Carleton
Cyber
Security
Club

Week 0: Introduction

Warning:

- This is for educational use only
- Don’t use it for other things or bad things will happen

Topics:

- Scanning
- Web Applications
- Password Cracking
- System Attacks
- Binary Exploitation
- Wireless Attacks
- Sniffing/Spoofing
- Post Exploitation
- IOT Device Security
- Defensive Security

Scanning:

- Tools: Nmap, ping, fping, masscan, netdiscover
- Focus: Correct Usage, and Vulnerability Analysis

- UDP vs TCP
- Ports and Services
- Being more specific for better results

- Timeline: Week 1

Web Applications:

- Tools: Dirbuster, SQLMap, Burpsuite, …
- Focus: Sql Injection, XSS, Broken Authentication and Session Management, Insecure Direct Object References, Cross Site Request Forgery, Misconfigurations, Insecure Cryptographic Storage, Redirect and Forwarding Misconfigurations, Insufficient TCP Protection (OWASP Top 10)
- Timeline: Week 2+

Password Cracking:

- Tools: John the Ripper, Hydra, Hashcat, ...
- Focus: Correct Usage

- Timeline: Week 1 or 2

System Attacks:

- Tools: Metasploit, Meterpreter, ...
- Focus: Vulnerabilities of different OS’s, and services, Privilege Escalation
- Timeline: Week 3

Binary Exploitation:

- Tools: gdb
- Focus: Buffer Overflows, Floating Point Errors, Memory Errors, Privilege Escalation
- Timeline: Week 4+

Wireless Attacks:

- Tools: ...
- Focus: Purely theoretical

- Timeline: Week 5+

Sniffing and Spoofing:

- Tools: Wireshark
- Focus: Man in the Middle Attacks, MAC spoofing, traffic interception
- Timeline: Week 6+

Post Exploitation:

- Tools: ...
- Focus: the bad and nasty (Purely Theoretical)

- Timeline: Week 7+

IOT Device Security:

- Tools: ...
- Focus: TBD

- Timeline: Week 8+

Defensive Security:

- Tools: ...
- Focus: Protecting ourselves from these attacks

- Timeline: Week 9+

Challenge/Hackathon:

- Tools: ...
- Focus: Completing a series of challenges for a prize
- Timeline: Week 10+