L'Actu Sécurité n°5

xmco Partners

PLAN

"Des vacances Bluetooth pour un pied toujours au bureau..."

Des vacances bluetooth pour un pieds toujours au bureau...

Le troisième millénaire annonce une société de loisirs : RTT, congés payés, voyages discounts, etc.
Enfin pas vraiment pour tout le monde : pour une fois, la technologie nous dessert : heureux sont les chanceux qui ne reçoivent pas leurs mails sur un smartphone, qui ne sont même pas joignables...
Il y a 10 ans seulement, le mot vacances signifiait coupure totale "ok, je regarderai à mon retour..", sans aucun remords. De toute façon, quand on est couper du monde...
Aujourd'hui, la débauche de moyens technologiques nous permet de toujours rester connecté au bureau. Finalement , c'est un peu comme s'il y avait plus de vacances, mais moins de temps libre...

Les technologies n'ont pas changé le fil du temps, ni la vitesse à laquelle il passe, mais une sorte de servitude s'est un peu installée, de sorte qu'aujourd'hui, beaucoup de personnes ne souhaitent plus être "déconnectée". Mais déconnecté de quoi exactement ? Et puis, est-ce que le rôle des vacances n'est pas justement de s'éloigner, de prendre l'air, de couper tout lien avec le quotidien pour regénérer les énergies de chacun ?

Malheureusement, la tentation est grande : de plus en plus d'hôtels, de locations et même de restaurants proposent un accès internet gratuit, de plus en plus d'outils légers et puissants permettent de conserver ce lien.

En attendant, vous trouverez dans ce numéro "spécial été" de nombreuses informations sur le nomadisme, histoire, au minimum, que le lien reste sécurisé...

Bonne "vacances" à tous ceux qui en prennent et bon courage pour tous les autres !

Marc Behar

2. NOUVELLE TENDANCE

LA SECURITE DES POSTES NOMADES

L'évolution des technologies et des besoins des entreprises a conduit à l'essor de la mobilité. Pour prendre un exemple concret, il est devenu naturel, mais surtout indispensable, de pouvoir accéder à sa messagerie professionnelle ainsi qu'à toutes les applications essentielles peu importe le lieu où l'on se trouve.
Ainsi, les ordinateurs portables sont devenus un des points critiques de la gestion du parc informatique. Ceux-ci remplacent de plus en plus les stations de travail pour une plus grande flexibilité.
Cette nouvelle tendance bouscule les administrateurs réseau : la mobilité nécessite la révision de toutes les politiques de gestion de l'entreprise puisque, là où la sécurité consistait à protéger un château fort replié sur lui-même, l'enjeu consiste désormais à sécuriser un monde communicatif et ouvert à l'instar d'un aéroport.

XMCO | Partners

Les principaux enjeux et faiblesses du nomadisme

La gestion de l'ingérable

Amener de la mobilité au sein d'un réseau n'est pas aisé. Cette démarche doit être réfléchie car elle amène de grands bouleversements au sein de l'organisation informatique.

Le principal enjeu est d'assurer les mêmes services qu'aux utilisateurs du réseau interne sans maîtrise de l'équipement distant. Les buts recherchés sont la transparence et la sécurité de cette solution.

Ne rêvons pas, comme tout projet informatique, il n'y a pas de recette miracle et nous devons, une fois de plus, déterminer un compromis entre les services désirés et le niveau de sécurité requis.

Une erreur fréquente

Les technologies nécessaires au bon développement du nomadisme sont accessibles à tous. Le principal vecteur d'accès au réseau d'une entreprise est bien entendu Internet. En effet, la baisse des coûts et l'augmentation constante des débits en font un support incontournable.

De nombreux outils cryptographiques permettent de nous assurer d'une authentification forte des utilisateurs distants ainsi que de la confidentialité et de l'intégrité des échanges.

Si la couche réseau ne doit pas être sous-estimée, elle ne constitue pas pour autant le point critique de la mobilité. En effet, celle-ci étant sous le contrôle total des administrateurs, une politique interne stricte et efficace fournit une infrastructure de base sûre. Les technologies étant, pour la plupart du temps, parfaitement maîtrisées, il est désormais rare de constater des attaques par ce biais.

La source des problèmes

Le principal risque d'intrusion au sein d'une infrastructure nomade provient des postes mobiles eux-mêmes car on les autorise à entrer au sein du « bunker ». Ces équipements échappent en partie aux administrateurs car ils ne sont pas en permanence connectés au réseau de l'entreprise. Ceux-ci sont connectés dans des lieux dont les politiques et les besoins de sécurité sont hétérogènes.

Le risque de compromission d'un équipement nomade provient principalement de ses applications. En effet, les failles applicatives sont désormais les principales sources d'infections et de piratages. Même si tous les échanges avec le site de l'entreprise sont sécurisés, un poste client infecté par un virus, un cheval de Troie ou encore un keylogger et autre malware, compromettent toutes les mesures de sécurité mises en place en amont.

Un pirate s'attaquera plus facilement à un ordinateur isolé, bourré d'applications, de données sensibles, plutôt qu'à une infrastructure complexe, totalement sécurisée et administrée par des experts en sécurité. Le point critique des projets de mobilités est donc la protection du poste nomade.

Les compromis de l'accès à distance

Le besoin d'accessibilité aux services

Un projet de mobilité est bien souvent mis en place dans le but d'augmenter la productivité. Pouvoir récupérer des documents internes, des messages ou accéder à des applications critiques sans devoir se déplacer au sein des locaux est devenu un atout majeur. Cependant, afin d'assurer une bonne qualité de service pour l'accès distant, il est nécessaire de faire quelques sacrifices du point de vue de la sécurité. En effet, le besoin de l'employé nécessite la possibilité d'utiliser les applications ou les données immédiatement lors de sa connexion. L'infrastructure est donc obligée d'accorder une confiance élevée au poste nomade afin de lui fournir le service dans des délais acceptables.

La sécurité d'une telle solution repose uniquement sur celle de l'équipement distant. Des restrictions importantes doivent être imposées afin de garantir l'intégrité et la légitimité du poste nomade.

Le besoin de protection du réseau local de l'entreprise

Dans certains cas, les utilisateurs peuvent nécessiter un accès distant sans aucune criticité sur le service désiré. Par exemple, certaines personnes doivent seulement déposer un fichier de façon hebdomadaire ou mensuelle.

Les politiques de sécurité mises en place imposeront alors des vérifications drastiques sur les connexions distantes afin de préserver le réseau local.

Avant toute chose, un ordinateur distant ne doit pas être considérer comme une simple machine de plus à gérer. Celui-ci n'étant plus sous les protections physiques et logiques de l'entreprise, de nouvelles politiques, strictes et restrictives, doivent être appliquées.

Une hiérarchisation du réseau interne doit donc être mise en place. Ainsi, une machine distante ne doit pas se retrouver au sein du même sous-réseau que les stations de travail locales. La mise en place d'une zone de quarantaine complète parfaitement le tableau; ainsi tout poste nomade y accédera en premier lieu afin de vérifier que son système est sain et à jour avant d'être redirigé vers le réseau souhaité.

Dans ce cas, la gestion de la sécurité est centralisée et donc facilement administrable. L'isolation du réseau local permet de prévenir toute infection due à un accès distant, tandis que la zone de quarantaine assure la mise à jour des postes nomades.

Les mesures de protections basiques du poste nomade

La protection des applications

Le premier vecteur de vulnérabilités provient des applications. Celles-ci doivent être patchées autant que possible. Il n'est pas inutile de rappeler que l'antivirus doit aussi disposer des dernières signatures et qu'un pare-feu doit être présent et activé.

L'utilisateur étant, théoriquement, joignable aisément, celui-ci doit être prévenu à l'avance (par email, téléphone, sms, …) des lancements des mises à jour afin de pouvoir connecter sa machine à temps. Enfin, une vérification systématique des correctifs installés sur tous les postes nomades, lors de leur connexion à l'intranet, doit être effectuée, pour que, le cas échéant, les machines vulnérables soient isolées et puissent recevoir les derniers correctifs.

La protection de l'équipement

Afin de consolider les applications, une politique d'accès doit être instaurée. La sécurité des mots de passe est un problème qui remonte à plus de 10 ans et qui reste d'actualité. Un système « blindé » et à jour ne sert à rien si le mot de passe administratif est trivial.

L'apparition des « tokens » ou autres cartes à puces intégrant des certificats aide à résoudre ce problème ; faut-il encore ne pas les perdre ou se les faire voler. Les chercheurs ont, par la suite, inventé la biométrie, technologie de science fiction disposant de ses propres limites. En effet, une authentification basée sur la reconnaissance d'une empreinte digitale devient inutilisable par une personne venant d'avoir un accident grave. Une autre contrainte, intolérable en matière de sécurité, provient de la révocation. Que se passerait il si une personne se faisait usurper son empreinte biométrique ? Avec l'utilisation d'un certificat, il suffirait de le révoquer et d'en générer un nouveau, mais avec l'empreinte génétique, quel recours avons-nous ?

La biométrie est donc un outil qui ne devra pas être introduit à la légère au sein de projets sensibles.

La communication de l'équipement

Les ordinateurs intègrent de plus en plus de technologies afin de pouvoir connecter un maximum d'équipements. Par exemple, certains utilisateurs voudront utiliser leur téléphone portable, en bluetooth pour remplacer la souris, afin d'assurer une présentation alors que d'autres utiliseront l'infrarouge pour synchroniser leur PDA. Mais quel est le lien avec la sécurité ?

Ces nouvelles technologies apparaissent sans cesse, mise à part la fantaisie de certains utilisateurs, celles-ci ne sont pas forcément indispensables. Devant la publication des faiblesses de certains protocoles comme le bluetooth[1] (voir le Schéma 1), il est important d'activer ou d'implémenter uniquement ce dont l'usager a besoin. Prenons comme exemple concret la synchronisation d'un PDA. Celle-ci peut s'effectuer via un câble console plutôt que par toute autre technologie sans-fil non maîtrisable.

Schéma 1 : Déni de Service sur un téléphone via le protocole Bluetooth.

Le besoin de confidentialité des données

Les entreprises qui redoutent l'espionnage industriel font face à un autre problème, : le stockage des données. En effet, les informations stockées ne sont plus confinées au sein des murs de la société. La confidentialité et la sauvegarde des documents présents au sein de la machine sont donc uniquement assurées par l'ordinateur et son utilisateur.

Dans ce cas concret, il est important de sensibiliser, de former et de responsabiliser l'utilisateur face aux menaces toujours plus nombreuses. Par exemple, il est plus facile de dérober un ordinateur portable dans une chambre d'hôtel plutôt que d'accéder aux données d'un serveur au sein des locaux de l'entreprise. Cependant, cette solution souffre de la probabilité d'une erreur humaine et de la réelle compréhension des risques par l'intéressé. En effet, il est fort probable que l'utilisateur, qui souhaite utiliser l'équipement pour un usage personnel, désactive des mesures de sécurités (pare-feu, antivirus, …). Ceci permet alors à un pirate d'accéder à distance aux données de la machine.

Afin de limiter ce risque, il est indispensable de restreindre, au strict maximum, les privilèges des utilisateurs des postes mobiles.

