**Lab 6-01 Perform Host Discovery using 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 its next-generation networking needs.

**Solution**

As a professional, ethical hacker or penetration tester, 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:** This lab uses the target IP **192.168.56.105** (Windows Server 2025) as an example. **Do not** use that IP on your network; use the IP address of your own virtual machine when performing the 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. |

**Lab 6-02: Explore Various Network Scanning Techniques using Nmap**

**Scenario**

A cybersecurity consultancy firm, CyberFort Solutions, has been hired by a retail company, RetailSecure Inc., to conduct a thorough security assessment of its internal network. The objective is to identify potential vulnerabilities by discovering open ports and running services within the organization's IT infrastructure. RetailSecure Inc. operates in a subnet range of 192.168.56.0/24, which includes servers hosting e-commerce platforms, payment gateways, and internal databases critical to its operations.

**Solution**

As a professional, ethical hacker or penetration tester, your task is to use Nmap to explore various network scanning techniques to identify open ports and services in the network. This will provide a detailed understanding of the services running on the organization's systems and help uncover potential entry points for attackers. The scan must include testing for different protocols and approaches, ensuring all aspects of the network are thoroughly evaluated.

Several built-in scripts in Nmap may be used to identify open ports and services using them during a scanning operation. It accomplishes this by sending the target host specially constructed packets and then analyzing the reply. Ping sweeps, OS detection, version detection, and other port scanning techniques (TCP and UDP) are all included in Nmap.

