Red Team Informational

Welcome to the first Red Team meeting!

Summary

- Mission
- What is Red Teaming and Penetration Testing
- Lecture 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?

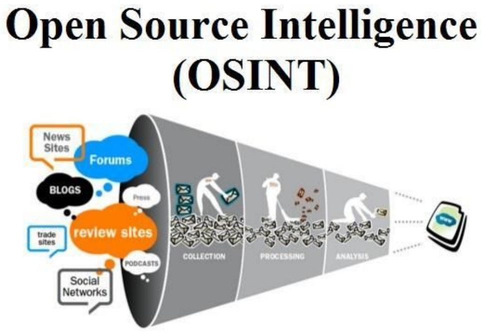
- Play the role of an adversary; attack systems and break defenses
- Encompases many different aspects of security ranging from network attacks to physical security
- Maintain access and hinder blue teams operations
- Pursue different avenues
- Assist with defense

Penetration Testing

- An aspect of red-teaming
- A form of legal hacking usually done by a pentesting/consulting company to find vulnerabilities and issues regarding the client’s infrastructure.
- For example, company A will approach Fire Eye and pay them to have their team of pen testers attack their company to find any ways they can infiltrate company A
- Based on Rules of Engagement

How will our lectures be structured?

- After a brief lecture we will give you access to a virtual machine were you will test out what you have learned!
- Tentative Schedule:
  - Penetration Testing Methodology 9/18
  - Network Reconnaissance and OSINT 9/25
  - Web Application Attacks 10/2
  - Bug Bounty 10/9
- If you want to present a topic or have a suggestion let us know!!



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 :)

amazon

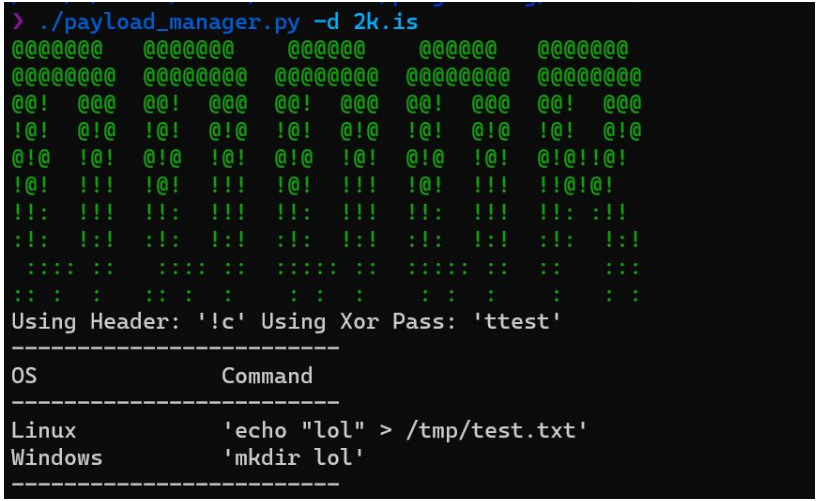
Deloitte.

Booz | Allen | Hamilton®

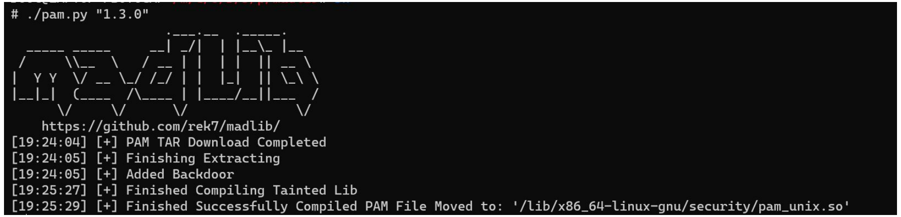
BOEING®

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!



```
❯ ./payload_manager.py -d 2k.is
@@@@@@@@   @@@@@@@@    @@@@@@@    @@@@@@@   @@@@@@@@
@@@@@@@@@  @@@@@@@@@  @@@@@@@@@  @@@@@@@@@  @@@@@@@@@
@@!   @@@  @@!   @@@  @@!   @@@  @@!   @@@  @@!   @@@
!@!   @!@  !@!   @!@  !@!   @!@  !@!   @!@  !@!   @!@
@!@   !@!  @!@   !@!  @!@   !@!  @!@   !@!  @!@!!@!
!@!   !!!  !@!   !!!  !@!   !!!  !@!   !!!  !!@!@!
!!:   !!!  !!:   !!!  !!:   !!!  !!:   !!!  !!: :!!
:!:   !:!  :!:   !:!  :!:   !:!  :!:   !:!  :!:   !:!
 :::: ::    :::: ::   ::::: ::   ::::: ::   ::    :::
:: :  :    :: :  :     : :  :     : :  :     :    : :
Using Header: '!c' Using Xor Pass: 'ttest'
--------------------------
OS                 Command
--------------------------
Linux              'echo "lol" > /tmp/test.txt'
Windows            'mkdir lol'
--------------------------
```



```
# ./pam.py "1.3.0"
                 .___.__  ._______.
  _____ _____    __| _/|  | |__\_ |__
 /     \\__  \  / __ | |  | |  || __ \
|  Y Y  \/ __ \_/ /_/ | |  |_|  || \_\ \
|__|_|  (____  /\____ | |____/__||___  /
      \/     \/      \/              \/
    https://github.com/rek7/madlib/
[19:24:04] [+] PAM TAR Download Completed
[19:24:05] [+] Finishing Extracting
[19:24:05] [+] Added Backdoor
[19:25:27] [+] Finished Compiling Tainted Lib
[19:25:29] [+] 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: 10/17
    - High School: 12/5
  - SUNY Albany Great Dane Defense Competition
    - CDOs own Red vs Blue competition: 11/14

UNIVERSITY AT ALBANY
AND
CYBER DEFENSE ORGANIZATION
GREAT DANE DEFENSE COMPETITION
A COMPETITION OUT OF THIS WORLD
NOVEMBER FOURTEENTH

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
- **Seasons Theme:** CTPC 2020 is focused on Industrial Control Systems (ICS)

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

What if we get to many applicants?

- In the case of multiple applicants for a position with limited spots or a full team we will arrange a tryout for the contested roles.
- Tryouts will be tailored to the role ie, technical tryouts may be a ctf, while reporting writing ones may have the applicants write a report within a specified amount of time

CPTC Critical Dates

- Apply on or before: 9/24
- Competition: October 31st - November 1st
- **Applications:** https://forms.gle/oAj22SsBUK48P1FF8

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

Questions?