WiCyS 2023

#role-join WiCyS
#signin wicys

WiCyS
women in cybersecurity

ROCHESTER INSTITUTE OF TECHNOLOGY
STUDENT CHAPTER

Schedule!

Weekly Meetings

Wednesdays at 7:00 PM in GCI Security Lab Golisano Hall 2740

Official WiCyS Website

RIT WiCyS Website

WiCyS@RIT 2022-2023
Spring Semester Schedule
Meetings at 7:00pm in GCI Security Lab Golisano Hall 2740

25 January	Semester Goals
1 February	Intro to Red Team
8 February	Maximize your College Experience
15 February	Building a CTF Challenge
22 February	SOC Talk
1 March	Preparing for Interviews
8 March	Midterm Madness
15 March	No Meeting - WiCyS Conference
22 March	Homelabbing with Ashley
29 March	Making the Most of Your Co-op
5 April	Intro to Pentesting
12 April	The Art of Fiddling
19 April	Eboard Elections
26 April	Spring Final Fun

WiCyS
women in cybersecurity

ROCHESTER INSTITUTE OF TECHNOLOGY
STUDENT CHAPTER

Announcements

- **Ops Program is recruiting!**
  - Excellent opportunity to build technical knowledge
  - Signup link is on the RITSEC discord in #annoucements
  - Deadline to apply is **next Friday, February 3, 2023.**
- **John Deere Cyber Tractor Challenge**
  - "John Deere is hosting a week-long invitational (**June 26-30**) event for students to take cybersecurity classes and perform assessments on our autonomous embedded technologies"
  - **All expenses paid**: **Free Travel, Free Stay, Free Food**
  - Deadline to apply is **March 13, 2023**

Announcements (Pt. 2)

- **WiCHacks!!!**
  - “A women and gender-minorities 24-hour hackathon hosted by Women in Computing at RIT. A hackathon is a collaborative programming event in which participants create an app, website, game, or other piece of software over the course of the event.”
  - Open to all skills levels, it’s an excellent opportunity to learn and win cool prizes and free swag
  - Takes place **March 4-5, 2023**
- **Movie Night!**
  - Fill out the when-to-meet for next week in #wicys-announcements

Who are we?

Michael “Atilla” Vaughan

Jason Howe

Ashley Nikirk

What is Red Team?

What makes a good red teamer?

What goes into tool dev?

What is Red Team?

- Group of people with an Offensive Security Mindset
- Given a task of breaking into a system or network
    - Generally trying to test the blue team/defenders
- Not focused on being quiet, but not being really loud either
- Will deploy on Windows, Linux, and Networking Devices
- Lateral Movement
- Lots of C2s, implants
- Persistence, Persistence, Persistence
    - One is None and Two is One

Making A Good Red Teamer

- Be Creative
- Be Committed
    - Be reliable
- Be Collaborative
- Be Curious

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.” - Sun Tzu

What Goes Into Tool Dev?

- Get inspiration for what you want to write
  - Look at MITRE ATT&CK framework and read APT reports
  - Red Team tool ideas repo
  - Watch conference talks
  - Threat Intelligence Blogs and #infosec
- Pick a programming language
  - Just start writing
  - Ask older people for help when you get stuck

MITRE ATT&CK™

Example: Father

- Question: How does a rootkit work?
  - Googled this (Found blogs and MITRE ATT&CK framework)
    - Found tons of information
  - Kernel vs User mode
  - Function Hooking

MITRE ATT&CK™

Example: Father

MITRE ATT&CK™

- Process
  - Choose a type (Kernel or User mode)
  - Learn to hook a function
  - Find important functions to hook
    - Source code / Google
    - Reverse engineering (Windows)
- **Write down everything you don't know**
  - Research what is on the list when you have time

Competitions

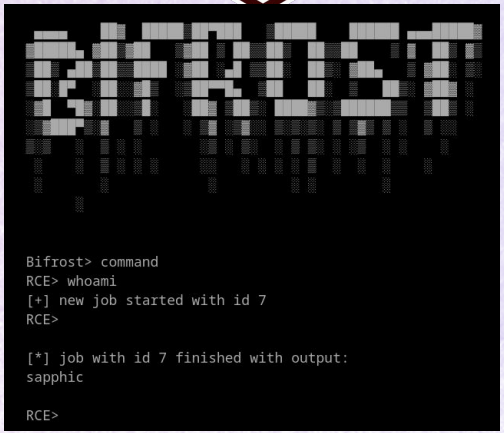
- Need to be fair to all teams
- Break schedule
    - Need to confirm every attack with the Red Team Chief(s)
- Never intentionally brick things
    - Respect Black Team
- Show up on time to deploy and comp
- Test your tools before you deploy ->

Tool Demos

Tool Demo: Bifrost

- Flasked based HTTPS C2 with a malleable agent
  - Async reverse shell
  - Built-in PWNboard

Bifrost PWNboard								
Hosts	Team 1	Team 2	Team 3	Team 4	Team 5	Team 6	Team 7	Team 8
MySQL	10.1.2.3	10.2.2.3	10.3.2.3	10.4.2.3	10.5.2.3	10.6.2.3	10.7.2.3	10.8.2.3
FTP	10.1.2.4	10.2.2.4	10.3.2.4	10.4.2.4	10.5.2.4	10.6.2.4	10.7.2.4	10.8.2.4
HTTP Dev	10.1.2.10	10.2.2.10	10.3.2.10	10.4.2.10	10.5.2.10	10.6.2.10	10.7.2.10	10.8.2.10
HTTP Web	10.1.2.2	10.2.2.2	10.3.2.2	10.4.2.2	10.5.2.2	10.6.2.2	10.7.2.2	10.8.2.2
SSH/ICMP 1	10.1.1.10	10.2.1.10	10.3.1.10	10.4.1.10	10.5.1.10	10.6.1.10	10.7.1.10	10.8.1.10
SSH/ICMP 2	10.1.1.40	10.2.1.40	10.3.1.40	10.4.1.40	10.5.1.40	10.6.1.40	10.7.1.40	10.8.1.40
LDAP/DNS	10.1.1.60	10.2.1.60	10.3.1.60	10.4.1.60	10.5.1.60	10.6.1.60	10.7.1.60	10.8.1.60
WinRM 1	10.1.1.70	10.2.1.70	10.3.1.70	10.4.1.70	10.5.1.70	10.6.1.70	10.7.1.70	10.8.1.70
WinRM 2	10.1.1.80	10.2.1.80	10.3.1.80	10.4.1.80	10.5.1.80	10.6.1.80	10.7.1.80	10.8.1.80



Red Team Story Time

Questions