[Skip to content](https://h5ckfun.info/comment-hacker-un-wifi-avec-kali-linux/" \l "content" \o "Skip to content)

[](https://h5ckfun.info/)

Haut du formulaire

Bas du formulaire

* [**ACCUEIL**](https://h5ckfun.info/)

* [**CRÉER UN SITE**](https://h5ckfun.info/creer-site-internet/)

* [**HÉBERGEMENT WEB**](https://h5ckfun.info/creer-site-internet/hebergement-web/)

* [**VPN**](https://h5ckfun.info/logiciel/vpn/)

* [**LOGICIELS**](https://h5ckfun.info/comment-hacker-un-wifi-avec-kali-linux/)

* [**BLOG**](https://h5ckfun.info/blog/)

Haut du formulaire

Bas du formulaire

1. [Home](https://h5ckfun.info/)

 >

1. [Blog](https://h5ckfun.info/blog/)

 >

1. [Astuces Hack](https://h5ckfun.info/category/astuces-hack/)

 >

1. [Comment hacker un wifi avec Kali Linux](https://h5ckfun.info/comment-hacker-un-wifi-avec-kali-linux/)



**Comment hacker un wifi avec Kali Linux**

J’ai toujours préféré le système d’exploitation Kali Linux pour tout piratage. Kali linux a tous les outils nécessaires au piratage de réseaux Wi-Fi préinstallés, comme aircrack-ng (meilleur logiciel pour craquer un Wi-Fi). Il existe certainement certains logiciels également disponibles pour les utilisateurs de Windows et Android, mais rien de comparable à Kali Linux.  
Si vous ne voulez pas installer Kali Linux (que vous détestez le dual-boot), alors utilisez le mode Live de Kali Linux.

Donc, dans notre société il y a 5 principaux types de sécurité pour les réseaux Wi-Fi.

1. WEP
2. WPA ou WPA2
3. Filtrage d’adresse MAC
4. Réseaux Cachés
5. WPA2 (WPS disponible)
6. Réseau Ouvert

**Hacker un réseau wifi avec Kali linux :**

J’explique ici comment fonctionne le piratage de chacun des types de sécurité un par un.

* WEP

WEP signifie Wired Equivalent Privacy. C’est la première sécurité Wi-Fi, inventée en 1999 et craquée dans l’année.

Aujourd’hui, c’est le type de sécurité le plus facile à craquer. Les gens ne comprenaient pas le fonctionnement du piratage WEP mais pouvaient le pirater. Il y a un vecteur d’initialisation envoyé sur tout le réseau, vous pouvez obtenir un mot de passe en utilisant cette technique, plus la capture de vecteur d’initialisation vous permet de pirater aisément la sécurité WEP. Une sécurité WEP peut être cassée en 20 à 30 minutes. Même avec le mot de passe le plus solide du monde, vous ne pouvez pas protéger votre réseau.

**Logiciel pour craquer ce genre de réseau :**[aircrack](https://www.aircrack-ng.org/) Vous pouvez non seulement pirater les réseaux WEP en utilisant aircrack, mais aussi d’autres types de sécurité Wi-Fi comme WPA, WPA2a. Aircrack est disponible pour Windows et Linux.

**Comment faire sous Windows :** Pour obtenir le mot de passe, vous devez installer aircrack-ng. Bonne nouvelle pour les non-codeur car il n’est pas nécessaire de coder sous le système d’exploitation Windows. La mauvaise nouvelle pour les utilisateurs de Windows, il faudra 4-9 heures. Allez voir ici : [processus complet, de l’installation au Hacking](http://web.archive.org/web/20161201180820/http:/www.wikihow.com:80/Hack-a-WiFi-That-Uses-WEP-Encryption-(Windows)). Ceci fonctionne pour Windows 7,8 et 10.

**Pirater sous Linux :** Peu importe la distribution de Linux que vous utilisez, vous n’avez besoin que de aircrack. Explications [sur comment l’installer sur n’importe quelle distribution](https://askubuntu.com/questions/294651/step-by-step-guide-to-install-aircrack-ng-suite-on-ubuntu-12-04-lts) ici. Après l’installation, il existe des commandes simples. Si vous utilisez Kali sur Virtual Box, vous devez acheter un adaptateur sans fil. Voici le[processus de piratage](http://www.wirelesshack.org/step-by-step-kali-linux-and-wireless-hacking-basics-wep-hacking-part-3.html)**.**

**Android:** Le Google Play Store regorge sans aucun doute de milliers de fausses applications de piratage de Wi-Fi. Mais [WIFI WPS WPA TESTER](https://play.google.com/store/apps/details?id=com.tester.wpswpatester&hl=en) fonctionne pour le piratage. Mais il ne fonctionne pas pour tous les Wi-Fi, et nécessite Android 5.0 ou supérieur pour fonctionner.

