
CRAB COIN
THE BAY COIN
THE EAY
SEASONING
SEAGULL COIN
RAVEN COIN
HON COIN
MARYLAND COIN
BSIDES
Charm


CACI
EVER VIGILANT


Booz
Allen


BLACK HILLS
Information Security
2008


TRIMARC


CORELLIUM


NATIONAL SECURITY AGENCY
CYBERSECURITY COLLABORATION CENTER
UNITED STATES OF AMERICA


APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY


CAPITOL
Technology University


Grafana Labs


FORETRACE


UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING
USD R&E
DEPARTMENT OF DEFENSE


trackd


tenable


LOCKHEED MARTIN


T.RowePrice


Anchor
Technologies


nDepth
SECURITY


Sparksoft


SQUADRA


Maryland
DEPARTMENT OF COMMERCE


ClearedJobs Net


SANS
GIAC
CERTIFICATIONS


no starch
press

TABLE OF CONTENTS

4 Welcome to BSidesCharm 2023

6 Code of Conduct
- Photo Policy
- Addtional Policy

7 Hiring Village

8 Workshops

12 Maps

15 Talk Schedule

16 Trainings Schedule

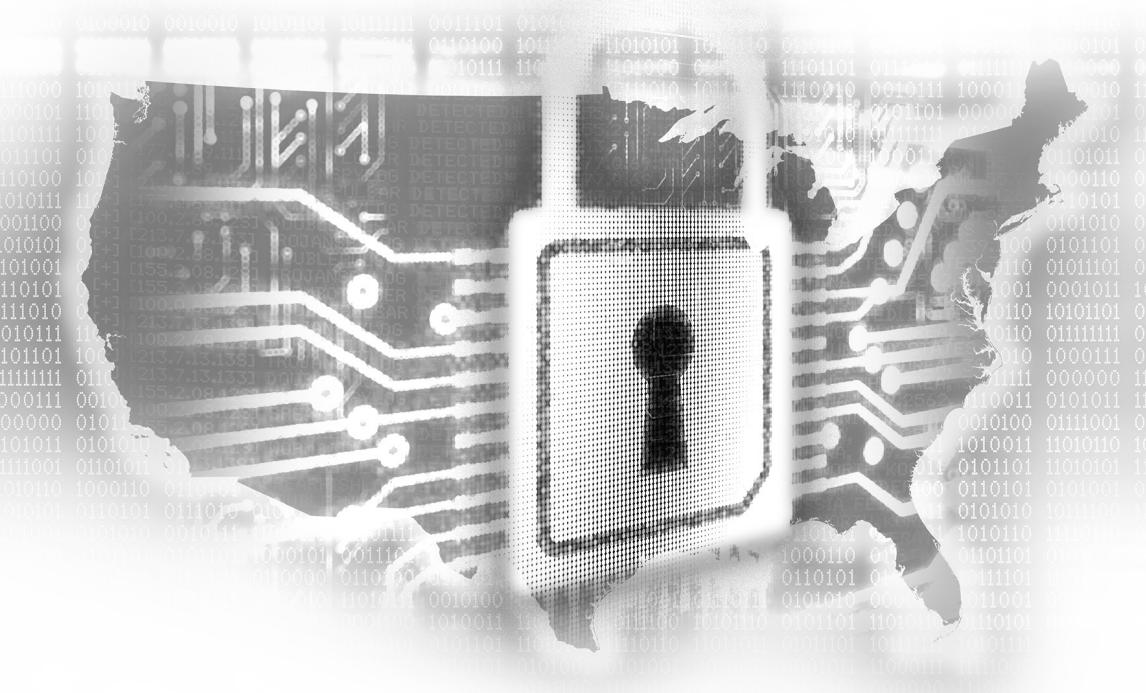
17 Keynote Presenters

19 Presentations

24 Training Events

Prepare, Defend, and Sustain the Cyber Domain

Invent your future
in Cybersecurity with CACI.



Reverse Engineering | Penetration Testing | Tools Development
Technical Targeting | ICS/SCADA | IoT and Embedded Systems

WE DO IT ALL

TOP WORK PLACES 2023 USA

Learn more at
careers.caci.com

EXPERTISE AND **TECHNOLOGY** FOR NATIONAL SECURITY

A *Fortune* World's Most Admired Company

CACI
EVER VIGILANT

www.caci.com

WELCOME TO BSIDESCHARM 2023!

Greetings and welcome to BSidesCharm 2023!

For those of you who have attended our event in the past, you will be thrilled to know that many of your favorite events, villages, and activities are returning this year. For those joining us for the first time, we extend a warm welcome and invite you to enjoy two days of enriching content from local speakers, hands-on training courses, workshops, villages, CTFs, networking with local industry professionals, and a peek into various cyber career opportunities.

Our Hiring Village is back again this year, offering unlimited opportunities for you to discuss your career growth, fine-tune your resume, and help you pursue your professional passions. They will be available on Saturday, during the day, in the Warfields Ballroom between Registration and the hotel lobby.

We are excited to welcome back many of our returning villages, and we are equally thrilled to present new ones, where you can learn new skills, explore new topics, and discover more of the natural talent found in our region. In addition to the Lockpick Village and the Radio Frequency CTF, which offer new challenges and learning experiences, we are also introducing the Battle of The Bots (BOTBs) a reverse engineering and capability development competition where the competitor is tasked to reverse engineer custom services to identify and exploit vulnerabilities in said services. To help you manage the unique mental stresses that we all face in our fields, the Health and Wellness Village will be present throughout the weekend.

Join us on Saturday afternoon for our BSidesCharm Happy Hour, immediately following the last talk of the day. This is the perfect opportunity for you to reconnect with old friends and make new ones over light snacks and beverages. Stick around after the Happy Hour for our Party on Saturday evening, which begins at 8 PM and offers a relaxing evening of video games.

We want to express our heartfelt gratitude to all the Organizers and Volunteers who have worked tirelessly for years to make this weekend possible. We extend our gratitude to our incredible speakers and trainers who are giving their time and knowledge generously this weekend. We thank all our Sponsors for their unwavering support, and our families, who have helped us navigate the challenges involved in putting on BSidesCharm 2023. Finally, we extend our thanks to you, our attendees, for your patience, understanding, and presence. We have worked hard to bring this event together for you, and we hope you leave this weekend with new knowledge and lasting friendships.

NSA CYBERSECURITY
WE'RE HIRING!

At NSA, have the best of both worlds: A meaningful career and work-life balance.

We offer competitive salary and benefits and unmatched purpose: At NSA, you can protect our democracy, privacy, security, and way of life from our adversaries.

You can also travel the world, receive tuition assistance, and enjoy an abundance of leave options, including vacation time, sick leave, paid parental leave, paid time off for physical fitness, and more...

www.intelligencecareers.gov/nsa

U.S. Citizenship is required. NSA is an Equal Opportunity Employer.

