Threat-Informed Challenge Development: Elevating Cybersecurity Training via CTFs

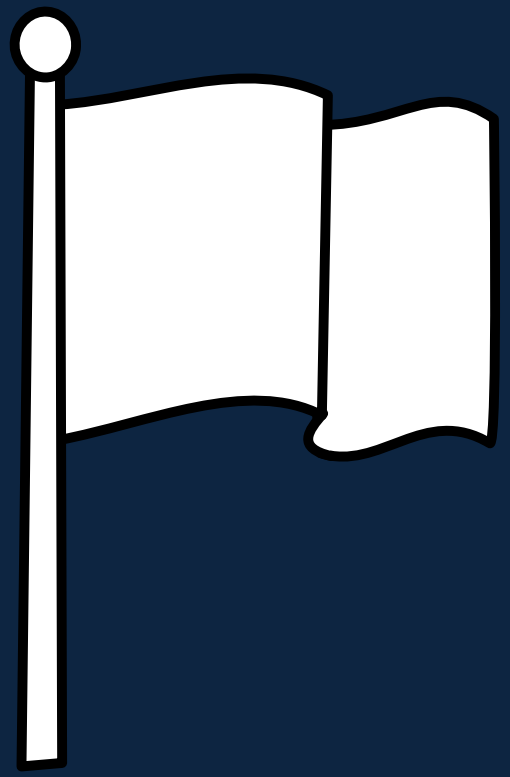
By Nicholas Reveliotis

September 9, 2023

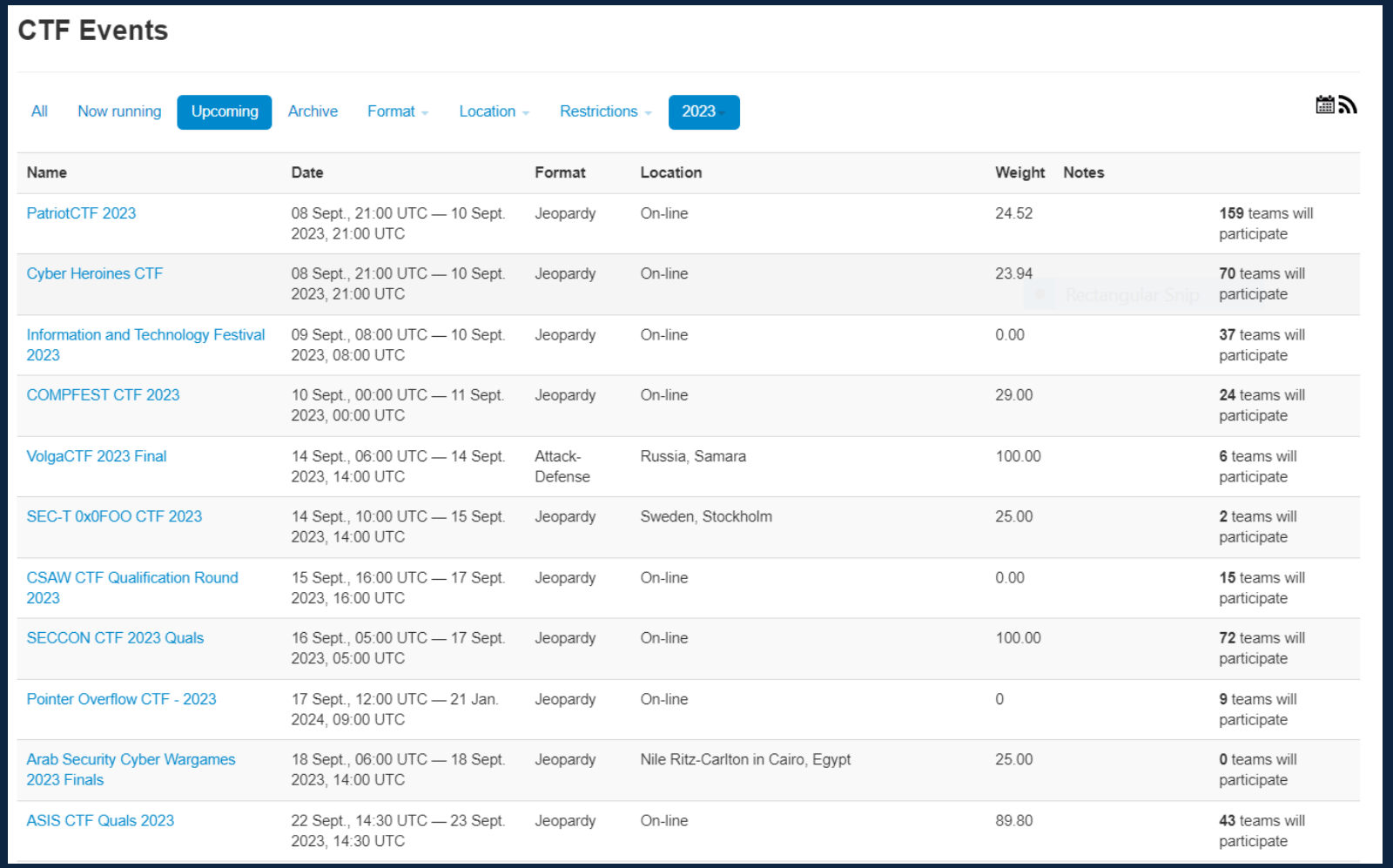
MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