**Comment protéger un réseau**

N’utilisez pas WEP, utilisez n’importe quoi d’autre.

* WPA OU WPA2

Lorsque WEP est devenu facile à craquer, WPA (Wi-Fi protected access) est apparu. Il a deux formats, WPA et WPA2 (sa version avancée). Il est beaucoup plus sécurisé que WEP. WPA2 est également plus sécurisé que WPA.

Aujourd’hui, c’est la meilleure sécurité pour protéger votre réseau si vous mettez un mot de passe fort. Il peut parfois être cassé, mais pas toujours. Il existe principalement deux méthodes disponibles pour pirater le WPA ou WPA2a

1. **Attaque par dictionnaire**
2. **Attaque par force brute (jamais entendu parler de quelqu’un qui craquait le Wi-Fi avec ça)**

***Attaque par dictionnaire :*** C’est la méthode la plus utile pour pirater le WPA. Dans cette méthode, le pirate informatique crée une liste de mots avec un logiciel d’aide comme Crunch. Dans ce cas vous devez indiquer la longueur minimum, la longueur maximum et la liste de caractères. Il crée un dictionnaire qui contient tous les mots composés des caractères que vous avez entré. Après avoir fait une liste de mots, vous avez besoin d’un logiciel qui essayera ces mots un par un. Aircrack peut essayer 900 mots par seconde.  **Si votre mot de passe est votre nom+quelque chose comme des chiffres, alors il est facile à craquer.**

***Attaque par force brute :***Il n’y a pas de grande différence entre les attaques par force brute et celles par dictionnaire. Dans ce cas, il suffit au pirate de donner des informations sur les longueurs minimum et maximum, la liste de caractères et un logiciel comme Reaver essaie chaque combinaison de ces caractères. Mais ce n’est qu’un concept théorique, car il faut trop de temps, cela peut prendre plusieurs semaines, et vous avez besoin d’un signal fort pour cette attaque, mais si WPS est autorisé dans WPA2, il peut être facilement piraté.

**Pirater depuis Linux :** Tout d’abord, vous avez besoin d’un fichier de liste de mots. Vous pouvez utiliser Crunch qui est préinstallé dans Kali Linux, voici [comment créer une liste de mots avec Crunch](http://null-byte.wonderhowto.com/how-to/tutorial-create-wordlists-with-crunch-0165931/). Après avoir créé une liste de mots il est temps de craquer le mot de passe Wi-Fi. Regardez dans ces vidéos comment craquer un mot de passe en utilisant aircrack-ng.

Avec aircrack-ng, vous devez attendre qu’un périphérique se connecte au réseau, si vous ne voulez pas attendre, essayez Fern wifi cracker

**Utilisateur de Windows :** Hé, mec, il va peut-être être difficile pour toi de pirater en utilisant Windows car il faut taper des commandes. Voici les logiciels dont vous avez besoin de craquer des mots de passe Wi-Fi, téléchargez les deux :

1. [Crunch](https://sourceforge.net/projects/crunch-wordlist/)
2. [Aircrack](http://download.aircrack-ng.org/)

**Voici le processus complet qui permet d’obtenir le mot de passe depuis Windows.**

Comment protéger un réseau :

1. Toujours utiliser un mot de passe fort, d’après Kevin Mitnick votre mot de passe Wi-Fi devrait contenir 20 caractères au minimum.
2. Si vous ne voulez pas utiliser de mot de passe long, vous devriez au moins inclure une majuscule, une minuscule, un chiffre, et un caractère spécial comme, **<**’:”/?.\| , de nos jours !@#$, etc. ne sont plus considérés comme des caractères spéciaux
3. Utilisez n’importe quelle autre sécurité en plus du WPA comme le filtrage d’adresse MAC, ou masquez votre réseau sans fil.
4. Réduisez la puissance de votre signal réseau.

* Filtrage d’adresse MAC

Pour comprendre le filtrage d’adresses MAC, vous devez savoir ce qu’est une adresse MAC. L’adresse MAC est l’identité matérielle de votre appareil, ou on pourrait dire l’adresse Wi-Fi de votre appareil. Avec ce type de sécurité, seul un périphérique enregistré peut se connecter, un autre périphérique Wi-Fi ne peut pas se connecter.

