Module 3

Lab 1: Perform Host Discovery

Lab Scenario

As a professional ethical hacker or pen tester, you should be able to scan and detect the active network systems/devices in the target network. During the network scanning phase of security assessment, your first task is to scan the network systems/devices connected to the target network within a specified IP range and check for live systems in the target network.

Lab Objectives

- Perform host discovery using Nmap

Overview of Host Discovery

Host discovery is considered the primary task in the network scanning process. It is used to discover the active/live hosts in a network. It provides an accurate status of the systems in the network, which, in turn, reduces the time spent on scanning every port on every system in a sea of IP addresses in order to identify whether the target host is up.

The following are examples of host discovery techniques:

- ARP ping scan
- UDP ping scan
- ICMP ping scan (ICMP ECHO ping, ICMP timestamp, ping ICMP, and address mask ping)
- TCP ping scan (TCP SYN ping and TCP ACK ping)
- IP protocol ping scan

Task 1: Perform Host Discovery using Nmap

Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Here, we will use Nmap to discover a list of live hosts in the target network. We can use Nmap to scan the active hosts in the target network using various host discovery techniques such as ARP ping scan, UDP ping scan, ICMP ECHO ping scan, ICMP ECHO ping sweep, etc.

1. By default, **Windows 11** machine is selected, click Parrot Security to switch to the **Parrot Security** machine. Login with **attacker**/**toor**.

If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

2. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

The password that you type will not be visible.

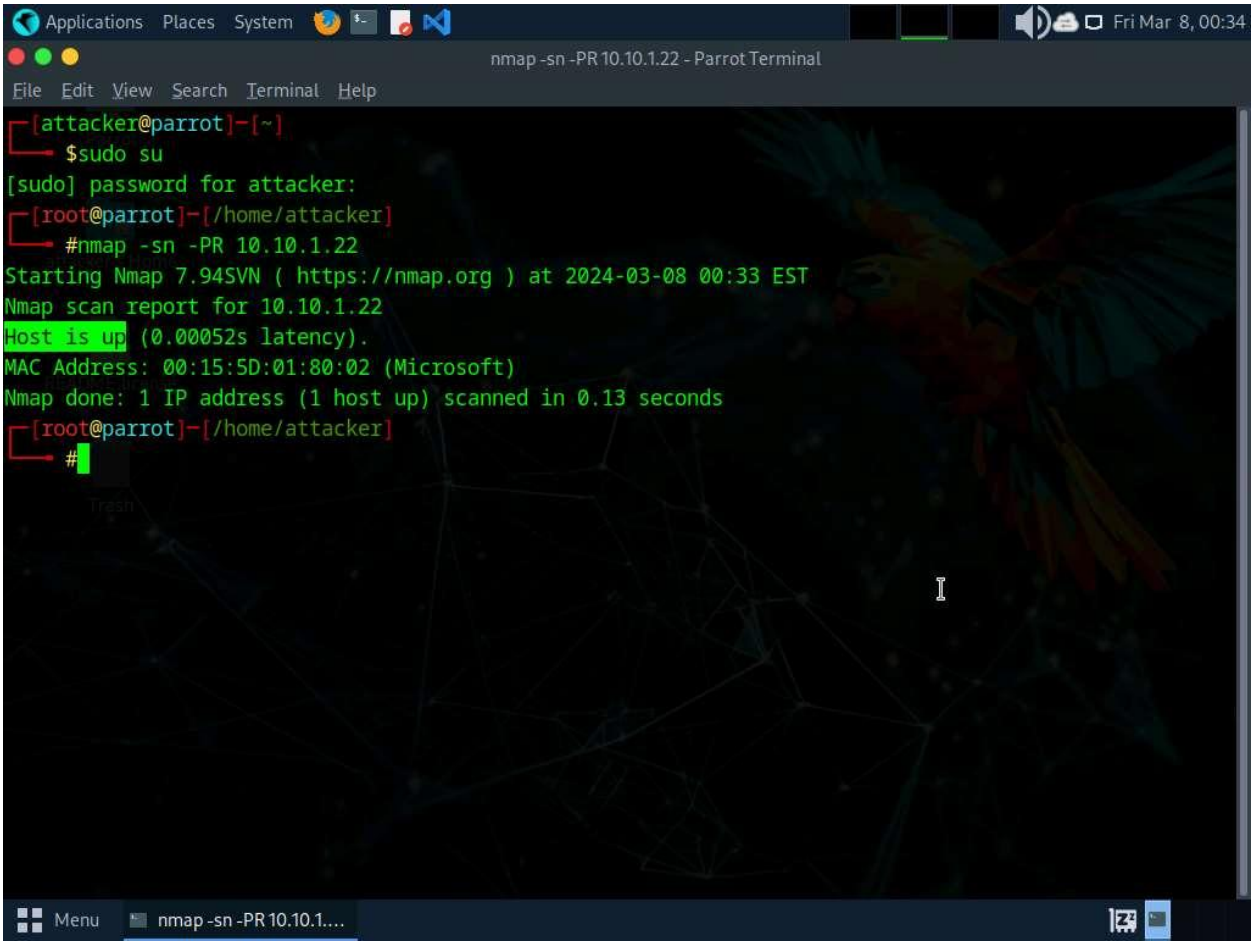
3. Run **nmap -sn -PR [Target IP Address]** command (here, the target IP address is **10.10.1.22**).

