## Lab 1: Nmap

### Scenario

A mid-sized IT company, TechSecure Solutions, is enhancing its cybersecurity posture and has tasked its internal security team to assess its network thoroughly. The team must identify open ports and running services across the organization's network as part of this assessment. This discovery will help them detect potential vulnerabilities and secure their systems proactively. The network infrastructure includes a mix of Linux and Windows servers, database systems, and IoT devices operating within a predefined subnet range. Additionally, the company uses IPv6-enabled devices to support their next-generation networking needs.

### Solution

As a professional, cybersecurity practitioner, you have been authorized by TechSecure Solutions to perform network scanning using Nmap, a versatile and powerful network scanning tool. Your task involves exploring various port and service discovery techniques offered by Nmap. Specifically, you will implement different scanning methods to identify open ports, running services, and the underlying protocols used within the network.

During a scanning process, Nmap's built-in scripts can be used to identify open ports and the services that are using them. It transmits tailored packets to the target host to achieve its goal and then checks the results. Nmap includes a variety of port scanning methods (TCP and UDP), OS and version detection, ping sweeps, and more.

**Note:** In this lab, the target IP address we use is **192.168.56.105** of Windows Server 2025. Do not use this lab IP address. Use your virtual machine IP address at the time when you are performing this lab.

|  |
| --- |
| 1. Turn on your **Windows Server 2025** and **PattotOS** virtual machines. Now, switch to the **ParrotOS** virtual machine. Open the **Terminal** and execute the following command: **sudo su** to run the programs as a root user. When prompted, enter your **root** password.    2. Execute the following command: **nmap -sn -PR [Target IP Address]**. The **-sn** disables port scan, and **-PR** performs ARP ping scan.  The scan results show that the target host is operational, as seen in the screenshot below. The host is active when an ARP response is received. ARP ping scan sends an ARP request to the target host.    3. Execute the following command: **nmap -sn -PU [Target IP Address]**. According to the scan findings, the target host is operational, as seen in the screenshot below. The **-PU** option does a UDP ping scan.  A UDP response indicates an active host. The UDP ping scan transmits UDP packets to the target host. Error messages like "host/network unreachable" or "TTL exceeded" may be returned if the target host is unavailable or offline.    4. We will now implement the ICMP ECHO ping scan. Execute the following command: **nmap -sn -PE [Target IP Address]**. The scan results show that the target host is operational, as seen in the screenshot below. The **-PE** carries out the ICMP ECHO ping scan.  An ICMP ECHO ping scan is the process of sending ICMP ECHO queries to a host. An ICMP ECHO reply will be returned if the target host remains alive. Finding active devices or figuring out whether the ICMP is getting through a firewall are two applications that benefit from this scan.    5. An ICMP ECHO ping sweep will now be used to find live hosts from various target IP addresses. Execute the following command: **nmap -sn -PE [Target Range of IP Addresses]**. According to the scan findings, the target host is operational, as seen in the screenshot below.  **Note:** In this lab task, we are scanning all the virtual machines under this subnet range of **192.168.56.2-192.168.56.254**.  The ICMP ECHO ping sweep makes ICMP ECHO requests to many hosts to locate active hosts from different IP addresses. If the host is still alive, it will respond with an ICMP ECHO.    6. Execute the following command: **nmap -sn -PP [Target IP Address]**. According to the scan findings, the target host is operational, as seen in the screenshot below. The -PP carries out the ICMP timestamp ping scan.  ICMP timestamp ping is a kind of ICMP ping in which the attacker requests a timestamp message to obtain the target host machine's current time.    7. Execute the following command: **nmap -sn -PM [target IP address]**. This **ICMP Address Mask Ping Scan** approach is an alternative to the usual ICMP ECHO ping scan, identifying whether the target host is alive, especially when administrators disable ICMP ECHO pings.    8. Execute the following command: **nmap -sn -PS [target IP address]**. This **TCP SYN Ping Scan** technique sends empty TCP SYN packets to the target host, and the ACK response means the host is active.    9. Execute the following command: **nmap -sn -PA [target IP address]**. The **TCP ACK Ping Scan** method sends empty TCP ACK packets to the target host; an RST response indicates that the host is active.    10. Execute the following command: **nmap -sn -PO [target IP address]**. The **IP Protocol Ping Scan** method delivers probing packets from several IP protocols to the target host. A host is active if any probe returns a response.    11. The process of discovering the target hosts in the target network utilizing various host discovery techniques is now complete. Close all open windows and record all of the data you have collected. |