Task 1: Network Scanning using Nmap

Step 1: Task Understanding

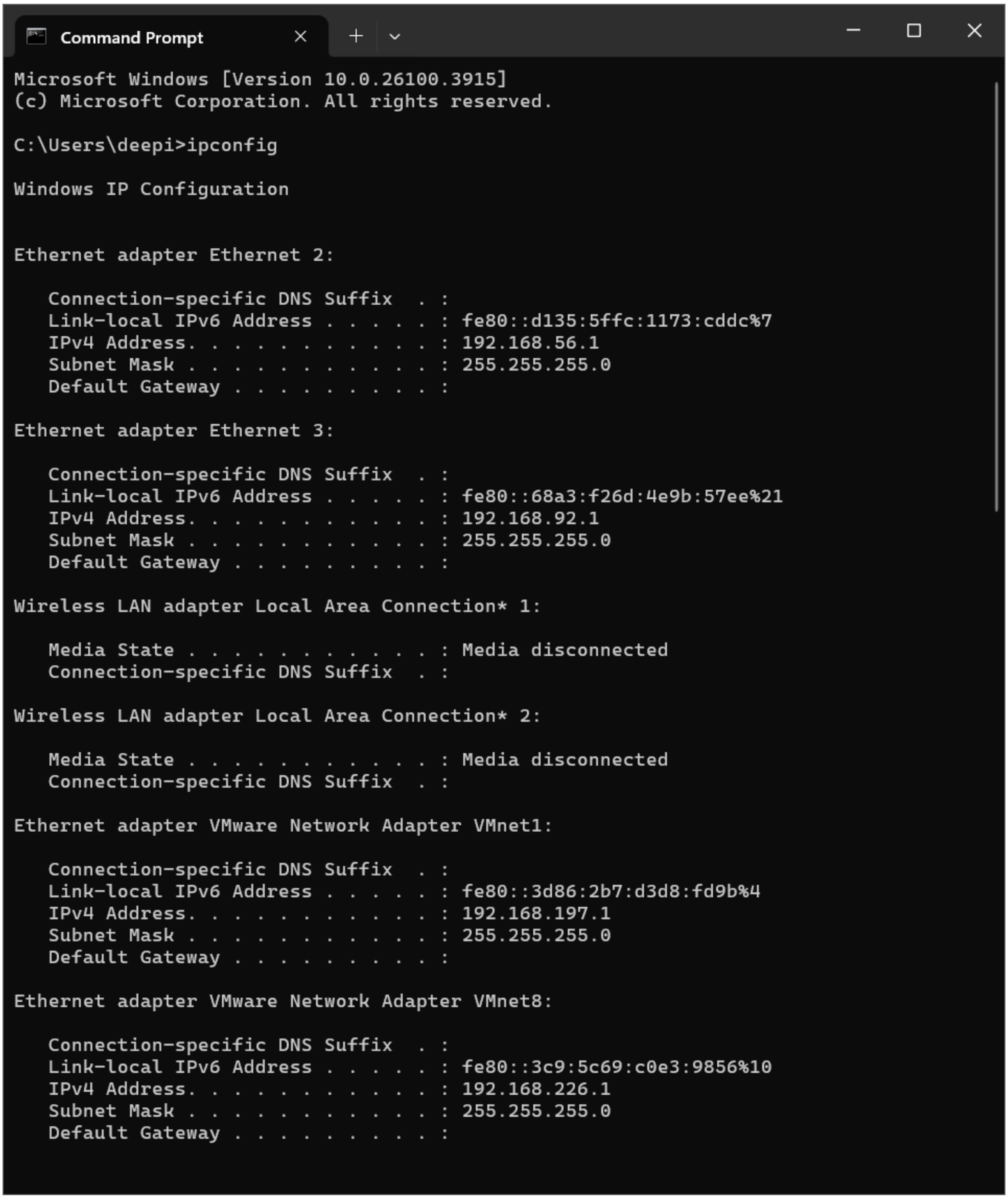
I started by understanding the task objective: to perform a local network scan using Nmap and identify open ports to learn about network exposure.

