Mon réseau wifi est-il sécurisé ?

No@rland
http://noarland.free.fr

I. Introduction

« Le sans-fil (WIFI) c'est mieux que le câble (RJ45, USB) ! ». Oui c'est fort possible, mais êtes-vous certain que personne ne se soit déjà introduit dans votre réseau?

En effet, la sécurité des réseaux sans fil est souvent une question prise à la légère. Imaginons qu'une personne non autorisée pénètre sur votre réseau. Elle est alors capable d'entrer en possession de vos informations et d'utiliser votre accès à internet. Son but pouvant être de télécharger ou d'accéder à des contenus illégaux. Prouver votre innocence deviendra alors extrêmement difficile.

« Il est facile de monter un réseau, mais il ne faut pas oublier de fermer la porte, que vous soyez ou non dans votre appartement. » *CCM*

II. Comment se protéger ?

Différentes techniques existent afin de protéger l'accès à son réseau sans fil, mais toutes ne sont pas fiables !

1. Masquer le nom de son réseau (SSID)

Le SSID permet d'identifier votre réseau à l'aide d'un nom. Il vous est possible de le cachez. Vous serez donc le seul à le connaître mais malgré tout les pirates sauront le trouver à l'aide d'outils spécialisés. C'est pourquoi ce paramètre ne constitue en rien une protection.

2. Protocoles de chiffrement

Quand vous utilisez un réseau wifi, vous communiquez à l'aide d'ondes, c'est pourquoi, des solutions ont été trouvées afin de sécuriser le contenu de vos échanges. Les clefs WEP, WPA, WPA2 permettent cela. Elles sécurisent l'accès au réseau et chiffrent les communications.

- La clef WEP est souvent utilisée par défaut, pourtant c'est une sécurité illusoire.
- Le protocole WPA utilise par défaut le chiffrement TKIP. Toutefois, la longueur et la complexité du mot de passe choisi reste ici très importante.
- Le WPA2 utilise le chiffrage AES, il reste la meilleure protection à ce jour. Bien sûr, plus votre mot de passe est fort plus vous serez à l'abri d'une intrusion.

3. Définir les pc ayant le droit de se connecter au réseau

Il est tout à fait possible d'indiquer au point d'accès sans fil que tel ou tel ordinateur peut ou non se connecter au réseau grâce à l'adresse physique (adresse MAC) des cartes wifi. Malheureusement, ce n'est en rien une protection puisqu'il est possible de falsifier l'adresse mac de sa carte réseau.

III. Mise en pratique…

Nous verrons dans cet exemple, un cas d'école qui est le déchiffrement d'une clef WEP. Bien sur cette faiblesse de sécurité du réseau sans fil est encore utilisée chez de nombreux particuliers. C'est pourquoi, il est important de noter que : « Le fait de s'introduire dans un système informatique est illégal et puni de 3 ans de prison et 30 000 euros d'amende. [Art. 323-1] ».

1. Pré-requis

Dans cet exemple j'utilise un Netbook ASUS (eeepc 1201nl) intégrant une carte wifi Atheros permettant l'injection de paquets.

Tout au long de cette démonstration, je travaille sur la distribution linux UBUNTU 10.04 à laquelle j'ai installé la suite logicielle Aircrack-ng contenant principalement les scripts suivants:

Airmon-ng :
Nous utiliserons ce script afin d'activer le mode "monitor" sur l'interface wifi du pc. Ce mode permet d'écouter des paquets d'informations WIFI mais aussi d'en injecter.

Airodump-ng :
L'utilisation de ce script permet la capture de trames wifi et donc des IVs (vecteurs d'initialisation) qui stockés dans un fichier serviront lors de la recherche de la clef d'authentification au point d'accès wifi. Il s'agit en réalité d'une mauvaise implémentation du chiffrement RC4 dans le protocole WEP qui laisse en clair des données sensibles. Cette vulnérabilité peut être exploitée lorsqu'un certain nombre d'informations est récolté.

Aireplay-ng :
Cet outil est utilisé afin d'injecter des trames dans le réseau wifi générant alors du trafic que nous captons avec le précédent script (Airodump-ng). Selon la protection du réseau, il faut implémenter différentes attaques (fausse authentification, dé authentification, demande de paquets ARP...).

