Network Port Scanning and Packet Analysis Report

Shubham Date: August 4, 2025

1 Objective

The goal of this task is to scan the local network to identify live hosts, open ports, and analyze network packets using Wireshark. This exercise builds practical knowledge of how services are exposed on a network and what information can be collected during reconnaissance.

2 Tools Used

- **Nmap** – for scanning the local network and identifying open/closed ports.
- **Wireshark** – for capturing and analyzing network packets.
- **Kali Linux** – as the attack machine.
- **Metasploitable 2** – as the vulnerable target VM (used for IP response only).

3 Network Scan with Nmap

3.1 Identifying IP Range

We first identified the local IP range using ‘ip a‘. In our setup, it was determined as `192.168.153.0/24`.

3.2 SYN Scan Execution

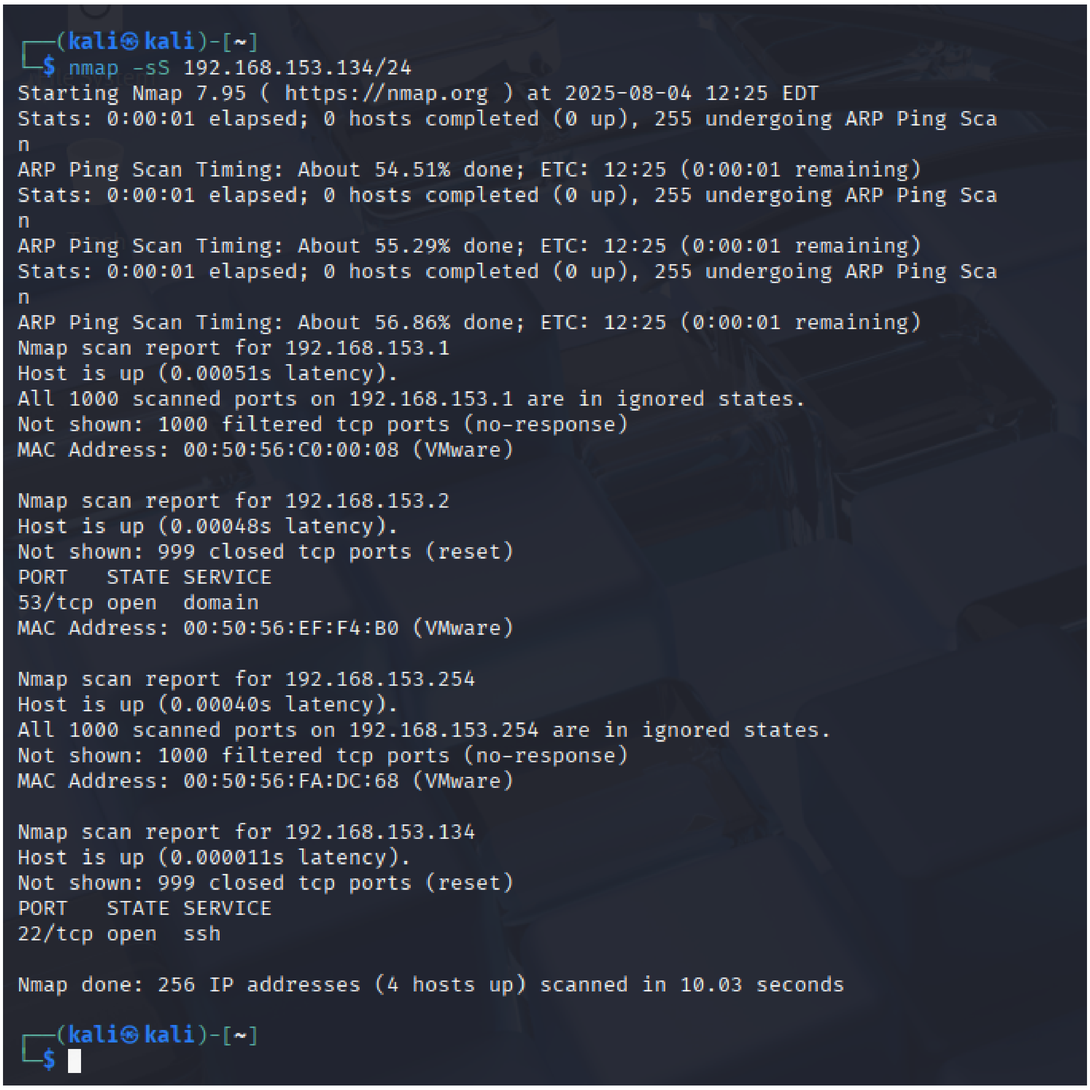
```
nmap -sS 192.168.153.0/24
```

The scan discovered 4 live hosts. Below is a summary of some relevant ports:

- **192.168.153.2** – Port 53 (DNS) open
- **192.168.153.134** – Port 22 (SSH) open

4 Packet Capture and Filtering with Wireshark

We captured packets using Wireshark during the Nmap scan and applied three filters to analyze different TCP behaviors:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.153.134/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 12:25 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Sca