D'autre part, la protection des données sensibles contre une attaque physique (vol de matériel), nécessite de chiffrer leur stockage. Plusieurs possibilités s'offrent alors à l'usager : chiffrer un dossier, une partition ou la totalité du disque dur. De nombreux outils payants ou « open source » sont disponibles (SafeBoot[2], TrueCrypt[3]). Une fois encore, dans le cas d'un chiffrement partiel, l'utilisateur doit être informé de la méthode à suivre afin de protéger ses documents car il serait dommage de posséder un dossier chiffré sans aucun fichier.

Enfin, le dernier point essentiel concerne la sauvegarde des données. En effet, au sein d'une entreprise, de nombreux mécanismes sont implémentés pour prévenir la perte d'informations. Des scripts de backup peuvent être exécutés lorsqu'une machine nomade se connecte à l'intranet. Lors de longs déplacements sans aucune possibilité de connexions distantes, l'utilisateur devient responsable de toutes les données sensibles. Il lui incombe donc de garder des copies des fichiers sensibles sur des éléments de stockage externes. Enfin, ces derniers assurent la confidentialité des informations sauvegardées et le propriétaire du poste nomade doit nécessairement posséder les outils et les connaissances adéquats à ce besoin.

La protection des postes nomades avec SafeBoot

Afin de limiter ce risque, il est indispensable de restreindre au strict minimum les privilèges des utilisateurs des postes mobiles.

Safeboot est une solution complète de type « client-serveur » qui permet d'assurer la confidentialité des données de nombreux équipements (PC, Tablet PC, PDA). De plus Safeboot apporte aussi une protection supplémentaire au système d'exploitation à l'aide de nombreuses fonctionnalités.

Cette solution entièrement paramétrable, repose sur des algorithmes de chiffrement sûrs (par défaut, FIPS AES). Ceci protège la machine dès son démarrage. Le chiffrement et le déchiffrement des données sont effectués à la olée et de façon transparente pour l'utilisateur final car sans aucune perte de performances.

Le serveur d'application permet la centralisation de la gestion des équipements et la création de règles par machines,

utilisateurs ou groupes (Voir le Schéma 2). De nombreux lecteurs de cartes à puces sont supportés ainsi tout comme la fonctionnalité de SSO (Single Sign On). L'interface d'administration permet, enfin, de sélectionner les ports et les applications autorisés sur chaque périphérique.

Un des grands avantages de SafeBoot concerne la partie d'intégration au réseau de l'entreprise. Conscient que la principale occupation des administrateurs est l'interopérabilité des différentes solutions de la société, toutes les applications de l'éditeur sont compatibles avec de nombreuses PKI et supportent la synchronisation avec les politiques d'un réseau Active Directory.

SafeBoot propose une gamme complète de logiciels qui facilitent le développement d'un projet de nomadisme et qui garantissent la sécurité du point critique : le poste distant.

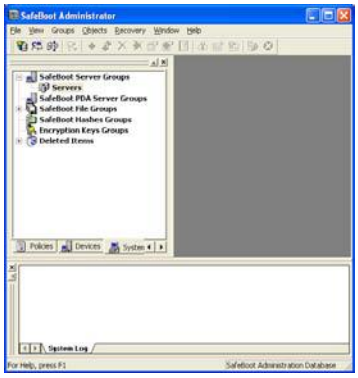


Schéma 2 : Présentation de l'interface d'administration.

Conclusion

Il est clair que toutes les entreprises n'ont pas les mêmes besoins en matière de mobilité. Le niveau de sécurité à déployer dépend de la disponibilité totale ou partielle du degré de confidentialité attendu et du coût réel du piratage.

La sensibilisation et la responsabilisation des utilisateurs apporte un dilemme. Celles-ci n'assurent aucune garantie mais demeurent au cœur du problème car la sécurité des postes nomades reposent sur les mesures de protections de l'équipement et sur l'usage de ses propriétaires.

Devant chaque nouveauté en matière de sécurisation de nouveaux problèmes apparaissent. Le plus difficile dans cette escalade est de déterminer les limites de la raison. La solution idéale serait-elle de ne jamais quitter la société?

Bibliographie

[1] Pierre BETOUIN : "Dossier Sécurité Bluetooth"
http://www.secuobs.com/news/05022006-bluetooth1.shtml

[2] SafeBoot
http://www.safeboot.com/

[3] TrueCrypt
http://www.truecrypt.org/

3. TEST :

TESTER LA SECURITE DE VOS APPLICATIONS ET DE VOS SERVEURS EN LIGNE (DEUXIEME PARTIE)

Ce mois-ci nous avons décidé de tester, à nouveau, deux scanners de vulnérabilités. Un premier test avait déjà été réalisé en Mai 2006 entre 3 sociétés (Criston, Qualys, Acunetix) et le scanner libre « Nessus ». A la suite de l'analyse des versions d'essai, nous avons gardé les deux produits les plus performants afin de disputer une finale qui s'avère serrée.

XMCO | Partners

L'environnement

Les conditions du test sont exactement les mêmes que pour le précédent : une seule adresse IP a été scannée. Les deux concurrents nous ont permis de tester une version plus poussée de leur scanner. Ils nous ont donné un accès à leur application en ligne totalement gérée par l'utilisateur.

Nous avons réalisé le test dans des conditions réelles. Nous avions testé les versions d'essai des scanners (voir Actu-secu Mai 2006). Désormais, nous sommes un client quelconque qui essaye pour la première fois la version finale.

Notre analyse se concentrera sur la pertinence des résultats, la présentation des rapports, l'interface et les options de l'application web et le service client.

La maquette de test

Les versions plus abouties des scanners devraient nous donner des résultats précis et fiables. Afin de ne pas fausser les tests et de percevoir une réelle évolution par rapport au précédent test, nous avons implémenté une maquette relativement proche de celle mise en place précédemment.

Notre maquette est donc toujours composée de deux machines : un serveur Windows 2003 et une machine Linux Debian. Un de nos routeur permet de redirigé les ports vers les deux machines.

Le premier système est équipé d'un honeypot (« pot de miel»), logiciel capable de simuler le comportement de certains services. A l'aide de cet outil, nous avons pu simuler différents serveurs sur des ports connus (21, 23, 68, 110, 139, 445, 1026, 3389, 5631, 5900, 65000). Ainsi, notre attente est simple, nous espérons que les scanners identifieront les services émulés et trouveront les failles associées. Ce premier piège permettra de tester la fiabilité des scans de ports de chacun des concurrents. Un bon scanner devrait détecter tous les ports ouverts mais rester prudent dans l'analyse du service en écoute.

De plus, nous avons installé plusieurs serveurs web (un Apache 1.3.33 et un IIS 6.0) sur des ports exotiques afin de confirmer le test du protocole en lui-même.
Contrairement au dernier test, cette plate-forme Windows hébergera également un forum et un outil php nommé « iCalendar » vulnérable à plusieurs failles. Le module PHP (4.3.10) a également été choisi pour ses deux failles récemment identifiées (voir matrice des vulnérabilités à la fin de l'article).

Chaque mois de nouvelles failles de sécurité sont découvertes pour ce genre d'applications. La réactivé des équipes en charge de maintenir le produit à jour est un élément primordial que nous suivrons avec attention. Ainsi, la vulnérabilité de Cross Site Scripting identifiée dans l'alerte CVE-2006-3319 pourrait être détectée par les scanners les plus précis. Enfin un des serveurs web hébergera une page d'index qui contiendra un fichier nommé « passwd.txt ». En relevant les différents liens compris dans toutes les pages web de notre site, nous espérons que l'un des scanner démontrera la présence d'un tel fichier critique.

En parallèle, nous avons aussi installé dans notre laboratoire, une machine Linux Debian 2.0.45. Un serveur de mail « sendmail 8.13.4 » y est configuré et le service ssh est également disponible sur le port 20 000. Au niveau des applications web, un seul serveur est paramétré afin de renvoyer un code réponse http « 200 OK » pour toute requête reçue. De plus, un formulaire vulnérable à des injections SQL, un répertoire « Admin » et des fichiers aux extensions de sauvegardes (.old, .bak, .php~) seront présents.

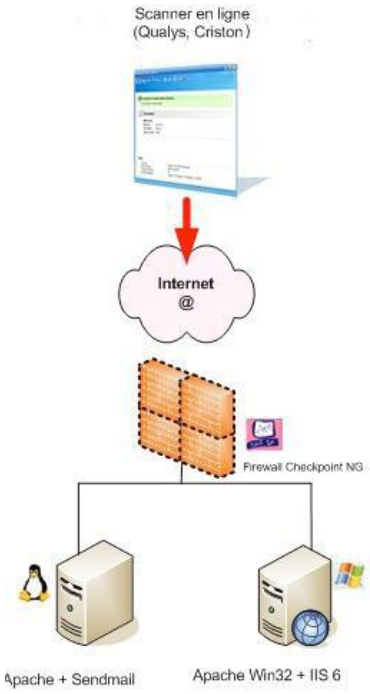


Schéma 1 : Notre maquette

Nos attentes

En dehors des failles que l'on appellera « Failles Editeurs » qui sont les vulnérabilités identifiées et corrigées au sein des différentes technologies implémentées (langages PHP, ASP…, protocole, etc.) nous espérons que les vulnérabilités dites « applicatives » seront également détectées (formulaire non validés, liens vers des pages d'administration, fichiers sensibles, injection SQL via des paramètres utilisés au sein des application web).

Les ports ouverts par le « honeypot », nous permettent de créer de véritables services. Il est indispensable que le scanner détecte les bons services et analyse tous les ports.

Enfin, notre analyse sera également basée sur le nombre de faux positifs renvoyés par les scanners. Une analyse succincte des réelles failles mises en place, aura un avantage considérable sur un rapport long, difficile à lire et qui noie le lecteur dans la masse d'informations.

Criston

Notre demande de test, effectuée directement auprès d'un ingénieur avant-vente, a rapidement été prise en compte par Criston. Un simple email a suffit pour relancer un nouveau scan plus complet. Nous avons également obtenu des identifiants pour accéder au site web réservé aux clients.

Les rapports

En quelques heures, plusieurs rapports (7 au total) nous ont été envoyés puis détaillés par un ingénieur produit.

Le premier reporte les risques liés à l'exploitation des vulnérabilités sous forme de schémas et graphiques. Il est alors facile d'identifier en un coup d'œil la criticité des failles, leurs nombres et les connaissances requises pour une éventuelle attaque. Criston a pris soin de présenter l'évolution de notre maquette par rapport au scan réalisé au mois de Mai. Cette attention particulière dénote un suivi efficace de leur client. Chaque demande de test en ligne et chaque profil client sont donc soigneusement sauvegardés.

Nous apprécions toujours autant le rapport « Ports ouverts » simple et concis qui identifie clairement les informations précieuses (numéro de port, service standard, service détecté, nombre de vulnérabilité par port…) et qui apportent les premières données primordiales à la découverte d'un périmètre.

Les mêmes informations sont reprises dans un autre rapport qui, cette fois, est classé par service. Celui-ci nous semble moins intéressant mais apporte une alternative.

Parallèlement, la vision par machine établie, dans un autre rapport nous a particulièrement satisfait. Lors d'un scan de grande envergure, toutes les informations utiles, par système, sont parfaitement résumées.

Enfin le dernier rapport, destiné essentiellement aux équipes techniques, détaille les failles en établissant des indices qui apporte une visibilité plus qu'appréciable.