CTF Competitions

- Provide opportunities to learn/practice tools & techniques
- Offer a network to collaborate/compete together
- Fun!
- But…
  - Frequently lack the realism of a **real-world environment**
  - Can be intimidating to beginners in the field
  - Many share the same jeopardy “find the flag” format



MITRE



CTF Events

All | Now running | Upcoming | Archive | Format | Location | Restrictions | 2023

Name	Date	Format	Location	Weight	Notes	
PatriotCTF 2023	08 Sept., 21:00 UTC — 10 Sept. 2023, 21:00 UTC	Jeopardy	On-line	24.52		**159** teams will participate
Cyber Heroines CTF	08 Sept., 21:00 UTC — 10 Sept. 2023, 21:00 UTC	Jeopardy	On-line	23.94		**70** teams will participate
Information and Technology Festival 2023	09 Sept., 08:00 UTC — 10 Sept. 2023, 08:00 UTC	Jeopardy	On-line	0.00		**37** teams will participate
COMPFEST CTF 2023	10 Sept., 00:00 UTC — 11 Sept. 2023, 00:00 UTC	Jeopardy	On-line	29.00		**24** teams will participate
VolgaCTF 2023 Final	14 Sept., 06:00 UTC — 14 Sept. 2023, 14:00 UTC	Attack-Defense	Russia, Samara	100.00		**6** teams will participate
SEC-T 0x0FOO CTF 2023	14 Sept., 10:00 UTC — 15 Sept. 2023, 14:00 UTC	Jeopardy	Sweden, Stockholm	25.00		**2** teams will participate
CSAW CTF Qualification Round 2023	15 Sept., 16:00 UTC — 17 Sept. 2023, 16:00 UTC	Jeopardy	On-line	0.00		**15** teams will participate
SECCON CTF 2023 Quals	16 Sept., 05:00 UTC — 17 Sept. 2023, 05:00 UTC	Jeopardy	On-line	100.00		**72** teams will participate
Pointer Overflow CTF - 2023	17 Sept., 12:00 UTC — 21 Jan. 2024, 09:00 UTC	Jeopardy	On-line	0		**9** teams will participate
Arab Security Cyber Wargames 2023 Finals	18 Sept., 06:00 UTC — 18 Sept. 2023, 14:00 UTC	Jeopardy	Nile Ritz-Carlton in Cairo, Egypt	25.00		**0** teams will participate
ASIS CTF Quals 2023	22 Sept., 14:30 UTC — 23 Sept. 2023, 14:30 UTC	Jeopardy	On-line	89.80		**43** teams will participate

