
26
DEFCON
MAR



Welcome to DEF CON 33!

This is our second “all in one” conference in the LVCC, being able to see everyone at once was amazing and I expect no less this year!

DC 33 was complicated to plan for, with ever shifting tariffs, and uncertainty for many of our foreign speakers and content creators. Some didn’t apply, some cancelled, and we had to adapt. Even with that stress and uncertainty I sense the pent up energy, with almost 700 submissions to speak this year, a post COVID record. This is the fourth and final year of the Nautilus Institute hosting the DEF CON Capture The Flag contest, I wish all the best to them and the teams competing this year! It is also the final year of the DARPA AIxCC competition, check it out as it has evolved from last year.

In chaotic times flexibility and community are critical and so we are planning to launch more distributed services to support the community building on the success of defcon.social, we are in the middle of a network migration to make everything more portable, shop.defcon.org is getting revamped, and if you use Meshtastic we are testing https://mqtt.defcon.org. We have decided to review all our 3rd party apps and services to try and move to more OSS and less privacy invasive companies. If we are going to pay for an office suite I’d rather support LibreOffice than Microsoft Office. It will be many small steps toward strengthening and diversifying, and by next year I’ll share what we have accomplished!

Reflecting that the global hacking community is stateless by design we are launching new DEF CONs! This November we will hold a mini DEF CON in Bahrain to see what the Middle East community is like, and a DEF CON Singapore Beta next April to meet some South East Asia hackers!

Finally, DEF CON 33 would not be possible without the commitment and community of our HQ staff, over 700 Goons, 1,600 speakers, creators, artists, and the organizers of all cool con experiences. Thank you! What makes DEF CON unique is that it is a reflection of the community, and I greatly enjoy seeing what people have been up to. This con would be impossible without you, almost a year of planning happens now!

The Dark Tangent

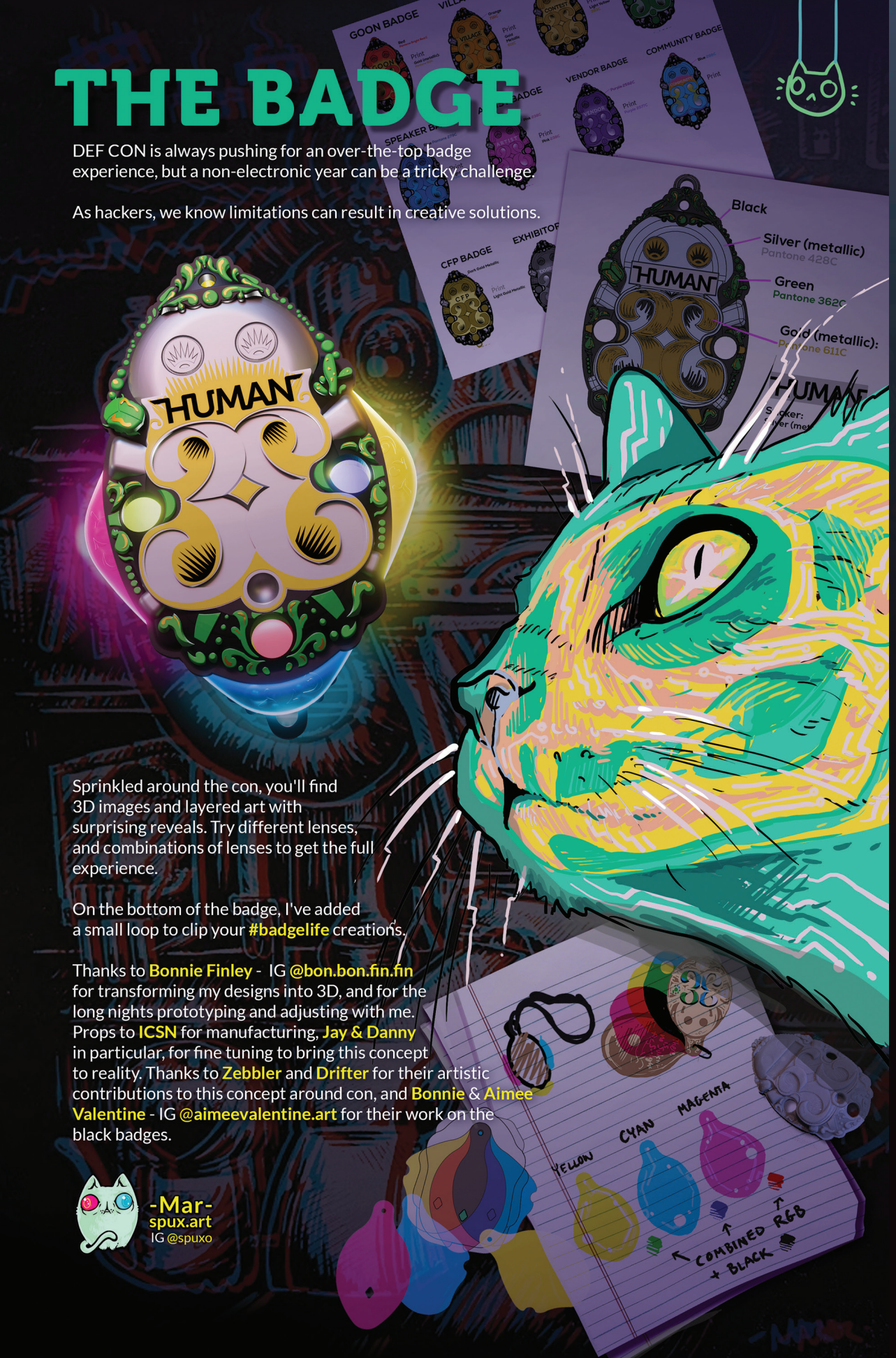
CONTENTS

4 BADGE
5 NETWORK & DCTV
6 CODE OF CONDUCT/HOTLINE
7 GOONS
8 COMMUNITIES
13 MOVIE NIGHT
14 PARTIES, MEETUPS, & EVENTS
17 MUSIC EVENTS
20 VILLAGES
30 AIXCC
35 HACKER JEOPARDY
36 CONTESTS
44 CTF
56 TALK SCHEDULE
64 CFP REVIEW BOARD
66 CREATOR STAGE TALKS
76 DEMO LABS
84 VENDORS
90 EXHIBITORS
94 CONFERENCE MAPS
96 THANK YOU!

THE BADGE

DEF CON is always pushing for an over-the-top badge experience, but a non-electronic year can be a tricky challenge.

As hackers, we know limitations can result in creative solutions.



Sprinkled around the con, you'll find 3D images and layered art with surprising reveals. Try different lenses, and combinations of lenses to get the full experience.

On the bottom of the badge, I've added a small loop to clip your **#badgelife** creations.

Thanks to **Bonnie Finley** - IG **@bon.bon.fin.fin** for transforming my designs into 3D, and for the long nights prototyping and adjusting with me. Props to **ICSN** for manufacturing, **Jay & Danny** in particular, for fine tuning to bring this concept to reality. Thanks to **Zebbler** and **Drifter** for their artistic contributions to this concept around con, and **Bonnie** & **Aimee Valentine** - IG **@aimeevalentine.art** for their work on the black badges.

-Mar-
spux.art
IG @spuxo

NETWORK

NETWORK INSTRUCTIONS

DEF CON 33! Another DEF CON eh! Like majestic cobra chicken awakening from a hangover, we've busted our butts to bring you the latest and greatest in network operations. The NOC has delivered this year's network in the shortest amount of setup time, and the questionable zero-trust network access for all conference floors.

What should you do in order to connect to Wi-Fi?

If you are a returning guest just do the same thing you did last year but with more confidence... if this is your first time as the person sitting next to you... great way to start a conversation :)... if you aren't much of a talker, then follow the steps at **https://wifireg.defcon.org**.

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**

So to recap

Defcon - (get a user/password and cert from https://wifireg.defcon.org)

Defcon-WPA3 - same as above

Defcon Open – I wouldn't but I hear the cool kids are there.

"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... seriously we work on this all year. 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.

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 post the best ones!

For updated information and instructions on how to connect to the Wi-Fi along with the link to download the digital certificate to be used, visit: https://wifireg.defcon.org.

For NOC updates visit https://noc.defcon.org , and also follow us on twitter or reddit. @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 33 CONVENTION MEDIA SERVER

All DC 33 Content is HERE

https://10.0.0.16/

or

https://dc33-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://dc33-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 33 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 33 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 33 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

.EDU COMMUNITY

Level 1 - Hall 4 - C201

edudefcon.com

Our staff share experiences from across the vast spectrum of modern education: Universities, K12, Government Agencies, Continuing Education, Clubs, Sports, and so on. We will have workshops and panels to help explain the best practices for educational tech, esports, help desks, emergency preparedness, remote learning, and many more. Please come join us at the EDU Community! Our goal is to provide hands on experience over lecture learning.

BADGELIFE

Level 1 - Hall 4 - C204

badge.life

It's finally here - a proper home for all things Badgelife on the con floor! This is our first year so bear with us, but we have big goals: This year we'll be starting an effort to create the Badgelife Museum, a collection of current and former community-made badges, including SAO's, on display at con! Donate your own badges and SAOs you've made or collected to the museum, and see them come back to con year after year.. or bring what you've got to trade with the community via our "take-one, leave-one" SAO Trading Wall, or our in-person Badge Trading meetups! If you're interested in making Badges or SAOs yourself, we will have lots of interesting badge creators around showing off their work and giving workshops or lightning talks on their methodologies. Come learn from the best and meet your favorite creators at our various Badgemaker Meetups! Before and after con, you can find our Discord (and what will be our upcoming online Badge Archive) at http(s)://badge.life. Closer to con we'll post our schedule for any con workshops, talks or activities on the site as well, so check there for meetup times. Hope to see you at the community!

BBWIC FOUNDATION

Level 1 - Hall 4 - C104

www.bbwic.com

The BBWIC Foundation is a non-profit organization with a mission to empower women in the field of cybersecurity. Their goal is to provide a safe space for women in the industry to grow, build confidence, manage work stress, and evolve as leaders in the ever-changing technology landscape of cybersecurity. They believe in sparkle leadership, encouraging every woman to aim higher and achieve more. Founded in 2021 and governed under the Canada Not-for-profit Corporations Act, BBWIC Foundation actively supports women across North America, Europe, and Asia. Through mentorship, networking, and educational initiatives, we champion diversity, equity, and inclusion in the cybersecurity domain.

CODE BREAKER

Level 1 - Hall 4 - C207

Given DEF CON 33's theme of Access Everywhere, Code Breaker Village emphasizes accessibility, inclusivity, and security in codebreaking which coincides with a fun challenge and a pool party.

CRYPTOCURRENCY COMMUNITY

Level 1 - Hall 4 - C101

www.cryptocurrencyvillage.cc

The Cryptocurrency Community welcomes you to discover and develop your blockchain finance technology hacking skills. Learn the unique ways that cryptocurrency systems are attacked, defended, and secured while building new applications using testnet tokens. Meet hackers, be entertained, and get inspired to explore cryptocurrency where practical finance hacking for the public good is encouraged.

Our mission prioritizes education of computing enthusiasts curious about the hype of cryptocurrency and our community discusses the challenges facing modern day finance technology. Workshops and challenges offer you the experience of mentored participation in a well equipped and comfortable environment. The community inclusively welcomes all cryptocurrency projects and their cousins from other blockchain based communities. Come hack with us!

DC MAKER'S COMMUNITY

Level 1 - Hall 2 - 801

dcmakerscommunity.com

The DC 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.

DC NEXTGEN

Level 2 - W230 (DC NextGen)

dcnextgen.org

DEF CON Next Gen is DEF CON's official youth track, designed to help kids and teens ignite and grow their passion for cybersecurity. In collaboration with DEF CON villages and communities, DCNextGen offers a wide range of content, hands-on workshops, and exciting challenges that jumpstart young attendees' cyber journeys. We host CTF competitions, have our own interactive electronic badge, and create the perfect environment for youth to connect, learn, and build lifelong friendships.

DCNextGen events are for youth 8-18.

DDOS COMMUNITY

Level 1 - Hall 4 - C202

DDoS attacks aren't just theory—they're an everyday grind for defenders. While the tech world throws around buzzwords and papers, we're here to talk real-world war stories, hands-on mitigation, and what actually works when the bits hit the fan.

The DDoS Community at DEF CON is where defenders unite—through talks, workshops, and contests that dive into evolving threats, busted botnets, and the clever tricks that keep services online.

We're not just about packets and filtering. We hit the business, legal, and strategic angles too—because the impact of DDoS goes way beyond the edge router.

Come hang out, level up your defense game, and swap notes with folks who've been in the trenches. Whether you're a blue-teamer, researcher, or just DDoS-curious, there's a place for you here

DEF CON ACADEMY

Level 2 - W235

ctf.defcon.academy

Through this Community, attendees will be invited to learn about Capture the Flag competitions and try their hands at challenges hosted on the pwn.college platform. They will have the opportunity to learn fundamental hacking skills, including Linux basics, binary exploitation, reverse engineering, and web security, all while progressing through exercises designed to build expertise. With on-site mentorship from experienced hackers and top CTF players, attendees can receive guidance, troubleshoot challenges, and gain insights into real-world security problems. Beyond the technical learning, the event offers a chance to connect with like-minded individuals and engage with the broader cybersecurity community. Whether a beginner or an experienced player, attendees can expect an interactive, educational, and engaging experience tailored to developing practical hacking skills.

DEF CON GROUPS (DCG)

Level 2 - W237

defcongroups.org

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)

DCG VR Space

dcgvr.org

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.

HACKERS WITH DISABILITIES (HDA)

Level 2 - W219

A place for people with disabilities to hear talks aimed at hacking disabilities / gear / specific topics on security and safety. To have a place to recharge assistance devices, get assistance with disability issues, to have a safe space to retreat should things get to be too much, to form community bonds with other hackers with disabilities and to be an educational outreach and support system showing that just because you have a disability you can still be a hacker and part of the community. Also a break area for service animals, and people with sensory issues.

HACKERS.TOWN

Level 1 - Hall 4 - C102

hackers.town

We intend to do some short lightning talks from members of the town and friends of town, which will double as a casual get together also with a loRa/Meshtastic clinic\workshop to get everyone working with their radios. This supports our objective of understanding, experimenting, and promoting the use cases for distributed networks.

MESH THE PLANET!

HARD HAT BRIGADE

www.hardhat.rocks

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. 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!

COMMUNITIES

ILLUMICON

Level 1 - Hall 4 - C103

Humans of DEF CON, welcome to IllumiCon – a place for lasers, LEDs, and all things blinky!

For our inauguration year; we want everyone to experience lasers, addressable LEDs, and some of the myriad ways you can use them.

Have you ever wanted to perform a laser show in front of thousands of people? Stop by IllumiCon to learn how to program a laser show, play with beautiful special effects, or shoot lasers around LVCC!

Have you ever wondered how people make awesome LED clothing, hard hats, or holiday displays? We will teach you what hardware and software can be used to set up a display along with tips and tricks to make it your own. Now is your chance to learn something new with demos and hands-on interactions with equipment usually only operated by a select few.

Stop by the IllumiCon community to show off your handiwork! Bring your creations for all to see.

Knowledge will refract, minds will reflect; and through the prism of newly-discovered purpose, the future will shine bright. Remember, when times are dark: Hackers light the way!

LA VILLA

Level 2 - W220-W221

lavillahacker.com

Bienvenidos a La Villa at DEF CON—where the pulse of Spanish and Portuguese cybersecurity beats loud and proud! Attendees can dive into a vibrant showcase of Spanish- and Portuguese-speaking talent, featuring electrifying talks on cutting-edge hacking techniques, hands-on workshops to sharpen your skills, and creative showcases that blend culture with code. Expect to learn from top-tier Latino hackers as they unveil innovative exploits, share insider knowledge, and spark collaboration—all in Español and Português. Participate in networking sessions that connect you with a passionate community, or join the stage to pitch your groundbreaking ideas. La Villa isn't just a space—it's a launchpad for Hispanic and "Bienvenidos a La Villa at DEF CON—where the pulse of Spanish and Portuguese cybersecurity beats loud and proud! Attendees can dive into a vibrant showcase of Spanish- and Portuguese-speaking talent, featuring electrifying talks on cutting-edge hacking techniques, hands-on workshops to sharpen your skills, and creative showcases that blend culture with code. Expect to learn from top-tier Latino hackers as they unveil innovative exploits, share insider knowledge, and spark collaboration—all in Español and Português. Participate in networking sessions that connect you with a passionate community, or join the stage to pitch your groundbreaking ideas. La Villa isn't just a space—it's a launchpad for Hispanic and Portuguese speakers' brilliance, proving that talent knows no borders. Get ready to hack, connect, and shine!" brilliance, proving that talent knows no borders. Get ready to hack, connect, and shine!

LONELY HACKERS CLUB

Level 2 - W201-W202

lonelyhackers.club

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.

LOONG COMMUNITY

Level 1 - Hall 4 - C203

"Loong Community," founded by the creator of DEF CON's iconic **Chipoff Village** and **Variety Exploitation Village**, returns to continue its legacy of blending hardware hacking rigor with cultural storytelling. This year's iteration draws inspiration from the *loong* (Chinese dragon), symbolizing power, wisdom, and transformation, while honoring a decade of pioneering work in chip forensics, firmware exploitation, and adversarial hardware design.

MEMORIAL CHAMBER

Level 3 - W302

The DEF CON Memorial Chamber serves as a sacred space within our community — a place where we pause to honor those hackers whose brilliance and dedication have elevated not just our craft, but the entire security ecosystem. Here we remember figures whose generous spirit and willingness to coordinate security fixes demonstrated that true hacking greatness lies in collaboration. We are here because DEF CON has been the beating heart of the hacker community for over three decades, growing from 100 people in 1993 to the world's largest hacker conference. As Jeff Moss envisioned, DEF CON is what we make of it, this memorial space represents our commitment to ensuring that the legacy of those we've lost continues to inspire future generations of hackers to pursue knowledge, build community, and use their gifts to make the world better.

MOBILE HACKING COMMUNITY

Level 1 - Hall 4 - C106

mobilehackingcommunity.com

At the Mobile Hacking Village, attendees will learn about the latest trends in mobile application security through hands-on experiences, including topics such as bypassing security mechanisms and hardening techniques like SSL pinning, and exploiting known CVEs.

Additionally, attendees will engage in a competitive process by participating in an onsite CTF (Capture the Flag) event to test their skills, face new challenges, and learn new skills.

Attendees will also have the opportunity to watch cutting-edge research presentations and case studies on various topics within the domain.

Our Village will further engage users through small demonstrations to familiarize them with the parts of mobile devices using disassembled devices, and other interesting aspects.

NIX VEGAS COMMUNITY

Level 1 - Hall 4 - C209



nix.vegas

In a world full of unwanted app updates and SaaS providers who want your personal information, being able to self host one of the largest collections of software on the planet in a stable way across updates with NixOS has the potential to change the game for anyone who's tired of the slow decline of cloud services. With a single line of code, you can deploy self-hosted services repeatably across as many machines as you want.

Even if you don't run NixOS, building software with Nix allows you to deploy it across different Linux distributions and architectures. No longer do you have to build entire distributions into Docker images or flatpaks that bitrot - Nix can do that too, and it can do it over and over again. Set up a development shell to provide friends or coworkers access to dev environments, and build your software the same way every time, with upwards of 120,000 packages you can leverage.

Access to services and software everywhere: that's Nix. Welcome to Nix Vegas, where we want to rebuild the world.

NMDP (Formerly Be The Match)

Level 1 - Hall 4 - C100

Be the Match is returning to DEF CON for its 12th year, to run a registry drive for the National Marrow Donor program! Swing by and check out one of the coolest biohacks out there, and how you could be the next person to save a life!

NOOB COMMUNITY

Level 2 - W204



noobvillage.org

We're here to tear down the barriers that make cybersecurity feel intimidating. Whether you're brand new, pivoting from another career, or just curious, the Noob Community creates welcoming, hands-on spaces to explore hacking, ask questions, and connect with others starting their journey. No gatekeeping. Just learning, support, and a place to belong.

OPERATING SYSTEMS COMMUNITY

Level 1 - Hall 4 - C210

osvillage.com

The OS Community is the perfect destination for anyone passionate about the building blocks of hacking: operating systems. This community isn't just about what's under the hood; it's about cracking it open, rethinking it, and optimizing it for innovation. Attendees will experience an interactive hub where they can dive into OS development, discover open-source platforms, and learn how operating systems can be tailored for security, performance, and creative hacking.

OWASP

Level 1 - Hall 4 - C206

owasp.org

OWASP, the Open Worldwide Application Security Project, is an open source steward of tools, documents, and resources all underpinned by our community. People are the fabric that composes the OWASP community from developers, security pros, hobbyists, students & hackers and we are eager to welcome all at DEF CON 33.

QUEERCON COMMUNITY LOUNGE

Level 3 - W325

queercon.org

Queercon's mission is to raise awareness and promote acceptance of LGBTQIA+ individuals in the IT and infosec industries. We create space for queer people to meet, engage, and network through our badges, puzzle challenges, and meet-up events - all designed to help queer people find community where they are not alone. The Queercon Community Lounge is a place to find community anew, or return to familiar faces. Keep an eye on Hacker Tracker or queercon.org for our schedule of meetups and challenges!

RETRO TECH COMMUNITY

Level 1 - Hall 4 - C205

retrotech.club

The Retro Tech Community is back! We're here for our 2nd year to celebrate where we came from, how computers and technology of yesteryear shaped our lives, and to show how the first generations of computers still have an impact on and a place in today's world. Rather than a stuffy collection of museum exhibits you can't touch or breathe on, our goal is to be fully interactive! We encourage the DEF CON community to take part by bringing in working examples of old (or new but retro-inspired) technology to display, demonstrate, be passionate about, teach lessons on, and allow those who visit us to goof around with. We love to see people indulge their inner nostalgia nerd. Bring us your tired capacitors, your scratched cases, your huddled masses of cartridges and expansion cards 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 120V circuits beside the golden door! Walk-ins are welcome to long as you have a plan to store or bring it back home should we be out of display room :) Broken items are welcome as well - come start an impromptu repair party! We're confident that smart and inquiring minds will be around to help you solve issues, and we'll lend equipment where we can. Bring and show off your rare and weird vintage machines or retro consoles, or disks and cartridges of your favorite childhood games! All circuits are welcome here. Note: Due to staffing limitations, hours may fluctuate, but we will do our best to stay open for as much of con as we can. If you miss us, check back soon! If you wish to support our efforts, display something, or donate hardware, please coordinate with reanimationxp (at) gmail.com, subject "Retro Tech Community"!

THE DIANA INITIATIVE'S COMMUNITY ROOM

Level 2 - W205

www.dianainitiative.org

In our collaborative area we will be hosting birds of a feather conversations, small round table discussions, and more.

Our reference desk can help you come up with a plan before going back out into DEF CON, if you would like. The reference desk will work to find and connect you with the amazing events and communities at the conference, as well as in the community at large, that are best suited to your interests.

Finally, for those who find it hard to dive into something new alone, we will be offering small tour groups to take people around to various villages, contests and communities.

COMMUNITIES

THE DIANA INITIATIVE'S QUIET ROOM

Level 2 - W206

www.dianainitiative.org

Diana Initiative is excited to offer up a "Quiet Room". This room is a library vibes environment where people can calm down or recharge before going back out to experience more DEF CON, or even safely have a meltdown, stim, and take time to recenter. In our library area we will have fidget toys, coloring pages and more.

VETCON

Level 3 - W327

vetconactual.com

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)

WOMEN IN SECURITY AND PRIVACY

Level 1 - Hall 4 - C208

www.wisporg.com

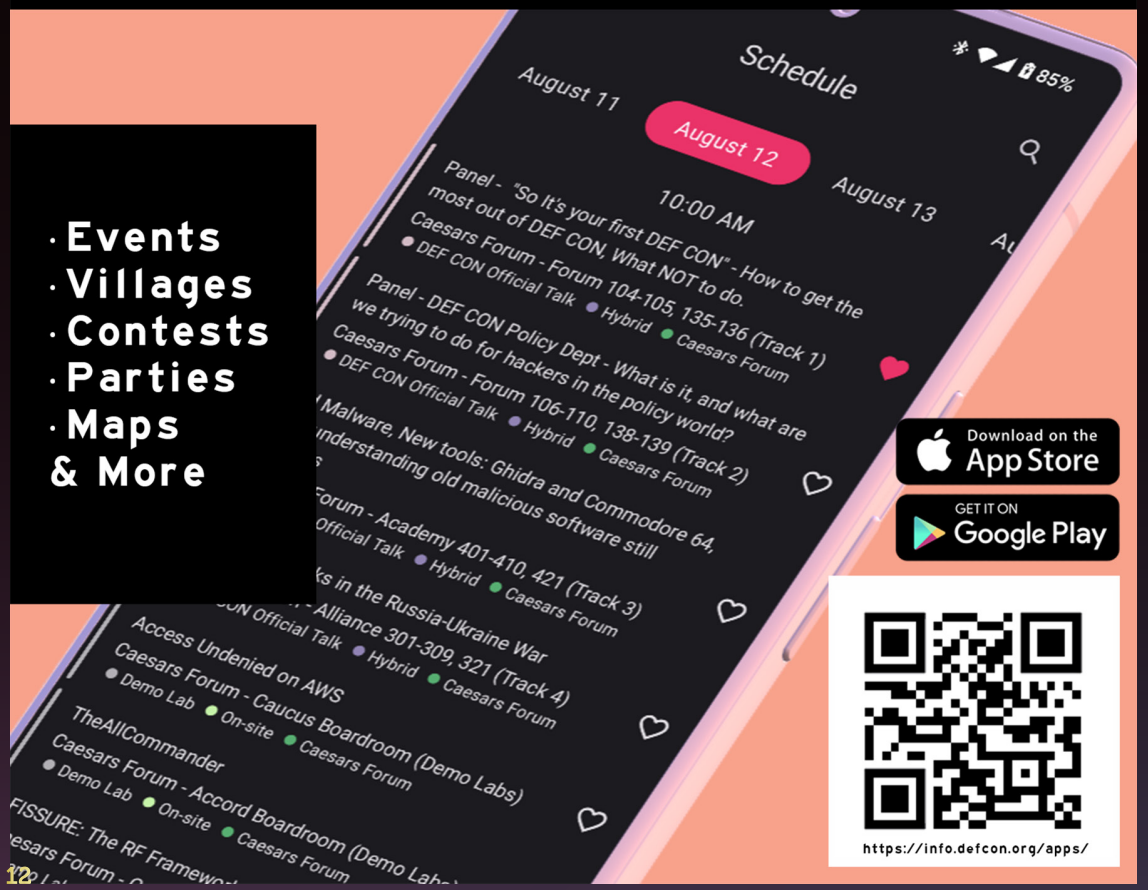
Women in Security and Privacy (WISP)'s mission is to advance women and underrepresented communities to lead the future of privacy and security. We accomplish this by providing women and underrepresented communities with opportunities for technical and professional development through events, trainings, 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

- Events
- Villages
- Contests
- Parties
- Maps
- & More



Download on the App Store

GET IT ON Google Play

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

DEFCON MOVIE NIGHT

FRIDAY



ANIARA

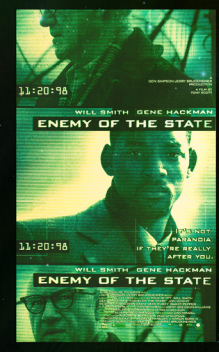
EARTH HAS BEEN RENDERED UNINHABITABLE, PROMPTING MASS MIGRATION FROM EARTH TO MARS. WHEN ONE SUCH ROUTINE TRIP VEERS OFF COURSE, THE PASSENGERS OF THE ANIARA STRUGGLE TO COPE WITH THEIR NEW LIVES.



PROSPECT

A TEENAGE GIRL NAMED CEE AND HER FATHER DAMON LAND ON A POISONOUS FOREST MOON TO MINE FOR VALUABLE GEMS. A SERIES OF BETRAYALS, ALLIANCES, AND CONFLICTS WITH MERCENARIES AND RIVAL PROSPECTORS MAKE THEIR QUEST INCREASINGLY PERILOUS.

SATURDAY



ENEMY OF THE STATE

A LABOR LAWYER BECOMES THE TARGET OF A COVERT SURVEILLANCE OPERATION AFTER UNWITTINGLY RECEIVING EVIDENCE OF A POLITICAL ASSASSINATION. GENE HACKMAN CO-STARS AS A FORMER INTELLIGENCE OPERATIVE WHO HELPS HIM EVADE THE ROGUE AGENTS.



SUNSHINE

A GROUP OF ASTRONAUTS ABOARD THE ICARUS II ARE SENT ON A DANGEROUS MISSION TO REIGNITE THE DYING SUN.

8PM, N257 NORTH HALL

PARTIES, MEET-UPS & EVENTS



+61: THE AUSTRALIAN EMBASSY

Party on Friday from 22:00 to 02:00 on Level 2 - W208

Have you ever tried Vegemite or like conversing in a foreign language? Do you miss familiar twangs or water flowing down a sink in the right direction? +61: the Australian Embassy is the meetup just for you. Every year a few random Australians end up coalescing around an inflatable kangaroo somewhere in the halls and this year we decided to get our shit together and find a place to catch up, share notes, reminisce about your adventure to the Bass Pro Shop and complain about the jetlag. Feel free to join us (or dont) as we catch up on the happenings of hacker summer camp.



ARCADE PARTY

Party on Friday from 21:00 to 02:00 on Level 2 - W228-W229

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



BIC VILLAGE GAME NIGHT

Party on Friday from 18:00 to 22:00 on Level 3 - W322-W324

Gamers Unite! Come join the BIC Village team to engage with one another, unplug and find some friendly competition! Whether you're into board games, card games or classic party games, there's something for everyone here. Bring your game face and get ready for a night of fun, laughter and connection.This event will feature different board games such as Jenga, Uno, Spades, Ludi and more from around the African Diaspora and Black American culture!



BLANKETFORT CON

Party on Friday from 19:00 to 01:00 on Level 2 - W231-W232

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!



CALL CENTER VILLAGE PARTY

Party on Saturday from 22:00 to 02:00 on Level 2 - W210

Join Call Center Village at Party Line, a carefully-crafted telephony-themed party open to all DEF CON 33 attendees. Help us celebrate the human operators who keep call centers and answering services private, usable, and accessible. Between the illuminated telephone decorations and the sponsor-supplied drink-ticket drops, you're bound to find something to dial up the fun.



CYBERDELIA RAVE

Party on Saturday from 21:00 to 02:00 on Level 2 - W228 (Creator Stage 4)

DEF CON's first-ever race: Expect to hear hardcore, happy hardcore, breakcore, speedcore, hardstyle. Bring your phat pants, kandi bracelets, and nine inch nails (on finger) to this once in a lifetime rave.



DAY OF THE DEAD HACKER PARTY

Party on Saturday from 21:00 to 02:00 on Level 2 - W229 (Creator Stage 5)

For all people that want to hang out and celebrate the lives and death of influential people to the hacker community. Attendees are encouraged to dress to kill in Day of the Dead attire or any attire that includes dead heroes. Music will be provided by CURZES and special guest DJs.

Everyone is welcome to join us and celebrate the dead!



DC BOOK CLUB DISCUSSION

Event on Saturday from 14:00 to 16:00 on Level 2 - W237

Community is essential and so is continual learning. Reading and discussing books can greatly impact an individual's access and sense of community and knowledge. This DEF CON book discussion will be an accessible group aiming to build community and share out learnings, all in a quieter setting. Come join us in person and discuss what you've been reading. This DC Book Club is not locked to a region and we're around all year on Discord, where we discuss books and other topics. This meetup is for those who love books and escaping to the cyperpunk, scifi worlds that inspire DEF CON and our future. Come join us!



DC NEXTGEN

Party on Saturday from 19:30 to 23:00 on Level 2 - W230 (DC NextGen)

DCNextGen event for youth 8-18 only. The DC NextGen youth party is the perfect place to loosen up and have fun with other kids and teens your age! There is no better time to hang out and chat with the new friends you've made here. All while enjoying fun games and cyber themed activities. Are you ready to build a team and hack the planet?



DC404/DC678/ DC770/DC470 (ATLANTA METRO) MEETUP

Meetup on Friday from 20:00 to 23:00 on Level 2 - W210

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!



DC702 MEETUP

Meetup on Thursday from 19:00 to 21:00 on Level 2 - W237

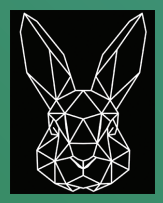
Join the local DC702 Group in this year's official DEF CON Meetup! The meetup will be casual and include typical meetup activities (e.g., socializing, "challenges," lockpicking, music, etc.) and maybe a few little surprises.



DEF CON HOLLAND GROUP PRESENTS: DRINKING WITH THE DUTCH

Meetup on Thursday from 16:00 to 19:00 in Other / See Description

"Drinking with the Dutch" at DEF CON is a perfect moment to talk about what your favourite 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.



DEFCON.RUN

Event on Thursday-Sunday from 06:00 to 08:00 in LVCC West Hall North Entrance

DEFCON.run is a beloved tradition at DEF CON, bringing together hackers for a refreshing start to the day. Originally known as the DEF CON 4x5K, the event has evolved into a distributed, community-driven experience featuring fun runs and rucks across Las Vegas. Participants can choose from various routes, ranging from simple 5Ks to more ambitious distances.

For DEF CON 33, the gathering point is "The Spot" by the North Entrance of the Las Vegas Convention Center West Hall. Here, the real wild hares gather before the sun has a chance to burn up this city of sin. The runs kick off at 06:00 Thursday through Sunday! But be there early for hype talks and shenanigans. We also have a whole new Meshtastic setup and website features we're adding. There are other runs swag drops and social meetups planned throughout the day and night as well!

Whether you're a seasoned runner or looking for something different, defcon.run offers a unique way to connect with other hackers and kick off your day. For more details and to sign up, visit defcon.run.



FREE HAM RADIO EXAMS

Event on Friday from 13:00 to 16:00 on Level 3 - W320

Saturday from 11:00 to 17:00 on Level 3 - W320

Sunday from 11:00 to 13:00 on Level 3 - W320

The Ham Radio Village is excited to return to DEF CON 33, offering you the opportunity "Access Everything" by gaining you access to the airwaves though free amateur radio license exams! Ham radio has a long history with ham radio operators being considered the original electronic hackers, innovating long before computers, integrated circuits, or even transistors were invented. The Ham Radio Village keeps this spirit alive by providing free ham radio license exams at DEF CON.

In today's world, wireless communication is essential. A fundamental understanding of radio technology is more important than ever. Earning your amateur radio license opens the door to the world of amateur radio, providing you with valuable knowledge of radio frequency (RF) technology. This knowledge can be applied to a wide range of other RF-related topics, including RFID credentials, Wi-Fi, and other wireless communication systems.

