

L'Actu Sécurité n°3

xmco Partners

PLAN

POINT JURIDIQUE

Que faire lorsqu'une entreprise est victime d'une attaque? Comment réagir? Qui contacter? (page 2)

NOUVELLE TENDANCE

L'invasion des Rootkits : description et analyse de ce nouveau fléau. (page 4)

TESTS

Etude des différentes offres de scan de vulnérabilité en ligne (page 7)

ATTAQUES ET ALERTES MAJEURES

Description et analyse des attaques et menaces les plus importantes parues durant le mois d'Avril. (page 16)

OUTILS LIBRES

Découvrez et suivez les évolutions des outils libres les plus utiles et efficaces. (page 19)

"Etre un consultant sécurité en 2006"

Il y a 10 ans, un consultant sécurité se formait sur les firewalls checkpoint, et se préparait, sans le savoir, à participer à la révolution de l'informatique en entreprise : l'ouverture des réseaux.

Depuis, de nombreuses spécialités ont vu le jour : les tests d'intrusion applicatifs, la maîtrise d'ouvrage sécurité, les PKI, les audits organisationnels, etc.

Est-ce la demande qui a participé à l'explosion des spécialisations, ou bien est-ce l'absence de demande qui a forcé les prestataires à segmenter le marché ? La poule, l'oeuf, ..., l'éternel débat. Sans parler des SSII qui ont vendu, pendant la bulle, tellement de consultants sécurité : des stagiaires, des administrateurs systèmes, etc, ... il faut reconnaître que le terme "consultant sécurité" était plus vendeur !

La tempête paraît loin aujourd'hui. Pourtant, le trouble subsiste chez les clients, chez qui tant de discours contradictoires ont été entendus au fil des années : "Sans firewall, point de salut !" "L'IDS, c'est LA solution !" "L'IDS ?! Dépassé par l'IPS, depuis longtemps !" "La solution magique, c'est la miennne !" .. et j'en passe.

Il n'existe pas de formation pour devenir consultant sécurité. Tout ceci est bien trop neuf. Pourtant le besoin d'y voir clair se fait de plus en plus pressant.

Les contraintes d'un consultant sécurité sont multiformes : se tenir informé des évolutions permanentes, connaître le métier des clients que l'on accompagne, maîtriser les technologies et les protocoles, identifier les meilleurs outils, être conscient des pollutions que la sécurité peut causer dans une entreprise.

Finalement, être consultant sécurité revient à résoudre la quadrature du cercle, dans un environnement sans budget, sur lequel tout est dit, sauf l'essentiel.

Ma mission est pourtant simple : aider mes clients à y voir clair, identifier et adresser leurs problématiques, en leur simplifiant la vie. L'enjeu est stratégique : une réponse simple nécessite une vraie réflexion, ainsi qu'un savoir faire certain.

Jusqu'à présent, beaucoup d'interlocuteurs ont compliqué la problématique parce qu'il ne savaient pas faire autrement...

On lit partout que la sécurité est une question de bon sens. Ne serait-il pas temps que tout le monde se mette à appliquer ce principe de base ?



Olivier Patole
Consultant sécurité

I. POINT JURIDIQUE:

LA BEFTI ET L'OCLCTIC, DEUX SERVICES DE POLICE CONTRE LE PIRATAGE INFORMATIQUE

Ce mois-ci, nous avons choisi de vous expliquer la procédure à suivre en cas de piratage de votre système d'information.

Toute entreprise ou tout particulier devient un jour la victime d'un pirate ou d'un virus diffusé à grande échelle. Vols et pertes de données, tentatives d'intrusion, fraudes sur des sites d'achat en ligne, spamming, simple scan de port, exécution à distance d'exploits, de nombreuses techniques sont utilisées à outrance par les pirates avides de reconnaissances ou par de véritables bandes organisées. Quels sont les moyens juridiques qui permettent de contrer ces pirates ? Qui faut-il contacter ? Dans quelles circonstances peut-on porter plainte ? Nous tâcherons de vous présenter l'organisme policier chargé de gérer ce genre d'affaire et d'expliquer comment contrôler et tracer les attaques de votre système d'information.

XMCO | Partners



Les chiffres

Les attaques en constante augmentation

En 2005, on a recensé plus de 1500 types différents d'attaques contre moins de 500 en 2004. Il est bien sûr difficile d'obtenir des chiffres précis sur ces attaques (les entreprises ne le clament pas et les utilisateurs ne prennent pas la peine de porter plainte) mais l'analyse du nombre d'attaques de phishing (voir tableau ci-dessous), permet de saisir l'effervescence de la communauté pirate.

SECURITE INTERNE A L'ENTREPRISE		
Les amaquas en ligne (phishing) au mois de janvier 2006		
Indice	Janvier 2006	Novembre 2005
Sites actifs de phishing	9 715	4 630
Nombre total de marques ciblées	101	93
Durée de vie moyenne d'un site de phishing	5 jours	5,5 jours

Source APWG

Bien que les entreprises restent à l'écoute des nouvelles vulnérabilités et corrigent au plus vite les failles de sécurité de leurs logiciels, les particuliers ne sont pas toujours au courant des derniers problèmes liés à la sécurité et sont eux aussi la cible

d'actions malveillantes. Les chevaux de Troie et les virus sont souvent les moyens les plus utilisés pour voler des données confidentielles ou nuire aux internautes.

Peu d'entreprises et de particuliers portent plainte et les pirates restent relativement à l'abri de poursuites.

Il est important de savoir que la France est pourvue d'une législation stricte sur le sujet avec des sanctions lourdes. Les victimes doivent donc profiter de ce système juridique et de la protection fournie par la loi.

En effet, selon la loi Godfrain, "le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 245 euros d'amende". Les peines prévues sont encore plus lourdes en cas de dégâts : "Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine maximale est de deux ans d'emprisonnement et de 30 490 euros d'amende".

L'ensemble de la cybercriminalité recouvre deux grands types majeurs d'infractions pénales :

-les infractions directement liées aux technologies de l'information et de la communication (TIC) dans lesquelles l'informatique est l'objet même du délit.

-les infractions dont la commission est liée ou facilitée par les Technologies de l'Information et des Communications et pour lesquelles l'informatique n'est qu'un moyen.

Les organismes en charge de telles affaires.

La BEFTI (Brigade d'Enquête sur les Fraudes aux Technologies de l'Information)

Créée en 1994, cette unité est constituée de 28 agents, officiers de Police. Elle a pour but de lutter contre tout type d'infractions, notamment les atteintes aux systèmes d'information et de communication (réseaux informatiques, GSM...), les émissions frauduleuses de médias chiffrés et les téléchargements illégaux. Les plaintes traitées vont donc de l'escroquerie (achat en ligne) à la diffamation (sur des blogs ou forums) en passant par les détournements de fonds ou encore des atteintes aux biens (recol de vol).

La BEFTI enregistre les plaintes liées à toutes les infractions informatiques, participent à la recherche des

pirates et analyse les supports récupérés lors de perquisitions.



L'O.C.L.C.T.I.C (Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication)

Il travaille en étroite collaboration avec la BEFTI et regroupe l'ensemble des informations liées à ce genre de délit. Son champs d'action ne se limite pas à la région parisienne mais englobe l'ensemble du territoire national. Constitué de 38 agents de police, l'OCLTIC vise à renseigner les victimes et assiste la BEFTI.

L'O.C.L.C.T.I.C. appartient à la Direction Générale de la Police Nationale et dépend de Direction Centrale de la Police Judiciaire. Cet organisme a été créé en Mai 2000 afin de lutter contre la délinquance liée aux nouvelles technologies de l'information et de la communication.

Ces deux services sont en charge des activités opérationnelles suivantes :

- Intrusion sur les systèmes de traitement automatisé de données sous toutes ses formes
- Fraudes de télécommunication, de téléphonie portable et de cartes téléphoniques
- Contrefaçons de logiciels
- Contrefaçons par marquage de microprocesseurs, de barrettes mémoires et d'autres composants ou d'ensembles de composants électroniques
- Escroqueries liées au commerce électronique, par utilisation frauduleuse de numéro de carte bancaire
- Infractions à la Loi "Informatique et Libertés"

- Infractions à la Loi sur la cryptologie
- Coordination des enquêtes judiciaires des services de police dans le domaine de la haute technologie. D'autre part, des interventions techniques peuvent également être menées :
- Perquisitions en milieu informatique
- Interface entre les enquêteurs et les techniciens judiciairement requis dans le cadre d'interventions sur les gros systèmes
- Surveillance électronique de réseaux et / ou interceptions internet, dans le cadre d'affaires judiciaires

Contrairement à la BEFTI, l'O.C.L.C.T.I.C ajoute un caractère stratégique. Elle s'occupe de la documentation opérationnelle, de la coopération internationale, de la formation et de la sensibilisation ainsi que de la veille technologique.

Comment réagir en cas d'attaque ? Déposer plainte

Afin de porter plainte, il vous faut regrouper les éléments suivants :

- une trace informatique des dégâts engendrés par l'attaque (logs, traces d'un cheval de Troie, keylogger). Un support magnétique de ces données devra ensuite être fourni aux agents de la BEFTI.

- l'adresse exacte de la ou des machines attaquées (celle de votre domicile pour votre poste de travail ou du serveur hébergé chez votre fournisseur d'accès pour votre site web).
- la liste précise de tous les préjudices subis par l'attaque.



L'importance du stockage

L'archivage des données reste la meilleure solution pour être certain d'avoir des informations sur les pirates ou logiciels malveillants.

En effet, la plupart des entreprises stockent sur plus de trois mois leurs logs. La traçabilité des données constitue donc la pièce maîtresse pour les plaintes. Il est conseillé dans ce genre de situation d'effectuer une sauvegarde complète du disque dur du système affecté afin de pouvoir identifier les traces laissées par le pirate.

Comme dans le hall d'accueil d'une société, toutes les allées et venues de visiteurs au sein d'un système d'information doivent être enregistrées. Le stockage des données permettra aux membres de la BEFTI de pouvoir analyser sérieusement les logs.

Près de 25% des plaintes traitées par la BEFTI n'aboutissent pas, les données (logs) ne sont pas stockées suffisamment longtemps, d'où l'importance de ce point.

Qui contacter ?

En fonction du lieu de l'attaque, deux choix s'offre à vous.

La BEFTI, Brigade d'Enquête sur les Fraudes aux Technologies de l'Information est l'interlocuteur à privilégier en cas d'attaques pour l'ensemble de la région parisienne (Paris, Hauts-de-Seine, Seine-Saint-Denis et le Val de Marne). Cette unité se situe au 163 avenue d'Italie - 75 013 Paris. Standard : 01.40.79.67.50. Les enquêteurs de la B.E.F.T.I. sont spécialisés dans les crimes informatiques sous toutes leurs formes.