Code of Conduct

Our "Code of Conduct" is "Be Excellent to Each Other".

Speakers and presenters appreciate and welcome legitimate questions and alternate points of view as that is how we all learn. Asking questions of a speaker during their talk, to get clarity or debate a point is acceptable and encouraged. However, heckling or haranguing the speaker is unacceptable behavior and will be considered harassment which could become grounds for you being asked to leave the conference.

If you are not sure, ask, or err on the side of basic decency and common courtesy. If you observe an individual engaged in behavior that would not be acceptable to have done to you, your best friend, your worst enemy, your sister, niece, daughter, brother, nephew, son, mother, father, or any human being, please ask them to stop. If you do not feel comfortable asking them yourself, please notify one of our staff that will have the following designations on their shirts: ORGANIZER or STAFF so we can respond.

If you are having an issue with a BSidesCharm participant of ANY badge type, find a radioed member of our Staff or Security Team in the red BSidesCharm T-shirts and advise them of your concerns.

Photo Policy

Planning to take pictures or videos? You need to alert everyone before you start so they can opt-out. Based on any request from anyone, you can be asked to delete a photo/video that includes that person. It is considered a common courtesy in our community to allow others to have the right not be photographed without their permission so please ask before taking pictures (everyone in the frame).

Additional Policies

NO SMOKING:
The Sheraton Baltimore North (and Baltimore County, MD) has a strict No Smoking policy within the building. This includes e-cigarettes, vapes, or any similar devices. Designated Smoking areas are provided in several outdoor locations around the property. ALCOHOL will be available from the Sheraton restaurant and bar and at the Saturday evening party. Alcohol is not permitted in any of the event rooms during talks, training or workshops. If you are drinking, please know your limits.

DO NOT ATTACK anything other than BSidesCharm CTF targets.

OUTSIDE FOOD & DRINK: The hotel has strict rules as to catering and bringing in outside food and drink.

HOTEL NOISE POLICY: The Sheraton has a quiet zone policy for the 3rd floor and above between 10PM and 6AM. Please be courteous and keep the noise down on those floors during those times.

BSidesCharm does not release any attendee information. Nothing to sponsors, nothing to other attendees.

Hiring Village

Hiring Village Warfields Ballroom
Saturday 12-4pm

Career Opportunities

Hiring Village offers an opportunity for BSides-Charm attendees to talk with companies about career opportunities. We have a fine assortment of small/medium/large companies from our local area that offer a mix of career opportunities. Come talk to our participating companies in a low-pressure environment and learn about what they have to offer!

Resume Review/Career Advice

Have career questions? Don't know how to break into the speciality area of your interest? Not sure what options might be a fit for you? Stop by! We will have volunteer mentors - subject matter experts in the domain that can help with career questions.

How dusty is your resume? Does it really reflect your skills, abilities and talents? What does it look like to someone reviewing you for a job? Everyone should have an up-to-date resume. Stop by and meet with volunteer resume reviewers to fine tune your resumes. You don't have to be job hunting to update your resume. Don't wait until you need it!

Hiring Village Participating Companies

National Security Agency · Cybersecurity Collaboration Center · United States of America

LOCKHEED MARTIN

SQUADRA

Sparksoft

ClearedJobs Net

APL Johns Hopkins Applied Physics Laboratory

T. Rowe Price

MENTAL HEALTH HACKERS VILLAGE.

The Mental Health Hacker's (MHH) mission is to educate tech professionals about the unique mental health risks faced by those in our field – and often by the people who we share our lives with – and provide guidance on reducing their effects and better manage the triggering causes. This will be done through numerous talks and speakers conducted within the village during the conference. There will also be fun activities, crafts, coloring, and more to help you reduce stress and take a mental break from the conference activities and attendees.

MHH also aims at providing support services to those who may be susceptible to related mental health issues such as anxiety, depression, social isolation, eating disorders, etc.

Please understand that MHH does not provide counseling or therapy services.

Their website can be found at https://www.mentalhealthhackers.org/

BATTLE OF THE BOTS

Battle of The Bots (BOTBs) is a reverse engineering and capability development competition where the competitor is tasked to reverse engineer custom services to identify and exploit vulnerabilities in said services. Once access is gained to the vulnerable systems, the competitor will plant their team's flag to score points. A twist on this king-of-the-hill style competition is that services will be rotating throughout the competition. Giving your bot the ability to "worm" through multiple services is critical for its survival!

The vulnerable services competitors are tasked to exploit will be a mix of real off-the-shelf vulnerable services (ex: Log4Shell) or custom-built services to represent widely exploited vulnerabilities within commercial software. This "CVE informed development" ensures that competitors are being tasked with realistic vulnerabilities and not fictitious "what-if" scenarios making your time investment at this competition beneficial to both blue teamers and red teamers alike.

New to reverse engineering and capability development? Vulnerable services are written in a mix of interpreted and compiled languages allowing competitors of all skill levels to engage with the competition! More on the blue team side? The BOTBs Staff will be capturing network traffic on the target environment to make available publicly after the competition.

BLACK CYBERSECURITY ASSOCIATION VILLAGE

The Black Cybersecurity Association is dedicated to increasing diversity and representation within the cybersecurity industry. Our village will provide a platform for networking and learning opportunities for individuals from underrepresented communities in cybersecurity. Join us for engaging discussions, hands-on workshops, and the chance to connect with industry leaders and peers.

LOCKPICK VILLAGE

The mission of The Open Organisation of Lockpickers (TOOOL) is to advance the general public knowledge about locks and lockpicking. By examining locks, safes and other such hardware and by publicly discussing our findings, we hope to strip away the mystery with which so many of these products are imbued.

The more that people know about lock technology, the better they are capable of understanding how and where certain weaknesses are present. This makes them well-equipped to participate in sport-picking endeavors and also helps them simply be better consumers in the marketplace, making decisions based upon sound fact and research.

Visit TOOOL and learn how to pick a lock or work on refining your current skills!

EXABEAM — CAPTURE THE FLAG

Put your security skills to the test! Challenge yourself and compete with peers in a formidable game of Exabeam CTF. Get a firsthand view into the power of Exabeam solutions and explore the power of automation and threat hunting using Exabeam behavior analytics.

You'll be presented with a series of challenges. When a challenge is solved, a "flag" is given and points awarded. Get the top score and earn bragging rights as an Exabeam CTF Champion and prizes!

All competitions include tutorials that guide users through the Exabeam solution so you can familiarize yourself before the game begins.

New to Exabeam or Capture the Flag? No problem. Fun will be had! Exabeam technical experts are on hand to offer in-game support.

Machine Learning & Data Science Village

The Data Science Village will consist of a CTFd server providing a structured way for village participants to work through a series of challenges leveraging Data Science for Defensive Cyber use cases. Data, notebooks, and/or Jupyter Notebook infrastructure will be provided (equivalent of like a SIEM) to allow participants to do real-world, data science-based "hunting." Participants will gain a familiarity in: 1) common Data Science infrastructure stacks, 2) the Python ecosystem for Data Science, and 3) ways to view Cyber Data through a Data Science lens.