**Note:** In this lab, the target IP address we use is **192.168.56.106** 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. Start your **Windows 11** and **Windows Server 25** virtual machines. Now, switch to the **Windows 11** virtual machine. Open any browser and go to the following website link: [**https://nmap.org/download#windows**](https://nmap.org/download#windows). Click on the **nmap-7.95-setup.exe** to Namp executable file.    2. After a file is downloaded, go to the **Downloads** folder. Double-click on the **nmap-7.95-setup.exe** to start the installation process. Click the **Yes** button if the **User Account Control** pop-up appears.    3. Click on the **I Agree** button.    4. Select the **Npcap 1.79** check box. Then, click on the **Next >** button.    5. Click on the **Install** button.    6. Click on the **I Agree** button to install Npcap.    7. Click on the **Install** button to start the Npcap installation process.    8. Click on the **Next** > button.    9. Click on the **Finish** button. The Npcap installation is finished.    10. Click the **Next** > button to proceed with the Nmap installation process.    11. Select the check boxes of the **Start Menu** Folder and **Desktop Icon**. Then click on the **Next >** button.    12. Click on the **Finish** button.    13. Click on the Windows Search **Icon** on the **Desktop**, search for **zenmap** in the search field, and click on **Open**.    14. The **Zenmap** appears; enter **nmap -sT -v [Target IP Address]** in the **Command** field and click on the **Scan** button. The TCP connect/full open scan is carried out by the **-sT**, and the verbose output (which includes all hosts and ports) is enabled by the **-v**. All of the target machine's open TCP ports and services are shown in the scan results.    15. For further information about the scan findings. Click on the **Ports/Hosts** tab. Nmap shows the scan's Port, Protocol, State, Service, and Version.    16. Click on the **Topology** tab to access the topology of the target network, which includes the IP address you provided. Click on the **Fisheye** option to obtain a clear view of the topology.    17. Click the **Host Details** tab to access the TCP connect scan details.    18. Click the **Scans** tab to see the TCP connect/full open scan command. Also, click on the **Services** tab on the left-hand pane of the window. This tab shows a list of services. Any of these services, along with their open ports, can be used to connect to the target network or host.    19. In this sub-task, we shall perform a stealth scan/TCP half-open scan, Xmas scan, TCP Maimon scan, and ACK flag probe scan on a firewall-enabled machine to observe the result. We need to enable a **Windows Firewall** on the **Windows Server 2025** machine to do this.  20. Switch to **Windows Server 2025** virtual machine. Go to the **Control Panel** **→** **System and Security** **→** **Windows Defender Firewall** **→** **Turn Windows Defender Firewall on or off**, and enable **Windows Defender Firewall**. Then, click on the **OK** button, and after that, close the **Control Panel** window.    21. Switch back to the **Windows 11** virtual machine. In the **Command** field of **Zenmap**, enter **nmap -sS -v [Target IP Address]** and click the **Scan** button.  Stealth scan/TCP half-open scan is done with **-sS**, and verbose output (which includes all hosts and ports) is enabled with **-v**. The scan results show the target machine's open TCP ports and services.    22. As shown in the above steps from **14** to **19**, you can gather detailed information from the scan result in the Ports/Hosts, Topology, Host Details, and Scan tab. Similarly, enter **nmap -sX -v [Target IP Address]** and click the **Scan** button. The **-sX** option performs the Xmas scan, and the **-v** option allows for verbose output (including all hosts and ports). The scan results show that the ports are either open or filtered on the target machine, indicating that a firewall has been configured.    23. In the Command field, enter **nmap -sM -v [Target IP Address]** and click on the **Scan** button. The **-sM** option performs the TCP Maimon scan, and the **-v** option allows for verbose output (including all hosts and ports). The scan results display whether the target machine's ports are open or filtered, suggesting a firewall has been configured.    24. In the Command field, enter **nmap -sA -v [Target IP Address]** and click on the **Scan** button. The **-sA** option performs an ACK flag probe scan, and the **-v** option enables verbose output (which includes all hosts and ports). The scan results show that the target machine's ports are filtered.    25. Switch back to the **Windows Server 2025** virtual machine. Turn off the **Windows Defender Firewall** from the **Control Panel,** as shown in **step 20**.  26. Switch back to the **Windows 11** virtual machine. In the Command field of **Zenmap**, enter **nmap -sU -v [Target IP Address]** and click the **Scan** button. The **-sU** option performs a UDP scan, and the **-v** option allows for verbose output (including all hosts and ports). This scan could take around 15-20 minutes. The scan results show the target machine's open UDP ports and services. After that, close the **Zenmap** window.    27. You can create your scan profile or choose the default scan profiles available in Nmap to scan a network. Click on the **Windows Search** on the **Desktop**, search for **zenmap** in the search field, and click on **Open**.    28. To select the default scan profiles available in Nmap. Click on the **Profile** drop-down. Then, click on the **New Profile or Command**. If a User **Account Control** pop-up appears, click on the **Yes** button.    29. The **Profile Editor** window opens. In the **Profile** tab, under the **Profile Information** section, enter a profile name and type **Null Scan** into the **Profile name field**. Click on the **Scan** tab.    30. On the **Scan** tab, select **Null scan (-sN)** in the **TCP scan**. In the **Non-TCP scans,** select **None**. In the **Timing template,** select **Aggressive (-T4)**. Click the **Enable all advanced/aggressive options (-A)** check box. Click on the **Save Changes** button.    31. To scan the target **IP address**, put it into the **Target field** in **Zenmap's** main window. Select the **Null Scan** profile that you created from the **Profile** drop-down list. Then, click on the **Scan** button. Nmap scans the target and displays the results on the Nmap Output tab. This scan could take approximately 15-20 minutes. This will create a new profile and add it to the profile list.    32. In the **Command** field, enter **nmap -sY -v [target IP address]** and click on the **Scan** button. An INIT chunk is transmitted to the destination host. An INIT+ACK chunk response indicates the port is open, while an ABORT Chunk response indicates the port is closed.    33. In the **Command** field, enter **nmap -sZ -v [target IP address]** and click the **Scan** button. A COOKIE ECHO chunk is sent to the target host; no response means the port is open, and an ABORT Chunk response means the port is closed.    34. Enter **nmap -sV [Target IP Address]** in the Command field**.** Then, click on the **Scan** button. The **-sV** command detects service versions. The scan results appear, displaying the open ports and the version of services running on them.    35. In the **Command** field, enter **nmap -A [Target Subnet]** and click on the **Scan** button. The **"\*" (asterisk)** wildcard allows you to search an entire subnet or IP range. The **-A** enables aggressive scan. The aggressive scan option allows you to detect the operating system (-O), scan the version (-sV), scan the script (-sC), and trace the route. You should not use -A on target networks without permission.  Nmap scans the entire network and displays information for all scanned hosts, including open ports and services, device type, operating system details, etc.    36. Select an IP address **192.168.56.106** from the list of hosts in the left pane and click on the **Host Details** tab. This tab shows information about **Host Status**, **Addresses**, **Operating System**, **Ports used**, and **OS Classes**. Associated with the selected host. The output might differ when you perform this task.    37. This concludes the demonstration of using various Nmap scanning techniques to discover target open ports, services, service versions, device type, OS details, and other information about active hosts in the target network. Close all open windows and document all of the information gathered. |

**Lab 6-03 Perform OS Discovery using Nmap Script Engine (NSE)**

**Scenario**

A financial services company, SecureFinTech, conducts a detailed security assessment of its internal network to strengthen its defenses against cyber threats. The company manages a diverse IT infrastructure that includes Windows and Linux servers, network devices, and IoT systems. These systems host critical applications such as databases, payment gateways, and employee management tools. As part of this assessment, the company needs to identify the operating systems running on these devices to evaluate potential vulnerabilities and understand which exploits could be effective against them.

