Le Blog du Hacker

Ce qui est sécurisé à 99% n'est pas sécurisé

7 Secrets sur le Hacking

Un guide issu de : http://www.leblogduhacker.fr

7 Secrets sur le Hacking

7 Secrets sur le Hacking

Disclaimer :

Le site web Le Blog Du Hacker dont ce document est issu présente des techniques à titre ***indicatif*** *et* ***préventif*** *uniquement. En aucun cas ces informations n'incitent à transgresser les lois. L'utilisateur s'engage à utiliser ces informations sous son entière responsabilité et dégage l'éditeur de toute responsabilité à cet égard.*

Table des matières

1 Un pirate n'est pas toujours un génie en informatique

Lorsqu'on cherche à définir les « vrais » hackers, on parlera généralement de **professionnels certifiés** en sécurité informatique dont le métier consiste à trouver des failles dans les systèmes, et à les **sécuriser**. On appelle ces personnes des « hackers éthiques ».

Certains hackers éthiques **sont reconnus dans les communautés pour leurs exploits**, ils n'ont donc pas forcément tous un diplôme ou une certification.

Ces hackers éthiques ne constituent qu'un **faible pourcentage** des hackers dans le monde. En effet, un hacker dans son sens premier est une personne passionnée par la **compréhension du fonctionnement intime** d'un **système informatique**. Le domaine dépasse donc la sécurité informatique pour rejoindre celui de la **programmation** ou de **l'électronique**.

Seulement, s'il y a bien une définition faussée (mais à la mode) du terme « hacker », c'est celle véhiculée par les

médias qui correspond au « pirate informatique ». Cette définition est si populaire qu'elle est souvent utilisée volontairement.

Ce ne sont pas les hackers éthiques qui piratent les internautes, et c'est justement pour cela qu'il nous faudrait utiliser les bonnes définitions : les pirates informatiques ne sont pas des hackers éthiques. Certes les méthodes et les outils sont les **mêmes**, mais les buts sont totalement **différents**.

L'expansion des méthodes ***RAD*** (*Rapid Application Development*) a beaucoup favorisé la création très **rapide** de programmes **malveillants** puissants. Maintenant n'importe quel internaute disposant d'un manuel et d'un environnement de développement intégré (comme *Visual Studio*) peut programmer des logiciels **puissants** sans connaissances spéciales.

Cela va même plus loin, les programmes tout faits eux-mêmes sont largement distribués et utilisables par le grand public.

Le piratage typique se produit par une personne **de l'entourage de la cible**, qui agit généralement par vengeance ou par gain personnel. Le pirate en question n'aura pas de grandes connaissances des outils utilisés et des **risques encourus par leur utilisation illégale**.

2 Celui qui vous pirate vous connaît habituellement bien

C’est la transition directe après le premier point.

On ne pirate que très rarement un compte pour le **plaisir** sachant notamment les conséquences qui peuvent s'en suivre.

Il y a de fortes chances qu'une personne de votre entourage proche ou éloignée soit à **l'origine** d'un piratage de votre compte.

Loin de moi l'idée d'accuser qui que ce soit, mais la preuve est là, **90%** des demandes de piratage qui me sont directement adressées sont liées à des histoires de **couples et de travail**. À ce propos, je **refuse** toutes les demandes de piratage en question.

Nous sommes tous minuscules sur *Internet*, et nous ne sommes souvent que des « utilisateurs normaux », c'est-à-dire des utilisateurs sans importance pour les grandes organisations de cyber terroristes.

Ces organisations n’ont pas de raisons fondées de vous pirater, elles ne s’en prennent pas aux particuliers mais plutôt aux gouvernements et aux **entreprises**.

Si vous aviez les compétences nécessaires pour pirater un compte *Facebook*, pirateriez-vous un compte d'un **inconnu** ? Ou trouveriez-vous plus **intéressant** de

pirater une personne de votre entourage, et donc que vous **connaissez** ?

Attention, il y a tout de même encore beaucoup de façons de se faire pirater « par hasard », en ayant peu ou aucun lien avec le pirate.

On citera notamment le piratage d'un site web **sur lequel vous étiez inscrit(e)**, ou le piratage **massif** visant des **une catégorie d'utilisateurs**. La catégorie d'utilisateurs pouvant par exemple être les clients d'un opérateur mobile visé par une campagne de ***phishing*** (ou **hameçonnage** en français). Des e-mails aléatoires sont envoyés à des adresses e-mail volées ou trouvées sur la toile en demandant des « mises à jour » fictives d'informations de compte.

Point important : la personne qui vous pirate de son plein gré, si elle vous connaît, est généralement **débutante** et fait des erreurs, il est donc aussi facile de la **reconnaître**.