Step 2: Nmap Installation

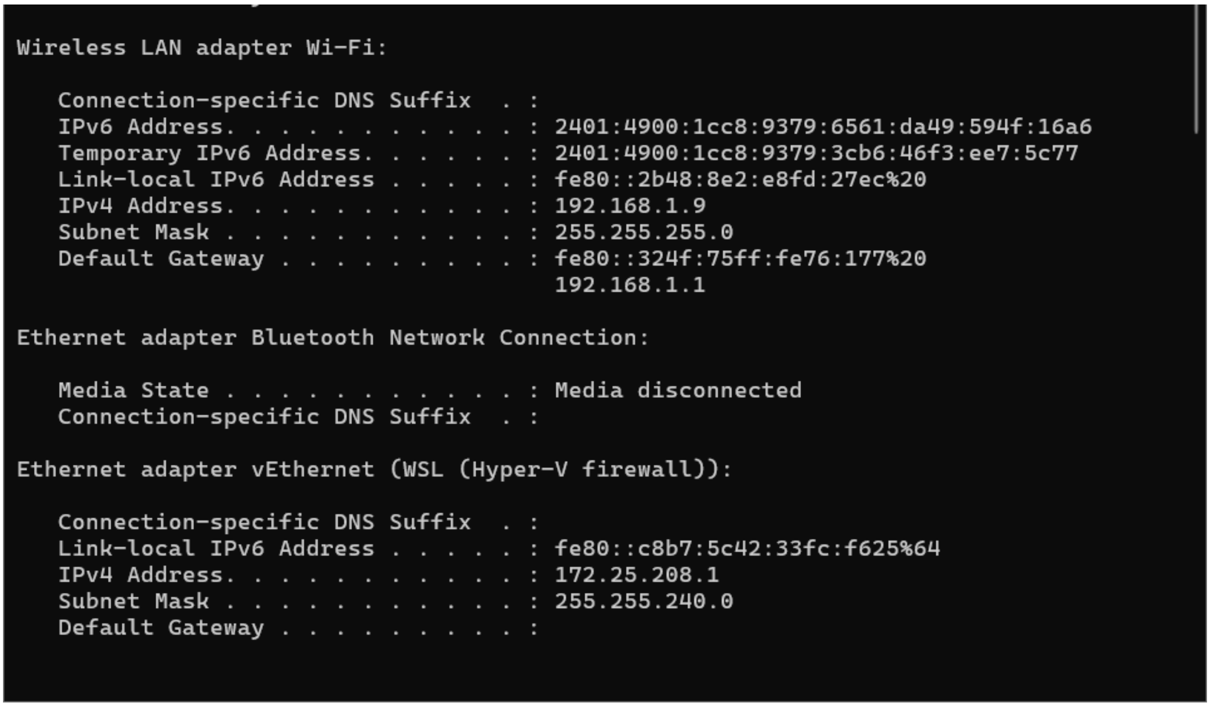
I downloaded and installed Nmap from its official website:
🔗 https://www.kali.org/tools/nmap/
I ensured it was properly added to the system PATH so I could use it in the Command Prompt.

