Local Network Port Scanning and Packet Analysis Report

S M Sravya
sravyaselvi35@gmail.com

1 Objective

The aim of this task is to understand network exposure by discovering live devices and identifying open ports within a local network. The exercise includes performing a TCP SYN scan using Nmap and analyzing packet-level responses using Wireshark.

2 Tools Used

- **Nmap** – For scanning local IP ranges and identifying open or closed ports.
- **Wireshark** – To capture and analyze TCP packet behaviors.
- **Kali Linux** – Used as the scanning system.
- **Virtual Network (VMware)** – Multiple VMs connected in NAT/Host-Only/Bridged mode.

3 Nmap Scan Execution

First, the local IP range was identified using `ip a`. Based on the result, the subnet was defined as:

```
192.168.119.0/24
```

The Nmap TCP SYN scan was run as follows:

```
sudo nmap -sS 192.168.119.0/24
```

This scan discovered multiple live hosts with various port states. A sample output is shown below.

4 Wireshark Packet Analysis

To further validate the scan, Wireshark was used to capture TCP packets during the Nmap scan.

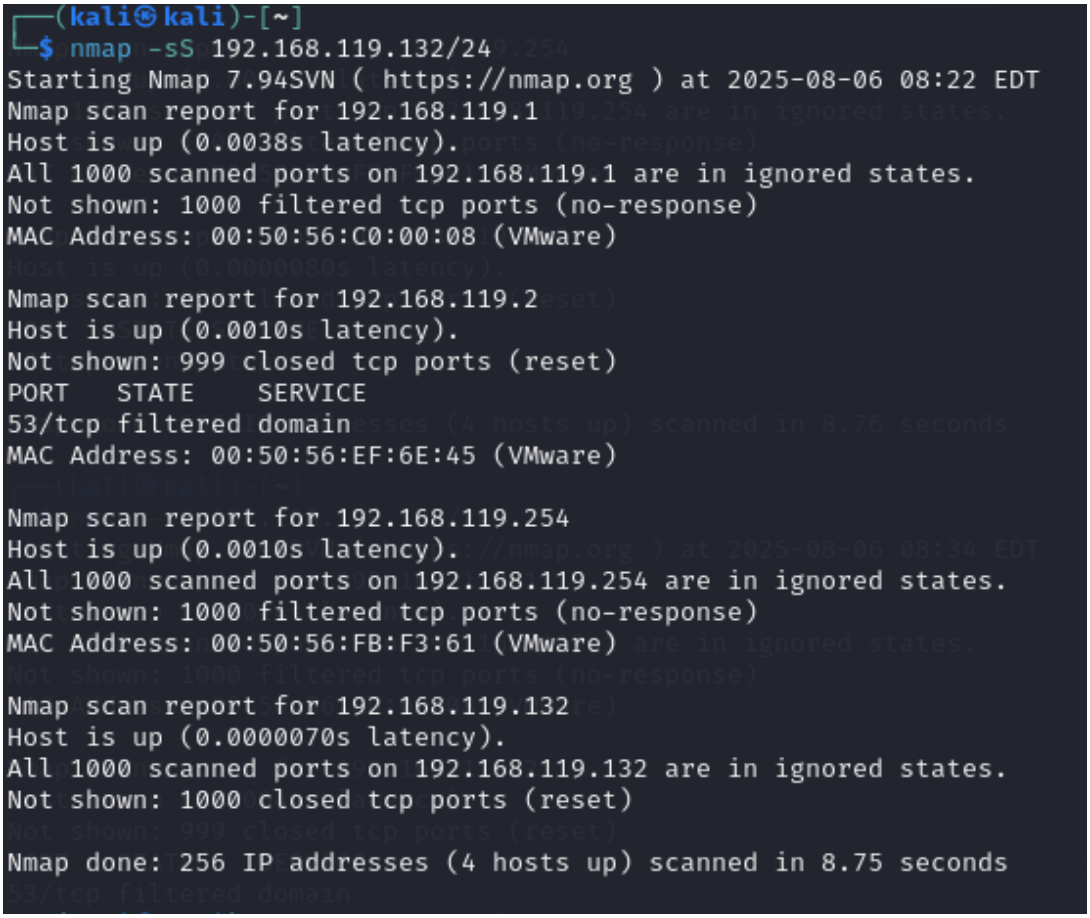

Figure 1: Figure 1: Nmap Output showing Hosts and Port States

4.1 SYN Packets (Connection Attempts)

Filter used:

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

This shows Nmap's initial connection attempts.

