
DEFCON
ENGAGE

Welcome to

DEFCON 32 ENGAGE

Welcome to DEF CON 32, the first time we are all in the same building since DEF CON 25!

Since last year the world has gotten particularly uncertain both politically and technologically. On top of the standard kinds of military and political strife we also have massive disinformation campaigns attempting to influence who the democratic countries elect this year. We are buried in synthetic personalities and microtargeted fascist manipulations. AI is fueling tech sector job uncertainty while it poisons the commons with nonsense and hallucinations.

In times of crisis the communities that support their members do better than those that don't. So, we engage!

We support the hacking community the best we can. We've expanded the number of DEF CON Communities and launched DC Nextgen, focused on helping younger hackers experience that joy of discovery. DEF CON Academy is something new we are trying this year to help provide guidance on your hacking journey at DEF CON. A new "Franklin" initiative is in Alpha testing this year, an experimental way to get hackers and researchers engaged in helping protect critical infrastructure. On the community tech front we have reencoded all the past DEF CON videos in the AV1 format to be more accessible and also included captions to help search engines surface past content. We self-host DEF CON. social, a Mastodon server to offer a distributed alternative to the community, run our Discord server, and operate Tor relays to help others in more restrictive environments get online safely. Over the next year we're going to add even more open source ways to interact with the DEF CON community. We're also always looking for good, human-scale projects to support.

Don't get distracted by the bullshit. As hackers we strive to understand how systems work - networks of hardware, software, people and policy. We speak truth to power and know what is in the manual is not the whole truth of how things operate. Do what you can when you can for what you believe in, and support others doing the same. Judge people on their actions, not their appearance. Provide useful feedback. File bug reports. Tell a favorite creator you like their work. Hack stuff. Be Human.

By next year some of the uncertainty will be gone, but the communities you support and friends you make will be just as important.

The Dark Tangent

CONTENTS

THE BADGE

Single board computers and microcontrollers like Raspberry Pi and Arduino captured my interest (along with so many others) during the rise of hackerspaces. As an artist involved in that scene at the time, I was excited for how quick and accessible they made projects that were typically the domain of more serious hardware engineers, and how these tools helped shift the scene itself towards becoming more open.

For DEF CON 32, I wanted to design a badge that was as open, accessible and customizable as possible, while telling the story of why we hold this ethos dear.

The theme this year is Engage, the challenge to get involved and take back the web & our spaces from enshittification. For those of us with fewer resources, it's harder to be present and stay engaged, and while there aren't always creative solutions, with strong communities we can carry each other.

The game on this badge is a dedication to the player, the attendee, the community member. To do what you can to get involved and make an impact, but to take care of yourself too.

The badge itself is just a little cat, but it does some pretty cool tricks thanks to the efforts of the people on this team

- Built with the newly released **Raspberry Pi RP2350**: as in, released this weekend, on these boards, for DEF CON attendees to play with before anyone else!
- Circuit design by RPi's engineering partners
- Firmware and uGB, the tiny bare-metal emulator for that classic handheld gaming system, by **DmitryGR**
- Game development & Art by **Bonnie Finley & Nutmeg Anne**
- Badge specific hardware plugins, development & support by GB Studio creator **Chris Maltby**
- ABS injection molded case to protect your badge from weekend shenanigans, 3D modeled by **Bonnie Finley**
- Touch Screen
- Screen Flip / Orientation Sensor for wearable gameplay
- Customizable RGB LEDs
- SAO support
- USB-C & rechargeable li-ion battery
- SD Card (also holds some goodies for your PC)
- IR communication
- Real Time Clock

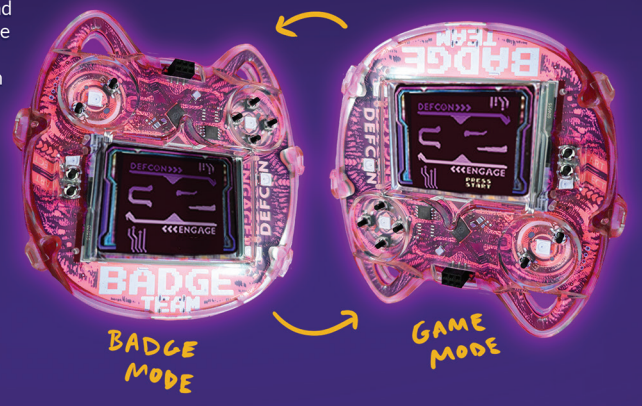
Thanks to **Will Tuttle** for concept & narrative collab, **Jason Scott** for game dialogue contributions **ICSN** as our production partner and **Dual Core**, **MC Frontalot** and **Legion303** for music and sounds.

Special thanks to **Joe Grand** for production testing, hardware support, and last minute adventures.

The badge can be customized in a any number of ways - from SAOs, to loading up your favorite classic ROMs, to creating your own with the open source drag-and-drop game creator GB Studio, to creating your own firmware using the RP2350 SDK, to really any way you'd use a microcontroller!

Check out **defcon.org/badge/32** or **spux.art** for details and extras

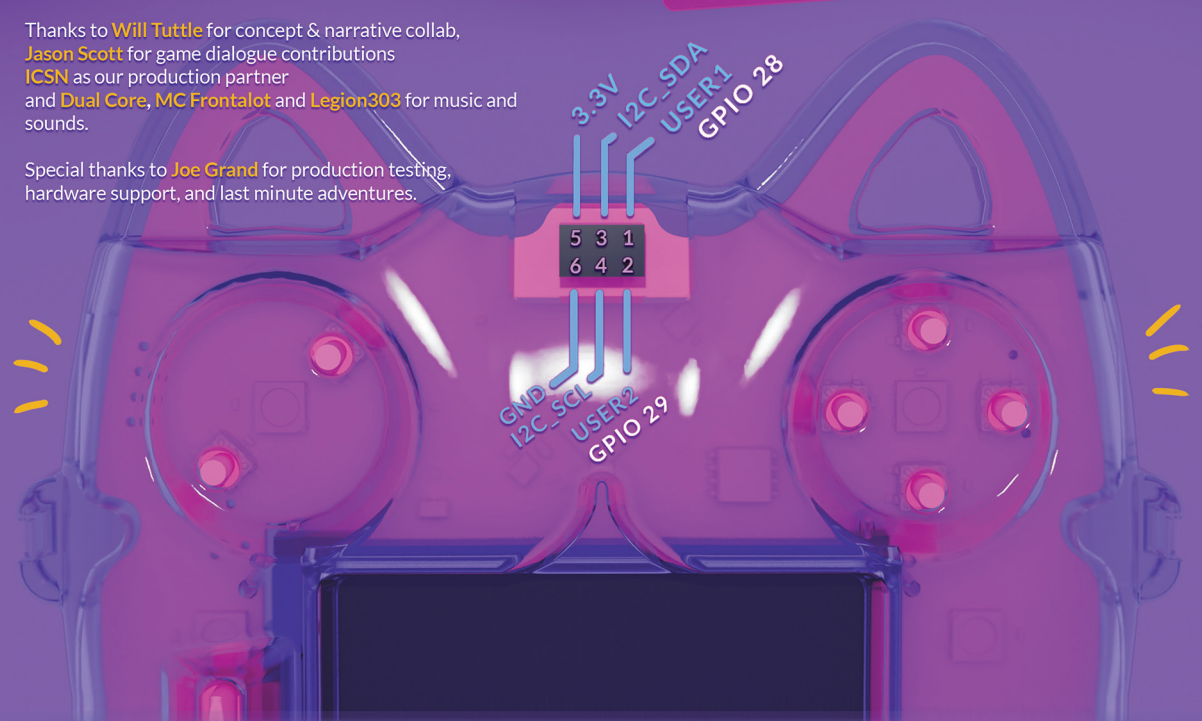
Happy Hacking! I can't wait to see what you create!
- Mar Williams -



A note from Raspberry Pi

"Raspberry Pi RP2350 is our new microcontroller. Like its predecessor RP2040, it's open, high-performance, and affordable. We've doubled the RAM, made it dual-architecture (dual Arm M33 or dual RISC-V), and added new security features. All the SDK software and on-chip boot ROM are open source; and the chip, including its security features, is fully documented and available without NDAs or other corporate bullshit. We think it'll be great for hardware security research, education and hacking.

Raspberry Pi is proud to be part of the badge and DEF CON 32. We look forward to meeting you at the Embedded Systems Village. See **rptl.io/rp2350** for more details."



NETWORK

NETWORK INSTRUCTIONS

DEF CON 32! Another year, another DEF CON eh, From the team that brought you the hits of the past, comes this years latest and greatest. The NOC is delivering the best questionable zero-trust network access on all conference floors. Updated AI optimization, IPv7, a skating rink in the roof, and Malört Canadian Club drinking, all should be working by the time you are reading this.

Now to the important stuff, what should you do in order to connect to Wi-Fi?

Remember there are three no more, no less official ESSIDs you should use to HACK THE PLANET!!!....or at least the table your sitting at.

The encrypted one with 802.1X authentication and digital certificate verification:

DefCon

The (other, yet legit) encrypted one with 802.1X authentication and digital certificate verification. But also, with some shiny WPA3 benefits:

DefCon-WPA3

And the original, unencrypted, stick-shift, no ABS, wildest-westest of the wireless networks:

DefCon-Open

"Choice. The problem is choice"

Wi-Fi and 802.1X authentication have had a pretty good relationship in the past few years. And, believe or not, we test stuff before we go onsite. But things might change and there might be some devices out there that really do not like 802.1X with PEAP authentication.

Important 802.1X fact: By configuring 802.1X and choosing for your device to "not verify server certificate" will probably not only let that device connect to one of the hundreds of rogue access points on the show floor but will also send your login credentials to a rogue radius server. Despite technology advancements, this is still no bueno and defeats the whole purpose of this authentication method.

The John Candy special (now upgraded to include Orange whips) : Be an advocate of cyber common sense™, and do not, I repeat, do NOT choose the same credentials (aka: username and password) used for stuff that matters: shopping sites, online-banking, AND, especially your windows domains (yeah, it keeps happening) to connect to the hacker conference network. Make something up, be creative and funny, cause we will be post the best ones!

For updated information and instructions on how to connect to the Wi-Fi with the n0t-s0-1337 Operating Systems along with the link to download the digital certificate to be used, visit: https://wifireg.defcon.org. And if you don't know how to properly configure the Wi-Fiz on your üb3r-1337 linux distro, you should consider a new platform. For NOC updates visit https://noc.defcon.org , and also follow us on twitter @DEFCON_NOC above all else have fun and be rad to each other!

DCTV

DEF CON will be televised!

Check out https://dctv.defcon.org for the latest info!

DEF CON 32 CONVENTION MEDIA SERVER

All DC 32 Content is HERE

https://10.0.0.16/

or

https://dc32-media.defcon.org/

Find this year's presentation materials, music, white papers, slides, and more plus leech files from all the past DEF CON conferences and the infocon.org conference archives!

We expect you to leech at full speed, and the server is warmed up and ready to go. Enjoy!

To make things easier for you here are some example wget commands:

EXAMPLE wget command to download all of DEF CON 25:

wget -np -m "https://dc32-media.defcon.org/infocon.org/cons/DEF CON/DEF CON 25/"

COC/HOTLINE

CONFERENCE CODE OF CONDUCT

Last updated 3.6.15

DEF CON provides a forum for open discussion between participants, where radical viewpoints are welcome and a high degree of skepticism is expected. However, insulting or harassing other participants is unacceptable. We want DEF CON to be a safe and productive environment for everyone. It's not about what you look like but what's in your mind and how you present yourself that counts at DEF CON.

We do not condone harassment against any participant, for any reason. Harassment includes deliberate intimidation and targeting individuals in a manner that makes them feel uncomfortable, unwelcome, or afraid.

Participants asked to stop any harassing behavior are expected to comply immediately. We reserve the right to respond to harassment in the manner we deem appropriate, including but not limited to expulsion without refund and referral to the relevant authorities.

This Code of Conduct applies to everyone participating at DEF CON - from attendees and exhibitors to speakers, press, volunteers, and Goons.

Anyone can report harassment. If you are at DEF CON and are being harassed, notice that someone else is being harassed, or have any other concerns, you can let us know by contacting any Goon, registration desk, or NFO booth, as well as by calling or texting the hotline at 725-222-0934. As a reminder, you can also contact the hotline during the con if you just need someone supportive to talk to. You can also file a report year-round by contacting safety@defcon.org. We encourage individuals to report CoC violations as soon as they're able to so we can begin our investigation before evidence is lost or destroyed, but it's never too late to make a report.

Conference staff will be happy to help participants contact hotel security, local law enforcement, or otherwise assist those experiencing harassment to feel safe for the duration of DEF CON.

Remember: The CON is what you make of it, and as a community we can create a great experience for everyone.

- The Dark Tangent

DEF CON SUPPORT HOTLINE

Mental wellness and physical safety are both important to us at DEF CON. If you're struggling, scared, or just need someone to voice a concern to, DEF CON Hotline is here to support you. Help is available to all, especially if talking to DEF CON Goons in person isn't a good option for you.

Hotline is confidential and available well into the early morning hours on conference days. Volunteers are standing by to listen and, if needed, connect you to appropriate support services. Whether that's SOC Goons or external services we partner with such as Kick at Darkness, The Rape Crisis Center Las Vegas, and the Nevada Coalition to End Domestic and Sexual Violence to provide expert resources for survivors. The Hotline team is diverse and undergoes extensive training including dedicated support for LGBTQ+. Hotline is here to listen.

You can reach DEF CON Hotline Goons during normal hours of operation to anonymously report any behavior violating our code of conduct or to find an empathic ear by phone call, text, or Signal at + 1 (725) 222-0934, or reaching out on Discord @defconhotline.

GOONS

DEF CON Goons are the electrons that enable the conference to run, and should you have a question or need help they are there for you. Here are some goon facts:

DEF CON 32 Goons should all have visible patches with their nickname on them so it is easier to remember who you talk to about what.

Goons are in one of two states, either ON duty or OFF duty.

If they are ON DUTY they will be wearing a current year, red, DEF CON 32 Goon shirt, a current year Goon badge, and a name patch.

If Goons are OFF DUTY they will not be wearing the red Goon shirt, but may still have a Goon badge on so they can still access the meeting spaces.

Goons ON DUTY are not supposed to drink alcohol.

Goons OFF DUTY have been known to drink alcohol.

PAST Goons may seen wearing previous red shirts or badges as they helped run a past DEF CON, but that DOES NOT make them a current DEF CON 32 Goon.

Please use the name patch if you have any feedback on Goons, good or bad. Feedback can be sent to feedback@defcon.org

Goons Goon for many reasons, but the pay isn't one of them. They put in long hours and many weeks or months of planning and take time off work to make the con happen for everyone. Please feel free to ask them questions if you have any desire to join the ranks at a future Con.

DEFCON.social provides for open discussion where different viewpoints are welcome and a high degree of skepticism is expected. 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. Come Join the Discussion! Find us at:

HTTPS://DEFCON.SOCIAL

COMMUNITIES

DC NEXTGEN

Level 1 - Hall 3 - Aisle 06-03

Friday and Saturday: 10:00 - 18:00; Sunday 10:00 - 13:00

DC NextGen's mission is to empower the Next Generation of young hackers. By creating an environment where hands on discoveries can reveal new and unexpected ways of thinking about security and technology. Let's explore and change the world together, one network at a time.

DCNextGen has a ton of awesome content planned for the youth hackers!

If you'd like a printed schedule of our events, stop by our community space! You can also find us in Hacker Tracker and online at dcnextgen.org.

DEF CON GROUPS (DCG)

Level 2 - Room W236

Friday and Saturday: 10:00 - 18:00; Sunday 10:00 - 13:00

DEF CON is a favorite island of misfit toys. Finding your people is something many people struggle to do in their lifetime. But when you do find DEF CON, you want to take it home with you. DEF CON Groups is the cure to the Con Blues and the conversations, resources, and support that the DEF CON Groups Community at DEF CON provides encourages the creation of new groups, connecting Humans with their local groups, and reinvigorates existing groups with a community space that allows for a chill room vibe and fun atmosphere. We invite POCs and Group Participants to join in conversation, collaboration, trading group related stories, and of course, stickers and laughs as well.

DEF CON GROUPS VR (DCGVR)

Virtual

Friday and Saturday: 10:00 - 18:00; Sunday 10:00 - 13:00

DEF CON Groups VR (DCGVR) addresses barriers preventing some hackers from attending the conference in person. Since DEF CON 28, DCGVR has offered an immersive virtual experience, allowing participants to socialize, present, and engage in panels, imitating the atmosphere of the physical event. Through VR technology, DCGVR fosters inclusivity, enabling global collaboration and contribution to the DEF CON community.

FRIENDS OF BILL W

Level 3 - Room W301

Thursday, Friday, Saturday: 12:00 - 13:00, 17:00 - 18:00; Sunday: 12:00 - 13:00

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 32 has you covered. Join us throughout the conference in the Friends of Bill W Community Space in room W301.

GAME HACKING COMMUNITY

Level 1 - Hall 4 - Aisle 01-03

Friday and Saturday: 10:00 - 18:00; Sunday 10:00 - 13:00

Welcome to the inaugural Game Hacking Community at DEF CON 32, where gaming and cybersecurity intersect in exciting and interactive ways. Our mission is to delve into various aspects of game security, fostering an environment of exploration, play, and learning.

At the Game Hacking Community, participants can engage in activities ranging from modding games to exploring the intricacies of memory hacking and multiplayer cheats and learning about game malware. Whether you're a beginner or an experienced hacker, we will have presentations and activities to challenge your skills.

Be part of the evolution of game security. Dive into our activities, engage with other game hackers, and explore opportunities to contribute to and support the Game Hacking Community. Let's play, learn, exploit, and perhaps even profit. See you there!

HARD HAT BRIGADE

Level 1 - Hall 2 - Aisle 08-02

Friday and Saturday: 10:00 - 18:00; Sunday 10:00 - 13:00

Ever see someone walking around DEF CON and wonder "what is up with the hard hats?"

The Hard Hat Brigade brings hackers together in the spirit of endless curiosity and tinkering. We use a common platform (hats) to combine art (bling) and hacker functionality (warez) to inspire others to explore outside of their comfort zones in a safe and welcoming community.

We encourage everyone to explore their creativity using art, electronics, mechanical design, or any other medium that piques their interest. Hats are inexpensive, widely available, and easy to modify to suit your needs. We started with hard hats but are not limited to any type of hat, so you have the freedom to choose whatever hat suits your fancy.

Despite everyone using a common platform, every creation is unique and embodies the personality of the creator. Walking around DEF CON, you can display your creation for all to see, and many will stop to ask you about what you have created. This allows you to talk about your experience, as well as inspire others to explore new ideas of their own.

One of the challenges at hacker summer camp has been finding people to connect with. By leveraging hard hats as a canvas, HHB has solved this challenge with something that is incredibly accessible while also offering a ton of variety. Gazing upon these creations, they reflect back the uniqueness of all the awesome hackers that we've been able to meet. In years past, we've had the opportunity to see how so many talented and creative hackers tackle the challenge of using the venerable hard hat as their muse. Just as fun, charming and skilled as so many attendees are, the hard hat has been a great vessel to carry their awesome projects.

Stop by our community space and make your trip memorable by trying on a hat, learning and sharing building techniques, networking with other hat loving hackers, and expressing yourself in your own hacker way. Keep on hacking!

HDA COMMUNITY

Level 1 - Room W110

Thursday, Friday, Saturday: 10:00 - 18:00; Sunday: 10:00 - 13:00

DEF CON has made HDA a community, and we now have a community room! This room will be dedicated to the attendees with ADA needs, their friends, helpers, and anyone who wants to hang out and be social! So far we plan on providing charging stations, chill out sessions, an open call for a modular synth jam session, and more to come! Let's all work together to make DEF CON Awesomely Accessible!

Visit the DEF CON Forums for the DEF CON 32 HDA Packet.

LA VILLA

Level 2 - Room W235

Friday and Saturday: 10:00 - 18:00; Sunday 10:00 - 13:00

La Villa Hacker is a vibrant initiative within the DEF CON community aimed at uniting and amplifying the voices of Latin American cybersecurity enthusiasts who speak Spanish or Portuguese. It offers a platform for these individuals to showcase their skills, share insights, and engage deeply with the global hacking and security community. The La Villa Hacker offers several core activities including talks, networking, and creative showcases, all conducted in Spanish or Portuguese to foster a strong sense of belonging and collaboration among Latino professionals at DEF CON.

LONELY HACKERS CLUB

Level 2 - Room W208

Friday and Saturday: 10:00 - 18:00; Sunday 10:00 - 13:00

Lonely Hackers Club is a group to help people navigate their first DEF CON and other conferences as well as helping people break into the field. We have a lot of people who are from all sorts of fields who can help people based on what they want to do for a career. We welcome everyone into the community and support everyone who needs/wants help.

MAKERS COMMUNITY

Level 1 - Hall 2 - Aisle 07-01

Friday and Saturday: 10:00 - 18:00; Sunday: 10:00 - 13:00

The DEF CON Maker's Community is the place where design, electronics, arts, crafts, software, and engineering all intersect. We serve as a home for ALL hackers and makers - providing tools, demos, talks and workshops (from makers like those in the Badgelife community), as well as exhibit space for highlighting current and past creations from some of your favorite DEF CON makers.

RETRO CLUB

Level 1 - Hall 4 - Aisle 04-01

Friday and Saturday: 10:00 - 18:00; Sunday: 10:00 - 13:00

The Retro Tech Community is here to celebrate where we came from, how computers and technology shaped our lives, and how even the most simple of computers still have an impact today this many years later. Rather than have a carefully curated collection of museum exhibits you can't touch or breathe on/around our goal is to empower the community in general to bring in working examples of old (or new but inspired by old) tech to display, demonstrate, be passionate about, teach lessons on, and for all those who visit us to hack on and goof around with. Bring us your tired capacitors, your scratched cases, your huddled masses of wirewrapped panels yearning to see voltage again, the wretched refuse of your teeming e-waste pile, bring these the tempest-tost to us, we lift our 20A 120Volt circuits beside the golden door! (But yes if you bring it, you must bring it home with you. If it's broken we will have a repair area set up and do the best we can!)

VETCON

Level 2 - Room W213-W214

Friday and Saturday: 10:00 - 18:00; Sunday: 10:00 - 13:00

Co-founded in 2018 by Jim McMurry and William Kimble, the founders of ThreatHunter.ai and Cyber Defense Technologies, respectively, the VETCON conference is the official Veteran event of the DEF CON Hacker Conference. VETCON, through its Discord server and in person events, connects and supports veterans in the Information Security field. The event is open to all DEF CON attendees with a focus on military veterans. VETCON is a networking event where attendees will be able to relax, play fun military and cybersecurity related games, network, and connect with other Veterans in the Infosec field.

VETCON Is a Conference for Veterans, Run by Veterans, During the Largest Hacker Conference, DEF CON.

WOMEN IN SECURITY AND PRIVACY (WISP)

Level 1 - Hall 3 - Aisle 05-04

Friday and Saturday: 10:00 - 18:00; Sunday: 10:00 - 13:00

Women in Security and Privacy (WISP)'s mission is to advance women and underrepresented communities to lead the future of privacy and security. We accomplish this by providing women and underrepresented communities with opportunities for technical and professional development through events, trainings, conferences, scholarships, mentoring, and job search. WISP is a 501(c)(3) non-profit organization.

HACKER TRACKER

The official DEF CON conference app

Stay up to date during DEF CON

https://info.defcon.org/apps/

- Events
- Villages
- Contests
- Parties
- Maps

& More

Download on the App Store

GET IT ON Google Play

https://info.defcon.org/apps/

FORUM.DEFCON.ORG

No matter what part of the DEF CON universe you're interested in, you should start at the DEF CON Forums. With a forum account you can reach out to a local DEF CON group, help us plan future events or even chat with other hackers. DEF CON's heart is its community, and the community meets at the DEF CON Forums. Join us!

https://play.google.com/store/apps/developer?id=DEF+CON+Communications,+Inc.

Download on the App Store

DEF CON FORUMS

DEFCON 32 ENGAGE

ROOM

320

8PM FRIDAY AND SATURDAY

FRIDAY

MAX HEADROOM/ELYSIUM

SATURDAY

ANTITRUST/THE CONGRESS

ULTRA HIGH QUALITY

DEF CON 32 MOVIE NIGHT

EXCEPTIONAL VALUE

PARTIES, MEET-UPS & EVENTS

ARCADE PARTY

Party on Friday from 21:00 to 02:00 in Level 1 - Room W106-W109 (Chillout 1)

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 32 attendees to enjoy and play, is hosted by the Military Cyber Professionals Association (a tech ed charity) and friends.

ASK THE EFF

Event on Friday from 17:30 to 21:30 in Level 3 - Room W307-W308

Electronic Frontier Foundation (EFF) is excited to be back at DEF CON. Our expert panelists will offer brief updates on EFF's work defending your digital rights, before opening the floor for attendees to ask their questions. This dynamic conversation centers challenges DEF CON attendees actually face, and is an opportunity to connect on common causes.

BLACKS IN CYBER LITUATION 2.0

Party on Friday from 19:00 to 02:00 in Level 3 - Room W314-W316

This party will take place in our allocated space, and will include an area with tables to welcome guests in for eating and card games as well as a large space for the main party to serve as a dance floor.

BLANKETFORT CON

Party on Friday from 19:00 to 01:00 in Level 3 - Room W305-W306

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!

CAPITOL TECHNOLOGY UNIVERSITY (CTU)

Event on Friday from 21:00 to 02:00 in Level 2 - Room W208

Join Capitol Technology University for a night of fun, drinks, and networking amongst like-minded peers! Capitol Tech's industry-expert leadership will be discussing exciting career paths in cybersecurity, as well as the future of cyber higher education.

CYCLEOVERRIDE DEF CON BIKE RIDE

Event on Friday from 18:00 to 18:00

At 6am on Friday, the @cycle_ override crew will be hosting the 13th DEF CON 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.

DC BOOK CLUB DISCUSSION

Event on Saturday from 14:00 to 16:00 in Level 2 - Room HallwayCon Lounge past W234

A quieter space for those who want to discuss what they are reading, recommend books, and trade books too. We will have a logo themed sticker.

DC NEXT GEN PARTY

Party on Saturday from 19:30 to 22:00 in Level 2 - Room W228-W230

Party with DEF CON NextGen. Enjoy some music, and some good conversation with other young DEF CON attendees!

DC702

Meetup on Thursday from 19:00 to 21:00 in Level 2 - Room W236

Join the local DC702 Group in this year's official DEF CON Meetup! The meetup will be casual and include typical meetup activities (e.g., socializing, "challenges," lockpicking, etc.) and maybe a few little surprises. To stay up-to-date, check out dc702.space/dc32-meetup.

DCG ATLANTA (DC404, 678, 770, 470)

Meetup on Friday from 16:00 to 19:00 in Level 2 - Room W236

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 25+ year legacy can catch up and share stories. Join us and meet your fellow ATL hackers!

DEF CON HOLLAND GROUP PRESENTS: VRIJMIBO

Meetup on Friday from 16:00 to 19:00 in Level 2 - Room HallwayCon Lounge past W234

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 DEF CON, 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.

DEF CON MOVIE NIGHT

Event on Friday, Saturday from 20:00 to 23:59 in Level 3 - Room W320

DEFCON.RUN

Event on Thursday-Sunday from 05:00 to 08:00, with random pop up meetings throughout the day in the con space.

Defcon.run is an evolution of the now long running DEF CON 4x5K running event. 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 small distributed groups around Las Vegas. It's the same old event but at a distributed scale!

Show up in the morning, 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. Full Information at https://defcon.run

EFF TECH TRIVIA

Event on Saturday from 17:30 to 21:30 in Level 3 - Room W307-W308

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 Badge and EFF swag pack. The second and third place teams will also win great EFF gear.

FRIENDS OF BILL W

Meetup on Thursday-Saturday from 12:00 to 13:00 and 17:00 to 18:00, and Sunday from 12:00 to 13:00, in Level 3 - Room W301

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 32 has you covered. Join us throughout the conference in the Friends of Bill W Community Space in room 301. Meetings will be Thursday, Friday, Saturday: 12:00-13:00, 17:00-18:00 Sunday 12:00-13:00

GOTHCON 2024

Party on Friday from 21:00 to 02:00 in Level 3 - Room W322 - W324

Returning for their 7th year, Gothcon invites you to come dance the night away with a line-up of some of the community's best dark dance music DJ's from across the US! Dress however you would like in whatever makes you feel comfortable and happy, and all are welcome (except nazis). Follow @dcgothcon on X for current updates on lineup and other surprises we have in store.

HACKER KARAOKE

Party on Friday and Saturday from 20:00 to 02:00 in Level 2 - Room W222 (Creator Stage 4)

We are the event to go to if you want to hang out, enjoy the festivities, sing along, and show ones hidden talent.

PARTIES, MEET-UPS & EVENTS

HAM RADIO EXAMS

Event on Friday from 13:00 to 16:00, Saturday from 11:00 to 17:00, and Sunday from 11:00 to 13:00 in Level 3 - Room W320

Ham radio is the original group of electronic hackers, starting long before computers, circuit chips, or even transistors. Continuing this pioneer spirit, The Ham Radio Village is offering free ham radio exams again at DEF CON! All are welcome to come and take the exam and get their amateur radio license upon passing. All three levels (technician, general, and amateur extra) of exams will be offered during DEF CON at the Ham Radio Village. Examinees are encouraged to study the question pool and take practice exams on ham.study.

Everything we do today involves wireless communications of some sort, and a basic knowledge of how radio works is crucial. Getting your amateur radio license and entering the world of amateur radio will better equip you with knowledge about what goes on in the radio frequency domain, and this can be applied to other RF topics (like RFID credentials, WiFi, or anything else that communicated wirelessly)

INTIGRITI HACK SHACK

Event on Saturday from 21:00 to 02:00 in Level 2 - Room W208

Join us at the Hack Shack Saturday night from 21:00-02:00 in room 208 for an evening full of exploits and fun! Enjoy some byte-sized bites, groove to our cyber beats, and mingle with the best in the bug bounty biz. Stop by Intigriti's booth in Exhibitors area before the party and grab a scratch card for your chance to win a free drink! Don't miss out on this bug bounty bonanza!

JACK RHYSIDER MASQUERADE

Party on Saturday from 21:00 to 01:00 in Level 3 - Room W325-W327

Come party with Jack Rhysider at the Darknet Diaries Masquerade party! You're not going to want to miss this event as there will be free swag, killer music, interactive exhibits, and of course Jack Rhysider.

LAWYERS MEET

Meetup on Friday from 19:30 to 22:00 in Level 2 - Room W228-W230

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.

POLICY MIXER @ DEF CON

Meetup on Friday and Saturday from 18:30 to 22:30 in Level 2 - Room W237

QUEERCON

Party on Friday from 22:00 to 02:00 in Level 3 - Room W325-W327

A fun gathering space for the lgbtqia+ community to listen to DJ dance music and party together. An inclusive and vibrant option with others in the community.