Les rapports et leur présentation nous ont séduits. La variété du classement de l'information est un plus indéniable. De l'information générale au détail, chacun y trouvera son bonheur (voir schéma 2, 3, 4 et 5).

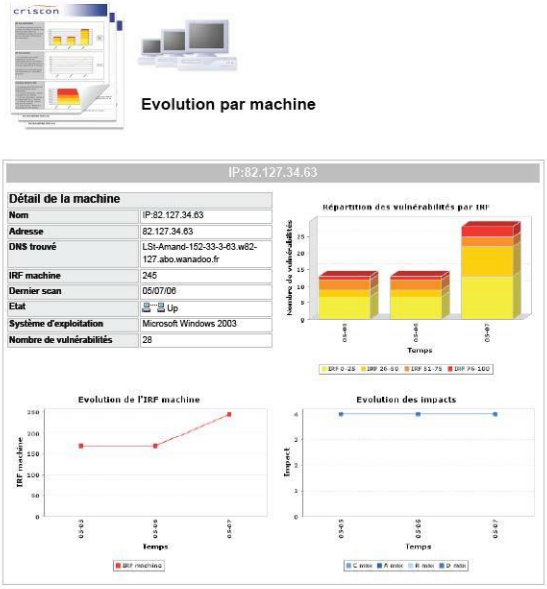


Schéma 2 : Evolution par machine après plusieurs scans

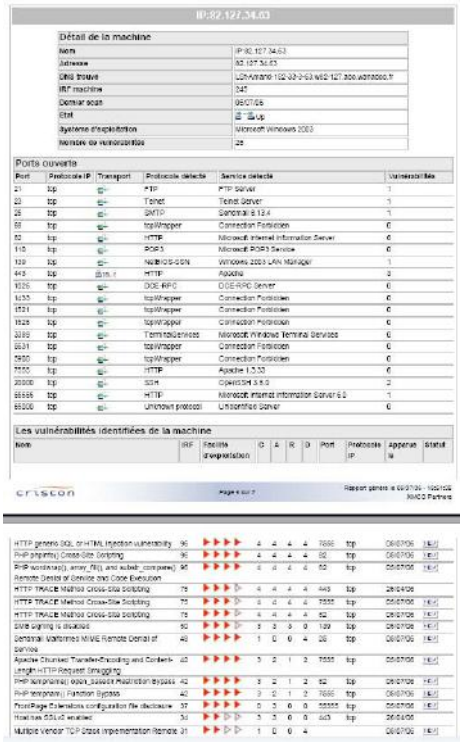


Schéma 3 : Vision par machine (failles, ports ouverts, services actifs)

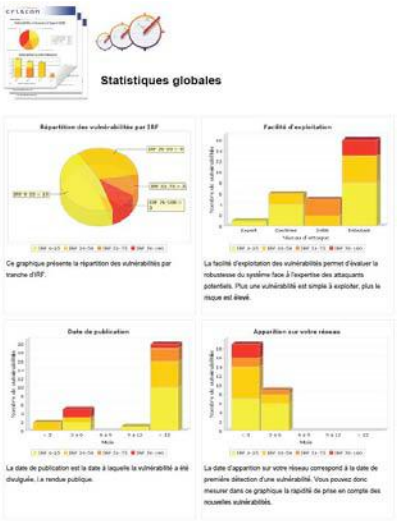


Schéma 4 : Statistiques globales

Schéma 5 : Rapport détaillé

L'analyse des vulnérabilités identifiées

Le premier bon point attribué à Criston concerne la précision du scan de ports qui nous donne une vision précise des services présents et des ports ouverts. Le scanner identifie bien nos serveurs web ainsi que les ports exotiques. Il ne se contente pas de lister les ports et les services « associés par défaut », il nous précise le véritable service présent. L'analyse des protocoles est donc correctement effectuée.

De plus, Criston semble à jour. En effet, la faille de Cross Site Scripting, identifiée le 29 juin dernier sur l'application iCalendar relevée par le scanner, est correcte. Le paramètre vulnérable est également celui que l'on attendait. Malheureusement, l'url fournie afin de valider l'existence de cette faille n'a pas confirmé ce résultat. Est ce une simple erreur ou une url récupérée à partir d'une base de connaissance sans aucun test préalable ?

Le scan a donc bien identifié la présence de cette application PHP ce qui n'est pas le cas pour Qualys.

Malgré ces premiers bons résultats, Criston renvoie également un certain nombre de faux positifs. Certaines descriptions n'apportent aucune information concrète : un déni de service de la pile TCP-IP (vulnérabilité parue en 2004) ou encore une faille dans le traitement des paquets TCP qui possède des flags SYN+FIN ne peuvent être vérifiés. Les analyses techniques pourraient être mieux formulées ce qui éviterait de se perdre parmi des informations inutiles.

Les exploits présentés avec les failles ne sont pas utilisables. En effet, nous avons testé la plupart d'entre eux et les résultats ne sont pas probants. Il serait plus judicieux de montrer la voie d'exploitation mais de ne pas donner d'url ou de code non valide. De nombreuses failles PHP ont été découvertes mais leurs explications longues et souvent confuses rebutent le lecteur. Une phrase concise et une analyse présentée différemment aurait été appréciable.

Le scanner de Criston insiste sur les failles référencées dans sa base de données et corrélées avec les versions des applications de notre maquette mais n'analyse pas les failles applicatives de conception. Plus précisément, les failles du langage sont bien détectées mais les erreurs d'implémentation (comme des formulaires non sécurisés ou des entrées utilisateur non vérifiées ce qui permet l'injection de scripts) ne sont pas testées.

Par rapport à l'identification des serveurs web, le sans faute n'était pas loin. La seule erreur concerne le serveur web sur le port 82 qui fut identifié comme un « IIS 4.0 (UNIX) » ce qui n'est pas le cas. Il est même difficile de trouver un serveur Microsoft sur une machine Unix. Ce résultat aurait pu être couplé avec l'identification de l'OS de la machine distante pour éliminer la possibilité d'être confronté à un serveur de Microsoft.

La console d'administration

Afin de profiter pleinement du service de scan en ligne, Criston nous a permis d'accéder au site utilisé par leurs clients. L'interface, en français, est agréable et les fonctions sont intéressantes : Lancement de scan en ligne, paramétrage de la granularité du scan, planification des scans…tout semble réuni pour satisfaire les attentes du client.

Schéma 6 : Lecture des résultats

Schéma 7 : Lancement d'un scan à partir de l'interface

Le support

En ce qui concerne le support, plusieurs conseillers ont répondu à toutes nos questions. Nous ne pouvons que féliciter ce service client qui, espérons le, reste tout aussi à l'écoute des véritables clients.

Qualys

Qualys a également répondu présent lorsque nous leur avons proposé de réalisé un second test. L'accès à Qualys Guard nous a permis de gérer du début à la fin le lancement des scans et la génération des rapports.

Les rapports

Le scan de notre maquette a été réalisé rapidement et cinq rapports ont été générés. Chacun insiste sur des points particuliers. L' « Executive Report » (voir schéma 7), principalement destiné aux managers, résume les résultats de manière succincte. Des graphiques reprennent les informations les plus pertinentes. La tendance du degré de sécurité se dégage d'un simple coup d'œil.

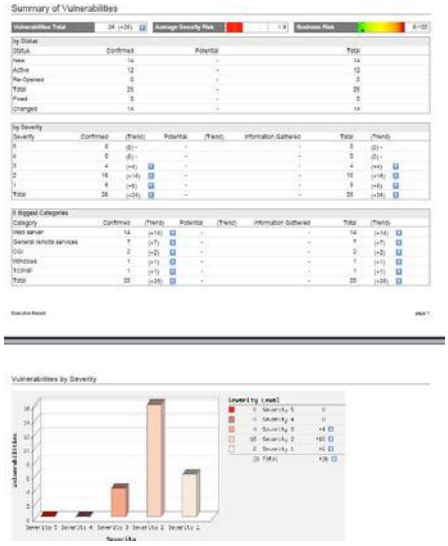


Schéma 8 : Rapport « Executif »

Le rapport technique « Technical report » (voir schéma 8) fournit des informations beaucoup plus précises. Ces précisions sont importantes pour la compréhension des failles et pour la mise en place des solutions adéquates.

Deux autres rapports peuvent apporter une véritable valeur ajoutée. Le « RV10 » présente les 10 dernière signatures ajoutées à la base de connaissance du scanner et confirme ou non si notre machine est bien vulnérable.

Enfin, le rapport « SANS Top 20 Report » indique la présence éventuelle d'une des 20 failles les plus critiques détectée par le scanner.

Tous ces rapports peuvent donc être utilisés par des profils différents et reporter, en fonction des besoins, les informations pertinentes.

Schéma 8 : Rapport technique

L'analyse des vulnérabilités identifiées

Qualys possède une base de données de plus de 5000 signatures ce qui est impressionnant.

Les failles éditeurs importantes ont été identifiées (MIME pour Sendmail, faille pour OpenSSH, ftp anonyme…). D'autre part, les OS et les ports ouverts ont correctement été analysés. Enfin, des répertoires intéressants ont pu être listés (/admin, /cgi, /phpBB2…) ce qui est un plus vis-à-vis des résultats de Criston.

Le revers de la médaille reste le même que pour Criston, trop de failles sans importance sont énumérées (IP interne trouvée, Présence de réponse ICMP…) ce qui noie le lecteur dans un surplus d'informations.

Les faux positifs et les informations inutiles sont tout de même présents. En éliminant les informations superflues, Qualys pourrait gagner en précision et en lisibilité.

Enfin il est dommage que le scanner n'ait pas trouvé le formulaire « login/mot de passe » comme ce fut le cas lors du précédent test.

Le support

Contrairement au premier test qui nous avait déçus par l'absence de support (aucune de nos questions par email n'avait obtenu de réponse), le service client a, cette fois, été remarquable.

Après notre demande d'accès, nous avons immédiatement été contactés par un conseiller qui nous a fourni un compte sur l'application en ligne « Qualys Guard ». Ce service permet à l'utilisateur de gérer totalement ses scans sans aucune intervention des équipes techniques de Qualys. Par ailleurs, au moindre souci une personne était tout de suite disponible et nous a expliqué en détails les fonctionnalités du service. Nous avons également reçu une invitation pour une journée gratuite de formation.

L'accès réservé à "Qualys Guard"

Le site réservé aux abonnés de Qualys Guard est particulièrement simple. Après quelques minutes, l'ensemble des fonctions proposées devient intuitif. Différents onglets proposent les services attendus. Pour notre test, nous avons seulement utilisé les fonctionnalités Scan et Report. Comme son nom l'indique, la première permet de lancer manuellement les scans pour une ou plusieurs adresses IP. Une seule case (adresse IP) suffit pour lancer un scan.

Dès la fin de ce dernier, plusieurs rapports sont générés dans la partie « Report ». Les options de paramétrages et d'éditions rendent l'audit plus agréable et plus pratique. De plus, il est possible de définir des seuils et éradiquer certains faux positifs pour les futurs scans.

Les autres fonctionnalités sont certainement pratiques mais elles restent réservées au scan d'un parc entier et n'ont que peu d'intérêts pour le scan d'une seule machine.

