Practical Penetration Testing 101

Look mom I’m a hacker now!

Words of warning

- Anything you do to a remote system without authorization is illegal
- Use common sense
- Federal prison is bad

Overview of Today

- Brief overview of the cyber kill chain
- We will be attempting to exploit a live system and relate that back to the cyber kill chain

Cyber Kill Chain

1- Reconnaissance

- Scans will be performed on a target’s network
- Use tools such as nmap
- Osint- Open-source intelligence

  Scanning Social media, Google Hacking, ect.

2 - Intrusion

- This is a point of entry for an attack
- Most commonly done through phishing or MiM attack

3 - Exploitation

- This is where an attacker will attempt to exploit a physical system on the network beyond the perimeter
- The attacker will use the system they are on to pivot to other boxes on the network

4 - Privilege Escalation

- An attacker will use vulnerabilities/misconfigurations on a box to gain “root” or administrator access
- All about elevating the attackers permissions, for example on a windows network the main goal would be domain controller

5 - Lateral Movement

- An attacker will then try to pivot across the network to other boxes and other subnets
- The attacker will also look out for sensitive PII

6 - Obfuscation

- Naturally, the attacker will try to hide their presence
- They will use timestoping, redirect logs, and removing data to do so

7 - Denial of Service

- Next an attacker will bring down the entire network
- This is done because it can cause harm to the infiltrated organization

  Uptime = $$$

  Imagine if this was done to Amazon

8 - Exfiltration

- An attacker will then cover their tracks and exit the network with all the stolen information
- What happens with this information depends on the attacker
- The attacker may leave behind backdoors

Live Demo

Now the fun part!