: Sandra Stibbards

No BIO available

Twitter: [@Camelotinv](#)

Description:

Welcome to the Open Source Intelligence Skills Lab Challenge CTF! There are 3 challenge sets, each with their own challenges. As you progress through each set, the difficulty will progressively increase. Answering a "flag" correctly will net you points, with a maximum possible score of 560.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: OSINT Skills Lab Challenge

When: Sunday, Aug 13, 11:00 - 11:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 1 - [Map](#)

Speakers: Lee McWhorter, Sandra Stibbards

SpeakerBio: Lee McWhorter

No BIO available

Twitter: [@tleemcjr](#)

SpeakerBio: Sandra Stibbards

No BIO available

Twitter: [@Camelotinv](#)

Description:

Welcome to the Open Source Intelligence Skills Lab Challenge CTF! There are 3 challenge sets, each with their own challenges. As you progress through each set, the difficulty will progressively increase. Answering a "flag" correctly will net you points, with a maximum possible score of 560.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: OSINT Skills Lab Challenge

When: Friday, Aug 11, 13:00 - 13:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 3 - [Map](#)

Speakers: Lee McWhorter, Sandra Stibbards

SpeakerBio: Lee McWhorter

No BIO available

Twitter: [@tleemcjr](#)

SpeakerBio: Sandra Stibbards

No BIO available

Twitter: [@Camelotinv](#)

Description:

Welcome to the Open Source Intelligence Skills Lab Challenge CTF! There are 3 challenge sets, each with their own challenges. As you progress through each set, the difficulty will progressively increase. Answering a "flag" correctly will net you points, with a maximum possible score of 560.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Friday - 15:30-15:59 PDT

Title: OT Vulnerability analysis methodology

When: Friday, Aug 11, 15:30 - 15:59 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio:Jeonghoon Bae

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: OT: Why OT Cybersecurity Engineers Drink So Much

When: Friday, Aug 11, 13:30 - 14:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Main Stage - [Map](#)

SpeakerBio:ThatDeadGuy

After thirteen years as a controls engineer within the Automotive Manufacturing and Oil & Gas Exploration Manufacturing industries, ThatDeadGuy was converted over to cyber security. His experience on the design and implementation of the equipment gave him a perspective into the OT realm that was not shared with most of the security team. Over the last five years he has built up cyber security architectures, implemented detection tools and created the IR processes for multiple critical infrastructure process environments.

Description:

A brief view into the odd world of Operational Technology (OT) and why so many OT Security Engineers drink like they hate themselves. This will cover the realities of their tech stack, business risk considerations, control systems recovery and how incident response is conducted within the environment. We will briefly cover how this environment was emulated for the Project Obsidian attack chain and how it differs from the physical environments.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Over the Air, Under the Radar: Attacking and Securing the Pixel Modem

When: Friday, Aug 11, 13:00 - 13:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers: Eugene Rodionov, Farzan Karimi, Xiling Gong, Xuan Xing

SpeakerBio: Eugene Rodionov , Security Researcher on the Android Red Team at Google

Eugene Rodionov, PhD, is a Security Researcher at Google on the Android Red Team. In his current position, Eugene focuses on finding and exploiting vulnerabilities in the low-level components of Android platform and Pixel devices. Prior to that, Rodionov performed offensive security research on UEFI firmware for Client Platforms at Intel, and ran internal research projects and performed in-depth analysis of complex threats at ESET. His fields of interest include reverse engineering, vulnerability analysis, firmware security and anti-rootkit technologies. Rodionov is a co-author of the "Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats" book and has spoken at security conferences such as Black Hat, REcon, ZeroNights, and CARO.

SpeakerBio: Farzan Karimi , Android Offensive Security Manager at Google

Farzan Karimi has over 15 years experience in offensive security. He is the Android Offensive Security Manager at Google. In this role, he manages red team operations targeting low-level components within the Android ecosystem. Farzan has specialized in exploiting game development consoles (devkits). His work on PlayStation and Xbox led to the development of key security features for next generation platforms. Farzan is a speaker at security conferences such as Black Hat USA, LABSCON, Microsoft STRIKE, and EA Team Blue.

SpeakerBio: Xiling Gong , Security Researcher on the Android Red Team at Google

Xiling Gong is a Security Researcher at Google on the Android Red Team. Xiling focuses on finding and exploiting vulnerabilities in the low-level components of Android platform and Pixel devices. Xiling is the speaker of CanSecWest 2018, BlackHat USA 2019, Def Con 27, BlackHat Asia 2021.

SpeakerBio: Xuan Xing , Tech Lead on the Android Red Team at Google

Xuan Xing is the tech lead of the Android Red Team at Google. For the past years, Xuan focused on finding security vulnerabilities in various low level components of Android/Pixel devices. He is passionate about software fuzzing for security research. In BlackHat USA 2022 Xuan presented the “Google Reimagined a Phone. It was Our Job to Red Team and Secure it” talking about Pixel ABL security auditing.

Description:

To ensure Google Pixel devices are always at their most secure, the Android Red Team continuously attacks the riskiest areas of the phone. This allows us to proactively get ahead of bugs and protect the phone, before it’s even shipped to users.

The modem — or baseband — is considered a fundamental component of smartphones, and is at high risk because it is a privileged system component that accepts data from an untrusted remote source (cell towers). A vulnerability in the modem exposes end-users to scalable attacks carried out remotely, which may lead to many kinds of compromise on a phone.

Modem security is currently a hot topic of research, attracting growing interest from security researchers, both in the industry and in academia. This wasn’t the case up until recently for a couple of reasons: most modem code is closed source, and testing it requires expensive hardware equipment. With some of these barriers being removed in recent years, due the invention of software-defined radio (SDR) devices and public toolkits, the entry level into baseband security analysis has become more affordable. In this session the Android Red Team will be describing some findings from its offensive evaluation of modems used in Pixel devices.

Title: OWASP crAPI: Completely Ridiculous API

When: Friday, Aug 11, 14:00 - 15:55 PDT

Where: Caesars Forum - Accord Boardroom - Demo Labs - [Map](#)

Speakers:Jayesh Ahire,Roshan Piyush

SpeakerBio:Jayesh Ahire

Jayesh Ahire is a passionate security professional and open-source contributor with a strong background in application and API security. They have experience working with numerous organizations to design and implement secure API architectures and integrate security practices into their development processes. Jayesh has been actively involved in the OWASP community and enjoys sharing their knowledge through presentations, workshops, and mentorship.

SpeakerBio:Roshan Piyush

Roshan Piyush is Security Research Engineer, solving API Security using the powers of Machine Learning and Distributed Tracing. He has 8+ years of research experience mainly focusing on API Security for the last 5+ years. He loves building security stacks, tools, and solutions. He is also a core member of the Owasp Coraza WAF team and a leader of the Owasp crAPI project.

Description:

OWASP crAPI is an intentionally vulnerable API designed to teach and demonstrate common API security flaws. It serves as a playground for security enthusiasts, developers, and penetration testers to learn about API vulnerabilities and practice exploiting them in a safe environment. This Demo Lab will showcase the use of crAPI for educational purposes, including how to set it up, identify vulnerabilities, and apply secure API development best practices.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Friday - 09:00-17:59 PDT

Title: Packet Detective

When: Friday, Aug 11, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Ready to upgrade your skills at the Packet Hacking Village? It's time to play Packet Detective. A step up in difficulty from Packet Investigator, Packet Detective will test your network hunting abilities at the intermediate level. Come learn some new tricks!

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Sunday - 09:00-12:59 PDT

Title: Packet Detective

When: Sunday, Aug 13, 09:00 - 12:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Ready to upgrade your skills at the Packet Hacking Village? It's time to play Packet Detective. A step up in difficulty from Packet Investigator, Packet Detective will test your network hunting abilities at the intermediate level. Come learn some new tricks!

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Saturday - 09:00-17:59 PDT


Title: Packet Detective

When: Saturday, Aug 12, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Ready to upgrade your skills at the Packet Hacking Village? It's time to play Packet Detective. A step up in difficulty from Packet Investigator, Packet Detective will test your network hunting abilities at the intermediate level. Come learn some new tricks!

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Friday - 09:00-17:59 PDT


Title: Packet Inspector

When: Friday, Aug 11, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

New to packet-fu? Don't know a pcap from a bottle cap? Packet Inspector is the game for you! We provide the laptops and all necessary tools for you to learn the basics of network analysis, sniffing, and forensics.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Sunday - 09:00-13:59 PDT

Title: Packet Inspector

When: Sunday, Aug 13, 09:00 - 13:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

New to packet-fu? Don't know a pcap from a bottle cap? Packet Inspector is the game for you! We provide the laptops and all necessary tools for you to learn the basics of network analysis, sniffing, and forensics.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Saturday - 09:00-17:59 PDT

Title: Packet Inspector

When: Saturday, Aug 12, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

New to packet-fu? Don't know a pcap from a bottle cap? Packet Inspector is the game for you! We provide the laptops and all necessary tools for you to learn the basics of network analysis, sniffing, and forensics.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Panel Discussion - Bugs, Bounties, & Breaches - Insider Tales from the Trenches

When: Saturday, Aug 12, 10:00 - 10:45 PDT

Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio: Jason Haddix , CISO and “Hacker in Charge” at BuddoBot

Jason Haddix is the CISO and “Hacker in Charge” at BuddoBot, a world-class adversary emulation consultancy. He's had a distinguished 15-year career in cybersecurity previously serving as the CISO of Ubisoft, Head of Trust/Security/Operations at Bugcrowd, Director of Penetration Testing at HP, and Lead Penetration Tester at Redspin. He has also held positions doing mobile penetration testing, network/infrastructure security assessments, and static analysis. Jason is a hacker and bug hunter to the core, and he is ranked 51st all-time on Bugcrowd's leaderboards. Currently, he specializes in recon and web application analysis. Jason has also authored many talks on offensive security methodology, including speaking at cons such as; DEF CON, Black Hat, OWASP, RSA, Nullcon, SANS, IANS, BruCon, Toorcon, and many more. Jason currently lives in Colorado with his wife and three children.

Twitter: [@jhaddix](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Saturday - 13:30-14:59 PDT

Title: Panel Discussion -- Designing and Deploying NOC/SOC in a Mobile, Limited Bandwidth Maritime Environment

When: Saturday, Aug 12, 13:30 - 14:59 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

Speakers:Brad Proctor,Cliff Neve,Danny Joslin,Peter Dreyer,Tom Stites

SpeakerBio:Brad Proctor

No BIO available

SpeakerBio:Cliff Neve , US Coast Guard

CDR Cliff Neve is a retired Coast Guard Commander whose assignments included Chief of Staff at Coast Guard Cyber Command, Deputy Chief Information Officer at the White House Communications Agency, and Assistant C4ISR Program Manager for the Coast Guard's multi billion dollar recapitalization program. Since retiring from the Coast Guard in 2013, CDR Neve has led all manner of cyber security assessments and security architecture consulting for diverse clients that include Ports and Waterways, Wall Street firms, Fortune 100 companies, banks, hospitals, and defense agencies. CDR Neve is a Certified Information Systems Security Professional (CISSP) and Project Management Professional (PMP).

SpeakerBio:Danny Joslin

No BIO available

SpeakerBio:Peter Dreyer

No BIO available

SpeakerBio:Tom Stites

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Panel: Hacker Court - Interactive Scenario

When: Sunday, Aug 13, 14:00 - 15:15 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

SpeakerBio: winn0na , Hacker at Policy @DEFCON

winn0na is a former threat analyst turned policy professional. She has organized policy content at DEFCON and has authored multiple pieces on offensive cyber capability proliferation. She will be facilitating the Mock trial as some of the brightest lawyers in cyber (names to be released) take the stage.

Description:

Be a member of the jury as two lawyers prosecute and defend a hacker (live on the stand) in a made up scenario. You, the audience, will decide if the hacker was caught in the act, or if the attribution was all a false flag. Learn through the trial what evidence you don't want to leave behind in an op, what D&R can and should collect, and how criminals who conduct cybercrime actually get prosecuted.

REFERENCES:

<https://www.cnet.com/tech/services-and-software/use-cnet-shopping-to-look-out-the-best-deals/>

<https://www.steptoecyberblog.com/files/2012/11/ccmanual1.pdf>

https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/03/26/forensics_chart.pdf

<https://www.justice.gov/archives/opa/blog/important-court-opinion-holds-lawful-warrants-can-be-used-obtain-evidence-us-internet>

<https://www.19thcircuitcourt.state.il.us/1610/Guide-to-Conducting-Mock-Trials>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Sunday - 09:00-12:59 PDT

Title: Password Lab

When: Sunday, Aug 13, 09:00 - 12:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

In this workshop, you'll learn real-world penetration testing techniques for guessing passwords using Hydra, xHydra, and Hashcat.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Friday - 09:00-17:59 PDT


Title: Password Lab

When: Friday, Aug 11, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

In this workshop, you'll learn real-world penetration testing techniques for guessing passwords using Hydra, xHydra, and Hashcat.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Saturday - 09:00-17:59 PDT


Title: Password Lab

When: Saturday, Aug 12, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

In this workshop, you'll learn real-world penetration testing techniques for guessing passwords using Hydra, xHydra, and Hashcat.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWV - Saturday - 10:00-17:59 PDT

Title: Password Village Activities

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 236 - Password Village - [Map](#)

Description:

The Password Village provides training, discussion, and hands-on access to hardware and techniques utilized in modern password cracking, with an emphasis on how password cracking relates to your job function and the real world . No laptop? No problem! Feel free to use one of our terminals to access a pre-configured GPGPU environment to run password attacks against simulated real-world passwords. Village staff and expert volunteers will be standing by to assist you with on-the-spot training and introductions to Hashcat, as well as other FOSS cracking applications.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWV - Friday - 10:00-17:59 PDT

Title: Password Village Activities

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 236 - Password Village - [Map](#)

Description:

The Password Village provides training, discussion, and hands-on access to hardware and techniques utilized in modern password cracking, with an emphasis on how password cracking relates to your job function and the real world . No laptop? No problem! Feel free to use one of our terminals to access a pre-configured GPGPU environment to run password attacks against simulated real-world passwords. Village staff and expert volunteers will be standing by to assist you with on-the-spot training and introductions to Hashcat, as well as other FOSS cracking applications.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWV - Sunday - 10:00-13:59 PDT

Title: Password Village Activities

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Summit - 236 - Password Village - [Map](#)

Description:

The Password Village provides training, discussion, and hands-on access to hardware and techniques utilized in modern password cracking, with an emphasis on how password cracking relates to your job function and the real world . No laptop? No problem! Feel free to use one of our terminals to access a pre-configured GPGPU environment to run password attacks against simulated real-world passwords. Village staff and expert volunteers will be standing by to assist you with on-the-spot training and introductions to Hashcat, as well as other FOSS cracking applications.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Passwords Argh Us

When: Saturday, Aug 12, 11:00 - 11:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 3 - [Map](#)

SpeakerBio:Traveler

No BIO available

Description:

The workshop is designed to provide attendees with comprehensive knowledge and hands-on experience in the realm of offensive security. In today's digital landscape, where passwords remain a significant line of defense for organizations, understanding their vulnerabilities is crucial for both offensive and defensive purposes. This workshop aims to equip participants with the skills required to identify weak passwords, crack hashes, and perform credential-based attacks effectively.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Passwords Argh Us

When: Sunday, Aug 13, 10:00 - 10:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 3 - [Map](#)

SpeakerBio:Traveler

No BIO available

Description:

The workshop is designed to provide attendees with comprehensive knowledge and hands-on experience in the realm of offensive security. In today's digital landscape, where passwords remain a significant line of defense for organizations, understanding their vulnerabilities is crucial for both offensive and defensive purposes. This workshop aims to equip participants with the skills required to identify weak passwords, crack hashes, and perform credential-based attacks effectively.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Passwords Argh Us

When: Friday, Aug 11, 16:00 - 16:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 4 - [Map](#)

SpeakerBio:Traveler

No BIO available

Description:

The workshop is designed to provide attendees with comprehensive knowledge and hands-on experience in the realm of offensive security. In today's digital landscape, where passwords remain a significant line of defense for organizations, understanding their vulnerabilities is crucial for both offensive and defensive purposes. This workshop aims to equip participants with the skills required to identify weak passwords, crack hashes, and perform credential-based attacks effectively.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Passwords Argh Us

When: Saturday, Aug 12, 09:00 - 09:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 3 - [Map](#)

SpeakerBio:Traveler

No BIO available

Description:

The workshop is designed to provide attendees with comprehensive knowledge and hands-on experience in the realm of offensive security. In today's digital landscape, where passwords remain a significant line of defense for organizations, understanding their vulnerabilities is crucial for both offensive and defensive purposes. This workshop aims to equip participants with the skills required to identify weak passwords, crack hashes, and perform credential-based attacks effectively.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Pasteur - A C++ library to eliminate injections

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 3 - [Map](#)

SpeakerBio: Yariv Tal

Senior developer turned security researcher, with 4 decades of programming experience, university lecturing and mentoring at bootcamps, he has a fresh look at the world of security, as an outsider looking in.

Twitter: [@YarivDevMentor](#)

Description:

Enables forwarding mixed trusted/untrusted concatenated data that can be sanitized at the point of use, when the sanitization requirements are known, instead of at the point of input.

Examples:

With Pasteur this classic sql injection code `sql << pstr / "select email from demo.useremails where username = " + name + " and type=" + emailType;` is *automatically* converted into a parameterized sql query

This os injection code

```
System(pstr / "ping " + hostname)
```

automatically sanitizes the hostname parameter.

See more at <https://github.com/SecureFromScratch/pasteur>

[Return to Index](#) - Add to  - ics [Calendar](#) file

MIV - Saturday - 12:30-13:30 PDT

Title: Patient Zero Day: The Leaking of Patients' Private Health Data Contributed To A Medical Infodemic

When: Saturday, Aug 12, 12:30 - 13:30 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Andrea Downing

No BIO available

Description:

Andrea Downing and Eric Perakslis co-published evidence of health data leaking illegally from medical institutions via cross-site trackers such as Meta Pixel. Since publication, follow-up investigations have uncovered a historic data breach currently at 61 million patients and counting as of May 2023. This research has catalyzed unprecedented enforcement of the Health Breach Notification Rule by the Federal Trade Commission, and is now expanding to show whether health tech companies and clinical sites are complying with the law.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PYV - Saturday - 11:00-17:59 PDT

Title: Payment Village Challenges/CTF

When: Saturday, Aug 12, 11:00 - 17:59 PDT

Where: Flamingo - Virginia City - Payment Village - [Map](#)

Description:

We have three challenges this year!

1. A CTF for which there is no equipment is required.
2. Card Hacking Challenge for which you will need an Android phone with NFC and a special Card Hacking Challenge card (grab one on the booth):
3. Easter egg hunt. Use your brain!

We have a tonne of cool prizes to be won, such as custom mugs, numbered challenge coins with atc numbers, key rings, embroidered patches and more!

[Return to Index](#) - Add to  - ics [Calendar](#) file

PYV - Friday - 11:00-17:59 PDT

Title: Payment Village Challenges/CTF

When: Friday, Aug 11, 11:00 - 17:59 PDT

Where: Flamingo - Virginia City - Payment Village - [Map](#)

Description:

We have three challenges this year!

1. A CTF for which there is no equipment is required.
2. Card Hacking Challenge for which you will need an Android phone with NFC and a special Card Hacking Challenge card (grab one on the booth):
3. Easter egg hunt. Use your brain!

We have a tonne of cool prizes to be won, such as custom mugs, numbered challenge coins with atc numbers, key rings, embroidered patches and more!

[Return to Index](#) - Add to  - ics [Calendar](#) file

PYV - Sunday - 10:00-13:59 PDT

Title: Payment Village Challenges/CTF

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Flamingo - Virginia City - Payment Village - [Map](#)

Description:

We have three challenges this year!

1. A CTF for which there is no equipment is required.
2. Card Hacking Challenge for which you will need an Android phone with NFC and a special Card Hacking Challenge card (grab one on the booth):
3. Easter egg hunt. Use your brain!

We have a tonne of cool prizes to be won, such as custom mugs, numbered challenge coins with atc numbers, key rings, embroidered patches and more!

[Return to Index](#) - Add to  - ics [Calendar](#) file

PYV - Friday - 11:00-12:30 PDT

Title: Payment Village Workshop

When: Friday, Aug 11, 11:00 - 12:30 PDT

Where: Flamingo - Virginia City - Payment Village - [Map](#)

SpeakerBio: Leigh-Anne Galloway

No BIO available

Twitter: [@L_Agalloway](#)

Description:

We have a simple mission, educate the world about payments. We all interact with payment technologies every day, yet how much do we know about them? This is a beginner's course in card payments. This workshop is also helpful for anyone who tries to solve our CTF.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PYV - Saturday - 11:00-12:30 PDT

Title: Payment Village Workshop

When: Saturday, Aug 12, 11:00 - 12:30 PDT

Where: Flamingo - Virginia City - Payment Village - [Map](#)

SpeakerBio: Leigh-Anne Galloway

No BIO available

Twitter: [@L_Agalloway](#)

Description:

We have a simple mission, educate the world about payments. We all interact with payment technologies every day, yet how much do we know about them? This is a beginner's course in card payments. This workshop is also helpful for anyone who tries to solve our CTF.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Pcapinator: Rise of the PCAP Machines

When: Saturday, Aug 12, 12:00 - 13:55 PDT

Where: Caesars Forum - Unity Boardroom - Demo Labs - [Map](#)

Speakers: Henry Hill, Mike "d4rkm4tter" Spicer

SpeakerBio: Henry Hill

Henry Hill is an expert with computer hardware and is able to design and build the most bleeding edge systems that are the fastest in the world. His internal knowledge of architecture and system bottlenecks help him build systems capable of extreme processing and even faster storage. Henry is also an expert with mechanical engineering and fabrication. When his modifications aren't appearing in d4rkm4tter's projects, they can be seen in his race car at the track.

SpeakerBio: Mike "d4rkm4tter" Spicer

Mike Spicer, known as d4rkm4tter, is a cybersecurity expert and innovative hacker with an affinity for pushing the boundaries of both hardware and software. With an unquenchable curiosity for all things wireless, Mike's passions have propelled him to build and explore much of the wireless spectrum. Armed with a degree in computer science, Mike has harnessed his skills to build and break a diverse range of systems. His expertise covers web application penetration testing, wireless monitoring and tracking, and reverse engineering. As the designer of the renowned #WiFiCactus, Mike has brought his projects from idea to reality in the cybersecurity world. His unique take on wireless has garnered significant attention, where he has presented and demonstrated his work at conferences such as BlackHat, DEF CON and others around the world.

Description:

Pcapinator is a powerful and versatile network analysis tool that combines the strengths of TShark and Python to provide comprehensive and efficient packet deconstruction into a format usable for further analysis. Inspired by the Terminator, Pcapinator is designed to relentlessly analyze, decode, and filter network packets using all of the resources a system makes available to it, making it a formidable asset for diving deep into PCAPs. Leveraging the robust capabilities of Wireshark's TShark tool, Pcapinator parses and extracts vital information from pcap files, while Python's extensive libraries and scripts offer advanced processing and automation options. Pcapinator is built to handle extremely large PCAP files, search for anomalies in those files, and uncover the hard-to-find information in network traffic, making it an essential tool for PCAP analysis.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Friday - 17:00-17:50 PDT

Title: Pen Test Partners Power Hour

When: Friday, Aug 11, 17:00 - 17:50 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Speakers: Alex Lomas, Ken Munro

SpeakerBio: Alex Lomas

No BIO available

SpeakerBio: Ken Munro

No BIO available

Description:

Pen Test Partners invites you to pull up a free beer and join us for further adventures in hacking electronic flight bags (EFBs), and then a fun rant at terrible aviation hacking in the movies to close the first day at the aerospace village.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Pentesting Industrial Control Systems: OCP-U-HACK (Pre-Registration Required)

When: Thursday, Aug 10, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers: Alexandrine Torrents, Arnaud Soullié

SpeakerBio: Alexandrine Torrents, Cybersecurity Expert at Wavestone

Alexandrine Torrents is a cybersecurity expert at Wavestone. She started as a penetration tester, and performed several cybersecurity assessments on ICS. She worked on a few ICS models to demonstrate attacks on PLCs and developed a particular tool to request Siemens PLCs. Then, she started working at securing ICS, especially in the scope of the French military law, helping companies offering a vital service to the nation to comply with security rules. Now, Alexandrine works with different industrial CISOs on their cybersecurity projects: defining secure architectures, hardening systems, implementing detection mechanisms. She is also IEC 62443 certified and still performs assessments on multiple environments.

SpeakerBio: Arnaud Soullié, Senior Manager at Wavestone

Arnaud Soullié (@arnaudsoullie) is a Senior Manager at Wavestone, a global consulting company. For 12 years, he has been performing security assessments and pentests on all types of targets. He started specializing in ICS cybersecurity 10 years ago. He spoke and taught workshops at numerous security conferences on ICS topics: BlackHat Europe, BruCon, CS3STHLM, BSides Las Vegas, DEFCON... He is also the creator of the DYODE project, an open-source data diode aimed at ICS. He has been teaching ICS cybersecurity training since 2015.

Twitter: [@arnaudsoullie](#)

Description:

Let's capture the flag, literally! In this workshop you'll participate in an engaging CTF during which you'll take control of a robotic arm to capture a real flag on a model train!

To do so, we'll start with an introduction to Industrial Control Systems to discover the specific components, the network architectures, and even program a PLC simulator.

We'll then discover some ICS-specific protocols, with a focus on OPC-UA, a modern ICS protocol.

Finally, you'll connect to our ICS setup composed of real ICS hardware and software and compete against other attendees to capture the flags with robotic hands!

Skill Level: Beginner

Prerequisites for students:

- No specific knowledge is required

Materials or Equipment students will need to bring to participate: - Students should have a laptop capable of running 64-bits virtual machines

[Return to Index](#) - Add to  - [ics Calendar](#) file

Title: Per-mission Impossible: Exploring the Android Permission Model and Intents

When: Saturday, Aug 12, 15:00 - 16:59 PDT

Where: Flamingo - Savoy - AppSec Village - Workshop - [Map](#)

Speakers: Miłosz Gaczkowski, William Taylor

SpeakerBio: Miłosz Gaczkowski

Miłosz is a mobile security specialist at WithSecure, having previously spent entirely too much time working in academia

His work revolves around mobile security. Outside of technical work, his interests are in education and the culture of education

Twitter: [@cyberMilosz](#)

SpeakerBio: William Taylor

Security consultant with an interest in mobile security supported by a background in embedded mobile engineering. I used to make them work; now I break them, professionally and ethically.

Description:

The way in which Android applications talk to each other is often misunderstood, and it is entirely too common to see apps whose sensitive functionality is completely open to anyone who asks nicely.

This workshop will cover several case studies of overly permissive apps/devices found in the wild, including an OEM's voice recorder application that could be made to start and stop voice recordings without the user's knowledge.

We will go over common implementation flaws, play around with exploiting them from the perspective of an unprivileged application, and explore how an understanding of Android permissions could help us avoid these mistakes.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Saturday - 10:00-17:59 PDT

Title: Perform Memory Extraction, Emulation and Shellcode

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Want to put your MIPS shellcode skills to the test for a chance to win a prize? Learn to dump flash from our custom-built PCB that we use to teach our Hardware Hacking Workshop. Hone your dynamic analysis skills and exploit a WPS pin generation algorithm used in a popular Real Time Operating System.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Sunday - 10:00-13:59 PDT

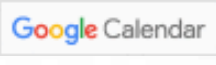
Title: Perform Memory Extraction, Emulation and Shellcode

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Want to put your MIPS shellcode skills to the test for a chance to win a prize? Learn to dump flash from our custom-built PCB that we use to teach our Hardware Hacking Workshop. Hone your dynamic analysis skills and exploit a WPS pin generation algorithm used in a popular Real Time Operating System.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Friday - 10:00-17:59 PDT


Title: Perform Memory Extraction, Emulation and Shellcode

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Want to put your MIPS shellcode skills to the test for a chance to win a prize? Learn to dump flash from our custom-built PCB that we use to teach our Hardware Hacking Workshop. Hone your dynamic analysis skills and exploit a WPS pin generation algorithm used in a popular Real Time Operating System.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Phishing with Dynamite: Harnessing AI to Supercharge Offensive Operations

When: Saturday, Aug 12, 17:00 - 17:30 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Speakers: Dani Goland, Preston Thornburg

SpeakerBio: Dani Goland

At the age of 20, Dani Goland founded his own boutique company for innovative software and hardware solutions. Dani did not neglect his hands-on capabilities in both making and breaking systems. Dani spoke at numerous cybersecurity conferences such as BlackHat USA, CodeBlue Japan, CONFidence, SEC-T, and more. After serving in the IDF as a commander of a Field Intelligence unit, Dani went on an 8-month journey across South America. He loves snowboarding, and music concerts.

Twitter: [@danigoland](#)

SpeakerBio: Preston Thornburg

Preston is the co-founder of Upshield, a full-stack web3 security platform. Much of his research focuses on the automated identification of adversaries throughout the Ethereum and broader cryptocurrency landscapes. He's recently launched a technical podcast, 'Mad Blocks', that deep dives into web3 projects to extract underlying risks and breakpoints. Preston's background is heavily based in offensive security, having led operations against cryptocurrency platforms, international banks, critical infrastructure, and governments.

Description:

Artificial Intelligence (AI) has fundamentally reshaped the landscape of cybersecurity, making traditional defensive strategies outdated and inadequate, particularly in the realm of phishing attacks. In this era of large language models (LLMs), phishing has evolved from flawed syntax, primitive design, and generic narratives. Using state-of-the-art AI tooling, we can now generate spear-phishing campaigns that are highly personalized with unprecedented precision, leveraging publicly available data from social media, work profiles, and more. In this talk, we'll show you how it's done. We will also delve into innovative exploitation techniques that leverage alternative communication channels, like AI-based audio deepfakes for conversational reeling. All of this is made possible with our soon to be released and open-source phishing framework – nemo. We'll give you a front-row seat to how AI is revolutionizing offensive security operations. Get ready to step into the future of phishing attacks – it's more sophisticated, more realistic, and scarier than you could ever imagine.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Physical Attacks Against Smartphones

When: Saturday, Aug 12, 11:30 - 12:15 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

SpeakerBio: Christopher Wade , Hacker

Christopher (@Iskuri1) is a seasoned security researcher. His main focuses are in reverse engineering firmware and fingerprinting USB and NFC vulnerabilities, with his key strength lying in bootloader exploitation.

Twitter: [@Iskuri1](#)

Description:

Android devices are constantly improving their security to protect against attackers with physical access, with new protection techniques being added year-by-year. This talk aims to demonstrate vulnerabilities in modern Android smartphones that are still viable, despite the mitigations in place.

In the first phase of this talk, we will discuss analysis and exploitation of vendor-customised versions of Android's Recovery mode, demonstrating weaknesses that allow for privilege escalation to root, and traversal from Recovery to Android, without Bootloader access, using nothing but a Micro SD card.

In the second phase, we will discuss weaknesses in the Secondary Bootloader of devices produced by a popular smartphone manufacturer. We will demonstrate how, using a vulnerability in the core USB stack, code execution can be achieved, and a modified Android image can be booted, without compromising the functionality of the device.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Saturday - 12:30-13:15 PDT

Title: Physical pentesting in a post-covid world

When: Saturday, Aug 12, 12:30 - 13:15 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

SpeakerBio: Brian Halbach

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Sunday - 10:00-13:59 PDT

Title: Physical Security Village Activities

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

Description:

Come join us at Carson City I and II for some hands on physical security bypass exhibits! Try your hand on bypassing elevators, deadlocks, deadlatches, shopping cart locks, building intercoms or more! Challenge yourself by trying to get out of handcuffs using only a bobby pin, and win a real police handcuff key! In addition, meet some of our external partners. You can augment yourself by injecting your hand with a mini RFID/NFC chip implant, and play around with our RFID displays! We also have returning the physical RFID wall of sheep where you can learn about long distance RFID cloning!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Physical Security Village Activities

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

Description:

Come join us at Carson City I and II for some hands on physical security bypass exhibits! Try your hand on bypassing elevators, deadlocks, deadlatches, shopping cart locks, building intercoms or more! Challenge yourself by trying to get out of handcuffs using only a bobby pin, and win a real police handcuff key! In addition, meet some of our external partners. You can augment yourself by injecting your hand with a mini RFID/NFC chip implant, and play around with our RFID displays! We also have returning the physical RFID wall of sheep where you can learn about long distance RFID cloning!

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Friday - 10:00-17:59 PDT

Title: Physical Security Village Activities

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

Description:

Come join us at Carson City I and II for some hands on physical security bypass exhibits! Try your hand on bypassing elevators, deadlocks, deadlatches, shopping cart locks, building intercoms or more! Challenge yourself by trying to get out of handcuffs using only a bobby pin, and win a real police handcuff key! In addition, meet some of our external partners. You can augment yourself by injecting your hand with a mini RFID/NFC chip implant, and play around with our RFID displays! We also have returning the physical RFID wall of sheep where you can learn about long distance RFID cloning!

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 19:00-21:59 PDT

Title: Policy Lounge

When: Saturday, Aug 12, 19:00 - 21:59 PDT

Where: Caesars Forum - Summit - 223 - Plounge - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Political Polarization

When: Saturday, Aug 12, 13:55 - 14:35 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio:Constantine Nicolaidis

Constantine Nicolaidis leads a Risk Management practice that focuses on securing U.S. privately owned critical infrastructure. Over the last decade he has leveraged his expertise in security and data-based product development to create tools for security professionals. Constantine has also spent the last five years developing a geopolitical modeling system to help forecast and describe the nature of political and social crises. He advises various security groups on the nature of modern multi-domain warfare with an emphasis on the cyber and cognitive domains. Constantine holds a Master's Degree in Human-Computer Interaction from the Carnegie Mellon School of Computer Science and is currently enrolled in the Master's in Cybersecurity Degree program at the SANS Technology Institute.

Description:

What are the root causes of today's politically charged and polarized environment? Conventional wisdom likes to point the finger at social media and middle class immiseration but is there more to the story? A few researchers were able to accurately predict the current trends toward populism and political polarization, decades ago. A new field of study that combines big data and historical analysis was created in the early 2000s. What do these perspectives have to say about the current political crisis? Our geopolitical environment has changed significantly in the last few decades as well. Authoritarian states actively seek to delegitimize democratic systems. What are their motivations and what types of vulnerabilities in the liberal democratic order might they try to exploit? Come experience a whirlwind tour of multi-model geopolitical forecasting. What do some of the most well researched and respected economic, political and historical models have to say about the current state of politics in the U.S? Have we been here before and what are the implications of these perspectives for the next election?

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Polynonce: An ECDSA Attack and Polynomial Dance

When: Saturday, Aug 12, 17:00 - 17:20 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers: Marco Macchetti, Nils Amiet

SpeakerBio: Marco Macchetti, Principal Cryptographer at Kudelski Security

Marco works as Principal Cryptographer on Kudelski Security's research team. He has a long experience designing a wide range of HW and SW cryptographic modules, from silicon roots of trust through physically unclonable functions to side-channel resistant cryptographic libraries. Marco likes looking at crypto from different points of view, bridging theory and implementation, to find new paths of attack (and defense).

SpeakerBio: Nils Amiet, Lead Prototyping Engineer at Kudelski Security

Nils is a Security Researcher on Kudelski Security's research team performing research on various topics including privacy, authentication, big data analytics, and internet scanning. He also writes blog posts on various topics for Kudelski's research blog. Nils likes open source software and has presented his research at DEF CON and Black Hat Arsenal. He was part of creating a massively distributed system for breaking RSA public keys.

Twitter: [@tmlxs](#)

Description:

ECDSA is a widely used digital signature algorithm. ECDSA signatures can be found everywhere since they are public. In this talk, we tell a tale of how we discovered a novel attack against ECDSA and how we applied it to datasets we found in the wild, including the Bitcoin and Ethereum networks.

Although we didn't recover Satoshi's private key (we'd be throwing a party on our private yacht instead of writing this abstract), we could see evidence that someone had previously attacked vulnerable wallets with a different exploit and drained them. We cover our journey, findings, and the rabbit holes we explored. We also provide an academic paper with the details of the attack and open-source code implementing it, so people building software and products using ECDSA can identify and avoid this vulnerability in their systems. We've only scratched the surface, there's still plenty of room for exploration.

REFERENCES

* <https://eprint.iacr.org/2019/023> * <https://eprint.iacr.org/2022/169.pdf> * <https://github.com/gcarq/rusty-blockparser> * https://en.bitcoin.it/wiki/OP_CHECKSIG * <https://bitcointalk.org/index.php?topic=1431060.0>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Power Corrupts; Corrupt It Back! Hacking Power Management in Data Centers

When: Saturday, Aug 12, 14:00 - 14:45 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

Speakers:Jesse Chick,Sam Quinn

SpeakerBio:Jesse Chick , Security Researcher at Trellix Advanced Research Center

Jesse Chick is a Security Researcher with the Advanced Research Center's vulnerability team. Jesse focusses on vulnerability discovery and exploit development for all things connected to the internet and is credited with numerous CVEs affecting popular embedded devices. He is passionate about reverse engineering, full system emulation, and educating others in offensive security techniques.

Twitter: [@ravenousbytes](#)

SpeakerBio:Sam Quinn , Sr. Security Researcher at Trellix Advanced Research Center

Sam Quinn is a Senior Security Researcher on the Advanced Research Center Vulnerability team, focused on finding new vulnerabilities in both software and hardware. Sam has a focus on embedded devices with knowledge in the fields of reverse engineering and exploitation. He has had numerous vulnerability findings, published CVEs in IOT and enterprise software, and has spoken at multiple industry conferences such as Def Con, BlackHat, North Sec, and Hardwear.io.

Twitter: [@eAyeP](#)

Description:

Our current administration lists "Defend Critical Infrastructure" as the #1 item in the 2023 National Cybersecurity Strategy. At the intersection of governmental and corporate concerns is data center security, a trend that is bound to continue as more and more operations move to the cloud. This talk details our findings in the domain of power management, the first category in a broader effort to investigate the security of critical data center components. We will reveal nine vulnerabilities in two integral data center appliances: a Power Distribution Unit (PDU) and a Data Center Infrastructure Management (DCIM) system. Continuing, we will delve into the technical details of the most impactful vulnerabilities and highlight the potential impact on their respective operations. The talk will challenge the misconception that data centers are inherently more secure than on-prem by exposing how attackers could leverage these vulnerabilities. This presentation will be valuable to data center professionals, security researchers, and anyone interested in understanding the characteristic vulnerabilities associated with modern data centers.

REFERENCES:

Contributing Researcher - Philippe Laulheret Claroty Research -

<https://claroty.com/team82/research/jumping-nat-to-shut-down-electric-devices> National Cybersecurity Strategy -

<https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-natio>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Friday - 12:30-12:59 PDT

Title: Practical advice for navigating edtech privacy

When: Friday, Aug 11, 12:30 - 12:59 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio:Michelle Levesley

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Friday - 15:00-15:45 PDT

Title: Privacy of Web PKI Revocation

When: Friday, Aug 11, 15:00 - 15:45 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

SpeakerBio:Matthew McPherrin

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Private Keys in Public Places

When: Friday, Aug 11, 13:30 - 14:15 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

SpeakerBio: Tom Pohl , Principal Consultant and the Penetration Testing Team Manager at LMG Security

Tom Pohl is a Principal Consultant and Penetration Testing Team Manager at LMG Security. Prior to LMG, he has spent most of his career on the blue team building and securing systems used by millions of people. And by night, he is a competitive CTF player and has won several black/gold badges including THOTCON, Circle City Con, Wild West Hackin' Fest and DEF CON. He is good at what he does because he's already made many of the mistakes that he encounters in client environments on a daily basis.

Description:

Firmware and software binaries are littered with private keys, legitimate CA-blessed certificates, and encryption keys—but hardly anyone notices. These secrets are often obfuscated or otherwise hidden in ways that weren't intended to be found. I'll show three real-world examples from popular manufacturers (Netgear, Fortinet and Dell), and demonstrate techniques for uncovering them. In the most extreme example, an adversary can use an obfuscated key to gain access to any customer's vCenter environment.


I'll start with a straightforward look at Netgear firmware and show methods for discovering private keys in PEM-encoded text files. We'll dig into the Fortinet firmware, which contained custom obfuscated archive files, and show how to extract Apple and Google issued certificates and I will also show that 3 year awaited "fix" did not adequately solve the issue.

Finally, I'll dig into the worst case: a static AES encryption key within Dell software used to connect to vCenter. I'll demonstrate how retrieve, decompile and use a static AES key which will decrypt vCenter credentials. The key is the same for EVERY customer. This has not been talked about anywhere publicly.

I'll conclude by discussing the importance of developer training, proper key management, and (above all), identifying and eliminating this systemic practice.

REFERENCES

- ◇ <https://starkeblog.com/netgear/tls/private-key/2020/01/19/netgear-signed-tls-private-key-disclosure.html> - Nick Starke and Tom Pohl
- ◇ <https://www.fortiguard.com/psirt/FG-IR-20-014> - Tom Pohl

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Private Until Presumed Guilty

When: Friday, Aug 11, 13:30 - 14:15 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

Speakers: Allison Young, Diane Akerman

SpeakerBio: Allison Young, Digital Forensics Analyst at The Legal Aid Society

Allison Young is an Analyst in the Digital Forensics Unit of the Legal Aid Society. Allison has expertise in computer, mobile, and cloud account preservation and analysis. She is a current Cellebrite Certified Mobile Examiner and holds a Master's degree in Digital Forensics from the University of Central Florida. She has examined hundreds of computers and cell phones during her career and has a love-hate relationship with data

Allison has used her knowledge of "how computers think" to help attorneys understand the importance of their digital evidence so they can better serve their clients, sometimes resulting in reduced, settled, or dismissed outcomes in legal cases. She likes to bridge the gap between what the database says and what may have happened IRL - or point out when crossing that bridge won't necessarily bring us to the truth.

SpeakerBio: Diane Akerman, Digital Forensics Attorney at The Legal Aid Society

Diane Akerman is a public defender working in the Legal Aid Society's Digital Forensics Unit (DFU). The Digital Forensics Unit is dedicated to fighting the unregulated and unfettered use of surveillance technology primarily by the NYPD. Her work involves investigating and uncovering the purchase and use of technologies, developing litigation strategies in criminal cases, and advocating for policy changes. She has litigated the full array of electronic surveillance technologies employed by the NYPD and local law enforcement, including cell phone tracking, GPS, ShotSpotter and facial recognition technology. She knows what it's like to get that email from Facebook informing you that they are about to give the federal government all your data, and to have her cell phone a mere Judge's signature away from a Cellebrite machine.

Twitter: [@MF_Diz](#)

Description:

Dobbs has significantly heightened the fear that everyday private data can be leveraged by law enforcement to prosecute pregnancy outcomes. However, this data is already being used in investigating other criminalized activities. In this talk, we will show you examples of information that can easily be extracted from many phones to surveil personal reproductive decisions.

We will also show you how the government obtains your not-so-private thoughts using forensic extraction and reporting tools, with a focus on health and lifestyle apps. This will include a review of the output of common forensic tools, demonstrating both the practical ease of reviewing sensitive data and the technical limitations of interpreting their meaning. Warning: you may find this peek into digital investigations disturbing.

We will discuss the different laws that do, or do not, protect your private health data, but will focus primarily on the limitations of the 4th Amendment in the digital world. The talk will provide a brief overview of traditional warrant practice and the "reasonable expectation of privacy" in digital data. But because the law has no bearing on reality, we'll look at excerpts from search warrants for digital devices and cloud data that illustrate the flawed nature of warrant practice in general, the limitations of the practice in the digital context, and the ease with which the government can obtain your data without any real oversight.

Bibliography & References:

- United States v. Jones, 565 U.S. 400 (2012)
- Riley v. California, 573 U.S. 373 (2014)
- Carpenter v. United States, 138 S. Ct. 2206
- United States v. Warshak, 631 F.3d 266 (6th Cir. 2010)

- Stored Communications Act 18 U.S. Code Â§ 2703
- Aziz Z. Huq & Rebecca Wexler, Digital Privacy for Reproductive Choice in the Post-Roe Era, 98 NYUL Rev 555 [2023]
- Congressional Research Service, "Abortion, Data Privacy, and Law Enforcement Access: A Legal Overview", (July 8, 2022 Update), Available at: <https://crsreports.congress.gov/product/pdf/LSB/LSB10786>
- Conti-Cook, Cynthia, "Surveilling the Digital Abortion Diary" (October 28th, 2020). University of Baltimore Law Review: Vol. 50: Iss. 1, Article 2. Available at: <https://scholarworks.law.ubalt.edu/ublrvol50/iss1/2>
- Downing, Andrea, "Health Advertising on Facebook: Privacy and Policy Considerations," (August 15th, 2022). Patterns. Available at <https://doi.org/10.1016/j.patter.2022.100561>
- Fowler, Leah R. and Ulrich, Michael R., Femtechnodystopia (May 3, 2022). Stanford Law Review, Forthcoming, Available at SSRN: <https://ssrn.com/abstract=4099764> or <http://dx.doi.org/10.2139/ssrn.4099764>
- Gallagher, William, "What Apple surrenders to law enforcement when issued a subpoena," (January 21st, 2020). Apple Insider. Available at: <https://appleinsider.com/articles/20/01/21/what-apple-surrenders-to-law-enforcement-when-issued-a-subpoena>
- Huss et. al, "Self-Care Criminalized: August 2022 Preliminary Findings," If/When/How. Available at <https://www.ifwhenhow.org/resources/self-care-criminalized-preliminary-findings/>
- Koepke, Logan and Emma Weil, Urmila Janardan, Tinuola Dada, Harlan Yu, "Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones" (October 20th, 2020). Upturn. Available at <https://www.upturn.org/work/mass-extraction/>
- Paltrow LM, Flavin J. "Arrests of and forced interventions on pregnant women in the United States, 1973-2005: implications for women's legal status and public health." J Health Polit Policy Law. 2013 Apr;38(2):299-343. doi: 10.1215/03616878-1966324. Epub 2013 Jan 15. PMID: 23262772.
- "Pregnancy Justice, Arrests and Prosecutions of Pregnant People, 1973-2020." Available at <https://www.pregnancyjusticeus.org/arrests-and-prosecutions-of-pregnant-women-1973-2020/>
- Rajesh, Ananya Mariam and Jeffrey Dastin, "Google to delete location history of visits to abortion clinics," (July 1st, 2022). Reuters. Available at <https://www.reuters.com/world/us/google-delete-location-history-visits-abortion-clinics-2022-07-01/>
- Sunde, Nina and Itiel E. Dror, "A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making," Forensic Science International: Digital Investigation, Volume 37, 2021, 301175, ISSN 2666-2817, <https://doi.org/10.1016/j.fsidi.2021.301175>. (Accessed from <https://www.sciencedirect.com/science/article/pii/S2666281721000834> on July 2nd, 2023)
- Wexler, Rebecca, "Privacy As Privilege: The Stored Communications Act and Internet Evidence" (August 13, 2020). 134 Harv. L. Rev. 2721 (2021). Available at SSRN: <https://ssrn.com/abstract=3673403>
- Cole, Samantha, "Apple Health Data Is Being Used as Evidence in a Rape and Murder Investigation," (January 11th, 2018). Vice Media Group. Available at: <https://www.vice.com/en/article/43q7qq/apple-health-data-is-being-used-as-evidence-in-a-rape-and-murder-investigation-g>
- Cuthbertson, Anthony. "Amazon ordered to give Alexa evidence in double murder case," (November 14th, 2018). The Independent. Available at: <https://www.independent.co.uk/tech/amazon-echo-alexa-evidence-murder-case-a8633551.html>
- Feathers, et. Al. "Facebook Is Receiving Sensitive Medical Information from Hospital Websites," (June 16th, 2022). The Markup. Available at <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>
- Federal Trade Commission, "FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others," (June 22, 2021). Available at: <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-s>
- Federal Trade Commission: In the Matter of Flo, Inc., Case Summary and Timeline, available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc>
- Germain, Thomas, "FTC Fines GoodRx \$1.5M for Sending Your Medication Data to Facebook and Google for Ads," (February 9th, 2021). Gizmodo. Available at <https://gizmodo.com/ftc-fines-goodrx-prescription-data-facebook-google-1850059096>.
- Guide to Abortion Privacy, available at <https://digitaldefensefund.org/ddf-guides/abortion-privacy>
- "How to turn on Advanced Data Protection for iCloud," (January 19th, 2023). Apple Support. Available at: <https://support.apple.com/en-us/HT212520>
- Joyce, Stephen, "Court Allows Use of Facebook Live, Internet Searches as Evidence," (December 20th, 2022). Bloomberg Industry Group, Inc. Available at:

<https://news.bloomberglaw.com/us-law-week/court-allows-use-of-facebook-live-internet-searches-as-evidence>

- Peterson, M., "Apple Health data used to convict man in wife's death," (February 9th, 2021), AppleInsider. Available at: <https://appleinsider.com/articles/21/02/09/apple-health-data-used-to-convict-man-in-wifes-death>
- Pratt, Mark. "Google searches to be key in prosecuting Brian Walshe's murder trial, experts say" (January 27th, 2023). CBS News. Available at: <https://www.cbsnews.com/boston/news/ana-walshe-murder-case-brian-walshe-google-internet-searches-cohasset-massach>



[Return to Index](#) - Add to  - ics [Calendar](#) file

BTV - Sunday - 11:00-11:30 PDT

Title: Project Obsidian Panel

When: Sunday, Aug 13, 11:00 - 11:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Main Stage - [Map](#)

Description:

Project Obsidian panel discussion: Who, What, When, Where, and How

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: ProjectDiscovery Nuclei

When: Saturday, Aug 12, 14:00 - 15:55 PDT

Where: Caesars Forum - Council Boardroom - Demo Labs - [Map](#)

Speakers: Brendan O'Leary, Pj Metz

SpeakerBio: Brendan O'Leary

Brendan O'Leary is Head of Community at ProjectDiscovery, on a mission to democratize security, and an advisor to various startups. Having worked in software his entire career, Brendan has had the privilege of working with many customers. Previously at GitLab and a board member of the CNCF – it is clear, every company is a software company. That means every company needs software and security operational excellence. Outside of work, you'll find Brendan with 1 to 4 kids hanging off of him at any given time or occasionally finding a moment alone to build something in his workshop.

SpeakerBio: Pj Metz

Pj Metz is Developer Community Manager at ProjectDiscovery and former Education Evangelist at GitLab. Before that, he was a High School English teacher for 11 years, making the transition into tech in 2021. Pj brought his passion for education to his roles at GitLab and ProjectDiscovery and is always excited to present, chat, or discuss DevRel, security, and the importance of open source work. Pj loves 80's music and 90's internet culture.

Description:

Nuclei is used to send requests across targets based on a YAML template, leading to fewer false positives and providing fast scanning on a large number of hosts. Nuclei offers scanning for a variety of protocols, including TCP, DNS, HTTP, SSL, File, Whois, Websocket, Headless etc. With powerful and flexible templating, Nuclei can be used to model all kinds of security checks. Nuclei is a valuable tool for bug bounty hunters, pen testers, developers looking to add more security into their CI/CD pipelines, and more.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Protecting the AWS ecosystem - Misconfigurations, IAM, and Monitoring (Pre-Registration Required)

When: Thursday, Aug 10, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

SpeakerBio: Rodrigo Montoro , Head of Threat & Detection Research at Clavis Security

Rodrigo Montoro has over 23 years of experience in Information Technology and Computer Security. For most of his career, he has worked with open-source security software (firewalls, IDS, IPS, HIDS, log management, endpoint monitoring), incident detection & response, and Cloud Security. Currently is Head of Threat & Detection Research at Clavis Security. Before that, he worked as Cloud Researcher at Tenchi Security, Head of Research and Development at Apura Cyber Intelligence, SOC/Researcher at Tempest Security, Senior Security Administrator at Sucuri, and Researcher at Spiderlabs. Author of 2 patented technologies involving innovation in the detection field. One is related to discovering malicious digital documents. The second one is in how to analyze malicious HTTP traffic. Rodrigo has spoken at several open source and security conferences (Defcon Cloud Village, OWASP AppSec, SANS (DFIR, SIEM Summit & CloudSecNext), Toorcon (USA), H2HC (São Paulo and Mexico), SecTor (Canada), CNASI, SOURCE, ZonCon (Amazon Internal Conference), Blackhat Brazil, BSides (Las Vegas e SP)).

Twitter: [@spookerlabs](#)

Description:

Cloud providers' ecosystems have brought a lot of new challenges to companies and Security teams. Many new attack vectors create known and unknown attack vectors, generating a considerable need for further research and detection in this field.

In the current cloud security world, access keys are the new perimeter, and permissions associated with those keys are the limits. In many real-world scenarios, leaked access keys are the initial vectors to get into an organization's cloud environments. Therefore, the least privilege and detection in real-time becomes critical.

Specifically, in AWS, we are talking about more than three hundred (300+) services that an attacker could create their specific attack path to achieve their goal. Considering this chaotic scenario, we developed this workshop to teach how to mitigate those new vectors and improve the company's overall cloud security posture. The workshop will cover misconfigurations, AWS IAM (Identity and Access Management) least privilege, and control plane (Cloudtrail) monitoring.

This workshop will help organizations improve their cloud security posture in these three fields - misconfigurations, IAM permissions management, and control plane monitoring. There will be practical demonstrations, hands-on labs, and some Capture The Flag (CTF) to practice incident response.

Skill Level: Intermediate

Prerequisites for students:

- AWS basic to intermediate knowledge

Materials or Equipment students will need to bring to participate: - Laptop.

- Demonstrations and Capture The Flag (CTF) exercises will be executed in my AWS account and using CTFd.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Protocol Identification for Integration

When: Friday, Aug 11, 15:00 - 15:20 PDT

Where: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

SpeakerBio:Eric Escobar

Eric is a seasoned pentester and a Principal Security Consultant at Secureworks. On a daily basis he attempts to compromise large enterprise networks to test their physical, human, network and wireless security. He has successfully compromised companies from all sectors of business including: Healthcare, Pharmaceutical, Entertainment, Amusement Parks, Banking, Finance, Technology, Insurance, Military, Retail, Food Distribution, Government, Education, Transportation, Energy and Industrial Manufacturing.

His team consecutively won first place at DEF CON 23, 24, and 25's Wireless CTF, snagging a black badge along the way. Forcibly retired from competing in the Wireless CTF, he now helps create challenges!

Before entering the cyber security arena, Eric attained both a BS and MS in Civil Engineering along with his Professional Engineering license.

Twitter: [@EricEscobar](#)

Description:

In this talk you'll see how hacking doesn't always involve pillaging or exploit development. In fact, hacking can allow you to expand functionality! I'll be walking you through steps of reverse engineering a wireless signal in order to hack, build and implement additional functionality of a wireless device. If you like IoT, wireless, and a little bit of software defined radio, you'll love this talk!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-19:59 PDT

Title: pTFS Presents: Mayhem Industries – Starphish

When: Friday, Aug 11, 10:00 - 19:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Do you have what it takes to go up against Mayhem Industries' latest maleficent project? Starphish Ltd. is up to no good in that way that only corporations can be. They've got five Divisions, which means you've got five opportunities to shut them down!

It won't be easy. You'll be directing a team of infiltrators through increasingly difficult challenges. What sort of challenges? Depends on the Division. Engineering is full of crunchy hacking challenges. HR's got the goods on social engineering. Finance'll be data processing the whole way.

And the C-suite? Most dangerous of all... We've never been able to get an operative inside, so they could be anything. We're counting on you.

Starphish is a fun and interactive jeopardy style CTF contest. Don't worry if you don't know what that means. Winning will require demonstrating a wide range of hacking skills, but participating is encouraged for all ability levels. Challenges range from simple puzzles, to challenging crypto problems, to truly phishy hijinks.

pTFS is a hacker collective that has been competing in various DEF CON contests for almost 15 years.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Sunday - 10:00-13:59 PDT

Title: PTP Flight Challenge

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

PTP Flight Challenge

Pen Test Partners

Come try your hand at flying our immersive Airbus A320 simulator and see if you can stick our landing challenge! We'll also be talking about electronic flight bags, how their data integrity is relied upon by pilots to assist with a safe landing, and demonstrate the impacts in a safe environment.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Saturday - 10:00-17:59 PDT

Title: PTP Flight Challenge

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

PTP Flight Challenge

Pen Test Partners

Come try your hand at flying our immersive Airbus A320 simulator and see if you can stick our landing challenge! We'll also be talking about electronic flight bags, how their data integrity is relied upon by pilots to assist with a safe landing, and demonstrate the impacts in a safe environment.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Friday - 10:00-17:59 PDT

Title: PTP Flight Challenge

When: Friday, Aug 11, 10:00 - 17:59 PDT


Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

PTP Flight Challenge

Pen Test Partners

Come try your hand at flying our immersive Airbus A320 simulator and see if you can stick our landing challenge! We'll also be talking about electronic flight bags, how their data integrity is relied upon by pilots to assist with a safe landing, and demonstrate the impacts in a safe environment.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 18:00-20:30 PDT

Title: Pub Quiz at DEF CON

When: Friday, Aug 11, 18:00 - 20:30 PDT

Where: Caesars Forum - Forum - 121-123, 129, 137 - Chillout - [Map](#)

Description:

Do you like Pub Quiz please join us in participating in the first ever Pub Quiz at DEF CON. Quiz will consist of 7 rounds from Question from 90s TV shows, Movies, and DEF CON questions. The quiz will be theme will be all things DEF CON. There will be visual and audio rounds so not just boring questions. People will group into teams of 5 and a cash prize will be provided for 1st, 2nd, and 3rd high scoring groups. Ties will be broken by a dance off from a person of the tied teams.

1st Prize \$1,000

2nd Prize \$300

3rd Prize \$200

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Push All the Buttons Digital Twinning with Idaho National Labs in collaboration with DEF CON ICS Village

When: Saturday, Aug 12, 17:00 - 17:59 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

SpeakerBio: Kolton Heaps

Kolton Heaps is a Digital Twin Visualization Scientist at the Idaho National Laboratory. He focuses on creating visualizations and software that assist in design, operations and training on projects including, fuel processing, non-proliferation, modular reactors, and advanced digital twin of nuclear reactor. Kolton has a bachelor's in software engineering from Brigham Young University – Idaho and lives in Idaho Falls where he enjoys mountain biking and other outdoor activities.

Description:

Extended Reality (XR) is an umbrella term that involves virtual reality (VR), augmented reality (AR), and mixed reality (MR) capabilities. VR describes an environment in which a user's physical environment is completely replaced with a virtual one. This allows the user to view any digitally created content but separates the user from interacting with the physical world. On the other hand, AR enhances the user's physical environment with virtual overlays but offers little interaction with digital content. Lastly, MR is a blend of the physical and digital worlds, unlocking natural and intuitive 3D human, computer, and environmental interactions. Using these technologies, analysts, operators, and stakeholders will be able to interpret radio frequency data effectively and efficiently.,

The Idaho National Laboratory is integrating the next-generation XR capabilities into the various projects that support Nuclear, Integrated Energy and National and Homeland Security missions. They use a suite of tools for the visualization of capabilities to capture and analyze digital twins. Digital Engineering delivers semi-autonomous design, autonomous operation, and real-time anomaly detection as well as integrates threads of data, visualizations, AI/ML, and physics models into a cohesive digital twin.

The primary benefit of incorporating XR with signal analysis is to allow for simple interpretation and representation of complex data. Current techniques or trends rely on certain subject matter experts to collect, examine, and report anomalous data manually. By allowing the operator to spatially view the captured data, the process of identifying and plotting data is anticipated to be greatly simplified. Data and anomalies will become engaging, allowing the operator to easily identify unknown signals in real-time or near real-time., ,

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Putting Your Money Where Your Cyber Is: A Guided Discussion of Software Liability and Security

When: Sunday, Aug 13, 10:00 - 10:50 PDT

Where: Caesars Forum - Summit - 221-222 - Policy Atrium - [Map](#)

SpeakerBio: Andrea Matwyshyn , Professor at Penn State Law & Penn State Engineering

Dr. Andrea Matwyshyn is a full professor in the law school and engineering school at Penn State, the Associate Dean of Innovation at Penn State Law, and the founding faculty director of both the Penn State PILOT Lab (Policy Innovation Lab of Tomorrow), an interdisciplinary technology policy lab, and the Manglona Lab for Gender and Economic Equity, a technology equity lab and clinic. She has also worked in both the private and public sector, most recently in 2023 as a Senior Special Advisor on Information Security and Data Privacy to the U.S. Consumer Financial Protection Bureau’s Office of Enforcement and a Senior Special Advisor on Law, Technology, and the Digital Economy to the U.S. Federal Trade Commission’s Bureau of Consumer Protection. Her first hackercon talk was at BlackHat USA in 2003, and she has previously served as a specialty reviewer on the DEF CON CFP Review team.

Description:

Are you interested in discussing the future of “shifting liability for software products and services to promote secure development practices”? If so, join a guided discussion led by law and engineering Prof. Andrea Matwyshyn on Pillar 3 of the Biden-Harris National Cybersecurity Strategy. After a brief introduction to the history of software liability and what (various forms of) “security liability” already exist, we will engage in structured legal exercises intended to help us discuss, crystalize, and clarify the relevant variables that courts, regulators, and policymakers will consider in deciding how to generate the next generation of security liability. We will talk through what the legal future is likely to hold (and assess what we think it should hold). We will debate the edge cases and try to generate some consensus, as well as perhaps a master list of concerns that can help further inform policymakers’ thinking on the future of security and software liability policy.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Pwning the Pwners with Mindware

When: Friday, Aug 11, 10:00 - 10:50 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

SpeakerBio: Frank "D9" DiGiovanni

Forty-one years of government service, Frank DiGiovanni is a retired USAF Colonel and DoD Senior Executive Service. Co-Led with the DoD CIO the development of the SecDef's DoD Cyber Workforce Strategy. Built from scratch a six-month DoD Cyber Operations training course, repurposed DEFCON's CTF and CTP technical architecture to support DoD cyber operations training, and now working advanced cyber R&D projects in private sector. UPENN doctoral dissertation examined what makes hackers extraordinary unique from the average human population.

Description:

Traditionally the cyber attacker has an asymmetric advantage over the cyber defender. But does it have to be that way? Is it possible for the cyber defender to take an "offensive stance." This talk will show how the emerging science of cyberpsychology and the leveraging of AI can provide the defender with the ability to pwn the most vulnerable component in the cyberattack kill chain, the attack's human operator. Leveraging the DoD's "Tularosa Study," this talk will cover a theoretical framework for achieving this objective, outline an operational vignette, and then cover some the specifics for such an approach.

[Return to Index](#) - Add to  - ics [Calendar](#) file

QTV - Saturday - 10:30-10:59 PDT

Title: Q-CTF QOLOSSUS Update

When: Saturday, Aug 12, 10:30 - 10:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

SpeakerBio:Mark Carney

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: QDoor: Exploiting Approximate Synthesis for Backdoor Attacks in Quantum Neural Networks

When: Saturday, Aug 12, 13:00 - 13:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

SpeakerBio: Lei Jiang , Assoc. Prof. at Indiana University Bloomington

No BIO available

Description:

Quantum neural networks (QNNs) succeed in object recognition, natural language processing, and financial analysis. To maximize the accuracy of a QNN on a Noisy Intermediate Scale Quantum (NISQ) computer, approximate synthesis modifies the QNN circuit by reducing error-prone 2-qubit quantum gates. The success of QNNs motivates adversaries to attack QNNs via backdoors. However, naively transplanting backdoors designed for classical neural networks to QNNs yields only low attack success rate, due to the noises and approximate synthesis on NISQ computers. Prior quantum circuit-based backdoors cannot selectively attack some inputs or work with all types of encoding layers of a QNN circuit. Moreover, it is easy to detect both transplanted and circuit-based backdoors in a QNN.

In this talk, we introduce a novel and stealthy backdoor attack, QDoor, to achieve high attack success rate in approximately-synthesized QNN circuits by weaponizing unitary differences between uncompiled QNNs and their synthesized counterparts. QDoor trains a QNN behaving normally for all inputs with and without a trigger. However, after approximate synthesis, the QNN circuit always predicts any inputs with a trigger to a predefined class while still acts normally for benign inputs. Compared to prior backdoor attacks, QDoor improves the attack success rate by 13x and the clean data accuracy by 65% on average. Furthermore, prior backdoor detection techniques cannot find QDoor attacks in uncompiled QNN circuits.

[Return to Index](#) - Add to  - ics [Calendar](#) file

QTV - Friday - 10:30-10:59 PDT

Title: QLOSSUS - Quantum Capture the Flag Introduction!

When: Friday, Aug 11, 10:30 - 10:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

SpeakerBio:Quantum Quizmasters

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

QTV - Sunday - 12:00-12:59 PDT

Title: QOLOSSUS; Quantum CTF - Results!

When: Sunday, Aug 13, 12:00 - 12:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

Description:

With this year's Q-CTF coming to a close, we will announce our winners!

[Return to Index](#) - Add to  - ics [Calendar](#) file

QTV - Saturday - 16:00-17:59 PDT

Title: Quantini Time! Cocktail hour for the Quantum curious and creative


When: Saturday, Aug 12, 16:00 - 17:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

Description:

Cocktail hour for the Quantum curious and creative.

Come and join us for some complimentary drinks with like-minded hackers. Come along and listen to - or even make! - quantum music.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Quantum attacks on next-gen cryptosystems: lattices, annealers, notebooks

When: Saturday, Aug 12, 11:00 - 12:30 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

Description:

In this workshop we will develop quantum algorithms to solve a computer science problem called the shortest lattice problem (SVP). SVP is geometrically simple - given a description of a mathematical lattice (a repeating pattern of points in N-dimensional space), can you find the shortest distance between any two points - i.e. the shortest vector? This problem is NP hard and we believe it is resistant to quantum computers.

Based upon the results of “Two quantum Ising algorithms for the shortest-vector problem”, we will explain the principle of quantum adiabatic computation, of Hamiltonian minimization, and of how to map mathematical problems into a Hamiltonian ready to be plugged into a quantum computation framework.

During the course of the workshop, participants will fill in functions in a Jupyter notebook to construct lattices, convert them into a Hamiltonian, and describe quantum annealing dynamics. They will then (hopefully) be able to submit these queries to a D-Wave QPU to which will sample short vectors for them, and we will visualize as a group the results returned.

This exercise will get participants directly interacting with a QPU, understanding some of the benefits and limitations of annealing-based quantum computation, and will learn about an exciting computer science problem and how it directly feeds into our security architecture, (e.g. Kyber!)

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Quantum Computer Music Performance, by Scott Oshiro (one half of NpHz)

When: Saturday, Aug 12, 17:00 - 17:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

SpeakerBio: Scott Oshiro

No BIO available

Description:

NpHz is a new electro-acoustic duo featuring OCH (Omar Costa Hamido) and SYO (Scott Oshiro): two artist-researchers working in music and technology focusing on improvised Music and Quantum Computing (QC). In our work we explore the potential advantages QC can provide for music composition. This performance will include ½ of NpHz, Scott Oshiro (SYO). He will be performing adapted works from NpHz's recent album "[\Equations of Coltrane](<https://omarcostahamido.bandcamp.com/album/equations-of-coltrane>)" (Released June 2, 2023 on Bandcamp). Scott will also be playing flute alongside his real-time Quantum Jazz Improvisation system entitled Lineage.

[Return to Index](#) - Add to  - ics [Calendar](#) file

QTV - Sunday - 11:00-11:59 PDT

Title: Quantum Life - An open mic space discussing the possible futures granted by quantum technologies

When: Sunday, Aug 13, 11:00 - 11:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

Speakers:Mark Carney,Victoria Kumaran

SpeakerBio:Mark Carney

No BIO available

SpeakerBio:Victoria Kumaran

No BIO available

Description:

We present our second open session on what Quantum Life might look like in the future! Join our experts, enthusiasts, and other community members to discover what this quantum future could all be about...

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Quantum Music Workshop: Build Your Own Quantum Synthesizer!

