****

**Department of Information Technology Engineering**

### **IT321-Ethical Hacking**

**AY:2023-2024**

**Lab1 A- Internet Foot-printing**

**Lab1 B- Network Scanning**

Name of Student : Adwait Purao UCID : 2021300101

Class : COMPS B

**Objectives:**

[1] Introduce the anatomy of ethical hacking

[2]To perform Network Reconnaissance Using Command Line

[3]To perform DNS Interrogation

[4]To perform Web Reconnaissance

**Outcomes: After completing the lab, you will be able to:**

[1] Identify and demonstrate the ethical hacking phases.

[2] Define footprinting and how it is accomplished.

[3] Identify many resources that can be used to footprint an organization

[4] Search an organization’s public Web pages and identify internal components

[5] Determine the IP address range assigned to a particular organization

[6] Identify host machines that are active within an organization

**System Requirements:**

[1] Kali Linux- Offensive

[2] Windows 7/ Windows XP- Client or victim

[3] Tools: ping,fping,nslookup,traceroute,arp,host,dig,TCPDUMP/Wireshark, nmap, etherape,ping etc

**Lab1 A- Internet Foot-printing**

1A- **Foot-printing**

**1A.1 Google Hacking Database**

**1A.2- Who is Database**

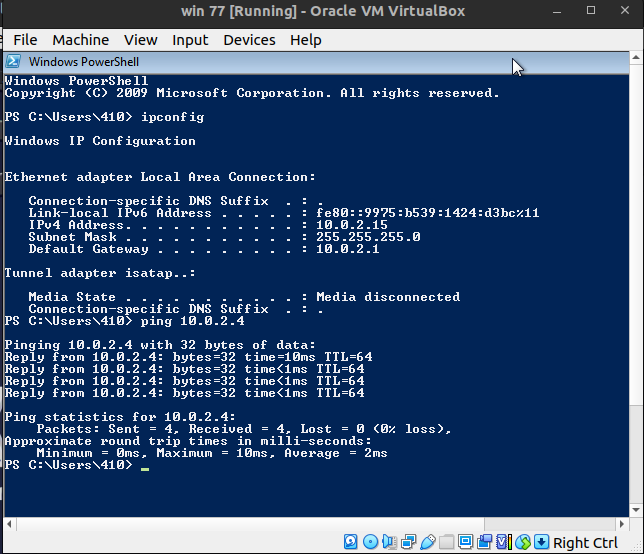
**1A.3 Other available resources**

1B **Network Footprinting**

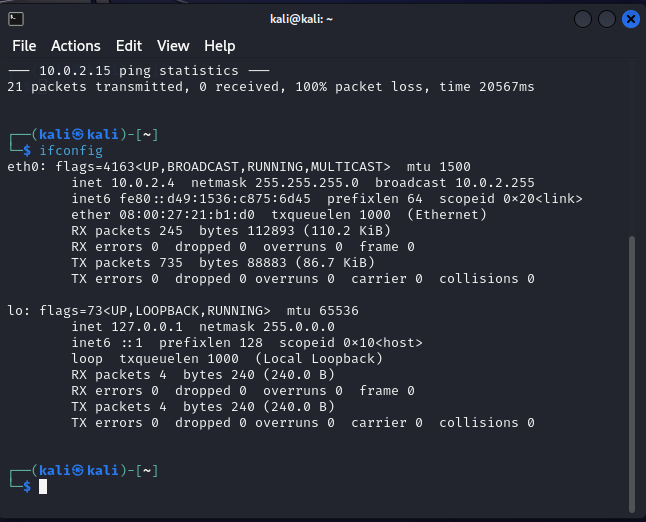
**1B.1 Network Reconnaissance using command-line tools**