n
ARP Ping Scan Timing: About 54.51% done; ETC: 12:25 (0:00:01 remaining)
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Sca
n
ARP Ping Scan Timing: About 55.29% done; ETC: 12:25 (0:00:01 remaining)
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Sca
n
ARP Ping Scan Timing: About 56.86% done; ETC: 12:25 (0:00:01 remaining)
Nmap scan report for 192.168.153.1
Host is up (0.00051s latency).
All 1000 scanned ports on 192.168.153.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.153.2
Host is up (0.00048s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:EF:F4:B0 (VMware)

Nmap scan report for 192.168.153.254
Host is up (0.00040s latency).
All 1000 scanned ports on 192.168.153.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:FA:DC:68 (VMware)

Nmap scan report for 192.168.153.134
Host is up (0.000011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 10.03 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

Figure 1: Figure 1: Nmap Output Showing Live Hosts and Open Ports

4.1 1. SYN Packets (Connection Attempts)

```
tcp.flags.syn == 1 and tcp.flags.ack == 0
```

This filter shows attempts to initiate TCP connections.

4.2 2. SYN-ACK Packets (Open Ports)

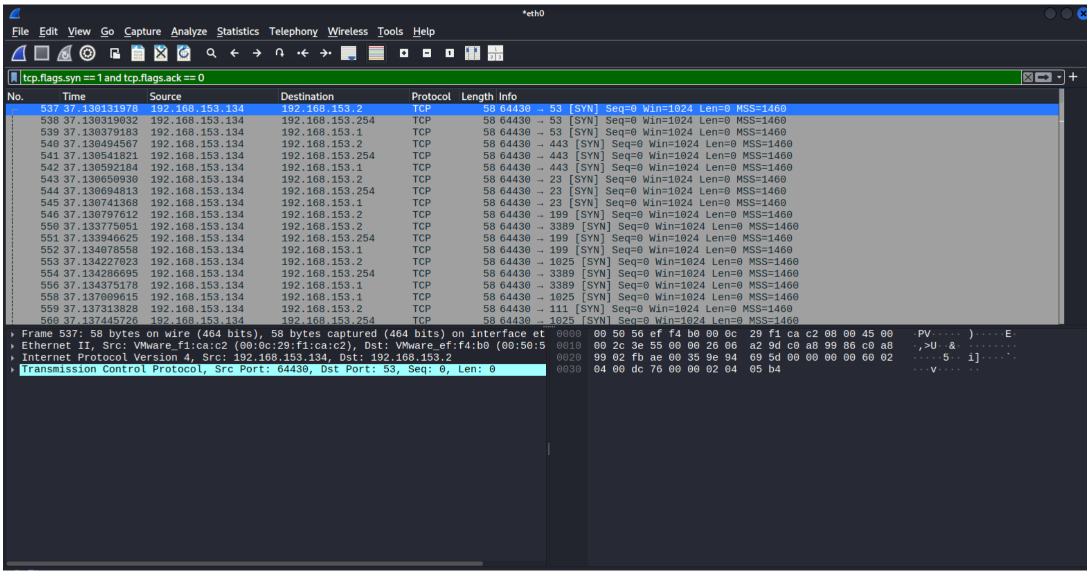
```
tcp.flags.syn == 1 and tcp.flags.ack == 1
```

This confirms which ports are open by checking the SYN-ACK responses.