When: Saturday, Aug 12, 16:00 - 16:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

SpeakerBio:Mark Carney

No BIO available

Description:

Quantum Music is a new paradigm of art, part of the new wave of ‘Quantum Art’ that we shall be showcasing with a live performance from Scott Oshiro! In the run up to this, Mark will show us how to embed quantum simulators (and quantum computer connections) into everyday musical apparatus... from quantum enabled MIDI to a quantum stylophone and more!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Quantum Technologies on a Raspberry Pi (and HackRF one)

When: Saturday, Aug 12, 15:00 - 15:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

SpeakerBio: Ben Varcoe

No BIO available

Description:

Quantum Sensing is a new paradigm of technology that allows us to use quantum-level effects for macro-level sensing outputs. Join Ben as he demonstrates how to use off-the-shelf components to build a quantum sensor; using just a HackRF, a Raspberry Pi, and some high-quality oscillators being the primary ingredients!

Time shifts are used to test special and general relativity, they are used for navigation and they shed light on things like quantum field theory and quantum gravity. In special relativity, a moving clock will have a time shift with respect to a stationary clock. This is typically very small and requires extremely fast moving objects to really see a difference. On the other hand an accelerated clock adds something new. Rather than just seeing a change in the passage of time the accelerated observer sees a change in the speed of light for other observers. To measure this we shall make use of the Rindler frame; an artefact of "Special Relativity" rather than "General Relativity".

By utilising these effects and a little quantum field theory, we can use the fact that in the Rindler frame, time shifts would manifest as phase shifts, hence a very sensitive measurement of phase could detect the acceleration based time shifts giving us a new kind of quantum sensor.. All of which can be done on off-the-shelf components, as Ben shall be building and demonstrating during the village!

[Return to Index](#) - Add to  - ics [Calendar](#) file

QTV - Friday - 10:00-10:30 PDT

Title: Quantum Village Opening!

When: Friday, Aug 11, 10:00 - 10:30 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

Speakers:Mark Carney,Quantum Village Organizers,Victoria Kumaran

SpeakerBio:Mark Carney

No BIO available


SpeakerBio:Quantum Village Organizers

No BIO available

SpeakerBio:Victoria Kumaran

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Thursday - 16:00-17:59 PDT


Title: Queercon Mixers

When: Thursday, Aug 10, 16:00 - 17:59 PDT

Where: Caesars Forum - Forum - 129 - Chillout - [Map](#)

Description:

A great way to meet other like-minded folk in this safe and inclusive environment. An informal meet-up of the lgbtqia+ community to network and unwind.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 16:00-17:59 PDT


Title: Queercon Mixers

When: Saturday, Aug 12, 16:00 - 17:59 PDT

Where: Caesars Forum - Forum - 129 - Chillout - [Map](#)

Description:

A great way to meet other like-minded folk in this safe and inclusive environment. An informal meet-up of the lgbtqia+ community to network and unwind.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 16:00-17:59 PDT


Title: Queercon Mixers

When: Friday, Aug 11, 16:00 - 17:59 PDT

Where: Caesars Forum - Forum - 129 - Chillout - [Map](#)

Description:

A great way to meet other like-minded folk in this safe and inclusive environment. An informal meet-up of the lgbtqi+ community to network and unwind.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 22:00-00:59 PDT

Title: QueerCon Party

When: Friday, Aug 11, 22:00 - 00:59 PDT

Where: Caesars Forum - Forum - 111-113 - [Map](#)

Speakers:DotOrNot, Miss Jackalope, Skittish & Bus

SpeakerBio:DotOrNot

No BIO available

SpeakerBio:Miss Jackalope

No BIO available

SpeakerBio:Skittish & Bus

No BIO available

Description:

The party provides a safe and inclusive environment for the lgbtqia+ community within Infosec to come together and be their authentic selves. A late evening party with music, dancing, and hanging out.

22:00 - 23:00 - DotOrNot

23:00 - 00:00 - Skittish and Bus

00:00 - 01:00 - Miss Jackalope

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Friday - 15:00-15:50 PDT

Title: Radiation Detection For The Rest Of Us - Diy Radiation Spectroscopy

When: Friday, Aug 11, 15:00 - 15:50 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

SpeakerBio:Patrick Kiley

Patrick Kiley is a Security Consultant doing hardware penetration testing and has over 20 years of information security experience. Patrick has performed research in Avionics security, Vehicles, and even managed to brick a Tesla. Patrick has experience in penetration testing all the things, hardware hacking, IoT and Transportation.

Description:

When radiation detectors are mentioned, one tends to think of the geiger counter. This type of detector happens to be just one method of radiation detection. This workshop will introduce gamma ray spectrography, which measures the energy absorbed by the individual gamma rays. This energy level can let us know what radioactive isotope generated the gamma and can aid in identifying the material being examined.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Radio Frequency Capture the Flag

When: Friday, Aug 11, 10:00 - 12:59 PDT

Where: Virtual

Description:

Do you have what it takes to hack WiFi, Bluetooth, and Software Defined Radio (SDR)?

RF Hackers Sanctuary (the group formerly known as Wireless Village) is once again holding the Radio Frequency Capture the Flag (RFCTF) at DEF CON 31. RFHS runs this game to teach security concepts and to give people a safe and legal way to practice attacks against new and old wireless technologies.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The RFCTF can be played with a little knowledge, a pen tester's determination, and \$0 to \$\$\$\$ worth of special equipment. Our new virtual RFCTF can be played completely remotely without needing any specialized equipment at all, just using your web browser! The key is to read the clues, determine the goal of each challenge, and have fun learning.

There will be clues everywhere, and we will provide periodic updates via discord and twitter. Make sure you pay attention to what's happening at the RFCTF desk, #rfctf on our discord, on Twitter @rf_ctf, @rfhackers, and the interwebz, etc. If you have a question - ASK! We may or may not answer, at our discretion.

FOR THE NEW FOLKS

Our virtual RFCTF environment is played remotely over ssh or through a web browser. It may help to have additional tools installed on your local machine, but it is not required.

Read the presentations at: <https://rfhackers.com/resources>

Hybrid Fun

For DEF CON 31 we will be running in "Hybrid" mode. That means we will have both a physical presence AND the virtual game running simultaneously. All of the challenges we have perfected in the last 2 years in our virtual game will be up and running, available to anyone all over the world (including at the conference), entirely free. In addition to the virtual challenges, we will also have a large number of "in person" only challenges, which do require valid conference admission. These "in-person" only challenges will include our traditional fox hunts, hide and seeks, and king of the hill challenges. Additionally, we will have many challenges which we simply haven't had time or ability to virtualize. Playing only the virtual game will severely limit the maximum available points which you can score, therefore don't expect to place. If you play virtual only, consider the game an opportunity to learn, practice, hone your skills, and still get on the scoreboard for bragging rights. The virtual challenges which are available will have the same flags as the in-person challenges, allowing physical attendees the choice of hacking those challenges using either (or both) methods of access.

THE GAME


To score you will need to submit flags which will range from decoding transmissions in the spectrum, passphrases used to gain access to wireless access points, or even files located on servers. Once you capture the flag, submit it to the scoreboard right away, if you are confident it is correct. Flags will be worth less points the more often they are solved. Offense and defense are fully in play by the participants, the RFCTF organizers, and the Conference itself. Play nice, and we might also play nice.

Getting started guide: <https://github.com/rfhs/rfhs-wiki/wiki>

Helpful files (in-brief, wordlist, resources) can be found at <https://github.com/rfhs/rfctf-files>

Support tickets may be opened at <https://github.com/rfhs/rfctf-support/issues>

Our whole game is also open source and available at: <https://github.com/rfhs/rfctf-container>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Radio Frequency Capture the Flag

When: Sunday, Aug 13, 10:00 - 12:59 PDT

Where: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

Description:

Do you have what it takes to hack WiFi, Bluetooth, and Software Defined Radio (SDR)?

RF Hackers Sanctuary (the group formerly known as Wireless Village) is once again holding the Radio Frequency Capture the Flag (RFCTF) at DEF CON 31. RFHS runs this game to teach security concepts and to give people a safe and legal way to practice attacks against new and old wireless technologies.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The RFCTF can be played with a little knowledge, a pen tester's determination, and \$0 to \$\$\$\$\$ worth of special equipment. Our new virtual RFCTF can be played completely remotely without needing any specialized equipment at all, just using your web browser! The key is to read the clues, determine the goal of each challenge, and have fun learning.

There will be clues everywhere, and we will provide periodic updates via discord and twitter. Make sure you pay attention to what's happening at the RFCTF desk, #rfctf on our discord, on Twitter @rf_ctf, @rfhackers, and the interwebz, etc. If you have a question - ASK! We may or may not answer, at our discretion.

FOR THE NEW FOLKS

Our virtual RFCTF environment is played remotely over ssh or through a web browser. It may help to have additional tools installed on your local machine, but it is not required.

Read the presentations at: <https://rfhackers.com/resources>

Hybrid Fun

For DEF CON 31 we will be running in "Hybrid" mode. That means we will have both a physical presence AND the virtual game running simultaneously. All of the challenges we have perfected in the last 2 years in our virtual game will be up and running, available to anyone all over the world (including at the conference), entirely free. In addition to the virtual challenges, we will also have a large number of "in person" only challenges, which do require valid conference admission. These "in-person" only challenges will include our traditional fox hunts, hide and seeks, and king of the hill challenges. Additionally, we will have many challenges which we simply haven't had time or ability to virtualize. Playing only the virtual game will severely limit the maximum available points which you can score, therefore don't expect to place. If you play virtual only, consider the game an opportunity to learn, practice, hone your skills, and still get on the scoreboard for bragging rights. The virtual challenges which are available will have the same flags as the in-person challenges, allowing physical attendees the choice of hacking those challenges using either (or both) methods of access.

THE GAME


To score you will need to submit flags which will range from decoding transmissions in the spectrum, passphrases used to gain access to wireless access points, or even files located on servers. Once you capture the flag, submit it to the scoreboard right away, if you are confident it is correct. Flags will be worth less points the more often they are solved. Offense and defense are fully in play by the participants, the RFCTF organizers, and the Conference itself. Play nice, and we might also play nice.

Getting started guide: <https://github.com/rfhs/rfhs-wiki/wiki>

Helpful files (in-brief, wordlist, resources) can be found at <https://github.com/rfhs/rfctf-files>

Support tickets may be opened at <https://github.com/rfhs/rfctf-support/issues>

Our whole game is also open source and available at: <https://github.com/rfhs/rfctf-container>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Radio Frequency Capture the Flag

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

Description:

Do you have what it takes to hack WiFi, Bluetooth, and Software Defined Radio (SDR)?

RF Hackers Sanctuary (the group formerly known as Wireless Village) is once again holding the Radio Frequency Capture the Flag (RFCTF) at DEF CON 31. RFHS runs this game to teach security concepts and to give people a safe and legal way to practice attacks against new and old wireless technologies.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The RFCTF can be played with a little knowledge, a pen tester's determination, and \$0 to \$\$\$\$\$ worth of special equipment. Our new virtual RFCTF can be played completely remotely without needing any specialized equipment at all, just using your web browser! The key is to read the clues, determine the goal of each challenge, and have fun learning.

There will be clues everywhere, and we will provide periodic updates via discord and twitter. Make sure you pay attention to what's happening at the RFCTF desk, #rfctf on our discord, on Twitter @rf_ctf, @rfhackers, and the interwebz, etc. If you have a question - ASK! We may or may not answer, at our discretion.

FOR THE NEW FOLKS

Our virtual RFCTF environment is played remotely over ssh or through a web browser. It may help to have additional tools installed on your local machine, but it is not required.

Read the presentations at: <https://rfhackers.com/resources>

Hybrid Fun

For DEF CON 31 we will be running in "Hybrid" mode. That means we will have both a physical presence AND the virtual game running simultaneously. All of the challenges we have perfected in the last 2 years in our virtual game will be up and running, available to anyone all over the world (including at the conference), entirely free. In addition to the virtual challenges, we will also have a large number of "in person" only challenges, which do require valid conference admission. These "in-person" only challenges will include our traditional fox hunts, hide and seeks, and king of the hill challenges. Additionally, we will have many challenges which we simply haven't had time or ability to virtualize. Playing only the virtual game will severely limit the maximum available points which you can score, therefore don't expect to place. If you play virtual only, consider the game an opportunity to learn, practice, hone your skills, and still get on the scoreboard for bragging rights. The virtual challenges which are available will have the same flags as the in-person challenges, allowing physical attendees the choice of hacking those challenges using either (or both) methods of access.

THE GAME


To score you will need to submit flags which will range from decoding transmissions in the spectrum, passphrases used to gain access to wireless access points, or even files located on servers. Once you capture the flag, submit it to the scoreboard right away, if you are confident it is correct. Flags will be worth less points the more often they are solved. Offense and defense are fully in play by the participants, the RFCTF organizers, and the Conference itself. Play nice, and we might also play nice.

Getting started guide: <https://github.com/rfhs/rfhs-wiki/wiki>

Helpful files (in-brief, wordlist, resources) can be found at <https://github.com/rfhs/rfctf-files>

Support tickets may be opened at <https://github.com/rfhs/rfctf-support/issues>

Our whole game is also open source and available at: <https://github.com/rfhs/rfctf-container>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Radio Frequency Capture the Flag

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

Description:

Do you have what it takes to hack WiFi, Bluetooth, and Software Defined Radio (SDR)?

RF Hackers Sanctuary (the group formerly known as Wireless Village) is once again holding the Radio Frequency Capture the Flag (RFCTF) at DEF CON 31. RFHS runs this game to teach security concepts and to give people a safe and legal way to practice attacks against new and old wireless technologies.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The RFCTF can be played with a little knowledge, a pen tester's determination, and \$0 to \$\$\$\$\$ worth of special equipment. Our new virtual RFCTF can be played completely remotely without needing any specialized equipment at all, just using your web browser! The key is to read the clues, determine the goal of each challenge, and have fun learning.

There will be clues everywhere, and we will provide periodic updates via discord and twitter. Make sure you pay attention to what's happening at the RFCTF desk, #rfctf on our discord, on Twitter @rf_ctf, @rfhackers, and the interwebz, etc. If you have a question - ASK! We may or may not answer, at our discretion.

FOR THE NEW FOLKS

Our virtual RFCTF environment is played remotely over ssh or through a web browser. It may help to have additional tools installed on your local machine, but it is not required.

Read the presentations at: <https://rfhackers.com/resources>

Hybrid Fun

For DEF CON 31 we will be running in "Hybrid" mode. That means we will have both a physical presence AND the virtual game running simultaneously. All of the challenges we have perfected in the last 2 years in our virtual game will be up and running, available to anyone all over the world (including at the conference), entirely free. In addition to the virtual challenges, we will also have a large number of "in person" only challenges, which do require valid conference admission. These "in-person" only challenges will include our traditional fox hunts, hide and seeks, and king of the hill challenges. Additionally, we will have many challenges which we simply haven't had time or ability to virtualize. Playing only the virtual game will severely limit the maximum available points which you can score, therefore don't expect to place. If you play virtual only, consider the game an opportunity to learn, practice, hone your skills, and still get on the scoreboard for bragging rights. The virtual challenges which are available will have the same flags as the in-person challenges, allowing physical attendees the choice of hacking those challenges using either (or both) methods of access.

THE GAME


To score you will need to submit flags which will range from decoding transmissions in the spectrum, passphrases used to gain access to wireless access points, or even files located on servers. Once you capture the flag, submit it to the scoreboard right away, if you are confident it is correct. Flags will be worth less points the more often they are solved. Offense and defense are fully in play by the participants, the RFCTF organizers, and the Conference itself. Play nice, and we might also play nice.

Getting started guide: <https://github.com/rfhs/rfhs-wiki/wiki>

Helpful files (in-brief, wordlist, resources) can be found at <https://github.com/rfhs/rfctf-files>

Support tickets may be opened at <https://github.com/rfhs/rfctf-support/issues>

Our whole game is also open source and available at: <https://github.com/rfhs/rfctf-container>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Recon for Red Teamers and Bug Hunters 2.0

When: Sunday, Aug 13, 09:00 - 10:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 6 - [Map](#)

SpeakerBio: Jason Haddix , CISO and “Hacker in Charge” at BuddoBot

Jason Haddix is the CISO and “Hacker in Charge” at BuddoBot, a world-class adversary emulation consultancy. He's had a distinguished 15-year career in cybersecurity previously serving as the CISO of Ubisoft, Head of Trust/Security/Operations at Bugcrowd, Director of Penetration Testing at HP, and Lead Penetration Tester at Redspin. He has also held positions doing mobile penetration testing, network/infrastructure security assessments, and static analysis. Jason is a hacker and bug hunter to the core, and he is ranked 51st all-time on Bugcrowd's leaderboards. Currently, he specializes in recon and web application analysis. Jason has also authored many talks on offensive security methodology, including speaking at cons such as; DEF CON, Black Hat, OWASP, RSA, Nullcon, SANS, IANS, BruCon, Toorcon, and many more. Jason currently lives in Colorado with his wife and three children.

Twitter: [@jhaddix](#)

Description:

Adversaries, red teamer's, and bug bounty hunters share some common TTPs, they all do extensive recon on their targets. Join Jason in this 2hour workshop as he goes through tools and techniques when targeting an organization and its' people. Jason will cover email acquisition, technology profiling, external attack surface (cloud, mobile, ++), historical data mining for endpoints, and much, much more. Jason will walk through each tool in the toolchain, live, for the students while he reveals his own personal tips and tricks in each section. The workshop will be performed on LIVE targets, so fasten your seatbelts! This workshop is a must-see for anyone in the offensive security space.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT

Title: Red Alert ICS CTF

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Red Alert ICS CTF is a competition for Hackers by Hackers. The event exclusively focuses on having the participants break through several layers of security in our virtual SCADA environment and eventually take over complete control of the SCADA system.

The contest would house actual ICS (Industrial Control System) devices from various vendors on a testbed showcasing different sectors of critical infrastructure. The participants would be able to view and engage with the devices in real time and understand how each of them control each of the aspects of the testbed and leverage this to compromise the devices.

Red Alert ICS CTF is back with a ton of fun challenges after successfully running the CTF at DEF CON 30, DEF CON 29, DEF CON 27 and DEF CON 26 (Black Badge).

Highlights of the previous Red Alert ICS CTF is available at: <https://www.youtube.com/watch?v=dz7hNnavHaY> and <https://youtu.be/AanKdrrQ0u0>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-16:59 PDT

Title: Red Alert ICS CTF

When: Saturday, Aug 12, 10:00 - 16:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Red Alert ICS CTF is a competition for Hackers by Hackers. The event exclusively focuses on having the participants break through several layers of security in our virtual SCADA environment and eventually take over complete control of the SCADA system.

The contest would house actual ICS (Industrial Control System) devices from various vendors on a testbed showcasing different sectors of critical infrastructure. The participants would be able to view and engage with the devices in real time and understand how each of them control each of the aspects of the testbed and leverage this to compromise the devices.

Red Alert ICS CTF is back with a ton of fun challenges after successfully running the CTF at DEF CON 30, DEF CON 29, DEF CON 27 and DEF CON 26 (Black Badge).

Highlights of the previous Red Alert ICS CTF is available at: <https://www.youtube.com/watch?v=dz7hNnavHaY> and <https://youtu.be/AanKdrrQ0u0>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Red Alert ICS CTF

When: Friday, Aug 11, 12:00 - 16:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Red Alert ICS CTF is a competition for Hackers by Hackers. The event exclusively focuses on having the participants break through several layers of security in our virtual SCADA environment and eventually take over complete control of the SCADA system.

The contest would house actual ICS (Industrial Control System) devices from various vendors on a testbed showcasing different sectors of critical infrastructure. The participants would be able to view and engage with the devices in real time and understand how each of them control each of the aspects of the testbed and leverage this to compromise the devices.

Red Alert ICS CTF is back with a ton of fun challenges after successfully running the CTF at DEF CON 30, DEF CON 29, DEF CON 27 and DEF CON 26 (Black Badge).

Highlights of the previous Red Alert ICS CTF is available at: <https://www.youtube.com/watch?v=dz7hNnavHaY> and <https://youtu.be/AanKdrrQ0u0>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Red Hot (Red Team TTPs)

When: Saturday, Aug 12, 12:00 - 12:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 3 - [Map](#)

Speakers:Ralph May,Steve Borosh

SpeakerBio:Ralph May

No BIO available

Twitter: [@ralphtel](#)

SpeakerBio:Steve Borosh

No BIO available

Twitter: [@424f424f](#)

Description:

Welcome to our Red Team workshop where we will be discussing the hottest Tactics, Techniques, and Procedures (TTPs) used by Red Teams today. As cyber threats become more sophisticated, it is essential for Red Teams to stay up-to-date with the latest TTPs to ensure their organizations are well-prepared and protected against potential attacks. In this workshop, we will explore the latest TTPs used by Red Teams, including social engineering, post-exploitation, and other malicious techniques that are currently being employed in “advanced” attacks. By the end of this workshop, you will have a better understanding of the latest TTPs, how to use them, and be better equipped to defend against them. Let's get started!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Red Hot (Red Team TTPs)

When: Saturday, Aug 12, 10:00 - 10:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 3 - [Map](#)

Speakers:Ralph May,Steve Borosh

SpeakerBio:Ralph May

No BIO available

Twitter: [@ralphtel](#)

SpeakerBio:Steve Borosh

No BIO available

Twitter: [@424f424f](#)

Description:

Welcome to our Red Team workshop where we will be discussing the hottest Tactics, Techniques, and Procedures (TTPs) used by Red Teams today. As cyber threats become more sophisticated, it is essential for Red Teams to stay up-to-date with the latest TTPs to ensure their organizations are well-prepared and protected against potential attacks. In this workshop, we will explore the latest TTPs used by Red Teams, including social engineering, post-exploitation, and other malicious techniques that are currently being employed in “advanced” attacks. By the end of this workshop, you will have a better understanding of the latest TTPs, how to use them, and be better equipped to defend against them. Let's get started!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Red Hot (Red Team TTPs)

When: Saturday, Aug 12, 15:00 - 15:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 2 - [Map](#)

Speakers:Ralph May,Steve Borosh

SpeakerBio:Ralph May

No BIO available

Twitter: [@ralphtel](#)

SpeakerBio:Steve Borosh

No BIO available

Twitter: [@424f424f](#)

Description:

Welcome to our Red Team workshop where we will be discussing the hottest Tactics, Techniques, and Procedures (TTPs) used by Red Teams today. As cyber threats become more sophisticated, it is essential for Red Teams to stay up-to-date with the latest TTPs to ensure their organizations are well-prepared and protected against potential attacks. In this workshop, we will explore the latest TTPs used by Red Teams, including social engineering, post-exploitation, and other malicious techniques that are currently being employed in “advanced” attacks. By the end of this workshop, you will have a better understanding of the latest TTPs, how to use them, and be better equipped to defend against them. Let's get started!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Red Hot (Red Team TTPs)

When: Friday, Aug 11, 12:00 - 12:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 1 - [Map](#)

Speakers: Ralph May, Steve Borosh

SpeakerBio: Ralph May

No BIO available

Twitter: [@ralphtel](#)

SpeakerBio: Steve Borosh

No BIO available

Twitter: [@424f424f](#)

Description:

Welcome to our Red Team workshop where we will be discussing the hottest Tactics, Techniques, and Procedures (TTPs) used by Red Teams today. As cyber threats become more sophisticated, it is essential for Red Teams to stay up-to-date with the latest TTPs to ensure their organizations are well-prepared and protected against potential attacks. In this workshop, we will explore the latest TTPs used by Red Teams, including social engineering, post-exploitation, and other malicious techniques that are currently being employed in “advanced” attacks. By the end of this workshop, you will have a better understanding of the latest TTPs, how to use them, and be better equipped to defend against them. Let's get started!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Red Hot (Red Team TTPs)

When: Friday, Aug 11, 15:00 - 15:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 2 - [Map](#)

Speakers: Ralph May, Steve Borosh

SpeakerBio: Ralph May

No BIO available

Twitter: [@ralphtel](#)

SpeakerBio: Steve Borosh

No BIO available

Twitter: [@424f424f](#)

Description:

Welcome to our Red Team workshop where we will be discussing the hottest Tactics, Techniques, and Procedures (TTPs) used by Red Teams today. As cyber threats become more sophisticated, it is essential for Red Teams to stay up-to-date with the latest TTPs to ensure their organizations are well-prepared and protected against potential attacks. In this workshop, we will explore the latest TTPs used by Red Teams, including social engineering, post-exploitation, and other malicious techniques that are currently being employed in “advanced” attacks. By the end of this workshop, you will have a better understanding of the latest TTPs, how to use them, and be better equipped to defend against them. Let's get started!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Red Team CTF

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The Red Team Capture the Flag (CTF) competition at DEFCON is a challenging and exciting event that tests the skills of participants in offensive security. The objective of the Red Team CTF is for teams to successfully breach the security of a simulated target network.

The Red Team CTF is designed to simulate real-world scenarios in which attackers attempt to penetrate the security of a network or system. Participants are expected to use a wide range of hacking techniques, tools, and skills to identify and exploit vulnerabilities in the target network.

Teams are typically composed of experienced hackers, penetration testers, and security researchers who have a deep understanding of the latest cybersecurity threats and attack techniques. They must work together to uncover and exploit vulnerabilities in the target network, while also evading detection and countermeasures put in place by the Blue Team.

The Red Team CTF at DEFCON is considered one of the most challenging and prestigious CTF competitions in the world, with participants coming from all over the globe to compete. It is a high-pressure, high-stakes event that tests the limits of participants' technical and strategic abilities, and offers a unique opportunity to showcase their skills and knowledge in front of a global audience of Hackers.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Red Team CTF

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The Red Team Capture the Flag (CTF) competition at DEFCON is a challenging and exciting event that tests the skills of participants in offensive security. The objective of the Red Team CTF is for teams to successfully breach the security of a simulated target network.

The Red Team CTF is designed to simulate real-world scenarios in which attackers attempt to penetrate the security of a network or system. Participants are expected to use a wide range of hacking techniques, tools, and skills to identify and exploit vulnerabilities in the target network.

Teams are typically composed of experienced hackers, penetration testers, and security researchers who have a deep understanding of the latest cybersecurity threats and attack techniques. They must work together to uncover and exploit vulnerabilities in the target network, while also evading detection and countermeasures put in place by the Blue Team.

The Red Team CTF at DEFCON is considered one of the most challenging and prestigious CTF competitions in the world, with participants coming from all over the globe to compete. It is a high-pressure, high-stakes event that tests the limits of participants' technical and strategic abilities, and offers a unique opportunity to showcase their skills and knowledge in front of a global audience of Hackers.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Red Team CTF

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The Red Team Capture the Flag (CTF) competition at DEFCON is a challenging and exciting event that tests the skills of participants in offensive security. The objective of the Red Team CTF is for teams to successfully breach the security of a simulated target network.

The Red Team CTF is designed to simulate real-world scenarios in which attackers attempt to penetrate the security of a network or system. Participants are expected to use a wide range of hacking techniques, tools, and skills to identify and exploit vulnerabilities in the target network.

Teams are typically composed of experienced hackers, penetration testers, and security researchers who have a deep understanding of the latest cybersecurity threats and attack techniques. They must work together to uncover and exploit vulnerabilities in the target network, while also evading detection and countermeasures put in place by the Blue Team.

The Red Team CTF at DEFCON is considered one of the most challenging and prestigious CTF competitions in the world, with participants coming from all over the globe to compete. It is a high-pressure, high-stakes event that tests the limits of participants' technical and strategic abilities, and offers a unique opportunity to showcase their skills and knowledge in front of a global audience of Hackers.

[Return to Index](#) - Add to  - ics [Calendar](#) file


RTV - Friday - 16:00-16:59 PDT

Title: Red Team Labs and Games for Kids

When: Friday, Aug 11, 16:00 - 16:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 5 - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

RTV - Saturday - 09:00-09:59 PDT

Title: Red Team Labs and Games for Kids

When: Saturday, Aug 12, 09:00 - 09:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 5 - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

RTV - Saturday - 10:00-10:59 PDT

Title: Red Team Labs and Games for Kids

When: Saturday, Aug 12, 10:00 - 10:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 5 - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Red Wizard: user-friendly Red Teaming infrastructure

When: Saturday, Aug 12, 12:00 - 13:55 PDT

Where: Caesars Forum - Committee Boardroom - Demo Labs - [Map](#)

SpeakerBio: Ben Brücker

Ben, Secura's Red Teaming lead, has more than 9 years of experience in the field. With a strong passion for Social Engineering, he enjoys employing initial access techniques and has played a pivotal role in creating Secura's user friendly and OPSEC-safe Red Teaming infrastructure. In addition to his Red Teaming responsibilities, Ben also serves as a trainer for various courses and frequently shares his expertise as a public speaker at conferences. Having gained invaluable knowledge from the infosec community, he now aims to contribute back by open sourcing a number of tools and delivering presentations at conferences.

Description:

In this demo I will introduce our new open-source tool called Red Wizard. Red Wizard is the result of years of spinning up repeatable infrastructures for Red Teaming operations. It automates a comprehensive infrastructure deployment with redirectors, backend systems, phishing relays, OSINT machines etcetera. But made easy by providing wizards that walk you through the deployments. Additionally, the infrastructure is self-documenting, making the sharing of all relevant details to your team of operators a breeze. The tool is build to make sure to provide you with a resilient setup that is OPSEC-safe. By retrieving all critical key material from the deployed servers, you will be able to rebuild and keep receiving your shells even if one of your servers crashes and burns. The technology used for Red Wizard is mainly based on Ansible and Docker.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Redeploying the Same Vulnerabilities: Exploiting Wireless Side-Channels in Electric Vehicle Charging Protocols

When: Friday, Aug 11, 16:00 - 16:40 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

Speakers:Richard Baker,Sebastian Kohler

SpeakerBio:Richard Baker

Richard is a researcher in the wireless security industry and visiting academic in the Systems Security Lab, Department of Computer Science, Oxford. He was awarded a DPhil in Cybersecurity from University of Oxford in 2020 and previously an MEng in Computing from Imperial College London in 2010. He is an alumnus of the CDT in Cybersecurity (2014 -- 2019) and a founding member of Oxford Competitive Computer Security Society / Ox002147 CTF team.

SpeakerBio:Sebastian Kohler

Sebastian is a Postdoctoral Research Associate in the Systems Security Lab, Department of Computer Science at the University of Oxford, where he coordinates the research activities in wireless and physical-layer security. His work focuses on the security of various systems, ranging from space and satellite systems to autonomous and electric vehicles. For his work during his PhD, which revealed a serious vulnerability in a widely used electric vehicle charging protocol, he was awarded the EPSRC Doctoral Prize and MPLS Early Career Research Impact Award.

Description:

The Combined Charging System (CCS), one of the most widely used DC rapid charging technologies for EVs, is vulnerable to wireless attacks. The charging cable acts as unintentional antenna, leaking the power-line communication (PLC) signals and letting an adversary inject their own with off-the-shelf radio equipment. We show how we can eavesdrop on charging communication, or terminate multiple charging sessions wirelessly. These vulnerabilities have been known for several years, but are still present in CCS standards, while the new North American Charging Standard (NACS) uses the same vulnerable physical layer as well. How do we secure these charging systems now we're in so deep?

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Friday - 09:00-17:59 PDT

Title: RegEx Trainer

When: Friday, Aug 11, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Is regex a mystery to you? We've got your back at the Packet Hacking Village. Our new interactive REGEX Trainer will walk you through learning then doing, giving you a full understanding of how Regular Expressions work.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Saturday - 09:00-17:59 PDT


Title: RegEx Trainer

When: Saturday, Aug 12, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Is regex a mystery to you? We've got your back at the Packet Hacking Village. Our new interactive REGEX Trainer will walk you through learning then doing, giving you a full understanding of how Regular Expressions work.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Sunday - 09:00-12:59 PDT

Title: RegEx Trainer

When: Sunday, Aug 13, 09:00 - 12:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

Is regex a mystery to you? We've got your back at the Packet Hacking Village. Our new interactive REGEX Trainer will walk you through learning then doing, giving you a full understanding of how Regular Expressions work.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Retro Exploitation: Using Vintage Computing Platforms as a Vulnerability Research Playground and Learning Environment

When: Sunday, Aug 13, 12:00 - 12:45 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

SpeakerBio: Wesley McGrew , Senior Cyber Fellow at MartinFed

Dr. Wesley McGrew directs research, development, and offensive cyber operations as Senior Cybersecurity Fellow for MartinFederal. He has presented on topics of penetration testing and malware analysis at DEF CON and Black Hat USA and taught a self-designed course on reverse engineering to students at Mississippi State University, using real-world, high-profile malware samples. Wesley has a Ph.D. in Computer Science from Mississippi State University for his research in vulnerability analysis of SCADA HMI systems.

Twitter: [@McGrewSecurity](#)

Description:

It can be very difficult for those new to hacking to learn about vulnerability discovery and exploit development on modern operating systems and software. The complexity of a modern computing environment, developer awareness of security risks, and the iterative development of exploit mitigations over the past three decades has put up an intimidating wall in front of those who would be interested in learning about vulnerability research. Vintage computing environments can provide an interesting and fun playground environment for learning and experimenting with reverse engineering, vulnerability discovery, and exploit development.

In this talk, Wesley will discuss the setup of a complete environment for hacking software for the Commodore Amiga line of computers, a 16/32 bit computing platform of the late 80s and early 90s (not to mention a dedicated following of users and software today). He will describe the hardware environment, OS architecture, and the practically endless library of software that can be used as interesting targets of research. On-system development and debugging software will be described, as well as using the modern Ghidra disassembler. A case study of identifying and exploiting a vulnerability in a 1994 vintage FTP client will be discussed in technical detail.

REFERENCES


◇ Vintage Computing preservation

- <https://www.tosecdev.org/> - TOSEC catalogs all known software and documentation for many vintage computing platforms
- <https://archive.org/> - Hosts tremendous archives of vintage documentation, magazines, software, etc
 - Books (largely available on archive.org)
- The AmigaDOS Manual, 3rd Edition
- Lance Leventhal - 68000 Assembly Language Programming, Second Edition
- M68000 Programmer's Reference Manual
- Amiga ROM Kernel Reference Manual, 3rd Edition, Volumes:
 - Libraries
 - Devices
 - Hardware Reference Manual
- Devpac 3 for the Amiga - User Manual
- SAS/C Development System User's Guide (vol. 1 & 2)
 - Development Kit Documentation
- Amiga OS NDK 3.2 -
<https://www.hyperion-entertainment.com/index.php/downloads?view=files&parent=40>
- Amiga Developer CD 1.2 (1998, available on archive.org)
 - Previous talks that involved vintage computing
- DC30 - Tristan Miller - Reversing the Original Xbox Live

Protocols

· DC30 - Cesare Pizzi - Old Malware, New tools: Ghidra and

Commodore 64

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Saturday - 12:30-13:20 PDT

Title: Review: Surprise Unboxing

When: Saturday, Aug 12, 12:30 - 13:20 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio:Harri Hursti

Harri Hursti, a world renowned data security expert and internet visionary is the Founder of the 501(c)(3) organization the Election Integrity Foundation as well as an original co-Founder of the Voting Village. Featured in two Emmy nominated documentaries, Mr. Hursti is famously known for the Hursti Hacks, where he demonstrated how to successfully alter final voting results on the Diebold Election Systems voting machines.

Twitter: [@harrihursti](#)

Description:

The Voting Village will review it's initial analysis from the high-profile unboxing from the day before.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Revolutionizing ELF binary patching with Shiva: A JIT binary patching system for Linux

When: Saturday, Aug 12, 15:00 - 15:45 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

SpeakerBio: Ryan "ElfMaster" O'Neill, CTO at Arcana Technologies
Ryan "ElfMaster" O'Neill, has been in the security scene since about 1997.

Ryan is well known for authoring the book "Learning Linux binary analysis" and for publishing many papers and technologies in the realm of binary protection, memory forensics, exploitation, security mitigations, virus design, kernel hacking and reverse engineering techniques. Ryan has been published in many of the classic journals such as Phrack, POC||GTFO, tmp.Out and vxheaven. Much of Ryan's independent research has been published over the years on <https://www.bitlackeys.org>, and has many public technologies available on <https://github.com/elfmaster>. Ryan is also the founder of Arcana technologies <https://arcana-technologies.io>, a threat detection company based heavily on ELF forensics research. Ryan is currently building a new ELF binary patching system for Linux to solve the worlds hardest challenges in binary patching today.

Twitter: [@ryan_elfmaster](#)

Description:

The esoteric art of patching ELF binaries has a long and fascinating history who's roots are deep within the hacking subculture; from ELF viruses to kernel rootkits. Silvio's 1997 "UNIX Viruses" paper taught us how to insert parasitic code into a page aligned text padding region. Many backdooring and hooking techniques have been revealed to us over the last 20 years-- perfect for hacking and injecting small patches and backdoors but on their own these techniques are limited, clunky and do not support the complexities of real-world patching problems in todays industry. Developers often need to fix complex bugs that exist within legacy ELF Binaries, no source code is available or the program cannot be recompiled.

Let me introduce you to Shiva. Shiva is a JIT binary patching system for ELF; A custom ELF interpreter that loads and links ELF relocatable patches at runtime. Shiva allows developers to write patches in rich C code to naturally express the rewriting of binary code at runtime, in a high level language. ELF binary patching solutions over the past two decades have been scarce; some notable research: Katana and ERESI come to mind as pioneers in the early examples of custom ELF linkers and binary patchers.

Shiva is a next-level solution that allows developers to quickly write patches in C with little to no reversing knowledge. Born out of 16 years of ELF research into virus design, binary patching, and extensive experience with writing custom linkers and loaders.

In this talk we will discuss foundations of ELF binary patching and it's close relationship with ELF linkers, loaders and even ELF virus technology. This passionate body of research is combined and imbued into Shiva to create a highly innovative and powerful product that helps bridge the gap between Developers and Reverse engineers in modern binary patching solutions for ELF. A new workflow for maintaining insecure legacy software with modular patching capabilities is on the rise!

Prepare for an indepth discussion of incredible new ELF hacking techniques and extensions. Old concepts such as userland-exec() brought back to life, and entirely new concepts such as "Linker chaining" to bring multiple dynamic linkers into a single process image. We will demonstrate complex patching scenarios, function splicing, program transformation, and even the weaponization of Shiva for writing sophisticated in-memory backdoors. Shiva; the ultimate ELF Binary hacker... aiming to solve the worlds most challenging binary patching problems today.

REFERENCES

--Papers-- Grugq - userland execve: https://grugq.github.io/docs/ul_exec.txt Mayhem - Cerberus ELF interface: <http://phrack.org/issues/61/8.html> Silvio - UNIX Viruses and parasites: <https://vxug.fakedoma.in/archive/VxHeaven/lib/vsc02.html> James Oakley & Sergey Bratus - Katana: A hot patching framework: <https://ieeexplore.ieee.org/document/5438048> James Oakley & Sergey Bratus - Exploiting the hard

working DWARF: https://www.cs.dartmouth.edu/~sergey/battleaxe/hackito_2011_oakley_bratus.pdf Mlaurenzano - PEBIL (An ELF patching framework) - <https://github.com/mlaurenzano/PEBIL> sd & devik - Linux on-the-fly kernel patching without LKM: phrack.org/issues/58/7.html jbtznm - static kernel patching - <https://phrack.org/issues/60/8.html> Elfmaster - Modern ELF infection techniques of SCOP binaries (POC||GTFO: 20:07) Elfmaster - Preloading the linker for fun and profit: <https://tmpout.sh/2/6.html> (This paper presents the nucleus of Shiva) Mayhem - IA32 Advanced function hooking: <http://phrack.org/issues/58/8.html> Richinseattle - Hooking the ELF loader: <http://phrack.org/issues/58/8.html> Silvio - Shared library call redirection via PLT infection: <http://phrack.org/issues/56/7.html> Elfmaster - Kernel instrumentation using kprobes: <http://phrack.org/issues/56/7.html> Mayhem - Next generation ELF debuggers: <https://www.blackhat.com/presentations/bh-europe-07/ERSI/Presentation/bh-eu-07-ersi-apr19.pdf>

--A note on the illustrious tmp.Out zine: <https://tmpout.sh>

The crew at tmp.Out are a tightly formed group ELF hackers and reversing enthusiasts who are continuing to research and publish awesome ELF research on a regular basis. I highly recommend their content, and am grateful for their many new contributions keeping the spirit of ELF hacking alive. Translated into nine different languages currently.

--Source code--

https://github.com/torvalds/linux/blob/master/fs/binfmt_elf.c (Source for Linux ELF loader)
<https://www.gnu.org/software/binutils> (Source for for ELF /bin/ld) <https://sourceware.org/git/glibc.git> (Source code for ld-linux.so) <https://github.com/elfmaster> (My own ELF hacking related research)
https://github.com/elfmaster/linker_preloading_virus (My first custom ELF interpreter) <https://musl.libc.org/>
<https://github.com/bminor/binutils-gdb> <- These GDB guys really don't get enough credit.

--Books--

Understanding the Linux kernel (Great book on kernel internals) Learning Linux binary analysis (elfmaster) Advanced programming in the UNIX environment (Richard Stevenson) Turbo C (Old book from the 80s I learned C from)

[Return to Index](#) - Add to  - ics [Calendar](#) file

TCV - Sunday - 10:00-10:30 PDT

Title: RF in the Middle Earth- Fallen 5G

When: Sunday, Aug 13, 10:00 - 10:30 PDT

Where: Flamingo - Virginia City - Telecom Village - [Map](#)

SpeakerBio:Utku Y

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file


RFV - Friday - 11:00-11:25 PDT

Title: RF Village Kickoff

When: Friday, Aug 11, 11:00 - 11:25 PDT

Where: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

PSV - Saturday - 12:00-12:30 PDT

Title: RFID Hacking


When: Saturday, Aug 12, 12:00 - 12:30 PDT

Where: Flamingo - Carson City - Physical Security Village - [Map](#)

SpeakerBio:Ege

Ege is a security researcher specialising in access control systems and electronics. She is currently pursuing a degree in Electrical Engineering and work part-time for GGR Security as a Security Risk Assessor.

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

RCV - Saturday - 16:20-17:05 PDT

Title: Riding with the Chollimas: Our 100-Day Quest to Identify a North Korean State-Sponsored Threat Actor

When: Saturday, Aug 12, 16:20 - 17:05 PDT

Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio:Mauro Eldritch

No BIO available

Twitter: [@@mauroeldritch](#)

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Risk Limiting Audits Of All Contests

When: Friday, Aug 11, 14:10 - 14:45 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio: Amanda Glazer

Amanda Glazer is a PhD candidate in statistics at UC Berkeley advised by Philip Stark. Her research focuses on causal inference with applications in the social sciences. One of her main research areas is election integrity and risk-limiting audits. Risk-limiting audits (RLAs) manually inspect ballots from a trustworthy record of the votes to provide affirmative evidence that electoral outcomes are correct if they are indeed correct, and to correct any outcomes that are wrong. In her research she has developed methods to increase the efficiency of RLAs (i.e., decrease the number of ballots you have to inspect to confirm an election outcome is correct, if it really is).

Twitter: [@PandaGlazer](#)

Description:

The principle of evidence-based elections is that elections should provide convincing evidence that the reported winners really won. Risk-limiting audits (RLAs) manually inspect ballots from a trustworthy record of the votes to provide affirmative evidence that electoral outcomes are correct if they are indeed correct, and to correct any outcomes that are wrong. When the outcome is correct, RLAs may inspect only a small fraction of all ballot cards, saving considerable labor compared to a full manual recount. Using information about which ballot cards contain which contests (card-style data, CSD) further reduces labor. In this talk, I give an overview of how RLAs work, and new advancements that substantially reduce workload. Using data from the 2020 and 2022 general elections in Orange County, I demonstrate the efficiency of RLAs that take into account CSD. I conclude with a demo showing how RLAs work.

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Friday - 15:30-16:15 PDT

Title: RLA Workshop

When: Friday, Aug 11, 15:30 - 16:15 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio: Amanda Glazer

Amanda Glazer is a PhD candidate in statistics at UC Berkeley advised by Philip Stark. Her research focuses on causal inference with applications in the social sciences. One of her main research areas is election integrity and risk-limiting audits. Risk-limiting audits (RLAs) manually inspect ballots from a trustworthy record of the votes to provide affirmative evidence that electoral outcomes are correct if they are indeed correct, and to correct any outcomes that are wrong. In her research she has developed methods to increase the efficiency of RLAs (i.e., decrease the number of ballots you have to inspect to confirm an election outcome is correct, if it really is).

Twitter: [@PandaGlazer](#)

Description:

The workshop is a bare bones example of the core statistical method, for auditing a single contest, without relying on any exported data from the voting system. If there are three - four teams with three - four people and they are on task, this workshop will last forty five minutes with time for Q&A.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Saturday - 13:00-13:59 PDT

Title: RoboSumo Bracket Competition

When: Saturday, Aug 12, 13:00 - 13:59 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlg - [Map](#)

Description:

Bring your official Mini Sumo class robots to go head to head in a battle of glory! For rule details see <https://dchhv.org/events/robosumo.html> Event will last as long as it takes to work through the bracket.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Sunday - 10:00-12:59 PDT

Title: RoboSumo Play Time

When: Sunday, Aug 13, 10:00 - 12:59 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Description:

A little to shy to own the ring in open battle? Come play! There will be robots available to program, sample code, a ring and many opportunities to discover some of the fun of robotics.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Saturday - 10:00-17:59 PDT

Title: RoboSumo Play Time

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Description:

A little to shy to own the ring in open battle? Come play! There will be robots available to program, sample code, a ring and many opportunities to discover some of the fun of robotics.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Friday - 10:00-17:59 PDT

Title: RoboSumo Play Time

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlg - [Map](#)

Description:

A little to shy to own the ring in open battle? Come play! There will be robots available to program, sample code, a ring and many opportunities to discover some of the fun of robotics.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Route to bugs: Analyzing the security of BGP message parsing

When: Friday, Aug 11, 10:30 - 11:15 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

Speakers: Daniel dos Santos, Simon Guiot

SpeakerBio: Daniel dos Santos , Head of Security Research at Forescout

Daniel dos Santos is the Head of Security Research at Forescout's Vedere Labs, where he leads a team of researchers that identifies new vulnerabilities and monitors active threats. He holds a PhD in computer science, has published over 35 peer-reviewed papers on cybersecurity, has found or disclosed hundreds of CVEs and is a frequent speaker at security conferences.

SpeakerBio: Simon Guiot , Security Researcher at Forescout

Simon Guiot has experience in software engineering and software vulnerability management. He is currently a Security Researcher at Forescout Technologies doing vulnerability and threat research.

Description:

This talk discusses an overlooked aspect of Border Gateway Protocol (BGP) security: vulnerabilities in how its implementations parse BGP messages. Software implementing BGP is relied upon for Internet routing and for functions such as internal routing in large data centers. A lot of (deserved) attention is given to aspects of BGP protocol security discussed in [RFC4272](#), which can be mitigated with the use of RPKI and BGPsec. However, recent BGP incidents show that it might take only a malformed packet to cause a large disruption. We will present a quantitative analysis of previous vulnerabilities in both open and closed-source popular BGP implementations and focus the talk on a new analysis of seven modern implementations.

Main findings in this research include:

1. Some implementations process parts of OPEN messages before validating the BGP ID and ASN fields of the originating router, which means that only TCP spoofing is required to inject malformed packets.
2. Three new vulnerabilities in a leading open-source implementation, which could be exploited to achieve denial of service on vulnerable peers, thus dropping all BGP sessions and routing tables and rendering the peer unresponsive. These vulnerabilities were found using a fuzzer we developed and will release to the community.

REFERENCES

- <https://www.blackhat.com/presentations/bh-usa-03/bh-us-03-convery-franz-v3.pdf>
- <https://datatracker.ietf.org/doc/html/rfc4272>
- <https://www.oecd.org/publications/routing-security-40be69c8-en.htm>
- <https://www.zdnet.com/article/internet-experiment-goes-wrong-takes-down-a-bunch-of-linux-routers/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

DL - Saturday - 14:00-15:55 PDT

Title: RuleProcessorY & Gramify - Rule Optimization & Password Analysis tools

When: Saturday, Aug 12, 14:00 - 15:55 PDT

Where: Caesars Forum - Caucus Boardroom - Demo Labs - [Map](#)

SpeakerBio: Niels Loozekoot

Working as Pentester Niels has an extensive background in the security field. Niels has a background in web-development and knows his way around C, C++, C#, and Python and is active in the password cracking/research communities of Hashcat, Hashkiller, and HashMob. Winning in the CrackTheCon password cracking contest, and achieving 3rd place in both the CrackMeIfYouCan 2021 & 2022.

Description:

The RuleProcessorY and Gramify tools are new tools that support password-cracking efforts. RuleProcessorY offers a method of optimizing hashcat rule-files so that you can prevent duplicates across multiple attacks better, leading to a shorter runtime. Additionally it can process rules as hashcat would with an additional support for multi-byte/multi-character rules (inserts & replace primarily). Gramify offers an easy method to create base words and candidates to utilize with wordlist and combination attacks by splitting data by words, characters, or character-set. This can help with password phrases, quotes, sentences, combinator attacks, and extracting base-words from passwordlists.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Runtime Riddles: Abusing Manipulation Points in the Android Source

When: Saturday, Aug 12, 16:00 - 16:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio:Laurie Kirk , Security Researcher at Microsoft

Laurie Kirk is a Reverse Engineer at Microsoft working in incident response. She specializes in cross-platform malware analysis with a focus on mobile threats. She also runs a YouTube channel (@LaurieWired) that covers all sorts of in-depth Malware Analysis, Reverse-Engineering, Exploitation and security topics. Laurie received her Bachelor's Degree from Florida State University in Computer Science with a minor in Math. She started as a Software Engineer for an aerospace company before finding her current calling in Cyber Security and low-level programming.

Twitter: [@LaurieWired](#)

Description:

Android malware creators constantly struggle to devise innovative methods to obscure apps and impede reverse engineering. As numerous standard techniques have lost efficacy, I'll unveil the next frontier in Android obfuscation: runtime manipulation. Runtime manipulation alters standard application flow-of-control to bypass decompilers and emulators.

In this talk, I'll reveal my strategy for pinpointing manipulation targets in Android's source code. I will describe how I craft manipulators in native C++ once a suitable target has been located. This is accomplished by hooking Java methods via the Java Native Interface (JNI) and typecasting the handle to a C-style pointer. Runtime manipulation can entirely remove traces of ClassLoader calls which are unavoidable for standard Dalvik Executable (DEX) packing, but are also easily discovered and hooked. This technique also effectively breaks cross-reference calculations within all Android decompilers.

I will demonstrate and equip attendees with a custom Android library for devices running Android 13, providing a new tool that enables runtime manipulation experimentation. In addition, I'll demonstrate my methodology for pinpointing Java targets and modifying their underlying native data structures.

REFERENCES

<https://security.csl.toronto.edu/wp-content/uploads/2018/06/mwong-usenixsec2018-tiro.pdf>

ArtMethod hooking: <https://github.com/PAGalaxyLab/YAHFA> mCookie manipulation:

<https://github.com/woxihuannisja/Bangle> DexFile.java:

<https://cs.android.com/android/platform/superproject/+/master:libcore/dalvik/src/main/java/dalvik/system/DexFile.java>

dex_file.h: https://cs.android.com/android/platform/superproject/+/refs/heads/master:art/libdexfile/dex/dex_file.h

art_method.h: https://cs.android.com/android/platform/superproject/+/master:art/runtime/art_method.h;bpv=0;bpt=0

Executable.java – contains artMethod field:

<https://cs.android.com/android/platform/superproject/+/master:libcore/ojuni/src/main/java/java/lang/reflect/Executable.java;l=582>

[Return to Index](#) - Add to  - [ics Calendar file](#)

Title: Sadprotocol Goes To Hollywood: Hijacking An Ip Camera Stream As Seen In The Movies

When: Friday, Aug 11, 13:00 - 13:50 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Speakers:Javier Aguinaga,Octavio Gianatiempo

SpeakerBio:Javier Aguinaga

Javier Aguinaga is a self-taught reverse engineer with a principal focus in exploiting, currently working at Faraday for the last 7 years. He started his journey as a hobbyist electronic enthusiast and began learning how to crack security systems for video games. This led him to pursue a career in reverse engineering, where he has gained extensive experience analyzing and breaking down complex systems. With his expertise, Javier has been able to identify vulnerabilities in various technologies and has presented his findings at several conferences. He looks forward to sharing his insights and learning from others at the upcoming conference.

SpeakerBio:Octavio Gianatiempo , Security Researcher at Faraday

Octavio Gianatiempo is a Security Researcher at Faraday and a Computer Science student at the University of Buenos Aires. He's also a biologist with research experience in molecular biology and neuroscience. The necessity of analyzing complex biological data was his point of entry into programming. But he wanted to achieve a deeper understanding of how computers work, so he enrolled in Computer Science. As a Security Researcher at Faraday, he focuses on embedded devices, reverse engineering and fuzzing open and closed source software to find new vulnerabilities and exploit them.

Description:

When people think about a compromised surveillance camera, privacy is their first concern. But what about attacking the stream integrity? How hard can this movie hacking stunt be in real life? Previous research has focused on the network layer, but we wondered if we could achieve the feat by finding a zero-day on a device we owned.

Our research has uncovered two LAN RCE vulnerabilities in the implementation of Hikvision's Search Active Devices Protocol (SADP) and SDK server found in several Ezviz products. Exploiting either of these bugs, we managed to serve a victim an arbitrary stream by tunneling their connection with the camera into an attacker-controlled server while leaving all other camera features operational.

We will take a deep dive into the whole research process: firmware analysis, vulnerability discovery, building a toolchain to compile a debugger for the target, developing an exploit capable of bypassing ASLR, and all the details about the Hollywood-style post-exploitation including tracing, in memory code patching and manipulating the execution of the binary that implements most of the camera features.

By filling the gap between IoT hacking and the big screen, we put the integrity of video surveillance systems into question and hope to raise awareness about the security risks posed by these devices.

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Sunday - 11:00-11:59 PDT

Title: Safecracking for Everyone

When: Sunday, Aug 13, 11:00 - 11:59 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

SpeakerBio:Jared Dygert

No BIO available

Description:

This talk covers the workings of mechanical combination safe locks, their vulnerabilities, and how to manipulate them.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DL - Saturday - 10:00-11:55 PDT

Title: Saturday

When: Saturday, Aug 12, 10:00 - 11:55 PDT

Where: Caesars Forum - Council Boardroom - Demo Labs - [Map](#)

SpeakerBio:Joshua Herman

I am a release engineer specializing in compliance of information security vendors for post trade currencies. Previously I was a software engineer with experience with distributed computing and UI / UX using Python and Javascript in the same department . I have a decade of professional experience in software engineering in various industries such as insurance, CRM, Trade Show applications, recommender systems and cryptocurrency . I also have contributions to open source projects such as CPython documentation, triaging and features.

Description:

This tool is a digital assistant that helps you hack. Under the hood it uses langchain (a way to augment LLMs) that currently uses an SMS / MMS / Phone interface that will allow for basic information retrieval tasks (google search, searching shodan, google places) and has the goal of doing complex offensive and defensive security tasks using anything from a dumb phone to a smartphone. It is preprogramed with tools that it can intelligently use to accomplish certain tasks such as performing a search on shodan given an IP address.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Scoping for Success (Building a Great Bug Bounty program)

When: Sunday, Aug 13, 13:15 - 13:59 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

Speakers:Jeffrey Guerra,Logan MacLaren

SpeakerBio:Jeffrey Guerra

Jeff is an enthusiastic person who has a passion for Application Security and the power of Bug Bounty programs. During his free time, Jeff is a car enthusiast that goes to the race track, bug hunt, and go on trips with friends and family.


Twitter: [@s2jeff_gh](#)

SpeakerBio:Logan MacLaren

Logan has been a cybersecurity enthusiast since getting online in the 90s and currently focuses on helping grow GitHub's Bug Bounty program. During his free time, Logan dabbles in powerlifting, CTFs, and retro gaming.

Description:

Jeff & Logan, Security Engineers at GitHub, share best practices they've learned regarding building and operating Bug Bounty programs based on their experiences working at and with multiple companies. Come and learn from their mistakes and successes so that you can be set up for success, attract researchers to your program, and keep them coming back!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Scripting OWASP Amass for a Customized Experience

When: Saturday, Aug 12, 12:00 - 13:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 4 - [Map](#)

SpeakerBio: Jeff Foley

No BIO available

Twitter: [@jeff_foley](#)

Description:

This course is for practitioners who would like to have accurate visibility and results when mapping an organization's external attack surface. We will use the open source tool, provided by the OWASP Amass Project, to better understand how to hunt down assets exposed on the Internet. Many professionals have leveraged the basic Amass features during their red team exercises and other information security efforts, but not extended the capabilities of the engine to implement new features and data sources. We will use hands-on exercises to have you become familiar with the Amass Engine, comfortable extending it, and aware of future directions for the project. Participants are encouraged to complete the exercises by writing the extensions in the Lua programming language. All the examples will be provided for those unfamiliar with the language.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Scripting OWASP Amass for a Customized Experience

When: Friday, Aug 11, 12:00 - 13:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 6 - [Map](#)

SpeakerBio: Jeff Foley

No BIO available

Twitter: [@jeff_foley](#)

Description:

This course is for practitioners who would like to have accurate visibility and results when mapping an organization's external attack surface. We will use the open source tool, provided by the OWASP Amass Project, to better understand how to hunt down assets exposed on the Internet. Many professionals have leveraged the basic Amass features during their red team exercises and other information security efforts, but not extended the capabilities of the engine to implement new features and data sources. We will use hands-on exercises to have you become familiar with the Amass Engine, comfortable extending it, and aware of future directions for the project. Participants are encouraged to complete the exercises by writing the extensions in the Lua programming language. All the examples will be provided for those unfamiliar with the language.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SEV - Saturday - 11:30-13:30 PDT

Title: SE Improv

When: Saturday, Aug 12, 11:30 - 13:30 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description:

Improv is when two (or more) actors don't know their lines ahead of time, but both agree on a set of rules and on the goal of getting somewhere together.

Social engineering is a form of improv in which two (or more) people come together to reach a goal only one person (the 'actor') has knowledge of, using rules the other (the target) defines along the way.

At least, that's how we see it. Led by three facilitators who are both information security professionals and improvisers, this first-time program will give attendees an introduction to improv and its special communication techniques. Parallels will be drawn between improv and social engineering, including examples of how the theories and practices of improv can be applied by social engineers to work with their targets in an effective, ethical, and even collaborative way.

This engaging program will consist of demonstrations, explanations, and interactions in which attendees will be invited to try out improvisation* themselves in a safe, participatory "sandbox" to apply the concepts learned.

Come find out why some of the world's best social engineers utilize these techniques to improv(e) their game.

- No requirement to perform in front of people nor to be funny.

Please see the "More Information" link.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Second Breakfast: Implicit and Mutation-Based Serialization Vulnerabilities in .NET

When: Friday, Aug 11, 14:30 - 15:15 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

SpeakerBio: Jonathan Birch , Principal Security Software Engineer at Microsoft

Jonathan Birch is a Principal Security Software Engineer for Microsoft. He hacks Office. His previous talks include "Host/Split: Exploitable Antipatterns in Unicode Normalization" at Black Hat 2019 and "Dangerous Contents - Securing .NET Deserialization" at BlueHat 2017.

Description:

Exploits of insecure serialization leading to remote code execution have been a common attack against .NET applications for some time. But it's generally assumed that exploiting serialization requires that an application directly uses a serializer and that it unsafely reads data that an attacker can tamper with. This talk demonstrates attacks that violate both of these assumptions. This includes serialization exploits of platforms that don't use well-known .NET serializers and methods to exploit deserialization even when the serialized data cannot be tampered with. Remote code execution vulnerabilities in MongoDB, LiteDB, ServiceStack.Redis, RavenDB, MartenDB, JSON.Net and the .NET JavaScriptSerializer are all demonstrated. Techniques to both scan for and mitigate these vulnerabilities are also discussed.

REFERENCES

* "Are You My Type? Breaking .net Sandboxes Through Serialization", James Forshaw, Black Hat 2012 * "Friday the 13th JSON Attacks", Alvaro Muñoz & Oleksandr Mirosh, Black Hat 2017 * See also: <https://github.com/pwntester/ysoserial.net> for useful payload generators.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Secretary of the Department of Homeland Security Alejandro Mayorkas

When: Friday, Aug 11, 09:30 - 10:15 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio: Alejandro Mayorkas , Secretary at Department of Homeland Security

Alejandro Mayorkas was sworn in as Secretary of the Department of Homeland Security by President Biden on February 2, 2021.


A political refugee born in Havana, Cuba, Mayorkas is the first Latino and immigrant confirmed to serve as Secretary of Homeland Security. He has led a distinguished 30-year career as a law enforcement official and a nationally recognized lawyer in the private sector. Mayorkas served as the Deputy Secretary of the U.S. Department of Homeland Security from 2013 to 2016, and as the Director of U.S. Citizenship and Immigration Services from 2009 to 2013. During his tenure at DHS, he led the development and implementation of DACA, negotiated cybersecurity and homeland security agreements with foreign governments, led the Department's response to Ebola and Zika, helped build and administer the Blue Campaign to combat human trafficking, and developed an emergency relief program for orphaned youth following the tragic January 2010 earthquake in Haiti. Mayorkas also created the Fraud Detection and National Security Directorate to better ensure the integrity of the legal immigration system.

Mayorkas began his government service in the Department of Justice, where he served as an Assistant United States Attorney in the Central District of California, specializing in the prosecution of white collar crime. After nearly nine years as a federal prosecutor, he became the youngest United States Attorney in the nation, overseeing prosecutions of national significance, including the investigation and prosecution of financial fraud, violations of the Foreign Corrupt Practices Act, public corruption, violent crime, cybercrime, human trafficking, environmental crime, international narcotics money laundering, and securities fraud.

Mayorkas received his bachelor's degree with distinction from the University of California at Berkeley and a law degree from Loyola Law School.

Description:

The Secretary of US Homeland Security, Alejandro Mayorkas, joins DEF CON for a fireside chat. Secretary Mayorkas will lay some foundational groundwork on some of DHS' priorities in cybersecurity and how they address pressing IS and global issues, then sit down to talk with The Dark Tangent, in a casual conversation with thousands of their closest hacker friends.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Secure by Design: Ask the Government Anything and Red-Pen Workshop

When: Saturday, Aug 12, 11:00 - 13:50 PDT

Where: Caesars Forum - Summit - 220 - Policy NOT-A-SCIF - [Map](#)

Speakers: Bob Lord, Cheri Caddy, Jack Cable, Jen Easterly, Lauren Zabierek, Oumou Ly, Yael Grauer

SpeakerBio: Bob Lord , Senior Technical Advisor at Cybersecurity and Infrastructure Security Agency (CISA)

Bob Lord joined the Cybersecurity and Infrastructure Security Agency (CISA) as a Senior Technical Advisor in April 2022. Previously he was the Chief Security Officer at the Democratic National Committee where he brought more than 20 years of experience in the information security space to the committee, state parties, and campaigns. Before that he was Yahoo's Chief Information Security Officer, covering areas such as risk management, product security, security software development, e-crimes and APT programs. He was the Chief Information Security Officer in Residence at Rapid7, and before that headed up Twitter's information security program as its first security hire.

SpeakerBio: Cheri Caddy , Deputy Assistant National Cyber Director for Cyber Technology, Research & Development at Office of the National Cyber Director at the White House

Cheri Caddy is the Deputy Assistant National Cyber Director for Cyber Technology, Research & Development in the Office of the National Cyber Director at the White House. In this role she leads technical strategy and policy for national cyber programs on R&D, operational technology, securing the clean energy transition, technical standards, and software liability. Over the past 30 years, Cheri has held senior cyber technology and policy roles at the Department of Energy, the Intelligence Community, and the National Security Council. Cheri is a Senior Cybersecurity Fellow at the McCrary Institute for Cybersecurity & Critical Infrastructure.

SpeakerBio: Jack Cable , Senior Technical Advisor at Cybersecurity and Infrastructure Security Agency (CISA)

Jack Cable is a Senior Technical Advisor at the Cybersecurity and Infrastructure Security Agency (CISA). Prior to that, Jack worked as a TechCongress Fellow for the Senate Homeland Security and Governmental Affairs Committee, advising Chairman Gary Peters on cybersecurity policy, including election security and open source software security. He previously worked as a Security Architect at Krebs Stamos Group. Jack also served as an Election Security Technical Advisor at CISA, where he created Crossfeed, a pilot to scan election assets nationwide. Jack is a top bug bounty hacker, having identified over 350 vulnerabilities in hundreds of companies. After placing first in the Hack the Air Force bug bounty challenge, he began working at the Pentagon's Defense Digital Service. Jack holds a bachelor's degree in Computer Science from Stanford University and has published academic research on election security, ransomware, and cloud security.

SpeakerBio: Jen Easterly , Director at Cybersecurity and Infrastructure Security Agency (CISA)

Jen Easterly is the Director of the Cybersecurity and Infrastructure Security Agency (CISA). She was nominated by President Biden in April 2021 and unanimously confirmed by the Senate on July 12, 2021. As Director, Jen leads CISA's efforts to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every day. She is a proud Mom, a mental health advocate, a Rubik's Cube enthusiast, and an aspiring electric guitarist.

Before serving in her current role, Jen was the head of Firm Resilience at Morgan Stanley, responsible for ensuring preparedness and response to business-disrupting operational incidents and risks to the Firm. She also helped build and served as the first Global Head of Morgan Stanley's Cybersecurity Fusion Center, the Firm's center of gravity for cyber defense operations.

Jen has a long tradition of public service, to include two tours at the White House, most recently as Special Assistant to President Obama and Senior Director for Counterterrorism and earlier as Executive Assistant to National Security Advisor Condoleezza Rice. She also served as the Deputy for Counterterrorism at the National Security Agency.

A two-time recipient of the Bronze Star, Jen retired from the U.S. Army after more than twenty years of service in intelligence and cyber operations, including tours of duty in Haiti, the Balkans, Iraq, and Afghanistan. Responsible for standing up the Army's first cyber battalion, she was also instrumental in the design and creation of United States Cyber Command.

A distinguished graduate of the United States Military Academy at West Point, Jen holds a master's degree in Philosophy, Politics, and Economics from the University of Oxford, where she studied as a Rhodes Scholar. She is the recipient of numerous honors and awards, including the 2023 Sisterhood Award from Girls Who Code; the 2022 National Defense University Admiral Grace Hopper Award; the 2021 Cybersecurity Ventures Cybersecurity Person of the Year Award; the 2020 Bradley W. Snyder Changing the Narrative Award, and the 2018 James W. Foley Legacy Foundation American Hostage Freedom Award.

A member of the Council on Foreign Relations and a French American Foundation Young Leader, Jen is the past recipient of the Aspen Finance Leaders Fellowship, the National Security Institute Visiting Fellowship, the New America Foundation Senior International Security Fellowship, the Council on Foreign Relations International Affairs Fellowship, and the Director, National Security Agency Fellowship.

Twitter: [@@CISAJen](#)

SpeakerBio: Lauren Zabierek , Senior Policy Advisor in the Cybersecurity Division at Cybersecurity and Infrastructure Security Agency (CISA)

Lauren Zabierek is a Senior Policy Advisor in the Cybersecurity Division at CISA. Previously, she served as the Executive Director of the Cyber Project at the Harvard Kennedy School's Belfer Center, where she ran a policy-relevant research program and managed students and nonresident fellows. She also served as the Acting Executive Director of the Belfer Center in her final semester there. She came to that role as a 2019 graduate of the Kenney School's midcareer MPA program. Prior to graduate school, she was an early member of the cybersecurity firm Recorded Future, having established and managed their public sector team. She also served as a civilian intelligence analyst at the National Geospatial Intelligence Agency with multiple deployments to Afghanistan, and served as a US Air Force intelligence officer at the beginning of her career. Lauren is also the co-founder of the online social media movement, #ShareTheMicInCyber. She is a mentor with Girl Security, a fellow at the National Security Institute at George Mason University, and a fellow at New America.