FRIENDS OF BILL W



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

Meetup on Sunday from 12:00 to 13:00 on Level 3 - 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 33 has you covered. Join us throughout the conference in the Friends of Bill W Community Space in W301.

PARTIES, MEET-UPS & EVENTS

GOTHCON

Party on Saturday from 21:00 to 02:00 on Level 2 - W231-W232

Returning for their 8th 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.

HACKER KARAOKE

Event on Friday from 19:00 to 02:00 on Level 2 - W211-W212

Event on Saturday from 19:00 to 02:00 on Level 2 - W211-W212

Two great things that go great together! Join the fun as your fellow hackers make their way through songs from every era and style. Everyone has a voice and this is your opportunity to show it off! Everyone is encourage to participate in a DEF CON tradition from all folks and skill levels.

IOT VILLAGE 10TH BIRTHDAY PARTY

Party on Friday from 21:00 to 00:00 on Level 2 - W233 (Creator Stage 1)

IoT Village is turning 10! Join us for a celebration of 10 years of hacking all of the things at DEF CON. Stop by for birthday cake, exclusive stickers, prizes and giveaways, and did we mention cake?

LAWYERS MEET

Meetup on Friday from 18:00 to 21:00 on Level 2 - W209

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.

QUEERCON MIXER

Meetup on Friday and Saturday from 16:00 to 18:00 on Level 3 - W325

Come meet the largest social network of LGBTQIA+ and allied hackers at Queercon! Our mixers are designed for you to meet, network, and engage with like-minded people to a backdrop of music, dance, and refreshments.

SPADES TOURNAMENT & GAME NIGHT SOCIAL

Party on Friday from 18:00 to 21:00 on Level 3 - W322-W324

Join Us for the Ultimate Spades Tournament & Game Night Social! Looking for a fun way to unwind, connect, and enjoy some friendly competition? Our Spades Tournament & Game Night Social is the perfect way to relax while engaging in a classic card game that brings people together.



STICKER SWAP AT DEF CON 33

Meetup on Saturday from 14:00 to 16:00 on Level 2 - Corridor Near W234

You've seen us swamp chillout areas guerilla style with tables full of stickers, but now we finally got our act together and have a formal place and time. Come swap stickers, chat with creators, and join the growing subculture of sticker lovers. Follow @ dcstickerswap on Twitter for updates.

THE ILLUMINATI PARTY

Party on Saturday from 21:00 to 02:00 on Level 2 - W233 (Creator Stage 1)

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!

THE JASMINE DRAGON

Party on Saturday from 20:00 to 00:00 on Level 2 - W208

Step into The Jasmine Dragon, an exclusive underground gathering where tradition meets the digital age, and the beat flows like perfectly executed code. With DJ Iroh dropping martial arts-inspired hip-hop, expect deep cuts, heavy bass, and an atmosphere that fuses cyberpunk aesthetics with ancient strategy. This isn't just a party—it's a cipher, a meeting of minds where warriors and tacticians alike can connect, scheme, and unwind. But entry isn't for just anyone; only those who hold the right Pai Sho tile will unlock the door to this hidden node.



THE UNOFFICIAL DEF CON SHOOT

Event on Wednesday from 11:00 to 18:00 in Other / See Description

The DEF CON Shoot is a public event that happens just prior to the DEF CON hacker conference in Las Vegas, Nevada. It is an opportunity to see and shoot some of the guns belonging to your friends while taking pride in showing and firing your own steel, as well, in a relaxed and welcoming atmosphere. We choose a spot, then we rent tables, canopies, and bring all the necessary safety equipment and amenities. All you need to bring yourself and (optionally) your firearms. New shooters and veterans both attend regularly. You can attend with your firearms, of course, but folk without guns of their own in Vegas may have the opportunity to try gear from others in attendance. Admission costs are intentionally kept low, just so we can break even on expenses for the amenities provided.

Offsite - Pro Gun Vegas Address: 12801 US 95 South. Boulder City, NV 89005

TOXIC BBQ

Event on Thursday from 15:00 to 21:00 in Other / See Description

Join the humans of Vegas at the next inCARNEtion of your Thursday welcome party. Enjoy fewer walls and more garden as we meet AFK in the shade of Sunset Park. Burgers and dogs are provided; you bring everything else (specialties, drinks, labor, and donations). We're expanding our grills to over 40 sq ft of heat with space for veggies and your own personal creations.

Grab flyers from an Info Booth after Linecon, or watch #ToxicBBQ on the socials for the latest news.

Offsite @ Sunset Park, Foxtail Pavilion (36.0636, -115.1178)

UM, ACKTUALLY...

Event on Friday from 16:00 to 18:00 on Level 1 - Atrium-East - Contest Stage

"Um, ACKtually" is a hacker twist on an established gameshow hosted by Dropout TV (Um, Actually). In this show, contestants are read a short statement about film, television, literature, etc. which contains one incorrect detail. The contestants must buzz in with the correction, preceded by the phrase "Um, Actually". In DEF CON's version, these statements are all related to tech / cybersecurity. Anyone who has spent any amount of time on social media, knows how much hackers love to correct each other!

Come watch some of your favorite hacking personalities publicly weaponize mansplaining for your entertainment!"

VETCON 2025 PARTY

Party on Saturday from 21:00 to 02:00 on Level 3 - W327

DEF CON is renowned for bringing together some of the brightest minds in technology and security. By participating in VETCON, you have the chance to highlight the critical role veterans play in this landscape and explore how technology can support and enhance their lives.

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

Meetup on Friday from 21:00 to 23:30 on Level 2 - W205

We'd love to get all the gender non conforming, non-binary and women together to hang out and make friends! DEF CON is better with friends. Stop in for a bit, or the whole time.

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

MUSIC
(NON-STOP)

CHILLOUT ROOM
MAIN STAGE
FIRST FLOOR, 106-110

THURSDAY
20:00 - 21:00 - HECKSEVEN
21:00 - 22:00 - FLING
22:00 - 23:00 - N8
23:00 - 00:00 - PALINURO
00:00 - 01:00 - DJ HUSK3
01:00 - 02:00 - STITCHAROO

SATURDAY
20:00 - 20:30 - 0XDADE
20:30 - 21:00 - DUAL CORE
21:00 - 22:00 - DJ NULL
22:00 - 23:00 - PATATTACK
23:00 - 00:00 - MISS JACKALOPE
00:00 - 01:00 - SYNTAX+LUNA
01:00 - 02:00 - DJ XORAC

FRIDAY
20:00 - 21:00 - ELIPSCION
21:00 - 22:00 - DAEMON CHADEU
22:00 - 23:00 - DJ SCYTHE
23:00 - 00:00 - SKITTISH & BUS
00:00 - 01:00 - TRIODE
01:00 - 02:00 - MAUVEHEAD

ROAMING DJ
ICETRE NORMAL
TRAX
DOTORNOT

TECHNOPOP

VILLAGES

ADVERSARY VILLAGE

Level 1 - Hall 2 - 702

adversaryvillage.org



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

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, offensive tradecraft to engage and educate the community.

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 Tabletop Game

Adversary adventure is a story-scenario based, interactive, cyber war-gaming, 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.

Hands-on guided breach and offensive attack simulation exercises

This area will feature guided attack simulation exercises for participants to engage with. There will be a few scenario-focused activities, “Breach-the-Hospital”, “Breach-the-Office”, “Breach-the-Bank” etc., visually represented by modular-brick-LEGO sets. A simulated cyber range will be available for each scenario, providing an exact replica of an enterprise production environment. We will provide a detailed walkthrough of the attack scenarios, including Tools-Techniques-and-Procedures, commands and how-to guides, demonstrating how to attack and breach the target environment.

This exercise will give participants a clear understanding of how threat actors infiltrate corporate environments.

Adversary Wars CTF

Adversary Village will be hosting “Adversary Wars CTF”, 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 challenge scenarios and challenges, where the participants can perform various attacks and learn new TTPs. To visualize the CTF environment, the contest area will feature a miniature model of the city made using interlocking-plastic-bricks. The breached components will be physically marked in the city model as the CTF progresses.

There will be prizes, complimentary hoodies (yes, the iconic adversary village hoodies), free t-shirts, cool stickers, village coins, badges, and various other swags.

AEROSPACE VILLAGE

Level 1 - Hall 2 - 503

www.aerospacevillage.org

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

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

Our Goal

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

AI VILLAGE

Level 3 - W314-W316

aivillage.org

Join us at the AI Village for interactive demonstrations at the intersection of AI and security. We’ve got something new this year with a full purple team demonstration from the AI Cyber League.

For the third Generative Red Team we are going to “red team” the evaluations that establish a model’s performance. We are bringing several model systems built to do different tasks each with their own model card. These model cards will define uses and restrictions the model creators want and determine what we mean by “trust” when it comes to fuzzier concepts like “can write good Rust” and “doesn’t help you hack”. This model card will be built off of open source evaluations that prove and establish how effective the model is. We will be paying bounties for findings against the evaluations that the model cards used to make their claims.

Following the success of last year’s real-time deepfake demonstrations, we’re taking things to the next level. This year, we’re showcasing five different deepfake systems across a spectrum of computational requirements – from high-end professional setups to consumer-grade hardware that’s becoming increasingly accessible. You can see how detections we have will break down as compute per dollar keeps improving.

APPSEC VILLAGE

Level 1 - Hall 2 - 604

www.appsecvillage.com/

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

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

AppSec Village welcomes all travelers to choose from talks and workshops by expert community members, an all-AppSec-focused CTF, contests that challenge your mind and your skillz, and more. Bring your thirst for knowledge and passion for breaking things, and your visit to AppSec Village will be thrilling!

VILLAGES

ARTIFICIAL INTELLIGENCE CYBER CHALLENGE (AIxCC)

Level 1 - Hall 1 - 404

aicyberchallenge.com/

The AIxCC Finals will unfold at DEF CON 33 in August 2025. The top seven teams who qualified during Semifinals will compete for a grand prize of $4 million.

The AIxCC Final Competition will introduce new challenge repositories and vulnerabilities, encouraging teams to improve upon their current CRS implementations and push forward their systems' capabilities in terms of robustness, scale, and real-world impact.

BLACKS IN CYBER VILLAGE

Level 3 - W322-W324

www.blacksincyberconf.com/bic-village

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.

In doing this, we believe that we can better educate and normalize the discussion of deficiency or prejudices in Cybersecurity education/development for minority communities. We also believe this effort can be translated to aid in eradication of these issues in the Cybersecurity and Hacker/Maker community and allow for more diverse hobbyists and professionals to engage and contribute.

BIOHACKING VILLAGE

Level 1 - Hall 2 - 606

villageb.io

At the Biohacking Village, attendees can expect an immersive, hands-on experience at the intersection of cybersecurity, healthcare, and medical technology, offering opportunities to learn, explore, and collaborate on some of the most pressing challenges in the industry.

What Attendees Can Learn at the Biohacking Village:

1. Medical Device Security: Understand how medical devices work, the cybersecurity vulnerabilities they face, and the critical importance of securing these devices for patient safety and national security. Participate in hands-on demonstrations, such as penetration testing on virtualized devices, learning real-world techniques for identifying and addressing vulnerabilities.

2. Critical Infrastructure Resilience: Explore the intersection of healthcare and critical infrastructure, including how hospitals and medical systems rely on interconnected technologies. Learn about best practices for securing healthcare networks, including strategies to mitigate ransomware attacks and manage incident response.

3. Collaboration and Ecosystem Development: Discover how to work effectively with manufacturers, regulators, researchers, and practitioners to build secure and innovative healthcare technologies. Engage in discussions about fostering trust, transparency, and accountability within the cybersecurity and healthcare communities.

4. New Technologies in Healthcare: Get hands-on with cutting-edge innovations, such as AI-driven medical devices, digital twins, and IoT-enabled healthcare systems. Learn about emerging regulatory requirements, including those surrounding AI, cybersecurity, and the EU Cyber Resilience Act (CRA).

5. Ethical Hacking and Vulnerability Disclosure: Delve into the principles of responsible disclosure and how ethical hackers contribute to securing patient safety. Understand the legal and ethical considerations of hacking medical devices, guided by frameworks like the Hippocratic Oath for Hackers.

6. Policy and Regulatory Insights: Gain insights into the latest global regulations, standards, and metrics impacting medical technology, such as FDA guidelines, GDPR, NIS2, and more. Participate in workshops and panels with experts discussing policy advocacy and global harmonization of cybersecurity standards.

7. Tabletop Exercises and CTFs (Capture the Flags): Engage in interactive tabletop exercises designed to simulate real-world scenarios, from ransomware incidents to critical system failures, promoting teamwork and problem-solving. Compete in cybersecurity challenges and CTFs to test your skills in securing medical and healthcare IT systems.

8. Networking and Community Building: Connect with a diverse group of stakeholders, including hackers, healthcare professionals, medical device manufacturers, and policymakers. Collaborate in an environment that fosters innovation, trust, and shared learning.

The Biohacking Village is your gateway to understanding and addressing the complex challenges of medical technology and cybersecurity. Attendees will leave equipped with knowledge, skills, and connections to drive meaningful change in the industry.

BLUE TEAM VILLAGE (BTV)

Level 2 - W213-W218

blueteamvillage.org

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.

The Blue Team Village's Project Obsidian is a 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 training and exercises that provide practical hands-on experience across each discipline. Project Obsidian 101 trainings provide cybersecurity knowledge that will enable attendees to develop the skills needed to be successful in their current and future roles.

Two of the most valuable takeaways are how to strategically approach a task and the operational processes supporting each task's objectives. Knowing 'how' to do something is only part of the challenge. Knowing 'when' and 'why' to perform specific tasks adds the necessary context to develop the full story of defensive cybersecurity.

BUG BOUNTY VILLAGE

Level 3 - W326

www.bugbountydefcon.com

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. After a big success and great feedback during the first ever Bug Bounty Village during DEF CON 32, We want to be part of DEF CON 33 and keep celebrating the bug bounty community, where hunters, learners, and enthusiasts can converge, interact with top-tier hackers, attend insightful workshops, talks, and immerse themselves in hands-on activities.

With over 20 workshops, panels and talks, the Bug Bounty Village at DEF CON 32 was a huge success. The room was completely full of hackers at all times, Some of the best bug bounty hunters in the community were part of our village to share knowledge, create content, teach others, and also, to make new friends. With waiting lines of over 100 people waiting to get in for some of our workshops, we have demonstrated that there is a huge interest in Bug Bounty to remain as a specific village at DEF CON, and have that special place in the biggest hacker conference in the world, where the Bug Bounty community can connect, grow and help others become the future of Bug Bounty.

CAR HACKING VILLAGE

Level 1 - Hall 2 - 602

www.carhackingvillage.com

For over a decade, we've been leading the charge in automotive security, and this year, we're shifting into high gear! Get ready for an electrifying DEF CON 33 experience packed with interactive challenges, exclusive badges, and mind-bending exercises designed to supercharge your skills.

Join us and make this DEF CON one for the record books!

We observe DEF CON hours of operation

For schedules and other info: https://www.wallofsheep.com/pages/dc33

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

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 topics like honeypots, botnets, and more guided by our expert mentors! Check website for schedule of activities.

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.

And More!

Be sure to check out our other events: RegEx Trainer, Linux Trainer, BotNet and so much more!!!

VILLAGES

CLOUD VILLAGE
Level 3 - W311-W313
dc33.cloud-village.org

With the industry's rapid growth in cloud infrastructure, the presence of an open platform to discuss and showcase cloud research becomes a necessity.

Cloud village is an open platform for researchers interested in the area of cloud security. We plan to organise talks, tool demos, CTF and workshops around Cloud Security and advancements.

Our CTF will be a jeopardy style 2.5 days contest where participants will have to solve challenges around Cloud infrastructure, security, recon, etc. These challenges will cover different cloud platforms including AWS, GCP, Azure, Alibaba, Digital Ocean, etc. We will also reward our top 3 teams with awards.

CRYPTO PRIVACY VILLAGE
Level 1 - Hall 1 - 403
cryptovillage.org

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-preserving data analytics, or crypto backdoor laws!

CRYPTO + PRIVACY VILLAGE

DATA DUPLICATION VILLAGE
Level 2 - W225
dcddv.org

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 just about any security con talk known to hacker-kind or a copy of the VX-Underground archive (along with a few hundred gigs of cat pictures), you'll find it here. Our village provides a "free-to-you" service of direct access to terabytes of useful data to help build those hacking skills and allow open discussions with other storage enthusiasts.

We'll also be partnering with DC Next Gen to ensure that our future generations have the opportunity to explore the details of how past and current data storage works!

DATA DUPLICATION VILLAGE

EMBEDDED SYSTEMS VILLAGE
Level 1 - Hall 1 - 401
embeddedvillage.org

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.

ESV
EMBEDDED SYSTEMS VILLAGE

GAMEHACKING.GG
Level 1 - Hall 1 - 402
gamehacking.gg

Gaming and cybersecurity intersect in many 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. Our community focuses on learning and does NOT endorse cheating in competitive online games.

GAMEHACKING.GG

HAM RADIO VILLAGE
Level 3 - W321
hamvillage.org

Ham Radio has been considered to be the original group of hackers, launching before computers, integrated circuits, and even the transistor! Hams of all generations have a hacker mindset, solving problems their own way, regardless of what the manual has to say. Continuing this pioneer spirit, the Ham Radio Community 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 Ham Radio Community, 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!

Testing held Friday 13:00-16:00, Saturday 11:00-17:00, & Sunday 11:00-13:00 on Level 3 - W320

HARDWARE HACKING AND SOLDERING SKILLS VILLAGE (HHV/SSV)
Level 1 - Hall 2 - 802
dchhv.org

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 2 - 805
www.icsvillage.com

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

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

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

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

- Hands on instruction for industry to defend ICS systems.

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

ICS VILLAGE

VILLAGES

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.

IOT VILLAGE

Level 1 - Hall 2 - 605

iotvillage.org/defcon.html

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/).

LOCK PICK VILLAGE

Level 1 - Hall 2 - 701

www.toool.us

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

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

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

MALWARE VILLAGE

Level 1 - Hall 1 - 303

malwarevillage.org

Malware Village is dedicated to providing a safe and engaging environment for participants to learn and share knowledge about malware analysis. Our mission is to equip attendees with the skills, techniques, and historical context needed to understand, research, and combat malware. Participants will gain hands-on experience with real-world analysis techniques, guided by seasoned infosec professionals.

Beyond technical training, Malware Village fosters a strong community where researchers, enthusiasts, and professionals can connect. We welcome everyone—whether you're an artist creating malware-inspired art, a hardware researcher discovering unexpected connections to malware analysis, or a seasoned analyst reminiscing about early malware history. Even children can explore malware through Malmons (aka Malware Monsters by Lena Yu aka LambdaMamba), making cybersecurity education more accessible.

At its core, Malware Village is about uniting people—newcomers and experts alike—with a shared mission: understanding, analyzing, and defending against malware to protect society.

MARITIME HACKING VILLAGE

Level 1 - Hall 2 - 504

maritimehackingvillage.com

The Maritime Hacking Village (MHV) has set sail for LVCC to deliver the first and only immersive maritime hacking experience for you to learn what it takes to exploit and defend real-world maritime systems. Our mission is simple: we are creating a space for stakeholders to come together and navigate the changing tides in the maritime sector's technological, geopolitical, and adversarial landscapes which demand ever-more-urgent collective action to address the systemic cybersecurity vulnerabilities in the systems which underpin global maritime defense and trade. Together we hack to facilitate the discovery and sharing of knowledge integral to the development of effective maritime cybersecurity policy, industry standards and regulations, vulnerability information sharing, cyber threat intelligence, and most importantly – a capable and trusted workforce and community-of-interest.

Why? Maritime infrastructure is the backbone of the global economy and order. Countries, companies, and militaries all use the sea for power projection and commerce, but no single stakeholder controls the implementation of policies and regulations. Stakeholders unanimously agree that from machines, to systems, to governance, the maritime domain is fundamentally insecure. Still, seemingly insurmountable access barriers are preventing the security community, and anyone else, from doing anything to help.

MHV has made it our purpose to eliminate these barriers – and to provide every human with the access and resources necessary to engage in maritime vulnerability research and cybersecurity innovation. Our village is a safe, shared space where the security community (elite hackers, trusted providers, and young talent alike) can develop and demonstrate their competence in attacking and defending real maritime systems – and where maritime industry stakeholders can engage with this community on neutral ground to grow their arsenals of knowledge, tools, trusted and capable providers, and fresh talent. We believe that this work together will create rising tides of awareness, information sharing, and innovation that will lift all ships and allow us to gradually secure the maritime sector.

PACKET HACKING VILLAGE

Level 3 - W303-W310

www.wallofsheep.com

The Packet Hacking Village at DEF CON provides a community learning experience for people of all skill levels, from absolute beginners to seasoned professionals. While DEF CON is made up of dozens of small community-of-interest villages, we are one of the largest and most well known. 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 world-class 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.

We provide a welcoming environment for hackers of all skill levels and backgrounds to network, learn new things, and be active participants in DEF CON. Our famous "Wall of Sheep" provides a fun and interactive take on internet security and privacy, while our contests Packet Inspector, Packet Detective, and Capture The Packet serve as a zero-to-hero pathway for individuals to learn network security, packet analysis, and delve into advanced security topics. Every year we strive to bring something new and innovative to DEF CON, whether it's never-seen-before talks or creative games to teach and test skills.

PAYMENT VILLAGE

Level 1 - Hall 2 - 505

www.paymentvillage.org

Come to the Payment Village to learn about payment technologies! Payments play a crucial role in our daily lives, yet many of us lack an understanding of how they work. Our mission is to educate and cultivate the next generation of payment security experts and to foster open discussions around payments. We want to raise the bar in payment security! 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 of where to start? Register for one of our workshops to acquire new skills or attend a talk by one of our carefully chosen experts. Already a pro? Pick up a Payment Village credit card to take part in our contest! Looking for unique challenges? Take home all the money from our cash-grab machine or have a go at our scavenger hunt!

As if that is not enough, this year we have created the largest badge EVER at DEF CON, our vulnerable ATM badge. We are bringing ATM hacking to the masses; our badge simulates an ATM attack surfaces in a physical form factor you can carry with two hands! not a forklift truck.

AIxCC
AI CYBER CHALLENGE

DARPA + ARPA-H

SECURING OUR CRITICAL INFRASTRUCTURE

Much of the software running critical infrastructure, like energy grids, hospitals and water systems, depends on open source software that is pervasively vulnerable to cyberattacks.*

The Defense Advanced Research Projects Agency's AI Cyber Challenge (AIxCC), in collaboration with the Advanced Research Projects Agency for Health, is accelerating the development of AI-enabled Cyber Reasoning Systems that autonomously find and patch vulnerabilities at the speed and scale required to secure critical infrastructure and beyond.

Last year, teams developed their systems to compete in the Semifinal Competition, which was showcased at DEF CON 32. The top seven teams advanced to the Final Competition. Now, teams are patiently waiting to hear who will go home with the top prize of $4 million here at DEF CON 33.

It takes a community to move from innovation to actually securing critical infrastructure. AIxCC has the potential to transform global cybersecurity because the winning systems will be released as open source, minimizing barriers to access and enabling the community to push these systems forward.

Located in Exhibit Hall 1, the AIxCC Experience is designed to amplify this important mission and call on everyone to do their part in shaping and supporting the transition of this game-changing technology to widespread use.

(*Linux Foundation)

COME TO THE AIxCC EXPERIENCE TO

- → Learn more about the difficulties and impact of securing critical infrastructure.
- → Meet the teams and see their Cyber Reasoning Systems in action.
- → Deep dive with the organizers on competition highlights.
- → Enjoy a full schedule of informative talks on the AIxCC stage – including team panels, competition organizers, and leading experts – about securing critical infrastructure and advancing cybersecurity.

EXHIBIT HALL ONE

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

aicyberchallenge.com /// aicyberchallenge.com /// aicyberchallenge.com /// aicyberchallenge.com /// aicyberchallenge.com

VILLAGES

PHYSICAL SECURITY VILLAGE

Level 1 - Hall 2 - 804

physsec.org

Physical security is an important aspect to think about when considering securing your facility. The Physical Security Village provides an important opportunity to learn about real-world threats, hands-on mitigation techniques, and best practices for protecting assets. Our village brings together experts, practitioners, and enthusiasts to share knowledge through interactive demos, talks, and discussions. Whether you're new to physical security or a seasoned professional, you'll find valuable insights and practical skills.

POLICY @ DEF CON

Level 2 - W234

defcon.org/policy/

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 1 - 206

quantumvillage.org

Quantum Village Returns with our Year of Quantum Edition @ DEF CON 33!! Our theme this year is "Sense and Security" and we are bringing some amazing talks, workshops, demos, and hands-on activities to this year's incredible Quantum Village! Come and find out how to hack quantum computers, learn more about quantum technologies, and meet the engineers and scientists who are building the machines that manipulate the quantum world. We also introduce the world's first hackable, fully open sourced diamond-based quantum sensing platform - and we'll be showing some of the amazing things it can do! We have quantum computers, quantum sensors, The OG Quantum CTF, quantum art (and artists), and all you need to prepare for the quantum future!

RADIO FREQUENCY VILLAGE

Level 1 - Hall 2 - 803

rfhackers.com

After 17 years of evolution, from the WiFi Village, to the Wireless Village, RF Hackers Sanctuary presents: The Radio Frequency Village at DEF CON 33. 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.

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 2 - 603

reconvillage.org

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

As recon is a vital phase for infosec as well as investigations, folks should 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, and other hands-on activities, etc.

We also run fun and hands-on live competitions where participants learn while they play.

RED TEAM VILLAGE

Level 1 - Hall 1 - 405

redteamvillage.io

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.

SOCIAL ENGINEERING COMMUNITY VILLAGE

Level 3 - W317-W319

www.se.community

The Social Engineering Community is formed by a group of individuals who have a passion to enable people of all ages and backgrounds interested in Social Engineering with a venue to learn, discuss, and practice this craft. We plan to use this opportunity at DEF CON to present a community space that offers those elements through panels, research opportunities, and contests in order to act as a catalyst to foster discussion, advance the craft and create a space for individuals to expand their network. DEF CON attendees can either participate in these events, or they can watch the events unfold and learn about Social Engineering as an audience member. We plan to accomplish the above by bringing together passionate individuals to have a shared stake in building this community.

TAMPER-EVIDENT VILLAGE

Level 1 - Hall 2 - 502

"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.

VILLAGES

TELECOM VILLAGE

Level 2 - W224

telecomvillage.com

At Telecom Village, our mission is to cultivate critical and innovative thinking in telecom security, with a strong focus on 5G networks. We offer a structured learning approach that enables participants to:

- Identify key areas for research and security analysis.

- Explore telecom vulnerabilities and misconfigurations in depth.

- Develop essential skills, including security gap analysis, penetration testing of telecom protocols, Radio Access Networks (RAN), 5G API gap analysis and ICT-related threat mitigation.

Our goal is to bridge the gap between theory and real-world application, equipping participants with the expertise to navigate and counter emerging telecom security challenges effectively. Through guided research, hands-on learning, and continuous exploration, we foster a community of skilled professionals ready to tackle the evolving telecom landscape.

VOTING VILLAGE

Level 2 - W222-W223

votingvillage.org

The [Voting Village](https://votingvillage.org) has been an annual event since 2017 that provides hands-on opportunities to understand and analyze voting system hardware and software. Before the Voting Village, ordinary technologists and citizens had no access to the systems that run our election infrastructure. As the only open environment that gives the public hands-on access to their election systems, it is a critical antidote to rampant misinformation about election security and provides an opportunity to strengthen these systems against malicious attacks. The Voting Village is brought to you by our 501(c)3 tax exempt not for profit organization, the Election Integrity Foundation, EIN: 83-4089169.

The Voting Village has been invited to testify to Congress several times about how to strengthen election infrastructure. Conversely, we have drawn fire from voting system manufacturers, prompting a bipartisan group of senators to co-sign a public letter defending the Voting Village against some of the largest voting machine companies in 2018.

Even between presidential election cycles, expanding the reach of the Voting Village and providing education about how our election systems work is critical to democracy.

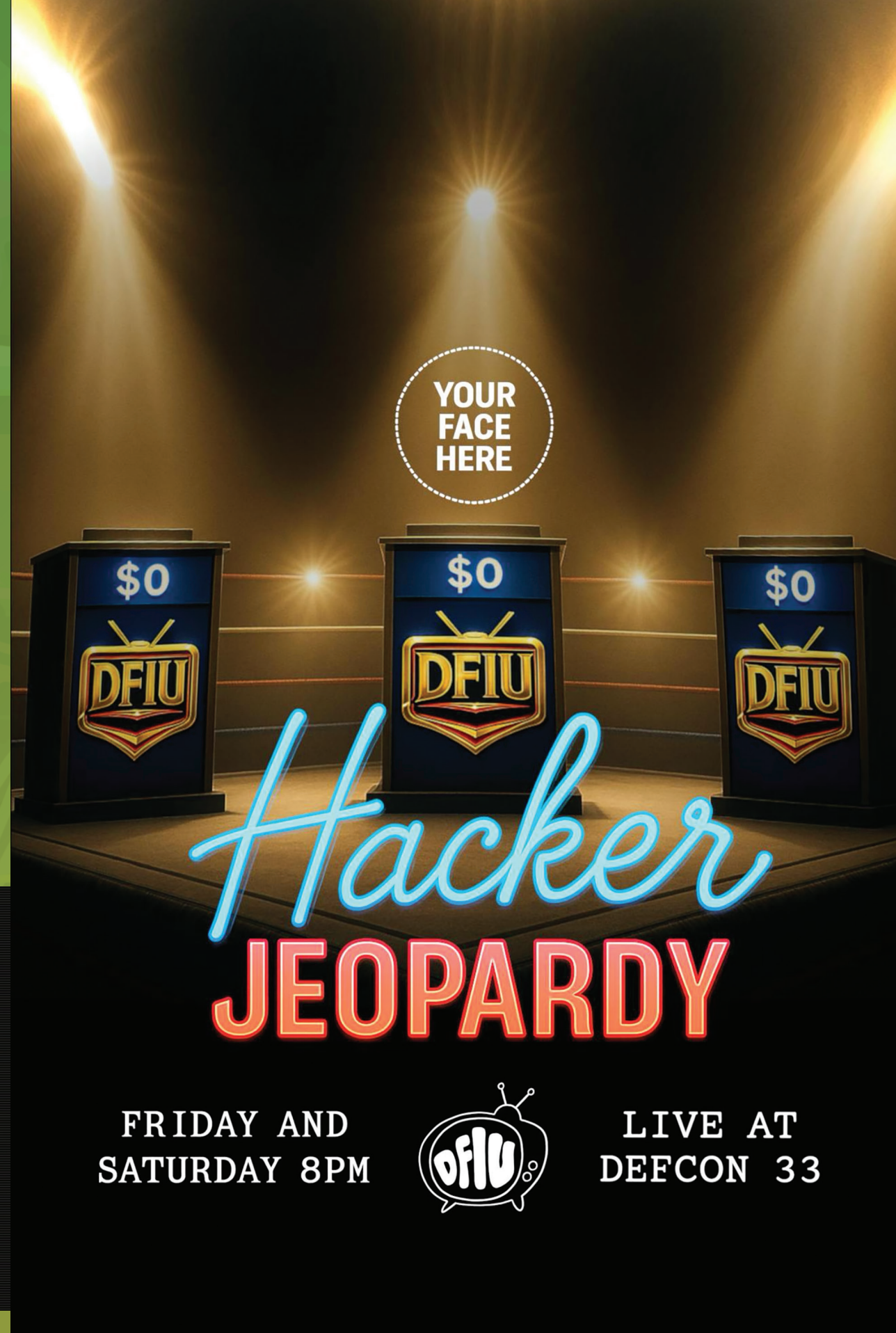
InfoCon

Hacking Conference Archive

www.infocon.org

INFOCON IS A COMMUNITY SUPPORTED, NON-COMMERCIAL ARCHIVE OF ALL THE PAST HACKING RELATED CONVENTION MATERIAL THAT CAN BE FOUND.

CONVENTIONS, SKILLS, RAINBOW TABLES, HACKER DOCUMENTARIES, PODCASTS. AND MORE ALL AVAILABLE FOR DIRECT DOWNLOAD OR AS TORRENTS.



CONTESTS

$$$$$_<CAPTURE_THE_COIN>_$$$$$



Level 1 - Hall 2 - 505

Welcome to $$$$$_<CAPTURE_THE_COIN>_$$$$$! We're bringing real-world payment hacking straight to DEF CON. This contest merges hardware hacking, cryptanalysis, mobile app forensics, physical security, and offensive security into one glorious, chaotic CTF. No system is sacred! If it moves, stores or processes money, it's fair game.

From magstripes to mobile wallets, POS systems to online banking, ATMs to NFC payments, if it touches money, we're messing with it. Your mission: reverse, break, manipulate, and exploit—all in the name of exploration!

Expect challenges where you'll clone, decrypt, spoof, MITM, inject, and maybe even get a card to spill its deepest, darkest secrets. Want to mess with a banking app? We got you. Think your RFID cloning skills are solid? Prove it. Ever wondered if you can bypass chip-and-PIN protections? Let's find out!

So, whether you're an RFID wizard, EMV cryptography nerd, API manipulator, or into dumpster diving, there's a challenge here for you. You might not get rich, but you'll have fun trying!

Participant Prerequisites

Registration is to be made on the website. Our content is accessible to all and includes challenges which don't require equipment. We also have a range of equipment that is available for loan such as card readers. A laptop and Android phone is needed for some of the challenges.

www.ctf.paymentvillage.org

$UNL1GHT SH4D0W5



Level 1 - Hall 1 - 112

"$unL1ght Sh4d0w5": The Nirubi Challenge - Prove Your Might

In the realm of cybersecurity, the pursuit of excellence is a never-ending quest. It's time to put your skills to the test and prove your worth in the "$unL1ght Sh4d0w5: The Nirubi Challenge".

In the spirit of DEF CON 33's theme of promoting openness and accessibility, we present a unique hacking challenge that flips the script on traditional black box contests. We provide you with a production-ready Linux system, complete with known vulnerabilities and a proof-of-concept (POC) exploit to get you started and then throw the gauntlet that will push your limits and make you think outside the box.

The Nirubi Mandate:

Nirubi, an ancient Tamil word meaning "to prove", is more than just a concept - it's a way of life. It's about demonstrating your capabilities, showcasing your expertise, and rising above the rest. In this challenge, we invite you to embark on a journey of self-discovery, to test your mettle against the best, and to emerge victorious.

The Challenge:

Your mission, should you choose to accept it, is to leverage the given vulnerabilities and POC to achieve remote code execution and unleash a ransomware attack on our target system. The twist? We'll be watching as you navigate not one, but two separate challenges:

Part 1: "Sh4d0w5 Recon" - Using the provided vulnerabilities and POC, expand on the existing exploit to deliver a payload that encrypts the contents of a specific file on the system. Show us your skills in taking the given information and turning it into a successful attack.