QUEERCON MIXER

Meetup on Thursday-Saturday from 16:00 to 18:00 in Level 2 - Room W231-W233 (Chillout 2)

Come by this informal mixer to meet others in the lgbtqia+ community who are a part of this wonderful world that is InfoSec. This is a safe and inclusive space to meet and talk to others with your shared experience and is a nice environment to network and unwind with a drink.

RAA FOR WORKGROUPS 3.11

Party on Saturday from 21:00 to 02:00 in Level 3 - Room W322 - W324

RAA For Workgroups 3.11 is a continuation of the Rent an Assassin series of parties from DC Shenanigans. Based on the World of Assassination from the Hitman video game franchise, RAA has been serving up clandestine client acquisition events in top-secret locations since DC30. This year marks our first-ever official DEF CON event, and we are excited to bring you some of the best DJs (and shenanigans) DEF CON has to offer.

STICKER SWAP AT DEF CON 32

Meetup on Saturday from 17:00 to 19:00 in HallwayCon Lounge past W234

We've ran The UnOfficial DEF CON Sticker Swap for 5 years now. Maybe a few other things. This year will be the officially official DC Sticker Swap, come visit for sticker hacker culture and to swap a bit of history.

THE ILLUMINATI PARTY

Party on Saturday from 21:00 to 02:00 in Level 3 - Room W303-W304

The Illuminati Party is excited to open our doors once again to all those who wish to join us at DEF CON for an OPEN party welcoming all of our Hacker Family! Follow us on X (Twitter: @IlluminatiParty)

THE PWNIE AWARDS

Event on Saturday from 10:00 to 10:00 in Level 1 - Hall 1 - Aisle 11-04 (Track 4)

The Pwnies are an annual awards ceremony celebrating and making fun of the achievements and failures of security researchers and the wider security community. Every year, members of the infosec community nominate the best research and exploits they've seen. The Pwnie Award nominations are judged by a panel of respected security researchers and former pwnie award recipients – the closest to a jury of peers a hacker is likely to ever get.

At this event DEF CON attendees will get a first person look at some of the most groundbreaking research and hacks in the cyber security community of the past year, and the winners get some well deserved recognition from the broader community for the great work they've done.

The Pwnie Awards have been a staple of the security research community for 17 years. People have traveled across the world to attend the ceremony and celebrate the accomplishments of their fellow researchers. You can see previous winners here: https://pwnies.com/previous/

THE UNOFFICIAL DEF CON SHOOT

Offsite Event on Wednesday at 11:00

Wednesday August 7th
Registration usually opens at 11am

OFFSITE: Pro Gun Vegas Address: 12801 US 95 South Boulder City, NV 89005

TOXIC BBQ

Offsite Event on Thursday from 15:00 to 21:00

The humans of Vegas invite you to our unofficial welcome party. Whether it's your 1st or 18th time, we're still in the EXACT SAME PLACE. Join us off-Strip in the shade for a volunteer-run grill and chill.

We stock the larder with the basics: burgers, dogs, meatless delights, and all the fixin's. You procure your favorite food, drinks, and sides to keep the party going. Volunteer for setup, grill-up, or clean-up. Most of all, show up and become a part of what makes Toxic BBQ the best place to start your con.

Check out https://www.toxicbbq.org for more news, and watch #ToxicBBQ for the latest info.

Off-site at Sunset Park, Foxtail Pavilion

VEILID DEV AND COMMUNITY MEETUP

Meetup on Friday from 12:00 to 13:30 in Level 3 - Room W322-W327

Cult of the Dead Cow and Hackers.Town are bringing you a meet and greet and chat session about Veilid Framework. Come by, say hi, talk shop, let's see each other in person and have a little fun! Veilid Foundation directors and many of the primary contributors will be there to share progress over the last year. Come by and help us to restore the future and ensure the privacy of the internet for generations to come!

VETCON

Party on Saturday from 21:00 to 02:00 in Level 1 - Room W106-W109 (Chillout 1)

Welcome to VETCON, the DEF CON Community event and of course, THE VETCON Party where veterans, active duty military, and even civilians looking for a taste of the action come together for a cyber rendezvous. Because let's face it, sometimes you need a little civilian perspective to hack the system!

WOMEN, GENDER NON-CONFORMING AND NON-BINARY MEETUP WITH THE DIANA INITIATIVE

Meetup on Saturday from 19:00 to 21:00 in Level 3 - Room W305-W306

The Diana Initiative is hosting a meetup where we'd love to get all the gender non conforming, non-binary and women attendees together to hang out and make friends! DEF CON is better with friends.

MUSIC LINEUP

dance while it's still legal

THURSDAY NIGHT

2000	DAEMON CHADEAU
2100	DOTORNOT
2200	PAT ATTACK
2300	DJ VULP
0000	CTRL/rsm
0100	GRIND613

SYN STAGE

CHILLOUT 2
LEVEL 2

ACK STAGE

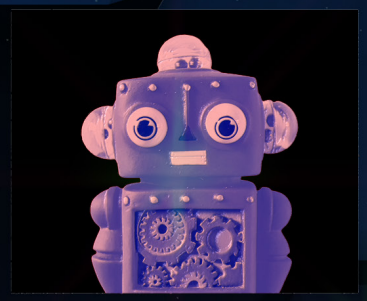
NORTH LOBBY
LEVEL 1

THURSDAY NIGHT

2000	STITCHAROO
2100	TALK SINN
2200	deaddoll
2300	CaptHz
0000	RELAY
0100	ACID-T

FRIDAY NIGHT

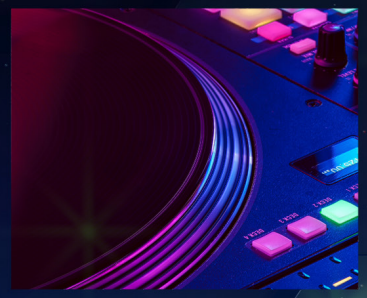
2000	ICETRE NORMAL
2045	OHM-I & NPC COLLECTIVE
2130	DUAL CORE
2215	YT CRACKER
2300	MC FRONTALOT
0000	COSTUME CONTEST
0015	ZEE
0115	TRIODE



RETRO SCI-FI FRIDAY

FRIDAY NIGHT

2000	CALL THE COPS
2100	DJ HABBS
2200	PANKLEDANK
2300	SCOTCH & BUBBLES
0000	DJ St3ring
0100	ARCHWISP



SATURDAY NIGHT

2000	DJ SCYTHE
2100	GRINDHAUS SELEKTOR
2200	SKITTISH AND BUS
2300	MISS JACKALOPE
0000	O'CRAVEN
0100	COSTUME CONTEST
0115	NINJULA

SATURDAY NIGHT

2000	KAMPF
2100	MATTRIX
2200	DR. MCGREW
2300	MAGIK PLAN
0000	SYNTAX + LUNA
0100	N8

VILLAGES

AI VILLAGE

LEVEL 1 - HALL 2 - AISLE 07-03

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

AI Village is focused on teaching you what you need to know to both defend and break AI. Come learn how ChatGPT, StableDiffusion, malware detectors, ML firewalls, and other AI based products work and how to break them. We have a talks track with world class ML security professionals talking about what they've seen and done in the industry. This year we've expanded the demo area into 8 stations with demos designed to get you up to speed with the underlying technology fast and hands on. Finally, we're running workshops in the morning on dedicated hardware and for the afternoon a generative red team event where you can assess open source models and defenses.

AIXCC

LEVEL 1 - HALL 3 - AISLE 05-06

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

The Artificial Intelligence Cyber Challenge (AIxCC) is a two-year competition and educational experience asking the best and brightest in AI and cybersecurity to defend the software on which the world relies. AIxCC will ask competitors to design novel AI systems to secure this critical code and will award a cumulative $29.5 million in prizes to teams with the best systems, including $7 million in prizes to small businesses to empower entrepreneurial innovation during the initial phase of AIxCC.

AIxCC will bring together leading AI companies that will work with DARPA to make their cutting-edge technology and expertise available for challenge competitors. These companies will collaborate with DARPA to enable competitors to develop state-of-the-art cybersecurity systems. AIxCC is collaborating closely with the open-source community to guide teams in creating AI systems capable of addressing vital cybersecurity issues, such as the security of critical infrastructure and software supply chains. Most software, and thus most of the code needing protection, is open-source software, often developed by community-driven volunteers. Further, open-source software comprises most of the code running on critical infrastructure in the United States today, including the electricity and telecommunications sectors.

AIxCC competitions will occur at one of the world's top cybersecurity conferences, DEF CON. The semifinal competition will be at DEF CON 2024, and the final competition at DEF CON 2025, where the top prize will be $4 million.

ADVERSARY VILLAGE

LEVEL 1 - HALL 4 - AISLE 03-05

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

Adversary Village is a community initiative which primarily focuses on adversary simulation, purple teaming, and adversary tradecraft. The village covers adversary emulation, threat/APT/ransomware emulation, breach and adversarial attack simulation, supply chain security, adversary tactics, research on nation-state sponsored threat-actors, adversary intelligence, life, adversarial mindset, adversary philosophy and hacker survival skills.

The goal of the Adversary Village is to build an open security community for the researchers and organizations, who are putting together new means, methodologies towards the simulation and emulation of adversary tactics and purple teaming.

Subsequent to feedback from past editions, Adversary Village shall focus on hosting hands-on deep technical workshops, live demonstrations, panel discussions and a ton of other hands-on activities on adversarial attack simulation/emulation, adversary tactics and hacker survival skills.

Adversary Village would have the following hands-on activities for this year at DEF CON;

Adversary simulator and purple teaming hands-on booth:

Adversary Simulator booth is a volunteer assisted activity, which has hands-on adversary emulation plans and exercises specific to a wide variety of threat-actors; these are meant to provide the participants with a better understanding of adversarial attack emulation. The booth will be hosting a simulated environment meant to recreate enterprise infrastructure, operational technology environment, which serves targets for various attack simulations.

The hands-on simulator booth also hosts an activity, which would need the participants to generate their own adversary emulation plans to assess the efficacy of the defense systems based on publicly available cyber threat intelligence.

Choose-your-own adversary adventure game:

Adversary adventure is a story-scenario based, interactive, choose-your-own adventure model interactive game. This is a gamified version of table-top exercises which is presented to the participants as they can choose to play as an attacker, post exploitation OR a Defender who is defending against an attacker group-threat actor OR even play as a CISO who is dealing with an adversarial situation such as a ransomware incident.

Hands-on deep technical workshops:

Adversary Village will feature a limited number of deep technical workshops focused on advanced adversary tradecraft and techniques.

Adversary Wars CTF:

Adversary Village will be hosting a CTF named "Adversary Wars", where the participants will have to pose as adversaries and replicate adversarial actions against each element of a "target" organization. Adversary Wars would have real world simulation of CTF scenarios and challenges, where the participants can perform various attacks and learn new attack vectors, TTPs, techniques, etc. To visualize the CTF environment, the contest area will feature a miniature model of the city made using interlocking-plastic-bricks. The breached components OR organization buildings will be physically marked in the city model as the CTF progresses.

Just like in previous years, winning teams in the CTF competition can expect fantastic prizes. Additionally, there will be complimentary hoodies (yes, the iconic adversary village hoodies), free t-shirts, cool stickers, village coins, badges, and various other swag for the village participants.

AEROSPACE VILLAGE

LEVEL 1 - HALL 2 - AISLE 07-02

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

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.

APPSEC VILLAGE

LEVEL 2 - ROOM W228-W230

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

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.

VILLAGES

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!

BIOHACKING VILLAGE

LEVEL 1 - HALL 3 - AISLE 05-07

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

Dive into the Future at the Biohacking Village: Welcome to the Intersection of Biology and Technology

Are you ready to explore the next frontier where technology meets biology? The Biohacking Village at DEF CON invites hackers, cybersecurity experts, biologists, and tech enthusiasts to delve into the exhilarating world of biohacking. This is your unique opportunity to be at the forefront of a revolution that's redefining the boundaries of biology, technology, and human potential.

Why the Biohacking Village?

- Uncover the Unknown: Embark on a journey to explore how hacking skills can unlock new potentials in biotechnology. Discover the secrets of DNA hacking, medical device exploitation, and more.

- Challenge Your Skills: Put your hacking abilities to the test in an entirely new domain. From breaking into sophisticated bioinformatics databases to uncovering vulnerabilities in the latest medical devices, challenge yourself like never before.

- A Hub of Innovation: Witness groundbreaking demonstrations and hands-on workshops led by pioneers in biotechnology and cybersecurity. The Biohacking Village is your chance to see the future as it unfolds.

- Collaborate and Create: Join a diverse community of hackers, scientists, healthcare professionals, and ethicists. Collaborate on projects that push the boundaries of what's possible in health, security, and technology.

- Ethical Hacking for the Greater Good: Use your skills to make a real-world impact. Contribute to projects focusing on improving public health, securing medical data, and enhancing the safety of biomedical devices.

What Awaits You?

- Innovative Talks & Panels: Engage with thought leaders discussing everything from CRISPR gene editing to the cybersecurity of implantable devices.

- Hands-on Workshops: Learn new skills in biohacking, from DIY biology to the art of securing complex bio-systems.

- Live Demonstrations: Experience cutting-edge technology in action, including live hacking of medical devices and bioinformatics systems.

- Networking Opportunities: Connect with like-minded individuals and industry leaders who share your passion for technology and innovation.

Join the Vanguard of Biocybersecurity

At the Biohacking Village, we're not just spectators; we're active participants shaping the future. Whether you're a seasoned hacker or just curious about the intersection of biology and technology, there's something for everyone. Be a part of a community that's breaking new ground and redefining the possibilities of technology and biology.

Embrace your curiosity, unleash your potential, and join us at the Biohacking Village – where the future of biohacking and cybersecurity converges.

BLACKS IN CYBER VILLAGE

LEVEL 3 - ROOM W314-W316

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

The Blacks In Cybersecurity (B.I.C.) Village seeks to bring culturally diverse perspectives to the holistic Cybersecurity community; by way of a series of talks and a capture the flag event. In providing these activities, we hope to help highlight Black experiences, innovations in the field, Black culture and educate the community about Black history.

The B.I.C. Village attracts and retains the presence of Hackers from the United States, Africa, Caribbean and Europe (so far) that are a part of the African Diaspora. This often underrepresented and misrepresented community harbors the drive, determination and stick-to-itiveness that is congruent to the Hacker Spirit yet, statistically lacks the proper resources to pursue careers or engage their perspectives on security topics and research.

Through the exposure and information provided by B.I.C. Village, we believe that we can normalize the discussion of deficiency or prejudices in Cybersecurity education/development for minority communities. We also believe this effort can be translated to allow for more diverse hobbyists and professionals to engage and contribute.

BLUE TEAM VILLAGE (BTV)

LEVEL 3 - ROOM W309-W313

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

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.

BUG BOUNTY VILLAGE

LEVEL 2 - ROOM W215

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

The global bug bounty community has witnessed exponential growth, with thousands of members actively engaged in the field. This thriving ecosystem now represents a legitimate and sought-after profession for hackers and cybersecurity specialists. It's time to acknowledge and celebrate this evolution by introducing a dedicated Bug Bounty Village at DEF CON, where hunters, learners, and enthusiasts can converge, interact with top-tier hackers, attend insightful talks, and immerse themselves in hands-on activities.

Our Bug Bounty Village promises to be a focal point for DEF CON attendees. It will feature exclusive talks by some of the world's foremost bug bounty hunters, who will unveil their groundbreaking techniques and share real-world vulnerabilities discovered through their exploits. Furthermore, representatives from leading global companies with established bug bounty programs will provide invaluable insights, guidance, and recommendations for both aspiring hunters and organizations keen on launching their bug bounty initiatives.

Inclusive Learning & Community Engagement:

Our village aims to cater to all levels of expertise, from beginners taking their first steps in bug hunting to seasoned professionals looking to enhance their skills. We will conduct a series of workshops that cover a wide spectrum of topics, ranging from fundamental concepts for newcomers to advanced techniques tailored to the most experienced hackers in the field. Participants will have the opportunity to delve into practical exercises and learn to utilize tools like Portswigger Burp Proxy effectively.

CAR HACKING VILLAGE

LEVEL 1 - HALL 4 - AISLE 0101

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

For 10 years, we've been rocking the automotive security scene, and this time, we're cranking up the excitement. Dive into hands-on challenges, snag cool badges, and tackle exercises that'll take your learning to a whole new level! Let's make this DEF CON the most unforgettable yet!

Friday 900 - 1800 | Saturday 900 - 1800 | Sunday 900 - 1300

For schedules and other info: https://www.wallofsheep.com/pages/dc32

The Packet Hacking Village at DEF CON provides a learning experience for people of all skill levels, from absolute beginners to seasoned professionals. We host practical training, network forensics and analysis games, and the renowned Capture The Packet event, which has been a Black Badge contest over 10 times and draws the best of the best elite hackers from around the world. Our mission has always been simple: to teach people good internet safety practices, and to provide an atmosphere that encourages everyone to explore and learn. Everyone is welcome, period - regardless of industry or experience. And when it's time to relax and escape the convention craziness, our DJs provide a chill atmosphere while they spin for the crowd in an open lounge area.

Wall Of Sheep

An interactive look at what can happen when you let your guard down on public networks, the infamous Wall of Sheep passively monitors the DEF CON network looking for traffic utilizing insecure protocols. Drop by, hang out, and see for yourself just how easy it can be! We strive to educate the "sheep" we catch, and provide a good-natured reminder that security matters, and someone is always watching.

Wall of Sheep DJ Community - WoSDJCo

Come chill with us while we play all your favorite deep tracks, underground house, techno, psytrance, dubstep yodeling, breaks, and DnB beats mixed live all weekends. Chill and enjoy the sick beats and ill stylings of our talented hacker DJs while you hack all the things. Check website for schedule.

Hardwired

Making network cable is fun... but what if it was also a time trial! In this event, players have to put their cabling skills to test while making cables and bridging connections on a live patch wall.

@wallofsheep @capturetp

CAPTURE THE PACKET

Capture The Packet - CTP

Come compete in the world's most challenging cyber defense competition based on the Aries Security Cyber Range, which DT has honored as a Black Badge event over 10 years. Tear through the challenges, traverse a hostile enterprise class network, and diligently analyze your findings in order to make it out unscathed. Glory and prizes await those that emerge victorious from this upgraded labyrinth, and only the best prepared and battle hardened will escape the fiendish crucible. Follow us on Twitter for the latest information on competition dates and times, as well as prizes at:

@Capturetp

Teams consist of up to 2 players and can register at the CTP table in the Packet Hacking Village.

Packet Inspector - Beginner/Intermediate

The perfect introduction to network analysis, sniffing, and forensics. Do you want to understand how hackers tap into a network, steal passwords, and listen to conversations? Packet Inspector is your boot camp! Using a license of the world famous Capture The Packet engine from Aries Security, we teach hands-on skills in a controlled real-time environment.

Join us in the Packet Hacking Village to start your quest towards getting a black belt in Packet-Fu.

Packet Detective - Intermediate/Advanced

Ready to upgrade your skills or see how you would fare in Capture The Packet? It's time to play Packet Detective. A step up in difficulty from Packet Inspector, Packet Detective will test your network hunting abilities with real-world scenarios at the intermediate level. Improve your network mastery in a friendly environment, learn from mentors and peers, and take another step closer to preparing yourself for the highly competitive Capture The Packet contest.

WALKTHROUGH WORKSHOPS

The Packet Hacking Village offers a revolving series of Walkthrough Workshops for people of all ages and skills, where participants will take a deep dive into a variety of topics. Join the self-guided journey to learn about anyh of the topics below, guided by our expert mentors!

Linux Trainer:

Knowing how to use the Linux command line is a critical skill for any good security practitioner. This trainer will have 10+ problems covering some of the most fundamental Linux commands. This trainer is for people new to field and for those who want to hone their Linux command line-fu.

Scapy Trainer:

Scapy is a powerful Python package that captures, reads, and manipulates packets. In this walkthrough, we will use it to capture packets on the network and work with pcap files and train a machine learning classifier with scikit-learn in order to differentiate between normal and anomalous records.

Botnet workshop:

Join us for an interactive workshop where we will walk you through the ins and outs of botnet deployment and operation via a command and control web server. Geared towards beginners, this workshop offers a hands-on approach to understanding how botnets function. You'll also learn an effective defense strategy against the botnet you have created. No experience needed we will give you everything you need!

Regular Expressions (REGEX) Trainer:

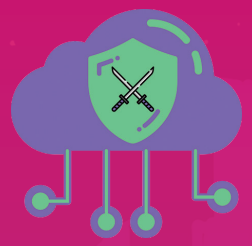
Regular Expressions or RegEX are used everywhere! If you aspire to be a Pentester, Threat Hunter, Programmer, Network Engineer, DevOps or really anything in technology today, RegEx is a skill all the greats have and the majority of the industry are terrible at. Come learn or brush up on your RegEx skills in on our live trainer.

VILLAGES

CLOUD VILLAGE

LEVEL 1 - HALL 2 - AISLE 09-01

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00



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, Alibaba, Digital Ocean, etc. We will also reward our top 3 teams with awards.

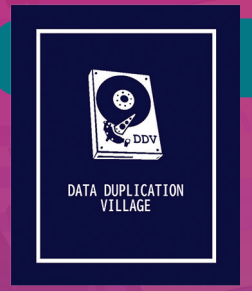
CRYPTO PRIVACY VILLAGE

LEVEL 1 - HALL 2 - AISLE 09-02

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

Launched in 2014, Crypto & Privacy Village (CPV) is a community-run village centred 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; 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!

CRYPTO + PRIVACY VILLAGE



DATA DUPLICATION VILLAGE

LEVEL 2 - ROOM W225

THURSDAY: 16:00 - 19:00; FRIDAY & SATURDAY: 10:00 - 17:00; SUNDAY: 10:00 - 11:00

The Data Duplication Village has all the updated bits and bytes available from infocon.org packed up into nice, neat packages. If you're looking for a copy of all the things, we've got what you need to fill up all your storage including a few nice hash tables and all of the DEF CON talks. Add to that just about every other security con talk known to hacker-kind! Our village provides a "free-to-you" service of direct access to terabytes of useful data to help build those hacking skills and talk with other storage enthusiasts.

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 8TB 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 so keep checking on dcddv.org for the latest. This year, we're adding new data to duplicate! Humans will be able to choose from the following data sources for duplication:

A) Infocon.org Archive - 6TB archive of all the past hacking convention videos that DT could find, built on last years collection and always adding more for your data consuming appetite.

B) Rainbow tables 1 of 3 - 6TB from freerainbowtables.com, the Lanman, MSQLSHA1, and NTLM hash tables plus freerainbowtables.com tools

C) Rainbow tables 2 of 3 - 6TB from freerainbowtables.com, the A5/1 GSM, and MD5 tables plus freerainbowtables.com tools

D) Vx Underground Archive - 6TB archive of the latest papers, samples, and code from Vx Underground

E) Rainbow tables 3 of 3 - 8TB of New NTLM-9 hash tables and a copy of the Infocon.org mirrors

EMBEDDED VILLAGE

LEVEL 1 - HALL 3 - AISLE 05-05

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

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.

HAM RADIO VILLAGE

LEVEL 3 - ROOM W321

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

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 DEF CON 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!

HHV/SSV

LEVEL 1 - HALL 2 - AISLE 10-01

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

Every day our lives become more connected to consumer hardware. Every day 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.

ICS VILLAGE

LEVEL 1 - HALL 3 - AISLE 06-05

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

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.

Exhibits. Interactive simulated ICS environments that 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), and 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! We will also have space dedicated to Maritime technology as well as Escape Rooms ran by Idaho National Labs and CISA. In addition to talks, hands-on demos/hacking, and escape rooms we are collaborating with BioHacking Village to demonstrate how Industrial Control Systems are used in Health Care.

VILLAGES

IOT VILLAGE

LEVEL 1 - HALL 2 - AISLE 08-04

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

[Hack all the things](https://www.youtube.com/watch?v=JZCmqMz1Wvo) at IoT Village!

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, including our 4 time black badge DEF CON CTF. Over the years, IoT Village has served as a platform to showcase and uncover hundreds of new vulnerabilities, giving attendees from around the globe 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)](https://www.ise.io/).

Follow both ISE (@ISEsecurity) and IoT Village (@IoTvillage) on Twitter for updates on talks, contests, and giveaways.

LOCK PICK VILLAGE

LEVEL 1 - HALL 2 - AISLE 07-03A

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

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 difficultly 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.

PAYMENT VILLAGE

LEVEL 2 - ROOM W202

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

Come to the Payment Village to learn about payment technologies, their history, and how hackers bypass security and fraud mechanisms to cash out! Payment technologies play a crucial role in our daily lives, yet many of us lack an understanding of how they work. We invite you to explore the history of payments and to learn how modern-day payments work. The village is jam-packed with hands-on experiences and exciting challenges!

Unsure where to start? Sign up for one of our workshops to get going. Do you have adept problem-solving skills? Pick up a Payment Village credit card and take part in our card hacking challenge! Looking for a unique challenge and want to get physical? Try our scavenger hunt. Bigger and better than last year! Try your hand at our cash-grab machines with real money. Catch as much money as you can to decipher the clues and solve the challenges.

PHYSICAL SECURITY VILLAGE

LEVEL 1 - HALL 2 - AISLE 08-03

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

The Physical Security Village explores the world of door hardware bypasses and techniques generally outside of the realm of cyber-security and lockpicking. Come learn some of these lock 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, defeating alarm systems and surveillance cameras, and cut-away and display models of common hardware to show how it works on the inside.

We are one of the easiest villages to get started in - read the instruction sheets we have or scan a QR code to learn the techniques, or ask any of our volunteers in the green shirts if you have questions! 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!

POLICY VILLAGE

LEVEL 2 - ROOM W237

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

The DEF CON community understands that creating a safer digital society requires collaboration between security and policy experts. Policy @ DEF CON provides a space for representatives of all areas of security to come together to educate and engage each other.

Tech policy is being written as we speak and we believe that including diverse expert voices will improve outcomes and help to bridge gaps between technical and policy practitioners. Senior government officials, nonprofit and private sector experts, security researchers, hackers, academics and technologists from around the world all come together at Policy @ DEF CON.

QUANTUM VILLAGE

LEVEL 1 - HALL 3 - AISLE 06-01

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

Attention Quantum Hackers - Quantum Village is Back for DEF CON 32! Come and explore and discover new technologies to hack - this year, we are focusing on quantum tech and society; from how to hack quantum networks to how 'thinking quantum' could change the world. We have a plethora of new activities, open to all levels, for hackers to come and learn quantum technologies - workshops, some talks, interactive demonstrations, and real quantum hardware! We also have the return of our infamous Quantum-CTF - pitch your wits against the Quantum Quizmasters and earn points for glory! Come and learn more about this exciting emerging field of technology and science, and become a QUANTUM HACKER!

We are very excited to bring back Quantum Village after our standing-room only success these last two years! This year we want to focus on looking at the parallels between how classical computing developed and became distributed and interconnected through LANs and WANs and later social networks, and how quantum computing is looking to do the same with the 'quantum internet', and what it means to have a 'social quantum network'. To this end we are working with some quantum infrastructure companies to have a real quantum network present at the event and ready for people to hack, e.g. via messing with the fibre lines we plan on distributing throughout the village.

We also want to use this analogy to get participants to ask questions about how quantum technologies can, should, and may fit into society at large, building on our 'Quantum Life' sessions in previous years that have lead to some really engaging discussions and thought provoking debates - all of which we would continue to build upon.

We also want to provide a bigger, more expansive Quantum CTF competition within the village that we would like to build our own hardware (e.g. badges) to present both as part of the challenge.

RADIO FREQUENCY VILLAGE

LEVEL 1 - HALL 3 - AISLE 05-03

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

After 17 years of evolution, from the WiFi Village, to the Wireless Village, RF Hackers Sanctuary presents: The Radio Frequency Village at DEF CON 32. 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, Radio Frequency Identification (RFID), Infrared (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.

Co-located with the RF Village is the RF Capture the Flag. Come for the talks, stay for the practice and the competition.

AIxCC

The AI Cyber Challenge (AIxCC) aims to accelerate the development of AI-driven systems to secure our critical infrastructure by fixing software vulnerabilities autonomously and at scale.

Visit the AIxCC Experience to witness the semifinals of this public prize competition. Teams' Cyber Reasoning Systems will compete to win one of the $2 million in semifinal prizes and a spot in the 2025 final competition.

Explore our cybersecure City of the Future where you can...

Immerse yourself in the competition.

Learn about the consequences of unsecured infrastructure and AI's potential to secure it.

Meet the Organizers and Collaborators producing the AIxCC.

HOURS

Friday: 10am-6pm
Saturday: 10am-6pm
Sunday 10am-2pm

Scan the QR code to check out a more detailed schedule of talks and City happenings.

VILLAGES

Who runs this thing?

RF Hackers Sanctuary is a group of all volunteers with expertise in radio security and various other related fields. We are the original creators of the WiFi Capture the Flag, Wireless Capture the Flag, and RF Capture the Flag. We are the original founders of the WiFi Village, Wireless Village, and RF Village. Often imitated, never duplicated.

RECON VILLAGE

LEVEL 1 - HALL 4 - AISLE 03-04

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

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 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, participate in Live Recon, and, most of all, have fun. At RV, we keep things simple, and the focus is on generating quality content using talks, workshops, CTF, live hacking, hackathons, etc. This year, we are launching a new hands-on event, i.e. Live Recon Contest, where we will challenge participants to perform recon on organization (pre-approved) - live and compete against each other to find as many as recon flags. This will include gauging skills like domain discovery, subdomain enumerations, GitHub Dorking, Metadata Extraction, data harvesting, social media profiling, threat intel mining, correlations and aggregations, and a lot more.

Also, to reduce the barrier to entry, we are going to host 101 Hands-on OSINT & Recon Workshops where people can learn and practice some new skills.

Similar to the previous years, there will be Awesome rewards for the winners, along with free t-shirts, stickers, village coins, and other schwag 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.

RED TEAM VILLAGE

LEVEL 2 - ROOM W204-W207

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

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. Attendees may spend all three days engaged in introductory workshops or challenge themselves in an immersive Capture the Flag competition to put their newly obtained skills to the test.

SOCIAL ENGINEERING COMMUNITY VILLAGE

LEVEL 3 - ROOM W317-W319

FRIDAY: 08:30 - 18:00; SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 14:00

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

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

- Vishing Competition (#SECVC): This edge-of-your-seat 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 to elicit as many objectives as possible. The highest score wins! This competition takes place only on Friday.

- Youth Challenge: Anyone 18 and under is invited to compete and learn about more than just Social Engineering; our challenges include areas in cryptography, network security, defusing intergalactic implosion bombs, and more. Can you stop the universe from imploding into what we're assuming is probably another universe but much smaller? We hope so! Otherwise, even the dolphins will have to find a new home.

- Cold Calls: This event lets DEF CON attendees sign up in the village (first come, first serve style) to place live phone calls inside 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!

- New: This year, we may have a couple more surprises up our sleeves – stay tuned and check out our website as it gets closer to DEF CON with our daily schedule!

TAMPER EVIDENT VILLAGE

LEVEL 1 - HALL 2 - AISLE 07-03

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

"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.