Aircrack-ng :
Ce dernier script est un programme de cracking. En effet Aircrack-ng peut retrouver une clef à l'aide de paquets ayant été capturés avec Airodump-ng dans le cas d'une clef WEP. Pour les autres types de clefs, il faut se munir d'un fichier dit dictionnaire afin de déchiffrer le précieux sésame d'authentification.

Bien sûr Il reste possible de réaliser vos essais sous Windows ou Mac OS. Pour cela vous devrez disposer d'une carte wifi 802.11b/g avec des drivers préalablement patchés pour l'injection, ainsi que de la suite Aircrack-ng associée à votre système d'exploitation.

2. Activation du mode moniteur

Pour cela nous devons ouvrir une console et taper la commande suivante.

Commande :	airmon-ng <start\stop> [interface]
Dans mon cas :	sudo airmon-ng start wlan0

```
Interface       Chipset         Driver

wlan0           Atheros         ath9k - [phy0]
                                (monitor mode enabled on mon2)
mon0            Atheros         ath9k - [phy0]
```

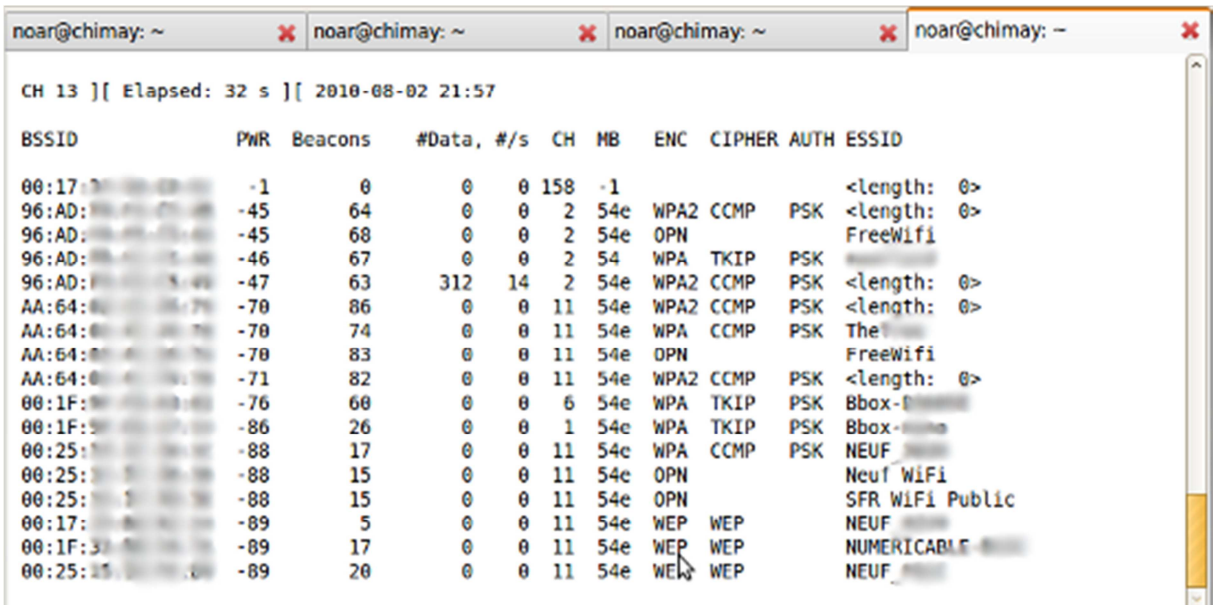
On obtient une nouvelle interface en mode monitor. Pour la suite, je vais utiliser l'interface mon0.

3. Choix d'un réseau

Nous allons maintenant visualiser l'ensemble des réseaux se trouvant à notre porté.

Commande : airodump-ng [interface]

Dans mon cas : airodump-ng mon0



On peut donc distinguer onze champs :

BSSID : adresse mac du point d'accès wifi (Box Adsl ou autres),
PWR : puissance du signal,
Beacons : nombre de paquets d'annonces envoyés par le point accès pour se faire connaitre sur le réseau.
#Data : nombre de paquets capturés (dans le cas d'une clef WEP seul les IV sont comptés).
#/s : nombre de paquets par secondes,
CH : numéro de canal d'émission utilisé par le point d'accès,
MB : vitesse maximum supporté par le point d'accès WIFI,
ENC : protocole de cryptage,
CIPHER : sur quel type de chiffrement se base le protocole de cryptage,
AUTH : protocole d'authentification utilisé,
ESSID : Nom du réseau wifi.

