

Purple Team

FA2025 • 2025-09-11

Intro to Blue Team

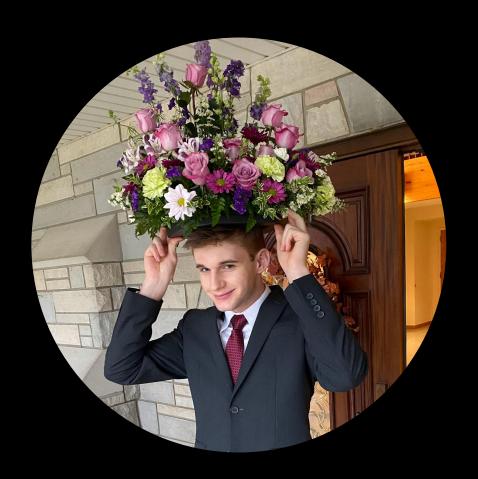
Bryce Kurfman & Michael Khalaf

ctf.sigpwny.com
sigpwny{blue_pill_please}



Bryce Kurfman, Acquirer of Hardware

- Helper & Purple Team Cyber
 Defense Lead
- B.S. Computer Science '27
- ICS Cybersecurity Engineer @ BW Design Group
- I have opinions about cucumbers



Michael Khalaf

- Helper & Purple Team Cyber
 Defense Lead
- MS Information Management + Computer Security
- Network Operations @ ITI (DARPA)
- Rush is the greatest rock band to exist.



Table of Contents

- Expectations
- Blue Team Approach
- Training Resources
- Flagship Competition: CCDC
- Flagship Competition: DoE CyberForce
- Cyber Defense Competitions: TL;DR
- Key Concepts
- Infrastructure Reminder



Expectations

- We have a limited number of proxmox PwnyOS logins
- If you miss 4 consecutive meetings, we will reallocate resources if necessary
- This is to accommodate whoever is actively participating



Our Approach

- We are here to share our own experience, approach, and methodology
- You will get the best return on your time investment by focusing on training
- We are dedicated students taking our own time to train and share
- If you are knowledgeable in one of these subject areas, ask to run a meeting!



Immediate Training Resources

- PwnyCTF by SIGPwny (https://ctf.sigpwny.com/)
 - Great place to learn the fundamentals, including forensics & reverse engineering!
- CyberDefenders.org (https://cyberdefenders.org/)
 - DFIR & SOC focused with *great* free content
- HackTheBox (https://www.hackthebox.com/)
 - On-demand vulnerable machines & networks, mostly red team with better blue content today than before
- TryHackMe (https://tryhackme.com/)
 - Designed for beginners, good for general training and exposure



Flagship Competition



National Collegiate Cyber Defense Competition



Flagship Competition: DoE CyberForce



CyberForce



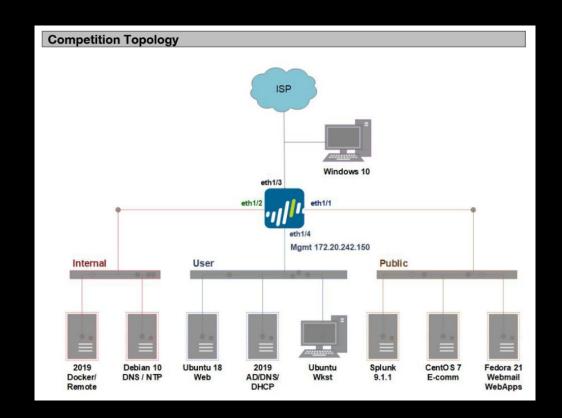
Flagship Competition: TracerFIRE





What is a Cyber Defense Competition?