- 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.

TELECOM VILLAGE

LEVEL 2 - ROOM W201

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

The Telecom Village is a platform for anyone with an interest in both the offensive and defensive facets of telecom security. The village is where a variety of events, including talks, CTFs, and discussions centred on telecom security, take place. The Telecom Village's primary focus would be on Telecom Security. We plan to host multiple hands-on events as part of the village 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 mini workshops and panels, spread across two days.

This Year we are planning to cover the following points Live4G/5G(SA) with Commercial BTS, internals and of a SIM Card, Simulating 4G/5G in a portal portable computing device, fundamentals of VoLTE/VoNR and its Attack vectors, MBSS for Telecom Security etc.

Telecom Security is an extremely focused and relatively closed domain within the Industry. We hope to bring this to a larger audience, ensure that they have a source which could act as a structure to facilitate learning and development in the sector. We will see larger adoption of Private 5G network across the globe and industries, which will come with it's own set of unique challenges. We hope this village will play a key role is development and identification of key talents/projects which will help in tackling security challenges that plagues the telecom sector.

VOTING VILLAGE

LEVEL 2 - ROOM W223-W224

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

The Voting Village is an interactive educational environment that provides the public with the unique opportunity to have 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. The Voting Village explores all aspects of election security and works to promote a more secure democracy.

VILLAGES

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 access to other experts as well as the option of joining us for our speaker track (TALKS) that will take place every day except for the last Sunday of DEF CON. 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 DEF CON.

Due to it being a presidential election year, the focus on elections is going to be extremely heightened. Having an open research environment like the Voting Village helps offset the misinformation and disinformation that is rampant leading up to a presidential election. The Voting Village not only addresses election infrastructure related issues but also focuses on information integrity as a critical element of our election system. Our talks given by the most reputable subject matter experts cover all of these election related topics.

XR VILLAGE

LEVEL 1 - HALL 4 - AISLE 0106

FRIDAY & SATURDAY: 10:00 - 18:00; SUNDAY: 10:00 - 13:00

Talks, playground for using XR tech, open bug hunt, bug bounty workshop, tech & art performances, VR gaming, and cross conference AR "Pokemon Go!" style collection experience. Federal agencies CISA and national laboratories Idaho & Pacific Northwest will be hosting interactive demos and an escape room in our space. They will be in collaboration with the ICS Village.

Workshop / Open Bug Hunt Pwn-a-Palooza (Collab with Hardware Hacking Village, Red Team Village)

The event is an open bug hunt with components of hardware hacking, XR rooted devices for workshop tie-in (VR headsets, glasses) and we are working with other villages and seeking support from industry pros to better direct the expectation of the hunt. We would like to offer prizing.

Playground

Open area for exploring emerging and existing XR tech; gaming, haptics, deconstructed devices to play with.

AR hunt / collection game

Collect village "stickers" throughout the con a la Pokemon Go! Style AR overlay that interacts with all the other villages at DEF CON. Think red mowhawks from Red Team Village, a viking from Adversary Village, a goat from OWASP, etc.

"I'M SORRY DAVE, I'M AFRAID YOU FUCKED IT UP"

DFIU

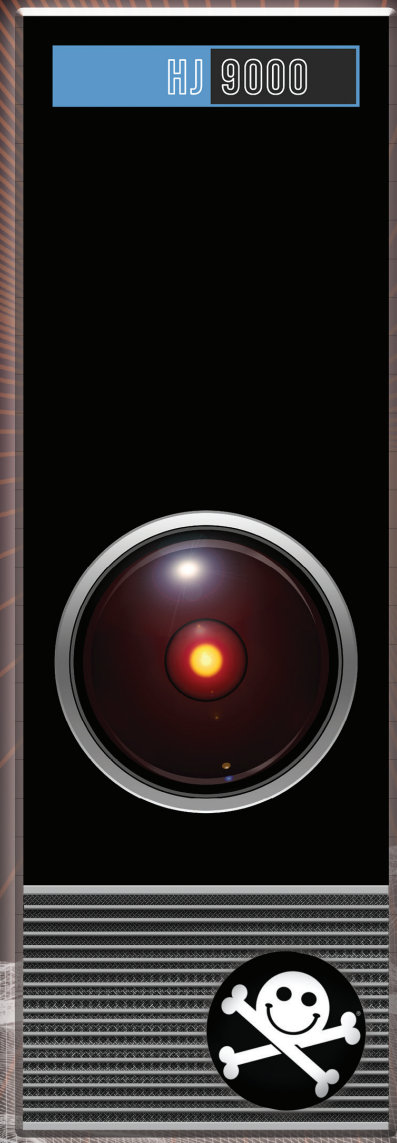
HACKER JEOPARDY

30th ANNIVERSARY EXTRAVAGANZA

DEFCON 32

Friday & Saturday @ 8p

TRACKS 1 & 2



CONTESTS

5N4CK3Y

Level 1 - Hall 4 - Aisle 02-01-B
In-Person Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-12:00

AND!XOR creates electronic badges filled with hacker challenges. We love doing this, especially coming up with unique ways for hackers to earn them. Introducing the newest member of our hacker-fam: 5N4CK3Y (Snackey). 5N4CK3Y is a vending machine hardware hacking project from AND!XOR. We retrofitted it into an IoT CTF based badge dispensing machine, bling and all. Find a flag on our web hosted CTF platform, you get a 5N4CK3Y dispense code, punch it in, and a badge is vended to you! Theraom hardware hacking, reverse engineering, OSINT, network security, and cryptography to name a few. There's a little bit of everything, so it's a perfect way to learn something at one of the many DEF CON villages and talking with people you meet, then attempt one of the CTF challenges to dispense a badge. Hardware hacking is our passion and we want people to learn on badges, but more importantly that there's a lot to learn at DEF CON so our CTF will hopefully serve a desire to learn something new and meet new friends while trying to earn a badge and hack it further.

@ANDnXOR

? CUBE

Level 1, Hall 4 - Aisle 02-02
In-Person Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-12:00

The Return of ? Cube

? Cube returns, weaving a tale that transcends the ordinary. This year, engagement is not just a theme—it's a journey through the multi-dimensional realms of hacking. Progressive Puzzles: Unlock the secrets of each compartment as you journey through progressively harder puzzles. From the Front's gentle introduction to the Top's formidable challenges, the Cube invites you to engage with the spectrum of cybersecurity domains. Physical Entry Unleashed: In a bold evolution, physical entry becomes a key component. Navigate the tangible aspects of physical entry, decoding not only in the digital realm but also as you immerse yourself physically in the enigmatic sides of ? Cube. Cryptic Narratives: As each compartment unfolds, the narrative of engagement takes shape. The puzzles, touching on encryption, penetration testing, and beyond. Silent Intricacies: Engage not only with the puzzles but also with the silent intricacies woven into the physical challenges. Decrypt messages, decipher patterns, and embrace the essence of DEF CON as you navigate the unseen and the tangible. Embark on the Engage Journey: ? Cube calls upon the curious and the bold. Embark on a journey where the puzzles transcend the digital divide, demanding both mental acuity and physical prowess. H4QEG5LCMUQEAICEMVTG-G33OEAZTEICSMVQWI6JAORXSAZLOM5QWOZJ7

http://0x3fcube.com/

A WALL OF BRIBES

Level 1 - Hall 4 - Aisle 02-02-F
In-Person Contest
Saturday: 10:00-16:00;
Sunday: 10:00-12:00

This is a contest about bribery. Bribery is not only allowed, it is required as part of the contest, since it's the only way to move up the leaderboard. Judges will evaluate the value of any given bribe (for example, an unusual sticker, etc.), and award points accordingly. Boring bribes will be rejected (i.e. cash). Players can expect to learn how to make a persuasive argument, and the nature of value in an (often) pay-to-win world that we live in.

ADVERSARY WARS CTF

Level 1 - Hall 4 - Aisle 03-05
In-Person Contest
Friday and Saturday: 10:00-17:00; Sunday: 10:00-12:00

Adversary Village will be hosting "Adversary Wars CTF", which is built around adversary attack simulation, offensive cyber security and purple team tactics.

Adversary War CTF centers around mimicking enterprise infrastructure and corresponding challenges. These challenges are meant to push the participants towards adopting various TTPs that adversaries and threat actors use within a definitive time frame. Adversary Wars would have real world simulation CTF scenarios and challenges, where the adversaries can simulate attacks and learn new attack vectors, cyber threat intelligence, threat actor profiles, TTPs, techniques, etc. There would be combined exercises which include different levels of adversary emulation.

As part of the Adversary Wars Capture-the-Flag competition a fictional city would be hosted virtually as a target for the participants. Like all cities, the Adversary city too would comprise of various infrastructure components including a hospital, bank, police station, fire station, army camp, city apartments, IT companies, university, government buildings, power plant, etc.

Each building will have a complex and realistic network infrastructure that includes a wide variety of components, including Windows/Linux systems, applications, industrial systems, Active directory, cloud environments, hybrid environments, and numerous other technology systems. A complex network of interconnected organizations, assumed to have been working properly, monitored by security operations center and cyber defense systems, supposed to be hackproof, until it wasn't. One fine day, the adversary city was breached by a threat actor. A wide variety of attacks were carried out by the threat actor, in the end they decided to shut the city for good and infected the remaining systems with ransomware.

CTF participants will need to rely on cyber threat intelligence to gather more information on the threat actor, understand and collect various attack tactics, tools, and exploits used by the adversary group. The participants will have to devise possible attack paths used by the adversary group, then simulate these activities against the target city's various components to recreate and understand how deeply the threat actor group breached the city's infrastructure and computer systems.

To visualize the CTF environment, the contest area will feature a miniature model of the city made using interlocking-plastic-bricks. The breached components OR organization buildings will be physically marked in the city model as the CTF progresses. This will also assist visitors and observers in understanding the contest's progress and gaining insight into what is happening behind targeted cyber-attacks, cyberwar, etc.

https://adversaryvillage.org/adversary-wars-ctf/
@AdversaryVillag

AI ART BATTLE

Level 1 - North Lobby (C&E Stage)
In-Person Contest
Friday: 13:00-15:00

13:00 -13:30 setup
13:30 - 14:00 qualifiers
14:00 -15:00 contest

This unique competition invites creative minds to dive into the world of artificial intelligence and art. The challenge is to craft the most imaginative prompts that will be used by generative AI models to create artwork.

Contestants will not be creating the art themselves; instead, they will focus on designing prompts for well-known topics that push the boundaries of creativity and innovation.

How It Works:

Select a Topic: Contestants will choose from a list of random topics.

These could range from historical events, famous literary works, mythical creatures, futuristic landscapes, to iconic pop culture references.

Craft a Prompt:

Using their creativity, contestants will write a detailed prompt designed to guide AI models in generating original artwork. The prompts should be clear, imaginative, and offer enough detail to spark the AI's artistic capabilities.

Submission: Each contestant will submit their prompt and the intended outcome.

AI Generation: The submitted prompts will be fed into a generative AI art model, which will create corresponding artworks based on the prompts.

A random panel will determine who the winners are.

AUTODRIVING CTF

Level 1 - Hall 4 - Aisle 01-05-B
In-Person Contest
Contest available online Friday 10:00 to Saturday 18:00

The AutoDriving CTF contest focuses on the emerging security challenges in autonomous driving systems. Various levels of self-driving functionalities, such as AI-powered perception, sensor fusion and route planning, are entering the product portfolio of automobile companies. From the security perspective, these AI-powered components not only contain common security problems such as memory safety bugs, but also introduce new threats such as physical adversarial attacks and sensor manipulations. Two popular examples of physical adversarial attacks are camouflage stickers that interfere with vehicle detection systems, and road graffitis that disturb lane keeping systems. The AI-powered navigation and control relies on the fusion of multiple sensor inputs, and many of the sensor inputs can be manipulated by malicious attackers. These manipulations combined with logical bugs in autonomous driving systems pose severe threats to road safety.

We design autonomous driving CTF (AutoDriving CTF) contests around the security challenges specific to these self-driving functions and components.

The goals of the AutoDriving CTF are the followings:

- 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.

- Provide CTF challenges that allow players to learn attack and defense practices related to autonomous driving in a well-controlled, repeatable, and visible environment.

- Build a set of vulnerable autonomous driving components that can be used for security research and defense evaluation.

The contest is based on a Jeopardy style of CTF game with a set of independent challenges. A typical contest challenge includes a backend that runs autonomous driving components in simulated or real environments, and a frontend that interacts with the players. This year's contest will follow the style of last year and includes the following types of challenges:

- "attack": such as constructing adversarial patches and spoofing fake sensor inputs,

- "forensics": such as investigating a security incident related to autonomous driving,

- "detection": such as detecting spoofed sensor inputs and fake obstacles,

- "crashme on road!": such as creating dangerous traffic scenarios to expose logical errors in autonomous driving systems.

- "smart planner": such as creating intelligent path planners for dangerous tasks that are difficult for human drivers

Most of these challenges will be developed using game-engine based autonomous driving simulators, such as CARLA and SVL. The following link contains some challenge videos, summaries from AutoDriving CTF at DEF CON 29 and DEF CON 30

https://drive.google.com/drive/folders/1JSVarIaQBm-seLC9XqkfrxnRQto4WM225?usp=sharing

https://www.youtube.com/channel/UCPPsKbVpx-wk-464KIzr8xKw

What's new in 2024

This year, we will unlock new traffic conflict scenarios that are observed from real-world driving logs such as Jaywalk and double parked vehicles. New difficulty

CONTESTS

levels will be added to challenges in such scenarios by integrating real downstream AI modules such as object tracking from open-source autonomous driving software like Apollo, Autoware and OpenPilot.

In order to enable the audience to experience the challenges more directly, we plan to set up a vehicle wheel controller on site and provide a driving game this year. Audiences can drive themselves to compete with the self-driving vehicle in some of the challenges. Driving game demo:

https://drive.google.com/drive/folders/1LIzJJ1I-3Eqj_e0_ntX5eFu82U9ObiEYB?usp=sharing

For players

- What do players need to do to participate AutoDriving CTF?

Most of the challenges do not require domain knowledge of autonomous driving software or adversarial machine learning, although knowledge of those helps. For example, the players can generate images the way they like (e.g., drawing, photoshopping) to fool the AI-components or write a short python script to control the vehicle. Some challenges, such as incident forensics likely would require players to learn domain knowledge such as sensor information format and how fusion works.

- What do we expect players to learn through the CTF event?

Players can (1) gain a deep understanding of real-world autonomous driving systems' design, implementation, and their corresponding security properties and characteristics; and (2) learn the attack and defense practices related to autonomous driving in a well-controlled, repeatable, visible, and engaging environment.

@autodrivingctf

AW, MAN PAGES

Level 1 - North Lobby (C&E Stage)
In-Person Contest
Friday: 12:00 - 13:00

How well do *you* know your man pages? Find out by teaming up with up to 3 other people (or come solo and get matched up with some new friends) and play "Aw, man...pages!". Across several rounds, your knowledge of man pages will be tested to the limit. Can you remember what command line flag is being described by its help text? Can you identify a tool just from a man page snippet? Can you provide the long-form flag when only given the short? Will you prove yourself worthy to be crowned the man page champion?

BETTING ON YOUR DIGITAL RIGHTS: 3RD ANNUAL EFF BENEFIT POKER TOURNAMENT AT DEF CON 32

Other / See Description
In-Person Contest
Begins Friday at 12:00 (11:00 for the pre-tournament poker clinic)

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 EFF! 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

BEVERAGE CHILLING CONTRAPTION CONTEST

Level 1 - Hall 4 - Aisle 01-04-B
In-Person Contest
Friday: 10:00-16:00; Saturday: 12:00-18:00

The Beverage Chilling Contraption Contest has been un-canceled! After a fantastic afternoon of day drinking celebrating the start of the 20th BCCC we've run out of beer. It's a disaster, a catastrophe! Fortunately, we had the wherewithal to scramble a crack beverage acquisition team to the streets of Las Vegas and found more! Don't ask where. Unfortunately, like the streets of Las Vegas, it's HOT and kinda sticky. We need you to help us fix this and get that beer as cold as the barren wasteland that is our generation's dreams of home ownership!

BIC CTF

Level 3 - Room W314-W316
Hybrid Contest
Contest available online Friday 12:00 to Saturday 23:59

The BIC Village Capture The Flag is a jeopardy style event designed to practice solving challenges in multiple categories. This event seeks to not only be a series of puzzles and challenges to solve, but a gamified way to learn concepts of social justice and Black history. This event will highlight previous, current and up & coming Black individuals and their contributions to technology. This year we are excited to bring back our physical challenge room with a variety of interactive components for players to interface with.

This event also aims to bring to the forefront a range of technologies that we will expose to the community that operate in our day-to-day lives and examine their capabilities; contributing to the discussion of privacy, social justice and civil rights. Our event will allow the DEF CON community to fully engage in "Reading all the stories, learning all the technologies, and hacking all the things."

https://www.blacksincyberconf.com/ctf

BIOHACKING VILLAGE CTF

Level 1 - Hall 3 - Aisle 05-07
In-Person Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-13:00

Welcome, elite hackers and cyber sleuths, to a CTF experience like no other - the "Code D.A.R.K. : Biohacking Village CTF Challenge". Merge the worlds of biology and cybersecurity in an adrenaline-pumping contest that tests your skills in ways you've never imagined. Thrilling and challenging cybersecurity adventure centered around a hospital setting as a scenario where participants engage in a race against time to secure or retrieve critical medical data, navigating through various cybersecurity puzzles and challenges, where participants act as guardians of critical biological data.

Unravel Biological Mysteries: Dive into a narrative where biotechnology meets cyber-warfare. Decode genetic puzzles, breach virtual lab networks, and outsmart bioinformatics security systems. Elevate Your Hacking Game: Challenge yourself with unique biocybersecurity scenarios. This isn't your typical CTF - it's a fusion of biotech intrigue and hardcore hacking. Compete and Collaborate: Team up with fellow biohackers and cyber warriors. Share knowledge, strategize, and show off your skills in a community where biology and bits intersect.

Gear Up for a Cyber-Biotech Showdown

- Immersive Scenarios: Each challenge is a step into a world where safeguarding biological data is as critical as securing digital assets.

- Skill Diversity: Whether you're a veteran hacker or a biotech enthusiast, Genome Raiders offers a range of puzzles that cater to a wide array of skills and interests.

https://www.villageb.io/capture-the-flag

BLUE TEAM VILLAGE CTF

Level 3 - Room W311-W313
In-Person Contest
CTF begins Friday 10:30;
CTF ends Saturday 18:00

The Blue Team Village (BTV) CTF is a cyber defense Capture the Flag 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 several incidents involving different operating systems and OT devices. You will have access to SIEM and Packet captures; however, just like in real life, these tools have issues you must overcome to uncover what happened.

Expect indexes to telemetry issues, raw data not extracted properly, and missing fields. Regex may be helpful. In addition, Arkime, the network monitoring tool, will only work partially and correctly. You must find ways to make the best of the telemetry provided, and remember that you can always extract the resulting pcaps!

The CTF challenges contestants to leverage diverse cyber defense skills, including Incident Response, Forensics, and Threat Hunting. Both host and network telemetry are required to solve all the flags.

BTV's Project Obsidian crew developed the CTF to allow anyone, regardless of skill or knowledge, to participate and sharpen their cyber defense skills. We recommend creating or joining a team if you are new to cyber defense. We highly recommend participating in the BTV's Project Obsidian workshop sessions if you are new to cyber defense. Sessions cover many of the topics on the CTF and will help you along the way.

https://www.blueteamvillage.org/ctf

CAPTURE THE PACKET

Level 2 - Room W216-W221
In-Person Contest
Friday and Saturday 10:00-18:00; Sunday: 10:00-12:00

This event was born out of the fires of DEF CON. Through years of analyzing network traffic for the Wall of Sheep and teaching others how to do the same, we built this system as a way to help the growing numbers in our community learn (fast). Then it quickly turned into the first defensive based CTF at DEF CON and is one of the longer running competitions at con with a twist... Each year we practically re-invent ourselves, bringing the latest tools & techniques along with never seen before content across 17 categories to unleash hell on the mostly-unsuspecting attendees. For '24 we have added tons of new content, and new types of challenges never seen before. (muehahaha)

https://www.capturethepacket.com
@capturetp

CAR HACKING VILLAGE CTF

Level 1 - Hall 4 - Aisle 01-01
In-Person Contest
Friday: 10:00-16:30; Saturday: 10:00-18:00; Sunday: 10:00-12:00

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 OEMs 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 10 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.

CONTESTS

We plan to use this event to keep drawing attention to the automotive security industry through hands-on challenges.

https://www.carhackingvillage.com/
@CarHackVillage

CHASSE PARTIE SYSTEMS CTF

Level 1 - Hall 4 - Aisle 01-04-E
Hybrid Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-13:00

The inception of this distinctive event occurred at DEF CON 31, initiated by a fortuitous encounter with CookieT while participating in LineCon for merch. Our shared passions fostered an immediate bond, and it was amidst this camaraderie that the idea for a future challenge germinated. Having previously engaged participants with puzzle-embedded challenge coins, I (Chasse) was inspired to expand the concept beyond a mere cipher. The aim was to design a contest that would appeal across a broad spectrum of skill levels by integrating a variety of puzzles, both modern and traditional, to attract a wider audience from a complete beginner new to the hackerspace to the more seasoned and advanced hacker. Observing the collective enthusiasm as participants unraveled the first simple coin puzzle was exhilarating, yet the quick resolution of the puzzle occasionally detracted from the overall experience for more advanced puzzle solvers. Throughout DEF CON 31, CookieT and I explored the feasibility of a web-based challenge CTF, laying the foundation for what would evolve into a pioneering contest and experience. Later Raven emerged from the shadows of cyberspace to help us chisel out the contest from Zeroes and Ones

With the announcement of DEF CON 32's theme, our concept was honed, ready to blend our creative talents into this year's challenge. We crafted an innovative combination of a narrative-driven journey game, scavenger hunt, and web-based Capture The Flag (CTF) challenges, all meticulously aligned with the DEC CON 32 "Engage" theme. This contest emerges as a holistic platform, introducing DEF CON newcomers to core security principles through an engaging narrative. Spanning a variety of fields including OSINT, cryptography, radio, telephony, password, and web security. It promises a rich, diverse experience! Participants, automatically divided into teams, are propelled on a quest to decode puzzles and unearth flags, with challenges designed to suit everyone from novices to veterans seeking sophisticated, intricate challenges. This contest transcends the conventional competition framework, evolving into an artful endeavor that illustrates the symbiosis of storytelling and technical puzzles to create a deeply immersive learning adventure. Imagined as an interactive storybook, it invites attendees to navigate their own routes, making their own choices that lead them through a story-rich exploration of security concepts and engagement even with each other.

The technical infrastructure of this experience is built on varied technologies. The main website, https://www.chassepartie.com, is developed with Ruby on Rails 7.1 and hosted on Heroku, with CloudFlare acting as our Web Application Firewall (WAF). This site functions as the scoreboard and narrative hub of the contest. Additionally, we have set up an XCP-NG hypervisor to host approximately 10 to 15 virtual machines as targets for participant engagement. Augmented reality markers are also in place, intended for deployment in communal areas like sticker boards, to enhance the experience. These elements are interwoven with the storyline, guiding attendees through what we believe is an unprecedented adventure-style CTF challenge named Chasse Partie Systems – Dystopian Apocalypse Resistance Terminal.

So come and join us on our deviant journey, what are you waiting for?

CLOUD VILLAGE CTF

Level 1 - Hall 2 - Aisle 09-01
Hybrid Contest
Friday 10:00 - Saturday 23:59

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 two 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

@cloudvillage_dc

CMD+CTRL AT DEF CON 32

Level 1 - Hall 4 - Aisle 03-06-D
In-Person Contest
Friday and Saturday 10:00-18:00; Sunday: 10:00-12:00

CMD+CTRL Web App Hacking Challenge gives you the opportunity to showcase your red team skills by attacking real web applications. The CMD+CTRL platform 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 world systems at risk.

At DEF CON 32: We will be replaying some of our Cyber Range Greatest Hits. We will be running 4 different Ranges with over a 150 challenges possible!

https://defcon32.cmdnctrl.net

CRACKMEIFYOUCAN

Level 1 - Hall 4 - Aisle 01-05
Online Contest
Friday
11:00 - Sunday 11:00

Zoogleta has been scheming to corporatize and enshittify the Internet through regulatory capture, squashing indy devs, and commodifying users.

You've been contacted by journalists and whistleblowers who need help sifting through some big dumps of encrypted data and password hashes.

Help them so they can publish the smoking gun, crash Zoogleta's stock price, and get their leadership and the corrupt politicians they own arrested by exposing their internal dirt, for great justice.

Time is of the essence! You will have 48 hours to crack as many files and hashes as possible.

Open to all, but pre-registration is recommended. Compete in the Street class for individuals or small teams, or in Pro if you do not want to sleep all weekend. Check out past years' contests at https://contest.korelogic.com/ , and the Password Village at https://passwordvillage.org/

https://www.crackmeifyoucan.com
@CrackMeIfYouCan@infosec.exchange

CRASH AND COMPILE

Level 1 - Hall 4 - Aisle 01-04-C
In-Person Contest
Qualifications:
Friday 10:00 to 15:00
Contest: Saturday 16:00 - 19:00

What happens when you take an ACM style programming contest, smash it head long into a drinking game, throw in a mix of our most distracting helpers, then shove the resulting chaos incarnate onto a stage? You get the contest known as Crash and Compile.

Teams are given programming challenges and have to solve them with code. If your code fails to compile? Take a drink. Segfault? Take a drink. Did your code fail to produce the correct answer when you ran it? Take a drink. We set you against the clock and the other teams. And because our "Team Distraction" think watching people simply code is boring, they have taken it upon themselves to be creative in hindering you from programming, much to the enjoyment of the audience. At the end of the night, one team will have proven their ability, and walk away with the coveted Crash and Compile trophy.

Crash and Compile is looking for the top programmers to test their skills in our contest. Do you have the problem solving and programming ability to complete our challenges? More importantly can you do so with style that sets your team ahead of the others? We encourage you to try your hand at the Crash and Compile qualifiers. Gather your team and see if you have the coding chops to secure your place as one of the top teams to move on to the main contest event.

Qualifications for Crash and Compile will take place 10:00 to 15:00. Come see us in contest area West Hall 4, or if you are excited to get started, qualifying can be completed from anywhere, as it takes place online at https://crashandcompile.org. You need a two hour block of time to complete the qualifying round. Points are awarded based on time to complete and problem difficulty.

https://crashandcompile.org/

CREATIVE WRITING SHORT STORY CONTEST

Virtual
Online Contest
Pre-con

The DEF CON Short Story contest is a pre-con contest that is run entirely online utilizing the DEF CON forums, Twitter, and reddit. This contest follows the theme of DEF CON for the year and encourages hackers to roll up their sleeves, don their proverbial thinking cap, and write the best creative story that they can. The Short Story Contest encourages skills that are invaluable in the hacker's world, but are often overlooked. Creative writing in a contest setting helps celebrate creativity and originality in arenas other than hardware or software hacking and provides a creative outlet for individuals who may not have another place to tell their stories.

So many hacker skills depend on your ability to tell a story. Whether it's social engineering, intrusion, or even the dreaded customer pentest report, ALL of these require the ability to tell a story. Storytelling is one of mankind's oldest traditions. Presenters even engage in storytelling when they get up on stage. A contest that celebrates and focuses on the ability to wind a yarn that captures and engages an audience is highly appropriate.

So why not?

@dcshortstory

CYBER DEFENDER - THE GAME

Level 1 - Hall 4 - Aisle 03-06-C
In-Person Contest
Friday and Saturday
10:00-18:00; Sunday: 10:00-12:00

Various cyber tools and techniques have been utilized based on information from past attacks. Game players will learn about different cyber security frameworks, cyber-attack processes, and how they can use utilised in a fun way. The game is built to teach key cyber terms, theory and apply techniques based on real-world scenarios.

As a player, you are part of a Global Cyber Protection Team (GCPT) assigned to the mission to prevent various attacks on critical infrastructure. Your task is to use the available information that your team has at your disposal to stop the adversary from achieving their objective.

Players will find themselves in a variety of future scenarios based on a specific industry/sector focus e.g. manufacturing, utilities, defense, finance. The task will be to defend each individual network/system to govern, identify, detect, respond and recover against

CONTESTS

abnormal/suspicious activities on the network. You will be working against a global hacker network who are threatening to disrupt the overall operations of global critical infrastructure sites for their own nefarious means.

Your team must protect various networks/systems as part of a global environment. If 5 or more systems are compromised and deactivated, the hacker network successfully disabled the global environment and can assume control of the entire environment. It is your mission to protect the environment and ensure the availability of the global system.

DARKNET-NG

Level 1 - Hall 4 - Aisle 02-01-D
Hybrid Contest
Friday and Saturday 10:00-18:00; Sunday: 10:00-12:00

Darknet-NG is an Alternate Reality Game (ARG), 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 final 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!

https://darknet-ng.network
@DarknetNg

DARPA'S ARTIFICIAL INTELLIGENCE CYBER CHALLENGE (AIXCC)

Level 1 - Hall 3 - Aisle 05-06
In-Person Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-14:00

DARPA and ARPA-H's Artificial Intelligence Cyber Challenge (AIxCC) will bring together the foremost experts in AI and cybersecurity to safeguard the software critical to all Americans. AIxCC is a two-year competition that asks competitors to design novel AI systems to secure this critical code and will award a cumulative $29.5 million in prizes to Teams with the best systems. In 2024, top teams will be awarded prizes of $2 million each, and will advance to the finals at DEF CON 33. The AIxCC Experience at DEF CON 32 is an immersive and interactive competition environment and educational space to inspire people and organizations to accelerate the development of AI-enabled cyber defenses. Attendees will explore a futuristic city where they can learn all about the competition, the technology, and the power of AI to help secure the software we all depend on.

Registration for AIxCC is no longer open to new contestants. AIxCC Preliminary Events were held March – July 2024.

Semifinalists will be announced here: https://aicyber-challenge.com/

https://aicyberchallenge.com/

DC KUBERNETES CAPTURE THE FLAG (CTF)

Level 1 - Hall 4 - Aisle 02-01-E
Hybrid Contest

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.

https://containersecurityctf.com/

DC STICKER DESIGN CONTEST

Virtual
Online Contest
Pre-con

Ancient warriors used tattoos as a means of indicating rank in battle; it was the sort of mark that told the tales of their various conquests - their struggles and triumphs. Similarly, traversing the halls of DEF CON, one can see more modern versions manifesting as stickers - especially on laptops and other electronic equipment.

We use stickers to break the ice with strangers, as a barter currency, to tell the tales of our struggles and triumphs. After all, is a hacker really a hacker without a laptop adorned with these markings?

Here's your chance to be part of hacker culture, by creating something that people around the world will treasure and proudly display. Submit original artwork in the theme of the con, that you believe best exemplifies hacker culture, that will be used as printed stickers.

On your marks... Make your mark.

