L'Actu Sécurité n°7

xmco Partners

PLAN

"Une rentrée agitée"

Bonjour.

Wi-Fi, Wi-Max, VoIP, ... Les nouvelles technologies occupent les devants de la scène dans ce septième numéro. Les menaces ne sont pas pour autant mises à l'écart, puisque de nombreuses vulnérabilités sur le fameux Internet Explorer ont été découvertes. Deux d'entre elles, d'ailleurs, sont largement exploitées sur Internet alors qu'aucun correctif n'est actuellement disponible...

En bref, nous vivons une rentrée mouvementée comme beaucoup de clients du marché. Traditionnellement, les quatre derniers mois de l'année représentent un vrai challenge pour beaucoup d'entre nous : les projets se sont accumulés, les planning se resserrent, les objectifs se rapprochent...

J'observe ce comportement depuis des années. Toutefois, une nouvelle tendance semble voir le jour dans le domaine de la sécurité : de plus en plus de clients s'organisent pour répartir leurs missions tout au long de l'année et pour échapper au traditionnel audit de fin d'année.

C'est à nous, cabinets de conseil, SSII, "vendeurs de viande", et autres offreurs de services de leur permettre de relever ce challenge éprouvant : faire un peu de sécurité, partout, tout le temps... Je fais partie de ceux, dans le débat de la poule et de l'oeuf, qui clament que nos offres de service peuvent aussi orienter le marché vers une plus grande maturité, vers une responsabilité mieux assumée et une gestion saine des enjeux de sécurité auquel les entreprises doivent faire face.

A cet effet, vous trouverez dans ce numéro le premier article d'une longue série : les cahiers de l'OWASP. L'OWASP est une méthodologie qui précise les bonnes pratiques en matière de sécurisation des applications Web. Notre cabinet a décidé de traduire cette méthodologie, et de présenter un chapitre par numéro. "La sécurisation des paiements en ligne" sera le premier sujet traité.

Enfin, vous trouverez une nouvelle rubrique au sein de notre newsletter : une tribune libre. Nous vous offrons la possibilité de vous exprimer, sur le sujet de votre choix (le thème de la sécurité n'est absolument pas impératif), sans aucune censure.
Pourquoi ? Tout simplement parce que nous avons tous une vie en dehors du boulot, et qu'il est agréable d'ouvrir nos horizons respectifs.
La seule contrainte imposée pour les souscriptions est de respecter notre indépendance : cette tribune ne doit pas constituer une publicité déguisée.

Je vous souhaite une bonne lecture !

Marc Behar

1. LES CAHIERS DE L'OWASP

LES PAIEMENTS SECURISES

Dans cette nouvelle rubrique, nous étudierons un des sujets présentés dans le guide OWASP (The Open Web Application Security Project). L'OWASP est un guide qui présente les points majeurs à respecter afin de renforcer la sécurité des applications.

Pour cette première étude, nous avons choisi de synthétiser pour vous le chapitre consacré aux paiements en ligne et au standard PCI DSS. Cet article s'adresse aux développeurs et aux responsables qui risquent de mettre en place des systèmes de paiements en ligne.

XMCO | Partners

OWASP

The Open Web Application Security Project

Les données bancaires sur Internet

Les paiements en ligne

Le commerce électronique est en plein essor. Les internautes utilisent de plus en plus les paiements en ligne pour toutes sortes d'achats. En mai 2005, les ventes en ligne avaient déjà augmentées de 53% par rapport à 2004.

Dans un tel contexte, la question du paiement sur Internet est primordiale à la fois pour l'acheteur et le vendeur. D'une part, le consommateur a besoin d'être rassuré face à l'usage d'outils informatiques et des techniques qu'il ne maîtrise pas forcément. D'autre part, le professionnel a besoin de solutions de paiement efficaces, rapides et fiables permettant au consommateur de réaliser, de la manière la plus fluide possible son acte d'achat.
Ainsi les internautes jugent la sécurité des achats en ligne insuffisante et 32% des français estiment que la sécurité des échanges bancaires n'est pas assurée.

La gestion des paiements sécurisés

La gestion des paiements en ligne est un point critique et constitue, ainsi, une pièce maîtresse des achats via Internet.
D'un côté, la plupart des clients font confiance au logo HTTPS en bas de leur navigateur et ne se soucient pas du fait que leurs données bancaires sont courtisées par les pirates.

De l'autre coté, sans le savoir, des entreprises ne respectent pas les règles et les bonnes pratiques pour assurer la confidentialité des données bancaires de leurs clients.

La sécurité des sites d'achats en ligne et, en particulier, la gestion des données critiques représente donc un enjeu crucial qui ne doit pas être négligé par les développeurs et les responsables Sécurité.

Le développement sécurisé des applications e-commerce

Le standard PCI DSS : Payment Card Industry Data Security Standard

Le PCI DSS est le standard industriel pour le traitement sécurisé des paiements par carte de crédit sur les sites web. Le PCI est maintenu par un consortium d'entreprises comme VISA, Mastercard ou encore American Express.

VISA MasterCard AMERICAN EXPRESS

Voici les 12 grands chantiers du PCI :

Objectifs	Actions
Construire et maintenir une infrastructure sécurisée	1. Installez et maintenez un firewall pour protéger vos données. 2. N'utilisez pas les mots de passe par défaut fournis avec les équipements et les logiciels.
Protéger les données du propriétaire de la carte.	3. Protégez les données stockées. 4. Toutes les transmissions contenant des données bancaires sur des réseaux publics (Internet, X25, ..) doivent impérativement être correctement chiffrées (VPN, SSL).
Maintenir un processus de gestion des vulnérabilités	5. Utilisez et maintenez vos antivirus à jour. 6. Développez et maintenez la sécurité de vos systèmes et de vos applications (appliquez les correctifs de sécurité).
Implémenter des mesures strictes en termes de contrôles d'accès	7. Restreignez l'accès aux seules données dont l'utilisateur a besoin ('business need-to-know'). 8. Chaque utilisateur doit posséder un identifiant unique. 9. Restreignez l'accès physique aux serveurs contenant des données sur les cartes bancaires des clients.
Surveiller et tester le système d'information	10. Surveillez et stockez les événements d'accès aux ressources et aux données bancaires des clients (Conservation et analyse de logs). 11. Testez régulièrement la sécurité de vos systèmes et de vos processus par des audits de sécurité.
Maintenir une politique de sécurité.	12. Assurez le maintien et la communication de la politique de sécurité pour tous les collaborateurs.

Les Meilleures Pratiques

D'autres mesures sont à adopter afin d'assurer la sécurité de telles applications. L'OWASP conseille de respecter les point suivants :

- Traitez les transactions immédiatement sur le site ou externalisez cette tâche auprès de votre banque.

- Ne stockez jamais les numéros de carte de crédit. Si ces numéros doivent être stockés, vous devez absolument suivre à la lettres les recommandations de votre PCI. Nous recommandons fortement de ne pas stocker des informations sur les cartes de crédit.