Gardez donc les programmes téléchargés et les virus en quarantaine. Ne supprimez pas non plus l'historique des sites visités ou les derniers e-mails. Ils peuvent servir à **pister** le pirate.

Plus d'informations et de statistiques ici :

http://www.leblogduhacker.fr/la-peur-des-hackers/

Plus d'informations sur le phishing :

http://www.leblogduhacker.fr/phishing-facebook-explications-contre-mesures/

3 Vous pouvez retrouver un pirate

Nous venons d'affirmer que le responsable du piratage de l'un de vos comptes est généralement une personne que vous **connaissez**. Vous pouvez facilement en avoir le cœur net si cette personne n'est pas très à l'aise en piratage.

Effectivement, il est possible de **décompiler** un programme malveillant comme n'importe quel autre programme.

On peut souvent, dans le cas des keyloggers, trouver **l'adresse e-mail** et **le mot de passe** du pirate dans le code source de son programme.

Cela est possible car le pirate doit fournir ces informations pour faire fonctionner son programme et donc pour recevoir les informations volées dans sa **boite mail**.

Des identifiants comme les mots de passe *FTP* ou d'autres services peuvent aussi être retrouvés.

Gardez donc toujours un historique des sites visités et programmes téléchargés, notamment ceux qui sont **suspects**. Car le jour où vous serez victime de piratage,

vous pourriez toujours au moins essayer de pister le hacker qui vous en veut.

Pour décompiler un programme, la méthode est relativement simple, il suffit de télécharger un programme appelé un « décompilateur » ou un « désobfuscateur » comme *.NET Reflector* et de faire un glissé-déposé du programme à décompiler.

.NET Reflector permet de récupérer les codes sources des programmes de la famille *dotnet* (.NET) c'est-à-dire *Visual Basic .NET* et *C#* entre autres. Nous avions mentionné ce type de programmes plus haut lorsqu'on parlait des méthodes de développement rapide « *RAD* ».

Les keyloggers et autres programmes malveillants sont souvent programmés avec un langage *dotnet*, il y a donc de grandes chances que la technique **fonctionne**.

Plus d'informations pour pister un hacker :

http://www.leblogduhacker.fr/comment-pister-un-hacker/

4 Un pirate finit souvent par être repéré

Vous connaissez probablement les groupes de « hackers » célèbres tels que *Anonymous* et *Lulzsec*. Peu importe leurs buts et leur influence, ils se font prendre un par un.

Prenez également le cas un peu plus ancien du piratage du *Sony Playstation Network*, le responsable de l'attaque a aussi été **trouvé rapidement**.

La découverte du réseau d'espionnage de la NSA (*National Security Agency*) prouve que nous pouvons être espionnés un peu partout à notre **insu**.

Les plus grandes entreprises ont donné leur accord pour fournir à la *NSA* les informations qu'elle voudrait rechercher, au besoin.

Pirater un système ou un utilisateur est **risqué**, vous prenez ce risque en effectuant des actions malveillantes peu importe votre pays.

Vous ne faites donc pas le poids face aux stratagèmes perfectionnés de la « cyber police », ne jouez pas les super

héros ou assumez les **conséquences**.

De plus, *Facebook*, *Google* ou encore *Microsoft* **payent** les hackers pour trouver des failles dans leurs systèmes et les signaler. Gagner de l'argent en « piratant » légalement n'est-il pas une meilleure idée ?

Voici l'article à ce sujet :

http://www.leblogduhacker.fr/gagner-de-largent-en-piratant/

Voici plus d'informations sur notre anonymat :

http://www.leblogduhacker.fr/etre-anonyme-sur-internet/

5 La faille, c'est VOUS

Un piratage réussi repose souvent sur la **ruse**.

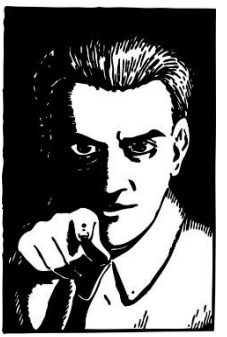
Rappelez-vous des fameux e-mails de *phishing* vous disant que vous avez **gagné au loto**, ou des sites web vous félicitant d'être le 1 000 000e visiteur.

Ces méthodes sont maintenant bien **connues**, mais le principe est resté le même et beaucoup de personnes cliquent **encore** sur des liens et téléchargent des programmes par **peur** ou par manque de connaissances.

Pourquoi par peur ?

Car, en guise d'exemple, des fenêtres **très semblables** aux fenêtres de *Windows* (entre autres) s'affichent vous informant que votre ordinateur contient des virus.

Les personnes à l'origine de ces pièges proposent ensuite des solutions tout-en-un pour **supprimer** ces virus **virtuels**.



En téléchargeant leur antivirus, vous **vous faites pirater** et vous ne vous en rendez même pas compte, vous êtes simplement content car tous les virus de votre ordinateur auront à ce moment **miraculeusement** disparu.