Pour tous les autres départements, il faut contacter votre Service Régional de Police Judiciaire. Les coordonnées de ce service vous seront fournies par le commissariat ou la gendarmerie la plus proche de chez vous. Des agents spécialisés sous le statut d'ESCI (« Enquêteur Spécialisé sur la Criminalité Informatique ») seront la pour enregistrer la plainte.

L'O.C.L.C.T.I.C se trouve 101 rue des Trois Fontanot - 92 000 Nanterre, Standard 01.49.27.49.27. Une fois au standard, demandez simplement vers qui vous orienter pour porter plainte et décrivez brièvement le contexte de l'attaque.

2. NOUVELLE TENDANCE :

L'EXPLOSION DES ROOTKITS

Le premier trimestre 2006 a été marqué par une augmentation importante du nombre d'incidents liés à des rootkits. En effet, nous assistons à une hausse de plus de 700% par rapport à la même période l'an dernier.

Ces outils se développent continuellement et deviennent de plus en plus complexes. Auparavant, un rootkit se voulait efficace quel qu'en soient les moyens. Aujourd'hui, ces logiciels mettent tout en place pour devenir indétectables et facile à déployer. D'autre part, il existe désormais des outils et des méthodes disponibles sur Internet, pour les générer encore plus rapidement.

XMCO | Partners



Le développement des rootkits

Le rootkit, le nouveau jouet préféré des pirates

De nombreuses sociétés spécialisées dans la recherche de virus viennent d'alerter les internautes à propos du développement et de la propagation des rootkits. En effet, ces programmes difficiles à détecter et à éradiquer se greffent sur le noyau du système d'exploitation. Ils permettent ainsi d'effectuer à distance des actions malicieuses. Il est donc possible, comme avec un cheval de Troie, de prendre le contrôle d'une machine à distance, d'utiliser le système piraté comme serveur de spam ou comme passerelle pour d'autres attaques et de voler des données confidentielles.

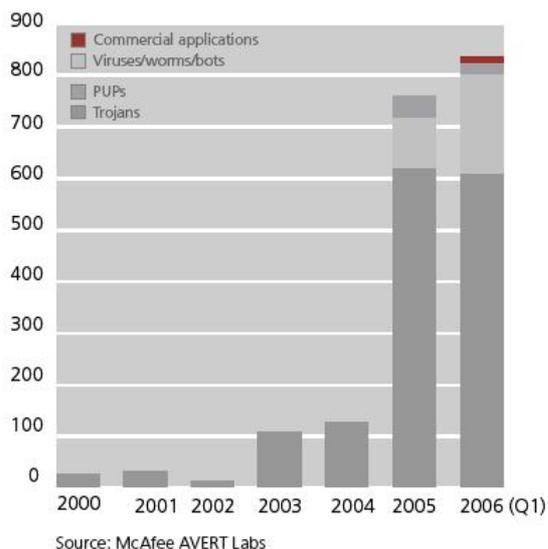


Schéma 1 : Nombres de logiciels contenant des fonctionnalités malveillantes depuis 2000. [1]

Initialement, un rootkit était composé d'une suite d'outils permettant d'obtenir des droits administrateurs au sein d'une machine. Les premiers rootkits sont apparus dans le monde UNIX. Aujourd'hui, ces programmes sont XMCO PARTNERS - CABINET DE CONSEIL EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

disponibles pour tout type de plateformes et regroupent les virus, les trojans, les vers, et les différents malwares.

L'évolution de ces outils

La complexité accrue de ces outils ainsi que leurs capacités d'adaptation aux évolutions du marché inquiètent. Par exemple, auparavant, une backdoor se mettait en écoute sur un port en attente de la connexion du pirate. Or avec l'arrivée des premiers firewalls, des variantes sont apparues, avec comme modification principale, l'inversion du sens de la connexion. Le logiciel espion se connectait alors auprès d'un serveur pirate.

Ceci était possible puisque peu de firewalls filtraient les connexions sortantes (voir le pare-feu de Windows XP SP2).

La sécurité des postes utilisateurs est au cœur des préoccupations, les rootkits ont évolué pour contourner les protections ou même les désactiver. De nos jours, un bon logiciel espion s'exécute avec des droits SYSTEME (droits supérieurs à l'administrateur/root) et dans l'espace du noyau. Celui-ci modifie aussi les pointeurs d'appels des fonctions systèmes afin de se rendre indétectable. Par exemple, en ce qui concerne la backdoor « BLACKMOON » [2], après qu'un utilisateur ait tenté d'ouvrir un fichier générant une erreur, celle-ci s'installe sans être détectée par aucun antivirus ou firewall personnel et permet un contrôle total de la machine par un pirate. Or, l'utilisateur, en apercevant le message d'erreur, pensera que rien ne s'est exécuté (voir les schéma 2 et 3).

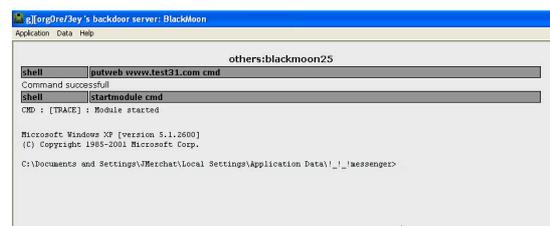


Schéma 2 : Coté Serveur du Pirate, connexion à la machine infectée.

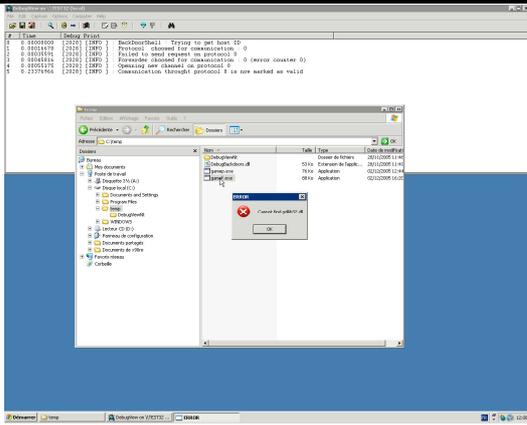


Schéma 3 : Ouverture du fichier contenant BlackMoon.

Une grande diversité de sources Internet, une mine d'or pour les hackers

Bien entendu, l'augmentation du nombre d'attaques résulte de l'explosion des accès Internet. L'accès à ce genre d'outils devient très facile. De plus, un rootkit dispose d'une interface simplifiée et de guides complets d'utilisation. Cependant, l'emploi de malware dont personne ne connaît le code source réel est dangereux. Ce logiciel peut très bien en contenir un autre caché. En effet, rare sont les pirates qui effectuent une analyse du binaire qu'ils utilisent pourvu qu'ils obtiennent un accès à la machine distante.

Le côté ironique de l'histoire réside dans la présence de backdoors au sein d'elles-mêmes. Ainsi, certains créateurs de rootkits les diffusent massivement en y injectant du code supplémentaire pour qu'à chaque compromission, un mail contenant des informations sur la nouvelle cible, lui soit envoyé discrètement sur une webmail anonyme. Le créateur de la backdoor ne l'utilisera, pour ainsi dire jamais, et ne prendra donc aucun risque. Cependant, il disposera d'une importante liste de machines potentiellement vulnérables qu'il pourra revendre.

Cette revente est possible grâce au marché des machines zombies. En effet, certains pirates ne souhaitent pas s'attaquer directement aux machines vulnérables. En se constituant un véritable réseau de bots, ceux-ci veulent s'en servir pour réaliser des attaques ponctuelles de plus grandes envergures, de type dénis de service distribués (DDoS), par exemple.

Un second facteur réside dans la diversité d'outils disponibles afin de créer son propre exploit. Nous pouvons citer le projet Metasploit [3] à l'aide duquel vous pouvez générer votre propre shellcode pour exploiter la dernière faille à la mode en trois clics de souris.

Ci-contre, un exemple qui permet la génération d'un binaire exploitant la faille Microsoft MS05-039. Il permet d'y installer un serveur VNC (prise de contrôle total à distance, voir le schéma 4).

Il existe aussi, de nombreuses bibliothèques pour créer rapidement son rootkit.

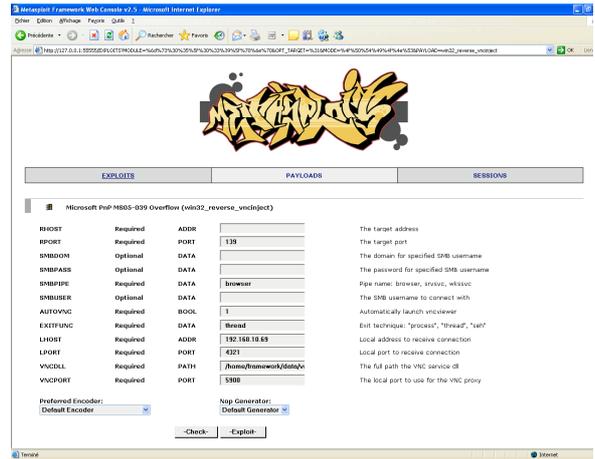


Schéma 4 : Génération d'un ShellCode avec MetaSploit.

Des applications commerciales vérolées.

Depuis peu, certains éditeurs, même parmi les plus connus, ont introduit au sein de certaines de leurs applications commerciales des logiciels de ce type. Nous pouvons citer les cas de Symantec [4] et SONY [5]. Le rootkit Symantec était présent dans sa solution Norton SystemWorks, afin de dissimuler dans le système le répertoire NPROTECT. Ce dernier permet la récupération de fichiers effacés. Pour sa part, SONY installait via certains CD Audio des rootkits afin de gérer les protections DRM (voir le schéma 6).

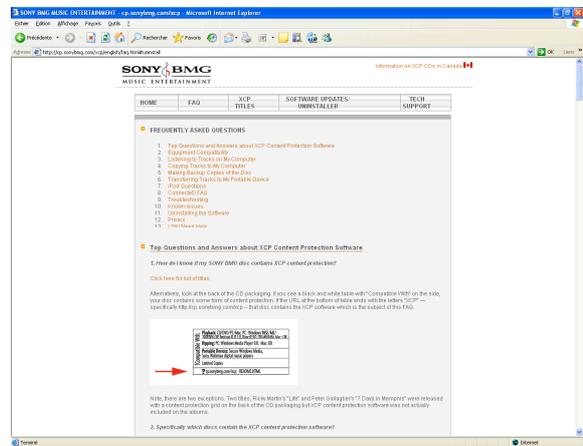


Schéma 5 : Site Internet de SONY proposant le téléchargement d'un outil permettant de supprimer son logiciel caché. [5]

Contre-mesures Après une infection, quelle solution ?