- Vous ne devez en aucun cas stocker les codes CCV, CCV2, PVV et le code PIN. Ces codes constituent des champs de validation utilisés par les systèmes bancaires pour protéger vos paiements et contrôler la validité de la carte. [Ce sont en quelques sortes les mots de passe de la carte, ndlr]. Le stockage de ces données est strictement interdit par le PCI.

Les codes de confirmation

Après chaque transaction correctement validée, un code de confirmation est retourné. Ce code est unique pour chaque transaction et ne possède pas de valeur intrinsèque. Il est important de conserver ce code, de l'écrire dans les logs, de le conserver pour le BackOffice et de l'envoyer par courriel au client.

Gérer les paiements récurrents

La seule raison commerciale de conserver les numéros de carte de crédit réside dans la gestion des paiements récurrents. Cependant, vous avez plusieurs responsabilités importantes au regard de ce mode paiement :

- Vous devez vous soumettre aux réglementations commerciales. La réglementation impose que vous conserviez une autorisation signée du possesseur de la carte de crédit. Ce morceau de papier sera d'une grande aide en cas de désaccord ou de conflit avec le client.

- Vous devez chiffrer obligatoirement les numéros de carte de crédit. Ceci est imposé par votre PCI et les meilleurs pratiques le conseillent.

- Vous devez limiter les paiements récurrents à une période d'un an maximum et ce, particulièrement lorsque le propriétaire de la carte n'est pas physiquement présent lors des transactions (ce qui est quasiment toujours le cas avec le commerce en ligne).

- Enfin il est impératif d'effacer toutes les données relatives à la carte de crédit dès que la période de paiement récurrent est terminée.

Le problème du chiffrement réside dans le fait que vous devez être capable de déchiffrer les données au moment opportun. Lors du choix de la méthode de chiffrement (3DES, RSA, AES, DEA,…) et de stockage, gardez en mémoire le fait que le serveur web frontal n'a pas besoin et ne doit pas être capable de déchiffrer ces données.

Les remboursements et les virements créditeurs

Il est possible de prendre quelques mesures simples pour réduire le risque associé à la gestion des remboursements :

- L'argent ne peut pas être négatif. Renforcez vos logiciels pour n'accepter que des valeurs positives ou nulles afin de prévenir l'utilisation de nombres négatifs.

- Tous les remboursements et les virements sur le compte d'un client doivent être tracées, auditées et confirmées par une autorisation manuelle.

- Votre site ne doit en aucun cas posséder des interfaces ou des fonctions permettant de créditer un compte client ou d'y effectuer des remboursements.

- N'envoyez pas la marchandise avant d'avoir reçu l'autorisation de votre passerelle de paiement (ou de votre banque).

- La grande majorité des numéros de cartes de crédit possède un lien entre le code banque (BIN) et le pays d'origine de la banque émettrice de la carte. Réfléchissez à ne pas envoyer des marchandises payées avec une carte étrangère ou provenant de pays « douteux ».

- Pour les paiements de grande valeur, préférez un paiement par téléphone avec une confirmation par fax.

Des clients vont essayer de se faire créditer leur compte trop souvent. Gardez un œil sur les clients qui demandent des remboursements et décidez s'ils présentent un risque trop élevé ou non.
Demandez toujours l'adresse email et le numéro de téléphone du client enregistré à la banque.

Dernier conseil

Faites savoir sur votre site que vous poursuivez en justice toutes les tentatives de fraudes (conformément à l'article L.323 du code pénal français, ndlr) et que toutes les transactions sont enregistrées.

Bibliographie

Payment Card Industry (PCI) Data Security Standard
https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

3. ETAT DE L'ART

WIFI &WIMAX

Les technologies sans fil se fondent petit à petit dans les systèmes d'information des entreprises.

Quelles en sont les applications actuelles ?
Quelles sont les perspectives futures ?
Quant est-il de la sécurité ?

XMCO | Partners

Adoption des technologies sans fil
Les projets et les applications en cours

Les technologies sans fil sont de plus en plus adoptées dans le milieu professionnel. La flexibilité de ces réseaux semble séduire un grand nombre d'entreprises. Les points d'accès aux réseaux sans fil s'installent en complément du système d'information de l'entreprise et garantissent la mobilité au sein de ses locaux. En effet, les salariés peuvent se connecter à partir des salles de réunion, des halls d'entrée ou encore de la cafétéria… Ces nouveaux dispositifs fournissent une fluidité d'accès aux informations à moindre coût.

Les progrès en terme de sécurité des réseaux Wifi y sont pour beaucoup car la facilité d'intrusion d'un réseau sans fil était le principal obstacle à son déploiement en milieu professionnel. De plus, une certaine maturité de ces technologies sans fil, permet une meilleure appréciation du danger qu'elles peuvent représenter. Leurs implémentations ont d'ailleurs lieu principalement au sein de DMZ ou autres Vlans isolés.

Le Wimax est une technologie relativement jeune. Les équipements en sont au stade embryonnaire. En effet, ils sont peu nombreux et très onéreux. Alors que cette technologie permet trois types d'utilisation (Boucle Locale Radio, Nomadisme et Mobilité), seule la BLR est exploitée significativement à ce jour.
En effet, les fournisseurs d'accès à Internet utilisent ce moyen afin de couvrir certaines régions rurales où l'acheminement de câbles n'était pas économiquement viable.

Standards et normes
Où en est-on ?

Actuellement, il existe trois normes pour le Wimax, 802.16a, 802.16d et 802.16e. Elles définissent respectivement l'utilisation du Wimax en Boucle Locale Radio, le Wimax Nomade (hotspot) et enfin le Wimax Mobile. L'évolution de la norme 802.16x a été motivée par le désir d'obtenir de la mobilité. Par exemple, la fonctionnalité de « roaming » est la principale différence entre 802.16d et 802.16e.

Du côté du Wifi, l'évolution est différente. Les principales avancées concernaient le débit et la sécurité. En effet, il a fallu rassurer l'utilisateur, après la découverte de nombreuses failles de sécurité au sein des mécanismes de protection des réseaux WIFI. Parmi les différentes évolutions, nous pouvons identifier 802.11a/b/g ou encore 802.11i et le très récent 802.11n (MIMO). La principale différence entre les versions a/b/g était le débit de transfert des données. La norme 802.11i a apporté la protection WPA2 qui garantit aujourd'hui un niveau de sécurité acceptable pour les réseaux WIFI. Enfin, le 802.11n propose un débit de transfert et une portée bien supérieur s(540Mb théorique et 50m au lieu de 30).

Et la sécurité ?

Le Wifi utilise la norme 802.1x pour l'authentification et la gestion des clefs de chiffrement. Il se base sur l'algorithme AES pour assurer la confidentialité des données.
Contrairement au WEP, où le réseau était vu comme un HUB, la norme 802.11i (WPA2) attribue une clef de session unique et temporaire à chaque machine. De ce fait, une machine ne peut voir « en clair » que les données qui lui sont destinées.

