Cybersecurity Daily Dairy

Day 7: Wi-Fi Deauthentication using ESP8266

Date: June 25, 2025

Topics Covered:

- Introduction to Wi-Fi deauthentication attacks
- ESP8266 as a deauthentication tool
- Wlan0 driver setup for monitor mode and packet injection

What I Did:

On Day 7, I learned how to use the ESP8266 NodeMCU microcontroller to perform Wi-Fi deauthentication attacks. I also worked on configuring the wlan0 Wi-Fi adapter in Kali Linux with the correct drivers to enable monitor mode and packet injection. These attacks mimic a denial-of-service (DoS) condition by disconnecting clients from the target Wi-Fi network.

Tools and Hardware Used:

- ESP8266 NodeMCU microcontroller
- Kali Linux system
- wlan0 Wi-Fi adapter (supports monitor mode and injection)

Steps Followed:

ESP8266 Setup

- Flashed the Wi-Fi Deauther firmware onto the ESP8266 using appropriate tools.
- Connected to the ESP8266 device’s access point after it powered on.
- Accessed the ESP8266's web interface using the default IP address (192.168.4.1) through a browser.
- Scanned available Wi-Fi networks via the interface.
- Selected the target network and initiated the deauthentication attack.

Key Learnings:

- The ESP8266 is a powerful and budget-friendly tool for wireless penetration testing.
- Deauthentication attacks simulate DoS by forcing devices to disconnect from access points.
- Successful wireless testing requires monitor mode and packet injection support, which depend on correct drivers and compatible Wi-Fi adapters.
- Such attacks are useful for auditing network security but must only be done on authorized networks to avoid legal and ethical issues.