We will work to have 2-3+ SMEs (bare minimum in Python) to help troubleshoot, educate, and answer questions. Participants will need their own laptops. Basic Python familiarity, pandas familiarity, and Defensive Data Familiarity will be helpful, but there will at least be a few basic challenges for all.

RADIO FREQUENCY CTF

Do you have what it takes to hack WiFi, Bluetooth, and Software Defined Radio (SDR)?

RF Hackers Sanctuary (the group formerly known as Wireless Village) is once again holding the Radio Frequency Capture the Flag (RFCTF) at BSidesCharm 2023. RFHS runs this game to teach security concepts and to give people a safe and legal way to practice attacks against new and old wireless technologies.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The RFCTF can be played with a little knowledge, a pen tester's determination, and $0 to $$$$$ worth of special equipment. Our new virtual RFCTF can be played completely remotely without needing any specialized equipment at all, just using your web browser! The key is to read the clues, determine the goal of each challenge, and have fun learning.

There will be clues everywhere and we will provide periodic updates via Discord and Twitter. Make sure you pay attention to what's happening at the RFCTF desk, #rfctf on our discord, on Twitter @rf_ctf, @rfhackers, and the interwebz, etc. If you have a question – ASK! We may or may not answer, at our discretion.

FOR THE NEW FOLKS

Our virtual RFCTF environment is played remotely over ssh or through a web browser. It may help to have additional tools installed on your local machine, but it isn't required.

Read the presentations at: https://rfhackers.com/resources
Check out the resources at: http://sdr.ninja/training-events/sdr-wctf/

HYBRID FUN

For BSidesCharm 2023 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.

RADIO FREQUENCY CTF GAME

To score you will need to submit flags which will range from decoding transmissions in the spectrum, passphrases used to gain access to wireless access points, or even files located on servers. Once you capture the flag, submit it to the scoreboard right away, if you are confident it is correct.

Flags will be worth less points the more often they are solved. Offense and defense are fully in play by the participants, the RFCTF organizers, and the Conference itself. Play nice.

TO PLAY OUR RF CTF GAME AT BSIDESCHARM 2023:

SSID: RFCTF_Contestant
Password: iluvpentoo

Getting started guide:
https://github.com/rfhs/rfhs-wiki/wiki

Helpful files (in-brief, wordlist, resources) can be found on the game web server at:

http://172.16.100.1 or
https://github.com/rfhs/wctf-files

Support tickets may be opened at https://github.com/rfhs/wctf-support/issues

TL;DR

Twitter: @rf_ctf and @rfhackers

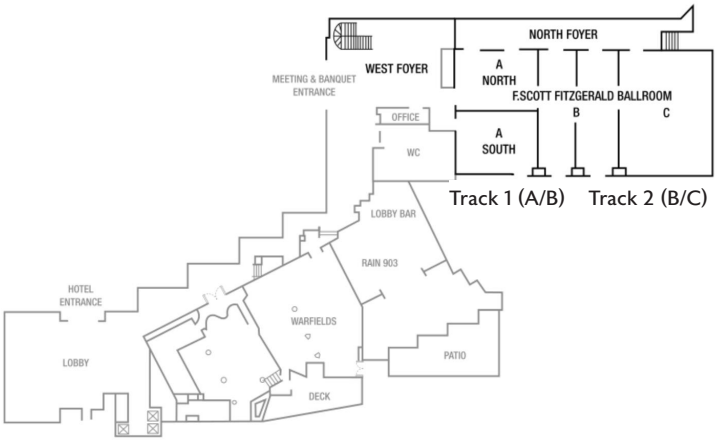
Discord: https://discordapp.com/invite/JjPQhKy