Le chiffrement des données et des clefs d'authentification du Wimax est basé respectivement sur les algorithmes AES (chiffrement symétrique) et RSA (chiffrement asymétrique). Des algorithmes qui ont fait leurs preuves et dont la mise en œuvre est recommandée par la DCSSI.

Cependant, la solidité des algorithmes de chiffrement repose sur des limites mathématiques, par exemple la factorisation de grands nombres premiers, etc…

La robustesse de ces algorithmes est donc relative. Que se passerait-il si de nouvelles méthodes arithmétiques ou de nouveaux moyens techniques voyaient le jour ?

De nombreux chercheurs affirment que ces cryptosystèmes seront tous impuissants face aux capacités de l'ordinateur quantique. D'ailleurs un algorithme qui permet de casser AES et destiné aux ordinateurs quantiques a déjà été publié.

Le Wimax est une technologie très jeune et nous ne lui connaissons que très peu de faille. Cependant, une analyse purement théorique du processus d'initialisation permet de mettre en évidence une faille de conception. En effet, lors de l'authentification, le client s'identifie auprès des stations BS de l'opérateur mais celles-ci ne s'identifient pas, à leur tour, auprès du client. Cette erreur de conception pourrait être exploitée par un attaquant afin de mener une attaque de type man-in-the-middle.

D'autre part, des attaques de type déni de service pourraient être menées à l'encontre de réseaux Wimax. En effet, cette technologie est basée sur les ondes radio et comme toute les technologies sans fil, elle émet sur la même bande passante de fréquence. Il est possible de paralyser le réseau.

D'un point de vue général, la sécurité du Wimax et les nouvelles normes Wifi, semblent satisfaisantes. Ces nouvelles technologies ne sont ni plus ni moins qu'un socle sur lequel seront implémentés des réseaux IP et plusieurs briques applicatives. De ce fait, toutes les failles traditionnelles et particulièrement, celles des applications et des services, Web resteront exploitables.

Les perspectives d'avenir

Evolution de ces technologies et les déploiements futurs

Dans un premier temps, les technologies Wimax et Wifi devraient être utilisées conjointement pour offrir plus de granularité. Les fournisseurs d'accès devraient continuer à s'équiper de manière à proposer des offres intéressantes aux habitants de zones rurales et enclavées. Ensuite, nous devrions voir apparaître les premiers « Hotspots » Wimax dans les grandes agglomérations, sur les aires de repos d'autoroutes, les aéroports, etc…

Dans un second temps, l'exploitation du Wimax Mobile devrait inciter l'utilisation de terminaux mobiles Wimax (certains constructeurs en proposent déjà). La vraie révolution de l'utilisation d'Internet se situe ici. La possibilité de se connecter de n'importe où à haut débit et à moindre coût devrait changer radicalement nos habitudes. De nombreux services devraient accompagner ce nouveau support de connectivité à la Toile.

L'exploitation du Wimax Mobile en France, en revanche, ne devrait apparaître que bien après car :

- Le coût de revient pour une couverture acceptable du territoire en Wimax Mobile est excessif (même si celui-ci est moins élevé que le coût de la 3G).
- Les licences Wimax, délivrées par l'Arcep, interdisent, pour l'instant, l'exploitation du Wimax Mobile.

Cependant, l'utilisation du Wimax Mobile devrait tôt ou tard être autorisée sur le territoire français au risque d'accuser un sérieux retard par rapport à nos voisins européens ou même par rapport à l'Asie. En effet, des projets de déploiement du Wimax Mobile sont déjà prévus pour l'année 2008 en Corée du Sud. Cette technologie devrait assurer une qualité de service convenable aussi bien pour la voix que les données. De ce fait elle se positionne comme une concurrente directe à la 3G et de son évolution HSDPA (3,5G ou 3G+). Ce changement devrait se traduire par l'apparition de nombreux services permettant d'exploiter pleinement cette nouvelle flexibilité de la connexion à Internet.

Les technologies sans fil et leurs concurrents

WIRELESS vs CPL

Le CPL ou "Courants Porteur en Ligne" est une nouvelle technologie qui utilise les lignes électriques afin de faire passer l'information à bas ou haut débit.

Le principal avantage du CPL face au Wifi et au Wimax est sa simplicité de déploiement quelque soit l'environnement. En effet, les technologies sans-fil sont très sensibles aux obstacles alors que le courant porteur se base sur le réseau électrique existant. Cependant, le CPL ne doit pas être un concurrent des technologies sans-fil mais un complément. Cette technologie peu, par exemple, servir à relier deux réseaux sans fil ou bien étendre le réseau sans câblage dans un lieu peu propice à la propagation des ondes radio.

3. DOSSIER SPECIAL : VOIX SUR IP

LES RISQUES LIES AU DEPLOIEMENT DES LA VoIP.

La course à la réduction des coûts d'une entreprise implique bien souvent la migration du service de téléphonie vers la Voix sur IP. Ce choix séduit par le retour sur investissements des communications. Cependant de nombreux paramètres sont bien souvent oubliés ou ignorés.

Avant de franchir le pas, il est nécessaire d'étudier les nouvelles contraintes engendrées.

Mis à part la surcharge du réseau de l'entreprise et la migration de nombreux équipements, la confidentialité des communications et l'efficacité des plans de secours sont remis en cause.
La convergence numérique va introduire de nouveaux services et par conséquent, de nouvelles vulnérabilités et de nouveaux vecteurs d'attaques.

XMCO | Partners

Les problématiques de l'implémentation VoIP

De nouvelles vulnérabilités

La Voix sur IP est une des technologies phares du moment. Téléphoner depuis un accès Internet vers n'importe quel point du globe à des coûts dérisoires envahit les rêves de tous les gestionnaires d'entreprises. Ce type d'architecture est donc implémenté afin d'aider l'entreprise à maîtriser ses coûts de production et non pour l'évolution technique.

Une fois de plus, l'investissement en matière de sécurité découle d'un compromis entre les besoins réels et les risques acceptables. La migration vers un réseau « Full IP » va donc altérer la sécurité que les administrateurs ont mis tant d'ardeur à mettre en place. Entre l'ajout de téléphones IP, de « softphone » et d'applications liées à cette nouvelle infrastructure, la charge du réseau devient beaucoup plus importante et sa disponibilité est remise en question.

La convergence numérique permet d'offrir de nouveaux services comme la messagerie unifiée. Le paradigme de l'informatique revient au devant de la scène : plus un système offre de services et plus celui-ci est vulnérable.

Les conséquences

Aujourd'hui le réseau téléphonique historique est fiable, disponible et performant. Même en cas de coupure de courant, le téléphone est opérationnel car l'alimentation électrique est acheminée par l'opérateur. L'atteinte à la confidentialité et à l'intégrité des communications demande des moyens ou des connaissances de haut niveau.

La migration vers un service de VoIP implique de nou veaux risques. Il faut noter que toutes les protections fournies par la téléphonie classique ne sont pas intégrées dans les fondements de cette nouvelle technologie. Ainsi, les attaques sont beaucoup plus faciles à exploiter et ne demandent pas toujours d'équipement spécifique.
Les contraintes de confidentialité de certaines communications ne sont plus assurées par défaut et la disponibilité du réseau de l'entreprise devient également un élément critique afin d'assurer un service minimum en cas de crise.

