Assignment -2

Footprinting

- Footprinting: Footprinting is the process of gathering information about a target system or network to create a profile or “footprint” of its infrastructure, services, and security posture.This information can include details about the organization’s domain names, IP addresses,network topology, employee names, email addresses, and more. Footprinting techniques often involve passive information gathering through sources like search engines, social media, public databases, and company website

Reconnaissance

- Reconnaissance: Reconnaissance, also known as “recon,” is the active process of scanning and probing a target system or network to gather additional information beyond what is available through passive footprinting. Reconnaissance activities typically involve techniques such as network scanning, port scanning, banner grabbing, and vulnerability scanning to identify potential points of entry or weaknesses in the target’s defenses. The goal of reconnaissance is to obtain detailed insights into the target’s infrastructure, services, and security vulnerabilities to aid in further analysis or exploitation.

Learning outcomes

In this module, you will complete the following exercises:

Exercise 1 – Reconnaissance Tools and Techniques

Exercise 2 – Conducting Active Reconnaissance in a Network

Exercise 3 – Conducting Passive Reconnaissance in a Network

Reconnaissance tools and techniques

- Reconnaissance, also known as Footprinting, is a method of collecting information about a target. It is the first phase and lays the foundation for the attack. With the discovered information, you can determine the attack surface of a target.

The following could be gathered about a target using reconnaissance:

Basic information using Web searches

Location of live systems on the network

Network size

Identification of open ports and running services

- Operating system version

- Reconnaissance can be split into three parts:

1. Footprinting: Collecting information about an organization in a passive manner.

2. Scanning: Using active reconnaissance methods, such as nmap scanning, to extract information about networks and systems.

3. Enumeration: After footprinting and scanning have been completed, you can use the information to find the area that you want to attack. For example, if the attacker finds out that a specific version of Apache is being used, then the attacker can narrow down the attack to exploit its vulnerabilities.

Types of reconnaissance

There are two types of reconnaissance:

1.Active

2.passive

1.Active reconnaissance:Using the active reconnaissance method, you directly interact with the system. For example, you can execute an nmap command to collect information about the open ports

Active reconnaissance can include the following methods:

- IP or Port scanning
- Operating system scanning
- Footprinting of existing services in a system
- Zone transfer on an internal DNS server
- Spidering the public Webpages
- Fuzzing

Social Engineering

- <u>2.Passive reconnaissance:</u>
- Passive reconnaissance is the opposite of active reconnaissance. You do not interactwith the system. Instead, you use various methods, such as a Web search, to find information about a target.
- Passive reconnaissance can use some of the following methods:
- Search the Whois database
- Browse through the target’s Website
- Perform Social Network scraping
- Search Google or any search engine
- Extract the DNS information
- Review blogs, public forums, and Websites
- Search breach databases and DarkWeb about the target

Kali Linux also includes reconnaissance or footprinting tools under different

categories, which are:

1. DNS Analysis
2. IDS/IPS Identification
3. Live Host Identification
4. Network & Port Scanners
5. OSINT Analysis
6. Route Analysis
7. SMB Analysis

