SIGPwny

Purple Team FA2026 • 2026-09-01

# Intro to Purple Team

Ronan Boyarski

# Ronan Boyarski

- Purple Team Offensive Cyber Lead
- MSCS Student
- Former competitive shooter

# Ronan Boyarski

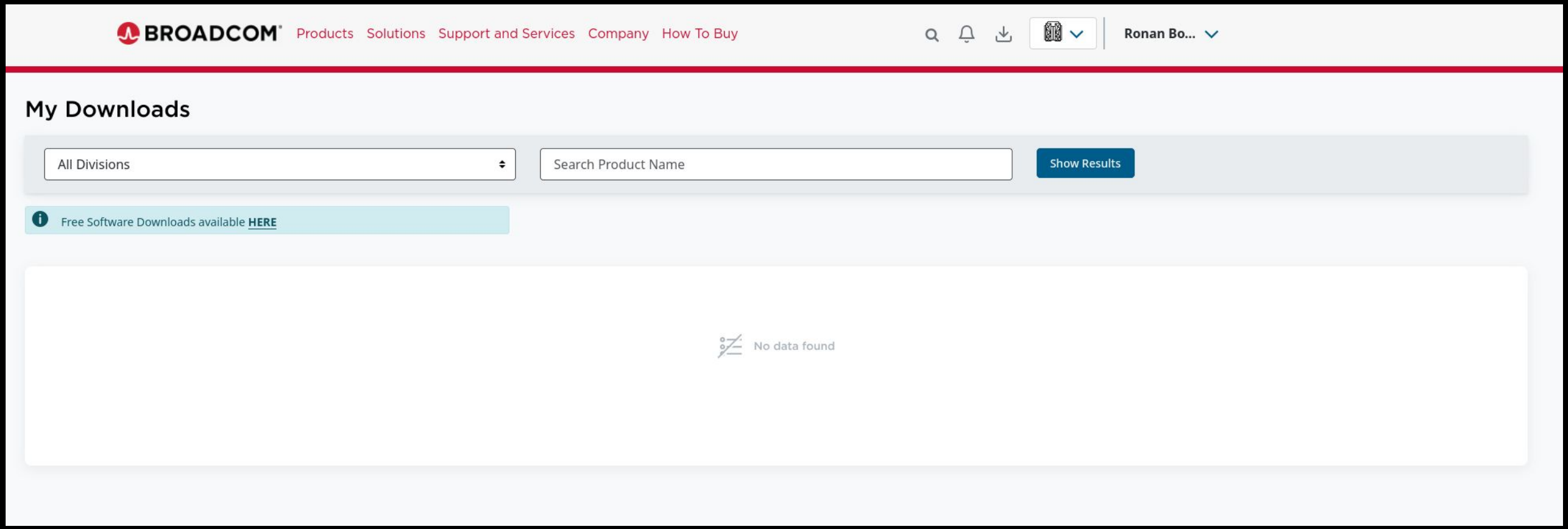
- Purple Team Offensive Cyber Lead
- MSCS Student
- Former competitive shooter
- Also I have a pig