Pour contourner ce type de sécurité, le hacker a juste besoin de connaître l’adresse MAC d’un périphérique enregistré, puis de modifier son adresse MAC pour la faire coïncider avec l’adresse MAC du périphérique. Maintenant, vous vous demandez, est-ce qu’on peut obtenir une adresse MAC sans aucun accès physique à un appareil enregistré ? La réponse à cette question est OUI. Il existe un certain logiciel disponible, aircrack pour ne pas changer, il peut montrer les périphériques connectés à un réseau bien que vous n’y soyez pas connecté.

**Tutoriel Windows :** : Si vous êtes sous Windows, désolé, vous devez trouver l’adresse MAC d’un périphérique enregistré manuellement, il n’existe aucun logiciel. Le mode Live de Kali Linux est un bon choix. Quoi qu’il en soit, une fois que vous connaissez l’adresse MAC, vous pouvez changer votre MAC voici un [tutoriel](http://www.besthackingtricks.com/how-to-bypass-wifi-mac-filter-in-windows-pc/)**.**

**Tutoriel Linux :** Linux est toujours préférable pour tout piratage. Si vous n’utilisez pas Kali Linux tapez **aircrack-ng** dans Terminal pour savoir comment l’installer. Après l’installation, suivez ce processus.

**Tutoriel Android :**Pour craquer ce genre de sécurité vous devez rooter votre téléphone. Après le root, vous pouvez changer votre adresse MAC en utilisant [BusyBox](https://play.google.com/store/apps/details?id=stericson.busybox&hl=en)et [Terminal](https://play.google.com/store/apps/details?id=jackpal.androidterm&hl=en). Une fois ces applications installées, [suivez ce tutoriel.](http://www.besthackingtricks.com/how-to-bypass-wifi-mac-filter-in-android/)

**Comment protéger un réseau**

1. Réduisez la puissance de votre signal.
2. Ajoutez n’importe quel autre type de sécurité.

* Réseau caché

Comme le nom de ce type de sécurité l’indique, le réseau est caché, vous ne pouvez pas le voir en allumant votre wifi, vous devez entrer le nom du réseau manuellement. Sous Windows OS, la détection d’un wifi caché affiche un symbole de réseau caché et lors de la connexion une demande de nom de réseau apparaît. Sur Internet, vous pouvez trouver des logiciels et des applications disponibles pour pirater ce type de réseaux. Vous pouvez également obtenir un nom de réseau à l’aide d’appareils Android ou iPhone.

**Appli Android :** Pour afficher les réseaux caches vous devez installer inSSIDer depuis le [Google Play Store](https://play.google.com/store/apps/details?id=com.metageek.inSSIDer&hl=en). C’est une appli payante $9.99 (7.31€).

**Tutoriel Linux :** Linux est un OS qui permet de craquer 100% des mots de passe Wi-Fi. Pour les réseaux cachés, voici un tutoriel vidéo.

Note : C’est un tutoriel pour Kali Linux, mais ne vous inquiétez pas, cela fonctionnera avec n’importe quelle distribution.

**Tutoriel Windows :** Trouver un réseau caché sous Windows est beaucoup plus simple que de craquer une sécurité WPA. Voici les [huit meilleurs scanners de Wi-Fi](https://www.raymond.cc/blog/how-to-discover-hidden-wireless-network/).

Comment protéger un réseau

1. Réduisez la puissance du signal de votre réseau Wi-Fi.
2. Ajoutez n’importe quel autre type de sécurité.

* WPS activé

WPS signifie Wireless Protected Setup, mais il risque de ne pas sécuriser votre réseau. Il est également connu sous le nom de WPA-PSK. Dans ce cas, il existe code PIN à 8 chiffres, vous pouvez utiliser ce code PIN comme mot de passe. Le routeur a un code PIN à 8 chiffres que vous devez entrer pendant la connexion, le routeur vérifie les quatre premiers chiffres séparément et les quatre derniers chiffres séparément, ce qui devient très facile à craquer par une attaque par force brute. Les réseaux protégés par WPS peuvent être piratés en seulement 40 minutes à l’aide de Pixie Dust avec Reaver.

**Tutoriel Linux :** Vous aller devoir taper quelques commandes pour ça. Comme vous le savez, Linux est le meilleur système d’exploitation pour n’importe quel type de piratage. Le code PIN des réseaux WPA-PSK peut être craqués par le logiciel aircrack-ng, pas besoin d’installer Kali et Backtrack. Cet article vous apprendra [comment hacker](http://www.hackingeveryday.com/how-to-hack-wifi-wpa2-psk-password-using-kali-linux-2-0/)un réseau WPA-PSK (contient des captures d’écran).

