NETWORK SECURITY ASSESSMENT REPORT

1. **Executive Summary:**

To know what is going on in our network traffic, tools like Nmap and Wireshark assist us by giving information on hosts that are up, unauthorized devices, etc. In this assessment we used Nmap to scan our network for devices and tried to scan some hosts to see if any ports are opened. We then used Wireshark to analyse the packets sent over the network and see if we have any unauthorized devices sending any traffic over the network.

2. **Introduction:**
    - **Objective:** To secure our own Wireless Fidelity network.
    - **Testing Approach:**
        - Discovery and Enumeration
        - Traffic Analysis
        - Report

3. **Scope:**

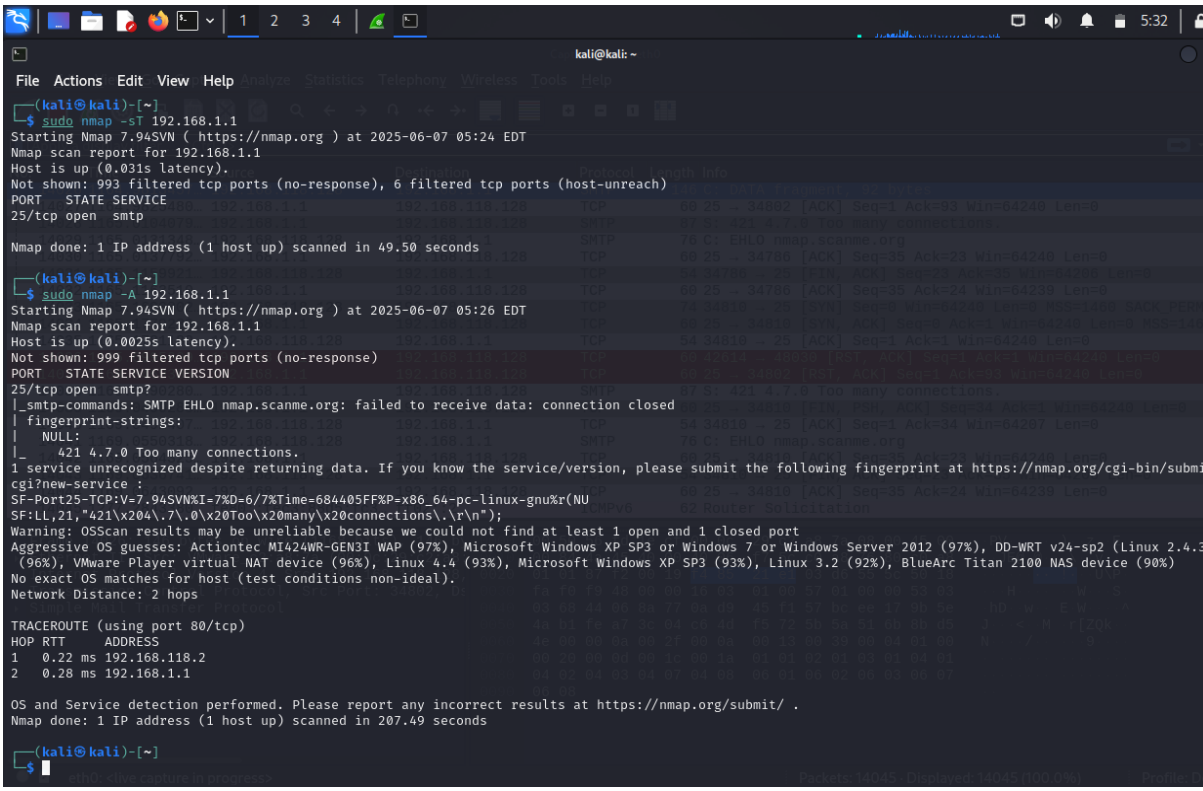
Thes test covered scanning wireless fidelity networks and capturing packets for traffic analysis.