**Solution**

As a penetration tester, you have been tasked with performing OS discovery using Nmap's Scripting Engine (NSE). The goal is to determine the operating systems of active hosts in the predefined subnet range by employing both active and passive banner-grabbing techniques. This process will provide the company with detailed insights into the OS landscape of their network, enabling them to prioritize patching and system hardening efforts.

A substantial quantity of useful information may be extracted from the target system using Nmap and the Nmap Script Engine (NSE). NSE offers scripts that extract various helpful information from the target system in addition to Nmap commands. You may use NSE to gather information about a target system, including its OS, computer name, domain name, forest name, NetBIOS computer name, NetBIOS domain name, workgroup, and system time.

**Note:** In this lab, the target IP address we use is **192.168.56.106** 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.

**Prerequisites:** Before starting this lab, install the Active Directory domain services and SMB 1.0 on the Windows Server 2025. Use the documentation provided below to install all these on Windows Server 2025.

[**https://www.ibm.com/docs/en/storage-scale-bda?topic=support-install-configure-active-directory**](https://www.ibm.com/docs/en/storage-scale-bda?topic=support-install-configure-active-directory)

[**https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server**](https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server)

|  |
| --- |
| 1. Start your **PattotOS** and **Windows Server 2025** virtual machines. Now, switch to the **ParrotOS** virtual machine. To run the programs as a root user, open the **Terminal** and execute the following command: **sudo su**. When prompted, enter your **root** password.    2. Execute the following command: **nmap -A [Target IP Address]**. The scan results, open ports, running services, their versions, and the target details, such as the operating system, computer name, and NetBIOS computer name, are displayed in the **Host script results** section. Use the **-A** to run an aggressive scan. It takes around ten minutes for the scan to finish.      3. Execute the following command: **nmap -O [Target IP Address]**. The scan results show the name of the operating system operating on the target machine, details about open ports, and the services that are using the open ports. The **-O** isused to perform the OS discovery.      4. Execute the following command: **nmap --script smb-os-discovery.nse [Target IP Address]**. The scan results are shown under the **Host script results** section, along with the target OS, machine name, NetBIOS computer name, and other information. The **--script** outlines the custom script and **smb-os-discovery.nse:** tries to use the SMB protocol (ports 445 or 139) to find the OS, computer name, domain, workgroup, and current time.      5. This concludes the lab using Nmap to find the operating system installed on the target machine. Shut down all open windows and document all your collected data. |

## Lab 6-04: Scan beyond IDS Firewall using Various Evasion Techniques

**Scenario**

A healthcare organization, MediSecure Systems, is conducting a thorough security evaluation of its network infrastructure to assess the effectiveness of its Intrusion Detection System (IDS) and firewalls. These security mechanisms protect the organization's sensitive data, including electronic health records and patient information. However, MediSecure Systems knows that even the most robust security perimeters may have vulnerabilities that attackers could exploit. They have engaged your services as a professional, ethical hacker to identify and address these gaps.

**Solution**

Your task is to test the resilience of their IDS and firewall by performing network scans using various evasion techniques. The objective is to simulate how a skilled attacker might bypass these defenses to map the network and identify vulnerabilities. The target network resides in the predefined range of subnets. It includes a combination of web servers, database servers, and application servers protected by an IDS and firewalls configured with strict security rules.

Nmap provides many capabilities to help understand complex networks with activated security measures and facilitates workarounds for improperly put protections. Nmap may be used to deploy various strategies beyond the security features of firewalls and intrusion detection systems.

**Note:** In this lab, the target IP address we use is **192.168.56.108** of Windows 11. Do not use this lab IP address. Use your virtual machine IP address at the time when you are performing this lab.

**Prerequisites:** Before starting this lab, install Wireshark on Windows 11. Use the documentation provided below to install Wireshark on Windows 11.