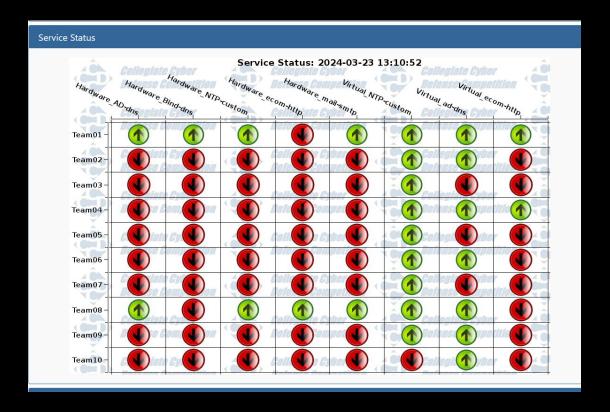
- Blue teamers (us) are given systems to secure and maintain the functionality of various services
 - Services are scored by uptime
 - Red team will try to take our services down
- We will be given business tasks (injects) to do simultaneously
- Additionally, we are tasked with responding to random incidents, so we must submit IR reports as a form of sociotechnical (incident response)





Competition Plan

- Immediate Plan
 - Access each system and gather information
 - Rotate passwords & secure users/groups (document everything)
 - Harden system & services
 - Enable/configure firewalls, containerize everything, install Wazuh, etc.
- Threat Hunt & Audit System for Persistence
- Incident Response
- Respond to Injects





The Most Important Thang(s)

Communicate, and have fun!

(and for the love of all that is holy, check the crontab)



Additional Notes

- Cyber Defense competitions often have intentionally unrealistic time frames
- Keep a level head
- Expect the unexpected
 - This is what defense-in-depth is for!



In order to perform website maintenance, our online store will be temporarily offline.

We apologize for the inconvenience and ask that you please try again later.





Key Concepts



Services

- Any individual / organization / enterprise requires exposing functionality
- Individual **boxes** (read: machines) expose **services**
 - A **service** is something accessible over the network that provides functionality
 - For example, web server, file share, secure shell
 - Each box can have multiple services; Some have none
- The collection of exposed services that provide meaningful functionality is called **attack surface**



Attack Surface Reduction

- The more services you have exposed, the more chances an attacker will have to attack one of them
- Almost everyone will be actively reducing their attack surface through networking
- Not every computer needs to be exposed to the internet in this way, routers contribute to massively reducing attack surface
- Not every service needs to be exposed to the internet, even on internet-exposed machines. This is done by a **firewall**
- Not every service needs to be exposed to your peers even on your own network this can be done via **host firewalls** or other methods



Mandatory Door Analogy

- Imagine you live in a house with many points of entry of varying levels of security
- Which has more ways in (all things being equal)?
 - A house with one door
 - A house with ten doors
 - A house with 1000 doors



Mandatory Door Analogy

- Imagine you live in a house with many points of entry of varying levels of security
- Which has more ways in (all things being equal)?
 - A house with one door
 - A house with ten doors
 - A house with 1000 doors
- Even if you are great at securing houses, you will have a **much** easier time locking down the house with one door versus 1000



Closing Doors

- How can we close the doors?
- A firewall will block off certain ports and services from access
 - For example, **only allow ports 22, 53, 80, 443** and **445**
- A router will block off certain hosts
 - For example, someone from the internet cannot directly connect to your personal computer
- We can use **tunneling** to have services run only on the computer and expose it to select other computers
- In Cyber Defense, the best first step is to start closing unnecessary doors



Vulnerabilities & Exploits

- A **vulnerability** is some specific weakness in your software (usually a service)
 - If we can run arbitrary commands on your service, then that's a vulnerability
 - If we can overflow the buffer and overwrite variables on the stack, that's a vulnerability
 - If we can upload arbitrary files on your computer, then that's probably a vulnerability
- An **exploit** is a specific piece of code that will enable compromising a service via a vulnerability
 - The specific exploit code to deliver a shell via a buffer overflow or arbitrary file upload would be an exploit
- Less doors generally mean less vulnerabilities

Vulnerability Management

- Many enterprises will have dedicated vulnerability management teams that will go hunt for known vulnerabilities in their network and fix them
- Some pieces of software (Active Directory, Windows OS) will have certain vulnerabilities that are **required** for functionality, which will create an attack surface even in a "perfectly secure" environment
- You will never be able to fully remove all of the vulnerabilities, meaning you will always have some attack surface exposed
- This is why defense-in-depth is necessary



Defense in Depth

- Essentially a layered defense, this is the most important defensive security concept
- Defenses will be layered and overlapping, allowing for multifaceted detection of activities
- For example, having multiple sources of telemetry and analysis for hosts and networks, proactive security policies that encourage patching, restrictive firewalls, remote log forwarding, and a vulnerability management team
 - All of these things cover similar areas, but do it differently, so what slips through one will get hit by another



