

Le Top 10 des meilleurs logiciels gratuits pour la sécurité

Par la rédaction, en ligne le 24/04/2006

Bruce Schneier affirme : « la sécurité est un processus et non un produit ». Il a parfaitement raison. Cependant, plusieurs outils gratuits peuvent permettre aux administrateurs réseau d'améliorer sensiblement le niveau de sécurité de leurs infrastructures. La condition étant bien évidemment de les utiliser dans un cadre bien défini, avec des règles et des procédures bien établies. Nous avons dressé pour vous une liste des 10 outils et logiciels gratuits les plus pratiques pour votre sécurité.

Nmap

Il était vraiment difficile de passer à côté de ce fabuleux « scanner de ports » open-source. Nmap représente aujourd'hui la solution la plus fiable et la plus performante pour dresser un état des lieux des services et ports accessibles sur un parc de machines. Disponible dans sa branche 4.x, Nmap intègre notamment des fonctionnalités d'OS Finger Printing et de « banner grabbing ». <http://www.insecure.org/nmap/>

Nessus Remote Security Scanner

Nessus est le scanner de vulnérabilités le plus utilisé en entreprise. Plus de 75.000 organisations à travers le monde ont déjà déployé ce logiciel. Pour une fois, soyons chauvins, c'est un Français qui est à l'origine de Nessus ! Renaud Deraison, son concepteur, est également à l'origine de l'éditeur Tenable Networks, basé aux Etats-Unis. <http://www.nessus.org>

John The Ripper

John The Ripper est l'arme ultime pour tester l'efficacité de ses mots de passe. Officiellement supporté par onze systèmes d'exploitation, sans compter les différentes architectures disponibles pour chacun des OS, « John The Ripper » intègre en natif les chiffrements DES, BSDI DES, MD5, Blowfish, Kerberos AFS DES et LanMan. De nombreux patches ont été développés afin de supporter d'autres types de mots de passe tels que ceux générés par MySQL, Lotus Domino, MS-SQL ou encore Oracle... <http://www.openwall.com/john/>

Nikto

L'insécurité de certains applicatifs Web n'est plus à démontrer. Pour évaluer la sécurité d'une application en ligne, Nikto peut se révéler être un compagnon indispensable. Sa base de données comporte des tests de sécurité portant sur plus de 200 serveurs Web différents et référence plusieurs milliers de scripts PHP, ASP, JSP, CGI connus pour être vulnérables. <http://www.cirt.net/code/nikto.shtml>

Ethereal

Il n'est pas facile d'avoir une visibilité sur les flux qui traversent ses réseaux. Vos utilisateurs passent-ils leur temps à discuter sur MSN ou à télécharger des fichiers illégaux à travers les réseaux peer-to-peer ? Ethereal a pour vocation de devenir l'analyseur de flux open-source (sniffer) le plus abouti, quasi-équivalent aux solutions commerciales du marché. <http://www.ethereal.com>

Eraser

Pour détruire un fichier, il ne suffit pas de le déplacer dans la corbeille. De nombreux outils de récupération de données peuvent permettre de remettre la main sur des informations que vous pensiez perdues à jamais. Eraser vous permettra d'effacer réellement ces données inscrites sur un disque dur en utilisant les méthodes Guttmann, Pseudorandom Data et US DoD 5220-22 M. Si la paranoïa vous accompagne au quotidien, ce logiciel open-source est fait pour vous. <http://www.heidi.ie/eraser/download.php>

P0f

P0f v2 est un outil permettant de faire de l'OS Fingerprinting de manière passive, c'est-à-dire sans initier aucune connexion ! Ainsi, uniquement en observant les flux qui transitent sur un réseau, il est possible de déterminer les systèmes d'exploitation des machines qui dialoguent. <http://lcamtuf.coredump.cx/p0f/p0f.shtml>

PuTTY

PuTTY est LE client Telnet et SSH pour plateformes Win32. Léger mais complet, tout administrateur réseau qui se respecte se doit d'installer PuTTY sur sa machine Windows. L'auteur du logiciel fournit également une implémentation gratuite de SCP et SFTP. Indispensable !

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

Kismet

Votre entreprise possède un réseau sans-fil ? Est-il bien sécurisé ? Quelle surface couvre t-il ? Kismet est un « sniffer » passif pour réseaux 802.11 qui vous permettra par exemple de découvrir d'éventuels points d'accès installés à votre insu ou de déterminer si votre installation est correctement configurée. En somme, Kismet vous permettra de voir l'invisible... <http://www.kismetwireless.net>

Cain & Abel

Vous avez perdu votre mot de passe de messagerie ? Peut être souhaitez-vous tout simplement tester le niveau de sécurité des mots de passe employés par vos utilisateurs ? Cain & Abel est certainement le meilleur outil gratuit du genre. En exploitant diverses techniques (sniffing, brute force, cache, ...) ,Cain & Abel est capable de retrouver en un temps record les mots de passe utilisés par de nombreuses applications.

<http://www.oxid.it/cain.html>