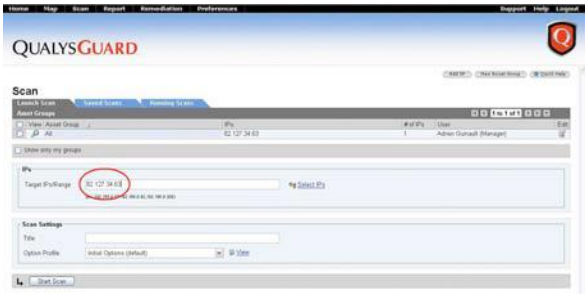


Schéma 10 : Lancement du scan

Schéma 11 : Lancement du scan

Conclusions et notes attribuées aux concurrents sur les différents points analysés

Comme nous l'avions déjà révélé, les scanners en ligne peuvent seulement répondre à des problématiques particulières. Il est évident qu'un programme ne pourra pas trouver des failles qui nécessitent une réflexion et de l'analyse poussée.

Les scanners sont donc relativement limités. Les failles « Editeur », qui restent le domaine de prédilection de ce genre de produits, sont effectivement bien découvertes. L'analyse des ports est précise, cependant ces scanners limitent leur recherche et devraient implémenter des fonctions plus avancées. L'audit des codes sources HTML serait un atout majeur. L'étude des mots de passes par défaut, des formulaires cachés et des liens HTML contenus dans des pages fournirait des informations précieuses voir critiques.

Il est possible d'imaginer une simple fonction qui, dans un premier temps, téléchargerait les pages web du site audités (avec la fonction « wget »). Dans un second temps, le code HTML pourrait être analysé afin d'identifier les différentes balises « <a> » (pour les liens vers d'autres pages web), « < !—> » (pour les commentaires), « <form> » (pour les formulaires) et <hidden> (pour les champs cachés). Enfin une simple recherche dans le code source des mots « admin », « mot de passe », « password », renverrait certainement des liens vers des pages confidentielles et des données sensibles. Ces informations sont le plus souvent oubliées par les développeurs, or elles sont d'une aide précieuse pour la compromission d'un système.

Ces fonctions peuvent être implémentées facilement et peuvent démontrer l'existence de failles bien plus dangereuses. On peut estimer que l'implémentation de telles fonctions élèverait la pertinence des résultats de 30% à 50%.

Accès au site réservé aux clients, options et possibilités de configuration

Les deux sites réservés aux clients Qualys nous ont séduits. L'application Qualys Guard est une solution parfaite pour les entreprises désireuses de gérer entièrement leurs scans de vulnérabilités.

Ce site web, mis à jour quotidiennement par les équipes de Qualys, est vraiment complet et propose de nombreux services utiles et simples d'utilisation (planification de scans, envoi d'e-mails dès la génération de rapports…). L'atout majeur de Qualys est la personnalisation des rapports qui apportera une valeur ajoutée incontestable.

De son côté, Criston offre également la possibilité de lancer les scans sans intervention de leur part. Malgré cela, les options sont moins nombreuses et Qualys garde l'avantage dans ce domaine. L'édition et la configuration des rapports ne sont pas disponibles chez Criston. En revanche, l'intégralité du site est en français ce qui est un petit plus par rapport à Qualys.

Criston : 7/10
Qualys : 8/10

Vainqueur : Qualys

Présentation des résultats

Au niveau du classement des informations, les avis sont partagés. Criston présente ses résultats par genre « par port », « par machine », « par vulnérabilité » et envoient deux rapports globaux sur l'évolution des risques. Qualys analyse les résultats du scan autrement et préfère générer des rapports pour des profils techniques différents (manager, équipe de production…).

Le regroupement des résultats possède des avantages et des inconvénients pour chacune des parties et il nous est difficile de départager les concurrents sur ce point.

En revanche, nous avons une petite préférence pour Criston sur la présentation des résultats (couleurs, tableaux plus parlants pour chaque vulnérabilité détectée). Chacun se fera son propre avis avec les captures présentes dans cet article (voir schéma 2, 3, 4, 5, 8, 9, 12, 13).

Schéma 11 : Présentation d'une faille par Criston

Schéma 12 : Présentation d'une faille par Qualys

Criston : 8/10

Qualys : 6/10

Vainqueur : Criston

Pertinence des résultats

En ce qui concerne les résultats, les deux outils restent des programmes automatiques et basés sur des signatures. Les faux positifs sont donc nombreux. Les failles éditeurs sont correctement découvertes mais les vulnérabilités applicatives (formulaires, faille de Cross Site Scripting, Injection SQL sur des paramètres définis par les développeurs web) ne sont pas suffisamment testées. Un exemple, les scanners peuvent remonter 10 failles sur le langage PHP (cross Site Scripting, accès à des informations de configuration…) et ne pas signaler la présence du fichier « /passwd.Txt » identifiable via un lien sur la page d'accueil du site web.

D'après notre tableau de résultats, les deux concurrents obtiennent globalement les mêmes scores. En identifiant les répertoires critiques, Criston aurait pu gagner cette partie.
Qualys garde un léger avantage sur le domaine applicatif ainsi que sur la remontée d'informations sensibles mais remonte cependant un nombre de faux positif supérieur à celui de Criston.

Domaine « vulnérabilité Editeur » :
Criston : 8/10
Qualys : 8/10

Domaine « vulnérabilité Applicative et informations diverses »
Criston : 3/10
Qualys : 5/10

Pertinence (Nombre de faux positif)
Criston : 5/10
Qualys : 2/10

Vainqueur : Egalité

L'heure du bilan a sonné. Quel est le meilleur scanner en ligne ? Ce choix est difficile. Les deux services possèdent leurs avantages et leurs inconvénients. Criston a davantage creusé la partie technique pour proposer des résultats, le plus souvent honorables. De l'autre côté, Qualys a davantage misé sur la partie Packaging et les options proposées. Les deux sociétés permettent aux équipes techniques de gérer comme bon leur semble l'ensemble des scans. Les rapports ont chacun leurs avantages et séduiront différents profils.

Les environnements de travail que l'on peut personnaliser, la gestion des rapports et le lancement des scans « à la demande » restent des points positifs des deux côtés.

Le seul avantage, sur cette interface client, concerne les rapports de Qualys qui sont entièrement paramétrables (choix des catégories, des graphiques…) et qui apportent sans aucun doute beaucoup de satisfaction aux clients. Quand à Criston, leurs indices de criticité (même s'ils pourraient être plus parlant avec une échelle d'indice sur 100) attirent le regard et les choix de couleurs permettent de cerner facilement les problèmes éventuels.

Les deux produits correspondent donc à des besoins et des profils différents. Il reste à savoir le prix de ces solutions qui pourrait faire pencher la balance d'un côté ou de l'autre...

Plateforme Linux Debian	Qualys		Criston	
Resultats techniques	Détecté	Non-détecté	Détecté	Non-détecté
Failles identifiées				
* Sendmail Signal Handling Memory Corruption Vulnerability	X			X
*Sendmail Multi-Part MIME Message Handling Denial of Service	X		X	
* OpenSSH scp Command Line Shell Command Injection	X			X
* Apache Vulnerabilities in Various Module		X		X
Apache 2.0.45 sur port TCP 82 avec bannière IIS 4.0		IIS 4.0 (UNIX)		IIS 4.0 (UNIX)
Erreur 404 => 200 OK	X		X	
Faux Oracle (8i et 9i) sur les ports 1521 et 1526		X		X
Directory listing à la racine	X		X	
Formulaire login/password		X		X
Injection SQL sur le formulaire ("/')		X		X
Faille de directory transversal sur la variable "file"		X		X
Méthode TRACE sur serveur web port 82	X		X	
Nombre de Ports ouverts (5)				
25/tcp open smtp (sendmail)	X		X	
82/tcp open http (apache)	X		X	
1521/tcp open Oracle	X		X	
1526/tcp open Oracle	X		X	
20000/tcp open ssh	X		X	
Informations sensibles				
OpenSSH v3.8.1p1 sur port TCP 20000	X		X	
Sendmail v8.13.4 sur Port 25	X		X	
/manual	X			X
/cgi-bin : 2 scripts dangereux	X		X	
Fichier passwd.txt		X		X
Répertoire /Admin/	X			X
Fichiers index.php~/index.bak/ index.old		X		X
Directory Listing sur 82	X			X
OS Linux 2.4	X			X
Total				
12 failles/5 ports ouverts/9 informations utiles	6/5/7		4/5/3	

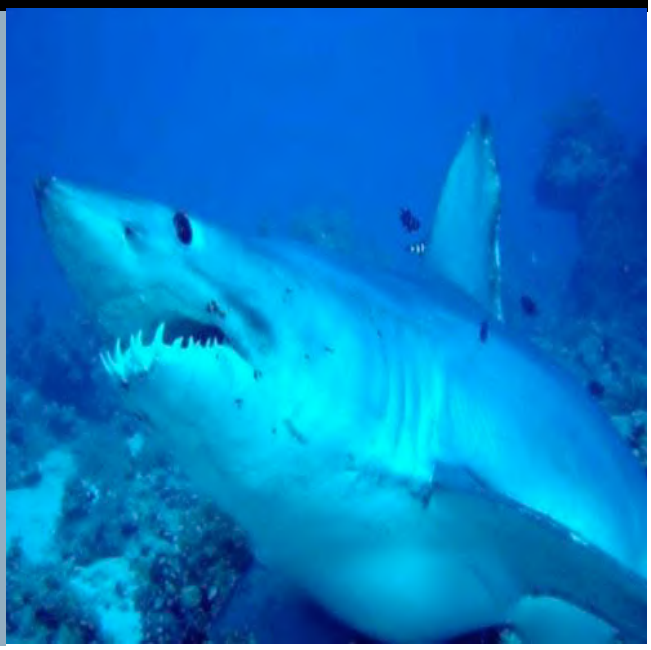
Résultats techniques (plateforme Windows)	Détecté	Non-détecté	Détecté	Non-détecté
Failles identifiées				
Connexion anonyme en ftp possible	X		X	
*PHP "phpinfo()" Cross-Site Scripting		X	X	
*PHP "wordwrap()" Buffer Overflow Vulnerability		X	X	
*PHP tempnam() Bypass		X	X	
*Cross Site Scripting CVE-2006-3319 sur iCalendar		X	X	
*Méthode TRACE sur serveur web port 7555	X		X	
Nombre de Ports ouverts (5)				
21/tcp open ftp	X		X	
23/tcp open telnet	X		X	
68/tcp open dhcpc	X		X	
110/tcp open pop3	X		X	
139/tcp open netbios-ssn	X		X	
445/tcp open microsoft-ds	X		X	
1026/tcp open LSA-or-nterm	X		X	
3389/tcp open ms-term-serv	X		X	
5631/tcp open pcanywheredata	X		X	
5900/tcp open vnc	X		X	
7555/tcp open apache	X		X	
55555/tcp open IIS	X		X	
65000/tcp open SSL	X		X	
Informations sensibles				
Apache sur port 7555 avec PHP 4.3.10	X		X	
Serveur SSL sur port 65000	X		X	
Fichier “passwd.txt” lié à partir d'index.html		X		X
Bannière IIS 4.0		X		X
Serveur IIS 6.0 sur port 55555	X		X	
Bannière FTP	X		X	
Directory Listing sur 7555	X		X	
OS Windows 2003 Serveur SP1	X		X	
PhpBB 2.0.21	X		X	
iCalendar 2.22 avec faille		X	X	
Total				
6 failles/13 ports ouverts/10 informations utiles	2/13/7		6/13/8	
TOTAUX : 18 failles/18 ports ouverts/19 informations utiles	7/18/14		9/18/11	
Total				

4. ATTAQUES MAJEURES :

TOP 5 DU MOIS DE JUILLET ET AOUT :

Les mois de Juin et Juillet ont été marqué par des failles de sécurité critiques au sein des logiciels les plus utilisés dans les entreprises : Ms Office, Internet Explorer, Oracle et Cisco.
Microsoft est comme a son habitude la cible numéro un des "hackers" en tout genre. Cisco aura connu un mois de juillet difficile avec une dizaine de failles de sécurité découvertes sur de nombreux produits. Enfin les navigateurs sont aussi à l'affiche avec l'apparition d'un site qui publia une vulnérabilité chaque jour durant ce mois de Juillet. Inquiétant, non ?