Catching Bad Guys

- Threat actors will do the following
 - Look for open doors
 - See if they know a way in (known vulnerability)
 - Break in (with a known or unknown vulnerability)
 - Enter your house (code execution and implant on your computers)
 - They will do this to establish command and control
 - The simplest command and control would be something like **SSH**
 - Establish **persistence** (drop malware to keep getting in over time)
 - This is basically propping the door open, or making a secret entrance
 - Steal your valuables



Catching Bad Guys

- We can catch folks snooping around the network by logging network traffic
- We can catch malware by logging files on the host
- We can automatically parse some of these logs, files and events
 - This is what **Antivirus** does
 - When you add behavioral detection, you get Endpoint Detection and Response (EDR)
- There are other sources
 - Process trees, memory dumps, disk carving, etc.
 - These generally demand skilled human analysts to reveal advanced attackers



Catching Bad Guys

- Generally, intrusions will be initially detected through automated alerts
 - Sometimes diligent users will report phishing or slow machines
- From there, an **Incident Responder** will triage the report and investigate
- If it's determined that there is a malicious actor, we will generally observe them briefly to determine their access and tactics, then remove them from the environment
 - This requires some core competencies, including malware reverse engineering, using EDR tools, packet captures, and general security awareness



Removing the Bad Guys

- Make sure to never delete or change any forensic evidence if possible
- Also, start the incident response process:
 - Isolate affected hosts
 - Search for and remove any persistence mechanisms
 - Remove backdoors, malicious user accounts
 - Patch vulnerabilities
 - Terminate malicious processes
 - etc.
- Sometimes, threat actors will wait a long time (>90 days!) for logs to **rotate**, which greatly complicates investigation and attribution

Threat Modeling

- **Threat Modeling** is understanding what services you offer and what attackers can do to go after them
- Threat Modeling overlaps heavily with risk management you are going to have a mental model, informed by **Cyber Threat Intelligence**, as to what your vulnerabilities are and how threat actors exploit them
- Threat Modeling will inform what concrete defense steps you can take with your limited time and resources
- Sometimes, red teamers will perform **Adversary Emulation**, where they will attack a network with the specific tactics of an adversary that we are worried about

MITRE ATT&CK

- MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics, techniques, and procedures (TTPs)
 - It is based on real-world observations derived from cyberattacks
- It helps defenders understand how attackers operate and enables a common tagging method for threat analysis
- Also helps inform adversary emulation and automated detection from Endpoint Detection and Response