Screenshot from ctftime.org 9/8/2023

MITRE

CTF Events

All | Now running | Upcoming | Archive | Format | Location | Restrictions | 2023

Name	Date	Format	Location	Weight	
PatriotCTF 2023	08 Sept., 21:00 UTC — 10 Sept. 2023, 21:00 UTC	Jeopardy	On-line	24.52	
Cyber Heroines CTF	08 Sept., 21:00 UTC — 10 Sept. 2023, 21:00 UTC	Jeopardy	On-line	23.94	
Information and Technology Festival 2023	09 Sept., 08:00 UTC — 10 Sept. 2023, 08:00 UTC	Jeopardy	On-line	0.00	
COMPFEST CTF 2023	10 Sept., 00:00 UTC — 11 Sept. 2023, 00:00 UTC	Jeopardy	On-line	29.00	
VolgaCTF 2023 Final	14 Sept., 06:00 UTC — 14 Sept. 2023, 14:00 UTC	Attack-Defense	Russia, Samara	100.00	
SEC-T 0x0FOO CTF 2023	14 Sept., 10:00 UTC — 15 Sept. 2023, 14:00 UTC	Jeopardy	Sweden, Stockholm	25.00	
CSAW CTF Qualification Round 2023	15 Sept., 16:00 UTC — 17 Sept. 2023, 16:00 UTC	Jeopardy	On-line	0.00	**15** teams will participate
SECCON CTF 2023 Quals	16 Sept., 05:00 UTC — 17 Sept. 2023, 05:00 UTC	Jeopardy	On-line	100.00	**72** teams will participate
Pointer Overflow CTF - 2023	17 Sept., 12:00 UTC — 21 Jan. 2024, 09:00 UTC	Jeopardy	On-line	0	**9** teams will participate
Arab Security Cyber Wargames 2023 Finals	18 Sept., 06:00 UTC — 18 Sept. 2023, 14:00 UTC	Jeopardy	Nile Ritz-Carlton in Cairo, Egypt	25.00	**0** teams will participate
ASIS CTF Quals 2023	22 Sept., 14:30 UTC — 23 Sept. 2023, 14:30 UTC	Jeopardy	On-line	89.80	**43** teams will participate

Screenshot from ctftime.org 9/8/2023

MITRE

Elevating CTF Competitions

- Major benefit of CTFs: **Gamification**
  - Keeping competitors engaged with hands-on learning
- Gamification of learning already exists in many fields
  - Software Engineering – Leetcode
  - Game Development – Game Jams
  - Foreign Language – Duolingo/Rosetta Stone
  - General – Hackathons, Kahoot
- CTFs provide gamification, but their learning potential can be improved

Threat-Informed Competitions

Ghidra Golf

Reverse-engineering focused on Ghidra script development

Battle of The Bots (PvP)

Reverse-engineering & capability development to breach vulnerable services in a king-of-the-hill format

Battle of The Bots (PvE)

Reverse-engineering & capability development to breach vulnerable services and worm/bot across enclosed networks

Ghidra Golf

- Hosted at Schmoocon 2023 in Washington, DC
- “Contestants are provided with a binary to download, reverse engineer and to test their code against, before submitting their Ghidra script for evaluation.”
- **Threat-Informed** Challenges
  - Automating commonly used reverse engineering techniques
  - Based off APT threat reports
- https://ghidra.golf

MITRE

Ghidra Golf Gamification & Training

- Individual challenges for points provide a gamified way to learn Ghidra scripting
  - Putting Green Challenges
    - Obtaining program metadata
    - Patching bytes in a binary
    - Enumerate methods of given classes
    - And more!
- Challenges **train** competitors by implementing commonly utilized reverse engineering techniques via Ghidra scripting

MITRE

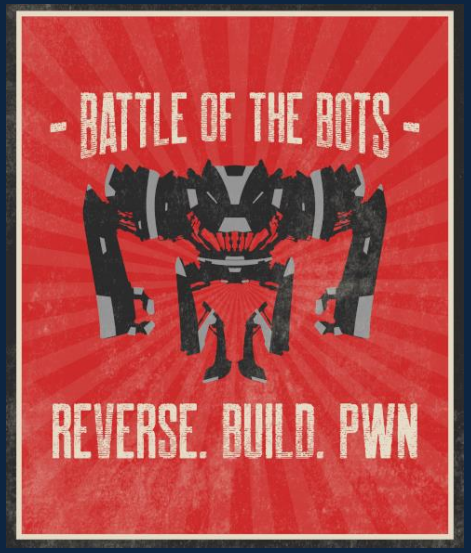
Ghidra Golf Artifacts

- Competitor-submitted Ghidra scripts with an opt-in to open-source
  - https://github.com/ghidragolf/ghidra_scripts
- Honorable Mentions
  - Pcode Emulator by mrexodia (creator of x64debug)
  - Golang Build Info Extractor by bfu
- Scripts can **assist** in future reverse engineering work