DC'S NEXT TOP THREAT MODEL (DCNTTM)

DCNTTM
DC'S NEXT TOP THREAT MODEL

Level 1 - Hall 4 - Aisle 01-05-A
Hybrid Contest
Friday and Saturday: 10:00-18:00

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).

https://threatmodel.us

DEF CON 32 BEARD AND MUSTACHE CONTEST

Level 1 - North Lobby (C&E Stage)
In-Person Contest
Saturday: 11:00-13:00

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 (unofficial) Beard and Mustache Contest highlights the intersection of facial hair and hacker culture.

For 2024 there will be four categories for the competition you may only enter one:

- Full beard: Self-explanatory, for the truly bearded.

- Partial Beard: For those sporting Van Dykes, Goatees, Mutton Chops, and other partial beard styles.

- 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.

http://dcbeard.net/
@DCBeardContest

DEF CON MUD

Virtual
Online contest
Dates TBD, approx 2 weeks prior to DEF CON, Friday: 24 hours Saturday 24 hours Sunday: 24 hours

Excited about DEF CON? want to hack on a custom 26 year old code base? Like to play text based games? The DEF CON MUD has you covered. Completely rebuilt for 2024, explore dungeons, mine, complete quests, explore, hack the game. The winner gets a human badge to DEF CON 32. This year we are running the contest virtually 2 weeks prior to DEF CON. Play an ancient form of game and see if you have what it takes. We will be leaving the game up during DEF CON for more shenanigans.

https://mud.defcon.wtf

DEF CON SCAVENGER HUNT

Level 1 - Hall 4 - Aisle 03-02
In-Person Contest
Friday and Saturday 10:00-18:00; Sunday: 10:00-12:00

Whether you're a seasoned DEF CON veteran or a curious newcomer, the DEF CON Scavenger Hunt promises to challenge your skills, tickle your wits, and ignite your hacker spirit. Our list is a portal to mystery, mischief, and mayhem. Assemble your team of up to five members, interpret the items, and submit your findings at the booth to our esteemed judges. Go beyond the basics for bonus points. Legends are born here.

Casual players will enjoy doing a handful of items, but you will need to devote your entire weekend if you want to win. It's not just about fame, glory, or boxes of swag; the true allure is the camaraderie of fellow hackers, the knowledge that you've etched your mark on DEF CON history, and the ultimate badge of honor: bragging rights. Nothing says "I'm a hacker" quite like being triumphant at the DEF CON Scavenger Hunt contest.

See you at the booth!

https://www.defconscavhunt.com
@defconscavhunt

EMBEDDED CTF

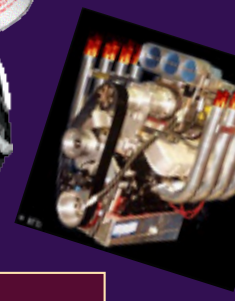
Level 1 - Hall 3 - Aisle 05-05
In-Person Contest
Friday and Saturday 10:00-18:00; Sunday: 10:00-13:00

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 case of use and have limited resources. This makes them both challenging and fascinating to work with, especially from a security perspective. Often these disciplines are dealt with individually, but understanding the custom relationships between hardware and software is vital to performing security research on these devices.

The embedded device 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

Nautilus Institute presents...

DEFCON32.CTF



Welcome to DEFCON32.CTF, our third year running Capture the Flag at DEF CON. We're pleased to represent the CTF community around the world at our favorite computer hacking conference.

While DEF CON hosts many CTF contests, we set this one apart by focusing on hard-core binary challenges that vex and torment the top teams from around the world, with depth and functionality to allow complex attack-defense tactics to develop. We're also bringing back LiveCTF head to head races, which brings even more excitement and strategic depth to an already complex contest.

Enjoying the CTF

We host teams that have traveled great distances to compete. Please respect their dedication and concentration to the game, and don't interrupt them.

Nautilus Institute members can be identified by the stylish lab coats, and will often be able to answer questions or help you understand how the game is going.

Spectators are welcome while the game is underway, but we will close the space to general humans while we set up and tear down the game daily.

Visit https://nautilus.institute for a more detailed schedule, including LiveCTF matches.

Qualifying

This year, we're bringing twelve teams to finals. Four of the teams have qualified through other contests: DEF CON CTF 2023, HITCON, 0CTF/TCTF, and PlaidCTF. The other eight were top teams in our qualifiers contest, held May 4 & 5 this year.

Want to take your place on the floor in 2025? Keep an eye on https://nautilus.institute for information about our qualifiers taking place in early 2025, and other qualifying contests. And in the meantime, study up on challenges from previous years, available on https://github.com/nautilus-Institute .

Thanks

We'd like to thank everyone who makes Capture the Flag possible at DEF CON. Whether you're a first-time attendee or a grizzled veteran, thank you for making DEF CON a special experience for us and our players. If you're a CTF player anywhere in the world, whether or not you qualified, thank you for the opportunity to build a contest that we hope you enjoy. And last but certainly not least, thanks to DT, the C&E team, and all DEF CON goons for running a great con year after year.

We hope you enjoy DEFCON32.CTF!

https://nautilus.institute

https://defcon.social/@nautilusinstitute

CONTESTS

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, 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. The competition provides a valuable opportunity to network with like-minded individuals and a chance to learn from others in the field hands-on.

Overall, the embedded device CTF contest is an exciting and educational experience that showcases the unique challenges and rewards of working with embedded devices. With the rise of the Internet of Things and the increasing integration of technology in our daily lives, embedded devices are becoming more ubiquitous, making this contest relevant and worth checking out. Whether you're a seasoned security professional or just starting in the field, the contest offers a chance to learn, test your skills, and have fun in a dynamic and competitive environment.

https://www.embeddedvillage.org
@EmbeddedVillage

FEET FEUD (HACKER FAMILY FEUD)

Level 1 - Hall 1 - Aisle 11-01:02 (Tracks 1-2)
In-Person Contest
Saturday: 18:30-19:30

Feet Feud (Hacker Family Feud) is a Cybersecurity-themed Family Feud style game arranged by members of the OnlyFeet CTF team and hosted by Toeb3rius (aka Tib3rius). Both survey questions and their answers are crowd-sourced from the Cybersecurity community. Two teams (Left Foot and Right Foot) captained by members of OnlyFeet and comprised of audience members go head to head, trying to figure out the top answers to the survey questions.

Attendees can either watch the game or volunteer to play on one of the two teams. Audience participation is also encouraged if either of the two teams fails to get every answer of a survey question.

Ultimately Feet Feud is about having a laugh, watching people in the industry attempt to figure out what randomly surveyed people from the Cybersecurity community put as answers to a number of security / tech related questions.

Survey: https://forms.gle/Thebx1vksze9fVsbA

GOLD BUG CHALLENGE

Level 1 - Hall 4 - Aisle 01-04-F
Hybrid Contest
Friday and Saturday
10:00-18:00; Sunday: 10:00-12:00

Love puzzles? Need a place to exercise your classical and modern cryptography skills? This puzzle can keep you intrigued and busy throughout DEF CON - and questioning how deep the layers of cryptography go.

The Gold Bug is an annual puzzle hunt at DEF CON, 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.

The Gold Bug is accessible to all, with some simpler puzzles for warmup or beginners (even kids!), and some that will require you to dig a little deeper. Whether you want to hack on puzzles solo or with a team, join us at https://goldbug.cryptovillage.org to get started!

https://goldbug.cryptovillage.org/
@CryptoVillage

HAC-MAN

Level 1 - Hall 4 - Aisle 02-01-C

Hybrid Contest
On-site Hours: Friday and Saturday 10:00-18:00; Sunday: 10:00-12:00

Becomes available online Thursday 12:00

Online and In-Person platforms will close Sunday 12:00

Players will only be able to turn in scavenger hunt items during On-site Hours.

This Pac-Man themed set of challenges takes Players on a journey through learning and demonstrating hacker and information security skills to earn points. With multiple subject-matter specific challenge groups and tracks, this hacker challenge game has something for everyone. You, dear Player, are Hac-Man (or Ms. Hac-Man, or Hac-Person), making your way through various dark mazes eating pellets, fruit, and ghosts. Each ghost represents a hacker puzzle or skills challenge. Upon completing each challenge, you'll be awarded points and can continue on to attempt further challenges. Many challenges have unlockable hints and location information, which you can unlock by spending your collected fruit.

There is a leaderboard! As you collect points, you'll show up on this leaderboard. The top 10 Players at the end of the game will be awarded various prizes from a prize pool.

https://scramble.roguesignal.io/

HACK3R RUNW@Y

Level 1 - North Lobby (C&E Stage)
Level 1 - Hall 4 - Aisle 03-06-B
In-Person Contest
Sign-ups: Friday 14:00-16:00

Contest: Saturday 13:00-15:00 (with a staging area to prep one hour before)

Get ready to strut your stuff, hackers! We're thrilled to announce the 6th annual Hack3r Runw@y returning to DEF CON 32, bigger and bolder than ever.

Calling all glamorous geeks, crafty coders, and fashionably functional folks: Dust off your soldering irons, grab your needles and threads, and unleash your creativity! Hack3r Runw@y challenges you to reimagine fashion through the lens of hacking.

Show us your wearable tech wonders in the following 4 categories for a chance to win in each category plus one coveted People's Choice trophy where ANYONE can win, but there will be a twist. Did you see this year's theme (hint).

Smart wear that wows: Integrate LEDs, microcontrollers, and sensors into your designs for dazzling functionality.

Digital design that dazzles: light it up with LEDs, bling with lights, but keep it passive.

Functional Fashion: masks and shields, hazmat suit, lockpick earrings, and cufflink shims.

Extraordinary style: Elevate your daily wardrobe with unique fabrics, passive design, 3d textures, optical illusions, cosplay, and security-inspired patterns.

No matter your skill level, Hack3r Runw@y has a place for you! Whether you're a seasoned maker or a coding newbie, join us in celebrating the convergence of creativity, technology, and style.

Winners selected by judges selection based on:

Uniqueness
Trendy
Practical
Couture
Creativity
Relevance
Originality
Presentation
Mastery

https://hack3rrunway.github.io/

HACKER JEOPARDY

Level 1 - Hall 1 - Aisle 11-01:02 (Tracks 1-2)
In-Person Contest
Friday and Saturday: 20:00-22:00

We are back for our 30th year at DEF CON! As always, it will be a mix of questions, answers and embarrassment. Contestants will try to outwit their other teams and prove that, yes, they are in fact smarter than a CISSP. Well, sometimes anyway. As usual, this will be a double-feature, with preliminary rounds occurring Friday night and the finals on Saturday.

This year, for our big anniversary, we will also be running a special Thursday night edition of Hacker Jeopardy - Celebrity Hacker Jeopardy! We will have some well-known faces competing in a single-evening event that should bring a fun twist to kick off what will be the biggest Hacker Jeopardy event in DEF CON history!

@HackerJeopardy

HACKFORTRESS

Level 1 - Hall 4 - Aisle 01-04-A
In-Person Contest
Friday: Free play 10:00 - 15:00,

Prelim Round 1: 16:00 - 17:00,

Prelim Round 2: 17:00 - 18:00,

Registration closes: 18:00

Saturday: Prelim Round 3: 11:00,

Prelim Round 4: 12:00,

Semi Finals Round 1: 14:00,

Semi Finals Round 2: 15:00,

Finals: 17:00

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.

http://hackfortress.net

HACKING BOUNDARY TERMINAL

Level 1 - Hall 4 - Aisle 03-06-E
In-Person Contest
Friday and Saturday:
13:00-18:00

In this MarSec event we will engage convention goers with a number of different tabletop games to help them understand the operational issues surrounding offensive and defensive cyber operations in a port complex. Players will become familiar with the various network components that support port and shipping operations from the underlying infrastructure to the system components at ports and commercial ships. A fictional terminal, Boundary Terminal part of the Port Elizabeth New Jersey complex, and a fictional shipping line, Worldwide Shipping Operations form the basis for all of three of our games. The games are: a short game designed to show the basic target set and linkages, a longer role-playing game where players can engage in detail with port systems, and a card driven game focused on detection, forensics, and counter-forensics. The role-playing game has been conducted as part of the MarSec portion of the ICS Village for the past two years, while the shorter version was added last year. This year we will add the counter-forensics game. All of the games are designed to be entertaining and engaging with prizes provided to the winners and best players (usually everyone gets a prize).

CONTESTS

HAM RADIO FOX HUNT

Level 1 - Hall 4 - Aisle 02-02-A
In-Person Contest
Friday and Saturday: 10:00-16:00; Sunday: 10:00-13:00

This contest is simple, and is designed to teach you the basics of transmitter direction finding and "fox hunting". We offer multiple levels of difficulty – whether you've never done a fox hunt before or are a seasoned pro, you can participate in the hunt! Learning how to locate the source of radio signals is an important tool you can add to your hacker arsenal. Whether you're hunting for a source of interference, a rogue wireless AP, or tracking down the FCC's monitoring vans, the real-world skills you will gain from this contest will be invaluable.

To participate in the beginner IR foxhunt you will need a device that can receive IR light in the 900nm range – such as many cell phones and digital cameras!

To participate in the RF foxhunt(s) you will need a radio or a scanner that can receive signals in the 2m and/or 70cm Amateur Radio Bands (144.000 MHz - 146.000 MHz, 420.000 MHZ - 450.000 MHz).

HARDWARE HACKING VILLAGE CTF

Level 1 - Hall 2 - Aisle 10-01
In-Person Contest
Friday and Saturday: 10:00-18:00

Grab some solder and update your JTAGulator! The Hardware Hacking Village (HHV) is back with another DEF CON hardware hacking-focused Capture the Flag (CTF) competition. 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.

https://dchhv.org/challenges/dc32

HARDWIRED

Level 2 - Room W216-W221
In-Person Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-13:00

This event was born out of the desire to teach an often-overlooked hardware and networking skill, and to provide the opportunity for experienced people to mentor others as they learn. DEF CON provides the perfect environment for people with no prior training to learn something useful and new. Hardwired networks are often overlooked in today's world of cellular connection and Wi-Fi, but they still play an important part in the backbone of information sharing. We believe that while cutting-edge technologies are thrilling, traditional skills-building still has its place, and we want to provide that opportunity to the DEF CON community.

HTB CTF: DATA DYSTOPIA

Level 1 - Hall 4 - Aisle 03-06
In-Person Contest

Friday and Saturday: 10:00-18:00; Sunday: 10:00-13:00

A powerful corporation, notorious for its unethical practices, leveraged their extensive data resources gathered from users, and their psychological profiles, to subdue the population into compliance. The immune few, realizing the extent of the corporate conspiracy, band together to expose and dismantle the corporation's grip on society. These individuals must navigate a dangerous world of surveillance and betrayal. Their mission is to ignite a global awakening and reclaim freedom from corporate domination.

Players will have to join the mission and participate in a CTF that would be beneficial for beginners and experienced players alike. The challenge categories will be Web, Cryptography, Forensics, PWN(binary exploitation) and Reverse Engineering. Various difficulty challenges from each category will be featured.

https://ctf.hackthebox.com/
@hackthebox_eu

ICS CTF

Level 1 - Hall 3 - Aisle 06-05
In-Person Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-13:00

The ICS Village CTF offers hands-on experiences with industrial control systems, which bridge technology with physics. Attendees engage with industry experts while solving challenges like a red vs blue manufacturing network process coupled with OT-specific jeopardy-stye challenges. This contest highlights vulnerabilities in industrial equipment and OT protocols. By simulating attacks on critical infrastructure, participants develop and practice DEF CON-level skills, enhancing their understanding with critical infrastructure and the world we rely on.

https://www.icsvillage.com/

IOT VILLAGE CTF

Level 1 - Hall 2 - Aisle 08-04
In-Person Contest
Friday and Saturday 10:00-18:00; Sunday: 10:00-13:00

The IoT village pi eating contest is a challenge where participants put their hardwear hacking experience to the test by going head to head with other hackers. Participants will be provided all the tooling necessary to get a root shell on an IoT device. Whoever roots the device in the shortest time wins.

https://scoreboard.iotvillage.org/

IT'S IN THAT PLACE WHERE I PUT THAT THING THAT TIME

Other / See Description
In-Person Contest
Friday and Saturday: 10:00-18:00

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.

@iitpwipttttt

LIVE RECON

LIVE RECON CONTEST

Level 1 - Hall 4 - Aisle 03-04
In-Person
Friday and Saturday 10:00-18:00

Contest Hours: Friday 10:00 - Saturday 18:00

Do you fancy doing live recon on Real Organizations? Then activate Yourself. And compete in a unique HACKER challenge.

This year we are launching a new nail biting Contest, i.e Live Recon where participants will compete with each other to perform a deep osint and recon on the target organization. Here are the details:

About the contest:

Join us for an electrifying two-day Live Reconnaissance Event. Whether you're a seasoned security expert, a curious newcomer or a bugbounty pro, this is your chance to test your skills in a high-octane environment.

Your Mission

Get ready to perform live reconnaissance on a curated list of companies. Dig deep and unearth critical information that could be game-changing. Use your analytical prowess and sharp instincts to explore, probe, and uncover hidden data.

Why Join the Hunt?

Experience Real-World Challenges: Face off against real-world scenarios.

Compete and Collaborate: Work with the best minds in the field.

Learn from the Masters: Recon on a massive scale.

Score Epic Prizes: Walk away with cool rewards.

Who's Invited?

If you've got a passion for cybersecurity and Recon, this event is for you. Whether you're a university student, a pro pentester, or a hobbyist eager to sharpen your skills, we want you! Teams are encouraged to register and bring a mix of talents to tackle these challenges head-on.

Get Ready to Recon!

Unleash your inner hacker and join us for a reconnaissance adventure you won't forget!

Please note that this is an in-person event, and winners need to be at DEF CON to collect their prizes. However, once we have announced the targets, participants can play it from anywhere online (as this is Recon on public and live targets).

https://reconvillage.org/live-recon-contest

LONELY HARD DRIVE

Level 1 - Hall 4 - Aisle 02-02-F
In-Person Contest
Friday and Saturday: 10:00-18:00, Sunday: 10:00-13:00

You have been randomly selected for additional security training. Be on the look out for one of our drives, USBs or surprise devices out here in Vegas, and follow along on @LonelyHardDrive for further clues to start hacking away at the puzzles. This is required for all LonelyCorp employees and Betty Pagefile is counting on you!

Discord: https://discord.gg/68pRuKdCpW

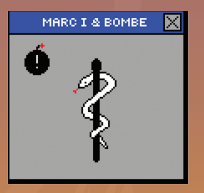
LONELY TAG

Level 1 - Hall 4 - Aisle 02-02-F
In-Person Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-13:00

How far will you go? Or, more accurately, how far was your tag's last reported location? Pre-register your team to receive one of a dozen tags, and check out our socials (@LonelyHardDrive) to watch the tags move across the map!

Discord: https://discord.gg/68pRuKdCpW

@LonelyHardDrive



MALWARE CONTESTS: MARC I & BOMBE

Level 1 - Hall 4 - Aisle 03-03
In-Person Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-13:00

MARC I: Malware Analysis Report Competition I

CONTESTS

In MARC I (Malware Analysis Report Competition I), participants collect and analyze real malware, then write an analysis report like a story, covering the entire scope of who, what, when, where, why, and how they found and analyzed the malware.

MARC I was created by Lena Yu (aka LambdaMamba) to provide malware enthusiasts with an opportunity to learn and showcase their passion and skills. Mastering malware analysis means mastering language. Essentially, we take a highly technical concept and simplify it into something that many can understand, similar to how a compiler translates high-level language into low-level language that a wide range of systems can understand.

When participants open-source and publish their work, it greatly contributes to improving the field of cyber defense. Let's make malware analysis knowledge go viral!

BOMBE: Battle of Malware Bypass and EDR

Try to capture malware by writing your own EDR, or become the malware to bypass detection! BOMBE (Battle of Malware Bypass and EDR) is a unique match where malware and EDR systems compete against each other inside a single VM boxing ring.

Our participants can choose if they want to be malware creator or EDR developer. Malware creators aim to exfiltrate credentials and transmit them to our designated server. On the other side, EDR developers will focus on detecting the malware's activities and report its findings. Both the malware and EDR, created by our participants, will battle each other directly inside a single VM. As they face off, they'll earn points for wins, moving up on the leaderboard. We also encourage them to keep improving their malware or EDR systems, system logs will be released after a few rounds.

BOMBE was created by Wei-Chieh Chao (aka oalieno) and Tien-Chih Lin (aka Dange). It is not just a competition, it's a learning platform. Participants engage with real-world scenarios, learning the circumstances between malware and EDR, a never-ending bypass and detect game. Showcase your skills! Whether you're a wizard at weaving undetectable malware or a mastermind in sophisticated defenses, this is your stage. Demonstrate your capabilities to a global audience, including potential employers and industry leaders.

https://digitalplaguedoctors.com/
@DigitalPlagueDr

OCTOPUS GAME

Level 1 - Hall 4 - Aisle 03-06-A
In-Person Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-13:00

Get ready to dive into the excitement of the third annual Octopus Game at DEF CON! Octopus Game is your chance to connect with fellow attendees while exploring all the fun and fascinating aspects of DEF CON. Whether you're new to DEF CON, a beginner at code-breaking, or simply seeking a stress-free contest, this is the perfect opportunity for you. Test your skills in clue reading and code-breaking as you join in on the fun!

You and your fellow pirates will embark on an exhilarating journey, armed with clues that unveil the path to the lost treasure of a legendary pirate, now guarded by the mighty Kraken. These quests will guide you through the vibrant landscape of the Con, offering a glimpse into the myriad opportunities and experiences awaiting exploration. Designed to welcome newcomers to the hacking world, this contest fosters connections among attendees and contributors alike. Whether you choose to collaborate with a small group or brave the challenge solo, the decision is yours. Yet, amidst the excitement, remember that only one can emerge victorious. With challenges tailored for entry-level participants and a kid-friendly environment, come join us for a thrilling adventure into the depths of the Kraken's Conundrum.

https://www.mirolabs.info/octopus-game-dc32
@OctopusGameDC

PHISH STORIES

Virtual

Online Contest

Phish Stories is a contest that combines the art of creative writing with the strategic challenge of social engineering, inviting participants to craft phishing emails that are both convincing and hilariously entertaining. It gives people at any level the chance to show off their skills in writing, social engineering, and humor to create a unique contest that allows for multiple ways to win. Writers, comedians, and Red-Teamers can all find a path to victory!

Participants are tasked with creating phishing emails targeting fictional company leaders. The goal is to produce emails that are not only convincing enough to prompt a click but also funny enough to entertain. Contestants must also provide a one-page backstory that gives the details of the approach and what happens after our unsuspecting company leader clicks on that link. Contestants receive background information on their targets to help craft their entries.

There are three winners in the contest.

The Ruler: Best overall combination of clickability and humor.

The Wizard: Best technical and clickable email.

The Jester: Funniest entry.

Reddit: https://reddit.com/u/phishstories

@phishstories

PHREAKME PRESENTED BY HACKEDEXISTENCE

Level 1 - Hall 4 - Aisle 02-02-C
Hybrid Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-13:00

The contest will be hosted on the Publicly Switched Telephone Network and will be live for access 24/7, with real world PSTN phone numbers to dial into.

The Hacked Existence team will be hosting a telecom based CTF. The CTF will be hosted on live VoIP lines routed through a modified asterisk PBX. This will allow participants to dial in to the CTF from a real world telephone routable phone number allowing them to hunt the PBX for flags. The flags will be based around utilizing historically accurate tactics, techniques, and procedures to manipulate emulated old school switching systems.

The purpose of our contest is to bring awareness around the still existing weaknesses in our telecom infrastructure and Interactive Voice Response Systems. Ideally visitors to our contest area will participate in the CTF allowing them to get a better understanding of telecom hacking in the year 2024 as well as a respect for the art of phreaking from yesteryears.

@HackedExistence @mainframed767

PINBALL HIGH SCORE CONTEST

Level 1 - Hall 4 - Aisle 02-01-A
In-Person Contest
Friday and Saturday: 10:00-18:00; Sunday 10:00-13:00

The inaugural Pinball High Score contest at DEF CON will run Friday and Saturday: 10:00-18:00, Sunday 10:00-13:00 with games available for daily High Score contests, daily challenges and open qualifying for a main tournament. The daily contests will allow any attendee to play pinball games and attempt to record a qualifying high score on each of the unique games. At 18:00 on Saturday main tournament qualifying will end and the top 8 players with the highest combined scores across all eligible machines will qualify for the Sunday finals event where they could become the first DEF CON Pinball Champion!

Achieving a high score may sound simple but pinball rulesets are very complex and the skill to complete a "Wizard Mode" or achieve a high score requires research, practice, knowledge and execution. Out of the box thinking, analytical skills and pattern recognition are traits that pinball players must exhibit to be successful and some games have rule sets that can be studied and exploited to achieve a high score. Hackers are at an advantage here and while this is just a pinball contest, I expect that the community is ready for this challenge.

Stern Pinball has prepared an exclusive DEF CON 32 digital badge that will be available for any attendee to earn for playing in this event. Additional DEF CON specific Insider Connect badges may be unlocked during game play.

Pinball developers have a long history of including Easter Eggs/COWS in games. Easter eggs "may" also be available for attendees to discover during the conference. Undocumented Easter eggs found by players during the event will be documented, verified and recognized.

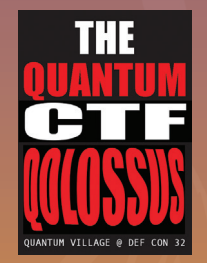
PUB QUIZ

Level 1 - North Lobby (C&E Stage)
In-Person Contest
Friday: 16:00-19:00

We are back with another Pub Quiz at DEF CON. Here at Pub Quiz, we felt the need to add additional prizes for 4th and 5th place. We had a very successful one last year and we have made some improvements to make it every better. So do you like Pub Quizzes?? If you do then get your butts to join us in participating in the 2nd Pub Quiz at DEF CON 32.

Quiz will consist of 7 rounds question will include 90's/2000's TV and Movies, DEF CON trivia, music, anime, and a little sex. The theme for our Pub Quiz will be all things that make DEF CON attendees exceptional. There will be a little something for everyone. The quiz will consist of visual and audio rounds along with some Con questions; we need to make sure we stimulate you peeps. We encourage people to get into teams of 5 or 6.

This is a social event, so we try to get people into Teams. You never know you may meet the love of your life. Did I mention CASH! Yes we will have cold hard cash prizes for the 1st, 2nd, 3rd, 4th, and 5th high scoring groups. As always if we do have ties will be break those ties with a good old fashion dance off from a person of the tied teams. The hosts and a few goons will help in judging.



QOLOSSUS

Level 1 - Hall 3 - Aisle 06-01
Hybrid Contest
Friday and Saturday: 10:00-18:00; Sunday 10:00-13:00

There's a new emerging tech in town, and it's name is Quantum! Following the past two years of Quantum CTF events held at the Quantum Village, we are pleased, proud, and excited to announce that our Q-CTF is indeed returning as Codename; QOLOSSUS! Pit your wits against the Atom, and come and see what devilish challenges from our Quantum Quizmasters await. Come and show your quantum prowess, and mastery of superposition and

CONTESTS

entanglement - design algorithms to break cryptography, hack our simulated quantum communications, and score points in our IRL activities. |Good Luck!⍰

https://quantumvillage.org/

RADIO FREQUENCY CAPTURE THE FLAG

Level 1 - Hall 3 - Aisle 05-03
Hybrid Contest
Friday and Saturday 10:00-18:00; Sunday: 10:00-13:00

In this game capture the flag you will be presented with real configurations of real wireless and radio technologies to attack. Practice your skill and learn new ones from Radio Frequency IDentification (RFID) through Software Defined Radio (SDR) and up to Bluetooth and WiFi. There may even be Infrared, if you have the eye for it.

RF Hackers Sanctuary is once again holding the Radio Frequency Capture the Flag (RFCTF) at DEF CON 32. 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 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.

This game doesn't let you sit still either, as there are numerous fox hunts, testing your skill in tracking various signals. If running around the conference looking for WiFi, Bluetooth, or even a Tire Pressure Monitoring System (TPMS) device sounds like fun, we are your source of a higher step count.

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.

https://rfhackers.com
@rf_ctf @rfhackers

REALI7Y OVERRUN

Level 1 - Hall 4 - Aisle 02-02-E
Hybrid Contest
Friday and Saturday: 10:00 - 18:00; Sunday 10:00 - 13:00

This is going to be an interactive live game that is driven by a near future storyline in which deepfakes and forgeries are so difficult to detect that bad actors and foreign governments are fully engaged in a war over people's minds. At the same time, the world is sitting on the brink of the so-called "singularity," as AI advancements have completely blurred the line between artificial and natural cognition, and the Turing test has been rendered decisively moot.

Teams will join the game and follow the storyline to clues that will give them hints about who they can trust and who they can't. The clues will follow the pattern of deepfakes and forgeries, asking players to figure out what's real and what's not, focusing on hacker and DEF CON focus areas such as authentication, trust, social engineering, hardware and software manipulation and more. They will be given a rich story that will lead them to research the underlying issues in trust and anonymous trust systems. They will also encounter challenges and tutorials on video and image validation and cryptographically safe messaging.

RED ALERT ICS CTF

Level 1 - Hall 4 - Aisle 03-07
In-Person Contest
Friday and Saturday: 10:00-17:00; Sunday: 10:00-12:00

Red Alert ICS CTF is a competition for Hackers by Hackers, organized by the RedAlert Lab of NSHC Security. The event exclusively focuses on having the participants clear a series of challenges and break through several layers of security in our OT environment and eventually take over complete control of the ICS components.

Red Alert ICS CTF is back with a ton of fun challenges after successfully running the CTF since DEF CON 26. Red Alert ICS CTF is proud to be among the Black Badge contests at DEF CON 31 and DEF CON 26.

The contest would house real world ICS (Industrial Control System) equipment from various vendors on 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 at DEF CON 32 would also be offering players the unique opportunity to compromise the latest cyber ranges on Maritime Cyber Security.

@icsctf

RED TEAM VILLAGE CTF

Level 1 - Hall 4 - Aisle 01-05-C
In-Person Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-13:00

The Red Team Capture the Flag (CTF) competition is back at DEF CON! It is a challenging and exciting event that tests the skills of participants in offensive security.

The Red Team CTF is designed to simulate real-world challenges in which attackers are put to the test. Participants are expected to use a wide range of hacking techniques, tools, and skills to identify and exploit vulnerabilities.

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 and solve challenges.

The Red Team CTF at DEF CON 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.

RESILIENCE CONTESTS

Level 1 - Hall 4 - Aisle 02-02-D
In-Person Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-13:00

SEC VISHING COMPETITION

Level 3 - Room W317-W319
In-Person Contest
Friday: 08:30 - 18:00

In this competition (#SECVC), 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!

This competition takes place only 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 and JC as they cover the behind the scenes of creating the SECVC, this year's lessons learned, team highlights, and tips for future competitors!