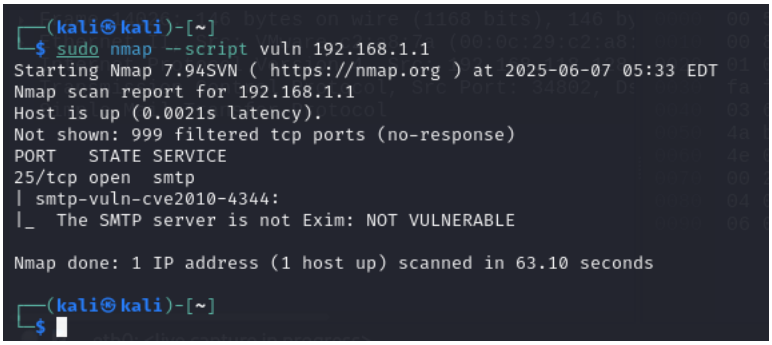
4. **Methodology:**
    - **Discovery and Enumeration:**

In order to know what devices are connected to your network, you'll need to perform a scan to know the hosts that are up, services running that can be exploited to perform further attacks, the operating system of the host etc. Nmap is a great tool that I used to perform my scans on the network.

From the screenshot below the code sudo nmap -sT (Ip address) provided me with hosts that are up and the open, closed and filtered TCP and UDP ports, the services running on those ports of targeted hosts on the network. We can see that the Simple Mail Transfer Protocol service is open on host 192.168.1.1 and unfortunately, we could not get the targeted host's operating system. The traceroute gives us the map of how data travels from the source host to its destination.

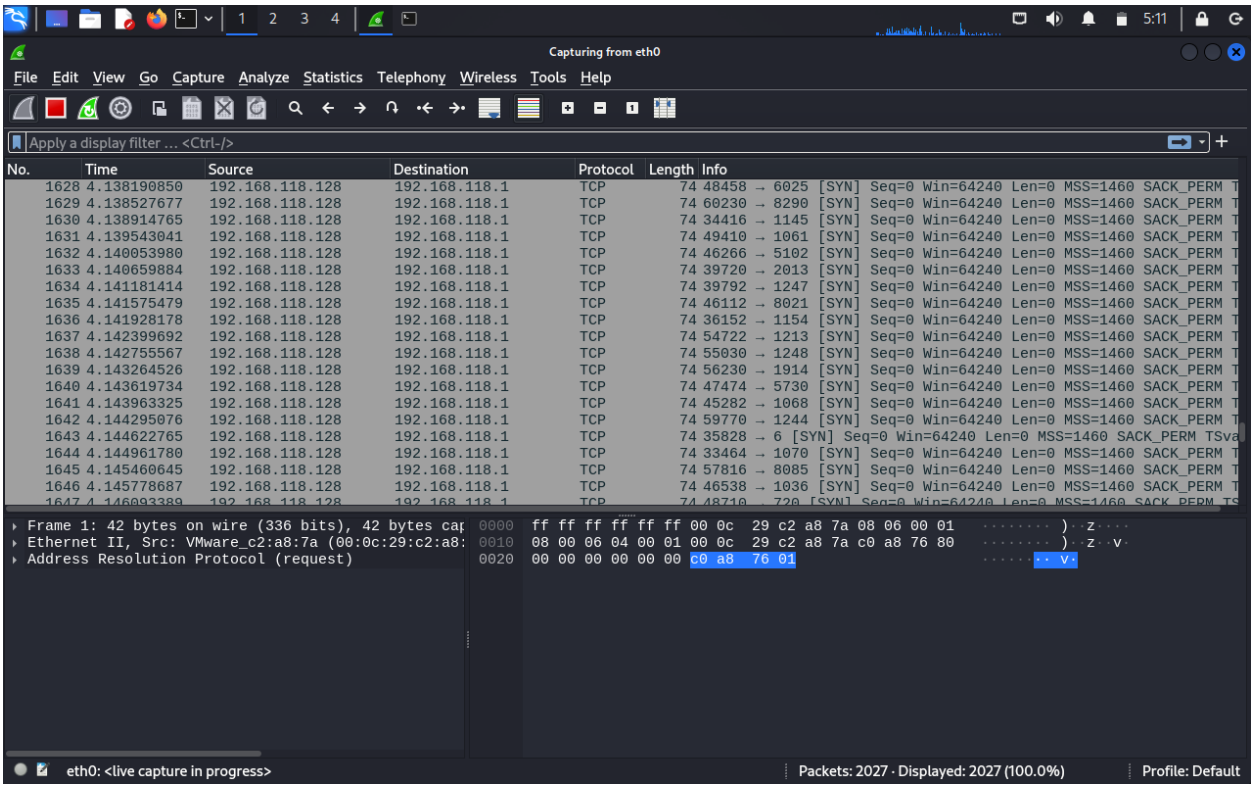
The sudo nmap –script vuln (Ip address) command is used to check for any vulnerabilities in the Common Vulnerabilities and Exposures.