MITRE

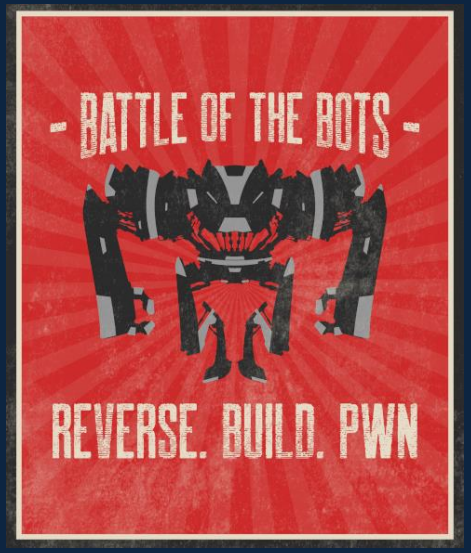
Battle of The Bots (BOTB) PvP

- Hosted at BSides Charm 2023 in Baltimore, MD
- “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.”
  - Persistence = Points
- **Threat-Informed** Challenges
  - Networks comprised of top CVEs seen in the wild
  - Post-exploitation persistence + C2
- https://www.battleofthebots.net



Battle of The Bots (BOTB) PvE

- Hosted at DEF CON 2023 in Las Vegas, NV
- “Competitor is tasked to reverse engineer custom services to identify and exploit vulnerabilities in said services. Competitors must then use the capabilities and exploits they have developed to gain access and pivot through branching networks that comprise a map.”
- 3 Maps (Networks)
  - Mainframe Madness – Text-based protocols & older vulnerabilities
  - CVE City – Comprised of commonly exploited CVEs
  - Spacepunk – Binary exploitation & reverse engineering
- https://www.battleofthebots.net



MITRE

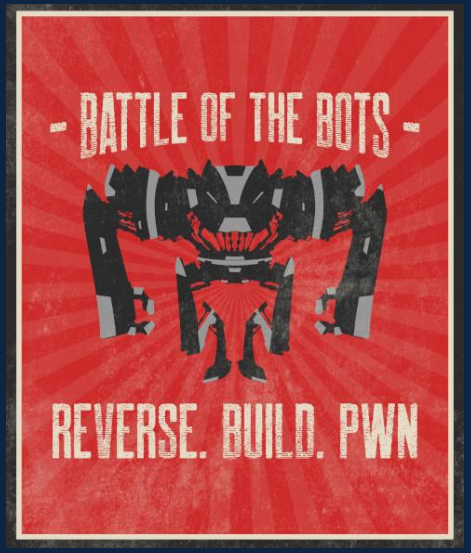
Battle of The Bots (BOTB) PvE+PvP Gamification & Training

- Gamification by earning points through
  - Popping boxes
  - Static challenges
  - Maintaining persistence (PvE)
- PvE **trained** competitors on maintaining persistence against other adversaries
  - Automating repeated attacks if foothold is lost
- PvP **trained** competitors on worm/bot development and network propagation
  - Combining software engineering and cybersecurity
- PvE & PvP **trained** competitors on capability development

MITRE

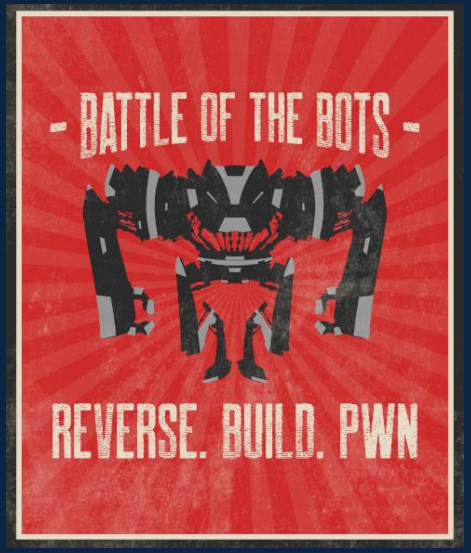
Battle of The Bots PvP Artifacts

- Network traffic was captured throughout the competition
- Evidence of
  - Network based exploits
  - Unauthorized authentications
  - Command and control (C2) to/from red-team machines (bind/reverse shells)
- Can be used for training in **incident response and forensics**