- SMTP Analysis
- SNMP Analysis
- SSL Analysis

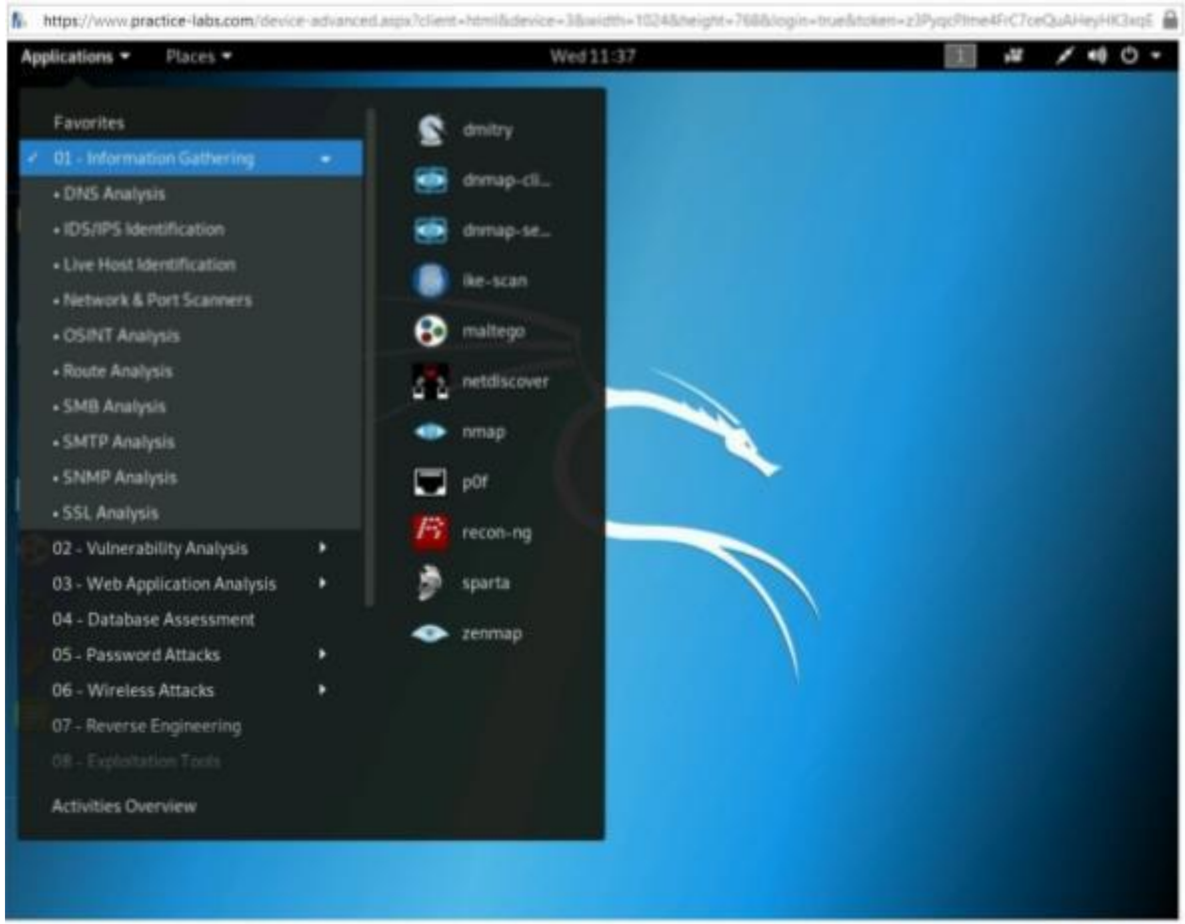


Figure 1.1 Screenshot of PLABKALI01: Displaying the categories of tools under 01- Information Gathering in the Applications menu.

- Need for Reconnaissance or Footprinting :Without footprinting, it would be difficult for a hacker to break into a system or network. Therefore, hackers spend a significant amount of time gathering information about the system or the network of an organization. Based on the collected information, hackers build their hacking strategy and execute it. As an ethical hacker, you gain the you perform following footprinting :

- Understand the Security Posture
- Reduce Attack Area
- Collect Maximum Information
- Draw Network Diagram

2.Conducting Active Reconnaissance in a Network

Active reconnaissance is a hands-on method where you interact with the system directly to collect information.

In this exercise, you will learn about conducting active reconnaissance.

- Identify Live Hosts on a Network
- Network Mapper, known as Nmap, is a network and host discovery tool. It is one of the most widely used tools for various activities, such as:
- Discovering hosts, services, and ports
- Fingerprinting operating systems
- Enumeration
- Discovering vulnerabilities on the local and remote host
- Finding the IP address of a remote system

Using Nmap, you can scan for targets by:

Scanning for a single IP: nmap 192.168.0.1

Scanning for a host by using its name: nmap host1.plab.com

Scanning an entire subnet: nmap plab.com/24, nmap 192.168.0.0/24, nmap 192.168.0.*

Scanning for a range of IP addresses: nmap 192.168.0.1-10

Scanning for a range and a system outside the range: nmap 192.168.0.1, 1.10

- In this task, you will use Nmap to identify the live systems on a network. To do this,<u>perform the following steps</u>
- <u>Step 1:</u>
- Ensure that you have logged into PLABKALI01.
- Crentials are:
- Username: root Password: Passw0rd
- <u>Step 2:</u>
- On the desktop, click Terminal.

