SIGPwny

Purple Team FA2025 • 2025-09-09

Intro to Red Teaming

First Last

Ronan Boyarski

- Purple Team Offensive Cyber Lead
- CS + Philosophy '26
- Former competitive shooter

CBCicada, the Unemployed

- Purple Team Offensive Helper
- Computer Engineering ‘26

- Hot take: ECE is better than CS

ctf.sigpwny.com

sigpwny{AdvancedPersistentFriends}

Virtual Machine Setup

Installation

- We will be passing around flash drives with installers
  - Contains a VMware installer by OS (Windows / Linux / MacOS)
  - Also contains the virtual disk file for the OS
- Runs PwnyOS
  - Debian-based distro with a bunch of tools pre-installed
  - Similar to Kali, but newer with many tools built from source / hand patched
  - Experienced users can install tools one by one on their current OS if preferred
- Backup Plan
  - We have a proxmox web interface if you would prefer to run the OS in the browser
  - Visit https://pwnyos.sigpwny.com:42070
  - We will DM you credentials if you need them

What is Purple Team About?

General Philosophy

- 50/50 mix of practical offensive and defensive security topics
- Defenders will understand what advanced attackers actually do
- Attackers will understand high-end defenses
- Both sides cover the same topic at the same time
  - For example, how do you attack and defend Active Directory
- 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

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 8 weeks, **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
  - You will get an understanding as to why operating undetected in modern environments is really 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, immediately
- Your two team leads are both feds ;)

Week-to-Week

- We've built a fictional domain and attack chain that follows the content from each week
    - This was a core piece of feedback from last year
    - You can go hands-on every meeting with content we go over
- External training is **necessary** to get the most out of these topics
    - HackTheBox and certifications are excellent (but expensive) resources
    - Talk to any of the leads if you have something specific you want to learn
    - We specialize in slightly different areas with different training experiences
- We compete!
    - Collegiate Cyber Defense Competition, CyberForce, TracerFIRE, HiveStorm

What do I mean by "Red Team"?

- My goal is not to just teach **penetration** testing or security in general, **but to give people the same skill set that real-world threat actors are using to compromise actual organizations**
- In order to begin with the fundamentals, this will begin more outdated and simplified and grow more modern and complex as the semester progresses
- By the end of the year, you should have a conceptual and practical understanding of what actual bad guys do, how to do it, and the environments they are targeting

How to Train

- Red teaming is **hard** (Don't worry! You can do hard things!)
- Security is not an academic discipline. You cannot *learn* things passively
- You must **do** security to actually build proficiency
  - This is like learning to fight, or shoot, or play a musical instrument
  - 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

Remote Code Execution != Hacking

- A lot of modern training resources give you the impression that hacking is just about getting code execution at all costs
- 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 true professional means red teaming responsibly
- This requires attention to detail that will not be explicitly covered in most training

Where are we going?

- The first 8 weeks will cover the basics of attacking insecure targets
- The remainder of the semester will cover attacking secure targets
- We have provisioned a cyber range for you
  - Fictional domain to work through week by week
  - Offensive boxes to attack that domain
- I would recommend HackTheBox academy or TryHackMe
  - TryHackMe is better for beginners, HackTheBox is better practice
- If you have the money and commitment, consider OSCP

SIGPwny Purple Cyber Range Infrastructure Disclosure

YOUR PROMISE TO US

We remind you, our infrastructure is provided to you on the sole basis that you will NOT use it nefariously. This is a cyber range we developed to assist the team with on hand training during our meeting sessions. It will ONLY be used for that purpose.

Should you not comply, we will revoke your access.

Next Meetings

2025-09-11 • This Thursday

- Intro to Blue Teaming
- Learn about what we do on the defensive side

2025-09-16 • Next Tuesday

- Network Security and Active Recon
- Learn how to enumerate and exploit targets over a network

ctf.sigpwny.com

sigpwny{AdvancedPersistentFriends}

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