Battle of The Bots PvE Artifacts

- Competitor-submitted worms/bots
  - Created in various languages including Python, Golang, and Bash
  - Demonstrated
    - Packaging and running exploits
    - Self-propagation
    - Network reconnaissance and enumeration
- Can be used for training in **reverse engineering**
- Also relevant for adversary emulation



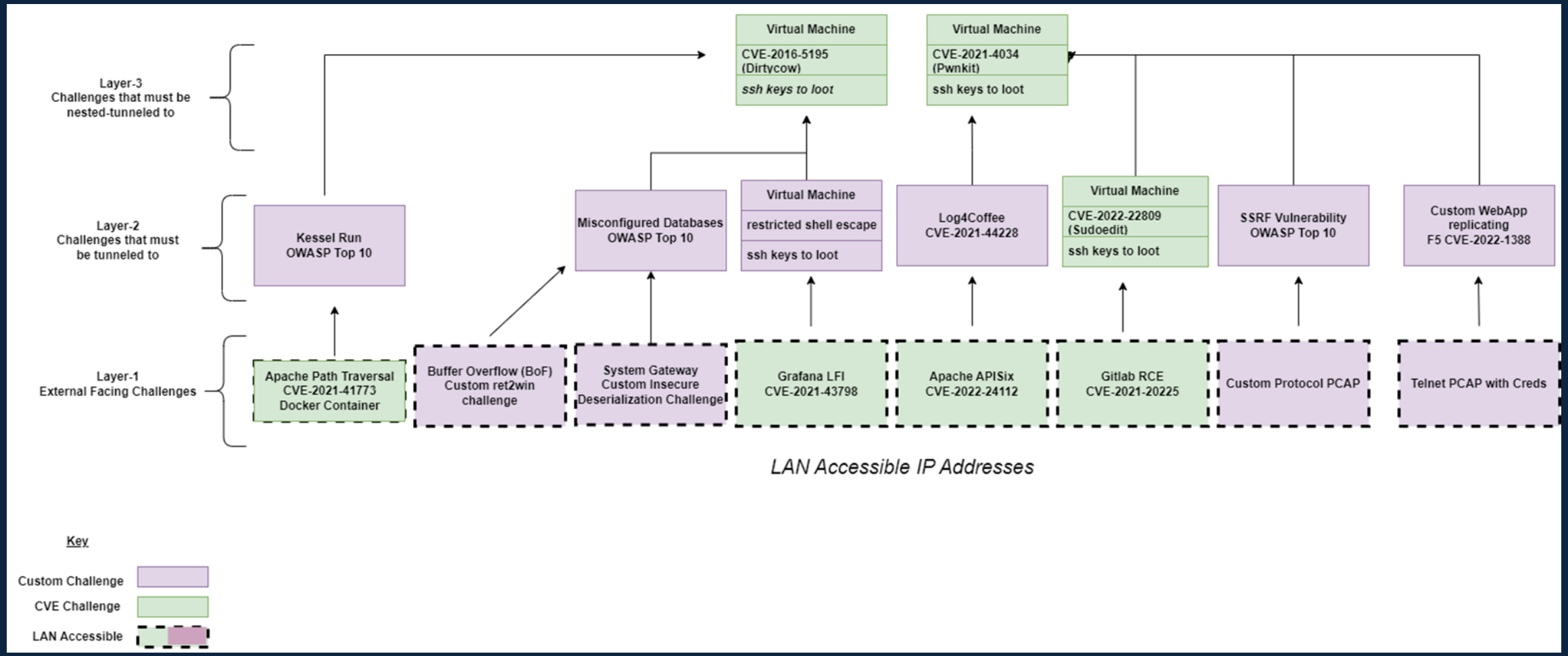
How Threat-Informed Competitions Are Built

Creating Realistic & Dynamic Networks (BOTB)

- Multiple machines, numerous networks, several services, and various vulnerabilities
- Docker - Separating deployments per challenge
  - Enables virtual networks
  - Incredibly performant
  - Provide isolation to host machine from rogue competitors
    - More info on this (and on the infrastructure for Ghidra Golf) here: Golfing With Dragons – Presented at Carneige Mellon SEI DevSecOpsDays 2023 (w/ Video)
  - Simplify tracking challenge status (CPU/memory usage & healthchecks)
- Provides **realism** by requiring competitors to pivot and advance across a realistic environment