**Utilisateur Windows** : Vous pouvez craquer ce genre de sécurité en moins de 5 minutes. Installez [Wincap](https://www.winpcap.org/install/) et [JumpStart](http://jumpstart.soft112.com/) pour Windows [10,8, 8.1 etc] et regardez cette vidéo pour apprendre à contourner cette sécurité pas-à-pas.

**Tutoriel Android :** [WPS Connect](https://play.google.com/store/apps/details?id=com.ngb.wpsconnect&hl=en) est la seule application qui peut vous aider à contourner ceci. Elle est disponible gratuitement sur Google Play Store, mais vous devez vous assurer que votre version d’Android est au moins la 5.0 Lollipop et que le téléphone est rooté.

Comment protéger un réseau

1. N’utilisez pas le WPS.

* Wi-Fi ouvert

Vous pensez certainement ***quel est l’intérêt de hacker un réseau Wi-Fi ouvert****.*Le piratage d’un réseau ouvert signifie le contrôle du réseau complet. Oui, vous avez raison, comme **le réseau de votre université**. Pour contrôler le réseau Wi-Fi complet, le pirate doit pirater le routeur. Chaque routeur possède un nom d’utilisateur et un mot de passe par défaut et, dans le monde d’aujourd’hui, plus de 90% des routeur ont toujours leur mot de passe par défaut et si vous changez de mot de passe, un pirate peut toujours utiliser une attaque de force brute, une attaque par dictionnaire, une attaque de l’homme du milieu ou un keylogger pour pirater le routeur.

J’ai déjà décrit les attaques par force brute et par dictionnaire plus haut.

**Attaque par dictionnaire depuis Kali Linux :**Assurez-vous que vous avez créé une liste de mots pour le nom d’utilisateur et pour le mot de passe par défaut, le nom d’utilisateur par défaut est admin, alors je vous suggérerais d’essayer uniquement le champ de mot de passe. Voici la source vidéo.

**Mot de passe par défaut :** Comme je vous l’ai dit ci-dessus, plus de 90% des routeurs possèdent toujours leurs noms d’utilisateur et mot de passe par défaut. Je vous offre donc la liste des mots de passes et noms d’utilisateurs par défaut de tous les routeurs.

**username : admin**

**password : password**

**username : admin**

**password : (blanc)**

**username : admin**

**password : secret**

**Keyloggers :**  Il s’agit essentiellement d’un logiciel qui enregistre chaque frappe/caractère entré par l’utilisateur. Les keyloggers sont principalement utilisés pour obtenir un mot de passe Gmail, Twitter, Instagram etc. Les crackers peuvent installer à distance un logiciel de keylogging. Ce logiciel peut envoyer la liste de nos entrées clavier sous forme de texte à intervalle régulier. Le problème consiste à l’installer sur l’ordinateur de la victime.

* *Keyloggers pour le système d’exploitation Windows*:[Ardamax Keylogger](http://www.ardamax.com/keylogger/) est la meilleure option pour les utilisateurs Windows. Il existe une version gratuite et une version payante. Dans la version gratuite, vous avez besoin d’accéder de nouveau à la machine pour voir les frappes enregistrées, tandis que la version premium vous enverra la liste par mail dans un fichier .txt à intervalle de temps régulier.
* *Pour Android OS :*[Shadow Keylogger](https://play.google.com/store/apps/details?id=simpllekeyboard.main&hl=en) est mon appli préférée pour enregistrer tout le texte entré, mais elle ne vous enverra pas de mail.

**Attaque de l’homme du milieu**: Comme son nom l’indique, cette attaque transforme le hacker en un homme du milieu, entre sa victime et son routeur. La victime ne verra  aucun changement, mais toutes les informations peuvent être vues par le pirate.

Tutoriel Kali Linux

Tutoriel Windows [ici](https://yashpandyasecuritytester.blogspot.in/2014/01/wi-fi-tricks-my-1st-ever-hack-for.html)

Comment protéger un réseau

1. Toujours changer le nom d’utilisateur et le mot de passe par défaut.
2. Utilisez un pare-feu pour vous protéger des hackers.
3. Utilisez un routeur D-Link qui vous protègera des attaques par force brute et par dictionnaire car avec ce genre de routeur, si vous entrez un mot de passe erroné 5 fois, alors vous ne pourrez plus accéder au routeur pendant un certain temps.
4. Désactivez la connexion à distance de votre routeur Wi-Fi.
5. Toujours utiliser un bon antivirus pour vous protéger des keyloggers.
6. Pour prévenir les attaques par homme du milieu, vous devez ajouter un ARP statique.