Plus d'informations en ligne à cette adresse :

http://www.leblogduhacker.fr/attention-votre-ordinateur-est-infecte/

Ces techniques sont issues de ce que l'on appelle « l'ingénierie sociale », c'est l'une des façons les plus populaires de vous pirater. Il s'agit d'exploiter les faiblesses dans le comportement humain, en se basant sur des concepts psychologiques.

Plus d'informations :

http://www.leblogduhacker.fr/cours-le-social-engineering/

Autre point, les smartphones, les ordinateurs publics et même les télévisions sont des outils qui utilisent l'informatique et qui peuvent être piratés. Les nouveaux moyens de communication donnent également des nouvelles pistes pour les créateurs de programmes malveillants.

Même avec toutes ces mises en garde, il n'est pas non plus question de devenir paranoïaque, mais juste **méfiant**.

En étant au courant des menaces, des habitudes et des techniques des pirates, vous serez à mesure d'analyser les **dangers** et d'éviter bien des arnaques et des ennuis.

En visitant régulièrement **Le Blog Du Hacker**, vous apprendrez ces techniques, et vous comprendrez les méthodes pour les contrer.

6 L'antivirus ne lance pas toujours l'alerte

À partir du moment où votre antivirus sonne, c'est qu'un virus a été **trouvé** et n'a pas été **exécuté**. (Même chose pour un site web malveillant)

Cela veut dire qu'effectivement votre antivirus fait du bon travail, mais ça ne certifie absolument **pas** qu'il n'y ait aucun **autre** virus sur l'ordinateur.

Un autre programme **malveillant** peut très bien fonctionner discrètement sur le PC depuis des mois sans se faire repérer.

Ça ne certifie pas non plus que le programme détecté n'a jamais été exécuté auparavant.

Cela est possible car un programme malveillant peut être **crypté** afin de le rendre **indétectable** par les antivirus.

Il est également possible de trouver la **signature** du virus à la main et de la changer sans altérer le fonctionnement du programme.

La plupart du temps, le hacker prendra soin de rendre son programme indétectable avant de l'envoyer, ce qui rend donc les antivirus inutiles.

Et même si à la longue l'antivirus finit par détecter le virus, c'est bien souvent **trop tard**.

Ne vous fiez donc pas aveuglément à votre antivirus en téléchargeant n'importe quel programme car vous ne serez pas nécessairement protégé à 100%.

Souvenez-vous également que les sites de *phishing* ne sont pas détectés, ils paraissent totalement **légitimes** et personne ne peut savoir ce qu'il se passe « derrière ».

Plus d'informations sur ces articles en ligne :

http://www.leblogduhacker.fr/pourquoi-les-antivirus-ne-sont-pas-vos-amis/

http://www.leblogduhacker.fr/un-antivirus-ca-sert-a-rien/

7 Il n'y a pas besoin de diplôme pour devenir bon

Que ce soit en hacking, en programmation ou en informatique de façon générale, il y a bien trop de personnes **qui ne passent pas à l'action** car elles ne pensent pas réussir.

Elles attendent de passer un certain diplôme ou d'atteindre un certain âge. D'autres personnes, au contraire, se pensent trop « vieilles » ou trop perdues en informatique. Pire encore, certaines suggèrent qu'il y aurait un certain *don* à posséder.

Je me dois de vous rassurer à ce sujet : **vous n'avez pas besoin d'attendre quoi que ce soit**, et il n'y a pas d'âge pour apprendre.

La meilleure chose que vous pouvez faire pour devenir bon est de commencer aujourd'hui. Vous ferez des erreurs, vous ferez peut-être de mauvais choix, mais cela vous aidera justement à prendre en main ce nouveau domaine et à vous améliorer.

Vous pouvez apprendre en partant de rien, cela fonctionne et prend simplement du temps. Si le temps n'est pas une ressource que vous souhaitez allouer, vous pouvez accélérer votre apprentissage en suivant un plan d'apprentissage.

Apprenez-en maintenant encore plus sur le hacking avec le guide « Les Bases de la Sécurité Informatique »

Ingénierie sociale, failles web, failles réseau, failles applicatives, tests d'intrusion…etc.

Vous saurez tout sur les hackers grâce à un guide spécialement adapté pour les débutants.

Mais aussi :

Les Secrets sur notre Anonymat : révélations troublantes sur votre anonymat.

Protéger son Ordinateur et sa Vie Privée : les hackers à votre service pour vraiment protéger votre PC.

Débuter avec Linux : apprenez Linux à partir de zéro grâce à un guide pratique.

N'hésitez pas à voir les autres guides ici.

Le Blog du Hacker

Ce qui est sécurisé à 99% n'est pas sécurisé