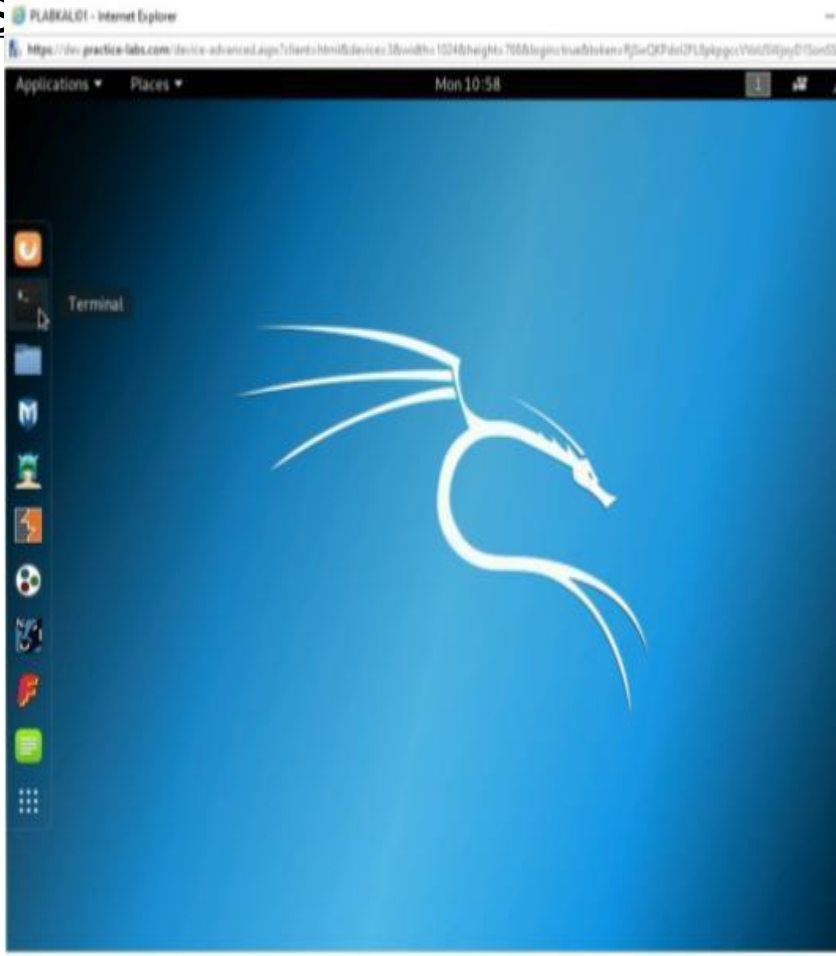