4.2 RST Packets (Closed Ports)

Filter used:

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

Closed ports responded with reset packets.

4.3 SYN-ACK Packets (Optional)

Filter:

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

Note: In this scan, no open ports were identified. Therefore, SYN-ACK packets were not observed. You can mention this as a valid observation in your findings.

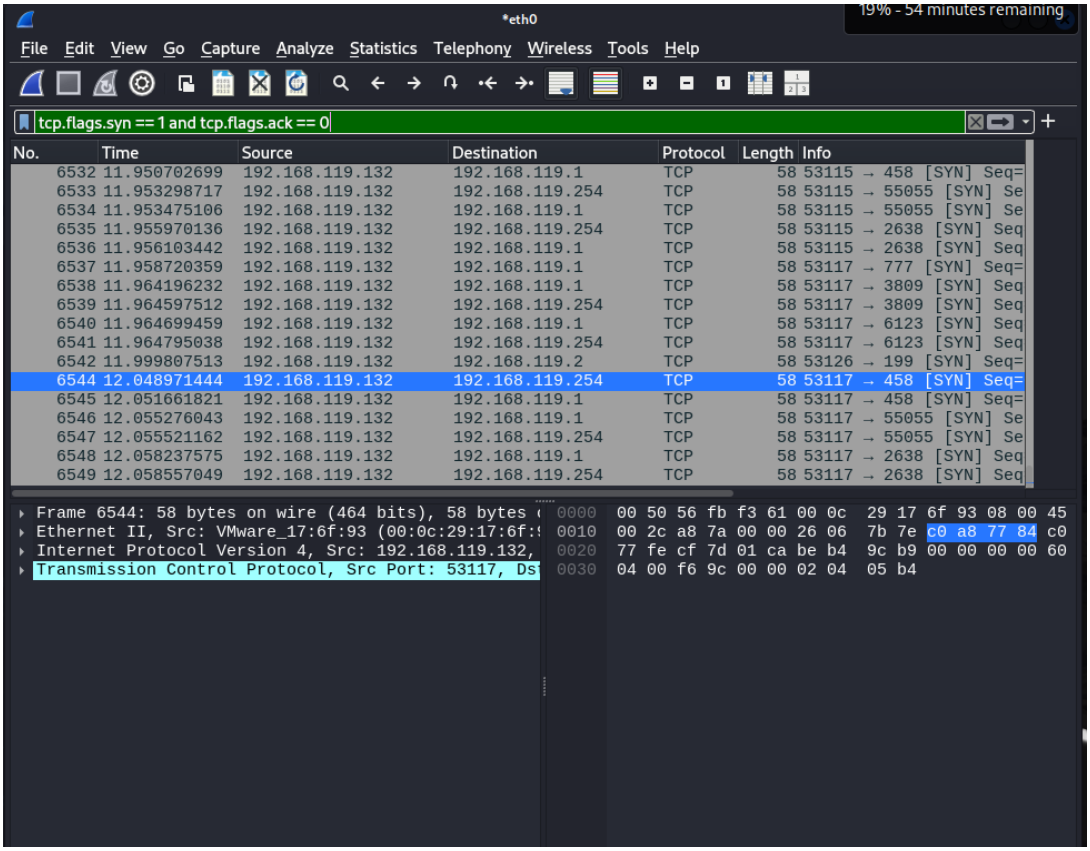

Figure 2: Figure 2: SYN Packets – Nmap attempting to connect

5 Observations

- Hosts such as `192.168.119.2` responded with filtered DNS port (53/tcp).
- Other hosts returned closed port states using RST packets.
- No open ports were detected in this scan; hence, no SYN-ACK responses were observed.
- Packet filtering helped understand how network services respond to scans.