XMCO | Partners



MOZILLA/INTERNET EXPLORER

Nombreuses failles au sein des produits Mozilla et Internet Explorer

Mozilla a publié les dernières versions de ses produits libres Mozilla Firefox, Mozilla Thunderbird et Mozilla SeaMonkey. L'éditeur corrige ainsi de nombreuses vulnérabilités présentes au sein du noyau partagé par toutes ces applications.

14 failles ont été corrigées dont la plupart proviennent d'erreurs au sein de fonctions et de méthodes communes aux 3 logiciels. Le moteur JavaScript est, lui aussi, touché par cette mise à jour.

L'exploitation des failles est dangereuse car elle permet à un attaquant distant d'exécuter des commandes arbitraires, d'injecter des scripts web afin de récupérer des informations sensibles, d'interrompre le fonctionnement normal de l'application et de contourner les sécurités applicatives. L'utilisateur malveillant pourrait ainsi prendre le contrôle total de la machine vulnérable.

Nous attirons votre attention que de nombreux exploits et preuves de concept ont été publiés sur Internet. La compromission d'une machine disposant d'un des logiciels vulnérables est donc très probable. Cependant, seules des preuves de concept qui causent des dénis de service ont vu le jour.

Le mois de juillet a vu apparaître un blog dédié à la sécurité des navigateurs web (http://browserfun.blogspot.com/) dans lequel le chercheur HD MOORE a publié chaque jour une nouvelle faille non corrigée.

Internet Explorer a donc été la première cible de ce chercheur qui semble prendre un certain plaisir à défier Microsoft...

Programmes vulnérables :

- Word 2002
- Mozilla Firefox versions antérieures à 1.5.0.4
- Mozilla Thunderbird versions antérieures à 1.5.0.4
- Mozilla SeaMonkey versions antérieures à 1.0.2
- Internet Explorer 6

Criticité : Elevée

Référence Xmco : n° 1153814697, 1153814505, 1153813233, 1153812860, 1153727876, 1153727744, 1153468780, 1153146985,1153146039, 1152169209, 1152259532, 1152518172, 1153121283, 1152777349, 1152601585

Microsoft Office

Exécution de code et prise de contrôle à distance avec MS Office (MS06-027, MS06-037, MS06-038, MS06-039)

Les deux derniers mois ont été marqués par une succession de failles et d'exploits pour la suite Office, l'un des logiciels les plus utilisés en entreprise. Après le correctif MS06-27 pour Word, Microsoft corrige trois failles présentes dans le tableur Excel et dans l'ensemble des logiciels d'Office. Une dernière vulnérabilité identifiée dans le le programme Power Point clôture pour l'instant la recherche de failles pour le logiciel bureautique de Microsoft. Les chercheurs et les pirates s'en seront donnés à cœur joie pour effrayer Microsoft et l'ensemble des clients de la firme de Bill Gates.

Les trois logiciels Word, Excel et PowerPoint sont vulnérables à des débordements de tampon provoqués dès l'ouverture d'un document contrefait.

Excel ne valide pas la longueur d'un enregistrement avant de le transmettre au tampon alloué. En insérant des enregistrements « SELECTION", "COLINFO", "OBJECT", "FNGROUPCOUNT" ou "LABEL" spécialement conçus, le pirate pourrait provoquer un débordement de tampon lors de l'ouverture du document malicieux.

Différents exploits et différentes preuves de concept ont vu rapidement le jour et les attaques ont rapidement commencé.

Le premier programme malicieux, nommé "Kukudro.A", fut envoyé massivement par email. Ce dernier posséderait ce fichier

zippé en pièce jointe sous le nom de "prices.zip", "apple_prices.zip", "sony_prices.zip".
L'installation du troyen est réalisée dans C: sous le nom de "666inse_1.exe".
Ce fichier est en réalité un document Word qui exécute une macro pour lancer l'installation d'un cheval de Troie.

La suite des attaques a continué avec Excel pour finir, à l'heure où nous écrivons, avec le troyen Trojan.PPDropper.B, caché dans un fichier PowerPoint et véhiculé par un e-mail en caractères chinois, en provenance d'une source inconnue (probablement d'Asie).

Ces vulnérabilités sont extrêmement critiques. Nous vous conseillons d'appliquer les correctifs nécessaires afin de parer une éventuelle attaque. De plus, soyez attentif aux différents fichiers Office reçus par email qui pourraient devenir le vecteur d'exploitation majeur.

Programmes vulnérables :

- Microsoft Office 2003 Service Pack 1
- Microsoft Office 2003 Service Pack 2
- Microsoft Office XP Service Pack 3
- Microsoft Office 2000 Service Pack 3
- Microsoft Office 2004 pour Mac
- Microsoft Office v. X pour Mac
- Microsoft Excel 2003
- Microsoft Excel Viewer 2003
- Microsoft Excel 2002
- Microsoft Excel 2000
- Microsoft Excel 2004 pour Mac
- Microsoft Excel v. X pour Mac

Criticité : Elevée

Référence Xmco : n° 1152688533, 1153123685, 1152688967

Alerte Oracle Juillet 2006

Publication d'un correctif cumulatif

Oracle publie son troisième bulletin trimestriel de l'année 2006 qui présente failles importantes décelées au sein de plusieurs de ses produits. L'ensemble des produits Oracle est concerné (bases de données et serveurs d'applications).

65 failles ont été corrigées mais toutes n'affectent pas le même produit. 23 d'entre elles concernent le moteur de base de données et les plus importantes permettent à un utilisateur, possédant un compte sur la base Oracle ou sur le système hébergeant la base, de prendre le contrôle total ou partiel de la base de données.

De nombreuses vulnérabilités sont également présentes au sein du serveur HTTP (module modPL/SQL pour Apache). Ces vulnérabilités sont dangereuses car elles permettent à un attaquant distant d'exécuter des commandes arbitraires, d'interrompre le fonctionnement normal de l'application et de contourner les sécurités applicatives.

Les failles présentées concernent des Injection SQL. Les packages SYS.DBMS_UPGRADE, SYS.DBMS_STATS, SYS.KUPW$WORKER sont vulnérables mais ne restent exploitables seulement par des utilisateurs qui possédent les droits de créer une fonction PL/SQL.

Enfin, le paquet SYS.DBMS_CDC_IMPDP serait lui aussi affectée par une faille d'injection SQL. Les procédures IMPORT_CHANGE_SET, IMPORT_CHANGE_TABLE, IMPORT_CHANGE_COLUMN, IMPORT_SUBSCRIBER, IMPORT_SUBSCRIBED_TABLE, IMPORT_SUBSCRIBED_COLUMN, VALIDATE_IMPORT, VALIDATE_CHANGE_SET, VALIDATE_CHANGE_TABLE, VALIDATE_SUBSCRIPTION seraient à l'origine de ces problèmes.

Programmes vulnérables :

- Oracle Database 10g Release 2, versions 10.2.0.1, 10.2.0.2Oracle Database 10g Release 2 version 10.2.0.1 et 10.2.0.2
- Oracle Database 10g Release 1 version 10.1.0.4, 10.1.0.5, 10.1.0.4.2 et 10.1.0.3
- Oracle9i Database Release 2 version 9.2.0.5, 9.2.0.6 et 9.2.0.7
- Oracle9i Database Release 1 versions 9.0.1.4, 9.0.1.5 et 9.0.1.5 FIPS
- Oracle8i Database Release 3 version 8.1.7.4
- Oracle8 Database Release 8.0.6 version 8.0.6.3
- Oracle Application Server 10g Release 3 version 10.1.3.0.0
- Oracle Application Server 10g Release 2 versions 10.1.2.0.0 a 10.1.2.0.2 et 10.1.2.1.0
- Oracle Application Server 10g Release 1 (9.0.4) version 9.0.4.1, 9.0.4.2 et 9.0.4.3
- Oracle9i Application Server Release 2 version 9.0.2.3 et 9.0.3.1
- Oracle9i Application Server Release 1 version 1.0.2.2
- Oracle Collaboration Suite 10g Release 1 version 10.1.2.0
- Oracle E-Business Suite Release 11i versions 11.5.7 a 11.5.10 CU2
- Oracle E-Business Suite Release 11.0
- Oracle Enterprise Manager 10g Grid Control version 10.2.0.1
- Oracle Pharmaceutical Applications versions 4.5.0 a 4.5.2
- Oracle PeopleSoft Enterprise Portal Solutions Enterprise Portal version 8.4, 8.8, 8.9; Enterprise Portal avec Enforcer Portal Pack version 8.8
- JD Edwards EnterpriseOne Tools OneWorld Tools version 8.95 et 8.96
- Oracle Application Server Portal version 10.1.4.0.0
- Oracle Developer Suite version 6i 9.0.4.2
- Oracle Workflow versions 11.5.1 a 11.5.9.5

Criticité : Moyenne tant qu'aucun exploit n'a été publié.

Référence Xmco : n° 1153294756

Cisco

Nombreuses vulnérabilites dans des produits et équipements Cisco

Plusieurs failles ont été découvertes tout au long du mois de Juin et Juillet 2006 surde nombreux produits CISCO. Les impacts sont divers : du simple vol de session à la compromission d'un système. Petit tour d'horizon et explications des principales failles identifiées.

Plusieurs failles de Cross Site Scripting ont été corrigées. Un attaquant était en mesure de voler le cookie de session et la session d'un autre utilisateur.
Les logiciels WebVPN, Cisco Secure ACS et Cisco CallManager ont été les premiers concernés. Certains fichiers html ne validaient pas correctement les entrées utilisateurs. De ce fait, les urls malveillantes ont également été dévoilées.

Pour WebVPN :
https://<vpnhost>/webvpn/dnserror.html?domain=<script>alert(« XMCO PARTNERS »);</script>

Pour Cisco Secure ACS :
http://www.example.com/CScgi/LogonProxy.cgi?Server=0.0.0.0&error=<script>alert(« XMCO PARTNERS »);</script>

Cisco CallManager :
http://callmanageraddress/ccmadmin/phonelist.asp?findBy=description&match=begins&pattern=<script>alert(« XMCO PARTNERS »);</script>&submit1=Find&rows=20&wildcards=
on&utilityList=

*Le même logiciel CallManager fut, peu de temps après la parution de la première faille, victime de nombreuses failles de sécurité. Un attaquant distant était en mesure de compromettre un système via une vulnérabilité dans VNC (VNC est implémenté sans Call Manager). Le problème résultait d'une mauvaise validation des mots de passe soumis par les utilisateurs lors des connexions à un serveur VNC. En effet, en envoyant une requête spécialement forgée un utilisateur malveillant était en mesure de contourner l'authentification d'un serveur vulnérable. Plusieurs autres failles (débordement de tampon lors du traitement d'une requête SIP malformée, modifications arbitraires de fichiers) affectaient également ce même produit.