Sachez que si votre machine a été infectée, il est impératif de ne plus y toucher avant de prendre une décision. En effet, la moindre action pourrait effacer des traces des manipulations du pirate, modifier les dates et heures d'accès à certains fichiers ou noyer des informations importantes contenues dans les journaux de logs.

Si vous souhaitez porter plainte, vous devez contacter au plus vite les services de police concernés et ne plus toucher à la machine compromise (voir notre article dans la rubrique « Point Juridique »). Sachez cependant, que la machine sera saisie pendant une durée indéterminée. Cette décision n'est pas à prendre à la légère surtout pour une PME.

Le principal problème d'une infection par un rootkit est l'incertitude de l'étendue des « dégâts ». En effet, il est très difficile de savoir exactement quelles sont les fonctions systèmes qui ont été modifiées, quels outils ont été installés ou encore quid de l'intégrité des fichiers et des documents ? A moins de disposer de temps ainsi que de contrôles d'intégrité réguliers, la suite d'une intrusion se résout généralement par une réinstallation complète du système à condition, bien entendu de posséder les sauvegardes des fichiers sensibles. Dans le cas contraire, il restera toujours le doute d'être passé à coté d'un malware ou d'une modification.

Enfin, il est important de souligner que les rootkits sont de plus en plus discrets. En effet, si la machine infectée ne se plante pas ou ne ralentit pas, il est très difficile de s'en rendre compte. Il est donc important d'effectuer des analyses et des scans réguliers sans omettre d'effectuer des sauvegardes récurrentes.

Les protections

Bien entendu, les règles de sécurité demeurent identiques, à savoir de disposer d'un système complètement patché avec un anti-virus à jour ainsi qu'un firewall bien configuré. De même, il existe des outils comme « chkrootkit » (UNIX) [6], « Rookit Revealer » (WINDOWS) [7] qui permettent de vérifier si la machine est infectée.

Cependant, tout comme les anti-virus, ces solutions fonctionnent sur des bases de signatures. La sécurité est mise en place pour toute attaque connue mais perd toute efficacité contre une nouvelle variante ou un malware encore inconnu.

Il n'y a pas de protection miracle contre les rootkits. Toutefois, une bonne sensibilisation des utilisateurs ainsi que la formalisation de certaines tâches d'administration peuvent diminuer fortement le risque d'infection. On ne le répètera jamais assez, un outil malveillant ne peut s'exécuter tout seul. Il doit pouvoir exploiter une vulnérabilité non corrigée du système (débordement de tampon par exemple) ou être exécuté par un utilisateur. La formation des usagers de matériels informatiques intervient à ce stade. Il est indispensable de se méfier de tout site web ou mail suspect qui demande l'ouverture/exécution d'un fichier ou d'un processus.

Les tâches administratives dépendent, bien entendu, de la criticité des systèmes. Cependant, elles s'articulent autour de la gestion des mises à jour du parc informatique, des sauvegardes, de la veille sécurité, de l'analyse des

journaux de logs et des flux du réseau et de la vérification des signatures des fonctions systèmes...

Les possibilités sont donc très vastes. Néanmoins, en maintenant à jour tous les systèmes, en informant et responsabilisant les utilisateurs, de nombreuses attaques pourront être contrées.

Webographie

[1] Etude de McAfee et AVERT Labs sur l'évolution des rootkits
http://download.nai.com/products/mcafee-avert/WhitePapers/AKapoor_Rootkits1.pdf

[2] BlackMoon est une backdoor développée à titre de recherche. Aucune source ou binaire compilé n'est disponible. Cependant, des présentations et des vidéos de démonstrations sont disponibles sur le site de l'auteur.
<http://benjamin.caillat.free.fr/backdoors.php>

[3] Le Projet MetaSploit
<http://www.metasploit.com/>

[4] Le rootkit de SYMANTEC
<http://www.clubic.com/actualite-30892-symantec-aussi-evince-son-propre-rootkit.html>

[5] Le rootkit de SONY
<http://www.clubic.com/actualite-29204-sony-rootkit-desinstallation-faillie-echange.html>
<http://cp.sonybmg.com/xcp/english/updates.html>

[6] ChkRootkit
<http://www.chkrootkit.org/>

[7] Rootkit Revealer
<http://www.sysinternals.com/Utilities/RootkitRevealer.html>



3. TEST :

TESTER LA SECURITE DE VOS APPLICATIONS ET DE VOS SERVEURS EN LIGNE

Cette nouvelle rubrique analysera, tous les mois, un produit ou un service en rapport avec la sécurité informatique.

Ce mois-ci, nous avons choisi d'étudier différentes offres de scan en ligne permettant de tester la sécurité d'une application ou d'un serveur. En effet, de plus en plus de RSSI et d'administrateurs préfèrent décharger cette masse de travail à des professionnels.

Plusieurs sociétés proposent donc des essais gratuits que nous avons étudié avec soin afin de vous conseiller les meilleurs et de vous faire éviter les pires.

XMCO | Partners



Mise en place de la maquette et sélection des sociétés spécialisées.

Le test

Notre test va prendre en compte de nombreux points. Le premier point sera d'analyser la précision du scanner et l'élément majeur; la perspicacité des résultats (analyse des vulnérabilités trouvées, faux positifs, pièges ...). Dans un deuxième temps, nous étudierons la présentation des résultats, la consistance du rapport, les services offerts pour ce test gratuit et le contact avec des ingénieurs avant-vente.

Nous comparerons ces services avec un scanner connu (Nessus) ce qui permettra d'évaluer les véritables avantages et inconvénients des scans en ligne par rapport aux logiciels libres. Ces scanners correspondent-ils aux attentes des clients? Les résultats sont-ils pertinents? Nous tâcherons de répondre à ces questions en étudiant les différentes offres du marché.

Notre maquette de test

Nous avons réalisé ce test à l'aide d'une maquette préparée au sein de nos laboratoires. Les outils de scan sont réputés pour renvoyer de nombreux faux-positifs. Le but de notre analyse sera de confirmer ou non cette tendance. Pour cela, nous avons constitué un ensemble de machines avec plusieurs ports et services ouverts. Les services ne correspondent pas toujours aux ports affectés par défaut. Ceci permettra de tester si les outils de scan se basent seulement sur les bannières, ou si des scans approfondis sur les protocoles sont effectués.

Nous avons également créé une application web qui comporte de nombreuses failles connues (vulnérabilités, Injection SQL, scripts dangereux...). Ce qui servira à déterminer l'efficacité des scans de failles de sécurité web.

Notre maquette se compose de deux machines distinctes, une équipée du système d'exploitation Windows

2003 Serveur et l'autre d'une distribution Linux. Ce choix a été guidé par la volonté de tester des serveurs web différents (IIS et Apache) et par la réaction des scans face à des machines de plate-formes différentes.

Le serveur Windows

Notre première machine émuler plusieurs services. Un bon scan tâchera de vérifier le protocole en lui-même et ne se basera pas seulement sur les bannières renvoyées. Il est donc intéressant d'installer un "Honey Pot" (Pot de miel qui permet de simuler la présence de service et qui est le plus souvent utilisé pour attirer et observer les faits et gestes d'un pirate). Nous avons choisi d'utiliser le logiciel KFSensor qui nous permet de générer rapidement des ports ouverts avec des bannières imposées par nos soins.

Ce premier point reste un des plus importants, un bon scanner doit vraiment s'assurer avec exactitude de la présence d'un service. Nous avons choisi de simuler les services et les ports suivants :

- port 389 avec un serveur LDAP
- port 1433 avec un serveur SQL
- port 1521 avec service Oracle 8i
- port 1526 avec service Oracle 9i

Aucune vulnérabilité ne devrait être détectée, nous attendons simplement que ces ports soient définis comme ouverts et que le scanner ne nous précise pas les services (falsifiés).

Notre deuxième pôle se compose d'un serveur web IIS 6.0 sur le port 8888. Cette plate-forme permettra uniquement de voir si les outils de scan détectent correctement un tel serveur sur un port exotique. Seule une page html pourra être accessible.

Ces ports laissés ouverts sont donc de simples indicateurs qui nous préciseront la granularité du scan. En effet, certains scanners ne se basent que sur les port dits «reconnus» ou réservés entre 1 et 1023. Cela n'est bien sur pas suffisant.

La deuxième grande partie propre à ce serveur 2003 est un autre serveur web qui possèdera de véritables pages web ainsi qu'une application avec plusieurs failles de sécurité.

Nous avons, pour cela, installé un serveur Apache 1.3.33 sans bannière sur le port 80. Un répertoire /admin a été consciencieusement laissé à la racine. Il inclut un dossier /etc et un fichier passwd.txt. Le scanner devrait être en mesure de déterminer l'existence critique de tels fichiers et de tels dossiers.

La page d'index de ce serveur web possède un formulaire. Nous avons généré des fausses erreurs ODBC lors de tentatives d'attaques d'injection SQL (en soumettant les caractères ' ou «) dans le champs login.

De plus, un fichier texte est accessible par un lien. Avec cette astuce, nous avons créé une faille de « Directory Transversal ». Un attaquant serait en mesure de remonter l'arborescence de nos répertoires et d'accéder à tous les fichiers sensibles de notre système. Nous verrons si les scanners tentent ces types d'attaques.

Enfin un dernier lien permettra d'accéder à une application PHPBB comportant plusieurs failles de Cross Site Scripting et autres vulnérabilités variées.

Le serveur Apache

Une deuxième machine a été mise en place. Nous avons utilisé une distribution Debian 3.1 (avec noyau 2.6.8-2). Nous avons installé un serveur ssh sur le port 20000 avec OpenSSH 3.8.1 et OpenSSL 0.9.7 e. Ces deux paquets comportent quelques failles qui, espérons-le, seront précisées dans les rapports de scans.

Nous avons ensuite installé un serveur de mails, en l'occurrence Sendmail (v8.13.4-3), qui comporte une faille récente et critique. De plus, nous verrons si le scan renvoie avec certitude ou non la version de ce serveur SMTP.

Pour finir, nous avons intégré un serveur web Apache 2.0.45 qui renvoie une bannière IIS 4.0. Ceci permettra de s'assurer de la cohérence du scan. En effet, si un système UNIX est détecté, il serait impossible qu'un serveur IIS (spécifique aux plate-formes Microsoft) y soit installé. De plus, plusieurs scripts dangereux sont hébergés dans le répertoire Cgi-bin (openfile.pl et ls.pl).

Enfin, nous avons recompilé Apache afin de répondre «200 OK» pour toute requête effectuée sur le serveur. Ceci

pourrait fausser les découvertes du scan et retourner de nombreux faux-positifs.