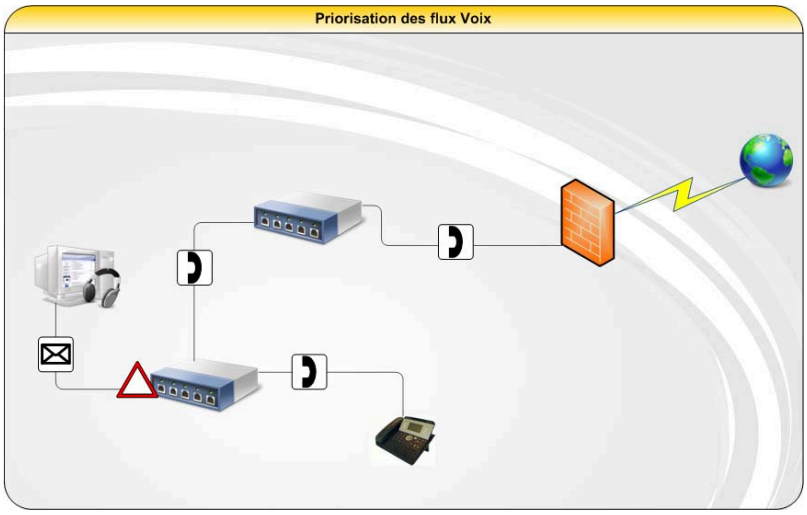
Avant de commencer la migration il est indispensable de revoir tous les plans de secours et de reprise d'activité. En effet, il faut assurer le cheminement des communications mais surtout la disponibilité des équipements téléphoniques en cas de congestion du réseau ou de panne électrique ; sans oublier de prioriser les appels d'urgence par rapport aux autres paquets IP.

Les contre-mesures

Le risque électrique peut être diminué par l'implémentation de la norme 802.3af [1] qui permet d'alimenter des équipements via le câble Ethernet. Cette mesure nécessite cependant un surcoût pour une entreprise qui ne possédent pas d'équipements réseaux compatibles. Il est ainsi indispensable d'assurer l'alimentation des éléments du cœur de réseau (ajout d'onduleurs, de groupes électrogènes…).

La confidentialité des échanges et l'authentification des destinataires est assurée par l'utilisation de la cryptographie.

Le besoin de disponibilité peut être garanti par des protocoles de gestion de la Qualité de Service au sein des différentes couches OSI. Le but de cette opération est de priser le trafic de la Voix dont le temps de latence est critique face au trafic des données.



Priorité d'un appel VoIP sur les autres paquets.

Les attaques liées à la VoIP

Les attaques physiques

L'implémentation de la norme 802.3af ne présente pas uniquement des avantages. En effet, l'élément fournissant l'alimentation électrique devient un équipement critique de l'architecture et un maillon faible de la sécurité.

Ainsi, une personne malveillante disposant d'un accès à l'équipement ou à son interface d'administration, pourrait provoquer d'importants dommages. Les conséquences vont d'un simple déni de service via une coupure de son alimentation à la dégradation matérielle de tous les équipements connectés par la modification de l'intensité et du voltage du courant émis sans compter les différentes normes entre les pays (US, EU, UK,…).

Les attaques des couches réseaux

La disponibilité du réseau, la confidentialité des échanges et l'intégrité de l'architecture VoIP sont vulnérables à de multiples attaques. Le réseau « VOIX » d'une entreprise est exposé aux mêmes problèmes que le réseau dit « DATA » sauf qu'il faut inclure, en sus, des contraintes temporelles.

La téléphonie qui ne nécessite que peu de bande passante, requiert toutefois un débit constant. Cette contrainte rentre en contradiction avec la politique du protocole IP : « Best Effort » [2].

Une architecture VoIP est donc sensible aux attaques de type déni de service ou de congestion du réseau. Un pirate pourrait obtenir des résultats similaires en forgeant des paquets malicieux à l'encontre des protocoles utilisés. Ce type de malversations est très facile à implémenter et à automatiser.

L'écoute passive du réseau est critique du point de vue de la confidentialité des communications. Cette technique permet à un pirate d'intercepter l'intégralité des conversations mais aussi des informations sensibles comme des numéros de cartes de crédits ou des codes secrets composés sur le pavé numérique du téléphone.

Par ailleurs, il existe aussi des attaques portant atteinte à l'intégrité de l'architecture VoIP. Celles-ci consistent à usurper l'identité d'un utilisateur ou à agir au sein du processus de facturation afin d'effectuer des appels gratuits. Un attaquant peut également insérer des paquets arbitraires, au sein de communications, dans le but d'altérer le contenu des messages. Une fois de plus, les composants vulnérables sont les couches basses du modèle OSI.

Les attaques applicatives

La mise en place de services connexes à la VoIP induit de nouveaux vecteurs d'attaques. Ces nouvelles applications n'en sont qu'à leurs prémices et sont donc sujettes à la publication de failles futures.

Plutôt que d'imaginer une attaque complexe, basée sur les protocoles réseaux, un pirate pourrait obtenir aisément les mêmes résultats en s'attaquant directement aux applications telles que les « softphones » ou les messageries unifiées. Celles-ci étant hébergées sur des machines, la sécurité des systèmes d'exploitation devient un point d'entrée supplémentaire. Les interfaces de configuration distante des équipements du réseau doivent être prises en compte dans la gestion des risques. Basées sur des applications web, ces interfaces d'administration font régulièrement l'objet de correctifs lors de la découverte de vulnérabilités. La gestion des correctifs de toutes les applications et de tous les équipements de l'architecture VoIP implique donc de nouveaux coûts indirects et ajoutent un maillon faible dans la chaîne de la sécurité.

Il ne faut pas oublier les autres composants de l'architecture. En effet, de nombreux serveurs sont nécessaires au bon fonctionnement des équipements (DHCP, TFTP, DNS, Passerelles, …). L'utilisation de ces serveurs n'est pas sécurisée et un pirate pourrait aisément usurper l'identité d'une de ces machines. Par exemple, en usurpant le serveur TFTP, utilisé par les téléphones IP, afin de télécharger leur logiciel interne, un pirate pourrait modifier la configuration des téléphones IP ou altérer leur fonctionnement.

Réflexion

Il est vrai qu'une migration vers une architecture de VoIP semble alléchante. Cependant, il est indispensable d'analyser rigoureusement tous les risques encourus en fonction des contraintes métiers et des coûts d'administration ou de maintenance.

Bibliographie

[1] 802.3af
http://grouper.ieee.org/groups/802/3/af/

[2] Présentation du protocole IP
http://en.wikipedia.org/wiki/Internet_Protocol
http://www.ietf.org/rfc/rfc791.txt

4. ATTAQUES MAJEURES :

TOP 5 DU MOIS DE SEPTEMBRE

Après avoir eu un mois d'Août relativement calme (hormis les nombreux bulletins Microsoft pour les vulnérabilités identifiées en Juillet), le mois de Septembre a relancé l'activité virale et la découverte de vulnérabilités. Microsoft est de nouveau au centre des débats et la sécurité d'Internet Explorer aura, une fois de plus, été remise en cause avec la publication d'exploits critiques. Par ailleurs, des vers se sont propagées via plusieurs messageries instantanées.