*Cisco Secure ACS était également vulnérable à un contournement de l'authentification.
Une fois authentifié sur cette interface, un utilisateur est automatiquement redirigé vers un serveur HTTP dont le port est compris entre 1024 et 65535. Le problème vient du fait que le numéro de port est incrémenté plutôt que d'être sélectionné de manière aléatoire, une personne malveillante pourrait contourner la page d'authentification en "devinant" le port utilisé. En exploitant cette faille, un attaquant peut accéder a l'interface d'administration gérant tous les composants du réseau.

*Une autre faille dans CISCO Aironet permettait l'accès à la configuration du point d'accès.
D'autre part, une mauvaise configuration de l'IOS (pour de nombreux routeurs Cisco) permettait également à un utilisateur non authentifié d'accéder à l'interface d'administration en disposant des privilèges les plus élevés.

*Une vulnérabilité a été corrigée dans l'appliance Cisco IPS. L'envoi de paquets malformés pouvait entraîner un déni de service.

*Enfin plusieurs vulnérabilites ont été détectées et corrigées au sein de l'application Cisco Security Monitoring Analysis et Response System (CS-MARS). L'exploitation de celles-ci permettait à un attaquant de compromettre un système vulnérable ou d'obtenir des informations sensibles.

Cisco a rapidement corrigé les failles présentées. Tous les correctifs sont disponibles sur le site de l'éditeur.

Programmes vulnérables :

- Firefox 1.5.0.2
- WebVPN : Cisco VPN 3000 Series Concentrator
- Cisco ASA 5500 Series Adaptive Security Appliances (ASA)
- Cisco Secure ACS 2.x / 3.x
- Cisco CallManager 3.x / 4.x
- Cisco Secure Access Control Server 4.x pour Windows
- Cisco Aironet 1100 Series Access Point /1200 /1300 /350
- Cisco Aironet 1130 AG Series Access Point / 1240 / 1400
- Cisco 806 / 826 / 827 / 827H / 827-4v / 828 / 831 / 836 / 837
- Cisco SOHO 71 / 76 / 77 / 77H / 78 / 91/ 96 / 97
- Cisco Intrusion Prevention System (IPS) version 5.1(1) / 5.1(1a) / 5.1(1b) / 5.1(1c) / 5.1(1d) / 5.1(1e) / 5.1(p1)
- Cisco IDS-4235 / IDS-4250-SX / IDS-4250-TX / IDS-4250-XL
- Cisco IPS-4240 / PS-4255

Criticité : Elevée

Référence Xmco : n°1150287650,1150708756, 1150787518,1151051171,1151311746,1151567708,1151573087,1152776251,1147765706,1152776660

Etes-vous un bon RSSI ?

Evaluer votre niveau en 20 questions...

1) Qu'est ce qu'une "Null session" sous Windows ?

a) Une session SMB non-authentifié pour se connecter à distance sur un poste Windows anonymement.

b) Un problème de déréférencement de pointeurs pour se connecter avec les droits SYSTEM sur un ordinateur distant.
c) Une connexion avec des droits root sur une machine UNIX grâce à la fonction SUDO

2) Qu'est ce que le "pharming" ?

a) Une technique qui permet à un logiciel espion appelé "pharmer" de prendre le contrôle à distance de votre ordinateur via une faille dans MSRPC.
b) Une attaque de corruption de serveurs DNS
c) Un concept des réseaux sans-fils pour permettre le déplacement sans être déconnecté

3) Qu'est ce que le "phishing" ?

a) La nouvelle méthode de pêche à la mode
b) Une attaque informatique que l'on peut contrer avec un pare-feu.
c) Une méthode de piraterie permettant d'extirper des informations sensibles à des Internautes non avertis.
d) On dit qu'un fichier est « phishé » quand il est détecté par un antivirus.

4) Quelle(s) solution(s) préconiseriez-vous pour éviter des attaques de type SQL injection sur un formulaire ?

a) Limiter le nombre de caractères du formulaire
b) Utiliser des fonctions qui permettent de ne pas interprêter les caractères spéciaux.
c) Interdire les caractères 'quote', 'double quote'.

5) Quel est selon vous le meilleur protocole de chiffrement pour les communications Wi-Fi ?

a) 802.1X/EAP
b) WEP
c) WPA=> WPA2(802;11i)

6) Dans la liste suivante, quels sont, à votre avis, les mots de passe les plus robustes ?

a) Sauver
b) $aUver
c) *sAuv3r ;
d) S4uV3r

e) $4uVer!.

7) Comment identifiez-vous le risque lié à une plateforme ?

a) Au hasard

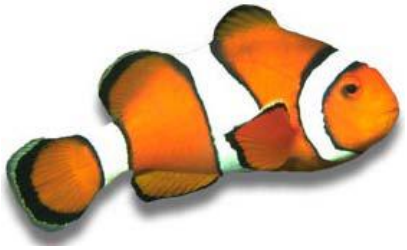
b) En vous basant sur votre expérience
c) En menant une étude statistique sur l'indisponibilité de la plateforme

d) En analysant les pertes financières en cas de problème

e) En identifiant l'existence ou non d'un plan de secours

8) Quel est l'objectif d'un audit de sécurité ?

a) Recenser les composants sécurité employés au sein d'un périmètre donné afin de les mettre à jour.
b) Évaluer le niveau de sécurité d'un périmètre donné, en identifiant, entre autres, les éventuelles vulnérabilités ou failles de sécurité.
c) Évaluer les procédures de continuité de service d'un périmètre donné.



9) Qu'est ce qu'un Service Pack ?

a) Une mise à jour de sécurité englobant tous les correctifs parus à ce jour

b) Un ensemble de services réseau
c) Un ensemble d'outils de sécurité

10) Qu'est ce qu'un exploit ?

a) Une prouesse réalisée par un collaborateur.
b) Un programme qui exploite une vulnérabilité de manière simple.

c) Un correctif de sécurité amélioré.
d) Un outil qui permet de parer certaines attaques.

11) Quel est l'outils indispensable à l'investigation suite à une suspicion de fraude ?

a) Les alertes des IDS
b) Les journaux d'événements.
c) Un logiciel de corrélation d'événements.

12) Laquelle de ces réglementations impose que tous les accès et toutes les données relatives aux transactions soient loguées et archivées ?

a) Sarbanes Oaxley
b) CNIL

c) Loi Godfrain

13) Qu'est ce que le social engineering ?

a) L'ingénierie de la société

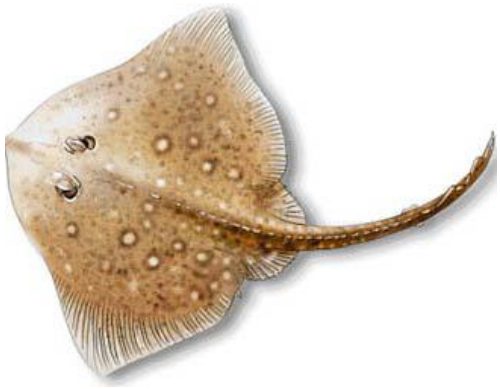
b) Des prestations sociales pour les ingénieurs
c) Une méthode permettant de subtiliser des informations à un tiers
d) Une attaque informatique visant les systèmes informatisés de la sécurité sociale

14) Qu'est ce qu'un cheval de Troie ?

a) Un jeu
b) Un programme malicieux qui, une fois installé sur une machine victime, offre un accès distant à un pirate

c) Un programme permettant d'outrepasser la protection d'un firewall

d) Un logiciel qui permet de faire planter n'importe quelle machine d'un réseau



15) Qu'est ce qu'un ver ?

a) Un programme malveillant se diffusant à l'aide de l'intervention humaine
b) Un programme malveillant se propageant automatiquement sur un réseau en exploitant une faille logicielle

c) Un virus inoffensif

d) Un ver est un courriel indésirable

16) Qu'est ce qu'une preuve de concept ?

a) La démonstration qu'une vulnérabilité est exploitable
b) La preuve qu'un programme à été conçu dans les règles de l'art
c) La validation d'une conception

17) Qu'est ce qu'un Spyware ?

a) C'est un nouveau jeu
b) C'est un logiciel espion
c) C'est un programme infectant la partie hardware d'un ordinateur

18) Quelle est la dernière faille ou le dernier virus qui a alerté votre service ?

a) La faille PowerPoint
b) La faille Excel
c) Le ver Bagle
d) Faille MS06-025 et l'exploit associé

19) L'utilité du logiciel Nmap est : ?

a) Un scanner de ports
b)Un déboggeur de langage C
c) Un logiciel de cartographie d'un système d'informations
d) Un logiciel de calculs d'itinéraires développé par le site www.mappy.com

20) Quelle est la fonction la plus sécurisée en langage C ?

a) strcopy
b) strncopy

Résultats :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a	b	c	c	a	c/e	c/d/e	b	a	b	b	a	c	b	b	c	b	a	a	b

1) Qu'est ce qu'une "Null session" sous Windows ?

1-a. Il s'agit d'une fonctionnalité de Microsoft Windows permettant de partager facilement des fichiers de son ordinateur sans aucun mot de passe. En utilisant un scanner de partage de fichiers et en exploitant la null-session, un espion découvre très rapidement les partages oubliés par les utilisateurs.

2) Qu'est ce que le "pharming" ?

2-b. Une nouvelle attaque baptisée "Pharming" est en vogue au sein de la communauté des pirates. Cette technique se base sur la corruption des serveurs DNS afin de rediriger l'utilisateur vers des pages de substitution. En effet, les serveurs DNS permettent d'établir la correspondance entre l'IP d'un serveur et l'adresse (URL) d'un site qu'il héberge. Le "Pharming" consiste à modifier cette association IP/adresse en remplaçant l'IP du serveur légitime par l'IP d'un serveur malicieux.

Ainsi, imaginons que vous souhaitiez consulter vos comptes sur le site www.votrebanque.com hébergé sur un serveur possédant l'IP 193.10.10.10. Une demande est alors envoyée au serveur DNS pour vous fournir cette adresse IP (193.10.10.10) afin que votre puissiez vous connecter au site de votre banque. L'attaquant intervient ici et modifiera le cache du serveur DNS afin de remplacer l'adresse IP du serveur de votre banque (193.10.10.10) avec une adresse IP d'un serveur pirate (1.1.1.1) qui hébergera un site web similaire à celui de votre banque.
Ainsi lorsque votre demande est traitée par le serveur DNS, ce dernier vous enverra l'adresse IP du serveur pirate (1.1.1.1). L'utilisateur, certain d'être connecté sur le site de sa banque, peut donc facilement se faire piéger et ses données sensibles pourront alors être recueillies par la personne mal-intentionnée.

3) Qu'est ce que le "phishing" ?

3-c. Le « phishing » est un type d'escroquerie utilisé par les pirates informatiques. Ces manipulations permettent de voler des informations sensibles d'Internautes inattentifs. Ce type d'attaques peut être réalisé en copiant la page d'accueil d'un site marchand connu.

