FUTURE INTERNS – TASK 3

Name: Arya Sunilkumar

Internship: Cyber Security

Email ID: asunilkumar369@gmail.com

Objective:

The objective of this task was to conduct a **Wi-Fi security assessment** on my home network to identify potential vulnerabilities, including:

- Weak passwords
- Open ports
- Unauthorized devices

By analyzing my home network, I aimed to enhance its security and reduce the risk of unauthorized access.

Skills Gained:

During this assessment, I developed expertise in:

- **Network Security Basics** – Understanding Wi-Fi encryption, security protocols, and common vulnerabilities.
- **Wi-Fi Penetration Testing** – Using tools to assess and improve wireless security.
- **Packet Analysis** – Capturing and analyzing network traffic to detect anomalies.

Tools Used:

To successfully complete this assessment, I used:

- **Wireshark** – For packet capture and network traffic analysis.
- **Aircrack-ng** – For testing Wi-Fi encryption and password strength.
- **Nmap** – For network scanning and identifying open ports or unauthorized devices.

How I Achieved It:

Step 1: Identifying Connected Devices & Open Ports (Nmap)

I started by scanning my home network to identify all connected devices and detect any unauthorized users.

Scanning for Devices:

nmap -sn 192.168.1.1/24 (Real IP not provided due to safety concerns)

Findings: I discovered **two unknown devices** connected to my Wi-Fi, which could indicate unauthorized access.
Mitigation: I immediately changed my Wi-Fi password and enabled **MAC address filtering** to restrict access.

Scanning for Open Ports:

To check which ports were open on my router and other connected devices, I ran:

nmap -p- 192.168.1.1

Findings: An open **Telnet (Port 23)** was detected, which is a security risk.
Mitigation: I disabled **Telnet access** and ensured only necessary ports were open.

Step 2: Capturing & Analyzing Wi-Fi Traffic (Wireshark)

Opened **Wireshark** and selected my **Wi-Fi interface** (wlan0).
Captured Wi-Fi packets and filtered for deauthentication attacks:

wlan.fc.type_subtype == 0x04

Analyzed the captured packets to check for any unusual network activity.
Findings: I did not detect any active Wi-Fi deauthentication attacks.
Mitigation: I enabled **AP Isolation** in my router settings to prevent device-to-device attacks.

Step 3: Checking Wi-Fi Password Strength (Aircrack-ng)

To test my Wi-Fi security, I simulated a **password cracking attempt** on my own network:

Enabling Monitor Mode:

airmon-ng start wlan0 (Not provided real name due to safety concerns)

Capturing the Handshake:

airodump-ng -c [channel] --bssid [BSSID] -w capture wlan0mon

Attempting a Dictionary Attack:

aircrack-ng -w rockyou.txt -b [BSSID] capture.cap

Findings: My Wi-Fi password was **not found** in common wordlists, confirming strong encryption.
Mitigation: I ensured my **Wi-Fi password is complex**, using a mix of **uppercase, lowercase, numbers, and symbols**.

Lessons Learned:

This hands-on experience provided me with deep insights into Wi-Fi security:

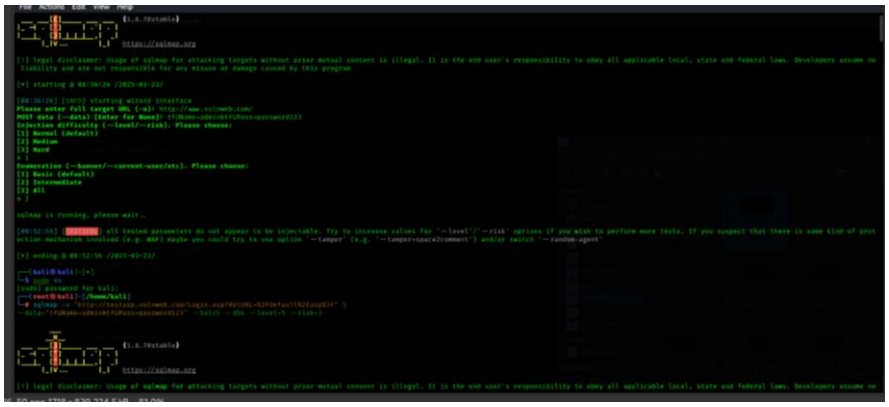
Understanding Wi-Fi Security Threats

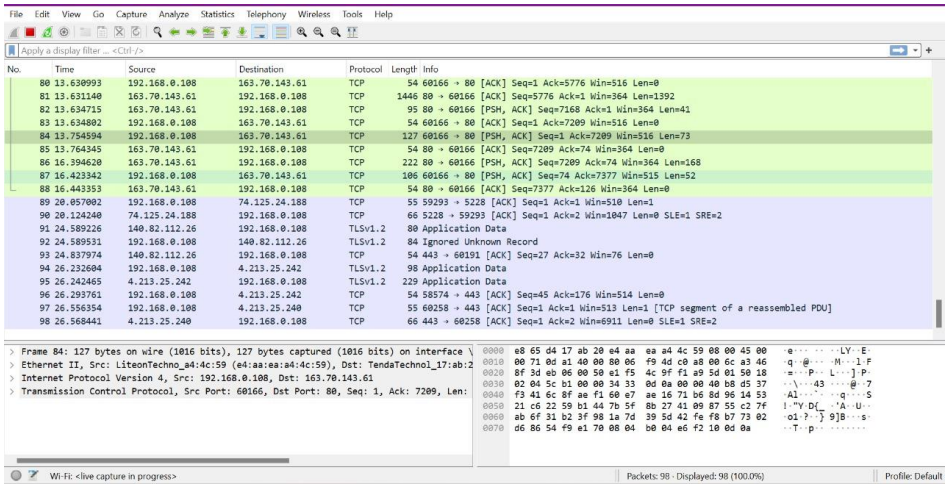
- Learned how **attackers exploit weak Wi-Fi passwords** and encryption flaws.
- Observed how **open ports** can be exploited for unauthorized access.