Judges: Ibetika, John Hammond, Snow

Coaches: Jason, JC, Jennifer

SOCIAL ENGINEERING COMMUNITY (SEC) YOUTH CHALLENGE

Level 3 - Room W317-W319
In-Person Contest
Friday: 09:00-18:00;
Saturday: 10:00-18:00

The Social Engineering Community needs your help and it's not exactly a big deal, but without your help, the entire universe is going to implode. Fortunately, some creative beings designed a failsafe just for this specific purpose, the Def Con Social Engineering Youth Challenge at DEF CON 32! Remember, DON'T PANIC!

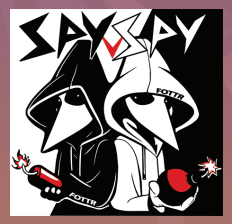
The implosion failsafe requires anyone under the age of 18 to complete some very specific problem-solving challenges that have been carefully designed for humans only (we don't know why these challenges were designed only for humans, but it's reasonable to assume this is another instance of dolphins playing a prank). Some examples of challenges are decoding alien messages, hacking intergalactic systems, and understanding the meaning of life. As you complete these challenges, the universe will be one step further from complete and utter obliteration.

As part of this protocol, you can expect the opportunity to learn valuable skills in cryptography, social engineering, network security, defusing intergalactic implosion bombs, and more. You'll need to keep your eyes on the sky and adapt to overcome serious obstacles designed by what we believe to be the least serious beings in the universe.

Will you be able to stop the universe from imploding into what we're assuming is probably another universe but much smaller? We hope so! Otherwise, even the dolphins will have to find a new home.

https://www.se.community/youth-challenge/

SPYVSPY



Level 1 - Hall 4 - Aisle 02-02-G
In-Person Contest
Friday and Saturday: 10:00-18:00

Embark on a thrilling espionage adventure with spyVspy! This contest imagines a world of spy games where contestants employ basic hacking, cryptography, and rogue skills to solve puzzles and uncover hidden caches strategically scattered throughout DEF CON (and beyond).

Contestants will engage in a real-world treasure hunt, where the locations of hidden caches are revealed by solving the types of puzzles you'd expect to see at DEF CON. Traditional ciphers, lockpicking, OSINT, and very basic hacking/pentesting skills may be required.

CONTESTS

spyVspy is intended for players of all skill levels. Whether you're a seasoned double-agent or just learning to be a covert operative, you will be able to compete and have fun in this event. Whatever skills you think you're missing can probably be learned on-the-job anyway.

https://www.fottr.io

TELECHALLENGE

Level 1 - Hall 4 - Aisle 02-02-B
Hybrid Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-13:00

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!

https://www.telechallenge.org

TINFOIL HAT CONTEST

Level 1 - Hall 4 - Aisle 01-04-D
In-Person Contest
Friday and Saturday: 10:00-17:00

Want to protect your noggin from Taylor Swift's PsyOps plot for global domination? Have you angered our new AI Overlords, and now need to hide? Or do those alien mind control rays just have you feeling 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 cerebellum . 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 for "Style". We provide all contestants a meter of foil, but you're welcome to acquire and use as much as you want from other sources.

http://www.psychoholics.org/tfh
@DC_Tin_Foil_Hat

VENATOR AURUM - A TREASURE HUNT

Other / See Description
In-Person Contest
Friday and Saturday: 10:00-18:00; Sunday: 10:00-13:00

Travel the seven seas to the seven wonders across time to test your skills across both old and new worlds. Every journey's end yields its own reward, but there is only one who can claim to be the first to the summit. Bring your entire tech arsenal or just a phone. Start at the broken compass and push forward into the known to seek the unknown. Wonders, plunder, and glory to those who test the waters and themselves.

https://venatoraurum.org

WHOSE SLIDE IS IT ANYWAY?

Level 1 - Hall 1 - Aisle 11-01:02 (Tracks 1-2)
In-Person Contest
Friday: 18:30-19:30

If someone had told us this silly contest would be in its 8th year there's no way we would have believed it. Even when we thought "hey, the gag is getting old, maybe it's time to hang it up" that turned out to be the year we'd gotten the most accolades from con goers during and after the contest. That was enough to recharge us and decide we'll do this until DC no longer exists. Proud isn't a grand enough word to describe how we feel to still be here and still making people laugh/feel better about themselves not being as stupid as us.

But to answer Why Us? WSIIA has always been about community. Whether you killed your deck or went down in a spectacular blaze of flames, this game is nothing without the people who play it and the audience who watches it. And if we're not doing it for the community, why the fuck are we even here? We'll remain here as long as you'll have us, riding on a wing, a prayer, and airplane bottles of Malort all the way to Year 10. Now on to the boilerplate pitch:

We're 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.

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.

@WhoseSlide

POLICY @ DEF CON

RM 237

FRIDAY AUG. 9

10:00 Harley Geiger, Peter Stephens, Adam Dobell -US and Internation Public Policy 101

12:00 Surprise Session - Check Hacker Tracker For More Info

13:00 Nasreen Djouini - The Value of Trust in the Open-source Software Ecosystem

14:00 Nicole Tisdale - Advocating for an Inclusive Cyber-Civil Rights Policy Agenda for Vulnerable Communities

15:00 Will Loomis - NSM-22 and the National Risk Management Plan: CISA Wants to Hear from You on How to Protect Our Nation's Critical Infrastructure

17:00 Surprise Session - Check Hacker Tracker For More Info

18:30 EVENING SOCIAL MIXER

SATURDAY AUG. 10

10:00 Michaela Lee - When the Lights Go Out: Building Resilient Access to Communications

11:00 Anjuli Shere- How can hackers support efforts to secure AI systems?

13:00 Randy Pestana - Global Perspectives in Cybersecurity: Challenging Norms and Expanding Horizons

14:00 Panel - What's next for the commercial CNE marketplace? A chance for you to influence the policy that will impact the future.

16:00 Surprise Session - Check Hacker Tracker For More Info

18:30 EVENING SOCIAL MIXER

SUNDAY AUG. 11

11:00 HACKER POLICY TRIVIA

CREATOR STAGE 4 TALKS

Friday 14:30 Jan Trzaskowski - Human Dignity in AI and Tech Policy

Friday 15:15 Rebecca Lively, Eddie Zaneski - Open Source Hacker Vs. Government Lawyer: Clashing Views on Fixing Tech in the DoD

Friday 16:00 Avi McGrady - Cybersecurity Schoolhouse Rock

Saturday 12:30 Emma Stewart - Pick Your Poison: Navigating a secure clean energy transition

Saturday 13:15 Harriet Farlow - Hacker vs AI: perspectives from an ex-spy

Sunday 10:30 Panel - Flying Blind: Navigating the Turbulent Skies of Aviation Cybersecurity Regulation

TALKS

Talks are listed by day/time/track. For full abstracts and bios of all the talks and their speakers, check out the Hacker Tracker app or find them on defcon.org at https://defcon.org/html/defcon-32/dc-32-speakers.html

FRIDAY

Jeff "The Dark Tangent" Moss

WELCOME TO DEF CON

Friday at 10:00 in Track 1 (Hall 1 - Aisle 11-01)
20 minutes

Erwin Karincic, Woody

MOBILE MESH RF NETWORK EXPLOITATION: GETTING THE TEA FROM GOTENNA

Friday at 10:00 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Tool, Demo, Exploit

Matt Burch

WHERE'S THE MONEY: DEFEATING ATM DISK ENCRYPTION

Friday at 10:00 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Exploit

Jacob Shams

SECURING CCTV CAMERAS AGAINST BLIND SPOTS

Friday at 10:00 in Track 4 (Hall 1 - Aisle 11-04)
20 minutes

Jon DiMaggio

BEHIND ENEMY LINES: GOING UNDERCOVER TO BREACH THE LOCKBIT RANSOMWARE OPERATION

Friday at 10:00 in Warstories Track (W322-W327)
45 minutes

General Paul M. Nakasone

SPIES AND BYTES: VICTORY IN THE DIGITAL AGE

Friday at 10:30 in Track 1 (Hall 1 - Aisle 11-01)
45 minutes

WangJunJie Zhang, YiSheng He

DEFEATING MAGIC BY MAGIC: USING ALPC SECURITY FEATURES TO COMPROMISE RPC SERVICES

Friday at 10:30 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes

Dennis Giese, Braelynn

OPEN SESAME - OR HOW VULNERABLE IS YOUR STUFF IN ELECTRONIC LOCKERS

Friday at 11:00 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo, Tool

Max 'Libra' Kersten

NO SYMBOLS WHEN REVERSING? NO PROBLEM: BRING YOUR OWN

Friday at 11:00 in Track 3 (Hall 1 - Aisle 11-03)
20 minutes | Tool

Thomas Roccia

THE XZ BACKDOOR STORY: THE UNDERCOVER OPERATION THAT SET THE INTERNET ON FIRE

Friday at 11:00 in Warstories Track (W322-W327)
45 minutes | Demo

Alexander Rubin, Martin Rakhmanov

ATOMIC HONEYPOT: A MYSQL HONEYPOT THAT DROPS SHELLS

Friday at 11:30 in Track 1 (Hall 1 - Aisle 11-01)
30 minutes | Demo, Exploit, Tool

James Kettle

LISTEN TO THE WHISPERS: WEB TIMING ATTACKS THAT ACTUALLY WORK

Friday at 11:30 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Tool, Demo, Exploit

Babak Javadi, Aaron Levy, Nick Draffen

HIGH INTENSITY DECONSTRUCTION: CHRONICLES OF A CRYPTOGRAPHIC HEIST

Friday at 11:30 in Track 4 (Hall 1 - Aisle 11-04)
75 minutes | Demo, Exploit

Anne Neuberger

FIRESIDE CHAT WITH DNSA ANNE NEUBERGER

Friday at 12:00 in Track 1 (Hall 1 - Aisle 11-01)
45 minutes

Harriet Farlow

ON YOUR OCEAN'S 11 TEAM, I'M THE AI GUY (TECHNICALLY GIRL)

Friday at 12:00 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo

The_Gibson

VEILID DEV AND COMMUNITY MEETUP

Friday at 12:00 in Warstories Track (W322-W327)
75 minutes

Nick Frichette

KICKING IN THE DOOR TO THE CLOUD: EXPLOITING CLOUD PROVIDER VULNERABILITIES FOR INITIAL ACCESS

Friday at 12:30 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes

Dr. Stefanie Tompkins, Dr. Renee Wegrzyn, Peiter "Mudge" Zatko

IF EXISTING CYBER VULNERABILITIES MAGICALLY DISAPPEARED OVERNIGHT, WHAT WOULD BE NEXT?

Friday at 13:00 in Track 1 (Hall 1 - Aisle 11-01)
45 minutes

HD Moore, Rob King

SSHAMBLE: UNEXPECTED EXPOSURES IN THE SECURE SHELL

Friday at 13:00 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo, Exploit, Tool

Andrew Case, Austin Sellers, Golden Richard, David McDonald, Gustavo Moreira

DEFEATING EDR EVADING MALWARE WITH MEMORY FORENSICS

Friday at 13:00 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Demo, Tool

Bill Woodcock

DIGITAL EMBLEMS: WHEN MARKINGS ARE REQUIRED UNDER INTERNATIONAL LAW, BUT YOU DON'T HAVE A RATTLE-CAN HANDY

Friday at 13:30 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes

Ken Gannon, Ilyes Beghdadi

XIAOMI THE MONEY - OUR TORONTO PWN2OWN EXPLOIT AND BEHIND THE SCENES STORY

Friday at 13:30 in Warstories Track (W322-W327)
45 minutes | Exploit

Jen Easterly

FIRESIDE CHAT AND AMA WITH THE DARK TANGENT AND JEN EASTERLY

Friday at 14:00 in Track 1 (Hall 1 - Aisle 11-01)
45 minutes

samy kamkar

OPTICAL ESPIONAGE: USING LASERS TO HEAR KEYSTROKES THROUGH GLASS WINDOWS

Friday at 14:00 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo, Exploit, Tool

Xiling Gong, Jon Bottarini, Eugene Rodionov, Xuan Xing

THE WAY TO ANDROID ROOT: EXPLOITING YOUR GPU ON SMARTPHONE

Friday at 14:00 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Demo, Exploit

Yakir Kadkoda, Michael Katchinskiy, Ofek Itach

BREACHING AWS ACCOUNTS THROUGH SHADOW RESOURCES

Friday at 14:30 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Demo, Exploit, Tool

Joe Grand, Bruno Krauss

JOE AND BRUNO'S GUIDE TO HACKING TIME: REGENERATING PASSWORDS FROM ROBOFORM'S PASSWORD GENERATOR

Friday at 14:30 in Warstories Track (W322-W327)
45 minutes | Demo, Exploit, Tool

DC101 PANEL

Friday at 15:00 in Track 1 (Hall 1 - Aisle 11-01)
60 minutes

Ceri Coburn, Dirk-jan Mollema

ABUSING WINDOWS HELLO WITHOUT A SEVERED HAND

Friday at 15:00 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo, Tool

Ryan Johnson

ANDROID APP USAGE AND CELL TOWER LOCATION: PRIVATE. SENSITIVE. AVAILABLE TO ANYONE?

Friday at 15:00 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Demo, Exploit

Aaron Grattafiori, Ivan Evtimov, Joanna Bitton, Maya Pavlova

TAMING THE BEAST: INSIDE THE LLAMA 3 RED TEAM PROCESS

Friday at 15:30 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes

Jayson E. Street

SOCIAL ENGINEERING LIKE YOU'RE PICARD

Friday at 15:30 in Warstories Track (W322-W327)
45 minutes | Demo

Mar Williams

MAKING THE DEF CON 32 BADGE

Friday at 16:00 in Track 1 (Hall 1 - Aisle 11-01)
60 minutes

Paul Gerste

SQL INJECTION ISN'T DEAD: SMUGGLING QUERIES AT THE PROTOCOL LEVEL

Friday at 16:00 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo, Exploit

Michael Gorelik , Arnold Osipov

OUTLOOK UNLEASHING RCE CHAOS: CVE-2024-30103 & CVE-2024-38021

Friday at 16:00 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Demo, Exploit, Tool

Aapo Oksman

LEVERAGING PRIVATE APNS FOR MOBILE NETWORK TRAFFIC ANALYSIS

Friday at 16:30 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Demo

Thomas Boejstrup Johansen

WHY ARE YOU STILL, USING MY SERVER FOR YOUR INTERNET ACCESS.

Friday at 16:30 in Warstories Track (W322-W327)
45 minutes

Paul Roberts, Chris Wysopal, Cory Doctorow, Tarah Wheeler, Dennis Giese

BRICKED & ABANDONED: HOW TO KEEP THE IOT FROM BECOMING AN INTERNET OF TRASH

Friday at 17:00 in Track 1 (Hall 1 - Aisle 11-01)
45 minutes

Damien Cauquil, Romain Cayre

ONE FOR ALL AND ALL FOR WHAD: WIRELESS SHENANIGANS MADE EASY !

Friday at 17:00 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo, Tool

Vivek Ramachandran, Jeswin Mathai

BREAKING SECURE WEB GATEWAYS (SWG) FOR FUN AND PROFIT

Friday at 17:00 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Demo, Exploit, Tool

Vladyslav Zubkov

EXPLOITING BLUETOOTH - FROM YOUR CAR TO THE BANK ACCOUNT$$

Friday at 17:30 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Exploit, Tool

Tony Sager

STRANGER IN A CHANGED LAND

Friday at 17:30 in Warstories Track (W322-W327)
20 minutes

SATURDAY

THE PWNIE AWARDS

Saturday at 10:00 in Track 1 (Hall 1 - Aisle 11-01)
45 minutes

Michael Orlitzky

LAUNDERING MONEY

Saturday at 10:00 in Track 2 (Hall 1 - Aisle 11-02)
20 minutes

Xavier Zhang

MUTUAL AUTHENTICATION IS OPTIONAL

Saturday at 10:00 in Track 3 (Hall 1 - Aisle 11-03)
20 minutes | Demo

Wesley McGrew

REVERSE ENGINEERING MICROPYTHON FROZEN MODULES: DATA STRUCTURES, RECONSTRUCTION, AND READING BYTECODE

Saturday at 10:00 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Demo, Tool

Deth Veggie, Walter J. Scheirer, Patrick "Lord Digital" Kroupa, John Threat, Emmanuel Goldstein, X, TommydCat

CULT OF THE DEAD COW & FRIENDS PRESENT: PRIME CUTS FROM HACKER HISTORY - 40 YEARS OF 31337

Saturday at 10:00 in Warstories Track (W322-W327)
105 minutes

Martin Doyhenard

GOTTA CACHE 'EM ALL: BENDING THE RULES OF WEB CACHE EXPLOITATION

Saturday at 10:30 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo, Exploit, Tool

S1nn3r

SMISHING SMACKDOWN: UNRAVELING THE THREADS OF USPS SMISHING AND FIGHTING BACK

Saturday at 10:30 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes

Stephen Sims

THE RISE AND FALL OF BINARY EXPLOITATION

Saturday at 11:00 in Track 1 (Hall 1 - Aisle 11-01)
45 minutes

Ron Ben-Yizhak, David Shandalov

SHIM ME WHAT YOU GOT - MANIPULATING SHIM AND OFFICE FOR CODE INJECTION

Saturday at 11:00 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Demo, Tool

Or Yair, Shmuel Cohen

QUICKSHELL: SHARING IS CARING ABOUT AN RCE ATTACK CHAIN ON QUICK SHARE

Saturday at 11:30 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo, Exploit, Tool

Michael Torres

SUDOS AND SUDON'TS - PEERING INSIDE SUDO FOR WINDOWS

Saturday at 11:30 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Exploit

Cory Doctorow

DISENSHITTIFY OR DIE! HOW HACKERS CAN SEIZE THE MEANS OF COMPUTATION AND BUILD A NEW, GOOD INTERNET THAT IS HARDENED AGAINST OUR ASSHOLE BOSSES' INSATIABLE HORNINESS FOR ENSHITTIFICATION.

Saturday at 12:00 in Track 1 (Hall 1 - Aisle 11-01)
45 minutes

Adnan Khan, John Stawinski

GRAND THEFT ACTIONS: ABUSING SELF-HOSTED GITHUB RUNNERS AT SCALE

Saturday at 12:00 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Demo, Tool

Tom Cross, Greg Conti

DECEPTION & COUNTER DECEPTION – DEFENDING YOURSELF IN A WORLD FULL OF LIES

Saturday at 12:00 in Warstories Track (W322-W327)
45 minutes

Enrique Nissim, Krzysztof Okupski

AMD SINKCLOSE: UNIVERSAL RING -2 PRIVILEGE ESCALATION

Saturday at 12:30 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Demo, Exploit, Tool

Matthew Bryant

THE SECRET LIFE OF A ROGUE DEVICE - LOST IT ASSETS ON THE PUBLIC MARKETPLACE

Saturday at 12:30 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes

Harry Coker, Jr.

FIRESIDE CHAT WITH NATIONAL CYBER DIRECTOR HARRY COKER, JR.

Saturday at 13:00 in Track 1 (Hall 1 - Aisle 11-01)
45 minutes

Aviad Hahami

OH-MY-DC: ABUSING OIDC ALL THE WAY TO YOUR CLOUD

Saturday at 13:00 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Demo, Tool

Joseph Cox

INSIDE THE FBI'S SECRET ENCRYPTED PHONE COMPANY 'ANOM'

Saturday at 13:00 in Warstories Track (W322-W327)
45 minutes

Jim Rush, Tomais Williamson

NTLM - THE LAST RIDE

Saturday at 13:30 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Exploit

Vangelis Stykas

BEHIND ENEMY LINES: ENGAGING AND DISRUPTING RANSOMWARE WEB PANELS

Saturday at 13:30 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Exploit

Mixæl Swan Laufer

ERADICATING HEPATITIS C WITH BIOTERRORISM

Saturday at 14:00 in Track 1 (Hall 1 - Aisle 11-01)
45 minutes | Demo, Tool

Jeffrey Hofmann, Colby Morgan

DISCOVERING AND EXPLOITING LOCAL ATTACKS AGAINST THE 1PASSWORD MACOS DESKTOP APPLICATION

Saturday at 14:00 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Demo, Exploit, Tool

Sam Curry

HACKING MILLIONS OF MODEMS (AND INVESTIGATING WHO HACKED MY MODEM)

Saturday at 14:00 in Warstories Track (W322-W327)
45 minutes | Demo

Allan Cecil

TROLL TRAPPING THROUGH TAS TOOLS - EXPOSING SPEEDRUNNING CHEATERS

Saturday at 14:30 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo, Tool

stacksmashing

ACE UP THE SLEEVE: FROM GETTING JTAG ON THE IPHONE 15 TO HACKING INTO APPLE'S NEW USB-C CONTROLLER

Saturday at 14:30 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Demo, Tool

Mikhail Shcherbakov

EXPLOITING THE UNEXPLOITABLE: INSIGHTS FROM THE KIBANA BUG BOUNTY

Saturday at 15:00 in Track 1 (Hall 1 - Aisle 11-01)
45 minutes | Demo, Tool

Silvia Puglisi, Roger Dingledine

MEASURING THE TOR NETWORK

Saturday at 15:00 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Tool

Daniel Messer

A SHADOW LIBRARIAN IN BROAD DAYLIGHT: FIGHTING BACK AGAINST EVER ENCROACHING CAPITALISM

Saturday at 15:00 in Warstories Track (W322-W327)
45 minutes

Helvio Carvalho Junior

HOOKCHAIN: A NEW PERSPECTIVE FOR BYPASSING EDR SOLUTIONS

Saturday at 15:30 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo, Exploit, Tool

Lennert Wouters, Ian Carroll

UNSAFLOK: HACKING MILLIONS OF HOTEL LOCKS

Saturday at 15:30 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Demo, Exploit

Jake Jepson, Rik Chatterjee

COMPROMISING AN ELECTRONIC LOGGING DEVICE AND CREATING A TRUCK2TRUCK WORM

Saturday at 16:00 in Track 1 (Hall 1 - Aisle 11-01)
20 minutes | Demo, Exploit

Bill Demirkapi

SECRETS AND SHADOWS: LEVERAGING BIG DATA FOR VULNERABILITY DISCOVERY AT SCALE

Saturday at 16:00 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Demo

Elonka Dunin, Klaus Schmeh

ENCRYPTED NEWSPAPER ADS IN THE 19TH CENTURY - THE WORLD'S FIRST WORLDWIDE SECURE COMMUNICATION SYSTEM

Saturday at 16:00 in Warstories Track (W322-W327)
45 minutes

Chanin Kim, Myounghun Pak

WATCHERS BEING WATCHED: EXPLOITING THE SURVEILLANCE SYSTEM AND ITS SUPPLY CHAIN

Saturday at 16:30 in Track 1 (Hall 1 - Aisle 11-01)
45 minutes | Demo, Exploit

Yan Shoshitaishvili, Perri Adams

DEF CON ACADEMY: CULTIVATING M4D SK1LLZ IN THE DEF CON COMMUNITY

Saturday at 16:30 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo

Vincent Lenders, Johannes Willbold, Robin Bisping

BREAKING THE BEAM: EXPLOITING VSAT SATELLITE MODEMS FROM THE EARTH'S SURFACE

Saturday at 16:30 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Demo, Exploit

Bramwell Brizendine, Shiva Shashank Kusuma

TECHNIQUES FOR CREATING PROCESS INJECTION ATTACKS WITH ADVANCED RETURN-ORIENTED PROGRAMMING

Saturday at 17:00 in Track 4 (Hall 1 - Aisle 11-04)
20 minutes | Demo

Pete Stegemeyer

A TREASURE TROVE OF FAILURES: WHAT HISTORY'S GREATEST HEIST CAN TEACH US ABOUT DEFENSE IN DEPTH

Saturday at 17:00 in Warstories Track (W322-W327)
45 minutes

Charles Fol

ICONV, SET THE CHARSET TO RCE: EXPLOITING THE GLIBC TO HACK THE PHP ENGINE

Saturday at 17:30 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo, Exploit

Michal Grygarek, Martin Petran, Hayyan Ali

NANO-ENIGMA: UNCOVERING THE SECRETS WITHIN EFUSE MEMORIES

Saturday at 17:30 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Demo

SUNDAY

Gareth Heyes

SPLITTING THE EMAIL ATOM: EXPLOITING PARSERS TO BYPASS ACCESS CONTROLS

Sunday at 10:00 in Track 1 (Hall 1 - Aisle 11-01)
45 minutes | Demo, Exploit, Tool

Eduard Agavriloae, Matei Josephs

AWS CLOUDQUARRY: DIGGING FOR SECRETS IN PUBLIC AMIS

Sunday at 10:00 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo, Tool

Alon Leviev

WINDOWS DOWNDATE: DOWNGRADE ATTACKS USING WINDOWS UPDATES

Sunday at 10:00 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Demo, Exploit, Tool

Moritz Abrell

UNLOCKING THE GATES: HACKING A SECURE INDUSTRIAL REMOTE ACCESS SOLUTION

Sunday at 10:00 in Track 4 (Hall 1 - Aisle 11-04)
20 minutes | Demo, Exploit

Jeffrey Knockel, Mona Wang

THE NOT-SO-SILENT TYPE: BREAKING NETWORK CRYPTO IN ALMOST EVERY POPULAR CHINESE KEYBOARD APP

Sunday at 10:00 in Warstories Track (W322-W327)
45 minutes | Demo

Rob Joyce

CHANGING GLOBAL THREAT LANDSCAPE WITH ROB JOYCE AND DARK TANGENT

Sunday at 10:30 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes

Daniel Bohannon, Sabajete Elezaj

(|(MALDAPTIVE:¯_(LDAP)_/¯=OBFUSC8T10N) (DE-OBFUSCATION &:=DE*TE)(!C=TION))

Sunday at 11:00 in Track 1 (Hall 1 - Aisle 11-01)
45 minutes | Demo, Tool

Thomas Sermpinis

THE HACK, THE CRASH AND TWO SMOKING BARRELS. (AND ALL THE TIMES I (ALMOST) KILLED AN ENGINEER.)

Sunday at 11:00 in Track 2 (Hall 1 - Aisle 11-02)
45 minutes | Demo, Exploit, Tool

JiaQing Huang, Hao Zheng, Yue Liu

DRAGON SLAYINGGUIDE: BUG HUNTING IN VMWARE DEVICE VIRTUALIZATION

Sunday at 11:00 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes

TALKS

atlas

AUTOMOBILES, ALCOHOL, BLOOD, SWEAT, AND CREATIVE REVERSING OF AN OBFUSCATED CAR-MODDING TOOL

Sunday at 11:00 in Warstories Track (W322-W327)
45 minutes | Demo, Tool

Riley Hassell

MODEM OPERANDI, OR: HOW I OWNED HUNDREDS OF MILLIONS OF BROADBAND BASEBANDS

Sunday at 11:30 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Demo, Exploit, Tool

Alessandro Magnosi

DRIVERJACK: TURNING NTFS AND EMULATED READ-ONLY FILESYSTEMS IN AN INFECTION AND PERSISTENCE VECTOR

Sunday at 12:00 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Exploit, Tool

Anthony Kava

SOLVING THE "LOVER, STALKER, KILLER" MURDER WITH STRINGS, GREP, AND PERL

Sunday at 12:00 in Warstories Track (W322-W327)
20 minutes | Demo

Andrew Carney, Perri Adams

AIXCC CLOSING CEREMONIES

Sunday at 12:30 in Hall 1 - Aisle 11-01:02 (Tracks 1-2)
45 minutes

Timm Lauser, Jannis Hamborg

REDEFINING V2G - HOW TO USE YOUR VEHICLE AS A GAME CONTROLLER

Sunday at 12:30 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes | Demo, Tool

HexRabbit Chen

CLASH, BURN, AND EXPLOIT: MANIPULATE FILTERS TO PWN KERNELCTF

Sunday at 12:30 in Warstories Track (W322-W327)
45 minutes | Demo, Exploit

Yisroel Mirsky

YOUR AI ASSISTANT HAS A BIG MOUTH: A NEW SIDE-CHANNEL ATTACK

Sunday at 13:00 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Demo, Exploit, Tool

CONTEST CLOSING CEREMONIES AND AWARDS

Sunday at 13:30 in Hall 1 - Aisle 11-01:02 (Tracks 1-2)
75 minutes

Suha Sabi Hussain

INCUBATED MACHINE LEARNING EXPLOITS: BACKDOORING ML PIPELINES USING INPUT-HANDLING BUGS

Sunday at 13:30 in Track 4 (Hall 1 - Aisle 11-04)
45 minutes

Alejandro Caceres

BRINGING DOWN NORTH KOREA

Sunday at 13:30 in Warstories Track (W322-W327)
45 minutes | Demo

David Meléndez, Gabriela (Gabs) Garcia

ABUSING LEGACY RAILROAD SIGNALING SYSTEMS

Sunday at 14:00 in Track 3 (Hall 1 - Aisle 11-03)
45 minutes | Demo

DEF CON CLOSING CEREMONIES & AWARDS

Sunday at 15:00 in Hall 1 - Aisle 11-01:02 (Tracks 1-2)
165 minutes

CONNECT

STUFF WE OPERATE

WEBSITE: HTTPS://DEFCON.ORG (.ONION SITE AVAILABLE)
DEF CON MEDIA: HTTPS://MEDIA.DEFCON.ORG (.ONION SITE AVAILABLE)
DEF CON GROUPS: HTTPS://DEFCONGROUPS.ORG (.ONION SITE AVAILABLE)
DEF CON FORUMS: HTTPS://FORUM.DEFCON.ORG (.ONION SITE AVAILABLE)
DEF CON INFO: HTTPS://INFO.DEFCON.ORG (.ONION SITE AVAILABLE)
DC NEXTGEN: HTTPS://DCNEXTGEN.ORG (.ONION SITE AVAILABLE)
DEFCON.SOCIAL (MASTODON): HTTPS://DEFCON.SOCIAL (.ONION SITE AVAILABLE)

STUFF WE HOST

DISCORD: HTTPS://DISCORD.GG/DEFCON
YOU TUBE: HTTPS://WWW.YOUTUBE.COM/USER/DEFCONCONFERENCE
TWITTER: HTTPS://TWITTER.COM/DEFCON
FACEBOOK: HTTPS://FACEBOOK.COM/DEFCON/ (.ONION SITE AVAILABLE)
INSTAGRAM: HTTPS://WWW.INSTAGRAM.COM/WEAREDEFCON/
REDDIT: HTTPS://WWW.REDDIT.COM/R/DEFCON (.ONION SITE AVAILABLE)
LINKEDIN: HTTPS://WWW.LINKEDIN.COM/COMPANY/DEF-CON

BUY STUFF

DEF CON STORE: HTTPS://SHOP.DEFCON.ORG
DEF CON TRAINING: HTTPS://TRAINING.DEFCON.ORG/

OTHER STUFF

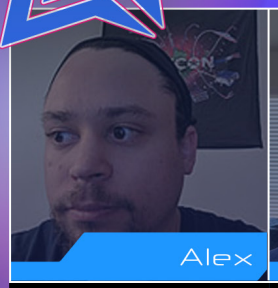
SOMAFM MUSIC CHANNEL: HTTPS://SOMAFM.COM/DEFCON/
DEF CON MUSIC: HTTPS://DEFCONMUSIC.ORG/
DEF CON NOC: HTTPS://NOC.DEFCON.ORG

DOWNLOAD THE PRESENTATION MATERIALS AND MORE FROM THE DEF CON MEDIA SERVER AT:

HTTPS://MEDIA.DEFCON.ORG/DEF CON 32/

DEF CON 32 CFP REVIEW BOARD

This is the l337 crew that makes sure DEF CON has the highest quality technical content. Every time you learn something amazing from a DEF CON talk, they deserve a lot of the credit. Or blame. We don't know your life.