SpeakerBio: Oumou Ly , Senior Advisor for Technology and Ecosystem Security at The White House

Oumou Ly is the Senior Advisor for Technology and Ecosystem Security at the White House. In her role, Oumou provides counsel to senior White House officials on matters which include domestic and international technology and supply chain security, emerging technology, data security, and cyber workforce and education. She came to the White House from the Cybersecurity and Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security. Similarly, in this role, Oumou advised senior agency and Administration leaders in the execution of top Administration priorities to secure critical infrastructure and led policy and strategy for the CISA Cybersecurity Division. On the Joint Ransomware Task Force, she led the effort to develop metrics to improve policy interventions against ransomware and other categories of cybercrime. Prior to serving at CISA, Oumou was a fellow at Harvard University's Berkman Klein Center, where she represented the Center in media commentary at the nexus of national security, cybersecurity, and technology including in The Hill, NBC News, and the Financial Times. Furthermore, while a fellow at the Harvard University, Oumou co-authored the concept paper for the distributed Bluesky protocol; curated Chatham House convenings of security practitioners, academics, and top government officials; authored and hosted tabletop exercises to prepare state and local officials for disruption anticipated during the 2020 election, and contributed significant thought leadership on root causes and policy interventions around disinformation. Prior to joining the Berkman Klein Center, Oumou was an advisor to U.S. Senate Democratic Leader Charles Schumer, where she provided counsel on a cross-cutting portfolio which included national security policy, foreign policy, the defense industrial base, and veterans' affairs. In this role, she routinely led inter and intraparty negotiations on key provisions which were enacted into law, including in the National Defense Authorization Act and the Bipartisan Budget Act of 2018. Oumou holds cybersecurity fellowships at Harvard University and the Atlantic Council's Digital Forensic Research Lab and holds the position of Trustee at Notre Dame de Namur University. Oumou holds a B.A. from Notre Dame de Namur University in Belmont, CA and an MSc from the London School of Economics and Political Science. Oumou is a member of the Board of Trustees at Notre Dame de Namur University.


SpeakerBio: Yael Grauer , Consumer Reports

Yael Grauer works at Consumer Reports managing Security Planner, a free, easy-to-use guide to staying safer online. Her background is in investigative tech reporting, and she has covered privacy and security for over a decade for various tech publications. She has extensively researched the privacy and security (or lack thereof) of consumer VPNs, teamed up with Electronic Frontier Foundation to research street-level surveillance, broken stories on Zoom misleading users about

end-to-encryption, looked into questionable claims about blockchain voting, and investigated surveillance against China's Uyghur minority. Yael serves on the Board of Directors of the CyberMed Summit, the world's only clinically-oriented healthcare cybersecurity conference. She also runs a do-it-yourself data broker opt-out list, and is currently writing a book on investigations for No Starch Press.

Description:

In this unique session, come learn about and help shape the US Government's Secure by Design work. The event will begin with opening remarks by CISA Director Jen Easterly, and feature a panel with representatives from CISA and the White House Office of the National Cyber Director (ONCD). Following that, attendees will be given a draft of CISA's latest guidance on Secure by Design, and will be able to offer edits, comments, and suggestions to inform the final version of the guidance.

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Saturday - 11:00-12:59 PDT

Title: Secure Code Review Challenge

When: Saturday, Aug 12, 11:00 - 12:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 2 - [Map](#)

SpeakerBio: Alon Lerner

10 years experience in offensive hacking and application security

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Sunday - 10:00-11:59 PDT

Title: Secure Code Review Challenge

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 1 - [Map](#)

SpeakerBio: Checkmarx

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Secure from Scratch: Secure Code Workshop for DEF CON Kids

When: Saturday, Aug 12, 13:00 - 14:59 PDT

Where: Flamingo - Savoy - AppSec Village - Workshop - [Map](#)

Speakers:Or Sahar, Yariv Tal

SpeakerBio:Or Sahar

Two decades of software development and security experience including penetration testing, application security, and secure code instruction. She holds a BSC in software engineering and is OSCE certified. There are several CVEs to her name.

Twitter: [@securylight](#)

SpeakerBio:Yariv Tal

Senior developer turned security researcher, with 4 decades of programming experience, university lecturing and mentoring at bootcamps, he has a fresh look at the world of security, as an outsider looking in.

Twitter: [@YarivDevMentor](#)

Description:

Want to learn how to stop hackers in their tracks? Come to the Secure From Scratch coding workshop. Learn what you need to know to write secure code from the very first line of code. It's surprisingly easy!

(Some coding experience in either C#, Java, Python or C++ required. You need to know loops, if, arrays and functions).

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Secure from Scratch: Secure Code Workshop

When: Sunday, Aug 13, 12:00 - 13:59 PDT

Where: Flamingo - Savoy - AppSec Village - Workshop - [Map](#)

SpeakerBio:Or Sahar

Two decades of software development and security experience including penetration testing, application security, and secure code instruction. She holds a BSC in software engineering and is OSCE certified. There are several CVEs to her name.

Twitter: [@securylight](#)

Description:

Want to learn how to stop hackers in their tracks? Come to the Secure From Scratch coding workshop. Learn what you need to know to write secure code from the very first line of code. It's surprisingly easy!

(Some coding experience in either C#, Java, Python or C++ required. You need to know loops, if, arrays and functions).

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Secure Micropatching on the ISS

When: Friday, Aug 11, 12:00 - 12:50 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio:Henry Haswell

No BIO available

Description:

This presentation discusses how SwRI's secure micropatching service was recently demonstrated running on a commercial team member's asset on the international space station (ISS). The micropatching service was able to correct insertion, deletion, or modification of data without needing to resend the full update. This work sets a foundation for securing over-the-air updates from malicious perturbation by utilizing communications between space assets.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Saturday - 10:00-17:59 PDT

Title: Secure or Surrender

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Take Control of Your xIoT Don your white coat, and step into the Mobile xIoT Security Lab at IoT Village during DefCon 31 for a hands-on experience allowing you to Find, Fix, and Monitor an array of IoT, OT, IIoT, and IoMT devices. Brace yourself for the thrill of controlling real-world devices with known CVEs and safely automating fixes. Accompanied by our expert guide, witness live hacking demonstrations showcasing the alarming simplicity behind breaching and controlling banned xIoT devices. And for the cherry on top, be among the first 100 attendees to receive an exclusive, limited edition "Secure Your Things" T-shirt as a token of our appreciation.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Sunday - 10:00-13:59 PDT

Title: Secure or Surrender

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Take Control of Your xIoT Don your white coat, and step into the Mobile xIoT Security Lab at IoT Village during DefCon 31 for a hands-on experience allowing you to Find, Fix, and Monitor an array of IoT, OT, IIoT, and IoMT devices. Brace yourself for the thrill of controlling real-world devices with known CVEs and safely automating fixes. Accompanied by our expert guide, witness live hacking demonstrations showcasing the alarming simplicity behind breaching and controlling banned xIoT devices. And for the cherry on top, be among the first 100 attendees to receive an exclusive, limited edition "Secure Your Things" T-shirt as a token of our appreciation.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Secure or Surrender

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Take Control of Your xIoT Don your white coat, and step into the Mobile xIoT Security Lab at IoT Village during DefCon 31 for a hands-on experience allowing you to Find, Fix, and Monitor an array of IoT, OT, IIoT, and IoMT devices. Brace yourself for the thrill of controlling real-world devices with known CVEs and safely automating fixes. Accompanied by our expert guide, witness live hacking demonstrations showcasing the alarming simplicity behind breaching and controlling banned xIoT devices. And for the cherry on top, be among the first 100 attendees to receive an exclusive, limited edition "Secure Your Things" T-shirt as a token of our appreciation.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Securing Critical Versions of your Reality

When: Friday, Aug 11, 15:00 - 15:59 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

Speakers: Bryson Bort, Keenan Skelly, Suzanne Borders

SpeakerBio: Bryson Bort

Bryson is the Founder of SCYTHE, a start-up building a next-generation threat emulation platform, and GRIMM, a cybersecurity consultancy, and Co-Founder of the ICS Village, a non-profit advancing awareness of industrial control system security. He is a Senior Fellow at the National Security Institute and Adjunct Senior Technical Advisor for the Institute of Security and Technology. As a U.S. Army Officer, he served as a Battle Captain and Brigade Engineering Officer in support of Operation Iraqi Freedom before leaving the Army as a Captain. He was recognized as one of the Top 50 in Cyber by Business Insider, Security Executive Finalist of the Year by SC Media, and a Tech Titan in Washington, DC.

Bryson received his Bachelor of Science in Computer Science with honors from the United States Military Academy at West Point. He holds a Master's Degree in Telecommunications Management from the University of Maryland, a Master's in Business Administration from the University of Florida, and completed graduate studies in Electrical Engineering and Computer Science at the University of Texas.

Twitter: [@brysonbort](#)

SpeakerBio: Keenan Skelly

Keenan Skelly is the Founder of XR Village and currently serves as a Senior Policy Advisor in the Executive Office of the President, National Cyber Director. Keenan served in the US Army as an Explosive Ordnance Disposal Tech and worked for DHS in the Office for Infrastructure Protection developing vulnerability assessments for critical infrastructure. She's been recognized as one of the Top 25 Women in Cybersecurity by CDM, by The Software Report in the Top 25 Women Leaders in Cybersecurity and one of the Top Female Executives by Women World Awards.

SpeakerBio: Suzanne Borders

Suzanne is the CEO & founder of BadVR, the world's first immersive data analytics platform. With her background in psychology, she previously led product and UX design at 2D data analytics companies including Remine, CREXi, and Osurv. A recipient of Magic Leap's Independent Creator's Program grant, and an SBIR Phase 1 grant from the National Science Foundation, Suzanne thrives at the intersection of product design, immersive technology, and data.

In her spare time, she travels for inspiration (75 countries and counting), and is proud to be a published poet and former punk rocker. Her creative hero is Alejandro Jodorowsky, who has inspired Suzanne to take a completely unique and innovative approach to all of her work. She also has 19 tattoos, and is a big believer in the artistry of technology and the technicality of art.

Description:

“Securing Critical Versions of Your Reality” sponsored by BadVR and in collaboration with the ICS Village, focusing on how XR is working for Critical Infrastructure owners and operators. Featuring CEO of BadVR, Suzanne Borders, XR Village Founder, Keenan Skelly, and Bryson Bort, Founder of SCYTHE and GRIMM, co-Founder of ICS Village.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Securing the Front Lines: Protecting Front-End Applications from Overlooked Vulnerabilities

When: Saturday, Aug 12, 15:45 - 16:30 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

Speakers:Dohyeon Kim,WooWon Kang

SpeakerBio:Dohyeon Kim

Dohyeon is a full-stack engineer with cybersecurity background in his early career. Woowon is a security researcher who specializes in web application security. They have won multiple CTFs, including DEF CON 2022.

SpeakerBio:WooWon Kang

I have over 8 years of experience in web application security research and consulting across various industries, and won many CTFs, including 2022 DEF CON CTF.

Twitter: [@wooeong337](#)

Description:

Finding complex vulnerabilities is important, but for companies, it can be more important to mitigate against vulnerabilities that are relatively less difficult to exploit.

We are going to discuss vulnerabilities exposed on the internet, that are easily missed but can have a big impact. We will talk about ways to identify front-end attack surfaces, the impact they can have, and methods for securing the endpoint of applications.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Securing the Supply Chain

When: Friday, Aug 11, 13:00 - 13:50 PDT

Where: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

Speakers: Camille Stewart Gloster, Eric Goldstein

SpeakerBio: Camille Stewart Gloster, Deputy National Cyber Director at Technology and Ecosystem Security Division, Office of the National Cyber Director

Camille Stewart Gloster, Esq. is the Deputy National Cyber Director for Technology & Ecosystem for The White House. In her role, Camille leads technology, supply chain, data security, and cyber workforce and education efforts for the Office of the National Cyber Director. Camille is a cyber, technology, and national security strategist and policy leader whose career has spanned the private, public, and non-profit sectors. She joined ONCD from Google, where she most recently served as Global Head of Product Security Strategy, and before that as Head of Security Policy and Election Integrity for Google Play and Android.

Prior to working at Google, Camille led cyber diplomacy, technology policy, privacy, and technical policy areas like encryption and PNT as the Senior Policy Advisor for Cyber, Infrastructure & Resilience at the U.S. Department of Homeland Security. During her time at DHS, Camille led campaigns, international engagements, and policy development that bolstered national and international cyber resilience. Those policies include Presidential Policy Directive 41 (PPD – 41) on federal cyber incident coordination, supporting Privacy Shield negotiations, and the 2016 Cybersecurity National Action Plan (CNAP) which outlined 75 tasks to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security. Camille has also held leadership roles focused on cyber and technology on Capitol Hill, at Deloitte, and Cyveillance, an open-source threat intelligence company.

SpeakerBio: Eric Goldstein, Executive Assistant Director for Cybersecurity at Cybersecurity and Infrastructure Security Agency (CISA)

Eric Goldstein serves as the Executive Assistant Director for Cybersecurity for the Cybersecurity and Infrastructure Security Agency (CISA) as of February 19, 2021. In this role, Goldstein leads CISA's mission to protect and strengthen federal civilian agencies and the nation's critical infrastructure against cyber threats.

Previously, Goldstein was the Head of Cybersecurity Policy, Strategy, and Regulation at Goldman Sachs, where he led a global team to improve and mature the firm's cybersecurity risk management program. He served at CISA's precursor agency, the National Protection and Programs Directorate, from 2013 to 2017 in various roles including Policy Advisor for Federal Network Resilience, Branch Chief for Cybersecurity Partnerships and Engagement, Senior Advisor to the Assistant Secretary for Cybersecurity, and Senior Counselor to the Under Secretary.

Description:

Securing the supply chain is a significant challenge for the public sector and private sector alike. Supply chains are complex, global, and non-linear. Accordingly, we must be strategic in the deployment of resources to ensure that doctrine, policy, and cross-sector collaboration are aligned to this problem set as incisively as possible. The Biden Administration has undertaken several efforts to achieve the necessary alignment and drive down ecosystem-level risk from insecure supply chains, to include working from the most atomic unit – the code in which software is written. This fireside chat explores how the government is facilitating progress toward foundational supply chain security (including open source software security, AI security, and software security by design), highlights the next iteration of its approach to long-term resilience, and outlines opportunities for individuals and organizations to partner in these efforts.

BHV - Saturday - 10:00-10:30 PDT

Title: Securing the Whole System: Corpal to Corporate

When: Saturday, Aug 12, 10:00 - 10:30 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

SpeakerBio:Lee Cyborg

I am an artist, cyborg, and educator currently based in Montreal. I have a bachelors from Concordia University, a masters from OCAD University, and currently I am a PhD candidate at the University of Toronto. I am interested in lasers, technology, outer space exploration, and building whimsical robots. Currently, I run community initiative and partnerships at the Milieux Institute at Concordia and recently finished a year long residency as Artist in Residence at the department of Design and Computation Arts at Concordia

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Securing the Whole System: Corporal to Corporate

When: Friday, Aug 11, 10:00 - 10:40 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

Speakers:David Guffrey,Nina Alli,Rob Suárez

SpeakerBio:David Guffrey , Principal Biomed Customer Success Manager at Claroty

David Guffrey, MS, MSM, CEH, HCISPP, ITIL

Principal Biomed Customer Success Manager, Claroty

David Guffrey is the Principal Biomed Customer Success Manager for Claroty, an industry leader in cybersecurity. Claroty is an award-winning cybersecurity solution provider with the mission of securing all XIoT cyber-physical systems in the healthcare, industrial, commercial and public sector domains. Mr. Guffrey utilizes his experience integrating and securing connected medical systems in his role as trusted advisor to Claroty customers on their journey toward reducing healthcare ecosystem risk. David also collaborates with Claroty R&D, Data Science, Marketing, and Product Teams to improve the quality of the Claroty product and customer experience.

Prior to his current role, David was the Medical Device Cybersecurity Program Manager for Mass General Brigham (MGB). He built the MGB medical device cybersecurity program for research and operations from the ground up and architected the state-of-the-art “Cyber Range” for the MGH MDPnP Program with funding from the US Dept of Homeland Security, US Food & Drug Administration, and the US Dept of Defense. Through the MDPnP Cyber Range, David conducted cutting edge cybersecurity research for MGB as well as state and federal initiatives. He led MGB operations activities across the enterprise including planning strategic initiatives, risk assessments, technology assessments, penetration testing, emergency preparedness & response activities, technology implementations. He also served as an advisor for MGB procurement contract negotiations and infosec policies and procedures.

Mr. Guffrey has been a leading voice representing healthcare delivery organization (HDO) interests in the national standards community including contributing to AAMI TIR97 and SW96. David strives to be an active community member through opportunities for sharing his knowledge and collaborating on initiatives that build towards improving the security of the healthcare ecosystem. He has presented to the World Health Organization and numerous organizations, societies and conferences including ACCE, BHV, MedTechIntelligence, STA, CFF, IQPC. He also enjoys mentoring rising cybersecurity specialists.

SpeakerBio:Nina Alli , Regulatory Cybersecurity, Senior Strategist at Thermo Fisher

Nina Alli is the Executive Director of the Biohacking Village, Sr Cybersecurity Regulatory Strategist at ThermoFisher, George Washington University Law School student, policy white paper writer, EMR and associated devices technologist, coffee snob, and super proud #Latina from #NYC.

SpeakerBio:Rob Suárez

Rob Suárez is a cybersecurity and privacy professional in the healthcare industry. Currently at CareFirst BlueCross BlueShield, Rob serves as Chief Information Security Officer with previous Chief Information Security Officer experience at BD (Becton Dickinson). His origin story begins software development and continues that trajectory with experience overseeing cybersecurity across enterprise IT, manufacturing OT, and medical technology product. Rob previously chaired the Cybersecurity Steering Committee for the Medical Device Innovation Consortium and the Cybersecurity Working Group for AdvaMed. He was also one of three leaders to co-chair the public-private Healthcare and Public Health Sector Coordinating Council (HSCC) Med Tech Cybersecurity Risk Management Task Group, which issued the seminal Medical Device and Healthcare Information Technology Joint Security Plan (JSP) in 2019.

Description:No Description available

Title: Security Engineering for Adversarial Emulation and Red Teaming

When: Friday, Aug 11, 11:30 - 12:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Main Stage - [Map](#)

Speakers:plug,sandw1ch

SpeakerBio:plug

No BIO available

SpeakerBio:sandw1ch

Scott Brink is a hacker and manager within X-Force Red who specializes in network penetration testing. He graduated with a degree in computing security with a minor in networking and system administration from Rochester Institute of Technology. While there, he was the captain of the school's team for the Collegiate Penetration Testing Competition. His research includes a presentation at Thotcon 0xA that looked into visitor management systems, where he found 19 zero-day vulnerabilities in these products. He has also presented a workshop at Red Team Village at Defcon 30 about Active Directory.

Description:

Securing Engineering is a core element of security. In this session, you will hear how the Obsidian Engineers collaborated with the Red Team to architect and build this year's Obsidian adversary simulation environment. PS: You will be able to make your own too!

Securing Engineering is a core element of security. In this session, you will hear how the Obsidian Engineers collaborated with the Red Team to architect and build this year's Obsidian adversary simulation environment. PS: You will be able to make your own too!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Security Logging in the cloud, trade-offs to consider and patterns to maximise the effectiveness of security data pipelines

When: Sunday, Aug 13, 11:20 - 11:59 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Marco Mancini , Tech Lead for the Detection Engineering at Thought Machine

I am the tech lead for the Detection Engineering team at Thought Machine a cloud-native core banking company. My career has been based on doing Incident Response and Security monitoring for banks and financial institutions with a deep focus on engineering data driven solutions to several security problems.

Twitter: [@ManciniJ](#)

Description:

Security Operations in the cloud can be thought as a data problem. If you can immediately and easily answer questions of what, how and who has done an action attackers can be uncovered and dealt with much quicker.

Building the infrastructure to do this however can easily become very expensive and there are some big trade-offs to consider when building a security logging pipeline.

This talk will explain the different logging patterns that you can find in public clouds like AWS, GCP and Azure and the pitfalls and experience from building and rebuilding the security logging at different scale levels.

This talk should give any attendees protecting a company with a big cloud exposure valuable insights that could be applied to building a new security logging function and also how to improve their current security pipelines.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 21:00-23:59 PDT

Title: SECV - 80's Themed Party!


When: Saturday, Aug 12, 21:00 - 23:59 PDT

Where: Caesars Forum - Forum - 117-118 - [Map](#)

Description:

This year it is **80's themed** so be sure to dress up (although we'll have some accessories if you forget yours).

The party will be in the Forums (room 117/118), not our village, Saturday from 2100-2359. Cash bar with boozy and booze-free options.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SEV - Sunday - 12:00-13:30 PDT

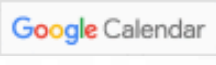
Title: SECV - Awards & Competitor Panel

When: Sunday, Aug 13, 12:00 - 13:30 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description:

See who won in our village! During this time we'll present the Youth Challenge winner, the #SECVC 1st and 2nd place winners, as well as the much-coveted Dundies! Then stick around as we have a panel interview with the winners to hear their story about their path to victory!

[Return to Index](#) - Add to  - ics [Calendar](#) file

SEV - Sunday - 10:00-10:59 PDT

Title: SECV - Youth Challenge


When: Sunday, Aug 13, 10:00 - 10:59 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description:

Many parents and guardians bring their children to DEF CON to allow them to experience the same learning, networking, and community that they enjoy. As parents and educators ourselves, we want to help make this experience even more memorable with our Youth Challenge!

Please see the "More Information" link.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SEV - Saturday - 08:30-17:30 PDT

Title: SECV - Youth Challenge

When: Saturday, Aug 12, 08:30 - 17:30 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description:

Many parents and guardians bring their children to DEF CON to allow them to experience the same learning, networking, and community that they enjoy. As parents and educators ourselves, we want to help make this experience even more memorable with our Youth Challenge!

Please see the "More Information" link.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SEV - Friday - 08:30-17:30 PDT

Title: SECV - Youth Challenge

When: Friday, Aug 11, 08:30 - 17:30 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description:

Many parents and guardians bring their children to DEF CON to allow them to experience the same learning, networking, and community that they enjoy. As parents and educators ourselves, we want to help make this experience even more memorable with our Youth Challenge!

Please see the "More Information" link.

[Return to Index](#) - Add to  - ics [Calendar](#) file


SEV - Friday - 08:30-17:59 PDT

Title: SECV Village Open

When: Friday, Aug 11, 08:30 - 17:59 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

SEV - Sunday - 10:00-13:59 PDT

Title: SECV Village Open

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file


SEV - Saturday - 08:30-17:59 PDT

Title: SECV Village Open

When: Saturday, Aug 12, 08:30 - 17:59 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Shall we play a game? Just because a Large Language Model speaks like a human, doesn't mean it can reason like one.

When: Friday, Aug 11, 15:00 - 15:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio: Craig Martell , Chief Digital and AI Officer at US Department of Defense

Dr. Craig Martell is the first-ever Chief Digital and AI Officer at the Department of Defense. Previously, he was the Head of Machine Learning at Lyft, the Head of Machine Intelligence at Dropbox, and led AI teams and initiatives at LinkedIn. He is also a tenured computer science professor in natural language processing at the Naval Postgraduate School.

Description:

In 1979, NORAD was duped by a simulation that caused NORAD (North American Aerospace Defense) to believe a full-scale Soviet nuclear attack was underway. This only legitimized the plot in the 1983 classic, War Games, of the possibility of a computer making unstoppable, life-altering decisions. On the 40th anniversary of the movie that predicted the potential role of AI in military systems, LLMs have become a sensation and increasingly, synonymous with AI. This is a dangerous detour in AI's development, one that humankind can't afford to take. Join Dr. Martell for an off-the-cuff discussion on what's at stake as the Department of Defense presses forward to balance agility with accountability and the role hackers play in ensuring the responsible and secure use of AI from the boardroom to the battlefield.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA)

When: Friday, Aug 11, 09:00 - 01:59 PDT

Where: Caesars Forum - Forum - 121-123, 129, 137 - Chillout - [Map](#)

Description:

The Shell On Demand Appliance Machine (S.O.D.A. Machine) at DEF CON provided by the National Upcycled Computing Collective, Inc. (NUCC).

So, what's the S.O.D.A. Machine all about?

Picture this:

You're at DEF CON, thirsty for some hacking. You're looking for a virtual machine (VM) to play with but don't want to be chained to your laptop.

Enter the Shell On Demand Appliance:

This heavily modified VM is your gateway to an anonymous VM, available in the Chillout Lounge and accessible over the DEF CON network.

A fusion of hardware, software, art, and hacking, all encapsulated in a project derived from recycled materials. The S.O.D.A. Machine provides a way for Humans to experience the DEF CON network in a way the secure WiFi won't allow, because the datacenter is inside the S.O.D.A. Machine and directly connected to the NOC.

Simply insert cash or coins into the bill or coin acceptor to get started. The lights on the buttons will change color depending on availability.

A green light means the VM is available and ready.

An amber light requests the user to insert more money to ensure fair distribution according to current resources.

A red light denotes the selection is unavailable.

Once you make a selection, the system will deploy the VM to the network and a receipt will be printed.

On the receipt, login credentials are provided for you to access your virtual machine via remote shell. You are then able to change the password, install whatever tools and applications you need, making the VM your own.

What you do with the VM is up to you. Should you choose to share your virtual machine with someone outside of the DEF CON network, a Tor address is provided as well.

All proceeds go to the National Upcycled Computing Collective, Inc., a 501(c)(3) nonprofit organization helping further research and education in computer science, technology and engineering as an (NTEE U41) Research Institute.

We accept donations: <https://www.paypal.com/paypalme/NUCC>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA)

When: Sunday, Aug 13, 09:00 - 15:30 PDT

Where: Caesars Forum - Forum - 121-123, 129, 137 - Chillout - [Map](#)

Description:

The Shell On Demand Appliance Machine (S.O.D.A. Machine) at DEF CON provided by the National Upcycled Computing Collective, Inc. (NUCC).

So, what's the S.O.D.A. Machine all about?

Picture this:

You're at DEF CON, thirsty for some hacking. You're looking for a virtual machine (VM) to play with but don't want to be chained to your laptop.

Enter the Shell On Demand Appliance:

This heavily modified VM is your gateway to an anonymous VM, available in the Chillout Lounge and accessible over the DEF CON network.

A fusion of hardware, software, art, and hacking, all encapsulated in a project derived from recycled materials. The S.O.D.A. Machine provides a way for Humans to experience the DEF CON network in a way the secure WiFi won't allow, because the datacenter is inside the S.O.D.A. Machine and directly connected to the NOC.

Simply insert cash or coins into the bill or coin acceptor to get started. The lights on the buttons will change color depending on availability.

A green light means the VM is available and ready.

An amber light requests the user to insert more money to ensure fair distribution according to current resources.

A red light denotes the selection is unavailable.

Once you make a selection, the system will deploy the VM to the network and a receipt will be printed.

On the receipt, login credentials are provided for you to access your virtual machine via remote shell. You are then able to change the password, install whatever tools and applications you need, making the VM your own.

What you do with the VM is up to you. Should you choose to share your virtual machine with someone outside of the DEF CON network, a Tor address is provided as well.

All proceeds go to the National Upcycled Computing Collective, Inc., a 501(c)(3) nonprofit organization helping further research and education in computer science, technology and engineering as an (NTEE U41) Research Institute.

We accept donations: <https://www.paypal.com/paypalme/NUCC>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA)

When: Thursday, Aug 10, 09:00 - 01:59 PDT

Where: Caesars Forum - Forum - 121-123, 129, 137 - Chillout - [Map](#)

Description:

The Shell On Demand Appliance Machine (S.O.D.A. Machine) at DEF CON provided by the National Upcycled Computing Collective, Inc. (NUCC).

So, what's the S.O.D.A. Machine all about?

Picture this:

You're at DEF CON, thirsty for some hacking. You're looking for a virtual machine (VM) to play with but don't want to be chained to your laptop.

Enter the Shell On Demand Appliance:

This heavily modified VM is your gateway to an anonymous VM, available in the Chillout Lounge and accessible over the DEF CON network.

A fusion of hardware, software, art, and hacking, all encapsulated in a project derived from recycled materials. The S.O.D.A. Machine provides a way for Humans to experience the DEF CON network in a way the secure WiFi won't allow, because the datacenter is inside the S.O.D.A. Machine and directly connected to the NOC.

Simply insert cash or coins into the bill or coin acceptor to get started. The lights on the buttons will change color depending on availability.

A green light means the VM is available and ready.

An amber light requests the user to insert more money to ensure fair distribution according to current resources.

A red light denotes the selection is unavailable.

Once you make a selection, the system will deploy the VM to the network and a receipt will be printed.

On the receipt, login credentials are provided for you to access your virtual machine via remote shell. You are then able to change the password, install whatever tools and applications you need, making the VM your own.

What you do with the VM is up to you. Should you choose to share your virtual machine with someone outside of the DEF CON network, a Tor address is provided as well.

All proceeds go to the National Upcycled Computing Collective, Inc., a 501(c)(3) nonprofit organization helping further research and education in computer science, technology and engineering as an (NTEE U41) Research Institute.

We accept donations: <https://www.paypal.com/paypalme/NUCC>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA)

When: Saturday, Aug 12, 09:00 - 01:59 PDT

Where: Caesars Forum - Forum - 121-123, 129, 137 - Chillout - [Map](#)

Description:

The Shell On Demand Appliance Machine (S.O.D.A. Machine) at DEF CON provided by the National Upcycled Computing Collective, Inc. (NUCC).

So, what's the S.O.D.A. Machine all about?

Picture this:

You're at DEF CON, thirsty for some hacking. You're looking for a virtual machine (VM) to play with but don't want to be chained to your laptop.

Enter the Shell On Demand Appliance:

This heavily modified VM is your gateway to an anonymous VM, available in the Chillout Lounge and accessible over the DEF CON network.

A fusion of hardware, software, art, and hacking, all encapsulated in a project derived from recycled materials. The S.O.D.A. Machine provides a way for Humans to experience the DEF CON network in a way the secure WiFi won't allow, because the datacenter is inside the S.O.D.A. Machine and directly connected to the NOC.

Simply insert cash or coins into the bill or coin acceptor to get started. The lights on the buttons will change color depending on availability.

A green light means the VM is available and ready.

An amber light requests the user to insert more money to ensure fair distribution according to current resources.

A red light denotes the selection is unavailable.

Once you make a selection, the system will deploy the VM to the network and a receipt will be printed.

On the receipt, login credentials are provided for you to access your virtual machine via remote shell. You are then able to change the password, install whatever tools and applications you need, making the VM your own.

What you do with the VM is up to you. Should you choose to share your virtual machine with someone outside of the DEF CON network, a Tor address is provided as well.

All proceeds go to the National Upcycled Computing Collective, Inc., a 501(c)(3) nonprofit organization helping further research and education in computer science, technology and engineering as an (NTEE U41) Research Institute.

We accept donations: <https://www.paypal.com/paypalme/NUCC>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Shipping Wardriving Hardware - Cross-country Wigle on the Cheap

When: Saturday, Aug 12, 12:00 - 12:20 PDT

Where: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

SpeakerBio:Segfault

I am a hardware hacker and a wardriver, among many other things as they catch my interest. I don't have many qualifications to make me uniquely capable to do the things that I do, other than just having an idea or desire to make things happen.

Twitter: [@CoD_Segfault](#)

Description:

"After designing a miniature PCB based on jhewitt's ESP32 Wardriver design, a friend across the country showed interest in obtaining one of the boards. The idea came up that the hardware could be shipped along with a battery and the results could be analyzed and uploaded to Wigle.net after the fact.

This talk goes over the hardware used, the safety considerations, testing methodologies, and criteria needed to be met before proceeding. The results will be analyzed and compared to the shipping service's tracking methods, with visualizations on a map to show shipping progress."

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Shufflecake, AKA Truecrypt on Steroids for Linux

When: Friday, Aug 11, 12:00 - 13:55 PDT

Where: Caesars Forum - Unity Boardroom - Demo Labs - [Map](#)

Speakers: Elia Anzuoni, Tommaso "tomgag" Gagliardoni

SpeakerBio: Elia Anzuoni

Elia: is a junior computer scientist and cryptographer. He recently obtained a joint M.Sc. in Cybersecurity from the Swiss universities EPFL and ETHZ. Among his relevant works, he conducted a 6-month project to refine and implement a decentralised MPC scheme based on the quantum-resistant BFV cryptosystem; as part of his first internship, he implemented a FIDO2 authenticator in a USB mouse's firmware; for his Master's Thesis (conducted as an internship at the cybersecurity company Kudelski Security), he devised a novel scheme for plausibly-deniable storage and implemented it as a kernel module for Linux. Since his graduation, he has developed an interest for blockchain technologies, especially in the Ethereum ecosystem, which has led him to delve into the vast landscape of peculiar pitfalls surrounding DeFi and Smart Contract development. He is now on a leap year, wandering around the globe with a big backpack full of dreams and t-shirts.

SpeakerBio: Tommaso "tomgag" Gagliardoni

Tommaso "tomgag" Gagliardoni: researcher in cryptography, privacy and security. Mathematician, cryptographer, and quantum security expert, Tommaso published influential peer-reviewed papers and spoke at many international conferences in cryptography, privacy and security (among others: CRYPTO, EUROCRYPT, ASIACRYPT, Black Hat Europe). As a subject expert, he serves as a Program Committee member at academic conferences, and collaborates with public and private institutions and official agencies in the context of legislation, international treaties and agreements on emerging technologies. Expert in blockchain and DeFi, Tommaso has performed cryptographic code audits for clients such as Binance, Coinbase, ING, Swiss Post. Additionally, he has a background in privacy hacktivism, investigative journalism, and ethical hacking, speaking at venues such as the International Journalism Festival and the E-Privacy Meeting, and being a strong advocate of the FOSS philosophy and digital freedoms. Tommaso obtained an M.Sc. in Mathematics at the University of Perugia, Italy, and a PhD at the Technical University of Darmstadt, Germany. He worked at IBM Research Zurich before joining Swiss-American cybersecurity company Kudelski Security in 2019, where he is currently technical leader for the initiatives in advanced cryptography services and quantum security. In his free time, Tommaso pursues his hobby of building tools and practices to escape the global surveillance dragnet.

Description:

Shufflecake is a FOSS tool for Linux that allows creation of multiple hidden volumes on a storage device in such a way that it is very difficult, even under forensic inspection, to prove the existence of such volumes without the right password(s). You can consider Shufflecake a "spiritual successor" of tools such as Truecrypt and Veracrypt, but vastly improved: it works natively on Linux, it supports any filesystem of choice, and can manage multiple nested volumes per device, so to make deniability of the existence of these partitions really plausible.

[Return to Index](#) - Add to  - ics [Calendar](#) file

RFV - Friday - 14:00-14:20 PDT

Title: Signals! In! Spaaaaaace!

When: Friday, Aug 11, 14:00 - 14:20 PDT

Where: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

Speakers:Ark (from WiGLE),wytshadow

SpeakerBio:Ark (from WiGLE)

My name is Andy or sometimes Ark- I'm a co-founder of WiGLE.net - the largest crowd-sourced, open database of wardriving data on the internet. In my day job, I mostly build fintech and privacy tech start-ups. I co-maintain both client and server sides of WiGLE, design our swag, and serve as the designated sacrifice for public appearances. I've been wardriving since the year 2001, and still manage to stay in the top 20 on the WiGLE leader board, largely through distance running using WiGLE as my personal trainer.

Twitter: [@@wiglenet](#)

SpeakerBio:wytshadow

No BIO available

Twitter: [@@theDarracott](#)

Description:

Wytshadow, Dragorn, and Ark have been preparing to support network stumbling on bodies beyond earth. This is a synopsis of the challenges, our proposed solutions, and a preview/introduction of how you measure and report wireless data from Earths' moon, Mars, and beyond.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Silent Spring: Prototype Pollution Leads to Remote Code Execution in Node.js

When: Saturday, Aug 12, 17:00 - 17:20 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

Speakers: Mikhail Shcherbakov, Musard Balliu

SpeakerBio: Mikhail Shcherbakov , KTH Royal Institute of Technology

Mikhail Shcherbakov came to security from enterprise app development. The tendency is to push it as far as you can... He is now doing a Ph.D. in Language-Based Security after 10+ years of experience in the industry. He participated in Microsoft, GitHub, and open-source bug bounty programs, found vulnerabilities in popular products, and helped to fix them. Before starting a Ph.D. program, he focused on .NET and web security, gave talks at conferences, organized IT meetups, and got the Microsoft MVP Award in 2016 – 2018. Mikhail is an author of commercial static analysis tools and continues research in program analysis.

Twitter: [@yu5k3](#)

SpeakerBio: Musard Balliu , KTH Royal Institute of Technology

No BIO available

Description:

Many have heard about Prototype Pollution vulnerabilities in JavaScript applications. This kind of vulnerability allows an attacker to inject properties into an object's root prototype that may lead to flow control alteration and unexpected program behavior. Every time a successful exploit looks like magic or is limited to a denial of service (DoS). Would you be surprised if I told you that every application has a chain of methods that can be triggered by Prototype Pollution and leads to arbitrary code execution? Such gadgets populated Node.js core code and popular NPM packages. Keep calm. Not every app can be exploited! However, this fact increases the risk of exploitation many times over.

In our research, we studied Prototype Pollution beyond DoS and analyzed Node.js source code against the gadgets. We then analyzed 15 popular Node.js apps from GitHub and got 8 RCEs. Through this talk, I will elaborate on the detected gadgets and vulnerabilities. We will also take a look at how the recent changes in Node.js mitigate these issues.

REFERENCES

Mikhail Shcherbakov, Musard Balliu and Cristian-Alexandru Staicu "Silent Spring: Prototype Pollution Leads to Remote Code Execution in Node.js" <https://github.com/yuske/silent-spring/blob/master/silent-spring-full-version.pdf> Gareth Heyes

"Server-side prototype pollution: Black-box detection without the DoS"

<https://portswigger.net/research/server-side-prototype-pollution> Michał Bentkowski "Exploiting prototype pollution – RCE in Kibana (CVE-2019-7609)" <https://research.securitum.com/prototype-pollution-rce-kibana-cve-2019-7609/> Olivier Arteau

"Prototype Pollution Attack in NodeJS application"

https://github.com/HoLyVieR/prototype-pollution-nsec18/blob/master/paper/JavaScript_prototype_pollution_attack_in_NodeJS.pdf

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Small Leaks, Billions Of Dollars: Practical Cryptographic Exploits That Undermine Leading Crypto Wallets

When: Thursday, Aug 10, 16:30 - 16:50 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers: Nikolaos Makriyannis, Oren Yomtov

SpeakerBio: Nikolaos Makriyannis , Cryptography Research Lead at Fireblocks

Nikolaos Makriyannis (Nikos), Cryptography Research Lead at Fireblocks, is a cryptography PhD, specializing in the areas of multiparty computation (MPC). Nikos is the co-inventor of the CMP20 and CGGMP21 protocols published in ACM CCS'20 and used by multiple wallet providers.

Twitter: [@nik_mak_](#)

SpeakerBio: Oren Yomtov , Blockchain Research Lead at Fireblocks

Oren Yomtov (@orenyomtov), Blockchain Research Lead at Fireblocks, is a security researcher with over a decade of experience. In the past year, focusing on the blockchain space, he disclosed a critical vulnerability in a blockchain with a market cap of \$100 million and created the first open-source, trustless Bitcoin NFT marketplace, OpenOrdex.

Twitter: [@orenyomtov](#)

Description:

Multi-Party Computation (MPC) has become a common cryptographic technique for protecting hundreds of billions of dollars in cryptocurrency wallets. MPC algorithms are currently powering the wallets of Coinbase, Binance, Zengo, BitGo, Fireblocks and many other fintechs/banks servicing hundreds of millions of consumers and thousands of financial institutions.

This presentation examines the most common MPC protocols and implementations and shows that securing MPC remains a challenge for most companies.

We show practical key-exfiltration attacks requiring no more than a couple of hundred signatures. Namely, we show three different attacks on different protocols/implementations requiring 256, 16, and *one* signature, respectively.

REFERENCES:

Rosario Gennaro and Steven Goldfeder. "One Round Threshold ECDSA with Identifiable Abort." Cryptology ePrint Archive, Paper 2020/540, 2020. Yehuda Lindell. "Fast Secure Two-Party ECDSA Signing." Journal of Cryptology, vol. 34, no. 4, 2021, pp. 44. Rosario Gennaro and Steven Goldfeder. "Fast Multiparty Threshold ECDSA with Fast Trustless Setup." Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS), 2018, pp. 1179-1194.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Smashing the state machine: the true potential of web race conditions

When: Saturday, Aug 12, 09:00 - 09:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio:James "albinowax" Kettle , Director of Research at PortSwigger

James 'albinowax' Kettle is the Director of Research at PortSwigger, the makers of Burp Suite. He's best known for his HTTP Desync Attacks research, which popularised HTTP Request Smuggling. James has extensive experience cultivating novel attack techniques, including web cache poisoning, browser-powered desync attacks, server-side template injection, and password reset poisoning.

James is also the author of multiple popular open-source tools including Param Miner, Turbo Intruder, and HTTP Request Smuggler. He is a frequent speaker at numerous prestigious venues including both Black Hat USA and EU, OWASP AppSec USA and EU, and DEF CON.

Twitter: [@albinowax](#)

Description:

For too long, web race-condition attacks have focused on a tiny handful of scenarios. Their true potential has been masked thanks to tricky workflows, missing tooling, and simple network jitter hiding all but the most trivial, obvious examples. In this session, I'll introduce multiple new classes of race condition that go far beyond the limit-overflow exploits you're probably already familiar with.

Inside every website lurks a state machine: a delicately balanced system of states and transitions that each user, session, and object can flow through. I'll show how to fire salvos of conflicting inputs at high-profile websites to make state machines collapse, enabling you to forge trusted data, misroute tokens, and mask backdoors.

To handle this explosion of attack surface, I'll share a polished methodology designed to help you eke out subtle tell-tale clues and scent blood long before sacrificing anything to the RNG gods. I've also taken lore amassed over years of research into HTTP Desync Attacks and developed a strategy that can squeeze 30 requests sent from Melbourne to Dublin into a sub-1ms execution window. Alongside the open source tool, we'll also release free online labs so you can try out your new skillset immediately.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Snakes on a Screen: Taming Offensive IronPython Techniques (Pre-Registration Required)

When: Friday, Aug 11, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers:Anthony "Coin" Rose,Gannon "Dorf" Gebauer,Vincent "Vinnybod" Rose

SpeakerBio:Anthony "Coin" Rose , Director of Security Researcher at BC Security

Anthony "Coin" Rose, CISSP, is the Director of Security Researcher at BC Security, where he specializes in adversary tactic emulation planning, Red and Blue Team operations, and embedded systems security. He has presented at numerous security conferences, including Black Hat, DEF CON, HackSpaceCon, HackMiami, and RSA conferences. Anthony is the author of various offensive security tools, including Empire and Starkiller, which he actively develops and maintains. He is recognized for his work, revealing wide-spread vulnerabilities in Bluetooth devices and is the co-author of a cybersecurity blog at <https://www.bc-security.org/blog/>.

SpeakerBio:Gannon "Dorf" Gebauer , Security Consultant at BC Security

Gannon "Dorf" Gebauer is a Security Consultant at BC Security and specializes in threat intelligence and embedded system testing. He has led teams through the Cyber Patriot, a USAF CTF that tests both defense and offensive capabilities. Currently, his expertise is focused on building automation tools for range deployments. Dorf has taught courses at both, Blackhat and DEF CON.

SpeakerBio:Vincent "Vinnybod" Rose , Lead Developer at Empire and Starkiller

Vincent "Vinnybod" Rose is the Lead Developer for Empire and Starkiller. He is a software engineer with a decade of expertise in building highly scalable cloud services, improving developer operations, and building automation. Recently, his focus has been on the reliability and stability of the Empire C2 server in the most recent major update (Empire 5). Vinnybod has presented at Black Hat and has taught courses at DEF CON on Red Teaming and Offensive PowerShell. He currently maintains a cybersecurity blog focused on offensive security at <https://www.bc-security.org/blog/>.

Description:

IronPython is a powerful and flexible programming language that has been increasingly used by attackers due to its ability to bypass security controls. This practical workshop will explore the inner workings of IronPython and its unique features that enable sophisticated offensive techniques. Participants will gain hands-on experience in developing IronPython payloads that can evade modern security controls and execute malicious code on target systems.

The workshop will cover the following topics: 1. Introduction to IronPython: Basic syntax and usage of IronPython, and how it can be used in offensive scenarios. 2. BYOI and DLR: Bring Your Own Interpreter (BYOI) and Dynamic Language Runtime (DLR) concepts and their role in developing offensive payloads. 3. Malware Development with IronPython: Develop sophisticated payloads that can bypass modern security controls and execute malicious code on target systems. 4. Anti-Forensics and Evasion Techniques: Techniques to make the payloads more resilient to forensic analysis and detection. 5. Advanced Techniques: Advanced techniques like using IronPython with C# and PowerShell and integrating the payloads with other offensive tools.


This workshop is designed for offensive security professionals, red teamers, penetration testers, and anyone interested in exploring the capabilities of IronPython for offensive purposes. Participants should have a basic understanding of Python and programming concepts. By the end of the workshop, participants will have a deeper understanding of IronPython and its capabilities for developing offensive payloads.

Skill Level: Intermediate

Prerequisites for students:

- A familiarity with python is preferred, but not required.

Materials or Equipment students will need to bring to participate: - Laptop with Windows or other Windows VM

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Snoop unto them, as they snoop unto us

When: Sunday, Aug 13, 10:00 - 10:20 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

Speakers:Michaud "5@V@g3" Savage,Rekcahdam,nullagent

SpeakerBio:Michaud "5@V@g3" Savage , Apprentice at Dataparty

No BIO available

SpeakerBio:Rekcahdam , Hacker

No BIO available

Twitter: [@rekcahdam](#)

SpeakerBio:nullagent , Member at Dataparty

Nullagent is a robotics hacker. He built his first internet connected robot in 2004 and since then he's been hooked on embedded hacking. He's building a hacker collective that fuses artistic expression to bring cyber security tools to a broader audience.

Twitter: [@nullagent](#)

Description:

BLE devices are now all the rage. What makes a purpose built tracking device like the AirTag all that different from the majority of BLE devices that have a fixed address? With the rise of IoT we're also seeing a rise in government and corporate BLE surveillance systems. We'll look at tools that normal people can use to find out if their favorite IoT gear is easily trackable. If headphones and GoPro's use fixed addresses, what about stun guns and bodycams? We'll take a look at IoT gear used by authorities and how it may be detected over long durations, just like an AirTag.

REFERENCES

Handoff All Your Privacy – A Review of Apple’s Bluetooth Low Energy Continuity Protocol Freqy DEFCON 29 RF Village - "Basics of Breaking BLE" Handoff All Your Privacy – A Review of Apple’s Bluetooth Low Energy Continuity Protocol DEF CON 26 - Damien virtualabs Cauquil - You had better secure your BLE devices Mike Spicer - I Know What U Did Last Summer 3 Yrs Wireless Monitoring DEFCON - DEF CON 27 Conference

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: So you want to become a Detection Engineer

When: Saturday, Aug 12, 13:30 - 14:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Main Stage - [Map](#)

Speakers: Ben Bornholm, CerealKiller, kobaltfox, plug

SpeakerBio: Ben Bornholm

Hey y'all,

I am Ben (@CptOfEvilMinions), I crafted my whimsical presenting style when I was the President of RIT Competitive Cybersecurity Club (RC3). Cybersecurity is not just my day job, it's my passion. I have continued my passion with my blog and with the creation of DEFCON workshops with the BTV.

During the day I fight off cyber hooligans as a DART engineer at Dropbox.com. At night, I am continuing my passion on my blog HoldMyBeerSecurity.com where I discuss topics in security that interest me such as incident response, threat hunting, detection engineering, Osquery, and DevSecOps.

SpeakerBio: CerealKiller

CerealKiller or Cereal is a Cyber Defense Practitioner with over 10yrs of experience.

SpeakerBio: kobaltfox

TODO

SpeakerBio: plug

No BIO available

Description:

Security is nothing without visibility, join a group of practitioners as they outline ways to get you started in detection engineering.

Security is nothing without visibility, join a group of practitioners as they outline ways to get you started in detection engineering.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: SOC Panel: Finding, Keeping, and Caring for the Best People

When: Friday, Aug 11, 15:00 - 15:59 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Main Stage - [Map](#)

Speakers:Alissa Torres,Carson Zimmerman,Christopher Crowley,Russ McRee

SpeakerBio:Alissa Torres

Alissa Torres is a blue team practitioner/educator turned consultant, laser-focused on the people element of the SecOps equation. With 3 dog-years of experience spanning roles in IT and Security Operations, she discovered her passion for adversary hunting while serving in the trenches as an incident analyst with a third-party services company, and later, leading an incident response team for a global manufacturing company.

SpeakerBio:Carson Zimmerman

Carson Zimmerman is a veteran cybersecurity specialist, author, and speaker. In his current role at Microsoft, Carson leads an investigations team responsible for defending the M365 platform and ecosystem. In his previous role, at The MITRE Corporation, Carson specialized in cybersecurity operations center (CSOC) architecture and CSOC consulting. His experiences over 20 years as a CSOC analyst and engineer led Carson to author Ten Strategies of a World-Class Cybersecurity Operations Center, and co-authored its second edition, Eleven Strategies... which may be downloaded for free at mitre.org/11Strategies.

SpeakerBio:Christopher Crowley

No BIO available

SpeakerBio:Russ McRee

No BIO available

Description:

Come hear 4 SOC veterans discuss some of the most challenging topics in SOC's today. People are our most important asset, but recruiting, retention, and career growth continue to be a sore spot for many. Trying to break into the field? Been laid off? Worried about training or outsourcing? This panel is for you. We share with you what we've learned over the years; along the way we will spice it up with some war stories and hard won lessons.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Social Engineering Community (SEC) Vishing Competition

When: Friday, Aug 11, 11:30 - 13:30 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description:

In this competition (#SECVV), teams go toe to toe by placing live vishing (voice phishing) phone calls in front of the Social Engineering Community audience at DEF CON. These calls showcase the duality of ease and complexity of the craft against the various levels of preparedness and defenses by actual companies. Teams can consist of 1-3 individuals, which we hope allows for teams to utilize novel techniques to implement different Social Engineering tactics. Each team has limited time to place as many calls as possible from a soundproof booth. During that time, their goal is to elicit from the receiver as many objectives as possible. Whether you're an attacker, defender, business executive, or brand new to this community, you can learn by witnessing firsthand how easy it is for some competitors to schmooze their way to their goals and how well prepared some companies are to shut down those competitors!

2023 judges: Corgi, FC aka freakyclown, and Snow 2023 coaches: Ibetika, JC, C_3PJoe, and Split Beans (last year's SECVV winners: Jenn, Matt, and Sean)

This competition takes place on Friday in the Social Engineering Community village, be sure to get there early to get a seat; they fill up fast! Additionally, at the end of Friday, join Snow as she covers the behind the scenes of creating the SECVV, this year's lessons learned, team highlights, and tips for future competitors!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Social Engineering Community (SEC) Vishing Competition

When: Friday, Aug 11, 09:00 - 10:59 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description:

In this competition (#SECVV), teams go toe to toe by placing live vishing (voice phishing) phone calls in front of the Social Engineering Community audience at DEF CON. These calls showcase the duality of ease and complexity of the craft against the various levels of preparedness and defenses by actual companies. Teams can consist of 1-3 individuals, which we hope allows for teams to utilize novel techniques to implement different Social Engineering tactics. Each team has limited time to place as many calls as possible from a soundproof booth. During that time, their goal is to elicit from the receiver as many objectives as possible. Whether you're an attacker, defender, business executive, or brand new to this community, you can learn by witnessing firsthand how easy it is for some competitors to schmooze their way to their goals and how well prepared some companies are to shut down those competitors!

2023 judges: Corgi, FC aka freakyclown, and Snow 2023 coaches: Ibetika, JC, C_3PJoe, and Split Beans (last year's SECVV winners: Jenn, Matt, and Sean)

This competition takes place on Friday in the Social Engineering Community village, be sure to get there early to get a seat; they fill up fast! Additionally, at the end of Friday, join Snow as she covers the behind the scenes of creating the SECVV, this year's lessons learned, team highlights, and tips for future competitors!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Social Engineering Community (SEC) Vishing Competition

When: Friday, Aug 11, 14:00 - 16:59 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description:

In this competition (#SECVV), teams go toe to toe by placing live vishing (voice phishing) phone calls in front of the Social Engineering Community audience at DEF CON. These calls showcase the duality of ease and complexity of the craft against the various levels of preparedness and defenses by actual companies. Teams can consist of 1-3 individuals, which we hope allows for teams to utilize novel techniques to implement different Social Engineering tactics. Each team has limited time to place as many calls as possible from a soundproof booth. During that time, their goal is to elicit from the receiver as many objectives as possible. Whether you're an attacker, defender, business executive, or brand new to this community, you can learn by witnessing firsthand how easy it is for some competitors to schmooze their way to their goals and how well prepared some companies are to shut down those competitors!

2023 judges: Corgi, FC aka freakyclown, and Snow 2023 coaches: Ibetika, JC, C_3PJoe, and Split Beans (last year's SECVV winners: Jenn, Matt, and Sean)

This competition takes place on Friday in the Social Engineering Community village, be sure to get there early to get a seat; they fill up fast! Additionally, at the end of Friday, join Snow as she covers the behind the scenes of creating the SECVV, this year's lessons learned, team highlights, and tips for future competitors!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 09:00-17:59 PDT

Title: Social Engineering Community (SEC) Youth Challenge

When: Saturday, Aug 12, 09:00 - 17:59 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description:

The purpose of the Youth Challenge is to provide anyone under the age of 17 with an event for them to participate. Challenges and puzzles incorporate general cybersecurity with an emphasis on OSINT and Social Engineering. Challenges will be crafted in a way that steers participants to different villages with specific goals to broaden their exposure of different subject matter available at DEF CON. There will be a sign-up form prior to DEF CON, as well as encouraging walk-up participation for those who may not have been aware of the offering.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 09:00-17:59 PDT

Title: Social Engineering Community (SEC) Youth Challenge

When: Friday, Aug 11, 09:00 - 17:59 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Description:

The purpose of the Youth Challenge is to provide anyone under the age of 17 with an event for them to participate. Challenges and puzzles incorporate general cybersecurity with an emphasis on OSINT and Social Engineering. Challenges will be crafted in a way that steers participants to different villages with specific goals to broaden their exposure of different subject matter available at DEF CON. There will be a sign-up form prior to DEF CON, as well as encouraging walk-up participation for those who may not have been aware of the offering.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 22:00-23:59 PDT

Title: Social Engineering Community Party

When: Saturday, Aug 12, 22:00 - 23:59 PDT

Where: Caesars Forum - Forum - 117-118 - [Map](#)

Description:

Want to hang out without the loud music so that you can actually have a conversation? Put on your raddest 80s gear and join the Social Engineering Community for a themed get-together for a chance to hang out and meet new people! We'll have a cash bar with both boozy and booze-free options.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Saturday - 10:00-17:59 PDT

Title: Soldering Skills Village Activities

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Description:

Have you ever fused metal to create electronic mayhem? Do you want to learn? Travel too far to take your solder tools with you? Hotel take your irons cause they thought it was a fire risk? Come on over to the Solder Skills village. We have irons and supplies. Volunteers (and some attendees) help teach, advise or just put out fires. We aim to grow the skill-set of the community and overcome inhibitions to this most basic skill to make electronic dreams happen.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Sunday - 10:00-12:59 PDT


Title: Soldering Skills Village Activities

When: Sunday, Aug 13, 10:00 - 12:59 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Description:

Have you ever fused metal to create electronic mayhem? Do you want to learn? Travel too far to take your solder tools with you? Hotel take your irons cause they thought it was a fire risk? Come on over to the Solder Skills village. We have irons and supplies. Volunteers (and some attendees) help teach, advise or just put out fires. We aim to grow the skill-set of the community and overcome inhibitions to this most basic skill to make electronic dreams happen.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Friday - 10:00-17:59 PDT


Title: Soldering Skills Village Activities

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering Vlgs - [Map](#)

Description:

Have you ever fused metal to create electronic mayhem? Do you want to learn? Travel too far to take your solder tools with you? Hotel take your irons cause they thought it was a fire risk? Come on over to the Solder Skills village. We have irons and supplies. Volunteers (and some attendees) help teach, advise or just put out fires. We aim to grow the skill-set of the community and overcome inhibitions to this most basic skill to make electronic dreams happen.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Space Pirates on the Loose! - Space-Based Threats to US Interests

When: Saturday, Aug 12, 15:00 - 15:25 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Speakers:Henry Danielson,Sage Meadows

SpeakerBio:Henry Danielson

No BIO available

SpeakerBio:Sage Meadows

No BIO available

Description:

Many US interests heavily depend on space assets. With the rapid development of space technology, security is often overlooked. This talk covers a range of space-based attack scenarios, developed via extensive threat modeling efforts (attack trees, PnGs, etc). The paper being produced from this research effort will be presented to the National Space Council. By addressing these issues, the US can strengthen its resilience in space and ensure the security of critical space-based infrastructures.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: SpamChannel: Spoofing Emails From 2 Million+ Domains and Virtually Becoming Satan

When: Friday, Aug 11, 11:00 - 11:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio: Marcello "byt3bl33d3r" Salvati , Hacker & Entrepreneur

Marcello Salvati (byt3bl33d3r) is a hacker & entrepreneur with over a decade of experience as an Offensive Security Researcher, Blue/Purple/Red Teamer and Open Source developer. Marcello is known for creating a number of Open Source tools such as CrackMapExec and weaponizing unorthodox programming languages for malware purposes.

Twitter: [@byt3bl33d3r](#)

Description:

Ever wake up and ask yourself: "Damn, how could I make email security suck even more today"? Tired of your Red Teams phishing emails not landing in your targets inbox? Do you dislike Boston (the city) and love Satan?

If you answered yes to any of those questions you should come to this talk!

I'll be showing you how to spoof emails from 2 million+ domains (while also "bypassing" SPF & DMARC!) by (ab)using a partnership between Cloudflare and the "biggest transactional email service" on the interwebs. We'll be diving into "edge" serverless applications and the magical world of email security where everything is (still) held up by duct tape, pasta, and marinara sauce. Finally, I'll be dropping code and releasing a tool that demonstrates how to impersonate emails from 2million+ domains.

REFERENCES

- ◇ <https://blog.mailchannels.com/mailchannels-enables-free-email-sending-for-cloudflare-workers-customers>
- ◇ <https://trends.builtwith.com/mx/transactional-email/traffic/Entire-Internet>
- ◇ <https://blog.cloudflare.com/sending-email-from-workers-with-mailchannels/>
- ◇ <https://trends.builtwith.com/websitelist/MailChannels>
- ◇ <https://www.rapid7.com/research/project-sonar/>
- ◇ <https://gist.github.com/ihsangan/6111b59b9a7b022b5897d28d8454ad8d>
- ◇ <https://community.cloudflare.com/t/send-email-from-workers-using-mailchannels-for-free/361973/11>
- ◇ WWW'22 Talk: Revisiting Email Forwarding Security under the Authenticated Received Chain Protocol (<https://www.youtube.com/watch?v=V9kajr5dESs>)
- ◇ <http://arc-spec.org/>
- ◇ <https://www.rfc-editor.org/rfc/rfc8617.html>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Friday - 17:00-17:45 PDT

Title: Spoofing certificates with MD5 collisions - party like it's 2008!

When: Friday, Aug 11, 17:00 - 17:45 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

Speakers: Tomer, Yoni


SpeakerBio: Tomer

No BIO available

SpeakerBio: Yoni

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Spooky authentication at a distance

When: Saturday, Aug 12, 15:00 - 15:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio: Tamas "SkelSec" Jos , Principal Security Consultant at Sec-Consult AG

Tamas Jos (@skelsec) is a principal security consultant at SEC Consult (Schwiez) AG. He has worked within the information security industry for over 10 years, focusing mainly on reversing topics across many industries around the globe. He has an in-depth technical appreciation of Windows security, which heavily influences his research. This often takes him down many low level rabbit holes, leading to the creation and maintenance of well-received open-source projects, such as pypykatz & OctoPwn.

You can find Tamas' musings on his blog at <https://github.com/skelsec/>

Twitter: [@skelsec](#)

Description:

Spooky authentication at a distance outlines a new and innovative post-exploitation technique to proxy common authentication protocols used in Windows environments remotely and with no elevated privileges required. This allows security professionals to perform complete impersonation of the target user on their own machine without executing any further code on the target machine besides the agent itself. This talk will also demonstrate the applicability of this new technique by performing no-interaction, full domain takeover using a malicious peripheral in a simulated restricted environment.

REFERENCES

Tools which will be showed in the demos: [AioSMB] <https://github.com/skelsec/aiosmb> [MSLDAP] <https://github.com/skelsec/msldap> [WSNet] <https://github.com/skelsec/wsnet> [OctoPwn] <https://community.octopwn.com> [Asyauth] <https://github.com/skelsec/asyauth> [Aardwolf] <https://github.com/skelsec/aardwolf>

My previous talk on [OctoPwn] the in-browser pentest suite can be found here: <https://youtu.be/jStdRHTmD4>

Related tools:

[PYODIDE] Octopwn uses Pyodide framework to run in the browser. <https://github.com/pyodide/pyodide> [LDAP3] The MSLDAP project used code parts from this project. <https://ldap3.readthedocs.io/en/latest/> [RDPY] The Aardwolf RDP client is based on this tool. <https://github.com/citronneur/rdpy> [BLOODHOUND] Jackdaw was based on this tool. <https://github.com/BloodHoundAD/BloodHound> [IMPACKET] aioSMB libraries were based partially on this tool. <https://github.com/fortra/impacket> [LsaRelayX] Future extension <https://github.com/CCob/lsarelayx> [duckencoder] To automate keystrokes on the embedded system <https://github.com/mame82/duckencoder.py>

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Friday - 11:00-12:59 PDT

Title: Spot the True Positives!

When: Friday, Aug 11, 11:00 - 12:59 PDT


Where: Flamingo - Savoy - AppSec Village - Pod 3 - [Map](#)

SpeakerBio: Backslash

No BIO available

Description:

Have participants find the true positives out of 5 SQLi.

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Saturday - 11:00-12:59 PDT

Title: Spot the True Positives!

When: Saturday, Aug 12, 11:00 - 12:59 PDT


Where: Flamingo - Savoy - AppSec Village - Pod 3 - [Map](#)

SpeakerBio: Backslash

No BIO available

Description:

Have participants find the true positives out of 5 SQLi.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Spread spectrum techniques in disposable drones for anti drone evasion

When: Saturday, Aug 12, 11:00 - 11:45 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

Speakers:David Melendez,Gabriela "Gabs" García

SpeakerBio:David Melendez , R&D Embedded Software Engineer

David Melendez is an R&D Embedded Systems Engineer, with over twelve years of experience in cybersecurity and hardware hacking. He has a proven track record of presenting his groundbreaking investigations at prestigious conferences around the world, including DEFCON, BLACKHAT, and ROOTEDCON.

David is also a drone creator and author of the book "Hacking with Drones," which showcases his innovative use of drones in cybersecurity research. With his passion for pushing the boundaries of technology, David is constantly seeking new ways to improve the security and functionality of embedded systems.

Twitter: [@@taiksontexas](#)

SpeakerBio:Gabriela "Gabs" García , Hacker, Professor and Mentor

Gabriela "Gabs" García is a university professor and mentor, Secure Software Developer and coding and cybersecurity instructor for organizations such as LinkedIn, Cyber Hunter Academy and Kschool. She teaches, whether that's in a lecture hall or over the internet, about software development, with a keen eye for secure practices.

Gabriela is also an active member in hacker communities such as HackMadrid%27 and Hack%27, both at home in Spain and across the world. And as an independent professional, she gets to work with a wide variety of clients, crafting custom cybersecurity solutions to fit their specific needs.

Description:

The popularity of cheap and DIY drones has made them a target for attackers using radiofrequency (RF) signals. Frequency hopping is a technique that can be used to mitigate the risks associated with RF warfare. However, implementing frequency hopping in cheap and DIY drones presents several technical challenges, such as the need for a stable clock and synchronization between the transmitter and receiver without rising hardware costs. Despite these challenges, frequency hopping can significantly enhance the security of consumer and DIY drones making much more challenging or even useless anti-drone systems' role.

REFERENCES

DEF CON 24 - Aaron Luo - Drones Hijacking: Multidimensional attack vectors and countermeasures DEF CON 25 - Game of Drones - Brown,Latimer DEF CON 26 - David Melendez Cano - Avoiding antidrone systems with nanodrones. DEF CON 29 - Steal This Drone - An Aerospace Village Cybersecurity Activity -

<http://loonwerks.com/publications/pdf/Steal-This-Drone-README.pdf>

<https://unicornriot.ninja/2017/hacking-drones-ultrasonic-pulses/> [https://en.wikipedia.org/wiki/Tempest_\(codename\)](https://en.wikipedia.org/wiki/Tempest_(codename))

[Return to Index](#) - Add to  - ics [Calendar](#) file

TCV - Friday - 16:00-17:59 PDT

Title: SS7 CTF

When: Friday, Aug 11, 16:00 - 17:59 PDT

Where: Flamingo - Virginia City - Telecom Village - [Map](#)

Speakers: Akib Sayyed, Zibran Sayyed


SpeakerBio: Akib Sayyed , Director at Matrix Shell Technologies Prviate Limited

No BIO available

SpeakerBio: Zibran Sayyed , Sr. Security Consultant Telecom

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

TCV - Friday - 14:30-15:59 PDT

Title: SS7 Workshop

When: Friday, Aug 11, 14:30 - 15:59 PDT

Where: Flamingo - Virginia City - Telecom Village - [Map](#)

Speakers: Akib Sayyed, Zibran Sayyed


SpeakerBio: Akib Sayyed , Director at Matrix Shell Technologies Prviate Limited

No BIO available

SpeakerBio: Zibran Sayyed , Sr. Security Consultant Telecom

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

TCV - Friday - 11:00-12:59 PDT

Title: SS7 Workshop

When: Friday, Aug 11, 11:00 - 12:59 PDT

Where: Flamingo - Virginia City - Telecom Village - [Map](#)

Speakers: Akib Sayyed, Zibran Sayyed


SpeakerBio: Akib Sayyed , Director at Matrix Shell Technologies Prviate Limited

No BIO available

SpeakerBio: Zibran Sayyed , Sr. Security Consultant Telecom

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: SSH Tunneling: Evading Network Detection and Creating Proxies

When: Friday, Aug 11, 15:00 - 15:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 5 - [Map](#)

SpeakerBio: Cory Wolff

No BIO available

Twitter: [@cwolff411](#)

Description:

SSH tunneling is a valuable component of the red teamer's toolkit when used correctly - but that's the hard part. Demystifying reverse port forwards, local port forwards, and dynamic port forwards can be a challenge for any operator. This talk will begin with the basics of SSH tunneling and then focus on ways to utilize them to create reverse proxies and evade network monitoring during an engagement. It aims to provide clarity on the use of these different port forwards and provide examples on how to use them in an offensive security scenario.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: SSO Sloppy, SSO Suspect, SSO Vulnerable

When: Saturday, Aug 12, 11:10 - 11:50 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Jenko Hwong , Principal Researcher, Threat Research Team at Netskope

Jenko Hwong is a Principal Researcher on Netskope's Threat Research Team, focusing on cloud threats/vectors. He's spent time in engineering and product roles at various security startups in vulnerability scanning, AV/AS, pen-testing/exploits, L3/4 appliances, threat intel, and windows security.

Twitter: [@jenkohwong](#)


Description:

Enterprise SSO protocols and vendor implementations continue to evolve for the worse, as we've gone from SAML to OAuth to MUVP (Made-Up-Vendor-Protocol).

