Day 8: Wi-Fi Deauthentication & WPA/WPA2 Password Cracking (June 26, 2025)

Topics Covered:

- Capturing WPA/WPA2 handshakes.
- Wi-Fi deauthentication attacks.
- Password cracking with Aircrack-ng and Hashcat.
- Monitor mode configuration.
- Ethical considerations for wireless testing.

What I Did:

I did a **Wi-Fi deauthentication attack** to get the **WPA/WPA2 handshake** when devices reconnected. Then, I tried to **crack the password** using **Aircrack-ng** and **Hashcat**.

Prerequisites:

- Linux system (Kali Linux/Arch).
- Tools: Aircrack-ng suite, Hashcat.
- Wi-Fi adapter with monitor mode and packet injection.

Steps Followed:

1. **Set Up Monitor Mode:** Identified wireless interface, enabled monitor mode, disabled conflicting services.
2. **Scan for Target Networks:** Scanned for Wi-Fi networks, noted BSSID and channel.
3. **Capture the WPA/WPA2 Handshake:** Monitored traffic on target network, saved to capture file.
4. **Perform Deauthentication Attack:** Sent deauthentication frames to trigger reconnection and capture handshake.
5. **Crack the Captured Password:** Used **Aircrack-ng** with a dictionary file (e.g., rockyou.txt) or **Hashcat** for brute-force.

Key Learnings:

- Deauthentication helps capture handshakes in WPA/WPA2.
- Monitor mode is needed for traffic capture.
- Password cracking success depends on wordlist quality.
- Wireless testing must be ethical and authorized.

Important Notes:

- Only test in legal, controlled environments.
- Good wordlists improve success.
- WPA3 is more secure.