Websites: http://rfhackers.com and http://sdr.ninja

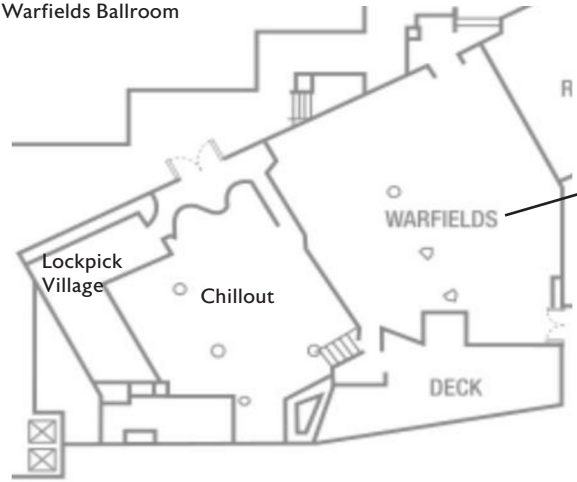
Github: https://github.com/rfhs

Official Support Ticketing System: https://github.com/rfhs/rfctf-support/issues

PLAZA LEVEL

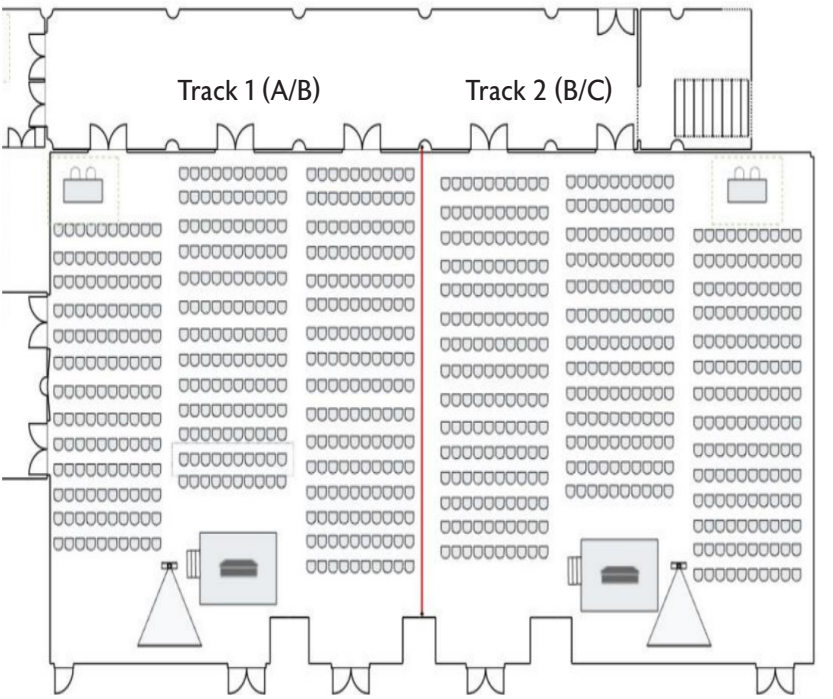


Warfields Ballroom



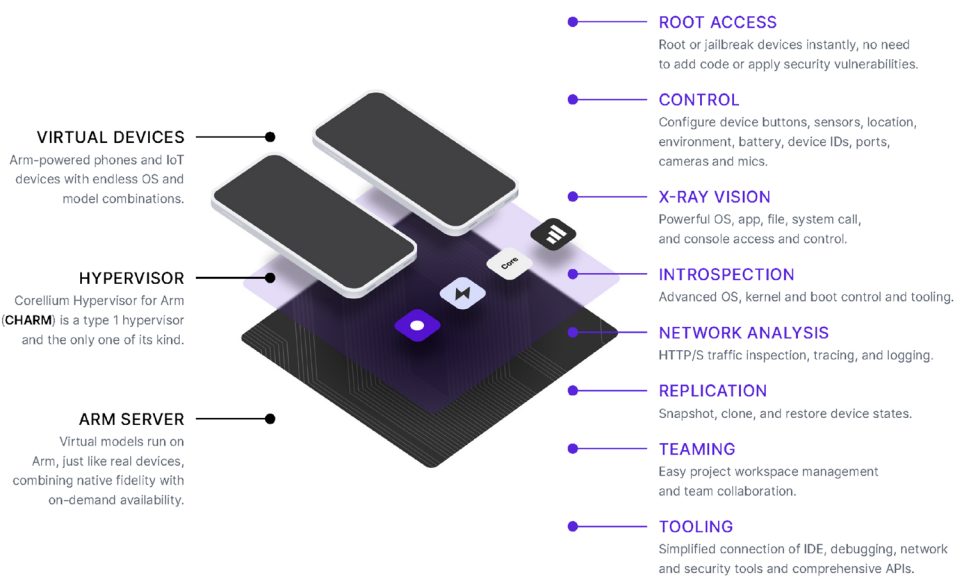
Hiring Village 12-4pm Saturday
Happy Hour 5:30-7pm Saturday
Video Game Party 8-11pm Saturday
Mobile Hacking Village Sunday

Fitzgerald Ballroom



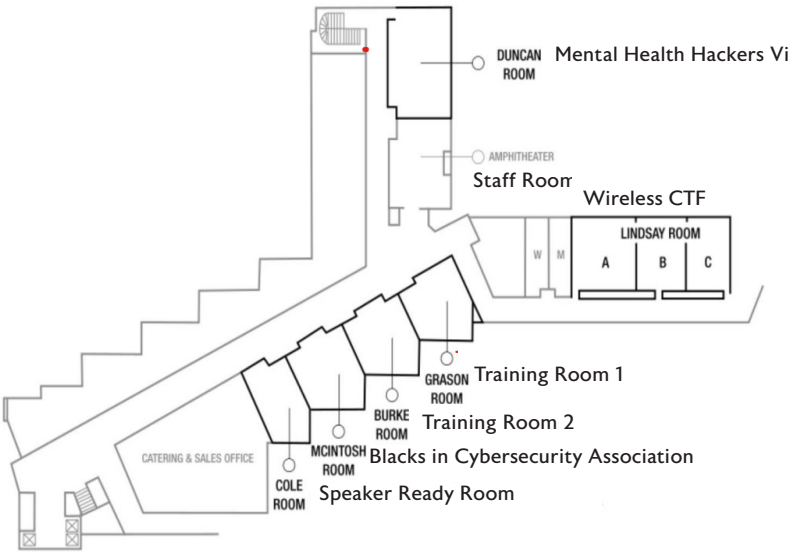
CORELLIUM

Virtual mobile Arm© based devices for research and pentesting

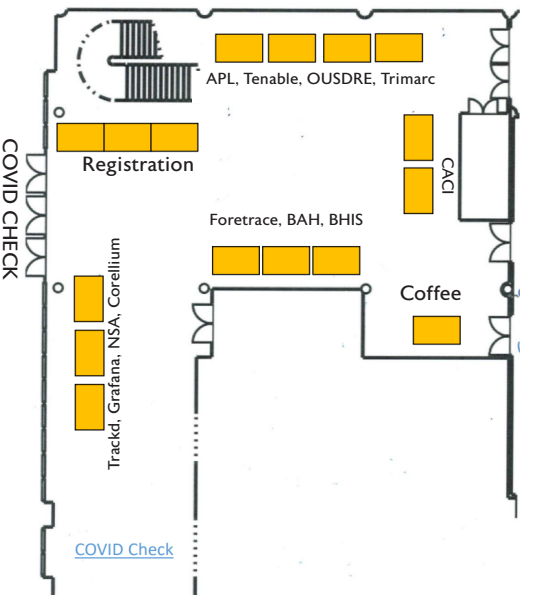


corellium.com

SECOND LEVEL



West Foyer



TALK SCHEDULE

SATURDAY

Time Slot	Track 1	Track 2
08:30 -17:0	Registration Opens	
09:50-10:00	Opening Remarks	
10:00 - 11:00	Keynote - Matthew Green	
11:00 - 11:30	Visit Our Sponsors and Villages	
11:30 - 12:00	Entering the Cybersecurity Field as a 17 Year Old - Sully Vicker	The Action Group Model for Incident Response - Shawn Thomas and Taylor Johnson
12:00 - 13:00	Baby Steps to the Future – Evolving into the Next-Gen SOC - Craig Bowser	AD and DNS: A Match Made in Heck - Jake Hildreth and Jim Sykora
13:00 - 14:00	Lunch on Your Own	
14:00 - 15:00	Make Better Risk Decisions to Prevent Future Cyber Attacks - Nathan Wenzler	Security Misconfigurations in the Cloud - "Oh Look, something fluffy!" - Kat Fitzgerald
15:00 - 15:30	Securing React Components - Tae'lur Myers Lambert	Shakespeare, Bacon, and the NSA - Brendan O'Leary
15:30 - 16:00	Hunting Mustang Panda: Exploiting PlugX DAT File Encryption with YARA - Sean Sabo	
16:00 - 17:00	Complexity for complexity's sake: The bane of cybersecurity programs - Nikki Robinson	Ten Ways to Frustrate Attackers in 2023 - Justin Palk
17:00 - 17:30	Don't Panic! A Guide to Proactive Security for Small Businesses - Ryan St. Germain and Clarissa Bury	Stop the Leak! Adversarial Thinking in Cybersecurity with PRE-ATT&CK - Nick Ascoli
17:30 - 19:00	BSidesCharm Happy Hour (Warfields Ballroom)	
20:00 - 23:00	BSidesCharm Party (Warfields Ballroom)	

