Day 55

Topic: Wireless Security

Objective: To understand Wi-Fi security standards and crack WEP/WPA passwords.

Theoretical Concepts:
We compared WEP (broken), WPA, WPA2, and WPA3. We explained the 4-Way Handshake used in WPA2 and how attackers capture it to crack the password offline.

Practical Work:
We put our wireless adapter into Monitor Mode using *airmon-ng*. We used *airodump-ng* to scan for nearby networks and capture packets. We simulated a de-authentication attack using *aireplay-ng* to force a client to disconnect and reconnect, allowing us to capture the WPA Handshake. We then cracked the handshake file using a dictionary attack.

Tools Used: Aircrack-ng Suite, Wireshark.

Outcome: Practical experience in auditing wireless network security.