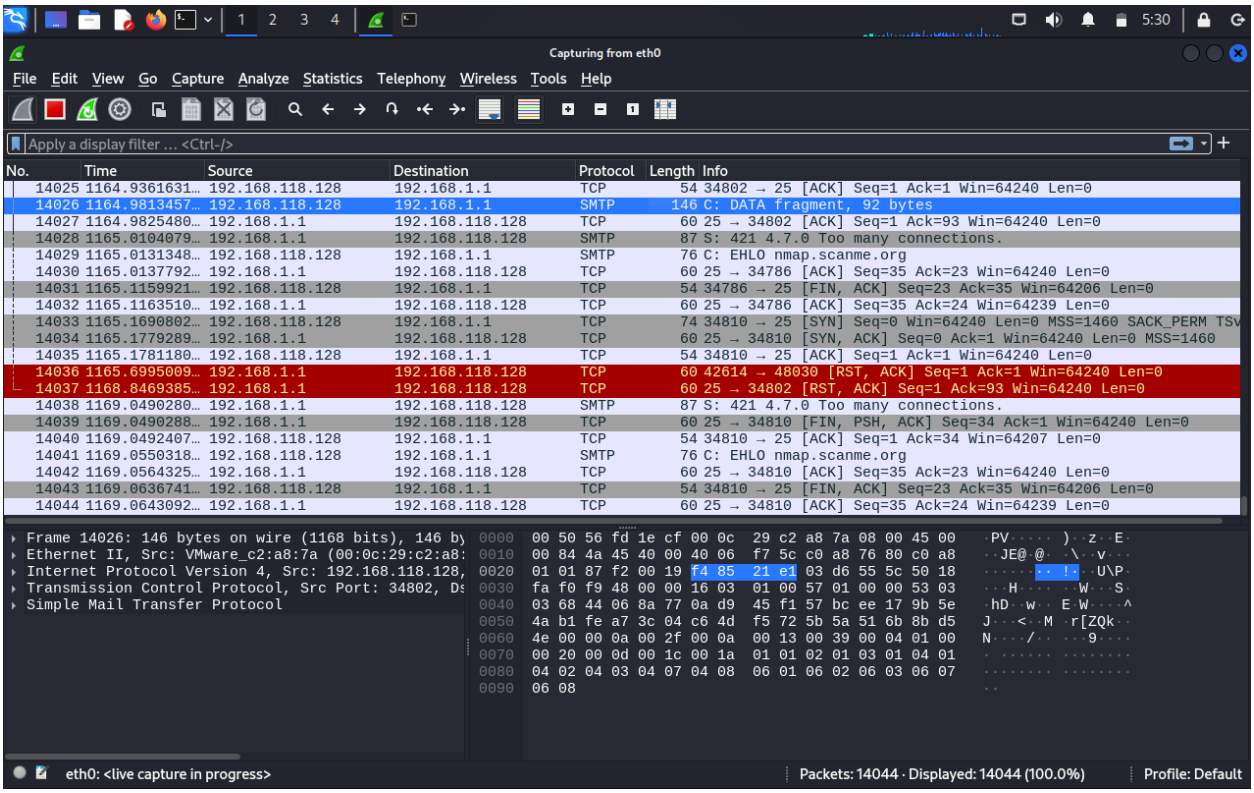




- **Traffic Analysis:**

I then analyzed the packets on the network, I looked into some Transmission Control protocol logs picked by Wireshark, some Simple Mail Transfer protocol logs picked from our target host connection too and searched through the lists of packets to check if and suspicious packets are being transferred over my network by unauthorized devices.


