Cyber Offense

GenCyber

Kailynn

Jordan

Hacker Narrative

A hacker group has successfully infiltrated the GenCyber network, extracted data, and corrupted multiple workstations. As a Cybersecurity Professional, you are responsible for finding the hacker group, figuring out what data has been removed, determining what machine(s) have been corrupted, reporting what happened, and providing a timeline.
But before you can tackle the situation, you must earn your Cybersecurity Professional Patches by going through extensive training to prepare you for the challenge ahead.

Why this Course is Essential

- You'll be able to perform a vulnerability assessment. (Which you'll perform for the GenCyber Network)
- Learn basic linux commands.
- Learn how to navigate Kali Linux to find out information about machines on your network.
- Apply the basic hacker methodology to understand how a full cycled attack is performed from reconnaissance to covering your tracks.

What is Cyber Offense AKA Red Teaming

The act of exploiting vulnerabilities and produce evidence alongside its report. Can exploit technical weaknesses within an organization's network.

Benefits of Pen-Testing

- Testing cyber defense-capabilities.
- Revealing vulnerabilities within computers, networks and applications.
- Finding security holes and plugging them before an attacker can take advantage of them.
- Supporting effective risk management by showing the real risk with the vulnerabilities encountered.

Tools

- Virtual Machine (Cyberlab)
- Kali Linux
- Metasploitable 2
- Network Mapper (Nmap)
- DVWA (Damn Vulnerable Web App)
- Metasploit

Tools

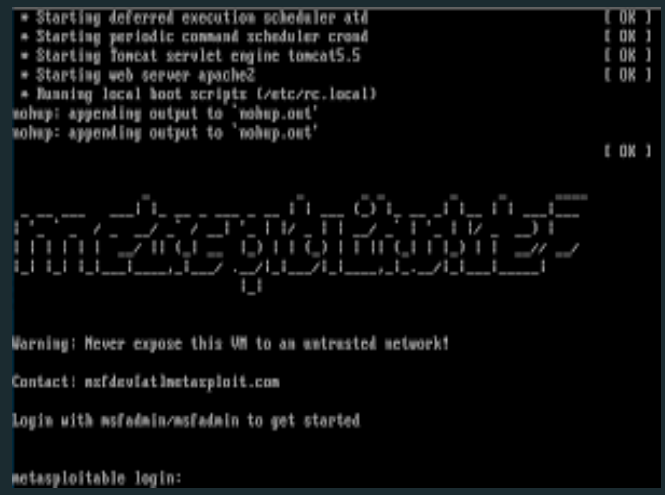
Kali Linux

Used for pentesting and to test skills.

DVWA

Damn vulnerable web app is a web application to get a better understanding on how to secure web apps.

Metasploitable 2



A vulnerable machine that you can exploit.

Basic Hacker Methodology

- Reconnaissance
- Scanning/Enumeration
- Gaining Access
- Maintaining Access
- Clear Tracks

Reconnaissance

Information gathering stage, this is where we collect as much information possible on our target.

Passive

- Gather background information through social media, public websites.

Active

- Scan Networks, Enumerate Targets, Scan for Vulnerabilities.

Activity:
Demo: Passive

Basic Linux Commands

01	**Command: ls**	• List files and directories.
02	**Command: clear**	• Clears terminal.
03	**Command: ifconfig**	• Interface Configuration. • Displays current ip address, netmask and broadcast address.
04	**Command: netdiscover**	• Scans for live host in network.
05	**Command: nmap [ip address]**	• Gives you information about your host that your scanning. • **Hint**: In dept information about services add: nmap -sV -O [ip address] (-sv scans services & -O scans operating system)

Scanning/Enumeration

Deeper than reconnaissance, being's vulnerability assessment.

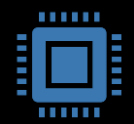
Port Scanning (Scan for information: Look for open ports, Services running)

Vulnerability Scanning (Check for weaknesses)

Activity:
Demo: Port Scanning

Gaining Access

Begin exploit based on information gather from previous research



This is where you now have access to the system by using various methods and tools.

Activity:
Demo: Exploit Port 80

Maintaining Access

The task here is to ensure access within the vulnerability that was exploited. This can be done by adding

- Backdoor
- Rootkit
- Trojans
- Malicious Files

Clear Tracks

DESTROY EVIDENCE OF TRACKS BY

DELETING VALUE OF LOGS

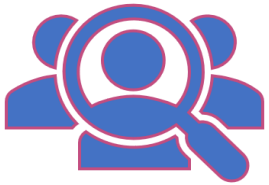
UNINSTALLING APPLICATIONS

DELETING FOLDERS CREATED

MODIFYING FILES

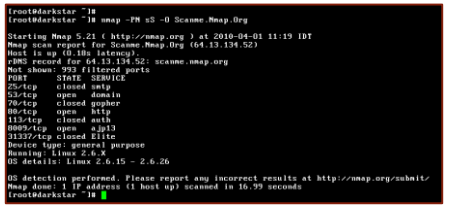
Lets Review

Reconnaissance



- Information Gathering
- Passive Reconnaissance
- Active Reconnaissance

Scanning & Enumeration



- Deeper Reconnaissance
- Vulnerability Scanning
- Example: Nmap Command

Gaining Access

- Exploiting Vulnerabilities
- Use previous information to exploit

Lets Review

Maintaining Access

- Ensure access to machine is maintained
- Example : Backdoor

Clear Tracks

- Destroy evidence of tracks
- Delete Logs
- Modify files
- Uninstall Applications

Task/Assignments

Beginners: Perform a Vulnerability Assessment

Directions Part 1:

1. Perform a vulnerability scan in search for weaknesses within Metasploitable 2
2. What is the IP address of Metasploitable 2
3. Port scan, look for open ports and services running. List 4 Ports that are open.
4. Pick 3 ports that are open: research what the network protocols do
   (For example FTP port 21: File Transfer Protocol)

Advanced: Exploit Metasploitable 2 Machine

Directions Part 2:

1. Use Metasploit to exploit the Metasploitable 2