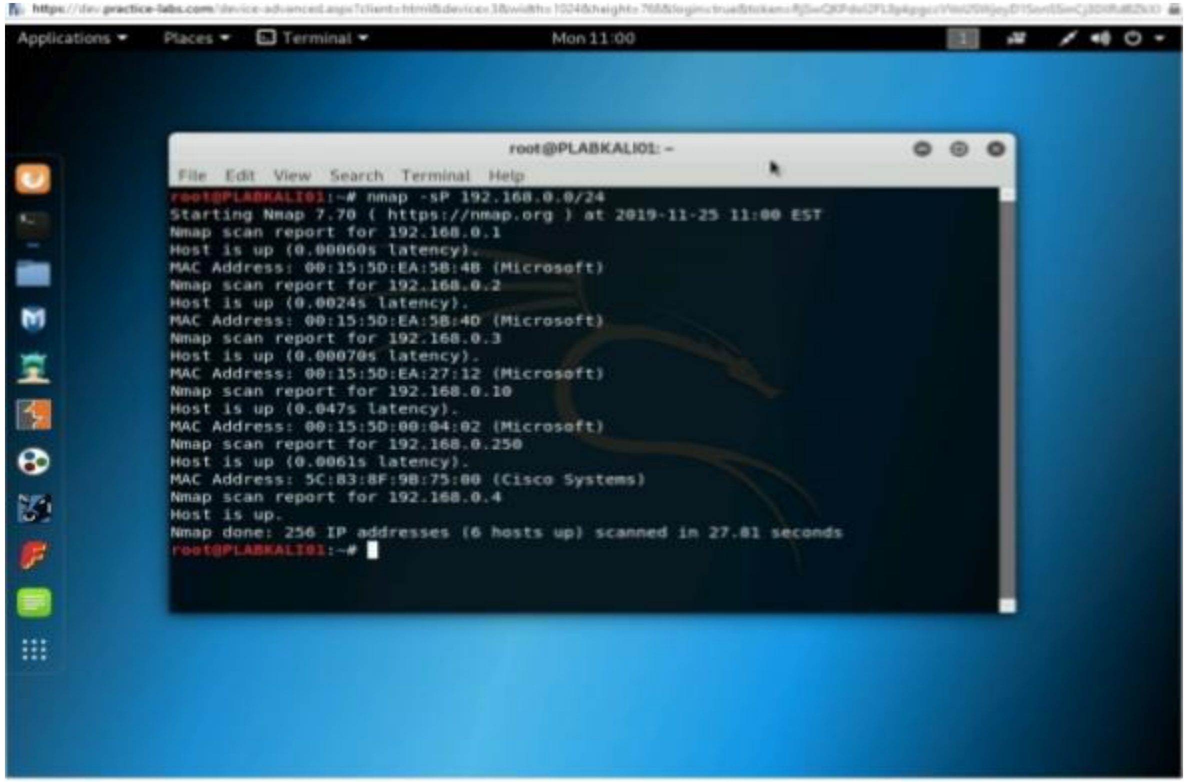