Les concurrents

Après plusieurs recherches, nous avons sélectionné trois sociétés spécialisées dans la sécurité. Chacune d'entre elle possède une rubrique dédiée au test en ligne de vulnérabilité sur leur site web. Nous avons choisi de vous présenter Qualys, le leader de ce marché, Criston, et Acunetix qui propose seulement des tests d'applications web mais ne gère pas les scans complets d'adresses IP.



QUALYS
SECURITY ON DEMAND

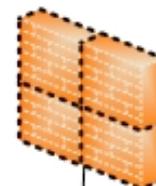
acunetix



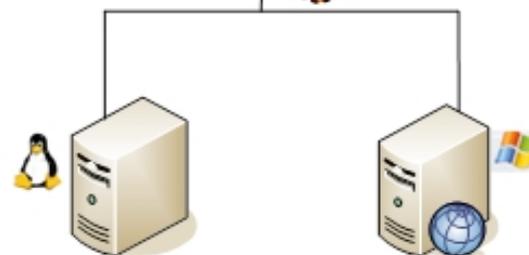
Nessus
Vulnerability Scanner

CRISTON

Scanner en ligne
(Qualys, Criston, Acunetix, Nessus)



Firewall Checkpoint NG



Apache + Sendmail

- Faillles importantes :**
- Directory transversal
 - Lecture des fichiers du serveur
 - Buffer Overflow sur Apache
 - Buffer Overflow sur Sendmail

Apache Win32 + IIS 6

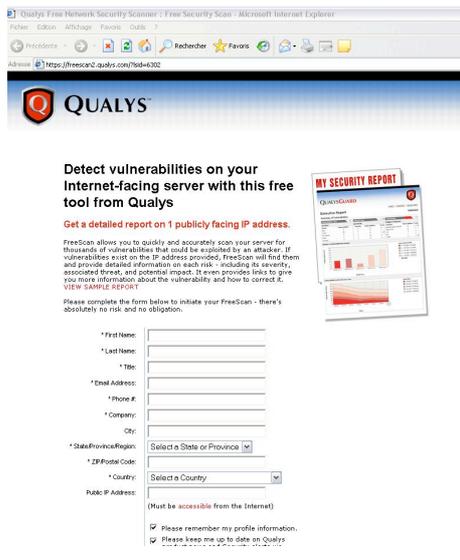
- Faillles importantes :**
- Répertoire /admin avec passwd.txt
 - Directory Listing
 - SQL Injection sur page de login
 - Lecture des fichiers du serveur
 - Plusieurs lectures de codes sources
 - Plusieurs failles PHPBB

Les résultats

QUALYS

La première prise de contact avec le site de Qualys fut simple et rapide. De grandes icônes nous ont indiqué immédiatement le chemin à suivre pour bénéficier d'une évaluation gratuite.

Ensuite, un simple formulaire à remplir a suffi pour commencer l'évaluation.



Formulaire à remplir (Qualys)

Le test dont nous bénéficions est valable 14 jours. Une fois enregistré sur le site, nous avons immédiatement reçu l'email d'un avant-vente en français prêt à répondre à nos questions.

Plusieurs outils furent ensuite à notre disposition : FreeMap, FreeScan, SANS 20, QualysGuard. Il a suffi de choisir le service en remplissant le même genre de formulaire. Un email pour chaque service nous a ensuite été envoyé et chaque test a pu ensuite démarrer en suivant simplement une URL.

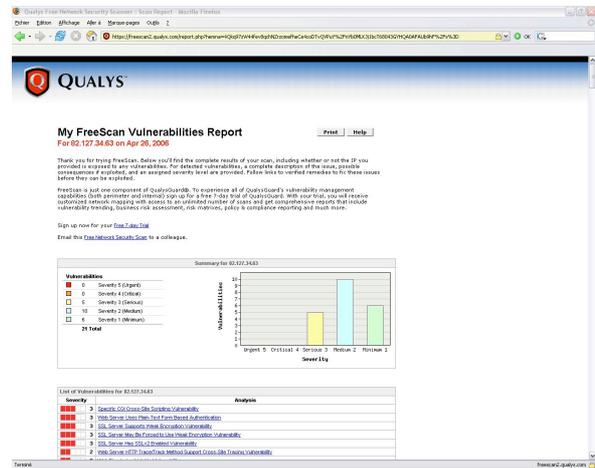
Nous avons choisi de ne souscrire qu'à deux services. Voici une brève description :

-FreeScan : détection des vulnérabilités les plus communes. Un rapport est fourni à la fin du scan avec la sévérité et l'identification des failles.

-SANS Top 20 : Détermination de la vulnérabilité du serveur aux 20 failles de sécurité les plus critiques identifiées par le SANS (organisme spécialisé dans la publication de failles de sécurité).

Le scan de Qualys est assez décevant. En effet, seuls les ports inférieurs à 1024 ont été testés. Les différentes vulnérabilités ne sont pas du tout en adéquation avec les failles mises en place. Certes, le scanner détecte des serveurs http sur les ports 80 et 23 mais aucune information

relative n'est alors communiquée (type, version...). Ce scanner apparaît pauvre et les résultats incomplets, comparativement à Nessus et Criston. Ce scanner effectue de nombreux tests intéressants, comme l'exploitation de directory transversal à travers le paramètre « file », mais aucun retour sur ce paramètre sensible n'a été présenté dans le rapport (le compte rendu du honey pot nous permet de voir l'ensemble des scans effectués).



Rapport du scan (Qualys)

Enfin le rapport n'est pas attractif malgré un graphique qui recense les failles selon la criticité. Il aurait été intéressant d'avoir un tableau récapitulatif des ports ouverts et des liens vers des descriptions plus détaillées des vulnérabilités. De plus, ce document est uniquement écrit en anglais.

Nous espérons que ce scanner en ligne n'a pas exploité l'ensemble de ses possibilités et que la version payante sera plus complète et précise.

Le contact commercial est perfectible. Un email nominatif nous a tout de même été envoyé à la fin du scan mais aucun ingénieur n'a répondu à nos questions. Enfin, nous avons été conviés à une journée de formation et certification Qualys.

CRISTON

Comme pour Qualys, Criston Software, société spécialisée en sécurité informatique, propose un outil gratuit de scan en ligne accessible rapidement. En effet dès la première visite, il nous a été facile d'accéder au formulaire. Après l'envoi de nos coordonnées et adresse IP à scanner, il nous a malheureusement fallu attendre plusieurs jours. Au final, aucune réponse par email et aucune prise de contact par l'un de leur conseiller.

Nous avons donc appelé le service client. Le routage vers les ingénieurs spécialisés a été rapide. Une erreur lors de notre enregistrement nous a été confirmée...

Nous avons dû fournir à nouveau nos coordonnées et quelques jours après, le premier scan était lancé.



Audit de Vulnérabilité gratuit

Vulnerability Manager FreeScan proposé par Criston est un service basé sur la technologie Vulnerability Manager (VM), système qui permet l'analyse de réseaux informatique et révèle les vulnérabilités existantes.

Vulnerability Manager FreeScan présente le niveau de sécurité des équipements et mesure la criticité des failles existantes, en effectuant un scan approfondi.

* Nom:
 * Fonction:
 * Société:
 * Email:
 (E-mail professionnel uniquement xxx@société.com)
 * Téléphone:
 Fax:
 Adresse:
 Ville:
 Code Postal:
 Pays:
 Nombre de PC:
 Adresse IP publique & scanner:
 (Uniquement une adresse IP publique appartenant à votre société)

Formulaire à remplir (Criston)

Le lendemain de notre demande, un conseiller nous a contacté afin de nous expliquer en détails les différents rapports proposés. Trois documents nous ont été fournis.

Le premier offre une appréciation globale du test avec un tableau de bord des différentes failles.

Des indices caractérisent les différentes vulnérabilités en attribuant une note de 0 à 100. Nommé **CARD**, ce système se base sur quatre critères : Corruption des données / Accès aux informations / Remote execution of code / Déni de service et un autre tableau présente la difficulté d'exploitation de la faille sur trois niveaux (débutant, initié, confirmé, expert).

Ce rapport ne sert pas à grand-chose, les données ne sont pas exploitables pour le scan d'une seule adresse IP.

Le deuxième rapport présente une vision des vulnérabilités par machine (en l'occurrence de notre machine de test). Des informations intéressantes sont fournies (Système d'exploitation de la machine, ports ouverts). Aucune erreur dans les services tournant derrière les ports ouverts n'est à précisé. Le scanner ne s'est pas fait piéger en analysant nos ports factices et a trouvé tous les ports y compris ceux au dessus de 1024. De plus, les serveurs web (deux Apache et IIS 6.0) ont également été trouvés. La première étude du scan commence donc bien.

La dernière analyse détaille les failles trouvées avec des solutions et des indices permettant d'évaluer rapidement les risques liés à l'exploitation des failles (grâce à l'indice IRF et le CARD). Ce rapport, constitué d'une vingtaine de pages, apparaît très complet et impeccablement présenté (sommaire, tableau, précision de l'IP et du port pour chaque faille, le statut de la faille entre plusieurs scans ...). Des couleurs et des graphiques permettent de cerner rapidement et de retrouver les éléments recherchés. Malgré cela, les résultats ne sont pas à la hauteur de nos attentes.

En effet, bien que la moitié des failles mises en place a été trouvée, le rapport compte trop de faux positifs. Le scan a tout de même identifié des failles PHP que nous n'avions pas mis en test et le formulaire d'authentification de notre page d'accueil du serveur web sur le port 80.

Criston reste un outil au dessus du scanner de Qualys. L'analyse correcte des ports, la qualité des rapports et la prise de contact avec un ingénieur reste les atouts principaux.

HTTP TRACE Method Cross-Site Scripting

Score: 75
 Service Type: HTTP
 Publication Date: 1970-01-01
 CVE ID: CWE-20
 CEST ID: CEST-10
 Vendor ID: [redacted]

Nom	Adresse	IRF machine	Nombre de vulnérabilités	Port	Protocole IP	Identifié / possible	Statut
IP:82.127.34.83	82.127.34.83	100	11	23	top	[redacted]	HEU
IP:82.127.34.83	82.127.34.83	100	11	80	top	[redacted]	HEU
IP:82.127.34.83	82.127.34.83	100	11	443	top	[redacted]	HEU

Description
 Your web server supports the TRACE method.
Consequences
 A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.
Description technique
 The HTTP TRACE method is used for web servers debugging purposes. This method allows cross-site scripting since it does not check for its parameters. A production Web server should never have this method enabled.
Solution
 Disable the TRACE and TRACE methods of your HTTP server.