1. **Ifconfig/ipconfig**

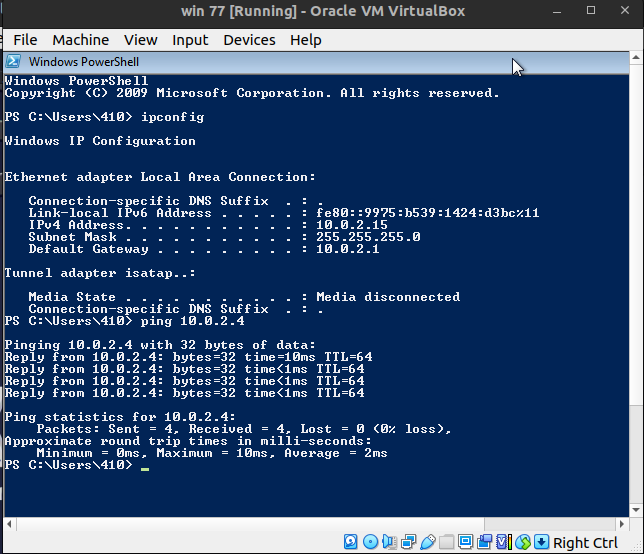
**Windows**

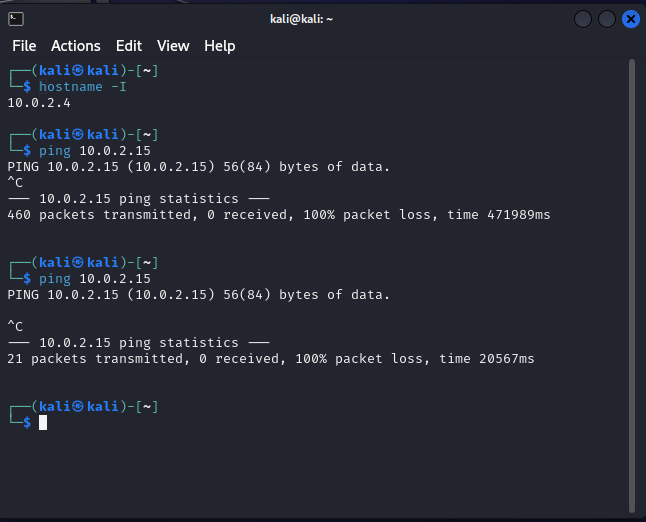
****

**Kali**

****

1. **Ping**

****

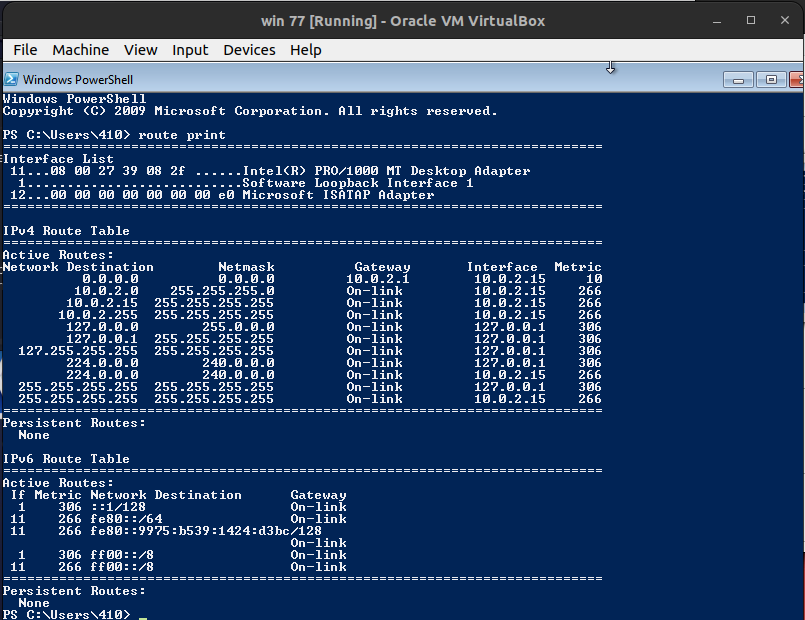
****

1. **Route (Traceroute/ Tracert)**

**Kali**

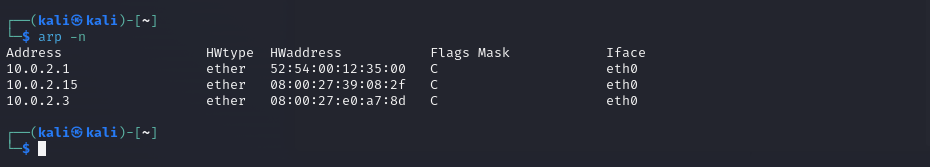
****

**Windows**

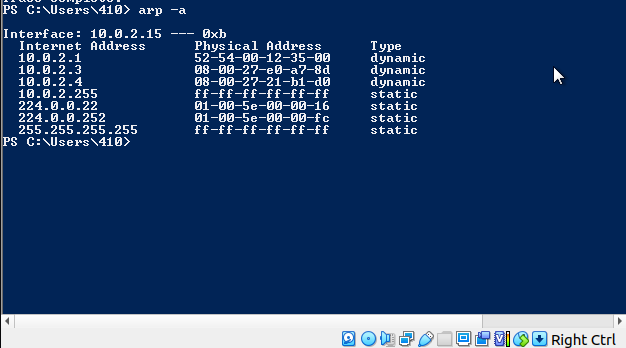
****

1. **Arp**

**Kali**

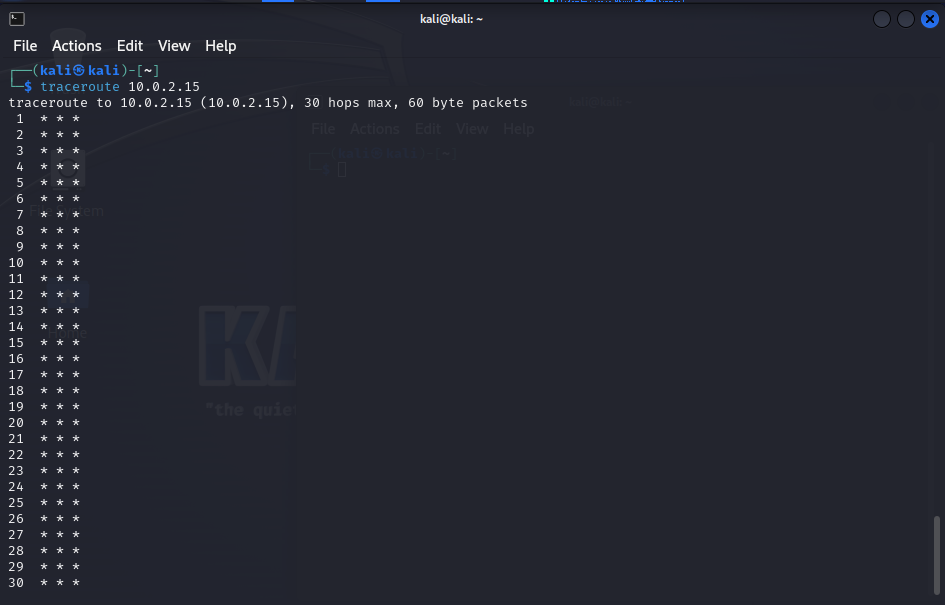
****

**Windows**

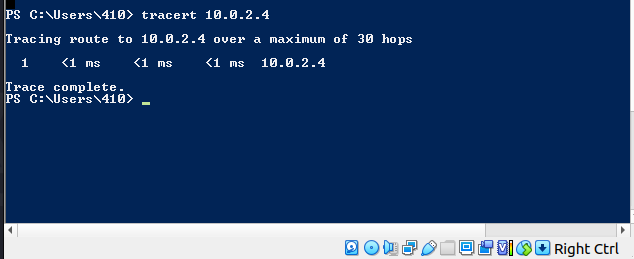
****

1. **Traceroute**

**Kali**

****

**Windows**

****

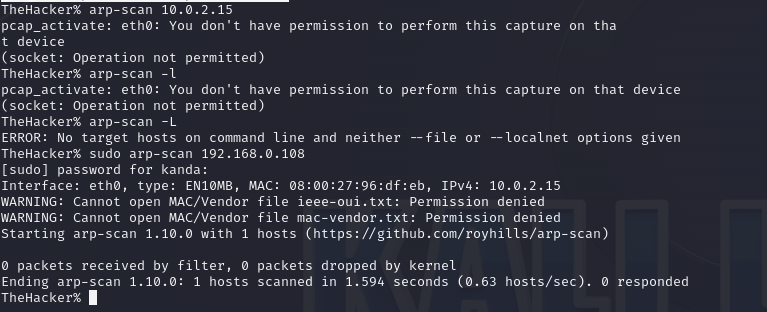
1. **Fping**

**Kali**

****

**Windows**

1. **Arp-scan**

****

**1B.2 DNS Interrogation**

1. **Nslookup**

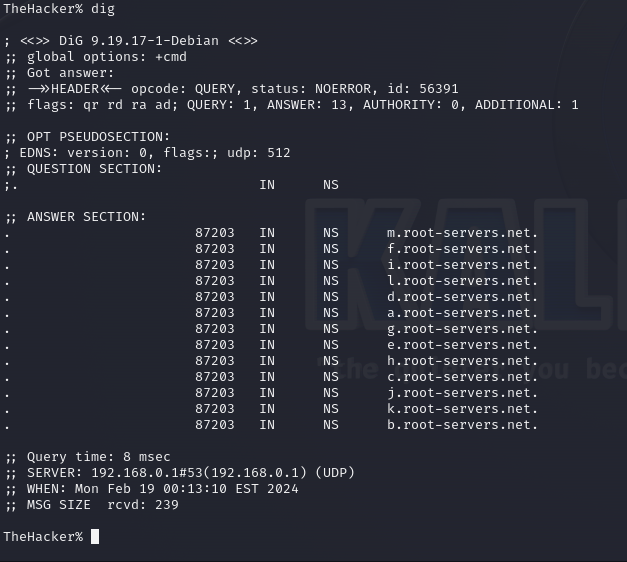
**Kali**

****

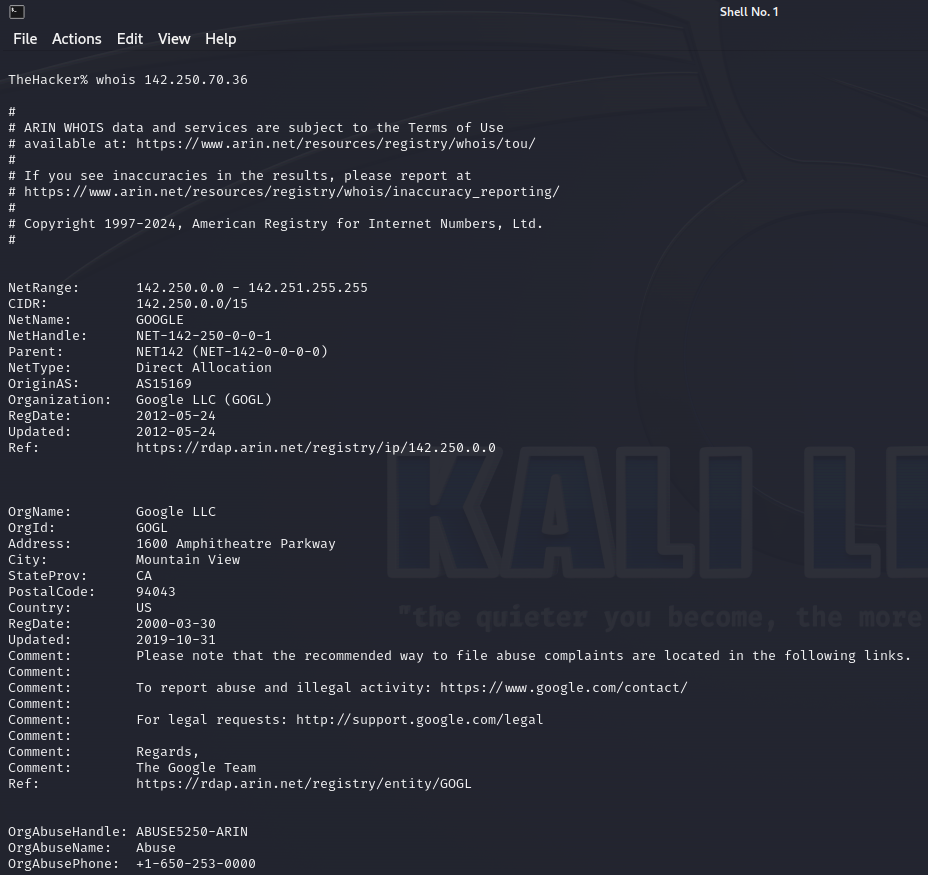
1. **Host**

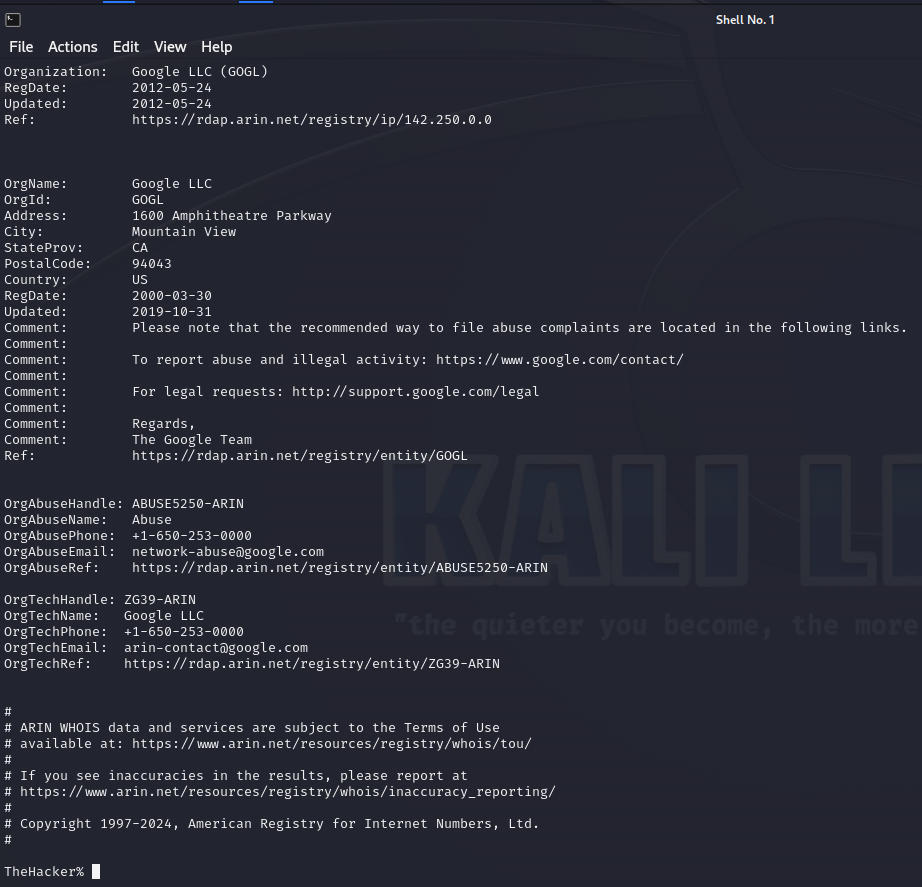
****

1. **Dig**

****

1. **Whois**

****

****

**1B.3 Web Reconnaissance**

1. **DNSstuff**
2. **Whois**

**Lab1 B- Network Scanning**

**Objective: Scan the network to identify open ports, OS detection, service scanning and vulnerability scanning.**

**Outcomes:**

1. To install and use network scanner (nmap) and web server scanner (nikto)

2. To explore various scanning mechanisms.

3. To enumerate the open ports and identify vulnerable services.

4. To detect the operating system and associated vulnerability

5. To identify the exploit with respect to vulnerable services.

**System Requirements:**

3 workstations installed with Kali Linux/Fedora Linux Core/Ubuntu and Windows XP

Nmap, nmapfe, zenmap etc

Background: ISO-OSI Layered Architecture of Computer Communication Network

| OSI Model Layer No | Layer | Layer Description | Protocols |
| --- | --- | --- | --- |
| Layer 7 | Application | This layer involves the application software that is sending and receiving data | HTTP, FTP, and Telnet |
| Layer 6 | Presentation | This layer defines how data is formatted or organized | ASCII, JPEG, PDF,  PNG, and DOCX |