**Download Link:** <https://www.wireshark.org/download.html>

**Documentation:** <https://www.stationx.net/how-to-install-wireshark/>

|  |
| --- |
| 1. Start your **PattotOS** and **Windows 11** virtual machines. Now, switch to the **Windows 11** virtual machine. Go to the **Control Panel** **→** **System and Security** **→** **Windows Defender Firewall** **→** **Turn Windows Defender Firewall on or off**, and enable **Windows Defender Firewall**. Then, click on the **OK** button, and after that, close the **Control Panel** window.    2. In the **Windows Search Bar,** type **Wireshark**. Click on the **Open**.    3. In this lab, we are selecting **Ethernet 2**. When you perform this lab in your virtual environment, it might be possible that there is a different network interface.    4. Switch to the **ParrotOS** virtual machine. Open the **Terminal** and execute the command, **sudo su,** to run the programs as a root user. When prompted, enter your **root** password.    5. Execute the following command: **nmap -f [Target IP Address]**. The **-f** switch splits the IP packet into tiny fragment packets.  You may still retrieve the results showing all open TCP ports and the names of the services using them, even if **Windows Defender Firewall** is enabled on the target machine, as shown in the screenshot below.    6. Switch to the **Windows 11** virtual machine. Wireshark has captured fragmented packets that you may inspect.    7. Switch to the **ParrotOS** virtual machine. Execute the following command: **nmap -g 80 [Target IP Address]**. In this command, you can use the **-g** or **--source-port** option to manipulate the source port. All open TCP ports and the names of the services that are using them are shown in the results.    8. Switch to the **Windows 11** virtual machine. In the Wireshark window, scroll-down, and you can observe the TCP packets indicating that port number 80 is used to scan other ports of the target host, as shown in the screenshot.    9. Switch to the **ParrotOS** virtual machine. Execute the following command: **nmap -mtu 8 [Target IP Address]**. The Maximum Transmission Unit (MTU) of this command is 8 bytes of packets, as indicated by the **-mtu** option.    10. Switch to the **Windows 11 machine** virtual machine. In the Wireshark window, scroll-down, and you can observe the fragmented packets having a maximum length of 8 bytes.    11. Switch to the **ParrotOS** virtual machine. Execute the following command: **nmap -D RND:10 [Target IP Address]**. In this command, **-D** performs a decoy scan, and **RND** generates random and non-reserved IP addresses (here, 10).    12. Now, switch to the **Windows 11** virtual machine. You can observe the packets displaying the various IP addresses in the source part of the Wireshark window by scrolling down.    13. Switch to the **ParrotOS** virtual machine. Execute the following command: **nmap -sT -Pn --spoof-mac 0 [Target IP Address]**. In this command, **--spoof-mac 0** represents randomizing the MAC address, **-sT** performs the TCP connect/full open scan, **-Pn** is used to skip the host discovery.    14. Switch to the **Windows 11** virtual machine. In the Wireshark window, scroll-down to observe the captured TCP.    15. This concludes the lab on how to use several evasion tactics in Nmap to get around IDS and firewall protection. Close all open windows and record all of the data you have collected. |

**Lab 6-05: Scan a Target Network using Metasploit**

**Scenario**

A company hires you to perform a penetration test of its network infrastructure. The company has a large network with multiple subnets and various services running on different machines. The objective of the penetration test is to identify vulnerabilities in the network and provide recommendations for improving the overall security posture.

**Solution**

As a penetration tester, scanning a target network using Metasploit is critical to the overall testing process. Metasploit can help identify open ports and services on the target network, which can be a starting point for further enumeration and exploitation.

Metasploit has a vast database of exploits and payloads that can be used to detect vulnerabilities in the target network. You can quickly determine if any target systems are vulnerable to known exploits by running Metasploit's pre-built modules.

|  |
| --- |
| 1. Open **Mate Terminal** on your Parrot OS and use the **sudo su** command to switch to the root user. Use the **msfdb init** command to initialize the database.    2. Use the **service postgresql start** command to start the PostgreSQL service. PostgreSQL is connected to the Metasploit initialized database. Use the **msfconsole** command to launch the Metasploit Framework.    3. Once Metasploit is started, use the **db\_status** command to check the database status; it is **connected to msf**.    4. Enter the **nmap -Pn -sS -A -oX Test 192.168.2.0/24** commandto scan the entire subnet.   * **-Pn flag** scans without DNS resolution (-n = no DNS resolution) because it is slow * **-sS flag** specifies the TCP SYN Scan * **-A flag** specifies the aggressive mode * **-oX Test flag** puts the XML output in a file named Test     5. Use the **db\_import Test** command to import and save the gathered data into the **Test** file.    6. Use the **hosts** command to list all the gathered hosts on the network.    7. Use the **services** command to list all the open ports and services running on them.    8. Use the **search** command to search for the keyword **portscan**. It lists all the modules that include the keyword **portscan**.    9. Use the **use auxiliary/scanner/portscan/syn** command to use this module for SYN scanning. Use the following commands to set the parameters;  **set PORTS 80**  **set RHOSTS target\_IP**  **set THREADS number\_of\_threads**  **run**  **Note:** PORTS specifies the target port. RHOSTS specifies the target host. THREADS specifies the number of threads used at a time. A thread is a unit of execution within a program that can carry out a particular task. In this case, the more threads you specify, the faster it scans. For example, specifying five threads will scan 5 hosts or 5 ports simultaneously, making the process faster.    10. Use the **back** command to exit the module. Use the **use auxiliary/scanner/portscan/tcp** command to use the TCP scanner module. Set the target host using the **set RHOSTS 192.168.2.100** command and enter **run** to execute.    11. Use the **use auxiliary/scanner/smb/smb\_version** command to find the SMB version. Use the following commands to set the parameters and run the scan;  **set RHOSTS target\_IP**  **set THREADS 10**  **run** |