# VM Setup

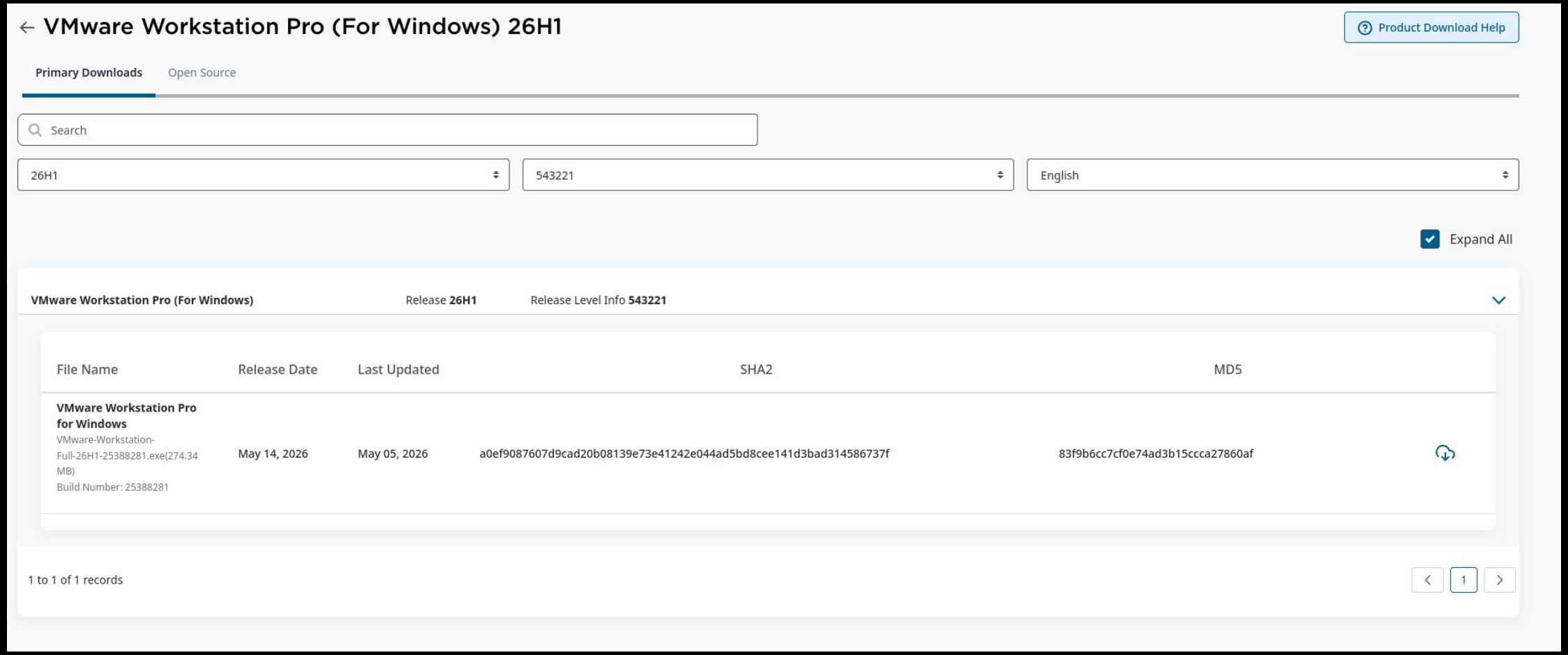
# Download VMWare

- Go here: https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion
- You may need to create a broadcom account
- Search for VMWare Workstation Pro on Windows
- Mac needs VMWare Fusion or UTM depending on Intel or ARM