SUNDAY

Time Slot	Track 1	Track 2
09:30 - 14:30	Registration Opens	
10:00 - 11:00	Keynote - Elissa Shevinsky	
11:00 - 11:30	Visit Our Sponsors and Villages	
11:30 - 12:00	Settle the Score: CVSS Fundamentals - Beth Moseng	Hack your brain: How to use IR skills to help with loss - Marc Muher
12:00 - 13:00	Detecting and Triaging Modern Windows Rootkits - Andrew Case	Blackbox Containers: Container Security in the Enterprise - Kenny Parsons
13:00 - 14:00	Lunch on Your Own	
14:00 - 15:00	Driving Your Own Vulnerability: How to Navigate the Road of BYOD Attacks - Dana Behling	Protecting Yourself From Supply Chain Attacks - Trust Is Overrated - Paul Asadoorian
15:00 - 16:00	It's all Magic(RAT) - A look into recent North Korean nation-state attacks - Asheer Malhotra	Measuring Your Zero Trust Maturity - Elizabeth Schweinsberg
16:00 -17:00	Closing Ceremony	

TRAINING SCHEDULE

SATURDAY

Time Slot	Training
08:30	Registration Opens
10:00 - 1730	Defensive PowerShell - James Honeycutt (Training Room 1)
10:00 - 17:30	Using Containers to Analyze Malware at Scale - Jose Fernandez (Training Room 2)

SUNDAY

Time Slot	Training
08:30	Registration Opens
11:30 - 15:00	Building (and Validating) Detections with Adversary Intelligence - Scott Small (Training Room 1)
11:30 - 15:00	An Introduction to Fuzzing - Sean Deaton and Ryan O'Neal (Training Room 2)

SPEAKERS

KEYNOTES

MATTHEW GREEN

Matthew D. Green, an associate professor of computer science and member of the Johns Hopkins University Information Security Institute, is a nationally recognized expert on applied cryptography and cryptographic engineering. His research includes techniques for privacy-enhanced information storage, anonymous payment systems, and bilinear map-based cryptography. He is one of the creators of the Zerocash protocol, which is used by the Zcash cryptocurrency, and a founder of an encryption startup Zeutro. He is the author of a popular blog, "A Few Thoughts on Cryptographic Engineering."

Elissa Shevinsky is a CTO known for her work in privacy, security and cryptocurrency. She is currently working with Paragon Tech as a fractional CTO. She was previously CTO and Interim CSO at Cointelegraph, a leading crypto news organization. Shevinsky has led several security and privacy startups, including roles as Head of Product at Brave and CEO at Soho Token Labs. In her free time, she explores wildlife sanctuaries and watches sci-fi reruns.

ELISSA SHEVINSKY

SATURDAY PRESENTATIONS

Entering the Cybersecurity Field as a 17 Year Old

Sully Vickers

Entering the cybersecurity field can often be frustrating and challenging. Sit it on this talk to hear about the experiences of a 17-year-old whos currently entering the cybersecurity field. What his suggestions are for others entering the field, possible changes for the field, and what companies can support future cybersecurity professionals.

Sully Vickers is a 17-year-old cybersecurity enthusiast who works as an independent contractor for MetaCTF, where he assists with privacy policy research and development and creates CTF challenges. Over the past few years, he has developed a keen interest in cybersecurity and has participated in several Capture the Flag (CTF) events, consistently ranking high in the competitions. Additionally, he has spoken with various CIOs, CISOs, and cyber executives to gain a better understanding of the field.

The Action Group Model for Incident Response

Shawn Thomas and Taylor Johnson

Ever feel like you just don't know what to do when the bad stuff happens? You can't get the support needed in the middle of an incident? Come chat about an action group model for incident response, a framework which provides coordination, ownership, and flexibility to account for the variable nature of incidents, all while encouraging development of employees at all experience levels.

Shawn Thomas
Director of Forensics and Incident Response at Yahoo

Taylor Johnson
Director of Threat Detection and Response at Yahoo.

AD and DNS: A Match Made in Heck

Jim Sykora, Jake Hildreth

Active Directory combines DNS functionality (with an LDAP database, Kerberos authentication, and some other stuff) to create a unified directory service platform. As such, the fates of AD and DNS will be forever linked. In fact, you might say they are now married. In this talk you will learn how to keep that marriage happy and healthy!

Jim Sykora is a Security Consultant at on identity security. Jim started his sysadmin path in 3rd grade & did a bunch of gigs before starting to blend operational experience & rampant curiosity with security knowledge.

Jake Hildreth is the Service Lead for the Active Directory Security Assessment (ADSA) at Trimarc & maintainer of the Locksmith AD CS remediation tool. His work at Trimarc focuses on assessing AD for F500 companies. He holds the CISSP and Security+ certs.

Make Better Risk Decisions to Prevent Future Cyber Attacks

Nathan Wenzler

Preventative security controls are more effective in reducing risk than reactive controls. This talk will explore ways to create more visibility and context into your cyber risks so you can preven

tively make better decisions about how, when and where to mitigate risks before they're exploited.

Nathan Wenzler is the Chief Security Strategist at Tenable, the Exposure Management company. Nathan has over 25 years of experience both in the trenches of and as executive management of Information Security programs for government agencies and private sector firms alike, often building them from scratch. He has served as an executive management consultant and vCISO for C-suite execs across a wide array of Fortune 1000, non-profit and government organizations looking to optimize and improve their security programs focusing on process, program and personnel improvements to mature and accelerate their Information Security and risk management efforts. Nathan's focus areas include vulnerability management, privileged access management, incident response, process and workflow improvements, executive level program management and the human-focused aspects of InfoSec.

Security Misconfigurations in the Cloud - "Oh Look, something fluffy!"

Kat Fitzgerald

Threat modeling the human security risk, or as others might call it, Security Misconfigurations in the cloud and all the fun attack vectors they create. Yep, it's clobberin time and this is what makes this job fun – helping others to find their own security problems before others do!

Based in Chicago and a natural creature of winter, you can typically find me sipping Grand Mayan Extra Anejo whilst simultaneously defending my systems using OSS, magic spells and Dancing Flamingos. Honeypots & Refrigerators are a few of my favorite things! Fun Fact: I rescue Feral Pop Tarts and have the only Pop Tart Sanctuary in the Chicago area.

Securing React Components

Tae'lur Myers Lambert

In this talk I will provide a brief overview of secure coding practices for developing web applications with ReactJS by presenting common software vulnerabilities and detailing ways to remediate and prevent insecure code being pushed to production.

I am a self-taught front-end developer and budding security enthusiast based out of Jacksonville, Florida. I am passionate about helping people break into tech from non-traditional background and love to share my love for tech through tutorials and social media.

Baby Steps to the Future – Evolving into the Next-Gen SOC

Craig Bowser

Most SOCs are unable to keep up with the attacks of today because they are constrained by a structure designed for the needs of yesterday. SOCs must evolve to become 'Next-Gen'. This talk will discuss what that means and present concrete steps organizations can take to evolve from today's rigid structures into a dynamic, agile entity that can quickly react to threats of today and tomorrow.

Craig Bowser is an Infosec professional with over 20 years of experience in the field. After ten years in the Air Force, he has worked as an Information Security Manager, Security Engineer, Security Analyst and Information System Security Officer for various government contractors. Currently he is a Senior Security Architect at GuidePoint Security. He has spoken at Black Hat, DerbyCon, BSides, and multiple SANS Summits. He holds the CISSP and multiple SANS GIAC certifications.