| Layer 5 | Session | This layer involves application session control, management, synchronization,  and termination | NetBIOS, PPTP,  RPC, and SOCKS |
| Layer 4 | Transport | This layer involves end-to-end  communication services | TCP and UDP |
| Layer 3 | Network | This layer involves logical system addressing | IPv4, IPv6, ICMP,  and IPSec |
| Layer 2 | Data link | This layer involves physical system addressing | ARP |
| Layer 1 | Physical | This layer involves the data stream that is  passed over the wire |  |

**Discovery scanning:**

Discovery scanning is the process of identifying live hosts on a network. In the context of

penetration testing, this is usually performed to identify potential targets for attack. The

objective here is not to exhaust resources in gathering information about targets but instead

to merely find out where the targets are logically located. The final product of our discovery

should be a list of IP addresses that we can use for further analysis. In this laboratory, we

will use how to discover hosts on a network by using protocols operating at **layer 2, layer 3,**

**and layer 4 of the OSI model.** This will include each of the following steps using:

* **Scapy** to perform layer 2 discovery
* **ARPing** to perform layer 2 discovery
* **Nmap** to perform layer 2 discovery
* **NetDiscover** to perform layer 2 discovery
* **Metasploit** to perform layer 2 discovery
* **ICMP** ping to perform layer 3 discovery
* **Scapy** to perform layer 3 discovery
* **Nmap** to perform layer 3 discovery
* **fping** to perform layer 3 discovery
* **hping3** to perform layer 3 discovery
* **Scapy** to perform layer 4 discovery
* **Nmap** to perform layer 4 discovery
* **hping3** to perform layer 4 discovery

**Procedure:** Let explore nmap: Network host scanner, port scanner, OS fingerprinting, Service scanner and vulnerability scanner.

