Overview

Cyber-attacks, which can take the form of Hacking websites, Man in the Middle (MITM), Denial of Service (DOS), and Phishing Emails, highlight the urgent need for prevention.

Team Responsibilities

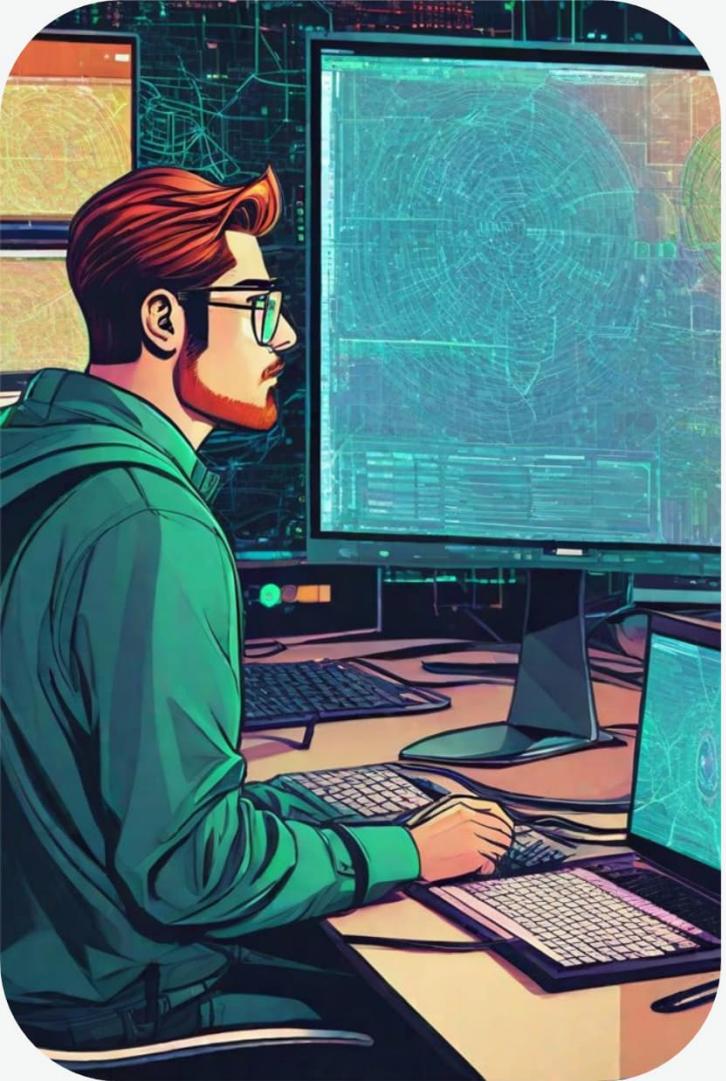
Attack 1: Ivan – Hacking Mr. Robot

Attack 2: Ozzy - MITM

Attack 3: Jordan - DoS and DDoS Simulations

Attack 4: Alpha - Phishing and Social Engineering

Attack 4: Largo - Mitigation Strategies



Hacking Mr. Robot

The Mr. Robot VM is a purposely built vulnerable environment that simulates real-world scenarios.

It is inspired by the TV series "Mr. Robot" and contains multiple vulnerabilities that can be exploited to practice and enhance penetration testing skills.

Steps:

1: Set Up Environment

2: Network Scanning

3: Enumeration

4: Vulnerabilities

5: Brute-force

6: Reverse Shell

Findings:

Finding	CVSS Score	Severity	Finding Name	Description	Recommendation
1	9	High	HTTP (80/tcp) - Apache HTTPD	Open ports 80 and 443 running Apache HTTPD, potential entry points	Ensure Apache is up-to-date and configure security headers
2	8	High	SSL Info	Missing security headers and outdated SSL configurations	Update SSL/TLS settings and add security headers
3	6	Medium	WordPress Plugins	Various plugins including outdated versions	Regularly update all plugins and monitor for vulnerabilities
4	5	Medium	WordPress Themes	Multiple themes including outdated versions	Update themes and remove unused ones
5	8	High	Configuration Issues	Missing security headers and outdated PHP version	Update server configurations and PHP version
6	9	Critical	Credentials Found	Username and password retrieved (elliot/ER28-0652)	Change all passwords and review user access controls
7	5	Low	Directories/Files	Various sensitive directories and files exposed	Restrict access to sensitive directories and files

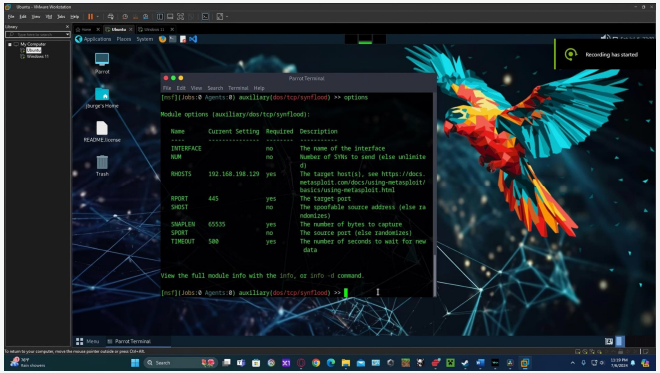
Man-In-The-Middle

- ✓ Attackers use man-in-the-middle attacks to harvest login credentials, personally identifiable information (PII), or other sensitive information and are, just like brute force attacks, used at the start of the cyber-attack lifecycle during the reconnaissance and exploitation stages.

- ✓ Address Resolution Protocol (ARP) poisoning and Domain Name System (DNS) spoofing are two common MITM attacks.

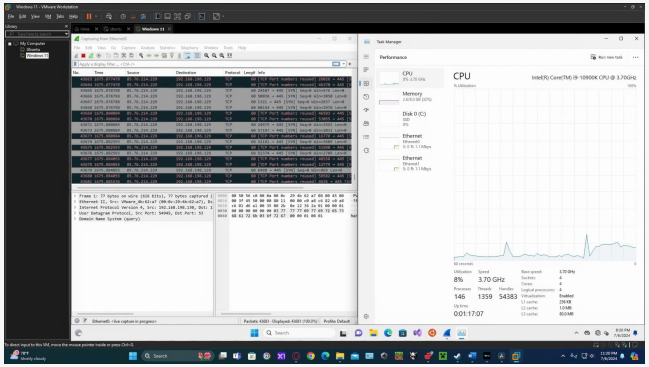
DoS and DDoS Simulations

- SYN FLOOD



Kali Machine

Target Machine



Phishing and Social Engineering

The fourth attack is creating a phishing email with the help of social engineering and a fake login page. Social Engineering is based on human interaction, where attackers use human emotions and tendencies against their victims. Phishing exploits are used to test employee vulnerability to fake/malicious emails.

Mitigation Strategies