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info
1628 4.138190850 192.168.118.128 192.168.118.1 TCP 74 48458 → 6025 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1629 4.138527677 192.168.118.128 192.168.118.1 TCP 74 60230 → 8290 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1630 4.138914765 192.168.118.128 192.168.118.1 TCP 74 34416 → 1145 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1631 4.139543041 192.168.118.128 192.168.118.1 TCP 74 49410 → 1061 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1632 4.140053980 192.168.118.128 192.168.118.1 TCP 74 46266 → 5102 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1633 4.140659884 192.168.118.128 192.168.118.1 TCP 74 39720 → 2013 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1634 4.141181414 192.168.118.128 192.168.118.1 TCP 74 39792 → 1247 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1635 4.141575479 192.168.118.128 192.168.118.1 TCP 74 46112 → 8021 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1636 4.141928178 192.168.118.128 192.168.118.1 TCP 74 36152 → 1154 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1637 4.142399692 192.168.118.128 192.168.118.1 TCP 74 54722 → 1213 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1638 4.142755567 192.168.118.128 192.168.118.1 TCP 74 55030 → 1248 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1639 4.143264526 192.168.118.128 192.168.118.1 TCP 74 56230 → 1914 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1640 4.143619734 192.168.118.128 192.168.118.1 TCP 74 47474 → 5730 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1641 4.143963325 192.168.118.128 192.168.118.1 TCP 74 45282 → 1068 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1642 4.144295076 192.168.118.128 192.168.118.1 TCP 74 59770 → 1244 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1643 4.144622765 192.168.118.128 192.168.118.1 TCP 74 35828 → 6 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva
1644 4.144961780 192.168.118.128 192.168.118.1 TCP 74 33464 → 1070 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1645 4.145460645 192.168.118.128 192.168.118.1 TCP 74 57816 → 8085 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1646 4.145778687 192.168.118.128 192.168.118.1 TCP 74 46538 → 1036 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
Frame 1: 42 bytes on wire (336 bits), 42 bytes cap
Ethernet II, Src: VMware_c2:a8:7a (00:0c:29:c2:a8:
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 0c 29 c2 a8 7a 08 06 00 01
0010 08 00 06 04 00 01 00 0c 29 c2 a8 7a c0 a8 76 80
0020 00 00 00 00 00 00 c0 a8 76 01
eth0: <live capture in progress>
Packets: 2027 · Displayed: 2027 (100.0%)
Profile: Default