-sn: disables port scan and **-PR**: performs ARP ping scan.

4. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

In this lab, we are targeting the **Windows Server 2022** (**10.10.1.22**) machine.

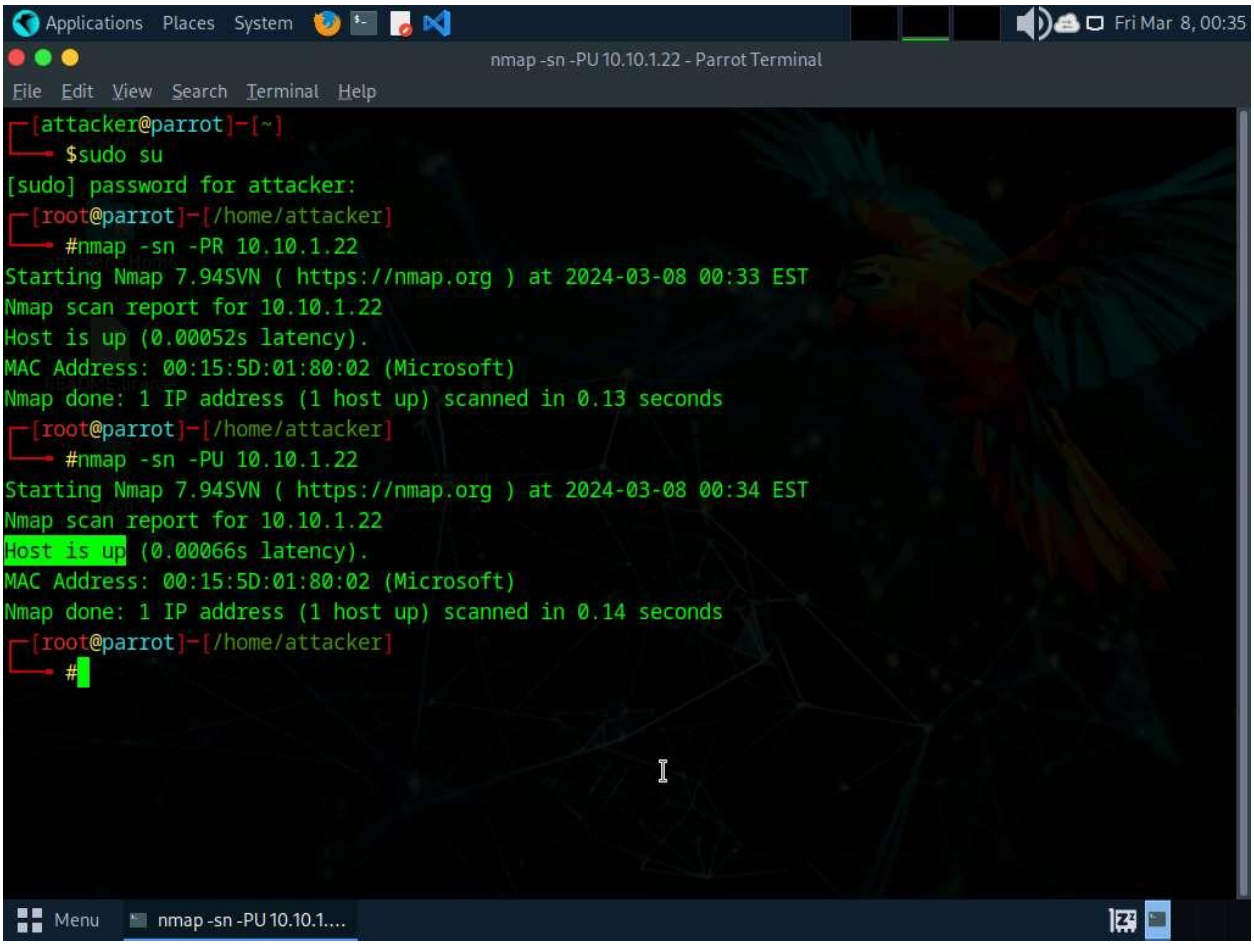
The ARP ping scan probes ARP request to target host; an ARP response means that the host is active.