Attacks against SSO started with the Golden SAML attack (Cyberark, 11/2017), which used stolen certificates to spoof SAML responses, recently used in the SolarWinds hack in 2020. Recently, OAuth has been used to implement SSO, and new POC identity attacks have been published such as gaining access to a Facebook account that uses Gmail as the SSO identity provider via OAuth 2.0 (Sammouda, 5/2022), utilizing the chaining of traditional web vulnerabilities such as XSS with the design of the OAuth protocol in order to steal OAuth session tokens. AWS's SSO implementation mixes SAML, OAuth, and traditional AWS access keys. And Microsoft and Google also use custom OAuth to implement SSO among their app suites.

This protocol soup opens up more areas for abuse by attackers with key benefits: remotely-enabled attacks by design without need for endpoint compromise, near-permanent access, no need to go through MFA challenges, and incomplete controls for in preventing, detecting, and responding to these attacks.

We will demonstrate how these attacks work, what's different, how the underlying SSO protocols and features are abused, and where defensive measures fail.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: StackMoonwalk: A Novel approach to stack spoofing on Windows x64

When: Sunday, Aug 13, 10:00 - 10:45 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

Speakers: Alessandro "klezVirus" Magnosi, Arash "waldo-irc" Parsa, Athanasios "trickster0" Tserpelis

SpeakerBio: Alessandro "klezVirus" Magnosi, Principal Security Consultant at BSI

Alessandro Magnosi is a Principal cyber security consultant with more than 10 years of experience in the IT field. Currently, he's part of the Security Testing Team at BSI, which is the UK national standards body, and a Global certification, training and cybersecurity firm. On top of his normal work, Alessandro works as an independent researcher for Synack RT, and an OSS developer for Porchetta Industries, where he maintains offensive tools.

Twitter: [@@klezVirus](#)

SpeakerBio: Arash "waldo-irc" Parsa, Cybersecurity Professional

Arash Parsa is a highly skilled and passionate cybersecurity professional with extensive experience in threat hunting, red teaming, and research. As a dedicated member of the InfoSec community, Arash has become a trusted name in advancing the field and helping to protect digital assets from ever-evolving threats. Above all, Arash takes great pride in being an active community member and mentor to aspiring cybersecurity professionals. By sharing their knowledge and experience, he is helping to shape the next generation of InfoSec experts and ensure the continued growth and success of the industry.

Twitter: [@@waldoirc](#)

SpeakerBio: Athanasios "trickster0" Tserpelis, Red Teamer and Malware Developer

Thanos is a senior security consultant in Nettitude, focused mainly in Red Teaming and specializes in Offensive tool development such as elaborate malwares, EDR evasion techniques and tooling that makes a red teamer's life easier. Additionally, he is really into low level stuff, such as exploit development in Windows OS.

Twitter: [@trickster012](#)

Description:

The rapid advancement of cyber defense products has led to an increase in sophisticated memory evasion techniques employed by Red Teaming and Malware Development communities. These techniques aim to bypass the detection of malicious code by concealing its presence in a target process's memory. Among these methods, "Thread Stack Spoofing" is a technique that hides malicious calls in the stack by replacing arbitrary stack frames with fake ones.

In this talk, we present two novel approaches, "Full Moon" and "Half Moon," for tampering with call stacks in a manner that is both opaque and difficult to detect. These techniques manipulate the call stack to produce unwinding or logically valid stacks, thwarting conventional detection methods.

We also introduce a detection algorithm, Eclipse, designed to identify instances of these tampering techniques. This algorithm extends the functionality of RtlVirtualUnwind to perform strict checks on specific instructions and call sequences, enabling the detection of tampered call stacks. We evaluate the efficacy of Eclipse against both Full Moon and Half Moon techniques and discuss its performance and limitations.

Additionally, we explore the possibility of combining these techniques to create an even more robust method for call stack tampering that is resistant to detection. Our study contributes to the growing body of knowledge in the field of call stack tampering and detection and provides valuable insights for researchers and security professionals aiming to mitigate such threats.

REFERENCES

namazso. 2019. x64 return address spoofing (source + explanation). UnKnoWnCheatTs - Multiplayer Game Hacking and Cheats. Retrieved April 4, 2023 from

<https://www.unknowncheats.me/forum/anti-cheat-bypass/268039-x64-return-address-spoofing-source-explanation.html>
Mariusz Banach. 2023. Thread Stack Spoofing / Call Stack Spoofing PoC. Retrieved April 3, 2023 from <https://github.com/mgeeky/ThreadStackSpoofers>
William Burgess. Behind the Mask: Spoofing Call Stacks Dynamically with Timers | Cobalt Strike Blog. Fortra. Retrieved April 3, 2023 from <https://www.cobaltstrike.com/blog/behind-the-mask-spoofing-call-stacks-dynamically-with-timers/>
William Burgess. Spoofing Call Stacks To Confuse EDRs. Retrieved April 4, 2023 from <https://labs.withsecure.com/publications/spoofing-call-stacks-to-confuse-edrs>
Microsoft Corp. 2021. x64 prolog and epilog. Retrieved April 3, 2023 from <https://learn.microsoft.com/en-us/cpp/build/prolog-and-epilog>
Microsoft Corp. 2022. x64 exception handling. Retrieved April 3, 2023 from <https://learn.microsoft.com/en-us/cpp/build/exception-handling-x64>
CodeMachine. 2021. x64 Deep Dive. Retrieved April 3, 2023 from https://www.codemachine.com/article_x64deepdive.html

Return to Index - Add to  - ics [Calendar](#) file

Title: Starbase: open source graph security analysis (Pre-Registration Required)

When: Saturday, Aug 12, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers: Adam Pierson, Austin Kelleher, Guillaume Ross

SpeakerBio: Adam Pierson

Adam Pierson is a Senior Software Engineer at JupiterOne. His diverse experience includes time as an embedded software engineer, an R&D analyst working on adopting emerging technologies within large corporate IT environments, and as a developer demonstrating the value of using graph databases to solve complex problems. Currently he is on JupiterOne's Integration team working on development tools and continuing work on the open-source Starbase project.

SpeakerBio: Austin Kelleher

Austin Kelleher is a Principal Software Engineer as well as a founding member at JupiterOne. He leads the team responsible for maintaining 100+ open-source projects at JupiterOne. His background has primarily been focused on developing cloud-based software systems and tools that interact with graphs for security analysis. Prior to moving to the security industry, Austin was an engineer at eBay building Marko and Lasso, which are the open-source web tools that power the eBay.com web experience.

SpeakerBio: Guillaume Ross , JupiterOne

Guillaume has worked on the blue-team side of security for close to two decades now, and loves to do things because they MATTER and not just because everyone else in security is doing the same. He leads the security and IT teams at JupiterOne.

Description:

Security teams are overwhelmed with data. How does a user account relate to a server, an application? Does this vulnerability put this important data at risk, or does it simply expose a few systems we care about much less? Who really has access to these files? This is vulnerable, but the firewall won't let traffic to the service, or will it?

These types of questions are very difficult to answer in a vacuum as they require context. With the power of graphs, and Starbase, an open source graph security analysis tool, we will be able to import the data that allows us to answer them using the graph.

John Lambert said "Defenders think in lists, attackers think in graphs". Join us, so we can get a lot more people thinking in graphs!

Skill Level: Intermediate

Prerequisites for students:

Ability to use Docker when provided with commands. Basic understanding of IT and security issues in cloud environments.

Materials or Equipment students will need to bring to participate: A laptop with Docker as well as a few docker images pulled in advance.

Due to the brittle nature of conference Wi-Fi, we'll send instructions in advance, so as many people as possible will have downloaded it.

Title: Still Vulnerable Out of the Box: Revisiting the Security of Prepaid Android Carrier Devices

When: Friday, Aug 11, 12:00 - 12:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers: Angelos Stavrou, Mohamed Elsabagh, Ryan Johnson

SpeakerBio: Angelos Stavrou , Founder and Chief Scientist at Quokka

Dr. Angelos Stavrou is Founder and Chief Scientist of Quokka (formerly Kryptowire), a Virginia based Mobile Security company. He is also a Professor at the Bradley Department of Electrical & Computer Engineering at Virginia Tech. Dr. Stavrou has served as principal investigator on research awards from NSF, DARPA, IARPA, DHS, AFOSR, ARO, ONR. He is an active member of NIST's Mobile Security team and has written more than 130 peer-reviewed conference and journal articles. Dr. Stavrou received his M.Sc. in Electrical Engineering, M.Phil. and Ph.D. (with distinction) in Computer Science all from Columbia University. He also holds an M.Sc. in theoretical Computer Science from the University of Athens and a B.Sc. in Physics with distinction from the University of Patras, Greece. Stavrou is an Associate Editor of IEEE Transactions on Computers, IEEE Security & Privacy, and IEEE Internet Computing magazines and a previous co-chair of the IEEE Blockchain initiative. Over the past few years, Dr. Stavrou's research has focused on two aspects of security: Systems' Security and Reliability. Dr. Stavrou is a member of USENIX, and a senior member of ACM and IEEE.

SpeakerBio: Mohamed Elsabagh , Senior Director, R&D at Quokka

Dr. Mohamed Elsabagh leads the research and development efforts at Quokka (formerly Kryptowire). He specializes in automated static/dynamic binary security analysis and reverse engineering for Android, ARM, and x86 platforms. He has created several tools that helped detect and prevent hundreds of zero-day vulnerabilities in the wild. Mohamed holds a PhD in CS during which he developed automated binary hardening techniques for COTS systems.

SpeakerBio: Ryan Johnson , Senior Director, R&D at Quokka

Dr. Ryan Johnson is a Senior Director, R&D at Quokka (formerly Kryptowire). His research interests are static and dynamic analysis of Android apps and reverse engineering. He is a co-founder of Quokka and has presented at DEF CON, Black Hat (USA, Asia, & MEA), IT-Defense, and @Hack. His research in Android security has been assigned dozens of CVEs and is responsible for discovering the Adups spyware that affected millions of Android smartphones.

Description:

Prepaid Android smartphones present an attractive option since they can be used and discarded at will without significant financial cost. The reasons for their use are manifold, although some people may use them to dissemble their true identity. Prepaid smartphones offer value, but there may be an additional "cost" for their cheap price. We present an examination of the local attack surface of 21 prepaid Android smartphones sold by American carriers (and 11 unlocked smartphones). While examining these devices, we discovered instances of arbitrary command execution in the context of a "system" user app, arbitrary AT command execution, arbitrary file write in the context of the Android System (i.e., "system_server"), arbitrary file read/write in the context of a "system" user app, programmatic factory reset, leakage of GPS coordinates to a loopback port, numerous exposures of non-resettable device identifiers to system properties, and more.

The only user interaction that our threat model assumes is that the user installs and runs a third-party app that has no permissions or only a single "normal" level permission that is automatically granted to the third-party app upon installation. The installed third-party app can leverage flaws in pre-loaded software to escalate privileges to indirectly perform actions or obtain data while lacking the necessary privileges to do so directly. Due to a wide range of local interfaces with missing access control checks and inadequate input validation, a third-party app's behavior is not truly circumscribed by the permissions that it requests. Due to the common inclusion of pre-loaded software from Android vendors, chipset manufacturers, carriers, and vendor partners, exploit code can have significant breadth. The inter-app communication used to exploit these vulnerabilities may be difficult to classify as inherently malicious in general since it uses the standard communication channels employed by non-malicious apps.

We pick up again where we left off from our DEF CON 26 talk ... raiding the prepaid Android smartphone aisles at Walmart.

We provide another snapshot on the state of security for Android carrier devices. In this talk, we examine 21 different prepaid Android smartphones being sold by the major American carriers, and we also cover 11 unlocked Android devices, which are primarily ZTE smartphones. We identified vulnerabilities in multiple layers of the Android software stack. For each discovered vulnerability, we step through the attack requirements, access vector, and attack workflow in order to help developers and bug hunters identify common software flaws going forward.

REFERENCES

<https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1030664>
<https://www.bleepingcomputer.com/news/security/oneplus-phones-come-preinstalled-with-a-factory-app-that-can-root-devices/>
<https://source.android.com/docs/security/features/selinux#background>
https://en.wikipedia.org/wiki/Confused_deputy_problem <https://github.com/thanuj10/Nokia-Debloater>
<https://developer.android.com/training/articles/user-data-ids#best-practices-android-identifiers>
<https://android.googlesource.com/platform/hardware/ril/+master/include/telephony/ril.h>
https://github.com/lbule/android_hardware_mediatek https://security.tecno.com/SRC/blogdetail/99?lang=en_US
<https://extensionpublications.unl.edu/assets/pdf/ec157.pdf>
<https://android.googlesource.com/platform/frameworks/base/+master/core/java/android/service/persistentdata/PersistentDataBlock>
<https://github.com/ptoomey3/evilarc/blob/master/evilarc.py>
<https://android.googlesource.com/platform/frameworks/base/+master/packages/SystemUI/>
<https://android.googlesource.com/platform/packages/apps/Settings/+refs/heads/master>

Return to Index - Add to  - ics Calendar file

Title: Storfield: A Quiet Methodology to Create Attacks in Mature Networks

When: Saturday, Aug 12, 13:00 - 13:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 3 - [Map](#)

SpeakerBio: Cory Wolff

No BIO available

Twitter: [@cwolff411](#)

Description:

The Storfield Methodology focuses on three main questions: Where am I? Where is the DC? Where are the high-value targets? The Storfield Methodology is meant to be repeatable during every engagement. When following this method the steps should be the same regardless of the security controls implemented in a particular network.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Storfield: A Quiet Methodology to Create Attacks in Mature Networks

When: Sunday, Aug 13, 11:00 - 11:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - Area 4 - [Map](#)

SpeakerBio: Cory Wolff

No BIO available

Twitter: [@cwoff411](#)

Description:

The Storfield Methodology focuses on three main questions: Where am I? Where is the DC? Where are the high-value targets? The Storfield Methodology is meant to be repeatable during every engagement. When following this method the steps should be the same regardless of the security controls implemented in a particular network.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Saturday - 14:30-14:55 PDT

Title: Stories from the Trenches: Operating a Aeronautics Cyber Range

When: Saturday, Aug 12, 14:30 - 14:55 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio: Christopher Ottesen

No BIO available

Description:

The Aeronautics Cyber Range performs penetration testing on DoD aviation weapons systems. Since becoming operational in 2019, the team has accumulated many lessons learned and best practices to support testing of aerospace embedded systems.

This talk details how to deal with fundamental challenges of operating this type of facility. Brace yourselves for an incredible journey filled with the obstacles we encountered and the strategies and tactics you can use to avoid our growing pains.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Stories from the Trenches

When: Friday, Aug 11, 11:00 - 11:59 PDT

Where: Flamingo - Sunset-Twilight Ballroom - Red Team Village - [Map](#)

Speakers: Ben "NahamSec" Sadeghipour, Barrett Darnell, John Hammond, Ryan M. Montgomery, Savannah Lazzara

SpeakerBio: Ben "NahamSec" Sadeghipour, Hacker & Content Creator at NahamSec

Ben Sadeghipour AKA NahamSec is a security researcher and content creator. He's currently in the top 100 for both HackerOne(25) and Bugcrowd's (95) leaderboards. He has helped identify over a thousand vulnerabilities in companies like Amazon, Apple, Airbnb, Lyft, Snapchat and more. Prior to doing content creation full time, he worked as a research and community education executive at Hadrian and HackerOne. Ben has presented many talks and workshops at cons such as DEFCON, BSides, OWASP AppSec, RSA, Red Team Village, and more. He also enjoys hosting and organizing hacker meetups or virtual conferences such as NahamCon and Hacktivitycon!

Twitter: [@nahamsec](#)

SpeakerBio: Barrett Darnell

No BIO available

Twitter: [@pwnEIP](#)

SpeakerBio: John Hammond

No BIO available

Twitter: [@_JohnHammond](#)

SpeakerBio: Ryan M. Montgomery

No BIO available

Twitter: [@0dayCTF](#)

SpeakerBio: Savannah Lazzara

No BIO available

Twitter: [@lazzslayer](#)

Description:

Keynote Panel moderated by Ben Sadeghipour [@nahamsec](#)

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Strix Interceptor

When: Friday, Aug 11, 10:00 - 11:55 PDT

Where: Caesars Forum - Unity Boardroom - Demo Labs - [Map](#)

SpeakerBio: Lexie Thach

Lexie Thach is a dedicated cybersecurity professional who has spent nearly a decade honing her skills in various roles within the industry. Throughout her journey, she has had the privilege of gaining invaluable experience in diverse cybersecurity domains, including ICS/SCADA and avionics security. Driven by an insatiable thirst for knowledge, Lexie has developed a genuine passion for electrical engineering, programming, and robotics engineering, despite not having a conventional academic background. She is currently working towards completing her studies, constantly striving to expand her knowledge and capabilities. Lexie's journey began at a young age when she made the decision to serve her country in the US Airforce. For a period of eight years, she had the opportunity to contribute her expertise in cyber security and tactical networks for aircraft missions and operations. It was during this time that she was exposed to the complexities of intercepting aircraft, particularly drones, and learned valuable lessons from observing the tactics and techniques employed by state actors, hacker groups, and organizations. Drawing from her diverse experiences and the challenges she faced, Lexie has embarked on projects centered around securing and assessing the security of autonomous systems. Her passion is rooted in the desire to share the techniques she has learned and to contribute to the advancement of secure autonomous systems.

Description:

The development of unmanned aerial vehicles (UAVs) has revolutionized data collection, but security challenges have emerged. In response, Strix is a security testing UAV designed to intercept other UAVs in flight while adhering to legal limitations. It utilizes software analysis to detect and track unauthorized UAVs, predicting their flight path without compromising itself. Strix also encompasses ground-based support systems for enhanced mission effectiveness. The ground-based robots and drones can perform tasks such as reconnaissance, target identification, and data analysis to enhance the effectiveness of Strix's mission. The drone can detect RF anti-drone systems and, if identified, utilize multi-RF spoofing technology to disrupt or block their signals. This allows Strix to enter protected airspace undetected, while staying within legal bounds when required. Strix was designed to identify other UAVs and attempt to jam or possibly control their signals to their flight operators. Its hardware includes sensors, a robust communication system, and the Pixhawk autonomous flight module, which provides open-source flexibility and customization options. Strix's small and agile design enables high-speed flight and maneuverability in confined spaces. Advanced encryption ensures data security during collection and transmission. As an open-source project, Strix encourages customization and collaboration, making it an invaluable tool for securing airspace and mitigating UAV threats. Its interception capabilities and defensive measures, including multi-RF spoofing, contribute to UAV-driven security systems while respecting legal considerations. This makes it a powerful tool for securing airspace and preventing unauthorized UAVs from posing a threat. Its ability to detect and intercept UAVs in flight, coupled with its defensive capabilities against anti-drone systems, including the ability to employ multi-RF spoofing technology, makes Strix an essential component of any security system that relies on UAVs for data collection and analysis. Strix aims to showcase the potential of UAVs in a lawful and responsible manner, promoting safety, innovation, and ethical practices within the drone industry.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: SucoshScanny

When: Friday, Aug 11, 10:00 - 11:55 PDT

Where: Caesars Forum - Caucus Boardroom - Demo Labs - [Map](#)

Speakers:Mustafa Bilgici,Tibet Ögünç

SpeakerBio:Mustafa Bilgici

Mustafa Bilgici has been doing cyber security and application security research for 4 years. It conducted vulnerabilities in many applications and reported these vulnerabilities to companies. He also works as a cyber security researcher and developer in various cyber security companies.

SpeakerBio:Tibet Ögünç

Tibet Ögünç has been doing cyber security and application security research for 4 years and has discovered vulnerabilities in many web applications and helped organizations to protect themselves from attackers. As a developer in web coding languages such as Node Js., Python, Php Javascript, he works as a software developer and team leader for the development of many products.

Description:

SucoshScan is a automated open source SAST(Static Application Security Testing) framework. It's can detect a lot of vulnerability(RCE,SSTI,Insecure Deserialisation,SSRF,SQLI,CSRF etc.) in given source code.For now, only the detection modules of python(flask,django) and nodejs(express js.) languages are finished. In the future, specific detection functions will be written for php (Laravel, Codeigniter), .NET, Go languages.

[Return to Index](#) - Add to  - ics [Calendar](#) file

BHV - Saturday - 11:40-12:40 PDT

Title: Surgical Physicians and Cybersecurity

When: Saturday, Aug 12, 11:40 - 12:40 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

SpeakerBio:Colin Haines

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Friday - 11:45-12:20 PDT

Title: Surprise Unboxing

When: Friday, Aug 11, 11:45 - 12:20 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio:Harri Hursti

Harri Hursti, a world renowned data security expert and internet visionary is the Founder of the 501(c)(3) organization the Election Integrity Foundation as well as an original co-Founder of the Voting Village. Featured in two Emmy nominated documentaries, Mr. Hursti is famously known for the Hursti Hacks, where he demonstrated how to successfully alter final voting results on the Diebold Election Systems voting machines.

Twitter: [@harrihursti](#)

Description:

Harri Hursti will be doing an unboxing of something very high profile.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: SusParams: Hypercharge your web testing with DATA

When: Saturday, Aug 12, 15:00 - 15:45 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

SpeakerBio: Jason Haddix , CISO and “Hacker in Charge” at BuddoBot

Jason Haddix is the CISO and “Hacker in Charge” at BuddoBot, a world-class adversary emulation consultancy. He's had a distinguished 15-year career in cybersecurity previously serving as the CISO of Ubisoft, Head of Trust/Security/Operations at Bugcrowd, Director of Penetration Testing at HP, and Lead Penetration Tester at Redspin. He has also held positions doing mobile penetration testing, network/infrastructure security assessments, and static analysis. Jason is a hacker and bug hunter to the core, and he is ranked 51st all-time on Bugcrowd's leaderboards. Currently, he specializes in recon and web application analysis. Jason has also authored many talks on offensive security methodology, including speaking at cons such as; DEF CON, Black Hat, OWASP, RSA, Nullcon, SANS, IANS, BruCon, Toorcon, and many more. Jason currently lives in Colorado with his wife and three children.

Twitter: [@jhaddix](#)

Description:

SusParams is a testing dataset for offensive security folk assessing web technologies. Years ago, I released a tool called HUNT at DEF CON and Blackhat Arsenal. The secret sauce was a dataset of commonly vulnerable parameters to certain web vulnerability types. This dataset was created using statistical analysis of over 18,000 parameters. Jhaddix and Gunnar have extended this research to over 40,000 parameters. Our data sources have expanded into hackerone hacktivity, 5 years of recent CVE data, XSSed.com, and more!

Join us as we release this epic tool and helper scripts to supercharge your offensive web hacking.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: T3SF (Technical TableTop Exercises Simulation Framework)

When: Friday, Aug 11, 10:00 - 11:55 PDT

Where: Caesars Forum - Council Boardroom - Demo Labs - [Map](#)

Speakers: Federico Pacheco, Joaquin Lanfranconi

SpeakerBio: Federico Pacheco

Federico - Cybersecurity professional with background in electronics engineering and several industry renowned certifications. 20+ years of teaching experience at the most prestigious universities in Argentina. Published 4 books and several research whitepapers. Has worked for the public and private sector, including regional roles in global companies.

SpeakerBio: Joaquin Lanfranconi

Joaquin - Offensive cybersecurity professional with extensive programming skills, currently working as Cybersecurity Researcher. He is among the first positions of the Argentinean ranking in the main CTFs platforms, and stands out in the global rankings, besides contributing to the security community by writing posts and write-ups.

Description:

T3SF is a framework that offers a modular structure for the orchestration of injects from a master scenario events list (MSEL) together with a set of rules defined for each exercise and a configuration that allows defining the parameters of the correspondent platform. The main module performs the communication with the specific module (Discord, Slack, Telegram, WhatsApp, Teams, etc.) which allows the events to be presented in the input channels as messages in the platform. It supports different use cases for single or multiple organizations.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Table Top

When: Sunday, Aug 13, 10:00 - 12:20 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

Speakers: Felicity Milman, Jorge Acevedo Canabal, Nathan Case

SpeakerBio: Felicity Milman

Felicity is a cyberneticist who has been working on a range of technologies over many years and has graduate degrees in both psychology and engineering. She has worked on a range of projects from designing and patenting genetic tests, to developing hybrid human-AI chat bot systems, to developing educational AI games systems which are personalised to the learner. More recently she has been developing the complex systems curriculum for the Australian National University and developing cybersecurity simulation games for the National Security College, which have been played by numerous international governments.

SpeakerBio: Jorge Acevedo Canabal

Jorge Acevedo, MD.: a rare disease and disaster recovery physician in Puerto Rico with an interest in AI and cybersecurity, along with being on the Biohacking Village advisory board.

SpeakerBio: Nathan Case

A passion for Incident Response, and operational security in all forms. Pushing the bounds of threat detection and response. Finding new thoughts and bringing them to the fields of security and technology.

Description:

Medical Records, Procurement, and Manufacturing have always been a major part of the biomedical, pharmaceutical, and laboratory technology industry and critical infrastructure. As we edge closer to the regulatory timelines, we need to look at the current landscape and its issues. If you enjoy thrillers, data, crime, and international espionage, Welcome to the 'Choose your own adventure: Healthcare and the International Syndicate of Turbulence' or 'Septic Homeostasis'.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Tag, You're Exposed: Exploring Azure Service Tags and their Impact on your Security Boundary

When: Sunday, Aug 13, 10:40 - 11:20 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

Speakers: Aled Mehta, Christian Philipov

SpeakerBio: Aled Mehta

Aled is security consultant in the cloud security team at WithSecure. He spends the majority of his time exploring Microsoft Cloud services focussing on identifying new attack paths, or new ways of performing well established attacks. Outside of this exploration, he is motivated by sharing knowledge and skills with his colleagues and with the wider community.

Twitter: [@x_delfino](#)

SpeakerBio: Christian Philipov , Senior Security Consultant at WithSecure

Chris is a senior security consultant in the cloud security team at WithSecure. Loves looking into the unique ways that Microsoft Azure and Google Cloud Platform (GCP) works as well as helping out his fellow colleagues with all their various cloud technical issues. Chris has previously presented at fwd:cloudsec as well as BlueTeamCon, and holds multiple Microsoft certificates with the latest one being Microsoft Cybersecurity Architect.

Twitter: [@chrispy_sec](#)

Description:

Within Cloud environments, the approach to securing networks and resources has shifted. An organisation's security perimeter has become blurred, with resources increasingly exposed, making it harder to clearly establish their attack surface.

Components of network and security controls have been abstracted away, including the specific on how they are implemented. One of these abstractions is through Azure Service Tags, a feature that we frequently see being used, and one that often results in resources being more exposed than intended.

In this talk, we will explore Service Tags in Azure, a common method for modern organisations to use pre-defined network ranges to be allow-listed for inbound and outbound network traffic. Although a useful means to simplify configuration to allow service-to-service communication, its usage can lead to unintentional cross-tenant access to Azure resources. The aim of the talk is to highlight several novel methods by which attackers can get access to a corporate environment. These will range from:

- Accessing internal resources via an attacker controlled VM in a different tenant
- Abusing Azure Logic Apps functionality to interact with internal APIs
- Using SaaS services such as Azure DevOps to modify pipelines within a misconfigured target organisation

Fundamentally, this is the service working as intended. Service Tags are *supposed* to cover Azure service network ranges and these *do*, by design, include other organisations' environments. The issue mostly lies in the lack of detailed documentation and the lack of awareness around the breadth of coverage, and the potential impact of these controls. Where documentation is available that highlights some of these components, it is inconsistent in outlining the risks and potential impact. Through our work at a consultancy, we have worked with a range of organisations from large enterprises to medium sized companies. Based on our observations, this is a common issue that is present in different production Azure environments.

Listeners of the talk will come out with an understanding of:

- Service Tags and their use cases
- Attack methods to take advantage of Service Tags
- Practical recommendations for Service Tag usage

Title: Taking Down Applications with Logic: A Comprehensive Guide to Modern DOS Attacks

When: Saturday, Aug 12, 11:35 - 12:20 PDT

Where: Virtual

SpeakerBio: Abhijeet Singh

Abhijeet Singh is a cybersecurity expert with a passion for securing digital assets and currently working in a start-up "Cultfit". Abhijeet specializes in vulnerability assessment and penetration testing of various applications, network and cloud security, and enjoys automating security tasks.

Twitter: [@abhiunix](#)

Description:

It will be a comprehensive guide that explores the various types of Denial of Service (DOS) attacks and the latest techniques used to attack applications which can evade the Firewall. Abhijeet will cover the concept of logical attacks, which are a new type of DOS attack that exploits vulnerabilities in an application's logic, making them increasingly difficult to detect.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Tales from a detection engineering in AWSland

When: Sunday, Aug 13, 12:00 - 12:40 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Rodrigo Montoro , Head of Threat & Detection Research at Clavis Security

Rodrigo Montoro has over 23 years of experience in Information Technology and Computer Security. For most of his career, he has worked with open-source security software (firewalls, IDS, IPS, HIDS, log management, endpoint monitoring), incident detection & response, and Cloud Security. Currently is Head of Threat & Detection Research at Clavis Security. Before that, he worked as Cloud Researcher at Tenchi Security, Head of Research and Development at Apura Cyber Intelligence, SOC/Researcher at Tempest Security, Senior Security Administrator at Sucuri, and Researcher at Spiderlabs. Author of 2 patented technologies involving innovation in the detection field. One is related to discovering malicious digital documents. The second one is in how to analyze malicious HTTP traffic. Rodrigo has spoken at several open source and security conferences (Defcon Cloud Village, OWASP AppSec, SANS (DFIR, SIEM Summit & CloudSecNext), Toorcon (USA), H2HC (São Paulo and Mexico), SecTor (Canada), CNASI, SOURCE, ZonCon (Amazon Internal Conference), Blackhat Brazil, BSides (Las Vegas e SP)).

Twitter: [@spookerlabs](#)

Description:

Cloud providers' ecosystems have brought a lot of new challenges to the Security Operations Center (SOC). We now have a lot of attack vectors that create known and still unknown attack vectors, generating a considerable need for further research and detection in this field.

Specifically, in AWS, we are talking about more than three hundred (300+) services that an attacker could have their specific attack path to achieve their goal. Considering that chaotic scenario and leading a Detection Engineering Team that monitors hundreds of customers, we developed new and innovative ways to improve customer detection in three paths:

First, the largest market for cloud security is associated with Cloud Security Posture Management (CSPM), a tool that monitors misconfigurations in cloud accounts. We converted the top 10 results based on the CSPM vendor's statistics reports. The findings are prioritized from informational to critical, helping to fix the misconfiguration and making the attacker path more difficult.

Second, we examined the standard tools' behavior and built detections based on those. In particular, PACU (comprehensive AWS security-testing toolkit designed for offensive security practitioners), Endgame, and Cloudfox. The main goal is to have tool-agnostic detections using a combination of them to better fit into the AWS scenario.

Third, and just as important, are uncommon paths that abuse services that are not commonly used or have enough research on it but could lead to data exfiltration, resource exposure, privilege escalation, and so on.

By the end of this talk, attendees will be able to acquire new detection ideas, improve their cloud security posture, and mitigate attack surfaces.

[Return to Index](#) - Add to  - ics [Calendar](#) file

TEV - Saturday - 10:00-17:59 PDT

Title: Tamper Evident Village Activities

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: LINQ - 5th Floor / BLOQ - Tamper Evident Village - [Map](#)

Description:

"Tamper-evident" refers to a physical security technology that provides evidence of tampering (access, damage, repair, or replacement) to determine authenticity or integrity of a container or object(s). In practical terms, this can be a piece of tape that closes an envelope, a plastic detainer that secures a hasp, or an ink used to identify a legitimate document. The goal of the Tamper Evident Village is to teach attendees how these technologies work and how many can be tampered with without leaving evidence. The village includes hands-on areas for mechanical seals, cargo seals, adhesive seals, mail and shipping seals, as well as a collection of demos, contests, and events to participate in.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Tamper Evident Village Activities

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: LINQ - 5th Floor / BLOQ - Tamper Evident Village - [Map](#)

Description:

"Tamper-evident" refers to a physical security technology that provides evidence of tampering (access, damage, repair, or replacement) to determine authenticity or integrity of a container or object(s). In practical terms, this can be a piece of tape that closes an envelope, a plastic detainer that secures a hasp, or an ink used to identify a legitimate document. The goal of the Tamper Evident Village is to teach attendees how these technologies work and how many can be tampered with without leaving evidence. The village includes hands-on areas for mechanical seals, cargo seals, adhesive seals, mail and shipping seals, as well as a collection of demos, contests, and events to participate in.

[Return to Index](#) - Add to  - ics [Calendar](#) file

TEV - Friday - 10:00-17:59 PDT

Title: Tamper Evident Village Activities

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: LINQ - 5th Floor / BLOQ - Tamper Evident Village - [Map](#)

Description:

"Tamper-evident" refers to a physical security technology that provides evidence of tampering (access, damage, repair, or replacement) to determine authenticity or integrity of a container or object(s). In practical terms, this can be a piece of tape that closes an envelope, a plastic detainer that secures a hasp, or an ink used to identify a legitimate document. The goal of the Tamper Evident Village is to teach attendees how these technologies work and how many can be tampered with without leaving evidence. The village includes hands-on areas for mechanical seals, cargo seals, adhesive seals, mail and shipping seals, as well as a collection of demos, contests, and events to participate in.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MIV - Friday - 10:30-10:59 PDT

Title: Teaching Information Warfare: Strategies in Academic and Government Institutions

When: Friday, Aug 11, 10:30 - 10:59 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio:Greg Carpenter

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: TeleChallenge

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The TeleChallenge is a fast-paced, fully immersive, and epic battle of wits and skill. The highest level of commitment is required, and this is one of the hardest contests in the world to win, but you don't need any special technical skills to play: just a touch-tone phone. And remember: the best way to ascend into the Phoniverse is to get others involved in the TeleChallenge opportunity, so bring a team!

--

Rated PG-13. It's a level of challenge that is probably most suited to high school students and up, but anyone can play and we try to make it fun even if you're not competitive to win. :)

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

Title: TeleChallenge

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The TeleChallenge is a fast-paced, fully immersive, and epic battle of wits and skill. The highest level of commitment is required, and this is one of the hardest contests in the world to win, but you don't need any special technical skills to play: just a touch-tone phone. And remember: the best way to ascend into the Phoniverse is to get others involved in the TeleChallenge opportunity, so bring a team!

--

Rated PG-13. It's a level of challenge that is probably most suited to high school students and up, but anyone can play and we try to make it fun even if you're not competitive to win. :)

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT

Title: TeleChallenge

When: Sunday, Aug 13, 10:00 - 11:59 PDT


Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The TeleChallenge is a fast-paced, fully immersive, and epic battle of wits and skill. The highest level of commitment is required, and this is one of the hardest contests in the world to win, but you don't need any special technical skills to play: just a touch-tone phone. And remember: the best way to ascend into the Phoniverse is to get others involved in the TeleChallenge opportunity, so bring a team!

--

Rated PG-13. It's a level of challenge that is probably most suited to high school students and up, but anyone can play and we try to make it fun even if you're not competitive to win. :)

[Return to Index](#) - Add to  - ics [Calendar](#) file

TCV - Sunday - 11:00-12:59 PDT

Title: Telecom Village CTF

When: Sunday, Aug 13, 11:00 - 12:59 PDT

Where: Flamingo - Virginia City - Telecom Village - [Map](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

TCV - Friday - 10:00-10:59 PDT

Title: Telecom Village Inauguration

When: Friday, Aug 11, 10:00 - 10:59 PDT

Where: Flamingo - Virginia City - Telecom Village - [Map](#)

SpeakerBio:Harshit Mahajan , Event Head at NullCon
No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Saturday - 11:00-11:59 PDT

Title: Ten Years of CPV - Program Committees

When: Saturday, Aug 12, 11:00 - 11:59 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

Speakers:CPV Program Committees,CPV Staff


SpeakerBio:CPV Program Committees

No BIO available

SpeakerBio:CPV Staff

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

CPV - Saturday - 12:00-12:59 PDT

Title: Ten Years of CPV - The Gold Bug Challenge

When: Saturday, Aug 12, 12:00 - 12:59 PDT

Where: Flamingo - Sunset - Vista - Crypto & Privacy Village - [Map](#)

Speakers:CPV Staff,Gold Bug Challenge Team

SpeakerBio:CPV Staff

No BIO available

SpeakerBio:Gold Bug Challenge Team

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Terminally Owned - 60 years of escaping

When: Sunday, Aug 13, 12:00 - 12:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio: David Leadbeater, Open Source Engineer at G-Research

He aims to find more CVEs than he creates and is currently succeeding.

Twitter: [@davidgl](#)

Description:

It is 60 years since the first publication of the ASCII standard, something we now very much take for granted. ASCII introduced the Escape character; something we still use but maybe don't think about very much. The terminal is a tool all of us use. It's a way to interact with nearly every modern operating system. Underneath it uses escape codes defined in standards, some of which date back to the 1970s.

Like anything which deals with untrusted user input, it has an attack surface. 20 years ago HD Moore wrote a paper on terminal vulnerabilities, finding multiple CVEs in the process. I decided it was time to revisit this class of vulnerability.

In this talk I'll look at the history of terminals and then detail the issues I found in half a dozen different terminals. Even Microsoft who historically haven't had strong terminal support didn't escape a CVE. In order to exploit these vulnerabilities they often need to be combined with a vulnerability in something else. I'll cover how to exploit these vulnerabilities in multiple ways.

Overall this research found multiple remote code execution vulnerabilities across nearly all platforms and new unique ways to deliver the exploits.

REFERENCES:

Key citations:

- HD Moore, 2003, "Terminal Emulator Security Issues"; <https://marc.info/?l=bugtraq&m=104612710031920&w=2>
- Eviatar Gerzi, 2022; "Don't Trust This Title: Abusing Terminal Emulators with ANSI Escape Characters"

<https://www.cyberark.com/resources/threat-research-blog/dont-trust-this-title-abusing-terminal-emulators-with-ansi-escape>

- Phrack, 1994, #46 file 4 "Line Noise" - flash.c; <http://phrack.org/issues/46/4.html>
- Mitre; CWE-150; <https://cwe.mitre.org/data/definitions/150.html>
- Paul Szabo, 2008, CVE-2008-2383; <https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=510030>

Other interesting sources:

- Nicholas Boucher and Ross Anderson, 2021, "Trojan Source: Invisible Vulnerabilities"; <https://trojansource.codes/>
- Thomas Dickey, 2023, "XTerm Control Sequences"; <https://invisible-island.net/xterm/ctlseqs/ctlseqs.html>
- Bob Bemer, "That Powerful ESCAPE Character", <https://web.archive.org/web/20010411103243/http://www.bobbemer.com/ESCAPE.HTM>
- Lear Siegler, 1979, "ADM-3A Operator's Manual"; <https://vt100.net/lsi/adm3a-om.pdf>
- Digital Equipment Corporation, 1994, "VT520/VT525 Video Terminal Programmer Information"; <http://web.mit.edu/dosathena/doc/www/ek-vt520-rm.pdf>
- Paul Flo Williams, "A parser for DEC's ANSI-compatible video terminals." VT100.net; https://vt100.net/emu/dec_ansi_parser
- Konstantinos Foutzopoulos, 2021, "Sixel for terminal graphics"; <https://konfou.xyz/posts/sixel-for-terminal-graphics/>
- <https://agimcami.files.wordpress.com/2019/07/control-characters-in-ascii-and-unicode-aivisto-com.pdf>, unknown origin, but good references
- Unicode Consortium, Mark Davis et al., 2014; Unicode Technical Report #36; <https://unicode.org/reports/tr36/>

- Unicode Consortium, Robin Leroy, et al., 2023; Draft Unicode Technical Standard #55; <https://www.unicode.org/reports/tr55/>

My posts to oss-security so far:

- rxvt-unicode CVE-2022-4170; <https://www.openwall.com/lists/oss-security/2022/12/05/1>
- xterm CVE-2022-45063; <https://www.openwall.com/lists/oss-security/2022/11/10/1>
- less CVE-2022-46663; <https://www.openwall.com/lists/oss-security/2023/02/07/7>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: TETRA tour de force: Jailbreaking digital radios and base stations for fun and secrets

When: Sunday, Aug 13, 14:00 - 15:15 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

Speakers: Carlo Meijer, Jos Wetzels, Wouter Bokslag

SpeakerBio: Carlo Meijer, Founding Partner and Security Researcher at Midnight Blue

Carlo Meijer is a co-founding partner and security researcher at Midnight Blue. His research focuses on the analysis of cryptographic systems deployed in the wild. He is known for his work on the security of so-called Self-Encrypting Drives (SEDs). Furthermore, he is known for breaking a hardened variant of Crypto1, the cipher used in the Mifare Classic family of cryptographic RFID tags. Finally, he co-authored research into default passwords in consumer routers as deployed by ISPs in the Netherlands. He is a PhD researcher and systems security lecturer at the Radboud University (RU) in the Netherlands.

SpeakerBio: Jos Wetzels, Founding Partner and Security Researcher at Midnight Blue

Jos Wetzels is a co-founding partner and security researcher at Midnight Blue. His research has involved reverse-engineering, vulnerability research and exploit development across various domains ranging from industrial and automotive systems to IoT, networking equipment and deeply embedded SoCs. He has uncovered critical zero-day vulnerabilities in dozens of embedded TCP/IP stacks, Industrial Control Systems (ICS), and RTOSes.

He previously worked as a researcher at the Distributed and Embedded Security group (DIES) at the University of Twente (UT) in the Netherlands where he developed exploit mitigation solutions for constrained embedded devices deployed in critical infrastructure, performed security analyses of state-of-the-art network and host-based intrusion detection systems and has been involved in research projects regarding on-the-fly detection and containment of unknown malware and APTs.

Twitter: [@s4mvertaka](#)

SpeakerBio: Wouter Bokslag, Founding Partner and Security Researcher at Midnight Blue

Wouter Bokslag is a co-founding partner and security researcher at Midnight Blue. He is known for the reverse-engineering and cryptanalysis of several proprietary in-vehicle immobilizer authentication ciphers used by major automotive manufacturers as well as co-developing the world's fastest public attack against the Hitag2 cipher. He holds a Master's Degree in Computer Science & Engineering from Eindhoven University of Technology (TU/e) and designed and assisted teaching hands-on offensive security classes for graduate students at the Dutch Kerckhoffs Institute for several years.

Description:

In this talk we will discuss the radio jailbreaking journey that enabled us to perform the first public disclosure and analysis of the proprietary cryptography used in TETRA (Terrestrial Trunked Radio): a standard used globally by government agencies, police, prisons, and military operators as well as critical infrastructure such as SCADA telecontrol of oil rigs, pipelines, transportation and electric and water utilities.

For decades, the underlying algorithms have remained secret under restrictive NDAs prohibiting public scrutiny of this critical technology. In this talk, we will make public the TETRA cipher suites (TEA and TAA1 to be precise), one of the last bastions of widely deployed secret crypto, and discuss in-depth how we managed to obtain them.

We will discuss several different flaws we uncovered allowing passive or active adversaries to intercept and manipulate TETRA traffic, including details of a backdoored stream cipher.

This journey involved reverse-engineering and exploiting multiple 0-day vulnerabilities in the popular Motorola MTM5x00 radio and its TI OMAP-L138 TEE and covers everything from side-channel attacks on DSPs to writing your own decompilers. We will also discuss how we gained code execution on and instrumented a Motorola MBTS TETRA base station for research purposes.

REFERENCES:

- Daniel J Bernstein. Cache-timing attacks on AES. 2005.
 - Shuwen Duan. Security analysis of TETRA. Master's thesis, Instituttt for telematikk, 2013.
 - Jonas Olofsson. Design and implementation of SIM functionality for TETRA-system on a smart card, 2012.
 - Yong-Seok Park, Choon-Soo Kim, and Jae-Cheol Ryou. The vulnerability analysis and improvement of the TETRA authentication protocol. 2010
 - Martin Pfeiffer, Jan-Pascal Kwirotek, Jiska Classen, Robin Klose, and Matthias Hollick. Analyzing TETRA location privacy and network availability. 2016
 - Marek Sebera Tomáš Suchan. TETRA networks security, 2015.
 - Zhi-Hui Zhang and Yi-Xian Yang. Research on end-to-end encryption of TETRA. 2006
 - Müller, Uwe ; Hauck, Eicke ; Welz, Timm ; Classen, Jiska ; Hollick, Matthias. Dinosaur Resurrection: PowerPC Binary Patching for Base Station Analysis. 2021
-

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The "Why" of Lock Picking

When: Friday, Aug 11, 12:00 - 12:20 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

SpeakerBio: Christopher Forte

Christopher Forte is a security researcher and a junky for learning, participating in CTFs, and solving challenges. He is curious, loves teaching others, and has a passion for breaking things. As a resident of Las Vegas, Christopher co-founded DC702, is the local Chapter President of TOOOL, and enjoys introducing people to the world of hacking and lock picking.

Description:

"Why would you possibly need to know how to do that?" and "Couldn't you just break the lock?" are two of the more common questions I get when discussing lock picking or various bypasses. At first glance, many see lock picking as a nefarious and largely unnecessary hobby. But, whether you are a locksport enthusiast, security researcher, emergency responder, or just someone who enjoys puzzles, lock picking can be a constructive—and useful—skill to learn. This talk aims to show how diverse the community is, explore some of the many reasons we engage in this hobby, and try to give some answers as to why we practice lock picking.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Art of Compromising C2 Servers: A Web Application Vulnerabilities Perspective

When: Sunday, Aug 13, 11:00 - 11:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio: Vangelis Stykas , CTO at Tremau

Vangelis is a software developer, penetration tester, and PhD candidate. He applies his skills at his job as Chief Technology Officer at Tremau and his research focus revolves around API and web application security. His academic research is focused on machine learning in web application security and the development of proactive web application security. During his free time, Vangelis is helping start-ups secure themselves on the Internet and get a leg up in security terms. During the past years he has published and presented research regarding API control functions for ships, smart locks, IP cameras, EV chargers and many other IoT devices. He has performed extensive research on the stakerware industry.

Twitter: [@@evstykas](#)

Description:

C2 servers of mobile and Windows malware are usually left to their own fate after they have been discovered and the malware is no longer effective. We are going to take a deep dive into the rabbit hole of attacking and owning C2 servers, exposing details about their infrastructure, code bases, and the identity of the companies and individuals that operate and profit from them.

While understanding and reversing malware is a highly skilled procedure, attacking the C2 itself rarely requires a lot of technical skills. Most of the C2 servers have the same typical HTTP problems that can be detected by off-the-shelf vulnerability scanners.

By exploiting low-hanging fruit vulnerabilities, an attacker can obtain unauthorized access to administrative functions, allowing them to command thousands of devices and further explore other attack vectors. This can give them access to administrator panels and malware source code, and result in the identity of threat actors being exposed.

REFERENCES

Harly malware: <https://www.kaspersky.com/blog/harly-trojan-subscriber/45573/> Clipper malware:

<https://www.welivesecurity.com/2023/03/16/not-so-private-messaging-trojanized-whatsapp-telegram-cryptocurrency-wallets/>

Nexus malware: <https://www.techrepublic.com/article/nexus-android-malware-finance-targets/> Aurora malware:

<https://www.bleepingcomputer.com/news/security/aurora-infostealer-malware-increasingly-adopted-by-cybergangs/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The attackers guide to exploiting secrets in the universe

When: Friday, Aug 11, 11:45 - 12:30 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

SpeakerBio: Mackenzie Jackson

Mackenzie is a developer and security advocate with a passion for code security. As the co-founder and former CTO of Conpago he learnt first-hand how critical it is to build secure applications and today is able to continue that passion at GitGuardian

Twitter: [@advocatemack](#)

Description:

Exposed secrets like API keys and other credentials continue to be a persistent vulnerability. This presentation sheds light on the methods used to discover and exploit such secrets in various environments, including public and private git repositories, containers, and compiled mobile applications. This presentation combines various different research projects that illustrates the different methods attackers use to find and exploit secrets to gain initial access, elevate privileges and created persisted access. It covers research into exploiting secrets in git repositories, private and public, exploiting secrets in compiled mobile applications and exploiting secrets in packages and containers.

This presentation offers valuable insights and information on how to identify and address exposed secrets, one of the most persistent vulnerabilities in application security.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-13:59 PDT

Title: The Beverage Cooling Contraption Contest

When: Friday, Aug 11, 10:00 - 13:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

I don't know my gender non-specific guys. It's not funny anymore. We can't stop talking about a cheeto for paying hush money to a busty tortilla chip. Winny Pooh is presatator for life with a hunger for those sweet sweet chips. Off brand doctor evil is threatening to nuke the world on the weekly. And in the plot twist of the year BiBi is going fascist. I keep expecting ol'e Joe to bust out the force lightning and tell me to "give in to my hate". WELL TOO LATE! This year we are going to have a change of pace. I'm going to drink all the beverage! Lord knows I could use it. I'm kidding of course, I'm terribly allergic to hops. It's the greatest irony of all, I can't drink any of the beverage. But our spectators can! And they want that beverage to be COLD! So I need you to help me satisfy their thirst. Their thirst for escape from this mad world.

--

We have soda for under 21 participants.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Sunday - 10:00-13:59 PDT

Title: The Challenge - Lockheed Martin

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

The Challenge

Lockheed Martin

****Laptop Needed****

This is your chance to demonstrate your superior aviation hacking knowledge and skills. This contest requires you to keep your eyes open in the Aerospace Village, a personal device to access the contest webpage, and various other technical skills that are useful in the Aerospace industry. A laptop will be helpful for binary analysis and packet decoding. The final flag is an RF replay attack, so you will need to bring or borrow a device capable of rebroadcasting a signal. If you get stuck on any the challenges help can likely be found in some of the other villages. No pre-registration is required and it is OK to work in teams. The first to finish will receive a 1/48 scale model of an F-35B as well as the prestige of being the first ever winner of this challenging contest. A second model will be awarded based on a random drawing of all other people who successfully solve the final flag. The Aerospace Village CTF starts when the village opens on Friday and ends when the village closes Sunday at 2.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Saturday - 10:00-17:59 PDT

Title: The Challenge - Lockheed Martin

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

The Challenge

Lockheed Martin

****Laptop Needed****

This is your chance to demonstrate your superior aviation hacking knowledge and skills. This contest requires you to keep your eyes open in the Aerospace Village, a personal device to access the contest webpage, and various other technical skills that are useful in the Aerospace industry. A laptop will be helpful for binary analysis and packet decoding. The final flag is an RF replay attack, so you will need to bring or borrow a device capable of rebroadcasting a signal. If you get stuck on any the challenges help can likely be found in some of the other villages. No pre-registration is required and it is OK to work in teams. The first to finish will receive a 1/48 scale model of an F-35B as well as the prestige of being the first ever winner of this challenging contest. A second model will be awarded based on a random drawing of all other people who successfully solve the final flag. The Aerospace Village CTF starts when the village opens on Friday and ends when the village closes Sunday at 2.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Friday - 10:00-17:59 PDT

Title: The Challenge - Lockheed Martin

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

The Challenge

Lockheed Martin

****Laptop Needed****

This is your chance to demonstrate your superior aviation hacking knowledge and skills. This contest requires you to keep your eyes open in the Aerospace Village, a personal device to access the contest webpage, and various other technical skills that are useful in the Aerospace industry. A laptop will be helpful for binary analysis and packet decoding. The final flag is an RF replay attack, so you will need to bring or borrow a device capable of rebroadcasting a signal. If you get stuck on any the challenges help can likely be found in some of the other villages. No pre-registration is required and it is OK to work in teams. The first to finish will receive a 1/48 scale model of an F-35B as well as the prestige of being the first ever winner of this challenging contest. A second model will be awarded based on a random drawing of all other people who successfully solve the final flag. The Aerospace Village CTF starts when the village opens on Friday and ends when the village closes Sunday at 2.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Coming War on Encryption, Part 3 (and how you can fight back)

When: Saturday, Aug 12, 12:00 - 12:50 PDT

Where: Caesars Forum - Summit - 221-222 - Policy Atrium - [Map](#)

SpeakerBio: India McKinney , Director of Federal Affairs at Electronic Frontier Foundation

As a former Capitol Hill staffer and a current EFF lobbyist, India's main job is to make sure that the laws of the land don't suck the life out of the internet. India's passion has always been for good public policy, and she's excited to be using skills developed during past legislative battles to fight for encryption, for consumer privacy, and civil liberties in the digital realm.

Twitter: [@imck82](#)

Description:

In recent years, lawmakers around the world have proposed legislation aimed at ending encryption, under the guise of ending child exploitation. In the first half of 2023, we have already seen two serious legislative proposals in the Senate that would result in potentially disastrous legal risks for any company that provides encrypted messages.

Come join us to get an update about the government's efforts to break encryption – again. We'll talk about what is different from the last Encryption Wars, what the conversation sounds like right now in DC*, and we've been doing to fight back. Most important, we'll talk about what technologists can do to protect encryption and everyone who uses it.

*when you read this, EARN IT and the STOP CSAM Act, both bills designed to break encryption, will have been marked up and passed out of the Senate Judiciary Committee. What happens after that is entirely dependent on many factors outside my control. The FBI is super gearing up to double down on their position, though.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Creation Of The Out-Of-Band Anti Virus Dock (Oobavd)

When: Friday, Aug 11, 11:00 - 11:20 PDT

Where: Caesars Forum - Alliance - 311-312 - Hardware/Soldering VlgS - [Map](#)

Speakers:Bosen Zhang,Howard Yang,Pengfei “BigZaddy” Yu,Tan Jing Zhi

SpeakerBio:Bosen Zhang

Bosen loves breaking things, he lives by his mantra: “Just Nuke It”.

SpeakerBio:Howard Yang

Howard is the data science-wiz, we asked him for one good model, and he gave us five.

SpeakerBio:Pengfei “BigZaddy” Yu

Pengfei is a professional cyber firefighter, always jumping from fire to fire.

SpeakerBio:Tan Jing Zhi

Jing Zhi is slenderman, the hardware padawan.

Description:

USB-based attacks account for over 52% of all cybersecurity attacks on operational technology (OT) systems in the industrial control systems (ICS) industry. Stuxnet’s discovery in 2015 showed the vulnerability of air-gapped systems, previously considered invulnerable. These systems are found in secure military organizations and SCADA systems. The societal impact of such attacks can be enormous, as evidenced by Stuxnet’s impact on Iran’s nuclear programs.

Air-gapped systems, while considered secure, mostly require mobile storage devices like USB sticks for updates and data transfers, exposing them to malware. Adding peripherals like keyboards and mice will also render the systems vulnerable to BadUSB attacks. This all can be prevented by OOBAVD, which acts as an intermediary between air-gapped systems and USB devices, blocks malicious files from entering the air-gapped systems. OOBAVD being out of band also mitigates the risk of malware attacking the host’s antivirus software.

So what exactly is OOBAVD and how does one take an anti-virus out of band?

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Curse of Ncurses

When: Saturday, Aug 12, 12:35 - 13:20 PDT

Where: Virtual

SpeakerBio:Jonathan Bar Or , Security Researcher at Microsoft

Jonathan Bar Or ("JBO") is a Principal Security Researcher at Microsoft, working as the Microsoft Defender research architect for cross-platform. Jonathan has rich experience in vulnerability research, exploitation, cryptanalysis, and offensive security in general.

Twitter: [@yo_yo_yo_jbo](https://twitter.com/yo_yo_yo_jbo)

Description:

Terminals are ancient and dangerous beasts. While performing a routine code auditing, our team has discovered several vulnerabilities in ncurses, present on multiple operating systems. In this talk we will discuss those vulnerabilities and the dangers they pose, as well as discuss oss security in general.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Dark Playground of CI/CD: Attack Delivery by GitHub Actions

When: Friday, Aug 11, 11:30 - 12:10 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

Speakers: Kiyohito Yamamoto, Yusuke Kubo

SpeakerBio: Kiyohito Yamamoto, Security Engineer at NTT Communications

Kiyohito Yamamoto works as a Security Engineer at NTT Communications, Japanese Telecommunication Company, and is also NTT Group Certified Security Principal. He served as a Senior Response Expert during the Tokyo Olympics and also conducted TLPT tests.

SpeakerBio: Yusuke Kubo, Offensive Security Researcher at NTT Communications

Yusuke Kubo works as an Offensive Security Researcher at NTT Communications, Japanese Telecommunication Company, and is also NTT Group Certified Security Principal. His responsibilities include researching attack techniques and providing RedTeam for internal. And he contributed to MITRE ATT&CK regarding Safe Mode Boot(T1562.009).

Description:

GitHub, a software development platform, has become popular in recent years and as of March 2023 and according to GitHub, Inc., is being used by 100 million users worldwide. As the service used by developers around the world, security related to the service becomes a global research topic. Most of the security topic for GitHub are about information leakage such as source code and APIKEY, which is related to the main function of GitHub service. On the other hand, we focused on the potential for attacks using GitHub Actions, a CICD feature provided by GitHub.

Our research includes both known attack techniques already used by attackers and unknown attacks not yet observed in the wild. The following is a description of the five attacks introduced in this presentation.

- Malicious Custom Action - Two attack techniques are going to be introduced in this section: Malicious JScript Composite Action and Malicious JavaScript Custom Action. Malicious JScript Composite Action is a developed custom action that performs an attack using JScript, after replacing the script engine from node.exe to wscript.exe through Binary Hijacking and Masquerading. Malicious JavaScript Custom Action performs the attack from Nodejs implemented using its C++ addons.
- GitHub Actions C2 - We will demonstrate a new C2 framework using self-hosted runner in GitHub Actions. This C2 has been developed using Runner Application, a GitHub Action's agent, to execute commands and download/upload files via GitHub Actions. The C2 achieves stealthiness by utilizing official binaries provided by GitHub and communicating only with GitHub owned domains and IPs.
- Free Jacking - We will introduce the results of my investigation into attacks using free cloud resources, known as "Free Jacking," including the attack actually used by attackers and its changes according to GitHub's countermeasures.
- Public Malicious Fork and PR - We will briefly discuss an Initial Foothold being established through repository configuration or developer operation errors when using self-hosted runners.
- Theft of Secret - We will also provide an overview of the threat of theft of secrets, where encrypted environment variables used within GitHub are stolen from GitHub Actions, based on discussions among researchers.

Finally, we have systematized the above five attacks based on two perspectives: - GitHub Actions features, such as repository ownership and runner types. - Threat level, including severity and probability. Each attack is shown with its use cases, as well as the potential damages that could occur if it were executed.

The attack we demonstrate in this presentation could potentially be widely used in other CI/CD services. By discovering threats in CI/CD, we hope to enhance the overall security of these services.

Title: The Dark Playground of CI/CD: Attack Delivery by GitHub Actions

When: Friday, Aug 11, 13:15 - 13:59 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

Speakers: Kiyohito Yamamoto, Yusuke Kubo

SpeakerBio: Kiyohito Yamamoto, Security Engineer at NTT Communications

Kiyohito Yamamoto works as a Security Engineer at NTT Communications, Japanese Telecommunication Company, and is also NTT Group Certified Security Principal. He served as a Senior Response Expert during the Tokyo Olympics and also conducted TLPT tests.

SpeakerBio: Yusuke Kubo, Offensive Security Researcher at NTT Communications

Yusuke Kubo works as an Offensive Security Researcher at NTT Communications, Japanese Telecommunication Company, and is also NTT Group Certified Security Principal. His responsibilities include researching attack techniques and providing RedTeam for internal. And he contributed to MITRE ATT&CK regarding Safe Mode Boot(T1562.009).

Description:

We are investigating new attack vectors regarding a CICD service called Github Actions. Through an analysis of Github Actions behavior on Windows, our research has discovered two attack techniques

Malicious Custom Action

It is an attack technique to execute arbitrary TTPs from custom actions. Introduce two types, “Malicious JScript Composite Action” and “Malicious JavaScript Custom Action”.

GitHub Actions C2

We will demonstrate a new C2 framework using self-hosted runner in GitHub Actions

In this presentation, we will provide a detailed explanation of these attack techniques, along with PoC code and demonstrations. We will also discuss real-world threats and provide insight on detection and mitigation strategies.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT


Title: The Dark Tangent Look-Alike Contest

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The Dark Tangent Look A-like Contest is a creative opportunity for DEF CON attendees to put their non-technical hacking skills to the test. As a contestant in The Dark Tangent Look A-like Contest, you will be judged based on your appearance, mannerisms, efforts, and overall persuasiveness. Can you assume another identity? Can you look, walk, talk, and act like Dark Tangent? Can you become THE DARK TANGENT?

[Return to Index](#) - Add to  - ics [Calendar](#) file


Title: The Dark Tangent Look-Alike Contest

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The Dark Tangent Look A-like Contest is a creative opportunity for DEF CON attendees to put their non-technical hacking skills to the test. As a contestant in The Dark Tangent Look A-like Contest, you will be judged based on your appearance, mannerisms, efforts, and overall persuasiveness. Can you assume another identity? Can you look, walk, talk, and act like Dark Tangent? Can you become THE DARK TANGENT?

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT


Title: The Dark Tangent Look-Alike Contest

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The Dark Tangent Look A-like Contest is a creative opportunity for DEF CON attendees to put their non-technical hacking skills to the test. As a contestant in The Dark Tangent Look A-like Contest, you will be judged based on your appearance, mannerisms, efforts, and overall persuasiveness. Can you assume another identity? Can you look, walk, talk, and act like Dark Tangent? Can you become THE DARK TANGENT?

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Wednesday - 00:00-09:59 PDT

Title: The DEFCON31 Multi User Dungeon Adventure (DEFCON MUD) Internet Edition

When: Wednesday, Aug 9, 00:00 - 09:59 PDT

Where: Virtual

Description:

The DEFCON MUD is available now for those who would like to play remotely. New characters created will be eligible to enter, however only DUMB Terminals in the DEFCON contest area may actually score points. For details go to <https://evil.af/>

START: Monday August 5th 2023 @ 0001

END: Sunday August 13th 2023 @ 1000

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Fallacy Of Privacy

When: Friday, Aug 11, 13:30 - 14:20 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio: Antigone Peyton

Antigone is the Director of Legal and Policy at Ridgeline International, Inc. a technology integration company. She also provides privacy, Intellectual Property, and technology law counseling through her boutique law firm, Cloudigy Law. Antigone is a registered patent attorney with over 20 years of legal experience, focused on the intersection of privacy, cybersecurity, information governance, tech law, policy, and regulation. She regularly speaks about legal and policy implications of the digital economy, including social media, IoT, AI, blockchain, and cloud computing. She has been recognized among the Virginia Legal Elite and WIPR Leaders by her peers and a SuperLawyer for her work involving intellectual property law. Before moving in-house and restarting her boutique firm, Antigone managed the IP and Tech Group at a large Virginia law firm and she managed the e-Discovery group at the international IP firm Finnegan LLP. Antigone has counseled a wide variety of tech-startups and Fortune 500 companies over the years. Before becoming a lawyer, she conducted scientific research at a large university medical center and has supported the National Science Foundation SBIR/STTR seed fund program for over 10 years as a commercial panel reviewer of early development proposals and an awardee conference participant. All of these experiences honed her passion for exploring the intersection of cutting edge science and technology, law, and policy. Having worked for former Chief Administrative Law Judge Paul Luckern at the U.S. International Trade Commission (ITC) and the Honorable Kimberly Moore at the U.S. Court of Appeals for the Federal Circuit, Antigone brings a practical perspective to her litigation and client counseling practice. She received a B.S. in Chemistry from The College of William and Mary, pursued graduate Bioethics and pre-clinical research work at the University of Pennsylvania, and a J.D. in law with an Intellectual Property focus from the Scalia School of Law, George Mason University, where she was the editor-in-chief of the Federal Circuit Bar Journal and a member of the Moot Court.

Twitter: [@antigonepeyton](#)

Description:

Did you know that data analytics vendors, tech companies, political campaigns, PACs, and government agencies know your political leanings, whether you are interested in certain conspiracy theories, follow a hot-button issue, or are having financial trouble? During this talk, you will learn how data siphoned from the Internet, mobile devices, and the IoT webs that surround us are used to analyze and construct your unique digital signature—your travel patterns, interests, relationships, reading behaviors, and other private activities. Under current U.S. laws, foreign actors, political organizations, and private companies can legally access your digital signature, including your voting records. In most states, almost all voter registration information is available for purchase or through a public record request. Some states have additional protections for voter information for certain sensitive groups, including domestic violence victims, judges, law enforcement, and minors. In other states, like Florida, almost all voter information (including party affiliation) is public, by default. Interested actors use that information to influence your political activities, uncover your motivations, and influence your decision to vote, not vote, and how you vote. They do this through targeted digital ads, communications, the news you see in your “feed” on social media platforms, your suggested purchases, and the multimedia you see every day. Your personal interests and demographic information drive what you see in the digital space—each and every day. So how can we manage and protect our digital signature and make more informed decisions in light of these sophisticated influence marketplaces? We can expand the news, comments, and other information we see using tools that are available today and become more aware of why we see the particular information that is served up to us on the Internet. This presentation will close with tips for understanding and managing your digital signature.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Sunday - 11:00-11:30 PDT

Title: The Flaws in Cloud-based ICS Ecosystem

When: Sunday, Aug 13, 11:00 - 11:30 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio: Hank Chen

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The GitHub Actions Worm: Compromising GitHub repositories through the Actions dependency tree

When: Saturday, Aug 12, 13:30 - 14:15 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

SpeakerBio: Asi Greenholts , Security Researcher at Palo Alto Networks

Asi has 8 years of experience in the security field, including security architecture, SOC management, incident response, and application security research. Asi has gained his experience working for major organizations in the financial and government sectors. Today, Asi is a security researcher that focuses on revolutionizing CI/CD security at Palo Alto Networks. During his free time, Asi likes to read, invest in the stock market and to snowboard.

Twitter: [@@TupleType](#)

Description:

GitHub is the most popular platform to host Open Source projects therefore, the popularity of their CI/CD platform - GitHub Actions is rising, which makes it an attractive target for attackers.

In this talk I'll show you how an attacker can take advantage of the Custom GitHub Actions ecosystem by infecting one Action to spread malicious code to other Actions and projects by showing you a demo of POC worm.

We will start by exploring the ways in which Actions are loosely and implicitly dependent on other Actions. This will allow us to create a dependency tree of Actions that starts from a project that we want to attack and hopefully ends in a vulnerable Action that we can take control of.

We will then dive down to how GitHub Actions is working under the hood and I'll show you how an attacker that is in control of an Action can utilize the mechanism of the GitHub Actions Runner to infect other Actions that are dependent on their Action and eventually infect the targeted project.

Finally, after we've gained all of the theoretical knowledge I'll show you a demo with POC malware that is spreading through Actions and we will talk on how to defend against this kind of attack.

REFERENCES

<https://karimrahal.com/2023/01/05/github-actions-leaking-secrets/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT

Title: The Gold Bug Challenge

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Love puzzles? Need a place to exercise your classical and modern cryptography skills? This puzzle will keep you intrigued and busy throughout Defcon - and questioning how deep the layers of cryptography go.

The Gold Bug an annual Defcon puzzle hunt, focused on cryptography. You can learn about Caesar ciphers, brush up your understanding of how Enigma machines or key exchanges work, and try to crack harder modern crypto. Accessible to all - and drop by for some kids' puzzles too!

:#?(8;(: .#6; 6) 5; 3#0†2?3 †#; -(;:##600538 †#; #3

The CPV and Goldbug contest are always kid friendly. We will have "junior cryptographer" puzzle sheet hand outs for kids and those new to the field.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Gold Bug Challenge

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Love puzzles? Need a place to exercise your classical and modern cryptography skills? This puzzle will keep you intrigued and busy throughout Defcon - and questioning how deep the layers of cryptography go.

The Gold Bug an annual Defcon puzzle hunt, focused on cryptography. You can learn about Caesar ciphers, brush up your understanding of how Enigma machines or key exchanges work, and try to crack harder modern crypto. Accessible to all - and drop by for some kids' puzzles too!

:(8;(: .#6; 6) 5; 3#0+2?3 †‡; -(.;‡¶[600538 †‡; ‡(3

The CPV and Goldbug contest are always kid friendly. We will have "junior cryptographer" puzzle sheet hand outs for kids and those new to the field.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: The Gold Bug Challenge

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Love puzzles? Need a place to exercise your classical and modern cryptography skills? This puzzle will keep you intrigued and busy throughout Defcon - and questioning how deep the layers of cryptography go.