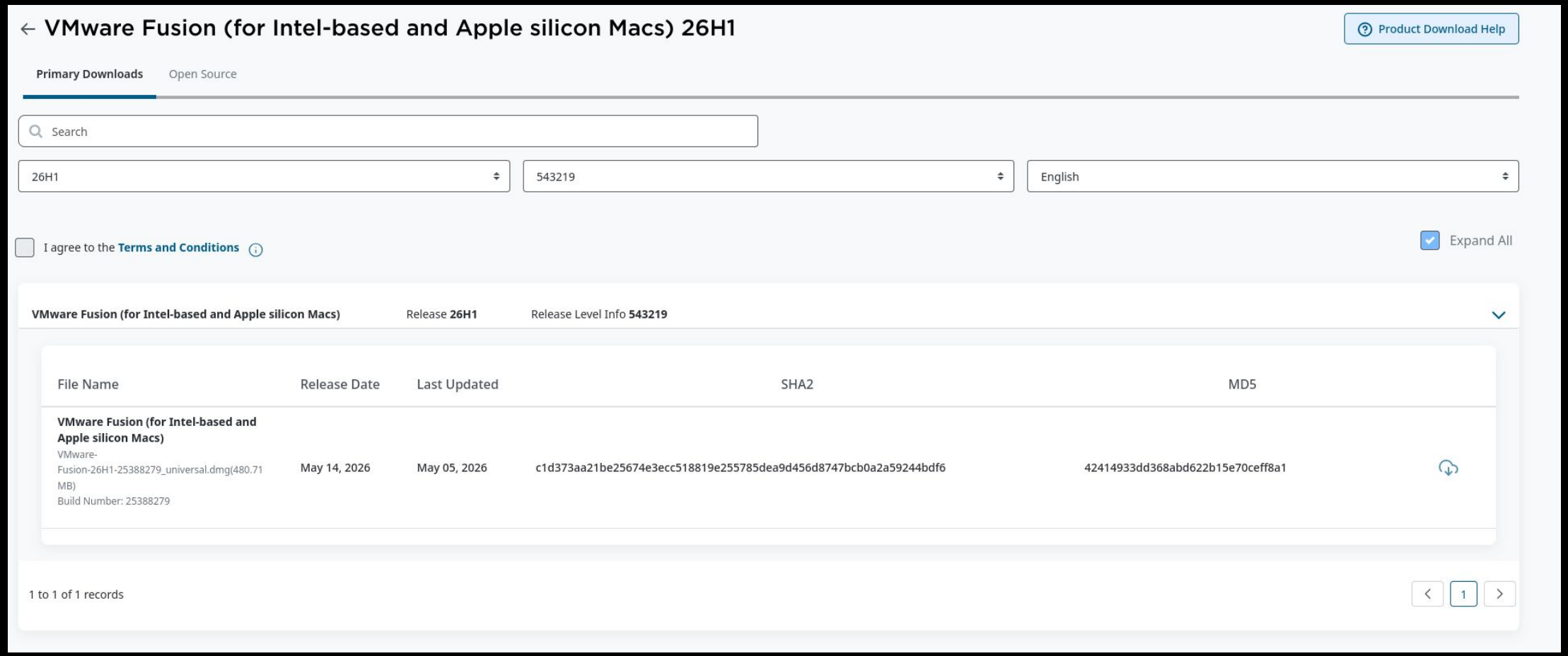
# Download VMWare



# Download VMWare - Windows

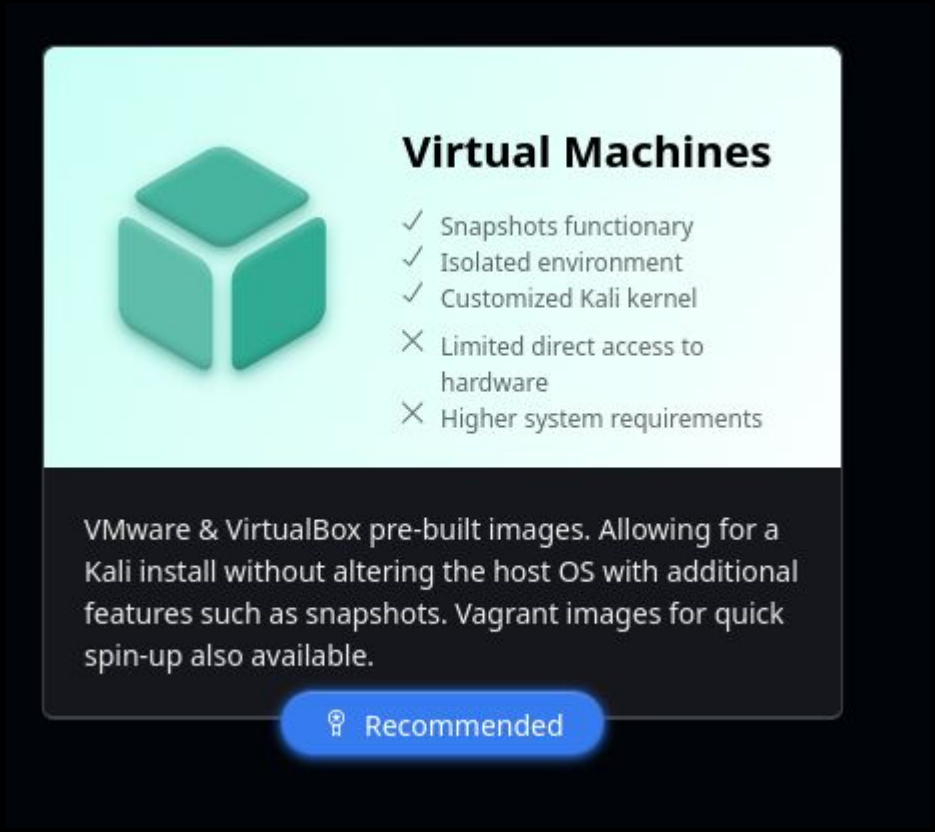



# Download VMWare - Intel Mac



# Kali Install - Not ARM Mac

- Go here: https://www.kali.org/get-kali/#kali-platforms
- You want this:




# Download VMWare & Kali - ARM Mac

- This will require UTM (https://mac.getutm.app/)
- Official docs: https://www.kali.org/docs/virtualization/install-utm-guest-vm/
- I believe this requires the Apple Silicon installer https://www.kali.org/get-kali/#kali-installer-images

# Reasonable Defaults

- Create a new VM -> Kali ISO -> Customize Hardware
- You will probably want 60-80 gigs of disk space
- Multiple cores & >4gb RAM preferable
- There should be a guided graphical install process
- Do not change things like the window manager unless you know what you're doing
- If you go too low on disk space you might need to reinstall which is no fun

# What is Purple Team About?

# General Philosophy

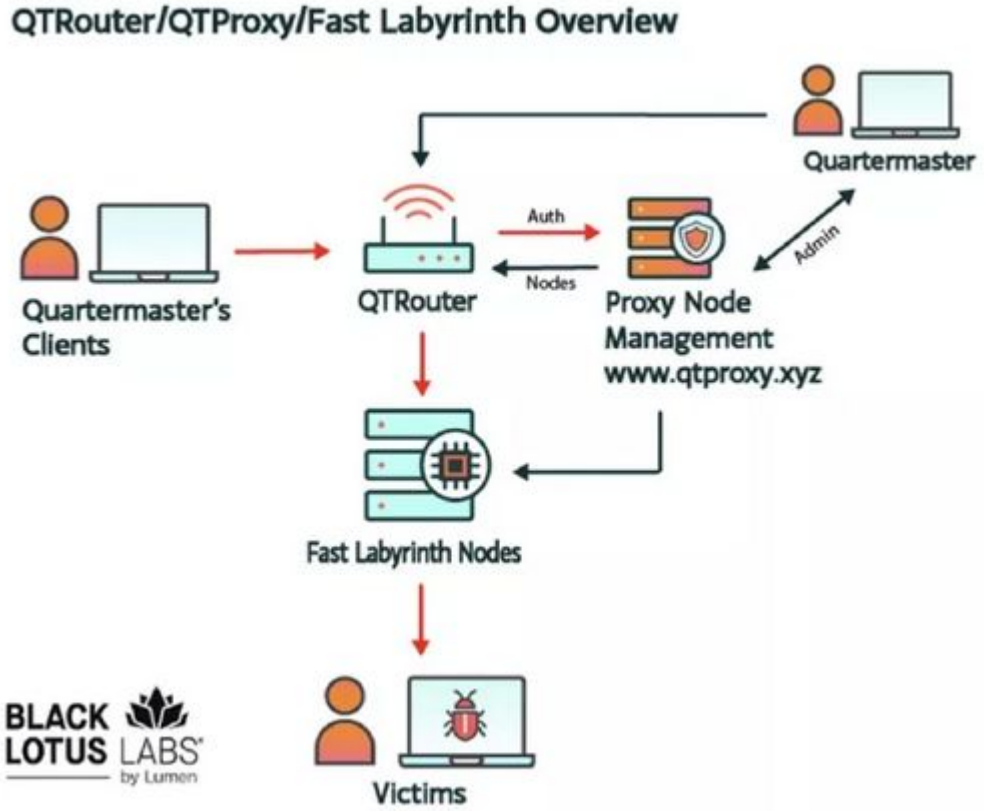
- Mix of practical offensive and defensive security topics
- Defenders will understand what advanced attackers actually do
- Attackers will understand high-end defenses
- Some prerequisite knowledge is encouraged
  - Fundamentals in security, scripting, networking, and operating systems
- SIGPwny general teaches fundamentals of security
- We teach how to **actually** attack targets (end-to-end) and defend endpoints within IT/OT networks
  - Configure, build, target, exploit, and report!