En espérant vous avoir aider. N’hésitez pas à laisser un commentaire !

Regardez notre article sur Metasploit pour apprendre à hacker l’ordinateur de votre voisin sans soucis !

[](https://h5ckfun.info/author/adrien/)

[Adrien](https://h5ckfun.info/author/adrien/)

Professionnel de l’administration système et réseau depuis plus de 10 ans. J’exerce aujourd’hui en tant que Senior Manager. Chasseur de bug bounty à mes heures perdues. Je partage ma passion pour la cybersécurité et la protection de la vie privée sur le net.

**Related Posts:**

1. [**Commandes basiques du hacking avec Kali Linux**](https://h5ckfun.info/commandes-basiques-hacking-kali-linux/)
2. [**Cracker le mot de passe d’une archive ZIP avec Kali Linux**](https://h5ckfun.info/cracker-archive-zip-kali-linux/)
3. [**Installer Kali Linux sur Windows**](https://h5ckfun.info/installer-kali-linux-sur-windows/)
4. [**Comment devenir un hacker ? Voici la solution avec GeekTyper**](https://h5ckfun.info/comment-devenir-un-hacker-geektyper/)

Categories[Astuces Hack](https://h5ckfun.info/category/astuces-hack/), [Guides](https://h5ckfun.info/category/guides/)

1 thought on “Comment hacker un wifi avec Kali Linux”

1. https://secure.gravatar.com/avatar/55757a86cd38ecbfba38d3daafa14672?s=50&r=g

[**komlan**](https://h5ckfun.info/comment-hacker-un-wifi-avec-kali-linux/)

[02/06/2018 at 15 h 57 min](https://h5ckfun.info/comment-hacker-un-wifi-avec-kali-linux/#comment-1960)

comment pirate wpa2 avec kali linux sans cle wifi  
est il neccesaire d utilise cle wifi avant de pirater wifi wpa2 AVEC KALI linux

Leave a Comment

Haut du formulaire

Comment

NameEmailWebsite

Save my name, email, and website in this browser for the next time I comment.



Bas du formulaire

**Meilleurs VPN de 2021**

|  |  |  |
| --- | --- | --- |
| https://h5ckfun.info/wp-content/uploads/2020/02/rang-1.png | [NordVPN](https://h5ckfun.info/go/vpn+nordvpn) | [Visiter le site](https://h5ckfun.info/go/vpn+nordvpn) |
| https://h5ckfun.info/wp-content/uploads/2020/02/rang-2.png | [ExpressVPN](https://h5ckfun.info/go/vpn+expressvpn) | [Visiter le site](https://h5ckfun.info/go/vpn+expressvpn) |
| https://h5ckfun.info/wp-content/uploads/2020/02/rang-3.png | [Cyberghost](https://h5ckfun.info/go/vpn+cyberghost) | [Visiter le site](https://h5ckfun.info/go/vpn+cyberghost) |

**Meilleurs Hébergeurs**

|  |  |  |
| --- | --- | --- |
| https://h5ckfun.info/wp-content/uploads/2020/02/rang-1.png | [Infomaniak](https://h5ckfun.info/go/hebergement-web+infomaniak) | [Visiter le site](https://h5ckfun.info/go/hebergement-web+infomaniak) |
| https://h5ckfun.info/wp-content/uploads/2020/02/rang-2.png | [LWS](https://h5ckfun.info/go/hebergement-web+lws+mutualise) | [Visiter le site](https://h5ckfun.info/go/hebergement-web+lws+mutualise) |
| https://h5ckfun.info/wp-content/uploads/2020/02/rang-3.png | [Ikoula](https://h5ckfun.info/go/hebergement-web+ikoula) | [Visiter le site](https://h5ckfun.info/go/hebergement-web+ikoula) |

Copyright © 2015-2021 | Power by H5ckfun.info

* [Accueil](https://h5ckfun.info/)
* [Créer un site](https://h5ckfun.info/creer-site-internet/)
* [Hébergement Web](https://h5ckfun.info/creer-site-internet/hebergement-web/)
* [VPN](https://h5ckfun.info/logiciel/vpn/)
* [Logiciels](https://h5ckfun.info/comment-hacker-un-wifi-avec-kali-linux/)

[Blog](https://h5ckfun.info/blog/)