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info
14025 1164.9361631… 192.168.118.128 192.168.1.1 TCP 54 34802 → 25 [ACK] Seq=1 Ack=1 Win=64240 Len=0
14026 1164.9813457… 192.168.118.128 192.168.1.1 SMTP 146 C: DATA fragment, 92 bytes
14027 1164.9825480… 192.168.1.1 192.168.118.128 TCP 60 25 → 34802 [ACK] Seq=1 Ack=93 Win=64240 Len=0
14028 1165.0104079… 192.168.1.1 192.168.118.128 SMTP 87 S: 421 4.7.0 Too many connections.
14029 1165.0131348… 192.168.118.128 192.168.1.1 SMTP 76 C: EHLO nmap.scanme.org
14030 1165.0137792… 192.168.1.1 192.168.118.128 TCP 60 25 → 34786 [ACK] Seq=35 Ack=23 Win=64240 Len=0
14031 1165.1159921… 192.168.118.128 192.168.1.1 TCP 54 34786 → 25 [FIN, ACK] Seq=23 Ack=35 Win=64206 Len=0
14032 1165.1163510… 192.168.1.1 192.168.118.128 TCP 60 25 → 34786 [ACK] Seq=35 Ack=24 Win=64239 Len=0
14033 1165.1690802… 192.168.118.128 192.168.1.1 TCP 74 34810 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSv
14034 1165.1779289… 192.168.1.1 192.168.118.128 TCP 60 25 → 34810 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
14035 1165.1781180… 192.168.118.128 192.168.1.1 TCP 54 34810 → 25 [ACK] Seq=1 Ack=1 Win=64240 Len=0
14036 1165.6995009… 192.168.1.1 192.168.118.128 TCP 60 42614 → 48030 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
14037 1168.8469385… 192.168.1.1 192.168.118.128 TCP 60 25 → 34802 [RST, ACK] Seq=93 Win=64240 Len=0
14038 1169.0490280… 192.168.1.1 192.168.118.128 SMTP 87 S: 421 4.7.0 Too many connections.
14039 1169.0490288… 192.168.1.1 192.168.118.128 TCP 60 25 → 34810 [FIN, PSH, ACK] Seq=34 Ack=1 Win=64240 Len=0
14040 1169.0492407… 192.168.118.128 192.168.1.1 TCP 54 34810 → 25 [ACK] Seq=1 Ack=34 Win=64207 Len=0
14041 1169.0550318… 192.168.118.128 192.168.1.1 SMTP 76 C: EHLO nmap.scanme.org
14042 1169.0564325… 192.168.1.1 192.168.118.128 TCP 60 25 → 34810 [ACK] Seq=35 Ack=23 Win=64240 Len=0
14043 1169.0636741… 192.168.118.128 192.168.1.1 TCP 54 34810 → 25 [FIN, ACK] Seq=23 Ack=35 Win=64206 Len=0
14044 1169.0643092… 192.168.1.1 192.168.118.128 TCP 60 25 → 34810 [ACK] Seq=35 Ack=24 Win=64239 Len=0
Frame 14026: 146 bytes on wire (1168 bits), 146 by
Ethernet II, Src: VMware_c2:a8:7a (00:0c:29:c2:a8:
Internet Protocol Version 4, Src: 192.168.118.128,
Transmission Control Protocol, Src Port: 34802, Ds
Simple Mail Transfer Protocol
0000 00 50 56 fd 1e cf 00 0c 29 c2 a8 7a 08 00 45 00
0010 00 84 4a 45 40 00 40 06 f7 5c c0 a8 76 80 c0 a8
0020 01 01 87 f2 00 19 f4 85 21 e1 03 d6 55 5c 50 18
0030 fa f0 f9 48 00 00 16 03 01 00 57 01 00 00 53 03
0040 03 68 44 06 8a 77 0a d9 45 f1 57 bc ee 17 9b 5e
0050 4a b1 fe a7 3c 04 c6 4d f5 72 5b 5a 51 6b 8b d5
0060 4e 00 00 0a 00 2f 00 0a 00 13 00 39 00 04 01 00
0070 00 20 00 0d 00 1c 00 1a 01 01 02 01 03 01 04 01
0080 04 02 04 03 04 07 04 08 06 01 06 02 06 03 06 07
0090 06 08
eth0: <live capture in progress>
Packets: 14044 · Displayed: 14044 (100.0%)
Profile: Default

5. **Identified Vulnerabilities:**
    - Open ports and services
    - Service/ Operating System version detection
    - Cleartext data exposure

6. **Mitigation Strategies:**
    - Ensure all protocols are encrypted and avoid plaintext protocols.
    - Disable unused services/ports.
    - Isolate critical workstations or network devices using firewalls etc.
    - Monitor network traffic using Wireshark, Nmap and Intrusion Detection System and Intrusion Prevention System.

7. **Conclusion:**

After the assessment I can say that the overall security posture is Low risk since No critical vulnerability and exposure was found and no unauthorized devices were detected too. Hence this targeted host is safe from data theft and operational disruption.