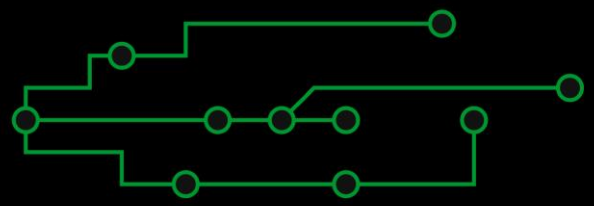
MITRE

Battle of The Bots PvP



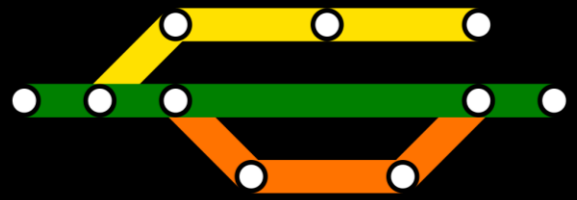
Battle of The Bots PvE Maps

MAINFRAME MADNESS



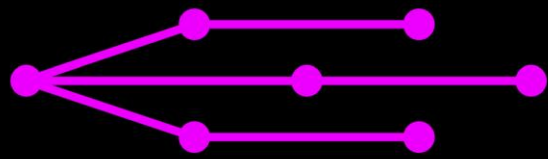
- Unencrypted traffic
- Insecure protocols
- Famous backdoors

CVE CITY



- Critical Vulnerabilities
- Critical Weaknesses
- OWASP Top 10

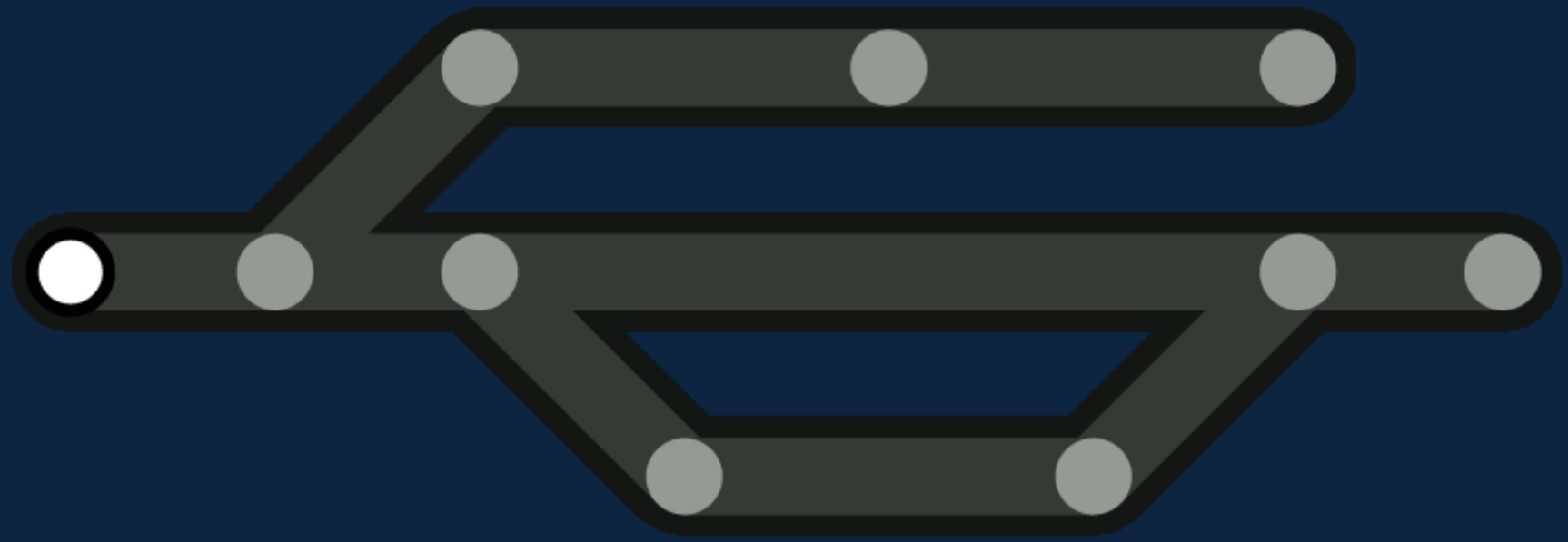
SPACE PUNK



- Reverse Engineering
- Binary Exploitation

MITRE

Battle of The Bots PvE CVE City Map



MITRE

The Threat-Informed Challenge Development Process

- **Discovery** – Querying the world for potential challenges
  - MITRE CVE + ATT&CK
  - CISA, OWASP, OSINT
- **Assessment** – Determining the viability of deployment
  - Docker *(BOTB)*
  - Reliable solvability – ex: avoiding race condition exploits
- **Deployment + Quality Assurance**
  - Tie networks together *(BOTB)*
  - Challenge verification
    - Metasploit module/PoC *(BOTB)*
    - Ghidra solution script *(Ghidra Golf)*