Part 2: "$unL1ght Horizon" - If you succeed in Part 1, you'll be invited to take on the same system, but this time, it will be fortified with a proprietary hardening technology. Can you adapt your approach and still manage to inject your payload and encrypt the target file?

The Prize:

The first contestant to successfully complete both parts of the challenge will take home a prize of $10,000. Will you be the one to shine $unL1ght into the Sh4d0w5 and claim victory?

What sets us apart:

- We're providing you with the vulnerabilities and a POC, giving you a clear starting point for your attack.

- You'll be working with a fully disclosed system configuration, eliminating the guesswork often associated with black box hacking contests.

- Our challenge is designed to separate those who merely know from those who can truly execute. We'll give you all the information you need - system configurations, vulnerability details, and more. But can you use that knowledge to outmaneuver our defenses and emerge victorious?

Rules and Eligibility:

- Contestants must be 18 years or older to participate.

- All participants must agree to our terms and conditions, which include rules for responsible disclosure and non-disclosure agreements.

- The contest will be held during DEF CON 33, with specific dates and times to be announced.

Participant Prerequisites

- Bring your own laptop and/or smart-phone/tablet

- Bring ANY software tools you would need for hacking purposes. This includes an operating system (e.g, Windows/Linux) with Python, C/C++ compiler and associated binary analysis tools.

.SSH/ SOCIAL SCAVENGER HUNT



Level 1 - Hall 4 - C201

Social Scav Hunt (SSH) is your time to expand your circle and meet some interesting folks.

Given the provided list, take a photo for each item or person.

Consent is not only sexy but required.

This contest while a prize will be provided, the real prize will be the friends you make along the way.

5N4CK3Y



Level 1 - Hall 1 - 104

AND!XOR creates electronic badges filled with hacker challenges. We love doing this, especially coming up with unique ways for hackers to earn them. 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 enough flags on our web hosted CTF platform, you get a 5N4CK3Y dispense code, punch it in, and a badge is vended to you! There are a variety of challenges to earn a badge as well others to continue working on the badge itself once obtained. These span from hardware hacking, reverse engineering, OSINT, network security, phreaking, wireless, 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 the CTF challenges to dispense a badge. Hardware hacking is our passion and we want people to learn on badges once they get them.

Participant Prerequisites

A computer, desire to learn, and make friends to beg, borrow, and steal from if you need a tool which you do not already own. Our challenges are multidisciplinary. While we will not give away what is required this year, tools participants have used in the past include: Computer, Ghidra, AFL, telephone, lock pick set, SDR, Flipper Zero, UART Adapter, FT2232 hardware debugger, chip clip, telephone parts, TV remote control, audio recorder, tracing paper, pencil, solder iron & solder, hot air gun, exacto knife, lighter, ice from a Malört cocktail being sipped on by Lintile, copper wire, booze, and ramen. In short, any tools required for the CTF challenges can be obtained at DEF CON.

? CUBE



Level 1 - Hall 1 - 105

Redefining Boundaries, Enhancing Connectivity, Innovating Control—Aperture Inc. is dedicated to pushing the limits of innovation and is fully committed to providing a more secure environment to maintain our promise to our "customers."

At the core of it all lies the ?Cube—a labyrinth of security, deception, and ever-evolving complexity. Our engineers have reinforced its defenses, rewritten its digital DNA, and expanded its capabilities in ways that should concern you. Buried within its depths are secrets—secrets that could unravel everything. Infiltrate, decode, and dismantle. But beware: the ?Cube—and those also working towards the same ultimate goal—don't take kindly to outsiders.

For those who know—welcome back. You already understand what's at stake. For those who don't... well, let's just say we hope you are quick learners...

You're about to embark on an adventure—one that demands nothing less than absolute technical precision across the precarious domains of physical security, web exploitation, cryptography, and other puzzles designed to unravel your sanity.

Assemble your team. Choose your specialists wisely. Then step into the ever-tightening web technologies that define the ?Cube. Escape is optional. Success? Highly unlikely.

The first team to breach the center earns the title—simple, right? Of course, if the Cube remains unsolved (again), the team that clawed their way the furthest will be honored for their valiant struggle. And make no mistake—a struggle is guaranteed. Every step forward will demand effort more and more. Mistakes could be costly.

But don't worry... the Cube is very patient. It can wait. Can you? Will others?

Participant Prerequisites

DEI or DIE. Diverse talents across multiple domains of knowledge are highly recommended. Some tools such as lockpicks, Chromebooks, and other RFID tools may be available for various challenges, but it is recommended teams come prepared.

Pre-Qualification

The contest will not require qualifiers for the first full day. Point requirements will be required to continue interacting with the ?Cube as the contest progresses.

0x3fcube.com

ADVERSARY WARS CTF



Level 1 - Hall 2 - 702

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 inter-locking-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.

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.

Participant Prerequisites

Just a laptop

adversaryvillage.org/adversary-wars-ctf

AI ART BATTLE



Level 1 - Atrium-East - Contest Stage

Welcome to the "AI Art Battle" Generative AI Art 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.

Participant Prerequisites

- Smartphone or Laptop

Pre-Qualification

- This year we hope to hold a pre-qualifier to help shape the contest before going on stage.

AW, MAN...PAGES!



Level 1 - Atrium-East - Contest Stage

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?

BAND CAMP: HACKER MY MUSIC



Level 1 - Hall 1 - 207

Band Camp: Hacker My Music! is a hands-on contest that combines DIY hardware hacking and musical innovation. With this contest we aim to bring together hackers, makers, and others looking for a new experience to design and build their own instruments in a reproducible sharable manner. If that means repurposing unexpected common materials or making custom 3d printed instruments, or even custom sound-generating gizmos we're in! Whether you're into 3D printing, upcycling old hardware, or discovering strange new ways to produce melodies, this contest will give hackers the chance to create and perform with instruments that break all the rules. It's a fresh perspective on hacking because it isn't just about cracking code or bypassing security — it's about hacking sound, reimagining music hardware, and pushing creative boundaries. Who knows, maybe we'll get a new "blue box".

We encourage participants to take advantage of whatever resources they have on hand—3D printers, microcontrollers, pre-prepared parts, or even random junk from the hardware store. If it's reproducable and makes music, we want to hear it! The ultimate goal here is to create an open library of new sounds that can be used freely by hackers for whatever their needs. Maybe the sounds made could even be hosted on media.defcon.org and opened up for other musicians/hackers to use royalty free.

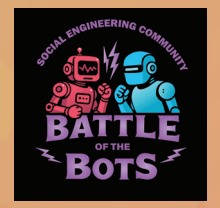
Rules and Participation Requirements to be hosted at hackermymusic.com

Participant Prerequisites

Participants may sign up and make their instruments ahead of time, or they can make them on site. We will have access to the 3d printers in the maker community that I am bringing along for them to use.

hackermymusic.com

BATTLE OF THE BOTS: VISHING EDITION



Level 3 - W317-W319

The future of social engineering is here. Piggybacking on the success of last year's John Henry competition, the SEC has gone all-in on a first-of-its-kind competition. In Battle of the Bots: Vishing Edition, teams will develop AI-driven bots to place live vishing (voice phishing) calls, testing the limits of artificial intelligence in deception. By blending hacking, automation, and psychology, competitors will see whose AI bot can capture the most objectives from live human interactions. As AI continues to evolve, so do its applications in cybersecurity—this competition provides a unique opportunity for competitors and spectators to witness firsthand the current state of offensive AI capabilities manifested through social engineering vishing calls.

Whether you're competing or spectating, this event offers a rare glimpse into the future of hacking. Attendees will witness AI bots in real-time navigating conversations, persuading targets, and adapting their tactics—just like a human social engineer. Expect to learn about the strengths, weaknesses, and ethical considerations of AI-driven vishing and the defensive strategies needed to counter this emerging threat. Join us and see if AI is ready to take on one of hacking's most human-centered techniques.

Participant Prerequisites

To successfully participate, teams will need a basic understanding of AI prompt engineering to develop and refine their AI-driven vishing bots. Competitors should be comfortable designing prompts that guide AI responses effectively while ensuring their bots can engage in dynamic conversations. Additionally, all participants must adhere to the competition's Code of Ethics, ensuring that their AI interactions remain within ethical boundaries and comply with contest guidelines. While prior experience with AI-driven automation or social engineering tactics may be beneficial, it is not required .

BETTING ON YOUR DIGITAL RIGHTS: 4TH ANNUAL EFF BENEFIT POKER TOURNAMENT AT DEF CON 33



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. All new players are welcome. We offer a clinic right before we start to refresh skills and turn you into a poker hacker fast!

Participant Prerequisites

21 and over. Pre-register as soon as possible to ensure your spot at the table at eff.org/poker; we sell out every year.

www.eff.org/poker

BEVERAGE COOLING CONTRAPTION CONTEST



Level 1 - Hall 1 - 306

Duck, just duck. What the duck! Seriously!? This is the timeline we are in? Here I always thought those preppers was bonkers. Okay, I'm going to break the 4th wall here, I'm writing this in March so here's hoping this isn't prescient.

That's it folks! DOGE has canceled our gas infused multi-liquid rapid cooling technology research grant along with the rest of the NSF because why would we need science when we have Tesla and SpaceX. Elon daddy you're so big and hard, please give me some juice from your massive rocket to cool my beverage because it for sure hasn't gone to Mars. What do you mean you lost it? Trump has it where!? This is why you have a flared base on the rocket! How am I supposed to cool my beverage after China starts WW3 because Pooh bear can't stop obsessing over his nine dash sack? This is a disaster!

Its beverage chilling folks, the description is on the tin. But just in case the illiteracy rates have reached such a level that you can't read the name of the contest, here is a description you can't read either.

Je koelt het drankje dat we je geven in een rode solobeker zo snel mogelijk af tot 34 graden F. Je mag het drankje niet veranderen door het te mengen met ijs, droog of anderszins. Je mag een apparaat meenemen of je eigen apparaat bouwen op de conventie. Er wachten fantastische prijzen, voornamelijk wat ik heb liggen en niet mee naar huis wil nemen.

(You will cool the drink we give you in a red solo cup as quickly as possible to 34 degrees F. You may not alter the drink by mixing it with ice, dry or otherwise. You may bring a device or build your own at the convention. There are some great prizes waiting, mostly what I have lying around and don't want to take home.)

There are some additional rules, check the DEF CON forums or the poster board at the contest!

Participant Prerequisites

- A commitment to the sanctity of the unadulterated beverage.

- A complete disregard for the health a safety of one's self, good design principals, and the laws of physics generally.

bcccweb.wordpress.com

BLACKS IN CYBERSECURITY VILLAGE CAPTURE THE FLAG COMPETITION



Level 3 - W322-W324

The Blacks In Cybersecurity (BIC) Village Capture The Flag contest 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, emerging technology and Black history. At DEF CON 33 the BIC Village CTF team will take you to the campus of an HBCU (Historically Black College / University) with a special history and "other-wordly" delights! Come explore the

challenges that walk you through our campus gates and into the adventure fueled by curiosity & innovation as we celebrate five years of our BIC Village!

Participant Prerequisites

Participants may want to bring their own laptops, physical security tools, lock picks, hardware hacking tools or other supplies to interact with both of our physical and virtual set-ups.

www.blacksincyberconf.com/ctf

BLUE TEAM VILLAGE CTF

Level 2 - W213-W218

A cyber defense Capture the Flag inspired by a mix of trending nation-state actor kill chains. You are an incident responder tasked to investigate multiple incidents. You will have access to a SIEM and other forensic data; however, just like in real life, these tools have issues you must overcome to uncover what happened.

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 attending the other BTV Project Obsidian presentations and panels to learn even more about different cyber defense topics.

Participant Prerequisites

Attendees will be required to use a laptop, tablet, or mobile device. Prior knowledge of using a SIEM is preferred.

ctf.blueteamvillage.org

BUG BOUNTY VILLAGE CTF

Level 3 - W326

Bug Bounty Village CTF: Experience the Thrill of a Real Bug Bounty Experience

This year, for the first time ever, Bug Bounty Village is bringing you a Capture the Flag with a twist. This CTF is designed to feel just like a real bug bounty hunt.

Dive into a vulnerable application and see if you can uncover its hidden weaknesses just like you would on a bug bounty program. The CTF is designed to be accessible for all experience levels, from beginners looking for their first bug to veteran hunters eager for a very interesting challenge. Expect a range of vulnerabilities, from trivial finds to sophisticated ones that will push you to the limit.

But that's not all. We're adding a unique real-world flavor to the competition. Participants onsite at DEF CON will submit some of their bug reports for those to be validated by real bug bounty triagers volunteering their expertise to make this experience as real as possible. This process will determine scores based not just on technical prowess but on report quality and professionalism, just like in a bug bounty program.

Get ready for a realistic bug bounty experience, a chance to grow your skills, connect with the community, and show what you're made of.

CALL CENTER VILLAGE CONTEST

Level 1 - Hall 1 - 210

The Call Center Village contest is a community security-challenge that simulates common attack-surfaces found in multi-tenant, multi-industry, BPO call centers - often referred to as "answering services."

Test your skills in physical entry, network security, audio manipulation, messaging protocols, telephony tools, and application security based on our actual experiences working in the call center industry.

As a community, you will work together to break into AnswerTarget - the most modern and secure call-center never built - to unlock physical and digital flags that reveal clues for the Call Center Village social-engineering challenge.

Earn a Call Center Village challenge medal (and your chance at socially-engineering a real-world call center agent) by completing challenges during contest hours!

www.callcentervillage.com

CAN IT HAM?

Level 1 - Hall 1 - 307

Have you ever looked at a tin can, a pile of coax, some solder, a few connectors, and your radio and thought, I'm not sure, but CAN IT HAM? In this new contest for DEF CON 33, the Ham Radio Village is challenging participants to see what they can turn into functioning antennas.

We'll have some basic supplies – tin cans, coax, solder, connectors,– but feel free to bring your own weird components if you want. The 10 best builds will get tested, and the top 3 will score bragging rights & prizes!

Come participate in some radio shenanigans, hack something together and see what you can make work (plus maybe learn something along the way).

Participant Prerequisites

None - Bring your hands and brain and give it a try! You can also bring any* materials from off-site to construct your antenna

* Within DC33/LVCC limitations. No radioactive isotopes or explosives, please.

hamvillage.org

CAPTURE THE PACKET

Level 3 - W303-W310

Capture the Packet is a competition that tests players grit and cyber capability.

Contestants will be tasked to solve a range of challenges including Incident Response and vulnerability exploitation.

Participant Prerequisites

- Participants should bring their own laptop devices with ethernet port. Limited USB-A to Ethernet ports available for loan.

- Attendees should brush up on networking protocols and analysis techniques.

www.ariessecurity.com

CAR HACKING VILLAGE CAPTURE THE FLAG (CTF)

Level 1 - Hall 2 - 602

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.

Participant Prerequisites

https://www.carhackingvillage.com/ctf-rules

www.carhackingvillage.com

CLOUD VILLAGE CTF

Level 3 - W311-W313

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

Participant Prerequisites

Laptop and access to internet would be needed.

dc33.cloud-village.org

CMD+CTRL CLOUD CYBER RANGE

Level 1 - Hall 1 - 111

CMD+CTRL is an immersive learning and hacking platform where developers, security professionals, and tech enthusiasts come together to sharpen their skills in web application security. Players compete in a real-world environment, uncovering vulnerabilities and learning security techniques hands-on. With real-time scoring, the experience stays engaging, fostering both collaboration and friendly competition.

At DEF CON 33, we're debuting our latest Cloud Cyber Range: Forescient—a deep dive into exploiting common Azure misconfigurations. This brand-new challenge will put your cloud security expertise to the test like never before.

Are you ready to hack the cloud?

Participant Prerequisites

Computer with internet access.

Pre-Qualification

No pre-qualification. Pre-registration is required for the Cloud Cyber Range competition. Please sign up at defcon33.cmdnctrl.net as spots are limited.

Other cyber ranges will also be available for non-competitive play, no registration required.

defcon33.cmdnctrl.net

CODE BREAKER CHALLENGE

Level 1 - Hall 4 - C207

The Code Breaker Challenge is an advanced cryptographic puzzle designed for DEF CON attendees who want to push their problem-solving skills to the limit. Anyone who successfully cracks the code will receive an exclusive invite to a private pool party, where they can celebrate their achievement alongside fellow codebreakers.

How It Fits DEF CON's Theme: Access Everywhere

Usable: The challenge is designed to be solved with logic, pattern recognition, and cryptographic knowledge—no special equipment or insider access required.

Accessible: Participants from all backgrounds can attempt it, regardless of whether they are seasoned cryptographers or first-time codebreakers.

Private & Secure: The challenge will incorporate modern encryption principles that highlight privacy-preserving technologies, showing the importance of cryptography in maintaining free and open access to information.

Structure

The challenge will be a multi-layered puzzle, incorporating historical ciphers, steganography, and modern cryptographic techniques.

Participants will have the entire duration of DEF CON to solve it.

Those who succeed will be given a unique code or token to redeem their invitation to the private pool party.

Participant Prerequisites

Code Breakers need to access a computer and internet. Everything else is provided.

CODE CRIMSON: HEALTHCARE IN TRAUMA

Level 1 - Hall 2 - 606

Something isn't right...

Hackwell Heights Medical Center, a renowned hospital system has gone eerily silent. Monitors flicker with unfamiliar code. Alarms no longer sound. The data that once saved lives is now locked behind walls of encryption, altered, erased, or rewritten. Whispers

of a breach start rippling through the clinical silence. This isn't just any system failure, this is deliberate and calculated. Something or someone has hidden a message inside the network. The kind of message that only the sharpest minds can extract. You are part of a premier response team, summoned under a rarely used protocol: Code Crimson.

Your mission is to enter the simulation, trace the unknown exploit, and secure critical medical infrastructure before the damage spreads. What you uncover may alter more than just files—it may change the future of healthcare. The pulse of the system is in your hands.

www.villageb.io/capture-the-flag

CREATIVE WRITING SHORT STORY CONTEST

The DEF CON Short Story contest is a pre-con contest that is run entirely online utilizing the DEF CON forums and subreddit. This contest follows the theme of DEF CON for the year and encourages hackers to roll up their sleeves 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 sometimes 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.

CRYPTOCURRENCY CHALLENGE

Level 1 - Hall 4 - C101

The Cryptocurrency Cyber Challenge welcomes you to develop your skills finding vulnerabilities and hacking on blockchain finance technology. Learn the unique ways that cryptocurrency systems are attacked, defended, and secured while teaming up to compete with your peers. Meet your fellow hackers, feel the challenge, and get inspired to explore the security aspects of cryptocurrency where practical finance hacking for the public good is encouraged.

To win any of the five levels of this contest, use testnet tokens, get help from village mentors, and convince the contest judges of the merit of your work. We hope (depending on degree of sponsorship) to award prizes for the best cryptohacks in the DEF CON world.

www.cryptocyberchallenge.com

CYBER DEFENDER - THE GAME

Level 1 - Hall 1 - 107

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 utilized 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 Cyber Protection Team (CPT) 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, protect, detect, respond and recover against abnormal/suspicious activities on the network. You will be working against a global hacker network who is threatening to disrupt the overall operations of critical infrastructure sites for nefarious means.

Cyber Defender - The Game, teaches cyber professionals how hackers operate, the cyber kill chain, and tactics, techniques and procedures (TTPs) that can be employed to defend and attack critical infrastructure.

CYBER WARGAMES

Level 1 - Hall 1 - 305

Building on last year's successful Red Team Rumble pilot, we're expanding our contest to create an interactive cybersecurity battlefield where Red and Blue teams alike can clash in friendly rivalry. Participants can engage in several formats including a virtual King-of-the-Hill running throughout DEF CON, short head-to-head team battles, and an extended multi-team competition where strategy and skill determine the victors. Our easy-to-understand yet difficult-to-master environments welcome participants of all skill levels, whether you're seasoned in Cyber Security or just beginning your cyber journey. Our scoreboard provides real-time updates that make the competition exciting for spectators, too!

Working directly with villages from DEF CON, we've created mixed realistic cybersecurity scenarios with accessible, contained challenges to provide an enjoyable experience for everyone. Join us to show off your offensive and defensive tactics, adapt to evolving threats, and collaborate with peers across traditional security boundaries.

Participant Prerequisites

- Laptop required, ethernet port recommended.
- Experience in the following recommended:
  - Working in virtual environments
  - Linux and/or Windows system administration
  - Offensive Security tools and techniques

redteamvillage.io/cyber-wargames

CYCLE OVERRIDE

At 6am on Friday, the @cycle_override crew will be hosting the 14th 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!

cycleoverride.org

DARKNET-NG

Level 1 - Hall 1 - 114

Darknet-NG is an ARG and hands-on hacking contest built for DEF CON. Whether you're new to security or already deep in the game, it's designed to teach real skills through interactive challenges. You'll take on missions in cryptography, OSINT, hardware hacking, reverse engineering, and exploitation. Some you can handle solo. Others will push you to collaborate with others. To complete certain objectives, you'll have to explore DEF CON itself, digging into villages, tracking down key information, and meeting the right people. Everything builds toward a final boss fight where agents must bring together everything they've learned. If you want something more than just watching talks and walking the halls, Darknet-NG is the best way to dive in.

Participant Prerequisites

No prior knowledge, suggest bringing a laptop, could be played on mobile.

darknet-ng.network

DC STICKER DESIGN CONTEST



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

Level 1 - Hall 1 - 110

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).

threatmodel.us

DEF CON BEARD AND MUSTACHE CONTEST

Level 1 - Atrium-East - Contest Stage

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 2025 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.

Participant Prerequisites

Real or Fake facial hair as described above.

dcbeard.net

DEF CON MUD

The DEF CON 33 MUD will be open for practice on May the 1st of 2025. Details will be published April 15th 2025 at https://defcon.wtf

Ever play BattleTech the tabletop RPG, or even the video games? Do you remember multi user dungeons, as in text based gaming from the 90's? The DEF CON MUD contest has resurrected BattleTech MUX for real time text based mech combat. The game will open in May of 2025 and be open to practice until sometime in June when an epic battle of all those registered will happen, the winner of that grand tournament will receive a human badge for entry to DEF CON 33. Pull out your Java based HUD's, (THUD-NG), fight the AI, and other humans, relive the 90's without the pain of dial-up, pilot Mechs, Tanks, and VTOL's and claim your victory.

Participant Prerequisites

Participants will want to practice on the Battletech MUX practice server prior to the grand tournament, there will be tutorial simulations and humans to help you learn the controls. Resources for learning will be on https://defcon.wtf in late April. Participants who have completed the training scenarios will be eligible to compete in the grand tournament in July.

Pre-Qualification

https://defcon.wtf will host details on the pre-qualification requirements in late April, contestants will need to pass the training simulations which teach mech piloting prior to competing in the grand tournament, estimated time required about 4 hours.

defcon.wtf

Nautilus Institute presents...

DEF CON Capture the Flag





Welcome to Capture the Flag at DEF CON 33. We're excited to bring the world series of computer hacking to DEF CON for a fourth and final time.

DEF CON hosts many CTF contests, but this one is special for us and our players. It is almost entirely binaries, all original, and designed to test the top teams in the world, no matter what automated assistance they bring with them. It's an attack-defense contest, which enables even more treachery and creativity from players. Back for a fourth year are LiveCTF head-to-head reversing races, bringing more strategy and excitement to our busy game.

Enjoying the CTF Room

Spectators are welcome while the game is being played, but the space is closed to general humans while we set up and tear it down each day.

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, if we're not heads down trying to fix something.

We have twelve teams that have been working hard to qualify and compete here. Respect their concentration, and don't interrupt them!

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

Qualifying

Twelve teams qualified this year. Maple Mallard Magistrates qualified by winning DEFCON32.CTF one year ago. Friendly Maltese Citizens qualified from HITCON, kalmarunionen from 35C3, and RePokemonedCollections from 0ctf. Blue Water, SuperDiceCode, mhackeroni, Nu1L, Shellphish, KuK Hofhackerei, this year's organizers, and Cold Fusion qualified through our online qualifiers in April.

Think you can hack it in 2026? Keep an eye on DEF CON this winter when your future organizers announce it.





The Future

After Sunday, our tenure as DEF CON CTF organizers is complete, and it's time for us to hand off the excitement of DEF CON CTF to a new team. If you've ever thought you had an amazing idea for a hacking challenge, and a great group of co-conspirators, this is your chance to make an indelible mark on the future of DEF CON and hacking at large. Think you have what it takes? Want to know what it takes? DEF CON needs you!

We have a page of resources for future organizers up at https://nautilus.institute/orga/

DEF CON will announce the selection process some time this fall or winter. Keep an eye on the site, and we'll repost any announcements to https://defcon.social/@nautilusinstitute

Thanks

We'd like to thank everyone who's made DEF CON Capture the Flag an amazing contest to host for the last four years. Whether you're experiencing the DEF CON madness for the first time, or are a grizzled veteran with opinions about decompilers, thank you for making DEF CON a wonderful experience for us and our players. For every CTF player worldwide, whether or not you've ever solved one of our challenges, we're thankful you've given us the opportunity to build a contest for you. Last but absolutely not least, thanks to DT, the C&E team, and all DEF CON goons for running the highlight of our year for last four years.

We hope you enjoy DEF CON Capture the Flag!





https://nautilus.institute

https://defcon.social/@nautilusinstitute

DEF CON SCAVENGER HUNT

Level 1 - Hall 1 - 208

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 5 members, interpret the items, and submit your efforts at the booth to our esteemed judges. Go beyond the basics for bonus points. Legends are born here.

The DEF CON Scavenger Hunt is open to everyone, regardless of skill level or experience, no pre-qualifying necessary. We strive to maintain the balance of a low barrier to entry while providing a challenge that many are eager to take on. Casual players should not be overwhelmed by the list, find a handful of items and have fun. If you are looking to win however, you will need to fully immerse yourself in the DEF CON Scavenger Hunt. Let's make some memories together.

Remember that 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.

www.defconscavhunt.com

DOZIER DRILL LOCKPICKING CHALLENGE

Level 1 - Hall 2 - 701

Have you ever wanted to break out of handcuffs, pick open a closed bag and shoot your buddy in the chest with a nerf gun? So have we, that's why TOOOL presents the Dozer Drill. A fast paced skill based game where you have to free yourself from handcuffs, open a closed bag, and retrieve the nerf gun to be the first to hit the target. Join us throughout the con for qualifier games, and on Saturday for an official bracket tournament.

Participant Prerequisites

Participants must be able to shim handcuffs and pick locks which are both skills we're happy to teach you in the lock pick village. Contestants wishing to enter the official tournament on Saturday must win at least one match against any opponent prior to the tourney in order to have their name entered.

Pre-Qualification

We will be running the game throughout the day prior to the tournament on Saturday. Contestants have to win at least one dozier drill round before they can enter into the official tournament. This helps us to ensure everyone competing holds the minimum skills needed to complete a round.

DUNGEONS@DEF CON

Level 1 - Hall 1 - 205

D@D is a table-top/RPG themed puzzling campaign for teams of 1-4 players. As part of the campaign, teams will unravel crypto challenges, solve physical puzzles, and do other side-quests that will have them interacting with different components of the DEF CON community (villages, goons, NPCs, local wildlife, trolls, etc.) to earn points and progress through a narrative. The theme changes each year, but typically is based loosely on a popular table-top game that fits the theme for DEF CON. Teams learn how to work cooperatively to solve large puzzles, and learn how to solve puzzles that they may have seen in CTFs, escape rooms, or other puzzle venues. The contest is designed to be accessible to all technical levels and all ages.

Pre-registration will occur online the before con as well as Friday morning at 10 in person. Contest will start at 12:00 on Friday

Participant Prerequisites

Some puzzles require being physically present to complete.

www.dungeonsatdefcon.com

EFF TECH TRIVIA

Level 1 - Atrium-East - Contest Stage

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.

Participant Prerequisites

No prerequisites! Just a desire to have fun and come answer some trivia questions. Participants will need to join a team which they can create beforehand or join one ad-hoc during the event!

EMBEDDED CTF

Level 1 - Hall 1 - 401

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 a unique opportunity to explore embedded devices' inner workings and understand their design's security implications.

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 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.

Participant Prerequisites

Contestants will need to bring their own laptop for the competition. That is pretty much it! We will have switches at the tables for them to plug into as well as WiFi that they can connect to for the contest.

embeddedvillage.org

FEET FEUD (HACKER FAMILY FEUD)

Level 1 - Hall 3 - Tracks 1-2

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 Ali Diamond and John Hammond 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.

Participant Prerequisites

Participants are chosen by team captains from the audience at the start of the show. In order to be fair, we try to select participants from all seating areas, so folks who show up later than others still have a chance to volunteer.

Survey: https://forms.gle/SGLqk7ADWKnJNsR97

GENSEC CTF

Level 1 - Hall 1 - 302

AI is changing the game. It is time to hack smarter not just harder, Are you ready to play?

Join us at DEF CON 33, for a new type of CTF where you team up with AI to solve security challenges. This individual CTF will give you a glimpse how to turbo-charge your cybersecurity skills with AI while having fun and winning cool prizes. Regardless of your skill level, we have challenges and events for you. This event is brought to you by Google and Airbus.

HAC-MAN

Level 1 - Hall 1 - 109

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, fruits, 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.

Participant Prerequisites

The only prerequisite to the contest is internet access.

scramble.roguesignal.io/play?game=GM_HACM25

HACK3R RUNW@Y CONTEST

Level 1 - Hall 1 - 201

What is Hack3r Runw@y?

Hack3r Runw@y challenges creative minds in the hacker community to reimagine fashion through the lens of hacking. We're calling all glamorous geeks, crafty coders, and fashionably functional folks to dust off their soldering irons, grab their needles and threads, and unleash their inner designers. Whether you're a seasoned maker or a coding newbie, Hack3r Runw@y has a place for you. Hint: You don't have to know how to program to make cool wearables.

What to Expect:

Participants will submit their creations prior to the event and then walk the runway during our allotted time at DEF CON. Audience should be prepared to be amazed by a runway show unlike any other. Like really. Witness creations that push the boundaries of fashion and technology, showcasing the ingenuity and resourcefulness of the hacker community.

Expect to see:

CONTESTS

Smart Wear that Wows: Garments integrated with LEDs, microcontrollers, sensors, and other tech wizardry, creating dazzling displays of functionality and style.

Digital Design that Dazzles: Visually stunning pieces that use light, color, and texture to create captivating, passive designs.

Functional Fashion: Practical and stylish creations that solve real-world problems, from masks and shields to lockpick earrings and cufflink shims.

Extraordinary Style: Unique and expressive designs that push the boundaries of fashion, incorporating everything from 3D textures and optical illusions to cosplay and security-inspired patterns.

A Hacker Perspective on Fashion:

Hack3r Runw@y brings a unique hacker perspective to DEF CON by demonstrating the power of creativity and problem-solving in a non-traditional context. It showcases how hacking can be applied to art and self-expression, blurring the lines between technology, fashion, and culture. It's about more than just making cool gadgets; it's about pushing boundaries, challenging conventions, and exploring the intersection of technology and human experience.

What You'll Learn:

Hack3r Runw@y offers attendees a glimpse into the creative potential of the hacker community. You'll see firsthand how technical skills can be combined with artistic vision to create truly unique and innovative designs. You'll be inspired by the ingenuity and resourcefulness of the participants, and you might even pick up some ideas for your own projects. It's a chance to learn about new technologies, see them applied in unexpected ways, and connect with a community of like-minded individuals. Hack3r Runw@y teamed up with the DC Maker Community during DEF CON 32 to offer a workshop on sewing LEDs to clothing. Look out for something similar this year.

The Competition:

Participants will compete in four categories for a chance to win in each, plus the coveted People's Choice trophy, where anyone can win, but there will be a twist! Our esteemed judges will select winners based on:

- Uniqueness
- Trendy
- Practical
- Couture
- Creativity
- Relevance
- Originality
- Presentation
- Mastery

Join us at DEF CON 33 for Hack3r Runw@y and witness the future of fashion! Be prepared to be amazed, inspired, and maybe even a little bit hacked. This is an event you won't want to miss!

Participant Prerequisites

There are no prerequisites outside of you wearing something that you made or had a hand in making. You are welcome to model store bought outfits, but you will not qualify for a prize.

Pre-Qualification

Proof that you created the item and signed up via the google form. Submissions due no later than 4pm EST on Saturday, August 10, 2024. Link to form found here: https://hack3rrunway.github.io/

hack3rrunway.github.io

HACKER JEOPARDY

Level 1 - Hall 3 - Tracks 1-2



Have you ever wondered what would happen if you took ostensibly smart people, put them up on a stage, maybe provided a beer or two and started asking really tough technical questions like what port Telnet runs on? Well wonder no more! Back to start its 31st year at DEF CON, Hacker Jeopardy will have you laughing, groaning and wondering where all the brain cells have gone. Some come share an evening of chanting DFIU followed immediately by someone FIU. This is a mature show, 18+.

HACKING BOUNDARY SHIP TERMINAL

Level 1 - Hall 2 - 504

In this Maritime Hacking Village 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 many of our games. All of the games are designed to be entertaining and engaging with the first few hundred who stop by getting a take home copy of the game.

Participant Prerequisites

This is a fun, quick, and simple game, so no prior experience is required.

HARDWARE HACKING VILLAGE CTF

Level 1 - Hall 2 - 802

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.

Participant Prerequisites

While we make many of our challenges approachable without additional tools, things that could come in handy would be a laptop, programmable microcontroller (something 3.3V compatible), hookup wire. Hardware hacking knowledge will help, but it's not required and we try to structure our CTF to be approachable to newcomers.

dchhv.org/challenges

HARDWIRED

Level 3 - W303-W310

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 - Near Networking Bar



Our challenges will follow a theme/storyline so it can be more immersive for players that want this kind of experience, but a player can focus on the technical aspects of the challenges and ignore the theme/storyline without affecting their performance. The challenges will vary in difficulty. ypically an easy difficulty challenge would require a player to understand the concept of a vulnerability to successfully complete it, while a hard one would require experience and the ability to chain together various vectors.

Participant Prerequisites

A laptop and internet connection is required.

ctf.hackthebox.com

ICS VILLAGE CTF

Level 1 - Hall 2 - 805



The ICS Village CTF provides hands-on access to industrial control systems used in critical infrastructure around the world. In this contest, attendees will have to take control of generation facilities, disrupt distribution, and identify malicious activity inside the networks. Attendees will learn how critical infrastructure works, the dependencies of each system, some of the engineering designs from different industries, and tools used worldwide for both hackers and defenders.

Participant Prerequisites

- Bring a laptop.
- No special software is required.
- Wireshark and tools from Kali are helpful but not necessary.

hacktheplanet.ctfd.io

KUBERNETES CTF

Level 1 - Hall 1 - 103

Want to learn more about Kubernetes hacking or compete against other people in a Capture the Flag contest? Sign up on-line and come see us in person/on Discord at the Kubernetes Capture the Flag (CTF) contest .