**NMAP:** Network exploration tool and security/port scanner

**Description:**

Nmap is short for Network Mapper. It is an open-source security tool for network exploration, security scanning, and auditing.

**1: Scan a single host or an IP address (IPv4)**

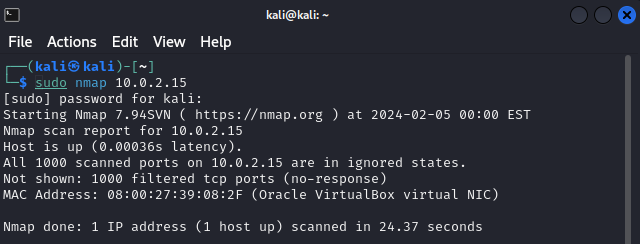
$sudo nmap 192.168.1.1

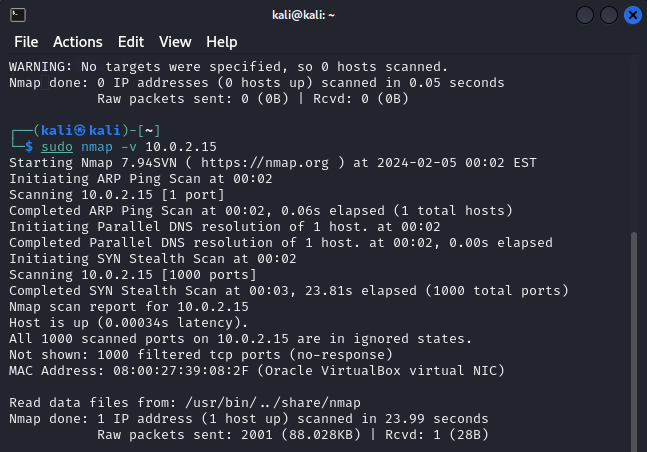
Scan a host name with more inf

$sudo nmap -v servername

**Short analysis:**

The command uses Nmap to check if the specified server (given by "servername") or IP address is active and running, while also scanning all available ports on the server. The -v flag in the Nmap command enables verbose mode, providing more detailed output during the scanning process.





**2. Scan multiple IP address or subnet (IPv4)**

$sudo nmap 192.168.1.1 192.168.1.2 192.168.1.3

works with same subnet i.e. 192.168.1.0/24

$sudo nmap 192.168.1.1,2,3

You can scan a range of IP address too:

$sudo nmap 192.168.1.1-20

You can scan a range of IP address using a wildcard:

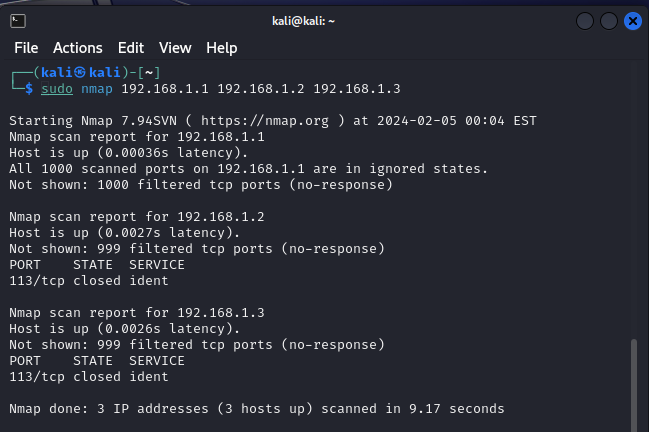
$sudo nmap 192.168.1.\*

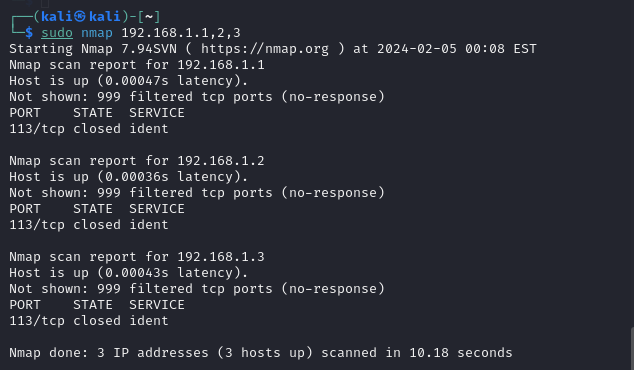
Finally, you scan an entire subnet:

$sudo nmap 192.168.1.0/24

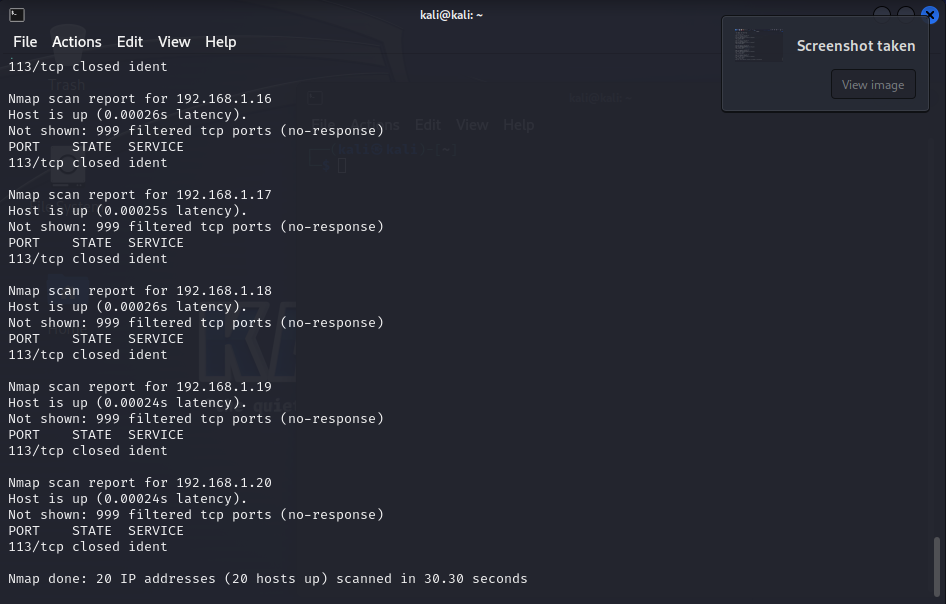
**Short analysis:**

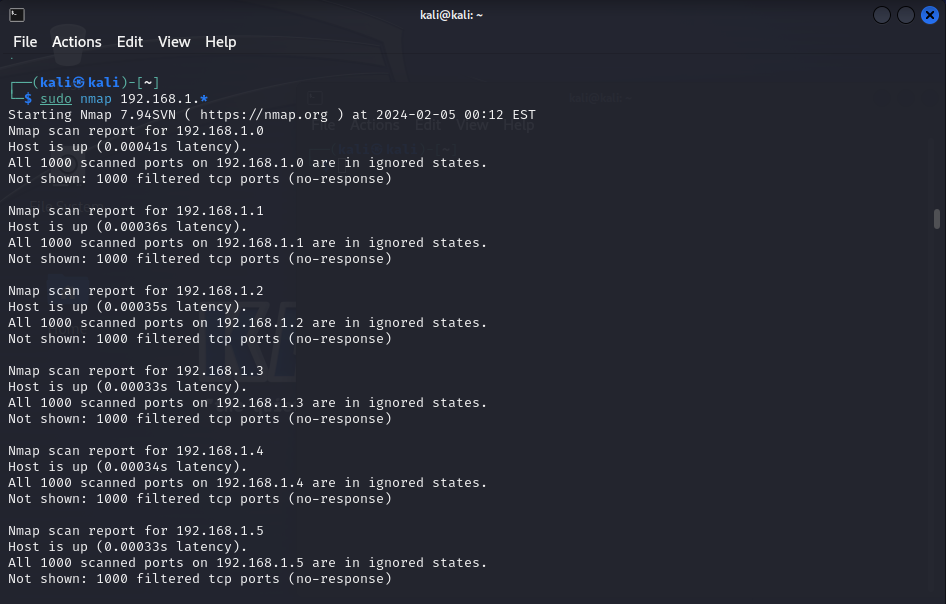
The above command show us that there are different ways to scan multiple IP addresses such as 192.168.1.1-20 which scans a range of IP addresses from 192.168.1.1 to 192.168.1.20, inclusive and we can also use wildcard (192.168.1.\*) to scan all hosts in the 192.168.1.0 subnet, where '\*' represents any valid host number (e.g., 192.168.1.1, 192.168.1.2, etc.).

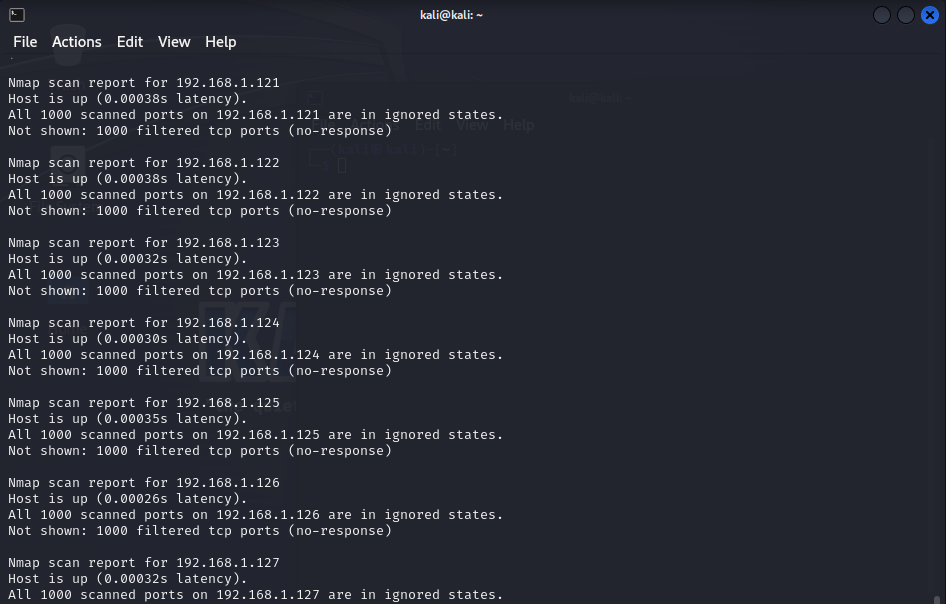


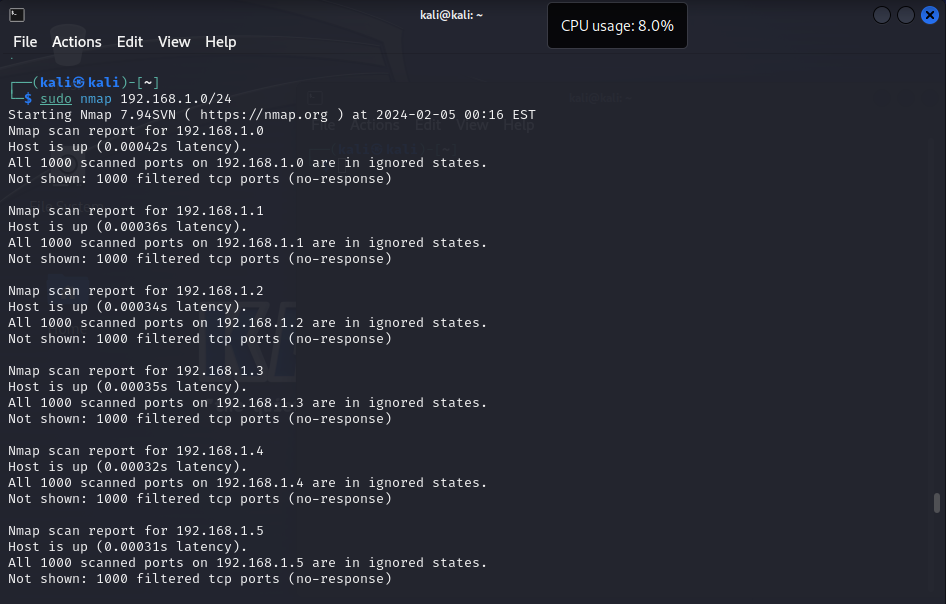












**3: Read list of hosts/networks from a file (IPv4)**

The -iL option allows you to read the list of target systems using a text file. This is useful to

scan a large number of hosts/networks. Create a text file as follows:

cat > /tmp/test.txt

Sample outputs:

192.168.1.0/24

192.168.1.1/24

10.1.2.3

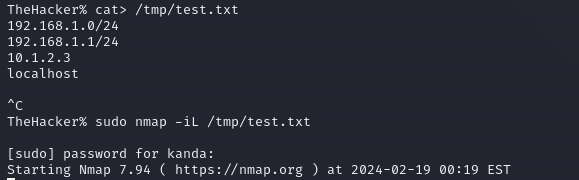
localhost

The syntax is:

$sudo nmap -iL /tmp/test.txt

**Short analysis:**

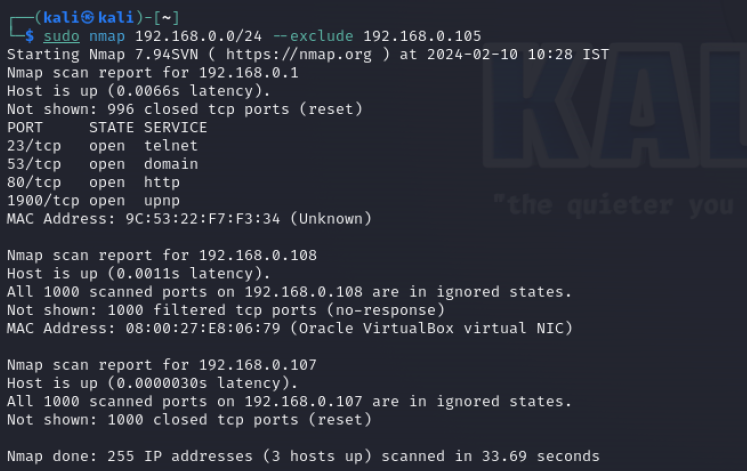
This command reads a file consisting of IP addresses and then scans them and get their network report.