Microsoft

Internet Explorer, PowerPoint et Word toujours aussi vulnérables.

Les trois logiciels préférés des pirates ont connus un mois de Septembre difficile. Plusieurs failles non corrigées ont été identifiées. Microsoft a donc publié des bulletin d'alerte afin de préconiser des solutions de contournements qui pourrait parer d'éventuelles attaques.

La première concerne le logiciel de traitement de texte Microsoft Word 2000. La faille provient d'une erreur inconnue et permet à un pirate d'exécuter du code arbitraire lors de l'ouverture d'un document Word judicieusement concu.
Son exploitation permettrait a un attaquant distant de compromettre un systeme vulnerable.
Cette vulnérabilité n'a toujours pas été corrigée, un mois après son identification…
Un cheval de Troie exploite actuellement ce problème et pourrait toucher un grand nombre de serveurs. [1]

PowerPoint a aussi été la cible d'une faille « zero-day ». Un troyen nommé «Trojan.PPDropper.E » et se présente sous la forme d'un document ".ppt". A l'ouverture de cette presentation contrefaite un cheval de Troie serait téléchargé et installé sur le poste cible.[2]

Interner Explorer ne finit pas d'être testé et piraté. Ce mois-ci trois failles critiques ont été identifiées mais seulement une seule a été corrigée (MS06-055). Chacune d'entre elles fait l'objet d'un débordement de tampon.

Le premier contrôle Active X vulnérable se nomme « daxctle.ocx ». L'origine de la faille serait une erreur présente dans le contrôle Active X « DirectAnimation Path » inclus dans le fichier daxctle.ocx. En passant un argument malformé à la fonction "CPathCtl::KeyFrame()", le pirate provoquerait un débordement de tampon et pourrait insérer le code qu'il souhaite exécuter sur la machine.[3]

Le deuxième faille critique concerne le langage VML utilisé par certains sites web afin d'insérer dans les pages Web des images vectorielles et d'en accélérer le chargement et l'affichage.
La faille résulte une erreur d'implémentation présente dans le fichier « Vgx.dll » utilisé, notamment, par Internet Explorer. Microsoft a rapidement publié un correctif (MS06-055) afin de limiter les risques. [4]

Enfin la dernière faille affecte le shell Windows mais est exposée via le contrôle Active X « WebViewFolderIcon ». En passant un argument malformé (0x7fffffff) à la méthode « setSlice », le pirate pourrait causer un déni de service ou exécuter du code arbitraire.

Chacune des failles présentées a été exploitée par des programmes malicieux publiés sur des sites spécialisés (MilW0rm, Metasploit) et permettaient de prendre le contrôle d'un poste vulnérable. [5]

Les failles corrigées

Après avoir corrigé près de 12 failles en Août (vulnérabilités identifiées en Juillet), le mois de Septembre aura été plutôt calme. En effet, peu de failles de sécurité ont été découverte en Août. Les bulletins mensuels de Microsoft auront donc été peu nombreux.

La première vulnérabilité (MS06-052) a été décelée et corrigée dans l'implémentation du protocole de multidiffusion PGM des systèmes d'exploitation Windows XP. Un attaquant distant était en mesure de compromettre une machine vulnérable en exploitant cette faille de sécurité. Le problème était lié à une mauvaise gestion de la mémoire par le service MSMQ (Microsoft Message Queuing). En envoyant un paquet multicast judicieuse

ment forgé, un attaquant pourrait exécuter du code arbitraire sur les machines cibles vulnérables.

La deuxième faille de sécurité concerne le service d'indexation (Indexing Service) implémenté sur toutes les plateformes Windows. Le problème résultait d'une mauvaise validation de certains paramètres des requêtes envoyées par le client. En incitant à visiter un site web malicieux, un client pouvait obtenir des informations sensibles et voler la session de la victime.

Une autre faille corrigée concerne le logiciel Publisher qui était vulnérable à un débordement de tampon lors de l'ouverture d'un fichier « .pub » spécialement conçu (chaîne de caractères malformée).

A l'heure où nous rédigeons cette newsletter, les vulnérabilités liées à Internet Explorer sont toujours exploitées. Une seule faille a été corrigée malgré la gravité de tous les problèmes qui affectent Internet Explorer. N'importe quel internaute pourrait simplement compromettre un système vulnérable en utilisant une preuve de concept diffusée sur Internet.

La faille "WebViewFolderIcon setSlice() » est, par exemple, exploitée par un simple script perl qui crée une page HTML malicieuse. En modifiant une seule ligne du fichier original, l'utilisateur qui visiterait la page malicieuse lancerait, sans le vouloir, l'exécution d'un fichier (cheval de Troie ou virus) hébergé sur un site web tiers.

Programmes vulnérables :

- [1] Microsoft Word 2000 / Microsoft Office 2000
- [2] Power Point 2000 /2002/2003/2004 pour Mac
- [3] Internet Explorer 5.01 SP4/6 SP1 sous Windows 2000 SP4 / Internet Explorer 6 SP1 pour toutes les plateformes
- [4] Internet Explorer

Criticité : Elevée

Référence Xmco :

- [1] n°1157444683, n°1158246765
- [2] n° 1159383235
- [3] n° 1158218855
- [4] n° 1158666689, n° 1158752454, n° 1158850686, n° 1159174636, n° 1159176757 et n° 1159349231
- [5]n°1159779319 et n° 1159779357

Virus

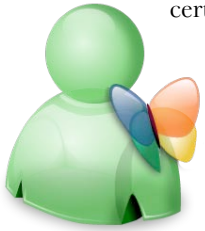
Les messageries instantanées MSN, AIM et Yahoo Messenger victimes de vers.

Les trois messageries instannées les plus utilisées ont été touchées, tour à tour, par des vers ravageurs. En effet, des programmes malicieux ont été développés afin de cibler les utilisateurs des logiciels MSN, AIM et Yahoo Messenger développées par les sociétés Microsoft, AOL et Yahoo.

Trois vers ont été identifiés entre le 20 et le 5 Octobre. Les virus ont été largement diffusés sur Internet et se propageaient via la liste des contacts de l'utilisateur abusé.

Le premier programme malicieux affecte MSN. Il envoie un lien via la messagerie instantanée de Microsoft (en anglais) comme les exemples suivants : Si la victime crédule suit cette adresse, un cheval de Troie est immédiatement téléchargé et exécuté sur le poste cible. Le lien est ensuite envoyé à tous les contacts MSN de la victime.
Les fichiers d'extension ".pif" sont normalement bloqués par Microsoft cependant il suffit de changer la casse ou d'encoder l'extension ".pif" afin de berner le logiciel.