6 Conclusion

This lab reinforced the understanding of TCP scans, open/closed port identification, and TCP flags through Nmap and Wireshark. The environment was a controlled VM network, and all scans were ethically conducted for learning purposes.

Appendix

- **nmap-scan-result.png** – Screenshot of Nmap results
- **wireshark-syn-filter.png** – SYN packets captured

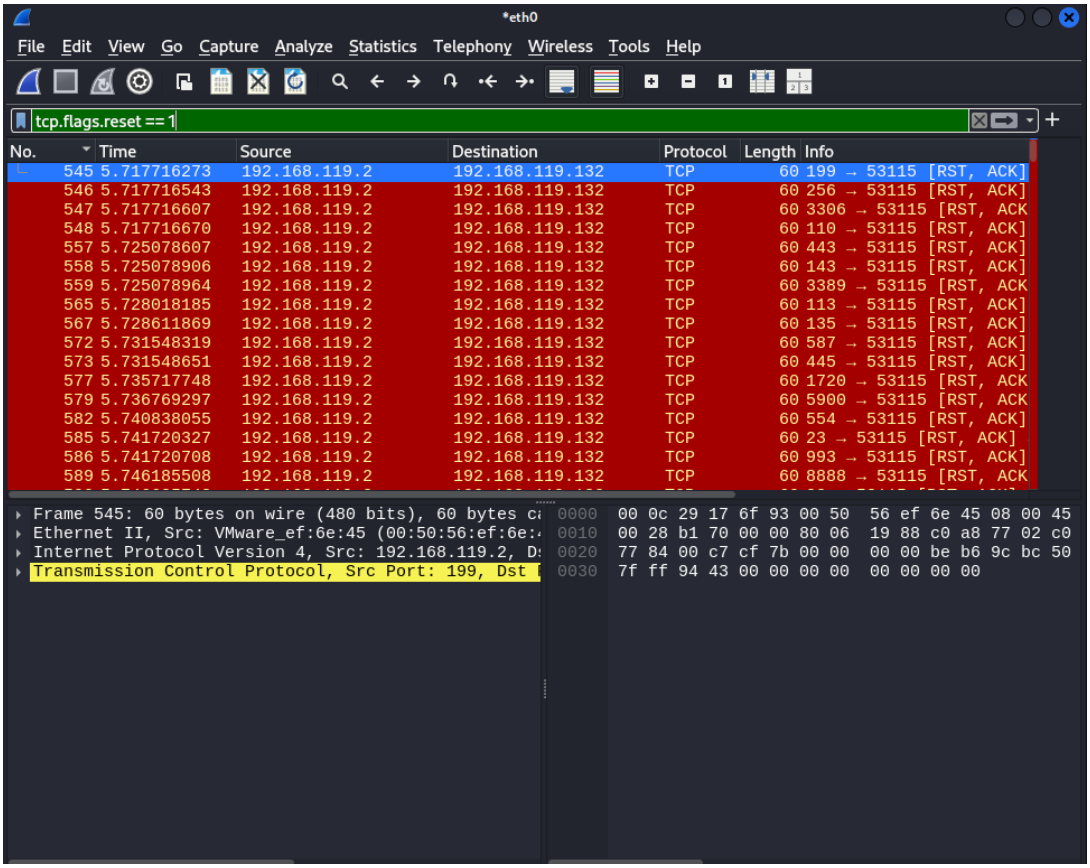

Figure 3: Figure 3: RST Responses – Ports closed

- **wireshark-rst-filter.png** – RST responses for closed ports

Note: This report is part of a cybersecurity lab task. All testing occurred in a safe and isolated virtual environment.