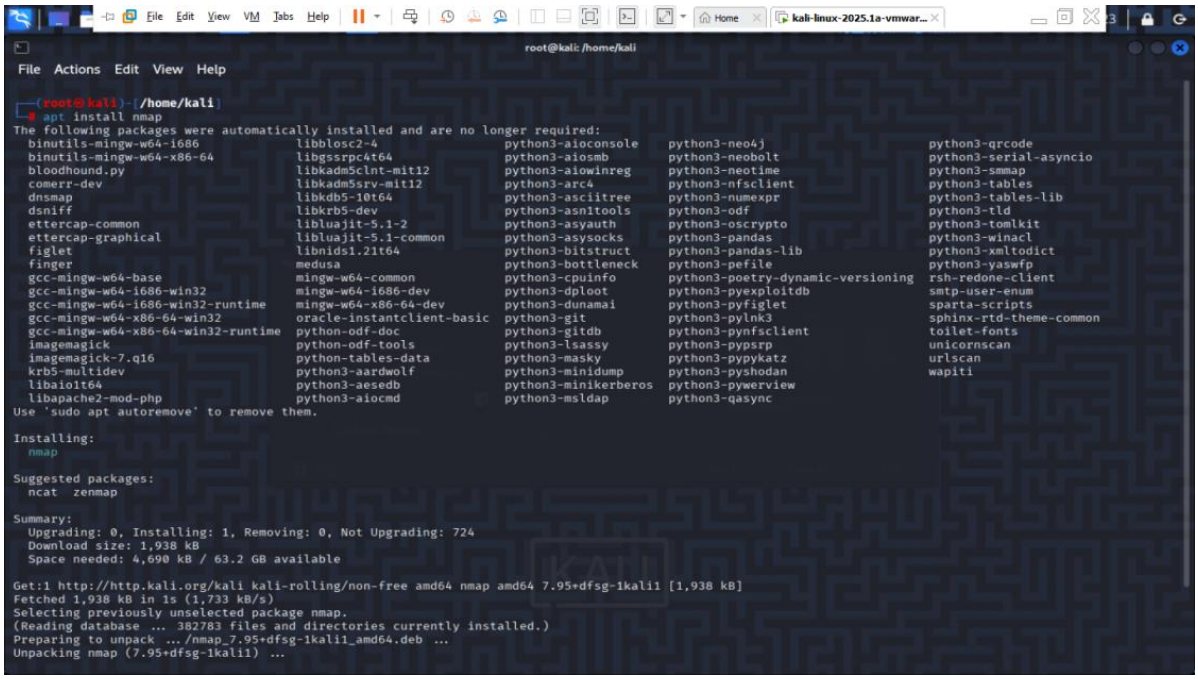
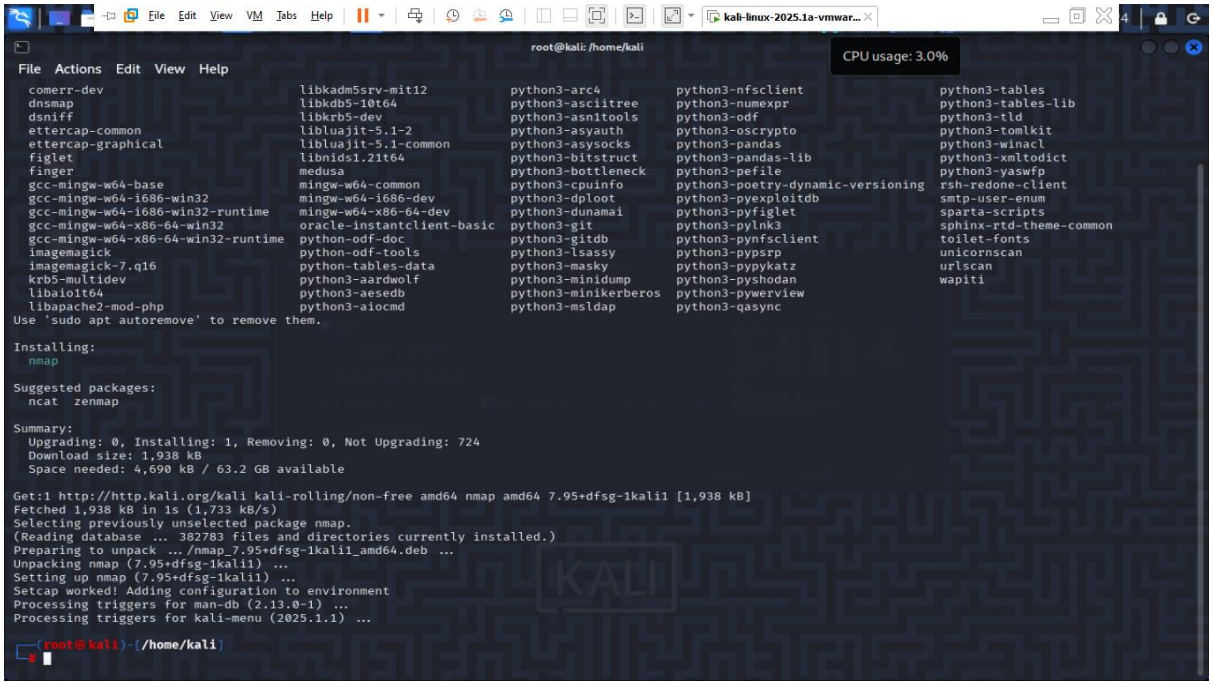
Operating system used : Kali Linux