Hunting Mustang Panda: Exploiting PlugX DAT File Encryption with YARA

Sean Sabo

YARA rules are an industry standard for identifying malware, but what about when the malware is encrypted with a custom encryption algorithm using mixed boolean-arithmetic? Understanding custom encryption algorithms enables analysts to craft YARA rules to target them. This talk walks through understanding Mustang Panda's custom encryption scheme for hiding PlugX and how to target it using YARA.

Sean is a cyber security professional with over 10 years of experience. For the last 5 years, he has been reverse-engineering malware and tracking various APT groups. He enjoys writing YARA rules and has contributed to the YARA code base. He currently works as a Senior Cyber Security Researcher at Recorded Future. Prior to that, he was at ThreatConnect and on the ASERT team at Arbor Networks.

Shakespeare, Bacon, and the NSA

Brendan O'Leary

A code-breaking Quaker poet who hunted Nazi spies? Truth is stranger than fiction, and the life of Elizebeth Smith Friedman is no exception. She broke codes during both World Wars and is credited as a founder of modern cryptology.

In this talk, we'll follow Elizebeth's journey, learn the history of cryptography, and apply those lessons to how we should view technology and technologists today.

Brendan O'Leary is Head of Community at Project Discovery, and spends his time connecting with developers, security engineers, contributing to open source projects, and sharing his thoughts on cutting-edge technologies on conference panels, meetups, in contributed articles and on blogs.

Complexity for complexity's sake: The bane of cybersecurity programs

Nikki Robinson

More tools! More frameworks! More security controls! Let's add all the things and stack them on top of each other! Nope, nope, and nope. This has been ineffective against major attacks like Solarwinds and Log4j. We need to keep security simple, not just for our security teams who are managing a menagerie of security tools, vulnerabilities, and threats, but also for our users.

Dr. Nikki Robinson is a Security Architect with IBM, as well as an Adjunct Professor with Capitol Technology University. She holds a DSc in Cybersecurity and a PhD in Human Factors, specializing research in vulnerability chaining. She is the co-host of the Resilient Cyber Podcast, holds several industry certifications and is also a Fellow with ICIT. With a background in IT operations, she focuses on solving large-scale cybersecurity problems in vulnerability management, and risk analysis.

Ten Ways to Frustrate Attackers in 2023 -

Justin Palk

Some misconfigurations and security oversights are so egregious they can allow attackers to compromise a network in hours or minutes, while some controls or architecture decisions just make attackers' lives miserable. I'll provide an attacker's view of what makes a network easy or hard for us to attack, including showing some tools you can use to ID these issues yourself before getting a pentest.

But in practice, Microsoft's "easy" approach to PKI often creates security issues in typical deployments. Luckily, you can eliminate the most common & most dangerous misconfigurations with a few easy checks.

Justin Palk has more than 16 years of experience in IT and information security, working in the academic, federal civilian government and health research sectors. He has held a variety of roles including sysadmin, developer, auditor, assessment team lead and now pentester. In the middle of his technical career Justin took a seven-year detour into state and local journalism. He regularly competes in CTFs. When not hacking or developing tools, Justin plays TTRPGs, writes cosmic horror, and brews.

Don't Panic! A Guide to Proactive Security for Small Businesses

Ryan St. Germain and Clarissa Bury

This talk will explore the importance of proactive cybersecurity measures for small and medium sized businesses and provide practical strategies and resources. Topics covered will include playbook development, tabletop exercises, threat intelligence, and open-source or low-cost resources.

Ryan St. Germain and Clarissa Bury work together on CrowdStrike's Strategic Advisory Services team where they create bespoke tabletop exercises and perform cybersecurity maturity assessments. Prior to becoming consultants, Ryan was the Manager of Security and Infrastructure and Clarissa was the Security Engineer for a small software and services company in the DC area.

Stop the Leak! Adversarial Thinking in Cybersecurity with PRE-ATT&CK

Nick Ascoli

File and data leakage have been responsible for some of the largest press-worthy cyber security incidents to date, and in recently, appear to be increasing in volume. This talk will propose a more authentic approach to adversarial thinking (informed by MITRE PRE-ATT&CK) designed to inform defensive priorities using the same exact techniques that adversaries are actually employing in the wild.

Nick Ascoli is a cybersecurity researcher and the founder and CEO of Foretrace, an External Attack Surface Management (EASM) solution. Nick has been a guest on the Cyber Wire podcast, and a speaker at GrrCON, Shmoocon, Defcon Skytalks, Blackhat Arsenal, SANS, and B-Sides conferences on SIEM, Recon, and UEBA topics

Settle the Score: CVSS Fundamentals - Beth Moseng

How do we, as an intelligence community, understand and distribute the severity of widespread vulnerabilities? On that note, how do we even categorize them? After years of developing a need for a widespread and company ambiguous importance monitoring system, CVE and CVSS was born. Knowing how exactly how to understand and use these systems is fundamental for defending and exploiting.

Hack Your Brain: Using IR skills to help recover from grief

Marc Muher

Incident responders use some variation of the PICERL framework (Preparation, Isolation, Containment, Eradication, Recovery, and Lessons Learned) when handling a problem. When the mind is dealing with grief, it uses a similar response pattern of Denial, Anger, Bargaining, Depression, and Acceptance. Identifying where you in these stages may help you deal with loss.
Marc Muher

I have Master's degrees in both Social Work and Cybersecurity.
CISSP.
Gifted in making spreadsheets about meetings
Talented at making meetings about spreadsheets
10 time Polar Bear Plunger.

Detecting and Triaging Modern Windows Rootkits

Andrew Case

Since Windows 10, Microsoft has added many new security features aimed at disrupting kernel level malware. To stay viable, rootkit developers have evolved how they load into the kernel, gain system control, and monitor activity. This talk walks through such techniques observed in the wild and how they are detectable through a combination of memory forensics and event log analysis.

Andrew Case is the Director of Research at Volexity, and has significant experience in incident response handling and malware analysis. He has conducted numerous large-scale investigations that span enterprises and industries. Case is a core developer of the Volatility memory analysis framework, and a co-author of the highly popular and technical forensics analysis book "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory."

Blackbox Containers: Container Security in the Enterprise

Kenny Parsons

Containers are essential in modern software development, but they come with security considerations. This talk will cover container foundations, operational impact, and security considerations throughout their lifecycle. Best practices for securing containerized apps will also be discussed.

Kenny Parsons is a Security Consultant for Set Solutions with over 15 years of experience in IT and Security. His passion for security started with an early interest in hacking and social engineering. Now, Kenny advises clients on complex environments, helping them to secure their infrastructure and microservice/container architectures. He provides clients with proper design, build, and runtime best practices for a rapidly changing container and cloud-first world.