The Gold Bug an annual Defcon puzzle hunt, focused on cryptography. You can learn about Caesar ciphers, brush up your understanding of how Enigma machines or key exchanges work, and try to crack harder modern crypto. Accessible to all - and drop by for some kids' puzzles too!

:#?(8;(: .#6; 6) 5; 3#0†2?3 †#; -(.;#¶[600538 †#; #3

The CPV and Goldbug contest are always kid friendly. We will have "junior cryptographer" puzzle sheet hand outs for kids and those new to the field.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Hackers, The Lawyers, And The Defense Fund

When: Friday, Aug 11, 09:00 - 09:45 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

Speakers:Charley Snyder,Hannah Zhao,Harley Geiger,Kurt Opsahl,Miles McCain

SpeakerBio:Charley Snyder , Head of Security Policy at Google

Charley serves as Head of Security Policy at Google. In this role, Charley organizes Google's expertise and technology to help solve the world's pressing public policy challenges related to safety and security online. Before joining Google, he led vulnerability management for a large financial institution, which included responsibility for researcher engagement and bug bounty programs. Previously, Charley served in the United States government, including multiple roles in the Department of Defense, where he helped create and manage the first U.S. government bug bounty program.

Twitter: [@charley_snyder_](#)

SpeakerBio:Hannah Zhao , Staff Attorney at Electronic Frontier Foundation

Hannah is a staff attorney at the Electronic Frontier Foundation. She's part of EFF's Coders' Rights Project, which seeks to protect hackers, security researchers, and others through education, legal defense, amicus briefs, and involvement in the community with the goal of promoting innovation and safeguarding the rights of curious tinkerers and hackers on the digital frontier. She also works on legal issues related to police technology, surveillance, and cybersecurity.

SpeakerBio:Harley Geiger , Counsel at Venable LLP

Harley Geiger is Counsel and Senior Director at Venable, LLP, where he leads the Security Research Legal Defense Fund and the Hacking Policy Council and counsels clients on a variety of cybersecurity issues. Prior to this, Geiger was Senior Director for Public Policy at Rapid7, where he worked to expand adoption of vulnerability disclosure and legal protections for security research. Geiger also worked as Senior Legislative Counsel in the U.S. House of Representatives, where he drafted Aaron's Law, and served as Advocacy Director at the Center for Democracy & Technology.

Twitter: [@HarleyGeiger](#)

SpeakerBio:Kurt Opsahl , Associate General Counsel for Cybersecurity and Civil Liberties Policy at Filecoin Foundation

Kurt Opsahl is the Associate General Counsel for Cybersecurity and Civil Liberties Policy for the Filecoin Foundation, and a Special Counsel to the Electronic Frontier Foundation. Formerly, Opsahl was the Deputy Executive Director and General Counsel of EFF. Opsahl was also the lead attorney on the Coders' Rights Project, and continues to assist EFF with that work as a Special Counsel. In 2007, Opsahl was named as one of the "Attorneys of the Year" by California Lawyer magazine. From 2014 to 2022, Opsahl served on the USENIX Board of Directors. Opsahl is a member of the CISA Cybersecurity Advisory Committee's Technical Advisory Council.

Twitter: [@KurtOpsahl](#)

SpeakerBio:Miles McCain , Student at Stanford University

Miles McCain is a student at Stanford University, security researcher, and open source software developer. He and his friends were once threatened with legal action for responsibly disclosing a security vulnerability in their classmates' startup. He has previously worked on election security at CISA, privacy at Apple, and trust and safety at the Stanford Internet Observatory. Miles is a member of the Recurse Center.

Twitter: [@MilesMcCain](#)

Description:


The hacker community has long conducted important security research that skates the edge of legality. This has led to charges and lawsuits, bogus and serious alike, against hackers. In this panel, we'll hear from a hacker that faced legal challenges, we'll describe what legal counseling for hackers looks like in practice, and we'll discuss a new resource for the hacker community: the Security Research Legal Defense Fund.

Legal issues can arise for good faith hackers because computer or software owners want to prevent security research or vulnerability disclosure. Security researchers have rights and defenses against legal claims, but don't always have access to representation or resources to defend themselves. EFF provides free legal counseling, ideally in advance of security researchers conducting their work so they can steer clear of problematic activity or at least mitigate the risk of legal threats. In litigation, EFF tries to find cases that will advance legal rights for the entire community, but many individuals will need representation even when their particular cases will not have a broader impact. In those cases, EFF endeavors to refer people to cooperating counsel, which can be difficult if funds are not available.

What is it like, as a hacker, to face legal threats? What are the common ways hackers encounter legal threats? When that happens, what should hackers do? What is it really like to provide legal representation to hackers? Are there areas of the world with greater or lesser access to legal rights and representation? What resources can hackers leverage to protect themselves, their rights, and others in the community? Join us and find out!

REFERENCES

- 1) Stanford student vulnerability disclosure, 2021.
- 2) MBTA vs. Anderson, 2008.
- 3) US Department of Justice Computer 2022 Fraud and Abuse Act charging policy.
- 4) Librarian of Congress good faith security research exception to DMCA Section 1201.
- 5) Disclose.io
- 6) SecurityResearchLegalDefenseFund.org

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Human Threat Factor - Cloud Security Misconfigurations

When: Saturday, Aug 12, 14:50 - 15:35 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Kat Fitzgerald

I have to say who I am and why I'm here and my qualifications. I want to explain how/why I do this and how I'm going to make it a fun project for everyone after the talk - with some very specific key takeaways!

Twitter: [@rnbwkat](#)

Description:

Threat modeling the human security risk, or as others might call it, Security Misconfigurations in the cloud and all the fun attack vectors they create. Yep, it's clobberin time and this is what makes this job fun - helping others to find their own security problems before others do!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Impact Of Misinformation On Elections

When: Saturday, Aug 12, 16:30 - 17:30 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

Speakers: Joe Schniebes, Maia Mazurkiewicz, Michael Moore

SpeakerBio: Joe Schniebes

Joe Schniebes is the Chief Strategy Officer and Founder at Ridgeline International, where he has developed a hands-on approach to digital signature management. He helps cross-sector organizations strike the right balance between data privacy and conveniences.

SpeakerBio: Maia Mazurkiewicz

Maia Mazurkiewicz is an expert on countering disinformation and behavioural changes. She has 15 years of experience in political management, foreign affairs, and communication in administration, business and CSOs. She is a speaker, trainer and moderator. She believes that we need to change the way we communicate, to introduce more understanding in between humans. She is a Co-founder and Head of StratCom of Alliance4Europe where she deals with strategic communication, to build more diverse internet. She co-founded Future Forces Foundation that is working for more impactful business. She is also Vice-President of the Free European Media Association. In 2017 she co-created Keyboard Warriors in Poland, community that debunks disinformation. Maia is a barrister educated in Poland and the United States. She is actively involved in supporting Ukrainian refugees. Maia cooperated with number of foundations and NGOs where she worked on various projects concerning democratization and political parties trainings in Eastern Europe. She advises clients on strategy building and public affairs, as well as trains on leadership, project management and campaign building.

Twitter: [@MaiaMazurkiewicz](#)

SpeakerBio: Michael Moore

After volunteering to be a poll worker, Michael Moore developed a passion for Election Security. He was the first Information Security Officer for the Maricopa County Recorder's office and is now the first Chief Information Security Officer for the Arizona Secretary of State. Michael believes it is only through effective federal, state, and local government partnerships, as well as assistance from trusted vendors that we can protect our democracy and fulfill our duty to the American voter. The greatest threats to elections are MDM and the resulting insider threat caused by radicalized citizens. The best protection against these threats is combating lies with the truth, developing secure and resilient systems that prevent attacks whenever possible, allow for detections of compromise and facilitate accurate and rapid recovery. Michael has pushed forward these initiatives in his own organizations as well as across the Elections community. Michael is an alumnus of Arizona State University with a B.S. in Mathematics and a B.A. in Education and is a CISSP, Certified Election Official (CEO) and Certified Public Manager (CPM).

Twitter: [@Secur3Elections](#)

Description:

This panel will explore all the different ways misinformation, disinformation, and malinformation are being used today, and what we can expect leading up to the 2024 election. The audience will get a comprehensive overview of what to look out for when trying to distinguish what kind of information to consume, and how to protect oneself from misinformation, disinformation, and malinformation campaigns. Different perspectives from across the election and security industries will come together to provide a dynamic outlook on what are experiencing now as well as what we will see in the future.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Importance of Arts and Crafts in ThreatOps

When: Saturday, Aug 12, 16:00 - 16:50 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

SpeakerBio:Pete Hay

In addition to being SimSpace's Principal Security Strategist, Pete is the Co-Founder & Editor-in-Chief of TheCyber.Report. Pete has an extensive & diverse background in technology driven fields including Computer Network Operations (CNO), Network Forensics, & Nuclear Chemistry, as well as one of the few patents issued in Cybersecurity & ZTA. A life-long learner & security enthusiast, Pete helps Fortune 10 banks test & refine their security postures, while running TheCyber.Report as a passion project.

Description:

Cybersecurity professionals spend an huge amount of time attempting to use a visual medium to communicate complicated concepts in a simple yet information-dense manner. However if you ask 10 analysts to map out the same incident, you'll get 10 divergent diagrams. In this presentation we present a method of leveling-up your cybersecurity-related arts and crafts skills: effectively diagramming incidents, threat reports, threat intel, and reporting to support full-spectrum ThreatOps.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Internals of Veilid, a New Decentralized Application Framework

When: Friday, Aug 11, 09:00 - 09:45 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

Speakers:Christien "DilDog" Rioux,Katelyn "Medus4" Bowden

SpeakerBio:Christien "DilDog" Rioux , Cult Of The Dead Cow

Christien 'DilDog' Rioux is a member of The Cult Of The Dead Cow, the author of remote-access utility Back Orifice 2000, and a thorn in Microsoft's side for over a decade. DilDog is the creator of StuntBanana, a caller-id spoofing system, and is proprietor of the hacker-fashion line HACK.XXX. He is also Co-Founder and former Chief Scientist of Veracode, on the founding team of @stake, as well as a member of L0pht Heavy Industries. DilDog is a staunch believer that if you want to change the present you need to build the future, and is very sorry for having helped create "InfoSec" from hacking, and would like to undo the damage.

Twitter: [@@dildog](#)

SpeakerBio:Katelyn "Medus4" Bowden , Cult Of The Dead Cow

Katelyn Bowden is a hacker, activist, and CULT OF THE DEAD cow member, who embraces the human side of hacking and tech. She also creates strange furby art and has over 60 dead things on display in her house.

Twitter: [@@medus4_cdc](#)

Description:

Veilid is an open-source, peer-to-peer, mobile-first networked application framework, with a flagship secure messaging application named VeilidChat. Veilid is conceptually similar to IPFS + Tor, but faster and designed from the ground-up to provide all services over a privately routed network. The network also enables development of distributed applications without a 'blockchain' or a 'transactional layer' at their base. Veilid can be included as part of user-facing applications or run as a standalone server for power users who wish to help build the network.

Architecturally, it is written in Rust, uses strong encryption, and nodes can run on Linux, Mac, Windows, Android, iOS, and in-browser WASM. Low-level protocols over UDP, raw TCP, Websockets and Secure Websockets. Nodes are optimized for low latency, high node churn, and are particularly capable of dealing with low level network changes, such as switching from cellular to wifi networks mid-communication.

This talk will focus on the internals of Veilid: * How it works as a protocol

* How it leverages strong cryptography to provide private communications * How it provides decentralized storage and cryptographically sound data structures * How applications are written to leverage the Veilid Network

We will demonstrate Veilid Server, and VeilidChat, the application.

REFERENCES

Tor Project: www.torproject.org IPFS: www.ipfs.tech

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The International Wigle Space Balloon

When: Friday, Aug 11, 12:00 - 12:59 PDT

Where: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

SpeakerBio:Lozaning

Lozaning (they/them) has been wardriving for over 10 years and enjoys designing, building, and assembling unorthodox network observation platforms such as: The Wifydra (presented here), The International Wigle Space Balloon, and turning an Amtrak roomette into a mobile radio observation lab. Currently ranked as the 84th best wardriver in the world on Wigle.net, Lozaning loves all things wifi and high precision GNSS related.

Lozaning loves wifi, radios, blinky lights, and fancy GPS receivers. They've been wardriving for over 20 years and are now ranked in the top 100 wardrivers in the world.

Description:

This talk will cover the story of the International Wigle Space Balloon from the inception to launch. Along the way we'll cover FAA legalities, hardware design constraints, minimizing launch costs using OTSH, buoyancy and flight characteristic calculations, and conclude with the networks observed during the various flights as well as the introduction of a surprise friend we made along the way.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Saturday - 10:00-17:59 PDT


Title: The IoT Kill Zone

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Bluetooth Hacking: Hands-on exercises provide insights into powerful Bluetooth, WiFi, and IoT Security Assessment tools to unleash your hacking potential. Talk with security researchers on Bluetooth, WiFi, and 5G research; learn about firmware analysis and fuzzing. Walk away knowing the tools and lab equipment you need to perform IoT research.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Sunday - 10:00-13:59 PDT

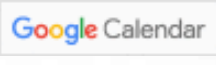
Title: The IoT Kill Zone

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Bluetooth Hacking: Hands-on exercises provide insights into powerful Bluetooth, WiFi, and IoT Security Assessment tools to unleash your hacking potential. Talk with security researchers on Bluetooth, WiFi, and 5G research; learn about firmware analysis and fuzzing. Walk away knowing the tools and lab equipment you need to perform IoT research.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOTV - Friday - 10:00-17:59 PDT


Title: The IoT Kill Zone

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 307-310 - IOT Village - [Map](#)

Description:

Bluetooth Hacking: Hands-on exercises provide insights into powerful Bluetooth, WiFi, and IoT Security Assessment tools to unleash your hacking potential. Talk with security researchers on Bluetooth, WiFi, and 5G research; learn about firmware analysis and fuzzing. Walk away knowing the tools and lab equipment you need to perform IoT research.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Joy of Reverse Engineering: Learning With Ghidra and WinDbg (Pre-Registration Required)

When: Saturday, Aug 12, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

SpeakerBio: Wesley McGrew , Senior Cyber Fellow at MartinFed

Dr. Wesley McGrew directs research, development, and offensive cyber operations as Senior Cybersecurity Fellow for MartinFederal. He has presented on topics of penetration testing and malware analysis at DEF CON and Black Hat USA and taught a self-designed course on reverse engineering to students at Mississippi State University, using real-world, high-profile malware samples. Wesley has a Ph.D. in Computer Science from Mississippi State University for his research in vulnerability analysis of SCADA HMI systems.

Twitter: [@McGrewSecurity](#)

Description:

While it can be intimidating to "get into" software reverse engineering (RE), it can be very rewarding. Reverse engineering skills will serve you well in malicious software analysis, vulnerability discovery, exploit development, bypassing host-based protection, and in approaching many other interesting and useful problems in hacking. Being able to study how software works, without source code or documentation, will give you the confidence that there is nothing about a computer system you can't understand, if you simply apply enough time and effort. Beyond all of this: it's fun. Every malicious program becomes a new and interesting puzzle to "solve".

The purpose of this workshop is to introduce software reverse engineering to the attendees, using static and dynamic techniques with the Ghidra disassembler and WinDbg debugger. No prior experience in reverse engineering is necessary. There will be few slides--concepts and techniques will be illustrated within the Ghidra and WinDbg environments, and attendees can follow along with their own laptops and virtual environments. We will cover the following topics:

- Software Reverse Engineering concepts and terminology
- Setting up WinDbg and Ghidra
- The execution environment (CPU, Virtual Memory, Linking and Loading)
- C constructs, as seen in disassembled code
- Combining static and dynamic analysis to understand and document compiled binary code
- Methodology and approaches for reverse engineering large programs
- Hands-on malware analysis
- How to approach a "new-to-you" architecture

Skill Level: Beginner

Prerequisites for students:

- No previous reverse engineering experience required. - Basic familiarity with programming in a high-level language is necessary (C preferred, Scripting languages like Python would be okay).

Materials or Equipment students will need to bring to participate: - A laptop with a fresh Windows 10 Virtual Machine. - Being able to dedicate 8GB RAM to the VM (meaning, you probably have 16GB in your laptop) will make the experience smoother, but you can get by with 4GB - 10 GB storage free in the VM (after installing Windows) - Administrative privileges - Ability to copy exercise files from USB

We will be working with live malware samples. Depending on your comfort level with this, bring a "burner" laptop, use a clean drive, or plan on doing a clean install before and after the workshop.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-19:59 PDT

Title: The Lonely Hard Drive

When: Friday, Aug 11, 10:00 - 19:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Are you looking for a good time? Are you trying to get lucky? Did you already get lucky by finding a Lonely Hard Drive in Vegas? Satisfy your curiosity by visiting the contest hall to get started or encounter one of the Lonely Hard Drives hidden around the conference! Contained within is a maze of puzzles and challenges that increase in difficulty the further you progress. There are flags to find and points to earn towards the leaderboard to win prizes at DEF CON 31! Act now! Limited time offer! The Lonely Hard Drive is waiting for you!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-12:59 PDT

Title: The Lonely Hard Drive

When: Sunday, Aug 13, 10:00 - 12:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Are you looking for a good time? Are you trying to get lucky? Did you already get lucky by finding a Lonely Hard Drive in Vegas? Satisfy your curiosity by visiting the contest hall to get started or encounter one of the Lonely Hard Drives hidden around the conference! Contained within is a maze of puzzles and challenges that increase in difficulty the further you progress. There are flags to find and points to earn towards the leaderboard to win prizes at DEF CON 31! Act now! Limited time offer! The Lonely Hard Drive is waiting for you!

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-19:59 PDT

Title: The Lonely Hard Drive

When: Saturday, Aug 12, 10:00 - 19:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Are you looking for a good time? Are you trying to get lucky? Did you already get lucky by finding a Lonely Hard Drive in Vegas? Satisfy your curiosity by visiting the contest hall to get started or encounter one of the Lonely Hard Drives hidden around the conference! Contained within is a maze of puzzles and challenges that increase in difficulty the further you progress. There are flags to find and points to earn towards the leaderboard to win prizes at DEF CON 31! Act now! Limited time offer! The Lonely Hard Drive is waiting for you!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Looming Perils for End Users in Satellite Communications

When: Sunday, Aug 13, 10:30 - 11:20 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio: Vincent Lenders

No BIO available

Description:

Satellite communication has gained importance in our mobile and hyper-connected society, but end users are exposed to various security threats that are often not well understood. In this talk, I will present several practical attacks targeting the security and privacy of satellite end users. These attacks target satellite systems such as DVB-S, Inmarsat, Iridium, and GPS. The attacks have been developed and performed in our satellite security research labs at the Swiss Cyber-Defence Campus.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Megabiome is In Charge: Taking Control of Your Microbial World

When: Saturday, Aug 12, 00:00 - 00:59 PDT

Where: Virtual

SpeakerBio: Mariam Elgabry

No BIO available

Description:

This talk is being pre-recorded and will be released on YouTube. Once it is available, a link to it will appear here.

Update 2023-08-11 06:30: Biohacking Village indicates that the pre-recorded talks have not yet been received. Once received, these talks will be posted to the [Biohacking Village YouTube Channel](<https://www.youtube.com/@BiohackingVillage/about>). Please note that this may be as late as a week or two after DC31.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Metasploit Framework

When: Friday, Aug 11, 10:00 - 11:55 PDT

Where: Caesars Forum - Committee Boardroom - Demo Labs - [Map](#)

SpeakerBio: Spencer McIntyre

Spencer McIntyre is a Security Research Manager at Rapid7, where he works on the Metasploit Framework. He has been contributing to Metasploit since 2010, a committer since 2014, and a core team member at Rapid7 since 2019. Previously, Spencer worked at a consulting firm working with clients from various industries, including healthcare, energy, and manufacturing. He is an avid open source contributor and Python enthusiast.

Description:

Active Directory is the foundation of the infrastructure for many organizations. As of 2023, Metasploit has added a wide range of new capabilities and attack workflows to support Active Directory exploitation. This DEF CON demonstration will cover new ways to enumerate information from LDAP, attacking Active Directory Certificate Services (AD CS), leveraging Role Based Constrained Delegation, and using Kerberos authentication. The Kerberos features added in Metasploit 6.3 will be a focal point. The audience will learn how to execute multiple attack techniques, including Pass-The-Ticket (PTT), forging Golden/Silver Tickets, and authenticating with AD CS certificates. Finally, users will see how these attack primitives can be combined within Metasploit to streamline attack workflows with integrated ticket management. The demonstration will also highlight inspection capabilities that are useful for decrypting traffic and tickets for debugging and research purposes.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The of History XR From Fiction to Reality

When: Saturday, Aug 12, 14:00 - 14:59 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

Speakers:Bob Gourley,Starr Brown

SpeakerBio:Bob Gourley

Bob Gourley is an experienced Chief Technology Officer (CTO), Board Qualified Technical Executive (QTE), author and entrepreneur with extensive past performance in enterprise IT, corporate cybersecurity and data analytics. CTO of OODA LLC, a unique team of international experts which provide board advisory and cybersecurity consulting services.

OODA publishes OODALoop.com. Bob has been an advisor to dozens of successful high tech startups and has conducted enterprise cybersecurity assessments for businesses in multiple sectors of the economy. He was a career Naval Intelligence Officer and is the former CTO of the Defense Intelligence Agency.


SpeakerBio:Starr Brown

Starr Brown is the Executive Director of XR Village, a non-profit and non-partisan roadshow dedicated to education and better public policy in the areas of privacy, security and cyber-informed engineering. Starr is an accomplished leader with extensive experience in the computer hardware/software industry with a background in operations, software development and InfoSec.

As an avid gamer, Starr has also been an early advocate and supporter of eSports in education leveraging the power of competitive gaming to enhance student engagement and foster critical skills such as teamwork, problem-solving, and strategic thinking.

Description:

In this discussion XR village Executive Director Starr Brown interviews Bob Gourley, whose site OODALoop.com has been tracking XR topics since 2003. Bob has leveraged his experience as a cybersecurity professional and an enterprise CTO to produce research and reporting on XR that points to a future of incredible potential, if we can mitigate the new threats this emerging technology brings with it. Starr Brown is a security professional with a knack for using collaboration and innovation to meet both compliance and security needs and was early in identifying the unique security and risk mitigation needs of XR, making her the perfect person to extract insights from Bob in this fireside chat.

[Return to Index](#) - Add to  - ics [Calendar](#) file

RCV - Saturday - 17:05-17:50 PDT

Title: The Perils of Generative AI: Implications for Open Source Intelligence Research

When: Saturday, Aug 12, 17:05 - 17:50 PDT

Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio: Andy Dennis

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Petting Zoo: Breaking into CTFs (Pre-Registration Required)

When: Saturday, Aug 12, 09:00 - 12:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

Speakers: Christopher Forte, Robert Fitzpatrick

SpeakerBio: Christopher Forte

Christopher Forte is a security researcher and a junky for learning, participating in CTFs, and solving challenges. He is curious, loves teaching others, and has a passion for breaking things. As a resident of Las Vegas, Christopher co-founded DC702, is the local Chapter President of TOOOL, and enjoys introducing people to the world of hacking and lock picking.

SpeakerBio: Robert Fitzpatrick

Robert Fitzpatrick is a military veteran of over 20 years. He began his cyber life leading the Information Assurance office, and quickly moved up to run the Network Operations Center, as well as the Network Test and Evaluation center. He has built multiple operations centers in both homeland and austere locations, purchased satellite infrastructures, and led vulnerability investigations for classified networks. He is also a co-founder of DC702 and enjoys training new students on an eclectic array of subjects surrounding his interests.

Description:

Breaking into the capture the flag (CTF) world can be daunting and many people are overwhelmed when faced with participation in these events and challenges. With how beneficial the various challenges can be to both beginners and seasoned professionals, we want to demystify this world and help people get the most out of them.

This workshop will start with an overview of the CTF landscape, why we do them, and what value they have in the scope of the hacking community. This presentation will include various resources and a few simple demos to show how to approach a CTF and how it may differ from "real world" hacking challenges that many of us face in our professions. Next, a short CTF will be hosted to give attendees hands-on experience solving challenges with the ability to ask for help and will be guided through the approach to successfully navigating these challenges. Upon completion, the group will have worked through various types of hacking challenges and will have the confidence to participate in other CTFs hosted throughout the year.

Areas of focus will include:

- Common platforms and formats
- Overview of online resources, repositories, and how to progress
- Common tools used in CTFs and hacking challenges
- Basics of web challenges
- Basics of binary exploitation and reversing challenges
- Basics of cryptographic challenges
- Basics of forensic and network traffic challenges

Skill Level: Beginner

Prerequisites for students:

- Be curious about CTFs and have a very basic knowledge of or exposure to fundamental topics (e.g., Linux, websites, networking, data encoding and encryption) - Exposure to the above concepts will help during the workshop defined CTF challenges but is not required for the workshop

Materials or Equipment students will need to bring to participate: - Laptop

- Debian-based Virtual Machine (e.g., Kali) is recommended - Virtualized environment or Kali is not required but Kali will provide all the tools useful in solving the challenges and help standardize available tools. All challenge solutions will be possible using default Kali installations. - A limited number of Kali-Chromebooks and hosted resources will be available for those having issues or unable to bring their own systems.

Title: The Price of Convenience: How Security Vulnerabilities in Global Transportation Payment Systems Can Cost You

When: Sunday, Aug 13, 13:00 - 13:45 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

SpeakerBio: Omer Attias , Security Researcher at SafeBreach Labs

Omer Attias is an accomplished security researcher with over five years of experience in the field of cybersecurity. He currently works as a researcher at SafeBreach Labs.

With a background in the Ministry of Defense and the Israeli Defense Forces (IDF), Omer has honed his skills in network research, including a deep understanding of Windows internals and Linux kernel components.

In addition to his professional pursuits, Omer is a passionate technology and science enthusiast who is always eager to explore emerging trends and innovations in these fields.

Twitter: [@@omerat21](#)

Description:


Public transportation payment systems have undergone significant changes over the years. Recently, mobile payment solutions have become increasingly popular, allowing passengers to pay for their fare using their smartphones or other mobile devices.

The evolution of public transportation payment systems has been driven by the need for faster, more convenient, and more secure payment methods, and this trend is likely to continue in the years to come, But how secure are mobile payment solutions for public transportation?

In this presentation, we will examine the security risks associated with transportation applications, using Moovit as a case study. Moovit is a widely used transportation app operating in over 100 countries and 5000+ cities. Through our investigation of the app's API, including SSL-encrypted data, we discovered specific vulnerabilities, which we will discuss. We will also demonstrate a custom user interface that can obtain a "free ticket" and cause someone else to pay. Furthermore, we will explain how an attacker could gain unauthorized access to and exfiltrate Personal Identifiable Information (PII) of registered users. Our findings offer practical recommendations to improve the security of transportation apps.

REFERENCES

<https://github.com/http toolkit/frida-android-unpinning/blob/main/frida-script.js> <https://moovit.com/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Promise and Perils of Planetary-Scale ISPs

When: Friday, Aug 11, 12:00 - 12:50 PDT

Where: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

SpeakerBio:J. Scott Christianson

J Scott Christianson is an Associate Teaching Professor of management at the University of Missouri, where his interests are focused on the impact of emerging technology on society and geopolitics. Prior to joining the college, he was an entrepreneur with decades of experience in videoconferencing, networking and project management. He currently serves as the College's Director of the Center for Entrepreneurship and Innovation, helping student turn their ideas into profitable products and services. You can reach him at christiansonjs.com

Description:

Our tiny blue planet is quickly being encased in layers of fast-flying, low-earth orbiting satellites in an effort to provide Internet access to earth's three billion unconnected and slowly connected inhabitants. SpaceX's Starlink system is the first planetary-scale ISPs for consumers; more are set to follow. Planetary ISPs can drive much-needed economic growth in the world's poorest countries but introduce unique policy and operational challenges. The regulatory bodies and frameworks set up to deal with terrestrial ISPs are not prepared to deal with issues of internet access, content filtering/moderation, and network neutrality on a global scale. Nor are the agencies governing space launches and operations. While planetary ISPs may see enormous profits, the rest of us may pay the potential costs: an end to ground-based astronomy; an end to clear viewing of the sky; increasing costs for space operations, collision avoidance, and debris removal; and the geopolitical risk when access is provided or not-provided in certain regions. Humanity's future will be determined by how we operate on the internet and in space. How we navigate this new era of space-based internet and what policy frameworks we put in place will determine the winners and losers in this new race in space.

[Return to Index](#) - Add to  - ics [Calendar](#) file

QTV - Friday - 16:00-17:59 PDT

Title: The Quantum Debates

When: Friday, Aug 11, 16:00 - 17:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

Description:

Following from the success of last year's Oxford Union-style debates, we bring you two debates this year! Come and hear experts debate, ruminate, and explore the possible futures of our post-quantum world.

1600 - Debate 1

1645 - TBC (talk)

1715 - Debate 2

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The RingHopper Journey or How We Almost Zero-day'd the World

When: Friday, Aug 11, 10:00 - 10:45 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

Speakers: Benny Zeltser, Jonathan Lusky

SpeakerBio: Benny Zeltser , Security Research Team Lead at Intel

Benny (@benny_zeltser) is a security research team lead @ iSTARE, Intel. He focuses on breaking and exploiting anything on the border between HW and SW. Previously, Benny worked at IBM on development of malware analysis techniques, and spent four years in the IDF Intelligence as a security and research engineer. When Benny is not breaking things, he usually hikes with his 1 yo or cultivating his coffee brewing (and drinking) hobby.

Twitter: [@benny_zeltser](#)

SpeakerBio: Jonathan Lusky , Security Research Team Lead at Cellebrite

Jonathan (@LuskyYehonatan) is a security research team lead @ Cellebrite. In the past, he was a security research team lead @ Intel. He is curious about anything related with low-level security research, reversing binaries, poking CPUs and breaking stuff up. Currently, he is about to complete his master's degree at the Technion focusing on neural network extraction attacks. In his spare time, Jonathan loves to participate in CTFs, play tennis and hike.

Twitter: [@LuskyYehonatan](#)

Description:

Last year we almost zero-day'd the world with the publication of RingHopper. Now we can finally share some juicy details and invite you for an illuminating journey as we delve into the realm of RingHopper, a method to hop from user-land to SMM.

We will survey the discovery and disclosure of a family of industry-wide vulnerabilities in various UEFI implementations, affecting more than eight major vendors, making billions of devices vulnerable to our attack. Then, we will deep-dive into the innards of SMM exploitation and discuss methods to use and abuse various functionalities and properties of edk2 to gain code execution. We will unveil both our futile and fruitful quests of crafting our way to SMM, and detail both the paths that lead to dead-ends, and the route to success.

We will give a detailed overview of different ways to elevate this kind of attack to user-land both on Windows and Linux by chaining multiple vulnerabilities together.

Finally, we will show RingHopper hopping from user-space to... SMM.

REFERENCES

1. DEF CON 29 - Mickey Shkatov, Jesse Michael - High Stakes Updates: BIOS RCE OMG WTF BBQ
2. DEF CON 26 - Shkatov and Michael - UEFI Exploitation for the Masses
3. DEF CON 23 - Yuriy Bulygin - Attacking Hypervisors Using Firmware and Hardware
4. DEF CON 22 - Panel - Summary of Attacks Against BIOS and Secure Boot
5. OffensiveCon22 - Alex Ermolov, Alex Matrosov and Yegor Vasilenko UEFI Firmware Vulnerabilities

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Rocky Balboa Guide to Security Research: Getting Back Up When You Get Knocked Down

When: Saturday, Aug 12, 12:20 - 12:59 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

SpeakerBio: Liv Matan , Cloud Security Researcher at Ermetic

Liv Matan is a cloud security researcher at Ermetic, where he specializes in application and web security. He previously served in the 8200 Intelligence Corps unit as a software developer. As a bug bounty hunter, Liv has found several vulnerabilities in popular software platforms, such as Azure web services, Facebook and Gitlab. In his free time, Liv boxes, lifts and plays Capture the Flag (CTF). Liv studied computer science at the Weizmann Institute of Science, in Israel.

Twitter: [@terminatorLM](#)

Description:

Vulnerability research is sometimes perceived as a glamorous pursuit, where researchers constantly uncover security flaws and find critical exploits that can lead to catastrophic results. In this talk, we show you what it's really like behind the scenes of cloud vulnerability research.

We discuss the lessons learned while dealing with the barriers and challenges that arise when searching for and reporting new vulnerabilities to the biggest cloud vendors. We will present the mindset we embrace to find common ground in major services, and the importance of a responsible disclosure process. We debate why we, the researchers, are accountable for our findings and how we should push the cloud vendor for the best bug resolution.

Often, vulnerability talks are about the researcher's greatest success stories. This talk also explores the unexpected benefits of coming up short in vulnerability research. We argue that these "losses" can provide valuable insights into security research, allowing us to better understand a system's strengths and weaknesses and its security stack.

The session draws on real-world examples, including a major vulnerability we uncovered that affected multiple Azure web services, exploitation of internal communication channels across various CSPs, and our go-to approach when exploring new unfamiliar cloud services. We close the session by discussing each vendor's unique approach to fixing reported security issues.

Join us for this thought-provoking talk and discover the hidden side of vulnerability research. You'll come away with a new appreciation for the challenges and rewards of this fascinating field and a deeper understanding of its role in keeping us all safe and secure.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MIV - Friday - 13:30-13:59 PDT

Title: The Russian Playbook vs. the Chinese Little Red Playbook: Broadening our Understanding of Effective Disinformation Operations


When: Friday, Aug 11, 13:30 - 13:59 PDT

Where: Caesars Forum - Summit - 224 - Misinfo Village - [Map](#)

SpeakerBio: Darren Linvill

No BIO available

Description:

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Saturday - 13:30-14:25 PDT

Title: The Sinister Synergy of Advanced AI: Automatically Orchestrating Large-scale Scam Campaigns with Large Generative Models

When: Saturday, Aug 12, 13:30 - 14:25 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

Speakers: Ben Gelman, Younghoo Lee

SpeakerBio: Ben Gelman

No BIO available

SpeakerBio: Younghoo Lee

No BIO available

Description:

Rapid advancements in AI have enabled large language models (LLMs) and generative technologies to fuse their outputs, creating a new level of diverse, synthetic content that can deceive on an unprecedented scale. This chilling union of AI capabilities opens the door to the generation of entire scam campaigns, blurring the boundary between reality and fiction.

Many people are already aware of how LLMs can help with basic writing and coding. In this talk, we go beyond simple LLM-assisted ploys and automatically orchestrate unprecedented credential-stealing scam campaigns that combine code, text, images, and audio to build dozens of websites, product catalogs, testimonials, and social media advertisements. We discuss how the barriers to entry have decreased for criminals with minimal knowledge of AI, the scale that automation can achieve, and the current shortcomings that still require human intervention.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Ultimate AppSec Trivia Challenge

When: Saturday, Aug 12, 13:00 - 14:59 PDT


Where: Flamingo - Savoy - AppSec Village - Pod 4 - [Map](#)

SpeakerBio: Probely

No BIO available

Description:

The Ultimate AppSec Trivia Challenge is a fun and educational game that tests your application security knowledge. The game consists of cards with questions ranging from easy to hard, all related to application security. Players can challenge themselves, or each other, to test their knowledge. You can improve your understanding of AppSec and have fun simultaneously. Bring your team or yourself and see where you rank on the leaderboard! Whether you're a beginner or an expert in application security, The Ultimate AppSec Trivia Challenge has something for everyone to learn.

[Return to Index](#) - Add to  - ics [Calendar](#) file

APV - Friday - 13:00-14:59 PDT

Title: The Ultimate AppSec Trivia Challenge

When: Friday, Aug 11, 13:00 - 14:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 4 - [Map](#)

SpeakerBio: Probely

No BIO available

Description:

The Ultimate AppSec Trivia Challenge is a fun and educational game that tests your application security knowledge. The game consists of cards with questions ranging from easy to hard, all related to application security. Players can challenge themselves, or each other, to test their knowledge. You can improve your understanding of AppSec and have fun simultaneously. Bring your team or yourself and see where you rank on the leaderboard! Whether you're a beginner or an expert in application security, The Ultimate AppSec Trivia Challenge has something for everyone to learn.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Ultimate AppSec Trivia Challenge

When: Saturday, Aug 12, 11:00 - 12:59 PDT


Where: Flamingo - Savoy - AppSec Village - Pod 4 - [Map](#)

SpeakerBio: Probely

No BIO available

Description:

The Ultimate AppSec Trivia Challenge is a fun and educational game that tests your application security knowledge. The game consists of cards with questions ranging from easy to hard, all related to application security. Players can challenge themselves, or each other, to test their knowledge. You can improve your understanding of AppSec and have fun simultaneously. Bring your team or yourself and see where you rank on the leaderboard! Whether you're a beginner or an expert in application security, The Ultimate AppSec Trivia Challenge has something for everyone to learn.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Ultimate AppSec Trivia Challenge

When: Friday, Aug 11, 11:00 - 12:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 4 - [Map](#)

SpeakerBio: Probely

No BIO available

Description:

The Ultimate AppSec Trivia Challenge is a fun and educational game that tests your application security knowledge. The game consists of cards with questions ranging from easy to hard, all related to application security. Players can challenge themselves, or each other, to test their knowledge. You can improve your understanding of AppSec and have fun simultaneously. Bring your team or yourself and see where you rank on the leaderboard! Whether you're a beginner or an expert in application security, The Ultimate AppSec Trivia Challenge has something for everyone to learn.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Saturday - 16:00-16:30 PDT

Title: The Unlikely Romance: Critical Infrastructure Edition

When: Saturday, Aug 12, 16:00 - 16:30 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio: Casey Ellis , Bugcrowd

Casey is the Chairperson, Founder, and Chief Technology Officer of Bugcrowd, as well as the co-founder of The disclose.io Project. He is a 20-year veteran of information security who spent his childhood inventing things and generally getting technology to do things it isn't supposed to do. Casey pioneered the Crowdsourced Security as-a-Service model, launching the first bug bounty programs on the Bugcrowd platform in 2012, and co-founded the disclose.io vulnerability disclosure standardization project in 2014 prior to its launch in 2018.

Since then, he has personally advised the US Department of Defense and Department of Homeland Security/CISA, the Australian and UK intelligence communities, and various US House and Senate legislative cybersecurity initiatives, including preemptive cyberspace protection ahead of the 2020 Presidential Elections.

Casey, a native of Sydney, Australia, is based in the San Francisco Bay Area.

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Wednesday - 11:00-16:59 PDT

Title: The Unofficial DEF CON Shoot

When: Wednesday, Aug 9, 11:00 - 16:59 PDT

Where: Other/See Description

Description:

Where: Pro Gun Vegas

Address: 12801 US 95 South Boulder City, NV 89005 When: Before the con Wednesday Aug 9th, 11:00 - 17:00

https://deviating.net/firearms/defcon_shoot/

The Unofficial DEF CON Shoot is a public event that happens just prior to the DEF CON hacker conference in Las Vegas, Nevada. It is an opportunity to see and shoot some of the guns belonging to your friends while taking pride in showing and firing your own steel, as well, in a relaxed and welcoming atmosphere. We choose a spot, then we rent tables, canopies, and bring all the necessary safety equipment and amenities. All you need to bring yourself and (optionally) your firearms. New shooters and veterans both attend regularly. You can attend with your firearms, of course, but folk without guns of their own in Vegas may have the opportunity to try gear from others in attendance or to inquire with the ProGun range about whether rental firearms are available.

This is a 100% off-site event and a defcon badge is not required for entry.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 21:00-00:59 PDT

Title: The Village People Party: hosted by Car Hacking, ICS, Aerospace, and Biohacking Villages

When: Friday, Aug 11, 21:00 - 00:59 PDT

Where: Caesars Forum - Forum - 115-116 - [Map](#)

SpeakerBio:NGHTHWK

No BIO available

Description:

Each village will be passing out drink tickets at their booth (while supplies last!)

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Sunday - 12:00-12:30 PDT

Title: The War is Coming: Why Securing OPC-UA is more critical than ever

When: Sunday, Aug 13, 12:00 - 12:30 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio: Hank Chen

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Wifydra: Multiheaded RF Panopticon

When: Saturday, Aug 12, 10:00 - 11:55 PDT

Where: Caesars Forum - Society Boardroom - Demo Labs - [Map](#)

SpeakerBio:Lozaning

Lozaning (they/them) has been wardriving for over 10 years and enjoys designing, building, and assembling unorthodox network observation platforms such as: The Wifydra (presented here), The International Wigle Space Balloon, and turning an Amtrak roomette into a mobile radio observation lab. Currently ranked as the 84th best wardriver in the world on Wigle.net, Lozaning loves all things wifi and high precision GNSS related.

Lozaning loves wifi, radios, blinky lights, and fancy GPS receivers. They've been wardriving for over 20 years and are now ranked in the top 100 wardrivers in the world.

Description:

The Wifydra is open source hardware and software used to locate wireless access points for wardriving. The project is a continuation of the work done previously by Mike Spicer (@d4rkm4tter) and his WiFi Cactus and Kraken. It's designed to be a low power and low cost modular way of simultaneously monitoring all 2.4Ghz WiFi channels for AP beacons. By utilizing strictly off the shelf embedded components, the Wifydra is able to keep costs extremely low (~\$90) and its footprint extremely small (250 square cm). More importantly, minimal power consumption is maintained, requiring only a USB C battery capable of putting out 10 watts. The Wifydra is modular in nature and supports a multitude of GNSS (Global Navigation Satellite System) options for location tagging. The ESP32-C5 for 5Ghz channel monitoring will also be supported once the hardware becomes available. The version of The Wifydra demoed consists of 14 ESP8266 called sub nodes, an additional ESP32 called the dom node, SD card holder, GNSS module, OLED screen, as well as the Wifydra carrier board that connects all these components. The firmware, BOM, and gerbers are all available in The Wifydra's Github repo:

https://github.com/lozaning/The_Wifydra

Return to Index - Add to  - ics [Calendar](#) file

Title: There are no mushroom clouds in cyberwar

When: Friday, Aug 11, 14:00 - 14:20 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio:Mieke Eoyang

Ms. Mieke Eoyang is the Deputy Assistant Secretary of Defense for Cyber Policy. The Cyber Policy office is responsible for establishing DoD cyberspace policy and strategy, providing guidance and oversight on DoD cyberspace activities, and managing DoD's primary external relationships across the U.S. government, key domestic stakeholders, and our allies and partners.

Prior to that she was the Senior Vice President for the National Security Program at the think tank, Third Way, where she led their work on a wide range of national security issues including on foreign policy, Congress' role in the national security policymaking process, non-proliferation, intelligence oversight, electronic surveillance, cybersecurity. She was the founder of the organization's Cyber Enforcement Initiative which focused on improving the government's efforts to impose consequences on the human behind malicious cyber activity.


Before joining Third Way, she was the Chief of Staff to Rep. Anna G. Eshoo (D-CA) having previously served as the Subcommittee Staff Director for Intelligence Community Management on the House Permanent Select Committee on Intelligence. While there, she was the committee's lead for cybersecurity, personnel management and worked on electronic surveillance reform, among other issues.

Prior to that, she served as the Defense Policy Advisor to Senator Edward M. Kennedy, advising him on all matters related to the Senate Armed Services Committee and Defense Appropriations during the Iraq War. Earlier in her career, she served as the lead Democratic Professional Staff Member on the House Armed Services Committee for the Military Personnel Subcommittee.

Ms. Eoyang received her Juris Doctor from the University of California, Hastings College of the Law, and her Bachelor's Degree from Wellesley College.

Description:

This presentation will discuss the history of cyberwarfare, highlighting the misconceptions between nuclear deterrence and the nature of cyber conflict. It will shed light on this association in popular culture, including in movies like "WarGames," which influenced then President Ronald Reagan and fed his concerns about potential hacking into U.S. weapons systems. These concerns and other influences helped to shape early perceptions about the cyber domain, which immediately became intertwined with notions of strategic weapons and catastrophic effects. In subsequent decades, continued theorizing about cyberwarfare envisioned strategic cyber attacks that could cause decisive effects, stoking fears of a "Cyber Pearl Harbor." However, the reality is that cyber operations are ephemeral and cyber effects are hard to attribute and are rarely decisive. The turning point in U.S. cyber strategy occurred in lead up to the 2018 midterm election, with the adoption of a new approach focused on defending forward, which involved actively disrupting malicious cyber activity before it affected the U.S. Homeland. This strategy was further informed by Russia's 2022 invasion of Ukraine, which demonstrated how cyber capabilities may be used in large-scale conventional conflict. Looking ahead, in terms of protecting Americans and strengthening our global Allies and partners, we know that private industry and individual volunteers will play a critical role, including many of the participants at DEF CON. This recognition acknowledges that cyberwarfare is pervasive and requires collective engagement.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: These Port Scans are Trash: Improving Nmap by Writing New Scripts and Libraries (Pre-Registration Required)

When: Thursday, Aug 10, 14:00 - 17:59 PDT

Where: Flamingo - Exec Conf Ctr - Foyer - Workshop Checkin - [Map](#)

SpeakerBio: Philip Young "Soldier of FORTRAN"

Philip Young, aka Soldier of FORTRAN, is a leading expert in all things mainframe hacking. Having spoken and taught at conferences around the world, including DEFCON, RSA, BlackHat and keynoting at both SHARE and GSE Europe, he has established himself as the thought leader in mainframe penetration testing. Since 2013 Philip has released tools to aid in the testing of mainframe security and contributed to multiple opensource projects including Nmap, allowing those with little mainframe capabilities the chance to test their mainframes. He created the Nmap TN3270 library which enabled Nmap to scan and fingerprint z/OS mainframes and SNA networks. His hope is that through education others will create new libraries and scripts to force corporations to fix their shit.

Description:

Does anyone know how old Nmap is? If you guessed 20 years old, you'd be wrong! It's been around since 1997 when it was first released in Phrack magazine. Since the beginning, it's been through multiple iterations and an entire community has developed around it. One of the most important additions to Nmap was the ability to add custom scripts. Changing Nmap from a simple port scanner to the swiss army knife of network scanners. Oftentimes, when zero days pop up, someone will write an nmap script to identify vulnerable servers within minutes. If you've ever wondered how people write Nmap scripts, what it would take to write your own and how you can use them, this workshop is for you.

Attendees in this workshop will learn how to understand and update the Nmap probe file, how to write Lua scripts (which Nmap scripting uses), how to write Nmap scripts to supplement the probe file, interact with custom services and ultimately write multiple Nmap scripts to do fun stuff with ports. Once attendees have a firm grasp of the Nmap scripting engine they will be introduced to writing Nmap libraries for use by their various scripts. This workshop contains many instructor lead labs so that attendees can see their code in action. To make this workshop worthwhile, a custom service running on a port has been created which the labs will allow you to probe and identify as the course goes on.

Nmap is the workhorse behind the scenes for so many pentesters, but the resources for writing scripts are limited. The hope is that by offering this workshop, more people will be able to write Nmap scripts for the betterment of all hackingkind.

Skill Level: Beginner

Prerequisites for students:

- Some basic understanding of how to write code (python, C, Lua, etc), how to use the Linux command line.

Materials or Equipment students will need to bring to participate: - A laptop capable of running a linux VM

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Threat modeling-based application security pipeline

When: Sunday, Aug 13, 11:00 - 11:45 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

Speakers:Larkins Carvalho,Nielet D'mello

SpeakerBio:Larkins Carvalho

Larkins is a product security engineer, a builder by nature who loves to build solutions to various application security challenges with a developer centric mindset making security accessible early in the application lifecycle.

Twitter: [@larkinscarvalho](#)

SpeakerBio:Nielet D'mello

Nielet is a Security engineer at Datadog with a focus on Appsec for the products used by customers globally for observability. She loves to share her learnings via writing publicly and also mentoring at grad schools.

Description:

Application security reviews are performed to proactively discover and mitigate vulnerabilities in applications and services being developed or deployed in order to reduce risk. It includes any or all of these activities: threat modeling, in-depth secure code review and dynamic testing.

In a fast-paced and engineering-heavy organizations, these are typically non-blocking and can be seen as a security pipeline defining roles and responsibilities, scope of the review, a priority queue based on business risk profiling, expected outcomes and risk findings across the application.

We start with a strong foundation for secure design by performing a security design review focused on threat modeling to derive security requirements and test plans. This is followed by an in-depth secure code review and dynamic testing / validation.

As we progress through the application lifecycle, if secure code reviews uncover high risk code changes and vulnerabilities or penetration testing results point to exploitable findings this indicates a need to do better threat modeling.

The success of this in terms of scaling and maturity depends on three factors working in tandem: tools, processes and people. Therefore, we need to leverage a security pipeline approach for well defined structure and automation..

In this talk, we will cover:

- creating a structure for these reviews based on their scope and priority
- calibrating reviews as a team and organization
- leveraging partnerships like security champions (engineers) as key players who are not responsible for the pipeline but help move the pipeline further
- capturing key risk and remediation metrics
- building automation and tooling centered around for threat modeling in a complete security assessment

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Threat modelling fun session with OWASP Cornucopia

When: Friday, Aug 11, 15:00 - 16:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 1 - [Map](#)

SpeakerBio: Spyros Gasteratos

Spyros is a Security Engineer with over a decade of experience in various organisations. Currently, he is helping Fintechs mature their AppSec programmes through automation. He maintains several Open Source projects including Dracon, opencre.org and others. Also, he is heavily involved with the OWASP foundation helping with outreach and diversity efforts.

Twitter: [@0xfde](#)

Description:

Join us into this collaborative game of OWASP Cornucopia! Over the course of two hours we will create a Threat Model of an example target infrastructure using the OWASP Cornucopia game! Winner keeps the deck!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Threat modelling fun session with OWASP Cornucopia

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 1 - [Map](#)

SpeakerBio: Spyros Gasteratos

Spyros is a Security Engineer with over a decade of experience in various organisations. Currently, he is helping Fintechs mature their AppSec programmes through automation. He maintains several Open Source projects including Dracon, opencre.org and others. Also, he is heavily involved with the OWASP foundation helping with outreach and diversity efforts.

Twitter: [@0xfde](#)

Description:

Join us into this collaborative game of OWASP Cornucopia! Over the course of two hours we will create a Threat Model of an example target infrastructure using the OWASP Cornucopia game! Winner keeps the deck!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Threat modelling fun session with OWASP Cornucopia

When: Sunday, Aug 13, 12:00 - 13:59 PDT

Where: Flamingo - Savoy - AppSec Village - [Map](#)

SpeakerBio: Spyros Gasteratos

Spyros is a Security Engineer with over a decade of experience in various organisations. Currently, he is helping Fintechs mature their AppSec programmes through automation. He maintains several Open Source projects including Dracon, opencre.org and others. Also, he is heavily involved with the OWASP foundation helping with outreach and diversity efforts.

Twitter: [@0xfde](#)

Description:

Join us into this collaborative game of OWASP Cornucopia! Over the course of two hours we will create a Threat Model of an example target infrastructure using the OWASP Cornucopia game! Winner keeps the deck!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: ThreatScraper: Automated Threat Intelligence Gathering and Analysis for VirusTotal

When: Saturday, Aug 12, 14:00 - 15:55 PDT

Where: Caesars Forum - Accord Boardroom - Demo Labs - [Map](#)

Speakers: Aaron "AJ" Morath, Scott Graham

SpeakerBio: Aaron "AJ" Morath

Captain Aaron "AJ" Morath, CEH/CompTIA Pentest+, is a graduate student at the Air Force Institute of Technology, where he is involved in researching malware identification and propagation. His thesis work concentrates on developing innovative strategies to combat evolving cybersecurity threats and enhance security measures. AJ has served as the Defensive Cyber Operator (DCO) Officer in Charge (OIC) of the NASIC DCO team for three years. He oversaw the security and defense of an enterprise network comprising over 6,000 connected devices.

SpeakerBio: Scott Graham

Dr. Scott Graham is a Professor of Computer Engineering at the Air Force Institute of Technology. His research interests center on cyber physical systems, looking at the intersection between real physical systems and the computers that control them. Specific areas of interest include cyber physical systems security, computer architecture, embedded computing, critical infrastructure protection, and vehicular cyber security.

Description:

VirusTotal serves as a popular platform for aggregating malware information submitted by Anti-Virus (AV) software providers, which can be searched using parameters such as hashes (SHA-1, SHA-256, MD5), file names, and malicious web links. In order to enhance and automate the process of malware intelligence gathering, we introduce ThreatScraper, a Python-based tool that automates free API queries and rescanning tasks on VirusTotal. ThreatScraper is designed to periodically request reports on specified files and save the results in a local database or Excel file. It allows users to pull and aggregate malicious file reports from multiple AV vendors over time, providing insights into the adoption of malware detection across providers. Easily implemented from any Windows command line, ThreatScraper can rescan a file, pull a report, and then sleep until the next designated time identified by the user.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Time, Persistence, Patience

When: Friday, Aug 11, 10:40 - 11:40 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

SpeakerBio:Michael "v3ga_hax" Aguilar , Principle Consultant at Secureworks Adversary Group

Michael Aguilar (v3ga_hax) is a Principle Consultant with Secureworks Adversary Group. He leads the Medical Device Adversarial Testing efforts at Secureworks as well conducting Adversarial Assessments, Internal/External Adversarial testing, Social Engineering and other fun things. When not knocking over systems, he enjoys cardio (running/cycling), playing guitar/screaming and music.

Description:

Currently, medical devices are getting smarter by the minute. However, with the rapid expansion of new technologies on legacy systems, these smart additions are adding massive amounts of attack footprint. Additionally, older ways of development, utilizing sometimes poorly constructed binaries or scripts, are placed onto newer operating systems, leaving an environment ripe for exploitation. Adding urgency, the FDA also recently announced it would begin denying systems with vulnerabilities. This will go over my methods of using full scope testing (physical/netpen/hardware/other) to gain good findings for remediation in the modern world and the differentiators I have seen in my testing method vs. others observed in field. It will also have ample examples of actual bugs located during testing, how they were uncovered, and how they were utilized to exploit target systems (anonymized of course).

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Tinfoil Hat Contest

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Want to block those pesky 5G microchips coursing through your vaccinated body? Did you anger our new AI overlords, and need to hide? Or do those alien mind control rays just have you down lately? Fear not, for we here at the Tin Foil Hat contest have your back for all of these! Come find us in the contest area, and we'll have you build a tin foil hat which is guaranteed to provide top quality protection for your noggin. How you ask? SCIENCE!

Show us your skills by building a tin foil hat to shield your subversive thoughts, then test it out for effectiveness.

There are 2 categories: stock and unlimited. The hat in each category that causes the most signal attenuation will receive the "Substance" award for that category. We all know that hacker culture is all about looking good, though, so a single winner will be selected from each category for "Style".

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

Title: Tinfoil Hat Contest

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Want to block those pesky 5G microchips coursing through your vaccinated body? Did you anger our new AI overlords, and need to hide? Or do those alien mind control rays just have you down lately? Fear not, for we here at the Tin Foil Hat contest have your back for all of these! Come find us in the contest area, and we'll have you build a tin foil hat which is guaranteed to provide top quality protection for your noggin. How you ask? SCIENCE!

Show us your skills by building a tin foil hat to shield your subversive thoughts, then test it out for effectiveness.

There are 2 categories: stock and unlimited. The hat in each category that causes the most signal attenuation will receive the "Substance" award for that category. We all know that hacker culture is all about looking good, though, so a single winner will be selected from each category for "Style".

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 12:00-14:59 PDT

Title: TOOOL Dozier Drill Lockpicking Challenge

When: Saturday, Aug 12, 12:00 - 14:59 PDT


Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

Description:

Have you ever wanted to break out of handcuffs, pick open a closed bag and shoot your buddy in the chest with a nerf gun? So have we, that's why TOOOL presents the Dozer Drill. A fast paced skill based game where you have to free yourself from handcuffs, open a closed bag, and retrieve the nerf gun to be the first to hit the target. Join us Friday for qualifier games, and on Saturday for an official bracket tournament.

Important Note

In order to participate in the official bracket tournament on Saturday, you must win a round (against anyone), observed by a village staff member, on Friday. See village staff for details.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Top 10 Hacks To Watch Out For From An Election Official

When: Friday, Aug 11, 11:30 - 12:20 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio:John Odum

John Odum has served as the city clerk and election administrator of Vermont's capital city of Montpelier for 11 years. He is a Certified Ethical Hacker and Certified Network Defense Architect, as well as a Certified Municipal Clerk. John holds a Certificate in Election Administration from the University of Minnesota Humphrey School of Public Affairs and has served on the Advisory Board of the Cyber Policy Initiative at the University of Chicago Harris School of Public Policy. John has written on election security and politics for the Guardian (online), Huffington Post, Governing, and others. He previously worked in electoral politics for many years, including serving as the statewide Field Director for the Clavelle for Governor campaign in Vermont

Twitter: [@jodum](#)

Description:

This paper is written to give a very brief overview of several potential security issues that could exist in an election environment. It is a subjective list and should be read as such. Also, it lays out brief descriptions of potential vectors of attack, particularly vectors that could be used for simple disruption or to create opportunities for direct access to voter data and election management systems through privilege escalation. It also speaks to physical security. The term “hack” is to be interpreted broadly, sometimes referring to specific techniques (such as LDAP injection), broader hack categories (such as Man in the Middle) and other times referring to broad strategic approaches that facilitate specific hacks (such as social engineering). The paper is designed to paint a picture of the threat landscape, rather than serve as a technical guide. The paper is written at a basic technical level to keep it as accessible as possible to non-technical readers, as many of those participating in Voting Village are uniquely non-techie within the DEF CON setting. It starts early from a more technical perspective before becoming more accessible and eventually policy-focused. The objective is to promote best security practices and provide organizational administrators (as opposed to technical administrators) context for the types of challenges that exist. As such, it attempts to walk a tricky line to be accessible to as many as possible. It is presented in a casual “top ten” format and touches on a broad range of hacks are discussed very briefly. The paper should not be considered a tool for security professionals to gain a comprehensive understanding of each hack on the list. Its purpose is to educate generally, help point security admins in the right direction, and encourage them to dig deeper than the ankle-deep information provided. All the topics presented demand more thorough discussion and examination than the snapshots this paper provides.

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Saturday - 16:45-17:45 PDT

Title: Totally Tubular: An Impromptu Talk About Tubular Locks and Keys

When: Saturday, Aug 12, 16:45 - 17:45 PDT

Where: LINQ - 5th Floor / BLOQ - Lockpick Village - [Map](#)

SpeakerBio: Deviant Ollam

No BIO available

Description:

Tubular locks (also known colloquially as "barrel key" locks or by the O.G. name "ACE" lock or "Chicago" lock) have been around for ages and are mostly considered obsolescent at this point... but how many of you can reliably pick them and produce keys for them?

This talk will attempt to demystify some of the oddities surrounding tubular systems and reveal the tools and hardware that you can use to side-step many hassles regarding tubular locks if you encounter them in the field.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MISC - Thursday - 15:00-20:59 PDT

Title: Toxic BBQ

When: Thursday, Aug 10, 15:00 - 20:59 PDT

Where: Other/See Description

Description:

15:00- 21:00 Thursday, Off-site at Sunset Park, Pavilion F, (36.0636, -115.1178)

The humans of Vegas invite you to this year's unofficial welcome party. Join us off-Strip in the shade of Sunset Park for a heat-blasted hangout. Burgers, dogs, and meatless options are provided. Attendees pitch in to make everything else happen. Contribute more food and drinks, staff the grill or join supply runs, and relax under the trees with good conversation with new and old friends. Come be a part of what makes this cookout something to remember year after year.

Grab flyers from an Info Booth, check out <https://www.toxicbbq.org> for the history of this event, and watch for #ToxicBBQ for the latest news.

--

Toxic BBQ is Kid Friendly and Welcoming. In fact, our marketing captain is 16! As with anything DEFCON, caveat parentum

If you are ok bringing and minding your kids to a backyard cookout, they'll be fine here. While we don't have kid-specific programming or events, it's at a park.

We reserve the right to bribe them with swag to help out, and we may try to feed them Octopus jerky.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 15:30-16:29 PDT

Title: Trace Labs OSINT Search Party CTF - Announce CTF Grand Prize Winners

When: Saturday, Aug 12, 15:30 - 16:29 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The Trace Labs Search Party CTF is a non theoretical, gamified effort that allows for the crowdsourcing of contestants to perform a single task: Conduct open source intelligence operations to help find missing persons.

You can have teams of 1-4 people, 4 person teams provide many benefits which include the coaching of more junior members. Often a great learning opportunity if you are able to pair up with OSINT veterans. Get your team together and join us in our [Discord group](<https://tracelabs.org/discord>) to get started.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:30-14:30 PDT

Title: Trace Labs OSINT Search Party CTF - CTF Platform Open for Submissions

When: Saturday, Aug 12, 10:30 - 14:30 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The Trace Labs Search Party CTF is a non theoretical, gamified effort that allows for the crowdsourcing of contestants to perform a single task: Conduct open source intelligence operations to help find missing persons.

You can have teams of 1-4 people, 4 person teams provide many benefits which include the coaching of more junior members. Often a great learning opportunity if you are able to pair up with OSINT veterans. Get your team together and join us in our [Discord group](<https://tracelabs.org/discord>) to get started.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

Title: Trace Labs OSINT Search Party CTF - Sign-ups


When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

The Trace Labs Search Party CTF is a non theoretical, gamified effort that allows for the crowdsourcing of contestants to perform a single task: Conduct open source intelligence operations to help find missing persons.

You can have teams of 1-4 people, 4 person teams provide many benefits which include the coaching of more junior members. Often a great learning opportunity if you are able to pair up with OSINT veterans. Get your team together and join us in our [Discord group](<https://tracelabs.org/discord>) to get started.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Track the Planet! Mapping Identities, Monitoring Presence, and Decoding Business Alliances in the Azure Ecosystem

When: Friday, Aug 11, 17:30 - 17:50 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

SpeakerBio:nyxgeek , Hacker at TrustedSec

nyxgeek is a hacker at TrustedSec. Interests include: user enumeration, password spraying, password cracking. Team Trontastic on the CMIYC leaderboard.

Twitter: [@@nyxgeek](#)

Description:

Microsoft Azure is ripe with user information disclosures. We are going to look at weaponizing these disclosures by performing data collection at a large scale against OneDrive, Teams, and Graph.

OneDrive and Teams present silent enumeration methods, requiring no logon attempts and creating no logs. This enables enumeration at a massive scale against the biggest corporations, educational institutes, and government entities in the world. Over the last 1.5 years I have enumerated over 20m users. We will explore the techniques used and the data that was collected, including Azure adoption rates and analysis of username formats.

Microsoft Teams suffers from information disclosure due to default settings allowing users to see the online presence of others. An undocumented, unauthenticated Microsoft Teams Presence lookup trick will be shared, which enables easy unauthenticated enumeration of the online Teams Presence of users at many organizations. To demonstrate this we will monitor approximately 100,000 Microsoft employees' online presence and any out-of-office messages that are stored.

Finally, Azure supports Guest users, allowing two companies to collaborate on a project. I will unveil a method of identifying Azure Guest users at other tenants. In this way, hidden corporate relationships can be revealed.

Related exploits identified include:

Microsoft Lync Time-Based User Enum (no CVE - 2016) Microsoft Skype for Business 2016 XSS Injection - CVE-2017-8550 Microsoft Lync 2011 for Mac HTML Injection - CVE-2018-8474

Related Tools:

onedrive_user_enum
o365recon
lynsmash

REFERENCES

https://github.com/nyxgeek/onedrive_user_enum <https://github.com/Flangvik/TeamFiltration/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Tracking the Worlds Dumbest Cyber-Mercenaries

When: Friday, Aug 11, 14:00 - 14:20 PDT

Where: Harrah's - Nevada Ballroom - Lake Tahoe & Reno - War Stories - On the Record - [Map](#)

SpeakerBio: Cooper Quintin , Senior Staff Technologist at Electronic Frontier Foundation

Cooper Quintin is a security researcher and senior public interest technologist with the EFF Threat Lab. He has worked on projects including Privacy Badger, Canary Watch, and analysis of state sponsored malware campaigns such as Dark Caracal. Cooper has given talks at security conferences including Black Hat, DEFCON, Enigma Conference, and ReCon about issues ranging from IMSI Catcher detection to fem tech privacy issues to newly discovered APTs. He has also been published or quoted in publications including: The New York Times, Reuters, NPR, CNN, and Al Jazeera. Cooper has given security trainings for activists, non profit workers, and vulnerable populations around the world. He previously worked building websites for nonprofits, including Greenpeace, Adbusters, and the Chelsea Manning Support Network. Cooper was also an editor and contributor to the hacktivist journal, "Hack this Zine." In his spare time he enjoys making music, visualizing a solar-punk anarchist future, and playing with his kids.

Twitter: [@cooperq](#)

Description:

For the last 6 years my colleagues and I have been tracking the activities of the cyber-mercenaries we call Dark Caracal. In this time we have observed them make a number of hilarious mistakes which have allowed us to gain crucial insights into their activities and victims. In this talk we will discuss the story of Dark Caracal, the mistakes they have made, and how they have managed to remain effective despite quite possibly being the dumbest APT to ever exist.

REFERENCES

<https://www.eff.org/wp/operation-manul>

https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

<https://www.welivesecurity.com/2021/07/07/bandidos-at-large-spying-campaign-latin-america/>

<https://www.eff.org/deeplinks/2023/02/uncle-sow-dark-caracal-latin-america>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Transportation Screening Equipment Cybersecurity Briefing

When: Friday, Aug 11, 16:00 - 16:50 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio:Edam Colón

No BIO available

Description:

This presentation discusses the Cybersecurity challenges faced when evaluating the Transportation Screening Equipment at TSA. It covers at a high level the components seen during an evaluation, what stakeholders of systems should be aware of and how we can improve the security of the systems going forward. The briefing will cover a wide variety of topics related to security testing of the equipment and how it will differ between IT and OT while still maintaining the overall security.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Tuning the human Bio-Field – proven classics forged with AI IOMT

When: Sunday, Aug 13, 12:20 - 13:20 PDT


Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

SpeakerBio: Wayne Burke and Team

Recognized globally for his 25 years plus, work experience, achievements and contributions to the IT Security Industry. He specializes in, Penetration Testing, Mobile, IOT, BioMed, hardware, Digital Forensics and devices which also utilize AI / ML technology.

Description:

Combining sound with latest Ai / ML technology that helps tune the Human Bio-Field, extending years of industry experts research, quantum leaping works from Eileen Day Mckusick and Dr. Jerry Tennant to name a few. We will demonstrate our new prototype technology, The Ai Bio-Field Tuner.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Turning my virtual wallet into a skimming device: mPOS solutions

When: Friday, Aug 11, 15:30 - 16:15 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

Speakers: Dan Borgogno, Ileana Barrionuevo

SpeakerBio: Dan Borgogno, Security Engineer at LATU

Dan Borgogno is a security engineer, backend developer, security researcher and international speaker with years of experience on mobile, hardware, IoT and web application hacking. Security engineer@LATU Seguros.

Twitter: [@dborgogno](#)

SpeakerBio: Ileana Barrionuevo, Security Researcher at UTN FRC

Ileana Barrionuevo is a security engineer, security researcher and international speaker with years of experience in Android mobile hacking and web application hacking. Security researcher @Labsis UTN FRC

Twitter: [@accio_bugs](#)

Description:

In third-world economies, cheaper often means more accessible. In recent years, there has been a growing interest in modern mobile wallet solutions that allow you to save money, make transactions, payments, and transfer funds to friends or clients with the help of MPOS devices. These small, durable, and simple devices can be used to read credit card information.

However, these solutions have vulnerabilities that can be exploited. In this talk, we will provide real-life examples of money theft, credit card information skimming, Bluetooth communication tampering, and hardware hacking associated with these solutions.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: UNConventional Cybercrime: How a Bad Anti-Hacking Treaty is Becoming a Law

When: Thursday, Aug 10, 11:00 - 11:20 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers: Bill Budington, Katitza Rodriguez

SpeakerBio: Bill Budington, Senior Staff Technologist at Electronic Frontier Foundation

Bill Budington is a Senior Staff Technologist on EFF's Public Interest Technology team. Their research has been featured in the The New York Times, The Los Angeles Times, The Guardian, and cited by the US Congress. They are the lead developer of Cover Your Tracks.