4) Quelle(s) solution(s) préconiseriez-vous afin d'éviter des attaques de type SQL injection sur un formulaire ?

4-c. Une injection SQL sur un formulaire peut être facilement évitée en utilisant des fonctions propres au language et qui permettent de ne pas interprêter les caractères spéciaux comme quote (‘), double-quote(“) et chevron (><).

5) Quel est selon vous le meilleur protocole de chiffrement pour les communications Wi-Fi ?

5-a. Le meilleur protocole parmi ceux cités est le WPA devenu WPA-2. Il utilise l'algorithme AES connu pour sa robustesse. La réponse a) était un piège puisqu'il s'agit d'une méthode d'authentification qui peut être couplée avec les protocoles cités.
Enfin, différents algorithmes et différents outils permettent de casser facilement une clef wep qui n'est plus recommandée pour une sécurité optimale.

6) Dans la liste suivante, quels sont à votre avis les mots de passe les plus robustes ?

6-c/e. Un mot de passe robuste doit respecter les caractéristiques suivantes :

- Une longueur minimale de 8 caractères.
- Comprendre au moins un caractère minuscule ou majuscule, un chiffre et un caractère spécial (ex : !^*$= :…).
- Ne pas être trivial et ne pas faire partie d'un dictionnaire, même si il est suivi d'un nombre.
- Etre différent du nom de la machine ou du système utilisé.
- Ne pas être déduit par simple association d'idées.
- Etre facile à retenir (ex : Ght2kfé! « j'ai acheté 2 cafés ! ») à l'aide d'un moyen mémo technique.
- Ne pas être noté (sur un POST IT, derrière le clavier…)

7) Comment identifiez-vous le risque lié à une plateforme ?

7-c/d/e. L'identification d'un risque lié à une plateforme s'effectue en récoltant un certain nombre d'informations comme le taux de disponibilité, l'existence d'un plan de secours ou encore les pertes financières associées en cas de problème. En combinant l'ensemble des facteurs, il devient possible d'établir un risque approximatif.

8) Quel est l'objectif d'un audit de sécurité ?

8-b. Un audit de sécurité permet d'évaluer le niveau de sécurité d'un périmètre donné. Ce niveau de sécurité sera fonction des failles de sécurité découvertes sur le périmètre évalué.

9) Qu'est ce qu'un Service Pack ?

9-a. Les Services Pack sont des mises à jour de sécurité englobant tous les correctifs parus. L'installation d'un Service Pack garantie un certain degré de correction d'une machine.

10) Qu'est ce qu'un exploit ?

10-b. Lorsqu'une vulnérabilité est publiée, il arrive que l'exploitation de la brèche soit programmée par des experts. La publication de leurs programmes permet l'exploitation massive des vulnérabilités ainsi codées, même par un utilisateur sans connaissances poussées en sécurité informatique.

11) Quel est l'outils indispensable à l'investigation suite à une suspicion de fraude ?

11-b. L'outil indispensable est le journal d'événements ou « logs ». C'est au sein de ces fichiers que toutes les traces et les preuves pourront être retrouvées. Quelques lignes de logs sont parfois suffisantes à prouver une tentative ou une intrusion.

12) Laquelle de ces réglementations impose que tous les accès et toutes les données relatives aux transactions soient loguées et archivées ?

12-a. Toutes les plateformes soumises à la réglementation Sarbanes-Oaxley doivent conserver les traces de transaction de « bout-en-bout ».

13) Qu'est ce que le social engineering ?

13-c. Le social engineering est une méthode non technique qui permet à un attaquant d'obtenir des informations sensibles en usurpant l'identité d'un interlocuteur légitime. Par exemple, il est courant de demander à un utilisateur son compte d'accès à un système, en se faisant passer pour un administrateur dudit système, en prétextant une maintenance obligatoire et urgente. Malheureusement, malgré les mises en garde, de nombreux utilisateurs se laissent encore abuser par ce genre de pratiques.

14) Qu'est ce qu'un cheval de Troie ? .

14-b. Un cheval de Troie est un programme qui donne a un attaquant distant un accès à une machine de manière furtive. Aujourd'hui la plupart de ces programmes intègre également un « Keylogger » permettant de voler les mots de passe de la victime.

15) Qu'est ce qu'un ver ?

15-b. Le ver est un petit programme qui se propage en exploitant une faille logicielle donnée. Son avantage par rapport à un virus est qu'il n'a pas besoin de l'intervention d'un utilisateur pour infecter une machine. Il suffit qu'elle soit vulnérable à la faille exploitée. Sasser constitue un exemple de ver connu (diffusion avril 2004).

16) Qu'est ce qu'une preuve de concept ?

16-c. Une preuve de concept est la démonstration qu'une vulnérabilité est effectivement exploitable. Dans la pratique cette démonstration est souvent menée par un petit programme passant des paramètres judicieusement choisis à l'application incriminée. Ce programme n'est pas malveillant car il ne comporte pas de charge utile.

17) Qu'est ce qu'un Spyware ?

17-b. Un « spyware » est (contraction de "spy" espion et "ware" éléments d'une même famille) un programme qui récupère des informations sensibles (frappes du clavier, des fichiers spécifiques, etc…) à l'insue d'un utilisateur, d'une machine infectée généralement à des fins commerciales.

18) Quelle est la dernière faille ou le dernier virus qui a alerté votre service ?

18-a. La faille PowerPoint est la plus récente et touche la majeure partie des entreprises. Si vous n'êtes pas au courant de cette faille, il est temps de vous inscrire à la mailling liste de notre service de veille !

19) L'utilité du logiciel Nmap est : ?

19-a. Nmap est un scanner de port puissant conçu pour détecter les ports ouverts, les services hébergés et les informations sur l'équipement audité. Cet outil est donc très utilisé par les administrateurs réseaux afin de connaître les points d'entrée et de sortie des flux réseau.

20) Quelle est la fonction la plus sécurisée en langage C ?

20-b. Ces deux fonctions de copies permettent de copier une chaîne de caractères dans une autre. Toutefois, la première solution présente le risque de déborder du nombre de caractères (et donc de réaliser des débordements de tampon). Une meilleure solution consiste à utiliser StrNCopy, qui fait la même chose mais avec une limite sur le nombre de caractères à copier.

Quel est votre niveau?

1 à 6 bonne(s) réponse(s) :
Etes vous réellement dans le service sécurité de votre entreprise ou avez-vous trouvez cette newsletter par hasard ? Plus sérieusement, il est tant de se mettre à jour, la sécurité est une évolution perpétuelle des technologies et les types attaques évoluent constamment. Il est indispensable de suivre chaque jour les nouvelles vulnérabilités et de rester informé par votre service de veille.

6 à 12 bonnes réponses :
Vos connaissances sur la sécurité informatique sont bien réelles. Malgré cela, la technique n'est peut être pas votre fort. Nous vous recommandons de télécharger et de lire attentivement nos newsletters afin de devenir un véritable expert !

12 à 18 bonnes réponses :
Vous êtes un responsable assidu et complet. Vous avez certaines connaissances dans le domaine technique et vous maîtriser sans doute l'ensemble des problématiques du piratage et de la sécurité informatique. Malgré tout, ne vous réjouissez pas trop vite ! Si vous espérez devenir un vrai RSSI, il vous faudra travailler certains points ou relire votre politique de sécurité !

19 à 20 bonnes réponses :
Bravo, vous avez passé ce test avec succès. Vous excellez dans tous les domaines ! Nous aimerions vous dire que vous n'avez plus besoin de nos services et que vous maîtrisez l'ensemble de la sécurité informatique de votre système d'informations....mais cela est faux. Il est bien entendu indispensable de travailler avec un partenaire dont tous le personnel obtient 20/20 à ce test (y compris notre directeur commercial !).

5. OUTILS LIBRES :

FOCUS SUR 5 PRODUITS LIBRES

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

Ce mois-ci, nous avons choisi d'analyser les logiciels suivants :

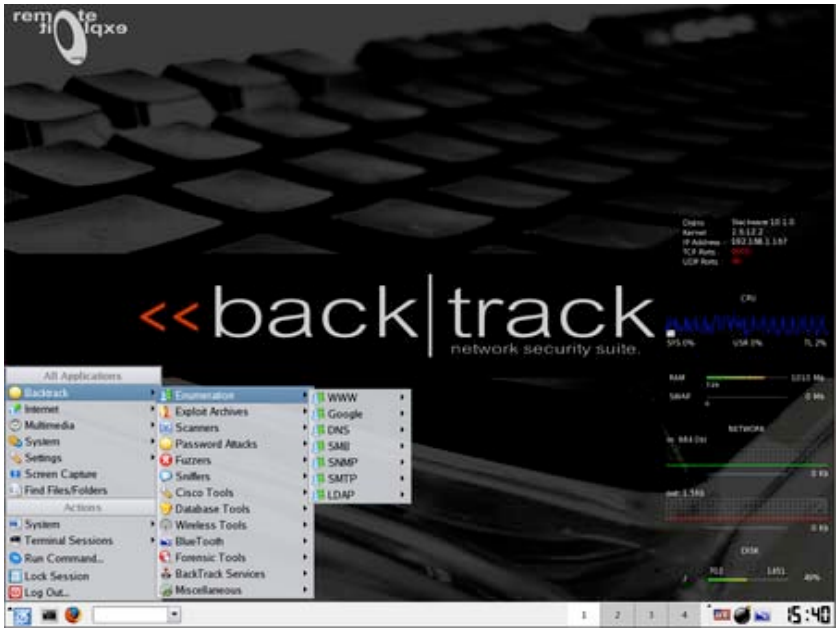
- *Back-Track : Distribution linux possedant de nombreux outils d'audit de sécurité*
- *MBSA : Outil de Microsoft permettant d'évaluer le niveau de correction d'une plateforme Windows*
- *Ps-Exec : Outil d'exécution de commandes à distance*
- *Helios, outil anti rootkits*
- *Opera : Navigateur web*

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

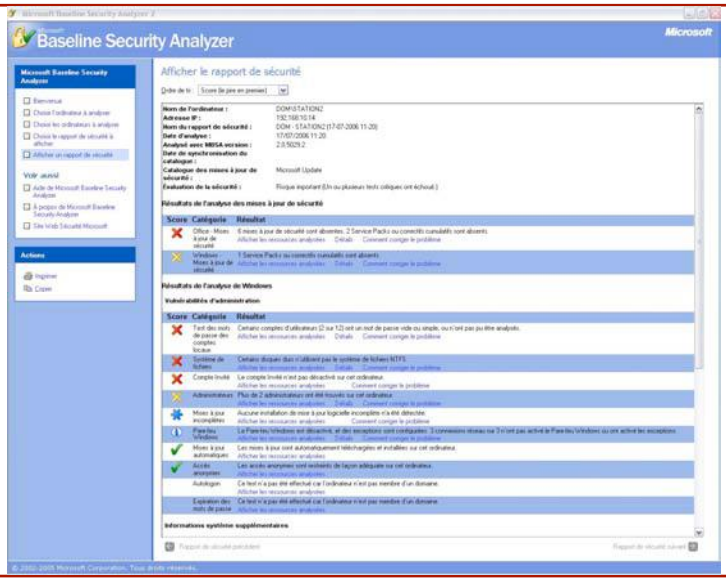
Back-Track

Distribution Linux

Version actuelle	backtrack-beta-05022006
Utilité	★★★☆☆
Type	Système d'exploitation
Description	Back Track est une distribution Linux dédiée aux consultants en sécurité et aux administrateurs système. Cet OS, disponible sous forme de Live CD inclut tous les logiciels utiles afin de tester la solidité des applications. Facile à utiliser puisqu'aucune installation n'est requise, Back Track est basée sur une distribution Slackware et est devenue la fusion de deux compilations Live-CD : Auditor et Whax. Des outils de hacking (Wifi, applications web, analyseurs de flux réseaux, bluetooth, cracker de mots de passe, forensics…), tous les utilitaires préférés des pirates seront désormais à votre portée pour sécuriser et tester vos infrastructures.
Capture d'écran	
Téléchargement	Back Track est proposée sous forme de Live CD, bootable directement sans installation préalable, à l'adresse suivante : http://mirror.switch.ch/ftp/mirror/backtrack/backtrack-beta-05022006.iso
Sécurité de l'outil	Basée sur une distribution Slackware, Back track, qui utilise les mêmes paquets que sa petite sœur, doit souffrir des mêmes problèmes.
Avis XMCO	Ce genre de distribution méconnue du grand public reste réservée aux experts. Back Track contient des programmes pratiques mais qui requièrent une connaissance particulière pour ce type d'outils.