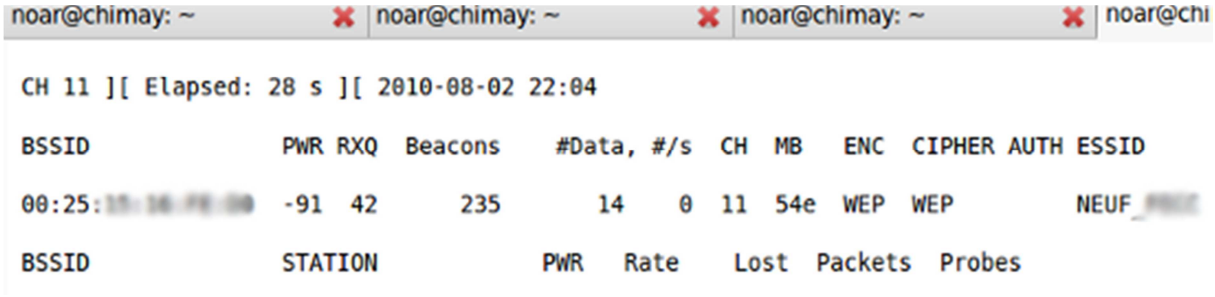
Pour la suite de cette mise en pratique nous utiliserons le réseau NEUF, tout en bas de l'imprime écran.

4. Capture des trames(IVs)

Nous ouvrons maintenant un nouvel onglet dans notre console.

Commande : airodump-ng --write [fichier de log] --channel [numéro] --bssid [adresse mac de l'AP] mon0

Dans mon cas : sudo airodump-ng --write /home/noar/IV.cap --channel 11 --bssid 00:25:xx:xx:xx:xx mon0



Tant que cette console reste ouverte, les données interceptées seront stockées dans un fichier, ici : /home/noar/IV.cap

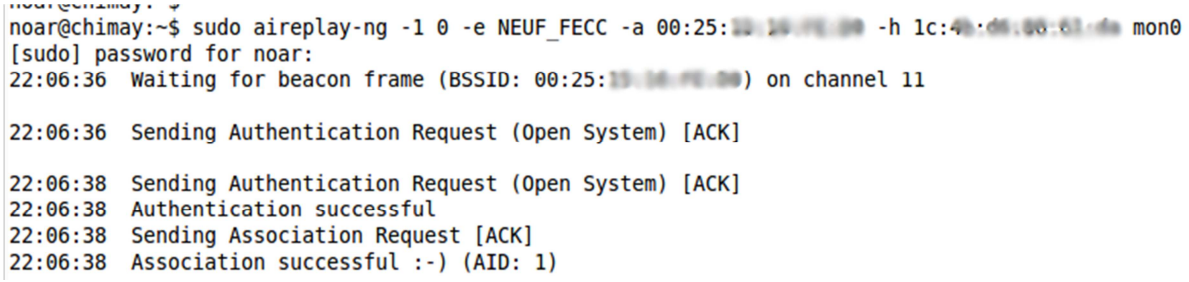
Toutefois, la capture de ces informations peut être très longue. C'est pourquoi, nous allons tenter de faire réagir le réseau, c'est le début de l'attaque.

5. Début de l'attaque

On ouvre de nouveau un onglet dans notre console afin de tenter une fausse authentification (paramètre '1') et dé authentification (paramètre '0') sur le point d'accès.

Commande: aireplay-ng -[paramètre] -e [ESSID] -a [@_mac_AP] -h [@_mac_station] [interface]

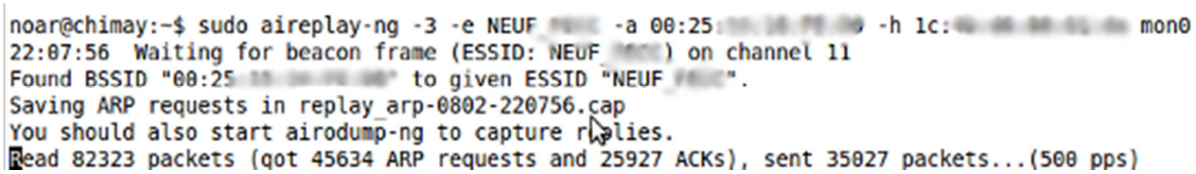
Dans mon cas: sudo airplay-ng -1 0 –e NEUF –a 00:25:xx:xx:xx:xx –h 11:22:33:44:55:66



Une fois notre association avec le point d'accès réalisée, nous passons à l'attaque du paramètre 3 (ARP Request Replay Attack) dont le but sera pour nous de générer de nouveaux vecteurs d'initialisations.