Tools Used : NMAP, Wireshark

Performed by Shourya Sharma

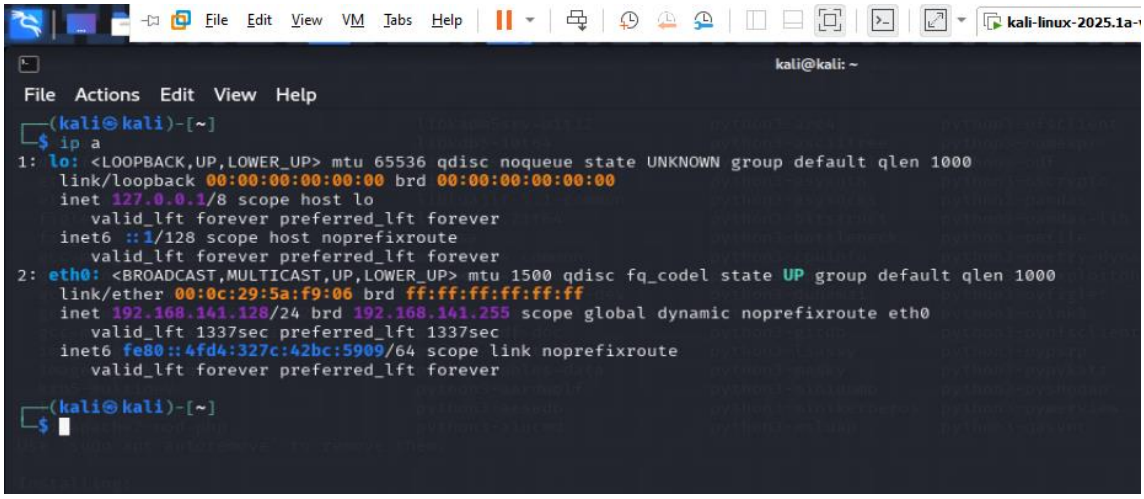
1. Installation of NMAP





2. Identification of Local IP Range

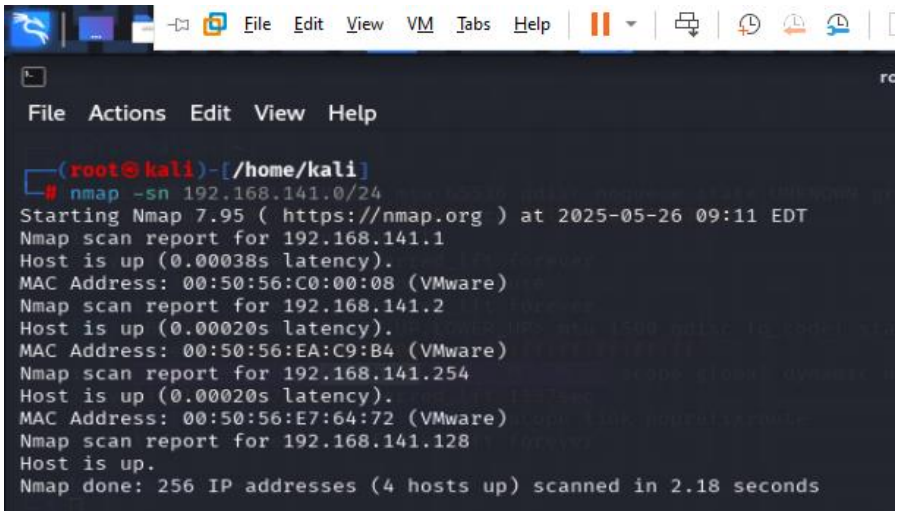
2.1. Checking IP Address



