WiFi hacking

source- https://youtu.be/wsa8N_IREN8?si=IRm3Kf0V99pIrQiy

> https://youtu.be/wsa8N_IREN8?si=IRm3Kf0V99pIrQiy

1. Introduction to WiFi & Networking Basics

- **What is WiFi:** WiFi is a wireless technology used to communicate within a Local Area Network (LAN) using radio signals instead of wires. It stands for Wireless Fidelity and belongs to the IEEE 802.11 family of standards.
- **Frequencies:** WiFi operates on unlicensed ISM (Industrial, Scientific, and Medical) frequency bands, such as 2.4 GHz, 5 GHz, and 6 GHz, which means users do not need a special license from authorities to use them.
- **IP & MAC Addresses:** To connect to the internet, an Internet Service Provider (ISP) assigns a Public IP address to your router. The router then assigns Private IP addresses to local devices using DHCP so they can communicate within the LAN. Every network device also has a unique, physical MAC (Media Access Control) address.
- **Key WiFi Terminology:**
  - **ESSID:** The visible name of the WiFi hotspot.
  - **BSSID:** The MAC address of the WiFi hotspot/router.
  - **Station ID:** The MAC address of the client/user's device.
  - **Handshake File:** A file containing a user's connection credentials (like the password) that is sent to the router for verification during the connection process.

2. WiFi Adapter Modes

WiFi adapters function in two primary modes:

- **Managed Mode:** The default mode on all devices. It is used to scan for nearby networks, submit passwords, and connect to a network to use internet services.
- **Monitor Mode:** A powerful, specialized mode used by hackers and security professionals. It allows the adapter to passively observe all wireless traffic in the area without connecting to any network, capture handshake files, and inject special packets (like deauthentication packets) into the network.

3. WiFi Generations and Security Protocols

WiFi security has evolved through several generations to fix vulnerabilities:

- **WEP (Wired Equivalent Privacy - 1997):** Very low security. It utilized RC4 encryption (64/128-bit) and a weak 24-bit Initialization Vector (IV). Because it used a single key for all communications and had a poor integrity checker (CRC-32), it was highly vulnerable to FMS (Fluhrer, Mantin, and Shamir) attacks.
- **WPA (WiFi Protected Access - 2003):** Improved security by introducing TKIP (Temporal Key Integrity Protocol), which generated a temporary key for communications rather than relying on a single key. It used 128-bit encryption, a 48-bit IV, and added MIC (Michael's Message Integrity Check) to verify data purity.
- **WPA2 (2004):** High security and currently the most widely used. It abandoned RC4 in favor of AES encryption and the CCMP protocol. It uses Pre-Shared Keys (PSK) and follows 802.1x standards with EAP (Extensible Authentication Protocol) for better authentication.
- **WPA3 (2018):** The most secure, modern standard. It uses AES GCMP and SAE-2 for integrity checks. Crucially, it introduces **PMF (Protected Management Frames)**, which completely prevents deauthentication and disassociation attacks.

4. Common Wireless Threats and Attacks

- **Access Point Theft (Evil Twin):** An attacker creates a fake hotspot with the exact same name (ESSID) as a legitimate network. Devices often automatically

connect to it based purely on the name, allowing the hacker to perform Man-in-the-Middle (MITM) attacks and steal data.

- **Deauthentication / Disassociation Attacks:** Using Monitor Mode, an attacker spoofs the router's MAC address and continuously sends "disconnect" packets to a legitimate user. When the user's device is forced offline and attempts to reconnect, the attacker captures the resulting Handshake File to crack the password.
- **ARP Cache Poisoning:** An attacker uses MAC and IP spoofing to trick the router and the user into thinking the attacker's machine is the intended destination for data. This allows the attacker to intercept and modify packets (MITM).
- **DoS and Authentication Flooding:** Overwhelming a target device or router with processing requests or fake login attempts, causing the network to hang, act erratically, or run out of IP addresses for legitimate users.
- **Beacons Flood:** Creating numerous fake WiFi network names to confuse users and prevent them from finding and connecting to the legitimate network.

5. WiFi Hacking Methodology & Practical Commands

Hackers generally follow a structured methodology: **Discovery** (finding the target and its GPS location) → **Traffic Analysis** (capturing packets) → **Launching Attacks** (like Deauth) → **Cracking Encryption** (cracking the handshake file) → **Compromising the Network**.

Key Kali Linux Commands:

- **Identify devices:** `lsusb`, `ifconfig` (shows interfaces), `iwconfig` (shows wireless details and mode).
- **Enable Monitor Mode (Manual):**
  1. `ifconfig wlan0 down` (turns off the adapter)
  2. `iwconfig wlan0 mode monitor` (changes to monitor mode)
  3. `ifconfig wlan0 up` (turns the adapter back on)
- **Enable Monitor Mode (Auto):** `airmon-ng start wlan0`.

- **Network Reconnaissance:** `airodump-ng wlan0` (scans all nearby networks, showing BSSIDs, ESSIDs, Channels, and connected Station IDs).
- **Targeted Packet Capture:** `airodump-ng wlan0 --bssid <Target_MAC> -c <Channel_Number> -w <File_Name>` (listens to a specific network and saves the traffic, waiting for a handshake).
- **Deauthentication Attack:** `aireplay-ng -0 100 -a <Router_BSSID> -c <Target_Client_MAC> wlan0` (sends 100 deauth packets to a specific client to force them off the network and capture their handshake upon reconnection).

6. Network Security & Defense

To secure a WiFi network against these threats, the following practices are recommended:

- **Avoid Default/Common Passwords:** Never use default admin credentials (like admin/admin) or common dictionary passwords that can be easily cracked via brute force.
- **Implement Firewalls & IDS:** Use hardware/software Firewalls, Intrusion Detection Systems (IDS), or Unified Threat Management (UTM) systems to filter malicious packets and block unauthorized access.
- **Upgrade to WPA3:** Whenever possible, use WPA3 encryption, as its Protected Management Frames (PMF) feature directly neutralizes deauthentication attacks.
- **Disable WPS:** Turn off the WPS (WiFi Protected Setup) button feature on your router to close known security loopholes.
- **Stay Updated:** Continuously update your router's firmware, system software, and security protocols to patch known vulnerabilities.