Wireless Hacking Methodology & Tools Cheat Sheet

# Wireless Hacking Methodology

1. Discover Wireless Networks – Identify nearby Wi-Fi networks using tools like airmon-ng, Kismet.

2. Capture Wireless Packets – Use airodump-ng, Wireshark to capture packets in monitor mode.

3. Analyze Packets – Look for authentication handshakes, probe requests, SSIDs, BSSIDs.

4. Identify Encryption Type – WEP, WPA, WPA2, WPA3.

5. Exploit Weaknesses – Apply suitable attacks based on encryption type (WEP cracking, WPA handshake capture, WPA3 downgrade attacks).

6. Crack Keys/Passwords – Use tools like Aircrack-ng, Pyrit, coWPAtty, hashcat.

7. Gain Access – Connect using cracked credentials or bypass methods (Rogue AP, Evil Twin).

8. Post-Exploitation – Sniff traffic, Man-in-the-Middle, inject packets, harvest credentials.

9. Maintain Access – Backdoors, persistent rogue APs.

10. Cover Tracks – Clear logs, disguise malicious APs.

# Wireless Hacking Tools Cheat Sheet

## airmon-ng

* Enable monitor mode on wireless card.
* Command: airmon-ng start wlan0

## airodump-ng

* Capture packets, identify APs and clients.
* Command: airodump-ng wlan0mon
* Capture handshake: airodump-ng --bssid <BSSID> -c <channel> -w capture wlan0mon

## aireplay-ng

* Deauthenticate clients to force handshake capture.
* Command: aireplay-ng --deauth 10 -a <BSSID> -c <ClientMAC> wlan0mon

## aircrack-ng

* Crack captured WPA/WEP keys using dictionary/wordlist.
* Command: aircrack-ng -w rockyou.txt -b <BSSID> capture.cap

## Wireshark

* Analyze captured packets, filter for protocols like http, ftp, dns, etc.
* Useful for credential sniffing post-connection.

## Kismet

* Wireless network detector, sniffer, intrusion detection system.
* Command: kismet -c wlan0

## Fern WiFi Cracker

* GUI-based wireless security auditing and attack tool.

## Portable Penetrator

* Commercial tool for automated wireless security testing and WPA key recovery.

## wepcrack

* Dedicated WEP cracking tool, faster on weak IV-based encryption.

## pyrit

* Leverages GPU/CPU for fast WPA/WPA2 cracking.
* Command: pyrit -r capture.cap -i wordlist.txt attack\_passthrough

## coWPAtty

* Automated dictionary attacks on WPA-PSK handshakes.
* Command: cowpatty -r capture.cap -f wordlist.txt -s <SSID>

## Reaver

* Attack WPS-enabled routers using brute force on PIN.
* Command: reaver -i wlan0mon -b <BSSID> -vv

## Airgeddon

* Bash script for automated wireless attacks including Evil Twin, DoS, and cracking.

## Wifite

* Automated wireless attack tool that chains aircrack-ng suite tools.
* Command: wifite