# What do we do?

- Learn & train fundamentals
  - Network Security
  - Linux & Windows OS Security
  - Attacking Active Directory
  - Malware Development & Detection
- Competitions
  - DoE CyberForce & CCDC
  - TracerFIRE
- Research
  - Find 0days & write malware


# Learn how to do stuff like this!

## FBI Disrupts China-Linked QTFY Infrastructure Used to Steal Data From U.S. Organizations




## CISA Red Team Compromised Two Critical Infrastructure Orgs, One Detected Nothing

Home > Campaigns > ArcaneDoor

### ArcaneDoor

ArcaneDoor is a campaign targeting networking devices from Cisco and other vendors between July 2023 and April 2024, primarily focused on government and critical infrastructure networks. ArcaneDoor is associated with the deployment of the custom backdoors Line Runner and Line Dancer. ArcaneDoor is attributed to a group referred to as UAT4356 or STORM-1849, and is assessed to be a state-sponsored campaign.[1][2]

ID: C0046
First Seen: July 2023 [1]
Last Seen: April 2024 [1]
Contributors: Jun Hirata, NEC Corporation; Sareena Karapoola, NEC Corporation India; Pooja Natarajan, NEC Corporation India
Version: 1.0
Created: 06 January 2025
Last Modified: 31 July 2026

Version Permalink

### Techniques Used

ATT&CK® Navigator Layers

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1583 | .003 | Acquire Infrastructure: Virtual Private Server | ArcaneDoor included the use of dedicated, adversary-controlled virtual private servers for command and control.[1] |
| | | .006 | Acquire Infrastructure: Web Services | ArcaneDoor included the use of OpenConnect VPN Server instances for conducting actions on victim devices.[1] |
| Enterprise | T1557 | | Adversary-in-the-Middle | ArcaneDoor included interception of HTTP traffic to victim devices to identify and parse command and control information sent to the device.[1] |
| Enterprise | T1071 | .001 | Application Layer Protocol: Web Protocols | ArcaneDoor command and control activity was conducted through HTTP.[1] |

# We Will Cover

- Basic VM setup
- Networking fundamentals & network security
- OS fundamentals & OS security
- Active Directory authentication & attacks
- How to write your own tools
- Digital Forensics
- Incident Response
- Malware Detection

# Don't Get Arrested II

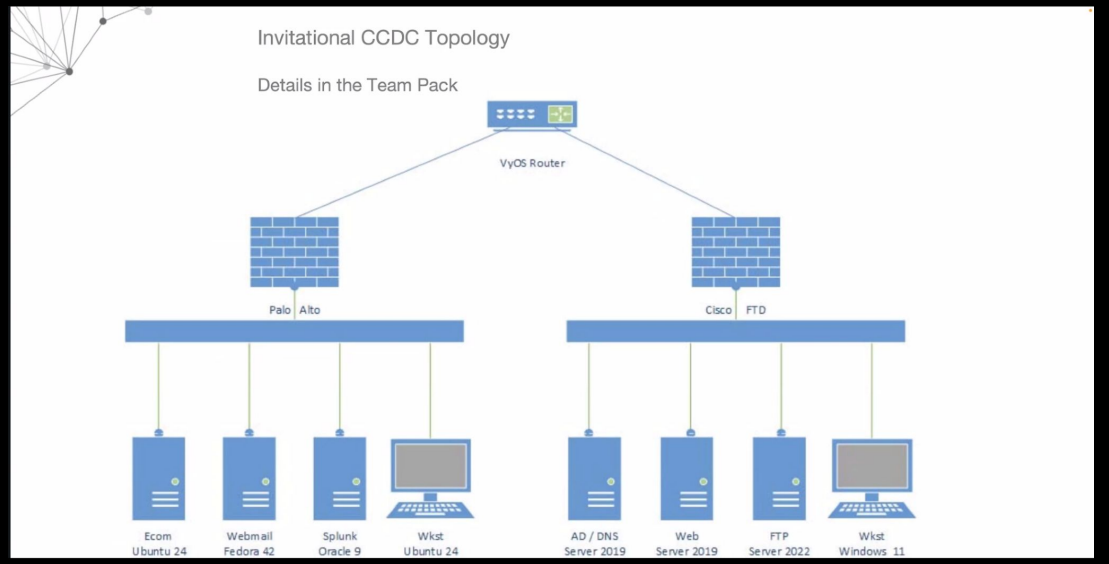
- The techniques used here can be used to attack real enterprises
  - If you try to do anything from the first semester, **you will be caught**
  - Do **NOT** try to do this against external targets / UIUC Active Directory
  - The last guy to try this got 24 months in jail and >20k in fines
- We will get into operating undetected later in the semester
  - Operating undetected in modern environments is hard (but not impossible)
  - Do **NOT** try to do this. If you can do this, then you will have no problem finding a high-paying job

# Remote Code Execution != Hacking

- Actual hackers are going to be taking extensive measures to conceal their identity and operation
- Real ethical red teamers must understand their tools
- Being a professional means red teaming responsibly
- This requires attention to detail that will not be explicitly covered in most training
- If you are interested in a **career path** in cybersecurity, feel free to talk to admins and helpers!

# Competitions

- Blue teamers (us) are given systems to secure and maintain the functionality of various services
  - Services are scored by uptime
  - Red team will try to take our services down
- We will be given business tasks to do simultaneously
- Submit Incident Response reports