Les liens vers les sites web hébergeant les chevaux de Troie ont été identifiés et bloqués. Il est certain que d'autres sites du même style remplacent actuellement ces derniers et exploitent les différentes failles IE, dont notamment la faille WebViewIconFolder non corrigée.



La seconde attaque de grande ampleur a été identifiée sur la messagerie instantanée AIM d'AOL.
Le ver baptise "W32.pipeline" est toujours actif et infecte chaque ordinateur qui ouvre un fichier infecté.

L'attaque se déroule ainsi : un utilisateur reçoit le message instantané suivant : "Salut, serais-tu d'accord si je télécharge une image de toi pour la mettre sur mon blog?".
Par la suite, une image nommée "image18.com" est envoyée. L'utilisateur crédule qui téléchargerait ce fichier deviendrait alors le maillon d'un réseau de machines infectées.

Les pirates pourraient lancer à partir de sa machine le téléchargement de malwares et donc prendre le contrôle total du poste affecte. Par ailleurs, le virus contaminerait toute la liste de contacts de la personne abusée.

Enfin, le logiciel "yahoo messenger" est également frappé par le même problème. Ce programme nomme "WORM_QUATIM.A" infecte les machines Windows en envoyant un lien malicieux à tous les contacts de la victime potentielle.

En suivant le lien, l'utilisateur lance le téléchargement du ver qui se cache sous le nom de "yahoo.exe" pour éviter d'être détecté par un antivirus.

Ensuite, ce dernier désactive le gestionnaire des tâches et l'éditeur de registre. De plus, la page par défaut d'Internet Explorer devient l'adresse d'un site qui héberge un cheval de Troie. Dès le lancement du navigateur, le logiciel malveillant sera alors téléchargé.
Le pirate serait donc en mesure de prendre le contrôle total du poste cible

Programmes vulnérables :

- [1] MSN, AIM et Yahoo Messenger

Criticité : Elevée

Référence Xmco :

- n° 1159187752
- n° 1160065984
- n° 1158921081

Adobe

Problème au sein du lecteur Flash

Microsoft a publié un bulletin d'analyse détaillée afin d'alerter les utilisateurs de la découverte de plusieurs vulnérabilités au sein du logiciel Flash Player distribué avec les systèmes d'exploitation suivants : Windows XP SP1, Windows XP SP2, Windows XP Professionnel x64.

Des pirates seraient en mesure de contourner des mesures de sécurité et de compromettre un système implémentant les versions de Flash Player affectées (Adobe Flash Player 8.0.24 et versions antérieures).

La première faille est liée au mauvais traitement des chaînes générées dynamiquement.
La deuxième vulnérabilité résulte d'une erreur liée à l'option "allowScriptAccess" qui permettait de mener des attaques de « cross domain scripting ».

Enfin, la dernière vulnérabilité provient d'une erreur qui se manifeste durant l'intéraction entre le contrôleur ActiveX et certains produits Microsoft Office. L'exploitation de la faille permettait à un attaquant d'exécuter un code Flash arbitraire en incitant un utilisateur à ouvrir un document Office judicieusement conçu.

Les vecteurs d'attaques sont donc l'hébergement d'un code Flash (fichier avec l'extension .SWF) au sein d'une page web ou l'ouverture d'un document Office lié à une animation Flash malicieuse.

Aucune preuve de concept n'a été publiée. Microsoft a d'ailleurs publié un bulletin afin d'alerter les clients des risques encourus sur certaines plateformes Windows qui intègrent le composant vulnérable.

Programmes vulnérables :

- Adobe Flash Player 8.0.24 et antérieures

Criticité : Elevée
Référence Xmco : n°1158161811

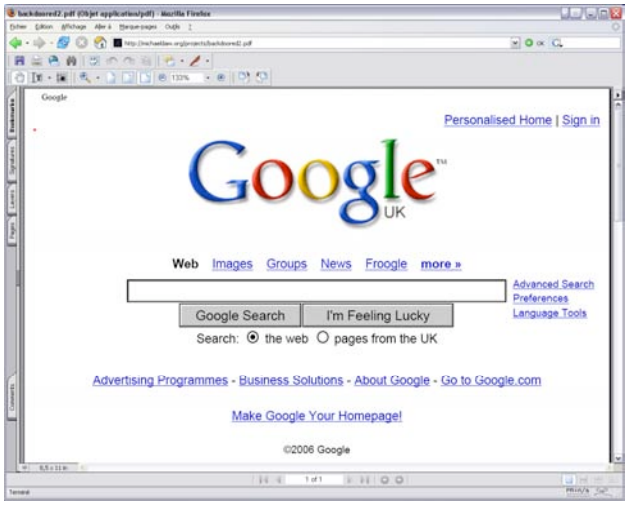
Preuves de concept liée aux fichiers PDF

Le chercheur David Kierznowski vient de publier des informations surprenantes sur l'utilisation malveillantes des fichiers PDF. En effet, il semblerait que certaines fonctionnalités d'Adobe Acrobat Reader pourraient être exploitées afin d'exécuter du code sans interaction avec l'utilisateur.

En effet, ce spécialiste démontre à l'aide de plusieurs preuves de concept comment injecter du code au sein d'un document PDF. Une fois créé, ce fichier malicieux est envoyé à la future victime. Dès son ouverture, l'utilisateur abusé serait redirigé vers un site web pirate. Le PDF d'apparence inoffensif deviendrait une arme redoutable.

Cette faille remet sérieusement en cause la sécurité du développement des équipes Adobe. De son côté Adobe explique cette découverte comme une fonctionnalité à part entière et ajoute "it's a not a bug, it's a feature".

Cette vulnérabilité pourrait donc être exploitée plus sérieusement et permettre ainsi la compromission d'un système.
Le mois d'Octobre aurait été le moment opportun pour utiliser cette faille. De nombreux sites web, créés dans le but d'exploiter les vulnérabilités d'Internet Explorer, ont vus le jour et pourraient être liés à un document PDF spécialement conçu...



Ouverture d'une page web au sein d'un document PDF

Programmes vulnérables :

- Symantec Veritas NetBackup PureDisk Remote Office Edition (toutes plateformes) version 6.0 GA MP1
- Symantec Backup Exec CPS Remote Agent 10.x
- VERITAS Backup Exec 10.x
- VERITAS Backup Exec 9.x
- VERITAS Backup Exec Remote Agent 10.x for Windows Servers
- VERITAS Backup Exec Remote Agent 9.x for Windows Servers

Criticité : Elevée
Référence Xmco : n° 1158836193

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 : utilitaires de sécurité et autres programmes nécessaires au sein d'une entreprise.