****

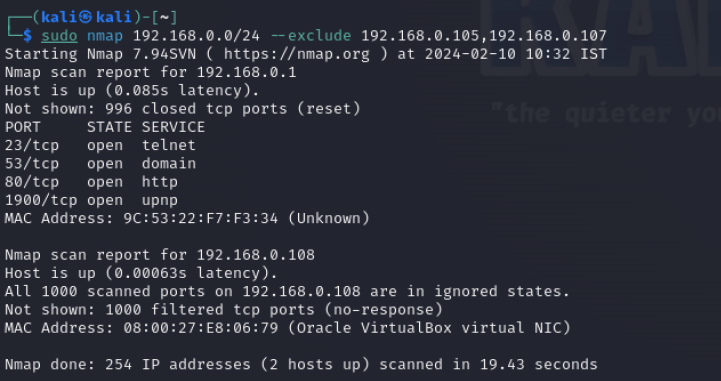
**4: Excluding hosts/networks (IPv4)**

When scanning a large number of hosts/networks you can exclude hosts from a scan:

$sudo nmap 192.168.1.0/24 --exclude 192.168.1.5



$sudo nmap 192.168.1.0/24 --exclude 192.168.1.5,192.168.1.254



OR exclude list from a file called /tmp/exclude.txt

$sudo nmap -iL /tmp/scanlist.txt --excludefile /tmp/exclude.txt

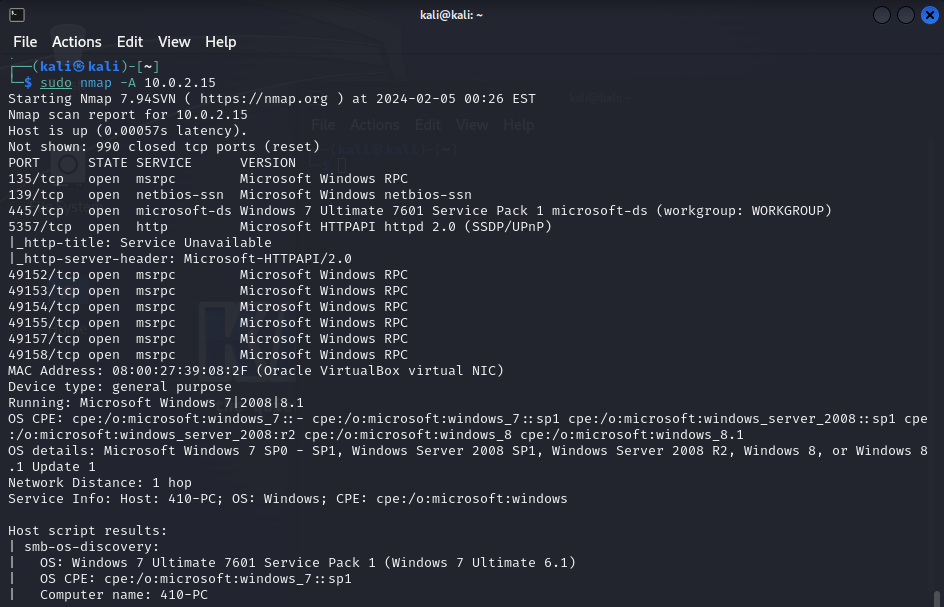
****

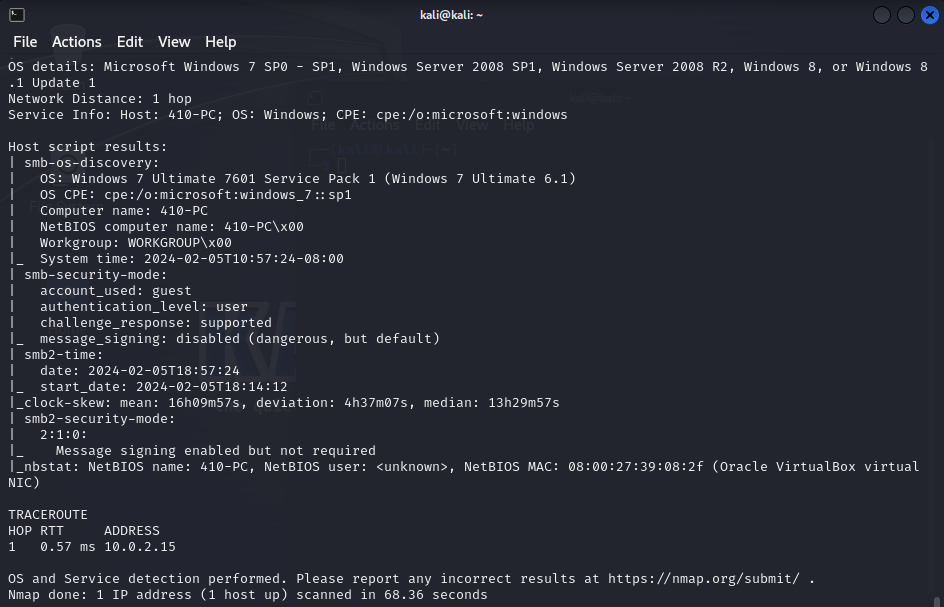
**Short analysis:**

To exclude specific IP addresses from scanning we can use –exclude option or we can make a file which contains IP addresses that we don’t want to scan and use –excludefile option.