# Competitive Expectations

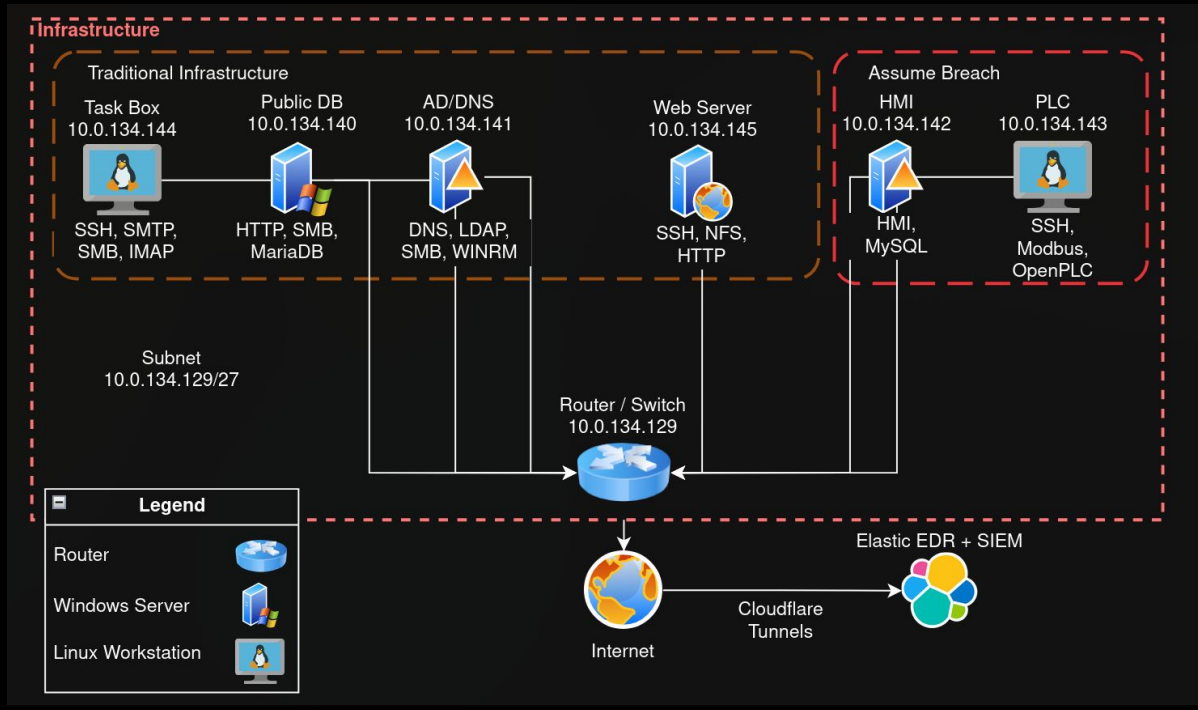
- Purple represents SIGPwny and UIUC overall externally at collegiate cyberspace events/competitions in cyber defense.
- Some competitions are less restrictive and open-invite. We can bring dozens to participate. Commit availability for this and communicate effectively.
- Some are restricted to one team per university and are the source of our national ranking. We insist on remaining competitive.
  - Roster selections will prioritize those with training/experience, demonstrated trust to the team, and/or meaningful contributions.
  - These environments **will** be tense. The team prefers those with this temperament and aptitude to be considered heavily more.

# Build Your Roadmap

- Cybersecurity is broad, and offensive and defensive involvement span many cyber subdomains. People spend their entire careers pursuing a handful of these domains. You will eventually find what resonates more with you.
- Generally you can begin with defense then pivot to offense
- Then specialize. You can be the SME for that area (subject matter expert). If you compete, you can assume relevant responsibilities on for the team's network. On a day to day, you can contribute with more exposure.

# CyberForce

- Defend an **Operational Technology** network
- Last year was an oil rig
- Requires both social and technical skills
- Last year we were the top team for defense and service uptime!

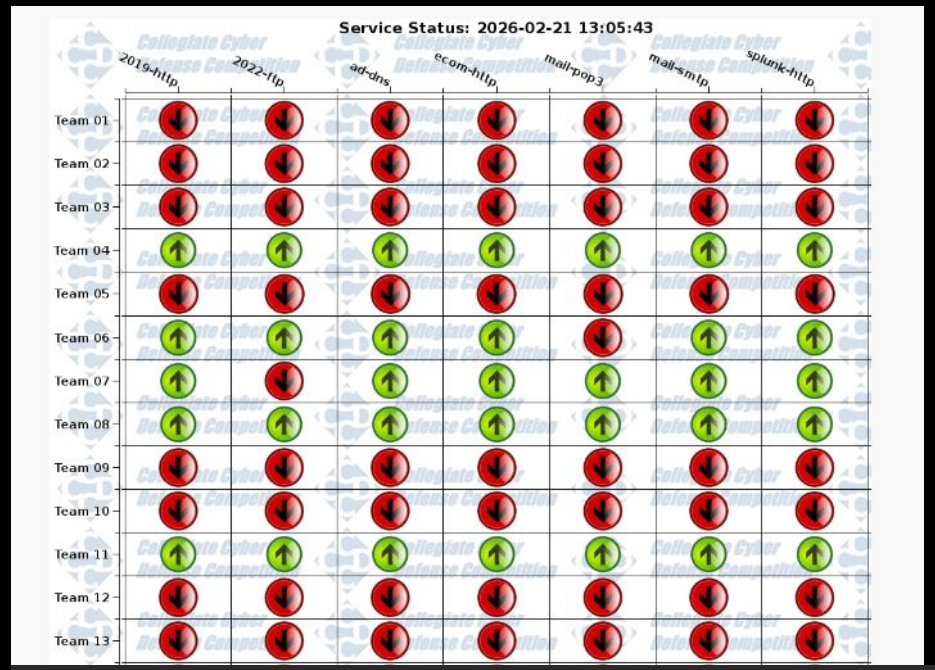




they hated our presentation :(

# CCDC

- Defend an **Information Technology** network
- Keep a variety of services running in a small simulated enterprise
- You are actively under attack!
- Respond to business tasks (injects)
- Respond to simulated users
- Simulates realistic SOC scenarios under tight and jam-packed deadlines




University of Illinois at Urbana-Champaign CCDC Team,

It was one of my greatest pleasures to make plans to include your team at the 2026 MWCCDC regional. Your team took 4th place overall, vindicating this decision.

Attached are feedback reports from the recent regional. Note that nearly all teams are assessed 'weak' on services in their report, but U of I was 8th on services. 84% response on injects was very good, and your inject scores were good.

