Comment pirater un Wifi ?

Date de dernière mise à jour : 14/12/2018 à 12:32

Les réseaux sans fil sont partout, certains sont gratuits et d'autres sont payants. Pouvoir se connecter à un réseau WiFi, même protégé par un mot de passe, est une nécessité importante de nos jours.

En effet, l'accès à Internet est vitale, non pas pour jouer, mais pour se tenir informé des actualités, des nouveautés, des faits du quotidien mais aussi pour le travail car tout ce passe par email dorénavant.

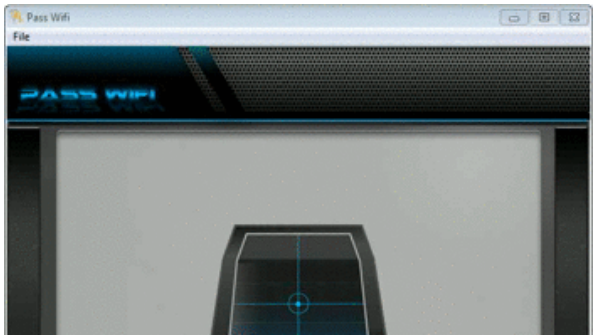
Sauf que si votre voisin ne vous a pas donné l'accès à Internet et que vous n'avez pas de réseau ou assez de crédit pour les données mobiles et bien vous ne pourrez pas vous connecter au Web.

Il est possible de **pirater un réseau WiFi**, mais si vous n'avez pas les bons outils avec vous, il vous sera impossible de trouver la combinaison exacte de la clé qui le protège.

Avec l'arriver des objets connectés, le WiFi est vraiment présent partout autour de nous. Nous allons vous expliquer clairement **comment hacker un réseau WiFi** mais nous n'incitons pas au piratage, ce que nous allons vous expliquer est seulement à but éducatif afin de comprendre comment les hackers piratent un réseau Internet et ce qu'ils peuvent faire la suite.

Méthode 1 : PASS WIFI
PASS WIFI est une application qui fonctionne sur mobile, tablette et ordinateur permettant de décrypter les mots de passe WiFi. A la base réservée à des professionnels, elle a été développé par des hackers qui, ne se voyant pas donné **l'accès à un réseau WiFi**, ont décidé de s'y connecté quand même en développant ce petit programme. Même les clés WEP ou WPA/WPA2/WPA3 ne lui résisteront pas.

Voici une démonstration :



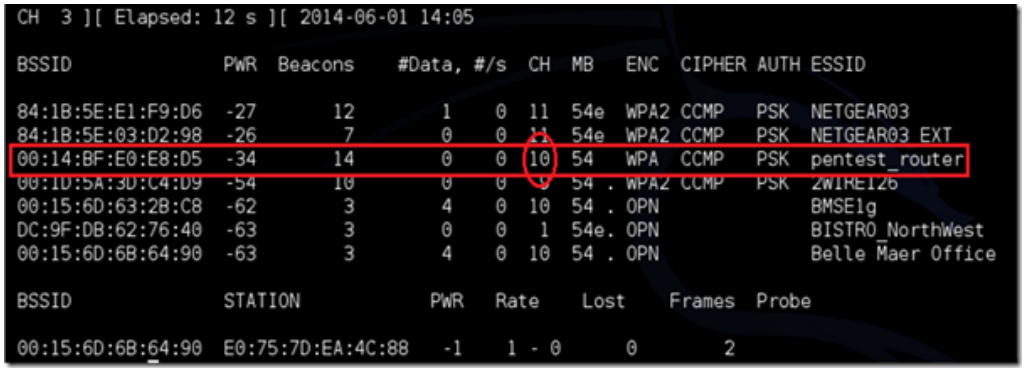
Son fonctionnement est tout simple, une fois installé sur votre appareil que vous voulez connecter au réseau, PASS WIFI va automatiquement analyser et **décrypter les connexions sans fil** pour afficher les mots de passe WiFi se trouvant à proximité.

Il affiche en temps réel les mots de passe de tous les routeurs se trouvant à côté de chez vous ! Il ne vous restera plus qu'à vous connecter dessus et à surfer librement sur la toile.

Vous pouvez télécharger PASS WIFI ici : https://www.passwordrevelator.net/fr/passwifi.php

Méthode 2 : utiliser Kali Linux

Le système d'exploitation Kali Linux est connu et reconnu pour sa pratique à pirater des clés WiFi protégées. C'est un système qui ne fonctionne qu'en ligne de code uniquement, il n'y a donc pas d'interface homme-machine. Son fonctionnement se fait par une suite d'enchaînement d'écrans qui permettent à la fin de récupérer les informations du routeur visé.



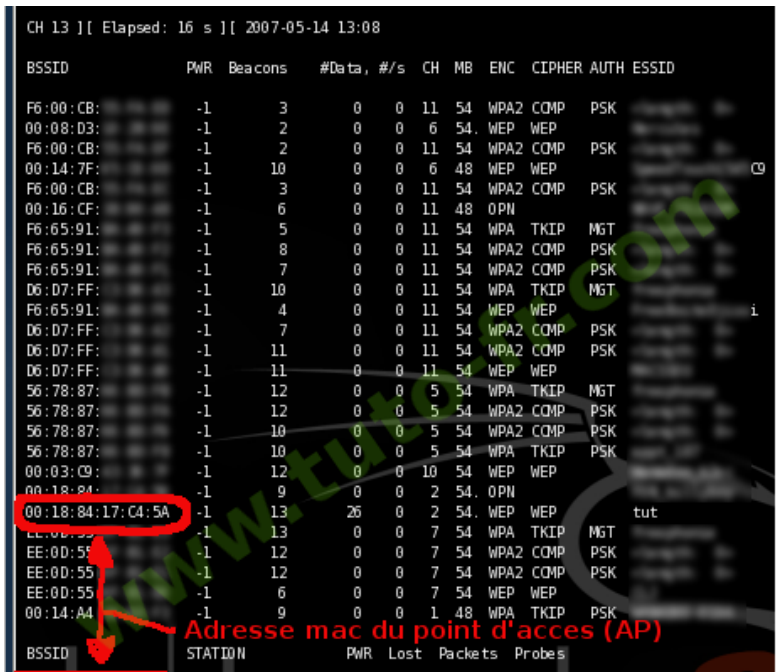
Les experts informatiques l'utilisent souvent pour **pénétrer des réseaux**, le FBI aussi, ils mettent en moyenne 3 minutes pour pirater un code WiFi.

La seule solution pour vous protéger des pirates est de changer régulièrement de clé WiFi, et d'utiliser un mécanisme de sécurisation performant (WPA2 au minimum) qui minimisera le risque, sans jamais l'annuler.

Méthode 3 : Utiliser Aircrack-ng

Ce logiciel est en fait une suite de logiciel qui se complète comprenant plusieurs programmes :

airodump-ng- : qui scanne et récupère les paquets des ondes WiFi.
aireplay-ng- : qui va simuler l'envoit de paquet en créant une fausse connexion Internet.
aircrack-ng : est le logiciel qui, comme un bouquet final, va vous afficher le mot de passe WiFi piraté si le nombre suffisant de paquets magiques a été atteint.



C’est une suite d’étapes et à partir de là, on peut distinguer que le programme **décrypte directement le mot de passe WiFi** sans tenir compte de sa difficulté ou de sa complexité.