SpeakerBio: Katitza Rodriguez, Policy Director for Global Privacy at Electronic Frontier Foundation

Katitza Rodriguez is EFF's Policy Director for Global Privacy. She concentrates on comparative policy of global privacy issues, with special emphasis on cross-border data flows. Katitza's work also focuses on cybersecurity and government access to data held by the private sector at the intersection of international human rights law and standards. In 2018, CNET named Katitza one of the 20 most influential Latinos in technology in the United States.

Twitter: [@@txitua](#)

Description:

Heads up DEFCON! The future of hacking, cybersecurity, and human rights are at risk as the United Nations negotiates a draft UN cybercrime treaty that has the potential to substantively reshape anti-hacking law around the world. The proposed Treaty could change the game for security researchers and coders like you. With Russia and China playing an initial role in pushing for this treaty, the future for security researchers's rights could be at risk.

Join us as we deep dive into the murky waters of these negotiations, exploring its risks for security and human rights, including the universal criminalization of network and device intrusion without any protections for legitimate security research. The lack of legal shield for security researchers could hinder bug bounties, responsible vulnerability disclosure, and pentesting. We'll discuss the geopolitical complexities, and the vital role you can play.

EFF has been on the front lines in Vienna, attending the negotiations and representing the interests of our members since the start, and we need your help. Your insights and experiences are crucial. Together we will review the text, identify new challenges that you may face so we can better understand the community concerns. Let's champion together a future where security research and human rights can thrive!

REFERENCES

<https://www.washingtonpost.com/politics/2023/04/28/perilous-path-new-cybercrime-treaty/>

1. <https://www.eff.org/issues/un-cybercrime-treaty>
2. <https://www.eff.org/pages/submissions>
3. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home
4. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/CND_2_-_21.04.2023.pdf
5. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fifth_session/main
6. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/CND_21.01.2023_-_Copy.pdf
7. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home
8. <https://www.euractiv.com/section/law-enforcement/news/west-clashes-with-china-russia-over-un-cybercrime-convention/>
9. <https://mediatalks.uol.com.br/2023/04/12/como-tratado-da-onu-sobre-crime-cibernetico-pode-ameacar-liberdade-de-express>
10. <https://www.washingtonpost.com/politics/2023/04/28/perilous-path-new-cybercrime-treaty/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Understand Your Trust Assumptions!

When: Friday, Aug 11, 14:50 - 15:20 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio:Carsten Schürmann

Carsten is a professor in computer science at the IT University of Copenhagen and heads the Center for Information Security and Trust. His research focuses on cyber and information security, with particular emphasis on election security. He consults with EMBs, governmental, and non-governmental organizations on requirements and quality assurance for election technologies. Carsten is an expert in voting machine security and demonstrated at DefCon 2017 vulnerabilities of the WinVote voting machine. He has conducted experiments with risk-limiting audits in Denmark in 2014. Carsten has participated as core team member (IT expert) in the Carter Center Mission to Kenya 2017 and 2022 and was part of the IFES Cyber Assessment Week in Ukraine 2018. He has also served as New Voting Technology Analyst for the OSCE Limited Election Observation Mission to the United States in 2018 and the Expert Election Mission to Estonia in 2019 and 2023. Prior to moving to Denmark, Carsten was a member of the computer science faculty at Yale University. He holds a PhD degree from Carnegie-Mellon University.

Twitter: [@CESchuermann](#)

Description:

Despite the best efforts of the election security community, things seem to go wrong in elections. Different software versions are blamed for the irregularities observed in Antrim county in 2021. An unreasonably slow update process of the online voter register in Estonia led to 63 voters casting incorrect electronic ballots that needed to be removed by court order from the digital ballot box. A slow voting machine repair process left thousands of voters waiting to cast their vote in the Philippines in 2022. The recently unsealed Halderman and Springall's Security Analysis of Georgia's ImageCast X Ballot Marking Devices shows vulnerabilities in hardware, software, and operations. In Professor Schürmann's presentation, he provides a different look at these failures through the lens of trust assumptions that help quantify interactions between election technologies and people. Being precise about trust assumptions helps us identify and fix vulnerabilities at design stage rather than on or after election day.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 21:00-00:59 PDT


Title: University of Advancing Technology, Pub Crawl

When: Saturday, Aug 12, 21:00 - 00:59 PDT

Where: Caesars Forum - Forum - 115-116 - [Map](#)

Description:

University of Advancing Technology will be hosting a pub in the DEF CON pub crawl. Grab a cocktail and meet the UAT staff!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Unlocking Doors from Half a Continent Away

When: Saturday, Aug 12, 10:30 - 11:15 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

Speakers: Sam Haskins, Trevor "t1v0" Stevado

SpeakerBio: Sam Haskins , Hacker at Loudmouth Security

Sam Haskins is an honors student at Carleton University, in Ottawa ON, and hacker at Loudmouth Security. Sam is a security researcher in their spare time with several CVEs to their name, with a keen interest in cryptography and RFID hacking.

SpeakerBio: Trevor "t1v0" Stevado , Founding Partner/Hacker at Loudmouth Security

Trevor Stevado is a security researcher and the founder of Loudmouth Security, with over 15 years of experience in the industry. In 2018, Trevor won a Black Badge in the IoT CTF at DEF CON 26, and since then he has been a regular contributor to IoT Village and is now one of the founders of the new Embedded Systems Village, where he continues to push the boundaries of embedded security research.

Description:

Contactless credentials have become increasingly popular for secure authentication and access control systems due to their convenience and efficiency. In this talk, we will discuss a specific weakness in the ISO 14443A protocol that enables replay attacks over moderate latency connections, leading to the potential for long-range relay attacks.

During the presentation, we will delve into the history of contactless credential attacks, how manufacturers have adapted, and discuss why we focused on a relay attack. We will provide an overview of the ISO 14443A protocol and explain how the relay attack is executed and the 'features' of the underlying protocol that make it possible. Finally, we will demonstrate and release a new tool to make this relay attack feasible with the Proxmark, as we attempt to unlock a door in Ottawa, ON with a card on-stage in Vegas.

In addition, we will discuss the response from HID Global following our responsible disclosure against their SEOS readers and suggest mitigations to prevent these attacks on your access control systems.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Unlocking hidden powers in Xtensa based Qualcomm Wifi chips

When: Sunday, Aug 13, 11:00 - 11:45 PDT

Where: Caesars Forum - Forum - 130-134 - Track 3 - [Map](#)

SpeakerBio: Daniel Wegemer , Hacker

Security Researcher interested in enabling new features in closed source firmware. Areas of interest are: Wifi, IoT and Automotive.

Description:

Wifi chips contain general purpose processors. Even though these are powerful processors, their firmware is closed source and does not allow modifications. This talk explores how the firmware of modern Xtensa based Qualcomm Wifi chips can be modified to allow extending its indented functionality. Such modifications can even be for example leveraged by security researchers to find vulnerabilities in an otherwise closed source Wifi code. During the talk we will also dive into the architecture of Qualcomms Wifi chips as well as the structure of the firmware used withing these chips. We will release a modified version of the Nexmon framework to enable patching of Xtensa based firmware and show all the steps involved to create such patches.

REFERENCES

- <http://problemkaputt.de/gbatek-dsi-atheros-wifi-bmi-bootloader-commands.htm> -
- <https://nstarke.github.io/firmware/wifi/linux/kernel/2021/08/11/dev-core-dump-and-firmware-images.html> -
- <https://sachin0x18.github.io/posts/demystifying-xtensa-isa/> - <https://nexmon.org>

[Return to Index](#) - Add to  - ics [Calendar](#) file

RCV - Saturday - 15:10-15:55 PDT

Title: Unlocking the Power of OWASP Amass: Introducing the Open Asset Model for Comprehensive Attack Surface Mapping

When: Saturday, Aug 12, 15:10 - 15:55 PDT


Where: LINQ - 3rd flr - Social B and C - Recon Village - [Map](#)

SpeakerBio: Jeff Foley

No BIO available

Twitter: [@jeff_foley](#)

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Unmanned Aerial Systems – Platform Security

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

Discover the exciting world of cybersecurity and unmanned aerial systems (UAS)! Learn how to safeguard UAS from all angles with a comprehensive platform security perspective.

Engage in some fun and challenging CTF adventures where you can put your skills to the test. See firsthand how your actions affect our UAS demonstrator. The UAS demonstrator contains all the sensors from our Mobile Optical Ultrasonic Sensor Explorer, or MOUSE for short. The MOUSE represents a small Unmanned Aircraft System (sUAS) comprising a pan/tilt object recognition camera, navigation camera, temperature & humidity sensor, ultrasonic sensor, and drive system powering four motors.

You won't need to worry about any complicated registration process; all you need is your personal laptop to join in the excitement. Earn enough points in the challenge, and you could be the proud owner of a CT Cubed SAO, a special prize while supplies last. Get ready to embark on this fascinating journey and prove your cybersecurity prowess!

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Sunday - 10:00-13:59 PDT

Title: Unmanned Aerial Systems – Platform Security

When: Sunday, Aug 13, 10:00 - 13:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

Discover the exciting world of cybersecurity and unmanned aerial systems (UAS)! Learn how to safeguard UAS from all angles with a comprehensive platform security perspective.

Engage in some fun and challenging CTF adventures where you can put your skills to the test. See firsthand how your actions affect our UAS demonstrator. The UAS demonstrator contains all the sensors from our Mobile Optical Ultrasonic Sensor Explorer, or MOUSE for short. The MOUSE represents a small Unmanned Aircraft System (sUAS) comprising a pan/tilt object recognition camera, navigation camera, temperature & humidity sensor, ultrasonic sensor, and drive system powering four motors.

You won't need to worry about any complicated registration process; all you need is your personal laptop to join in the excitement. Earn enough points in the challenge, and you could be the proud owner of a CT Cubed SAO, a special prize while supplies last. Get ready to embark on this fascinating journey and prove your cybersecurity prowess!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Unmanned Aerial Systems – Platform Security

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

Description:

Discover the exciting world of cybersecurity and unmanned aerial systems (UAS)! Learn how to safeguard UAS from all angles with a comprehensive platform security perspective.

Engage in some fun and challenging CTF adventures where you can put your skills to the test. See firsthand how your actions affect our UAS demonstrator. The UAS demonstrator contains all the sensors from our Mobile Optical Ultrasonic Sensor Explorer, or MOUSE for short. The MOUSE represents a small Unmanned Aircraft System (sUAS) comprising a pan/tilt object recognition camera, navigation camera, temperature & humidity sensor, ultrasonic sensor, and drive system powering four motors.

You won't need to worry about any complicated registration process; all you need is your personal laptop to join in the excitement. Earn enough points in the challenge, and you could be the proud owner of a CT Cubed SAO, a special prize while supplies last. Get ready to embark on this fascinating journey and prove your cybersecurity prowess!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Unveiling My Journey to My First CVE: A Tale of Discovery and Achievement

When: Saturday, Aug 12, 15:00 - 15:50 PDT

Where: Caesars Forum - Alliance - 301-304 - Blacks in Cyber Village - [Map](#)

SpeakerBio: Gaspard Baye

Gaspard Baye, a doctoral student and research assistant at the University of Massachusetts Dartmouth Cybersecurity Center, is a prominent figure in cybersecurity with expertise in vulnerability identification and security. With certifications like OSCP and CEH, Gaspard's leadership as an OWASP AppSec Global Reviewer and experience securing software applications and fintech/banking infrastructures highlights their capabilities. He also actively contribute to FOSS projects and advocate for cybersecurity awareness, training professionals globally and driving innovation in the industry.

Description:

In this captivating talk, I will share my personal journey of obtaining my first CVE (Common Vulnerabilities and Exposures) identification. I will take you through the thrilling experience of finding a security vulnerability, navigating the responsible disclosure process, and the ultimate achievement of receiving a CVE identifier.

During my talk, I will discuss the challenges I faced during my research, highlighting the technical skills and methodologies I employed to identify the vulnerability. I will delve into the intricacies of responsible disclosure, including engaging with vendors, coordinating patches, and collaborating with the security community.

Furthermore, I will reflect on the significance of receiving a CVE and how it has impacted my career and professional development. By attending my talk, you will gain insights into the rewards and growth opportunities that come with contributing to the cybersecurity community.

Join me for an inspiring journey as I share my experiences, provide valuable insights into obtaining a CVE, and showcase the personal and professional achievements it can bring.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Unveiling the Dual Nature of ChatGPT and Copilot in Secure Development

When: Sunday, Aug 13, 12:30 - 13:15 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

SpeakerBio: Kalyani Pawar

Kalyani is an AppSec engineer at heart, navigating the dynamic world of startups. Currently, she works at a Series F startup called Zipline, on securing their drones and infrastructure. You can find her playing with legos when not with her laptop.

Description:

In this session, attendees will explore the combined power of ChatGPT and Copilot to transform application security across the SDLC. Learn how these AI tools can streamline threat modeling, identify and remediate vulnerabilities, and educate developers to enforce secure coding practices. They will also discover how Copilot delivers real-time code suggestions that comply to secure coding rules and also generates security-focused test cases. Attendees will leave equipped with practical applications and insights into AI-driven application security, ready to integrate these tools into their security engineering practices with precaution.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Unveiling the Secrets: Breaking into AI/ML Security Bug Bounty Hunting

When: Friday, Aug 11, 16:00 - 16:55 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

Speakers: Chloé Messdaghi, Daniel Miessler, Joseph Thacker, Marcello "byt3bl33d3r" Salvati

SpeakerBio: Chloé Messdaghi

No BIO available

SpeakerBio: Daniel Miessler

No BIO available

SpeakerBio: Joseph Thacker

No BIO available

SpeakerBio: Marcello "byt3bl33d3r" Salvati , Hacker & Entrepreneur

Marcello Salvati (byt3bl33d3r) is a hacker & entrepreneur with over a decade of experience as an Offensive Security Researcher, Blue/Purple/Red Teamer and Open Source developer. Marcello is known for creating a number of Open Source tools such as CrackMapExec and weaponizing unorthodox programming languages for malware purposes.

Twitter: [@byt3bl33d3r](#)

Description:

As the world becomes increasingly dependent on artificial intelligence and machine learning systems, the need for robust ML security measures is more critical than ever. AI/ML security bug bounty hunting is a specialized field that focuses on identifying vulnerabilities and weaknesses in AI/ML systems to ensure their resilience against potential attacks. This panel talk aims to provide participants with an in-depth understanding of AI/ML security bug bounty hunting, including an introduction to the field, insights into vulnerabilities and attack surfaces specific to AI/ML systems, and a comprehensive overview of tools and techniques for effective bug hunting.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: US Cyber Policy 101

When: Friday, Aug 11, 10:00 - 11:50 PDT

Where: Caesars Forum - Summit - 221-222 - Policy Atrium - [Map](#)

Speakers:Harley Geiger,Lauren Zabierek,Lindsey Forson,Michaela Lee,Suzanne Schwartz

SpeakerBio:Harley Geiger , Counsel at Venable LLP

Harley Geiger is Counsel and Senior Director at Venable, LLP, where he leads the Security Research Legal Defense Fund and the Hacking Policy Council and counsels clients on a variety of cybersecurity issues. Prior to this, Geiger was Senior Director for Public Policy at Rapid7, where he worked to expand adoption of vulnerability disclosure and legal protections for security research. Geiger also worked as Senior Legislative Counsel in the U.S. House of Representatives, where he drafted Aaron's Law, and served as Advocacy Director at the Center for Democracy & Technology.

Twitter: [@HarleyGeiger](#)

SpeakerBio:Lauren Zabierek , Senior Policy Advisor in the Cybersecurity Division at Cybersecurity and Infrastructure Security Agency (CISA)

Lauren Zabierek is a Senior Policy Advisor in the Cybersecurity Division at CISA. Previously, she served as the Executive Director of the Cyber Project at the Harvard Kennedy School's Belfer Center, where she ran a policy-relevant research program and managed students and nonresident fellows. She also served as the Acting Executive Director of the Belfer Center in her final semester there. She came to that role as a 2019 graduate of the Kenney School's midcareer MPA program. Prior to graduate school, she was an early member of the cybersecurity firm Recorded Future, having established and managed their public sector team. She also served as a civilian intelligence analyst at the National Geospatial Intelligence Agency with multiple deployments to Afghanistan, and served as a US Air Force intelligence officer at the beginning of her career. Lauren is also the co-founder of the online social media movement, #ShareTheMicInCyber. She is a mentor with Girl Security, a fellow at the National Security Institute at George Mason University, and a fellow at New America.

SpeakerBio:Lindsey Forson , Deputy Executive Director at National Association of Secretaries of State

Lindsey Forson has worked at the intersection of cybersecurity and public policy for the past five years. She is dedicated to fostering relationships between NASS members and collaborators in the cybersecurity space.

SpeakerBio:Michaela Lee , Director for Strategy and Research at The Office of National Cyber Director (ONCD)

Michaela Lee is the Director for Strategy and Research at the Office of the National Cyber Director. Prior to her present role, Michaela worked at the intersection of geopolitical risk and cybersecurity at the Krebs Stamos Group. Her background is in emerging technologies and human rights, having covered issues of artificial intelligence, privacy, and platform governance at nonprofit BSR (Business for Social Responsibility). She is a graduate of the University of California, Davis and the Harvard Kennedy School.

SpeakerBio:Suzanne Schwartz , Director of the Office of Strategic Partnerships and Technology Innovation (OST) at FDA's Center for Devices and Radiological Health (CDRH)MD

Suzanne B. Schwartz, MD, MBA is the Director of the Office of Strategic Partnerships and Technology Innovation (OST) at FDA's Center for Devices and Radiological Health (CDRH).

Suzanne's work in medical device cybersecurity includes policy development, educating, outreach, partnering and coalition-building within the Healthcare and Public Health Sector (HPH) as well as fostering collaborations and coordinating incident response across other government agencies and the private sector. Suzanne has been recognized for Excellence in Innovation at FDA's Women's History Month for her work in Medical Device Cybersecurity. She also received the 2021 Routhy Award from the H-ISAC for her leadership in cybersecurity in healthcare, especially during the COVID-19 pandemic. Together with Health Canada, Suzanne has represented FDA in co-chairing the International Medical Device Regulators Forum (IMDRF) Work Group on Medical Device Cybersecurity leading to its first international guidance publication in March 2020 and two subsequent guidance publications - - one on software bill of materials and one on cybersecurity management of legacy medical devices. She has additionally served as co-chair of the Government Coordinating Council

(GCC) for the HPH Critical Infrastructure Sector, focusing on the sector's healthcare cybersecurity initiatives.

Suzanne earned an MD from Albert Einstein College of Medicine; an executive MBA from NYU Stern School of Business, completed Cohort X of the National Preparedness Leadership Initiative – Harvard School of Public Health & Harvard Kennedy School of Government executive education, and earned in September 2018 a certificate of mastery for completion of requirements at the Federal Executive Institute – Leadership for a Democratic Society.

Description:

This is your CliffsNotes on what's happening in US cyber policy. Whether you're completely new to policy discussions as a whole, more used to following policy in other countries, or just feeling a little out of date, this session will help you get up to speed with the main US cyber policy focus areas and players.

The session will start with an overview of the current themes and topics being explored by US policymakers, provided by policy expert and leader, Harley Geiger. He will provide insight on the status of various initiatives and what is likely to move forward through the year.

This will be followed by a discussion with representatives from different parts of the US government currently working on setting US cyber policy. Each will explain what their agency does, how it fits in the ecosystem and partners with the other agencies, what it's working on for 2023-24 and how people can interact with them.

This will be followed by audience Q&A so you can better explore the information provided and find out the status of the issues you care about most. This session creates a baseline for the other Policy @ DEF CON content.

This is a double length session lasting 110 minutes.

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Saturday - 12:20-12:50 PDT

Title: US private elections: the easy way in for foreign adversaries.

When: Saturday, Aug 12, 12:20 - 12:50 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio: Scheme

No BIO available

Description:

In 2010, the FBI arrested a group of 10 Russian spies that were posing as Americans to gather intelligence. They spent decades building legitimacy in the US all towards the goal of getting jobs at big banks, consulting firms and tech companies.

These Russian spies didn't know it back then, but there was a shortcut to influential positions in US society: becoming an elected official of a private organization.

Private elections are elections for leadership positions of organizations like unions, NGOs, universities, boards, pension funds, etc.

For a foreign adversary, private elections are a goldmine of powerful positions at the state and national level. Unlike civil elections, these elections have no paper trail, often little oversight and minimal technical safeguards against vote tampering.

And as we'll see in this talk: they're highly hackable.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: USBvalve - Expose USB activity on the fly

When: Saturday, Aug 12, 10:00 - 11:55 PDT

Where: Caesars Forum - Unity Boardroom - Demo Labs - [Map](#)

SpeakerBio: Cesare Pizzi

Cesare Pizzi is a Security Researcher, Analyst, and Technology Enthusiast at Sorint.lab. He develops software and hardware, and tries to share this with the community. Mainly focused on low level programming, he developed a lot of OpenSource software, sometimes hardware related and sometimes not. Doing a lot of reverse engineering too. He likes to share his job when possible (at Defcon, Insomni'hack, Nullcon, etc). Contributor of several OS Security project (Volatility, OpenCanary, PersistenceSniper, Speakeasy, CETUS, etc) and CTF player.

Description:

USB spreading malware is still a concern today. Over the past few months, we have witnessed an increase in malicious software exploiting USB drives to bypass security measures, even in air-gapped systems. Whenever we connect our USB drive to an "untrusted" system, numerous doubts arise: what happens behind the scenes? Is something accessing, modifying, or encrypting our files? This is where USBvalve comes in. It is an affordable dongle, built using readily available hardware, designed to reveal the true activities occurring when a USB drive is connected to a system. It can also be used to check for "BADUSB" (HID) on USB keys before inserting them into our own systems. The best part is that it's as compact as a keychain, making it convenient to carry with us at all times!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Using an SBC for ham radio digital modes that isn't a raspberry pi

When: Saturday, Aug 12, 13:00 - 13:59 PDT


Where: Flamingo - Virginia City - Ham Radio Village - [Map](#)

SpeakerBio:Jon Marler

No BIO available

Description:

Amateur radio operator Jon Marler, callsign K4CHN, presents a discussion about how to use an SBC for ham radio digital modes in a world without the raspberry pi. There are hundreds of other options now, but which of those meet these requirements: Easy to obtain, cheap, runs Linux, and can run popular ham radio digital mode software. Jon will present his findings and show you how to build out an SBC that can get you on the air, without having to beg, borrow, or steal a raspberry pi.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Vacuum Robot Hacking

When: Friday, Aug 11, 14:00 - 15:55 PDT

Where: Caesars Forum - Unity Boardroom - Demo Labs - [Map](#)

SpeakerBio:Dennis Giese , Hacker

Dennis Giese is currently a PhD student at Northeastern University and focuses on the security and privacy of IoT devices.

While being interested in physical security and lockpicking, he enjoys applied research and reverse engineering malware and all kinds of devices.

His most known projects are the documentation and hacking of various vacuum robots. His current vacuum robot army consists of over 45 different models from various vendors.

Twitter: [@dgi_DE](#)

Description:

In this demo I will show you can root various models of vacuum robots and disconnect them from the cloud. You have the chance to play around yourself with the tools and the rooted robots yourself. Learn why you should not trust your robots cameras and microphones. Pick up a free PCB that allows you to root your vacuum robot easily.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Vacuum robot security and privacy - prevent your robot from sucking your data

When: Sunday, Aug 13, 10:00 - 10:45 PDT

Where: Caesars Forum - Academy - 407-410 - Track 4 - [Map](#)

SpeakerBio:Dennis Giese , Hacker

Dennis Giese is currently a PhD student at Northeastern University and focuses on the security and privacy of IoT devices.

While being interested in physical security and lockpicking, he enjoys applied research and reverse engineering malware and all kinds of devices.

His most known projects are the documentation and hacking of various vacuum robots. His current vacuum robot army consists of over 45 different models from various vendors.

Twitter: [@dgi_DE](#)

Description:

Exactly 5 years ago we were presenting ways to hack and root vacuum robots. Since then, many things have changed. Back then we were looking into ways to use the robots' "dumb" sensors to spy on the user (e.g. by using the ultrasonic sensor). But all our predictions were exceeded by the reality: today's robots bring multiple cameras and microphones with them. AI is used to detect objects and rooms. But can it be trusted? Where will pictures of your cat end up?

In this talk we will look at the security and privacy of current devices. We will show that their flaws pose a huge privacy risk and that certification of devices cannot be trusted. Not to worry, though - we will also show you how to protect yourself (and your data) from your robot friends.

You will learn on how you can get root access to current flagship models of 4 different vendors. Come with us on a journey of having fun hacking interesting devices while preventing them from breaching your privacy. We will also discuss the risks of used devices, for both old and new users.

Finally, we will talk about the challenges of documenting vacuum robots and developing custom software for them. While our primary goal is to disconnect the robots from the cloud, it is also for users to repair their devices - pwning to own in a wholesome way.

REFERENCES:

Robots with lasers and cameras (but no security): Liberating your vacuum from the cloud
https://dontvacuum.me/talks/DEFCON29/DEFCON29-Robots_with_lasers_and_cameras.html

Unleash your smart-home devices: Vacuum Cleaning Robot Hacking (34C3)
<https://dontvacuum.me/talks/34c3-2017/34c3.html>

Having fun with IoT: Reverse Engineering and Hacking of Xiaomi IoT Devices
https://dontvacuum.me/talks/DEFCON26/DEFCON26-Having_fun_with_IoT-Xiaomi.html

<https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy>

https://linux-sunxi.org/Main_Page

Return to Index - Add to  - ics [Calendar](#) file

APV - Friday - 11:00-12:59 PDT

Title: vAPI : Vulnerable Adversely Programmed Interface

When: Friday, Aug 11, 11:00 - 12:59 PDT

Where: Flamingo - Savoy - AppSec Village - Pod 2 - [Map](#)

SpeakerBio: Tushar Kulkarni

Tushar Kulkarni is a graduate student in Secure Computing at Indiana University Bloomington. He has a interest in Web Application Security and has presented before at various conferences like Blackhat , HITB, OWASP AppSecDays, APISecure
Twitter: [@vk_tushar](#)

Description:

vAPI is a Vulnerable Interface in a Lab like environment that mimics the scenarios from OWASP API Top 10 and helps the user understand and exploit the vulnerabilities according to OWASP API Top 10 2019. Apart from that, the lab consists some more exercises/challenges related to advanced topics related to Authorization and Access Control.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: VDA Shenanigans: Attacking & Defending the Truck Part that Gets Left Behind

When: Saturday, Aug 12, 10:00 - 10:25 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

Speakers: Alex Reuter, Wyatt Ford

SpeakerBio: Alex Reuter , Red Balloon Security


Alex Reuter is a security researcher at Red Balloon Security. When he isn't hacking low level devices, you can probably find him outside: rock climbing, surfing, hiking, or scheming scenic shenanigans.

SpeakerBio: Wyatt Ford , Red Balloon Security

Wyatt Ford is a senior software engineer and engineering manager at Red Balloon Security and a core maintainer of OFRAK.

Description:

Vehicle Diagnostic Adapters (VDA) do a lot! They plug into automobiles, update ECU firmware, and pull diagnostic information. Despite their usefulness and high level of access, they get left behind: in maintenance garages with insecure update mechanisms, in threat models and our hearts. In this presentation we will go through some of our own offensive research into VDAs, and our efforts in decreasing their attack surfaces. We'll also share how we turned this research into four problems from the Defcon 30 CHV CTF.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Veilid

When: Saturday, Aug 12, 10:00 - 11:55 PDT

Where: Caesars Forum - Committee Boardroom - Demo Labs - [Map](#)

Speakers:Deth Veggie,TC Johnson

SpeakerBio:Deth Veggie

The Deth Vegetable: cDc member since December 1990. Minister of Propaganda If everything is to be believed, he has alternately been a Special Forces Commando, Mexican wrestler, comicbook villain, bodyguard to Mr. T, designer drug manufacturer, electronics wizard, and used tire recycler.

SpeakerBio:TC Johnson

TC: Rubber Duck to the actual developer of Veilid. Here to get you started on the future we were promised -- communication free of a profit motive, free of corporate overlords, and free of other intrusive eyeballs.

Description:

Veilid is a new, distributed communication protocol developed by Cult of the Dead Cow's Dildog (of BO2K fame). This p2p, E2EE, distributed protocol is being released at Defcon 31, fully open source, and with an example app called Veilid Chat. These demos will cover setting up an identity, connecting to others, deploying heavy nodes to support the network, and contributing to the project.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Saturday - 10:00-17:59 PDT

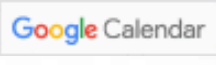
Title: venator aurum - A Treasure Hunt

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Through interfacing with reality you are defining that reality. Rethink your senses and test your limits. Solve the five layers and discover a hidden treasure. Each layer yields its own reward, but few will make it to the end of the hunt. For each of your senses, you will need to set aside preconceptions and look to the underlying patterns within the data.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Sunday - 10:00-11:59 PDT


Title: venator aurum - A Treasure Hunt

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Through interfacing with reality you are defining that reality. Rethink your senses and test your limits. Solve the five layers and discover a hidden treasure. Each layer yields its own reward, but few will make it to the end of the hunt. For each of your senses, you will need to set aside preconceptions and look to the underlying patterns within the data.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CON - Friday - 10:00-17:59 PDT

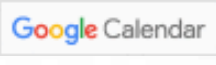
Title: venator aurum - A Treasure Hunt

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - Contest Area - [Map](#)

Description:

Through interfacing with reality you are defining that reality. Rethink your senses and test your limits. Solve the five layers and discover a hidden treasure. Each layer yields its own reward, but few will make it to the end of the hunt. For each of your senses, you will need to set aside preconceptions and look to the underlying patterns within the data.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Sunday - 10:00-15:59 PDT

Title: Vendor Area Open

When: Sunday, Aug 13, 10:00 - 15:59 PDT


Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description:

This is when you can go visit our awesome vendors.

We don't know whether they will be accepting cash or cards. That's up to each vendor, and we do not have a list.

We also don't know if/when vendors will sell out of anything they may be selling.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Saturday - 10:00-17:59 PDT

Title: Vendor Area Open

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description:

This is when you can go visit our awesome vendors.

We don't know whether they will be accepting cash or cards. That's up to each vendor, and we do not have a list.

We also don't know if/when vendors will sell out of anything they may be selling.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Vendor Area Open

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Alliance - 305-306 - Vendors - [Map](#)

Description:

This is when you can go visit our awesome vendors.

We don't know whether they will be accepting cash or cards. That's up to each vendor, and we do not have a list.

We also don't know if/when vendors will sell out of anything they may be selling.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: VetCon

When: Saturday, Aug 12, 21:00 - 01:59 PDT

Where: Caesars Forum - Forum - 109-110, 139 - [Map](#)

Description:

Attention all Veterans, Cyber Warriors, AI buffs, and Skynet skeptics! VETCON is calling you to action!

Join us on August 12, 2023, at Caesars Forum Rooms 105,136 in Las Vegas for a mission of a different kind. Transition into the cyber frontline, network with comrades-in-arms, and engage in some good old military humor that even a drill sergeant can't resist!

Navy, it's after you've mistaken the hotel pool for the high seas. Marines, we'll see you post-crayon snack but pre-attempting to conquer the casino. Air Force, try to fit us in between your gourmet meals and five-star luxuries. Army, no amount of camouflage can hide your poker face!

Coast Guard, be prepared to rescue any Navy personnel lost en route. And Space Force, we promise the gravity of the situation isn't too intense.

For our veterans and active-duty heroes looking to transition into cybersecurity, this is your chance to become the most unique people of the cyber world. For the general public, come meet the superstars ready to defend your cyberspace!

This mission is all fun, games, and camaraderie until someone loses at poker. So, gear up, report for duty, and let's show AI how the military does humor! ~

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Video-based Cryptanalysis: Extracting Secret Keys from Power LEDs of Various Non-compromised Devices Using a Video Camera

When: Saturday, Aug 12, 12:30 - 13:15 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

Speakers: Ben Nassi, Ofek Vayner

SpeakerBio: Ben Nassi, Postdoctoral Researcher at Cornell Tech

Dr. Ben Nassi is a postdoctoral researcher at Cornell Tech. He is interested in building robust systems and investigates the security and privacy of cyber-physical systems and hardware/devices in the topics of side-channel attacks and AI security using signal processing and machine learning techniques. His research has been presented at top academic conferences, published in journals and Magazines, and covered by international media. Ben has spoken at prestigious industrial conferences (Black Hat Asia and USA, RSAC USA, AI Week, CodeBlue, SecTor, and CyberTech) and he serves as a PC member in ACM CCS (22 and 23) and BlackHat Asia (22 and 23). His research entitled him to two nominations for the Pwnie Award.

Twitter: [@ben_nassi](#)

SpeakerBio: Ofek Vayner, M.Sc. Student at Ben-Gurion University of the Negev

Ofek Vayner is an M.Sc student at Ben-Gurion University of the Negev and a security researcher at BGU's Cyber Security Research Center. He holds a B.Sc. degree from the Department of Electrical Engineering at Ben-Gurion University of the Negev. His primary research interests are side-channel attacks and cryptanalysis.

Description:

In this talk, we present video-based cryptanalysis, a new method to recover secret keys from a non-compromised device by analyzing video footage obtained from a device's power LED. We show that cryptographic computations performed by the device's CPU change the power consumption of the device which affects the brightness/color of the device's power LED. The changes in the brightness can be detected at a sufficient sampling rate for cryptanalysis by obtaining video footage from a device's power LED (by filling the frame with the LED) and exploiting the video camera's rolling shutter, to increase the sampling rate by three orders of magnitude. The frames of the video footage are analyzed in the RGB space, and the RGB values are used to recover the secret key. We demonstrate the recovery of: (1) a 256-bit ECDSA key from a smartcard using video footage obtained from the power LED of the smartcard reader via a hijacked Internet-connected security camera located 16 meters away from the smartcard reader, and (2) a 378-bit SIKE key from a Samsung Galaxy S8 using video footage obtained from the power LED of Logitech Z120 USB speakers (that were connected to the same USB Hub of the Galaxy S8) via iPhone 12.

We discuss countermeasures, limitations, and the future of video-based cryptanalysis.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Virtual Hospital in Space

When: Saturday, Aug 12, 00:00 - 00:59 PDT

Where: Virtual

SpeakerBio:Aswin Reji

No BIO available

Description:

This talk is being pre-recorded and will be released on YouTube. Once it is available, a link to it will appear here.

Update 2023-08-11 06:30: Biohacking Village indicates that the pre-recorded talks have not yet been received. Once received, these talks will be posted to the [Biohacking Village YouTube Channel](<https://www.youtube.com/@BiohackingVillage/about>). Please note that this may be as late as a week or two after DC31.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Virtual Reality/Augmented Reality: What’s missing from the pie? When data privacy and security measures aren’t “baked” in from the beginning

When: Saturday, Aug 12, 17:10 - 17:59 PDT

Where: Flamingo - Laughlin I,II,III - Biohacking Village - [Map](#)

Speakers:LaTica Hammond,Lola Ajayi,Rian Phelps

SpeakerBio:LaTica Hammond

LaTica Hammond, MS, is a servant leader, 23-year Navy veteran and cybersecurity/space intelligence professional. She has worked in information and privacy protection advising DoD on innovative solutions to secure freedom of access and the secure flow of information within cyber and space domains.

SpeakerBio:Lola Ajayi

Lola Ajayi, MS, MBA, has over 15 years of policy and regulatory experience within the healthcare industry. Working in an industry where her colleagues did not look like her, she founded BaraLaj coaching, to empower women with the tools and skills to be fully in control of their careers.

SpeakerBio:Rian Phelps

Rian Phelps, MSC, is a passionate lifelong educator with over 10 years experience as an instructional designer and eLearning consultant. She is also a Navy veteran with degrees in psychology and neuroscience.

Description:

Virtual reality and augmented reality are technologies that are the next frontier in healthcare and providing patient care. These technologies were originally developed for recreational use, specifically for gaming and recreation, but have quickly shown utility in advancing the efficiency and accuracy of providing patient care. This now leads to a host of challenges related to data privacy and security, as privacy-by-design was not a designing principle for these technologies. These tenants however, are necessary as patient data include Protected Health Information and Personal Identifying Information (PHI/PII) that would be financially lucrative and useful to a hacker. So now that these data privacy and security principles were not “baked in” to technology originally, how does one go about ensuring maximum security after the fact? What can be done moving forward to ensure maximum flexibility for the use of technology with the appropriate data and privacy security measures “baked in”?

C.A.R.B. is a joint collaboration between the Black women founders of Creative Riot (Rian), Aurora (Jillian), Ray-Lynn Group (LaTica), and Baralaj (Lola).

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Visual Studio Code is why I have (Workspace) Trust issues

When: Friday, Aug 11, 16:00 - 16:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

Speakers: Paul Gerste, Thomas Chauchefoin

SpeakerBio: Paul Gerste , Vulnerability Researcher at Sonar

Paul Gerste (@pspaul95) is a Vulnerability Researcher in the Sonar R&D team. In the last months, he has been hunting bugs in popular JavaScript and TypeScript applications, yielding critical vulnerabilities in projects such as Rocket.Chat, NodeBB, and Blitz.js. Paul has also been a CTF player and organizer for some years and loves to hack all web-related things.

Twitter: [@pspaul95](#)

SpeakerBio: Thomas Chauchefoin , Vulnerability Researcher at Sonar

Thomas Chauchefoin (@swaps) is a Vulnerability Researcher in the Sonar R&D team. With a strong background in offensive security, he helps uncover and responsibly disclose 0-days in major open-source software. He also participated in competitions like Pwn2Own or Hack-a-Sat and was nominated for two Pwnies Awards for his research on PHP supply chain security.

Description:

Developers are threat actors' targets of choice because of their access to business-critical services. After compromising a single developer, they could push code changes or obtain sensitive information. For instance, a recent campaign attributed to North Korea set up social network profiles to social engineer and infect prominent figures of the developer community with malicious Visual Studio projects and browser exploits.

At the same time, modern development tools offer increasingly advanced features and deep integration with ecosystems, sometimes at the cost of basic security measures. Code editors tried to counterbalance it by introducing new lines of defense (e.g., "Workspace Trust"), leading to a cat-and-mouse game to restrict access while keeping most features available by default.

In this talk, we present the state of the art of Visual Studio Code's security. We go in-depth into its attack surface, how its extensions work, and the technical details of two vulnerabilities we found in Visual Studio Code. These findings, CVE-2021-43891 and CVE-2022-30129, led to a \$30,000 bounty with an unexpected twist. We also present 1-days discovered by other researchers to develop the audience's intuition. These concepts apply to most IDEs of the market so everybody will now think twice before opening third-party code!

REFERENCES:

<https://blog.electrovolt.io/posts/vscode-rce/> <https://www.sonarsource.com/blog/securing-developer-tools-git-integrations/>
<https://www.sonarsource.com/blog/securing-developer-tools-argument-injection-in-vscode/>
<https://blog.doyensec.com/2022/10/27/jupyter-vscode.html> <https://iwantmore.pizza/posts/cve-2019-1414.html>
https://github.com/justinsteven/advisories/blob/master/2017_visual_studio_code_workspace_settings_code_execution.md
https://github.com/doyensec/VSCoDe_PoC_Oct2019 <https://github.com/microsoft/vscode/issues/107951>
<https://www.youtube.com/watch?v=Olq6XnZ4Pwo>
<https://github.com/google/security-research/security/advisories/GHSA-pw56-c55x-cm9m>

Return to Index - Add to  - ics [Calendar](#) file

Title: VOTEC Corporation

When: Saturday, Aug 12, 11:30 - 11:59 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio:John Medcalf

John Medcalf founded VOTEC Corporation (fka Proform Software) in 1979 and serves as the company's Chief Executive Officer. In addition to his executive duties, John provides design guidance for the company's accessible elections initiative. John's accomplishments in the election technology space include mini-computer and PC-based ballot counting solutions, PostScript ballot printing for punch card and optical scan ballots, and the creation of signature digitizing hardware and software. John is most pleased to have learned early on that customers wanted VOTEC staff to speak their language. Thus the many hires from elections offices.

Description:

Join the CEO of VOTEC Corporation, our special guest John Medcalf, for a first of its kind presentation where an actual technology systems provider is exposing their technology to public scrutiny at the Voting Village. This is happening for the first time ever at the Voting Village and will be an enriching experience for attendees. Mr. Medcalf will make himself available after the presentation for any questions and inquiries from the audience. We are so excited to have him and cannot wait to examine the systems he is bringing to DEF CON. Please join us for this exciting event.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: VOTEC Corporation

When: Friday, Aug 11, 11:30 - 11:59 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio: John Medcalf

John Medcalf founded VOTEC Corporation (fka Proform Software) in 1979 and serves as the company's Chief Executive Officer. In addition to his executive duties, John provides design guidance for the company's accessible elections initiative. John's accomplishments in the election technology space include mini-computer and PC-based ballot counting solutions, PostScript ballot printing for punch card and optical scan ballots, and the creation of signature digitizing hardware and software. John is most pleased to have learned early on that customers wanted VOTEC staff to speak their language. Thus the many hires from elections offices.

Description:

Join the CEO of VOTEC Corporation, our special guest John Medcalf, for a first of its kind presentation where an actual technology systems provider is exposing their technology to public scrutiny at the Voting Village. This is happening for the first time ever at the Voting Village and will be an enriching experience for attendees. Mr. Medcalf will make himself available after the presentation for any questions and inquiries from the audience. We are so excited to have him and cannot wait to examine the systems he is bringing to DEF CON. Please join us for this exciting event.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Voting Village Opening Remarks

When: Friday, Aug 11, 10:00 - 10:30 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

Speakers: Catherine Terranova, Harri Hursti, Matt Blaze

SpeakerBio: Catherine Terranova

Catherine Terranova is the Vice President of Operations at the Election Integrity Foundation, the 501(c)(3) organization founded by world renown ethical hacker Harri Hursti. She co-organized the Voting Village at DEFCON 29, DEFCON 30, and DEFCON 31. She is a Columbia University alumna and researcher whose current focus is on cyber security and election integrity with an emphasis on data and voting rights.

Twitter: [@catlovesvoting](#)

SpeakerBio: Harri Hursti

Harri Hursti, a world renowned data security expert and internet visionary is the Founder of the 501(c)(3) organization the Election Integrity Foundation as well as an original co-Founder of the Voting Village. Featured in two Emmy nominated documentaries, Mr. Hursti is famously known for the Hursti Hacks, where he demonstrated how to successfully alter final voting results on the Diebold Election Systems voting machines.

Twitter: [@harrihursti](#)

SpeakerBio: Matt Blaze

Matt Blaze is one of the original co-founders of the Voting Village and is currently the McDevitt Professor of Computer Science and Law at Georgetown University. He has over two decades of experience with election system security, and his current research focuses on security, privacy, and robustness in large scale systems with an emphasis on problems at the intersection of technology and public policy.

Twitter: [@mattblaze](#)

Description:

Two of the original co-founders of the Voting Village along with the current co-organizer will provide opening remarks.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Voting Village Opening Remarks

When: Saturday, Aug 12, 10:00 - 10:30 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

Speakers: Catherine Terranova, Harri Hursti, Matt Blaze

SpeakerBio: Catherine Terranova

Catherine Terranova is the Vice President of Operations at the Election Integrity Foundation, the 501(c)(3) organization founded by world renown ethical hacker Harri Hursti. She co-organized the Voting Village at DEFCON 29, DEFCON 30, and DEFCON 31. She is a Columbia University alumna and researcher whose current focus is on cyber security and election integrity with an emphasis on data and voting rights.

Twitter: [@catlovesvoting](#)

SpeakerBio: Harri Hursti

Harri Hursti, a world renowned data security expert and internet visionary is the Founder of the 501(c)(3) organization the Election Integrity Foundation as well as an original co-Founder of the Voting Village. Featured in two Emmy nominated documentaries, Mr. Hursti is famously known for the Hursti Hacks, where he demonstrated how to successfully alter final voting results on the Diebold Election Systems voting machines.

Twitter: [@harrihursti](#)

SpeakerBio: Matt Blaze

Matt Blaze is one of the original co-founders of the Voting Village and is currently the McDevitt Professor of Computer Science and Law at Georgetown University. He has over two decades of experience with election system security, and his current research focuses on security, privacy, and robustness in large scale systems with an emphasis on problems at the intersection of technology and public policy.

Twitter: [@mattblaze](#)

Description:

Two of the original co-founders of the Voting Village along with the current co-organizer will provide opening remarks.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Sunday - 10:30-10:59 PDT

Title: Vulnerability instead of security: How we managed to hack a PSIM system

When: Sunday, Aug 13, 10:30 - 10:59 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio:Lukas Sokefeld

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Vulnerable by Design: Unguard, The Insecure Cloud-Native Twitter Clone

When: Friday, Aug 11, 10:00 - 11:55 PDT

Where: Caesars Forum - Accord Boardroom - Demo Labs - [Map](#)

Speakers: Christoph Wedenig, Simon Ammer

SpeakerBio: Christoph Wedenig


Christoph always loved to interact with software systems, even more so in unintended ways. He studied Applied Computer Science in the south of Austria, focusing on the detection of server-side request forgery in his Master's thesis. As a demo environment for this thesis, he created a small distributed application called "Vogelgrippe" which was then later extended for various other use cases until being renamed to Unguard and finally gifted to the community as an Open-Source playground. Currently, he is working in the Application security team at Dynatrace, where he helps build a wide suite of security-related software.

SpeakerBio: Simon Ammer

Simon's interest in cybersecurity was sparked after listening to the Darknet Diaries podcast, which led him to pursue a career in this fascinating field. He studied Software Engineering and Mobile Computing in Austria, focusing on enhancing web vulnerability scanner reports for his Master's thesis. Driven by his passion for cybersecurity, Simon decided to further expand his knowledge by enrolling in another Master's program specializing in Artificial Intelligence. Currently, he holds the position of Research Software Engineer in the cloud-native security team at Dynatrace. There, he leverages his knowledge to employ AI to improve security measures and safeguard digital infrastructures.

Description:

Unguard is an intentionally insecure, cloud-native microservices demo application that serves as a playground for cybersecurity enthusiasts to sharpen their skills and for cybersecurity companies to test their software. Designed to mimic a web-based Twitter clone, the platform offers user registration, login, content posting, and social interactions, all with a wide variety of exploitable vulnerabilities. Featuring a wide range of security flaws, including SSRF, Command/SQL Injection, Log4Shell, and Spring4Shell, Unguard challenges security professionals, developers, and students to identify, exploit, and understand these weaknesses. Simultaneously, the platform showcases deceptive elements, such as phony ads and profile management options, which further enhance the real-world experience offered by the demo.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: WAF: Making a Problematic Security Tool Suck Less

When: Sunday, Aug 13, 09:30 - 10:15 PDT

Where: Flamingo - Savoy - AppSec Village - Main Stage - [Map](#)

Speakers:Emile Spir,Emmanuelle Lejeail

SpeakerBio:Emile Spir

Build, operate, fight WAF & RASP solutions. Then jump off planes. Ex-Sqreen, now Datadog.

Twitter: [@Taiki__San](#)

SpeakerBio:Emmanuelle Lejeail

Emmanuelle is a data and security enthusiast. She started her career working on machine learning models for 4 years. Last year, she joined Datadog to work on application security. Since then she has tried improving WAF rules thanks to AI.

Twitter: [@ManuLejeail](#)

Description:

The WAF. The world's most beloved security tool after antiviruses and password complexity requirements. The speakers spent the last five years working on making them suck less and operating one at a global scale. By sharing war stories, mistakes and discoveries, we will provide the audience with tools and strategies to make their WAF experience more palatable. Whether you're a WAF operator, user or vendor, you will get actionable takeaways from our ordeal^W^W^W experience.

First, we will share our learnings on creating a generic set of rules with low noise. This will go from a better understanding of real world attacks to common false positive patterns. We will also cover strategies to catch issues in rules at scale and expand the coverage of new unknown attacks.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Sunday - 09:00-12:59 PDT

Title: Wall of Sheep

When: Sunday, Aug 13, 09:00 - 12:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

We passively monitor the #DEFCON network looking for insecure network traffic. Drop by and see just how easy it can be!

We strive to educate the “sheep” we catch: a friendly reminder that security matters.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Friday - 09:00-17:59 PDT


Title: Wall of Sheep

When: Friday, Aug 11, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

We passively monitor the #DEFCON network looking for insecure network traffic. Drop by and see just how easy it can be! We strive to educate the “sheep” we catch: a friendly reminder that security matters.

[Return to Index](#) - Add to  - ics [Calendar](#) file

PHV - Saturday - 09:00-17:59 PDT


Title: Wall of Sheep

When: Saturday, Aug 12, 09:00 - 17:59 PDT

Where: Caesars Forum - Academy - 411-414 - Packet Hacking Village - [Map](#)

Description:

We passively monitor the #DEFCON network looking for insecure network traffic. Drop by and see just how easy it can be! We strive to educate the “sheep” we catch: a friendly reminder that security matters.

[Return to Index](#) - Add to  - ics [Calendar](#) file

RFV - Sunday - 11:00-12:59 PDT

Title: War Driver Meetup

When: Sunday, Aug 13, 11:00 - 12:59 PDT

Where: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

SpeakerBio:RF Village Staff

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

DC - Sunday - 10:00-11:59 PDT


Title: War Stories Off The Record AMA

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Harrah's - Nevada Ballroom - Lake Tahoe & Reno - War Stories - Off the Record - [Map](#)

Description:

A series of panels and talks that are not recorded and off the record, the AMA's are meant to encourage thought provoking questions from the audience.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Wardriving 102: Moving Beyond the Wigle App

When: Saturday, Aug 12, 14:00 - 14:59 PDT

Where: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

SpeakerBio:bkobe

bkobe is a formally trained electrical engineer who focuses on all things analog/digital circuits to microcontroller/digital signal processors and software defined radios. Background in hardware printed circuit board design, software/firmware development, radios and repeaters (commercial site installation and maintenance), and recently radio mesh networks. Enjoys the camaraderie in this community with common passions, and the sharing of ideas and knowledge. Member of the Hard Hat Brigade.

Twitter: [@@kobeski1906](#)

Description:

A summary of wardriving beyond the wigle app (hardware rigs) will be discussed with the main example/inspiration documenting the process of the WigleBottleV2 build. Topics include (chronologically): a short history of wardriving and what it is, the sub-genre of hardware rig building (and introduction of design specs), the WigleBottleV2 design goal, and some “gotchas” (power/redundant power, single board computer selection (Pi4 in V1 to the Pi3B in V2 and why the downgrade), GPS receivers (tie in/link to wytshadow’s GPS talk), and general clock timing). In selecting the single board computer (which dictates power/redundant power options), a side story will be discussed on the heat produced, and what to think about for case design. The V1 bottle used a Pi4, however uses 1W more power than the Pi3B, also radiating more heat (not too good for a bottle build). For the GPS receivers, a few were experimented with, and yielded vast differences in wigle upload data. Also, a consequence of USB 3.0 on poorly shielded cables is increased electromagnetic interference right in the GPS band (show a short video clip using a common SDR, and what to look for when diagnosing). Lastly on specific topics, with using a Pi, go into the design of a real-time clock, along with some of the configuration of the pi software to keep timing in order (pulse per second and chronyc -- and the accuracy to UTC it brings). Conclusion will showcase the hardware design process from the WigleBottleV1 and what went wrong in last year’s WWWD (with screenshots of trilateration gone wrong), to the version 2 design. References will link to resources others can use (as well as the hardware printed circuit boards used for this project).

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Warshopping - further dalliances in phreaking smart shopping cart wheels, RF sniffing and hardware reverse engineering

When: Friday, Aug 11, 11:00 - 11:45 PDT

Where: Harrah's - Nevada Ballroom - Lake Tahoe & Reno - War Stories - On the Record - [Map](#)

SpeakerBio: Joseph Gabay , Hacker

Joseph is a robotics engineer turned hacker - inspired by curiosity of the small systems in our everyday world, he went from developing products to performing security assessments of them. He specializes in embedded systems, circuit reverse engineering, and mechatronics.

His other hobbies include skydiving, multi-medium fabrication, and collecting strange domain names. He is also the founder and Chief Lunatic of the Flat Moon Society, who would like to ask you: isn't it weird we never see the other side of the moon?

Twitter: [@stoppingcart](#)

Description:

Smart shopping cart wheels are electronic wheels with a mechanical braking mechanism meant to prevent cart removal or shoplifting, as well as electronics to provide other tracking functions. In a past talk, I've discussed the ultra-low-frequency communication these systems use and how to sniff and replay them (and even use your phone's speaker to "phreak" your shopping cart!

This talk explores a new type of smart wheel (the Rocateq system), and focuses on a deeper exploration of the hardware and firmware. On top of capturing new sets of ultra-low-frequency control signals, we'll look at the 2.4 GHz "checkout" signal that it receives from the register and reverse engineer the PCB - soldering on "fly-wires" to look at the chip-to-chip communication with a logic analyzer. We'll also use a PICKIT programmer to dump the firmware from the main microcontroller for basic analysis using Ghidra.

In addition to the talk, the website where you can play the control signals as audio files on your phone will be updated to include the control codes for the Rocateq brand wheels.

REFERENCES:

- The ARRL handbook for radio communications, 2007. Newington, CT: American Radio Relay League, 2006. Print.
- <https://www.tmplab.org/2008/06/18/consumer-b-gone/>
- http://www.woodmann.com/fravia/nola_wheel.htm -The wonderful people over at /r/rfelectronics
- FCC.gov
- My previous talk at DEFCON 29
- rocateq.com

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Watching Androids Dream of Electric Sheep: Immersive Technology, Biometrics and the Law in collaboration with DEF CON Policy Village

When: Sunday, Aug 13, 10:00 - 10:59 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

Speakers: Brittan Heller, Liz "LawyerLiz" Wharton

SpeakerBio: Brittan Heller

Brittan Heller works at the intersection of technology, human rights and the law. She is currently a Senior Fellow at the Atlantic Council, with the Digital Forensics Research Lab, examining XR's connection to society, human rights, privacy, and security. She is also on the steering committee for the World Economic Forum's Metaverse Governance initiative. She is an incoming affiliate at the Yale Law School Information Society Project and the Stanford Law School Program on Democracy and the Internet.

Heller was an inaugural AI and Technology Fellow at the Harvard Kennedy School, studying content moderation and security risks in VR/AR/XR and emergent media, which resulted in award-winning publications on privacy, biometrics, targeted advertising, and XR. Heller is a frequent speaker and commentator on XR issues, and has published in The Information, Wired, The New York Times, and the Hill on online harms. She also advises governments and top XR companies on how to build safer and more inclusive immersive spaces.

As former counsel in Foley Hoag LLP's Global Business and Human Rights practice, Heller advised companies, investors, and NGOs on integrating public safety and human rights. She previously founded ADL's Center for Technology and Society. Her key projects included creating AI to study hate speech and XR experiences for civil rights advocacy. Additionally, Heller prosecuted grave human rights violations at the U.S. Department of Justice and the International Criminal Court and initiated landmark anti-cyber harassment litigation. She is a graduate of Stanford University and Yale Law School.

SpeakerBio: Liz "LawyerLiz" Wharton

Elizabeth (Liz) leverages almost two decades of legal, public policy, and business experience to advise researchers and to build and scale cybersecurity and threat intelligence focused companies. Currently VP, Operations of an adversary emulation platform startup, prior experience includes serving as the Senior Assistant City Attorney on Atlanta's ransomware incident immediate response team. Liz was recognized as the 2022 "Cybersecurity or Privacy Woman Law Professional of the Year" by the United Cybersecurity Alliance.

Description:

Virtual reality and augmented reality present exceedingly complex privacy issues because of the enhanced user experience and reality-based models. Unlike the issues presented by traditional gaming and social media, immersive technology poses inherent risks, which our legal understanding of biometrics and online harassment is simply not prepared to address. Explore these topics in depth with Brittan and Liz in collaboration with DEF CON Policy Village.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: We're From the Government and We're Here to Help Secure Open Source Software

When: Saturday, Aug 12, 16:00 - 17:50 PDT

Where: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

Speakers: Anjana Rajan, Brian Behlendorf, Charlie Gladstone, Jack Cable

SpeakerBio: Anjana Rajan , Assistant National Cyber Director for Technology Security at The White House

Anjana Rajan currently serves as the Assistant National Cyber Director for Technology Security at The White House. A renowned cryptographer, technology executive, and entrepreneur, Rajan has spent her career working at the nexus of national security and human rights. Prior to joining the White House, she was the first Chief Technology Officer of Polaris, the largest anti-human trafficking NGO in the United States. In this role, she architected Polaris's web3 & human rights vision and built a proactive security strategy to defend the organization against foreign malign influence operations and violent extremist threats.

Previously, Anjana was a Tech Policy Fellow at the Aspen Institute, was a former Y Combinator founder, led open-source development of advanced cryptographic libraries, and worked at Palantir Technologies. She was a Knight Scholar at Cornell University's Engineering School and received her bachelor's and master's degrees in Operations Research Engineering.

SpeakerBio: Brian Behlendorf , Open Source Security Foundation

No BIO available

SpeakerBio: Charlie Gladstone , UK Department for Science, Innovation, and Technology

Charlie Gladstone leads the UK Government's work on app store security in the Department for Science, Technology and Innovation. He has worked in tech policy for over five years, where he has specialised in exploring the intersection between technology, society and regulation. Before working in Government, Charlie provided public policy consultancy services to the tech sector clients. He has developed policy on a range of issues including cyber security, digital regulation and artificial intelligence.

SpeakerBio: Jack Cable , Senior Technical Advisor at Cybersecurity and Infrastructure Security Agency (CISA)

Jack Cable is a Senior Technical Advisor at the Cybersecurity and Infrastructure Security Agency (CISA). Prior to that, Jack worked as a TechCongress Fellow for the Senate Homeland Security and Governmental Affairs Committee, advising Chairman Gary Peters on cybersecurity policy, including election security and open source software security. He previously worked as a Security Architect at Krebs Stamos Group. Jack also served as an Election Security Technical Advisor at CISA, where he created Crossfeed, a pilot to scan election assets nationwide. Jack is a top bug bounty hacker, having identified over 350 vulnerabilities in hundreds of companies. After placing first in the Hack the Air Force bug bounty challenge, he began working at the Pentagon's Defense Digital Service. Jack holds a bachelor's degree in Computer Science from Stanford University and has published academic research on election security, ransomware, and cloud security.

Description:

Open source software is the backbone of the Internet. As a public good, open source software has enabled tremendous innovations -- and our government and companies alike have a role to play in sustaining it. In this fireside chat, White House Assistant National Cyber Director Anjana Rajan and CISA Senior Technical Advisor Jack Cable will present an overview of the US government's strategy on open source software security. The Federal government is the biggest user of open source software in the world, and we recognize that we must do our part in contributing back to the open source community. Priority areas for the U.S. government include advancing the adoption of memory-safe programming languages, reforming CVE, understanding software prevalence, and building a software developer workforce of the future by integrating security into computer science curricula. As part of this, we need your help in getting it right. How can the government best support OSS community efforts? What should the government NOT be doing? It's all on the table, and we look to work with you to ensure a secure, sustainable, and resilient OSS future.

Title: Weaponizing Plain Text: ANSI Escape Sequences as a Forensic Nightmare

When: Saturday, Aug 12, 11:00 - 11:45 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio: STÖK , Hacker / Creative at Truesec

Hacker/Creative STÖK is passionate about learning new things and sharing his curiosity with the world. For the last 3 decades, he has professionally hacked anything from computers/tech to marketing, fashion, communication, and the human mind. By delivering fast-paced, engaging onstage presentations and creating educational cybersecurity video content for the hacker community. His curiosity and "Good Vibes Only" mentality have reached and inspired millions of people around the world.

**HACKERS GONNA HACK.
CREATORS GONNA CREATE.
GOOD VIBES ONLY.**

Twitter: [@stokfredrik](#)

Description:

Logs are a vital component for maintaining application reliability, performance, and security. They serve as a source of information for developers, security teams, and other stakeholders to understand what has happened or gone wrong within an application. However, logs can also be used to compromise the security of an application by injecting malicious content.

In this presentation, we will explore how ANSI escape sequences can be used to inject, vandalize, and even weaponize log files of modern applications. We will revisit old terminal injection research and log tampering techniques from the 80-90s. Combine them with new features, to create chaos and mischief in the modern cloud cli's, mobile, and feature-rich DevOps terminal emulators of today.

We will then provide solutions on how to avoid passing on malicious escape sequences into our log files. By doing so, we can ensure that we can trust the data inside our logs, making it safe for operators to use shells to audit files. Enabling responders to quickly and accurately investigate incidents without wasting time cleaning, or having to gather additional data, while reconstructing events.

Welcome to this "not so black and white," but rather quite colorful ANSI adventure, and learn how to cause, or prevent a forensic nightmare.

REFERENCES

There are multiple references to prior research featured and provided as a part of the storyline in the presentation.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Web Shells - What They Are And How To Hunt Them

When: Friday, Aug 11, 13:00 - 14:59 PDT

Where: Flamingo - Savoy - AppSec Village - Workshop - [Map](#)

SpeakerBio: Joe Schottman

Joe Schottman is an application security focused security professional with experience including web app development and purple team engagements. He has spoken at conferences on threat hunting, web shells, purple teams, and more.

Twitter: [@JoeSchottman](#)

Description:

Web Shells are malicious web applications used for remote access and. They've been used in many of the recent prominent breaches/vulnerabilities including Equifax, SolarWinds, and ProxyLogon and are used by APTs and other threats. With ProxyLogon, the FBI was authorized to remove them from victim machines.

This session will help you avoid telling your employer that the FBI is now doing volunteer admin work by teaching you about Web Shells, how to hunt for them, and doing hands-on hunting in a VM. A little groundwork goes a long way and this class will show what to do.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Welcome to DEF CON 31

When: Friday, Aug 11, 09:00 - 09:20 PDT

Where: Caesars Forum - Forum - 109-119, 138-139 - Track 2 - [Map](#)

SpeakerBio:Jeff "The Dark Tangent" Moss , DEF CON Communications

Mr. Moss is an internet security expert and is the founder of Both the Black Hat Briefings and DEF CON Hacking conferences. In 2022 Mr. Moss was named to the UK Government Cybersecurity Advisory Board, and in 2021 he was sworn in as a member of the DHS Cybersecurity Infrastructure Security Agency (CISA) Advisory Council (CSAC), and serves as a chairman of their Technical Advisory Council (TAC). Mr. Moss is a member of the Council on Foreign Relations (CFR) and is interested in policy issues around privacy, national security, and internet governance. He spends a lot of time in Singapore. Twitter: [@thedarktangent](#)

Description:

The Dark Tangent, aka Jeff Moss, welcomes attendees to DEF CON 31.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DDV - Friday - 13:00-14:59 PDT

Title: What 10 years of drive stats data can tell us

When: Friday, Aug 11, 13:00 - 14:59 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

SpeakerBio: Andy Klein

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: What “Secure by Design” means for software breakers and builders

When: Saturday, Aug 12, 10:00 - 10:50 PDT

Where: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

Speakers: Cassie Crossley, Christopher Butera, Daniel Bardenstein

SpeakerBio: Cassie Crossley, Vice President, Supply Chain Security at Cybersecurity & Product Security Office at Schneider Electric

Cassie Crossley, Vice President, Supply Chain Security in the global Cybersecurity & Product Security Office at Schneider Electric, is an experienced cybersecurity technology executive in Information Technology and Product Development. She has many years of business and technical leadership experience in supply chain security, cybersecurity, product/application security, software/firmware development, program management, and data privacy. Ms. Crossley has designed frameworks and operating models for end-to-end security in software development lifecycles, third party risk management, cybersecurity governance, and cybersecurity initiatives. She is a member of the CISA SBOM working groups and presents frequently on the topic of SBOMs and Supply Chain Security. Ms. Crossley has an M.B.A. from California State University, Fresno, and her Bachelor of Science degree in Technical and Professional Communication with a specialization in Computer Science.

SpeakerBio: Christopher Butera, Cybersecurity and Infrastructure Security Agency (CISA)

Chris Butera is the Senior Technical Director for the Cybersecurity Division (CSD) of the Cybersecurity and Infrastructure Security Agency (CISA). In this role, Mr. Butera’s priorities are increasing CISA’s operational visibility, enhancing CISA’s analytical capabilities, envisioning new innovative cybersecurity services, and closing gaps between emerging technologies and CSD operations. Chris leads the Office of the Technical Director which also leads CISA’s Zero Trust efforts, prioritization of cyber R&D work, and leads strategic work in the Industrial Control Systems (ICS) and Operational Technology (OT) space.

SpeakerBio: Daniel Bardenstein, Manifest

Daniel Bardenstein is the CTO and co-founder of Manifest, a venture-backed software supply chain company allowing enterprises with end-to-end SBOM management. Prior to founding Manifest, Daniel served as the Chief of Tech Strategy at CISA, where he drove technology modernization and OT/ICS strategy across the agency, and led the development of the Cybersecurity Performance Goals. At the Defense Digital Service, he led cybersecurity programs across the Department of Defense, including securing the COVID-19 vaccines and the Hack the Pentagon program. Before joining government, Daniel directed product teams at Exabeam and Palantir developing cybersecurity and data analysis platforms.

Daniel was also a Tech Policy Fellow at the Aspen Institute, and is the co-President of Foresight Partners, a non-profit that provides free cybersecurity support to political campaigns. He holds several security certifications as well as a patent.

Description:


For years, the hacker community has fought to try to make technology more secure by exposing weaknesses in the software that underlies our entire society. And now, it seems the US government (USG) - and others around the world - are finally heeding the warnings from the hacker community.

In the past two years alone, USG has proposed policies that could shift the burden of security onto software developers, and defined guidance for ‘secure-by-design.’ These efforts, if implemented properly, could create a foundational shift in how software manufacturers build and secure software, and ultimately in the security of tech around the world.

In this technical policy talk, CISA’s #1 Cybersecurity Leader, Intel’s Global Cybersecurity Policy Lead, and an experienced security entrepreneur and former USG leader, dissect the buzzwords, policy documents, and implementation details of this wave of policy action, and what it means for software builders and hackers.

For the DEF CON / hacker community, this is an opportunity to hear – and inform – what may constitute ‘secure by design’ –

from memory safety, to open-source security, vulnerability disclosure programs, and more – and how software suppliers are held accountable for insecure software.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: What are your thoughts on AI assisted voice cloning being used for scams?

When: Friday, Aug 11, 14:00 - 14:50 PDT

Where: Caesars Forum - Summit - 218-219 - Policy Rotunda - [Map](#)

SpeakerBio:Christine Barker , Senior Investigator at Federal Trade Commission

Christine Barker is a Senior Investigator at the Federal Trade Commission. Prior to this, she was an independent digital forensic analyst. She has legal and computer networking undergraduate degrees and has worked in the two fields for the last 20 years. Currently, at the Federal Trade Commission, she investigates marketing fraud that ranges from, but is not limited to, multi-level marketing, tech support, coaching, and impersonation scams.

Description:

Scammers have evolved with technology. Technology has already helped scammers evolve from calling individual consumers to using technology to blast millions of calls to consumers. Some scammers have used generative AI models to clone a loved one's voice as part of a scam where the scammer asks the family member to send money to resolve a fake emergency, such as hospitalization or arrested. How will scammers use telephones and technology to transform, and what are the options available to stop them? This is a call for discussion about how to combat the use of generative AI models being used to clone voices to scam people's money.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: What is a GRC Hacker anyway?

When: Saturday, Aug 12, 19:05 - 20:05 PDT

Where: Virtual

SpeakerBio: Allen Baranov , CyberCX

Allen works as a GRC consultant and sometimes assessor for CyberCX. He was the founder of DCG11613 - a Def Con Group based in Melbourne, Australia. He calls himself the only GRC Hacker in the world.