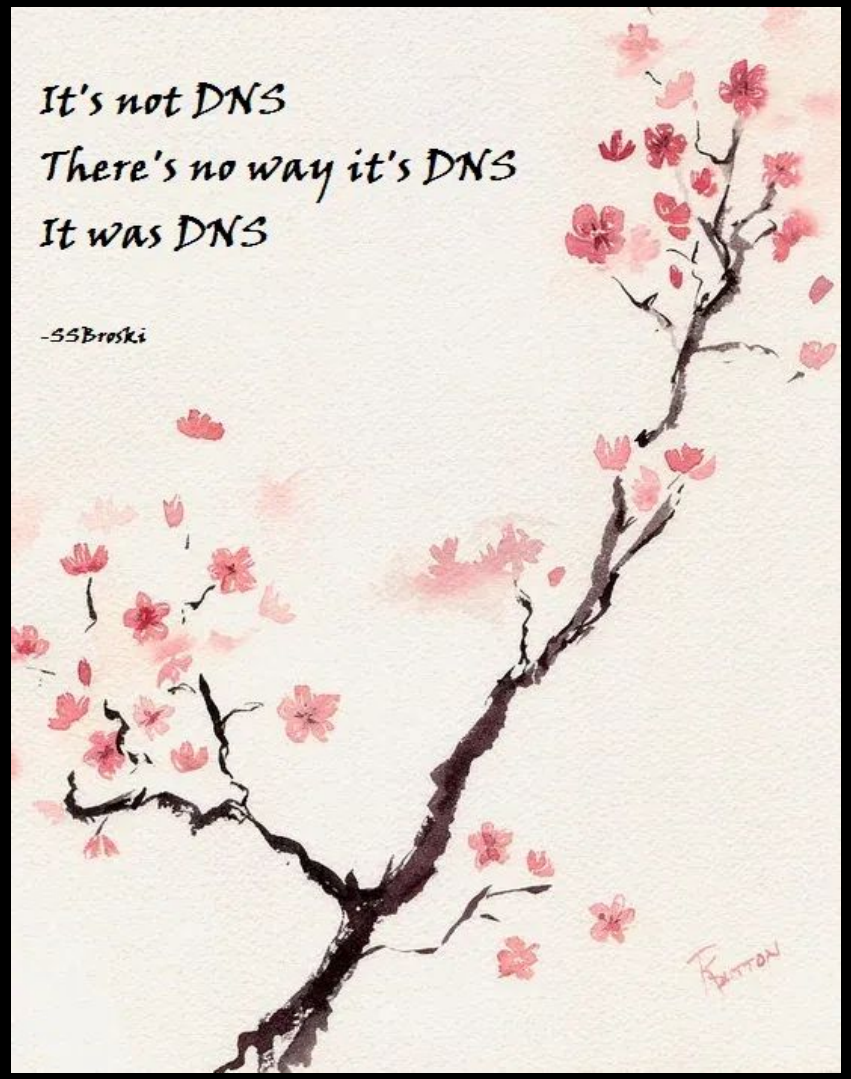
Your assessment from the red team was especially good, 3rd for the event and pretty close to the 2nd place team.

U of I is on the map as one of the very best CCDC teams in the Midwest, and joins the Illinois rivalry with DePaul, SIU, and IIT.

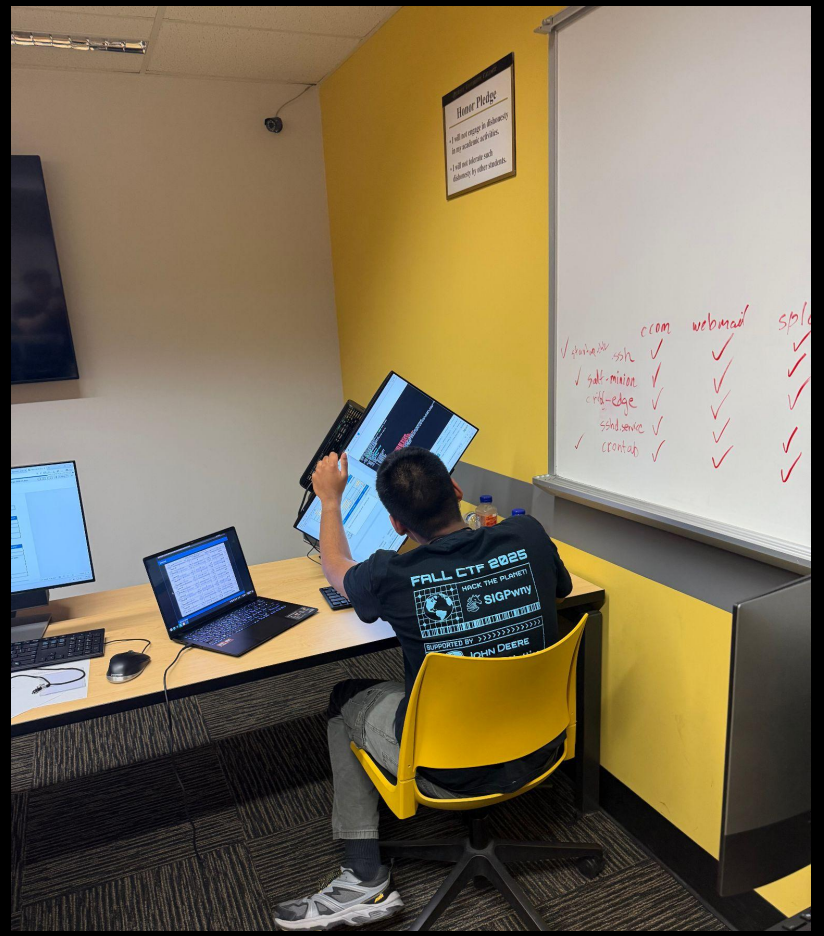
I look forward to working with your team in the 2027 MWCCDC season.