Step 3: Finding Local IP Range

Using the command ipconfig, I found my IPv4 address (192.168.1.9) and identified the network range as 192.168.1.0/24.



```
Microsoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

C:\Users\deepi>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d135:5ffc:1173:cddc%7
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::68a3:f26d:4e9b:57ee%21
   IPv4 Address. . . . . . . . . . . : 192.168.92.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3d86:2b7:d3d8:fd9b%4
   IPv4 Address. . . . . . . . . . . : 192.168.197.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3c9:5c69:c0e3:9856%10
   IPv4 Address. . . . . . . . . . . : 192.168.226.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

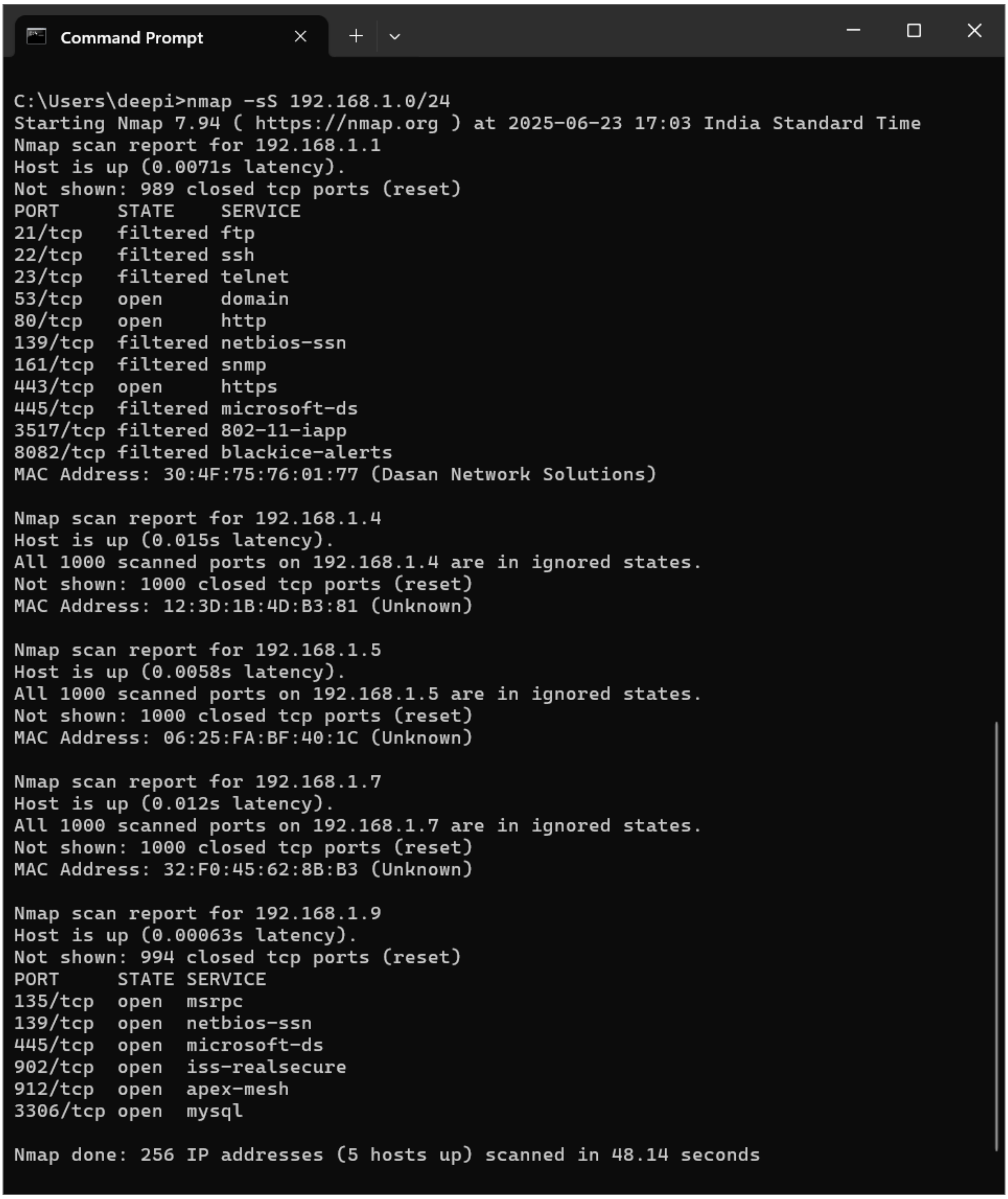


```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:1cc8:9379:6561:da49:594f:16a6
   Temporary IPv6 Address. . . . . . : 2401:4900:1cc8:9379:3cb6:46f3:ee7:5c77
   Link-local IPv6 Address . . . . . : fe80::2b48:8e2:e8fd:27ec%20
   IPv4 Address. . . . . . . . . . . : 192.168.1.9
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::324f:75ff:fe76:177%20
                                       192.168.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter vEthernet (WSL (Hyper-V firewall)):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c8b7:5c42:33fc:f625%64
   IPv4 Address. . . . . . . . . . . : 172.25.208.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
```

Step 4: Running the TCP SYN Scan

Command used: nmap -sS 192.168.1.0/2

This performed a TCP SYN scan to discover live devices and their open ports.



```
C:\Users\deepi>nmap -sS 192.168.1.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-06-23 17:03 India Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.0071s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
53/tcp   open     domain
80/tcp   open     http
139/tcp  filtered netbios-ssn
161/tcp  filtered snmp
443/tcp  open     https
445/tcp  filtered microsoft-ds
3517/tcp filtered 802-11-iapp
8082/tcp filtered blackice-alerts
MAC Address: 30:4F:75:76:01:77 (Dasan Network Solutions)

Nmap scan report for 192.168.1.4
Host is up (0.015s latency).
All 1000 scanned ports on 192.168.1.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 12:3D:1B:4D:B3:81 (Unknown)