Kenny's expertise has been recognized by industry leaders, and he was recently a guest speaker at DEFCON DC940 in DFW, Texas, and on the "Ready. Set. Secure." podcast.

Driving Your Own Vulnerability: How to Navigate the Road of BYOD Attacks

Dana Behling

Preventing attacks that use Bring Your Own Vulnerable Drivers pose a unique threat to Windows security, but what makes a driver vulnerable, and how prevalent are vulnerable device drivers? In addition to answering these questions, this talk provides categories of vulnerabilities that are unique to Windows drivers and provides real world case studies to illustrate the theoretical concepts.

Dana Behling is a senior threat researcher at VMware Carbon Black. With a background in software development and reverse engineering, she has spent decades dissecting and explaining malware to facilitate practical security outcomes.

Her work has been instrumental in safeguarding the systems of some of the world's largest corporations and government agencies. In her free time, Dana indulges in science fiction and fantasy audio books and gardening.

Protecting Yourself From Supply Chain Attacks - Trust Is Overrated

Paul Asadoorian

How can you trust all of the hardware and software you use on a daily basis? Hardware, firmware, and software have a unique (often complex) supply chain. I believe we extend far too much trust to the supply chain and do not verify the integrity of our hardware and software components. Using open-source and free tools learn how to enumerate and validate the integrity of your devices in this talk!

Paul Asadoorian is currently the Principal Security Evangelist for Eclypsium, focused on firmware and supply chain security awareness. Paul's passion for firmware security extends back many years to the WRT54G hacking days and reverse engineering firmware on IoT devices for fun.

Paul is the host of one of the longest-running security podcasts, Paul's Security Weekly, and enjoys coding in Python, telling everyone he uses Linux as his daily driver, poking at the supply chain, & reading about UEFI.

It's all Magic(RAT) - A look into recent North Korean nation-state attacks

Asheer Malhotra

This presentation will illustrate the entire cyber-kill chain, hands-on-keyboard activity and corresponding MITRE ATT&CK mappings for a series of successful intrusions carried out by the North Korean APT group "Lazarus" against energy companies across the world. We also provide an analysis of MagicRAT and associated, bespoke malware families used by the APT group.

Asheer Malhotra is a threat researcher specializing in malware analysis, reversing, detection technologies and threat disclosures within Cisco Talos. He has been researching malware threats for about a decade now at FireEye, Intel, McAfee and now at Talos.

His key focus is tracking nation state attacks (APTs) across the world. Asheer holds an M.S in Computer Science with a focus on Cyber Security.

Measuring Your Zero Trust Maturity

Elizabeth Schweinsberg

Zero Trust is all the rage in security these days. Where do you begin when trying to move towards a more mature zero trust architecture for your organization? Using the CISA Zero Trust Maturity Model, the Zero Trust team at Centers for Medicare and Medicaid Services customized a framework for our environments to better track progress across various axes. We want to share how we did this with you.the groups over the course of the past two years. The presentation will start by showing the initial patterns and themes of malicious documents and lures used by the groups in 2020. The presentation will finish with an evolutionary analysis of Transparent Tribe and SideCopy's tactics resulting in the deployment of their Windows malware implants

Elizabeth Schweinsberg is a Digital Services Expert with the US Digital Service after 9 years in corporate threat detection and incident response with Facebook and Google. She works to keep the internal networks safe from malware, hackers, and the Internet. Ms. Schweinsberg has been in the computer industry for over a decade and in digital forensics since 2005 in both the Government and private sector.

When not behind the computer, she can often be found behind a book or sewing machine.

POWERSHELL CRASH COURSE

This Defensive PowerShell workshop is an immersive, hands-on learning experience. You will use PowerShell Remoting (PowerShell v7) to parse text base and Windows Event logs. You will also query both local and remote registries. You will learn about an additional Windows firewall log and enable and create a custom object.

Defensive PowerShell is a follow-on workshop from my PowerShell Crash Course. Unlike my PowerShell Crash Course, this workshop is primarily hands-on. We start with a presentation to discuss what you will do in the lab/walkthrough. We will disable PowerShell v2, enabling some additional PowerShell and Firewall logs. By default, you remote into PowerShell v5; you will enable PowerShell v7 remoting and use it to query and modify a remote registry. We will also use PowerShell v7 remoting to query both Windows texts based and evtx based logs. You will convert the text-based logs into a custom object. You will use PowerShell techniques to analyze the custom object. You will spend a lot of time learning different techniques to parse the Windows event logs.

PREREQUISITES

The course will require a virtualized Windows 10 on your host machine. It is recommended that your host machine be a Windows machine. If you show up with a Mac or Linux, we will set up PowerShell Remoting over SSH instead of PowerShell v7 Remoting. That will be the only difference; everything else will be the same.

Trainer: James Honeycutt (@P0w3rChi3f)

Mr. Honeycutt has served in the military for 26 years. He has spent most of that time working in IT Operations in various positions, from helpdesk to a Microsoft Windows systems administrator. He currently works for the Maryland National Guard Cyber Protection Team (CPT) as a Cyber Operations Technician focusing on incident response, forensics, and being the resident "Windows Expert." He likes to give back to the community by presenting at local events

USING CONTAINERS TO ANALYZE MALWARE AT SCALE

This workshop will focus on teaching participants how to handle malware and analyze samples using both Windows and Linux containers. The workshop will focus leveraging open-source tools, and techniques to build out a simple analysis queue pipeline to allow students to analyze multiple samples at scale within a controlled environment.

The workshop will give students experience in creating repeatable workflows to not only perform malware analysis, but also how to leverage automation for svimilar tasks using boilerplate workflows.

PREREQUISITES

Laptop with WiFi capabilities

Trainer: José Fernández (@jfersec)

José Fernándezv is the President & owner of CompSec Direct. He is an InfoSec researcher with over 20 years of experience in the IT field. Jose specializes in InfoSec research by applying offensive methodologies towards practical defensive measures. Jose's background in CNO, CND & engineering has allowed him to work in some of the most technically demanding environments throughout his career in both private & public sector. Mr. Fernandez is a Veteran & a Puertorrican Hacker Dude.

BUILDING (AND VALIDATING) DETECTIONS WITH ADVERSARY INTELLIGENCE

We will demonstrate workflows & use publicly available tools to gather & process intelligence on key current threats (top infostealers), identify potential TTP detection gaps, and close those gaps with new detections & validation tests. We'll also show how teams can be more proactive by considering defenses for technique implementations beyond just those reported in public intelligence.

The term "threat-informed defense" has gained recent popularity, but what does it actually look like in practice? This session will provide highly practical tips & guidance for members of virtually any security team – regardless of size or maturity level – to help kickstart (or advance) their threat-informed journey.Relying entirely on publicly available resources, we will jump into the weeds of workflows used to gather & process intelligence on key current threats (in this example, top recently-active infostealer malware), identify potential TTP detection gaps, and close those gaps with new detections & security tests. We will also show how teams can take steps to be more proactive and consider defenses & tests for technique implementations beyond just the immediate ones reported in recent public intelligence. The host anticipates attendees will walk away with a renewed appreciation for a threat-informed approach to security, and inspiration for their next work sprint or side project!