Ce mois-ci, nous avons choisi d'analyser des logiciels essentiels dans l'administration d'un réseaux :

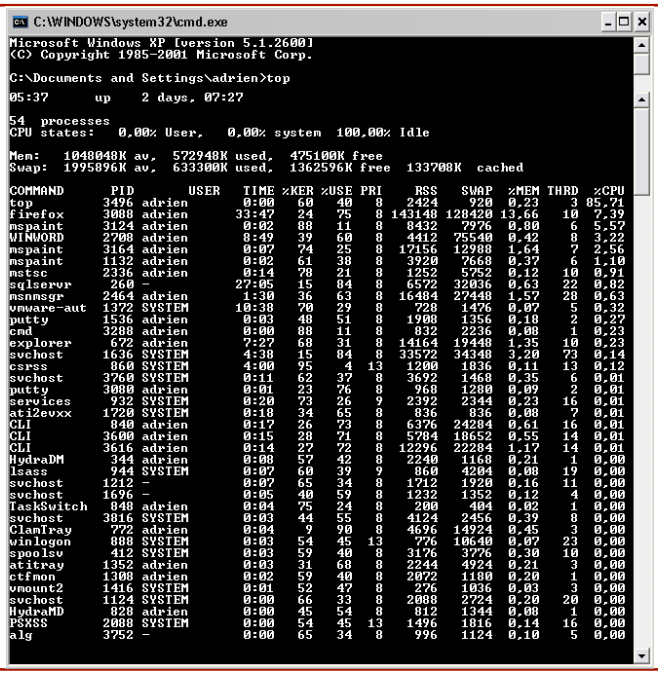
- *Windows Services for Unix : logiciel qui permet d'utiliser les commandes Unix via l'interpreteur de commandes Windows*
- *VNC : outils qui permet de prendre le contrôle d'un ordinateur à distance*
- *VmWare : virtualisation de systèmes d'exploitation*
- *Sync Toy : Utilitaire de sauvegarde de Microsoft*
- *MySQL Front : un Client SQL dotée d'une interface graphique*

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

Windows Service for Unix

Outil Windows

Version actuelle	3.5
Utilité	
Type	Logiciel qui permet d'utiliser certaines commandes Unix sous Windows
Description	Windows Services for Unix est un logiciel capable d'intégrer un grand nombre de commandes UNIX à l'interpréteur de commandes Windows. La pauvreté du langage DOS pose souvent quelques soucis. Ce programme révolutionne le fameux « cmd.exe » qui devient un véritable shell à part entière. Les commandes grep, ls, ps, cat ouvrent une porte que les plateformes Windows laissaient fermée. Ce logiciel inclu également toute une panoplie de composants qui simplifieront la vie des amateurs du monde UNIX
Capture d'écran	
Téléchargement	Utilisable sur toutes les plateformes Windows ce logiciel est disponible à l'adresse suivante : http://www.microsoft.com/france/windows/sfu/decouvrez/detail.mspx
Sécurité de l'outil	Aucune faille n'a été répertoriée depuis la première publication du logiciel.
Avis XMCO	Windows Services for Unix est un logiciel indispensable aux utilisateurs Windows qui souhaiteraient obtenir toutes la richesse des commandes Unix. Le besoin d'interopérabilité entre les deux plateformes est devenu indispensable.

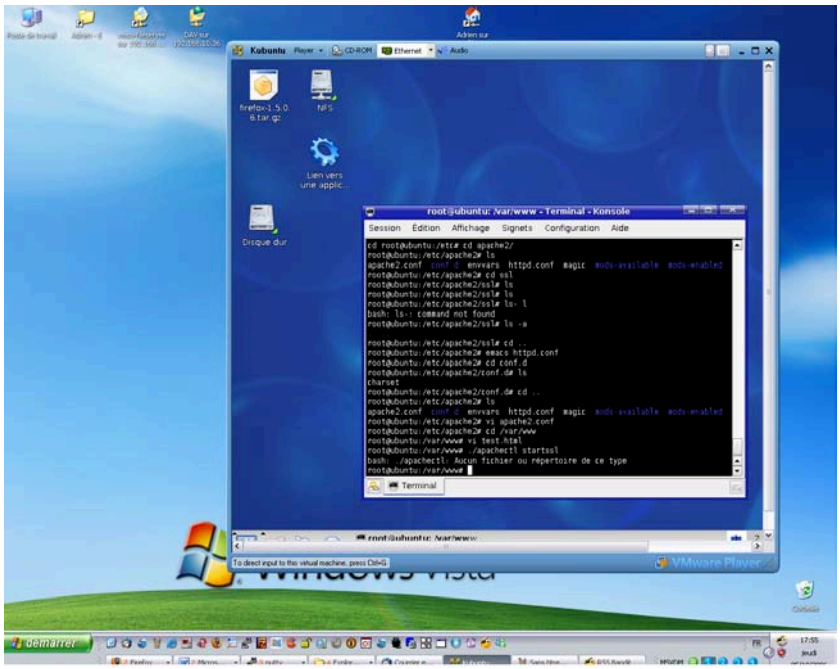
VNC

Administration à distance

Version actuelle	4.2.6
Utilité	★★★★☆
Type	Prise de contrôle via un réseau IP
Description	VNC est le frère cadet du Bureau à distance de Windows. Ce logiciel permet à un ordinateur (client) de prendre le contrôle d'un ordinateur distant (serveur) à travers un réseau. VNC est léger, Open Source et disponible sur de nombreuses plateformes. La configuration est simple : la partie serveur doit être configurée via un mot de passe qui sera demandé lors de la connexion à partir du poste client.
Capture d'écran	
Téléchargement	VNC existe sur toutes les plateformes (UNIX, HP-UX, Windows, Solaris…). Il suffit de remplir un formulaire afin de pouvoir télécharger le logiciel disponible gratuitement à l'adresse suivante : http://www.realvnc.com/cgi-bin/download.cgi
Sécurité de l'outil	Plusieurs failles ont été identifiées mais une seule fut jugée critique et corrigée rapidement (v4.1). Cette dernière était exploitée par un programme malicieux afin de contourner l'authentification. La liste de ces vulnérabilités est disponible à l'adresse suivante : http://secunia.com/product/3719/?task=advisories
Avis XMCO	Cet outil est un excellent programme qui facilitera l'administration à distance de vos machines. Cependant, ce logiciel ne remplace pas le "bureau à distance" intégré par défaut sur la plupart des plateformes Windows qui est, incontestablement, le meilleur moyen de gérer les machines distantes.