Nmap scan report for 192.168.1.5
Host is up (0.0058s latency).
All 1000 scanned ports on 192.168.1.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 06:25:FA:BF:40:1C (Unknown)

Nmap scan report for 192.168.1.7
Host is up (0.012s latency).
All 1000 scanned ports on 192.168.1.7 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 32:F0:45:62:8B:B3 (Unknown)

Nmap scan report for 192.168.1.9
Host is up (0.00063s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
3306/tcp open  mysql

Nmap done: 256 IP addresses (5 hosts up) scanned in 48.14 seconds
```

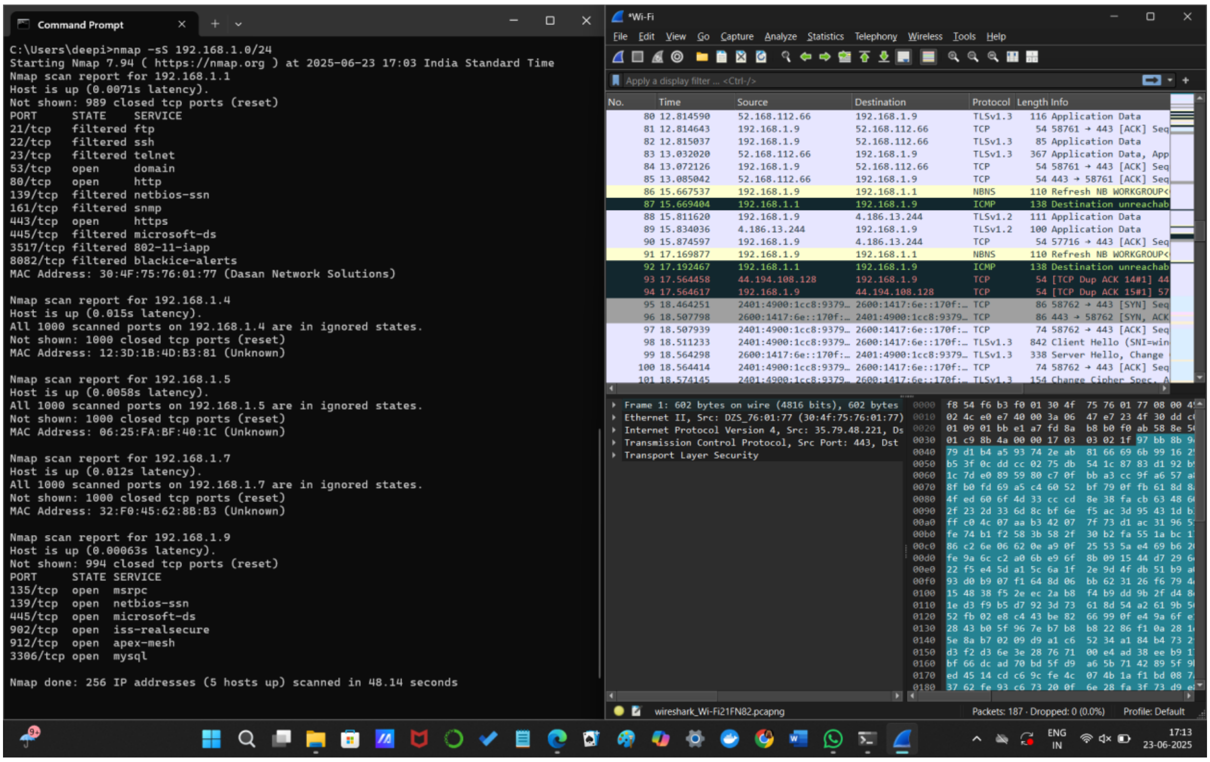
Step 5: Saving the Scan Results

Command used: nmap -sS 192.168.1.0/24 > scan_result.txt

This saved the results to a text file for documentation.

Step 6: (Optional) Wireshark Usage

I opened Wireshark, selected my network interface, and captured traffic during the scan to visualize the packets being exchanged.



Command Prompt
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
wireshark_Wi-Fi21FN82.pcapng
Packets: 187 · Dropped: 0 (0.0%)
Profile: Default
ENG
IN
17:13
23-06-2025

```
C:\Users\deepi>nmap -sS 192.168.1.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-06-23 17:03 India Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.0071s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
53/tcp   open     domain
80/tcp   open     http
139/tcp  filtered netbios-ssn
161/tcp  filtered snmp
443/tcp  open     https
445/tcp  filtered microsoft-ds
3517/tcp filtered 802-11-iapp
8082/tcp filtered blackice-alerts
MAC Address: 30:4F:75:76:01:77 (Dasan Network Solutions)