Figure 2.1 Screenshot of PLABKALIo1: Clicking the Terminal icon i
left pane.

- Step 3:
- The terminal window is displayed. You will now perform a ping scan to discover the live hosts in a network. Type the following command:
- nmap –sP 192.168.0.0/24



```
root@PLABKALI01:~# nmap -sP 192.168.0.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:00 EST
Nmap scan report for 192.168.0.1
Host is up (0.00060s latency).
MAC Address: 00:15:5D:EA:58:48 (Microsoft)
Nmap scan report for 192.168.0.2
Host is up (0.0024s latency).
MAC Address: 00:15:5D:EA:58:4D (Microsoft)
Nmap scan report for 192.168.0.3
Host is up (0.00070s latency).
MAC Address: 00:15:5D:EA:27:12 (Microsoft)
Nmap scan report for 192.168.0.10
Host is up (0.047s latency).
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Nmap scan report for 192.168.0.250
Host is up (0.0061s latency).
MAC Address: 5C:83:8F:98:75:00 (Cisco Systems)
Nmap scan report for 192.168.0.4
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 27.81 seconds
root@PLABKALI01:~#
```

Figure 2.2 Screenshot of PLABKALI01: Showing the output of the nmap - sP command.

Press enter

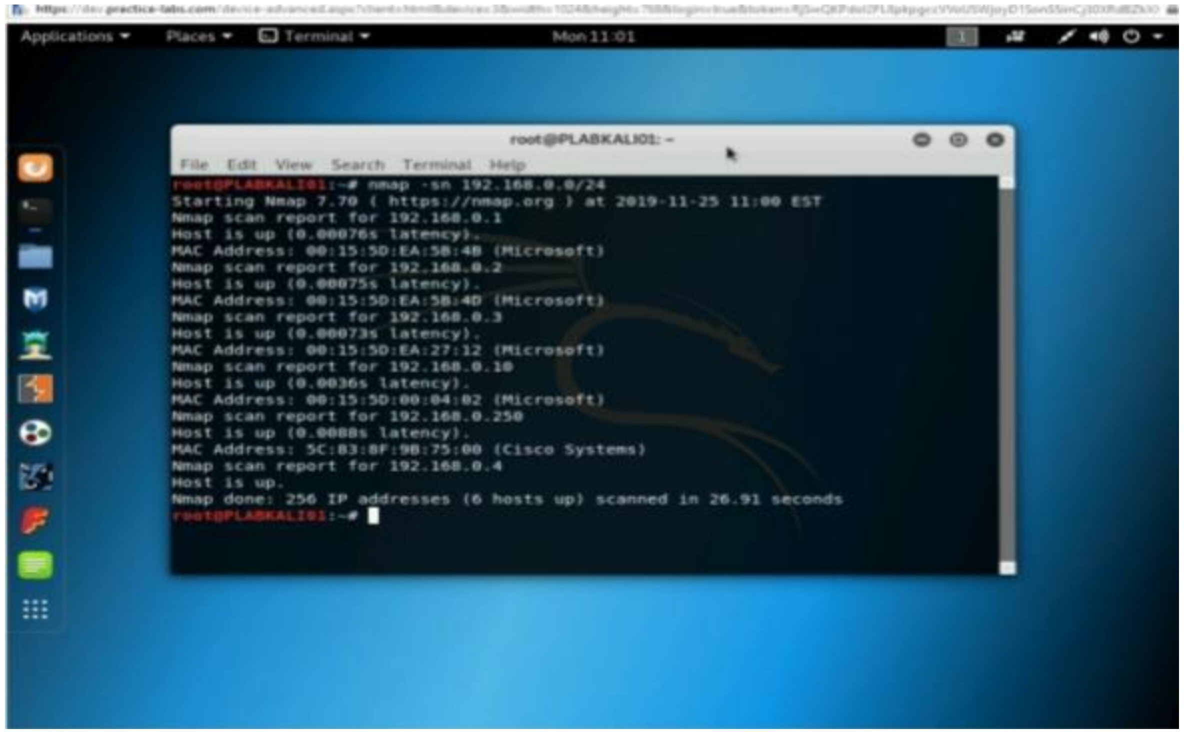
The output of the command is displayed. Notice that there were six hosts that were detected. It has found five systems in the lab environment, including Kali. Along with this, the gateway IP, 192.168.0.250, is also found.

Step 4:

Clear the screen by entering the following command:

- Clear screen

- You can also perform a scan without ping. To do this, type the following command:
- nmap –sn 192.168.0.0/24
- Press Enter.
- The output of the command is displayed. Notice that without the ping scan, it has detected six systems on the network.