**5: Turn on OS and version detection scanning script (IPv4)**

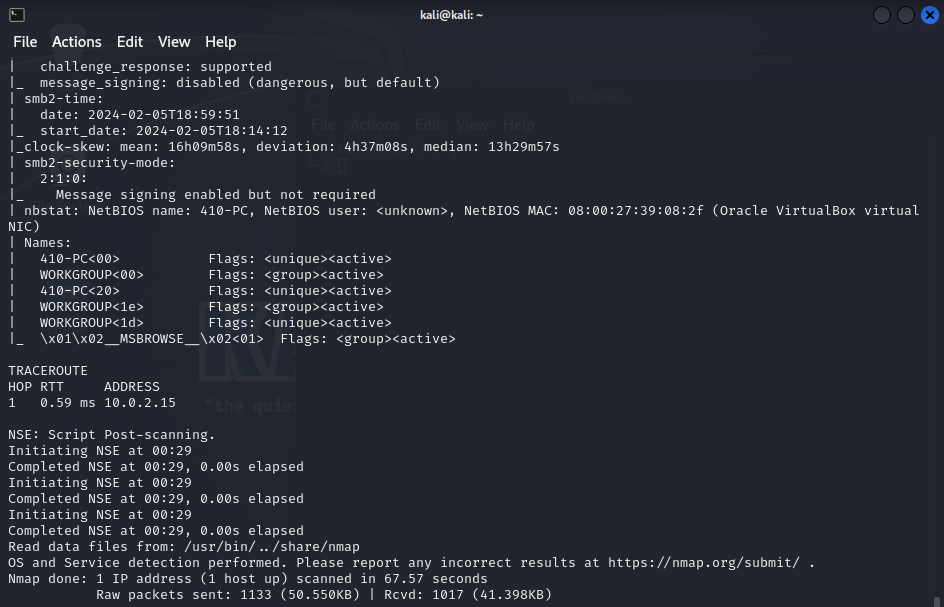
$sudo nmap -A 192.168.1.254



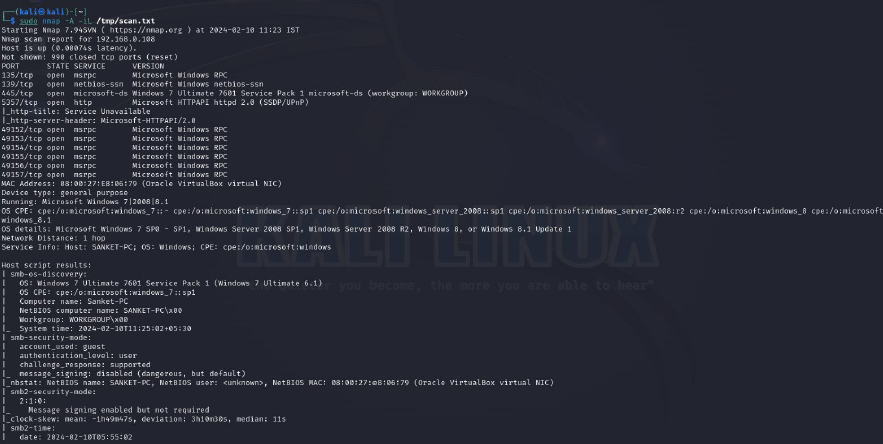


$sudo nmap -v -A 192.168.1.1





$sudo nmap -A -iL /tmp/scanlist.txt



**Short analysis:**

In this we are performing aggressive scan (-A) on the host. The aggressive scan includes OS detection, version detection, script scanning, and traceroute.

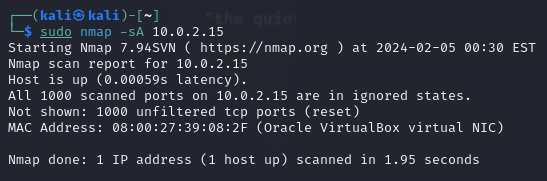
**6: Find out if a host/network is protected by a firewall**

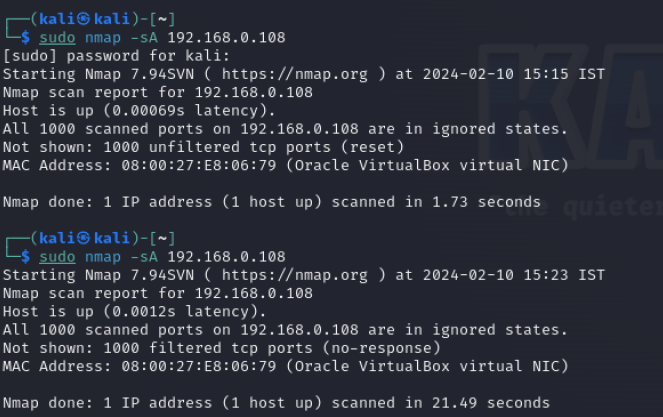
$sudo nmap -sA 192.168.1.254

$sudo nmap -sA server1

**Short analysis:**

Here we are performing TCP ACK scan, Nmap sends TCP ACK packets to determine the state of the ports if ports are filtered then it indicate it has a firewall and if it has unfiltered port then it don’t has firewall.

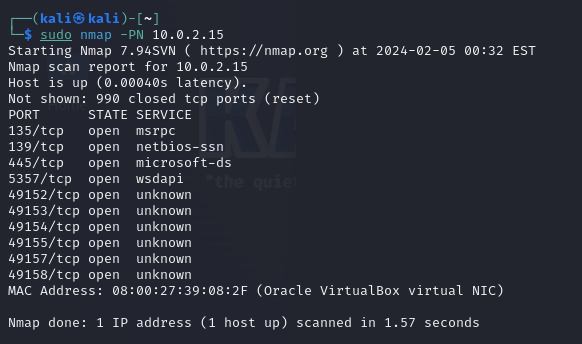




**7: Scan a host when protected by the firewall**

$sudo nmap -PN 192.168.1.1

$sudo nmap -PN server1

****

**Short analysis:**

Can be used for scanning host when it is protected with firewall and obtain information. It performs scans on a host without using

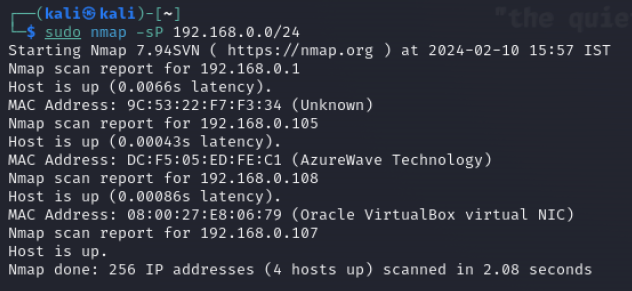
host discovery. It assumes that the target is online, regardless of whether it responds to ping requests.

**8: Scan a network and find out which servers and devices are up and running**

This is known as host discovery or ping scan:

$sudo nmap -sP 192.168.1.0/24

$sudo nmap done: 256 IP addresses (4 hosts up) scanned in 2.80 second



**Short analysis:**Uses the -sP option to perform a ping scan to determine which hosts are online.

**9: How do I perform a fast scan?**

$sudo nmap -F 192.168.1.1



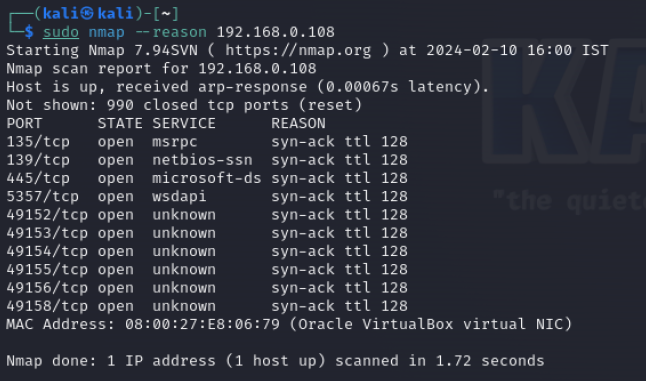
**Short analysis:**

Uses the -F option to perform a fast scan. The fast scan is a quicker version of the default scan and focusing on identifying open ports on the target host.