Nmap scan report for 192.168.1.4
Host is up (0.015s latency).
All 1000 scanned ports on 192.168.1.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 12:3D:1B:4D:B3:81 (Unknown)

Nmap scan report for 192.168.1.5
Host is up (0.0058s latency).
All 1000 scanned ports on 192.168.1.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 06:25:FA:BF:40:1C (Unknown)

Nmap scan report for 192.168.1.7
Host is up (0.012s latency).
All 1000 scanned ports on 192.168.1.7 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 32:F0:45:62:8B:B3 (Unknown)

Nmap scan report for 192.168.1.9
Host is up (0.00063s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
3306/tcp open  mysql

Nmap done: 256 IP addresses (5 hosts up) scanned in 48.14 seconds
```

```
No.  Time       Source                  Destination             Protocol Length Info
  80 12.814590  52.168.112.66           192.168.1.9             TLSv1.3  116 Application Data
  81 12.814643  192.168.1.9             52.168.112.66           TCP       54 58761 → 443 [ACK] Seq
  82 12.815037  192.168.1.9             52.168.112.66           TLSv1.3   85 Application Data
  83 13.032020  52.168.112.66           192.168.1.9             TLSv1.3  367 Application Data, App
  84 13.072126  192.168.1.9             52.168.112.66           TCP       54 58761 → 443 [ACK] Seq
  85 13.085042  52.168.112.66           192.168.1.9             TCP       54 443 → 58761 [ACK] Seq
  86 15.667537  192.168.1.9             192.168.1.1             NBNS     110 Refresh NB WORKGROUP<
  87 15.669404  192.168.1.1             192.168.1.9             ICMP     138 Destination unreachab
  88 15.811620  192.168.1.9             4.186.13.244            TLSv1.2  111 Application Data
  89 15.834036  4.186.13.244            192.168.1.9             TLSv1.2  100 Application Data
  90 15.874597  192.168.1.9             4.186.13.244            TCP       54 57716 → 443 [ACK] Seq
  91 17.169877  192.168.1.9             192.168.1.1             NBNS     110 Refresh NB WORKGROUP<
  92 17.192467  192.168.1.1             192.168.1.9             ICMP     138 Destination unreachab
  93 17.564458  44.194.108.128          192.168.1.9             TCP       54 [TCP Dup ACK 14#1] 44
  94 17.564617  192.168.1.9             44.194.108.128          TCP       54 [TCP Dup ACK 15#1] 57
  95 18.464251  2401:4900:1cc8:9379…    2600:1417:6e::170f:…    TCP       86 58762 → 443 [SYN] Seq
  96 18.507798  2600:1417:6e::170f:…    2401:4900:1cc8:9379…    TCP       86 443 → 58762 [SYN, ACK
  97 18.507939  2401:4900:1cc8:9379…    2600:1417:6e::170f:…    TCP       74 58762 → 443 [ACK] Seq
  98 18.511233  2401:4900:1cc8:9379…    2600:1417:6e::170f:…    TLSv1.3  842 Client Hello (SNI=win
  99 18.564298  2600:1417:6e::170f:…    2401:4900:1cc8:9379…    TLSv1.3  338 Server Hello, Change
 100 18.564414  2401:4900:1cc8:9379…    2600:1417:6e::170f:…    TCP       74 58762 → 443 [ACK] Seq
 101 18.574145  2401:4900:1cc8:9379…    2600:1417:6e::170f:…    TLSv1.3  154 Change Cipher Spec, A
```

```
› Frame 1: 602 bytes on wire (4816 bits), 602 bytes
› Ethernet II, Src: DZS_76:01:77 (30:4f:75:76:01:77)
› Internet Protocol Version 4, Src: 35.79.48.221, Ds
› Transmission Control Protocol, Src Port: 443, Dst
› Transport Layer Security
```