David Durkee

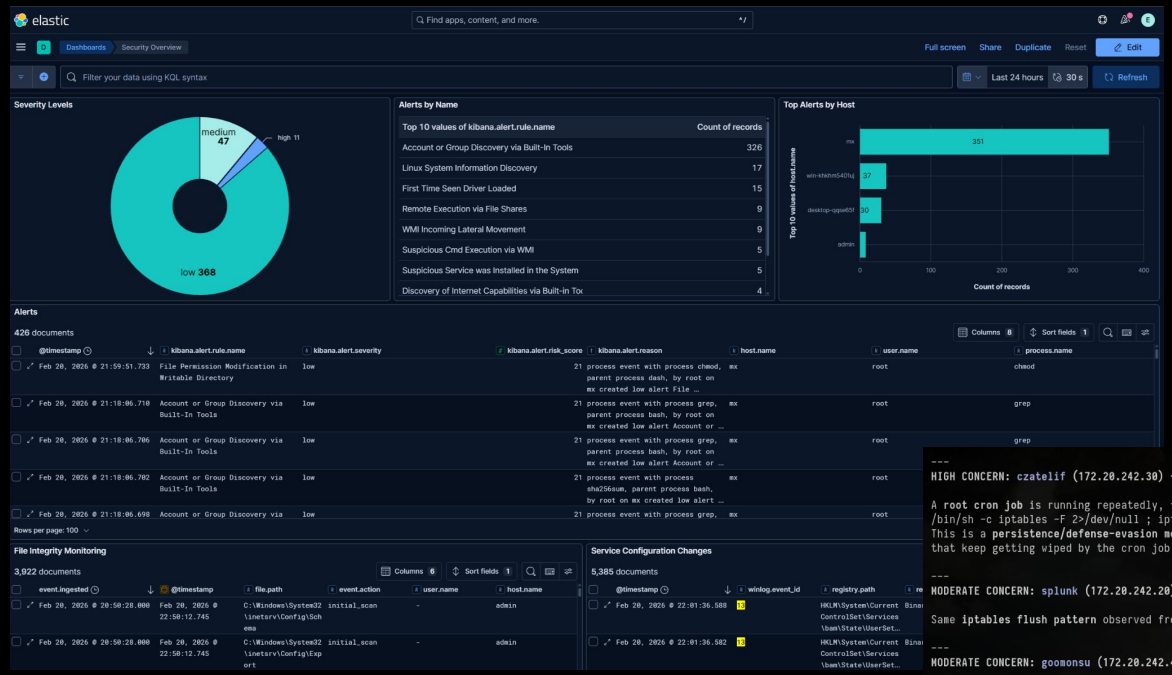
# The CCDC Experience

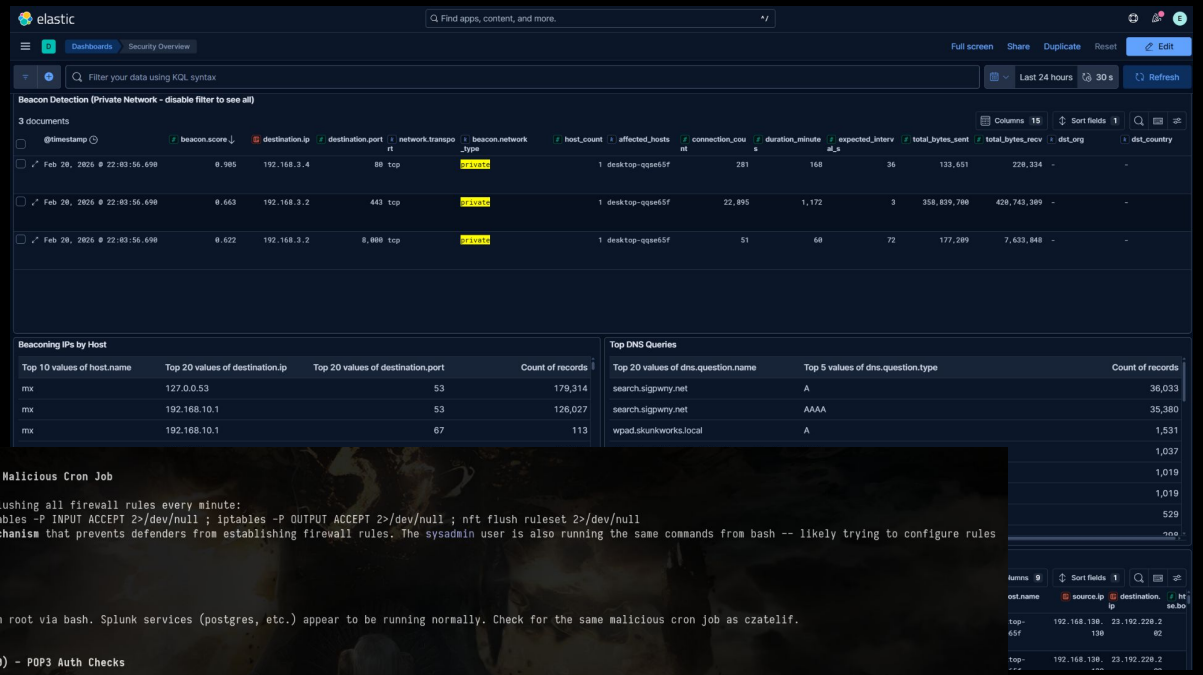



```
Never gonna give you up
Never gonna let you down
Never gonna run around and desert you

~ Your friendly neighborhood Red Team ~

Never gonna give you up
Never gonna let you down
Never gonna run around and desert you

~ Your friendly neighborhood Red Team ~

sysadmin@goomonsu:~$ _
```



# Defensive Tool Development




---

**HIGH CONCERN: czatelif (172.20.242.30) - Malicious Cron Job**

A **root cron job** is running repeatedly, flushing all firewall rules every minute:
`/bin/sh -c iptables -F 2>/dev/null ; iptables -P INPUT ACCEPT 2>/dev/null ; iptables -P OUTPUT ACCEPT 2>/dev/null ; nft flush ruleset 2>/dev/null`
This is a **persistence/defense-evasion mechanism** that prevents defenders from establishing firewall rules. The sysadmin user is also running the same commands from bash -- likely trying to configure rules that keep getting wiped by the cron job.