Alex

BIO Jack of Few Trades, Master of None

AKA None yet. Working on it.

AlxRogan

BIO Alx does things he probably shouldn't. Ask him about capacitors, hacker jeopardy, or brawndo.

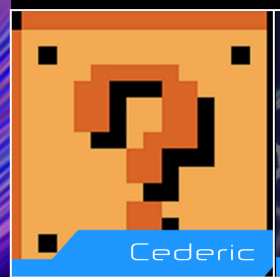
AKA AY-AY-RON

Ash

BIO Resurrenctionist of electromechanical detritus.

Carnal Ownage

BIO It's on LinkedIn if you actually care.



Cederic

BIO I press F5 for a living

AKA Ling

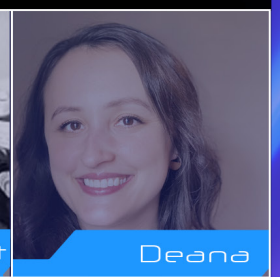
Clavinger

BIO Has consistently forgotten to submit a bio for the Review Board.

AKA FishSupreme

dead addict

BIO Isn't a good enough human being to be self-deprecating in his bio.



Deana

BIO Green witch, cold lizard person,enjoys overthrowing the male industrial complex in her spare time.

Dino

BIO Proud South African hacker, Founder of Telspace Systems and paying it forward one day at a time

Effffn

BIO DEF CON NOC lead, drunk panda herding, beer geeking and running.

Elizabeth

BIO Team oxford comma, champagne champion, and aviation geek.Building better tech policy & businesses, not the kind of lawyer that you call for bail money.

Jay Healey

BIO Says cyber waaaaay too much.

Jeff Moss

BIO Founder, DEF CON.

AKA The Dark Tangent

John Fulmer

BIO Takes it more than one day at a time as he's sure he'll live forever;
Living proof alcohol is a preservative.

Jon2

BIO Processing....

Magen

BIO Incurable travel addict and unapologetic coffee maven. Works hard so her plants can live their best lives.

Malware Unicorn

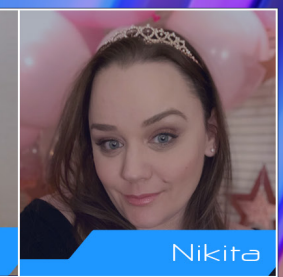
BIO Likes reversing and developing malware. Blue team to red team convert. Pursues making free content for the community.

Marcia Hoffman

BIO Doing my best to make the Internet better and keep people out of trouble.

Medic

BIO Tries to keep his head low. Takes things apart and can sometimes put them back together.



Nikita

BIO Director of Content & Coordination. Problem Solver. Chicken Soup repairwoman. SecurityTribe.

NOObz

BIO I am a terrible alibi.

PWCrack

BIO 400lb hacker with a 197 IQ and about 15% of your password.

Shaggy

BIO Master of Sleights.

Snow

BIO Your friendly neighborhood Con-Artist.

Solstice

BIO Wifi hacker. Red team guy. Random lulz generator.

Suggy

BIO Self-appointed DEF CON 4x5k run ambassador and expert party escape artist.

Zack Fasel

BIO Can be found drinking all the wines, hacking all the things, and generally being extra.

Zoz

BIO International Man of Mystery.

The Hoff, Dr. Weird

CREATOR STAGE TALKS

Professor Rachel Cummings on behalf of Crypto Privacy Village

DIFFERENTIAL PRIVACY BEYOND ALGORITHMS: CHALLENGES FOR SUCCESSFUL DEPLOYMENT

Friday at 10:00 in Creator Stage 1 (Hall 2 - Aisle 07-04)
60 minutes

Niyo Little Thunder Pearson on behalf of ICS Village

DOES THE WORLD NEED ANOTHER THREAT MODEL, THE ROAD TO EMB3D

Friday at 10:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes | Tool

Luke McLaren on behalf of XR Village

PWNING THROUGH THE METAVERSE - QUEST HEADSET VULNERABILITY RESEARCH

Friday at 10:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
60 minutes | Exploit

Roni "Lupin" Carta on behalf of Bug Bounty Village

PRACTICAL EXPLOITATION OF DOS IN BUG BOUNTY

Friday at 10:00 in Creator Stage 4 (W222)
60 minutes

Moritz Laurin Thomas on behalf of ICS Village

ATTACK AND DEFENCE IN OT - SIMULATING ATTACKS AGAINST HYDROELECTRIC POWER PLANTS LEVERAGING ICS FIRING RANGES

Friday at 10:30 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes | Demo

Grey Fox on behalf of Crypto Privacy Village

TRAVEL BETTER: EXPEDIENT DIGITAL DEFENSE

Friday at 11:00 in Creator Stage 1 (Hall 2 - Aisle 07-04)
30 minutes

Office of the National Cyber Director on behalf of Aerospace Village

ONCD PRESENTATION ON NEW SPACE CYBER FRAMEWORK

Friday at 11:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
60 minutes | Tool

Martin Pratt on behalf of XR Village

NATIONAL LABS USE OF XR

Friday at 11:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Demo

Daniel "Blaklis" Le Gall on behalf of Bug Bounty Village

FROM EASY WINS TO EPIC CHALLENGES: BOUNTY HUNTER EDITION

Friday at 11:00 in Creator Stage 4 (W222)
60 minutes

Joe "securelyfitz" FitzPatrick on behalf of HHV/SSV

CUSTOM CHEAP, EASY AND SAFE BADGES - WITHOUT STARTING FROM SCRATCH

Friday at 11:30 in Creator Stage 1 (Hall 2 - Aisle 07-04)
60 minutes | Demo

Vivek Ramachandran, Jeswin Mathai on behalf of Adversary Village

SNEAKY EXTENSIONS: THE MV3 ESCAPE ARTISTS

Friday at 11:30 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Demo

Jared Dygert on behalf of Lock Pick Village

SAFECRACKING FOR EVERYONE

Friday at 12:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
60 minutes

Gregory Carpenter, DrPH on behalf of Adversary Village

TOUGH ADVERSARY? DON'T BLAME SUN TZU

Friday at 12:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes

Catherine Ullman on behalf of Packet Hacking Village

THE CURIOUS CASE OF ALICE AND BOB: WHAT YOU CAN (AND CANNOT!) DO AS DIGITAL INVESTIGATORS

Friday at 12:00 in Creator Stage 4 (W222)
60 minutes

Andrew M, Ege Feyzioglu on behalf of Physical Security Village

RFID 101

Friday at 12:30 in Creator Stage 1 (Hall 2 - Aisle 07-04)
30 minutes | Demo

Cybelle Oliveira , Mauro Eldritch on behalf of Adversary Village

MFT: MALICIOUS FUNGIBLE TOKENS

Friday at 12:30 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Demo

Karen Ng, Sam Mayers on behalf of Physical Security Village

BYPASS 101

Friday at 13:00 in Creator Stage 1 (Hall 2 - Aisle 07-04)
60 minutes | Demo

Jamie Hardy, Rachael Tubbs, Steve McGregory, Ted Harrington on behalf of IOT Village

PREPARING FOR THE FUTURE: A DISCUSSION OF OUR RAPIDLY EVOLVING THREAT LANDSCAPE

Friday at 13:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes

Pavel Khunt, Thomas "Cr0wTom" Sermpinis on behalf of Car Hacking Village

V2GEVIL: GHOST IN THE WIRES

Friday at 13:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Tool

Geoff Horvath, Winson Tam on behalf of Packet Hacking Village

MOWIRELESS MOPROBLEMS: MODULAR WIRELESS SURVEY SYSTEMS AND THE DATA ANALYTICS THAT LOVE THEM

Friday at 13:00 in Creator Stage 4 (W222)
30 minutes | Tool

Dylan "The Magician" Baklor on behalf of Lock Pick Village

DOORS, CAMERAS, & MANTRAPS: OH MY!

Friday at 13:30 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes

Harry Krejsa on behalf of Car Hacking Village

BUILDING A SECURE AND RESILIENT NATIONWIDE EV CHARGING NETWORK: THE ROLE OF HACKERS IN THE CLEAN ENERGY REVOLUTION

Friday at 13:30 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes

Josh Pyorre on behalf of Packet Hacking Village

SIGNATURE-BASED DETECTION USING NETWORK TIMING

Friday at 13:30 in Creator Stage 4 (W222)
60 minutes | Tool

Billy Graydon on behalf of Physical Security Village

PHYSICAL SECURITY ASSESSMENT BASICS FOR INTERNAL EMPLOYEES

Friday at 14:00 in Creator Stage 1 (Hall 2 - Aisle 07-04)
30 minutes

Joe Slowik on behalf of ICS Village

THE RISK AND REWARD OF DISTRIBUTED INDUSTRIAL CONTROL

Friday at 14:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes

Jonghyuk Song, Seunghee Han, Soohwan Oh on behalf of Car Hacking Village

UDSONCAN ATTACKS: DISCOVERING SAFETY-CRITICAL RISKS BY FUZZING

Friday at 14:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Exploit

Carlota Bindner, Deral Heiland on behalf of IOT Village

EXPLORATION OF CELLULAR BASED IOT TECHNOLOGY

Friday at 14:30 in Creator Stage 1 (Hall 2 - Aisle 07-04)
60 minutes | Demo

Mars Cheng on behalf of ICS Village

MAPPING THE LANDSCAPE: TOP 10 CYBERSECURITY TRENDS IN CRITICAL INFRASTRUCTURE FOR 2024

Friday at 14:30 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes

CREATOR STAGE TALKS

Danilo Erazo on behalf of Car Hacking Village

HOW I DISCOVERED AND HACKED LEARNING CODES OF THE KEY JOB OF A CAR ASSEMBLED IN MY COUNTRY

Friday at 14:30 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Demo

Jan Trzaskowski on behalf of Policy Village

HUMAN DIGNITY IN AI AND TECH POLICY

Friday at 14:30 in Creator Stage 4 (W222)
45 minutes

Daniel Beard on behalf of BioHacking Village

BREAKING BOUNDARIES: POPPING SHELLS IN THE AIRGAP WITH $10 AND A DASH OF ARDUINO MAGIC

Friday at 15:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes | Tool

Martin "masorx" Strohmeier, Vladyslav "yso" "schwytz" Zubkov on behalf of Car Hacking Village

EXPLOITING BLUETOOTH - FROM YOUR CAR TO THE BANK ACCOUNT$$

Friday at 15:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Tool

Eddie Zaneski, Rebecca Lively on behalf of Policy Village

OPEN SOURCE HACKER VS. GOVERNMENT LAWYER: CLASHING VIEWS ON FIXING TECH IN THE DOD

Friday at 15:15 in Creator Stage 4 (W222)
45 minutes

Ricky "HeadlessZeke" Lawshae on behalf of IOT Village

I HACKED MY MAZDA WITH AN IPOD

Friday at 15:30 in Creator Stage 1 (Hall 2 - Aisle 07-04)
30 minutes | Demo

Michael "v3ga" Aguilar on behalf of BioHacking Village

DYSFUNCTIONAL UNITY: THE ROAD TO NOWHERE

Friday at 15:30 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes | Demo

Andrzej Olchawa on behalf of Aerospace Village

GROUND CONTROL TO MAJOR THREAT - HACKING THE SPACE LINK EXTENSION PROTOCOL

Friday at 15:30 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Demo

Matt Burch on behalf of IOT Village

WHERE'S THE MONEY: DEFEATING ATM DISK ENCRYPTION

Friday at 15:50 in Creator Stage 1 (Hall 2 - Aisle 07-04)
40 minutes | Exploit

Matt Domko on behalf of Crypto Privacy Village

DATA ON DEMAND: THE CHALLENGES OF BUILDING A PRIVACY FOCUSED AI DEVICE

Friday at 16:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
60 minutes

Martin "masorx" Strohmeier on behalf of Aerospace Village

ANALYZING THE SECURITY OF SATELLITE-BASED AIR TRAFFIC CONTROL

Friday at 16:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Exploit

Avi McGrady on behalf of Policy Village

CYBERSECURITY SCHOOLHOUSE ROCK

Friday at 16:00 in Creator Stage 4 (W222)
30 minutes

Dennis "c0ldbru" Pelton on behalf of Makers Community

SO YOU WANNA KNOW HOW TO MAKE BADGES

Friday at 16:30 in Creator Stage 1 (Hall 2 - Aisle 07-04)
60 minutes | Demo

Daniel Isler on behalf of Adversary Village

MASTER SPLINTER'S INITIAL PHYSICAL ACCESS DOJO: STORYTELLING OF A COMPLEX ADVERSARIAL

Friday at 16:30 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes

Bryson Bort , Tom VanNorman on behalf of ICS Village

ICS 101

Friday at 16:30 in Creator Stage 4 (W222)
30 minutes

Alexandru Lazar, Dan Berte on behalf of IOT Village

BEYOND SUNSET: EXPOSING THE OCCULTATIONS LURKING IN LARGE-SCALE OFF-GRID SOLAR SYSTEMS

Friday at 17:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes | Exploit

David "Icer" Maynor on behalf of XR Village

BE THE GHOST IN THE SHELL BARRIER MAZES FTW

Friday at 17:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
60 minutes | Exploit

Charlie Waterhouse, Nikhil "niks" Shrivastava on behalf of Bug Bounty Village

REFLECTIONS ON A DECADE IN BUG BOUNTIES: EXPERIENCES AND MAJOR TAKEAWAYS

Friday at 17:00 in Creator Stage 4 (W222)
60 minutes

Cecilie Wian, Per Thorsheim on behalf of Crypto Privacy Village

FOOL US ONCE, FOOL US TWICE... HACKING NORWEGIAN BANKS

Friday at 17:30 in Creator Stage 1 (Hall 2 - Aisle 07-04)
30 minutes

Brandon Lee, Hyo Jin Lee on behalf of IOT Village

INSIDE DASH CAM: CUSTOM PROTOCOLS AND DISCOVERED 0-DAYS

Friday at 17:30 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes | Exploit

Larry Pesce on behalf of IOT Village

SBOMS THE HARD WAY: HACKING BOB THE MINION

Saturday at 10:00 in Creator Stage 1 (Hall 2 - Aisle 07-04)
30 minutes | Demo

Fernando De La Peña Llaca on behalf of BioHacking Village

BRIDGING SPACE AND MEDICINE

Saturday at 10:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
60 minutes | Demo

Abhijith "Abx" B R, Adam "_whatshisface" Pennington, Daniel DeCloss , Keenan Skelly, Ken Kato on behalf of Adversary Village

FORMIDABLE ADVERSARIES: RESPONDING TO BREACHES, RANSOMWARE, AND STATE-SPONSORED THREAT ACTORS

Saturday at 10:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
60 minutes

Mike Raggo on behalf of Packet Hacking Village

USING AI COMPUTER VISION IN YOUR OSINT DATA ANALYSIS

Saturday at 10:00 in Creator Stage 4 (W222)
60 minutes | Demo

Joshua Herman on behalf of IOT Village

PSYCHIC PAPER: MAKING EINK ACCESS BADGES ACCESSIBLE FOR ANYONE

Saturday at 10:30 in Creator Stage 1 (Hall 2 - Aisle 07-04)
45 minutes

Mixæl Swan Laufer on behalf of BioHacking Village

ERADICATING HEPATITIS C WITH BIOTERRORISM

Saturday at 11:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
60 minutes | Tool

Melvin Langvik on behalf of Adversary Village

EVADING MODERN DEFENSES WHEN PHISHING WITH PIXELS

Saturday at 11:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Demo

Denis Smajlović on behalf of Packet Hacking Village

INTRODUCTION TO IPV6

Saturday at 11:00 in Creator Stage 4 (W222)
30 minutes | Demo

Eric Forte, Mark Mager on behalf of IOT Village

WHAT TO EXPECT WHEN YOU'RE EXPLOITING: ATTACKING AND DISCOVERING ZERO-DAYS IN BABY MONITORS AND WI-FI CAMERAS

Saturday at 11:15 in Creator Stage 1 (Hall 2 - Aisle 07-04)
45 minutes | Exploit

CREATOR STAGE TALKS

Dr. Muhsinah Morris on behalf of XR Village

STUDENT ENGAGEMENT DOESN'T HAVE TO SUCK

Saturday at 11:30 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Demo

Jeff Guerra, Jonathan Kuskos, Katie Trimble-Noble, Logan MacLaren, Sam (erbbysam) Erb on behalf of Bug Bounty Village

HUNTERS AND GATHERERS: A DEEP DIVE INTO THE WORLD OF BUG BOUNTIES

Saturday at 11:30 in Creator Stage 4 (W222)
60 minutes

Michael Brown on behalf of HHV/SSV

THE WILD AND WONDERFUL WORLD OF EARLY MICROPROCESSORS WITH A FOCUS ON THE 6502

Saturday at 12:00 in Creator Stage 1 (Hall 2 - Aisle 07-04)
60 minutes | Demo

Paul Brownridge on behalf of ICS Village

I AM STILL THE CAPTAIN NOW!

Saturday at 12:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes | Demo

Dylan Fox on behalf of XR Village

XR FOR ALL: ACCESSIBILITY AND PRIVACY FOR DISABLED USERS

Saturday at 12:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes

Tim Chase on behalf of ICS Village

MANUFACTURING- LESSONS LEARNED, LESSONS TAUGHT

Saturday at 12:30 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes

Ken Munro on behalf of Aerospace Village

GPS SPOOFING: IT'S ABOUT TIME, NOT JUST POSITION

Saturday at 12:30 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes

Emma Stewart on behalf of Policy Village

PICK YOUR POISON: NAVIGATING A SECURE CLEAN ENERGY TRANSITION

Saturday at 12:30 in Creator Stage 4 (W222)
45 minutes

Federico Lucifredi on behalf of HHV/SSV

ALL YOUR KEYBOARDS ARE BELONG TO US!

Saturday at 13:00 in Creator Stage 1 (Hall 2 - Aisle 07-04)
60 minutes | Demo

Matt Burrough on behalf of Lock Pick Village

LOCKSPORT COMPETITIONS: COMPETE IN THE OLYMPICS OF LOCKS

Saturday at 13:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes

Angelina Tsuboi on behalf of Aerospace Village

FLY CATCHER - HOW I DEVELOPED A LOW-COST RASPBERRY PI BASED DEVICE FOR ADS-B SPOOF

Saturday at 13:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Tool

Harriet Farlow on behalf of Policy Village

HACKER VS AI: PERSPECTIVES FROM AN EX-SPY

Saturday at 13:15 in Creator Stage 4 (W222)
45 minutes

AND!XOR on behalf of Makers Community

HOW WE BUILT OUR REDACTED THING THIS YEAR, 5N4CK3Y, && AMA PANEL ON MAKING BADGES

Saturday at 13:30 in Creator Stage 2 (Hall 3 - Aisle 06-02)
45 minutes

Kyle Murbach on behalf of Aerospace Village

SMALL SATELLITE MODELING AND DEFENDER SOFTWARE

Saturday at 13:30 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Tool

Abhinav Panda, Bradán Lane, Hamster on behalf of Makers Community

COLOR BLASTED BADGE MAKING: HOW HARD COULD IT BE ?

Saturday at 14:00 in Creator Stage 1 (Hall 2 - Aisle 07-04)
60 minutes

James Utley, Joshua HIll, Phil Rhodes on behalf of BioHacking Village

YOU GOT A LIGHTER? I NEED TO DO SOME ELECTROPORATION.

Saturday at 14:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Tool

Gunnar Andrews on behalf of Bug Bounty Village

EFFICIENT BUG BOUNTY AUTOMATION TECHNIQUES

Saturday at 14:00 in Creator Stage 4 (W222)
30 minutes

Giacomo Longo, Vincent Lenders on behalf of Aerospace Village

RF ATTACKS ON AVIATION'S LAST LINE OF DEFENSE AGAINST MID-AIR COLLISIONS (TCAS II)

Saturday at 14:15 in Creator Stage 2 (Hall 3 - Aisle 06-02)
45 minutes | Exploit

Lucas Potter, Meow-Ludo Disco Gamma Meow-Meow , Xavier Palmer on behalf of BioHacking Village

THE PAST, PRESENT, AND FUTURE OF BIOWEAPONS

Saturday at 14:30 in Creator Stage 3 (Hall 4 - Aisle 04-02)
45 minutes

Diego Jurado, Joel "Niemand_Sec" Noguera on behalf of Bug Bounty Village

LEVERAGING AI FOR SMARTER BUG BOUNTIES

Saturday at 14:30 in Creator Stage 4 (W222)
45 minutes

Karen Ng, Terry Luan on behalf of Physical Security Village

BYPASS 102

Saturday at 15:00 in Creator Stage 1 (Hall 2 - Aisle 07-04)
30 minutes | Demo

Shishir Gupta on behalf of ICS Village

WAR GAMES: RED TEAM FOR OT (BASED ON REAL WORLD CASE STUDIES)

Saturday at 15:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes

Braelynn Hacker, Dennis Giese on behalf of Embedded Village

REVERSE ENGINEERING AND HACKING ECOVACS ROBOTS

Saturday at 15:15 in Creator Stage 3 (Hall 4 - Aisle 04-02)
45 minutes | Demo

Chloé Messdaghi, Kasimir Schulz on behalf of Bug Bounty Village

I'VE GOT 99 PROBLEMS BUT A PROMPT INJECTION AIN'T PINEAPPLE

Saturday at 15:15 in Creator Stage 4 (W222)
45 minutes

Tim Clevenger on behalf of Physical Security Village

ACCESS CONTROL DONE RIGHT THE FIRST TIME

Saturday at 15:30 in Creator Stage 1 (Hall 2 - Aisle 07-04)
30 minutes

Nastassia Tamari, Nitin Natarajan on behalf of BioHacking Village

DID CHANGE CHANGE HEALTHCARE CYBER RESPONSE?

Saturday at 15:30 in Creator Stage 2 (Hall 3 - Aisle 06-02)
60 minutes

Chad Shortman on behalf of Physical Security Village

YOUR SMARTCARD IS DUMB: A BRIEF HISTORY OF HACKING ACCESS CONTROL SYSTEMS

Saturday at 16:00 in Creator Stage 1 (Hall 2 - Aisle 07-04)
60 minutes | Demo

Kevin Mitchell on behalf of Car Hacking Village

"BLUETOOTH BLUES: UNMASKING CVE 2023-52709 - THE TI BLE5-STACK ATTACK"

Saturday at 16:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Exploit

CREATOR STAGE TALKS

Will Kay on behalf of Packet Hacking Village

DIAMOND-TIPPED SPEARS, 99% SUCCESS RATE TECHNIQUES YOU NEED TO WORRY ABOUT

Saturday at 16:00 in Creator Stage 4 (W222)
30 minutes | Demo

Andrzej Olchawa on behalf of Aerospace Village

OFFENSIVE SECURITY TESTING: SAFEGUARDING THE FINAL FRONTIER

Saturday at 16:30 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes | Exploit

Varjitt Jeeva on behalf of Car Hacking Village

PROGRAMMING A CTS-V GAUGE CLUSTER INTO AN ATS-V, OUT OF PURE SPITE

Saturday at 16:30 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Demo

Adel Karimi on behalf of Packet Hacking Village

DECODING GALAH, AN LLM POWERED WEB HONEYPOT

Saturday at 16:30 in Creator Stage 4 (W222)
30 minutes | Tool

Bob Wall, Patrick Walsh on behalf of Crypto Privacy Village

ATTACKS ON GENAI DATA AND USING VECTOR ENCRYPTION TO STOP THEM

Saturday at 17:00 in Creator Stage 1 (Hall 2 - Aisle 07-04)
30 minutes

Randi Tinney on behalf of Aerospace Village

FROM THEORY TO REALITY: DEMONSTRATING THE SIMPLICITY OF SPARTA TECHNIQUES

Saturday at 17:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes | Demo

DEF CON Villages on behalf of Car Hacking Village

THE VILLAGE PEOPLES' PANEL - WHAT REALLY GOES ON IN A VILLAGE?

Saturday at 17:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
60 minutes

Ezz Tahoun, Lynn Hamida on behalf of Packet Hacking Village

EXPOSING COORDINATED ATTACKS HIDING IN THE SHEER NOISE OF FALSE POSITIVES AND LONE INCIDENTS: A DATA SCIENCE CORRELATION AND CONTEXTUALIZATION JOURNEY OF LOGS, EVENTS, AND ALERTS

Saturday at 17:00 in Creator Stage 4 (W222)
60 minutes | Demo

Jeff Man on behalf of Crypto Privacy Village

GUR RIBYHGVBA BS PELCGBTENCUL

Saturday at 17:30 in Creator Stage 1 (Hall 2 - Aisle 07-04)
30 minutes

Matt Gaffney on behalf of Aerospace Village

A DIVE INTO WORLD OF AIRCRAFT PKI

Saturday at 17:30 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes

Gastón Aznarez, Octavio Gianatiempo on behalf of HHV/SSV

TAKING OFF THE BLINDFOLD: DETECTING PERSISTENT THREATS ON DRAYTEK EDGE DEVICES

Sunday at 10:00 in Creator Stage 1 (Hall 2 - Aisle 07-04)
60 minutes | Demo

ET on behalf of Crypto Privacy Village

PORN & PRIVACY

Sunday at 10:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes

Paul Davilar on behalf of XR Village

HUNTER X TRIAGER BUG HUNTING IN THE WILD

Sunday at 10:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
60 minutes

Justin "Rhynorater" Gardner on behalf of Bug Bounty Village

TOP WAR STORIES FROM A TRYHARD BUG BOUNTY HUNTER

Sunday at 10:00 in Creator Stage 4 (W222)
60 minutes

Elonka Dunin, Klaus on behalf of Crypto Privacy Village

FAMOUS AND NOT-SO-FAMOUS UNSOLVED CODES

Sunday at 10:30 in Creator Stage 2 (Hall 3 - Aisle 06-02)
60 minutes

Lukas McCullough on behalf of Physical Security Village

PHYSICAL OSINT

Sunday at 11:00 in Creator Stage 1 (Hall 2 - Aisle 07-04)
30 minutes

Mark Foudy on behalf of Adversary Village

EXPLOITING VOICE CLONING IN ADVERSARIAL SIMULATION

Sunday at 11:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Demo

Dr. Robert (Rob) Hickey, Mike Weigand on behalf of Policy Village

FLYING BLIND: NAVIGATING THE TURBULENT SKIES OF AVIATION CYBERSECURITY REGULATION

Sunday at 11:00 in Creator Stage 4 (W222)
60 minutes

Billy Graydon, Lucas Rooyakkers on behalf of Physical Security Village

FITNESS OF PHYSICAL RED TEAMERS

Sunday at 11:30 in Creator Stage 1 (Hall 2 - Aisle 07-04)
30 minutes

Matt Thomassen, Sean McKeever on behalf of Aerospace Village

WARFLYING IN A CESSNA

Sunday at 11:30 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes | Demo

Leo Tsaousis on behalf of Adversary Village

KUBERNETES ATTACK SIMULATION: THE DEFINITIVE GUIDE

Sunday at 11:30 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Demo

Andrew "DigitalAndrew" Bellini on behalf of IOT Village

ANYONE CAN HACK IOT - A BEGINNER'S GUIDE TO HACKING YOUR FIRST IOT DEVICE

Sunday at 12:00 in Creator Stage 1 (Hall 2 - Aisle 07-04)
60 minutes | Demo

Lillian Ash Baker on behalf of Aerospace Village

THE INTERPLAY BETWEEN SAFETY AND SECURITY IN AVIATION SYSTEMS

Sunday at 12:00 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes

Lacey Harbour on behalf of BioHacking Village

3DU: HOMO (E)X MACHINA

Sunday at 12:00 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes

Brandon Colley on behalf of Packet Hacking Village

WINNING THE GAME OF ACTIVE DIRECTORY

Sunday at 12:00 in Creator Stage 4 (W222)
60 minutes | Demo

Ava Petersen, Justin Mott on behalf of IOT Village

FINDING 0DAYS IN VILO HOME ROUTERS

Sunday at 12:30 in Creator Stage 2 (Hall 3 - Aisle 06-02)
30 minutes | Exploit

Adam Batori, Robert Pafford on behalf of Aerospace Village

BEHIND THE BADGE: HOW WE USED AND ABUSED HARDWARE TO CREATE THE AV BADGE FOR DC32

Sunday at 12:30 in Creator Stage 3 (Hall 4 - Aisle 04-02)
30 minutes | Demo

Anthony Hendricks on behalf of Crypto Privacy Village

WU-TANG IS FOR THE CHILDREN: HOW STATES LAWS INTENDED TO PROTECT CHILDREN RAISE OTHER PRIVACY AND LEGAL RISKS

Sunday at 13:00 in Creator Stage 4 (W222)
30 minutes

DEMO LABS

5GHOUL FRAMEWORK - 5G NR ATTACKS & 5G OTA FUZZING

Matheus Eduardo Garbelini, Sudipta Chattopadhyay
Saturday from 10:00 to 11:45 in W305

5Ghoul Fuzzer is an over-the-air security testing tool and fuzzing framework that leverages a rogue 5G NR base station to systematically create test cases targeting 5G-capable smartphones or Qualcomm USB-based modems. Moreover, such framework contains test case scripts to launch attacks exploiting 10 implementation-level vulnerabilities ranging from DoS to Downgrades that affect commercial 5G modems from major chipset vendors such as Qualcomm and MediaTek. The tool is released open sourced, but it is also continuously experimented with newer devices. For example, there are two more 5G implementation vulnerabilities that are under embargo and will be released by the end of this month in the open source repository and website maintained for the project.

Audience: Mobile, Offense

AUTOMATED CONTROL VALIDATION WITH TOMMYKNOCKER

Jeremy Banker
Friday from 14:00 to 15:45 in W303

Tommyknocker is an open source project designed to facilitate automation of continuous security control validation, bringing some of the processes developers have been using for years for regressing testing, to the security world. It allows users to easily create test scenarios using docker images and standard scripts to perform one or more test actions, followed by the ability to easily check common tooling (SIEM, IDS, Log aggregators) for any expected alerts or log entries. Using Tommyknocker, security organizations can add test cases each time a new security control is created, so that any time a change is made in the environment, the continued functioning of existing controls can be validated. Many times, security organizations will only test controls when they are first implemented, and potentially a few times a year for audit purposes. With Tommyknocker, controls can be tested multiple times per day, ensuring that alerts are raised as soon as possible when a control ceases to function correctly, or is compromised by a threat actor.