```
0000  f8 54 f6 b3 f0 01 30 4f  75 76 01 77 08 00
0010  02 4c e0 e7 40 00 3a 06  47 e7 23 4f 30 dd
0020  01 09 01 bb e1 a7 fd 8a  b8 b0 f0 ab 58 8e
0030  01 c9 8b 4a 00 00 17 03  03 02 1f 97 bb 8b
0040  79 d1 b4 a5 93 74 2e ab  81 66 69 6b 99 16
0050  b5 3f 0c dd cc 02 75 db  54 1c 87 83 d1 92
0060  1c 7d e0 89 59 80 c7 0f  bb a3 cc 9f a6 57
0070  8f b0 fd 69 a5 c4 60 52  bf 79 0f fb 61 8d
0080  4f ed 60 6f 4d 33 cc cd  8e 38 fa cb 63 48
0090  2f 23 2d 33 6d 8c bf 6e  f5 ac 3d 95 43 1d
00a0  ff c0 4c 07 aa b3 42 07  7f 73 d1 ac 31 96
00b0  fe 74 b1 f2 58 3b 58 2f  30 b2 fa 55 1a bc
00c0  86 c2 6e 06 62 0e a9 0f  25 53 5a e4 69 b6
00d0  fe 9a 6c c2 a0 6b e9 6f  8b 09 15 44 d7 29
00e0  22 f5 e4 5d a1 5c 6a 1f  2e 9d 4f db 51 b9
00f0  93 d0 b9 07 f1 64 8d 06  bb 62 31 26 f6 79
0100  15 48 38 f5 2e ec 2a b8  f4 b9 dd 9b 2f d4
0110  1e d3 f9 b5 d7 92 3d 73  61 8d 54 a2 61 9b
0120  52 fb 02 e8 c4 43 be 82  66 99 0f e4 9a 6f
0130  28 43 b0 5f 96 7e b7 b8  b8 22 86 f1 0a 28
0140  5e 8a b7 02 09 d9 a1 c6  52 34 a1 84 b4 73
0150  d3 f2 d3 6e 3e 28 76 71  00 e4 ad 38 ee b9
0160  bf 66 dc ad 70 bd 5f d9  a6 5b 71 42 89 5f
0170  ed 45 14 cd c6 9c fe 4c  07 4b 1a f1 bd 08
0180  37 62 fe 93 c6 73 20 0f  6e 28 fa 3f 73 d9
```

Step 7: Analyzing the Results

I reviewed the open ports and IPs found in the scan. Then I researched what services commonly run on those ports and identified possible risks.

Step 8: GitHub Submission

I uploaded the scan_result.txt file and a detailed README.md to my GitHub repository along with the answers to the interview questions.

What I Learned

- How to identify IP ranges and scan a local network using Nmap
- The working of TCP SYN scans
- How to observe network traffic using Wireshark
- The significance of port scanning and open ports
- Basics of network reconnaissance and network security

Key Topics Covered

- Port Scanning
- TCP SYN Scan
- IP Ranges
- Network Reconnaissance
- Open Ports
- Network Security Basics

Interview Questions:

1. What is an open port?

An open port is a network port that is configured to accept incoming connections. It indicates that a service or application is actively listening and can be accessed remotely.

2. How does Nmap perform a TCP SYN scan?

Nmap sends a SYN (synchronize) packet to the target port. If it receives a SYN-ACK (acknowledgement) response, it identifies the port as open. If it receives an RST (reset) response, the port is closed. Since the full TCP handshake isn't completed, this scan is fast and stealthy.

3. What risks are associated with open ports?

Open ports can expose vulnerable services to attackers. If those services are misconfigured or outdated, they can be exploited to gain unauthorized access, install malware, or gather sensitive data.

4. Explain the difference between TCP and UDP scanning.

TCP scanning uses a reliable, connection-based protocol and gives clearer results based on responses. UDP scanning is connectionless and more stealthy, but harder to interpret since many services don’t reply unless queried correctly.

5. How can open ports be secured?

Open ports can be secured by using firewalls to block unused ports, disabling unnecessary services, using strong authentication, applying patches and updates, and regularly monitoring network traffic.

6. What is a firewall's role regarding ports?

A firewall filters incoming and outgoing network traffic. It can block or allow specific ports and services, helping to reduce the attack surface and prevent unauthorized access.

7. What is a port scan and why do attackers perform it?

A port scan is a method of probing a host for open ports. Attackers perform it to identify which services are running and look for vulnerabilities they can exploit to gain access or cause damage.

8. How does Wireshark complement port scanning?

Wireshark captures and analyzes live network traffic. It helps visualize how scanning traffic looks on the network and how devices respond to scanning attempts, making it useful for learning and detecting suspicious behavior.