---

**MODERATE CONCERN: splunk (172.20.242.20)**

Same **iptables flush pattern** observed from root via bash. Splunk services (postgres, etc.) appear to be running normally. Check for the same malicious cron job as czatelif.

---

**MODERATE CONCERN: goomonsu (172.20.242.40) - POP3 Auth Checks**

Running Dovecot POP3 service with repeated `unix_chkpwd` calls for users like `chase.logan` and `charles.labelle`. This could be:
- Legitimate mail service being scored
- Password brute-force attempts against POP3

---

**DOMAINCONTROL-1 (172.20.240.102) - No process telemetry yet**

No endpoint process events found in the last 8 hours. It was only registered at 16:01, so this is expected. The DNS beacon to `104.77.144.79:53` (score 0.948) resolves to legitimate Akamai CDN hostnames -- **likely benign** Windows DNS resolution.

---

**BENIGN / False Positives**

| Destination | Score | Verdict |
|---|---|---|
| `67.4.56.154:80` (scoring.ccdcscoring.net) | 0.665 | **CCDC scoring engine** - all new hosts POSTing to `/data`. Safe. |
| `1.1.1.1:53` (Cloudflare DNS) | 0.834 | Normal DNS resolver traffic |
| `172.20.240.102:53` (Domain Controller) | 0.832/0.746 | Internal DNS to DC. Expected. |
| `104.77.144.79:53` (Akamai DNS) | 0.948 | Queries for `a767.dspw65.akamai.NET` etc. Legitimate Akamai CDN lookups |
| Microsoft IPs (172.183.7.x, 52.x, etc.) | 0.7-0.834 | Windows telemetry/update traffic |
| `10.48.14.24:8089` | 0.759 | Splunk management port. Likely Splunk forwarder traffic. |
| `192.168.10.53:53` | 0.558 | Internal DNS resolver |

# TracerFIRE

- Forensics competition, no active defense
- You will have a simulated organization breached by multiple threat groups
- Investigate and figure out:
  - What happened?
  - How did they get in?
  - Who are they?
  - What is their objective?

# How To Prepare

# Meaningful Training Requires Effort

- Red teaming is **hard**!
- Security is not an academic discipline
- You cannot *learn* things passively
- You must **do** security to actually build proficiency
  - Building even basic proficiency requires repeated practice
  - There are no "experts" in this field - just people with a lot of real experience
- We will provide you an environment to start doing security
  - The internal training can't cover everything, so it’s important to find this externally (we will show you where!)

# Training Is Encouraged & Noticed Here

Proficiency in this space is contingent on your ability to employ resources: *walkthroughs, labs, cyber ranges, certifications*

- We strongly encourage you choose pathways within these sites and bring your knowledge to Purple.
  - Start with the fundamentals, then build towards specialization
- Those who do train are evidently more capable in this space and can contribute significantly more
  - This is legitimate resume experience for technical aptitude and training sections. Well respected by employers.
- Training on your own, prior experience, and involvement are the main factors for who makes it onto the most selective teams

# Training Resources

- HackTheBox (https://www.hackthebox.com/)
  - On-demand vulnerable machines & networks, mostly red team
  - Recently also added general CTF, DFIR, SOC practice as well as structured learning content. **highly recommended**
- PwnyCTF (https://ctf.sigpwny.com/)
  - Still a great way to learn basics, less relevant in purple team
- CyberDefenders.org (https://cyberdefenders.org/)
  - DFIR & SOC focused with *great* free content
- TryHackMe (https://tryhackme.com/)
  - Designed for beginners, good for general training and exposure
  - Free content may be lower quality, updates less frequently than HTB

# Certs Are Expensive; Knowledge Is Cheap

- Knowledge
  - Participating in Purple Team - ALL FREE
  - TryHackMe subscription - $8 per month w/ student discount
  - HackTheBox academy content - $8 per month w/ student discount
  - HackTheBox all boxes unlock - $25 per month
  - HackTheBox **advanced prolabs** - $49 per month
- Certificates
  - Hackthebox CPTS - $210 per exam attempt
  - eJPT - $250 per exam
  - PJPT/PNPT - $500 per exam
  - CRTO - £365 course + exam attempt
  - Any Offsec cert (OSCP, OSEP, OSED, etc) - $**1750+**

**You don’t have to commit to cybersecurity to learn cybersecurity.**

# Skill Levels

- **Beginner** <- most of you are here
  - able to understand basic programming, OS, networking
  - **willing to engage in structured learning and practice**
- **Intermediate** <- we will cover content until here
  - comfortable performing common offensive and defensive tasks
  - e.g. enumerate and compromise common systems, perform basic privilege escalation and lateral movement, analyze logs and alerts, and investigate straightforward incidents
  - Certificates like CPTS, OSCP, CCD, etc are within reach with targeted prep.
- **Advanced/Career-ready**
  - We won't cover every advanced topic in depth. You should be comfortable exploring independently at this stage.
  - Feel free to talk to our members for guidance

# Next Meetings

`2026-09-3` • **This Thursday**

- Setup Meeting! Get a Kali VM up and running

`2025-09-16` • **Next Tuesday**

- Network Security Fundamentals