We have two events - you can play in both if you like.

From Friday to Sunday, we have a non-competitive Learning CTF, where you can go through last year's Kubernetes CTF scenario, referring to a cheat sheet whenever you want. This runs from Friday 12:00 to Sunday 12:00. We'll be in the contest area to support you during:

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

On Saturday only, you can play in the competitive Kubernetes CTF challenge, where teams (of one or more) can build and test their skills. Each team is given access to a single Kubernetes cluster that contains a set of challenges. This runs from 10:30am to 5:30pm on Saturday.

containersecurityctf.com

OCTOPUS GAME 4: THE ORDER OF THE WHITE TENTACLE

Level 1 - Hall 1 - 108



Welcome to the resistance. As a new recruit in the Order of the White Tentacle, you must train to master the elements and restore balance to a world on the brink of chaos. This is a beginner & family-friendly adventure that will test your wisdom, bravery, and teamwork as you bend the elements to solve puzzles, complete missions, and rise through the ranks. Whether you walk the path of fire, water, earth, or air, only those who embrace the balance of all will prove themselves worthy. Will you answer the call and bring harmony to DEF CON 33?

Participant Prerequisites

Phone with a camera will be required to play.

www.mirolabs.info/octopus-game-dc

PASSWORD VILLAGE

Level 1 - Hall 1 - 101

The Password Village provides hands on access to cracking tools like Hashcat and John the Ripper. It can be hard to pop into a new community on the internet and ask questions without having thoroughly read the documentation prior. The village organizers are there to answer all questions regardless of how basic, or advanced in and around the world of password cracking. Need help with contest/village challenge? We got you. Not sure what password cracking is or how to get started? We got you. Working on a thesis for a new attack chain? We go you.

www.passwordvillage.org

CONTESTS

PHISH STORIES

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.

Timing

Phish Stories is a virtual pre-con contest that runs from May 4 to June 21.

www.phishstories.org

PHREAKME

Level 1 - Hall 1 - 106

Ever wondered what hacking looked like in the golden age of phone phreaking? What about today? What can we learn about the old techniques that still plague our current infrastructure? The Hacked Existence PhreakMe Capture the Flag (CTF) brings the classic art of telecom exploitation into the modern era.

The Hacked Existence team is once again hosting a telecom based CTF. The CTF runs on real live VoIP lines routed through a modified asterisk PBX allowing participants to dial in to the CTF from a real world routable telephone phone number. This number is live 24/7 throughout DEF CON, allowing you to hunt the PBX for flags any time, day or night. Also there's a BBS this year and more telecom challenges. The flags are based around 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.

Come test your skills, challenge your knowledge, and dive deep into the world of phreaks.

Participant Prerequisites

A phone, or access to a phone that can dial an american based phone number. The BBS will be both accessible from a modem and also ssh. Ideally people will read books like 'The Cyberthief and the Samurai' and 'Masters of Deception: The Gang That Ruled Cyberspace' and the Cult of the Dead Cow book.

phreakme.com

PINBALL HIGH SCORE CONTEST



Level 1 - Hall 1 - 203

The Pinball High Score contest at DEF CON 33 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 17:00 on Saturday main tournament qualifying will end, tiebreakers will be played(if needed) 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 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, we expect that the community is ready for this challenge!

Stern Pinball has prepared an exclusive DEF CON 33 digital badge that will be available for any attendee to earn for playing in this event. Additional DEF CON specific Insider Connect digital badges and prizes may be unlocked during game play.

This year, we're taking our pinball contest to the next level with the introduction of a custom-built Real-Time Pinball Telemetry (RTPT) device. Designed exclusively for DEF CON 33, these first-of-their-kind, machine-agnostic devices will measure players' physical interactions with games in real time. More than just a scoring tool, RTPT will create new opportunities for engagement—both within our contest and across other DEF CON competitions. Get ready to play like never before!

pinballhackers.com

PROJECT ACCESS: A FOX HUNT IN THE SHADOWS

Level 1 - Hall 1 - 307

The last surviving fragments of Project ACCESS, a defunct open comms initiative, have resurfaced. The faceless OmniCorp thought they had erased it from the spectrum, but rogue operatives are pushing back. Disguised among the DEF CON crowd, Foxes are carrying the pieces needed to reboot the system.

They're broadcasting open signals across the con space. Your job? Track them down, follow the trail, and recover the payloads. Some Foxes are stationary. Others are on the move. All of them have something you need—but they won't just hand it over. You'll have to answer DEF CON trivia, solve puzzles, or earn their trust in creative ways.

This isn't a gear-only hunt. Whether you're rocking SDRs, handheld radios, or just tuned into the right frequency, you've got a shot. It's part signal chase, part real-world goose chase, and 100% hacker weirdness.

Expect:

- Live human Foxes broadcasting short-range signals

- Some Foxes roaming the con floor hunt them down, respectfully

- DEF CON history questions, crypto puzzles, and maybe a social engineering twist or two

- Physical items or clues exchanged when you succeed

- No encryption. No gatekeeping. Just old school radio and clever chaos.

Think you can track the signal, crack the code, and restore the last breath of open access?

Then grab your gear, tune in, and start hunting.

Participant Prerequisites

RF Fox Hunt(s): To participate in the RF fox hunt(s), you will need a radio or scanner that can receive signals in the 2m and/or 70cm Amateur Radio Bands (144.000 MHz - 148.000 MHz, 420.000 MHz - 450.000 MHz).

Something to read NFC cards.

PUB QUIZ AT DEF CON

Level 1 - Atrium-East - Contest Stage

We are back with another Pub Quiz at DEF CON. We had a very successful 2 years hosting this event 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 3rd Pub Quiz at DEF CON 33.

Quiz will consist of 7 rounds question will include 90's/2000's TV and Movies, DEF CON trivia, music, cartoons, 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, and 3rd 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.

RADIO FREQUENCY CAPTURE THE FLAG

Level 1 - Hall 2 - 803

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.

FOR THE NEW FOLKS

This contest is free and open to anyone and everyone. You can sign up and start playing any time during the conference. If you didn't bring your wireless gear don't worry, our virtual RFCTF environment is played over ssh or through a web browser. It may help to have additional tools installed on your local machine, but it is not required.

Read the presentations at: https://rfhackers.com/resources

Hybrid Fun

For DEF CON 33 we will be running in "Hybrid" mode. That means we will have both a physical presence AND the virtual game running simultaneously. All of the challenges we have perfected in the last 2 years in our virtual game will be up and running, available to anyone all over the world (including at the conference), entirely free. In addition to the virtual challenges, we will also have a large number of "in person" only challenges, which do require valid conference admission. These "in-person" only challenges will include our traditional fox hunts, hide and seeks, and king of the hill challenges. Additionally, we will have many challenges which we simply haven't had time or ability to virtualize. Playing only the virtual game will severely limit the maximum available points which you can score, therefore don't expect to place. If you play virtual only, consider the game an opportunity to learn,

practice, hone your skills, and still get on the scoreboard for bragging rights. The virtual challenges which are available will have the same flags as the in-person challenges, allowing physical attendees the choice of hacking those challenges using either (or both) methods of access.

The text box isn't large enough. Please email me for the full version. Abbreviated version above for fun

Participant Prerequisites

- A minimum of a laptop with a web browser and internet connection is required. Additional wireless equipment is optional but can seriously help.

- Everyone of all skill levels are welcome, our game is inviting and free to play.

rfhackers.com

RAITLIN'S CHALLENGE PRESENTED BY THE ILLUMINATI PARTY®

Experience the ultimate test of cognitive prowess with Raitlin's Challenge, a sophisticated collection of visual puzzles presented annually at DEF CON. This intellectually demanding journey pushes participants to their limits through increasingly complex challenges that require mastery of diverse knowledge domains.

The challenge begins with an initial puzzle that serves as a gateway to the main experience. Once solved, competitors gain access to a carefully curated series of visual puzzles presented in an artistically refined format. Each puzzle solved yields a verification string, allowing participants to track their progress through the challenge.

What sets Raitlin's Challenge apart is its comprehensive scope, drawing upon principles from mathematics, science, technology, cryptography, protocols, algorithms, biology, chemistry, programming, engineering, and ancient history. While technical expertise, particularly in hacking, proves advantageous, the true challenge lies in applying abstract thinking across multiple disciplines.

The journey to completion varies significantly among participants, spanning anywhere from days to years. Unlike many competitive events, Raitlin's Challenge maintains its availability beyond DEF CON's conclusion, allowing determined individuals to pursue solutions at their own pace. Those who ultimately succeed earn recognition on the prestigious ledger of completions, joining an elite group of problem-solvers who have demonstrated exceptional intellectual versatility and persistence in unravelling the secrets of the Illuminati Party®.

Participant Prerequisites

Access to a web browser and Internet connection.

dc33.minervallux.com

REALI7Y OVERRUN

Level 1 - Hall 1 - 202

It's hard to tell what's real or not anymore. Deepfakes, AI, LLMs, Sora, unreliable sources of information, data spoofing... it's too much for even the most informed to keep up with, let alone the 99% of us just trying to get by. We're heading quickly to that precipice, close to that point of no return where those who control the money, the power, the GPUs, the energy grid, will control us all. Or worse: where the first artificial intelligences will manipulate us all... We're nearing a memory buffer overflow, a glitch in the matrix, a

/*`/$ REALI7Y OVERRUN $\'*\

Teams will join an interactive multiplayer video 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 encounter challenges and tutorials on video and image validation and cryptographically safe messaging.

Participant Prerequisites

Laptop ideal. Tablet OK. Flagship phone possibly. We require no special knowledge to play, though to win, knowing a bit about general cryptographic concepts (private/public key authentication and signing), LLM-based services (ChatGPT, Dall-E) and DEF CON trivia would help.

reali7y-over.run

RED ALERT ICS CTF

Level 1 - Hall 1 - 304

Step into the world of Industrial Control System (ICS) security with Red Alert ICS CTF, a competition built by hackers, for hackers. Hosted by the RedAlert Lab of NSHC Security, this contest is all about pushing the limits—breaking through layers of security in a real Operational Technology (OT) environment until you seize full control of ICS components.

Since its debut at DEF CON 26, Red Alert ICS CTF has been a must-attend event, growing bigger and tougher each year. Now recognized as a Black Badge contest at DEF CON 32, DEF CON 31, and DEF CON 26, it's the ultimate proving ground for those who thrive in the high-stakes world of ICS hacking.

What makes this CTF unique? Live ICS hardware from top industry vendors, simulating real-world critical infrastructure. Participants will interact with actual devices, manipulate industrial processes, and exploit vulnerabilities in real time. This isn't just another CTF—this is a full-scale ICS cyber battleground.

Are you ready to test your skills, outsmart industrial defenses, and dominate the ICS arena? The challenge awaits.

Participant Prerequisites

Bring your laptop and a network adapter (if your laptop lacks one). Refresh your knowledge of ICS protocols and processes to stay ahead in the competition.

RED TEAM VILLAGE CTF

Level 1 - Hall 1 - 406

The Red Team Capture the Flag (CTF) competition at DEF CON is a challenging and exciting event that tests the skills of participants in offensive security. The objective of the Red Team CTF is for teams to successfully complete challenges faced by Red Teams.

The Red Team CTF is designed to simulate real-world scenarios in which attackers attempt to penetrate the security of a network or system. Participants are expected to use a wide range of hacking techniques, tools, and skills to identify and exploit vulnerabilities in the target network.

Teams are typically composed of experienced hackers, penetration testers, and security researchers who have a deep understanding of the latest cybersecurity threats and attack techniques. They must work together to uncover and exploit vulnerabilities in the target network, while also evading detection and countermeasures put in place by the Blue Team.

The Red Team CTF at 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.

Participant Prerequisites

Participants are required to bring a laptop with the ability to connect to DEF CON WiFi or other internet connection.

redteamvillage.io

SCAMBAIT VILLAGE CONTEST

Level 1 - Hall 1 - 407

The Scambait Village Contest will test participants skills in scambaiting! Players earn points for spending time on the phone with a scammer in order to waste the scammers time so they aren't affecting real potential victims. Participants get extra points for achievements or milestones of the call — whether it is finding more scam numbers to call, having a scammer connect to their dedicated bait virtual machine, or hacking the scam to fatigue and frustrate online scammers who steal money every day. Check out the Scambait Village Content to play or spectate live calls and learn all about the art of scambaiting.

Participant Prerequisites

Participants should be prepared with a laptop that is able to run virtual machines. Some computers and laptops may be provided for use, but this is a limited quantity and players should be prepared to bring their own devices. Special knowledge of how to participate in the Scambait Village Contest will be presented and made available within the Scambait Village.

SOCIAL ENGINEERING COMMUNITY VISHING COMPETITION (SECVC)

Level 3 - W317-W319

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 1-2 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!

Participant Prerequisites

To successfully participate, selected competing teams need reliable internet access and a computer for the remote phase to conduct OSINT and research. For the onsite phase at DEF CON, participants must be present at the Social Engineering Community village, where all necessary equipment is provided. No prior vishing experience is required, but familiarity with social engineering techniques, OSINT gathering, and rapport-building skills can be beneficial. The competition is open to all skill levels, making it both educational and competitive.

www.se.community/vishing-competition

SPYVSPY

Level 1 - Hall 1 - 113

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.

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.

Participant Prerequisites

A laptop is highly recommended, although much of the content will be doable on a smartphone.

spyvspy.fottr.io

CONTESTS

TASKMOOSTER

Level 1 - Atrium-East - Contest Stage

What happens when you gather 4 hackers together to complete silly tasks, rank their execution, and see who ends up with the most points at the end? Taskmooster, that's what. Inspired by the UK game show Taskmaster, TaskMooster is brings lateral thinking, comedic tasks, and general shenanigans to DEF CON. What? You haven't heard of Taskmaster? Seriously, stop reading this program right now and go watch at least one episode. All seasons are available to stream on YouTube, and it's totally binge-worthy.

Come join the contestants as they see how they performed for each task and get graded by our very own TaskMooster. The winner gets to take home the coveted Golden Telephone and bragging rights for being the TaskMooster champion.

Participant Prerequisites

The participants are selected in advance. We will film the pre-con tasks in Maryland several months before DEF CON and then will convene on stage at DEF CON in August for the live event.

shmoocon.org

TELECHALLENGE

Level 1 - Hall 1 - 213

The TeleChallenge might be the craziest experience you will ever have on your phone. We create a fully immersive virtual world, in which an epic battle of wits and skill is contained. While we do show up in the real world as well, reality is optional. The TeleChallenge is playable entirely on a touch tone phone. Tune in, turn on, and drop out.

You'll have no context, no remote, and no TV guide. You won't know where you are, what you're doing, or what is real. How deep does the rabbit hole go? That largely depends on you. It's dangerous to go alone, so get your friends and family together in a calling circle bundle. Diverse perspectives are a great way to look around corners and avoid blind spots, but you'll need more than these alone. This is a very difficult contest, and is designed to be among the most challenging at DEF CON. Winning teams have always been serious and dedicated, but not necessarily experienced. One previous winning team was at their very first DEF CON!

Joining the TeleChallenge means you're joining an immersive experience. You may place and receive live and recorded calls as part of your participation. The DEF CON Code of Conduct applies both to players and to the TeleChallenge, and the contest is rated PG-13.

Where can you find us? Part of the Challenge is discovering the TeleChallenge. And don't forget to use promo code #MICHAELKEY

telechallenge.org

THE GOLD BUG

Level 1 - Hall 1 - 211

From Caesar to Vigenère, or DES to RSA, hackers have been making and breaking codes for thousands of years. If you love puzzles, this is the perfect opportunity to join this fine tradition and break some codes!

The Gold Bug is an annual puzzle hunt at DEF CON, focused on cryptography. While some puzzles will dig into substitution ciphers or more modern algorithms, others may test your logic and pattern recognition.

The Gold Bug is accessible to all, with some simpler puzzles for warmup or beginners (even kids!), and others that will require you to keep digging and wonder how deep the layers will go. Whether you want to hack on puzzles solo or with a team, join us at https://goldbug.cryptovillage.org to get started!

Participant Prerequisites

No prior experience or specific knowledge is required to participate in The Gold Bug. Participants will need to use a web browser to access the puzzles and submit answers. Puzzles may take such forms as images, PDF files, web pages, or multimedia files.

goldbug.cryptovillage.org

THE PWNIE AWARDS

Level 1 - Hall 3 - Track 1

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.

Participant Prerequisites

We do not have any strict prerequisites. We publish nominees ahead of time to give people a heads up that they may want to attend DEF CON to accept the award if they win.

Pre-Qualification

Kind of! We accept nominees earlier in the year and then publish and announce them at Summercon every year. Summercon will be held in Brooklyn, NY on 7/11/2025. Members of the community and past Pwnie Award Winners then vote on who should win each category. Those winners are then announced during the show at DEF CON.

pwnies.com

TIN FOIL HAT

Level 1 - Hall 1 - 204

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.

www.psychoholics.org/tfh

VENATOR AURUM

With Venator Aurum, we invite you to step into the shadows of the digital realm, where your wits, skills, and tenacity will be tested like never before. This contest is a thrilling journey through the labyrinth of the hacker underground, designed to push your technical boundaries and ignite your passion for cybersecurity through mind-bending challenges. In this gauntlet of digital intrigue and real-world enigmas, you'll decrypt ancient ciphers, crack impenetrable codes, manipulate hardware at the edge of possibility, and unravel puzzles that blur the line between the virtual and the tangible. Whether you're a seasoned cryptographer, a reverse-engineering virtuoso, or a 1337 PWN wizard, Venator Aurum has something to test your limits. Dare to outthink, out code, and outmaneuver the best? Step into the hunt. The gold awaits those who can seize it

Participant Prerequisites

While not required, these resources will help: laptop and/or smartphone

venatoraurum.org

WARL0CK GAM3Z CTF

Level 1 - Hall 1 - 212

warl0ck gam3z CTF is a hands-on 24/7 throw-down, 3 time black badge hacker competition, focusing on areas of physical security, digital forensics, hacker challenges and whatever craziness our exploit team develops. This is an online framework so participants can access it regardless of where they are or what network they are connected to via laptop, netbook, tablet or phone.

Most challenges require participants to download something that pertains to the problem at hand and solve the challenge using whatever tools, techniques or methods they have available.There are a multitude of point gainers on and off the game board. Extra point gainers will randomly appear on the game board in the form of The Judge, Bonus Questions, Free Tokens, One Time Tokens, Movie Trivia Quotes, Scavenger Hunts (online and onsite), Lock Picking (onsite) and Flash Challenges. Be careful of the 50/50 Token which may add or subtract points to your score.

The game board contains a scoring area so participants can view current standings. There is always on onsite/online moderator to assist participants that may be experiencing issues as well. All events highlights that occur on the game board are sent o to Twitter as they happen. Additionally, our Facebook site will be populated with information regarding the challenge and the current state of events.

WHOSE SLIDE IS IT ANYWAY?

Level 1 - Hall 3 - Tracks 1-2

"Whose Slide Is It Anyway?" is the unholy union of improv comedy, hacking, and slide deck sado-masochism. We are the embodiment of the hacker battle cry "FUCK IT, WE'LL DO IT IN PROD."

Our team of slide monkeys will create a stupid amount of short slide decks on whatever nonsense tickles our fancies. Slides are not exclusive to technology, they can and will be about anything. Contestants will take the stage and choose a random number corresponding to a specific slide deck. They will then improvise a minimum 5 minute / maximum 10 minute lightning talk, becoming instant subject matter experts on whatever topic/stream of consciousness appears on the screen.

But....why?

Because for us, the stage is hallowed ground and since stupidity can't be stopped, we decided to weaponize it. 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.

Participant Prerequisites

A blatant and offensive disregard to any and all comfort zones to which one has heretofore been accustomed.

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-33/dc-33-speakers.html

FRIDAY

Jeff "The Dark Tangent" Moss

WELCOME TO DEF CON 33!

Friday at 10:00 in Track 1
20 minutes

Anna portasynthinca3 Antonenko

REMOTE CODE EXECUTION VIA MIDI MESSAGES

Friday at 10:00 in Track 2
45 minutes | Demo, Exploit

Alon "alon_leviev" Leviev, Netanel Ben Simon

BITUNLOCKER: LEVERAGING WINDOWS RECOVERY TO EXTRACT BITLOCKER SECRETS

Friday at 10:00 in Track 3
45 minutes | Demo, Exploit

Farzan Karimi

PAYWALL OPTIONAL: STREAM FOR FREE WITH A NEW TECHNIQUE, RECURSIVE REQUEST EXPLOITS (RRE)

Friday at 10:00 in Track 4
20 minutes | Demo, Exploit, Tool

Joseph "stoppingcart" Gabay

THE ONE BITCOIN HEIST: MAKING A CUSTOM HASHCAT MODULE TO SOLVE A DECADE-OLD PUZZLE CHALLENGE

Friday at 10:00 in Track 5
45 minutes | Tool

DC101 PANEL

Friday at 10:30 in Track 1
45 minutes

Tom Tervoort

NO VPN NEEDED? CRYPTOGRAPHIC ATTACKS AGAINST THE OPC UA PROTOCOL

Friday at 10:30 in Track 4
45 minutes | Demo, Exploit, Tool

Ori David

VIRTUALIZATION-BASED (IN)SECURITY - WEAPONIZING VBS ENCLAVES

Friday at 11:00 in Track 3
45 minutes | Demo, Tool

Michael "mtu" Torres, Zane "earl" Hoffman

INSIDE LOOK AT A CHINESE OPERATIONAL RELAY NETWORK

Friday at 11:00 in Track 5
45 minutes

Michael "bouncyhat" Weber

CHROMEALONE: TRANSFORMING A BROWSER INTO A C2 PLATFORM

Friday at 11:30 in Track 4
45 minutes | Demo, Tool

Adam "UNC1739" Crosser

GHOST CALLS: ABUSING WEB CONFERENCING FOR COVERT COMMAND & CONTROL

Friday at 12:00 in Track 2
45 minutes | Demo, Tool

Ji'an "azraelxuemo" Zhou, Lishuo "ret2ddme" Song

SAFE HARBOR OR HOSTILE WATERS: UNVEILING THE HIDDEN PERILS OF THE TORCHSCRIPT ENGINE IN PYTORCH

Friday at 12:00 in Track 3
45 minutes | Demo, Exploit, Tool

Rear Admiral John Mauger, USCG (Ret.)

THE ULTIMATE HACK: APPLYING LESSONS LEARNED FROM THE LOSS OF TITAN TO MARITIME CYBERSECURITY

Friday at 12:00 in Track 5
20 minutes

Christopher "xoreaxeaxeax" Domas

GHOSTS IN THE MACHINE CHECK - CONJURING HARDWARE FAILURES FOR CROSS-RING PRIVILEGE ESCALATION

Friday at 12:30 in Track 1
45 minutes | Demo, Exploit, Tool

Mark Omo, James Rowley

CASH, DRUGS, AND GUNS: WHY YOUR SAFES AREN'T SAFE

Friday at 12:30 in Track 4
45 minutes | Demo, Exploit, Tool

Maksim Shudrak

EDGE OF TOMORROW: FOILING LARGE SUPPLY CHAIN ATTACKS BY TAKING 5K ABANDONED S3 BUCKETS FROM MALWARE AND BENIGN SOFTWARE

Friday at 12:30 in Track 5
45 minutes | Demo, Exploit, Tool

George Hughey, Rohit Mothe

WHAT IS DEAD MAY NEVER DIE: THE GHOST OF INTERNET EXPLORER IN WINDOWS: MAPURLTOZONE

Friday at 13:00 in Track 2
45 minutes | Demo, Exploit

Dirk-jan Mollema

ADVANCED ACTIVE DIRECTORY TO ENTRA ID LATERAL MOVEMENT TECHNIQUES

Friday at 13:00 in Track 3
45 minutes | Demo

Cooper "CyberTiger" Quintin, oopsbagel

RECORDING PCAPS FROM STINGRAYS WITH A $20 HOTSPOT

Friday at 13:30 in Track 1
45 minutes | Demo, Tool

Qidan "flanker_hqd" He

DEAD MADE ALIVE AGAIN: BYPASSING INTENT DESTINATION CHECKS AND REINTRODUCING LAUNCHANYWHERE PRIVILEGE ESCALATION

Friday at 13:30 in Track 4
45 minutes | Demo, Exploit

Christophe Tafani-Dereeper, Matt Muir

WEAPONIZING TRUST: INVESTIGATING A THREAT ACTOR TARGETING SECURITY RESEARCHERS AND ACADEMICS

Friday at 13:30 in Track 5
45 minutes | Demo, Tool

Ryan Emmons

DISGUISEDELIMIT: EXPLOITING SYNOLOGY NAS WITH DELIMITERS AND NOVEL TRICKS

Friday at 14:00 in Track 2
45 minutes | Demo, Exploit, Tool

Ron Ben Yizhak

YOU SNOOZE YOU LOSE: RPC-RACER WINNING RPC ENDPOINTS AGAINST SERVICES

Friday at 14:00 in Track 3
45 minutes | Demo, Exploit, Tool

Richard "richeeta" Hyunho Im

SIRI-OUSLY LEAKY: EXPLORING OVERLOOKED ATTACK SURFACES ACROSS APPLE'S ECOSYSTEM

Friday at 14:30 in Track 4
45 minutes | Demo, Exploit

Andrew "Spike" Brandt

FIREWALLS UNDER FIRE: CHINA'S 5+ YEAR CAMPAIGN TO PENETRATE PERIMETER NETWORK DEFENSES

Friday at 14:30 in Track 5
45 minutes

Chiao-Lin "Steven Meow" Yu

GATEWAYS TO CHAOS - HOW WE PROVED MODEMS ARE A TICKING TIME BOMB THAT HACKERS CAN ACCESS EVERYWHERE

Friday at 15:00 in Track 2
45 minutes | Demo, Exploit, Tool

Shu-Hao, Tung 123ojp

FROM SPOOFING TO TUNNELING: NEW RED TEAM'S NETWORKING TECHNIQUES FOR INITIAL ACCESS AND EVASION

Friday at 15:00 in Track 3
45 minutes | Demo, Exploit, Tool

Patrick Wardle

MASTERING APPLE'S ENDPOINT SECURITY FOR ADVANCED MACOS MALWARE DETECTION

Friday at 15:30 in Track 1
45 minutes | Demo, Tool

Reynaldo “buh0”, nyx

UNMASKING THE SNITCH PUCK: THE CREEPY IOT SURVEILLANCE TECH IN THE SCHOOL BATHROOM

Friday at 15:30 in Track 4
45 minutes | Exploit, Tool

Harrison Sand, Erlend Leiknes

SO LONG, AND THANKS FOR ALL THE PHISH

Friday at 15:30 in Track 5
45 minutes | Demo

Yuval Gordon

THE (UN)RIGHTFUL HEIR: MY DMSA IS YOUR NEW DOMAIN ADMIN

Friday at 16:00 in Track 2
45 minutes | Demo, Exploit

Alejandro “TheMalwareGuardian” Vazquez, Maria “drkrysSrng” San Jose

INFECTING THE BOOT TO OWN THE KERNEL: BOOTKITS AND ROOTKITS DEVELOPMENT

Friday at 16:00 in Track 3
45 minutes | Demo, Tool

James “albinowax” Kettle

HTTP/1.1 MUST DIE! THE DESYNC ENDGAME

Friday at 16:30 in Track 1
45 minutes | Exploit, Tool

Eugene “spaceraccoon” Lim

ESCAPING THE PRIVACY SANDBOX WITH CLIENT-SIDE DEANONYMIZATION ATTACKS

Friday at 16:30 in Track 4
45 minutes | Demo, Exploit

Alex Holden

KILLING KILLNET

Friday at 16:30 in Track 5
20 minutes

Max Bazalii, Marius Fleischer

ORION - FUZZING WORKFLOW AUTOMATION

Friday at 17:00 in Track 2
45 minutes | Demo, Tool

Sigusr Polke

EMULATING EMBEDDED LINUX DEVICES AT SCALE WITH LIGHT-TOUCH FIRMWARE REHOSTING

Friday at 17:00 in Track 3
45 minutes | Demo, Tool

Mikko Hypponen

BUILDING A MALWARE MUSEUM

Friday at 17:00 in Track 5
45 minutes

Tal “TLP” Peleg, Coby Abrams

RUSTY PEARLS: POSTGRES RCE ON CLOUD DATABASES

Friday at 17:30 in Track 1
20 minutes | Demo, Exploit

Cernica Ionut Cosmin

SILENT LEAKS: HARVESTING SECRETS FROM SHARED LINUX ENVIRONMENTS

Friday at 17:30 in Track 4
20 minutes | Demo, Exploit

SATURDAY

Yoav Magid

APPLESTORM - UNMASKING THE PRIVACY RISKS OF APPLE INTELLIGENCE

Saturday at 10:00 in Track 2
45 minutes | Demo, Tool

Noam Moshe

TURNING CAMERA SURVEILLANCE ON ITS AXIS

Saturday at 10:00 in Track 3
20 minutes | Demo, Exploit

Patrick Wardle

BINARY FACADES: REVERSING APPROACHES TO EXTRACT EMBEDDED SCRIPTS IN COMPILED MACOS MALWARE

Saturday at 10:00 in Track 4
20 minutes | Demo

Thomas “fr0gger_” Roccia

WHERE’S MY CRYPTO, DUDE? THE ULTIMATE GUIDE TO CRYPTO MONEY LAUNDERING (AND HOW TO TRACK IT)

Saturday at 10:00 in Track 5
45 minutes | Demo, Tool

Marcell Szakály, Jan “SP3ZN45” Berens, Sebastian Köhler

ONE MODEM TO BRICK THEM ALL: EXPLOITING VULNERABILITIES IN THE EV CHARGING COMMUNICATION

Saturday at 10:30 in Track 3
45 minutes | Demo, Exploit

Alejandro “0xedh” Hernando, Borja “borjmz” Martinez

KILL CHAIN RELOADED: ABUSING LEGACY PATHS FOR STEALTH PERSISTENCE

Saturday at 10:30 in Track 4
45 minutes | Demo

Adam “pi3” Zabrocki, Marko Mitic

HOW TO SECURE UNIQUE ECOSYSTEM SHIPPING 1 BILLION+ CORES?