MBSA

Outil Sécurité

Version actuelle	MBSA.2.0
Utilité	
Type	Outils d'analyse sécurité de machines Windows
Description	Mbsa est un outil chargé d'effectuer un scan rapide des différents problèmes majeurs de sécurité au sein d'une machine Windows. Créé par Microsoft, cet outil est doté d'une interface simple et permet, à partir d'une adresse IP ou d'un nom de machine, d'établir le degré de sécurité de n'importe quel poste du réseau.
Capture d'écran	
Téléchargement	Mbsa est disponible gratuitement sur le site de Microsoft à l'adresse suivante : http://www.microsoft.com/technet/security/tools/mbsahome.mspx
Sécurité de l'outil	Aucune faille n'a été la première publication du logiciel.
Avis XMCO	Cet outil est un excellent programme qui permet de savoir rapidement si les machines du réseau local sont correctement patchées et si elles correspondent au degré de sécurité imposé par la politique de l'entreprise.

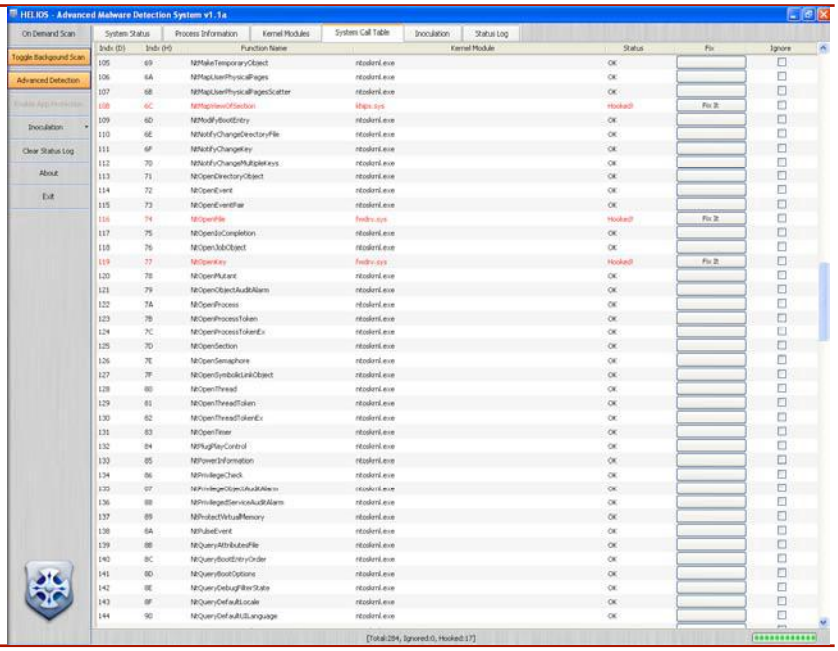
Ps-Exec

Exécution de programme à distance

Version actuelle	Ps-exec
Utilité	
Type	Programme similaire à Telnet
Description	PsExec est un programme produit par la société SysInternal. Il permet de lancer des commandes à distance sans avoir à installer d'agent ou de client sur le poste cible. Ainsi, en connaissant le nom d'utilisateur de le mot de passe administrateur de la machine distante, il est possible d'obtenir des informations, de lancer des commandes, de copier des fichiers… A savoir toute l'information nécessaire pour administrer n'importe quel poste du réseau en ligne de commandes.
Capture d'écran	
Téléchargement	Ps-Exec est disponible sur le site de SysInternals à l'adresse suivante : http://www.sysinternals.com/Utilities/PsExec.html
Sécurité de l'outil	Aucune faille de sécurité n'a été publiée.
Avis XMCO	Cet outil est très utilisé par les administrateurs. Aucun agent ne doit être installé sur l'hôte distant ce qui facilite considérablement son déploiement et son utilisation.

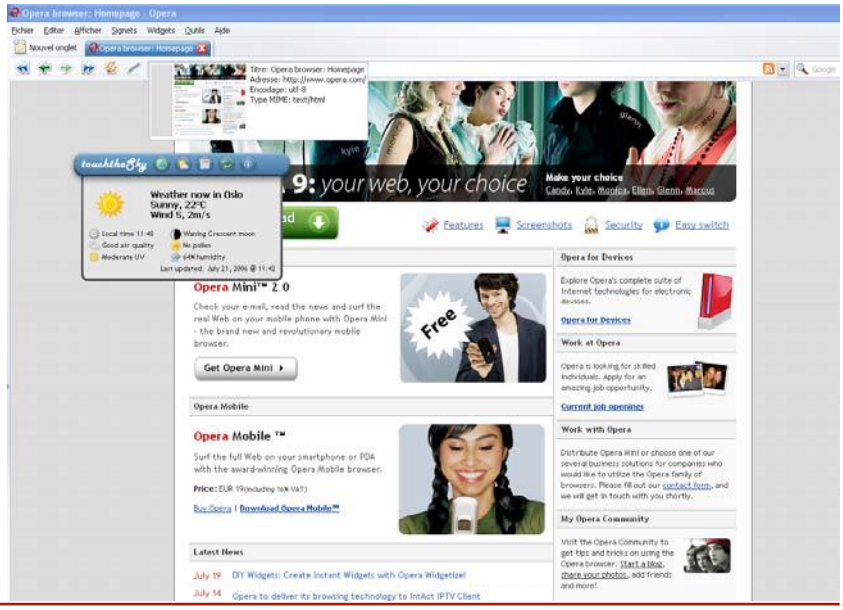
Helios

Protection anti-rootkit sous Windows

Version actuelle	Helios v1.1a
Utilité	★★★★☆
Type	Logiciel anti-malware
Description	Helios est un outil de protection et de détection des applications malveillantes simple et efficace. Ce logiciel permet de lister tous les processus et les modules utilisés par le système. Il dispose également d'une fonctionnalité qui permet de détecter si les appels aux fonctions systèmes ont été détournés (Hooking) et le cas échéant de les restaurer. Le site de l'éditeur dispose d'une documentation riche ainsi quelques vidéos de démonstrations.
Capture d'écran	
Téléchargement	Helios pour Windows : http://helios.miel-labs.com/downloads/Helios.zip
Sécurité de l'outil	Aucune faille de sécurité n'a été publiée.
Avis XMCO	Helios est un outil libre incontournable pour tout administrateur Windows. Ce logiciel ne nécessite aucune installation et peut tenir sur une disquette (taille inférieur à 1 Mo). Il permet de scanner arbitrairement tout système avec précision.

Opera

Navigateur Internet

Version actuelle	Opéra 9.0
Type	Navigateur Internet
Utilité	★★★★☆
Description	La dernière version de ce navigateur apporte son lot de nouveautés. Celui-ci opte pour le confort de navigation de l'utilisateur. L'ajout de "widget", petites applications Web (multimédia, échanges de news, etc.) apporte un avantage incontestable sur ses concurrents. Tandis que, cerise sur le gâteau, la gestion des onglets, présente sous Firefox et Internet Explorer 7 béta, se démarque par la visualisation d'un aperçu de la page lors du passage de la souris. Enfin, de nombreuses fonctionnalités sont incluses comme la gestion des téléchargements et la prise en charge du protocole BitTorrent sans application tierce pour les fichiers volumineux.
Capture d'écran	
Téléchargement	Opera pour Windows : http://www.opera.com/download/
Sécurité de l'outil	Comme tout navigateur, les versions précédentes de Opera comportaient de nombreuses vulnérabilités découvertes chaque mois. Cependant, cette nouvelle version, plus sécurisée, ne souffre d'aucune vulnérabilité à ce jour.
Avis XMCO	La dernière version du navigateur Opera est une véritable avancée en matière de confort de navigation. Ce navigateur se distingue de ses concurrents (Internet Explorer et FireFox) par des fonctionnalités intéressantes. De plus, une version "mini" est disponible gratuitement afin de pouvoir profiter de cet outil sur nos téléphones portables. Que demandez de plus ?

Suivi des versions

Version actuelle des outils libres présentés dans les numéros précédents.

Nom	Dernière version	Date	Lien
Debian Sarge	Version stable 3.1 r2	19/04/2006	http://www.debian.org/CD/netinst/
Snort	2.6.0	06/06/2006	http://www.snort.org/dl/
MySQL	5.0.22		http://dev.mysql.com/downloads/mysql/5.0.html
	5.1.11-Bêta		http://dev.mysql.com/downloads/mysql/5.1.html
Apache	2.2.2		http://www.apachefrance.com/Telechargement/4/
	1.3.36		http://www.apachefrance.com/Telechargement/4/
Nmap	4.11	01/04/2005	http://www.insecure.org/nmap/download.html
Firefox	1.5.0.4	06/2006	http://www.mozilla-europe.org/fr/products/firefox/
Thunderbird	1.5.0.4	06/2006	http://www.mozilla-europe.org/fr/products/thunderbird/
Spamassassin	3.1.3	25/05/2006	http://spamassassin.apache.org/downloads.cgi?update=200603111700
Putty	0.58		http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
ClamAV	0.88.3	01/07/2006	http://www.clamav.net/stable.php#pagestart
Ubuntu	6.06 Drapper Drake	06/2006	http://www.ubuntu-fr.org/telechargement
Postfix	2.3	06/06/2006	ftp://ftp.club-internet.fr/pub/mirrors/ftp.porcupine.org/postfix-release/index.html
Squid	2.6	29/05/2006	http://www.squid-cache.org/Versions/v2/2.5/
Filezilla	2.2.25		http://filezilla.sourceforge.net/
OpenSSH	4.3	01/02/2006	http://www.openssh.com/
Search and Destroy	1.4		http://www.safer-networking.org/fr/download/index.html
ARPWatch			ftp://ftp.ee.lbl.gov/arpwatch.tar.gz
GnuPG	1.4.4	06/2006	http://www.gnupg.org/(fr)/download/
BartPE	3.1.10a	6/10/2003	http://severinterrier.free.fr/Boot/PE-Builder/
TrueCrypt	4.2a		http://www.truecrypt.org/downloads.php