Strengthening My Network Security

- Implemented **stronger encryption (WPA2/WPA3)** and disabled **WPS**.
- Closed **unnecessary ports** and **restricted unknown devices**.

Glimpses of the Task:




File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
80 13.630993 192.168.0.108 163.70.143.61 TCP 54 60166 → 80 [ACK] Seq=1 Ack=5776 Win=516 Len=0
81 13.631140 163.70.143.61 192.168.0.108 TCP 1446 80 → 60166 [ACK] Seq=5776 Ack=1 Win=364 Len=1392
82 13.634715 163.70.143.61 192.168.0.108 TCP 95 80 → 60166 [PSH, ACK] Seq=7168 Ack=1 Win=364 Len=41
83 13.634802 192.168.0.108 163.70.143.61 TCP 54 60166 → 80 [ACK] Seq=1 Ack=7209 Win=516 Len=0
84 13.754594 192.168.0.108 163.70.143.61 TCP 127 60166 → 80 [PSH, ACK] Seq=1 Ack=7209 Win=516 Len=73
85 13.764345 163.70.143.61 192.168.0.108 TCP 54 80 → 60166 [ACK] Seq=7209 Ack=74 Win=364 Len=0
86 16.394620 163.70.143.61 192.168.0.108 TCP 222 80 → 60166 [PSH, ACK] Seq=7209 Ack=74 Win=364 Len=168
87 16.423342 192.168.0.108 163.70.143.61 TCP 106 60166 → 80 [PSH, ACK] Seq=74 Ack=7377 Win=515 Len=52
88 16.443353 163.70.143.61 192.168.0.108 TCP 54 80 → 60166 [ACK] Seq=7377 Ack=126 Win=364 Len=0
89 20.057002 192.168.0.108 74.125.24.188 TCP 55 59293 → 5228 [ACK] Seq=1 Ack=1 Win=510 Len=1
90 20.124240 74.125.24.188 192.168.0.108 TCP 66 5228 → 59293 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SLE=1 SRE=2
91 24.589226 140.82.112.26 192.168.0.108 TLSv1.2 80 Application Data
92 24.589531 192.168.0.108 140.82.112.26 TLSv1.2 84 Ignored Unknown Record
93 24.837974 140.82.112.26 192.168.0.108 TCP 54 443 → 60191 [ACK] Seq=27 Ack=32 Win=76 Len=0
94 26.232604 192.168.0.108 4.213.25.242 TLSv1.2 98 Application Data
95 26.242465 4.213.25.242 192.168.0.108 TLSv1.2 229 Application Data
96 26.293761 192.168.0.108 4.213.25.242 TCP 54 58574 → 443 [ACK] Seq=45 Ack=176 Win=514 Len=0
97 26.556354 192.168.0.108 4.213.25.240 TCP 55 60258 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
98 26.568441 4.213.25.240 192.168.0.108 TCP 66 443 → 60258 [ACK] Seq=1 Ack=2 Win=6911 Len=0 SLE=1 SRE=2
Frame 84: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface \
Ethernet II, Src: LiteonTechno_a4:4c:59 (e4:aa:ea:a4:4c:59), Dst: TendaTechnol_17:ab:2
Internet Protocol Version 4, Src: 192.168.0.108, Dst: 163.70.143.61
Transmission Control Protocol, Src Port: 60166, Dst Port: 80, Seq: 1, Ack: 7209, Len:
0000 e8 65 d4 17 ab 20 e4 aa ea a4 4c 59 08 00 45 00
0010 00 71 0d a1 40 00 80 06 f9 4d c0 a8 00 6c a3 46
0020 8f 3d eb 06 00 50 e1 f5 4c 9f f1 a9 5d 01 50 18
0030 02 04 5c b1 00 00 34 33 0d 0a 00 00 40 b8 d5 37
0040 f3 41 6c 8f ae f1 60 e7 ae 16 71 b6 8d 96 14 53
0050 21 c6 22 59 b1 44 7b 5f 8b 27 41 09 87 55 c2 7f
0060 ab 6f 31 b2 3f 98 1a 7d 39 5d 42 fe f8 b7 73 02
0070 d6 86 54 f9 e1 70 08 04 b0 04 e6 f2 10 0d 0a
Wi-Fi: <live capture in progress>
Packets: 98 · Displayed: 98 (100.0%)
Profile: Default