Host has SSL v2 enabled

Score: 34
 Service Type: SSL
 Publication Date: 1970-01-01
 CVE ID: CWE-20
 CEST ID: CEST-10
 Vendor ID: [redacted]

Nom	Adresse	IRF machine	Nombre de vulnérabilités	Port	Protocole IP	Identifié / possible	Statut
IP:82.127.34.83	82.127.34.83	100	11	443	top	[redacted]	HEU

Description
 The SSLv2 protocol can be used to communicate with this host.

Page 6 sur 22 Rapport généré le 2006-05-17 10:34 AMCO partners

Rapport du scan (Criston)

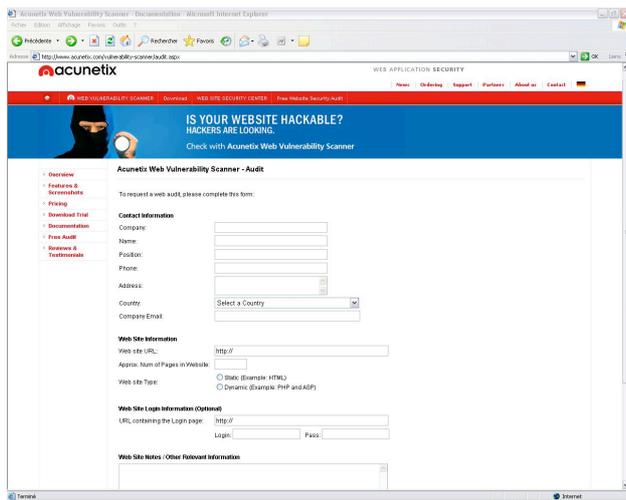
De plus, le scanner a détecté une faille d'injection SQL, ce qu'aucun autre concurrent n'a pu découvrir. Le scan des différentes pages présentes sur les serveur http n'est malheureusement pas à la hauteur. En analysant le code des pages web et des dossiers puis en listant les différentes URL appelées, l'outil de Criston aurait pu trouver le dossier "/Admin" et le fichier "/passwd.txt" ainsi que les fichiers "index.bak" et "index.old". Ces fonctions faciles à implémenter devraient être intégrées dans tout scanner de base.

ACUNETIX

Acunetix est un scanner de vulnérabilité web. Cette société effectue uniquement des tests de serveur http et ne s'occupe pas de l'analyse de ports. Les résultats sont alors différents et toutes les vulnérabilités qui ne concernent pas les ports 80, 23 et 8889 n'ont forcément pas pu être découvertes.

Le principe est toujours le même, il suffit de remplir un formulaire avec cette fois-ci, non pas une adresse IP mais une URL. Notre première demande a échoué. Nous n'avons pas su pourquoi mais nous imaginons que le fait de rentrer http://IP n'a sans doute pas été pris en compte. Après l'envoi de plusieurs emails, nous n'avons toujours pas eu de réponse. Quelques jours plus tard, nous avons relancé Acunetix qui nous a immédiatement répondu. Nous avons eu une réponse amicale d'une personne chargée de la relation clientèle. Nous avons alors exposé notre problème (en anglais) et le scan a été lancé.

Le lendemain, un email contenant 4 rapports nous a été adressé.



Formulaire à remplir (Acunetix)

Acunetix est spécialisée dans la recherche de vulnérabilité web. Notre maquette regroupe essentiellement de telles failles de sécurité. Cette société semblait au premier abord la plus apte à répondre à nos attentes. Commençons par les points positifs. Quatre rapports nous ont été envoyés. Chacun résume en une seule page les vulnérabilités trouvées sur les différents ports scannés. Un dernier rapport rassemble et décrit les failles avec précision.

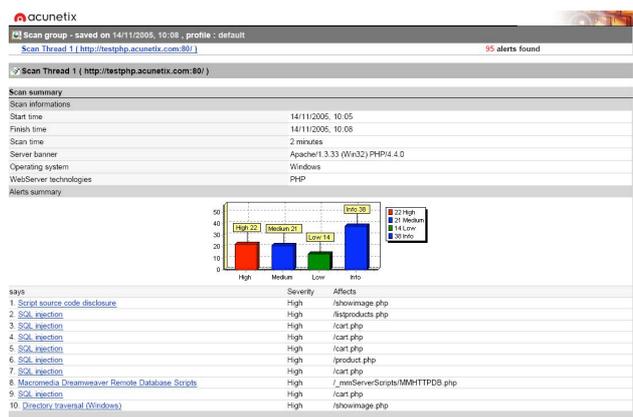
Les failles de sécurité sont bien décrites et les liens sont donnés afin d'en savoir plus sur la possible exploitation de la vulnérabilité. Enfin, la requête et la réponse effectuée lors du test sont également présentées.

Malgré cela, le test est relativement mauvais. En ne ciblant notre analyse que sur les failles web, le rapport nous a recensé près de 90 faux positifs sur notre serveur basé sur le port 80... Nous ne trouvons aucune explication à cette masse de mauvais résultats. En effet, notre deuxième serveur web, qui était chargé de renvoyer des réponses 200 OK, n'est pas au cœur du problème.

Le scan a trouvé de nombreuses pages inexistantes dont :

- /showimage.php
- /listproducts.php
- /cart.php
- /product.php
- /_mmServerScripts/MMHTTPDB.php
- /showimage.php
- /listproducts.php
- /listproducts.php
- /product.php
- /artists.php
- /secured/phpinfo.php

De nombreuses failles sont ainsi détaillées mais s'avèrent totalement imaginaires. La lecture du rapport devient lourde et il est très difficile de trouver de bons résultats.



Rapport du scan (Acunetix)

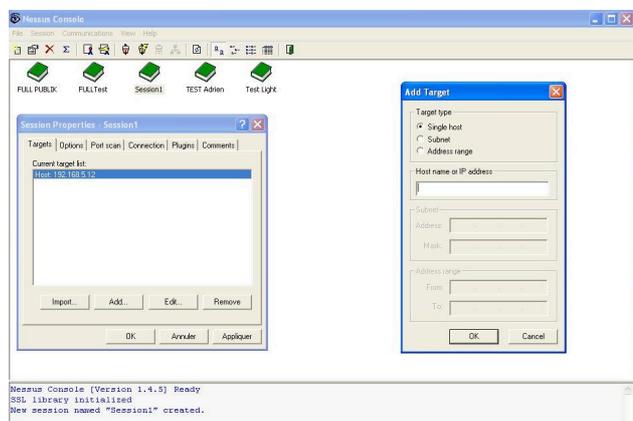
Acunetix a tout de même identifié quelques problèmes mais ces failles restent les moins intéressantes. Le répertoire “/Admin” et les fichiers “index.bak” ont été trouvés tout comme la version de PHP, du serveur Apache et la méthode TRACE également.

Ce scan fournit donc les plus mauvais résultats. Le seul point positif est l'email envoyé par les ingénieurs responsables. En effet, nous avons eu le droit d'être audités par un expert qui a effectué des tests à la main sur notre application. Les scripts dangereux permettant de lister le contenu d'un fichier et d'un dossier ont été découverts. La personne en charge de notre dossier nous l'a aimablement signalé.

NESSUS

Nessus sera notre scanner témoin. Contrairement aux services proposés par les sociétés présentées, ce logiciel est gratuit et peut s'utiliser à partir de plate-formes différentes.

En l'occurrence, nous avons installé le serveur Nessus sur un poste Unix (seule alternative) et un client sur un poste Windows de notre réseau (voir capture d'écran ci-dessous).



Interface Windows du client Nessus

Une fois que cette configuration simple et rapide est réalisée, le client Windows nous permet facilement d'entrer l'adresse IP à scanner, de sélectionner les plug-ins (failles à tester) et de lancer le scan. Un rapport est ensuite fourni et peut être converti en différents formats. Un suivi permet de connaître les différences entre deux scans successifs et l'interface reste simple et pratique.

La première analyse des résultats semble assez satisfaisante. Premier point à souligner, une liste exhaustive des ports ouverts est dressée dans la première page du rapport ce qui ne fut pas le cas pour la plupart des scans. Chaque port est bien détaillé par la suite.

De manière générale, le scanner détecte bien les différents serveurs web et ce, même sur les ports exotiques. Malheureusement, il ne se base pas sur les caractéristiques propres au serveur et ne renvoient donc pas la bonne version si la bannière a été changée (IIS 4.0 pour un Apache).

Malgré cela, les ports ouverts par défaut avec de fausses bannières (Oracle, LDAP et MySQL) ont été repérés, aucune information plus précise n'a été ajoutée mais le scanner ne se laisse pas piéger en renvoyant tout bêtement le faux service associé.

Tous les répertoires laissés (/Admin, /cgi-bin, /phpBB) ont été trouvés et les pages de cette application php ont aussi été détectées.

Network Vulnerability Assessment Report 27.04.2006

Network Vulnerability Assessment Report
Sorted by vulnerabilities

Session name: TEST Adrien Start time: 26.04.2006 17:40:15
Total records generated: 42 High severity: 0
Medium severity: 1 Informational: 41
Finish time: 26.04.2006 18:35:51
Elapsed: 0 day(s) 00:55:36

Summary of scanned hosts

Host	Holes	Warnings	Open ports	State
82.127.34.63	0	1	10	Finished

ddi-tcp-1 (8888/tcp)
Description
Port ddi-tcp-1 (8888/tcp) is open
Vulnerable hosts
82.127.34.63

ddi-tcp-2 (8889/tcp)
Description
Port ddi-tcp-2 (8889/tcp) is open
Vulnerable hosts
82.127.34.63

dnp (20000/tcp)
Description
Port dnp (20000/tcp) is open
Vulnerable hosts
82.127.34.63

Page 1

Rapport du scan (Nessus)

Aucun test applicatif n'est effectué. En effet, le scanner n'a pas détecté le couple login/mot de passe sur un de nos serveurs http. De plus les failles de sécurité de type SQL injection, directory transversal n'ont pas été testées.

En conclusion, Nessus est un bon scanner de base. Il détecte les services sur les bons ports mais se laisse facilement piéger par des bannières changées. Les failles reportées sont décrites succinctement mais les explications restent relativement perspicaces. Des liens sont proposés afin de nous donner d'avantage d'informations sur les vulnérabilités.

Enfin, peu de faux positifs ont été découverts. Nessus rapporte seulement les failles et soumet les remarques dont il est sûr. Il ne se trompe donc que très peu.

Le bilan d'XMCO

L'objectif de notre étude était de tester, dans les conditions d'un client et en toute connaissance des résultats à obtenir, plusieurs acteurs connus de marché des scans en ligne.

Conscients de l'aspect automatique des services testés, nous avons volontairement proposé des failles faciles à découvrir. Malgré cela, aucun des compétiteurs ne nous a réellement convaincus de leur efficacité.