Audience: Offense, Audit/Policy, Defense, Purple Team, SecOps

BLUETOOTH LANDSCAPE EXPLORATION & ENUMERATION PLATFORM (BLEEP)

Paul Wortman
Friday from 10:00 to 11:45 in W306

The purpose of the tool platform is to provide both novice and experienced Bluetooth researchers a "swiss-army knife" for device exploration and enumeration. The Bluetooth Landscape Exploration & Enumeration Platform (BLEEP) is capable of discovering Bluetooth Low Energy (BLE) devices, connecting to them, and enumerating the device as well. BLEEP leverages Python3, BlueZ, and the Linux D-Bus to provide a terminal user interface for identifying and interacting with BLE implements. The I/O capabilities of the toolset include read I/O, performing writes, and capturing of notification signals. The purpose of using these low-level libraries is to maintain small granularity control over the interactivity between BLEEP and the BLE environment.

Audience: Bluetooth, Offense

BYPASSIT - USING AUTOIT & SIMILAR TOOLS FOR COVERT PAYLOAD DELIVERY

Ezra Woods, Mike Manrod
Friday from 12:00 to 13:45 in W304

BypassIT is a framework for covert delivery of malware, using AutoIT, AutoHotKey, and other Live off the Land (LotL) tools to deliver payloads and avoid detection. These techniques were derived from reversing attacks observed in the wild by DarkGate and other MaaS actors, revealing universal principles and methods useful for red teaming or internal testing. The framework will consist of a series of tools, techniques, and methods along with testing and reporting on effectiveness, as it relates to evading multiple specific antivirus products.

Audience: Offense, Malware, Defense

CLOUD OFFENSIVE BREACH AND RISK ASSESSMENT (COBRA)

Anand Tiwari, Harsha Koushik
Friday from 10:00 to 11:45 in W308

Cloud Offensive Breach and Risk Assessment (COBRA) is an open-source tool designed to empower users to simulate attacks within multi-cloud environments, offering a comprehensive evaluation of security controls. By automating the testing of various threat vectors including external and insider threats, lateral movement, and data exfiltration, CNBAS enables organizations to gain insights into their security posture vulnerabilities. CNBAS is designed to conduct simulated attacks to assess an organization's ability to detect and respond to security threats effectively.

Audience: Defense, Cloud, Offense

CODASM - HIDING PAYLOADS IN PLAIN .TEXT

Moritz Laurin Thomas
Saturday from 12:00 to 13:45 in W305

CODASM aims to decrease a stageless payload's Shannon entropy, which was found to be a simple but annoying detection vector used by EDRs. It's a Python program that processes arbitrary binary inputs and produces a C program consisting of two parts: a buffer holding generated x86-64 ASM instructions with the original payload encoded into it, and a set of functions that can decode the ASM at runtime. The buffer is designed to be compiled into the final payload's .text section, thus it looks like regular (if not functional) code to AVs, EDRs and analysts. This encoding effectively decreases the payload's Shannon entropy but comes with a significant increase in output size. The demo will cover usage of the tool and dissection/reverse engineering of the resulting payload.

Audience: Defense, Offense, Malware Development

CYBER SECURITY TRANSFORMATION CHEF (CSTC)

Florian Haag, Matthias Göhring
Saturday from 10:00 to 11:45 in W307

Imagine GCHQ's CyberChef integrated in BurpSuite with live modification of requests at your fingertips. That's exactly what we had in mind when we built the Cyber Security Transformation Chef (CSTC) a few years ago. The CSTC is an extension to the popular BurpSuite Proxy built for experts working with web applications. It enables users to define recipes that are applied to outgoing or incoming HTTP requests/responses automatically. Whatever quirks and specialties an application might challenge you with during an assessment, the CSTC has you covered. Furthermore, it allows to quickly apply custom formatting to a chosen message, if a more detailed analysis is needed. After the initial release the CSTC is finally back! It contains new features and improvements such as many new operations to be used in recipes, inclusion of community requested features and a refactoring of the codebase. Alongside the CTSC we will launch a new public repository with recipes we found useful in our experience as penetration testers and of course open for contribution by the community. This helps the community to solve common challenges and getting started working with the CSTC.

Audience: AppSec, Offense

DISTRIBRUTED - DISTRIBUTED ATTACK FRAMEWORK

Ismail Melih Tas, Numan Ozdemir
Friday from 12:00 to 13:45 in W303

Penetration testing tools often face limitations such as IP blocking, insufficient computing power, and time constraints. However, by executing these tests across a distributed network of hundreds of devices, these challenges can be overcome. Organizing such a large-scale attack efficiently is complex, as the number of nodes increases, so does the difficulty in orchestration and management. distribRuted provides the necessary infrastructure and orchestration for distributed attacks. This framework allows developers to easily create and execute specific distributed attacks using standard application modules. Users can develop their attack modules or utilize pre-existing ones from the community. With distribRuted, automating, managing, and tracking a distributed attack across hundreds of nodes becomes straightforward, thereby enhancing efficiency, reducing time and costs, and eliminating Single Point of Failure (SPoF) in penetration testing.

Audience: Offense, DevOps, Security Research

DOCKER EXPLOITATION FRAMEWORK

Emmanuel Law, Rohit Pitke
Friday from 10:00 to 11:45 in W303

Docker Exploitation Framework is a cross-platform framework that is focused on attacking container environments (think Kubernetes, docker, etc). It can identify vulnerabilities, misconfigurations, and potential attack vectors. It also helps to automate different stages of a successful kill-chain through features such as:

- Vulnerability scanning
- Container breakouts
- Pod2pod lateral movement
- File layers deep inspection and extraction
- Attack surface discovery and mapping
- Privilege escalation, etc

Audience: AppSec, Offense

DROP-PI

Doug Kent, Robert Ditmer
Saturday from 14:00 to 15:45 in W306

The Drop-Pi is a suite of software developed on a Raspberry Pi to facilitate the automatic bypassing of 802.1x/NAC implementations (pre 802.1x-2010 standards) and establish discrete remote access into target networks. Designed with physical penetration testing in mind, the Drop-Pi can establish remote access inside a target network within a matter of seconds after being plugged in, affording assessors with a quick in and out on an objective. Its built with common and easily sourced hardware which allows for easy and quick provisioning of multiple Drop-Pi devices. When it's not feasible to utilize a target network for egress traffic, the Drop-Pi can easily be configured to employ a wireless connection or mobile hotspot to facilitate access in and out of the network.

Audience: Offense

FACTION

Josh Summitt
Saturday from 12:00 to 13:45 in W308

FACTION is an all-encompassing solution for streamlined security assessment workflows and enhancing collaboration within your teams. In addition, It's fully open source and extendable so it can integrate within diverse environments. FACTION's key benefits are that it cuts reporting time down to more than half for manual pen-tests, keeps tabs on all outstanding vulnerabilities with custom alerts based on your SLAs, becomes the hub of shared information for your assessments enabling other teammates to replay attacks you share, facilitates large scale assessment scheduling that typically becomes hard to manage when your teams are doing more than 100 assessments a year, and is fully extendable with REST APIs and FACTION Extensions.

Audience: Offense, Vulnerability Management, AppSec, Defense, Red Team

DEMO LABS

GARAK

Erick Galinkin, Leon Derczynski
Friday from 14:00 to 15:45 in W306

Garak, Generative AI Red-teaming and Assessment Kit, is a vulnerability scanner for large language models (LLMs) and dialogue systems. It has a host of different probes, each working on different vulnerabilities and payloads. It connects to a broad range of different LLMs. The attacks range between static tests of fixed prompts, to dynamically assembled prompts, to probes that respond to existing model behavior when working out their next move. Community contribution plays a big part of Garak already, with an active repo & over 300 members in the Discord. Garak can assess and attack anything that takes text and returns text, and is already used by many industry players in assessment of internal and external models, including NVIDIA and Microsoft as well as a range of emerging AI Security startups; it's the #1 ranked tool for LLM security on Hackernews. But we think it's mostly a lot of fun.

Audience: Offense, AI, Defense

GC2 - THE FIRST SERVERLESS COMMAND & CONTROL

Lorenzo Grazian
Saturday from 12:00 to 13:45 in W306

GC2 is the first serverless command and control. This project aims to demonstrate how attackers could take advantage of third-party tools (Google Sheets and Google Drive) to execute commands and exfiltrate information from a compromised system. First released in 2021, became well known in April 2023 after being mentioned in Google's Threat Horizons Report.

Audience: Defense, Offense, DevOps

HIDE & SEEK

Jonathan Fischer, Matthew Richard
Friday from 14:00 to 15:45 in W304

The Injectyll-HIDe project (released at DEF CON 30) is back and better than ever! The hardware implant utilizes the same standard features that you have come to know and love (keystroke recording, keystroke injection, mouse jiggler, etc.) but it has evolved into so much more. The functionality has been steadily growing over its initial release to offer users even more tools! But wait, there's more! We're proud to show off the new SEEK shields this year at the CON! Tired of running a covert mesh network? Want to try out new RF technologies? We've added LoRa and LoRaWAN to the mix as well! These shields are field swappable and work with the existing C2 and implant code to give you the versatility that you need to continue evading detection. Attendees should be prepared to flip 0ut over these features, as well as some new additions to the project that we will be announcing at DEF CON. Who's ready for a high stakes game of hacker's HIDe and SEEK?

Audience: Offense, Red Team, Hardware

HOPPER - DISTRIBUTED FUZZER

Luciano Remes, Wade Cappa
Friday from 14:00 to 15:45 in W308

Hopper is a Coverage-Guided Greybox Distributed Fuzzer, inspired by AFL++, and written in Golang. Like other fuzzers, Hopper operates as a standard command-line interface tool, allowing you to run fuzz campaigns to find vulnerabilities and exploits in software. Hopper's mutation algorithm, energy assigning strategy, and out-of-process coverage gathering, are all inspired by AFL++, the current state of the art fuzzer. However, Hopper's distributed strategy differs substantially than AFL++ in an attempt to define a new distributed fuzzing paradigm. AFL++ and LibFuzzer have clear scaling limitations in larger environments, notably the AFL++'s rudimentary multi-machine mode. As an early prototype, Hopper addresses these limitations by implementing a deduplicating communication schema that establishes a consistency invariant, minimizing repeated work done by fuzzing nodes. Hopper is a standalone, new piece of software developed from scratch in the spirit of exploration, this is not yet another python plugin/extension for AFL++. Hopper is currently available on GitHub, including containerized runnable campaign demos. Tooling and observability are first class features, in the form of a TUI to monitor fuzzing campaigns, usage docs, and quick-start scripts for orchestrating fuzz campaigns.

Audience: Security Research, Offense, AppSec

MAESTRO

Chris Thompson
Saturday from 10:00 to 11:45 in W303

Maestro is a post-exploitation tool designed to interact with Intune/EntraID from a C2 agent on a user's workstation without requiring knowledge of the user's password or Azure authentication flows, token manipulation, and web-based administration console. Maestro makes interacting with Intune and EntraID from C2 much easier, as the operator does not need to obtain the user's cleartext password, extract primary refresh token (PRT) cookies from the system, run additional tools or a browser session over a SOCKS proxy, or deal with Azure authentication flows, tokens, or conditional access policies in order to execute actions in Azure on behalf of the logged-in user. Maestro enables attack paths between on-prem and Azure. For example, by running Maestro on an Intune admin's machine, you can execute PowerShell scripts on any enrolled device without ever knowing the admin's credentials!

Audience: Cloud, Offense

MITRE CALDERA

Mark Perry, Rachel Murphy
Saturday from 10:00 to 11:45 in W308

MITRE Caldera is a scalable, automated adversary emulation, open-source cybersecurity platform developed by MITRE. It empowers cyber practitioners to save time, money, and energy through automated security assessments. Caldera not only tests and evaluates detection/analytic and response platforms, but it also provides the capability for your red team to perform manual assessments with computer assistance. This is achieved by augmenting existing offensive toolsets. The framework can be extended to integrate with any custom tools you may have. The development team behind the platform is a group of red teamers, software developers, exploit writers, cyber threat analysts, AI researchers, cybersecurity engineers, and computer scientists. They all pursue the common goal of building a premier adversary emulation platform for our security defenders around the world.

Audience: Purple Team, Defense

MITRE CALDERA FOR OT

Blaine Jeffries, Devon Colmer
Saturday from 14:00 to 15:45 in W303

Caldera for Operational Technology (C4OT) is an extension to the open-source Caldera adversary emulation platform. Adversary emulation has long helped defenders of information systems exercise and improve their cyber defenses by using real adversary techniques. While Caldera has been out since 2021, C4OT was released September 2023. Specifically, C4OT exposes native OT protocol functions to Caldera. The initial release of C4OT supported three popular OT protocols (Modbus, BACnet, and DNP3). Since then, we have added support for two more protocols (IEC61850 and Profinet). Today, we are actively working on support for the space protocol GEMS. By utilizing Caldera and the C4OT plugins, end-users can emulate threat activity across both Enterprise and Operational networks with ease.

Audience: Purple Team, Defense, Offense, Operational Technology, Red Team

MORIARTY

Anthony "Coin" Rose, Jake "Hubble" Krasnov
Saturday from 14:00 to 15:45 in W307

Moriarty is a.NET tool designed to identify vulnerabilities for privilege escalation in Windows environments. Building upon Watson and Sherlock, Moriarty extends their capabilities by incorporating advanced scanning techniques for newer vulnerabilities and integrating additional checks. This tool supports a wide range of Windows versions, from Windows 10 to Windows 11 and Server versions 2016, 2019, and 2022. Moriarty differentiates itself by its ability to enumerate missing KBs and detect a variety of vulnerabilities linked to privilege escalation, offering suggestions for potential exploits. The tool's extensive database includes well-known vulnerabilities such as PrintNightmare (CVE-2021-1675), Log4Shell (CVE-2021-44228), and SMBGhost (CVE-2020-0796), among others.

Audience: Offense

MPT - PENTEST IN ACTION

Jyoti Raval
Saturday from 12:00 to 13:45 in W307

In ever evolving software development world, security is also becoming fast paced. Hence, each product going through the pentest cycle has to be managed effectively and efficiently. Managing multiple pentests and testers is important. A single pane of glass view for managing pentests and testers is what the goal of this tool is.

Audience: AppSec

NEBULA - 3 YEARS OF KICKING *AAS AND TAKING USERNAMES

Bleon Proko
Friday from 10:00 to 11:45 in W307

Cloud Penetration Testing has become a hot topic in the offensive community, as the cloud based infrastructures have been slowly taking the place on-prem ones used to have. This requires a tool to help with it. Nebula is a cloud Pentest Framework, which offers reconnaissance, enumeration, exploitation, post exploitation on AWS, Azure, DigitalOcean and above all opportunity to extend even more. It is built modulary for each provider and each attack, allowing for a diversity in attack surface. This coupled with the client-server architecture, allows for a collaborated team assessment of a hybrid cloud environment.

Audience: Offense, Defense, Cloud

OPEN HARDWARE DESIGN FOR BUSKILL CORD

Melanie Allen
Saturday from 12:00 to 13:45 in W303

An open hardware design for BusKill cables that uses 3D printing and easily sourceable components. BusKill cables are hardware Dead Man's Switches that use USB events to trigger a laptop to lock, shutdown, or self-destruct when the laptop is physically separated from the operator.

Audience: Defense, Hardware

SCAGOAT - EXPLOITING DAMN VULNERABLE SCA APPLICATION

Hare Krishna Rai, Prashant Venkatesh
Friday from 14:00 to 15:45 in W305

SCAGoat is a deliberately insecure web application designed for learning and testing Software Composition Analysis (SCA) tools. It offers a hands-on environment to explore vulnerabilities in Node.js and Java Springboot applications, including actively exploitable CVEs like CVE-2023-42282 and CVE-2021-44228 (log4j). This application can be utilized to evaluate various SCA and container security tools, assessing their capability to identify vulnerable packages and code reachability. As part of our independent research, the README includes reports from SCA tools like semgrep, snyk, and endor labs. Future research plans include incorporating compromised or malicious packages to test SCA tool detection and exploring supply chain attack scenarios.

Audience: DevOps, Security Engineers, Security Research

SERBERUS

Patrick Kiley
Friday from 12:00 to 13:45 in W308

The Serberus is a serial Man-in-the-Middle hardware hacking tool designed to connect to embedded devices . It has 4 channels and has headers to interface with up to 3 UARTs simultaneously and also has the ability to connect to JTAG, SPI, I2C and SWD interfaces. During this talk I will introduce the Serberus and what makes it different than other, similar tools. It has a level shifter and switch to allow you to connect to

DEMO LABS

logic voltages of 1.8, 2.5 and 3.3v or any arbitrary voltage between 1.65v and 5.5v, matching that of your target. The Serberus is unique in that it was designed to use open source tools like the Akheron proxy in order to MitM serial communications. I will demonstrate the Serberus connecting to a wifi router, to a JTAG, I2C or SPI target and I will also show the MitM capabilities on the serial connection between an aircraft transponder and its avionics system. The Serberus project is free and open source with all board layouts, gerbers and schematics published.

Audience: Hardware

SKYNET

Craig Chamberlain, Rewanth Tammana
Friday from 12:00 to 13:45 in W306

Skynet is an AI project (just kidding.) It is meant to be a sort of unified theory of detection, enabling us to plot any detection artifact types on screen around an entity and decision them faster and more accurately. While plotting alert sets, attack trees, and kill chains has been done, for the presentation of alert sets and cases, we are planning to use graphing as the primary presentation, triage and decisioning mechanism, at scale, using a novel combination of heuristics and machine learning. It is an alert manager made by users, for users.

Audience: Defense

TEMPEST

Kirk Trychel
Saturday from 10:00 to 11:45 in W304

Tempest is a command and control framework written in 100% Rust. It began as a research project and personal challenge, but has grown into a very effective c2 framework. The original concept was to write a simple yet effective c2 framework, and design continues to focus on this simple goal. Because it started out as a research project with a learning goal, the framework is not directly based on any existing c2 frameworks and the vast majority of code will not be found anywhere else.

Audience: Defense, Offense

TENGU MARAUDER

Leonardo Serrano, Lexie Thach
Friday from 12:00 to 13:45 in W305

The Tengu Marauder, derived from a previous security drone project, is a portable wheeled robot equipped with an ESP32 Marauder, currently in its testing phase. Designed for simplicity and efficiency, the Tengu Marauder serves as an alternative and interactive tool for WiFi network security testing. Its capabilities include WiFi scanning, deauthentication attacks, packet sniffing, and other wireless security tests. The compact design ensures ease of construction and maintenance using readily available parts and straightforward code integration. Essentially an advanced RC robot, the Tengu Marauder operates headless via XBee, providing a fun and engaging platform for testing the security of network-controlled devices over WiFi, such as IoT smart home devices and smaller WiFi-controlled drones like the Ryze Tello. This project would not have been possible without the development help, test runs, and support from the Philadelphia RAICES organization, the Philadelphia DEF CON group, and DeciSym.AI.

Audience: Robotics, Drones, Hardware, RF, Security Engineers

TESTBED VIRTUAL FACTORY

Borja Pintos Castro, Camilo Piñón Blanco
Saturday from 10:00 to 11:45 in W306

As the landscape of industrial control systems (ICS) evolves, the security vulnerabilities inherent in these systems have become increasingly important. In response to this escalating situation, in this paper, we present the development of a virtualized cybersecurity research testbed tailored for these environments. Addressing the challenge of limited access to proprietary OT network data for research purposes, our this talk proposes a comprehensive framework for simulating industrial environments, aiming to facilitate the development and testing of cybersecurity solutions by providing functionalities for network traffic logging, attack impact simulation, generation of labeled multivariate time series sensor datasets, among others, bridging the gap between theoretical research and practical application needs, especially in situations of low data availability and data-driven cybersecurity research.

Audience: Defense

THE METASPLOIT FRAMEWORK V6.4

Jack Heysel, Spencer McIntyre
Saturday from 12:00 to 13:45 in W304

The Metasploit Framework released version 6.4 earlier this year, including multiple improvements to Kerberos-related attack workflows. The latest changes added support for forging diamond and sapphire tickets, as well as dumping tickets from compromised hosts. Metasploit users can now exploit unconstrained delegation in Active Directory environments for privilege escalation as well as use pass-the-ticket authentication for the Windows secrets dump module. These new Kerberos improvements increase the ways in which tickets can be forged, gathered, as well as used. Additionally, Metasploit has added support for new protocol based sessions, allowing users to interact with targets without uploading payloads, thus increasing their evasive capabilities. These new sessions can be established to database, SMB and LDAP servers. Once opened, they enable users to interact and run post modules with them, all without running a payload on the remote host. Finally, version 6.4 includes a complete overhaul of how Metasploit handles its own DNS queries. These improvements ensure that users pivoting their traffic over compromised hosts are not leaking their queries and offer a high degree of control over how queries should be resolved. This demonstration will cover these latest improvements and show how the changes can be combined for new, streamlined attack workflows using the latest Metasploit release.

Audience: Offense

THE WORLD WIDE PARAWEB

Nathan Sidles
Friday from 12:00 to 13:45 in W307

Paraweb empowers people to publish and surf invisibly on a World Wide Web without the telltale traffic patterns that can betray our use of Tor and VPNs to network monitors. Paraweb is a wide-area hypermedia information retrieval initiative that combines steganography and open Web 1.0-inspired protocols to hijack and embed itself as a parasitic communications network inside existing social network websites like Tumblr, Instagram, and Reddit. Paraweb publishers can steganographically encode HTML-based, para-hyperlinked sites within innocuous media, then post those media on social network sites indistinguishably from benign content creators. Paraweb surfers can traverse these media as benign social network users, decoding the contents of para-sites as they appear normally in their searches, traversals, and feeds. Paraweb traffic is designed to blend indistinguishably with normal Web 2.0 and social network traffic, enabling Paraweb netizens to "hide in plain sight." Paraweb's loose and open-source combination of steganography and web-based protocols extends the hard-shell defenses of the encrypted web to the realms of deniability and stealth.

Audience:

THEALLCOMMANDER 2.0

Matthew Handy
Saturday from 14:00 to 15:45 in W305

TheAllCommander is an open-source tool which offers red teams and blue teams a framework to rapidly prototype and model malware communications, as well as associated client-side indicators of compromise. The framework provides a structured, documented, and object-oriented API for both the client and server, allowing anyone to quickly implement a novel communications protocol between a simulated malware daemon and its command and control server. For Blue Teamers, this allows rapid modeling of emerging threats and comprehensive testing in a controlled manner to develop reliable detection models. For Red Teamers, this framework allows rapid iteration and development of new protocols and communications schemes with an easy to use Python interface. The framework has many tools or techniques used by red teams built in to allow out-of-the-box modeling, including emulated client browser HTTPS traffic Remote Desktop tunneling, and UAC bypass.

Audience: Offense, Defense

VOLATILE VAULT - DATA EXFILTRATION IN 2024

Moritz Laurin Thomas, Patrick Eisenschmidt
Friday from 10:00 to 11:45 in W305

In red team operations, selecting the right tools for data exfiltration is critical, yet comes with obstacles such as triggering Data Exfiltration Prevention (DEP) systems. We present "Volatile Vault" as a solution, a custom-built platform tailored to evade DEP detection. Our tool encrypts the data on the client-side and then provides a modular approach for uploading said data. Some of the currently implemented upload strategies are chunked HTTP uploads to multiple domain fronted endpoints (AWS) or QUIC as an alternative protocol.

Audience: Offense, AppSec, Defense

VOVK - ADVANCED YARA RULE GENERATOR V2.0

Benjamyn Whiteman, Vishal Thakur
Saturday from 14:00 to 15:45 in W304

Vovk is a toolset that can be used to create YARA rules. The Vovk DEF CON 2024 version will be released at DEF CON.

Audience: Reverse Engineer, Defense, Threat Hunting, Malware Analysis

XENOBOXX - HARDWARE SANDBOX TOOLKIT

Cesare Pizzi
Friday from 14:00 to 15:45 in W307

Malware frequently employs anti-VM techniques, which can vary in their difficulty to detect and counteract. While integrating anti-detection measures in our labs is a frequently used option, we should also consider using a real hardware sandbox, even if this sounds weird. By leveraging the awesome PCILeech project and DMA hardware access, XenoboxX provides a suite of tools for analysis tasks, such as dumping dynamically allocated memory and searching for IoC. These tools allow us to inject code at kernel level through DMA, making detection significantly more challenging and giving a new perspective to the analysis.

Audience: Hardware, Forensic, Reverse Engineer, Defense

ZIP IT UP, SNEAK IT IN - INTRODUCTION OF APKINSPECTOR

Kaloyan Velikov, Leonidas Vasileiadis
Friday from 10:00 to 11:45 in W304

apkInspector is a tool designed to tackle Android APKs, helping to uncover and decode the evasive tactics used by malware. It can decompress APK entries and extract detailed information such as entry names and sizes, making it easy to analyze the contents of an app. The tool also processes and decodes Android XML (AXML) files into a human-readable format, all while considering the sneaky evasion tactics that malware might employ. apkInspector is able to also identify specific evasion techniques used by malware to bypass static analysis, providing crucial insights for security analysis. It is built to function both as a standalone command-line interface (CLI) for direct operations and as a library that can be integrated into other security tools, enhancing its utility and adaptability in various cybersecurity environments.

Audience: GRC, Security Research, Offense, Mobile, Defense, AppSec

VENDORS

AARONIA/AUDIOVIDEO BRANDBUILDER
aaronia.com

Aaronia is a leading supplier of measurement equipment for RF and EMC applications and signal decoding. We offer innovative and high-precision spectrum analyzers, antennas, signal generators and test equipment. Visit us at the exhibition to learn more about our solutions for telecommunications, research and industry!

BOARDSOURCE
boardsource.xyz

Boardsource offers custom mechanical keyboards and accessories for mechanical keyboard enthusiasts. With products ranging from DIY kits to premium aluminum boards, you're sure to find something that interests you whether you're new to the hobby or a seasoned veteran.

CIGENT TECHNOLOGIES
www.cigent.com

Cigent, leaders in data recovery and removal, have built a storage device (for laptops, desktops, external media) with built-in data security. The drive by default makes data "invisible" - unreadable at the sector level, requiring MFA and Cigent software to access the storage. Advanced key creation and storage methodology have been implemented making it virtually impossible(?) to access the key. Additionally there is a dedicated microprocessor that monitors for attempts to wipe or clone the drive, boot off of an alternate OS, or ransom the drive - the drive automatically protects the data if it is attacked. It also has full drive erasure with unique firmware verification that confirms every block was truly wiped. Oh and wait - there's more...!

CRYPTOCURRENCY HACKERS
www.cryptohack.cc

Cryptocurrency Hackers (CRYPTOHACK) support your exploration of modern finance technology by distributing free of charge and commercially sold items at the DEF CON Vendor area. Have you wondered how a POS, ATM, hardware wallet or secure element work? Stop by the Cryptocurrency Hackers vendor area to gain new perspectives of finance technology.

At CRYPTOHACK we do not exclusively serve blockchain based technology, and encourage idea exchange of any finance hacking for common good. We distribute items relating to a number of projects including Monero, Bitcoin, Ethereum, and others. Show your cryptohacker colours with high quality wearables and custom badges. Try new devices, devkits, and electronics, with on site presence of manufacturers. Inform yourself of new developments in finance by exploring our stand, your one stop shop for fintech hacker products and information.

Since DEF CON 26 (2017) we have served a family and child friendly environment. We thank all the 6-12 year old hackers for your continued interest!

CYBER SWAMPLORDS
www.jollymediagroup.com

Dive into the swampy wonderland of the Cyber Swamplords booth! Straight out of the wilds of Central Florida, we're a motley crew from Jolly Media Group, Rot13Labs, and The Moth and Mantis, here to electrify DEF CON 32 with our unique blend of hacker culture and gear. From custom electronic badges and quirky SAOs to unique PCB jewelry and hacker-themed apparel, we've got the perfect gear to spark your interest. Swing by for some laughs, free #quack, and a taste of that one-of-a-kind Florida charm. Join us for a gator-good time and let's make some swamp magic together!

ELECTRONIC CAT
www.electroniccats.com

Electronic cats is a company based in Mexico where open source hardware is designed and assembled, with special focus on infosec with products widely used like the magspoof, catsniffer and hunter cat

ELECTRONIC FRONTIER FOUNDATION
www.eff.org

EFF is the leading defender of online civil liberties. We promote innovator rights, defend free expression, fight illegal surveillance, and protect rights and freedoms as our use of technology grows.

HACKER WAREHOUSE
www.HackerWarehouse.com

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From RF Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need.

HACKERBOXES
hackerboxes.com

HackerBoxes is the monthly subscription box for hardware hacking, DIY electronics, cybersecurity, and hacker culture. Each monthly HackerBox includes a carefully curated collection of projects, components, modules, tools, supplies, and exclusive items. HackerBox hackers connect online as a community of experience, support, and ideas. Your HackerBox subscription is like having a tiny hacker convention in your mailbox every month.

HACKERS FOR CHARITY
https://hackersforcharity.org/

HAK5
hak5.org

Discover the devices that have found their way into the hearts and tool-kits of the modern hacker. Notable for ease of use. Celebrated by geek culture. From comprehensive WiFi audits to covert network implants and physical access mayhem - Hak5 Gear gets the job done.

VENDORS

HOTWAN
www.hotwan.com

Hotwan will be selling our Premier product, the “AI Red Team Assistant”.

The system’s focus is on the automation of several hundred security and hacker tools integrated with AI. No Internet is required. It is designed to assist in Penetration Test engagements and Red Team exercises.

Technologies include Scanners (Recon), Exploiters, OSINT, Bug Bounty, Web, API, Network, IoT, GCP, AWS, Azure, Kubernetes, Windows, Linux, Mac, Source Code Analysis, C2, Privilege Escalation, Exfiltration and more.

For more info, https://www.hotwan.com/product and check out our “Hacker Tool Talk” channel on YouTube: https://www.youtube.com/channel/UCDk_uCv4WB1uErp8p_xCt9Q

INTREPID CONTROL SYSTEMS, INC.
www.intrepidcs.com

Intrepid Control Systems offers OEMs and Tier 1 suppliers comprehensive solutions for maximizing data from connected vehicles, including ICE and new energy. With 30+ years of expertise, they specialize in vehicle diagnostics, cloud connectivity, visualization, and OTA solutions, aiding in product development and production quality. Their presence spans worldwide with offices in every major automotive center.

KEYPORT
www.mykeyport.com

Keyport® combines keys, pocket tools, and tech into one secure everyday multi-tool. We are selling our latest modular product line (co-branded DEF CON 32 Limited Editions) including the key hiding Keyport Pivot, Modules, Inserts, and accessories.

MAR WILLIAMS
https://patreon.com/spux
https://www.instagram.com/spuxo/

Mar Williams is DEF CON’s resident artist, created this year’s official DEF CON badge, and has had a hand in informing the aesthetic of the conference since DC17. You can find their art throughout the hallways, on DEF CON tshirts, stickers and other swag. Mar will have high quality, signed prints of their DEF CON art available, as well as a selection of other art, stickers, plushes, and vaguely cat shaped baubles.

MISCREANTS
shopmiscreants.com

Miscreants is creating clothing for hackers heavily influenced by streetwear and security culture, looking to document the past, present, and future of cybersecurity history. As a brand, we strive to deliver original pieces that belong in your closet for decades.

NETOOL
netool.io

The netool.io Pro2, network engineering in your pocket. Connects to your iOS or Android device to detect a list of protocol including Tagged VLANs, CDP, LLDP, DHCP and more. Configure switches by a press of a button.