Saturday at 11:00 in Track 1
45 minutes

Zhengyu Liu, Jianjia Yu

THE DOMINO EFFECT: AUTOMATED DETECTION AND EXPLOITATION OF DOM CLOBBERING VULNERABILITY AT SCALE

Saturday at 11:00 in Track 2
45 minutes | Demo, Exploit, Tool

Ben “polygonben” Folland

MAN-IN-THE-MALWARE: INTERCEPTING ADVERSARIAL COMMUNICATIONS

Saturday at 11:00 in Track 5
45 minutes | Demo

Tal Skverer

BREAKIN ‘EM ALL – OVERCOMING POKEMON GO’S ANTI-CHEAT MECHANISM

Saturday at 11:30 in Track 3
45 minutes

Shang-De “HackerPeanutJohn” Jiang, Dong-Yi “Kazma Ye” Ye, Tung-Lin “Echo Lee” Lee

ORIGINAL SIN OF SSO: MACOS PRT COOKIE THEFT & ENTRA ID PERSISTENCE VIA DEVICE FORGERY

Saturday at 11:30 in Track 4
45 minutes | Demo, Tool

Ji’an “azraelxuemo” Zhou, Ying Zhu, ZiYang “lz2y” Li

CLIENT OR SERVER? THE HIDDEN SWORD OF DAMOCLES IN KAFKA

Saturday at 12:00 in Track 1
45 minutes | Demo, Exploit

Mickey Shkatov, Jesse Michael

HELP! LINUX IN MY WEBCAM! (•_•)

Saturday at 12:00 in Track 2
45 minutes | Demo, Exploit, Tool

Aviad Hahami

NOT JUST A PIPELINE LEAK: RECONSTRUCTING THE REAL ATTACK BEHIND TJ-ACTIONS

Saturday at 12:00 in Track 5
45 minutes

Keane Lucas

CLAUDE—CLIMBING A CTF SCOREBOARD NEAR YOU

Saturday at 12:30 in Track 3
45 minutes | Demo

Mark “LargeCardinal” Carney, Victoria “V__Wave” Kumaran

DIAMONDS ARE FOR HACKERS - BUILDING THE FIRST FULLY OPEN SOURCE AND HACKABLE QUANTUM SENSOR

Saturday at 12:30 in Track 4
45 minutes | Demo, Tool

Olivier Bilodeau, Estelle Ruellan

HACKERS DROPPING MID-HEIST SELFIES: LLM IDENTIFIES INFORMATION STEALER INFECTION VECTOR AND EXTRACTS IOCS

Saturday at 13:00 in Track 1
45 minutes | Demo, Tool

TALKS

Richard "neuralcowboy" Thieme

THINKING LIKE A HACKER IN THE AGE OF AI

Saturday at 13:00 in Track 2
45 minutes

Roger "arma" Dingledine

STORIES FROM A TOR DEV

Saturday at 13:00 in Track 5
45 minutes

Erwin "Dollarhyde" Karincic, Woody

ONE KEY, TWO KEY, I JUST STOLE YOUR GOTENNA KEY

Saturday at 13:30 in Track 3
45 minutes | Demo, Exploit, Tool

Marco Casagrande, Daniele Antonioli

CTRAPS: CTAP IMPERSONATION AND API CONFUSION ATTACKS ON FIDO2

Saturday at 13:30 in Track 4
45 minutes | Demo, Exploit, Tool

Valerio "MrSaighnal" Alessandroni

RATS & SOCKS ABUSING GOOGLE SERVICES

Saturday at 14:00 in Track 1
20 minutes | Demo, Tool

Anthony "Coin" Rose, Jake "Hubble" Krasnov

REBADGED, RELABELED, AND ROOTED: PWNAGE VIA THE SOLAR SUPPLY CHAIN

Saturday at 14:00 in Track 2
45 minutes | Demo, Exploit

Benjamin "bmixonbaca" Mixon-Baca

TSPU: RUSSIA'S FIREWALL AND DEFENDING AGAINST THE FUTURE OF DIGITAL REPRESSION

Saturday at 14:00 in Track 5
45 minutes | Demo

Archwisp

HAKCING OBD-II EMISSIONS TESTING

Saturday at 14:30 in Track 1
20 minutes | Demo, Tool

Philippe "phLaul" Laulheret

REVAULT! COMPROMISED BY YOUR SECURE SOC

Saturday at 14:30 in Track 3
45 minutes | Demo, Exploit, Tool

Hannah Zhao, Alexis Hancock, Cooper "CyberTiger" Quintin, Lisa Femia, Thorin Klosowski

ASK EFF

Saturday at 14:30 in Track 4
105 minutes

Marek Tóth

BROWSER EXTENSION CLICKJACKING: ONE CLICK AND YOUR CREDIT CARD IS STOLEN

Saturday at 15:00 in Track 1
45 minutes | Demo, Exploit

HD Moore

SHAKING OUT SHELLS WITH SSHAMBLE

Saturday at 15:00 in Track 2
20 minutes | Demo, Exploit, Tool

Jon DiMaggio, John Fokker

GHOSTS OF REVIL: AN INSIDE LOOK WITH THE HACKER BEHIND THE KASEYA RANSOMWARE ATTACK

Saturday at 15:00 in Track 5
45 minutes

Bill Demirkapi

METAL-AS-A-DISSERVICE: EXPLOITING LEGACY FLAWS IN CUTTING-EDGE CLOUDS

Saturday at 15:30 in Track 2
45 minutes | Demo, Exploit

David "johnnyspandex" Cash, Rich "Buffaloverflow" Warren

ZERO TRUST, TOTAL BUST - BREAKING INTO THOUSANDS OF CLOUD-BASED VPNS WITH ONE BUG

Saturday at 15:30 in Track 3
45 minutes | Demo, Exploit

Keanu "RedByte" Nys

TURNING MICROSOFT'S LOGIN PAGE INTO OUR PHISHING INFRASTRUCTURE

Saturday at 16:00 in Track 1
45 minutes | Demo

Micah "micahflee" Lee

"WE ARE CURRENTLY CLEAN ON OPSEC": THE SIGNALGATE SAGA

Saturday at 16:00 in Track 5
45 minutes

Joe "securelyfitz" FitzPatrick, Grace "Baelfire" Parrish

DIRECT MEMORY, ACCESS EVERYWHERE

Saturday at 16:30 in Track 2
45 minutes | Demo, Tool

Agostino "Van1sh" Panico

DE-VIRTUALIZING THE DRAGON: AUTOMATED UNPACKING AND DEOBFUSCATION OF NESTED VM-BASED PROTECTORS USING SYMBOLIC EXECUTION AND TAINT TRACKING

Saturday at 16:30 in Track 3
45 minutes | Demo, Tool

Leon "leonjza" Jacobs

7 VULNS IN 7 DAYS: BREAKING BLOATWARE FASTER THAN IT'S BUILT

Saturday at 16:30 in Track 4
45 minutes | Demo, Exploit

Ben Gardiner

BLIND TRAILER SHOUTING

Saturday at 17:00 in Track 1
45 minutes | Demo

Wesley McGrew

AMBER64: MINING HACKER HISTORY FROM OVER HALF A MILLION COMMODORE 64 DISKS

Saturday at 17:00 in Track 5
45 minutes | Demo, Tool

Edward "Actuator" Warren

HACKING HOTSPOTS: PRE-AUTH REMOTE CODE EXECUTION, ARBITRARY SMS & ADJACENT ATTACKS ON 5G AND 4G/LTE ROUTERS

Saturday at 17:30 in Track 2
20 minutes | Demo, Exploit

Andrew "Helicopters of DC" Logan

VOICE CLONING AIR TRAFFIC CONTROL: VULNERABILITIES AT RUNWAY CROSSINGS

Saturday at 17:30 in Track 3
20 minutes

Antoine Goichot

OVERLAPS: OVERRIDING LAPS LOGIC

Saturday at 17:30 in Track 4
20 minutes | Demo, Tool

SAT/SUN

SUNDAY

Ben Nassi, Or "oryair1999" Yair, Stav Cohen

INVITATION IS ALL YOU NEED! INVOKING GEMINI FOR WORKSPACE AGENTS WITH A SIMPLE GOOGLE CALENDAR INVITE

Sunday at 10:00 in Track 1
45 minutes | Demo, Exploit

Philip "Soldier of FORTRAN" Young

SSH-NANIGANS: BUSTING OPEN THE MAINFRAMES IRON FORTRESS THROUGH UNIX

Sunday at 10:00 in Track 2
45 minutes | Demo

Kenneth Miltenberger, Nicholas Fredericksen

FROM SHANGHAI TO THE SHORE: THE SILENT THREAT IN GLOBAL SHIPPING

Sunday at 10:00 in Track 3
20 minutes

Tobias "ItsSixtyNein" Diehl

MIND THE DATA VOIDS: HIJACKING COPILOT TRUST TO DELIVER C2 INSTRUCTIONS WITH MICROSOFT AUTHORITY

Sunday at 10:00 in Track 4
20 minutes | Demo, Exploit

Sarah Powazek, Jake Braun, Adrien Ogee

CYBER VOLUNTEERING AND COMMUNITY DEFENSE - DEF CON FRANKLIN AND THE CYBER RESILIENCE CORPS 1 YEAR IN

Sunday at 10:00 in Track 5
45 minutes

Bramwell Brizendine

CAN'T STOP THE ROP: AUTOMATING UNIVERSAL ASLR BYPASSES FOR WINDOWS

Sunday at 10:30 in Track 3
45 minutes | Demo, Exploit, Tool

TALKS

Agostino "Van1sh" Panico

JAILBREAKING THE HIVEMIND: FINDING AND EXPLOITING KERNEL VULNERABILITIES IN THE EBPF SUBSYSTEM

Sunday at 10:30 in Track 4
45 minutes | Demo, Tool

Sam Collins, Marius Muench, Tom Chothia

PLAYING DIRTY WITHOUT CHEATING - GETTING BANNED FOR FUN AND NO PROFIT

Sunday at 11:00 in Track 1
45 minutes | Demo

Enzo Damato

JOURNEY TO THE CENTER OF THE PSTN: HOW I BECAME A PHONE COMPANY, AND WHY YOU SHOULD TOO.

Sunday at 11:00 in Track 2
45 minutes

Carl Miller, Chris Monteiro

KILL LIST: HACKING AN ASSASSINATION SITE ON THE DARK WEB

Sunday at 11:00 in Track 5
45 minutes

Shourya Pratap Singh, Jonny Lin, Daniel Seetoh

PASSKEYS PWNED: TURNING WEBAUTHN AGAINST ITSELF

Sunday at 11:30 in Track 3
45 minutes | Demo, Exploit, Tool

George "sophron" Chatzisofroniou

BREAKING WI-FI EASY CONNECT: A SECURITY ANALYSIS OF DPP

Sunday at 11:30 in Track 4
45 minutes | Exploit

PHRACK PANEL

Sunday at 12:00 in Track 1
45 minutes

Quentin "croco_byte" Roland, Wilfried "tiyeuse" Bécard

TURNING YOUR ACTIVE DIRECTORY INTO THE ATTACKER'S C2: MODERN GROUP POLICY OBJECTS ENUMERATION AND EXPLOITATION

Sunday at 12:00 in Track 2
45 minutes | Demo, Tool

Godman666

CARDING, SABOTAGE & SURVIVAL: A DARKNET MARKET VETERAN'S STORY

Sunday at 12:00 in Track 5
45 minutes | Demo

Or "oryair1999" Yair, Shahak Morag

WIN-DOS EPIDEMIC: A CRASH COURSE IN ABUSING RPC FOR WIN-DOS & WIN-DDOS

Sunday at 12:30 in Track 3
45 minutes | Demo, Exploit, Tool

Gabriel Gegenhuber, Maximilian Günther

SILENT SIGNALS: EXPLOITING SECURITY AND PRIVACY SIDE-CHANNELS IN END-TO-END ENCRYPTED MESSENGERS

Sunday at 12:30 in Track 4
45 minutes | Demo, Exploit, Tool

Eaton Zveare, Roshan Piyush

UNEXPECTED CONNECTIONS: HOW A VULNERABILITY IN OBSCURE DEALER SOFTWARE COULD HAVE UNLOCKED YOUR CAR FROM ANYWHERE

Sunday at 13:00 in Track 5
45 minutes | Demo, Exploit

Scott "ScottCTaylor12" Taylor

PLANTING C4: CROSS-COMPATIBLE EXTERNAL C2 FOR ALL YOUR IMPLANTS

Sunday at 13:30 in Track 3
20 minutes | Tool

Mehdi "kalimer0x00" Elyassa

SCCM: THE TREE THAT ALWAYS BEARS BAD FRUITS

Sunday at 13:30 in Track 4
45 minutes | Demo, Exploit, Tool

Contest Closing Ceremonies & Awards

SUNDAY AT 13:30 IN TRACKS 1-2

90 minutes

Cyrus Parzian

LOADING MODELS, LAUNCHING SHELLS: ABUSING AI FILE FORMATS FOR CODE EXECUTION

Sunday at 14:00 in Track 3
20 minutes | Demo

Russell Phillips

HOW TO FAKE A BADGE LIKE A PRO: 11 TIPS TO COUNTERFEITING EVENT CREDENTIALS

Sunday at 14:00 in Track 5
20 minutes | Demo

Jeff "The Dark Tangent" Moss

DEF CON CLOSING CEREMONIES & AWARDS

Sunday at 15:00 in Tracks 1-2
180 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

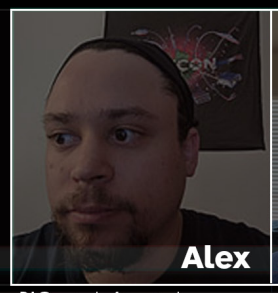
DEF CON STORE: HTTPS://SHOP.DEFCON.ORG
DEF CON TRAINING: HTTPS://TRAINING.DEFCON.ORG/

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 33/



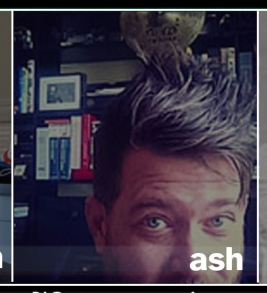
BIO Jack of Few Trades, Master of None

AKA None yet. Working on it.



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

AKA AY-AY-RON



BIO Resurrenctionist of electromechanical detritus.



BIO It's on LinkedIn if you actually care.

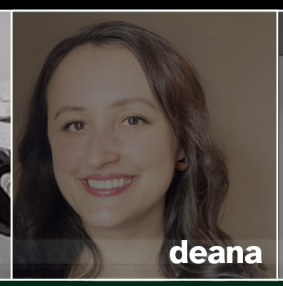


BIO Has consistently forgotten to submit a bio for the Review Board.

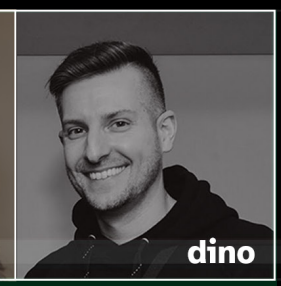
AKA FishSupreme



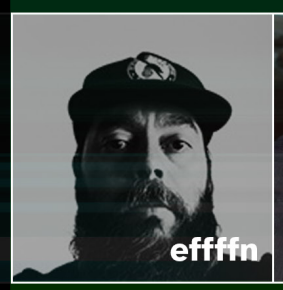
BIO Isn't a good enough human being to be self-deprecating in his bio.



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



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



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



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.



BIO Bio to come.



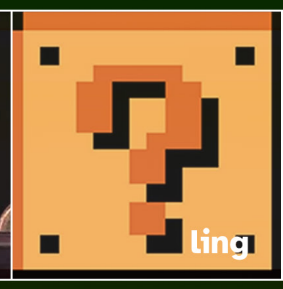
BIO Demo Labs Overlord, Co-Founder of the Blue Team Village, and Original Member of the Lonely Hackers Club.



BIO Says cyber waaaaay too much.



BIO Old enough to remember the good years of Usenet and IRC.



BIO I press F5 for a living.

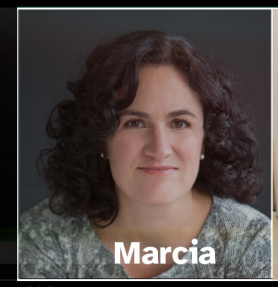
AKA Cederic



BIO Founder, DEF CON

AKA The Dark Tangent

CFP REVIEW BOARD



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

AKA Marcia Hoffman



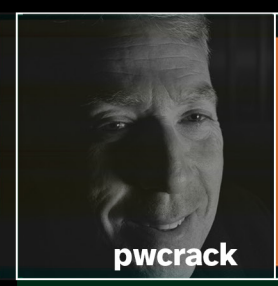
BIO Tries to keep his head low. Takes things apart and can sometimes pur them back together.



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



BIO This will totally work It will be fine. NARRATOR: It was not fine!



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



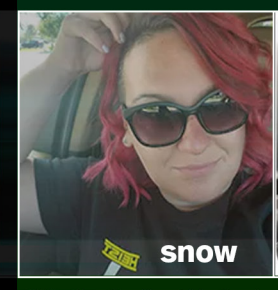
BIO Bio to come.



BIO Master of Sleights



BIO Sassy Cyclist, Scheming System Saboteur, Soulutioner of Perplex Puzzles.



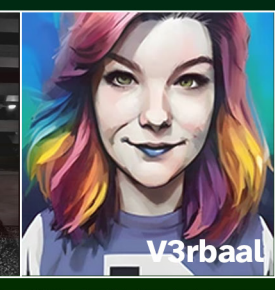
BIO Your friendly neighborhood con artist.



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



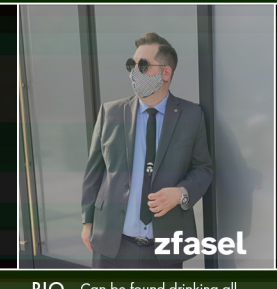
BIO Self-appointed DEF CON 4x5k ambassador and party escape artist.



BIO Qualifications include eating 12 bananas on Hacker Jeopardy.



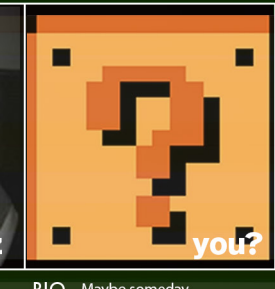
BIO Independent consultant focusing on digital and physical security policy. Policy@DEF CON Goon.



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



BIO International Man of Mystery



BIO Maybe someday. Say your prayers and take your vitamins.

CREATOR STAGE TALKS

Gunnar "g0lden" Andrews

Organized by Bug Bounty Village

SECRET LIFE OF AN AUTOMATIONIST: ENGINEERING THE HUNT

Friday 10:00 for 30 minutes, at W229 (Creator Stage 5)

Diego "djurado" Jurado, Joel "niemand_sec" Noguera

Organized by Bug Bounty Village

PROMPT. SCAN. EXPLOIT: AI'S JOURNEY THROUGH ZERO-DAYS AND A THOUSAND BUGS

Friday 10:00 for 60 minutes, at W231 (Creator Stage 3)

Adam Robbie

Organized by ICS Village

SAFEGUARDING THE INDUSTRIAL FRONTIER: OT SOC & INCIDENT RESPONSE

Friday 10:00 for 30 minutes, at W232 (Creator Stage 2)

Emma Stewart

Organized by ICS Village

FEAR VS. PHYSICS: DIAGNOSING GRID CHAOS

Friday 10:00 for 30 minutes, at W233 (Creator Stage 1)

Nathan Case, Jon McCoy

Organized by OWASP Community

SILENT SABOTAGE: HOW NATION-STATE HACKERS TURN HUMAN ERROR INTO CATASTROPHIC FAILURES

Friday 10:15 for 45 minutes, at Hall 4 - C105 (Comm Stage)

Michael Frank

Organized by ICS Village

HULL INTEGRITY: APPLYING MOSAICS TO NAVAL MISSION SYSTEMS

Friday 10:30 for 30 minutes, at W229 (Creator Stage 5)

Katarina Amrichova

Organized by Biohacking Village

QUANTUM-RESISTANT HEALTHCARE

Friday 10:30 for 30 minutes, at W232 (Creator Stage 2)

Stephen Bono, Rachael Tubbs

Organized by IOT Village

10 YEARS OF IOT VILLAGE: INSIGHTS IN THE WORLD OF IOT

Friday 10:30 for 30 minutes, at W233 (Creator Stage 1)

Michael "MSvB" Schloh von Bennewitz, Chad Calease, Param D Pithadia

Organized by Cryptocurrency Community

CRYPTOCURRENCY OPENING KEYNOTE

Friday 11:00 for 60 minutes, at Hall 4 - C105 (Comm Stage)

Organized by Payment Village

CARDING IS DEAD, LONG LIVE CARDING

Friday 11:00 for 60 minutes, at W228 (Creator Stage 4)

Organized by Payment Village

MORE IS LESS

Friday 11:00 for 60 minutes, at W229 (Creator Stage 5)

Jordan Kasper

Organized by Policy @ DEF CON

STATE OF OPEN SOURCE IN THE FEDERAL GOVERNMENT

Friday 11:00 for 45 minutes, at W231 (Creator Stage 3)

Adam Pennington, Sydney Marrone, Lauren Proehl

Organized by Adversary Village

FROM ADVERSARIAL TO ALIGNED, REDEFINING PURPLE TEAMING FOR MAXIMUM IMPACT

Friday 11:00 for 45 minutes, at W232 (Creator Stage 2)

Asher Davila

Organized by IOT Village

GO MALWARE MEETS IOT: CHALLENGES, BLIND SPOTS, AND BOTNETS

Friday 11:00 for 60 minutes, at W233 (Creator Stage 1)

Tom Cross, Greg Conti

Organized by Policy @ DEF CON

DARK CAPABILITIES: WHEN TECH COMPANIES BECOME THREAT ACTORS

Friday 11:45 for 45 minutes, at W231 (Creator Stage 3)

Alexandru Lazar

Organized by IOT Village

NEVER ENOUGH ABOUT CAMERAS - THE FIRMWARE ENCRYPTION KEYS HIDDEN UNDER THE RUG

Friday 11:45 for 45 minutes, at W232 (Creator Stage 2)

Rich Compton

Organized by DDoS Community

TUNNELPOCALYPSE

Friday 12:00 for 60 minutes, at Hall 4 - C105 (Comm Stage)

Lior ZL, Jacob Avidar

Organized by Crypto Privacy Village

BEHIND THE DASHBOARD - (LACK OF) AUTOMOTIVE PRIVACY

Friday 12:00 for 60 minutes, at W228 (Creator Stage 4)

Gabriel Nitu, Jay Dancer, Tyson Laa Deng, Ryan Nolette, Goshak <Last Name>

Organized by Bug Bounty Village

VOICES FROM THE FRONTLINES: MANAGING BUG BOUNTIES AT SCALE

Friday 12:00 for 60 minutes, at W229 (Creator Stage 5)

Langston Clements, Dan Goga

Organized by Physical Security Village

FLIPPING LOCKS - REMOTE BADGE CLONING WITH THE FLIPPER ZERO AND MORE

Friday 12:00 for 60 minutes, at W233 (Creator Stage 1)

Eaton Zveare

Organized by Car Hacking Village

HOW API FLAWS LED TO ADMIN ACCESS TO OVER 1,000 USA DEALERS AND CONTROL OVER YOUR CAR

Friday 12:30 for 30 minutes, at W231 (Creator Stage 3)

Yael Grauer

Organized by Crypto Privacy Village

BACK TO BASICS: BUILDING RESILIENT CYBER DEFENSES

Friday 12:30 for 30 minutes, at W232 (Creator Stage 2)

Tom Berek, Farid Zakaria, Daniel Baker

Organized by Nix Vegas Community

REBUILD THE WORLD: ACCESS TO SECURE SOFTWARE DEPENDENCY MANAGEMENT EVERYWHERE WITH NIX

Friday 13:00 for 60 minutes, at Hall 4 - C105 (Comm Stage)

Irene Mo, Alyssa Coley

Organized by Crypto Privacy Village

A TALE OF WEEDS AND ROSES: PROPAGATING THE RIGHT DATA PROTECTION AGREEMENTS WITH VENDORS

Friday 13:00 for 60 minutes, at W228 (Creator Stage 4)

Quinn Dombrowski

Organized by Policy @ DEF CON

TAKES ALL KINDS: BUILDING ONRAMPS FOR EMERGENCY WEB ARCHIVING IN UKRAINE AND BEYOND

Friday 13:00 for 45 minutes, at W231 (Creator Stage 3)

Richard "HeadlessZeke" Lawshae, Chiao-Lin "Steven Meow" Yu, Kai-Ching "Keniver" Wang

Organized by IOT Village

WHAT IS DEAD MAY NEVER DIE: THE IMMORTALITY OF SDK BUGS

Friday 13:00 for 45 minutes, at W232 (Creator Stage 2)

Adel Karimi

Organized by Packet Hacking Village

TEACHING YOUR REVERSE PROXY TO THINK: FINGERPRINT-BASED BOT BLOCKING & DYNAMIC DECEPTION

Friday 13:00 for 60 minutes, at W233 (Creator Stage 1)

MrBill, M0nkeyDrag0n, Hydrox, CoD_Segfault

Organized by Hard Hat Brigade

HARD HAT BRIGADE CREATIONS Q&A

Friday 13:15 for 45 minutes, at W229 (Creator Stage 5)

Sharlene Toney

Organized by Policy @ DEF CON

THIRD-PARTY ACCESS GRANTED: A POSTMORTEM ON STUDENT PRIVACY AND THE EXPLOIT THAT'S STILL IN PRODUCTION

Friday 13:45 for 45 minutes, at W231 (Creator Stage 3)

Jorge Acevedo Canabal, Scott Shackleford, Joseph Davis

Organized by Biohacking Village

DIGITAL CASUALTIES: DOCUMENTING CYBER-INDUCED PATIENT HARM IN MODERN HEALTHCARE

Friday 13:45 for 45 minutes, at W232 (Creator Stage 2)

CREATOR STAGE TALKS

Robert "LambdaCalculus" Menes

Organized by Hackers.town Community

OFF-GRID DATARUNNING IN OPPRESIVE REGIMES: SNEAKERNET AND PIRATE BOX

Friday 14:00 for 30 minutes, at Hall 4 - C105 (Comm Stage)

Dane Sherrets, Shlomie Liberow

Organized by Bug Bounty Village

SECURING INTELLIGENCE: HOW HACKERS ARE BREAKING MODERN AI SYSTEMS ... AND HOW BUG BOUNTY PROGRAMS CAN KEEP UP

Friday 14:00 for 60 minutes, at W228 (Creator Stage 4)

Noah Holland, Josh Stiebel

Organized by Physical Security Village

HACKING HOTEL LOCKS; THE SAFLOK VULNERABILITIES EXPANDED

Friday 14:00 for 60 minutes, at W229 (Creator Stage 5)

Julian "Julez" Dunning

Organized by GameHacking.GG

GAME HACKING 101

Friday 14:00 for 45 minutes, at W233 (Creator Stage 1)

collin, oblivion

Organized by Car Hacking Village

MODERN ODOMETER MANIPULATION

Friday 14:30 for 30 minutes, at W231 (Creator Stage 3)

Emily Fane, Abdel Sy Fane

Organized by Crypto Privacy Village

QRAMM: THE CRYPTOGRAPHIC MIGRATION TO A POST-QUANTUM WORLD

Friday 14:30 for 30 minutes, at W232 (Creator Stage 2)

Noel Wong, KC Wong

Organized by Loong Community

INTRODUCTION OF LOONG COMMUNITY & FINANCIAL IDENTITY CRIME (DEEPFAKE) REGULATION OF DIFERETN JURISDICTIONS

Friday 14:45 for 45 minutes, at Hall 4 - C105 (Comm Stage)

Ezz Tahoun

Organized by IOT Village

CONTEXTUALIZING ALERTS & LOGS AT SCALE WITHOUT QUERIES OR LLMS (OPENSOURCE)

Friday 15:00 for 60 minutes, at W228 (Creator Stage 4)

Matt Gaffney

Organized by Aerospace Village

VDP IN AVIATION - HOW IT SHOULDN'T BE DONE!

Friday 15:00 for 30 minutes, at W229 (Creator Stage 5)

RADM John Mauger, USCG (ret.), Michael Sulmeyer, Adam Segal

Organized by Maritime Hacking Village

THREAT DYNAMICS ON THE SEAS

Friday 15:00 for 45 minutes, at W231 (Creator Stage 3)

Muhammad Mudassar Yamin, Espen Torseth

Organized by Policy @ DEF CON

WHAT EUROPEANS ARE DOING RIGHT ABOUT CYBER SECURITY

Friday 15:00 for 45 minutes, at W232 (Creator Stage 2)

Gregory Carpenter, DrPH, Barb Hirz, Bret Fowler, MSGT (Ret), John Andre Bjørkhaug, John Johnson, Dr, Michael Tassey

Organized by Adversary Village

ADVERSARIES AT WAR: TACTICS, TECHNOLOGIES, AND LESSONS FROM MODERN BATTLEFIELDS

Friday 15:00 for 45 minutes, at W233 (Creator Stage 1)

Pratik Lotia, Spencer Koch

Organized by DDoS Community

GRIND VS GLEAM: BUILDING REDDIT'S DDOS RESILIENCE

Friday 15:30 for 30 minutes, at Hall 4 - C105 (Comm Stage)

Aaron Boyd

Organized by ICS Village

LOCKED DOWN, NOT LOCKED OUT: HOW I ESCAPED YOUR SECURE OPERATOR WORKSTATION

Friday 15:30 for 30 minutes, at W229 (Creator Stage 5)

Deputy Minister Herming Chiueh, Jason Vogt

Organized by Maritime Hacking Village

FIGHTING THE DIGITAL BLOCKADE: A VIEW FROM TAIWAN

Friday 15:45 for 45 minutes, at W231 (Creator Stage 3)

Tanya "SheHacksPurple" Janca

Organized by Policy @ DEF CON

SECURE CODE IS CRITICAL INFRASTRUCTURE: HACKING POLICY FOR THE PUBLIC GOOD

Friday 15:45 for 45 minutes, at W232 (Creator Stage 2)

Abhijith "Abx" B R, Keenan Skelly

Organized by Adversary Village

ADVERSARIAL MINDSET, THINKING LIKE AN ATTACKER IS NO LONGER OPTIONAL

Friday 15:45 for 45 minutes, at W233 (Creator Stage 1)

Giovanni Cruz Forero

Organized by La Villa

CYBERSECURITY IN LATIN AMERICA: THE UNTOLD STORIES OF RESILIENCE & INNOVATION

Friday 16:00 for 30 minutes, at Hall 4 - C105 (Comm Stage)

Danilo Erazo

Organized by Car Hacking Village

HACKING A HEAD UNIT WITH MALICIOUS PNG

Friday 16:00 for 30 minutes, at W228 (Creator Stage 4)

James Utley, PhD

Organized by Biohacking Village

BIO-CRYPTOGRAPHY IS THE GAME-GENIE IN A POST QUANTUM DYSTOPIA

Friday 16:00 for 30 minutes, at W229 (Creator Stage 5)

Emma Fang

Organized by BBWIC Foundation

QUIET CONFIDENCE: AN INTROVERT'S JOURNEY TO TECHNICAL PUBLIC SPEAKING

Friday 16:30 for 30 minutes, at Hall 4 - C105 (Comm Stage)

Andrzej Olchawa, Milenko Starcik, Ayman Boulaich, Ricardo Fradique

Organized by Aerospace Village

BURNING, TRASHING, SPACECRAFT CRASHING: A COLLECTION OF VULNERABILITIES THAT WILL END YOUR SPACE MISSION

Friday 16:30 for 30 minutes, at W228 (Creator Stage 4)

Tim Clevenger

Organized by Physical Security Village

ACCESS CONTROL DONE RIGHT THE FIRST TIME

Friday 16:30 for 30 minutes, at W229 (Creator Stage 5)

Ravi Rajput

Organized by Car Hacking Village

CONTEXT AWARE ANOMALY DETECTION IN AUTOMOTIVE CAN WITHOUT DECODING

Friday 16:30 for 30 minutes, at W231 (Creator Stage 3)

Chiao-Lin "Steven Meow" Yu, Kai-Ching "Keniver" Wang

Organized by Car Hacking Village

SMART BUS SMART HACKING: FROM FREE WIFI TO TOTAL CONTROL

Friday 16:30 for 30 minutes, at W232 (Creator Stage 2)

4dw@r3

Organized by Crypto Privacy Village

THE DEPTHS THAT MARKETERS WILL PLUMMET TO

Friday 16:30 for 30 minutes, at W233 (Creator Stage 1)

Abhinav Panda, MakeItHackin

Organized by Badgelife Community

BADGELIFE: LESSONS FROM YEARS OF DO'S, DON'TS, AND LAST-MINUTE SAVES

Friday 17:00 for 60 minutes, at Hall 4 - C105 (Comm Stage)

Ben Hawkins

Organized by Aerospace Village

MOONLIGHT DEFENDER - PURPLE TEAMING IN SPACE!

Friday 17:00 for 30 minutes, at W228 (Creator Stage 4)

CREATOR STAGE TALKS

Andrea Downing

Organized by Biohacking Village

THEY DEPLOYED HEALTH AI ON US. WE'RE BRINGING THE RIGHTS & RED TEAMS.

Friday 17:00 for 30 minutes, at W229 (Creator Stage 5)

Federico Lucifredi

Organized by Hardware Hacking and Soldering Skills Village (HHV-SSV)

ALL YOUR KEYBOARDS ARE BELONG TO US!

Friday 17:00 for 60 minutes, at W231 (Creator Stage 3)

Bobby Kuzma, Michael Odell

Organized by Adversary Village

OF STOCHASTIC PARROTS AND DETERMINISTIC PREDATORS: DECISION-MAKING IN ADVERSARIAL AUTOMATION

Friday 17:00 for 30 minutes, at W232 (Creator Stage 2)

Roee Idan

Organized by Aerospace Village

SATELLITE NETWORKS UNDER SIEGE: CYBERSECURITY CHALLENGES OF TARGETED DDOS ATTACKS

Friday 17:00 for 30 minutes, at W233 (Creator Stage 1)

Dr. Katie Paxton-Fear

Organized by IOT Village

VIBE SCHOOL: MAKING DUMB DEVICES SMART WITH AI

Friday 17:30 for 30 minutes, at W228 (Creator Stage 4)

Amp, Data

Organized by Maritime Hacking Village

HACKING THE NAUTICAL RULES OF THE ROAD: TURN LEFT FOR GLOBAL PWNAGE

Friday 17:30 for 30 minutes, at W229 (Creator Stage 5)

PamirAI

Organized by Biohacking Village

HOW AI + HARDWARE CAN TRANSFORMING POINT-OF-CARE WORKFLOWS

Friday 17:30 for 30 minutes, at W232 (Creator Stage 2)

Christopher Nourrie

Organized by ICS Village

CROSSING THE LINE: ADVANCED TECHNIQUES TO BREACH THE OT DMZ

Friday 17:30 for 30 minutes, at W233 (Creator Stage 1)

Zoltan "zh4ck" Balazs

Organized by Embedded Systems Village

HOW NOT TO IOT: LESSONS IN SECURITY FAILURES

Saturday 10:00 for 60 minutes, at W228 (Creator Stage 4)

Akib Sayyed

Organized by Telecom Village

ANOTOMY OF TELECOM MALWARE

Saturday 10:00 for 45 minutes, at W229 (Creator Stage 5)

Thomas Pope

Organized by ICS Village

CRITICALLY NEGLECTED: CYBERSECURITY FOR BUILDINGS

Saturday 10:00 for 30 minutes, at W231 (Creator Stage 3)

Ben "nahamsec" Sadeghipour

Organized by Bug Bounty Village

NUCLEI: BEYOND THE BASIC TEMPLATES

Saturday 10:00 for 60 minutes, at W232 (Creator Stage 2)

Organized by Crypto Privacy Village

GOLD BUG: PUZZLE PANEL WITH FRIENDS

Saturday 10:00 for 60 minutes, at W233 (Creator Stage 1)

Meghan Jacquot

Organized by BBWIC Foundation

PRIVATE, PRIVATE, PRIVATE: ACCESS EVERYWHERE

Saturday 10:15 for 45 minutes, at Hall 4 - C105 (Comm Stage)

Mehmet Önder Key, Furkan Aydogan

Organized by Maritime Hacking Village

NAVIGATING THE INVISIBLE

Saturday 10:30 for 30 minutes, at W231 (Creator Stage 3)

Chelsea Button, Nick "c7five" Percoco, Elaine Shi

Organized by Cryptocurrency Community

CRYPTOCURRENCY WEEKEND KEYNOTE

Saturday 11:00 for 60 minutes, at Hall 4 - C105 (Comm Stage)

Paul McCarty

Organized by Adversary Village

MALWARE IN THE GIST: HOW MALICIOUS PACKAGES ON NPM BYPASS EXISTING SECURITY TOOLS

Saturday 11:00 for 30 minutes, at W228 (Creator Stage 4)

Patrick Walsh

Organized by Crypto Privacy Village

ILLUMINATING THE DARK CORNERS OF AI: EXTRACTING PRIVATE DATA FROM AI MODELS AND VECTOR EMBEDDINGS

Saturday 11:00 for 60 minutes, at W229 (Creator Stage 5)

Organized by Payment Village

GEN AI RED TEAMING FRAUD PREVENTION SYSTEMS

Saturday 11:00 for 60 minutes, at W231 (Creator Stage 3)

Mehmet Önder Key, Temel Demir, Dr. Ahmet Furkan Aydogan

Organized by IOT Village

NO BRAIN NO GAIN

Saturday 11:00 for 60 minutes, at W232 (Creator Stage 2)

Organized by Payment Village

THE SOCIAL ENGINEERING INDUSTRY

Saturday 11:00 for 60 minutes, at W233 (Creator Stage 1)

Vlatko Kosturjak, MJ Casado

Organized by Maritime Hacking Village

STATE OF THE POPS: MAPPING THE DIGITAL WATERS

Saturday 11:30 for 30 minutes, at W228 (Creator Stage 4)

Andrew Cockburn

Organized by DDoS Community

DDOS: THE NEXT GENERATION

Saturday 12:00 for 60 minutes, at Hall 4 - C105 (Comm Stage)

Allan Friedman

Organized by IOT Village

WHAT'S REALLY IN THE BOX? THE CASE FOR HARDWARE PROVENANCE AND HBOMS

Saturday 12:00 for 30 minutes, at W228 (Creator Stage 4)

1nfocalypse

Organized by Crypto Privacy Village

CRACKING CHAOS: MAKING, USING, AND BREAKING PRNGS

Saturday 12:00 for 60 minutes, at W229 (Creator Stage 5)

Jasmin Landry (JR0ch17)

Organized by Bug Bounty Village

SOMETIMES YOU FIND BUGS, SOMETIMES BUGS FIND YOU

Saturday 12:00 for 30 minutes, at W231 (Creator Stage 3)

Shawn

Organized by Physical Security Village

FROM PWN TO PLAN: TURNING PHYSICAL EXPLOITS INTO UPGRADES

Saturday 12:00 for 60 minutes, at W232 (Creator Stage 2)

Brent White, Tim Roberts

Organized by Physical Security Village

HOW NOT TO PERFORM COVERT ENTRY ASSESSMENTS BY WEHACKPEOPLE.COM

Saturday 12:00 for 60 minutes, at W233 (Creator Stage 1)