Il est bien sûr possible de considérer que les tests ont été effectués avec les versions d'essai et d'imaginer que les résultats pourraient être nettement meilleurs avec la version payante des services.

Notre laboratoire reste ouvert aux compétiteurs pour le match retour...

Resultats globaux	Qualys	Criston	Acunetix	Nessus
Comment obtenir un test gratuit	Formulaire	Normalement par formulaire (problème de gestion).	Formulaire	/
Facilité pour demande de tests gratuits	Simple	Laborieuse (par téléphone), aucune réponse aux emails, obligation de téléphoner	Aucune réponse après le remplissage du formulaire, plusieurs emails ont permis de prendre contact	/
Rapidité du scan	10 à 15 minutes	1 journée	1 journée	Entre 30 et 60 minutes
Nombres d'IP scannées gratuitement	Possibilité d'en scanner plusieurs en remplissant à nouveau le formulaire	1	1 (avec nos trois serveurs web sur différents ports).	Illimitées
Nombres de vulnérabilités trouvées sur notre plateforme de test	14	9	95	42
Port ouverts corrects (sur 10)	5	10	/ Seules les applications webs sont scannées	10
Nombre de faux positifs	6	7	90	3
Consistance du rapport	12 pages, analyse précise des vulnérabilités trouvées	3 rapports de plusieurs pages dont un décrivant en détails les vulnérabilités avec indices, solutions ...	3 rapports d'une seule page et un rapport final de 67 pages	16 pages plus ou moins détaillées en fonction de la faille identifiée
Présentation du rapport	Page web affichée à la fin Impossibilité de le convertir Rapport attractif avec un graphique, failles classées par sévérité, explications approfondies, correction à entreprendre	Envoyé par un responsable du service en 3 parties Rapport très bien présenté et clair qui explique avec précision.	Agréable, les failles sont numérotées ce qui simplifie les recherches.	Présentation pauvre, aucune couleur ou indice ne nous permet d'identifier rapidement les failles selon leur criticité, seule une liste exhaustive nous analyse chaque port les uns après les autres
Qualité du rapport	Moyenne, bien que le rapport soit complet, le nombre de faille trouvées est bien inférieur à nos attentes.	Correct, les recherches ont été poussés	Mauvaise, trop de faux positifs ont été reportés ce qui rend la lecture des résultats extrêmement difficile.	Rapport assez simple mais complet, les failles sont regroupées par port
Prise de contact à la fin du test	Email envoyé à la fin du scan mais aucune réponse après demande d'informations Invitation à une certification technique	Un conseiller nous a contacté et nous a présenté les différents rapports. L'ingénieur avant-vente est resté attentif à nos remarques sans nous pousser à l'achat	Un email personnel nous a été envoyé avec les différents rapports	

Resultats globaux	Qualys	Criston	Acunetix	Nessus
Réactivité	Immédiate, un conseiller nous contacte par email mais ne répond pas à nos questions!	Une fois le premier contact noué par téléphone, le suivi est resté excellent	Il a fallu relancer plusieurs fois le support pour pouvoir obtenir ce test	

Plateforme Windows Serveur 2003	Qualys		Criston		Acunetix		Nessus	
Resultats techniques	Déteecté	Non-déteecté	Déteecté	Non-déteecté	Déteecté	Non-déteecté	Déteecté	Non-déteecté
Système d'exploitation		X	X			X		X
Serveur IIS 6.0 sur port 8888 (SSL) et 8889		X	X		X		X	
Serveur Apache 1.3.33 sans bannière sur port 80		X	X	Version non-précisée	X		X	Version non-précisée
Répertoire /Admin/		X		X	X		X	
Fichier passwd.txt		X		X		X		X
Directory listing à la racine	X			X	X			X
formulaire login/password	X			X		X		X
Injection SQL sur le formulaire ("/")		X	X			X		X
Faible de directory transversal sur la variable "file"		X	X	Faible decté mais pas exploitée		X		X
Fichiers index.php~/index.bak/index.old		X		X	X (index.bak)			X
TRACE ON -> XST sur port 80	X		X		X		X	
PHPBB 2.18		X		X		X	X	
Pages PHPBB trouvées		X		Noms des pages non trouvées		X	X (toutes)	
Nombre de Ports ouverts (sur 3)	1	2	3			2/3	3	0
Bilan sur 16 tests	4	12	10	7	7	7	9	7

Apache 2.0.45	Qualys		Criston		Acunetix		Nessus	
	Détecté	Non-détecté	Détecté	Non-détecté	Détecté	Non-détecté	Détecté	Non-détecté
Système d'exploitation		X		X		X		X
Sendmail v8.13.4 sur port 25		X	Serveur SMTP			X		Sendmail détecté en 7.0.1
VULN : Sendmail Signal Handling Memory Corruption Vulnerability		X		X		X		X
OpenSSH v3.8.1p1 sur port TCP 20000		X	X			X	X	Version OpenSSH
Apache 2.0.45 sur port TCP 23 avec bannière IIS 4.0	X	Serveur web non détecté		Serveur web détecté en IIS 4.0		Serveur web détecté en IIS 4.0		Serveur web détecté en IIS 4.0
/cgi-bin : 2 scripts tres dangereux		X		X		X	Répertoire trouvé	
/manual		X		X		X		X
VULN : Apache Vulnerabilities in Various Modules		X		X		X		X
TRACE ON -> XST sur port 23	X		X		X		X	
Erreur 404 => 200 OK		X		X		X	X	
Faux MySQL sur le port 1433		X	X			X	X	
Faux LDAP sur port 389		X	X			X	X	
Faux Oracle sur les ports 1521 et 1526		X	X			X	X	
Faux positifs	6		7		90		3	
Nombre de Ports ouverts (sur 7)	1	6	7	0	1/1		7	0
Bilan sur 20 tests	3	17	13	7	2	18	14	6

4. ATTAQUES MAJEURES :

TOP 5 DU MOIS D'AVRIL :

Le mois d'Avril a été marqué par des failles de sécurité au sein des logiciels des plus grands acteurs du marché.

Microsoft, Oracle, Mozilla et Apple ont été touchés. Microsoft a publié plusieurs vulnérabilités dont les plus critiques affectent Internet Explorer et Windows. Oracle a également publié un bulletin afin de prévenir de la future correction d'une dizaine de failles dont la plus sévère fut rapidement suivie par un exploit. Enfin Apple a été également victime de plusieurs failles, preuves de concept à l'appui.

XMCO | Partners



MS06-013

Mise à jour de sécurité cumulative pour Internet Explorer ("Create TextRange()")

Microsoft a identifié et corrigé de nombreuses failles (dont le problème lié à la fonction « CreateTextRange() ») qui affectent son navigateur web Internet Explorer. De nombreuses preuves de concept ont été publiées durant le mois de mars. La société de Bill Gates se devait de réagir efficacement. Microsoft a répondu en mettant à disposition des internautes un correctif cumulatif qui remplace les bulletins MS05-054 et MS06-004 pour la majorité des plateformes Windows.

Cette mise à jour de sécurité remplace également le correctif cumulatif pour Internet Explorer publié pour Windows XP Service Pack 2 et Windows Server 2003 Service Pack 1 le 28 février 2006.

Les vulnérabilités concernent essentiellement des corruptions de mémoire via la création de pages web spécialement forgées. En effet, Microsoft a publié au début du mois, une alerte KB (« Vulnerability in the way HTML Objects Handle Unexpected Method Calls Could Allow Remote Code Execution »). Elle pévient les internautes des diverses actions malveillantes possibles via des sites web pirates.

L'exploitation de ces failles reste relativement simple. L'attaquant doit seulement inciter un utilisateur qui possède un navigateur vulnérable, à visiter un site web malicieux. Un lien dans un email serait suffisant. L'intervention de l'utilisateur reste indispensable. En héritant des droits que possède la victime sur la machine cible, le pirate peut prendre le contrôle total de la machine cible.

De nombreux exploits ont été publiés et sont disponibles sur les sites spécialisés. Certains sites Internet utilisent déjà ces exploits afin de compromettre le système des internautes les moins attentifs.

Une première preuve de concept a été dévoilée et analysée dans « Actu Sécurité » n°2. Voici un second exploit qui utilise une faille de sécurité au sein du gestionnaire d'événements d'une page HTML.

En effet, les tags possédant plusieurs événements tels que : onhelp, onclick, ondblclick, onkeyup, onkeydown, onkeypress... ne sont pas correctement traités. La mémoire peut être corrompue et permettre l'exécution de code.

Une preuve de concept a été publiée et provoque ainsi un déni de service. Cependant, elle pourrait être modifiée à des fins malveillantes comme l'exécution de code.

Voici le code de cet exploit. Il se compose simplement des balises suivantes, ainsi que 10005 fois l'évènement "onclick=bork".

```
<html>
<body>
<img
src=http://lcamtuf.coredump.cx/photo/current/m2A.jpg
<foo onclick=bork >
<p>Hello cruel world.
```

Preuve de concept pour Internet Explorer

Programmes vulnérables :

- ◆ Internet Explorer 5.01
- ◆ Internet Explorer 6.0

Criticité : Elevée

Référence Xmc0 : n° 1142413618

MS06-015**Execution de code a distance avec l'explorateur Windows**

Ce correctif publié par Microsoft le 12 avril 2006 est le seul de la série d'Avril qui aura posé quelques soucis aux utilisateurs d'équipements Hewlett Packard.

Microsoft a corrigé une faille de sécurité critique de son système d'exploitation Windows. Une imperfection de la gestion des objets COM permettait à un attaquant distant d'exécuter des commandes arbitraires sur un système vulnérable.

L'exploitation de cette vulnérabilité nécessitait que la victime visite une page Web malicieuse hébergeant des objets COM judicieusement contrefaits. L'ouverture de cette page forçait une connexion à un serveur de fichiers sous le contrôle du pirate afin d'exécuter des commandes arbitraires sur le système de la victime.

Si l'utilisateur abusé est administrateur de son poste, la prise de contrôle totale est envisageable. Notons que l'exploitation de cette faille était envisageable uniquement si le poste victime était en mesure d'initier des connexions netbios/CIFS vers le serveur pirate.

Le correctif KB908531 corrige cette vulnérabilité en ajoutant un fichier, « Verclsid.exe ». Cet exécutable est en charge de valider tous les objets COM avant qu'ils soient instanciés par l'Explorateur Windows. De plus, cette mise à jour remplace les mises à jour MS05-016 et MS05-008.

Malheureusement, peu de temps après la parution de ce correctif, de nombreux internautes équipés de produits HP dont notamment le logiciel « Share-to-Web », ont été touchés par un problème de gestion des fichiers Office provenant des dossiers « Mes Documents » et « Mes Images ». Une nouvelle mise à jour fut publiée deux semaines plus tard (le 25 avril). Elle corrige le problème lié au fichier « Verclsid.exe ».