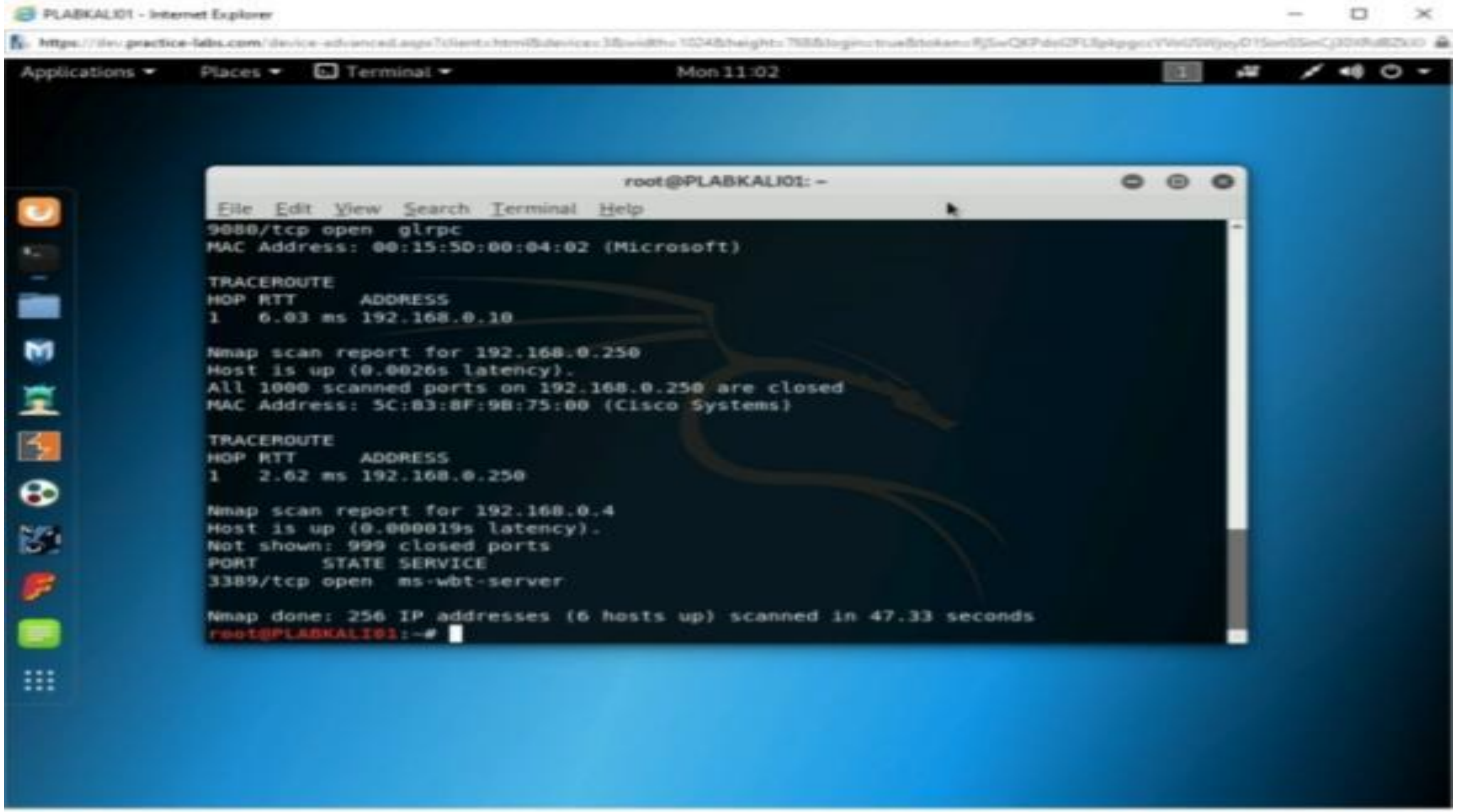


```
root@PLABKALI01:~# nmap -sn 192.168.0.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:00 EST
Nmap scan report for 192.168.0.1
Host is up (0.00076s latency).
MAC Address: 00:15:5D:EA:58:48 (Microsoft)
Nmap scan report for 192.168.0.2
Host is up (0.00075s latency).
MAC Address: 00:15:5D:EA:58:4D (Microsoft)
Nmap scan report for 192.168.0.3
Host is up (0.00073s latency).
MAC Address: 00:15:5D:EA:27:12 (Microsoft)
Nmap scan report for 192.168.0.10
Host is up (0.0036s latency).
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Nmap scan report for 192.168.0.250
Host is up (0.0088s latency).
MAC Address: 5C:83:8F:98:75:00 (Cisco Systems)
Nmap scan report for 192.168.0.4
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 26.91 seconds
root@PLABKALI01:~# 
```

- Step 5:
- Clear the screen by entering the following command:
- clear

You can also trace the path between your system and each of the hosts that is live on the network. To do this, type the following command:

- nmap –traceroute 192.168.0.0/24
- Press Enter.
- Notice the output of the command. In the output, the hops from your system to the systems on the network are displayed. Since this is within the same IP subnet, there is a single hop. The output also displays open ports on each live system.