2.2. Scanning and Identifying Ports

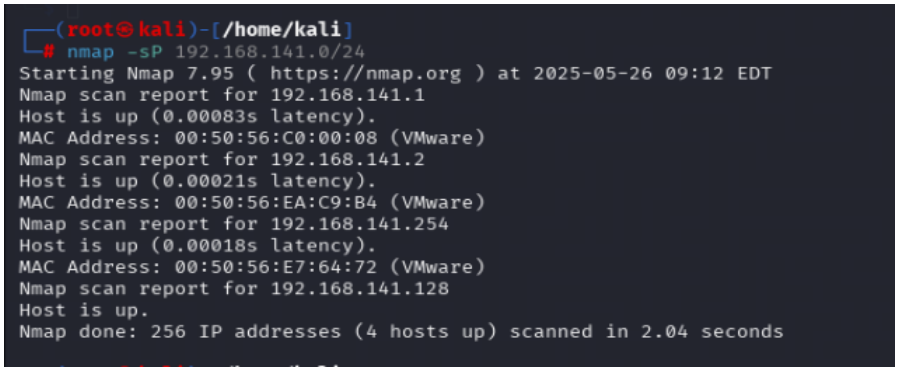
2.2.1 Scanning Local Subnet

Code used : nmap –sn 192.168.141.0/24



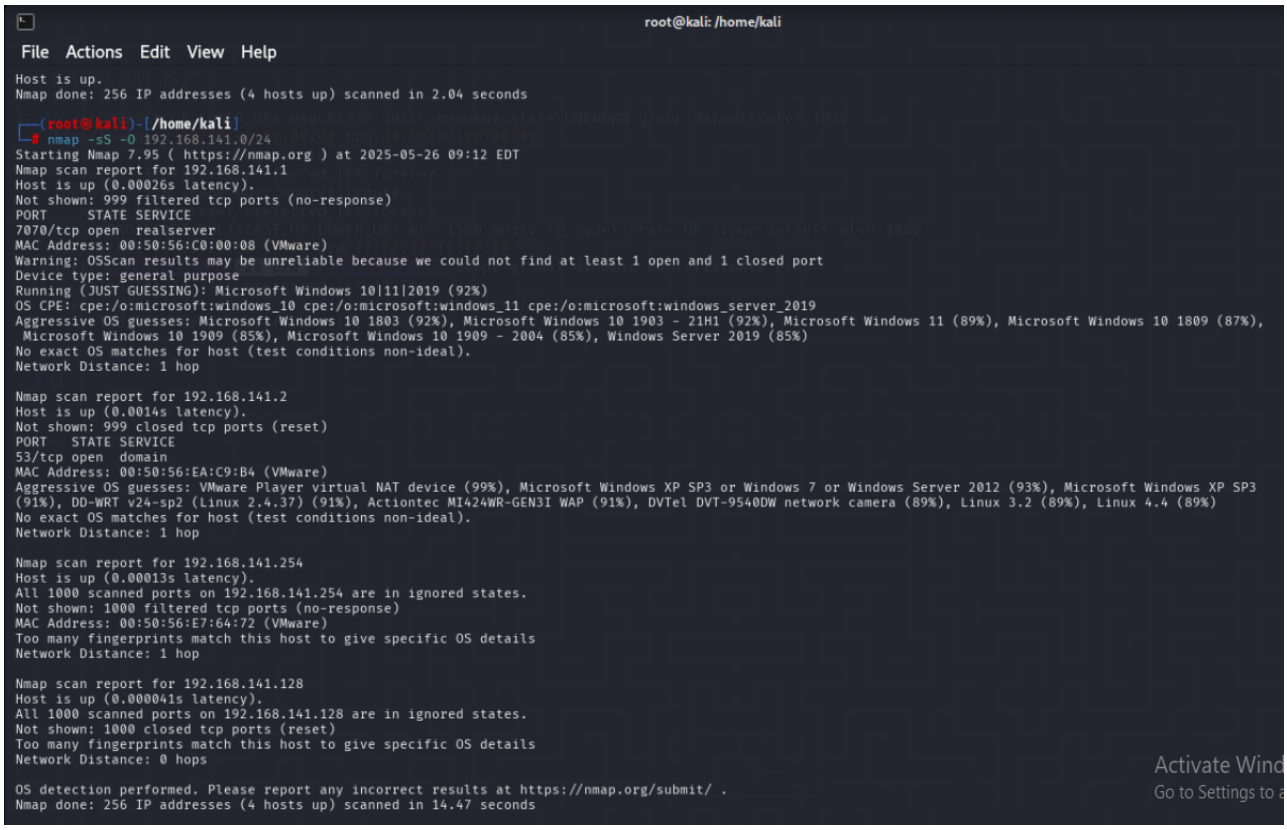
2.2.2 Port Scanning.