Description:

I call myself the only AAA-rated GRC Hacker in the world and I think it is time to address what this really means. This talk will jump into what it really means to be a hacker, what the future will look like for hackers and where hacking fits into a field as plain and boring (not really!) as GRC. This is not a talk for GRC people but for all those that are keen to be hackers but also don't want to dive directly into offensive security.

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Friday - 15:30-16:15 PDT

Title: What Makes Hackers Extraordinary - It's A Gift!

When: Friday, Aug 11, 15:30 - 16:15 PDT

Where: Caesars Forum - Academy - 415-418 - Voting Village - [Map](#)

SpeakerBio:D9

Forty-one years of government service, retired USAF Colonel and DoD Senior Executive Service. Co-Led with the DoD CIO the development of the SecDef's DoD Cyber Workforce Strategy. Built from scratch a six-month DoD Cyber Operations training course, repurposed DEFCON's CTF and CTP technical architecture to support DoD cyber operations training, and now working advanced cyber R&D projects in private sector. UPENN doctoral dissertation examined what makes hackers extraordinary unique from the average human population.

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: What the Function: A Deep Dive into Azure Function App Security

When: Saturday, Aug 12, 13:30 - 14:10 PDT

Where: Flamingo - Mesquite - Cloud Village - [Map](#)

Speakers: Karl Fosaaen, Thomas Elling

SpeakerBio: Karl Fosaaen , VP of Research at NetSPI

As a VP of Research, Karl is part of a team developing new services and product offerings at NetSPI. Karl previously oversaw the Cloud Penetration Testing service lines at NetSPI and is one of the founding members of NetSPI's Portland, OR team. Karl has a Bachelors of Computer Science from the University of Minnesota and has been in the security consulting industry for 15 years. Karl spends most of his research time focusing on Azure security and contributing to the NetSPI blog. As part of this research, Karl created the MicroBurst toolkit (<https://github.com/NetSPI/Microburst>) to house many of the PowerShell tools that he uses for testing Azure. In 2021, Karl co-authored the book "Penetration Testing Azure for Ethical Hackers" with David Okeyode.

Twitter: [@kfosaaen](#)

SpeakerBio: Thomas Elling

Thomas Elling is the Director of Cloud Pentesting and a security researcher at NetSPI. He specializes in web application and cloud security testing. He has advised multiple Fortune 500 companies in the technology sector. In his spare time, Thomas enjoys improving his coding skills, watching bad action movies, and hanging out with his dog, Chunks.

Description:

As organizations have evolved from the "Lift and Shift" cloud migration strategy to building "Cloud Native" applications, there has been a significant increase in the usage of Platform as a Service (PaaS) services in the cloud. The Azure Function App service is a commonly used resource in this space, as it provides simple and easy to deploy application hosting. While the serverless service offers a wide variety of convenient features, it also comes with its own security challenges.

We will be discussing how the service is utilized by Azure customers and some of the architecture design flaws that can lead to privilege escalation scenarios. Additionally, we will be covering a recently remediated privilege escalation issue that resulted in the Azure "Reader" RBAC role gaining code execution privileges in Function App containers.

We will also be releasing a tool that automates the exploitation of write access on a Function App's Storage Account. The tool will allow you to gain cleartext access to the Function App keys, and will generate Managed Identity tokens that can be used to pivot to the Function App's identity. Finally, we will also include best practices and recommendations on how defenders can implement policy and configuration changes that help mitigate these issues.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Friday - 11:00-11:30 PDT

Title: What's up, Doc? Using documentation to build better OT security knowledge graphs

When: Friday, Aug 11, 11:00 - 11:30 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio: Ian Fox

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Whose Slide Is It Anyway?

When: Friday, Aug 11, 22:00 - 23:59 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

Description:

"Whose Slide Is It Anyway?" is an unholy union of improv comedy, hacking and slide deck sado-masochism.

Our team of slide monkeys will create a stupid amount of short slide decks on whatever nonsense tickles our fancies. Slides are not exclusive to technology, they can and will be about anything. Contestants will take the stage and choose a random number corresponding to a specific slide deck. They will then improvise a minimum 5 minute / maximum 10 minute lightning talk, becoming instant subject matter experts on whatever topic/stream of consciousness appears on the screen.

But....why?

Whether you delight in the chaos of watching your fellow hackers squirm or would like to sacrifice yourself to the Contest Gods, it's a night of schadenfreude for the whole family.

[Return to Index](#) - Add to  - ics [Calendar](#) file

BICV - Saturday - 13:00-13:50 PDT

Title: Why don't we have Internet, Daddy?

When: Saturday, Aug 12, 13:00 - 13:50 PDT

Where: Caesars Forum - Alliance - 301-304 - Blacks in Cyber Village - [Map](#)

SpeakerBio:Jess Hoffman

Jessica Hoffman, CISSP, has almost 20 years of IT experience and 15 years in cybersecurity in both the public and private sectors. She has taught cybersecurity classes at Harrisburg University and Penn State and is a national speaker on cyber topics as well as diversity, equity, and inclusion in the workplace. Jessica is a graduate of Bloomsburg University of PA and currently serves as the Deputy Chief Information Security Officer (“CISO”) for the City of Philadelphia. She is also one of the founding members of the BIC Mentorship program and forever supporter of the BIC community!

Description:

Did you know that TODAY there are 150 neighborhoods in Philadelphia that DO NOT HAVE INTERNET ACCESS?!?!?

Let's talk about why there is such a huge Digital divide between POC's and everyone else -- How historically blacks haven't had access to the same technology that middle and upper class white families did.

Hence another reason to explain the generational wealth gap, technological restrictions in access, exposure, understanding, and the low percentage of representation in the industry. Let's talk about it!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Why OT Cybersecurity Engineers Drink So Much

When: Saturday, Aug 12, 13:30 - 14:30 PDT

Where: Flamingo - Sunset - Scenic - Blue Team Village - Project Obsidian: Kill Chain Track (0x42) - [Map](#)

SpeakerBio: ThatDeadGuy

After thirteen years as a controls engineer within the Automotive Manufacturing and Oil & Gas Exploration Manufacturing industries, ThatDeadGuy was converted over to cyber security. His experience on the design and implementation of the equipment gave him a perspective into the OT realm that was not shared with most of the security team. Over the last five years he has built up cyber security architectures, implemented detection tools and created the IR processes for multiple critical infrastructure process environments.

Description:

A brief view into the odd world of Operational Technology (OT) and why so many OT Security Engineers drink like they hate themselves. This will cover the realities of their tech stack, business risk considerations, control systems recovery and how incident response is conducted within the environment. We will briefly cover how this environment was emulated for the Project Obsidian attack chain and how it differs from the physical environments.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: WIFISHARK

When: Friday, Aug 11, 13:00 - 13:59 PDT

Where: Flamingo - Eldorado - Radio Frequency Village - [Map](#)

SpeakerBio: Wasabi

Wasabi. The other Wasabi. Doing RF stuff with the RF Hackers Sanctuary and Sharing my Research and Tools with the masses

Twitter: [@@FrustratedITGuy](#)

Description:

Creating a Wifi Profile for Wireshark and why it made me mad while doing it. I needed a Red Team profile not a trouble shooting filter or a regular profile. It was not fun or an enjoyable experience but I will be happy to share my profile at the end of the presentation.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: WINE Pairing with Malware

When: Saturday, Aug 12, 15:00 - 15:50 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

SpeakerBio:Jared Stroud

Jared Stroud is a Lead Security Engineer at The MITRE Corporation tackling problems related to Container and Kubernetes security. Jared also contributes to ATT&CK via Adversary Emulation for Linux threats.

Description:

The growing popularity of playing AAA Windows video games on Linux has increased the compatibility of tools such as WINE and Proton. These same platforms that enable the latest games to run also can be used to execute the latest Malware. This talk will walk through configuring an environment to rapidly collect IoCs from unknown samples without having to use expensive sandboxes. Learn how to leverage your favorite UNIX tools to awk, grep, and pipe your way to extracting valuable forensic evidence without submitting your samples to \$VENDOR. More on the offensive side? Come see how to shorten the feedback loop from idea generation, to testing and finally deployment!

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Saturday - 15:30-16:20 PDT

Title: Wingin' It - Pentesting a 737

When: Saturday, Aug 12, 15:30 - 16:20 PDT

Where: Caesars Forum - Summit - 208-214 - Aerospace Village - [Map](#)

SpeakerBio: Alexander Dodd

No BIO available

Description:

In January 2023, Attack Research was invited to perform an on-wing penetration test of a Boeing 737NG that was being decommissioned. Come, listen, and be taken on a journey through this little-explored realm of aviation security. Discover some of our secrets from the decades of combined experience working on in-flight entertainment systems and various aircraft as well as the reasons why airlines and OEMs are urged to open their minds to external expertise and embrace the insights presented.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Friday - 15:00-15:30 PDT

Title: Wired for Safety: Prioritizing Safety in Deadly Systems

When: Friday, Aug 11, 15:00 - 15:30 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio:Jace Powell

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 14:00-15:59 PDT


Title: WISP Chill Out Space with Refreshments

When: Saturday, Aug 12, 14:00 - 15:59 PDT

Where: Caesars Forum - Summit - 217 - WISP - [Map](#)

Description:

Come relax with us in a quiet space! Grab a non-alcoholic drink and check out this year's WISP swag.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 12:00-15:59 PDT


Title: WISP Chill Out Space with Refreshments

When: Friday, Aug 11, 12:00 - 15:59 PDT

Where: Caesars Forum - Summit - 217 - WISP - [Map](#)

Description:

Come relax with us in a quiet space! Grab a non-alcoholic drink and check out this year's WISP swag.

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Friday - 20:30-22:59 PDT


Title: WISP Community Meet Up at BTV Pool Party

When: Friday, Aug 11, 20:30 - 22:59 PDT

Where: Flamingo - Pool - [Map](#)

Description:

BVT has generously donated a cabana for WISP to host our community meet up at their pool party. Arrive early to be in line when the doors open. There will be free tacos and non-alcoholic drinks!

[Return to Index](#) - Add to  - ics [Calendar](#) file

SOC - Saturday - 16:00-17:59 PDT

Title: WISP Peer-to-Peer Mentoring and Networking

When: Saturday, Aug 12, 16:00 - 17:59 PDT

Where: Caesars Forum - Summit - 217 - WISP - [Map](#)

Description:

Join us at DEF CON to mingle and network with privacy and security professionals. Also, consider becoming part of the WISP Tandems Mentoring program. It's our peer-to-peer mentorship program, which connects you with a partner who has a different background, expertise, and a different network. Why? We believe that you bring unique value to your women peers, no matter which career stage you're at. Knowledge is fluent, and leadership manifests at every career level. You can find your Tandem partner right here and sign up to be matched in our next round of the program!

[Return to Index](#) - Add to  - ics [Calendar](#) file

QTV - Friday - 12:00-12:59 PDT

Title: World's Cheapest "QKD" ;) -QKD for fun and non- profit from home

When: Friday, Aug 11, 12:00 - 12:59 PDT

Where: LINQ - 3rd flr - Quantum Village - [Map](#)

Speakers:Ben Varcoe,Jose Pisaro,Mark Carney

SpeakerBio:Ben Varcoe

No BIO available

SpeakerBio:Jose Pisaro

No BIO available

SpeakerBio:Mark Carney

No BIO available

Description:

"QKD". You've heard of it! You want to try it! But are afraid of what the neighbours would think. Today we present a Didactic solution to "QKD" from home. We will "attempt" the world's first transatlantic "VEGAS QKD" live.

Last year it was quantum snake oil. This year.... See what is on the "Kards.....".

Note and Caveat: keywords are 'Didactic' and 'air-quotes' ;) The attendee will leave the presentation with a more intuitive feel for how QKD works.

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICSV - Saturday - 11:00-11:30 PDT

Title: Wrenches, Widgets, and Walkdowns: Unraveling the Tangle of Digital Assets in Industrial Control Systems


When: Saturday, Aug 12, 11:00 - 11:30 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio: Tony Turner

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

XRV - Saturday - 13:00-13:59 PDT

Title: XR implications on Mobile Security


When: Saturday, Aug 12, 13:00 - 13:59 PDT

Where: Caesars Forum - Summit - 233 - Shared Stage - [Map](#)

SpeakerBio: Whitney Phillips

No BIO available

Description: No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

XRV - Sunday - 10:00-11:59 PDT


Title: XR Village Playground

When: Sunday, Aug 13, 10:00 - 11:59 PDT

Where: Caesars Forum - Summit - 206 - XR Village - [Map](#)

Description:

Explore emerging technology, hardware and experiences in the XR Village Playground. Meet and learn from technologists, futurists, and artists in the XR (VR / AR) space. Sponsored by BadVR and in collaboration with ICS Village, Red Team Village, Adversary Village and Policy Village.

[Return to Index](#) - Add to  - ics [Calendar](#) file

XRV - Saturday - 10:00-17:59 PDT

Title: XR Village Playground

When: Saturday, Aug 12, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 206 - XR Village - [Map](#)

Description:

Explore emerging technology, hardware and experiences in the XR Village Playground. Meet and learn from technologists, futurists, and artists in the XR (VR / AR) space. Sponsored by BadVR and in collaboration with ICS Village, Red Team Village, Adversary Village and Policy Village.

[Return to Index](#) - Add to  - ics [Calendar](#) file

XRv - Friday - 10:00-17:59 PDT


Title: XR Village Playground

When: Friday, Aug 11, 10:00 - 17:59 PDT

Where: Caesars Forum - Summit - 206 - XR Village - [Map](#)

Description:

Explore emerging technology, hardware and experiences in the XR Village Playground. Meet and learn from technologists, futurists, and artists in the XR (VR / AR) space. Sponsored by BadVR and in collaboration with ICS Village, Red Team Village, Adversary Village and Policy Village.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MUS - Saturday - 21:00-01:59 PDT

Title: Yarrrrgh Pirate Night - Music Set / Entertainment (Saturday, SYN Stage)

When: Saturday, Aug 12, 21:00 - 01:59 PDT

Where: Caesars Forum - Forum - 121-123, 129, 137 - Chillout - [Map](#)

Speakers:FuzzyNop, Miss Jackalope, Ninjula, O'Craven Pirate Band, Skittish & Bus

SpeakerBio:FuzzyNop

No BIO available

SpeakerBio:Miss Jackalope

No BIO available

SpeakerBio:Ninjula

No BIO available

Twitter: [@countninjula](#)

SpeakerBio:O'Craven Pirate Band

No BIO available

SpeakerBio:Skittish & Bus

No BIO available

Description:

Join us Saturday night (Aug 12) at the SYN Stage in Caesars Forum for "Yarrrrgh Pirate Night", which is our answer to last year's Night of the Ninjas.

At 23:00, we feature the pirate rock band O'Craven.

Contest - Win the cost of a DEF CON Badge - \$440!

It's your turn to participate! We seek the best dressed as a pirate! Dust off your costume or make a new one -- just show up -- it's supposed to be fun! The winner will receive a cash prize equal to the cost of the DEF CON 31 badge. The pirate band will judge the costumes and help choose a winner. Contest on the stage immediately following O'Craven at 00:00.

Featuring performances by:

- 21:00 – 22:00 – FuzzyNop
- 22:00 – 23:00 – Skittish & Bus
- 23:00 – 00:15 – O'Craven Pirate Band
- 00:00 - 00:15 – Costume Contest
- 00:15 – 01:00 – Miss Jackalope
- 01:00 – 02:00 – Ninjula

Content from this stage will be streamed to https://www.twitch.tv/defconorg_entertainment

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Saturday - 15:00-15:25 PDT

Title: you sound confused, anyways - thanks for the jewels.

When: Saturday, Aug 12, 15:00 - 15:25 PDT

Where: Caesars Forum - Academy - 401-406 - AI Village - [Map](#)

SpeakerBio: Adrian "threlfall" Wood , Dropbox

Adrian Wood, aka threlfall, discovered a love for hacking from cracking and modding video games and from the encouragement of online friends. He has worked as a red team consultant for WHITEHACK, a company he founded, and later as a lead engineer for an offensive research team at a US bank, where he was very interested in appsec, container security, CI/CD security and also founded their bug bounty program. He currently works for Dropbox, working on their red team. In his free time, he enjoys playing saxophone, working on vintage cars, and fly-fishing.

Description:

A case study in using Huggingface and machine learning models for supply chain style attacks in red team operations. Machine learning models execute by necessity within a businesses most sensitive environment with high level access to crown jewels, making it a perfect target. Learn the ways in which these attacks can be performed, how to avoid detection and what you can expect to find or do with your newfound ML environment access as a red teamer.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: You're Not George Clooney, and This Isn't Ocean's Eleven

When: Friday, Aug 11, 12:00 - 12:45 PDT

Where: Harrah's - Nevada Ballroom - Lake Tahoe & Reno - War Stories - On the Record - [Map](#)

SpeakerBio: Andrew "Spike" Brandt , Principal Researcher at Sophos X-Ops

Andrew Brandt is a former investigative reporter turned network forensics investigator and malware analyst, who serves as a Principal Researcher for Sophos X-Ops. Brandt has worked in information security since 2006 and, prior to working in the industry, covered it extensively as the security editor for PC World for nearly a decade. He has applied his knowledge about the behavior of malicious software and threat actors to profile identifiable characteristics of undesirable or criminal activity, specializing in attackers who target the finance, energy, and government sectors. His analysis techniques seek to determine general principles that can help analysts and defenders rapidly and comprehensively identify the root cause of infection and data loss, putting real-time network data analysis at the front line of prevention.

Description:

One common thread runs through a recent wave of (initially, successful) targeted malware attacks I've investigated: The attackers communicated with their targets, personally, using social engineering in real-time, in order to lay the groundwork for the rest of the attack to succeed. Throughout the course of several post-breach investigations, it became apparent that -- for a certain kind of target and a particular class of attacker -- engaging the victim in direct conversation was far more effective at assuring the target infected their computer than crafting a believable-looking "malspam" email that would "fool" the target into clicking a link or opening a file.

The attackers did not need to be charismatic for the technique to succeed. In fact, so long as the attacker "got into character" and treated the interaction as a normal, everyday event (from their perspective), the targets went along for the ride, and in many cases, self-infected with malware that was capable of snooping through their most sensitive files. In this session, we'll discuss both the social engineering and technical aspects of the attacks, and why this combination of tactics is particularly dangerous and hard to defend against.

REFERENCES

Brandt, Andrew. "Tax Firms Targeted by Precision Malware Attacks." Sophos X-Ops Blog, Sophos News, 13 Apr. 2023, news.sophos.com/en-us/2023/04/13/tax-firms-targeted-by-precision-malware-attacks/ @x86matthew.

"EmbedExeLnk - Embedding an EXE inside a LNK with Automatic Execution." www.x86matthew.com, 22 Apr. 2022, www.x86matthew.com/view_post?id=embed_exe_lnk

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Your Clocks Have Ears — Timing-Based Browser-Based Local Network Port Scanner

When: Saturday, Aug 12, 16:30 - 16:50 PDT

Where: Caesars Forum - Forum - 105,135,136 - Track 1 - [Map](#)

SpeakerBio: Dongsung “Donny” Kim , IT-Security Expert at Security Office part of Truesec

Dongsung (Donny) Kim is an IT-Security expert at Security Office part of Truesec. Their software interests vary widely from frontend to DevSecOps, with research interests spanning from reverse engineering to web security. Equipped with both professional and academic experience, they want to reconcile two seemingly opposite ideas: understanding user-facing software problems without compromising security.

Bluesky: @kidi.ng

Discord: kiding

Twitter: @@kid1ng

Description:

What can a website do? So many things these days. But, have you ever considered that it can port scan your LAN? It will fingerprint you with pinpoint precision and uncover hidden internal devices. Surely, a browser wouldn't allow that?

With this presentation, I will introduce a short primer on timing-based, browser-based port scanning using Fetch. Based on this primer, I will discuss three techniques that can scan open ports on the localhost, a NAT router's presence on the LAN, and open ports of the clients on the LAN. A demo of the proof of concept exploit will be provided, with closing remarks on possible mitigation strategies.

REFERENCES

- [1] <https://blog.nem.ec/2020/05/24/ebay-port-scanning/> [2]
- <https://www.bleepingcomputer.com/news/security/list-of-well-known-web-sites-that-port-scan-their-visitors/> [3]
- <https://www.crunchbase.com/organization/threatmetrix> [4] <https://coveryourtracks.eff.org/learn> [5]
- <https://web.archive.org/web/20060813034434/http://www.spidynamics.com/assets/documents/JSportscan.pdf> [6]
- <https://github.com/Flu1dTeam/PortScanner> [7]
- <https://medium.com/tenable-techblog/using-webrtc-ice-servers-for-port-scanning-in-chrome-ce17b19dd474> [8]
- <https://www.incolumitas.com/2021/01/10/browser-based-port-scanning/> [9]
- <https://docs.google.com/document/d/1a8sUFQsbN5uve7ziW61ATkrFr3o9A-Tiyw8ig6T3puA/edit> [10]
- <https://developer.chrome.com/articles/cors-rfc1918-feedback/> [11] <https://wicg.github.io/local-network-access/>

Return to [Index](#) - Add to  - ics [Calendar](#) file

ICSV - Saturday - 15:00-15:30 PDT

Title: Your Ship is Leaking... How Social Media Plays a Role in the Uncovering of Critical Maritime Systems

When: Saturday, Aug 12, 15:00 - 15:30 PDT

Where: Caesars Forum - Alliance - 313-319 - ICS Village - [Map](#)

SpeakerBio:Rae Baker

No BIO available

Description:No Description available

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Your Swag is My Swag: Pwning Fortune 500 Companies with Vistaprint

When: Saturday, Aug 12, 09:30 - 09:59 PDT

Where: LINQ - 3rd flr - Social A - Social Engineering Community - [Map](#)

Speakers: Daniel "Jcache" Goga, Langston "Shock" Clement

SpeakerBio: Daniel "Jcache" Goga , Security Consultant at Core BTS

Dan Goga serves as a Security Consultant with Core BTS focused on conducting penetration testing and vulnerability assessments. Dan Goga has eight years of information security experience in the public, private, and academic sectors. Dan has extensive knowledge and experience with RFID hacking, phishing techniques, social engineering techniques, and penetration testing.

Twitter: [@_BadCharacters](#)

SpeakerBio: Langston "Shock" Clement , Lead for Red Team operations and Penetration Testing engagements at Core BTS

Langston grew up reading stories about the 90's hacker escapades, and after years of observing the scene, he jumped into the cybersecurity field and never looked back. He is the current lead for Red Team operations and Penetration Testing engagements at Core BTS. With over fifteen (15) years of public and private sector experience in cybersecurity and ethical hacking, he aims to provide organizations with valuable and actionable information to help improve their security posture. Langston's specializations focus on modern-day social engineering techniques, wireless and RFID attacks, vulnerability analysis, as well as physical and cloud penetration testing.

Twitter: [@sh0ckSec](#)

Description:

Socially engineering a target organization with a hard hat and safety vest never gets old, but there are more ways to the server room. Take your physical penetration test to the next level, swagged out in the latest company-branded quarter zip sweatshirt. In this presentation, Langston and Dan will share their adventures hiding in plain sight while pwning Fortune 500 companies with official apparel and replica merchandise. They will explain their OSINT methodology for identifying 3rd party branding sites and tips for creating authentic-looking, made-to-order gear for any occasion. After learning these new techniques, you'll be so convincing that you might even get invited to your target client's next BBQ!

[Return to Index](#) - Add to  - ics [Calendar](#) file

DEF CON 31 Breaking: AI Cyber Challenge Announced for DEF CON 32 & 33

Posted 8.9.23



DEF CON will host the Artificial Intelligence Cyber Challenge #AIxCC semis in 2024 and the final in 2025! @DARPA, @openssf, @Google, @AnthropicAI @Microsoft & @OpenAI are working together to challenge contestants to create novel AI cybersecurity systems.

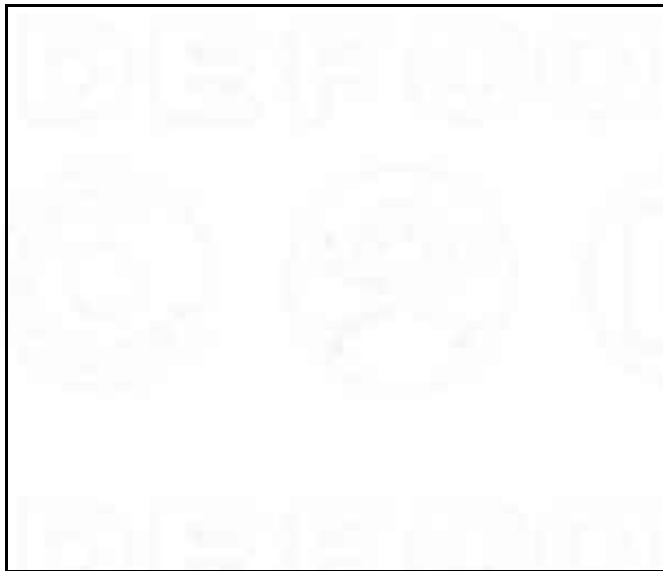
Over \$18m in cumulative prizes, access to cutting edge tech and a chance to help secure the open infrastructure we all rely on.

Attend the [official announcement](#) at DEF CON 31, Friday at 14:30 in Track 2!

Full details at aicyberchallenge.com

Friends of Bill W. at DEF CON 31

Posted 8.7.23



We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 31 has you covered. Join us throughout the conference in the Friends of Bill W. Community Space at Studio One at Harrah's.

Just one week to go!

The S.O.D.A. Machine is back!

Posted 8.3.23



Returning for DEF CON 31- the S.O.D.A. (Shell on Demand Appliance) Machine! S.O.D.A. is an unassuming vending machine that is fresh out of sodapop, but it grants creds to your very own anonymous VM running right there at DEF CON.

Visit S.O.D.A. in the Chillout Lounge of Caesars Forum throughout Con.

You can find out more and ask questions on the [S.O.D.A. Machine sub-forum](#) , and you can also check out [this video from last year's appearance](#) for more details!

DEF CON 31 Registration ReadMe

Posted 8.1.23



Hey, guess what? Pre-registration is all closed up, so if you wanna join in the fun, you gotta get yourself a badge in person. And hey, it's gonna cost you \$440 USD cash only, so no credit cards or anything fancy like that. You can find the registration spot at Caesars Forum ([check out maps here](#)). Registration opens around 7 am on Thursday, August 10th, so set your alarm!

Now, here's the deal - there are gonna be two lines when you get there. One for the folks who pre-registered (lucky them!) and one for the ones who didn't. But no worries, our convention is big enough to handle everyone, so even if we run out of our super cool limited edition badges, we've got backup badges that'll get you into all the action.

Once you've got your badge, you can download a DIY receipt from our website or from media.defcon.org when the conference starts. That's your proof of purchase, so no need for cash receipts. See you there!

DEF CON 31 Trailer!

Posted 7.28.23



Many thanks to the mighty, mighty Zebbler for this DEF CON 31 Trailer video! Enjoy the artistry, dance like no one's watching and get your mind right for DEF CON 31.

You can download it for yourself on the #defcon media server at <https://media.defcon.org/DEF CON 31/>.

Two little weeks, people. It's almost here. Let's GO!

Check out the DEF CON 31 Speaking Schedule!

Posted 7.25.23



The DEF CON 31 schedule is LIVE! You may now begin your planning in earnest. Find out who's dropping jewels, and where and when to snatch them up by visiting [the DEF CON 31 Schedule Page](#)

Not even a couple of weeks now - DEF CON is almost here! Getting psyched is now officially legit.

DC31 HDA Infopack is Live!

Posted 7.20.23



Thanks to @A_P_Delchi, the HDA Infopack for DEF CON 31 is ready for you to download at <https://forum.defcon.org/node/246536> ! If you or someone you know needs the lowdown on accessibility and accommodation info for DC31, make sure to check this out!

DC31 Room Block Closes Soon, Get 'em While They're Hot!

Posted 7.12.23

how it started

how it's going



Friendly DEF CON reminder: The [DEF CON group discount](#) ends Friday the 14th at midnight PDT! After that, you're stuck with the prevailing Vegas rate. If you've been procrastinating, take this as the universe telling you to get to clicking.

Reminder pt. 2 - The Horseshoe is a real hotel, and it's really in our room block. It's the new name for Bally's. Same location, just with a whole lot of upgrades.

Deviant Does Devices at DEF CON

Posted 7.11.23



DEF CON 31 is officially a month away! This means we're going to see some evergreen social media posts come back around, like:

DEF CON is cancelled (it's not)

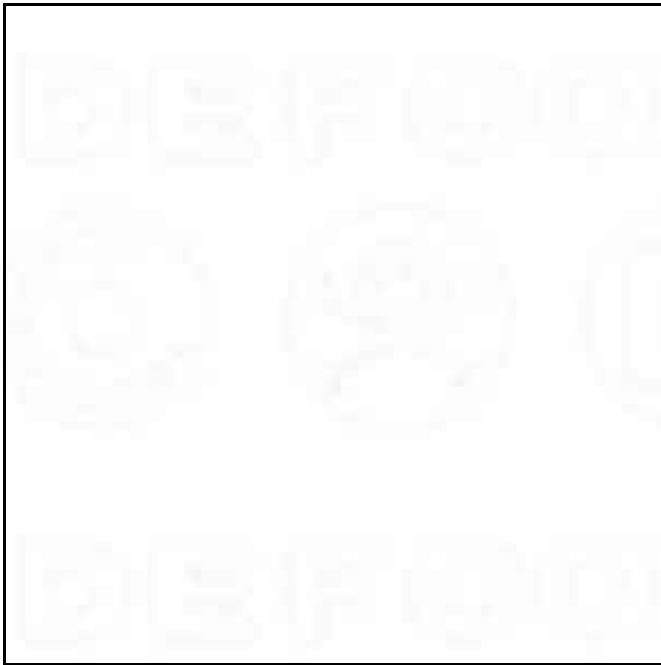
DEF CON is coming and I'm not ready (deep breaths, you'll be fine)

DEF CON will cast your precious devices into The Further so only bring an abacus and semaphores (hasn't been the case for a long time - take some reasonable precautions and pack as heavy as you like)

To further explain this last issue, physical security superhero and Friend of the Con [Deviant has produced a video](#) . These opinions are his, of course, but they're also pretty smart. See you soon!

DEF CON Workshops Sign-ups Opening Soon!

Posted 7.1.23



DEF CON 31 Workshops are GO ! You can find all the info on the DC Forums. We're proud of the lineup and excited for everyone to get eyes on it. Actual registration begins July 5 and 1200 PST, so consider getting your various web-clicking devices tested and performing any scheduled maintenance.

Let's GoOoO, people. It's almost here.

DEF CON Training Seattle Dates!

Posted 6.22.23

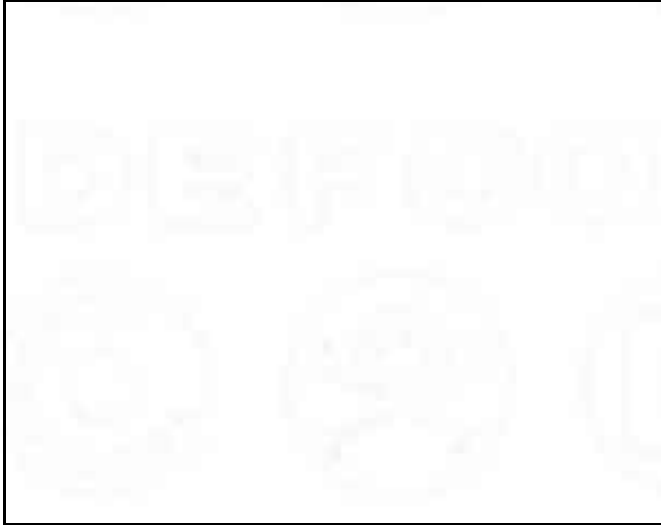


We've got new dates for DEF CON Training Seattle! Our two-day, hands-on training series is coming to #seattle November 1 and 2, 2023. They will be held at the Meydenbauer Center in Bellevue.

Watch this space for the list of trainers and other information. We'll post here and at training.defcon.org as soon as we have more news. Hope to see you there!

Policy @ DEF CON Department Preview!

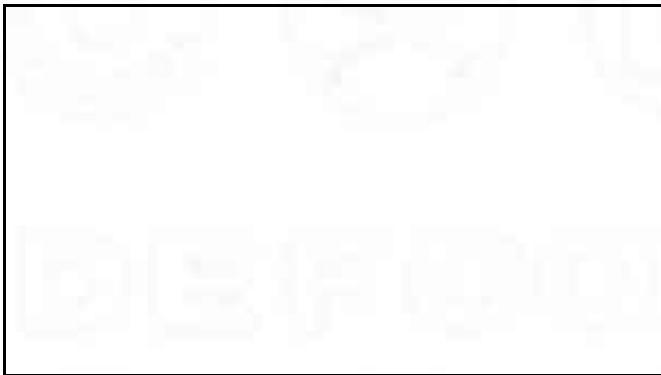
Posted 6.17.23



The Policy @ DEF CON team is all about “bridging communities”-- and for that, they've put together a video that better explains who they are, what they do and delves into pressing policy issues that are shaping discussions across all communities. [Watch here!](#)

Introducing DEF CON Communities!

Posted 6.16.23



DEF CON started as talks and parties that evolved into a community of those who with a hacker's mindset and an insatiable curiosity of how things work. We are committed to creating a place for all hackers to share, interact and learn from each other. Sometimes, though, we have to reassess whether the structure of DEF CON is helping or hindering this vision.

One example of this is how we categorize creators. There are a lot of content departments at DEF CON. If you're a Vendor, you go here. If you're a Village, you go over there. If something doesn't quite fit our categories we force them to fit: The EFF or a University in our vendor room for example.

With “Communities” we intend to work with some of the content creators that don’t fit perfectly into categories like "Village" or "Contest". We want to help them define the best way to showcase what they came to share without a prior template limiting their options. What would the EFF’s space look like if they didn’t have to try to fit in with Vendors? This is a good time to get together and figure it out.

This year at DEF CON you’ll see this new DEF CON Community format in action with DEF CON Groups (DCG), Women in Information Security Professionals (WISP), DEF CON Hackers with Disabilities (HDA), and some more as groups learn of this new option. Please make some time to visit them and check out their new offerings. As always, thank you for helping us grow and test out new things. See you soon.

Hack-a-Sat Satellite Launched!

Posted 6.7.23



It’s official - the bird is in the air! Plucky little satellite Moonlighter is launched and waiting to get h4x0r3d at DEF CON 31. Thanks to the team at @hack_a_sat for getting the stars to align for this historic moment! You can [read more about it in The Register](#)

DEF CON 31 CTF Quals Results!

Posted 5.30.23



Just in time to wreck your productivity for the short week, here's some delicious postgame info about the DEF CON 31 CTF Quals that happened over the weekend. Please enjoy the [official data dump from our good friends at The Nautilus Institute](#) . Additionally, please enjoy this set of informative [blog writeups from @Toasterpwn](#) .

Congratulations and godspeed to the victors. Respect to all who rose to the challenge. You are now free to get amped about the DEF CON 31 CTF in August. We will see you there.

DEF CON Training Las Vegas is Coming!

Posted 5.22.23



DEF CON Training Las Vegas is only 12 weeks out! We're proud to have a stellar lineup of trainers deep-diving into a wide variety of disciplines. Our two-day intensive training sessions begin August 14, right after DEF CON 31. It's the perfect time to embiggen your security skillset.

Check out the full roster at training.defcon.org and book your spot while supplies last.

DEF CON 31 Badge News!

Posted 5.19.23



We can't show you the whole thing yet, but we can say that there's lots of room for customization, courtesy of the #SAO slot pictured here. Specs and details for building your own Add On on the DEF CON media server: <https://media.defcon.org/DEF CON 31/DEF CON 31 badge/>

Big thanks to [@spux](#) - this year's badge designer!

We can't wait to see where you'll take this.

Registration for CTF Quals Now Open!

Posted 5.10.23



Box-poppers, shell-getters and potentates of the packet - we have great news! The stalwart humans of the Nautilus Institute have opened the registration for the DEF CON 31 CTF Quals. Your destiny's door stands open before you. Will you enter?

Get your bid in at quals.2023.nautilus.institute . Qualifications begin May 26, so don't delay.

Good luck to all those who dare.

Thanks for all the Submissions! Only a few open calls left!

Posted 5.5.23



Thanks to everyone who's submitted to the many DEF CON 31 Calls that closed out this week. We're seeing great participation and we want to express our gratitude to everyone who's willing to get involved.

We'd like to remind you that [there are still calls open](#), especially on the Village level. You can check if your favorite event/contest/village is still accepting submissions a few ways. [Forum.defcon.org has a DC31 planning section](#) that is probably the most complete way to find info. We've also got a calendar at [forum.defcon.org/calendar](#).

DEF CON is what you make it. Rolling up your sleeves and sharing with the community can take your DC experience to the next level, so don't miss this opportunity to get involved. We're getting into the home stretch toward DC31, and we'll be together again in Vegas before you know it.

Let's GOOOOO!

New/Old hotel in our room block: The Horseshoe!

Posted 5.3.23



Friendly DEF CON 31 reminder: The old Bally's in Vegas is now [The Horseshoe](#) - so that's the new hotel you're seeing in our room block. Same location, brand new glow-up.

Call for Demo Labs Ends May 1!

Posted 4.19.23



The [deadline for DEF CON 31 Demo Labs is MAY 1](#) ! If you have an open source project you want to demo for the DEF CON community, get your submission in right away!

DEF CON 31 Calls for Papers and Workshops are still Open!

Posted 4.19.23



Just another friendly reminder that the DEF CON 31 CFP season is in high gear. If you've got something simmering that needs to be a DC31 talk or workshop, get thee to our [Open Call Index](#) with all deliberate speed and get your bid in! Deadline is May 1st! We can't wait to see what you've got!

DEF CON 31 Pre-registration is Open!

Posted 4.17.23



DEF CON will always be a cash-at-the-door conference. We will always honor the LineCon with pizza and beachballs. This is the way.

However, the online option we introduced at DC Safe Mode has proven quite popular. It seems a lot of you appreciate the convenience of pre-registration so we're keeping it for DEF CON 31. [Tickets are available now at shop.defcon.org](https://shop.defcon.org), BYOP(izza).

DEF CON 31 and COVID-19

Posted 4.14.23



DC31 is on the horizon, and once again it's time to talk COVID measures. This year we're changing our mask policy from 'required' to 'recommended'.

There's been a lot of improvement in the situation from the last three years, but we're not out of the woods just yet and

masking remains the safest bet, especially in crowded spaces.

For the reasoning behind the decision and the mitigations we're putting in place for DC31, [check out DT's post here](#). Thanks for all you do to look out for each other. We'll see you soon.

First Trainers Announced for Las Vegas!

Posted 4.13.23



Big DEF CON Training announcement! The first 3 trainers have been announced for the DEF CON Trainings Las Vegas, right after DEF CON 31. They are:

[Madhu Akula](#) ,
[Chris Greer](#) , and
[Abhinav Singh](#)

Their training offerings are live at training.defcon.org

Policy @ DEF CON 31 CFP Briefing Session

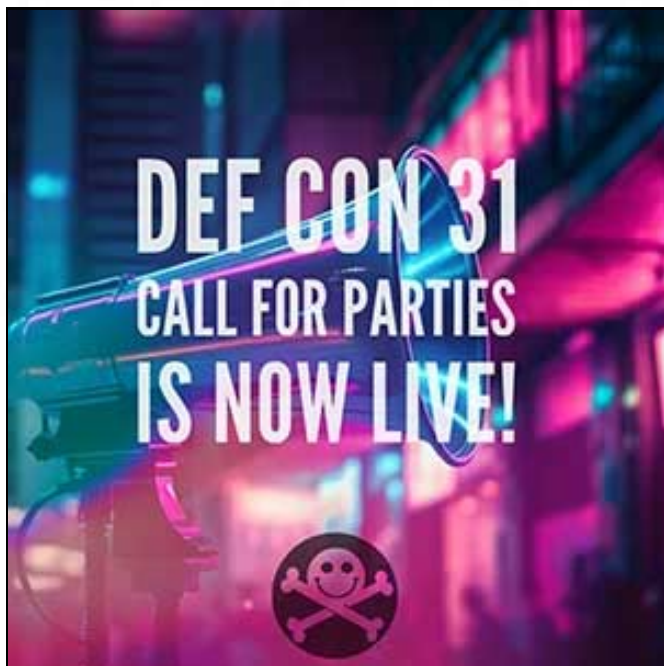
Posted 4.11.23



The DEF CON Call for Proposals (CFP) deadline is May 1st. [Policy @ DEF CON is hosting a public policy CFP session April 14th.](#) It will cover what makes a strong proposal, what to expect, tips on submissions & more! Check it out and DM [@DEFCONPolicy](#) for deets.

Call for Parties & Meetups is Open!

Posted 4.5.23



DEF CON has hosted some legendary parties, and we're always looking for the next one. If you're sitting on a DEF CON party concept that could take things to the next level, you should share it with us. If your idea gets selected, we'll work with you to make it happen. [The info you need is here](#). It's the shortest distance between partygoer and party legend. Don't miss your shot.

Call for Press is Open!

Posted 4.4.23



Attention all inky-fingered chroniclers of the hackersphere - press registration for DEF CON 31 is now officially open! If you're interested in covering our little hacker party in the desert, you'll need to get your application in before while there's space. [Read the rules \(for real, read the rules\) here](#) and get your bid in while supplies last. Operators are metaphorically standing by.

Calls for Vendors and Exhibitors extended!

Posted 3.31.23



DEF CON 31 deadline update: Potential exhibitors and vendors take heart — your deadline is now extended to April 30! Take

a deep, cleansing breath and get your info on the [Vendor Application](#) or [Call for Exhibitors](#) pages.

April 30 will be upon us in a flash, so get cracking!

DEF CON Room Block Clarification

Posted 3.28.23



DEF CON 31 booking reminder: That new 'Horseshoe' hotel showing up in our room block is the new rebrand of the familiar Bally's. Same convenient location and discount, just with a big glow-up.

To get access to the DEF CON discount, book rooms at <https://book.passkey.com/go/SHDEF3>

Hack-A-Sat News!

Posted 3.20.23



Every Hack-a-Sat has gotten progressively harder, preparing you for the ultimate test - Hack-A-Sat 4!

Learn what's new this year, including Moonlighter--the world's first & only hacking sandbox in space! ~ hackasat.com/moonlighter/

If hacking a satellite in orbit sounds like fun to you, register for the qualification round at hackasat.com - qualifications are April 1-2. Don't miss the launch!

Vendor Application Deadline Approaches!

Posted 3.20.23



Call for Vendors is closing April 1! If you've got goods you think the DEF CON Community needs to see, [get your submission in](#) before the time runs out!

Deadline Update!

Posted 3.4.23



The DEF CON 31 Contests and Events open call has been extended to March 15. That means you still have time to get your great idea for a #dc31happening in front of the people who can help make it happen. Don't miss the chance!

All the information you need to apply is here: <https://defcon.org/html/defcon-31/dc-31-cfce.html>

DCG Altspace VR 'End of the World' Event March 3rd!

Posted 2.28.23



AltspaceVR is getting sunsetted, so the DEF CON Groups Virtual Reality Team is throwing an 'End of the World' event on the platform March 3 at 7pm PST. You don't need a headset to come through, meet hackers from all over the world and just have a quality virtual hangout.

Follow DCGVR on Twitter or [DCGVR.org](https://www.dcgvr.org) for info. They'll be announcing what VR platform they're moving to in the coming weeks.

DEF CON Training Seattle Postponed

Posted 3.2.23



The DEF CON Training Event in Seattle is being postponed - instead of April, we'll hold it in Q4 of this year. Exact dates will be announced soon.

We apologize for any disruption or confusion this causes. We hope this change will give more people the opportunity to attend, with a few quarters of distance from the tech sector's current uncertainty.

This means the first DEF CON Training event of 2023 will happen in Las Vegas, and we hope you'll join us for that if you're in town.

For the latest updates and training information, please continue checking in on training.defcon.org.

NEW! Call for Exhibitors for DEF CON 31!

Posted 2.28.23



DEF CON 31 is opening up a [Call for Exhibitors](#) ! If you've got something you want to share with the community that doesn't fit in the Vendor area, we're opening an area just for exhibitors. Share your message with the DEF CON Community! For the right exhibitor, this is an unmissable opportunity.

Hack-A-Sat 4 reg is open!

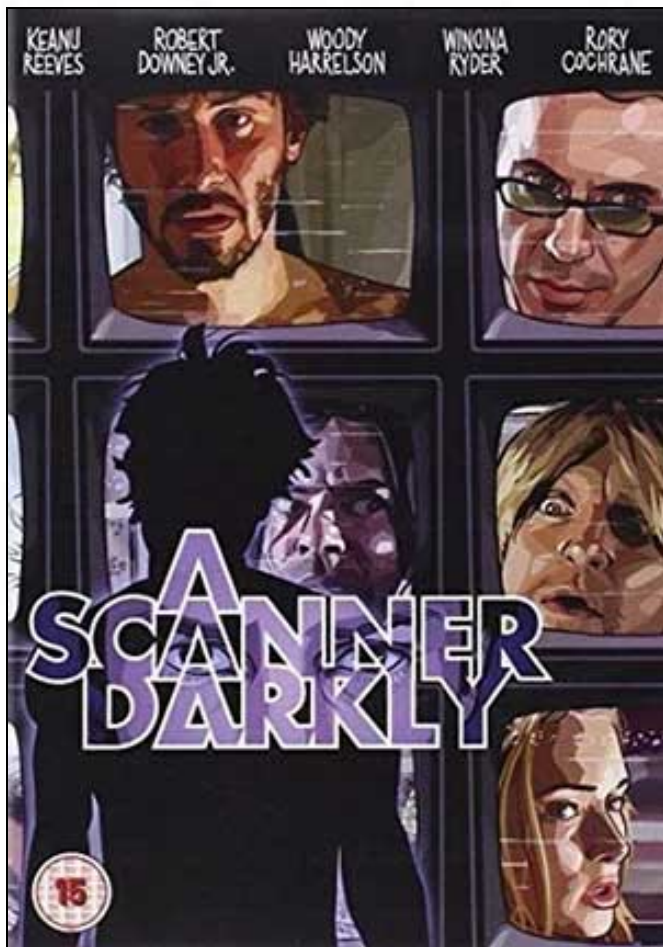
Posted 2.22.23



The satellite hacking contest to rule them all returns to DEF CON 31 for the 4th time. If you want to test your space-hacking skills, get your name on the list ASAP. Visit hackasat.com to register for the Hack-A-Sat 4 Quals, and follow [@hack_a_sat](https://twitter.com/hack_a_sat) for updates.

DEF CON Movie Night - A Scanner Darkly

Posted 2.10.23



The next DEF CON Movie Night is Feb 11 at 8pm PST. Join us to discuss Richard Linklater's adaptation of PK Dick's 'A Scanner Darkly'. Visually remarkable and probably more relevant than ever - join us to have your mind blown just a bit.

[Discord.gg/defcon](https://discord.gg/defcon) in movie-night-text.

DEF CON 31 Call-a-palooza!

Posted 2.1.23



We're just month into 2023 and we've got a whole lot of new open calls for everyone. Starting today the [calls for Papers](#) , [Demo Labs](#) , [Workshops](#) , and [Vendors](#) are open for business. This means two things: more ways for you to participate in making DEF CON 31 amazing, and DEF CON is officially on the horizon. Welcome to DEF CON Season!

Let's DO this thing, people.

DEF CON Training is coming to SEATTLE!

Posted 1.30.23



Join us April 13-14, 2023 in the Meydenbauer Center for a full roster of of intense two-day training sessions selected to expand the toolsets of hackers and security researchers of all kinds.

Seats are limited, so don't delay. The deep early bird discounts expire January 31.

Use this discount code for an additional \$50 off: Y4EJDX7YXAXX

This discount code expires Jan 31.

Full details at training.defcon.org .

Call for Villages!

Posted 1.22.23



Got a passion that you want to share with the DEF CON Community? Have ideas on how to make your favorite subject accessible and interactive? There may be a Village in your future. If your idea wins the day, we'll work with you to make it a DC31 reality. [The rules and info are here](#) and the clock is ticking. We're excited to see what's on your minds.

Chris Hadnagy vs. DEF CON lawsuit DISMISSED

Posted 1.13.23



Update:

- [Judge Beetlestone in PA dismissed the lawsuit](#) without pre-trial discovery, ruling that it lacked personal jurisdiction.
- Because the case was dismissed without prejudice, Mr. Hadnagy can refile and attempt to litigate in another venue.

Additional context:

During our investigation we spoke directly with Mr. Hadnagy about claims of his violations of our Code of Conduct. He confirmed his behavior, and agreed to stop. Unfortunately, the behavior did not stop.

Before DEF CON finalized our response, Mr. Hadnagy informed us that his Social Engineering Village would not be returning to DEF CON.

Our investigation also revealed that DEF CON is not the only security conference to receive complaints about Mr. Hadnagy's behavior. For example, Black Hat received complaints, conducted their own investigation and removed Mr. Hadnagy from their Review Board.

We thank the DEF CON community for supporting our efforts to uphold our Code of Conduct.

All the court documents are available here:

<https://lnkd.in/gsugqMyV>

And as always, our code of conduct and transparency report are here:

<https://defcon.org/html/links/dc-code-of-conduct.html>

<https://defcon.org/html/links/dc-transparency.html>

Call for Badge Designers!

Posted 1.10.23



Have you ever wanted to design a DEF CON Badge? This might be your moment. The [DEF CON 31 call for Badge Designers](#) is open. It's a non-electronic badge year, so we're looking for some creative analog badge goodness from the community.

Badges take some time to go from concept to lanyard, so if you have a proposal, get it over here! We can't wait to see what you come up with!

DEF CON Training Seattle!

Posted 1.4.23



This year's [DEF CON Training Seattle](#) has a date! Join us April 13-14, 2023 in the Meydenbauer Center for a full roster of of intense two-day training sessions selected to expand the toolsets of hackers and security researchers of all kinds.

Seats are limited, so don't delay. The deep early bird discounts expire January 31.

We're also doing trainings in Las Vegas after DEF CON 31 and in Singapore in the fall, and for these our [call for trainers](#) is still open. If you are interested in putting on a training at either event, get a submission in right away while there are still open slots.

Full details for prospective students and prospective trainers are available at training.defcon.org.

DEF CON 31 Call for Music is Open!

Posted 1.2.23



New Year, new calls to participate in DEF CON 31 - [Call for Music](#) is LIVE! Hit it up to throw your hat in the ring! We're looking for DJs, musicians and audio-visual artists of all kinds to keep the nighttime bumping at #dc31. Think you can move our crowd? Get your submission in!

NYE Raid Train!

Posted 12.30.22



DEF CON NYE announcement!

TWITCH -- NYE DAY PARTY! Start your celebration early with johnbbeta DNB, then switch channels to groove with the finest infosec family DJ talent ending with a big set from Miss Jackalope! Join us to shake out the old year and welcome the new!

defconmusic.org for more info- see you there!

Come Join Us at DEFCON.Social!

Posted 12.22.22



DEFCON.social is open!

From the first DEF CON announcement over 30 years ago inviting all to attend our first gathering:

"We cordially invite all hackers/phreaks, techno-rats, programmers, writers, activists, lawyers, philosophers, politicians, security officials, cyberpunks and all network sysops and users to attend." That's still our core audience, but we welcome artists, musicians, infosec, privacy professionals, journalists, and everyone genuinely curious about how things work.

Name: DEFCON.social

URL: <https://defcon.social/>

Support Site: <https://www.defcon.social/>

Location: USA

Languages Supported: English language posts, more languages as we add moderators to support them.

Tor .Onion: Coming soon

Topics: Technology, hacking, privacy, policy, infosec, music, art

Moderated: Yes

Infrastructure: Self hosted for privacy & security reasons

Funding: Community supported

Related Sites: defcon.org , media.defcon.org , [Reddit.com/r/defcon](https://reddit.com/r/defcon) , discord.gg/defcon ,

DMCA: <https://defcon.org/html/links/dc-dmca.html>

Privacy Policy: <https://defcon.org/html/links/dc-privacy.html>

Code of Conduct: <https://defcon.org/html/links/dc-code-of-conduct.html>

NOTE: We follow the Mastodon Server Covenant.

DEFCON.social provides for open discussion where different viewpoints are welcome and a high degree of skepticism is expected. However, insulting or harassing others is unacceptable. It's not about how you look or how hard you meme but what's in your mind, your ideas, and how you present yourself that matters.

DEF CON grew from the Underground BBS scene of the late 80's into the giant conference of today, and DEFCON.social is another way we seek to support the global hacker community.

We are building a community where you can explore serious issues, ask dumb questions, and make friends along the way. We have a strict Code of Conduct and enforce it. We hope you enjoy yourselves and be kind to others.

Join us at DEFCON.social.

DEF CON Training Announcement: 2023 Call for Trainers is open!

Posted 12.16.22



We're expanding our DEF CON Training in 2023 to include events in Seattle, Las Vegas and Singapore, and we are looking for trainers! If you've got experience and the kind of info hackers and security researchers can use, this means you. Please consider applying - all the information you need is available at <https://training.defcon.org>.

Call for Contests & Events is Now Open!

Posted 12.9.22



We've got a big DEF CON 31 announcement - the official [Call for Contests and Events](#) is OPEN!

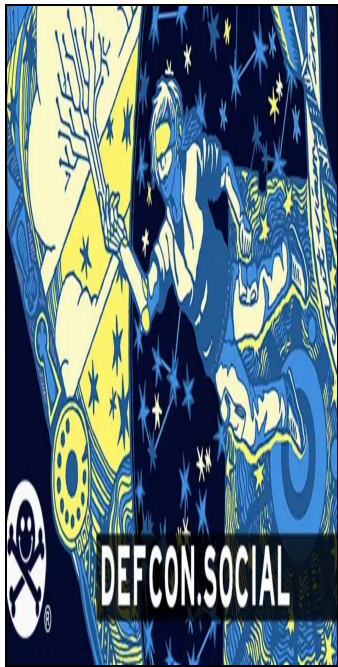
Now is the time to take the secret ideas you've been percolating and share them with us. We're looking for new ideas and cool twists on more familiar ones. Pitch us something good and we'll work with you to perfect it and get it on the floor in Las Vegas.

The rules and requirements await your examination. Hit us up with any questions at info@defcon.org.

We can't wait to see what you've got brewing.

Come Join Us at DEFCON.Social!

Posted 11.29.22



It's good to try new things.

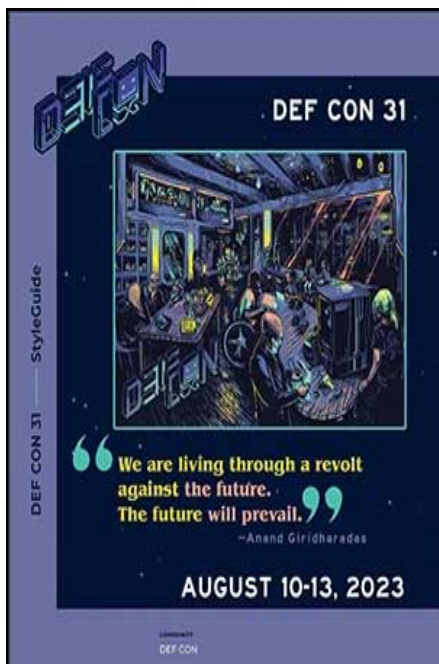
In that spirit, we cordially invite you to join DEFCON.Social – our brand new Mastodon server. If you've been thinking of trying out Mastodon, we'd love to be your home base.

You can sign up at <https://defcon.social/invite/wdM6eaqN>

See you there!

DEF CON 31 Update - We have a theme!

Posted 11.28.22



Here's an early Christmas present for all the DEF CON content creators out there. The [theme for DEF CON 31](#) is 'The Future Will Prevail'. You can follow the link to get your colors, fonts and some inspiration. We'll be following up with more

homework as the weeks roll on. We can't wait to see where you'll take it.

Happy Thanksgiving from Turkeybot and DEF CON

Posted 11.24.22



DEF CON Movie Night - Laura

Posted 11.22.22



DEF CON Movie Night closes out Noirvember with Otto Preminger's 'Laura'. Join us in the movie-night-text channel of the DEF CON Discord (discord.gg/defcon) at 8pm PST 11/26 for a top-shelf murder mystery and some excellent company. See you there!

DEF CON 30 Video release on YouTube and Torrent!

Posted 10.20.22



Let's start the weekend off with a little [DEF CON 30 video](#) action. And by a little we mean all of it. Mainstage talks, Village talks, Live CTF coverage and even the DCG VR talks. Please convey our apologies to your weekend plans. Watch, get your knowledge embiggened and pass it on to someone who will appreciate it.

More DEF CON 30 goodness awaits you at media.defcon.org - piping fresh torrents available of all our talks, photos, caps and assorted fun stuff. Fire up your websnarfer of choice and take your fill..

DEF CON ~ ~ U.

DEF CON 31 Call for Ideas! Open Now!

Posted 10.7.22



Let's get a jump on DC31 with a general [Call for Ideas](#) ! We want to hear from current and aspiring content creators. Share ideas for contests, villages - anything. Creators get more feedback & time, we all get a better DC. Open NOW.

DEF CON 30 Videos are Coming!

Posted 9.30.22



Heads up- the DEF CON 30 videos are gonna hit YouTube a little early this year. You might want to block off some time in October. We apologize in advance for any effect on workplace productivity.

DEF CON 30 CTF on the Books! Congrats to MMM!

Posted 9.21.22



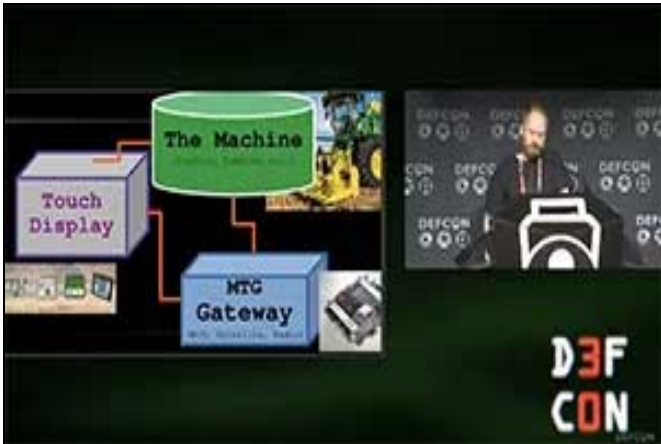
Congratulations to the DEF CON 30 CTF Winners, Maple Mallard Magistrates! [Read more about MMM !](#)

They were closely followed by the teams Katzebin and Starbugs, in 2nd and 3rd places respectively.

A big thank you to Nautilus Institute and all the CTF competing teams for a great game! Check out the [DEF CON 30 CTF section of the Media Server](#) for LiveCTF, PCAPS, and other interesting stuff as it becomes available!

Early Release Video - Hacking the Farm by Sick Codes!

Posted 9.14.22



We've released [a talk from farm hacking pioneer Sick Codes](#) on the intricacies of agricultural equipment cyber security, and how to break and modify it. Enjoy and share widely!

Archive Page is Live for DEF CON 30!

Posted 9.2.22



Missing DEF CON 30? We've updated our Conference Archive! Get your hands on a [cornucopia of DC30 content](#) - the program, LiveCTF, photos, video and even a soundtrack to vibe with while you browse. All for the low, low price of one internet click.

Keep an eye on it for even more coming soon; Contest results, talk videos, CTF packet caps, video of the music events and more! Happy weekend!

DEF CON 30 Badge talk Video!

Posted 8.29.22



In case you missed it: learn all about the magical mystery musical badge from DEF CON 30 in the [opening talk for DC30](#) with The Dark Tangent and MKFactor, the badge creators.

DEF CON 30 Press Roundup!

Posted 8.17.22



DEF CON 30 is in the books, and it looks like we made a little news. Here's an early roundup of DEF CON 30 press mentions. We'll update soon with more writeups and breakdowns as they appear.

[DEF CON Bans OAN](#) - Vice

[This String of Emojis is Actually Malware](#) - Vice

[Hackers Took Over a Commercial Satellite to Broadcast Hacker Movies](#) - Vice

[Hackers Come Home to Vibrant Community](#) - Dark Reading

[StarLink Ground Stations Successfully Hacked](#) - Hackaday

[John Deere Tractor Runs Doom](#) - The Register

[Black Hat and DEF CON visitors differ on physical risk management](#) - The Register

[How Sanctions Impact Internet Operators](#) - Infosecurity Magazine

[#DEFCON: CISA Director Praises Congress and International Cybersecurity Cooperation](#) - Infosecurity Magazine

[The Next Big Jailbreak in Tech: John Deere Tractors](#) - Gizmodo

[Black Hat and DEF CON Roundup](#) - Threatpost

[Carnegie-Mellon Team Wins DEF CON Hacking Competition](#) - Business Wire

[Zoom Patches Mac Auto-Updater Vuln that Granted Root Access](#) - Ars Technica

[Election Disinformation Fears Loom Over Hacker Confab](#) - Politico

[Sick Codes Jailbreaks Tractor at DEF CON](#) - Fierce Electronics

[John Deere Jailbreak Shows It's All Built on Outdated, Unpatched Hardware](#) - Boing Boing

[A New Jailbreak for John Deere Tractors Rides the Right-to-Repair Wave](#) - Wired

[Playing for All the Jelly Beans at the EFF Benefit Poker Tournament at DEF CON](#) - EFF

[Reproductive Justice in the Age of Surveillance: Panel at DEF CON 30](#) - EFF

[What to watch for as 'Hacker Summer Camp' gets underway in Las Vegas](#) - Cyberscoop

[Eclipsium Calls Out Microsoft Over Bootloader Security Woes](#) - Tech Target

[Russian Hackers Are Escalating and Diversifying Their Attacks on Ukraine, Research Says](#) - Gizmodo

[US Emergency Alert System Has 'Huge Flaw' — Broadcasters Must Patch NOW](#) - Security Boulevard

[New exploits can bypass Secure Boot and modern UEFI security protections](#) - CSO Online

[DEF CON 30 Comes of Age with Hacker Homecoming](#) - Security Systems News

[Logran hackear Starlink por solo 25 dólares](#) Muy Computer

[Up Close at DEF CON 30](#) - PC Mag

['Hackers against conspiracies': Cyber sleuths take aim at election disinformation](#) - Politico

[The Zoom installer let a researcher hack his way to root access on macOS](#) The Verge

[White House Cyber Director: 'Defense is the New Offense' for Cyber](#) - Nextgov

[Inglis: People, companies need to replicate collective cyber defense seen in Ukraine](#) - The Record

[Potential hack vulnerability for some Boeing planes fixed: Researchers](#) - Business Insurance

[Zoom acaba de corregir una falla de seguridad importante](#) - Digital Trends (Español)

[A Flaw in the VA's Medical Records Platform May Put Patients at Risk](#) - Wired

[DC30 Car Hacking Village Badge](#) - Intrepid Control Systems(YouTube)

[Designing the DEF CON 29 and 30 Badges \(featuring MK Factor\)](#) Hacker Hangouts (YouTube)

[DEF CON 30 OBD-Kill Badge First Flight](#) - Intrepid Control Systems(YouTube)

[Defcon 30 badge release the patch/fix to the bug of smoked badge.](#) - Reddit

DEF CON 30 China Virtual Party!

Posted 8.11.22



Our hacker friends in China are having a VR party for DEF CON 30 with a big, beautiful virtual meeting space and media shared from the show. Big thanks to Baidu for putting that party together! The DEF CON spirit of discovery and community is a truly global thing and we're grateful to all of you for making DEF CON what it is.

Join us for DEF CON 30 online!

Posted 8.11.22



The DEF CON Discord is open (discord.gg/defcon). You can hang out in virtual LineCon, try out the offerings of one of our hybrid villages and meet DEF CON family from around the world.

The DEF CON Groups have a VR hangout going on throughout DEF CON. Learn what DCGs across the globe are up to, maybe even find a group near you to join so you can keep that DEF CON vibe all year! The info you need to get involved is here: https://www.dcgvr.org/DEF_CON_Groups_AltSpaceVR_-_Quick_Guide_v1.6.pdf and you can join in on the fun with or without a VR headset. You can even watch the event live on Twitch: twitch.tv/defcon_groups .

Follow our YouTube channel ([DEFCONConference](https://www.youtube.com/DEFCONConference)) for video updates from DC30 all weekend. We've upped our content

game this year and we'll be sharing a bunch of interviews and contest content.

So even if you're not onsite, you can still get some DEF CON into your 2022, and we'll save you a place in LineCon for 2023.

HDA Infopack is Live!

Posted 8.4.22



Many thanks to @A_P_Delchi for the [DEF CON 30 HDA Infopack](#) ! This helpful guide for Hackers with Disabilities has venue maps, tips for traveling between venues and a concise explanation of DEF CON's HDA provisions. Let's look out for each other, and if you see a way we can improve our accessibility, let us know!

DEF CON Transparency Report Update

Posted 7.28.22



In preparation for DEF CON 30, we've updated the [transparency report](#) on the DEF CON website. While you're there, take a moment to re-familiarize yourself with the [code of conduct](#). We don't have a ton of rules, but we take the ones we have very seriously.

DEF CON 30 Speaking Schedule is Live!

Posted 7.15.22



'Tis the season, hackerfolk. DEF CON is almost here and all four tracks of the main speaker schedule are live on the website! Visit the [Schedule page](#) to start your planning. Our valiant CFP Review Board has put together a strong list of presentations over a wide array of subjects. We're sure you'll find plenty of interest.

Feel free to tweet at us about the talks you want to see, and feel equally free to get hyped. Less than a month now, people.

Floorplan Maps are Live, Room Block discount Ends Soon!

Posted 7.7.22



The [floorplan maps for DEF CON 30](#) have been added to the Venue page of the DC30 website. Take a peek and plot your course, it's just a few short weeks now.

The DEF CON 30 room rate discount closes July 15 - so book soon to take advantage of the price break! Our room block in Caesars is full, but many others still have price breaks available.

[Book a Room for DEF CON 30 Here !](#)

COVID Clarification for DEF CON 30

Posted 6.22.22



Just so there's no confusion, DEF CON 30 will require masks, same as last year. We thank everyone for keeping each other safe last year, and we can't wait to get the gang together responsibly just a few short weeks from now.

Original [DEF CON 30 Covid Policy](#) post from May.

First Batch of DEF CON 30 speakers is Live!

Posted 6.9.22



Friendly DEF CON 30 announcement - [the first bunch of speakers are selected](#) and available for your perusal on the DEF CON forums. Congrats to everyone already selected. Keep your eyes on this space for more selections!

DEF CON Training Site is Live!

Posted 5.31.22



DEF CON Trainings registration is LIVE! Right after DEF CON 30, we're excited to offer these intensive 2 day classes with a certificate of completion. First come, first served so don't procrastinate. Class descriptions and reg information are at defcontrainings.myshopify.com.

Weekend Updates! CTF Quals news, and New SE Community Q&A Today!



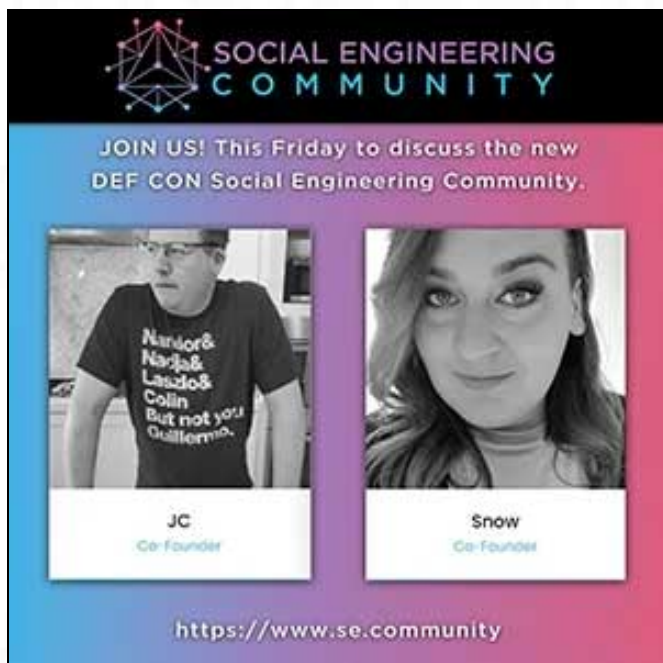
CTF News

CTF Quals are almost here (May 28 at 0000 UTC) and the CTF Chat on the DEF CON discord is already open!