Commande: aireplay-ng -[paramètre] -e ESSID -b @_mac_AP -h @_mac_station interface

Dans mon cas: sudo airplay-ng -3 –e NEUF –a 00:25:xx:xx:xx:xx –h 11:22:33:44:55:66



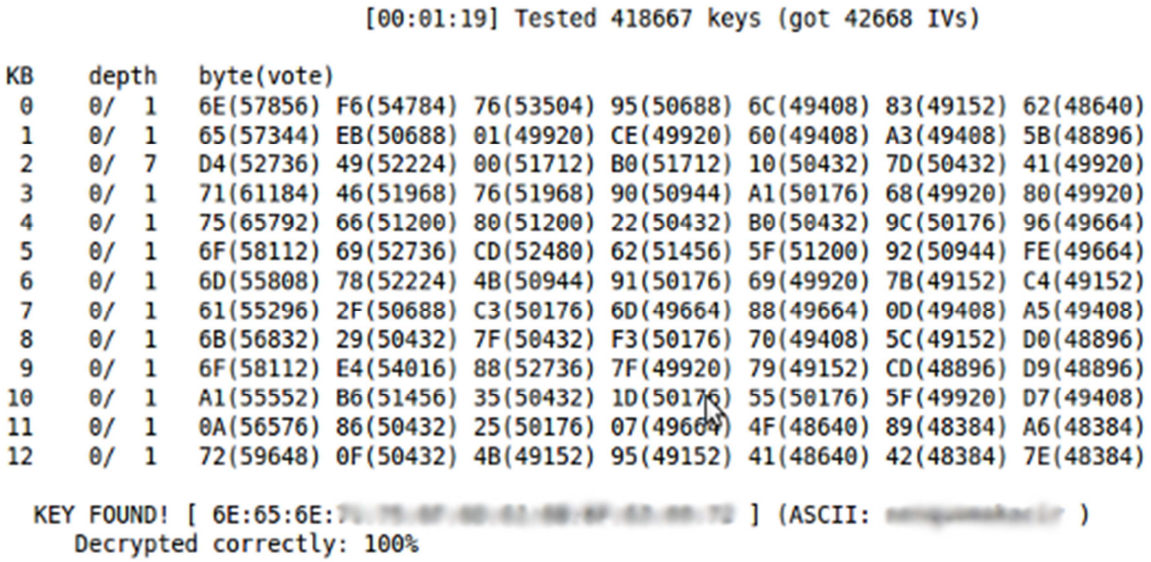
On observe que nous récupérons des paquets ARP (got ARP), ce qui suite à notre injection génère du trafic sur le réseau wifi nous permettant d'observer dans l'onglet où s'exécute la commande Airodump l'augmentation des #data.

6. Déchiffrement de la clef WEP

Il nous est maintenant possible de débuter le chiffrement de la clef WEP. De nouveau dans un nouvel onglet nous exécutons:

Commande : aircrack-ng [chemin du fichier de capture airodump]

Dans mon cas : sudo aircrack-ng /home/noar/Bureau/IV.cap



Et voilà la clef du réseau est déchiffrée en moins de trois minutes. Vous noterez le nombre d'IVs obtenus avant d'exécuter cette commande.

IV. Conclusion

J'espère vous avoir montré grâce à cet article à quel point, il est facile de s'introduire dans un réseau sans fil. De plus avec l'arrivée de la loi HADOPI, de nombreuses personnes vont s'efforcer de télécharger à partir de votre réseau afin de ne pas recevoir la petite lettre de l'Etat. N'hésitez donc plus à remplacer votre bonne vielle clef WEP par le protocole de chiffrement WPA2.

V. Pour aller plus loin

Ubuntu → http://www.ubuntu-fr.org/

Backtrack → http://wiki.backtrack-fr.net/index.php/Accueil

Aircrack-ng → http://www.aircrack-ng.org