PREREQUISITES

Laptops with internet connection, Sysmon, Atomic Red Team (& Invoke-Atomic Powershell framework), Chainsaw log parsing tool (Github)

Trainer: Scott Small

Scott Small is a security & intelligence practitioner and expert in cyber threat intelligence & threat modeling, open source research & investigations, and data analysis & automation. He is currently CTI Director at Tidal Cyber. Scott has advised enterprise & public sector security teams across maturity levels on technical & strategic intelligence applications and using technology to identify & mitigate risk. He actively contributes to the professional community & open source security projects.

An Introduction to Fuzzing

Fuzzing is still one of the leading methods for finding vulnerabilities in applications. And it doesn't have to be hard. This course gives both a high-level overview on the theory of fuzz testing as well as concrete practical exercises. Students will learn how to fuzz real-world applications to uncover actual software vulnerabilities in applications still shipped in 2023.

Students might not complete every exercise. And that's OK! All of the exercises are included as Docker containers on GitHub so students can always revisit missed topics.

Prerequisites

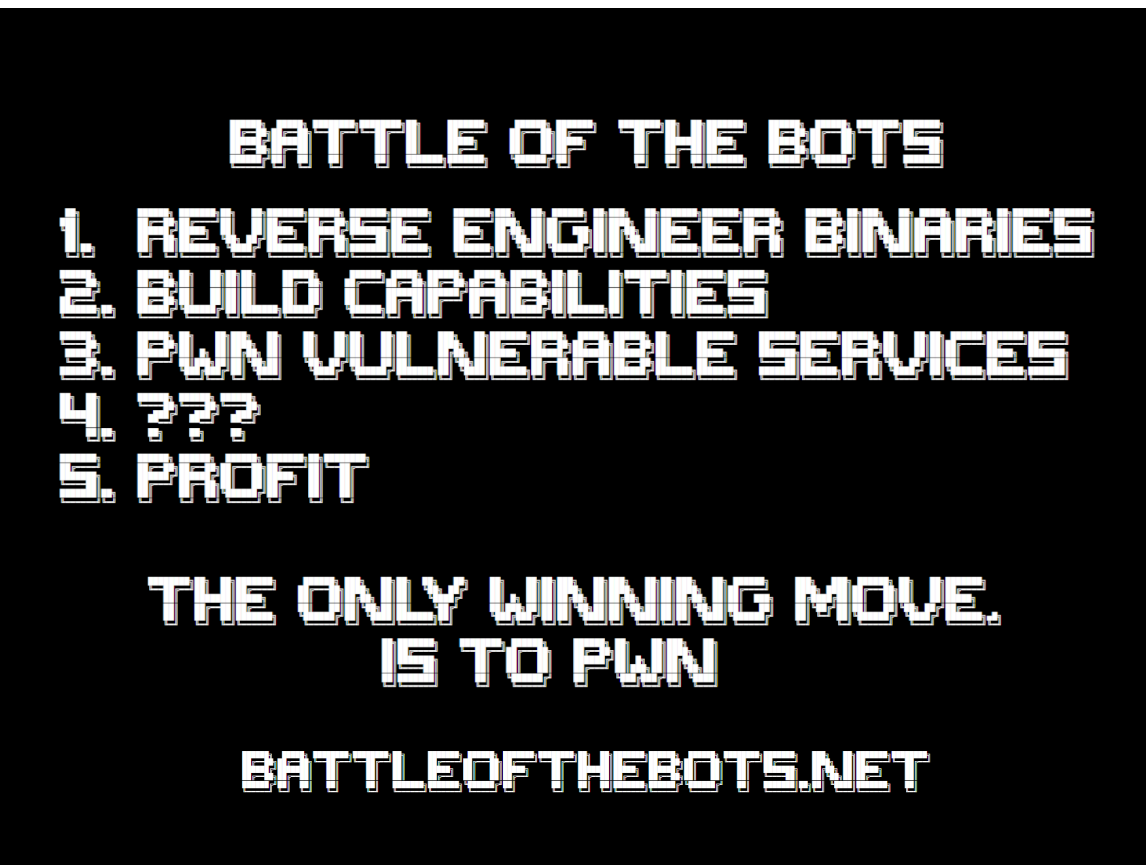
- A basic understanding of C and compilation.
- Working knowledge of git and how to clone repositories.
- An understanding of Docker is helpful, though not necessary, as all of the exercises are included as Docker containers.
- Without Docker, students are encouraged to build AFL++ on their host before the class.
- AFL++ supports macOS (Intel and Apple Silicon) and Linux. Windows users should have a Linux VM or Docker installed.

Sean Deaton (@WhatTheFuzz), Ryan O'Neal

Sean is an alumnus of the United States Military Academy (B.S. 2017) and Georgia Tech (M.S. 2021), where he studied Computer Science. After commissioning as a Cyber Officer in the U.S. Army, Sean served as a developer with the 780th MI BDE. He now works as a vulnerability researcher for Blue Star and Bogart Associates, with particular interests in fuzzing, data flow analysis, and decompilation theory.

When he's not finding bugs or working on training material, he spends his time at the dog park trying to burn off his corgi's seemingly unlimited energy.

Ryan O'Neal is a vulnerability researcher employed by the US Army. His research focuses on static analysis, symbolic execution and fuzzing, and he draws upon his experience as a web developer, cloud application developer and devops engineer to create innovative solutions. His passion is discovering and developing new techniques to address difficult questions in program security, and seeing which databases are vulnerable to SQL injection by entering his last name.



CHARITY TABLES

BLACKS IN CYBERSECURITY

The official mission of Blacks In Cybersecurity™ (BIC) is to encourage the participation of the Black community in Cybersecurity. BIC seeks to conduct a premier conference series and community emphasizing our influence and participation in Cybersecurity and STEM.

UNALLOCATED SPACE

Unallocated Space is a 501(c)(3) charitable organization in Severn, Maryland. Their mission is to foster creative and technical growth through open collaboration by providing tools and resources within the greater Baltimore-Washington Metro area. Please learn more at https://www.unallocatedspace.org.

ISSA

ISSA is the community of choice for international cybersecurity professionals dedicated to advancing individual growth, managing technology risk and protecting critical information and infrastructure. The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

For more information about the Central Maryland chapter, please visit our website at https://issa-centralmd.org.

NO STARCH DISCOUNT

Discount code **CHARM23** is open to all BSides Charm attendees for 30% off at nostarch.com from Apr 29–May 14, 2023.

The 10 ebook vouchers each contain a unique code and instructions for redemption. Vouchers can be redeemed at nostarch.com for $20 off of any ebook purchase from Apr 29–Jun 30, 2023.