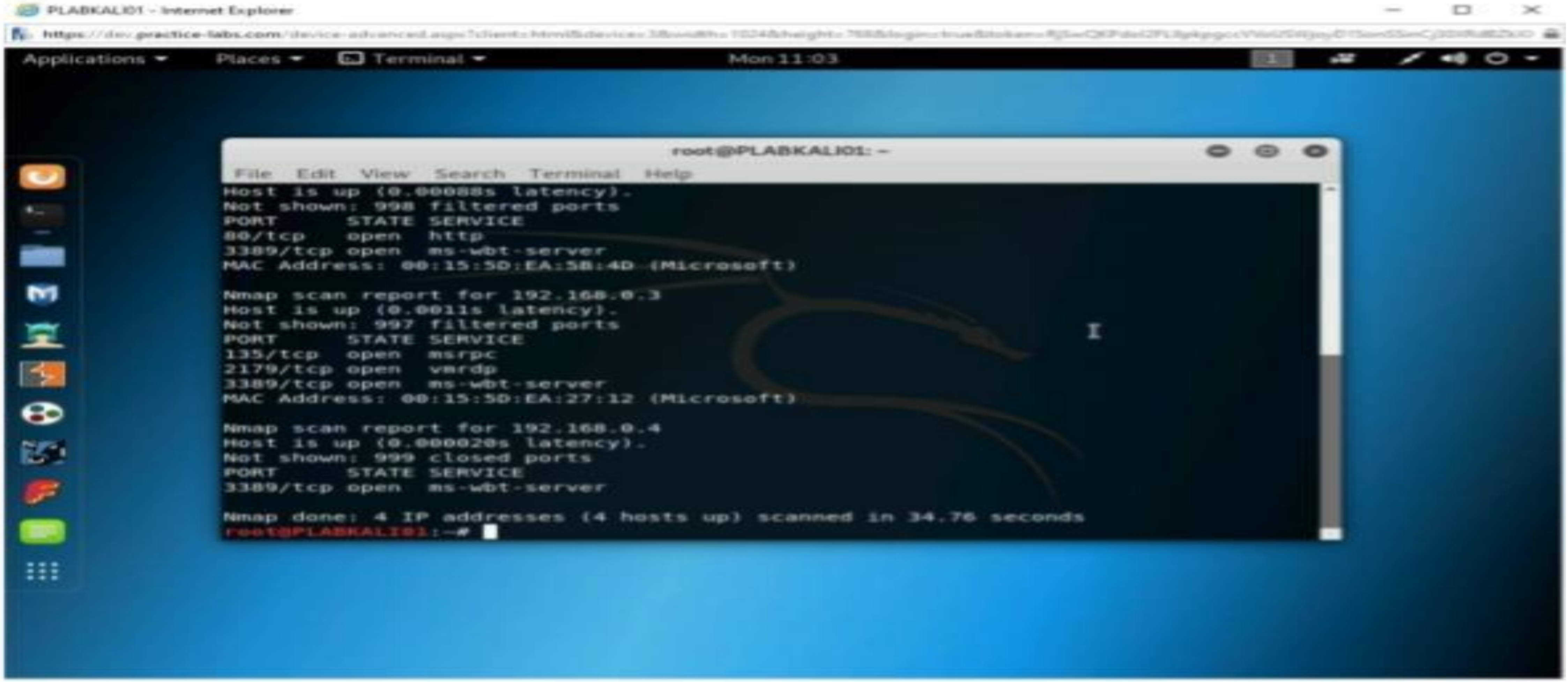


```
9080/tcp open  glrpc
MAC Address: 00:15:5D:00:04:02 (Microsoft)

TRACEROUTE
HOP RTT     ADDRESS
1   6.03 ms 192.168.0.10

Nmap scan report for 192.168.0.250
Host is up (0.0026s latency).
All 1000 scanned ports on 192.168.0.250 are closed
MAC Address: 5C:83:8F:9B:75:00 (Cisco Systems)

TRACEROUTE
HOP RTT     ADDRESS
1   2.62 ms 192.168.0.250

Nmap scan report for 192.168.0.4
Host is up (0.000019s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap done: 256 IP addresses (6 hosts up) scanned in 47.33 seconds
root@PLABKALI01:~#
```

Figure 2.4 Screenshot of PLABKALI01: Showing the output of the nmap - - traceroute command.

- Step 6:
- Clear the screen by entering the following command:
- clear
- You can also scan for live hosts on a network using an IP address range. To do this type the following command:
- Nmap 192.168.0.1-4
- Press Enter.
- The output of the command is displayed. Notice that only four hosts are listed in the scan. Without any parameters, the nmap command scans for the live systems and open ports.

open ports.