5. Run **nmap -sn -PU [Target IP Address]** command, (here, the target IP address is **10.10.1.22**). The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

-PU: performs the UDP ping scan.

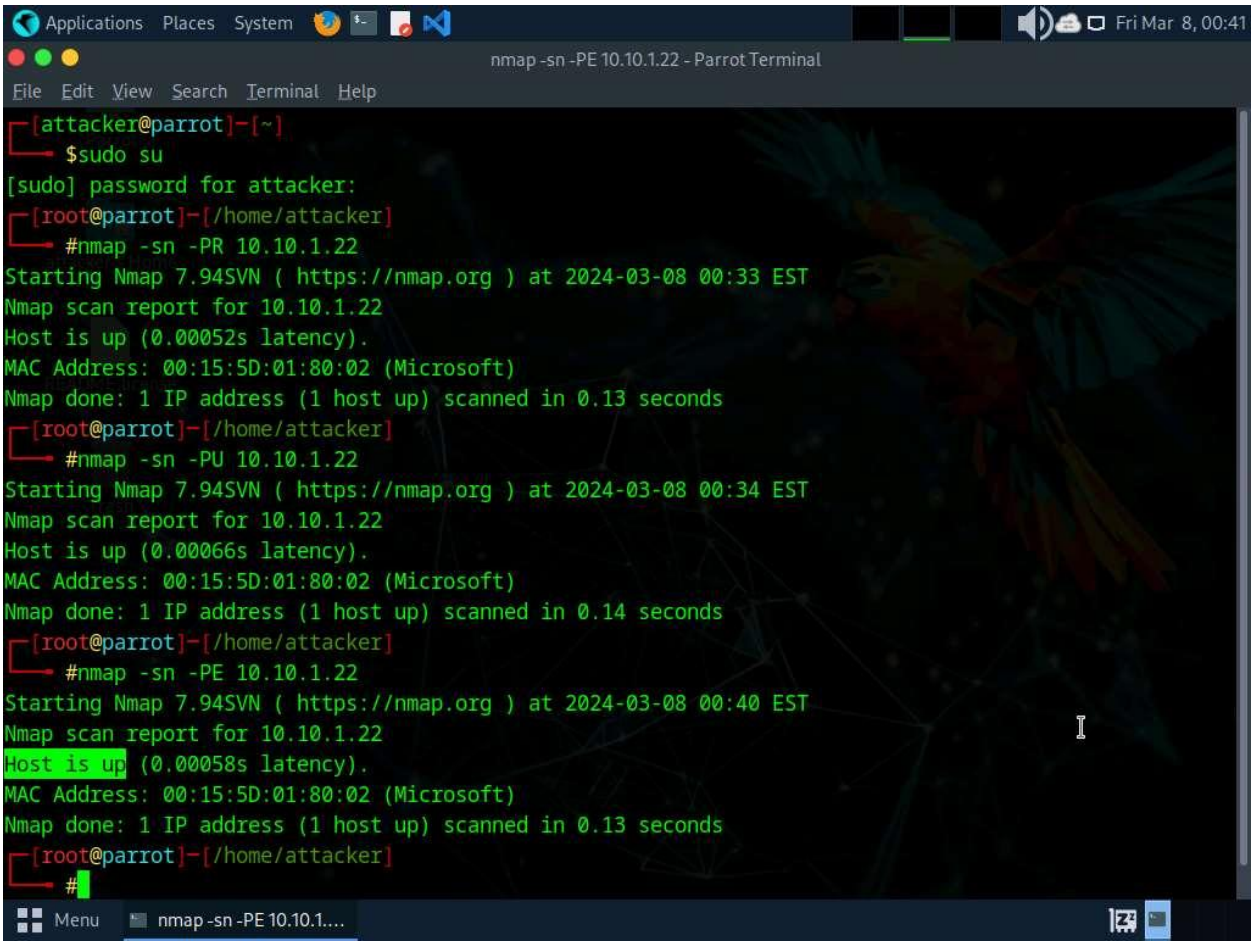
The UDP ping scan sends UDP packets to the target host; a UDP response means that the host is active. If the target host is offline or unreachable, various error messages such as “host/network unreachable” or “TTL exceeded” could be returned.