			ATT	&CK Matrix fo	or Enterprise						
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and	Exfiltration	Impact
11 techniques	16 techniques	23 techniques	14 techniques	45 techniques	17 techniques	33 techniques	9 techniques	17 techniques	18 techniques	9 techniques	15 techniques
Content injection	Cloud Administration	Account Manipulation (7)	Abuse Elevation Control Mechanism is	Abuse Elevation Control Mechanism is	Adversary in the Middle us	Account Discovery (4)	Exploitation of Remote	Adversary in the Middle or	Application Layer Protocol is	Automated Difficultion on	Account Access Removal
Drive by Compromise	Command and Stripting	BITS Jobs	Access Token	Access Token	Brute Force (c)	Application Window Discovery	Internal Spearshishing	Archive Collected Data on B	Communication Through	Data Transfer Size	Data Destruction (1)
Exploit Public-Facing Application	Interpreter (12)	Boot or Logon Autostart Execution rup	Manipulation (5)	Manipulation (5)	Contentials from	Drowser Information	Lateral Tool Transfer	Audio Capture	Removable Media	Limits	Data Encrypted for Impact
External Remote Services	Container Administration Command	Boot or Legen	Account Manipulation (f)	BITS Jobs	Password Stores (N	Discovery	Remote Service Session	Automated Collection	Content Injection	Exfiltration Over Alternative Protocol ///	Data Manipulation in
Hardware Additions	Deploy Container	Initialization Scripts (0)	Boot or Logon Autostort Execution Autostort	Build Image on Host	Exploitation for Credential Access	itation for Cloud Infrastructure	Inspecting (I)	Reporter Session	Data Encoding (2)	Exhibitation Over C2	Defacement
Phohing up	ESX Administration	Cloud Application Integration	Seet or Legen	Debugger Evasion	Forced Authentication	Cloud Service	Remote Services (c)	Hjacking	Data Obfuscation (3)	Channel	Dak Wee or
Replication Through		Compromise Host	Initialization Scripts (8)	Deckluscate/Decode Files or Information	Forge With	Dashboard	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (2)	Exfiltration Over Other Network Medium //	Email Bombing
Removable Media	Exploitation for Client Execution	Software Binary	Create or Modify System	Deploy Container	Credentials (3)	Cloud Service Discovery	Software Deployment	Data from Cloud Storage	Encrypted Channel (I)	Exfiltration Over	Endpoint Donial of
Supply Chain Compromise ry	Input Injection	Create Account (s)	Domain or Tenant Policy	Direct Volume Access	Input Capture (q	Cloud Storage Object Discovery	Tools	Data from Configuration (Repository or	Fallback Channels	Physical Medium (1)	Service (4)
Trusted Relationship	Inter-Process	Create or Modify System Process in	Modification (2)	Domain or Tenant Policy	Modify Authentication Process to	Container and Resource	Taint Shared Content	Data from information	Hide Infrastructure	Exfiltration Over Web Service up	Financial Theft
valid accounts to	Communication (I) Native API	Event Trippered	Escape to Host	Modification (I)	Multi-Factor Authentication Interception	Discovery	Use Alternate Authoritication Material (c)	Repositories (5)	Ingress Tool Transfer	Scheduled Transfer Transfer Data to Cloud Account	Firmware Corruption
Wi-Fi Networks		Execution (17)	Event Triggered Execution (ct)	Ernal Speeding		Debugger Evasion		Data from Network	Multi-Stage Channels Non-Application Layer Protocol		Inhibit System Recovery
	Scheduled Task/Job (5)	Exclusive Control		Execution Guardialis (5)		Device Driver Discovery					Network Denial of Service //s
	Serverless Execution	External Remote Services	Escalation	Exploitation for Defense Evasion	Authentication Request Seneration	Domain Trust Discovery		Data from Removable	Non-Standard Port		Resource Hijacking ₍₂₎
	Shared Modules	Hijack Execution Flow (12)	Hilack Execution Flow on 1	File and Directory		File and Directory Discovery Group Policy Discovery		Media Data Staged (2)	Protocol Tunneling		Service Stop
	Software Deployment Tools	Implant Internal Image	Process Injection (12)	Permissions Modification (3)							System Shutdown/
	System Services (s)	Modify Authentication Process on	Scheduled Task/Job (6)	Hide Artifacts (10)	Dumping (i)	Log Enumeration		Email Collection (6)	Remote Access Tools	ı	Rebeet
	User Execution (4)	Modify Registry	Valid Accounts (c)	Hijack Execution Flow (12)	Steel Application Access Token	Network Service		Input Capture (c)	Traffic Signaling in	l	
	Windows Management Instrumentation	Office Application	ication	Impair Defenses (11)	Steal or Forge Authoritication Continuous	Discovery		Screen Capture Video Capture	Web Service (1)		
		Startup (s)		Impersonation		Network Share Discovery					
		Power Settings		Indicator Removal (10)	Steal or Forge Kerberos	Network Sniffing					
		Pre-OS Boot _(II)		Indirect Command Execution	Tickets (to	Password Policy					
		Scheduled Task/Job (q)		Masquereding	Steal Web Session Cookie	Discovery					
		Server Software Component (s)		Modify Authentication	Unsecured	Peripheral Device Discovery					
I		Software Extensions (p)		Process _(ii) Modify Cloud Corrects	Credentials (III	Permission Groups					
I		Traffic Signaling (2)		Modify Cloud Corepute Infrastructure (II)		Discovery (I)					
		Willid Accounts (d)		Modify Cloud Resource	-	Process Discovery					
				CHARLES		comy remarkly					



Next Meetings

2025-09-16 • This Tuesday

- Network Security & Active Recon
- Bring your OSI knowledge

2025-09-18 • Next Thursday

- Network Security & Lateral Movement
- Examine trace files (captures) and map out out attack chains.

2025-09-23 • This/Next Thursday/Sunday

- Web Hacking For Red Teamers



ctf.sigpwny.com
sigpwny{blue_pill_please}

Meeting content can be found at sigpwny.com/meetings.

