TASK-03

Wi-Fi Security Assessment of Home Network

➢ Introduction:

This task involved conducting a Wi-Fi security assessment on my personal home network to evaluate its resilience against unauthorized access and other vulnerabilities. The goal was to identify weak points and recommend security improvements.

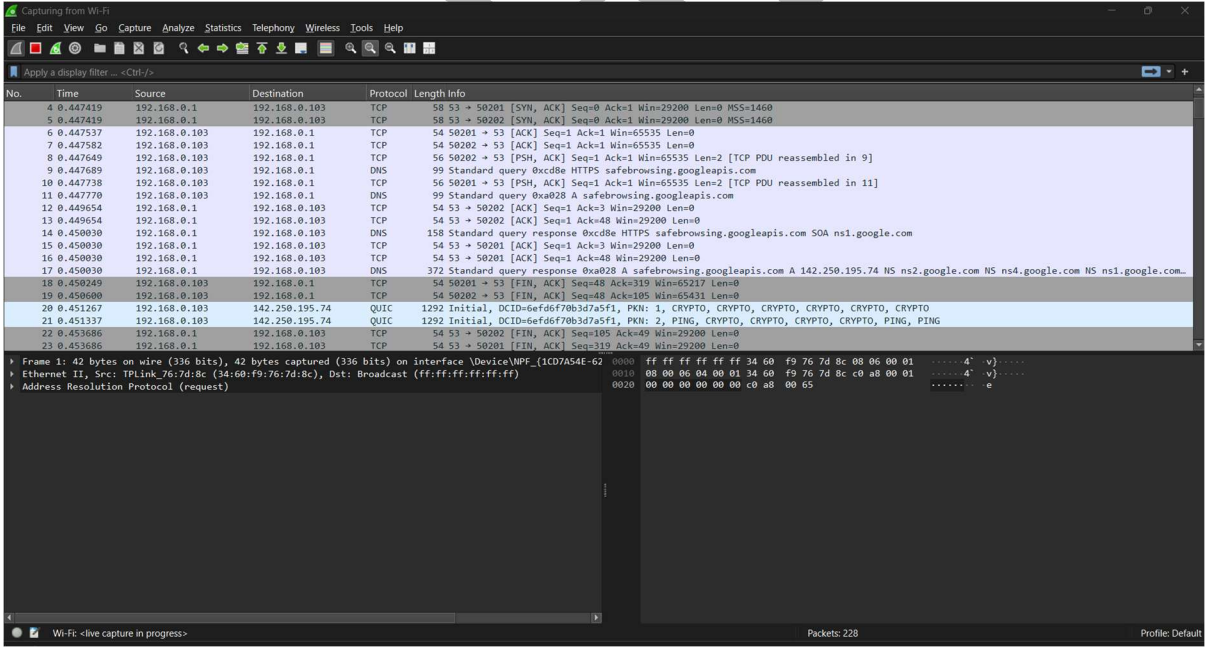
➢ Tools Used:

- Wireshark – For monitoring network traffic.
- Nmap – For scanning open ports and detecting connected devices.

➢ Methodology:

1. Wi-Fi Traffic Analysis (Wireshark):

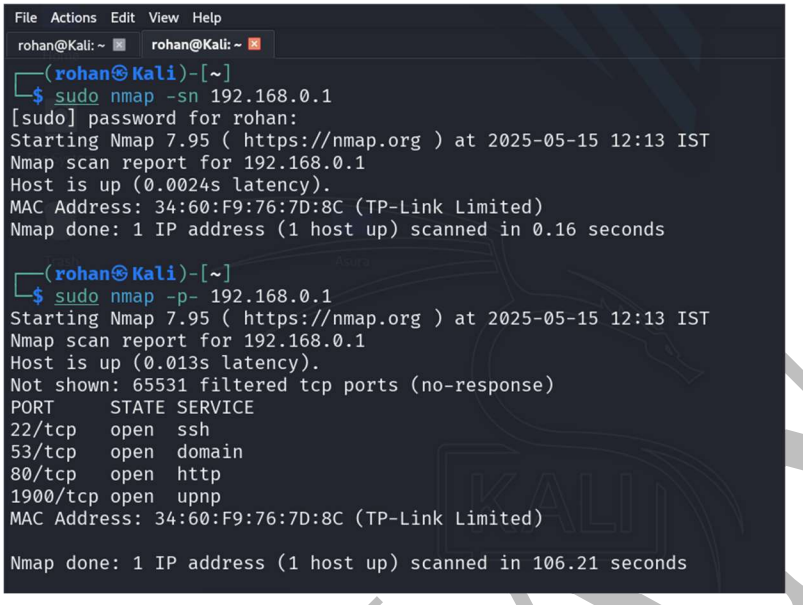
- Opened **Wireshark**.
- Selected the wireless network interface.
- Captured wireless packets to inspect any unencrypted traffic.
- Checked for suspicious activity or unauthorized data transmission.



2. Network Scanning (Nmap):

- Scanned the home network to detect active devices and open ports:
  sudo nmap -sn 192.168.0.1/24

- Conducted a basic TCP port scan on the router:
  sudo nmap -p- 192.168.0.1



3. **Observations:**

Observations Category	Observations
Wi-Fi Encryption	WPA2-Personal (AES)
Password Strength	Good (12+ characters, special symbols)
Unauthorized Devices	No unauthorized devices found
Open Ports on Router	Ports 80 (HTTP),Port 22(TCP), 53 (TCP) open
Traffic Monitoring	No unencrypted sensitive information detected

4. **Vulnerabilities Identified:**

- Default Router Login Credentials were not changed.
- HTTP management access to router (unsecured web access).
- No VPN used for added encryption.

6**. Recommendations:**

- Change router admin credentials from default to a strong, unique password.
- Disable remote management over HTTP; use HTTPS only if needed.

- Enable MAC address filtering to restrict access to known devices.
- Regular firmware updates for the router to patch vulnerabilities.
- Use a VPN for extra security