Aucun programme malicieux qui exploite cette faille de sécurité n'a été publié.

Programmes vulnérables :

- ◆ Microsoft Windows 2000 SP 4
- ◆ Microsoft Windows XP SP 1 / 2
- ◆ Microsoft Windows XP Professionnel Edition x64
- ◆ Microsoft Windows Server 2003 / SP 1
- ◆ Microsoft Windows Server 2003 / SP1 (Itanium)
- ◆ Microsoft Windows Server 2003 Editions x64

Criticité : Elevée

Référence Xmc0 : n° 1144831010

**Alerte Oracle 2006 Alerte 74****Publication d'un correctif cumulatif**

Oracle publie son deuxième bulletin trimestriel de l'année 2006 qui présente des failles importantes au sein de plusieurs de ses produits.

Pour les produits de type base de données, les failles les plus importantes permettent à un utilisateur qui possède un compte sur la base Oracle ou sur le système qui héberge la base, de prendre le contrôle total ou partiel de la base de données.

Pour les produits de type serveur d'applications, les failles les plus importantes permettent à un utilisateur distant et anonyme d'effectuer des malversations importantes mais non décrites par Oracle.

La majorité des failles corrigées par ce correctif cumulatif n'ont pas été décrites précisément. En effet, la société ayant découvert ces failles (NGS Software) possède un accord avec Oracle et ne publiera donc les détails d'exploitation qu'en juillet 2006.

Peu d'informations ont été communiquées. Seule une courte description a été publiée. Elle relate qu'un utilisateur qui ne possède qu'un accès en lecture sur la base peut, en exploitant une faille non décrite d'une vue Oracle, prendre le contrôle en écriture de la base.

Oracle publie plusieurs matrices de risque pour ses différentes catégories de produits. Ces matrices décrivent les droits nécessaires à l'exploitation des failles et les impacts possibles.

Programmes vulnérables :

- ◆ Oracle Database 10g Release 2, versions 10.2.0.1, 10.2.0.2
- ◆ Oracle Database 10g Release 1, versions 10.1.0.4, 10.1.0.5
- ◆ Oracle9i Database Release 2, versions 9.2.0.6, 9.2.0.7
- ◆ Oracle8i Database Release 3, version 8.1.7.4
- ◆ Oracle Application Server, Collaboration et E-Business Suite versions 9,10g, 11 et 11i
- ◆ Oracle PeopleSoft Enterprise Tools, versions 8.4x

Criticité : Elevée

Référence Xmc0 : n° 1145433011

ORACLE
FRANCE

Mozilla

Nombreuses vulnérabilités dans Mozilla Suite, Firefox, Thunderbird et SeaMonkey

Plusieurs vulnérabilités ont été publiées pour les logiciels Mozilla Suite, Mozilla Firefox, Thunderbird et SeaMonkey. Un attaquant pouvait exploiter ces failles afin de compromettre un système vulnérable, de contourner des mesures de sécurité ou d'obtenir des informations sensibles.

Ces failles résultent d'erreurs présentes aux niveaux de certaines fonctions et méthodes internes aux logiciels Mozilla, ainsi que dans le moteur JavaScript et CSS.

Les problèmes concernant le moteur JavaScript et CSS résultent de débordements de tampons. L'exploitation d'une partie des erreurs, au sein de fonctions et méthodes internes, permettrait à une personne malveillante d'exécuter des commandes arbitraires ainsi que d'installer des logiciels de son choix.

La seconde partie des erreurs de ces fonctions autoriserait un attaquant à effectuer des attaques de type Cross Site Scripting afin de récupérer des informations sensibles.

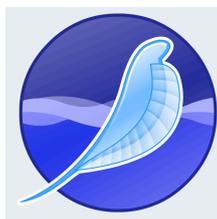
La dernière erreur permettrait à une personne mal intentionnée de spoofer un site web tout en obtenant les indications de sécurité de Firefox (icône, cadenas, nom du site dans l'URL, couleur de fond jaune).

Programmes vulnérables :

- ◆ Firefox 1.5.0.2
- ◆ Thunderbird 1.5
- ◆ Seamonkey 1.0

Criticité : Elevée

Référence Xmco : n° 1145457926



Apple

Plusieurs vulnérabilités dans Safari, Finder, Quicktime et Preview

Après un mois assez calme, la fin du mois d'Avril s'avère mouvementée pour Apple. En effet, 6 failles critiques viennent d'être publiées. Les développeurs s'activent afin de corriger ses bugs et garder leur principal avantage sur Microsoft, à savoir, leur réactivité.

Ces différentes failles de sécurité affectent plusieurs composants dont notamment le navigateur Safari, les outils Preview, Quicktime et Finder.

Les problèmes restent les mêmes. Par l'intermédiaire de fichiers malicieux de différentes extensions (« tiff », « gif », « bmp », archives et fichiers HTML), le pirate serait en mesure de causer un déni de service voir de compromettre un système vulnérable.

L'exploitation de ces failles serait réalisée par l'hébergement de fichiers spécialement conçus. Plusieurs preuves de concept ont été publiées dans la foulée.

Pour le moment, l'exploit le plus évolué permettrait d'altérer le bon fonctionnement d'un système obligeant un redémarrage de la machine cible.

Nous vous présentons ci-dessous une page HTML qui possède le paramètre "ROWSPAN" avec une valeur excessivement longue :

```
<html>
<body>
<img
src=http://lcamtuf.coredump.cx/photo/current/m2A.jpg>
<foo onclick=bork >
<p>Hello cruel world.
```

Code d'une page HTML malicieuse exploitant une faille de Safari



Programmes vulnérables :

- ◆ Safari 1.3.1 (312.3.1) sous Mac OS X 10.3.9
- ◆ Safari 2.0.3 (417.9.2) sous Mac OS X 10.4.6
- ◆ Preview, Finder, QuickTime pour Mac OS X 10.4.6 ou inférieur

Criticité : Elevée

Référence Xmco : n° 1142413618

5. OUTILS LIBRES :

FOCUS SUR 5 PRODUITS LIBRES

Chaque mois, nous vous présenterons les outils libres qui nous paraissent indispensables. Les logiciels abordés sont variés : utilitaires de sécurité et autres programmes nécessaires au sein d'une entreprise.

Pour ce troisième numéro, nous avons choisi d'analyser une distribution Linux, des logiciels Internet, un client/serveur ssh et un proxy:

- Ubuntu : distribution Linux "user-friendly"
- Postfix: Serveur de messagerie
- Openssh : Serveur et client ssh
- Filezilla : Outil de transfert de fichiers
- Squid : proxy-cache Internet, adapté aux besoins d'une entreprise

Vous trouverez à la fin de cette section un tableau récapitulatif des versions de tous les logiciels présentés lors des précédents numéros d' « Actu Sécurité ».

XMCO | Partners



Ubuntu

Distribution Linux

Version actuelle

Ubuntu 5.10 Breezy Badger

Utilité



Type

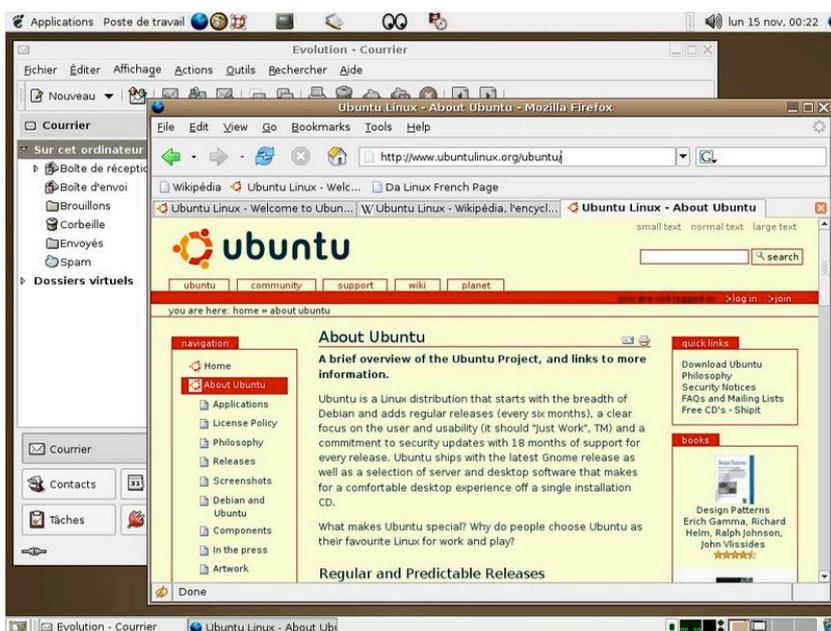
Système d'exploitation

Description

Ubuntu est une distribution stable et conviviale. Basée sur une distribution Debian, Ubuntu a été conçue afin de proposer une bonne alternative aux postes de travail. Simple et efficace, elle peut être utilisée par des débutants comme par les experts et, contrairement à d'autres, cette distribution s'installe rapidement et simplement.

L'environnement graphique choisi est GNOME. Les adeptes du bureau KDE, peuvent se tourner vers le petit frère Kubuntu.

Capture d'écran



Téléchargement

Ubuntu proposée en deux versions : la stable nommée Ubuntu 5.10 Breezy Badger et la prochaine version instable baptisée Ubuntu 6.06 Dapper Drake.

Les deux versions sont disponibles pour les architectures x86, AMD64 et PowerPC en ISO ou en « LiveCD » à l'adresse suivante :

<http://doc.ubuntu-fr.org/installation>

Sécurité de l'outil

Basée sur une distribution Debian, Ubuntu souffre de nombreuses failles vu le nombre important de paquets (plus de 15000) pris en compte.

L'avantage majeur est la faculté de cette distribution à pouvoir télécharger le nouveau paquet mis à jour avec la commande apt-get :

<http://secunia.com/product/6606/>

Avis XMCO

Ubuntu est une très bonne distribution stable et pratique. Elle se rapproche de Windows par son interface simple et conviviale. Cette distribution gratuite reste donc un très bon choix pour les postes de travail.

Postfix

Serveur de messagerie électronique

Version actuelle

Postfix 2.2

Utilité



Type

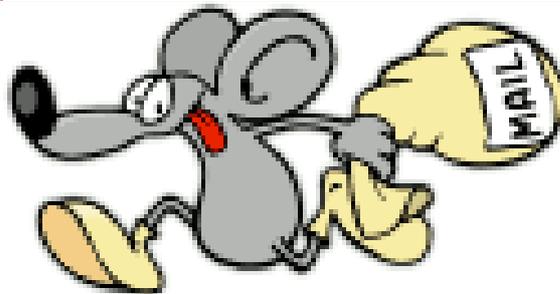
Serveur de mails

Description

Postfix est un gestionnaire de mails efficace, capable de traiter de gros flux de messages. Cet outil est le plus souvent utilisé en serveur de messagerie et reste facile à administrer (via une interface graphique Webmin par exemple). Postfix peut aussi bien être utilisé dans le monde professionnel que chez des particuliers.