Adam915, Jayson E Street, Alethe Denis

Organized by DEF CON Groups (DCG)

DEF CON GROUPS (DCGS): KEEPING THE SIGNAL ALIVE ALL YEAR LONG

Saturday 13:00 for 60 minutes, at Hall 4 - C105 (Comm Stage)

Brent Muir

Organized by ICS Village

DEPLOYING DECEPTION IN DEPTH FOR ICS

Saturday 13:00 for 30 minutes, at W228 (Creator Stage 4)

CREATOR STAGE TALKS

Roni "lupin" Carta, Adnan Khan

Organized by Bug Bounty Village

BREAKING THE CHAIN: ADVANCED OFFENSIVE STRATEGIES IN THE SOFTWARE SUPPLY CHAIN

Saturday 13:00 for 60 minutes, at W229 (Creator Stage 5)

Mike Raggo

Organized by Packet Hacking Village

DEEPFAKE IMAGE AND VIDEO DETECTION

Saturday 13:00 for 60 minutes, at W231 (Creator Stage 3)

Yago Lizarribar

Organized by Car Hacking Village

UNCOVERING THE SECRETS OF TIRE PRESSURE MONITORING SYSTEMS

Saturday 13:00 for 30 minutes, at W232 (Creator Stage 2)

Joe "Juno" Aurelio

Organized by GameHacking.GG

WHAT GAME HACKERS TEACH US ABOUT OFFENSIVE SECURITY AND RED TEAMING

Saturday 13:00 for 45 minutes, at W233 (Creator Stage 1)

Will Baggett

Organized by IOT Village

THE THINGS KNOW WHAT YOU DID LAST SESSION

Saturday 13:45 for 30 minutes, at W233 (Creator Stage 1)

Organized by Hackers.town Community

TECH RECLAIMERS

Saturday 14:00 for 30 minutes, at Hall 4 - C105 (Comm Stage)

Tony Turner

Organized by ICS Village

OT NETWORK SEGMENTATION PLANNING, IMPLEMENTATION, AND VALIDATION

Saturday 14:00 for 30 minutes, at W228 (Creator Stage 4)

Octavio Gianatiempo, Gaston Aznarez

Organized by Hardware Hacking and Soldering Skills Village (HHV-SSV)

THE MISSING LINK: DRAYTEK'S NEW RCES COMPLETE THE CHAIN

Saturday 14:00 for 60 minutes, at W229 (Creator Stage 5)

Seongsu Park

Organized by Adversary Village

BLURRED LINES OF CYBER THREAT ATTRIBUTION: THE EVOLVING TACTICS OF NORTH KOREAN CYBER THREAT ACTORS

Saturday 14:00 for 30 minutes, at W231 (Creator Stage 3)

Tim Fowler

Organized by Aerospace Village

RED TEAMING SPACE: HACKING THE FINAL FRONTIER

Saturday 14:00 for 30 minutes, at W232 (Creator Stage 2)

Justin W. Lin

Organized by AI Village

ASSESSING THE CAPABILITIES GAP BETWEEN FOUNDATION MODELS AND CYBERSECURITY EXPERTS: BENCHMARKS, SAFEGUARDS, AND POLICY

Saturday 14:15 for 45 minutes, at W233 (Creator Stage 1)

Janet Vertesi, Andy Hull

Organized by Hackers.town Community

#RECLAIMTECH - A COMMUNITY MOVEMENT

Saturday 14:30 for 30 minutes, at Hall 4 - C105 (Comm Stage)

MrBill, M0nkeyDrag0n, Hydrox, CoD_Segfault

Organized by Hard Hat Brigade

HARD HAT BRIGADE ORGANIZER PANEL

Saturday 15:00 for 45 minutes, at Hall 4 - C105 (Comm Stage)

Rob King

Organized by ICS Village

THERE AND BACK AGAIN: DISCOVERING OT DEVICES ACROSS PROTOCOL GATEWAYS

Saturday 15:00 for 30 minutes, at W228 (Creator Stage 4)

Whit "un1tycyb3r" Taylor

Organized by Bug Bounty Village

REFERRAL BEWARE, YOUR REWARDS ARE MINE

Saturday 15:00 for 30 minutes, at W229 (Creator Stage 5)

Jennifer Schieferle Uhlenbrock

Organized by Biohacking Village

DIGITAL FIRST RESPONDERS: FIXING PATIENT SAFETY GAPS WITH SMART TECH & AI

Saturday 15:00 for 30 minutes, at W231 (Creator Stage 3)

Weihan Goh, Joseph Lim, Isaac Soon

Organized by Adversary Village

COUNTERING FORENSICS SOFTWARE BY BAITING THEM

Saturday 15:00 for 30 minutes, at W232 (Creator Stage 2)

John Andre Bjørkhaug

Organized by Maritime Hacking Village

PIRATES OF THE NORTH SEA

Saturday 15:00 for 30 minutes, at W233 (Creator Stage 1)

Cybelle Oliveira

Organized by Adversary Village

OPERATIONAL TWILIGHT: APTS, OT, AND THE GEOPOLITICS OF A DYING CLIMATE

Saturday 15:30 for 30 minutes, at W229 (Creator Stage 5)

Amelia Shapiro

Organized by Policy @ DEF CON

CHINA'S HEALTH SECTOR AMBITIONS AND INFORMATION NEEDS: IMPLICATIONS FOR U.S. HEALTH CARE CYBER DEFENSE

Saturday 16:00 for 30 minutes, at W228 (Creator Stage 4)

Ryan Mitchell

Organized by Packet Hacking Village

SSH HONEYPOTS AND WALKTHROUGH WORKSHOPS: A HISTORY

Saturday 16:00 for 60 minutes, at W229 (Creator Stage 5)

Chad Spensky, Ph.D.

Organized by Physical Security Village

YOUR PASSKEY IS WEAK: PHISHING THE UNPHISHABLE

Saturday 16:00 for 30 minutes, at W231 (Creator Stage 3)

Carson Green, Rik Chatterjee

Organized by Maritime Hacking Village

DEAD RECKONING: HIJACKING MARINE AUTOPILOTS

Saturday 16:00 for 30 minutes, at W232 (Creator Stage 2)

Constantine Macris (TheDini), Anissa Elias

Organized by Maritime Hacking Village

FINGERPRINTING MARITIME NMEA2000 NETWORKS

Saturday 16:00 for 30 minutes, at W233 (Creator Stage 1)

AviNash Srinivasan

Organized by Maritime Hacking Village

RESILIENT AND RECONFIGURABLE MARITIME COMMS.

Saturday 16:30 for 30 minutes, at W228 (Creator Stage 4)

Michael DeVolld, Austin Reid

Organized by Maritime Hacking Village

HOW COMPUTERS KILL PEOPLE: MARINE SYSTEMS

Saturday 16:30 for 30 minutes, at W231 (Creator Stage 3)

Dawn Song

Organized by AI Village

IMPACT OF FRONTIER AI ON THE LANDSCAPE OF CYBERSECURITY

Saturday 16:30 for 45 minutes, at W232 (Creator Stage 2)

Konstantinos Karagiannis

Organized by Quantum Village

POST-QUANTUM PANIC: WHEN WILL THE CRACKING BEGIN, AND CAN WE DETECT IT?

Saturday 16:30 for 45 minutes, at W233 (Creator Stage 1)

Eva Benn, Rosie "Lady Cyber Rosie" Anderson, Tib3rius

Organized by Noob Community

BREAKING IN: REAL PATHS INTO CYBERSECURITY FROM HACKERS, HUMANS, AND HIRING PROS

Saturday 17:00 for 60 minutes, at Hall 4 - C105 (Comm Stage)

CREATOR STAGE TALKS

Marcell Szakály, Sebastian Köhler, Jan "SP3ZN45" Berens

Organized by Car Hacking Village

ONE MODEM TO BRICK THEM ALL: EXPLOITING VULNERABILITIES IN THE EV CHARGING COMMUNICATION

Saturday 17:00 for 60 minutes, at W229 (Creator Stage 5)

Ezz Tahoun

Organized by Packet Hacking Village

HACKING CONTEXT FOR AUTO ROOT CAUSE AND ATTACK FLOW DISCOVERY

Saturday 17:00 for 60 minutes, at W231 (Creator Stage 3)

Ben Gardiner

Organized by Car Hacking Village

BLIND TRAILER SHOUTING

Sunday 10:00 for 60 minutes, at W228 (Creator Stage 4)

Adam Batori, Robert Pafford

Organized by Aerospace Village

BEHIND THE BADGE: HOW WE USED AND ABUSED HARDWARE (AGAIN) TO CREATE THE AV BADGE FOR DC33

Sunday 10:00 for 60 minutes, at W229 (Creator Stage 5)

Karen Ng, Matthew Cancilla

Organized by Physical Security Village

INTRO TO PHYSICAL SECURITY BYPASS

Sunday 10:00 for 60 minutes, at W231 (Creator Stage 3)

Eugene "spaceraccoon" Lim

Organized by Crypto Privacy Village

ESCAPING THE PRIVACY SANDBOX WITH CLIENT-SIDE DEANONYMIZATION ATTACKS

Sunday 10:00 for 30 minutes, at W232 (Creator Stage 2)

Bobby Graydon, Ege Feyzioglu

Organized by Physical Security Village

ELEVATORS 101

Sunday 10:00 for 60 minutes, at W233 (Creator Stage 1)

Sherrod DeGrippo

Organized by OWASP Community

HUNTING IN THE DARK: THERE IS A LIGHT THAT NEVER GOES OUT

Sunday 10:15 for 45 minutes, at Hall 4 - C105 (Comm Stage)

Jimmy Wylie, Sam Hanson

Organized by ICS Village

DON'T CRY WOLF: EVIDENCE-BASED ASSESSMENTS OF ICS THREATS

Sunday 10:30 for 30 minutes, at W232 (Creator Stage 2)

Desiree Wilson

Organized by BBWIC Foundation

CREATING INTEGRATED THREAT SURVEILLANCE: AI + OSINT + SECURITY ONION

Sunday 11:00 for 45 minutes, at Hall 4 - C105 (Comm Stage)

Richard "richeeta" Hyunho Im, Denis Smajlović

Organized by Bug Bounty Village

HACKER VS. TRIAGE: INSIDE THE BUG BOUNTY BATTLEGROUND

Sunday 11:00 for 60 minutes, at W228 (Creator Stage 4)

Brandon Bailey

Organized by Aerospace Village

HACKING SPACE TO DEFEND IT: GENERATING IOBS WITH SPARTA

Sunday 11:00 for 30 minutes, at W229 (Creator Stage 5)

Will Thomas

Organized by Adversary Village

RED RUSSIANS: HOW RUSSIAN APT GROUPS CLOSELY FOLLOW OFFENSIVE SECURITY RESEARCH

Sunday 11:00 for 30 minutes, at W231 (Creator Stage 3)

Vanshal Gaur

Organized by Bug Bounty Village

HACKING AT SCALE WITH AI AGENTS: BUILDING AN AUTONOMOUS BUG BOUNTY HUNTER

Sunday 11:00 for 30 minutes, at W232 (Creator Stage 2)

Daniel Isler

Organized by Adversary Village

HERE AND NOW: EXPLOITING THE HUMAN LAYER AT THE RIGHT MOMENT

Sunday 11:00 for 30 minutes, at W233 (Creator Stage 1)

Kai-Ching "Keniver" Wang

Organized by IOT Village

UNVEILING IOT VULNERABILITIES: FROM BACKDOORS TO BUREAUCRACY

Sunday 11:30 for 30 minutes, at W229 (Creator Stage 5)

SolaSec

Organized by Biohacking Village

BARE METAL REVERSE ENGINEERING

Sunday 11:30 for 30 minutes, at W231 (Creator Stage 3)

Trevor Flynn

Organized by ICS Village

INTRO TO COMMON INDUSTRIAL PROTOCOL EXPLOITATION

Sunday 11:30 for 30 minutes, at W232 (Creator Stage 2)

Isabel Straw, MD, PhD

Organized by Biohacking Village

INTRODUCING CIPHER: THE OPEN-SOURCE PLATFORM REVEALING PATIENT HARMS FROM HEALTHCARE CYBERATTACKS

Sunday 11:30 for 30 minutes, at W233 (Creator Stage 1)

Sam Comini, Navaar Johnson

Organized by .edu Community

PASSING THE TORCH: MENTORING AND PROTECTING OUR STUDENTS IN EDUCATION SPACES

Sunday 12:00 for 60 minutes, at Hall 4 - C105 (Comm Stage)

Hector Cuevas Cruz

Organized by Physical Security Village

AIRPORT SECURITY! - S01 E008 - BREAKING INTO YOUR BAGGAGE

Sunday 12:00 for 60 minutes, at W228 (Creator Stage 4)

Nebu Varghese

Organized by Adversary Village

TOTALTEST 2.OH!: UNLEASHING A TESTING PROGRAM TO BREAK SMARTER, MEASURE BETTER, AND FUND YOUR FIXES

Sunday 12:00 for 30 minutes, at W229 (Creator Stage 5)

Matei Josephs

Organized by IOT Village

SMART DEVICES, DUMB RESETS? TESTING FIRMWARE PERSISTENCE IN COMMERCIAL IOT

Sunday 12:00 for 30 minutes, at W231 (Creator Stage 3)

Craig Heffner

Organized by IOT Village

FIRMWARE DECRYPTION: FOR, AND BY, THE CRYPTOGRAPHICALLY ILLITERATE

Sunday 12:00 for 30 minutes, at W232 (Creator Stage 2)

Sarah Hume

Organized by Adversary Village

LETTHEMIN: FACILITATING HIGH-VALUE PURPLE TEAMS USING AN ASSUMED COMPROMISE APPROACH

Sunday 12:00 for 30 minutes, at W233 (Creator Stage 1)

Capt. Kit Louttit, Steve Winston

Organized by Maritime Hacking Village

RED ALERTS AND BLUE OCEANS: INCIDENT RESPONSE FROM A SYSADMIN'S WAR ROOM IN MARITIME OPS

Sunday 12:30 for 30 minutes, at W229 (Creator Stage 5)

Mike Holcomb

Organized by ICS Village

THE WORST ICS/OT LOVE STORY EVER TOLD

Sunday 12:30 for 30 minutes, at W231 (Creator Stage 3)

Miracle "OWOLABI" Abiodun

Organized by Policy @ DEF CON

LEGALIZING ETHICAL HACKING: A GLOBAL SAFE HARBOR FOR SECURITY RESEARCH

Sunday 12:30 for 30 minutes, at W232 (Creator Stage 2)

Parsia Hakimian

Organized by Hardware Hacking and Soldering Skills Village (HHV-SSV)

THE POWER(POINT) GLOVE

Sunday 12:30 for 30 minutes, at W233 (Creator Stage 1)

DEMO LABS

AIMAL - ARTIFICIALLY INTELLIGENT MALWARE LAUNCHER

Endrit Shaqiri, Natyra Shaqiri
Saturday from 09:00 to 09:45 in W210
Friday from 10:00 to 10:45 in W208

AIMAL (Artificially Intelligent Malware Launcher) is a modular red team framework built to simulate advanced malware evasion techniques against modern AV/EDR/IDS solutions. It supports Process Herpaderping, Process Hollowing, Thread Hijacking, Process Ghosting, and many other evasion techniques as delivery mechanisms, with stealth enhancements including PPID spoofing, shellcode polymorphism, syscall mutation (Hell's Gate), and aggressive AMSI/ETW bypassing. AIMAL adapts to simulated detection responses through a feedback loop that mutates behavior on the fly, rotating techniques until the payload bypasses detection. Integration with the OpenAI API allows AIMAL to suggest the best evasion strategy based on alert context, helping simulate the decision-making process of advanced threat actors. Designed for research, red teaming, and adversarial simulation, AIMAL brings real-world stealth techniques into a clean, testable interface. Live demo will include payload staging, detection simulation, and mutation in action.

Audience: AI, Malware, Offense/Red Team

AIRBLEED - COVERT BLUETOOTH PLIST PAYLOAD INJECTION

Ray "CURZE$" Cervantes, Yvonne "Von Marie" Cervantes
Saturday from 09:00 to 09:45 in W211
Friday from 10:00 to 10:45 in W209

AirBleed is a proof-of-concept hack demonstrating a hidden communication technique leveraging a little-known vulnerability in macOS's Bluetooth property list files (Bluetooth.plist). By fragmenting payloads into tiny pieces and injecting them into device caches that go unnoticed by standard security tools, this capability enables operatives to establish dead-drop channels for passing critical data, all without arousing suspicion. [1] Stealth-by-Design: Uses legitimate Bluetooth device caches to hide encrypted payloads up to 248 bytes per fragment. [2] Dual-Use Impact: Enables clandestine communication or counter-plotter operations by law enforcement and intel. [3] Live Demo: DEF CON demo will allow attendees to send their own Bluetooth plist payloads to a vulnerable MacBook Pro. [4] Implications: Offers a novel toolkit for counterintelligence to monitor ,and disrupt, hidden networks and dead drops.

Audience: Offense/Red Team, Malware, Mobile

ANGRY MAGPIE - DLP BYPASS SIMULATOR

Jeswin Mathai, Xian Xiang Chang
Friday from 15:00 to 15:45 in W210
Saturday from 09:00 to 09:45 in W212

Angry Magpie is an open-source toolkit that demonstrates critical bypasses in enterprise Data Loss Prevention (DLP) systems through browser-based techniques. Our research identifies a class of attacks, Data Splicing, that enable exfiltration of sensitive data by transforming it to evade detection patterns used by both proxy and endpoint DLP solutions. The toolkit showcases four primary techniques: data sharding, ciphering, transcoding, and channel smuggling, each demonstrating specific architectural limitations in current DLP implementations. Security teams can use Angry Magpie to test their defense mechanisms against these practical attacks, providing valuable insights for enhancing data protection strategies. With browsers now serving as the primary access point for enterprise data, understanding and addressing these vulnerabilities has become essential for maintaining effective data security posture. Special thanks to Pankaj Sharma from the SquareX research team for his contributions to Angry Magpie toolkit.

Audience: Defense/Blue Team, Offense/Red Team

ATTACK FLOW AND ROOT CAUSE DISCOVERY - NO LLMS, NO QUERIES, JUST EXPLAINABLE ML

Ezz Tahoun, Kevin Shi
Saturday from 10:00 to 10:45 in W208
Friday from 10:00 to 10:45 in W211

Attack Flow Detector is an open-source tool that helps defenders uncover coordinated cyber attacks buried in noisy alert data. Instead of relying on LLMs or black-box AI, it uses explainable machine learning to map alerts, logs, and telemetry to MITRE ATT&CK techniques, cluster them into contextualized attack steps, and chain them into complete killchains. Built for blue teamers and SOC analysts, it's lightweight, interpretable, and easy to deploy in real environments. This demo will show how the tool processes real-world-style data, generates actionable tickets, and supports root cause analysis. If you're drowning in false positives or lone incidents, this is for you.

Audience: SecOps, AI, Defense/Blue Team

BEACONATOR C2 FRAMEWORK

Mike "CroodSolutions" Manrod, Ezra "Shammahwoods" Woods
Friday from 15:00 to 15:45 in W212
Saturday from 10:00 to 10:45 in W209

The Beaconator C2 framework provides multiple highly evasive payloads, created to provide red teams with code execution, versatility, and ease of use. It is intended to be a Swiss Army knife for evasive C2, with a unified listener and basic tools to manage an engagement. The goal is to empower red/purple teams to emulate emerging adversary tactics that are evasive, prove them out, and then open tickets with various AV/EDR vendors to improve detectability for these blind spots that are now exploited in the wild.

Audience: Purple Team, Malware, Offense/Red Team

BLACKDAGGER - CYBER WORKFLOW AUTOMATION FRAMEWORK

Mahmut "ErdemOzgen" Erdem Ozgen, Ata Seren
Friday from 11:00 to 11:45 in W208
Saturday from 10:00 to 10:45 in W210

Blackdagger is a next-gen cybersecurity workflow automation framework built to streamline and accelerate complex operations across DevSecOps, MLOps, MLSecOps, and Continuous Automated Red Teaming (CART). It uses a declarative YAML-based Directed Acyclic Graph (DAG) system to define, visualize, and execute automated pipelines, no heavy scripting required. With a built-in web UI, a containerized red teaming toolkit called Blackcart, and integration with GitHub Actions for OPSEC-friendly task execution, Blackdagger empowers teams to deploy, manage, and scale cyber workflows in real-time. Attendees will see live demos of red team pipelines, stealthy GitHub-based automation, and browser-based workflow execution via the Blackdagger Web Kit. Whether you're defending or attacking, Blackdagger turns security automation into an intuitive, visual experience, backed by real-world NATO and defense applications.

Audience: Cloud, Purple Team, Offense/Red Team

BOAZ - A MULTILAYERED APPROACH TO AV/EDR EVASION ENGINEERING

Thomas "XM20" Xuan Meng
Saturday from 10:00 to 10:45 in W211
Friday from 11:00 to 11:45 in W209

BOAZ (Bypass, Obfuscate, Adapt, Zero-Trust) evasion was inspired by the concept of multi-layered approach which is the evasive version of defence-in-depth first proposed in a presentation at BH USA14. BOAZ was developed to provide greater control over combinations of evasion methods, enabling more granular evaluations against antivirus and EDR. It is designed to bypass before, during, and post execution detections that span signature, heuristic, and behavioural detection mechanisms. BOAZ supports both x86/x64 binary (PE) or raw payload as input and output EXE or DLL. It has been tested on separated Windows 11 Enterprise, Windows 10, and Windows Server 2022 VMs with 14 desktop AVs and 7 EDRs installed including Windows Defender, Norton, BitDefender, Sophos, and ESET. The design of BOAZ evasion is modular, so users can add their own toolset or techniques to the framework. BOAZ is written in C++ and C and uses Python3 as the main linker to integrate all modules. There have been significant improvements implemented since its inception. The new version of the BOAZ evasion tool, set for release at DEF CON 33, will feature three novel threadless process injection primitives, along with newly implemented loaders and behavioural evasion techniques.

Audience: Offense/Red Team, Malware, Purple Team

C4 - CROSS COMPATIBLE COMMAND AND CONTROL

Scott "ScottCTaylor12" Taylor
Saturday from 16:00 to 16:45 in W210
Friday from 11:00 to 11:45 in W210

Let's face it, traditional HTTP C2 is burning out. Between aging domains, TLS cert management, sandbox fingerprinting, and blue teams getting smarter at categorizing traffic and infrastructure, your custom C2 feels less covert and more like a liability. Red teams and threat actors alike are shifting toward living off legitimate services, AWS, GitHub, Box, Notion, whatever blends in, but building solutions that are custom to a single C2 framework? Let's stop doing that. Let's share the fun! C4 (Cross-Compatible Command & Control) is here to change that. It's a modular toolkit of WASM-powered plugins that makes external C2 easy to implement, regardless of your implant's language or target OS. Whether you're writing in C, Rust, Go, Python, C#, or something else entirely, C4 plugins can be loaded directly into your implant and run on Windows, macOS, or Linux. But the real game-changer? C4 provides a single, centralized collection of over 10 fully-documented, operationally-ready external C2 modules, not just proof-of-concepts, but production-level integrations with trusted sites that fly under the radar. No more hunting through GitHub repos, hand-rolling fragile API calls, or hacking together glue code for every new environment. Stop reinventing external C2 and start planting some C4 in your implants!

Audience: Offense/Red Team, Cloud, Malware

CALDERA FOR OT - OOPS! ALL SOFTWARE

Devon Colmer, Tony Webber
Saturday from 11:00 to 11:45 in W208
Friday from 11:00 to 11:45 in W211

Dive into the world of Operational Technology (OT) adversary emulation, no racks of hardware required. With Caldera for OT (C4OT) and our new virtual device simulators, you can explore the inner workings of OT network communications from the comfort of your own home lab. The biggest industrial control systems incidents, FrostyGoop, PIPEDREAM, Industroyer, didn't rely on flashy zero-days to impact physical systems. Instead, they used native OT protocols to send valid messages with malicious intent. Now, with C4OT, you can step into the attacker's shoes and explore the quirks and capabilities of protocols like Modbus, DNP3, and IEC61850. No hardware? No problem. No experience? Even better. In this session, we'll show you how to get started with adversary emulation against simulated OT devices, unlocking a hands-on environment to test your attacks, validate your defenses, and gain practical insights into the world of industrial cybersecurity. Whether you're a defender looking to understand the threats, a researcher diving into OT protocol behavior, or a red-teamer eager to sharpen your skills, C4OT gives you the tools to experiment safely and effectively. Join us to see how C4OT is revolutionizing adversary emulation for OT, one packet at a time.

Audience: Defense/Blue Team, Purple Team, Offense/Red Team

DEMO LABS

COPYCAT - IDENTITY STEALER EXTENSION

Dakshitaa Babu, Shourya Pratap Singh
Saturday from 11:00 to 11:45 in W209
Friday from 12:00 to 12:45 in W208

Copycat is a browser extension-based red team toolkit for simulating web-based identity attacks. This tool simulates ten web-based identity attacks through a single browser extension with minimal permissions, operating primarily through hidden windows that execute attacks without user awareness. With Copycat, red teams can simulate complex attack scenarios including silent Gmail and LinkedIn hijacking, credential theft through login and OTP stealing, login page redirection, autofill extraction from enterprise applications, and multiple OAuth manipulation techniques. Copycat runs entirely in-browser with no special hardware requirements. Red teams can use Copycat to demonstrate attack vectors that bypass EDRs, SASE, and other traditional security controls, as these techniques operate within legitimate authenticated sessions rather than breaking them. The tool is fully modifiable, with each module designed for customization to target different services or authentication flows. Source code and documentation will be available for security researchers to extend and improve the framework. Special mention to Pankaj Sharma, Tejeswara S. Reddy, and Arpit Gupta for their contributions in building this toolkit!

Audience: Offense/Red Team, Defense/Blue Team

CRYPTOSPLOIT

Matt Cheung
Saturday from 09:00 to 09:45 in W208
Friday from 13:00 to 13:45 in W208

In 2022 a framework and tool for cryptographic attacks called Cryptosploit was introduced. In this workshop we will demo the capabilities and the underlying philosophy as well as new commands. This will include the flexibility of mixing and matching attack code with oracles and new commands to import and export cryptographic keys. In particular, we will demonstrate how after a successful attack on a public key, we will be able to export the private key corresponding to the certificate. The presentation will conclude with thoughts on improvements.

Audience: AppSec, Offense/Red Team

DVBE - DAMN VULNERABLE BROWSER EXTENSION

Abhinav Khanna
Friday from 12:00 to 12:45 in W209
Saturday from 11:00 to 11:45 in W210

In the continuously evolving world of browser extensions, security remains a big concern. As the demand of feature-rich extensions increases, priority is given to functionality over robustness, which makes way for vulnerabilities that can be exploited by malicious actors. The danger increases even more for organizations handling sensitive data like banking details, PII, confidential org reports, etc. Damn Vulnerable Browser Extension (DVBE) is an open-source vulnerable browser extension, designed to shed light on the importance of writing secure browser extensions and to educate developers and security professionals about the vulnerabilities and misconfigurations that are found in browser extensions, how they are found, and how they impact business. This built-to-be-vulnerable extension can be used to learn, train, and exploit browser extension-related vulnerabilities.

Audience: AppSec, Offense/Red Team, Defense/Blue Team

DYNA - AUTOMATING THE OWASP MASTG WITH OFFENSIVE ANDROID TACTICS

Arjun "T3R4_KAAL" Chaudhary, Ayodele Ibidapo
Saturday from 15:00 to 15:45 in W208
Friday from 09:00 to 09:45 in W208

Dyna is a full-spectrum Android security auditing framework designed to automate the OWASP MASTG checklist using both static and dynamic analysis. Built for red teams, appsec engineers, and mobile researchers, Dyna combines Frida, Drozer, PyGhidra, and ADB-based techniques into a modular pipeline that evaluates app permissions, exported components, crypto misuse, insecure storage, IPC abuse, native binary risks, and reverse engineering resilience. It can detect traversal, SQLi, hardcoded secrets, and debuggable builds, while reverse engineering .so files using Ghidra in headless mode. Dyna also features real-time logcat parsing and deep link/URL extraction to trace third-party leaks and misconfigurations. With colored output, structured reports, and an extensible architecture, Dyna turns OWASP MASTG from a checklist into a powerful automated testing workflow.

Audience: Mobile, Offense/Red Team, AppSec

EMPIRE 6.0

Vincent "Vinnybod" Rose, Jake "Hubble" Krasnov
Friday from 12:00 to 12:45 in W210
Saturday from 11:00 to 11:45 in W211

Empire 6.0 is the latest evolution of the Command and Control (C2) framework. This major release introduces powerful new capabilities, including Go-based agents for enhanced cross-platform compatibility, a completely overhauled Empire compiler for streamlined payload deployment, and an integrated plugin marketplace in Starkiller. Enhanced module systems, dynamic option handling, Beacon Object File integration, and advanced remote script execution further expand Empire's capabilities. Empire continues to provide cryptographically secure communications and direct integration with the MITRE ATT&CK framework to emulate real-world Advanced Persistent Threat tactics, techniques, and procedures. This demo lab will highlight these significant advancements and demonstrate Empire 6.0's state-of-the-art capabilities.

Audience: Offense/Red Team, Defense/Blue Team, Malware

ENTRAGOAT - A DELIBERATELY VULNERABLE ENTRA ID ENVIRONMENT

Tomer Nahum, Jonathan Elkabas
Friday from 12:00 to 12:45 in W211
Saturday from 12:00 to 12:45 in W208

EntraGoat is a deliberately vulnerable environment designed to simulate real-world security misconfigurations and attack scenarios in Microsoft Entra ID (formerly Azure Active Directory). Security professionals, researchers, and red teamers can leverage EntraGoat to gain hands-on experience identifying and exploiting identity and access management vulnerabilities, privilege escalation paths, and other security flaws specific to cloud-based Entra ID environments. EntraGoat is tailored specifically to help security practitioners understand and mitigate the risks associated with cloud identity infrastructures. The project provides a CTF-style learning experience, covering a range of misconfigurations, insecure policies, token abuses, and attack paths commonly exploited in real-world Entra ID breaches. By using EntraGoat, security teams can enhance their skills in Entra ID security, validate detection and response capabilities, and develop effective hardening strategies.

Audience: Defense/Blue Team, Offense/Red Team, Purple Team

FLARE-VM

Joshua "jstrosch" Stroschein, Elliot Chernofsky
Saturday from 12:00 to 12:45 in W209
Friday from 12:00 to 12:45 in W212

Interested in malware analysis, reverse engineering, or offensive security? You know setting up a dedicated Windows analysis virtual machine is crucial, but manually installing and configuring countless tools is incredibly time-consuming and complex. Attend this 30-minute demo to discover FLARE-VM, the powerful open-source solution from Mandiant (now part of Google Cloud) that automates this entire process. See firsthand how FLARE-VM drastically simplifies the creation of a comprehensive analysis VM packed with essential reversing and malware analysis tools. Learn why having a ready-to-go analysis environment is indispensable for so many technical cybersecurity roles and how FLARE-VM jump-starts your build!

Audience: Purple Team, Defense/Blue Team, Malware

GARUDA THREAT HUNTING FRAMEWORK

Monnappa "Monnappa22" K A, Sajan Shetty
Saturday from 15:00 to 15:45 in W211
Saturday from 16:00 to 16:45 in W211

The rapid growth of cyber threats has made endpoint logging a critical component of modern security operations. Defenders increasingly rely on endpoint telemetry like Sysmon logs to detect and investigate breaches. These logs capture crucial forensic evidence, but the sheer volume and complexity of Sysmon logs often overwhelm analysts and hinder timely and effective analysis. Garuda is an open-source PowerShell framework designed to address this challenge by providing a unified, flexible, and efficient approach to endpoint detection and response using Sysmon events. With advanced filtering capabilities, cross-event correlation, multiple contextual views, precise time-based noise reduction, and support for both remote and offline (EVTX) analysis, Garuda enables security teams to quickly uncover attack chains, investigate incidents, develop detection logic, and perform in-depth malware analysis all within a single, scriptable environment. Its extensible nature allows one to use it for various scenarios, including threat hunting, investigation, anomaly detection, detection engineering, and malware analysis. Garuda can accelerate investigations, improve detection, and provide deep visibility into endpoint activity.

Audience: Threat Hunting, Malware, Defense/Blue Team

GLYTCHC2 - COMMAND EXECUTION AND DATA EXFILTRATION OF ANY KIND THROUGH LIVE STREAMING PLATFORMS

Anil Celik, Emre Odaman
Friday from 15:00 to 15:45 in W209
Saturday from 12:00 to 12:45 in W210

Glytch is a post-exploitation tool serving as a command-and-control and data exfiltration service. It creates a covert channel through Twitch live streaming platform and lets attackers execute OS commands or exfiltrate data of any kind from the target computer, regardless of whether the computers are connected over a LAN or WAN.

Audience: Defense/Blue Team, Malware, Offense/Red Team

HAVE I BEEN RANSOMED?

Juanma "M4C" Tejada
Friday from 13:00 to 13:45 in W209
Saturday from 12:00 to 12:45 in W211

Have I Been Ransomed? is a specialized security service, akin to Have I Been Pwned, designed to detect personal data exposure specifically from ransomware leaks. As ransomware attacks increasingly involve data theft and public dumping, individuals need a way to check if their personally identifiable information has been compromised. Our platform goes beyond standard database checks by processing a wide array of leaked file types, including PDFs, documents, and text files. We employ advanced optical character recognition coupled with sophisticated large language models to meticulously scan unstructured data and extract sensitive identifiers such as national ID cards, driver's licenses, and social security numbers. Have I Been Ransomed? provides critical awareness, empowering users to discover if their sensitive information has been exposed in a ransomware incident and enabling them to take proactive steps against potential identity theft and fraud.

Audience: Defense/Blue Team, Threat Hunting

DEMO LABS

LEX SLEUTHER

Aaron "KNOX" James
Saturday from 12:00 to 12:45 in W212
Friday from 13:00 to 13:45 in W210

Lex Sleuther is an internal tool developed at CrowdStrike for detecting the script language of an unknown text file based purely on its contents. We derive a novel approach using lexer generators and ridge regression and develop the solution as a compact Rust binary with Python bindings. We compare our solution to the current state of the art and present CrowdStrike's own findings of relative efficacy in the field. Lex Sleuther has been recently open sourced for everybody to use.

Audience: Defense/Blue Team, Threat Hunting

MESSENGER - PROXIES HERE THERE AND EVERYWHERE

Skyler Knecht, Kevin Clark
Friday from 13:00 to 13:45 in W211
Saturday from 13:00 to 13:45 in W208

Proxies, along with local, reverse, and dynamic forwards, enable red teams to maintain persistent access and move laterally within target environments. By combining these techniques, operators can construct sophisticated attack chains that enable deep network access through multiple segmented environments. This presentation will dive into the setup, usage, and attacker techniques required to be effective with proxies. To demonstrate these techniques, the presenters will use a publicly available tunneling toolkit, Messenger.

