**Name: Tanvir Ahmed**

**Date: June 12 2025**

**Phase 2. Identify Targets and Run Scans**

**Intro**

After thorough reconnaissance using various tools from the OSINT framework, the next step in a penetration test is active reconnaissance, especially port scanning.The goal is to identify live hosts and exposed services that may have vulnerabilities. In this scanning, Kali Linux machines would be utilized in collaboration with many different tools to figure out vulnerabilities and sites that can be targeted for exploitation.

**Network Scanning**

**Procedure:**

**Nnamp:**

In kali linux the very first thing to check on a target is to use nmap. Nmap is a network scanner used to discover hosts and services in a computer network. Using Nmap, we can scan Artemis by sending packets and in response, it will show the open ports in the host network.

For example if the command “nmap [www.artemis.com](http://www.artemis.com)” were typed in the terminal of Kali it would produce all the open ports of that site. This technique is called banner grabbing, it gathers information from computer systems in a network and its services. For more specific port commands like “nmap -sV -sC [www.artmeis.com](http://www.artmeis.com) -p 21” can be used to check the version and activeness of the service on port 21. The goal is to find potential vulnerability in services running on the network to determine possible attack vectors.

**Challenges:**

Nmap is time consuming, each command takes time to scan and sometimes the scan can be blocked by firewalls, especially on enterprise networks. Nmap scans can also be detected by IDS and IPS.

Ex:



**Telnet**

To access the command line interface of the remote computer, in this case Artemis, telnet is used. It helps manage files on the remote computer by mimicking as if you are physically there. Similar to nmap it can test and scan for services running on the host network and is useful for banner grabbing and enumeration.

**Challenges:**

Telenet is basic and lacks encryption, everything is shown in plain text and can be easily detected through log monitoring and IDS.

**Zenmap**

Zenmap is another tool that is very handy for port scanning. It has a Graphical User Interface unlike Nmap. It gives more control over configuration and scanning for TCP, UDP and specific port ranges. The tool utilizes Nmap to provide results on version of the service version, service state and network topology.

**Challenges:**

Zenmap is also time consuming and even slower than Nmap due to the GUI.

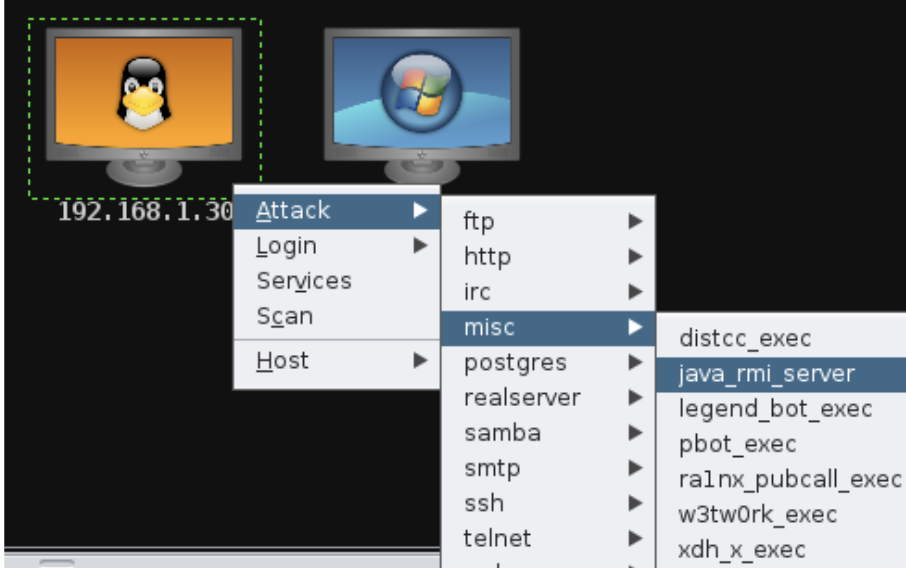
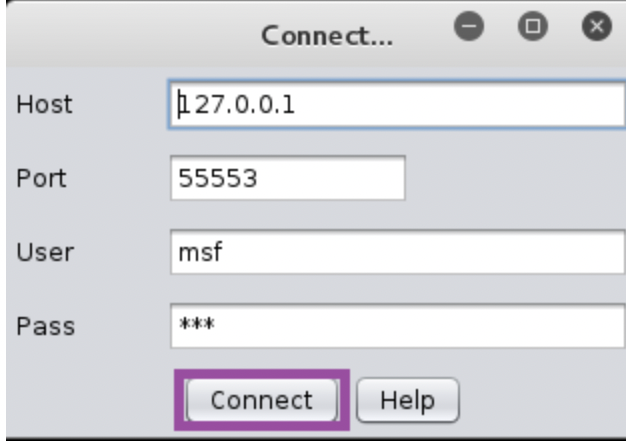
**Armitage**

Port scanning sometimes requires a more indepth active recon with metasploit. Using the command line interface, first, we need to go to the Armitage Directory. Armitage acts as a front end to run the metasploit through a user-friendly environment. After logging in using msfconsole, ports are scanned using command “db\_nmap” with the target network. Once the hosts are shown in the console, it is time to run metasploit for specific enumeration. An execution is created for the host network with the command “./armitage”, specifying the network, port, and username and password of msfconsole. The GUI of Armitage gives the flexibility to scan various services of the target to find attack vectors. It also allows attacks using various protocols including ftp, and http to gain credentials of the target network.

**Challenges:**

Armitage can be slow, especially when dealing with multiple services and scanning within the GUI.

Ex:



**Metasploit**

As discussed, Metasploit can be used through Telnet and Armitage, but Metasploit by itself is a powerful tool that can perform scanning. After logging in with msfadmin, it gives the ability to check which hosts are live in the target subnet. With the help of msfadmin, service scanning is possible with metasploit. For host discovery commands like “set RHOST target” are used for internal networks. After accessing the network other subnets can be scanned and enumerated. Metasploit can be tailored and scanned for specific vulnerabilities utilizing credentialed scan via msfadmin.

**Challenges:**

Metasploit is slower than Nmap, especially for large networks. It also lacks advanced scanning options and can be detected by IDS/IPS.

**Conclusion:**

With port scanning and identifying the target through the network using tools like Nmap, Zenmap, Armitage, Telent, and Metasploit, enough information can be gathered to move forward with exploitation. These tools help in identifying the vulnerabilities by revealing which ports are open, what services are running, and whether these ports have potential weaknesses. Once the scanning is complete, the attack vectors are determined to gain access to the target system.