Red Team Informational

Welcome to the first Red Team meeting!

Summary

- Mission
- What is Red Teaming and Penetration Testing
- Meeting structure
- Why you should join
- Tool development
- Events:
  - Red vs Blue
  - Capture the Flag (CTF) Competitions
  - Collegiate Penetration Testing Competition (CPTC)
- Ethics

Mission

- The primary goal of CDO is to encourage technical development and social networking outside of the classroom
- Help to develop skills in computer networking, Open Source Intelligence (OSINT), systems programming, and Linux administration through lectures and hands on experience

What is Red Teaming?

- Play the role of an adversary; attack systems and break defenses
- Encompases many different aspects of security ranging from network attacks to physical security
- Maintain access and hinder blue teams operations
- Pursue different avenues
- Assist with defense

Meeting Structure

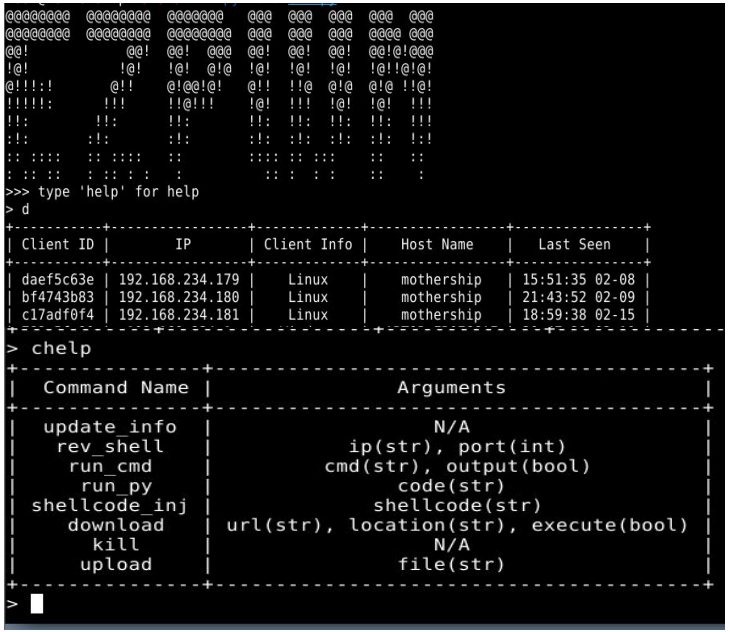
- Bi-weekly meetings on Tuesdays 7pm on discord
- Hands-on activities and theory
- XSS Lab
- SQLi Lab
- Tool Development Lab
- Introduction to Threat Intelligence
- Feel free to suggest topics you are interested in

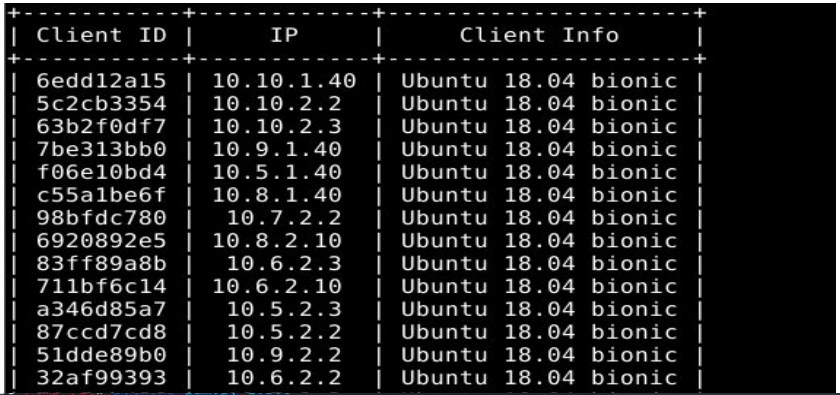
Why should I join?

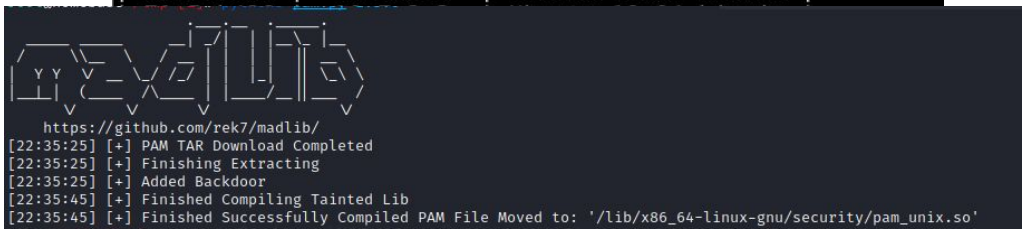
- Helps to build real world hands on experience
- Most events have recruiters, that are looking for skilled technical people
- Great way to network with employers and other students in different universities
- It's a lot of fun :)

Tool Development

- Competitions are a great way to test out new tools
- Developing you own tooling and implants is a great way to learn about development, networking, and operating systems!







Upcoming Competitions and Events

Red vs. Blue

- Given access to machines before competition
- Maintain access and hinder operations for Blue Team
- Great way to learn about Windows, Linux, and Firewall infrastructure
- Dates:
  - University at Buffalo Lockdown
    - University: 5/1

Capture the Flags

- A capture the flag contest is a competition designed to challenge its participants to solve computer security problems
- RITSec - TBD
- Interested? Let us know, we can find more!

What is CPTC?

- **Main Objective:** Improving the security posture of a fictitious organization and reporting on risks in a manner that is similar to a real professional environment
- **Theme:** The Collegiate Penetration Testing Competition provides a vehicle for up and coming cyber security student teams to build and hone the skills required to effectively discover, triage, and mitigate critical security vulnerabilities

What is CPTC?

- **Environment:** This competition is unique in offering a simulated environment that mimics real-world networks
- **Last Seasons Theme:** CTPC 2020 focused on Industrial Control Systems (ICS)
- Date yet to be announced for 2021

What will our CPTC Team look like?

- **Team Size:** a team can consist of 3-8 people (max 6 people to actually compete, 2 may be used for alternates)
- **Composition:** We are working towards filling positions with individuals that have expertise in the following:
  - Windows
  - linux
  - Web Application
  - Penetration Testing
  - Report Writing and presentation skills

Ethics

- Our activities will be done with a set goal and scope
- Members are obligated to act accordingly with laws and school rules. Any indication that a member is doing something unethical may lead to the individual being removed from the team or banned from meetings

Contact

- Discord Meeting Channel: UA_CDO #red-team
- Captain: Raphael Karger, rkarger@albany.edu
- Co-Captain: Mike Antoniades, mantoniades@albany.edu, d3#2757

Questions?