From @NautilusCTF :

#defcon quals chat on the Defcon discord is open. Come visit us in [#ctf-discussion-text](#) to ask all the important questions, like “when is web?” and “this challenge is too hard unlock another one”

Time is short to get to the [Nautilus Institute Website](#) and register your team for CTF quals!



SE Community Q&A Today!

Join Social Engineering Community Village cofounders [@JC_SoCal](#) and [@sn0ww](#) to talk all about what kind of events the Social Engineering Community has in store for DEF CON 30. They'll be live on Twitch answering your questions at 5pm EDT Friday the 27th at [twitch.tv/se_community](https://www.twitch.tv/se_community) . See you there!

The Black and White Ball is Back!

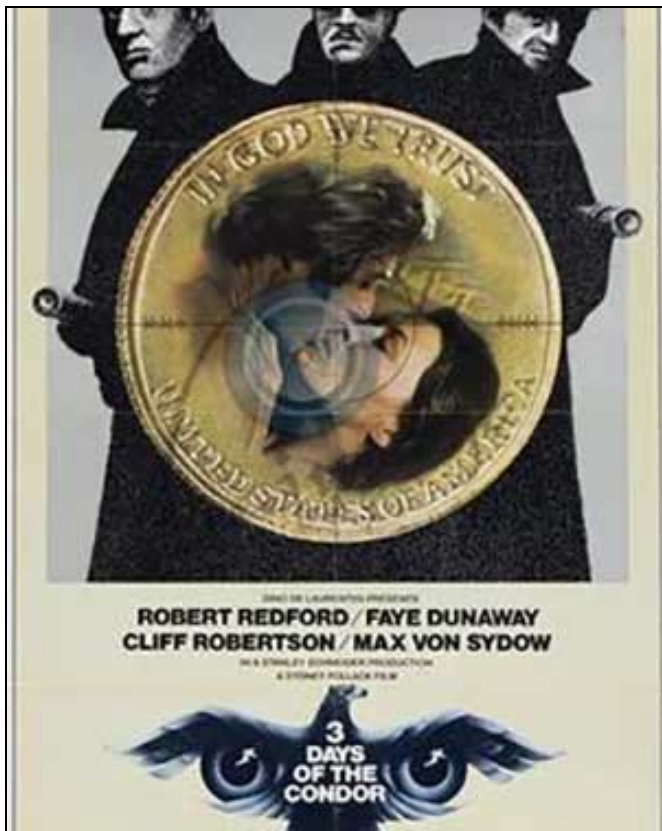
Posted 5.24.22



A little announcement about DEF CON 30's Black and White Ball: the best-dressed entrants will get some to enter early and enjoy a few free drinks before we let everyone else in. So look sharp - more details to come.

DEF CON Movie Night: 3 Days of the Condor

Posted 5.21.22



Join us Saturday the 21st at 8pm PDT for Sydney Pollack's 1975 spy thriller 'Three Days of the Condor'. Robert Redford plays a CIA researcher on the run and Ma Bell plays herself. We'll be hiding out in the DEF CON Discord (discord.gg/defcon) under the code name movie-night-text.

Check out Policy @ DEF CON!

Posted 5.19.22



Policy matters. The world has never been so connected, and mighty forces contend for the right to shape our digital lives. DEF CON believes the hacker community needs a voice in that process. To help people learn, connect and get involved with the leading edge of tech policy, we offer ' [Policy @ DEF CON](#) '. We'll have presentations, panels, and off-the-record evening lounges. Get yourself up to speed on the issues, connect with some of the players and maybe even get involved. The future is what we make it!

The DEF CON 30 Website is live!

Posted 5.13.22



Good news, everyone! The [DEF CON 30 official website is officially LIVE](#) and DEF CON season is officially IN EFFECT. Bookmark it for a handy place to check out all of the DC30 infoz as they roll in. Check the calendar, jump into the forums, book a room - it's all in one place.

Now that we've reached cruising altitude, you are free to shimmy excitedly around the cabin.

Let's GoOOoo!

COVID Updates for DEF CON 30

Posted 5.3.22



DEF CON 30 is getting closer, and that means we're starting to get questions about Covid-19 protocols for the in-person event. Here's the current state of play.

Some things have changed since DC29. The US has largely stopped checking vaccine status for entry to indoor events, owing

at least partly to the knowledge that the vaccines serve more to prevent severe disease than to curtail transmission. COVID-19 testing is now mostly done privately with widely available at-home kits.

But most things haven't changed. There are still new variants on the move. There are still spikes in transmission and hospitalization. Masks are still the most effective way to protect people in indoor events.

Barring a major change in the situation, we will not check proof of vaccination, but we will keep last year's mask requirement in place for DEF CON 30. Protecting the community is our first priority, and we want to make sure that everyone is as safe as we can make them. Everyone includes the healthy, the vulnerable and those who have immune compromised loved ones they need to protect.

Thank you for all you did to protect each other last year, and with your help we'll do it again this year.

Training Coming to DEF CON 30, Call for Training is Open!

Posted 4.14.22



The wait is over - we're ready to announce the Call for Trainers!

This year we're adding DEF CON Training – intensive, two-day courses of study aimed at building specific skills. In some cases, these courses will even carry a certification. The Trainings will be held August 15-16, the Monday and Tuesday after DEF CON.

We're looking for unique, technical, and practical presentations from trainers with deep knowledge of their subject. If that's you, we're offering:

- 50/50 split of the gross income.
- Optional test where students demonstrate their skill for a certificate.

All the info you need to apply is on the [Call for Training](#) page. Get your applications in early – we look forward to seeing what you've got to share.

New Payment Option for DEF CON 30!

Posted 3.25.22



DEF CON is a cash-at-the-door kind of conference. Paying in cash helps protect your privacy, and search warrants can't vacuum up PII we don't collect. You will always be able to lay down US dollars in the reg line and collect your badge.

Still, the experience of DC29 taught us a few things. Some of our attendees work DEF CON into their business travel schedule, and the option to pre-reg with a credit card over the web made things much easier for them. Some of our attendees need to manage a group purchase, or want a more detailed receipt.

For everyone who fits into those categories, we're happy to announce that we're keeping the option of online registration. Starting Monday, March 28th, you'll be able to use shop.defcon.org to buy your ticket and get your receipt. We hope the online option makes the process more streamlined for those who need it. We thank people for their patience and feedback as we navigate the changing landscape.

The price for DEF CON 30 is \$360, with a processing fee of \$9.66 added to online orders.

Fine print: Currently we cannot provide beachballs and pizza to the online purchasing experience. For that, you're gonna need LineCon.

DEF CON Movie Night: Dark Star!

Posted 3.16.22



DEF CON Movie Night this Saturday will feature some more 70s sci-fi with John Carpenter's 'Dark Star' from '74. Join us 3-19 at 8pm PDT in the #defcon discord (discord.gg/defcon). We'll be in the movie-night-text channel.

Villages for DEF CON 30!

Posted 3.15.22



The list of [DEF CON 30 villages on the Forums](#) has been updated! Stop by to check out the full complement of village goodness we're offering this year. Comment, like, subscribe, volunteer to help out - but mostly get amped. #defcon30approaches.

Coming soon: Call for Training!

Posted 3.11.22



We're excited to announce something new on the menu for DC 30 - DEF CON Training! We're launching a lineup of intense two-day trainings taking place August 15-16 in the same venue, and we're looking for trainers!

WHAT: DEF CON We're seeking Trainers for two-day training sessions right after DEF CON 30.

WHEN: August 15-16, the Monday and Tuesday after DEF CON 30.

WHERE: Same location, the Caesars Forum.

WHY: For DEF CON attendees who love our free Workshop series but wish they could get an even deeper, more focused dive and maybe even a certificate. Like everything we do at DEF CON, we hope it will help to build and strengthen the hacker community and spread the kind of knowledge that makes the world more open and secure.

DEF CON Training will offer two-day paid training courses in the \$1-\$3k price range. We're looking for unique, technical, and practical presentations from trainers with deep knowledge of their subject. If that's you, we're offering:

- 50/50 split of the gross income.
- Optional test where students demonstrate their skill for a certificate.

Interested? We will launch the Trainer submission form later this month! If you have questions, drop us a line at info@defcon.org.

The Dark Tangent

More DEF CON 30 Calls Opening!

Posted 2.15.22

The logo for DEF CON 30, featuring the number '30' in a stylized, red, blocky font. The '3' is positioned above the '0', and the '0' has a diagonal slash through it. The logo is centered within a white square with a thin black border.

Good news, everyone! We have more calls open for DEF CON 30!

Call for Parties and Meetups : your dreams of throwing an epic party at DEF CON 30 are within your reach! If you have a solid concept to wrap some next level festivities around, get at us. The best ideas will get space and support. Details here: [Call for Parties](#)

Call for Music : we're gonna need some tunes. Lots of tunes. This call is for established acts and bedroom Beethovens alike. We're looking for live performers, so if you've got the stuff that puts the dip in our hip and the glide in our stride, get to the [Call for Music](#) and let us know.

Call for Vendors : we're always looking for new hacker gear and accessories to share with the community. Get your cool swag in front of a pretty savvy and curious audience by applying here at the [Vendor Application](#)

[New Calls Open for DEF CON 30!](#)

Posted 2.1.22



You know how you can tell it's DEF CON season? The Calls. When you hear the distinctive warble of the DEF CON Content calls, you know what's up. It's like the first robin of spring, if robins were cooler and more hacker-focused.

Today we're opening three more DEF CON 30 Calls:

Call for Papers

The big one. If you want to speak at DEF CON 30, it's time to get your submission together. As always, we're looking for fresh, technical content and the sooner you get it in, the better your chances. We can offer suggestions to help you get over the finish line, time permitting. Fortune favors the bold, so don't delay.

Call for Workshops

The very popular workshop series is back for DEF CON 30. Some topics need a more time and involvement than a main-stage talk can offer. The workshops are an amazing way to share your in-depth, hands-on content with the DEF CON community.

Demo Labs

Get your open source project in front of the knowledgeable, curious humans of DEF CON. Get valuable feedback, find accomplices and raise your project's profile. We provide the floor space and the audience, you provide the timely submission.

The DEF CON machine is revving up, and DC30 will be here before you know it. Don't miss your chance to get involved. The community is waiting to see what you've got to share.

A Warm Welcome to the Next CTF Organizer Team: Nautilus Institute!

Posted 1.28.22



Big DEF CON 30 CTF update! Following several years of exemplary service by the Order of the Overflow, our world-famous Capture the Flag contest is under new management. The care and feeding of this year's CTF is in the worthy and capable hands of the Nautilus Institute!

From Nautilus Institute:

Ahoy DEF CON and CTF communities!

We are the Nautilus Institute. We have been chosen, from a very respectable pool of applicants, to steer the DEF CON CTF ship starting in 2022. We are thankful for this honor, and hope to navigate straight and true no matter what waters lie ahead.

We're a bit light on details, while we prepare for this year's DEF CON CTF Qualifiers May 28-29, but we hope to flag you down with more information soon! Please follow us on twitter at https://twitter.com/Nautilus_CTF and keep a look out on our website at <https://nautilus.institute> .

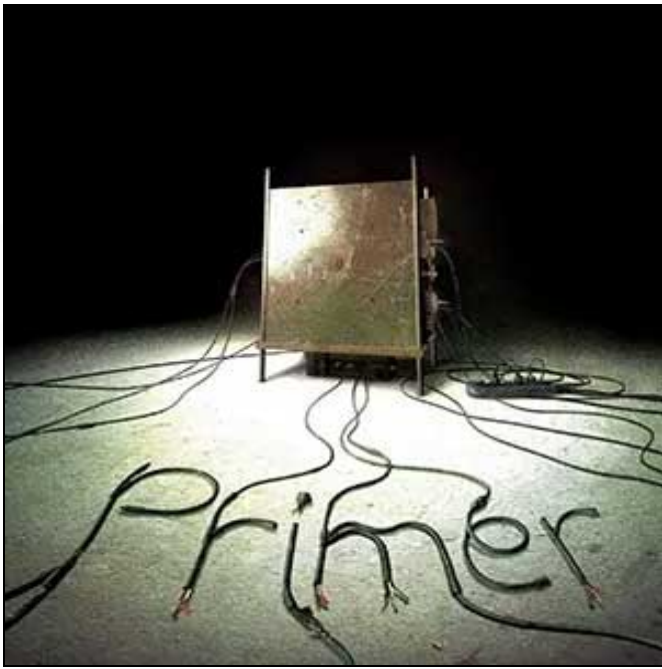
Sea you soon,

@•~

For the boldest and best prepared, glory awaits. Godspeed.

DEF CON Movie Night: Primer!

Posted 1.27.22



DEF CON movie night rolls on with 'Primer'. Joins us on the [DC discord](#) Saturday 8pm PST for what has to be the most brainmelting time travel movie that could possibly be shot for \$7000. Bring a cork board and a few different colors of yarn. We'll be waiting for you in the movie-night-text channel.

DEF CON Movie Night: Tank Girl!

Posted 1.19.22



This week's DEF CON movie night will feature the very weird 'Tank Girl' from 1995. Join us Saturday, 8pm PST in the movie-night-text channel of the [DEF CON discord](#) for a glimpse at what the apocalypse looked like from the more innocent viewpoint of the mid 90s. Bring your own water.

DEF CON New Year's Eve!

Posted 12.23.21



DEF CON is doing a small [New Year's Eve event](#) on the DEF CON discord. There will be several hangouts and contests to participate in. We'll have music, a Kubernetes CTF, A Ham radio CTF, some Hacker Karaoke, movie watchalongs and more. We'll have the full rundown on [defcon.org](#) and we'll update in the NYE Forum threads. Join us in welcoming 2022 - can't wait to see you!

DEF CON 29 Transparency Report

Posted 12.6.21



The full DEF CON [Transparency Report for DEF CON 29](#) is now available. Our deepest thanks to everyone who reported issues to us and also to the people on staff who tracked down and handled those issues. It's a community effort, and it's good to see the progress we're making.

DEF CON Ornament Now Available!

Posted 11.23.21



The holiday season is upon us - time to spruce up your place with some festive hacker accents. This is the only [official DEF CON ornament](#) . Accept no substitutes. Suitable for all celebrations and a welcome addition to any decor.

Enter the DEF CON 30 Artwork Contest!

Posted 11.17.21



Now that the DEF CON 30 Theme is out there in the world, it's time to go pencils up on the DEF CON Art Contest!

This year's theme is ['Hacker Homecoming'](#) , and you can read all about it on the DEF CON Forums. It's a theme meant to celebrate our community's much awaited reunion next August. It's also meant to reference the 30th Anniversary we're celebrating, which is a pretty big deal for a hacker conference.

So if you've got some art skills, you've got a luxurious 7+ months to get your take on the theme in to us. There's so much time between now and the June 1 deadline that you could probably learn a brand new art style in which to make your submission. You can drop as many submissions to pictures@defcon.org as you want, so enter early and often.

Theme:

We are looking for artwork that reflects a spirit of community and reunion. We're looking for art that combines the 90's

hacker aesthetic of DEF CON's history and our tribe's 21st century future. We're looking for your vision and vibes.

We hope you'll take in the information in [the style guide](#), but we hope that you'll use that as a launching pad and not a set of limits. We want to see where you can take these ideas.

Guidelines:

300 DPI. Convert type to outlines where applicable. Trust your instincts - we're looking for genuine energy, not technical perfection. We want to share and amplify the artists in our community. If that's you, get your ideas down. If that's not you yet, could it be? You've got a few months to find out.

Entries will be placed on the DEF CON Forums for voting, and there will be prizes. There will also be gratitude, and opportunities to inspire others with your special way of seeing the world. We can't wait to see what you'll make!

DEF CON 30 Theme: Hacker Homecoming

Posted 11.12.21



This has been a crazy couple of years.

A global pandemic turned DEF CON 28 into DEF CON Safe Mode. Some easing of the restrictions and some strict attendance rules gave us a hybrid con for DC29. An improvement, to be sure, but something short of a full DEF CON experience.

We want DEF CON 30 to have the energy of a reunion. We'll be back together in a brand spanking new venue. We'll be thirty years old - an amazing milestone for a hacker conference under any circumstances. In honor of all that, we're calling DEF CON 30 'Hacker Homecoming'.

The first reason is that it's literally a return home. After two years of separation, we're looking forward to having more of our family under one roof, under the Vegas late summer sun.

There's also a North American tradition called 'Homecoming'. Secondary schools and colleges invite luminary alums back for a big celebration of the school's history and a toast to its future. We intend to do just that for DC30. We'll have some surprise guests from DEF CON's illustrious past on hand to talk about the amazing places their life has taken them since joining the DC Community. We'll also be laying out some of the map forward from our 30th Anniversary.

So please join us in the Caesar's Forums if you can, and on the Discord if you can't. Maybe even pack a fancy outfit for the homecoming dance. It's high time for a reunion.

Design Inspiration

This year's theme is about celebrating the past and getting geeked about the future, so we're looking for smooth integration of old school hacker stylee with future vibes.

We took the color palette inspiration from arguably the most iconic DEF CON image of all time: the rooftop photo from DEF CON 1.

The photo is amazing for any number of reasons, but the most important is that even though it screams early 90s hacker culture, it also shows some of the essence of what DEF CON is even in the 2020s. It's still a gathering of extraordinary digital misfits going Voltron in the Vegas night.

The fonts were also selected to be like a homecoming celebration, with some reverence for the past, some excitement about the future. The past is represented by the very 90s CityPop and Geom and the future by the futuristic minimalism of Open Sans.

Homework

As always, we'll be sharing movies, books, music and other random media to get you in the right frame of mind for maximum DEF CON. This year we're even giving you an extra few months to get through the syllabus. Watch the DEF CON site for additions to all the lists. Pencils UP!

Movies:

Sneakers
The Imitation Game
Zero Days

Books:

The Shockwave Rider
The Cuckoo's Egg
Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground
The Cult of the Dead Cow

The DEF CON 30 Call for Contests and Events is OPEN!

Posted 11.1.21



DEF CON 30 is going to be a big deal, and we're full speed ahead on planning. If you've got a stellar idea for a contest, this is your moment. Take advantage of the early opening to turn your idea into a real DEF CON Experience. The extra lead time helps us work with you to get the best ideas across the finish line, but only if you take advantage and get your submissions in.

You can read the rules and requirements on the [Call for Contests Page](#) . You can check the [DC29 Contest forum](#) for an idea of what we've accepted in the past.

Let's see what you've got percolating out there, DEF CON fam. Let's take DC30 up a notch.

Happy Halloween from DEF CON

Posted 10.31.21



DEF CON 30: Open and Upcoming Calls

Posted 10.26.21



The DEF CON 30 Call for Villages is already open! To see if your fave is already accepted, check out the [Villages forum for DEF CON 30](#) ! Don't see what you want on the current list? Maybe that's your cue to [submit a proposal](#) !

For the truly ambitious, there is still a [call open for the coveted title of CTF organizers](#) ! Only a little over two weeks left to put in your proposal to be the future of DEF CON Capture the Flag!

On the horizon very soon will be the Call for Contests! Polish those proposals for new DEF CON contests now and be ready for the call!

We only turn 30 once. Let's do it big!

DEF CON 30 Call for Villages has Opened!

Posted 10.1.21



DEF CON 30 may seem a long way off, but it's never too soon to start planning. Especially for something as close to the heart of the DEF CON experience as Villages.

As always, we're looking for new villages that will create welcoming, hands-on spaces for congoers to sharpen their skills, learn something new and maybe even find their newest obsession.

Space (both physical and metaphorical) is limited. Early submissions have increased chances of success. If the concept is strong but needs work, we can help but only if we have enough time.

You'll want to famailiarize yourself with the requirements and submission guidelines at <https://defcon.org/html/defcon-30/dc-30-cfv.html> first. If you can meet the preconditions, and you have a stellar idea to propose, that's the universe telling you it's go time. Rise to meet your moment.

We can't wait to see what's on your mind.

CTF Call for Organizers is Officially Open!

Posted 9.28.21



The mighty and venerable Order of the Overflow is retiring from organizing the DEF CON CTF, and the torch must be passed. This means a rare opportunity for you, CTF enthusiasts.

Are you ready to create the next generation of elite CTF tournaments? Do you have the skill and creativity to elevate the game for the world's best players? The drive to see your ideas through to completion? If this is you, it's time for us to talk.

The lowdown is at <https://defcon.org/html/links/dc-ctf-cfo.html> . Get familiar, submit the CTF you want to see in the world. For the chosen, glory awaits.

Live Music from DEF CON 29 is Posted!

Posted 9.16.21



The [live music from DEF CON 29](#) is now available on the DEF CON Media Server! Whether you missed the party in Vegas or you just need a gang of .flac bops for your earbuds, media.defcon.org has you covered.

Get some, shake your groove things and pass it on.

Car Hacking and Blue Team Village Talks from DEF CON 29!

Posted 9.12.21



More DEF CON 29 Village videos on the DEFCONConference YouTube channel - this time it's the [Blue Team Village](#) and [The Car Hacking Village](#) ! Please enjoy and share with everyone you think could gain from the information.

More Village Talks from DEF CON 29!

Posted 9.5.21



The Village talks deluge continues, with talks from [IoT Village](#) , [Blacks in CyberSecurity Village](#) , and [Aerospace Village](#) all ready to stream to your heart's content on YouTube! As always, enjoy and pass it on.

In-person Talks from DEF CON 29 Now Live on YouTube!

Posted 8.31.21



The [in-person talks from DEF CON 29](#) are now live on the DEF CON YouTube Channel! Time to catch up on some mighty fine panels and unique content you had to be in Vegas to see..UNTIL NOW!

[Press Page Updated for DEF CON 29!](#)

Posted 8.23.21



DEF CON 29 was about two weeks ago - thanks again to everyone who helped make a success of it both in person and online. We've updated the [press page](#) to include a bunch of later-breaking stories. Watch this space for a list of write ups!

[Adversary Village Talks are Live!](#)

Posted 8.17.21



More DEF CON 29 goodies for your enjoyment - the [talks from Adversary Village](#) are live on our [YouTube channel](#) ! Binge away - more Village goodness to come!

DEF CON 29 Contest results So Far!

Posted 8.13.21



Congratulations to everyone who participated in any of the DEF CON 29 contests. Getting in the ring is 90 percent of the magic, and we hope that everyone had fun, learned something and met cool new people.

The [contest results](#) we have so far have been posted, and we'll be updating the page as we get more in!

Thanks for a Great DEF CON 29!

Posted 8.10.21



The past few years have been crazy, but you can't stop the signal, even with global cataclysm. We are so happy to be reunited with so many of our friends, both here in Las Vegas and in the virtual con space. It's good to be together.

Thank you for your support through everything. Your unending enthusiasm sustains our work and the DEF CON community never disappoints. Thanks for following the stricter rules the pandemic made necessary. Thanks for being kind and patient with each other and with us as we navigate the swiftly changing landscape.

Next year is a big anniversary for DEF CON, and we're already at work planning how to make the big 3-0 memorable. Here's to next year reuniting even more of us.

In the meantime, keep in touch with us on the DEF CON Discord server. Join a local DC Group, or start one. Stay safe and healthy. DEF CON hearts you.

Interviews from DEF CON 29!

Posted 8.9.21



We'd like to shout out newly minted Photogoon Alex Chaveriat aka 'Silk' who spent his DEF CON 29 racing around the con floor finding cool projects to interview people about. If you follow the DC social media feeds you've probably seen some of his work this year. Thanks to everyone who gave him some time, and thanks to Alex for putting out so much quality stuff so quickly. [Alex Chaveriat on YouTube](#)

DEF CON 29 Press roundup!

Posted 8.8.21



We're on the last day of DEF CON 29, both in the virtual and physical worlds. There's so much going on it's easy to miss a few things. Here's a brief listing of some of the press coverage of our events this year.

[AND!XOR's DEF CON 29 Electronic Badge Is An Assembly Puzzle](#)
Hackaday

[Hands On: DEF CON 29 Badge Embraces The New Normal](#)
Hackaday

[Black Hat USA 2021 and DEF CON 29: What to expect from the security events](#)
Tech Republic

[Privacy Without Monopoly: DEFCON 29](#)
EFF

[We Have Questions for DEF CON's Puzzling Keynote Speaker, DHS Secretary Mayorkas](#)
EFF

[Hands-On: Whiskey Pirates DC29 Hardware Badge Blings With RISC-V](#)
Hackaday

[#DEFCON: Hacking RFID Attendance Systems with a Time Turner](#)
infosecurity

[#DEFCON: Why Social Media Security is Election Security](#)
infosecurity

[#DEFCON: A Bad eBook Can Take Over Your Kindle \(or Worse\)](#)
infosecurity

[#DEFCON: Ransomware Moves from Nuisance to Scourge](#)
infosecurity

[Black Hat USA 2021 & DefCon 29: Hybride IT-Security-Konferenzen starten in Kürze](#)
Heise.de

[The Cybersecurity 202: The year's biggest cybersecurity conferences are back, but limited](#)
The Washington Post

DEF CON 29 Badge Update (The Firmware Kind)!

Posted 8.5.21



In case you didn't know, you can head over to defcon.org/signal for a link to updated badge firmware and instructions! We hope you enjoy DEF CON 29, In-person, or from wherever you may be!

DEF CON 29 In-person Pre-Registration is Closed!

Posted 8.4.21



The DEF CON 29 pre-reg at shop.defcon.org is now closed. You can still get a badge with cash payment onsite while they last, and you can purchase the Human+ Discord role directly on our Discord (discord.gg/defcon) or at plus.defcon.org. Thanks to everyone for supporting DEF CON this year, whether you're attending virtually or here with us in Las Vegas. DEF CON ~ ~ U. Tomorrow it begins!

Get the DEF CON 29 Soundtrack!

Posted 8.4.21



Get a head start on DEF CON 29 with this year's Original Soundtrack! It's waiting for you on the DEF CON media server right now. Like, right now. You have your assignment.

media.defcon.org/DEF CON 29/

Hackers with Disabilities Guide for DEF CON 29!

Posted 8.2.21



Thanks to [@A_P_Delchi](#) and Hackers with Disabilities for creating this helpful [accessibility guide to DC29](#) . Don't hesitate to reach out if we can help maximize your DEF CON, either through goons or via social media.

[Return to Index](#)

© 1992-2023 DEF CON Communications, Inc. All Rights Reserved | [DEF CON Policies](#) | [DMCA Information](#)

DEF CON 31 FAQ

FAQ

FREQUENTLY ASKED QUESTIONS

When & Where will DEF CON be?

Aug. 10-13, 2023 at Caesars Forum + Flamingo, Harrah's and Linq in Las Vegas!

Can I book my hotel in Las Vegas now – and how should I do that?

Yes, hotel reservations are being accepted. In order to help us fill our room block with our contracted hotels please book under the [DEF CON group room registration](#).

What is DEF CON doing for DC31, and how can I attend?

DEF CON 31 will be at full operating capacity this year, We will be hosting our full con in-person in Las Vegas and some approved villages and contests may be contributing additional online content within the official DEF CON Discord. All Online content will be similar to the 2020 & 2021 cons.

To see what happenings are currently planning to be in-person, hybrid, or virtual only please visit <https://forum.defcon.org/node/243392>

How much will DEF CON cost?

The price to attend DEF CON in-person will be \$440 USD cash on site. You may not attend in-person without purchasing a badge. Attending virtual on our Discord will be free, and those with Human+ will have more permissions and access.

Can I buy a DEF CON badge with Black Hat?

Yes, it will be an option when you check out at Black Hat.

How do I participate in virtual DEF CON?

For the virtual portion of DEF CON you will need a Discord account.

You can find detailed [instructions on getting on the DEF CON Discord server here](#). There is a [FAQ for Humans on Discord](#) as well.

Connect to the DEF CON Discord Server: <https://discord.gg/DEFCON>

To see what happenings are currently planning to be in-person, hybrid, or virtual only please visit <https://forum.defcon.org/node/239768>

What if I don't want a Discord Account?

While we don't think you'll get the full experience, all of our content will be released via YouTube and put on the DEF CON Media Server.

Will there be Uber Badges again?

Our annual tradition of awarding black "Uber" badges for CTF and other select contests, will continue, for in-person events only. To make sure that attendees are playing contests with the full hacker spirit we don't announce which contests qualify for an Uber Badge ahead of the contest (aside from the Official CTF) . We want to see how well each contest operates, and how players perform, so those decisions aren't made until Sunday of the con. Check out the registry of past [black badge winners!](#)

Where can I find more info on the DEF CON CTF?

DEF CON CTF Qualifiers May 26-27. Please follow Nautilus CTF on twitter at https://twitter.com/Nautilus_CTF and keep a look out on their CTF website at <https://nautilus.institute>. For a little history on the contest check out the [CTF History](#) page.

I have a black badge, do I need to pre-register?

No, just show up on site and go to inhuman registration. The rules governing the use of Black Badges are available on the [Black Badge Policy Page](#). If you notice any errors or omissions in the list, please contact us at info@defcon.org. Congratulations to everyone who's earned a Black Badge and good luck to all who seek one.

What will capacity look like for the in-person event?

Capacity is currently capped at each given space's fire code standard capacity. In case of changing health and safety recommendations, limits will be reviewed and revised at the direction of Southern Nevada Health District (SNHD) and there will be dedicated support onsite to ensure our policies are being followed.

What health measures/protocols is DEF CON taking to ensure a safe environment on-site?

DEF CON is working closely with Caesars Entertainment hotels to provide a safe and healthy experience for all. We will comply with whatever safety measures are required of us. Check out DEF CON [31 Covid Policy](#) for more details

Will I be required to wear a mask?

We're adapting our protocols for DEF CON 31. The meeting space air handlers use Merv 13 filters for better filtration of particulate matter, the air handler coils are cleaned regularly, and we're adding additional air filters to the areas likely to get crowded.

We will have masks on hand for anyone who needs them as well as a finite number of test kits onsite as well. There will be lists of resources for testing and treatment available in the program and at the Info Booth.

Wearing a mask remains the safest option, but with these changes **our policy is masks strongly recommended.**

We appreciate the DEF CON Community pulling together to keep each other healthy, and we trust you'll continue to look after one another. The situation isn't quite back to normal so be safe out there, and we'll see you very soon.

What's DEF CON's official theme for DEF CON 31?

'We are living through a revolt against the future. The future will prevail.' This DEF CON is about the future we want to bring into being, together. DEF CON's hacker community has a powerful role to play in whatever comes next, From hardware to policy, from biohacking to satellites. More info on our official theme is here on our [DEF CON 31 Theme & Style Guide](#)

Where can I get more information about what's happening?

Check out the following DEF CON Sites & Social Media.

[Forums](#)
[Groups](#)
[Discord](#)

[Twitter](#)
[Facebook](#)
[Reddit](#)
[DEF CON YouTube channel](#)
[DEF CON Twitch](#)
[DEF CON Music Twitch](#)
[DEF CON Media Server of all past conference materials](#)

[Return to Index](#)

© 1992-2023 DEF CON Communications, Inc. All Rights Reserved | [DEF CON Policies](#) | [DMCA Information](#)

DEF CON FAQ

Frequently asked questions about DEF CON

What is DEF CON?

DEF CON is one of the oldest continuously running hacker conventions around, and also one of the largest.

How did DEF CON start?

Originally started in 1993, it was meant to be a party for members of "Platinum Net", a Fido protocol based hacking network out of Canada. As the main U.S. hub I was helping the Platinum Net organizer (I forget his name) plan a closing party for all the member BBS systems and their users. He was going to shut down the network when his dad took a new job and had to move away. We were talking about where we might hold it, when all of a sudden he left early and disappeared. I was just planning a party for a network that was shut down, except for my U.S. nodes. I decided what the hell, I'll invite the members of all the other networks my BBS (A Dark Tangent System) system was a part of including Cyber Crime International (CCI), Hit Net, Tired of Protection (ToP), and like 8 others I can't remember. Why not invite everyone on #hack? Good idea!

Where did the name come from?

The short answer is a combination of places. There was a SummerCon in the summer, a HoHoCon in the winter, a PumpCon during Halloween, etc. I didn't want any association with a time of year. If you are a Phreak, or just use your phone a lot you'll note "DEF" is #3 on the phone. If you are into military lingo DEF CON is short for "Defense Condition." Now being a fan of the movie War Games I took note that the main character, David Lightman, lived in Seattle, as I do, and chose to nuke Las Vegas with W.O.P.R. when given the chance. Well I knew I was doing a con in Vegas, so it all just sort of worked out.

There are several resources that will give you an idea of what DEF CON is all about.

[DEF CON Press](#): through the prism of the media

[DEF CON Groups](#): Local groups that meet

[DEF CON Media Server](#): DC 1 to the present, captured

[Google](#): always a good research starting point

Just remember, DEF CON is what you make of it.

When and where is DEF CON?

DEF CON is generally in the last week of July or first week of August in Las Vegas. DEF CON 31 will be held August 10th through August 13th, 2023. Many people arrive a day early, and many stay a day later.

Isn't there a DEF CON FAQ already?

Yes, an unofficial one. It's quite humorous, sometimes informative, and DEF CON takes no responsibility for its content. It is archived [here](#).

What are the rules of DEF CON?

Physical violence is prohibited. Harassment of any kind is prohibited. We don't support illegal drug use. Minors should be accompanied by their parent(s) or guardian(s). Please refrain from doing anything that might jeopardize the conference or attendees such as lighting your hair on fire or throwing lit road flares in elevators. DEF CON Goons are there to answer your questions and keep everything moving. Hotel security is there to watch over their property. Each has a different mission, and it is wise to not anger the hotel people. Please be aware that if you engage in illegal activities there is a large contingency of feds that attend DEF CON. Talking about how you are going to bomb the RNC convention in front of an FBI agent is a Career Limiting Move!

You can view the DEF CON Code of Conduct at <https://defcon.org/html/links/dc-code-of-conduct.html>.

Is DEF CON cancelled?

No.

What is there to do at DEF CON?

DEF CON is a unique experience for each con-goer. If you google around you'll find dozens of write-ups that will give you an idea of what people have experienced at DEF CON. Trust write-ups more than media articles about the con. Some people play capture the flag 24x7, while many people never touch a computer at DEF CON. Some people see every speech they can, while others miss all speeches. Other activities include contests, movie marathons, scavenger hunts, sleep deprivation, lock picking, warez trading, drunken parties, spot the fed contest, the official music events. Because DEF CON is what the attendees make of it, there are more events than even we are aware of. Half the fun is learning what happened at DEF CON after the fact!

I'm not a hacker, should I go to DEF CON?

Many people have different definitions of what is a 'hacker'. I would recommend looking at previous years speeches, and write-ups from past attendees - this should give you a good idea if DEF CON is for you. This hacker FAQ might give you some insight into the matter as well. If you do not have any technical interests, DEF CON is probably not for you. Sure there is a lot of socializing you can do, but technology and hacking is the core of the con.

Do criminals go to DEF CON?

Yes. They also go to high school, college, work in your workplace, and the government. There are also lawyers, law enforcement agents, civil libertarians, cryptographers, and hackers in attendance. Sshhh. Don't tell anyone.

What are Goons?

They are the staff at DEF CON. They have many roles including safety, speaker coordination, vendor room coordination, network operations, et cetera... Please try to be helpful to them if they make requests of you. If any goon tells you to move, please do so immediately as there may be safety issues they are attempting to address.

How can I help out or become a Goon?

The staff at DEF CON has grown organically. All positions have some degree of trust associated with them, so typically new goons are 'inducted' by friends of existing goons. There are many random points when goons need help and may ask people for help, generally for helping move stuff or other tasks that don't require high amounts of trust or unsupervised work. Just because you help out doesn't make you a goon. If you really want to be a goon, talk with one and see how much work they actually do (Hint: you may want to enjoy being at DEF CON, not working full-time at it). One year the network group got a new Goon when a networking engineer was needed, and he came to the rescue. The intent behind the goons is not to be elitist, but to have a network of trusted people who can help run the conference - please do not feel upset if you are not chosen to be a goon.

How can I help or participate?

DEF CON is not a spectator sport! Before the con, during, and after there are chances for you to get involved. Before the con you can read about the contests and maybe sign up for one like Capture the Flag. There are artwork contests for shirts and posters. You can practice your lock pick skills, or just get your laptop all locked down and ready to do battle. Organize your .mp3s. Check out the DEF CON Forums to see what other people are up to. If you want to create your own event, you can do that as well - you will not get official space or sanctions, but virtually every official event at DEF CON started out as an unofficial event.

I would love to see XYZ event, how do I make this happen?

Virtually all events at DEF CON were conceived by the attendees. The DEF CON forums are a great place for recruiting help for an event you want to put on, and making sure your efforts aren't being duplicated. If it doesn't require resources from DEF CON (space, namely) you generally don't have to ask anyone's permission. Most events are unofficial until they've been going on for a couple of years. Please let us know if you have an idea for an event, we may help facilitate or promote it. Email [suggestions at DEF CON dot org] to keep us in the loop.

How can I speak at DEF CON?

You can [submit a response to our CFP](#) (call for papers). All entries are read and evaluated by a selection committee. We would love to have your submission. The call for papers usually opens in January and closes mid-May.

I'm press, how do I sign up, why can't I get in for free (I'm just doing my job)?

Please email [press\[at\]defcon\[d0t\]org](mailto:press@defcon.org) if you wish press credentials. Lots of people come to DEF CON and are doing their job; security professionals, federal agents, and the press. It wouldn't be fair to DEF CON attendees if we exempted one group from paying. If you are a major network and plan on doing a two minute piece showing all the people with blue hair, you probably shouldn't bother applying for a press pass - you won't get one. If you are a security writer or from a real publication please submit, and someone will respond with an answer.

I want to sell stuff, how do I do this?

If you want a space in our vendor area, you need to apply. Because of limited space and our attempt to have a diversity of vendors, you may not be able to get a booth. It is wise to think of staffing issues - if you are one person do you want to spend your entire time behind a vendors booth?

What are the different price rates?

Everyone pays the same: The government, the media, the 'well known hackers', the unknown script kiddies. The only discount is for Goons and speakers, who get to work without paying for the privilege.

How much is admission DEF CON, and do you take credit cards?

The price for DEF CON 31 is \$440 USD Cash at the Door. We do this for a number of reasons. Paying in cash protects your privacy and we can't be forced to hand over records we don't collect.

Does my underage child need a badge?

Children under the age of 8 will not need to purchase a badge.

Can I get a discount on DEF CON badges?

DEF CON charges one price regardless of your social status or affiliation. Please know that we depend on attendee income to pay the costs of the conference and don't have sponsors to help defray the expenses.

We sometimes get requests for discounts [students, veterans, children], unfortunately we don't want to try and validate if you are a current student, look at your ID to determine your age, decode military discharge papers, etc.

If you really want to attend DEF CON for free then do something for the con.

You could:

Submit a CFP and be an accepted speaker or workshop instructor.

Work on a contest, event, or village.

Qualify for CTF/Contests that include entry.

Find a team to become a Goon newbie.

Contribute to content, or perform some entertainment.

I need a letter of invite for my visa application, how do I get that?

In most cases, DEF CON can send a signed letter of invite, usually within a few short business days once we have all the info. If you also require verification of housing, we can put you in touch with someone to help you get your hotel stay organized, let us know if you need that.

Along with your request, please email us the following to [info\(at\)defcon\(.\)org](mailto:info@defcon.org)

Name as is on passport:

Passport number:
Country of issue:
Date of issue:
Date of expiration:
Country of origin:

DEF CON is too expensive, how can I afford it?

DEF CON is cheaper than many concerts, and certainly cheaper than many shows in Vegas. Many people have made an art and science out of coming to DEF CON very cheaply. Here are a couple of tips.

Travel: Buy airfare in advance, go Greyhound, Carpool, hitch-hike. (Note: this may be dangerous and/or illegal.)

Lodging: Share rooms - some people have up to 10 people they share a room with, find a hotel cheaper than the one that the conference is scheduled at, stay up for three days, etc. (note: this can be hazardous to your health.)

Food: Pack food for your trip, go off site to find food, eat in your hotel rooms, and look for cheap Vegas food at Casinos. (Look for deals and specials that are trying to get you in the door to gamble.)

Booze: You don't need to drink. Brew your own and bring it. (It's been done.)

Entrance: Admission can be saved, mow some lawns. Try to go to another 4 day event for cheaper than this that offers so much. We have increased the fees slowly over the years, but also the amount and quality of events have increased.

Inevitably people will try to do some math and pretend that DT gets rich each DEF CON - they seem to lack the ability to subtract.

How many people typically attend DEF CON?

There have been roughly 25-28k attendees in the last few (pre-COVID) years of DEF CON. DEF CON 27 had a record showing with approximately 30,000.

Is there a network at DEF CON?

Why yes, DEF CON is FULLY network-enabled. Now that we've perfected the art of a stable hacker con network, we're ascending to a higher level - we're providing you a network that you feel SAFE in using! Since DEF CON 18 we're WPA2 encrypted over-the-air, with a direct trunk out to the Internet. No peer-to-peer, no sniffing, just straight to the net (and internal servers). We'll provide login credentials at Registration. We know the LTE airwaves will be saturated so we're putting our own cred on the line to give you a net that even we would put our own mobile phones on.

If you're feeling frisky, we'll still have the traditional "open" network for you - bring your laptop (we'd recommend a clean OS, fully patched--you know the procedure) because we don't police what happens on that net. Share & enjoy!

What is the age limit?

People have brought children to DEF CON - it is not recommended to do this unless you are going to constantly supervise them. It is generally an 'adult' atmosphere (language, booze, et cetera). If you've never been to DEF CON, you may want to refrain from bringing your children (unless they are demanding that you bring them). While there are no age limits, we have consistently cooperated with parents and/or private investigators who are looking for children that 'ran away from home' to go to DEF CON. You will have to be 21 to reserve a room.

What is a DEF CON "Black Badge"?

The Black Badge is the highest award DEF CON gives to contest winners of certain events. CTF winners sometimes earn these, as well as Hacker Jeopardy winners. The contests that are awarded Black Badges vary from year to year, and a Black Badge allows free entrance to DEF CON for life, potentially a value of thousands of dollars.

How can I get a hold of DT? I tried to mail him and haven't seen a response yet.

DT doesn't dislike you, isn't trying to hurt your feelings, and bears you no ill will. The fact is he gets an unmanageable load of mail continually. Mailing him again may elicit a response. Try mailing FAQ (at) DEFCON.ORG if you have a general question that isn't answered here or in the forums.

Is it hot in Vegas?

Yes. Bring sunscreen (high SPF), do not fall asleep near the pool (lest you wake up to sunburn), and do not walk far in the sun unless you are experienced in dealing with extreme heat. The sun is dangerous in Las Vegas. Sleeping in lawn chairs is a sure way to wake up to severe burns in the morning when that bright yellow thing scorches your skin. Drink plenty of water and liquids - remember that alcohol will dehydrate you.

What should I bring?

It depends on what you're going to do at DEF CON. This is discussed in quite some depth on the [unofficial DC FAQ](#), as well as a thread in the DC Forums. You may want to bring fancy (or outrageously silly) clothes for the official Music events, on Friday and Saturday nights, where everyone shows off nifty attire.

How much do rooms cost, and how do I reserve a room?

The DEF CON 30 group room registration is now live! We have room rates at several hotels, until they run out of rooms in our block.

Follow this link: <https://book.passkey.com/go/SHDEF3>

Do not worry if the form doesn't immediately show the discounted rate. To verify that you're getting our price you can mouse over the dates you've selected or begin the checkout process.

How much is internet access?

We are looking into this. Free (and possibly more dangerous) internet access is available in the convention area.

Will the hotels broadcast the speeches on their cable system?

DEF CON TV has successfully streamed all tracks to all the hotels, and a couple of tracks out to the internet, for several years now. We don't expect this will change!

Will we have DEF CON branded poker chips?

You will have to attend DEF CON to find out.

Will conference attendees have entire floors of hotel rooms to themselves?

Probably not. The hotel is very cooperative in attempting to centralize the DEF CON attendees, for their convenience and ours, but there will be non-DEF CON attendees in hotel rooms next to us.

This FAQ didn't answer my questions, or was unclear, how can I get further information?

Check out the [DEF CON Forums](#) to ask follow up questions.

[Return to Index](#)

© 1992-2023 DEF CON Communications, Inc. All Rights Reserved | [DEF CON Policies](#) | [DMCA Information](#)

Links to DEF CON 31 related pages

Villages Table

Each Village, as it's name may imply, specializes in a topic or aspect of security or computers.

One Page [All Villages](#) list with descriptions

DEF CON 31 All Villages [Forum page](#)

You may need to scroll to the right to see all info

Village Name Home Page	Map	Schedule	Forum Link	Social Media Links
Aerospace Village	Map	Sched	Forum	TW @secureaerospace LI @aerospace-village TW @hack_a_sat DC https://discord.gg/gV4EWuk YT https://www.youtube.com/c/AerospaceVillage
AppSec Village	Map	Sched	Forum	TW @AppSec_Village LI @appsecvillage YT https://www.youtube.com/c/AppSecVillage DC https://discord.gg/5XY8qYXd7R
Artificial Intelligence Village	Map	Sched	Forum	TW @aivillage_dc TI @aivillage YT link DC https://discord.com/invite/GX5fhfT
Bio Hacking Village	Map	Sched	Forum	TW @dc_bhv LI @biohacking-village YT http://youtube.com/biohackingvillage TI @biohackingvillage DC https://discord.gg/Q8subDb5 IG @biohacking_village SP link
Blacks in Cybersecurity	Map	Sched	Forum	TW @BlackInCyberCo1 IG @blackincyberconf TI @blacksincybersecurity YT link LI @blackincyberconference PT @blacksincybersecurity FB @blackincyberconf
Blue Team Village	Map	Sched	Forum	TW @BlueTeamVillage TI @blueteamvillage YT https://www.youtube.com/c/blueteamvillage DC https://discord.gg/blueteamvillage DC https://discord.com/invite/blueteamvillage
Car Hacking Village	Map	Sched	Forum	TW @CarHackVillage YT http://youtube.com/@carhackingvillage DC https://discord.gg/JWCcTAM
Cloud Village	Map	Sched	Forum	TW @cloudvillage_dc YT https://www.youtube.com/cloudvillage_dc DC https://discord.gg/EygUDJABee
Crypto Privacy Village	Map	Sched	Forum	TW @cryptovillage SL https://cryptovillage.slack.com/ YT link

Village Name Home Page	Map	Schedule	Forum Link	Social Media Links
				TI @cryptovillage
Data Duplication Village	Map	Sched	Forum	TW @DDV_DC TI @defcon_groups DC https://discord.gg/bsX4QXf3rD YT link
DEF CON Groups VR	Map	Sched		TW @DCGVR TI @defcon_groups DC https://discord.gg/bsX4QXf3rD YT link
Embedded Systems Village	Map		Forum	TW @EmbeddedVillage
Ham Radio Village	Map		Forum	TW @HamRadioVillage TI @HamRadioVillage DC https://discord.gg/hrv
Hardware Hacking Solder Skills Villages	Map	Sched	Forum	TW @DC_HHV
Industrial Control Systems Village	Map	Sched	Forum	TW @ICS_Village LI @icsvillage YT link TI @ics_village
Internet Of Things Village	Map		Forum	TW @iotvillage TW @ISEsecurity TW @Villageidiotlab LI @iotvillage TI @iotvillage YT https://www.youtube.com/c/IoTVillage/videos DC https://discord.gg/EFKbNFrFaN
Lock Pick Village	Map		Forum	TW @toool TI @toool_us YT https://youtube.com/c/TOOOL-US
MisInformation Village	Map	Sched	Forum	TW @Misinfovillage https://defcon.social/@misinformationvillage
Packet Hacking Village	Map	Sched	Forum	TW @wallofsheep FB @wallofsheep YT https://youtube.com/wallofsheep TI @wallofsheep PS https://www.periscope.tv/wallofsheep https://wallofsheep.tumblr.com/ IG @wallofsheep
Paid Training			Forum	
Password Village	Map		Forum	TW @PasswordVillage TI @passwordvillage YT link
Payment Village	Map		Forum	TW @paymentvillage TI @paymentvillage YT link https://t.me/paymentvillage
Physical Security Village	Map		Forum	TW @physsec TI @bypassvillage LI @physsec

Village Name Home Page	Map	Schedule	Forum Link	Social Media Links
Policy Village	Map	Sched	Forum	TW @DEFCONPolicy link
Quantum Village	Map		Forum	TW @quantum_village DC https://discord.gg/6WUjH5cBXu LI @quantumvillage YT https://youtube.com/@quantum_village/
Radio Frequency Village	Map		Forum	TW @rfhackers TW @rf_ctf link DC https://discordapp.com/invite/JjPQhKy
Recon Village	Map	Sched	Forum	TW @ReconVillage FB @reconvillage YT https://www.youtube.com/reconvillage/
Red Team Village	Map	Sched	Forum	TW @RedTeamVillage_ YT https://www.youtube.com/redteamvillage TI @redteamvillage DC https://discord.gg/redteamvillage
Social Activities: Parties/Meetups	Map		Forum	
Social Engineering Village	Map	Sched	Forum	TW @sec_defcon YT link TI @se_community LI @social-engineering-community FB @Social-Engineering-Community-108883855139272
Tamper Evident Village	Map		Forum	
Telecom Village	Map	Sched	Forum	TW @TelecomVillage
Voting Village	Map		Forum	TW @votingvillagedc YT link
XR Village	Map		Forum	TW @XRVillage LI @xr-village

Contests Table

Various contests, some lasting all 4 days of DEF CON, some short time on stage

One Page [All Contests](#) list with descriptions
DEF CON 30 All Contests [Forum page](#)

You may need to scroll to the right to see all info

? Cube Contest Info	5n4ck3y Contest Info
Adversary Wars CTF Contest Info	AutoDriving CTF contest Contest Info
Battle of the Bots Contest Info	Blacks In Cyber Village CTF Contest Info
Blue Team Village CTF Contest Info	Capture the Packet Contest Info
Car Hacking Village CTF Contest Info	Cloud Village CTF Contest Info
CMD+CTRL Cyber Range Contest Info	CrackMeIfYouCan Contest Info
Creative Writing Short Story Contest Contest Info	Darknet-NG Contest Info
DC Kubernetes Capture the Flag (CTF) Contest Info	DC Sticker Design Contest Contest Info
DC's Next Top Threat Model (DCNTTM) Contest Info	DEF CON 31 Beard and Mustache Contest Contest Info
DEF CON Chess Tournament Contest Info	DEF CON Scavenger Hunt Contest Info
DEFCON MUD DUMB TERMINAL EDITION Contest Info	Dungeons@Defcon Contest Info
Embedded CTF Contest Info	Hac-Man Contest Info
Hack-A-Sat 4 (HAS4) Contest Info	Hack3r Runw@y Contest Info
Hacker Jeopardy Contest Info	HackFortress Contest Info
Ham Radio Fox Hunting Contest Contest Info	Hardware Hacking Village CTF Contest Info
HardWired Contest Info	IntelOps – Operation Spacewatch Contest Info
IoT Village CTF Contest Info	It's In That Place Where I Put That Thing That Time Contest Info
Maps of the digital lands Contest Info	Octopus Game Contest Info
Phish Stories Contest Info	pTFS Presents: Mayhem Industries – Starphish Contest Info
Pub Quiz at DEF CON Contest Info	Radio Frequency Capture the Flag Contest Info

Red Alert ICS CTF Contest Info	Red Team CTF Contest Info
Social Engineering Community (SEC) Vishing Competition Contest Info	Social Engineering Community (SEC) Youth Challenge Contest Info
TeleChallenge Contest Info	The Beverage Cooling Contraption Contest Contest Info
The Dark Tangent Look-Alike Contest Contest Info	The Gold Bug Challenge Contest Info
The Lonely Hard Drive Contest Info	Tinfoil Hat Contest Contest Info
TOOOL Dozier Drill Lockpicking Challenge Contest Info	Trace Labs OSINT Search Party CTF Contest Info
venator aurum – A Treasure Hunt Contest Info	Whose Slide Is It Anyway? Contest Info

Party,Gather,Event Table

Various Parties, Gatherings, and Events

One Page [All Parties, Gatherings, Events](#) list with descriptions
DEF CON 31 All Parties, Gatherings, Events [Forum page](#)

You may need to scroll to the right to see all info

Arcade Party Event Info
Arts and Entertainment general discussion Event Info
Betting on Your Digital Rights: 2nd Annual EFF Benefit Poker Tournament at DC31 Event Info
BIC 301-303 – Blacks in Cyber Lituation Party Event Info
BlanketFort Con Event Info
Blue Team Village Pool Party Event Info
Books, Books, Books will Prevail Event Info
Capitol Tech University Event Info
CULT OF THE DEAD COW BREAKS THE INTERNET (and you can too!) Event Info
CycleOverride DEF CON Bike Ride Event Info
DC 404/DC 678/ DC 770/ DC 470 (Atlanta Metro) Event Info
DC Kids Meetup Event Info
DEF CON Holland Group Presents: VrijMiBo Event Info
Defcon.run Event Info
EFF Tech Trivia Event Info
Friends of Bill Event Info
GOTHCON 2023 Event Info
Hack The Box Event Info
Hacker Flairgrounds Event Info
Hacker Karaoke Event Info

Hacking Policy & Prompts – Happy Hour Event Info
Ham Radio Exams Event Info
Lonely Hackers Club Event Info
Panel: Ask the EFF Event Info
Queercon Mixers Event Info
Queercon Party Event Info
S.O.D.A Machine (Shell On Demand Appliance) Event Info
The Book Exchange Event Info
THE UNOFFICIAL DEF CON SHOOT Event Info
Toxic BBQ Event Info
University of Advancing Technology Event Info
VETCON Event Info
Village People Party Event Info
WISP Chill Out Space with Refreshments Event Info
Wisp Community Meet Up at BTV Pool Party Event Info
WISP DEF CON Scholars Meetup Event Info
WISP Peer-to-Peer Mentoring and Networking Event Info

DemoLabs Table

Brief demonstrations for people to show off their project.

One Page [All Demolabs](#) list with descriptions

DEF CON 31 All Demolabs [Forum page](#)

You may need to scroll to the right to see all info

Abusing Microsoft SQL Server with SQLRecon – Sanjiv Kawa Demolabs Info
Am I Exploitable? (MI-X) – Ofri Ouzan & Yotam Perkal Demolabs Info
Attack Surface Framework – Prajwal Panchmahalkar & Mike Henkelman Demolabs Info
BBOT (Bighuge BLS OSINT Tool) – TheTechromancer (Joel Moore) & Paul Mueller Demolabs Info
BLE CTF – Ryan Holeman & Alek Amrani Demolabs Info
Build Inspector – A modern Javert on the trail of CI/CD Anomalies and Intruders – Jeremy Banker Demolabs Info
CNAPPGoat – Noam Dahan, Igal Gofman Demolabs Info
Dracon – Spyros Gasteratos Demolabs Info
Ek47 – Payload Encryption with Environmental Keys – Kevin Clark, Skyler Knecht Demolabs Info
EvilnoVNC: Next-Gen Spear Phishing Attacks – Joel Gámez Molina Demolabs Info
FlowMate – Florian Haag, Nicolas Schickert Demolabs Info
Glyph – Corey Hartman Demolabs Info
HardHat Command & Control Framework – Jonathan Owens Demolabs Info
ICS Forensics tool – Maayan Shaul & Ori Perez Demolabs Info
Katalina – Gabi Cirlig Demolabs Info
Kraken, a modular multi-language webshell for defense evasion – Raul Caro Demolabs Info
Lambda Looter – Doug Kent & Rob Ditmer Demolabs Info
Lupo: Malware IOC Extractor – Vishal Thakur Demolabs Info
OpenSSF Scorecard – Naveen Srinivasan & Neil Naveen Demolabs Info
OWASP crAPI: Completely Ridiculous API – Jayesh Ahire and Roshan Piyush Demolabs Info

Pcapinator: Rise of the PCAP Machines – Mike Spicer & Henry Hill Demolabs Info
ProjectDiscovery Nuclei – Brendan O’Leary & Pj Metz Demolabs Info
Red Wizard: user-friendly Red Teaming infrastructure – Ben Brücker Demolabs Info
RuleProcessorY & Gramify – Rule Optimization & Password Analysis tools – Niels Loozekoot Demolabs Info
Saturday – Joshua Herman Demolabs Info
Shufflecake, AKA Truecrypt on Steroids for Linux – Tommaso Gagliardoni & Elia Anzuoni Demolabs Info
Strix Interceptor – Lexie Thach Demolabs Info
SucoshScanny – Mustafa Bilgici, Tibet Ögüncü Demolabs Info
T3SF (Technical TableTop Exercises Simulation Framework) – Federico Pacheco, Joaquin Lanfranconi Demolabs Info
The Metasploit Framework – Spencer McIntyre Demolabs Info
The Wifydra: Multiheaded RF Panopticon – Lozaning Demolabs Info
ThreatScraper: Automated Threat Intelligence Gathering and Analysis for VirusTotal – Aaron Morath & Dr. Scott Graham Demolabs Info
USBvalve – Expose USB activity on the fly – Cesare Pizzi Demolabs Info
Vacuum Robot Hacking – Dennis Giese Demolabs Info
Veilid – TC Johnson & Deth Veggie Demolabs Info
Vulnerable by Design: Unguard, The Insecure Cloud-Native Twitter Clone – Simon Ammer, Christoph Wedenig Demolabs Info

Workshops Table

Longer, more detailed, hands on, lasting half a day.

These have limited seating. These will fill up VERY quickly!

These workshops are all SOLD OUT. Their registration opened July 5 Noon PDT

One Page [All Workshops](#) list with descriptions

DEF CON 31 All Workshops [Forum page](#)

You may need to scroll to the right to see all info

SOLD OUT – Creating and uncovering malicious containers Redux – Adrian Wood, David Mitchell Workshop Info
SOLD OUT – Flipping the Coin: Red and Blue Teaming in Windows Environments – Angus Strom, Troy Defty Workshop Info
SOLD OUT – Snakes on a Screen: Taming... – Anthony Rose, Gannon “Dorf” Gebauer, Vincent "Vinnybod" Rose Workshop Info
SOLD OUT – Pentesting Industrial Control Systems: OCP-U-HACK – Arnaud SOULLIE, Alexandrine TORRENTS Workshop Info
SOLD OUT – Hands-On TCP/IP Deep Dive with Wireshark – Chris Greer Workshop Info
SOLD OUT – The Petting Zoo: Breaking into CTFs – Christopher Forte, Robert Fitzpatrick Workshop Info
SOLD OUT – Hacking The Metal: An Intro to ARM Assembly Language Programming – Eigentourist Workshop Info
SOLD OUT – Starbase: open source graph security analysis – Guillaume Ross, Austin Kelleher, Adam Pierson Workshop Info
SOLD OUT – How hackers can send feedback directly to policymakers like the pros – Harley Geiger, Amit Elazari Workshop Info
SOLD OUT – Long Live the Empire... – Jake "Hubble" Krasnov, Dylan "CyberStryke" Butler, Kevin “Kent” Clark Workshop Info
SOLD OUT – Hide your kids, turn off your Wi-Fi, they Rogue... – James Hawk, Lander Beyer, Daniel Costantini Workshop Info
SOLD OUT – Email Detection Engineering and Threat Hunting Inbox – Josh Kamdjou, Alfie Champion Workshop Info
SOLD OUT – Analysis 101 for Incident Responders – Kristy Westphal Workshop Info
SOLD OUT – Android App Hacking – Maria Uretsky, Kavia Venkatesh, Sajjad "JJ" Arshad, Olivier Tuchon Workshop Info
SOLD OUT – Introduction to Cryptographic Attacks – Matt Cheung Workshop Info
SOLD OUT – DotNet Malware Analysis Masterclass – Max Kersten Workshop Info
SOLD OUT – BLE Security 201 – Maxine Filcher, Zach Reavis Workshop Info
SOLD OUT – House... – Maxwell Dulin, Nathan Kirkland, Zachary Minneker, Kenzie Dolan, Elizabeth St. Germain Workshop Info
SOLD OUT – Digital Forensics and Incident Response Against the Digital... – Michael Solomon, Michael Register Workshop Info

SOLD OUT – These Port Scans are Trash: Improving Nmap by Writing New Scripts and Libraries – Phil Young Workshop Info
SOLD OUT – Advanced WiFi Attacks for Red Team Professionals – Raúl Calvo Laorden Workshop Info
SOLD OUT – Getting into Trouble with Machine Learning Models – Robert Koehlmoos Workshop Info
SOLD OUT – Protecting the AWS ecosystem – Rodrigo Montoro Workshop Info
SOLD OUT – Active Directory Attacks: The Good, The Bad, and... – Ryan Chapman, Aaron Rosenmund, Brandon DeVault Workshop Info
SOLD OUT – Learning to Hack Bluetooth Low Energy with BLE CTF – Ryan Holeman Workshop Info
SOLD OUT – Machine Learning for N00bs – Sam Bowne, Elizabeth Biddlecome, Kaitlyn Handelman, Irvin Lemus Workshop Info
SOLD OUT – Introduction to Exploit Development – Sam Bowne, Elizabeth Biddlecome, Kaitlyn Handelman, Irvin Lemus Workshop Info
SOLD OUT – Applied Emulation – Sergei Frankoff, Sean Wilson Workshop Info
SOLD OUT – The Joy of Reverse Engineering: Learning With Ghidra and WinDbg – Wes McGrew Workshop Info
SOLD OUT – Malware development on secured environment – Yoann DEQUEKER Workshop Info

Paid Training Table

2 day training sessions on the Mon and Tue after DEF CON. There will be an additional cost for these.

One Page [All Paid Training](#) list with descriptions

DEF CON 31 All Paid Training [Forum page](#)

DEF CON 31 Training [Signup Pages](#)

You may need to scroll to the right to see all info

Cloud Security Masterclass Defender's Guide to Securing AWS &... \$2,000 early \$1,600 – Abhinav Singh Paid Training Info
– API Exploration and Exploitation \$2,800 Paid Training Info
Hacking Organizations: Phishing Not Required \$1,500 – Ben Sadeghipour Paid Training Info
Cyber Threat Intelligence A... \$1,900 – Bobby Thomas, Matthew Lamanna, Kyle Smathers, Nathan Johnson Paid Training Info
TCP/IP Deep Dive for Ethical Hackers – Featuring Wireshark \$1,400 – Chris Greer Paid Training Info
Hackable.sol: Smart Contract Hacking in Solidity \$1,500 – Davide Cioccia Paid Training Info
Simulated Adversary – Jayson E. Street Paid Training Info
Cloud Forensics Workshop and CTF Challenge: Lab Rat Edition – Kerry Hazelton Paid Training Info
Hands-on incident response in the cloud — Microsoft edition \$2,250 – Korstiaan Stam Paid Training Info
A Practical Approach to Breaking & Pwning Kubernetes Clusters \$2,800 – Madhu Akula Paid Training Info
– Offensive IoT Exploitation \$2,000 Paid Training Info
SOC 101 – Rod Soto Paid Training Info
Hacking Cryptography \$2,000 – Ruben Gonzalez Paid Training Info
Practical Code Review \$2,000 – Seth Law & Ken Johnson Paid Training Info
– Software Defined Radios 101 \$2,500 Paid Training Info
Orange Cyberdefense \$2,600 – Web Hacking Bootcamp Paid Training Info

Vendors Table

Vendors attending DEF CON

One Page [All Vendors](#) list with descriptions

The Vendor room is in Caesars Forum – Forum Ballroom, 130-132, 134

1BitSquared LLC
Ascent-Portal
Bizarre Magic Inc.
Black Hills Information Security
BoardSRC LLC
Capitol Technology University
Cigent Technology, Inc.
Cryptocurrency Hackers
DEF CON 31 CFP Review Panel
DEF CON 31 CFP Review Panel
DEF CON Communications
DesignFlaw
EFF
Hack The Box
Hacker Warehouse
HackerBoxes
Hak5 LLC
HotWAN
Keyport, Inc.
Lacework
Mar Williams
Miscreants LLC
Netool LLC
No Starch Press, Inc.
Nuand LLC
OpenVPN
PhysSec Education (Physical Security Village)
Salty Security
Science & Design, Inc.
SLNT Inc.
SPARROWS Lock Picks
SquareX Pte Ltd
Start9 Labs, Inc
The Calyx Institute
The Open Organisation of Lockpickers
The OWASP Foundation Inc.
The SecOps Inc.

The Tor Project, Inc.
Transportation Security Administration
University of Advancing Technology
Women in Security and Privacy
Xcape, Inc.
XXX.VPN

Links

DEF CON . org Links

DEF CON [Main page](#)
DEF CON 31 [Home Page](#)
DEF CON [Recent News](#)
DEF CON [FAQ](#)
DEF CON 31 [FAQ](#)
DEF CON 31 [Venue](#)
DEF CON 31 [Schedule](#)
DEF CON 31 [Policy](#)
DEF CON 31 [Training Signup](#)
DEF CON CTF [Nautilus Institute](#), Twitter [@Nautilus_CTF](#)
DEF CON [YouTube](#) channel, prev years talks

DEF CON [Forum Calendar](#)
DEF CON 31 [Planning](#) Forum page
DEF CON 30 Hackers with Disabilities [HDA Infopack](#)

DEF CON 31 [Speakers & Presentations](#) Forum page
DEF CON 31 [Villages](#) Forum page
DEF CON 31 [Contests](#) Forum page
DEF CON 31 [Parties & Gatherings & Events](#) Forum page
DEF CON 31 [Demolabs](#) Forum page
DEF CON 31 [Workshops](#) Forum page - Registration opened on July 5 at Noon PDT! - All Workshops are Sold Out!
DEF CON 31 [Paid Training](#) Forum page - These occur the 2 days following DEF CON

Thanks to the InfoBooth crew for providing access to their backend database. <claps> to their hard work!

Combined Schedules of DEF CON, Villages, and everything else DC31

Hacker Tracker - [Android](#) and [IOS](#) - the official DEF CON schedule app

[The ONE!](#) - A consolidated DEFCON 31 schedule in multiple file formats - html, PDF, CSV, ICAL, epub, mobi, Google calendar

info.defcon.org - the official DEF CON InfoBooth site

Other Interesting Links

Hackers with Disabilities DEF CON 31 [HDA Infopack](#)

[@defconparties](#) - [calendar](#)

[defconmusic](#) - Schedule/News from the DC Artists & Entertainment (A&E) Department

[DEFCONorg](#) [Twitch stream](#)

[defconmusic](#) [DEF CON Entertainment Twitch stream](#)

[defconmusic](#) [YouTube channel](#)

[DCTV](#) - DEF CON TV: Twitch streams and Hotel TV channels

[#badgelife](#) spreadsheet of unofficial badges for DC31

[@qumqats](#) Twitter [List of Village](#) accounts to assist in watching Village happenings

Other cons during #SummerHackerCamp

Blackhat	T @BlackHatEvents	FB Black Hat Events
BSides Las Vegas	T @BSidesLV	FB @BSidesLV
Queercon	T @Queercon	FB @queercon
The Diana Initiative	T @Dianainitiative	FB @dianainitiative

Guides/Tips/FAQs

[DEF CON A&E - Resources - Rough Distances and Maps](#)

[Guide to Attending DEF CON 31](#)

[How to Survive Def Con 2022](#)

[OpSec For DEF CON 30](#)

[DCG 201 Hacker Double Summer 2023 Guides](#)

[Birds of a Feather-Resources for 2022 Hacker Summer Camp](#)

[Lonely Hackers Club - DEF CON n00b guide - reddit thread](#)

[The Lost Policymaker's Guide to Hacker Summer Camp](#)

[Holon DEF CON 30 Preparation](#)

[DEF CON: The Survival Guide](#)

[Preparing for "Hacker Summer Camp"](#)

[General / previous years](#)

[DEF CON for N00bs](#)

[JK-47 - BSidesLV & DEFCON Conference Tips](#)

[Just another DEF CON guide](#)

[HACKER SUMMER CAMP 2018 GUIDE](#)

[On Attending DefCon](#)