MITRE

An Example – BOTB Log4Shell (CVE-2021-44228)

- **Discovery**
  - Within CISA's Top 15 Routinely Exploited Vulnerabilities in 2021
- **Assessment**
  - We can dockerize a Java application
- **Deployment + Quality Assurance**
  - Connect docker network on a particular path
  - PoC = Log4J exploit with custom header
    - Adequately leverage reverse engineering and capability development skills

MITRE

Combining Threat-Informed Challenge Development in a Realistic Network Environment

- Two Vulnerabilities
  - GitLab ExifTool (CVE-2021-22205)
  - Sudo Pwfeedback Buffer Overflow (CVE-2019-18634)
- Enable lateral movement via a GitLab runner
  - CI/CD pipelines are incredibly common in development environments

MITRE

Combining Threat-Informed Challenge Development in a Realistic Network Environment

- Multi-step approach (Chaining Exploits)
  - Breach into GitLab host using ExifTool vulnerability
  - Create a repository to spawn a shell on the Sudo host
    - .gitlab-ci.yml will run on Sudo host via GitLab Runner
  - Use Sudo vulnerability for privilege escalation to plant your flag

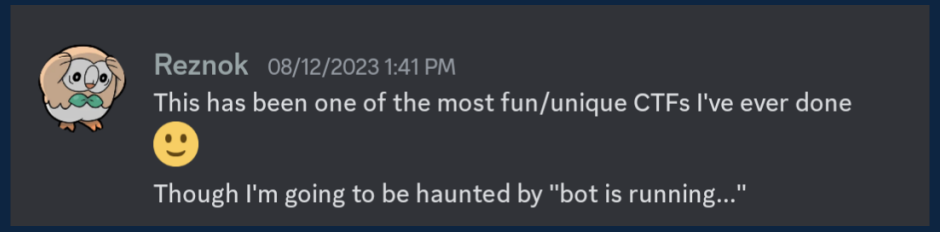
The Benefits of Threat-Informed Competitions as Training

- Realistic environments & challenges further enable the transition of core skills to real-world exercises
- Utilize gamification to train competitors in cybersecurity areas
  - Enticing to those new to the space
  - Keeps learners/competitors engaged
- Competition artifacts **conducive** to future exercises and training for the community

MITRE

Does it work?

- Unique competition formats were enticing
  - 71 competitors for Ghidra Golf
  - 40 competitors for Battle of The Bots PvP
  - 60 competitors for Battle of The Bots PvE
  - Growing Discord community >100 members
- Positive competitor feedback
  - Emphasis on **learning**
    - “Can’t wait to bring these skills into the office”
  - Approachable and engaging challenges



Loved that it was an original concept, requiring a worm. It made it an amazing blend of hacking and dev skills which I absolutely loved.

MITRE

Does it work? - Continued

- Competition artifacts applicable to **real-world** vulnerabilities and exploits
  - User-submitted Ghidra scripts *(Ghidra Golf)*
    - Various reverse-engineering automation scripts
  - “Red-Team” packet captures *(BOTB PvP)*
    - Useful for incident response and forensics training
  - User-submitted worms/bots *(BOTB PvE)*
    - Useful for adversary emulation, reverse engineering, and forensics training

Conclusion

- CTFs gamification provide an engaging avenue for competitors to learn
- We can elevate CTFs by implementing **Threat-Informed Challenges**
  - Enables competitors to learn/practice skills applicable to real-world exercises
  - Equip competitors with skills applicable beyond the competition
  - Generates realistic artifacts useful for future training
- Threat-Informed CTFs provide a hands-on approach to cybersecurity training

Niko Reveliotis

https://www.linkedin.com/in/nicholas-reveliotis-0a8640175

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®