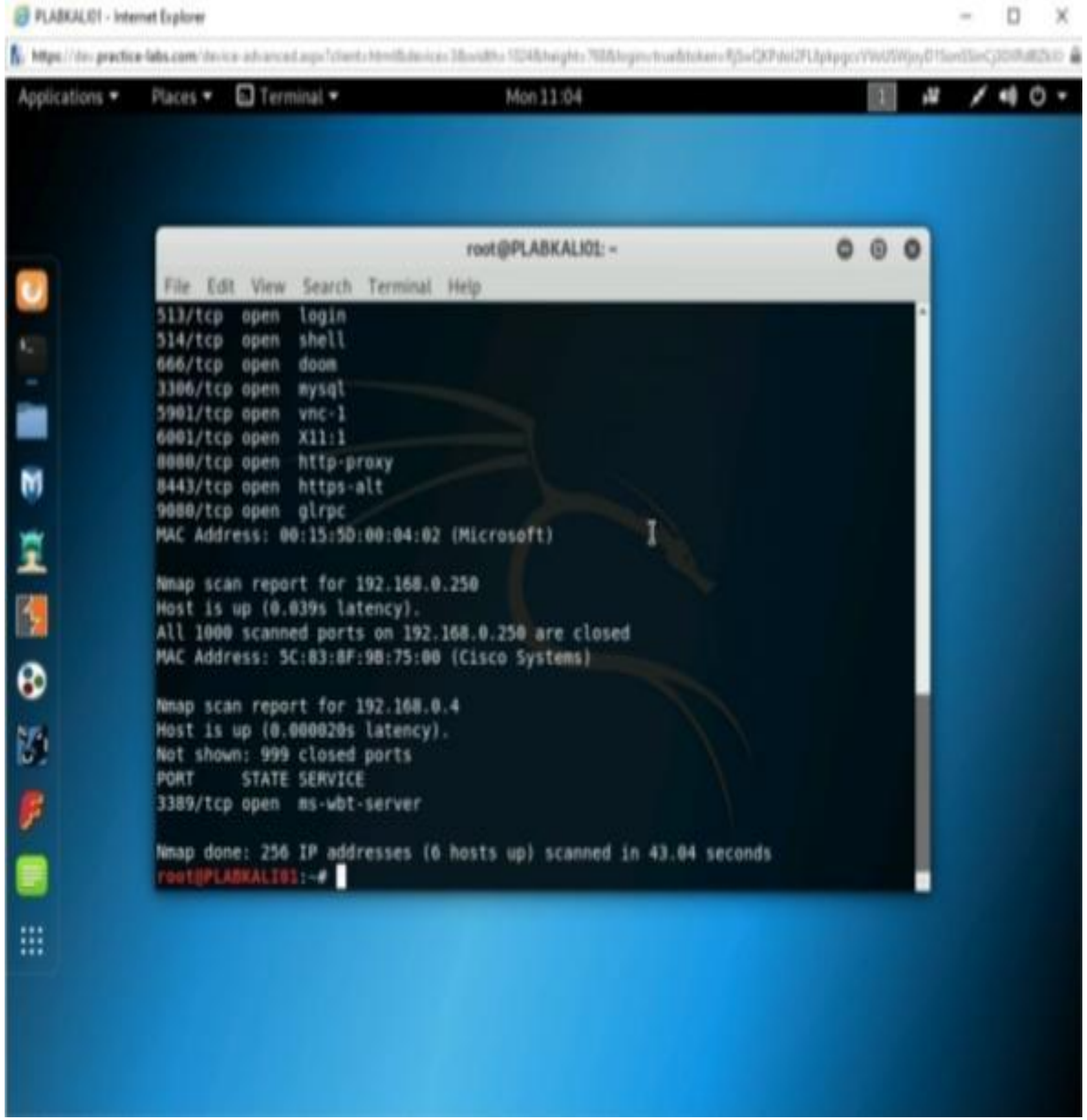


```
Host is up (0.00088s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:EA:58:4D (Microsoft)

Nmap scan report for 192.168.0.3
Host is up (0.0011s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:EA:27:12 (Microsoft)

Nmap scan report for 192.168.0.4
Host is up (0.000020s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap done: 4 IP addresses (4 hosts up) scanned in 34.76 seconds
root@PLABKALI01:~# 
```

Figure 2.5 Screenshot of PLABKALI01: Showing the output of the nmap command with a series of IP addresses.

- Step 7:
- Clear the screen by entering the following command:
- Clear
- You can also use a wildcard to scan an IP range. To do this, type the following command:
- nmap 192.168.0.*
- Press Enter.
- Notice the output of the command. It has searched for all live systems in the subnet of 256 IP addresses.

- Figure 2.6 Screenshot of PLABKALI01: Showing the output of the nmap command with a wildcard.



```
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 00:15:5D:00:04:02 (Microsoft)

Nmap scan report for 192.168.0.250
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.0.250 are closed
MAC Address: 5C:83:8F:9B:75:00 (Cisco Systems)

Nmap scan report for 192.168.0.4
Host is up (0.000020s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap done: 256 IP addresses (6 hosts up) scanned in 43.04 seconds
root@PLABKALI01:~#
```