**10: Display the reason a port is in a particular state**

$sudo nmap --reason 192.168.1.1

$sudo nmap --reason server1



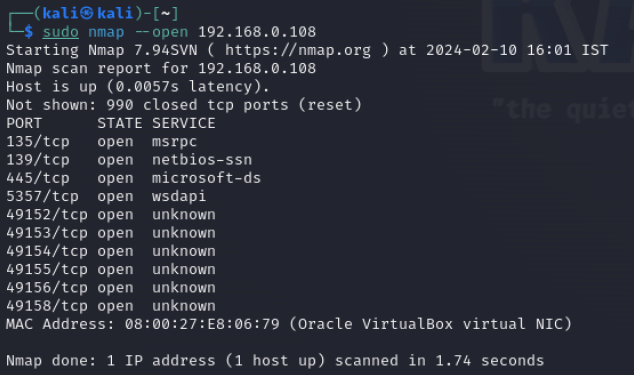
**Short analysis:**

Uses the --reason option to include additional information about why a port is in a particular state.

**11: Only show open (or possibly open) ports**

$sudo nmap --open 192.168.1.1

$sudo nmap --open server1



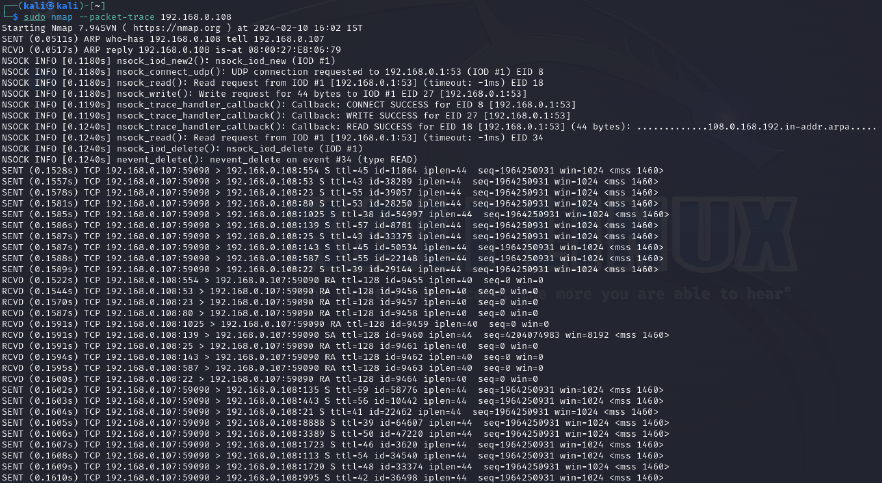
**Short analysis:**

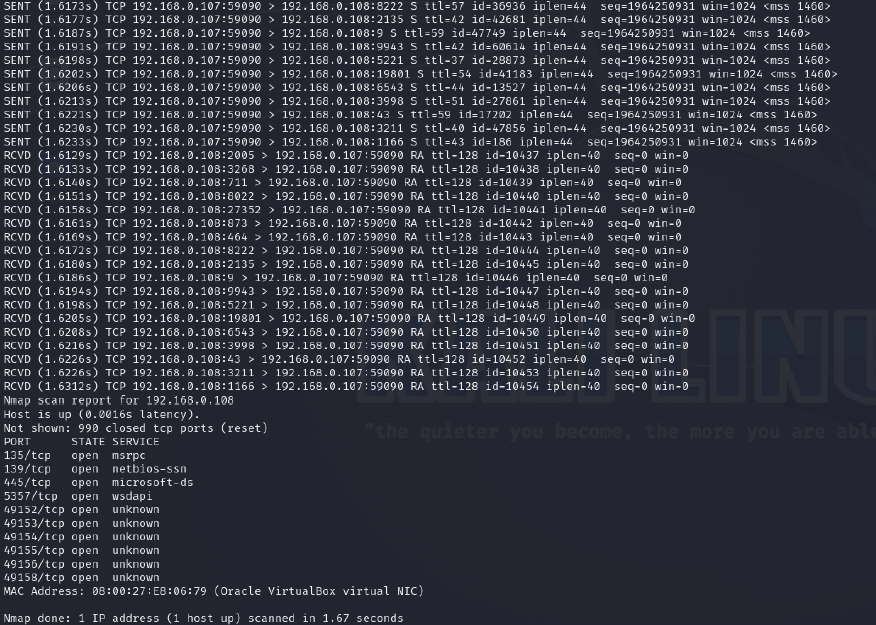
Uses the --open option to filter and display only the open ports during the scan.

**12: Show all packets sent and received**

$sudo nmap --packet-trace 192.168.1.1

$sudo nmap --packet-trace server1





**Short analysis:**

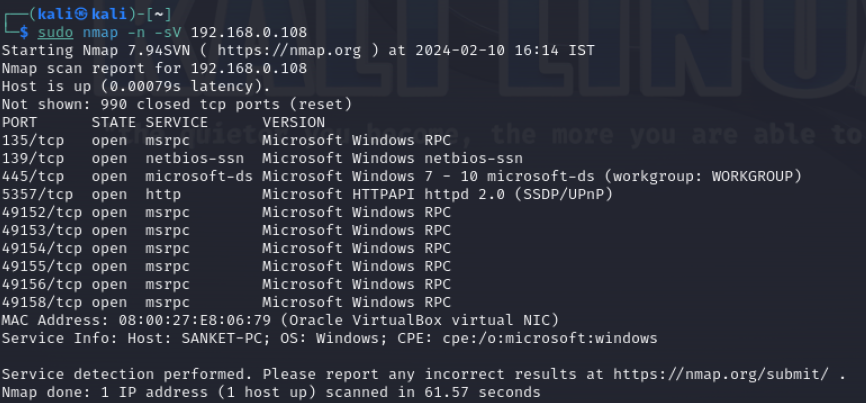
Uses the --packet-trace option to show the detailed packet tracing information during the scan. It shows the individual packets sent and received during the scanning process.

**13. To find the identify particular vulnerability for further exploit**

$sudo nmap -sT -A --script=smb-check-vulns -Pn --script-args=unsafe=1 192.168.56.103

Or

$sudo nmap -n -sV 192.168.56.103



**Short analysis:**

Performs a version detection scan on the host. The -n option disables DNS resolution for faster scanning, and -sV enables the identification of service and version information on open ports.

Analysis of nmap scan results

Refer:Nmap Scan to CSV (R3)

<https://laconicwolf.com/2018/02/04/nmap-scan-csv/>

Nmap results save as xml

$nmap -xO nmap\_scan.xml -sT ....

Converting nmap\_scan.xml to nmap\_scan.csv is simple:

$python3 nmap\_xml\_parser.py -f nmap\_scan.xml -csv nmap\_scan.csv

**Conclusion:**

Therefore, we have utilized diverse network exploration commands with nmap to extract information about both the network and the host, providing additional details that could be exploited for potential malicious attacks on a target.