6. Now, we will perform the ICMP ECHO ping scan. Run **nmap -sn -PE [Target IP Address]** command, (here, the target IP address is **10.10.1.22**). The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

-PE: performs the ICMP ECHO ping scan.

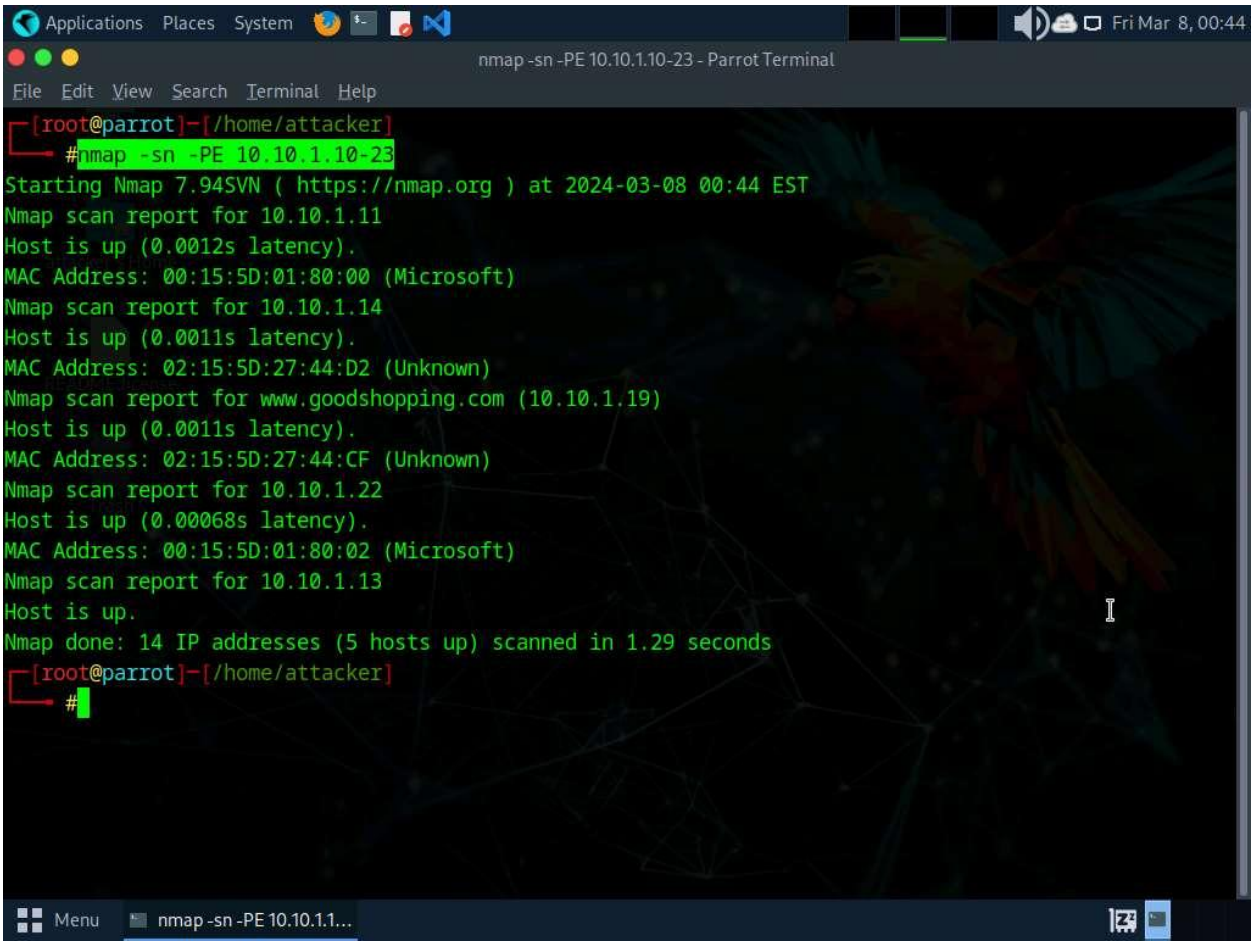
The ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the target host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if the ICMP is passing through a firewall.