4.3 3. RST Packets (Closed Ports)

```
tcp.flags.reset == 1
```

Ports sending RST indicate that they are closed.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

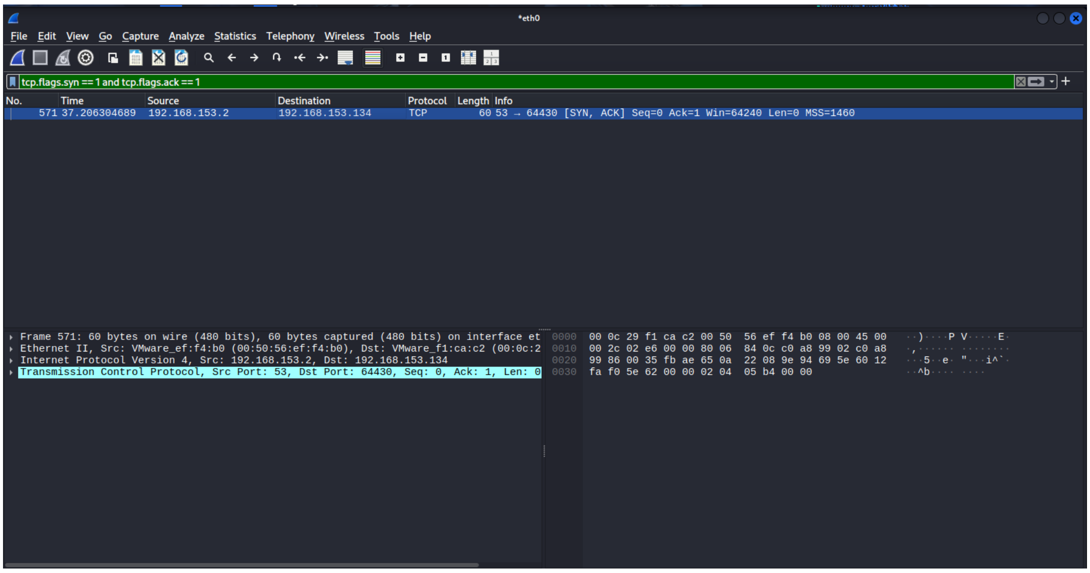
```
tcp.flags.syn == 1 and tcp.flags.ack == 0
```

```
No.  Time         Source           Destination      Protocol Length Info
 537 37.130131978 192.168.153.134  192.168.153.2    TCP      58 64430 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 538 37.130319032 192.168.153.134  192.168.153.254  TCP      58 64430 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 539 37.130379183 192.168.153.134  192.168.153.1    TCP      58 64430 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 540 37.130494567 192.168.153.134  192.168.153.2    TCP      58 64430 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 541 37.130541821 192.168.153.134  192.168.153.254  TCP      58 64430 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 542 37.130592184 192.168.153.134  192.168.153.1    TCP      58 64430 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 543 37.130650930 192.168.153.134  192.168.153.2    TCP      58 64430 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 544 37.130694813 192.168.153.134  192.168.153.254  TCP      58 64430 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 545 37.130741368 192.168.153.134  192.168.153.1    TCP      58 64430 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 546 37.130797612 192.168.153.134  192.168.153.2    TCP      58 64430 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 550 37.133775051 192.168.153.134  192.168.153.2    TCP      58 64430 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 551 37.133946625 192.168.153.134  192.168.153.254  TCP      58 64430 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 552 37.134078558 192.168.153.134  192.168.153.1    TCP      58 64430 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 553 37.134227023 192.168.153.134  192.168.153.2    TCP      58 64430 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 554 37.134286695 192.168.153.134  192.168.153.254  TCP      58 64430 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 556 37.134375178 192.168.153.134  192.168.153.1    TCP      58 64430 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 558 37.137009615 192.168.153.134  192.168.153.1    TCP      58 64430 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 559 37.137313828 192.168.153.134  192.168.153.2    TCP      58 64430 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 560 37.137445726 192.168.153.134  192.168.153.254  TCP      58 64430 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

