
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
- Encompasses 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!

```

#####  #####  #####  ###  ###  ###  ###  ###
#####  #####  #####  ###  ###  ###  #####  ###
@!      @!      @!  @!  @!  @!  @!  @!  @!
!@!      !@!  !@!  @!  !@!  !@!  !@!  !@!
@!!!!      @!!  @!@!@!  @!!  !!@  @!@  @!@  !!@
!!!!:      !!!  !!@!!!  !@!  !!!  !@!  !@!  !!!
!!:      !!:  !!:  !!:  !!:  !!:  !!:  !!:
!::      !::  !::  !::  !::  !::  !::  !::
::  ::::  ::  ::::  ::  ::::  ::  :::
:  ::  ::  ::  ::  ::  ::  ::  ::

>>> type 'help' for help
> d
+-----+
| Client ID |      IP      | Client Info | Host Name | Last Seen |
+-----+
| daef5c63e | 192.168.234.179 | Linux      | mothership | 15:51:35 02-08 |
| bf4743b83 | 192.168.234.180 | Linux      | mothership | 21:43:52 02-09 |
| cl7adf0f4 | 192.168.234.181 | Linux      | mothership | 18:59:38 02-15 |
+-----+

> chelp
+-----+
| Command Name | Arguments |
+-----+
| update_info  | N/A       |
| rev_shell   | ip(str), port(int) |
| run_cmd     | cmd(str), output(bool) |
| run_py      | code(str) |
| shellcode_inj | shellcode(str) |
| download    | url(str), location(str), execute(bool) |
| kill        | N/A       |
| upload      | file(str) |
+-----+

> █

```

Client ID	IP	Client Info
6edd12a15	10.10.1.40	Ubuntu 18.04 bionic
5c2cb3354	10.10.2.2	Ubuntu 18.04 bionic
63b2f0df7	10.10.2.3	Ubuntu 18.04 bionic
7be313bb0	10.9.1.40	Ubuntu 18.04 bionic
f06e10bd4	10.5.1.40	Ubuntu 18.04 bionic
c55a1be6f	10.8.1.40	Ubuntu 18.04 bionic
98bfcd780	10.7.2.2	Ubuntu 18.04 bionic
6920892e5	10.8.2.10	Ubuntu 18.04 bionic
83ff89a8b	10.6.2.3	Ubuntu 18.04 bionic
711bf6c14	10.6.2.10	Ubuntu 18.04 bionic
a346d85a7	10.5.2.3	Ubuntu 18.04 bionic
87ccd7cd8	10.5.2.2	Ubuntu 18.04 bionic
51dde89b0	10.9.2.2	Ubuntu 18.04 bionic
32af99393	10.6.2.2	Ubuntu 18.04 bionic

```

https://github.com/rek7/madlib/
[22:35:25] [+] PAM TAR Download Completed
[22:35:25] [+] Finishing Extracting
[22:35:25] [+] Added Backdoor
[22:35:45] [+] Finished Compiling Tainted Lib
[22:35:45] [+] Finished Successfully Compiled PAM File Moved to: '/lib/x86_64-linux-gnu/security/pam_unix.so'

```

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 Antoniadou, mantonadiades@albany.edu, d3#2757

Questions?