7. Now, we will perform an ICMP ECHO ping sweep to discover live hosts from a range of target IP addresses. Run **nmap -sn -PE [Target Range of IP Addresses]** command (here, the target range of IP addresses is **10.10.1.10-23**). The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

In this lab task, we are scanning **Windows 11**, **Windows Server 2022**, **Windows Server 2019**, and **Android** machines. If Android machine is down, navigate to the **Resources** tab and select **Android**. Click **Power and Display** icon from the top section of the page, from the drop-down options, select **Reset/Reboot** and click **Yes**.

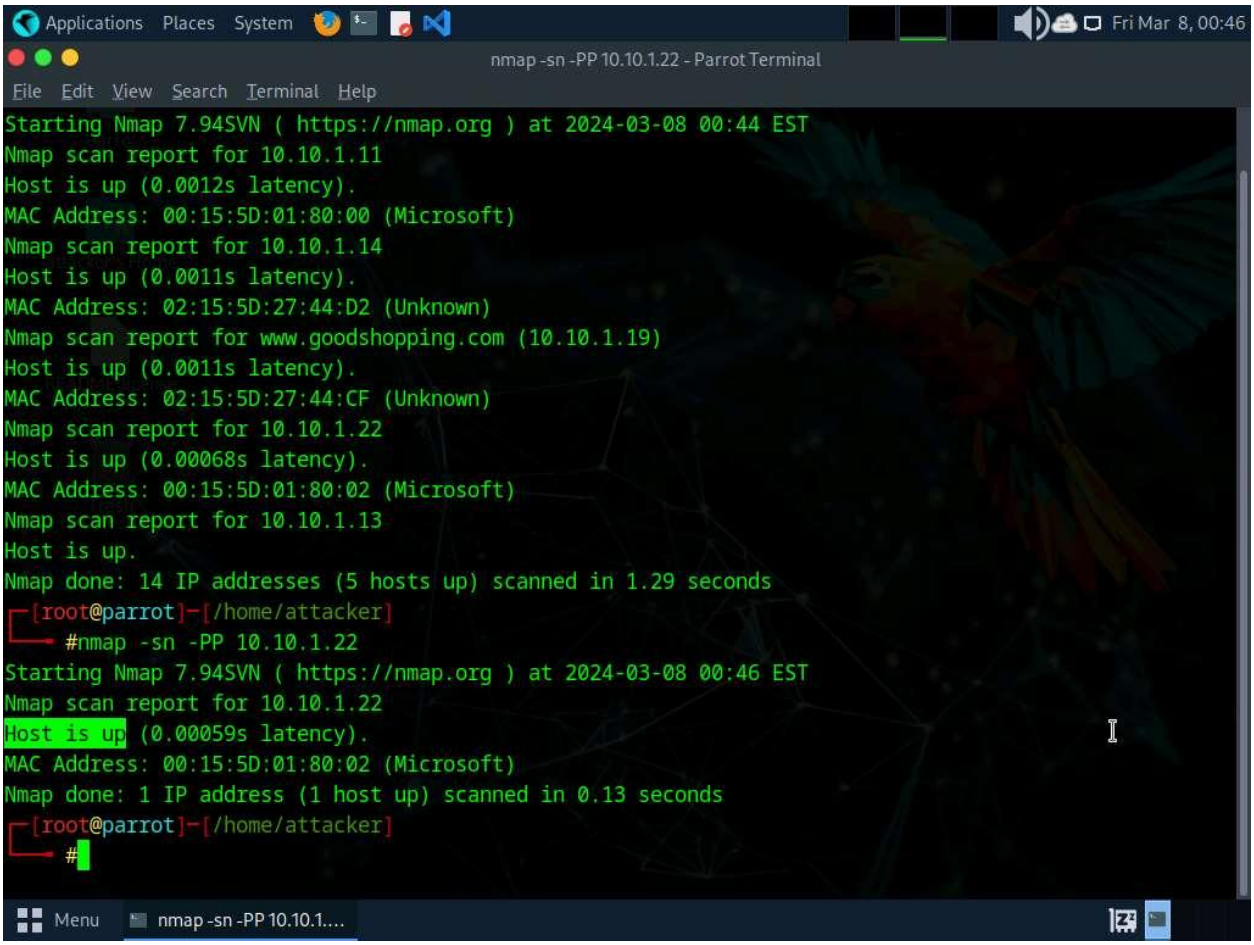
The ICMP ECHO ping sweep is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is alive, it will return an ICMP ECHO reply.



8. Run **nmap -sn -PP [Target IP Address]** command, (here, the target IP address is **10.10.1.22**). The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

-PP: performs the ICMP timestamp ping scan.

ICMP timestamp ping is an optional and additional type of ICMP ping whereby the attackers query a timestamp message to acquire the information related to the current time from the target host machine.



9. Apart from the aforementioned network scanning techniques, you can also use the following scanning techniques to perform a host discovery on a target network.

    - **ICMP Address Mask Ping Scan**: This technique is an alternative for the traditional ICMP ECHO ping scan, which are used to determine whether the target host is live specifically when administrators block the ICMP ECHO pings.

 # nmap -sn -PM [target IP address]

    - **TCP SYN Ping Scan**: This technique sends empty TCP SYN packets to the target host, ACK response means that the host is active.

 # nmap -sn -PS [target IP address]

    - **TCP ACK Ping Scan**: This technique sends empty TCP ACK packets to the target host; an RST response means that the host is active.

 # nmap -sn -PA [target IP address]

    - **IP Protocol Ping Scan**: This technique sends different probe packets of different IP protocols to the target host, any response from any probe indicates that a host is active.

 # nmap -sn -PO [target IP address]

10. This concludes the demonstration of discovering the target host(s) in the target network using various host discovery techniques.
11. Close all open windows and document all the acquired information.

Question 3.1.1.1

Perform an ICMP ECHO ping sweep to discover live hosts on your network subnet. Find the number of live hosts in the subnet (10.10.1.2-23).

7 Correct

Question 3.1.1.2

Perform host discovery using Nmap to find the IP address of the machine hosting www.goodshopping.com.

10.10.1.19 Correct