```
› Frame 537: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface et
› Ethernet II, Src: VMware_f1:ca:c2 (00:0c:29:f1:ca:c2), Dst: VMware_ef:f4:b0 (00:50:5
› Internet Protocol Version 4, Src: 192.168.153.134, Dst: 192.168.153.2
› Transmission Control Protocol, Src Port: 64430, Dst Port: 53, Seq: 0, Len: 0
```

```
0000  00 50 56 ef f4 b0 00 0c  29 f1 ca c2 08 00 45 00   ·PV·····)·····E·
0010  00 2c 3e 55 00 00 26 06  a2 9d c0 a8 99 86 c0 a8   ·,>U··&·········
0020  99 02 fb ae 00 35 9e 94  69 5d 00 00 00 00 60 02   ·····5··i]····`·
0030  04 00 dc 76 00 00 02 04  05 b4                     ···v······
```

Figure 2: Figure 2: Wireshark SYN Packet Capture


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.syn == 1 and tcp.flags.ack == 1
```

```
No.  Time         Source          Destination      Protocol Length Info
 571 37.206304689 192.168.153.2   192.168.153.134  TCP      60 53 → 64430 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
```

```
› Frame 571: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface et
› Ethernet II, Src: VMware_ef:f4:b0 (00:50:56:ef:f4:b0), Dst: VMware_f1:ca:c2 (00:0c:2
› Internet Protocol Version 4, Src: 192.168.153.2, Dst: 192.168.153.134
› Transmission Control Protocol, Src Port: 53, Dst Port: 64430, Seq: 0, Ack: 1, Len: 0
```

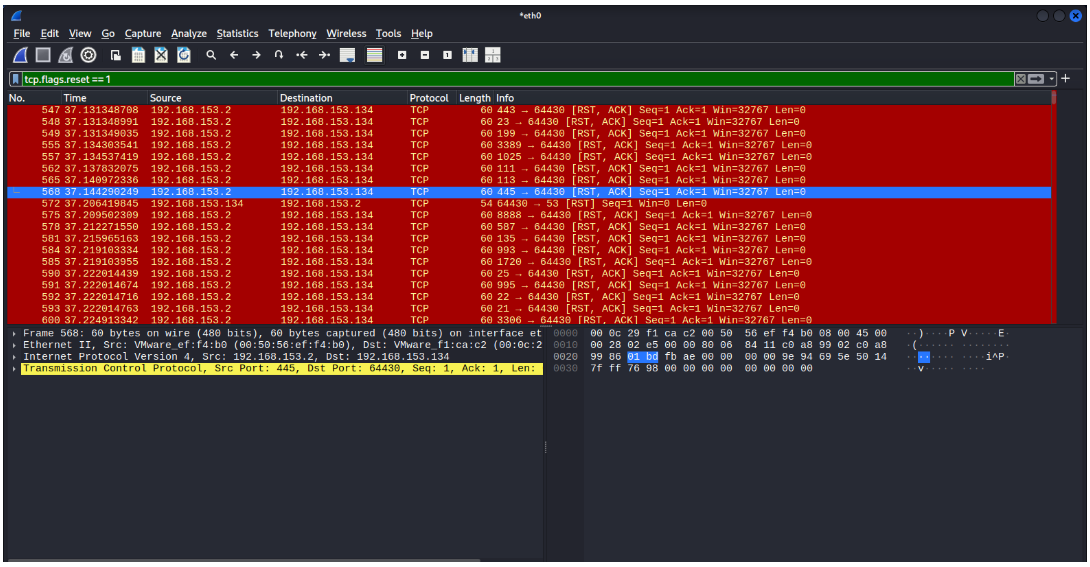
```
0000  00 0c 29 f1 ca c2 00 50  56 ef f4 b0 08 00 45 00   ··)····PV·····E·
0010  00 2c 02 e6 00 00 80 06  84 0c c0 a8 99 02 c0 a8   ·,··············
0020  99 86 00 35 fb ae 65 0a  22 08 9e 94 69 5e 60 12   ···5··e·"···i^`·
0030  fa f0 5e 62 00 00 02 04  05 b4 00 00               ··^b········
```