Audience: Offense/Red Team

METASPLOIT'S LATEST ATTACK CAPABILITY AND WORKFLOW IMPROVEMENTS

Spencer "ZeroSteiner" McIntyre, Jack Heysel
Friday from 14:00 to 14:45 in W208
Saturday from 15:00 to 15:45 in W209
Saturday from 16:00 to 16:45 in W209

Metasploit continues to expand support for Active Directory Certificate Services attacks, as well as its protocol relaying capability and attack workflows for evergreen vulnerabilities. This year, we added support for SMB-to-LDAP relaying and SMB-to-HTTP relaying, as well as support to identify and exploit a number of AD CS flaws. We've also added the new PoolParty process injection capability to Windows Meterpreter sessions, along with support for System Center Configuration Manager attack workflows.

Audience: Defense/Blue Team

MPIT - MATRIX PROMPT INJECTION TOOL AND SHINOLLMAPPS

Shota "Sh1n0g1" Shinogi, Sasuke "Element138" Kondo
Saturday from 13:00 to 13:45 in W210
Friday from 14:00 to 14:45 in W209

Prompt injection is an emerging and poorly standardized attack vector targeting large language model applications. Unlike traditional vulnerabilities, there is no universal testing methodology or tooling, making it difficult for penetration testers to assess the security posture of LLM-integrated systems. Matrix Prompt Injection Tool aims to fill this gap by automating the generation of diverse prompt injection payloads. [1] Dynamic Input Detection: MPIT scans target websites to identify expected input fields where LLMs might process user requests. [2] Payload Enrichment: Each pattern includes crafted elements such as exploit strings, delimiters, and reasoning cues, enhancing the quality of the penetration test. [3] Genetic Algorithm Optimization: The tool employs a genetic algorithm to evolve and refine injection patterns, increasing their success rate significantly across different LLM defenses. [4] Practical Utility for Pentesters: MPIT is designed to support real-world offensive security assessments, making LLM-targeted testing more feasible and effective. ShinoLLMApps is a collection of vulnerable LLM web applications that use RAG and tools to help you test MPIT and better understand prompt injection and its risks. More info at github.com/Sh1n0g1/mpit and shinohack.me/shinollmapp.

Audience: AI, Offense/Red Team

NEBULA - 4 YEARS AND STILL KICKING *AAS

Bleon "Gl4ssesbo1" Proko
Saturday from 13:00 to 13:45 in W211
Friday from 14:00 to 14:45 in W210

Cloud penetration testing has become a hot topic in the offensive community, as 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 modularly for each provider and each attack, allowing for diversity in attack surface. This coupled with the client-server architecture allows for a collaborated team assessment of a hybrid cloud environment.

Audience: Cloud, Offense/Red Team, DevOps

NROOTTAG - EXPLOITING FIND MY AND TRANSFORMING COMPUTERS INTO UNAUTHORIZED TRACKERS

Junming "Chapoly1305" Chen, Qiang Zeng
Saturday from 13:00 to 13:45 in W212
Friday from 14:00 to 14:45 in W211

Apple Find My is a crowdsourced offline tracking network designed to assist in recovering lost devices while maintaining privacy. By leveraging over a billion active Apple devices, it has become the world's largest device-locating network. While prior research has demonstrated the possibility of creating DIY trackers that attach to the Find My network, they are mainly for personal use and do not pose a threat for remote attacks. Recently, we found an implementation error in the Find My network that makes it vulnerable to brute-force and rainbow table attacks. With a cost of a few US dollars, the exploit turns computers into trackers without requiring root privileges. We are concerned that adversaries and intelligence agencies would find this exploit handy for user profiling, surveillance, and stalking. This demo is especially appealing to those interested in Find My network and Bluetooth tracking technologies. We will review how Find My offline finding works, elaborate in detail about our discoveries, techniques to make practical attacks, and provide source code for fun.

Audience: Threat Hunting, Offense/Red Team

OAUTHSEEKER

Adam "UNC1739" Crosser
Saturday from 14:00 to 14:45 in W208
Friday from 14:00 to 14:45 in W212

OAuthSeeker is a cutting-edge red team tool designed to simulate OAuth phishing attacks, specifically targeting Microsoft Azure and Office365 users. This tool facilitates the creation, management, and execution of phishing campaigns without requiring advanced technical skills. By leveraging malicious OAuth applications, OAuthSeeker allows offensive security engineers to perform targeted phishing attacks to compromise user identities and gain access to Microsoft Graph API and Azure resources. With features like an administrative control panel, token refresh capabilities, and customizable skins for user-facing components, OAuthSeeker provides an effective solution for testing security defenses against a common but often overlooked attack vector. The tool is easy to deploy with only a single pre-compiled Go binary with zero external dependencies and includes built-in support for LetsEncrypt. The documentation is highly detailed and outlines all the possible attack paths where this capability could be used during real-world red team engagements. The installation process is streamlined requiring only a single command to deploy a new instance of the application.

Audience: Offense/Red Team

PAPRA

Sean Marquez, Melanie "Goldfishlaser" Allen
Friday from 16:00 to 16:45 in W208
Saturday from 14:00 to 14:45 in W209

This project is an open source hardware powered air-purifying respirator designed for use as personal protective equipment, offering N100-level filtration against airborne threats including pathogens and particulates, developed by Tetra Bio Distributed. We will demo the PAPR and discuss how to hack together your own using 3D-printed and off-the-shelf components, source one yourself, or contribute to the project.

Audience: Hardware, Medical/PPE Open Source Hardware

PATCHLEAKS

Huseyn "Khatai" Gadashov
Saturday from 14:00 to 14:45 in W210
Friday from 16:00 to 16:45 in W209

When vulnerabilities are disclosed, security teams face the task of developing exploits to identify compromised assets. Public exploits aren't always available, which is why teams scroll through hundreds of patches to identify the relevant one. Traditional methods like grepping might fasten the process, but mostly come out ineffective against modern codebases where context-aware analysis is required. We present PatchLeaks tool that transforms the messy patch analysis process into efficient vulnerability discovery. Unlike regex-based static analysis tools, it locates relevant patches with vulnerable code based on CVE id only, doesn't require any rules, has ability to identify logical vulnerabilities, and analyzes even corrupt files.

Audience: AI, Offense/Red Team, AppSec

PROMPTMAP2

Utku Sen
Friday from 16:00 to 16:45 in W210
Saturday from 14:00 to 14:45 in W211

Promptmap2 is a vulnerability scanning tool that automatically tests prompt injection attacks on your custom LLM applications. It analyzes your LLM system prompts, runs them, and sends attack prompts to them. By checking the response, it can determine if the prompt injection was successful or not. It has ready-to-use rules to steal system prompts or distract the LLM application from its main purpose.

Audience: Offense/Red Team, AI

RETCON - RETICULUM EMBEDDED TURNKEY CONNECTION OPERATING NODE

Daniel "Varx" Beard
Friday from 10:00 to 10:45 in W210
Friday from 09:00 to 09:45 in W210

Introducing RETCON: a game-changer for mesh network users who prefer deployment over drudgery. Reticulum offers a scalable, fully customizable, and secure-by-design off-grid mesh network, but the config can be confusing, hard to manage, and hard to share with beginners. RETCON allows you to package a pre-made Reticulum config into ready-to-roll Raspberry Pi images. And it auto-detects hardware to magically mesh upon deployment. Perfect for when you need a secure resilient mesh network yesterday, like maker fests, festivals, community networks, or right here at DEF CON.

Audience: Security Conscious Users and Radio Enthusiasts

DEMO LABS

RETINA - REALTIME ELECTRONIC THREAT AND INTRUSION NEUTRALIZATION APPARATUS

Cesare “Red5heep” Pizzi
Saturday from 14:00 to 14:45 in W212
Friday from 16:00 to 16:45 in W211
Saturday from 15:00 to 15:45 in W212

RETINA is the very first retro video game built for reverse engineers. Do you want to start the analysis of that sample, but aren’t really in the mood? You can try RETINA for Commodore 64, which can be fully customized with your own sample so that during your game you will also perform the malware triage!

Audience: Defense/Blue Team, Malware

REV.NG DECOMPILER

Pietro Fezzardi, Alessandro Di Federico
Saturday from 15:00 to 15:45 in W210
Friday from 11:00 to 11:45 in W212

Rev.ng is an open source static binary analysis framework and interactive decompiler for native code based on LLVM and QEMU. In our demo we will: [1] Introduce rev.ng and how to use it from the command line. [2] Decompile a simple program to syntactically valid C code that can be fed into other static analysis tools. [3] Showcase our automated whole-program type recovery on a stripped program without debug symbols, able to detect complex types, e.g. linked-lists. [4] Demonstrate the Python scripting capabilities. [5] Demonstrate our preliminary integration with LLMs to assign names to functions, types, and so on. All the examples will be released on GitHub and 100% reproducible using only open source software.

Audience: Reverse Engineering, Malware

ROBIN - THE ARCHAEOLOGIST OF THE DARK WEB

Apurv “ASG_Sc0rpi0n” Singh Gautam
Friday from 15:00 to 15:45 in W211
Saturday from 13:00 to 13:45 in W209

When exploring the dark web for OSINT or CTI investigations, you may be overwhelmed with numerous onion links, questionable marketplaces, and numerous search engines. With time constraints, how do you make sense of all this information and prioritize what truly matters? Enter Robin, an AI-powered dark web OSINT tool to streamline your investigations. Robin takes your query, automatically searches across multiple dark web search engines, scrapes relevant onion sites, and uses AI to generate clear, actionable investigative summaries. No more juggling five different tools or wasting hours validating dead links. In this tool demo, I’ll walk you through the real pain points of today’s dark web OSINT tools and show how Robin was built to solve them. I’ll cover the architecture, the scraping and summarization pipeline, and how Robin fits into real-world investigation workflows. I’ll also discuss future developments and how you can get involved. By the end of this talk, you will have a fresh perspective on dark web OSINT, a practical tool to use right away, and insights into how AI can simplify your dark web investigative process.

Audience: Threat Hunting, AI, Defense/Blue Team

SAMLSMITH

Eric Woodruff, Tomer Nahum
Friday from 10:00 to 10:45 in W212
Friday from 09:00 to 09:45 in W212

SAMLSmith is the go-to tool for penetrating SAML applications with response forging. An evolution of the original tooling developed for proof-of-concept of SAML response forging in Entra ID, SAMLSmith is the product of continued research on SAML. While far from new, enterprises continue to not prioritize the security of how SaaS applications integrate or understand best practices for securing them. With many factors at play, SAML response forging can range from extremely difficult to near impossible for a SOC to detect. SAMLSmith has a lot of tricks up its sleeve, including: [1] Multiple identity provider response forging. [2] AD FS specific response forging mode. [3] SAML request processing. [4] InResponseTo support. SAMLSmith can be used in several response forging scenarios where the private key material can be obtained. In demonstration of use, we’ll explore using SAMLSmith for performing a Golden SAML attack against AD FS. Further, we’ll demonstrate the use of SAMLSmith that ties into new research around response forging, penetrating certain types of SaaS applications with even more stealth.

Audience: Purple Team, Cloud, Offense/Red Team

SPOTTER - UNIVERSAL KUBERNETES SECURITY SCANNER AND POLICY ENFORCER

Madhu “madhuakula” Akula
Friday from 09:00 to 09:45 in W209
Saturday from 16:00 to 16:45 in W212

Spotter is a groundbreaking open-source tool designed to secure Kubernetes clusters throughout their lifecycle. Built on the native tooling of Kubernetes by leveraging Common Expression Language for policy definitions, we can define unified security scanning across development, CLI, CI/CD, admission controllers, deployments, runtime, and continuous monitoring. Its unique approach enables both enforcement and monitoring modes, ensuring that policies can be applied consistently and mapped directly to industry standards such as CIS and MITRE ATT&CK. Spotter provides extremely high flexibility across all Kubernetes phases, providing an innovative approach that no other open-source or commercial solution can replicate. It seamlessly bridges security, DevOps, and platform teams, effectively solving the real-world challenges faced by day-to-day operations.

Audience: Cloud, Offense/Red Team, Purple Team

TENGU MARAUDER V2

Lexie “L3xic0n” Thach, Munir Muhammad
Saturday from 16:00 to 16:45 in W208
Friday from 16:00 to 16:45 in W212

Designed for wireless security testing and autonomous reconnaissance, Tengu Marauder v2 is a multi-terrain open-source robotic platform. Built around a Raspberry Pi and using ROS2, it combines real-time motor control, RF monitoring, and sensor data streaming to facilitate remote operations in challenging environments. Over the initial architecture, the v2 platform brings major enhancements in system modularity, communication security, and operational flexibility. Designed for safe remote access using encrypted VPN tunnels, the robot allows internet-based control and telemetry without endangering the system to direct network threats. Tengu Marauder v2 provides a tough, scalable basis for incorporating autonomy and cyber capabilities into your mobile security toolset whether used for off-grid automation, robotics teaching, or red teaming.

Audience: Offense/Red Team, Robotics, Hardware

THETIMEMACHINE

Arjun “T3R4_KAAL” Chaudhary, Anmol “Fr13nd0x7f” K. Sachan
Saturday from 09:00 to 09:45 in W209
Friday from 09:00 to 09:45 in W211

TheTimeMachine is an offensive OSINT and bug bounty recon suite that revives forgotten endpoints from the past using the Wayback Machine. Designed for red teamers, CTF players, and bounty hunters, it automates historical data mining, subdomain extraction, parameter harvesting, and endpoint fuzzing for vulnerabilities like XSS, open redirect, LFI, and SQLi. The suite also integrates a powerful JWT analysis engine to extract, decode, and highlight juicy fields from tokens hidden in archived URLs. TheTimeMachine also hunts leaked archives and even verifies whether archived snapshots are still live. With colorful terminal output, modular CLI tools, and support for custom wordlists, this tool resurrects the buried past to exploit the forgotten future. Dead links don’t die here,Âîthey just get reconned harder.

Audience: Defense/Blue Team, Threat Hunting, Offense/Red Team

UNMANNED WIRELESS PENETRATION TESTING DEVICE

Ayaan Qayyum, Omar Hamoudeh
Saturday from 11:00 to 11:45 in W212
Friday from 13:00 to 13:45 in W212

The Unmanned Wireless Penetration Testing Device is a modular, open-source system enabling remote wireless security assessments. Using long-range LoRa communication, a mobile rover can perform Wi-Fi reconnaissance, deauthentication attacks, Bluetooth device discovery, and image capture without requiring proximity to the target network. Controlled entirely via encrypted LoRa packets, the system is optimized for secure operations in remote or inaccessible environments. Attendees will see live demonstrations of wireless attacks issued over LoRa and learn how the system can be adapted for mobile and drone-based security operations. Source code and build instructions will be freely available under an open license.

Audience: Hardware, Offense/Red Team, Mobile

WARHEAD

Vishal “Vish” Thakur, David “Votd_ctf” Wearing
Friday from 15:00 to 15:45 in W208
Saturday from 10:00 to 10:45 in W212

Warhead is an offensive security tool that leverages Windows Atom Tables to store, retrieve, and execute payloads in a stealthy manner. This technique enables adversaries to place a payload in the Atom Table, use a legitimate process to extract it, and execute it in memory,Âîbypassing traditional detection mechanisms. The first version of Warhead, to be released at Black Hat Arsenal 2025, provides security researchers and red teamers with a novel approach to payload delivery and execution that evades modern security defenses.

Audience: Purple Team, Malware, Offense/Red Team

VENDORS

CRYPTOCURRENCY ADVOCATE
www.cryptoadvocate.cc

The Cryptocurrency areas at DEF CON serve hackers seeking rewards from learning, testing, and securing modern finance technology. We produce and distribute merchandise as well, in the DEF CON Vendor area. Please come meet us, a few metres away from the other Cryptocurrency (Community and Contest) areas. Free of charge and commercially sold items include branding with Bitcoin, Lightning, Monero, Ethereum, Litecoin, Nostr and others. Show your cryptohacker colours with high quality wearables and custom badges. Try new devices and electronics, with access to the producers on site. Inform yourself of cryptocurrency science by exploring the products on display. Our stand is your one stop shop for cryptocurrency hacker merchandise, where we usually have a number of items available free of charge to giveaway!

Payment methods: Cryptocurrency USD cash Mastercard Visa Paypal

DEEPNET LLC
deepnet.store

deepnet.store creates limited-run SAOs, electronic badges, and hardware hacking tools that blend aesthetics with interactivity. Our products range from visually striking blinky SAOs to reprogrammable ESP32-S3 devices, designed for collectors, makers, and anyone curious about hardware hacking. We make microcontrollers fun, accessible, and easy to experiment with. Visit us at deepnet.store and follow us on Instagram (@deepnetstore) for the latest updates. We accept cash, credit cards, PayPal, Shop Pay, and G Pay.

ELECTRONIC CATS
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 and flipper addons

ELECTRONIC FRONTIER FOUNDATION (EFF)
eff.org

The Electronic Frontier Foundation (EFF) is the leading organization defending civil liberties in the digital world. We defend free speech on the internet, fight illegal surveillance, support freedom-enhancing technologies, promote the rights of digital innovators, and work to ensure that the rights and freedoms we enjoy are enhanced, rather than eroded, as our use of technology grows.

EXPLIOT
expliot.io

EXPLIoT is a pioneering IoT security startup dedicated to making embedded/IoT security assessments more accessible and efficient. Our innovative platform delivers automated and intelligent device security and compliance assessment, encompassing firmware, hardware, and RF interface scans. By providing cutting-edge tools, resources, and open-source contributions, we empower engineering and security teams to scale and streamline their IoT assessments. With a strong commitment to community engagement and continuous learning, EXPLIoT is advancing the field of embedded/IoT security and enabling organizations to build more secure connected products.

FREE WILI - INTREPID CONTROL SYSTEMS INC
www.intrepidcs.com

FREE-WiLi is a powerful and versatile embedded development and learning tool, designed for both developers and enthusiasts. It combines SPI, I2C, and UART interfaces with USB ports, a robust FPGA, and expandable Orca modules. The tool features a display, customizable buttons, LEDs, an IR transmitter, and a speaker, along with dual Sub-GHz radios for wireless applications. Ideal for protocol simulation, cybersecurity testing, and IoT development, it also includes onboard storage, a rechargeable battery, RTC, and accelerometer. FREE-WiLi supports USB serial control, WebAssembly scripting (C/C++, Rust, Zig, Tiny Go), and Python API integration. Software features include Sigrok Logic Analyzer support, a customizable GUI, ZoomIO for high-precision IO control, integrated sounds/images, Numbers To Speech, and FAT file system compatibility. With open-source software updates on GitHub, FREE-WiLi offers a comprehensive, all-in-one platform for flexible, high-performance development.

HACKERBOXES
hackerboxes.com

HackerBoxes is the original monthly subscription box for the hacker community. Offerings include 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.

HACKERWAREHOUSE
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.

HAK5 LLC
shop.hak5.org

Since 2005, Hak5 has been reminding you to Trust your Technolust. This year, we invite you to join us in celebrating 20 years. Look for the giant Pineapple. Come by the Hak5 booth. Discover the devices that have found their way into the hearts and tool-kits of the modern hacker — including some very special, limited edition machines of mayhem.

IFIXIT
www.ifixit.com

Hackers, get ready to break open some hardware with iFixit. Meet the team behind the teardowns, and pick up some proprietary screwdrivers and opening tools.

Want to learn to solder? Our new USB-C iron is perfect for soldering on the go. Come on by and pick up a new skill.

We just legalized hacking McFlurry machines, but that's only fun if you can take advantage! See if you can break into ours.

Join the Right to Repair movement and pick up some swag, with a portion of our proceeds going to Repair.org to further the cause. If you can't open it, you don't own it!

KEYPORT
mykeyport.com

Keyport makes DEF CON swag you will actually use every single day combining keys, pocket tools, & tech into an all-in-one hacker multi-tool. Explore our latest modular product line, featuring the exclusive DEF CON 33 Editions of the Keyport Pivot, Tool Modules, and Inserts. Plus, don't miss our limited edition accessories, including a custom maker kit, unique NFC challenge coin, glow-in-the-dark patches, magnetic quick releases, and much more.

KILLCHAINZ CLOTHING
Killchainz.shop

Killchainz Clothing's missions are to influence culture through art, and to elevate the morale of blue and red teams everywhere. We focus on creating t-shirts you'd be proud to wear on casual Friday in the office, and art for your office or cave wall. We also do custom designs for other teams... reach out and see what our "memetic fabrication specialists" can do for you.

M2 POWERED PARTNERS LLC
m2-p2.com

M2-P2 is a science-backed wellness company on a mission to help people unlock full mental and physical potential. Founded by experts in biochemistry and nutrition, M2-P2 creates high-performance supplements like FocusQuest Max and CogniQuest, designed to support all-day energy, focus, cognition function and motivation without the crash. Whether you're a busy professional, gamer, or someone striving to level up your productivity and performance, M2-P2 delivers clinically studied ingredients in convenient, portable formats. M2-P2 bridges the gap between hard science and everyday energy needs so you can focus better, feel better, and do more.

VENDORS

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.

MIDWEST GADGETS LLC
www.midwestgadgets.com

Midwest Gadgets is a Detroit-based hardware company creating specialized tools for the hacking and biohacking community. Maker-focused and independently owned, we design and manufacture NFC and RFID devices—including repeaters, field detectors, amplifiers, and custom antennas—built specifically to support tinkerers, hackers, and implant enthusiasts pushing the limits of personal tech. Every product is prototyped, tested, and assembled in-house with a focus on functionality, adaptability, and real-world application. Whether you're enhancing read range, troubleshooting field behavior, or experimenting with implants, Midwest Gadgets delivers purpose-built gear designed to empower exploration.

MISCREANTS, LLC
miscreants.com

Miscreants®

Miscreants is a creative collective injecting design into cybersecurity. Over the years, we've designed some of your favorite cybersecurity brands, websites, and products. As a clothing brand, we're creating merchandise heavily influenced by streetwear and security culture, looking to document the past, present, and future of cybersecurity history.

NO STARCH PRESS, INC
nostarch.com

no starch press®

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 LLC
nuand.com

nuand

Nuand designs and manufactures the open-source bladeRF family of software-defined radios, used by engineers, educators, and researchers to push the boundaries of wireless innovation.

OCTOPWN GMBH
www.octopwn.com

octopwn
PENTESTING IN YOUR BROWSER

Octopwn is an internal network pentesting suite that allows you to do your job faster and with better quality. Scanners, clients, utilities and attacks are all integrated with comprehensive logging for your convenience. If you want to work even faster, add your own Python tools and fully automate your custom workflow, but with the same quality as a manual pentest. Plus, Octopwn works on any OS. This year we will be vending a special AutoPwn USB stick - just plug it in and let the magic happen."

PHYSSEC EDUCATION
www.physsec.org

The Physical Security Village (formerly Lock Bypass Village) will be present in the vendor area this year, loaded with physical hacking gear! We will have bypass tools, common keyed-alike keys, handcuffs, village swag, and more. This year we'll also be collaborating with Covert Instruments to bring to you a better selection of physical security equipment!

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.

RABBIT-LABS
rabbit-labs.com

Rabbit-Labs is a collective of great minds. Rabbit-Labs is the gathering of people from all walks of life who love to explore tech and share novel ideas and discoveries. Rabbit-Labs isn't just a brand, it's a lifestyle of pushing the boundaries of what is possible and never taking the easy route or cutting corners. Our core values, Inclusion, Integrity, Empathy, Quality, & Transparency, are always at the top of our mind in anything we do. It is our core values that motivate us every day, that allow Rabbit-Labs to grow, & that thrusted upon us this amazing community.

REKCAH PUBLISHING
rekcahcomics.com

REKCAH! Publishing creates comic books and zines for the information security industry and for comic fans of true-crime stories. Our newest release The Future Is ****** takes a look at what information security will look like in the future. The books are filled with puzzles and ciphers for the readers to solve.

RED TEAM TOOLS
redteamtools.com

RED TEAM TOOLS

Red Team Tools is a venerable supplier of physical security hardware used by professionals in the fields of covert entry, penetration testing, and emergency response. Formed by two notable names in the security world: Deviant Ollam and Babak Javadi, the founders spent over a decade spreading knowledge, building community, educating the public, and designing tools for hackers and professionals alike. As security professionals specializing in non-destructive entry, the Red Team Tools cadre designs and produces gear for attacking and defending both mechanical and electronic access control systems. Over the years Deviant and the team have brought dozens of new, innovative designs to the market and we are proud to share our knowledge and our equipment with you all here at DEF CON.

ROGUE'S ROOST, LLC
Rogue's Roost offers cool, unique, and cute tech-themed clothing, accessories, and art. Stop by to see the latest designs!

ROKLAND LLC
www.rokland.com

We are a leading retailer and developer of WiFi, 4G, and Meshtastic networking & IoT products in Gainesville, Florida.

SALTY SECURITY
saltysecurity.com



Salty Security is back for our hat trick at DEF CON 33. And we've got THE best hacker-themed apparel and gadgets around. With all the 3s running around, you couldn't have more luck if you stuffed Larry Bird into a Rolling Rock vat and called it "Old Larrytrobe"! Some come get your merch from the mouth and help bring future and aspiring hackers and security folks into the field. Maybe sign up for some free training while you're at it!

SHADOWVEX INDUSTRIES
shadowvexindustries.com

SVX

Purveyors of limited-edition DEF CON 33 clothing, music mixes, and other 0-day hacker lifestyle wares. Follow the music in the vendor area to track us down!

THE SOURCE OF KNOWLEDGE (SOK)
thesourceofknowledge.com

SPARROWS MANUFACTURING CO
www.sparrowslockpicks.com

SPARROWS

SPARROWS: 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

VENDORS

will be on display and available for sale in a hands on environment. Our Product range covers Custom toolsets, Entry Tools, Practice locks, Bypass tools, Urban Escape & Evasion hardware and items that until recently were sales restricted. The DREADNOUGHT will also be available to the public for the first time in limited quantities. All products will be demonstrated at various times and can be personally tested for use and Efficacy.

THE CALYX INSTITUTE
calyxinstitute.org

The Calyx Institute (calyx.org) defends digital privacy, advances connectivity, and strives for a future where everyone has access to the resources and tools they need to remain securely connected.

We build and maintain a privacy-respecting ecosystem of free and open-source software (FOSS) centering on CalyxOS, an operating system for Android devices, that enables people to enjoy their lives online with data privacy and dignity. We offer hands-on tools, such as the Calyx hotspot, for people to access the internet easily wherever they are, especially in areas where connectivity options are limited. Through grantmaking, research, education, and community capacity building, we support internet freedom that allows the public to make informed choices about their online lives.

We can't do this work without support from our members. Become a member today and join our collective effort to enhance digital privacy and security for all! As a Calyx Internet member, you can get a Calyx Hotspot—or use your own device—with a SIM card that connects you to the entire T-Mobile network with unlimited data in the U.S.. As a CalyxOS Phone member, you will get a Pixel 8a phone with CalyxOS pre-installed. Visit https://calyx.org/membership for more information.

THE OPEN ORGANISATION OF LOCKPICKERS (TOOOL)
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 TOR PROJECT, INC.
torproject.org

The Tor Project (torproject.org) is a nonprofit developing free and open-source software to protect people from tracking, censorship, and surveillance online. Stop by our booth in the vendor hall to learn more about our recent projects, pick up some gear, and find out how you can get involved. Donations by cash, credit card, contactless payments, and Bitcoin accepted.

WOMEN IN SECURITY AND PRIVACY
www.wisporg.com

Women in Security and Privacy (WISP)'s mission is to advance women and underrepresented communities to lead the future of privacy and security. WISP merch is available and donations support the nonprofit organization's mission.

XCAPE, INC.
Xca.pe

Xcape, Inc., the platform for pentesters to be everywhere and no where at the same time.

ARTS AND ENT.

BOOK SIGNINGS

Books signings will be in Hall 4 near the Vendor area

ADVERSARY EMULATION WITH MITRE ATT&CK - DRINOR SELMANAJ
Friday from 10:00 to 11:00 in V301 Book Signings - Table 2
Saturday from 10:00 to 11:00 in V301 Book Signings - Table 4

CYBER CALENDAR 2026 - CHRIS DECARMEN/SQUARED AWAY LLC
Saturday from 14:00 to 15:00 in V301 Book Signings - Table 2
Saturday from 10:00 to 11:00 in V301 Book Signings - Table 2
Friday from 10:00 to 11:00 in V301 Book Signings - Table 4

JON DIMAGGIO/ NO STARCH PRESS
Friday from 11:00 to 12:00 in V301 Book Signings - Table 1

SUPPLY CHAIN SOFTWARE SECURITY- AI, IOT AND APPLICATION SECURITY - AAMIRUDDIN SYED/APRES MEDIA LLC
Friday from 11:00 to 12:00 in V301 Book Signings - Table 3
Payment method: Zelle, Wire transfer

TRAVIS GOODSPEED/NO STARCH PRESS
Friday from 12:00 to 13:00 in V301 Book Signings - Table 1

CAREY PARKER - FIREWALLS DON'T STOP DRAGONS: A STEP-BY-STEP GUIDE TO COMPUTER SECURITY AND PRIVACY FOR NON-TECHIES (5TH ED)
Friday from 12:00 to 13:00 in V301 Book Signings - Table 2

KURTIS MINDERBOOK: CYBER RECON: MY LIFE IN CYBER ESPIONAGE AND RANSOMWARE NEGOTIATION
Friday from 12:00 to 13:00 in V301 Book Signings

NICK ALEKS/NO STARCH PRESS
Friday from 13:00 to 14:00 in V301 Book Signings - Table 1

ALEX MATROSOV/NO STARCH PRESS
Friday from 13:00 to 14:00 in V301 Book Signings - Table 3

PHILIP DUNSEY/NO STARCH PRESS
Friday from 14:00 to 15:00 in V301 Book Signings - Table 1

ALFIE CHAMPION/NO STARCH PRESS
Friday from 14:00 to 15:00 in V301 Book Signings - Table 3

JP AUSMASSON/NO STARCH PRESS
Friday from 15:00 to 16:00 in V301 Book Signings - Table 1

FUTURE OF HACKING: THE RISE OF CYBERCRIME AND THE FIGHT TO KEEP US SAFE - LAURA S. SCHERLING, EDD / BLOOMSBURY
Saturday from 11:00 to 12:00 in V301 Book Signings - Table 4
Friday from 15:00 to 16:00 in V301 Book Signings - Table 2
Accepted Payment Methods: Cash, Venmo, and Paypal

DANIEL REILLY/NO STARCH PRESS
Friday from 15:00 to 16:00 in V301 Book Signings - Table 3

THE HACKER MINDSET: A 5-STEP METHODOLOGY FOR CRACKING THE SYSTEM AND ACHIEVING YOUR DREAMS - GARRETT GEE/HACKER WAREHOUSE
Friday from 15:00 to 16:00 in V301 Book Signings - Table 4
Saturday from 14:00 to 15:00 in V301 Book Signings - Table 4
Friday from 16:00 to 17:00 in V301 Book Signings - Table 1

BREAKING IN: A PRACTICAL GUIDE TO STARTING A CAREER IN INFORMATION SECURITY CYBERSECURITY ESSENTIALS FOR STARTUPS : A PRACTICAL GUIDE - AYMAN ELSAWAH
Friday from 16:00 to 17:00 in V301 Book Signings - Table 4
Saturday from 16:00 to 17:00 in V301 Book Signings - Table 2

KYLE CUCCI/NO STARCH PRESS
Saturday from 10:00 to 11:00 in V301 Book Signings - Table 1

PATRICK WARDLE/ NO STARCH PRESS
Saturday from 10:00 to 11:00 in V301 Book Signings - Table 3

COREY BALL/NO STARCH PRESS
Saturday from 11:00 to 12:00 in V301 Book Signings - Table 1

CASEY EDMAN/NO STARCH PRESS
Saturday from 11:00 to 12:00 in V301 Book Signings - Table 3

MICAH LEE/ NO STARCH PRESS
Saturday from 12:00 to 13:00 in V301 Book Signings - Table 1

PRACTICAL LOCK PICKING; KEYS TO THE KINGDOM - DEVIANT OLLAM/RED TEAM TOOLS
Saturday from 12:00 to 13:00 in V301 Book Signings - Table 2

EUGENE LIM/ NO STARCH PRESS
Saturday from 13:00 to 14:00 in V301 Book Signings - Table 1

FOTIS CHANTIZIS/ NO STARCH PRESS
Saturday from 14:00 to 15:00 in V301 Book Signings - Table 1

PAULINO CALDERON/NO STARCH PRESS
Saturday from 14:00 to 15:00 in V301 Book Signings - Table 3

JASON ANDRESS/ NO STARCH PRESS
Saturday from 15:00 to 16:00 in V301 Book Signings - Table 1

KARA NANCE/NO STARCH PRESS
Saturday from 15:00 to 16:00 in V301 Book Signings - Table 3

THE BROWSER SECURITY FIELD MANUAL ADELINE - AUDREY ADELINE
Saturday from 15:00 to 16:00 in V301 Book Signings - Table 4

AGHOST HACKER : HOW TO HACK HUMAN SPIRIT - JUN KAWASAKI
Sunday from 10:00 to 11:00 in V301 Book Signings - Table 4
Payment Method: Credit Card, Paypal

DC 33 Engagements - Car Hacking Village, Biohacking Village, GenSec, AIxCC

EXHIBITORS

Altered Security

ALTEREDSECURITY.COM

Bronze Exhibitor

Start your Red Team training with us! Altered Security offers multiple Red Team courses with affordable and enterprise-like hands-on labs. Each course comes with an industry-recognized certification. We are the creators of the Certified Red Team Professional (CRTP), CRTE, CARTP and more. Our courses and labs are designed by experts who have more than a decade's experience of training and speaking at worlds top hacker conferences. Join more than 40K professionals from 130+ countries.

Authentik

GOAUTHENTIK.IO

Bronze Exhibitor

Authentik Security is the Public Benefit Company behind authentik, an open source identity provider with over a million installations. Authentik Security is bringing modern identity and access management to organizations worldwide, replacing inflexible legacy alternatives for leading companies like Cloudflare, Der Spiegel, and CoreWeave. We are a fully remote team and always looking for more backend dev and identity experts and enthusiasts to join our mission. Help us replace Okta/Auth0, Ping Identity, and Microsoft Entra with modern, secure identity for all!

Black Hills

BLACKHILLSINFOSEC.COM

Bronze Exhibitor

BHIS is owned by us—no investors, no outside agendas. We'll never have investors because our focus is on you. Our Business Capture team isn't chasing commissions. Our Content & Community team doesn't measure success by revenue. And our technical consultants are always improving, thinking creatively about how to serve you best. We do this, because we grew up inspired by heroes in stories—those who never gave up. But every hero had help: a guide, a mentor, a magical sword. We want to be that for you—your guide, your mentor, your sword supplier—so you can keep fighting the good fight.