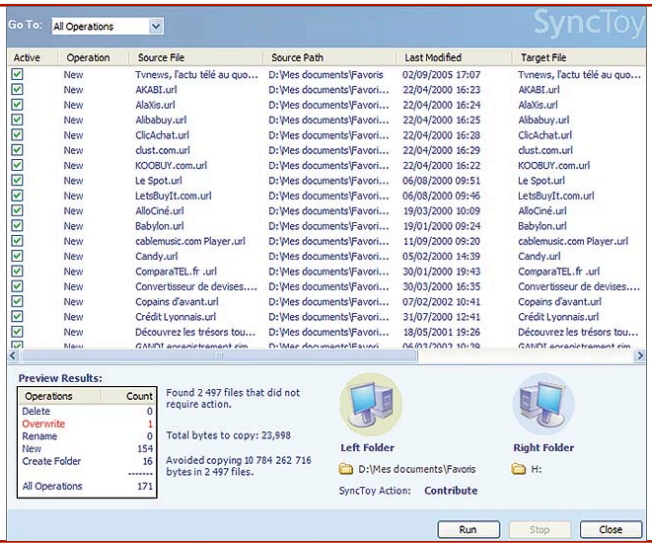
VmWare Player

Virtualisation

Version actuelle	1.0.2
Utilité	★★★★★
Type	Lecteur de machines virtuelles
Description	Le logiciel Vmware est un outil de virtualisation de systèmes d'exploitation. Il permet, sur une machine physique, d'exécuter, en parallèle, d'autres machines d'OS différents. Contrairement à la version « Workstation » qui permet de créer ses propres machines virtuelles, l'outil Vmware Player propose seulement d'exécuter des machines déjà configurées. L'interêt est multiple : création d'un réseau, confinement d'une machine, test de logiciels de plateformes différentes… Cet outil simplifiera les tests d'installation de logiciel au sein d'une entreprise aux plateformes multiples.
Capture d'écran	
Téléchargement	Vmware existe sur toutes les plateformes Linux et Windows et peut être téléchargé à l'adresse suivante : http://www.realvnc.com/cgi-bin/download.cgi
Sécurité de l'outil	Deux ont été identifiées et sont présentées à l'adresse suivante : http://secunia.com/product/6594/?task=advisories
Avis XMCO	Vmware player est un excellent produit qui a révolutionné la virtualisation. Ce logiciel vous offre la possibilité de composer un véritable réseau sur une seule machine physique. Il vous sera alors possible de tester toutes sortes de logiciels sans avoir aàdégrader votre OS. De plus, l'éditeur propose, sur son site, un grand nombre de machines virtuelles variées et gratuites (UNIX, Windows) ce qui remplace l'interêt de la version Workstation.

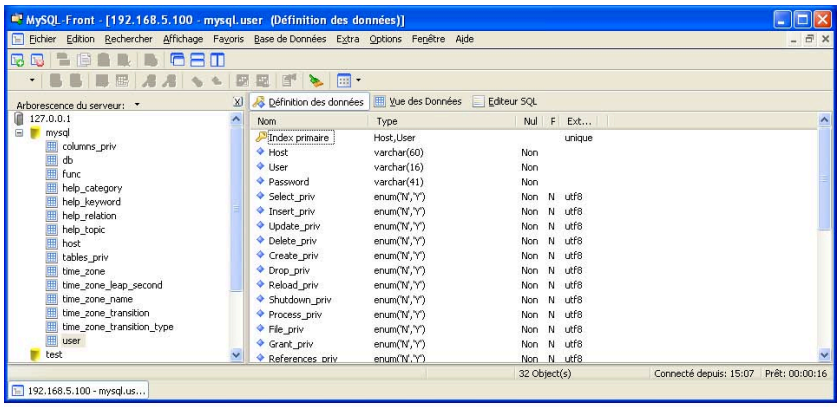
Sync Toy

Sauvegarde de fichiers

Version actuelle	1.2
Utilité	
Type	Sauvegarde de fichiers
Description	Sync Toy est un logiciel de sauvegarde qui permet de synchroniser des dossiers en quelques clic. Vous pourrez simplement gérer la copie de vos données sur une clef USB, sur un serveur distant ou sur un autre support amovible. Cet outil est développé par Microsoft et propose plusieurs modes de sauvegarde. La configuration est simple. Il suffit de choisir le répertoire d'origine et le répertoire de destination et d'appuyer sur Run. Pratique et efficace !
Capture d'écran	
Téléchargement	SyncToy est disponible pour Windows XP à l'adresse suivante : http://www.microsoft.com/downloads/details.aspx?FamilyID=E0FC1154-C975-4814-9649-CCE41AF06EB7&displaylang=en
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	Cet outil est un programme simple et complet qui facilitera la copie de vos données. Il suffit seulement de choisir le type de sauvegarde (synchronize, echo, subscribe, contribute, combine), de sélectionner un répertoire source et un répertoire cible. En fonction du type de sauvegarde choisi, les données seront copiées et/ou modifiées dès qu'un changement survient sur un des dossiers choisis.

MySQL Front

Client MySQL

Version actuelle	3.2
Utilité	
Type	Interface graphique d'accès aux bases de données MySQL
Description	MySQL Front est un client MySQL qui permet de gérer et d'administrer vos bases de données depuis un poste distant. Son interface graphique permet d'accéder simplement aux bases de données via une interface graphique simple et intuitive. Cet outil permet de créer, supprimer et modifier les structures des tables, de lancer des requêtes, de répliquer des tables ou encore de gérer les utilisateurs.
Capture d'écran	
Téléchargement	Seule la version 3.0 de MySQL Front est gratuite et disponible sur le site suivant: http://www.clubic.com/lancer-le-telechargement-9175-0-mysql-front.html
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	MySQL Front est un excellent client MySQL. Fini les lignes de commandes, vous pouvez gérer vos bases de données via une interface agréable et pratique.

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	2.6.0.2	15/09/2006	http://www.snort.org/dl/
MySQL	5.0.24		http://dev.mysql.com/downloads/mysql/5.0.html
	5.1.11-Bêta		http://dev.mysql.com/downloads/mysql/5.1.html
Apache	2.2.3		http://httpd.apache.org/download.cgi
	1.3.37		http://httpd.apache.org/download.cgi
Nmap	4.11	01/04/2005	http://www.insecure.org/nmap/download.html
Firefox	2 beta 2	06/2006	http://www.mozilla-europe.org/fr/products/firefox/
Thunderbird	1.5.0.7	09/2006	http://www.mozilla-europe.org/fr/products/thunderbird/
Spamassassin	3.1.5	30/08/2006	http://spamassassin.apache.org/downloads.cgi?update=200603111700
Putty	0.58		http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
ClamAV	0.88.4	07/08/2006	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	2.2.28		http://filezilla.sourceforge.net/
OpenSSH	4.4	27/09/2006	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	1.4.5	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

Nom	Dernière version	Date	Lien
Back-Track	V1		http://www.remote-exploit.org/index.php/BackTrack_Downloads
MBSA	2.0	20/08/2006	http://www.microsoft.com/technet/security/tools/mbsahome.mspx
Ps-Exec	1.7		http://www.sysinternal.com/Utilities/PsExec.html
Helios	v1.1a	6/10/2003	http://helios.miel-labs.com/2006/07/download-helios.html
Opera	9.02		http://www.opera.com/download/
Internet Explorer 7	Internet Explorer 7 Release Candidate 1		http://www.microsoft.com/windows/ie/downloads/default.mpsx
Outil de suppression de logiciels malveillants	1.19		http://www.microsoft.com/downloads/details.aspx?FamilyID=ad724ae0-e72d-4f54-9ab3-75b8eb148356&DisplayLang=fr
F-Secure Blacklight	Blacklight Beta		http://www.f-secure.com/blacklight/try_blacklight.html
Writely	Writely beta		http://www.writely.com
Nessus	3.0.3		http://www.nessus.org/download