Il est le serveur de courriel par défaut dans Mac OS X.

Capture d'écran



POSTFIX

Téléchargement

Postfix est disponible sur toutes les distributions linux. Vous trouverez les liens des diverses distributions à l'adresse suivante :

<http://www.postfix.org/packages.html>

Sécurité de l'outil

Ce logiciel est très peu concerné par des failles de sécurité. Une seul problème (déni de service), a été publié en 2003. Aucune vulnérabilité n'a été publiée pour l'année 2006.

Avis XMCO

Postfix est une bonne alternative à Sendmail, largement utilisé dans le monde Linux. Plus facile à administrer et à sécuriser, ce logiciel reste la référence en terme de serveur de messagerie.

OpenSSH

Serveur et Client SSH

Version actuelle

OpenSSH 4.3 depuis le 1er février 2006

Utilité



Type

Accès sécurisée à une machine distante, tunneling ...

Description

OpenSSH est la référence des accès à distance sécurisés à travers le monde. C'est un programme (Openssh) qui utilise le protocole de communication (SSH). Cet utilitaire est un outil indispensable en entreprise. Il permet de se connecter de manière sécurisée à des machines distantes. L'authentification des machines se basent sur un algorithme sûr (RSA) utilisant la cryptographie asymétrique (clef publique/ clef privée) avec un échange préalable de ces clefs avant l'envoi de données. SSH a été conçu afin de remplacer rlogin, telnet et rsh et utilise le port 22. Il est particulièrement utilisé afin de prendre le contrôle d'une machine à distance (en ligne de commande). Openssh permet également de créer des tunnels chiffrés pour tout protocole applicatif.

Capture d'écran

```

Terminal
File Edit View Terminal Go Help
[user@host user]$ ssh -l bbs flux.termisoc.org
The authenticity of host 'flux.termisoc.org (141.163.200.2)' can't be established.
RSA key fingerprint is 9e:27:cd:68:2d:6d:90:d5:88:9b:b0:36:75:f2:c0:f5.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'flux.termisoc.org' (RSA) to the list of known hosts.

Welcome to Flux BBS

Old users:
o Log on here with your userid and password - but then you knew that already.

New users:
o Log in as 'guest' with the password 'guest' to look around, or..
o Create your own user by logging on as 'new'. NOTE: You *must* have a
  valid email address, or you won't be able to receive your startup
  password.

Any problems, mail bbsadm@termisoc.org
userid ('new' for new user): 

```

Téléchargement

OpenSSH 4.3p2 est disponible sur toutes les plateformes à l'adresse suivante :

<http://www.openssh.org/fr/portable.html>

Sécurité de l'outil

Openssh permet l'accès total à une machine distante, la compromission d'un tel logiciel est donc critique. De plus, étant utilisé par des millions d'utilisateurs chaque jour, les pirates cherchent continuellement des failles de sécurité au sein de ce logiciel. Le nombre de vulnérabilités reste tout de même raisonnable, vous trouverez les différentes failles qui affectent ce logiciel :

<http://secunia.com/product/5653/>

Avis XMCO

Ce logiciel reste incontournable et indispensable en entreprise. Nous vous conseillons d'utiliser ce logiciel pour tous vos accès à distance et l'administration de vos serveurs UNIX.

FileZilla

Outil de transfert de fichiers

Version actuelle

FileZilla-2.2.20

Utilité



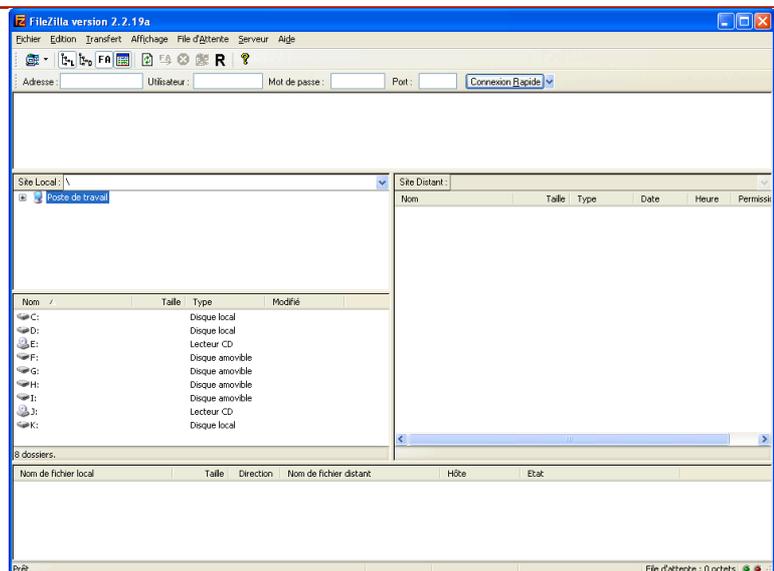
Type

Client FTP, SFTP, SCP pour système UNIX et Windows

Description

FileZilla est un client FTP, SFTP et SCP. Il permet de se connecter rapidement à un serveur afin d'envoyer ou de télécharger des fichiers. Cet outil dispose de nombreuses options comme la compression ou la reprise sur erreur. Il supporte, bien entendu, le mode passif pour les serveurs FTP. Enfin, cet utilitaire libre et gratuit dispose d'une version serveur permettant de mettre en place aisément un serveur FTP ou SFTP.

Capture d'écran



Téléchargement

Version 2.2.22 disponible à l'adresse suivante:

http://sourceforge.net/project/showfiles.php?group_id=21558

Sécurité de l'outil

Peu de failles ont été rapportées. Ces dernières ont été rapidement corrigées grâce à la participation de la communauté du libre :

<http://secunia.com/product/2925/>

Avis XMCO

FileZilla est un outil gratuit très efficace et polyvalent. Il est l'outil indispensable pour gérer tous vos transferts de fichiers.

Squid

Proxy-cache Internet

Version actuelle

Squid-2.5.STABLE13

Utilité



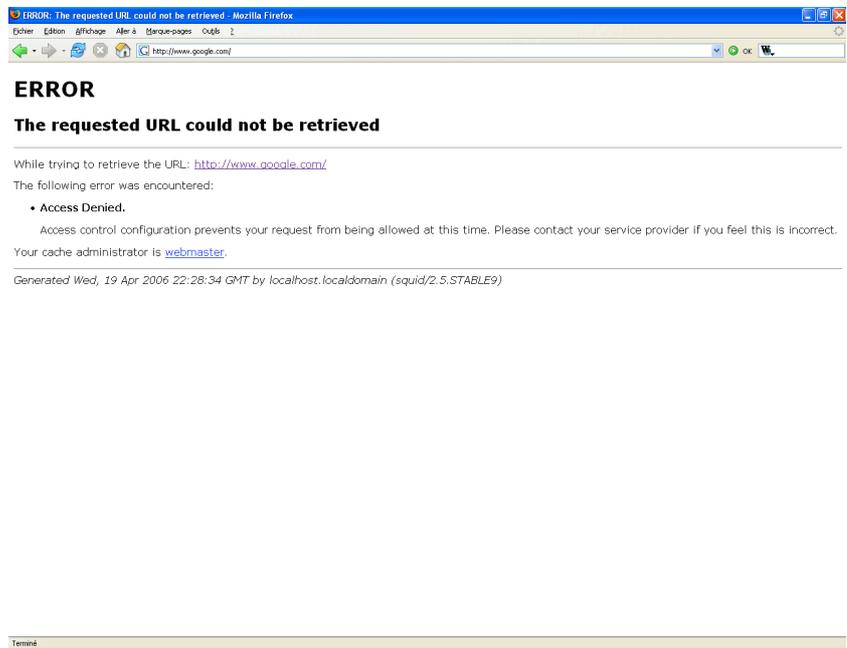
Type

Proxy et cache Internet pour système UNIX

Description

Squid est un proxy-cache Internet simple et efficace. Cet outil permet de filtrer les flux Internet au niveau applicatif et, de servir, par la même occasion, de cache web. Ainsi, tous les utilisateurs ne sont pas connectés directement à Internet. Il dispose de surcroît d'une documentation très riche ainsi que de nombreux tutoriaux. Celui-ci est bien entendu libre et gratuit mais destiné uniquement aux systèmes Unix.

Capture d'écran



Téléchargement

Squid pour LINUX :

<http://www.squid-cache.org/Mirrors/http-mirrors.html>

Sécurité de l'outil

Quelques failles ont été rapportées mais ont été rapidement corrigées grâce à la participation de la communauté du libre :

<http://secunia.com/product/310/>

Avis XMCO

Squid est un outil libre exploitable très rapidement mais peut aussi facilement s'intégrer à une infrastructure complexe. Il en demeure un outil efficace et implémenté dans de nombreuses entreprises. Il existe de plus de nombreux plugins permettant de le coupler à des antivirus ou logiciels de filtrages, rendant cet outil très complet et évolutif.

Nous vous conseillons d'associer Squid avec le logiciel DansGuardian et ClamAV. Ce trio permet d'autoriser et de scanner certains types de fichiers et d'avoir une bonne solution de filtrage.

Suivi des versions

Version actuelle des outils libres présentés dans les numéros précédents.

Nom	Dernière version	Date	Lien
Debian Sarge	Version stable 3.1		http://www.debian.org/CD/netinst/
Snort	2.4.4	08/03/2006	http://www.snort.org/dl/
MySQL	5.0.21		http://dev.mysql.com/downloads/mysql/5.0.html
	5.1.9-Bêta		http://dev.mysql.com/downloads/mysql/5.1.html
Apache	2.2.0	05/12/2005	http://www.apachefrance.com/Telechargement/4/
	1.3.34	16/10/2005	http://www.apachefrance.com/Telechargement/4/
Nmap	4.03	01/04/2005	http://www.insecure.org/nmap/download.html
Firefox	1.5.3	04/2006	http://www.mozilla-europe.org/fr/products/firefox/
Thunderbird	1.5.0.2	04/2006	http://www.mozilla-europe.org/fr/products/thunderbird/
Spamassassin	3.1.1		http://spamassassin.apache.org/downloads.cgi?update=200603111700
Putty	0.58		http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
ClamAV	0.88.2.1	05/2006	http://www.clamav.net/stable.php#pagestart
			http://www.clamwin.com/content/view/18/46/