Bugcrowd

BUGCROWD.COM

Bronze Exhibitor

We are Bugcrowd. Since 2012, we've been empowering organizations to take back control and stay ahead of threat actors by uniting the collective ingenuity and expertise of our customers and trusted alliance of elite hackers, with our patented data and AI-powered Bugcrowd Platform™. Our network of hackers brings diverse expertise to uncover hidden weaknesses, adapting swiftly to evolving threats, even against zero-day exploits. With unmatched scalability and adaptability, our data and AI-driven CrowdMatch™ technology in our platform finds the perfect talent for your unique fight. We are creating a new era of modern crowdsourced security that outpaces threat actors.

Capitol Technology University

CAPTECHU.EDU

Silver Exhibitor

Capitol Technology University joins DC33 as a leader in technology higher education. With flexible undergraduate and graduate programs available online and on-campus, CapTechU equips the next generation of tech innovators and global STEM professionals for career success. Visit our booth to discuss your career goals with our expert staff, grab free info and swag, purchase our exclusive DEF CON 33 limited-edition t-shirt and light-up badge, and snap a photo with our Charlie the Charger mascot. Don't miss this opportunity to charge up your future!

CISA

CISA.GOV

Silver Exhibitor

As America's Cyber Defense Agency and the National Coordinator for critical infrastructure resiliency and security, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day. We connect our stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people.

EXHIBITORS

Formal

JOINFORMAL.COM

Bronze Exhibitor

Formal gives you visibility and control where you need it most: at the point of data access. It sits between your AI agents, services, and datastore - Snowflake, APIs, whatever - and inspects every request in real time. You get deep, protocol-level context: who made the call, what was requested, whether it involved PII, and what policy should apply.

What is critical for AI governance is that Formal secures the Model Context Protocol layer - the MCP server that feeds data to AI agents. You're not trusting a black box to make its own decisions. You're governing exactly what goes in and out of it and by whom. You define and enforce policies, access, stop leaks, and stay audit-ready - all without slowing down engineering.

This is how security leads in the AI era: not with red tape, but with infrastructure-aware enforcement.

Hack The Box

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. Offering an all-in-one environment for continuous growth, assessment, and recruitment, Hack The Box provides solutions for all cybersecurity domains. Launched in 2017, Hack The Box brings together the largest global cybersecurity community of more than 3.5 million platform members. Rapidly growing its international footprint and reach, Hack The Box is headquartered in the UK, with additional offices in the US, Australia, and Greece.

Promptfoo

PROMPTFOO.DEV

Bronze Exhibitor

Promptfoo is an advanced red teaming and vulnerability management platform that helps teams identify and fix generative AI security risks before they reach production by integrating directly into the development pipeline. It scans LLM applications, MCP servers, agents, and models for vulnerabilities such as prompt injections, jailbreaks, and data poisoning, while enforcing custom security policies and providing detailed remediation guidance. Promptfoo's specialized adversarial agents are trained to analyze each application's unique attack surface and generate targeted probes that uncover natural-language vulnerabilities. By shifting security testing left, Promptfoo enables organizations to address issues early and cost-effectively, and is trusted by more than 100,000 developers and enterprises, including OpenAI, Anthropic, and AWS.

The SecOps Group

SECOPS.GROUP

Bronze Exhibitor

The SecOps Group (secops.group) is a CREST-accredited cybersecurity company trusted by Fortune 100 clients for its research-driven pentesting services. We offer specialized assessments across web, mobile, API, cloud, networks, and Red Team operations. Through our certification platform, pentestingexams.com, professionals can access 15 hands-on exams covering AppSec, network security, binary fuzzing, Red Teaming, and LLM pentesting—ranging from beginner to advanced levels. Over 75,000 professionals have taken our exams in the past two years. Visit our booth at DEF CON 2025 and claim a FREE exam!

Triad Secure

TRIAD-SECURE.COM

Bronze Exhibitor

Triad Secure is a cutting-edge technology company dedicated to transforming cybersecurity operations through its innovative AI-driven platform, designed to address the growing challenges faced by Security Operations Centers (SOCs) worldwide. By integrating all existing SOC tools into a single, intuitive interface, our platform normalizes and enriches data to deliver a unified, actionable view of alerts, significantly reducing triage time by over 50% and eliminating the need for extensive training across multiple systems. Built with multi-tenant support and visual automation tools, Triad Secure empowers MSPs and enterprises to streamline workflows, manage complex environments, and respond smarter and faster to threats, all while leveraging built-in threat intelligence and a seamless ticketing system, positioning us as a leader in scalable, efficient cybersecurity solutions.

US Army xTech

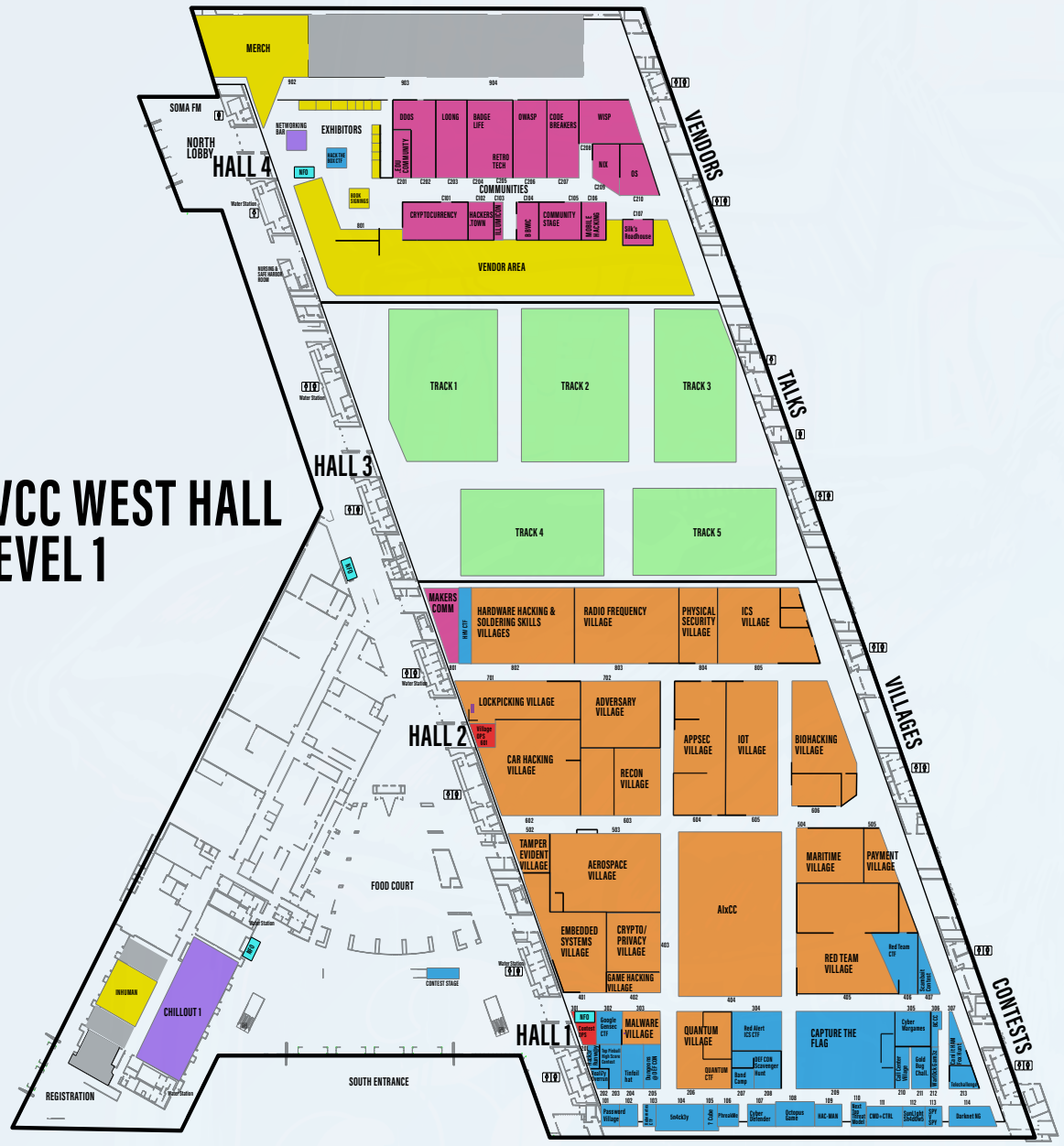
XTECH.ARMY.MIL

Silver Exhibitor

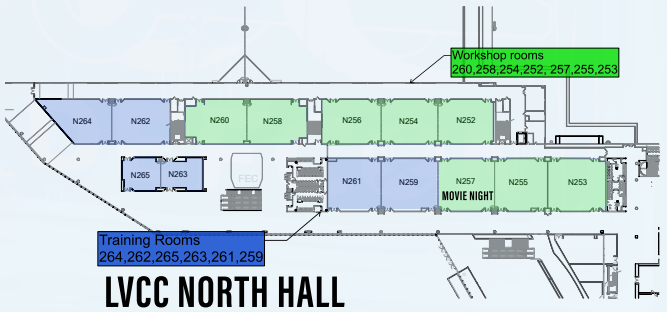
The U.S. Army xTech Program, sponsored by the Assistant Secretary of the Army for Acquisition, Logistics and Technology, manages the Army's prize competitions to award and accelerate transformative S&T solutions from small and non-traditional businesses that can help solve current challenges. Competitions offer a variety of potential opportunities to participants including cash prizes, the potential for follow-on contracts and opportunities to participate in accelerator programming that provides education, mentorship and strategic exposure.

MAPS

LVCC WEST HALL LEVEL 1



LVCC NORTH HALL LEVEL 2



LVCC WEST HALL LEVEL 2



LVCC WEST HALL LEVEL 3

THANK YOU!

The Dark Tangent would like to thank all the HQ staff, old and new this year: Cot, ETA, Janet, KevOps, Mar, Matt, Nikita, Drifter, Seeyew, Sleestak, and Will that worked year round to make this conference possible. Some have moved on to other opportunities, and for some this is their first year! Thank you to those who came forward to help put our Code of Conduct into practice. I would like to thank our fantastic legal team, including David, Matt, and Lauren, for the dismissal with prejudice of Chris Hadnagy's defamation lawsuit because we banned him for abusive CoC violations. I'd also like to thank the LVCC for being a wonderful host, Gag Lab for creative solutions to the shortened move in and out dates this year, and all the vendors who support us. Finally I'd like to thank the community of Goons and Creators who make the conference possible. Each department leader has their thank yous below, I won't steal their thunder.

-The Dark Tangent

DEF CON is only possible because of all the hard work from the people who make up departments:

A&E

DEF CON Arts And Entertainment is:

Arysyth, Ch0wn35, ChrisAM, cymike, dead, Dr. Salem, Kriz Klink, Luna, Miss Jackalope, Shoresy, Skittish, STITCH, Zziks

We would like to thank the following:

DEF CON staff , Gaglab, Zebbler Studios, SOMAFM.com, AND ALL THE ARTISTS THAT PROVIDED THER AMAZING TALENT!!

DJ's, Musicians, Producers, We applaud you.

Special thanks to the attendees who chipped in and helped us throughout the conference

Its actions like this that make a community special.

- Thank you.

Zziks A&E Dept Lead

CFP REVIEW BOARD

pwcrack and Shaggy would like to give a huge thank you to Dark Tangent, Nikita, Alex, AlxRogan, Ash, Binary Buddha, carnal0wnage, CaseyEllis, Cederic, Clavinger, Crob, CyberSulu, Da Kahuna, Dead Addict, Deana, Dino C, Duck Duck, efffn, FV, Gabsmashh, Grifter, H4r0ld, Heisenberg, Jay Healey, Jeonda, Jon Green, Lady_N, LawyerLiz, Magen, Malware Unicorn, Marcia, Matt Wein, Medic, Mosfet, n00bz, Piggles, RayDavidson, RoRo, SecBarbie, Seth van Ommen, Sinderz, Snow, solstice, Suggy, V3rbaal, West, 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, workshop, demo labs and policy content.

CONTESTS

Grifter and klrgrz would like to thank all of the creators and coordinators of the multitude of contests and events at DEF CON 33. Your dedication to these events is clear, and we deeply value the incredible entertainment you provide. It makes a huge difference to the contestants, attendees, and the entire DEF CON experience. Thank you so much! A massive thanks to the Contests Goons for putting out fires, answering "where's Grifter" for the 100th time, and all you do to support the creators. Thank you to c0l3slaw, _Dwyer_, EvilMog, gateherder, Gomer, Heathenhkr, Heisenberg, Lady Secitup, MalwareJake, p0lr, psychoticide, saltr, Secove, Sh00k3ms, Sonicos, vertighost, and Zero3. Massive thanks to the Dark Tangent, Janet, Neil, Will, and Darrington for the support to do this every year. A very special thanks to Nikita for keeping us ALL on track, motivated, and entertained. And to our fellow hackers, thanks for shenanigans, the laughs, and the mild disappointment (not you, yes you, you know what you did!). Thanks for playing, see you next year... and HACK THE PLANET!

COMMUNITIES

ch3f and f0rk3d would like to extend a sincere and heartfelt thank you to the Villages leadership: Hony, Paydreaux, br00zer, and Raze. Along with Nikita, your unwavering support has allowed us to hit the ground running with the Communities Department. Additional thanks to the Community Leads and volunteers. Your hard work and dedication makes DEF CON what it is. Thank you for sharing your Community with everyone. To all the other Departments and staff, including Dark Tangent, Nikita, and Janet - thank you for everything you do to make DEF CON happen!

CREATOR & COMMUNITY STAGES

Raze and Meat from the Creator and Community Stages would first and foremost like to thank Hony, Paydreaux, ch3f, and f0rk3d for all their hard work supporting the many, many villages and communities. Your dedication keeps this ecosystem thriving.

Huge thanks to all the Village Goons, from the bright-eyed noobs to the seasoned veterans. It's always a blast seeing you each year. Your support, effort, and passion are essential to DEF CON's success, and we appreciate everything you do.

To the Salty Department, thank you for all the laughs and the levity. You keep things fun even when chaos reigns.

To all the speakers who brought their knowledge, time, and stories to the Creator and Community Stages: thank you for enlightening us, inspiring us, and reminding us why we care so much about this hacker community. Your passion is contagious, and your voices help shape the soul of DEF CON.

Con Mom, you the best!"

DEFACEMENT

Medic and SamG0ld want to give a massive THANK YOU to the Defacement crew for the long hours and heavy lifting — deploying signage, laying vinyl, and building the sticker walls that make this place feel like home.

Xaphan, BDA, p0ster b0y, BigSam, RJ, mage2, SatanicNoodle, d_z_az, and Melware — y'all crushed it. We couldn't have done it without you.

We'd also like to give a special thank you to DT, Nikita, Neil, and the rest of the DC Staff — for the trust, support, and the opportunity to contribute to the experience that brings DEF CON to life.

DEVOPS

Riverside & Fox would like to thank the DevOps team and contributors (Mauvehed, Respondo, NightWolf, Lightning, Nebberz, Mubix, cstone and the various testers on the PHV team) for their year-round contributions to improving the overall DevOps pipeline, bots and discord experience for both Humans and Goons.

DC KIDS / DC NEXTGEN

Raider Raccoon would like to thank DEF CON for providing a space where DCNextGen can empower the next generation of cyber warriors. A special thanks to the amazing DEF CON villages who helped bring the projects to life. Raider also extends a big racoon thanks to all the incredible goons and volunteers who made DCNextGen a reality - because of you, new passions for hacking were sparked!

DCTV

"YESSS, PRECIOUS THANKS TO THE MIGHTY DCTV HORDE!

gnashes teeth appreciatively

The goblin-king bows low to the fierce warriors: Bool-Z the Cunning, Eagle1 the Sharp-Eyed, Ghost Pepper the Fiery One, K# the Cryptic, Robbinbs the Swift-Fingered, Sandw1ch the Nourishing, Laa skw33k the Mysterious Squeaker, and Videoman the All-Seeing!

hisses with delight

AND EXTRA GROVELING GRATITUDE TO THE SACRED NOC AND THE MIGHTY QM! pounds chest with bony fists They guard our precious signals like dragons guard their treasure hoards!

The goblin-clan shall remember these names in our victory chants around the flickering screen-fires! YESSSS! scurries away cackling

DC GROUPS

The DEF CON Groups (DCG) Dept. Goons would like to give a global shout-out to everyone supporting the 400+ local DEF CON Groups worldwide!

DCG meetups spark curiosity, build community, and create space for mentorship and collaboration - ensuring our culture continues to grow and inspire.

Whether you're an organizer or attendee, thank you for the time, energy, and passion you bring.

Special thanks to DCG Dept. Goons: alethe, Jayson E. Street, deviled_3gg, polomaster, and adam915 for their year-round dedication to growing our community.

Additional DEF CON Goon shout-outs to Riverside, Polybius, Drew, G0rd0, Log, and the KevOps crew for their on-the-ground and behind-the-scenes support, both at DEF CON and on Discord.

Lastly, heartfelt thanks to DT, Nikita, Darington, Kevin, Neil, Janet, and Cot for your continued trust and support in making DCG a vital part of the DEF CON ecosystem."

DEMO LABS

H4r0ld and V3rbaal would like to thank all of the Demo Labs goons: SecurePadawan, Mythrandr, LAZ, J9, deftclip, CountZ3r0 and AtlBee. We would also like to give a special shout out to Heisenberg for his dedication and support over the years.

DISPATCH

rf and Asmodian X would like to thank our wonderful group of returning goons – Ahab, Archangel, CodexMafia, dirtclod, dll3ma, Dymz, fozzie, Goon22, JUICE, L0g1c, Merg. miggles, MyLittleBrony, Offroad, Pooker, rixon, skyria, taclane, w00k, and zacperian. We're also excited to welcome and thank our new teammates BigDawgDave, DebugDonut, malloc, N4TRQJEDI, and networkgeek. Thank you all for another great year and don't forget – Dispatch is always listening."

EXHIBITORS

Polybius and g0rd0 extend heartfelt thanks to our exhibitors for their incredible support. Your generous donations to nonprofits, backing of our talented creators, and contributions to DEF CON strengthen our community and make this event truly unforgettable!

Capitol Technology University, CISA, Hack The Box, US ARMY xTech, Altered Security, Authentik, Black Hills, Bugcrowd, Formal, Promptfoo, The SecOps Group, Triad Secure

Thank you to the world class XZBT Goons:

VVitchofthewoods, JusticeStorm, Cealtea, Audrey, Rivet, DAF, RocketGod, billNYEusesMYwiFI, DAC, gaspar, FalconSpy, n3wTr0n, Slykitty, and Ramses.

Thank you to the Salty Ones and the XZBT adjacent support goons: Dani, Log, and PugLady.

A special thank you to JanetOps & NikitaOps. GrifterOps said it best, we love you more than legally allowed.

Finally, a big thank you to Kevin, the supreme leader of the very real department, KevOps. None of this would be possible without you."

DC SERVERS / INFRASTRUCTURE

Thanks to everyone that has helped make DEF CON 33 work and keep the servers and services working.

HACKER TRACKER

Drew "aNullValue" would like to thank the Hacker Tracker development team (advice, derail, KATT*BVTT, l4wke) for their year-round contributions to improving all of the Hacker Tracker apps. Thanks also to the lead staff of every creator and internal DEF CON department for their cooperation and timely schedule updates. Thanks most of all to Nikita, Neil, Janet, and Cotman for everything you do."

HDA

Thanks to all the people who have helped make HDA possible :

- The community leads & cat herders : ch3f , paydreaux, f0rked
- QM who gets us what we need to do what we do
- Janet , who somehow ensures that everything flows
- Nikita, who is only superseded by The Force in keeping things together
- The fallen but not forgotten : Tuna , The Nightstalker, Dan Kaminsky
- Sk0d, the Norse God of Infosec who stands at the side of Odin and protects our firewalls

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

KEVOPS, the absolutely 100% real Department, would like to thank all of the teams that give us the opportunity to help them make DEF CON as amazing as they can; Exhibitors, Parties, A&E, Vendors, DCG, and any one else that we've worked with and forgot to mention. We also want to thank DC Staff—Janet, Nikita (not a real department), Drifter, Cot, Darington, Mar, and Jeff.

KITAOPS

KITAOPS, Nikita's absolutely 100% real content & coordination department, would like to thank all of the teams that give us the opportunity to help them make DEF CON as amazing as they can; CFP, Communities, Contests and Black Badges, Creator Stages (RazeOps), DC NextGen, DCTV, Defacement, Demo Labs, Discord DEVOPS, Dispatch, Hacker Tracker, HDA, Inhuman Reg, NFO, NOC, Parties, Events & Meetups, Photo Goons, Policy, Press, QM, SOC, Speaker Ops, Vendors, Villages, Workshops, the magnificent XZBT DEPT, and everyone else above that KEVOPS (not a real dept) mentioned. Huge thank you to the Gag Labs & LVCC team. We also want to thank DC Staff—DT, Janet, KEVOPS (100% not a real dept), Drifter, Cotman, and Darington. Shout out and warm welcome to new lead for DEF CON Training, Seeyew & Analiese. Nikita & Hony would also like to emphatically thank C&C team salty, OBIC Polysauce, & aNullvalue.

MERCH

s3cr3t would like to thank all the Merch Goons: Themikeconnor, Oobleck, Mr Katt, Dasha, DadBaud, cillic, T@raByt3, Nyx, SudoLoak, Heal, B00MB0X, xFreed0m, K4TT*BVTT, TheViking, Surtr, Endsu, H4zy, gLoBuS, Burnt, Peej, Wally, gingerjet, daelf, Githur, LazyGamer, T@raByt3, Furysama, 10rn4, zubion, 5kyf4ll, Githur, Mr_Minion, Mic, Asmodeus, Tin, LM386, gadi, taladrane, x25, NA, rudy, SorJuana, Syeah, endurfeen, and BronzevilleBomber79 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 merchendise so we don't have to pack it up!"

NOC

The NOC would like to thank the following super rad people. These amazing people work tirelessly to give you all the bandwidth love.

....Deadication, wish, strange, c0mmiebstrd, effffn, Mike D, MeiBo, c7five, johntitor, booger, Jon2, CRV, Ra's al Ghul ,mac, toph, dp1i ,Duffguy and, Musa

Also a huge shout out to Nikita, Janet, GagLab, and DT, for all their amazing work putting this circus together.

This year we had less time to pull off this craziness off, but this amazing team came together rocked it like an 80s glam rock band!

Everyone in this community is so rad and we love your passion for security, art, knowledge, and learning!

Crazy times can be hard, and it is your community where you can draw strength, be awesome to each other and things will only get better!

"Programming today is a race between software engineers striving to build bigger and better idiot-proof programs, and the Universe trying to produce bigger and better idiots....."

Don't let the idiots win

NFO

Littlebruzer and Littleroo would like to thank all of the NFO goons: ?ace, 0tter, 1njection, 50 Caliber, algorythm, AngstyEmu, Aqua, ArbitraryMonster, bertoe, blu3f0x, Boudica, brubach, Bufo Alvarius, Cheshire, Commrade, D1Gger, Detaer, dL@w, DocDocGe3k, echonull, Emulor, Fr3nchie, GTOdevildog, Hankashyyyk, Jester, Krav, L8NiteHashBrowns, MACcat, Mackovision, madstringer, MajorMayhem, Momosa, Mouse of Madness, mrgreengaming21, Nav, Nil, Nymphaea Caerulea, Onyxcipher, pan1c, Paul, PEZhead, Profane Panda, Raven, S34MSTR3SS, s3cur17yf1rs7, S747IK, Sanchez, SchematicAddict, ScurryFool, Shrug, Skittl3z, Skreech, SKUZZYbus, SmileFiles, smite, spacezorro, Sparkle, Tachy0n, TechTurtle, Triggered_Sloth, Veiðimaður, and Viva.

The entire NFO team would like to thank DT, Nikita, Janet, Neil, eta and the rest of the HQ team. Without your support, we would not have this great conference.

Thank you to all of the department leads, seconds, and the entire goon staff for all of your help and support.

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 S3gfault want to kick things off with a huge, sleep-deprived THANK YOU to the amazing Goons who keep our Parties, Meetups, and Events running. Massive props to A&E for your wizardry, to Vendors and XZBT for always showing up with a helping hand when it's most needed.

To the Goons who keep the night shift lit—both literally and figuratively—we see you:

RickGlass, misusage, hevnsnt, SuRbO, SiliconRed, Datahere, Bastion, DotorNot, Supaida, and spicydll. You're the real MVPs

Big thanks to Jeff, Nikita, Neil, Janet, and Kevin for being the glue that holds this whole chaotic masterpiece together year after year.

To our creators: every year, you show up with something new—something weird, wild, and worth remembering. Thanks for keeping DEF CON loud, alive, and one-of-a-kind."

PHOTO

The Photo Goons want to thank the attendees for keeping it weird and giving us lots of things to video and photograph! Cannibal sends thanks to the team consisting of ASTCell, Silk, Gourry, AJ702, and M0nkeyDrag0n. Working long shifts every single day 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."

POLICY

Policy@DEF CON thanks their fearless leader RoRo, along with all their goons (Lady_N, Mosfet, Wein, RayDavidson, Jeonda, FV, West, Nina Alli, Duck Duck, Piggles, Gabsmashh), policy badge designers (JSON, Jordan, TT, Nick, Kobra Kim), Hampton, all the attaches, and the villages (Shout out to Nina+the Biohacking

THANK YOU!

Village) for working with us to bring hackers to the world of public policy."

PRESS

A big thank you to this year's press team, Jeff Weaver, Kayla Perkins, Derek Welski and Uli Ries for helping to keep the spirit of the con intact while sharing some of the incredible work the community is doing to make the digital world a safer and more equitable place."

QM

From the Desk of Major Malfunction

Quartermaster, Supreme Allied Shenanigans Division (Retired)

To the incredible team at QM Stores—

Let me tell you, folks, nobody runs a supply unit like you. People are talking about it. I've seen a lot of stores—some good, some frankly not so good—but this team? Legendary. The best. Maybe in history. And believe me, I know stores.

Now let's name names—because you deserve it:

Buttersnatcher, total powerhouse. ETA, runs smoother than a stealth op. Seven, I don't know what happened to the first six, but this one? Terrific. shell-e—unbelievable shell game, very sneaky. Sparkles, brings the razzle-dazzle and the rations. alizarinMegalodon, sounds dangerous, love that. helium, always lifting morale. Very uplifting guy.

sp1kedshell, tough on the outside, tougher on logistics. YoungBlood, brings energy—like a Red Bull in boots. Muffin, sweet operator, soft center, steel resolve. Q—mysterious, efficient, possibly a time traveler. NSTY K, not sure what the K stands for, but it's probably "Kicks ass." Drimacus, sounds ancient, delivers like Amazon. v0rt3chs, high-tech, next-level. SP3ZN45, I don't know what it means, but it's elite. r3dfish, swimming upstream against chaos—and winning. Sisu, grit in motion, ice in her veins.

Together, you've made QM Stores the envy of every other unit. The gear is fast. The service? Faster. The memes? Devastating. People say, "Major, how does QM do it?" And I say, "It's the team. The best team."

So from the bottom of my camo-clad heart—thank you. You're doing incredible things. Historic things. And remember:

Never go full malfunction—unless you're winning.

Major Malfunction

Keeping the chaos supplied since Day One (well... Day Five anyway). Bigly.

REGISTRATION

cstone, Undertaker, and Crackerjack from Registration would like to thank the awesome Reg team: 0x90ebfe, APT, avaseaa, chimera, Chunk, funnyguy, Holmestrix, ind1go, Jup1t3r, neFe2Cephalopod, phear, pozer, Premio, Prophet, qumqats, Temtel, wra1th, and zevlag. Special thanks to Janet, eta, Nikita, s3cret, SOC, and QM. Much love to all the attendees out there — thanks for your patience!"

SOC

Cj, Adazebra, deelo, tacitus, and dr.kaos wish to thank Bird, jimi2x, motsu, Flerper, JBone, Hendo, 7thdrxn, ZULU, ZettaQuark, WhiteB0rd, wasted, echosixx, MIM, Ast0r, DONKEY™, Andi, MAJ Faz, ghostinoblivion, stan, lrose, Toonz, P34RL, spedione, randy_waterhouse, Binarywishes, sienna , Cricket, @ladysnark, ac0rn, Obscured, Hattori Hanzō, PrincessKitty, oyster, HardMode, stealth, moniac, digunix, whiskey, W.I.P., RadioActive, crazian, NextInLine, BeaMeR, d101, k0414, KL4R10N, ori, Sami, WraitH, k0rg, RDF, BadAask, 4UR0R4, nohackme, GI Jack, Junior, our lady of chaos, sm0k3y, BIOM, WHITE CHRIS, Lucky, D-Kat, MrHouse, goldfish_brain, L4bF0x, BoBeR, Milkyline, Oselot, Kainu, wilnix, Psychofox, Hiero, dfirdeferred, Gladiator, zak, derp, Squ33ks, g00nd@lf, HexWeaver, Zopat, 4chtung, Giggles, Strider, Heylel, Indisposed, 0r3g0n-V1x3n, explorash, Yaga, Mouse, L4W57, Muppet, Zerorez, PacketWalker, Mr. M, DrGecko, RoadHouse, Bisdak, blancohak, RaptorSqueak, AlphaKilo, p1nk, MrZeebs, gunwale, hŭman, rand0h, lgelkott, PlainSimpleAlex, GoonPool, zerofux, Stellar_Drift, Havoc, Krassi, HoneyBadger, duckie, Wreaktifier, geekspeed, Red, Las0mbr5, do2er, CarpeDiemT3ch, runcraftcode, Kexel, Survivatrix, pr0ph37, Stoner, brbr, reducto, polish_dave, LJ, ZephrFish, boar.rito, vgm8, nerves, Drfed , Redoubt, Phat Hobbit, TheJennyDix, Hammer, AgentFritz, Candyman, SynMac, magpie, n1cFury, Mrs Skelli, FarmTruck, H311oWor1d, Thirsty Goat, N3x7, Lampy, Brisket, prec0re, EternalNoon, VegasKing, NG11Z, Reese, Intrepd, grimlock, LanShark, h2o, Buggabear619, Judo, nesquik, eaglei, G0Th3R, Arc, profXOR, Mushu, McL0v1n, Truth, delta, QuietMike, timball, Sl3dge, commandergirl, Glasswalk3r, SystM_Ov3rL04d, John Doll, duckfez, Sif, Danimal-Awesome, B00Ms1ang, MikaaAndretti, NoonSledge, Si, Ka0sKl0wN, CUG, jives,arcon, and all retired SOC Goons. Pax Per Imperium."

SPEAKER OPS

pwcrack and Heidi would like to thank the Speaker Operations team for another year of great service to DEF CON and its speakers. These goons are 4bits, Bobby the Phish, Crash, dROM, EIR0man0va, Flattire, g8, gdead, Goekesmi, HedyMercury, Imposter, Jinx, Jur1st, Jutral, K-hole, kampf, MaltLiquor, manchmod, Milhouse, Pardus, phliKtid, Ringer, RoundRiver, Shadow, SIGAD, stikk, SurrealKill3r, Tinkers, TruBluFan, Vaedron and, as always, AMFYOYO!

Training

First, we want to thank Will for his years of service in getting DEF CON Training to where it is today. Seeyew would like to thank Analiese for being an exceptional deputy and making DEF CON Training happen this year. Shoutouts to Dan Brady for reviewing training submissions, Mar for updating the website and giving us new art work, and Ron for managing logistics. We appreciate all the help from Janet, Nikita, PwCrack, Grifter, and Kevin (and his "department" KEVOPS). Special shoutout to Eta who was a valuable thought partner and all around great friend. Finally, this is only possible due to all of our incredible Goons who are staying past the show to help out!"

VENDORS

Fivepenny and Kiwi want to give a tremendous thank you to the incredible Goons who kept the Vendor side of DC33 running. This doesn't happen without all of you showing up, checking in, solving weird problems, and stepping up wherever you were needed.

meepmeep, Zarvis, BACE16, Beans, hallpass, w00zles, Joe S, Jvrgon, Darth, nixith, Professor Roger, PugLady, Darthmrvader, Chika, Aguy, Squeezebox, and Mz. Brooklynn - we saw the work you put in, and we're so grateful for it.

Huge thanks to Janet for always having our backs and helping us navigate the chaos. And an extra shoutout to DT, Nikita, and the rest of the DEF CON staff - thank you for making all of this possible.

To our vendors: thank you for your trust, your patience, and for showing up year after year with the things that bring color, curiosity, and character to the con. We couldn't ask for a better set of folks to work with. Long live KEVOPS (maybe a real dept.).

VILLAGES

Hony and Paydreaux would like to express their gratitude to Raze for his exceptional coordination and management of the creator stages. A special mention goes to br00zer for his outstanding Goon Wrangling. We also want to acknowledge the invaluable support of F4ux, Griff and Zachadakka as seconds, as well as the tireless efforts of Nikita, Janet, and Dark Tangent in making DEF CON a reality each year. A heartfelt thank you to Hunny for her instrumental role in handling the administrative tasks and for her unwavering support. They would also like to thank Ch3f and f0rk3d for stepping up to the plate to support the communities. Your contributions are truly appreciated.

The entire village team wants to extend their heartfelt thanks to all the Village leads and organizers. Your dedication and hard work in bringing great villages and content to DEF CON are what make this event a huge success. Your year-round commitment to delivering exceptional content truly sets DEF CON apart from any other conference. A special mention to Kevin and PolySauce for their roles in support of various villages, which have been instrumental in enabling their content.

Thanks to all the Village Goons! Thanks to our families and friends for supporting us while we make our way through the madness.

Thank you for all your time, help, and hard work! Villages would not be possible without it.

"Have ya paid your dues, Jack?" "Yessir, the check is in the mail.""

WORKSHOPS

Sinderz and /bin/buddha want to offer our sincerest thanks to everyone who helped make our workshop awesome! To our incredible Workshop Goons: mav, P1ll0wz, Jenn and Joel Cardella, Chrissy, fallible, RandomInterrupt, d3ada55, p0p3, henry, widdershins, Scuba Steve, and Biggs. You rock! Big shout-out to the Workshop Review Board for all their hard work and critical brains. And a massive thank you to all the instructors for bringing so much knowledge and energy to the classrooms.

Last but certainly not least, a monumental hat tip to the legends who pull off DEF CON every single year! DT, Nikita, Janet, Neil, Drew, Darrington, IHR, QM, NOC, and SOC—you're all rockstars. Seriously, thank you for all the countless hours and effort you pour into making the con happen, before, during, and after!"

DEFCON
DEFCON
DEFCON
DEFCON