Code Used : nmap –sP 192.168.141.0/24



3. Performing TCP-SYN Scan

3.1. OS (Operating System) Identification with Stealth Scan



```
root@kali: /home/kali
File  Actions  Edit  View  Help
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.04 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -O 192.168.141.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 09:12 EDT
Nmap scan report for 192.168.141.1
Host is up (0.00026s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
7070/tcp open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|11|2019 (92%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_server_2019
Aggressive OS guesses: Microsoft Windows 10 1803 (92%), Microsoft Windows 10 1903 - 21H1 (92%), Microsoft Windows 11 (89%), Microsoft Windows 10 1809 (87%),
 Microsoft Windows 10 1909 (85%), Microsoft Windows 10 1909 - 2004 (85%), Windows Server 2019 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.141.2
Host is up (0.0014s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:EA:C9:B4 (VMware)
Aggressive OS guesses: VMware Player virtual NAT device (99%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (93%), Microsoft Windows XP SP3
(91%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Actiontec MI424WR-GEN3I WAP (91%), DVTel DVT-9540DW network camera (89%), Linux 3.2 (89%), Linux 4.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.141.254
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.141.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E7:64:72 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.141.128
Host is up (0.000041s latency).
All 1000 scanned ports on 192.168.141.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 14.47 seconds
```

4. Finding & Observations

4.1. It is observed that 4 IP Addresses were found, those being

- 192.168.141.1
- 192.168.141.2
- 192.168.141.254
- 192.168.141.128

Out of those 4 IP Addresses only 2 were found to be functional, other 2 were in ignored state