Figure 3: Figure 3: Wireshark SYN-ACK Response

5 Common Ports and Their Services

Port	Protocol	Common Service
22	TCP	SSH
53	TCP	DNS
80	TCP	HTTP
443	TCP	HTTPS
3306	TCP	MySQL
21	TCP	FTP

Table 1: Table 1: Common TCP Ports and Services


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.reset == 1
```

```
No.  Time          Source           Destination      Protocol Length Info
547 37.131348708  192.168.153.2    192.168.153.134  TCP      60 443 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
548 37.131348991  192.168.153.2    192.168.153.134  TCP      60 23 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
549 37.131349035  192.168.153.2    192.168.153.134  TCP      60 199 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
555 37.134303541  192.168.153.2    192.168.153.134  TCP      60 3389 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
557 37.134537419  192.168.153.2    192.168.153.134  TCP      60 1025 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
562 37.137832075  192.168.153.2    192.168.153.134  TCP      60 111 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
565 37.140972336  192.168.153.2    192.168.153.134  TCP      60 113 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
568 37.144290249  192.168.153.2    192.168.153.134  TCP      60 445 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
572 37.206419845  192.168.153.134  192.168.153.2    TCP      54 64430 → 53 [RST] Seq=1 Win=0 Len=0
575 37.209502309  192.168.153.2    192.168.153.134  TCP      60 8888 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
578 37.212271550  192.168.153.2    192.168.153.134  TCP      60 587 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
581 37.215965163  192.168.153.2    192.168.153.134  TCP      60 135 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
584 37.219103334  192.168.153.2    192.168.153.134  TCP      60 993 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
585 37.219103955  192.168.153.2    192.168.153.134  TCP      60 1720 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
590 37.222014439  192.168.153.2    192.168.153.134  TCP      60 25 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
591 37.222014674  192.168.153.2    192.168.153.134  TCP      60 995 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
592 37.222014716  192.168.153.2    192.168.153.134  TCP      60 22 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
593 37.222014763  192.168.153.2    192.168.153.134  TCP      60 21 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
600 37.224913342  192.168.153.2    192.168.153.134  TCP      60 3306 → 64430 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
```

```
› Frame 568: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface et
› Ethernet II, Src: VMware_ef:f4:b0 (00:50:56:ef:f4:b0), Dst: VMware_f1:ca:c2 (00:0c:2
› Internet Protocol Version 4, Src: 192.168.153.2, Dst: 192.168.153.134
› Transmission Control Protocol, Src Port: 445, Dst Port: 64430, Seq: 1, Ack: 1, Len:
```

```
0000  00 0c 29 f1 ca c2 00 50  56 ef f4 b0 08 00 45 00   ··)····P V·····E·
0010  00 28 02 e5 00 00 80 06  84 11 c0 a8 99 02 c0 a8   ·(······ ········
0020  99 86 01 bd fb ae 00 00  00 00 9e 94 69 5e 50 14   ········ ····i^P·
0030  7f ff 76 98 00 00 00 00  00 00 00 00               ··v····· ····
```

Figure 4: Figure 4: Wireshark RST Responses for Closed Ports

6 Analysis and Learnings

- Nmap identified multiple active hosts and open ports.
- Port 22 (SSH) was open on the scanned host.
- Port 53 (DNS) was open on another virtual host.
- Wireshark packet filtering helped confirm the behavior of open and closed ports via TCP flags.

7 Conclusion

This lab provided practical exposure to scanning a local network and interpreting TCP handshakes using Wireshark. Such reconnaissance is foundational for vulnerability assessment. This project was limited to port scanning and network packet analysis only — no exploitation frameworks (like Metasploit) were used.

Appendix

Included Files:

- Metasploitable2 Vulnerability Scan.pdf – Nessus HTML export
- Screenshots – Nmap and Wireshark outputs (SYN, SYN-ACK, RST)

This document was written as part of a cybersecurity lab task. All activity occurred in a controlled VM environment.