FUTURE_CS_03

Wi-Fi Security Assessment

Objective:

To assess the security of the current Wi-Fi network for potential vulnerabilities including weak passwords, open ports, and unauthorized devices.

Environment Details:

- **Network Type:** Wifi Router
- **Encryption:** WPA2-PSK
- **Assessment Device:** Kali Linux (No external Wi-Fi adapter)

Tools Used:

- nmap
- netdiscover
- Wireshark

Findings:

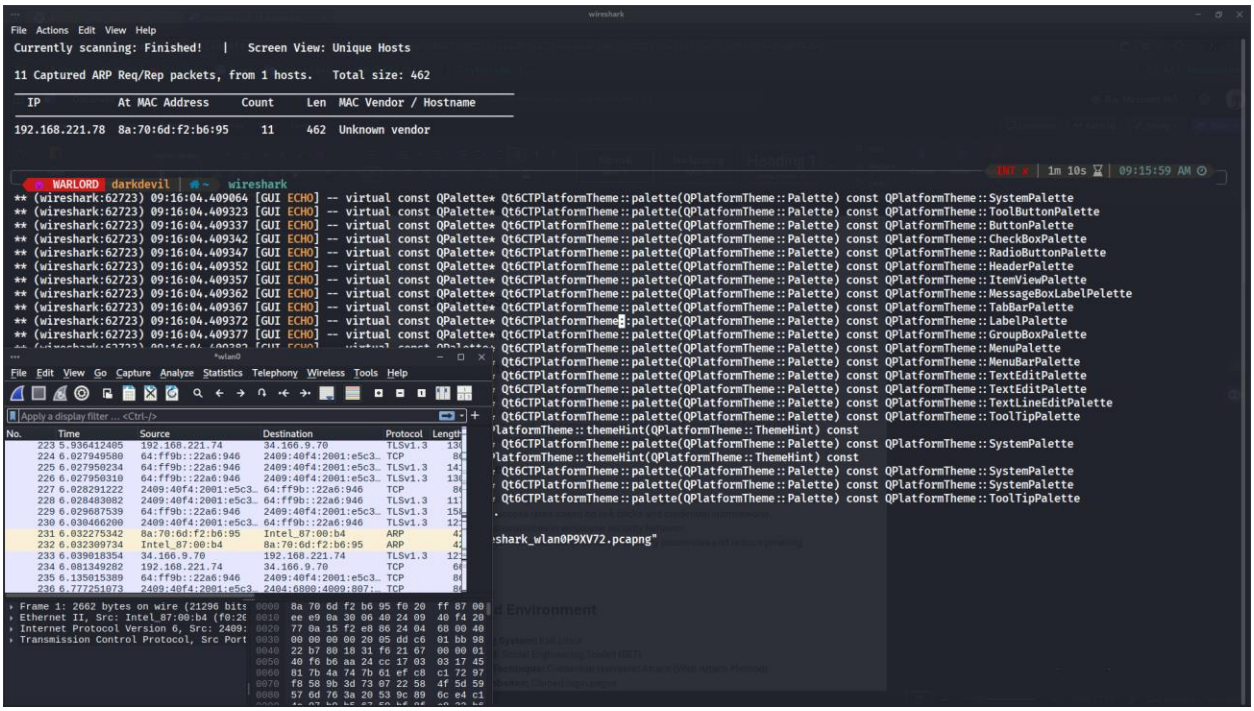
Password	Weak password used for hotspot (12345678)
Encryption	WPA2-PSK
Open Ports	No open ports found on gateway (nmap -sV 192.168.43.1)
Connected Devices	2 devices found using nmap and netdiscover
Unauthorized Devices	No unknown devices detected

Recommendations:

- Use a **strong password** (16+ characters with mix of symbols).
- Regularly **monitor connected devices** with tools like nmap.
- If supported, enable **MAC address filtering** on the hotspot.
- Avoid using default or predictable passwords.

Conclusion:

Despite hardware limitations, the assessment highlighted key weaknesses (like password strength) and demonstrated basic network scanning techniques. Further testing with a proper Wi-Fi adapter is recommended for advanced assessments.



Report Prepared by :

Suryaganthan R

Cybersecurity Student

Date : 7 June 2025