NO STARCH PRESS
nostarch.com

No Starch Press has been publishing the finest in geek entertainment since 1994. Come by to see our latest books, t-shirts and swag, and meet some of authors and our founder, Bill Pollock. Everything is discounted!

NUAND
nuand.com

Nuand is proud to join DEF CON this year and present new bladeRF products! Our versatile and high-performance bladeRF platform empowers researchers, developers, and security professionals to explore the wireless spectrum like never before. With capabilities that extend from radio-frequency analysis to security, our open-source ecosystem fosters innovation in radio communication and cybersecurity. Visit our booth to experience firsthand the power of bladeRF and meet our team of experts, who are passionate about providing the tools necessary to unlock new frontiers in wireless technology.

OCTOPWN
www.octopwn.com

Octopwn is a fast and reliable pentesting suite for manual internal network pentesters that runs entirely in your browser. Scan, run clients, perform attacks and log everything on any device you want that can run Chrome, enabled by pyodide and Webassembly. During DEF CON, we will sell a special Plug&Pwn edition of Octopwn on a USB stick, that you can take with you anywhere and it just works. Feel free to come by and have a look!

PHYSICAL SECURITY VILLAGE
www.physsec.org

The Physical Security Village (formerly Lock Bypass Village) will be present in the vendor area too this year, loaded with physical hacking gear! We will have bypass tools, common keyed-alike keys, handcuffs, village swag, and more. We’ll have hands-on exhibits in the Village area where you can go and try out your new toys right away, without ever leaving DEF CON! Whether you’re new to hacking the physical world, or a seasoned pro, we’re sure we’ll have something for your needs (or at least... something you really want but totally don’t need). All proceeds go towards the cost of putting on the village each year.

SLNT
slnt.com

SLNT is the leader in the mobile Faraday bag market with multiple patents, 6 Government contracts and customers that range from Google, Palantir to SOCOM and the Air Force. SLNT Faraday bags block full spectrum EMFs including Cell, Wifi, Sat/Nav, Bluetooth, H/EMP, GPS, Solar Flare and Key Fobs. Our bags are made to fit into the modern individuals lifestyle so they can effortlessly and stylishly protect their digital lives against unseen threats. All SLNT products are third party tested and exceed Military Standards. Go well, Go SLNT.

VENDORS

SOURCE OF KNOWLEDGE
www.thesourceofknowledge.com

SPARROWS LOCK PICKS
www.sparrowslockpicks.com

Manufacturer of Lock Picks & COVERT ENTRY TOOLS

With the largest selection of lock picks, covert entry and SERE tools available at DEF CON it's guaranteed we will have gear you have not seen before. New tools and classics will be on display and available for sale in a hands on environment. Our Product range covers Custom toolsets, Dimple picks, Disc Picks, Entry Tools, Practice locks, Bypass tools, Urban Escape & Evasion hardware and items that until recently were sales restricted. SPARROWS LOCK PICKS will be displaying a full range of gear including the newly released All Access bump keys, Dimple picks and The Monkey Paw. The "Folder" prototype will also be available for its first public viewing. All products will be demonstrated at various times and can be personally tested for use and Efficacy.

SALTY SECURITY
saltysecurity.com

Salty Security offers uniquely themed and originally designed merchandise that caters to the hacker mindset and lifestyle. Come by our booth for all your sticker, apparel and tech gadget needs, or find us online at https://saltysecurity.com!

SCAM STUFF
scamstuff.com

Brian Brushwood, host of National Geographic's Hacking the System, Discovery's Scam School, The Modern Rogue on YouTube, and most importantly: the podcast "World's Greatest Con." We can't say why, but you should probably get caught up on that podcast before DEF CON.

SCIENCE & DESIGN
scidsg.org

Science & Design, Inc. is a 501(c)(3) non-profit product development organization. Their flagship product is Hush Line, a lightweight tip line-as-a-service platform. No PII is required to sign up, and whistleblowers can send a message without creating an account. This year, Science & Design is proud to launch the Hush Line Personal Server, a consumer hardware Tor-only encrypted tip line inspired by our initial launch at DEF CON31! It comes in a custom-designed milled aluminum case with an e-paper display that guides you through a command-line-free setup. As a thank you for the inspiration, we're giving away a FREE Personal Server to an attendee, valued at $500! Come by the booth to learn more!

SHADOWVEX
shadowvexindustries.com

Purveyors of limited edition clothing, music, art, stickers and more. Unique 0-day swag just for DEF CON 32. Follow the music in the vending area to find our booth!

TOOOL
www.toool.us

The Open Organisation Of Lockpickers is back as always, offering a wide selection of tasty lock goodies for both the novice and master lockpicker! A variety of commercial picks, handmade picks, custom designs, practice locks, handcuffs, cutaways, and other neat tools will be available for your perusing and enjoyment! Stop by our table for interactive demos of this fine lockpicking gear or just to pick up a T-shirt and show your support for locksport. All sales exclusively benefit Toool, a 501(c)3 non-profit organization. You can purchase picks from many fine vendors, but ours is the only table where you know that 100% of your money goes directly back to the hacker community.

THE CALYX INSTITUTE
calyxinstitute.org

The Calyx Institute was founded to promote and defend the right to digital privacy and to offer thoughtfully designed educational and technological resources to those who would otherwise lack online access and security. We develop privacy-focused tools, educate the public about the importance of digital privacy, and foster the expansion of the free and open-source software ecosystem. At Calyx, we believe that everyone has an equal right to exist in online spaces without fear of surveillance, hacking, or other breaches of consent, and we strive to create a world where everyone is equipped with the tools and information they need to make informed choices about their online lives. From our inception, we have been (and remain) committed to a revenue model that allows us to prioritize people and privacy over profit.

THE TOR PROJECT
torproject.org

The Tor Project is a nonprofit developing free and open source software to protect people from tracking, censorship, and surveillance online. Tor's mission is to advance human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Stop by our table to learn more, pick up some gear, and find out how you can get involved.

WISP
www.wisporg.com

Women in Security and Privacy is a global non-profit committed to advancing women and underrepresented communities to lead the future of privacy and security. WISP's annual programming includes educational and skills workshops, mentoring and networking events, and career advancement and leadership training. WISP also provides stipends and scholarships for women and people from underrepresented communities to attend conferences and to receive training and certifications.

XCAPE
xcapeinc.com

Xcape Inc. is a cybersecurity firm known for its innovative solutions. They craft custom hardware and software for pen testing, giving them a unique level of control. They go beyond basic assessments, offering actionable insights to fortify client defenses. Xcape prioritizes staying ahead of threats through a collaborative approach, working with clients to build long-term partnerships.

EXHIBITORS

CAPITOL TECHNOLOGY UNIVERSITY

www.captechu.edu

Silver Exhibitor

Capitol Tech is Washington D.C.'s premier STEM University – supplying human capital to America's most technologically advanced government agencies and their private sector supply chains. With an education laser-focused on STEM careers, Capitol Technology University uniquely positions students for top roles in the region's booming tech hub.

HACK THE BOX

www.hackthebox.com

Silver Exhibitor

Hack The Box is the Cyber Performance Center with the mission to provide a human-first platform to create and maintain high-performing cybersecurity individuals and organizations. Hack The Box is the only platform that unites upskilling, workforce development, and the human focus in the cybersecurity industry, and it's trusted by organizations worldwide for driving their teams to peak performance.

INTIGRITI

www.intigriti.com

Silver Exhibitor

With Intigriti, you have access up to 90,000 ethical hackers working continuously to find vulnerabilities in your software, networks and systems before cybercriminals do. Intigriti's triage team sits between the ethical hackers and you to ensure you are only receiving valid vulnerability submissions that need to be fixed on our pay-for-impact model.

TRY HACK ME

tryhackme.com

Silver Exhibitor

Elevate your security expertise with TryHackMe, the world's leading technical cyber security training platform designed exclusively for security professionals. Offering over 800 hands-on labs, we cater to all skill levels, from novice to expert. Dive deep into red teaming, blue teaming, and DevSecOps as our platform delivers unparalleled training across various cyber security domains. Through a blend of realistic challenges and robust learning resources, TryHackMe empowers individuals and teams to translate knowledge into action, mastering their skills through real-world scenarios, hands-on challenges and immersive learning experiences.

2600

2600.com

Bronze Exhibitor

2600 Magazine is the definitive guide to the hacker culture, publishing on paper since 1984. Despite the demise of bookstores, distributors, and print, 2600 is still here!

ALTERED SECURITY

alteredsecurity.com

Bronze Exhibitor

Start your Red Team journey with Altered Security. We are your partners in hands-on red team and cloud red team training. Altered Security - celebrating your success.

BLACK HILLS INFORMATION SECURITY

blackhillsinfosec.com

Bronze Exhibitor

Black Hills Information Security (BHIS) focuses on helping organizations understand their security risks and improve their defenses against cyber threats through a combination of testing, assessment, education, and consulting services. Creators of Backdoors & Breaches, Antisyphon Training, and numerous open-source security tools.

SQUAREX

sqrx.com

Bronze Exhibitor

SquareX helps organisations detect, mitigate and threat-hunt web attacks happening against their users in real-time, including but not limited to malicious sites, files, scripts, and networks.

MAPS

LVCC WEST HALL LEVEL 1

LVCC WEST HALL LEVEL 2

LVCC WEST HALL LEVEL 3

THANK YOU!

The Dark Tangent would like to thank:

The DEF CON HQ staff: Cayce, Cot, Darington, Janet, Jeff, Kevin, Mar, Neil, Nikita, Tom and Will.

It takes over 500 of Goons to organize DEF CON. Their hard work and spirit is what make the con possible, and I would like to thank them all, as well as their families that support their efforts year round. Every year some Goons join and some leave. I'd like to call out the following Goons who are retiring after 10 or more years, earning themselves a Gold Badge and free attendance for life!

Br1ck - 11 years (SOC)

DaKahuna - (Speaker Ops, Workshops CFP)

Gattaca - (Speaker Ops)

morph1x - 11 years (SOC)

The Saint - (Quarter Master)

This year I want to recognize our new convention management company, Tag Team, for their invaluable work and insight in moving into the LVCC and navigating all the new and different rules and regulations. Without them the show would have been almost impossible to pull off after the unexpected venue change. Thanks Mo!

Finally I would like to thank everyone who supports DEF CON and the hacking community year round by attending and supporting conferences, researching, submitting talks, running the community services we all use, and creating the incredible experiences that make hacking such a dynamic and thriving international community.

-The Dark Tangent

DEF CON is only possible because of all the hard work from the people who make up departments:

ARTS & ENTERTAINMENT:

ChrisAM would like to thank everyone responsible for this year's entertainment & decor: Krisz Klink, Zziks, Great Scott, dead, CTRL, stitch, davesbase, Miss Jackalope, ch0wn35, Shoresy, raypath, Salem, Luna, Skittish, Bus!, Zebbler Studios, SomaFM, GAG LAB, and all the DJs and artists who donated their time and talent to this event.

CFP REVIEW:

pwcrack and Shaggy would like to give a huge thank you to Dark Tangent, Nikita, Alex and the DC32 Content Reviewers for Talks and Workshops: AlxRogan, Ash, Beau Woods, BinaryNinja, carnal0wnage, Cederic, Clavinger, DaKahuna, Dead Addict, Deana, Dino C, effffn, Grifter, H4r0ld, Heisenberg, Jay Healey, Jon Green, LawyerLiz, Magen, Malware Unicorn, Marcia, Matt Wein, Medic, n00bz, Pete, RoRo, SecBarbie, Seth, Sinderz, Snow, solstice, Suggy, Verbaal, yan, zfasel and Zoz. This team puts in countless hours to review, research and assess submissions so that DEF CON can present the best main stage and workshop content.

CONTESTS:

Grifter would like to thank all of the creators and coordinators of the multitude of contests and events at DEF CON 32. The time, effort, and passion that goes into your events does not go unnoticed, and the entertainment you bring not only to the contestants, but to the general attendees and overall atmosphere of DEF CON is hugely appreciated, so thank you so so much. A huge thanks also goes to the C&E Goons for making sure things go smoothly and for anticipating challenges and meeting them head on as they occur, so thank you to secove, kaybz, saltr, gomer, psychoticide, p0lr, Heathenhkr, klrgrz, vertighost, Dr3@mWitch, Sh00k3ms, MalwareJake, TactiKoolSec, Secitup, c0l3slaw, J9, rugger, and eli; this wouldn't be possible without you. Big thanks to the Dark Tangent, Janet, Darrington, Neil, and Will...and of course a massive thanks to Nikita, the one who keeps us all motivated by friendship and fire, truly the best of us, without whom none of this would happen, we love you more than is legally allowed but we're okay with it. Lastly, to our fellow hackers, thank you for coming out, for making us laugh, groan, and everything in between, and of course...thanks for playing.

COMMUNITIES

DEF CON Communities would like to thank: ch3f, Seams, Kevin, f0rk3d, Fl3x, tr3s, p1nk13s aka k1ng salam1, Raze, the entire village goon team, shout out to Scorprion and Wolf, the illegitimate KevOps, Disc0untM34t, BAMF, anullvalue, #3rdWebSite, Cotman and all the leads who had our back. Most of all thank you to the communities: DC NextGen, DCG, DEF CON Groups & DCGvr, Game Hacking, Hard Hat Brigade, HDA, La Villa, Lonely Hackers Club, Makers, Retro Tech, VETCON, and Women In Security and Privacy Community.

CONTENT & COORDINATION (NIKITA):

My gratitude goes out to the C&C team, Dept leads, Creators (Villages, Contests, Communities), to GOONS & Friends. Thank you for bringing your heart & dedication to the table, together we made the impossible possible, again. Thank you Janet for being my partner in crime. Thank you BAMFs for being there 24/7. Thanks to Cotman all of the work on the DC Forums, and Hacker Tracker for keeping us in sync. Thank you KevOPs, for being the Wolfe. Thank you Amanda and everyone involved with AIxCC, your passion inspires. Thank you to the truly talented behind the scenes show support: the wonderful Merlin, Tag Team, Gag-Lab, Mo, Emo, Craig, Julie, Amy, Sean, Jay, Garret, Ben.

Thank you for your belief in who we are, your faith in us to pull off this crazy unconventional convention. Also, KevOps is not a real dept.

DESIGN AND DEFACEMENT:

Drifter would like to give a big shout out to the Defacement Team: Medic, S4mG0ld, xaphan, BDA, BigSam, RJ and p0sterb0y for their momentous effort to keep you on track and aware of your surroundings. Huge thanks to Nikita, Sleestak and Mar for support on the printed program, and especially aNullValue for all the help processing the mountain of data.

DEVOPS:

Riverside and Fox would like to thank all of the DevOps goons:

Ari, BSE, cstone, Lightning, mauvehed, Nebberz, NightWolf, respondo, TCMBC, thephreak, VoltageSpike. A shout out to the Packet Hacking Village team for being the bot beta testers year round.

DC KIDS:

This year is the first official launch of DCNextGen and we are beyond thankful to everyone who worked behind the scenes and on site to make this possible. They brought this years theme as they made sure the Next Generation of hackers are given engaging hands on content and materials to help them learn, grow, make mistakes, and explore. This helps give the Next Generation a voice and a platform to make an impact.

Thank you to everyone on the DCNextGen team for being active and on top of projects. Thank you to all the villages for including new hackers into your spaces and to our amazing class, CTF, artists and badge designers for bringing this content to the next generation of hackers. Of course an extra big thank you to DEF CON for providing us with the resources needed to inspire the next generation of hackers.

DCTV:

Thank you to our amazing DCTV team: Eagle1, Ghost Pepper, K#, Robbinbs, Sandw1ch, Skw33k, and Videoman. Mom and Dad are very proud of you! Many thanks to the NOC, and special thanks to Harry and Phil for their support..

DEF CON GROUPS:

The DEF CON Groups (DCG) Board would like to give a worldwide shout-out to every individual who has contributed to the 400+ local DEF CON Groups across the globe!

Our meetups bring the natural intrigue and curiosity of our "inner hacker" together. They allow us to collaborate, share ideas, and provide mentorship that ensures our community will continue to thrive and positively impact the world.

So whether you are an organizer or attendee, we sincerely appreciate the time, effort, and energy you invest in bettering our community.

A special shout-out goes to our Virtual Reality (VR) event volunteers: AldeBaran, Charmander, Drip, Ferric, Giglio, hoodiePony, Scribbles, TX, and Xray. Their work helps extend the DEF CON experience to those unable to attend in person.

DCG would like to recognize their Board Members and GOONS: Jayson E. Street, ADAM915, 800xl, alethe, April, CylentKnight, d4rkm4tter, deviled_3gg, Fyrew4ll, gabsmashh, and polomaster for their dedicated support, promotion, and enthusiasm in fostering new communities for DCG members over the past year.

Finally, a sincere "THANK YOU" to DT, Nikita, Darington, Will, and Cot. We are truly grateful for your consistent and unwavering support.

DEMOLABS:

Heisenberg, H4r0ld, and V3rbaal would like to give a shout out to all the folks in the community who put in some truly outstanding Demolabs submissions. We also want to thank the fantastic set of Demolab goons this year - De-CERT, deftclip, J9, LAZ, and Mythrandr.

DISPATCH:

RF and Asmodian X would like to thank our wonderful group of returning Dispatch goons – Archangel, CodexMafia, dirtclod, dll3ma, Dymz, fozzie, Goon22, JUICE, Logic, Merg, miggles, mylittlebrony, Offroad, Pooker, rixon, shrinkydink, skyria, taclane, w00k, WOB, yosg, and zacperian – and everyone else that makes DEF CON amazing every year!

EXHIBITORS:

Polybius would like to thank the Exhibitors for supporting our community through donations to nonprofits, supporting our creators as well as our conference itself!

2600 Magazine, Altered Security, Black Hills Information Security, Capitol Technology University, Hack The Box, Intigriti, SquareX, and Try Hack Me

Thank you to my world class XZBT Goons:

G0rd0, hackterr, VVitchofthewoods, aur053, JusticeStorm, DAF, Kiwi, DAC, gaspar, RocketGod, Cealtea, billNYEusesMYwiFI, and the world famous Parties Department lead goon, log.

Polybius would like to give a special thank you to Nikita, Janet, DT, Will, Neil, Cot, Darington, and Mar.

And last but not least, I would like to thank the man, the myth, the legend... Kevin, aka KEVOPS, aka...

DEF CON SERVERS (COTMAN):

Thanks to everyone that has helped make DEF CON 32 work.

HACKERTRACKER

aNullValue would like to thank the HackerTracker team (advice, derail, and l4wke) for their year-round contributions to improving the app. Enormous thanks to Nikita, Cotman, Neil, and many, many others for their assistance in keeping all of the DEF CON conference content up-to-date. Special thanks to the NFO team, for helping us help humans help themselves. Finally, thank you to the lead staff of each and every department and village for their cooperation and timely schedule updates.

INHUMAN REG:

Inhuman Registration Aster & Estebang, would like to thank Cstone, Undertaker, Will, Nikita, Janet, Wendy, KC, McMayhem, Cylon, 50ph33 and all the department heads for putting up working with us.

KEVOPS

The KEVOPS department would like to thank so, so many people..

Hony, Pedro, Chef, Grifter, Secove, Log, Fivepenny, Hannah - What a year, right? I couldn't imagine a group of people less deserving of the long hours and the pain than you eight, but I also don't think we could have done it without you. I hope that in time, you'll all learn that KEVOPS is not my handle, its my department.

Polybius, the best Exhibitor lead we could have asked for, and the KEVOPS second. Thanks for always being there to have my back.

Janet and Nikita, none of us, quite literally, could do any of this without you two. Thank you for trusting me and for the massive amount of work you two put in year round.

Jeff, Neil, Darington, Cot, Will, and Mar, it is always a pleasure to work with each of you. I look forward to learning and contributing more and more every year, and to many more DEF CON's together

To all the Villages, Communities, Contests, Parties, Artists, Vendors, Exhibitors, Department Leads, and Goons, thank you for making DEF CON the most amazing part of my year each and every year. Some days DEF CON can get a bit overwhelming, and it's hard to push past the burn out. But almost like you all see the "Kevin's fading out" signal shown up on the night sky like my own personal Bat signal, one of you always comes around and reminds me why I love doing this.

And of course, to all of the attendees. Keep it weird.

MERCH:

s4cr3t would like to thank all the Merch Goons: @Mr_Minion, 10rn4, 5kyf4ll, AtomicMaya, B00MBOX, BurntRice, cillic, D20Owlbear, daelf, Dasha, Endsu, furysama, G0nZu1, gadi, gingerjet, Githur, gLoBuS, H4zy, Heal, J3ssa, KATT*BVTT, LazyGamer, lickity, Mick, Mr Katt, Nola, Nyx, Oobleck, Pablo, Peej, Sid, spiggy, Sudo Loak, Surtr, T@raByt3, theViking, VintageSadly, Wally, and webjedi for all their hard work.

Special thanks to the DEF CON staff for all they do year round, Mar for the art, the other departments that make DEF CON possible, and of course the humans who buy the merchandise so we don't have to pack it up!

To our friends who were unable to join us, we will save you some boxes.

NOC:

The NOC would like to thank the following super rad people ....Deadication, Musa ,Wish, Booger, Jon2, Strange, c0mmiebstrd, CRV, c7five, mac, effffn, Mike D, toph, dp1i, and our newest members MeiBo, Tater, Duffguy.

We are also giving a huge shout out to Nikita, Janet, Mo (and his team) and DT, for all their amazing work putting this circus together.

This is my first-year writing this and I want to say thank you to everyone in this community for building and creating such an amazing con!

This has been a wild year, and now that you're reading this means you made it!

San Dimas High School Football Rules!

NFO:

Littlebruzer and Littleroo would like to thank all of the NFO goons: 0tter, 50 Caliber, algorythm, AngstyEmu, Aqua, ArbitraryMonster, Bertoe, blu3f0x, Boudica, brubach, Bufo Alvarius, Cheshire, Commrade, D1Gger, Detaer, dL@w, DMoneyGe3k, Elhazred, Fr3nchie, GTOdevildog, Hankashyyyk, Hop, Krav, Mackovision, madstringer, Major Mayhem, mind, Momosa, Mouse of Madness, Nav, Nil, Nymphaea Caerulea, Paul, Reloadrtr, S34MSTR3SS, S3cur17yf1rs7, S747IK, Sanchez, SchematicAddict, ScurryFool, shrug, Skittl3z, SKUZZYbus, SmileFiles, Sparkle, sysaaron, Tachy0n, TACSAT, TechTurtle, Triggered_Sloth, Viva, zuul

The entire NFO team would like to thank DT, Nikita, Janet, Will, Neil, and the rest of the HQ team. Without your support, we would not have this great conference.

A shout out to the HackerTracker team: Advice, aNullValue, derail, and l4wke for their hard work on the mobile applications and the web site.

Thank you humans for the interesting questions and allowing us to tell you where to go and how to get there.

PARTIES:

Log and Kevin would like to thank our wonderful Parties and Meetups Goons: Datahere, misusage, SuRbO, hevnsnt, s3gfault, RickGlass, and Silicon Red.

We would like to extend special thanks to everyone who organizes and operates a Party or Meetup, the DJs who provide the music, the DEF CON A&E Department, the KEVOPS Department, and our friends over at the DEF CON XZBT Department.

PHOTO:

Cannibal sends thanks to the Photo Goons! ASTCell, Silk, Gourry, AJ702, and M0nkeyDrag0n. Working long shifts every single day

THANK YOU!

to capture the nuances and shenanigans that make DEF CON what it is. The Photo Goons would also like to recognize all the other departments, every one of which is critical to making the DEF CON compile. Photo also wants to thank the attendees for keeping it weird and giving us lots of things to video and photograph!

PRESS:

A big thank you to the Press team Claire Tils, Jeff Weaver, Sylvia Aranda and Carson Riley and the many DEF CON departments that work tirelessly to keep the community the center of this event.

QUARTERMASTER:

QM Stores would like to spank the naughty children Buttersnatcher, Seven, Major Malfunction, Sisu, YoungBlood, Muffin, Q, Drimacus, Sparkles, Sp1kedshell, Shell-e, Basically Jesus, SP3ZN45, Ahlana, Helium, alizarinMegalodon, The Saint, AWildBeard, Multigrain, Cell Wizard, the kids from the other playpens that keep our toys clean and mostly free of bodily fluids, and the humans that don't put their fingers in the electricity holes or use our projectors as footstool. The rest of you... go to your room and think about what you've done.

REGISTRATION:

cstone would like to thank all the goons that make Registration work: 0x90ebfe, APT, chimera, Chunk, Crackerjack, funnyguy, Holmestrix, ind1go, Jup1t3r, Phear, phreak, pozer, premio, Prophet, qumqats, Temtel, Undertaker, wra1th, and zevlag. Super extra special thanks to Janet, Nikita, Will, s3cr3t, and everyone at QM. (Noid said I could take that pallet jack, it's cool). And an extra special thank you to the DEF CON attendees for their patience and support.

SOC:

Cj, AdaZebra, Wham, deelo and Tacitus wish to thank: Arc, motsu, L4bF0x, nohackme, delta, QuietMike, HardMode, Igelkott, EMP, Sif, candyman, duckfez, DuuMayne, moniac, Cocktail, 0r3g0n V1x3n, PrincessKitty, Si, AgentFritz, DaddyFed, wilnix, LJ, BeaMeR, Zerorez, M0rph1x, Kardec, malloc, polish_dave, lys, Colonel Ghona, Daruma, theboog, bee, Stoner, HellGiraffe, Sami, Rivet, sienna, n1cFury, Br1ck, sl3dge, W.I.P., Intrepd, Junior, Survivatrix, K0414, bird, Havoc, NextInLine, Binarywishes, Priest, Mr. M, Jenny Dix, Sm0k3y, tacitus, Strider, Jilwee, smo0otchy, ZephrFish, Lucky, DONKEY, stan, prec0re, BMP51, SysTm_Ov3rL04d, Jedi, Curs0r, p1nk, zerofux, ori, PacketMonster, Oselot, wasted, Durp, dr.kaos, nerves, Spedione, Anna, Roadhouse, rand0h, HoneyBadger, Glasswalk3r, KaOsKl0wN, Red, FarmTruck, goldfishbrain, 7thdrxn, BrBr, Mr.Zeebs, nesquik, Kitty Hegemon, Disco, zombie, Pacer1128, John D, Ryan, Randy_Waterhouse, Phat_Hobbit, Our Lady of Chaos, YT, Kexel, th0m4s, Wreaktifier, Wr4th, g33kspeed, Fogame, Thirsty Goat, mouse, Gadi, Faz, CarpeDiemT3ch, WHITE CHRIS, DoktorMayhem, scrimshaw, Truth, flerper, arcon, c0verfire, H20, BIOM, MIM, Sonicos, duckie, Siviak, do2er, St1ngray, SynMac, Andi, Heylel, WraitH, noon3, JBone, reducto, c1ph3rflux, GI_Jack, cymike, Dr0me, SecretAgentSquirrel, Lady Hydra, ZettaQuark, Mrs Skelli, 4UR0R4, Zopat, Redoubt, judo, Murmaid3r, G00dn1t3, Ast0r, skroo, Zulu, M0, c0yot3, Echo Sixx, BadAask, jimi2x, milkyline, PacketWalker, Alice Kalli, Bisdak, 4chtung, timball, Giggles, Hattori Hanzo, whiskey, TBD, Toonz, m@il.man, ac0rn, AlphaKilo, Oyster, Infojanitor, pr0ph37, Krassi, n3x7, Yaga, WhiteB0rd, Las0mbra and gunwale Thank you for all you do. Pax Per Imperium.

SPEAKER OPS:

pwcrack and Pasties would like to thank the Speaker Operations team for another year of great service to DEF CON and its speakers. These goons are CLI, Crash, dROM, Flattire, g8, gdead, Goekesmi, Heidi, Jinx, Jur1st, Jutral, K-hole, kampf, MaltLiquor, Milhouse, Mnky, notkevin, Pardus, phliKtid, RoundRiver, Shadow, SIGAD, Stikk, SurrealKill3r, P!bbl3, Tinkers, TruBluFan, Vaedron and, as always, AMFYOYO!

VENDORS:

Fivepenny would like to thank the DEF CON staff! Nikita and Janet, y'all work wonders! Kevin, aka KEVOPS, thanks for putting up with my million questions! To our awesome Vendors: your flexibility and kindness as we transitioned into a new space have been invaluable. We appreciate you! And a special thank you to the fabulous Vendor Goons: N3rdH3rder, PugLady, L@dy$n@rk, hexyll, FZ, Professor Roger, Squeezebox, Zarvis, Mz. Brooklynn, Samantha, Alyssa, and Alisha. You all rock!

VILLAGES:

Hony and Paydreaux would like to thank Raze for stepping up and coordinating, and running the creator stages. Special shout out to br00zer for his master Goon Wrangling. Additionally we'd like to extend special thanks to F4ux and Zachadakka for their support as a seconds, as well as Nikita, Janet, and Dark Tangent for everything they do to make DEF CON a reality each year. We would like to extend a special thank you to Fl3x and Hunny for really stepping in and helping with the administrative stuff (you really are the best).

Hony, Paydreaux, Raze and the village team want to thank all the Village leads and organizers for everything they do to make DEF CON a huge success by bringing great villages and content here, for us to experience. Their year round dedication and sacrifice to the delivery of the exceptional content truly sets DEF CON apart from any other conferences. Thanks to KevOPs from Vendor/Exhibitor for helping to marry up additional support for various villages enabling their content and parties!

Special Thanks to LVCC, for giving us a home!

Thanks to the Goons:

Raze, br00zer, F4ux, Angel, Zachadakka, config, Griff, margraf, Sven, 0xn00b, Kamikze, FL3X, Aragorn, k4sp3r h4us3r, TallWireless, Tuh-kak-as, SpreadLove, M4N4TI, Gobl1n, Shammazon, 3p1nk13S, Cygnus, Medic51538, Ch3f, ether, Clutch, AnarKy, echo , JayaLamp, f0rk3d, KnightOwl, Se@ms, Binsby, Δ, Emphatic, DE11, Twiga, ch3at3r, kennashka

THANKS for all your time, help, and hard work!! Villages would not be possible without it.

"It's in that place where I put that thing that time."

WORKSHOPS:

Sinderz and Binary Buddha would like to thank our tireless Workshop goons: lawyerliz, mav, P1ll0wz, Jenn and Joel Cardella, Chrissy, Fallibile, RandomInterrupt, d3ada55, p0p3 and henry. We also want to express our gratitude for the Workshop Review Board for all their efforts and meaningful feedback.

We especially want to show our appreciation for all of the instructors who bring their energy to the classrooms. Thank you for sharing your expertise.

Never to be forgotten, we'd like to offer a huge hat tip of appreciation for the amazing folks and all the work they do that goes into making DEF CON happen every year, especially when facing the crazy unknowns that a new venue poses. DT, Nikita, Janet, Will, Neil, Darrington, IHR, QM, NOC, HackerTracker and SOC; thank you all for all the efforts both before, during and after the con.