4.2. IP Address with open ports are:-

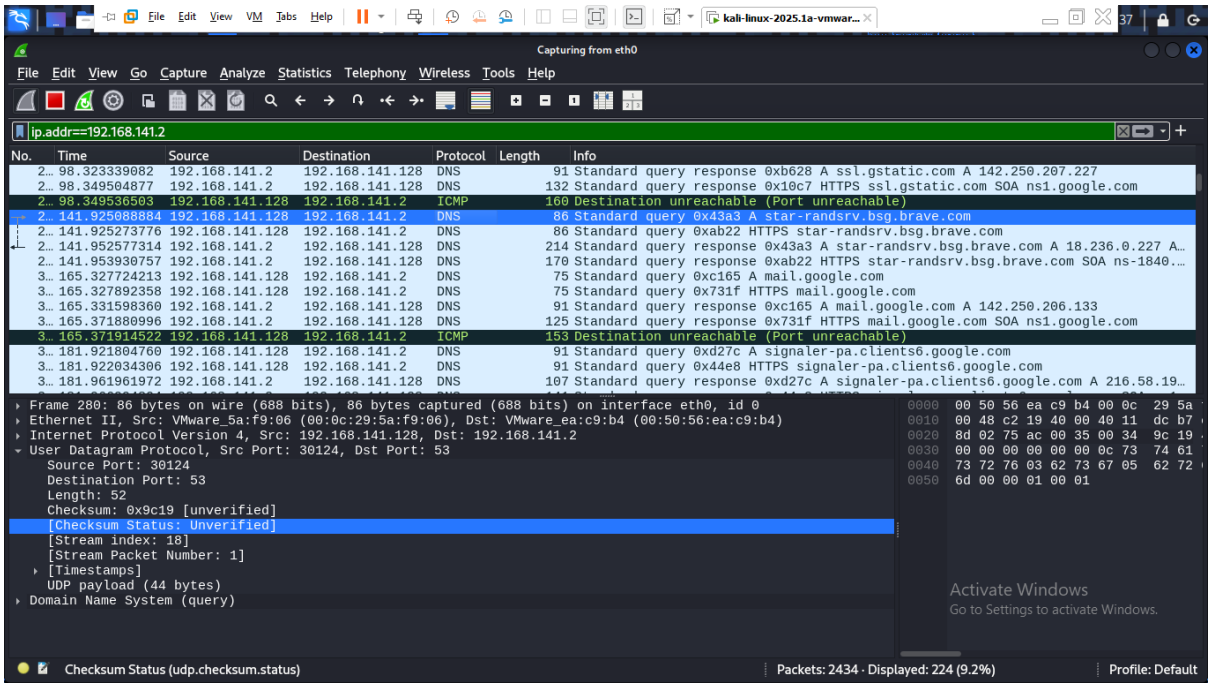
1. 192.168.141.1 – 7070
- 7070 – Commonly used for Media streaming, it is now is used for RealPlayer streaming (RTSP – Real-Time Streaming Protocol)
2. 192.168.141.2 – 53
- 53 – It is the default port used by the DNS (Domain Name System) to establish and communicate between the Client & the Server.

4.3 Operating System

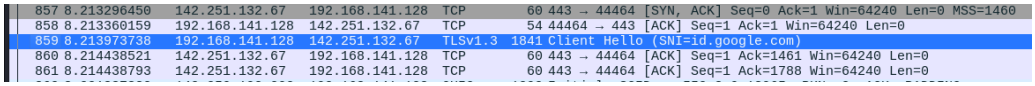
- According to the scanning it is found that the OS maybe Windows 10/11

5. Wireshark Analysis

1. Traffic travelling to and from the IP Address 192.168.141.2



2. Behind the scenes when a user tries to access a website (in this case google is the example)



Here the user sends an request to the internet to access google.com

1. Client → Server	SYN	Request to connect
2. Server → Client	SYN, ACK	Accept & respond
3. Client → Server	ACK	Final confirmation

In this manner the connection between the client and the server is established and the user is able to connect to the internet.

6. Commonly run services on Port 53 & 7070

- 53 – It is the default port used by the DNS (Domain Name System) to establish and communicate between the Client & the Server.
- 7070 – Commonly used for Media streaming, it is now is used for RealPlayer streaming (RTSP – Real-Time Streaming Protocol)

7. Risks on Open port

While useful to communicate some common risks that run on open ports are

- Unauthorized access - Open ports can highlight services that can exploit to get admission in the attacker system.
- Religion exploitation - Weaknesses (eg, old software) can be targeted in listening services on open ports, which can be targeted.
- Information leakage - Misconfed services can reveal sensitive information like system banners, user names or internal IP. Ports such as
- Brute-Force attack-22 (SSH) or 3389 (RDP) can be targeted for password-hired attacks.
- Malware communication-open port can be used by malware for command-end-control (C2) or data exfoliation.

8. Saving the File

- Command used : nmap –sS –O 192.168.141.0/21 –oN Scan-Results.txt
  - This saves the file in normal TXT Format