Hakin9

PRACTICAL PROTECTION HARD CORE IT SECURITY MAGAZINE

Nº 7/20010 (47) Online ISSN 1731-7037

TÉLÉPHONIE VOIP

ASTERISK – SUCCÈS DE L'OPEN SOURCE
SÉCUIRTÉ DE LA TÉLÉPHONIE

SERVEURS MANDATAIRES

RÔLE DES PROXYS DANS LA SÉCURITÉ

LES ATTAQUES EVIL TWIN

L'UTILISATION D'UNE EVIL TWIN
PAR SOCIAL ENGINEERING

NAGIOS

SUPERVISEZ VOTRE RÉSEAU GRÂCE À NAGIOS

SSH

CONNEXION SÉCURISÉE GRÂCE À SSH

formations
& Certification professionnelle

Plus de 350 formations agréées par les éditeurs et constructeurs et 4000 sessions délivrées par an font de Global Knowledge un organisme de formation référent en informatique, en management des Systèmes d'Information et gestion de projets IT.

Global Knowledge a été élu «Meilleur partenaire Formation de l'année» par Cisco, VMware et Citrix!

Les Essentiels Réseaux, Virtualisation, Voix, Sécurité

- Les réseaux : architectures, mise en oeuvre et perspectives
- Enjeux et solutions d'un environnement virtuel
- Voix sur IP : les fondamentaux
- La VoIP sécurisée
- Les fondamentaux de la sécurité informatique
- CISSP Préparation à la Certification
- Hacking Defined Advanced : se protéger contre les agressions du SI

Gouvernance & Management Informatique

- La gouvernance et performance des Systèmes d'information
- Les tableaux de bord de la performance informatique
- Rentabilité et valeur ajoutée des investissements informatiques
- Cobit Foundation et la gouvernance des SI
- ITIL v3 Foundation
- Le cas Wall Street : simulation sur ITIL v3 et ISO 20000
- ISO/IEC 20000 Foundation
- ISO/IEC 27002 Foundation
- Maîtriser et accompagner les changements
- Développer le leadership et les qualités de pilotage des managers
- Devenez manager coach de votre équipe

Gestion de projet PMI / Prince 2

- Introduction au management de projets
- La gestion des projets informatiques (IT)
- PMP Bootcamp : Préparation à la certification
- Prince 2 Foundation

Client/Serveur/Messagerie Microsoft

- Installation et configuration du client Windows 7
- Planifier les déploiements et administrer les environnements Windows 7
- Configuration et administration de SharePoint Server 2010 *nouveau*
- Développer et personnaliser les applications pour Sharepoint 2010 *nouveau*
- L'essentiel de l'administration de serveurs Windows 2008
- Configurer et dépanner une infrastructure réseau Windows 2008
- Active Directory pour Windows Server 2008
- Configuration, administration et dépannage de Exchange Server 2010
- Concevoir et déployer des solutions de messagerie avec Exchange 2010 *nouveau*
- Mise en œuvre et maintenance des outils de communications unifiées avec OCS R2

Virtualisation VMware, Microsoft & Citrix

- VMware What's New vSphere 4 (mise à jour des connaissances)
- VMware vSphere 4 : installation, configuration et administration
- VMware View : installation, configuration et administration
- VMware vSphere 4 : Troubleshooting *nouveau*
- VMware vSphere 4 : Design *nouveau*
- Mettre en oeuvre la virtualisation sous Windows 2008 (Hyper-V)
- Administrer les postes de travail avec MDOP
- Déployer et administrer System Center Virtual Machine Manager
- Planifier, déployer et gérer System Center Configuration Manager
- Mettre en oeuvre et gérer System Center Operations Manager 2007
- Mettre en oeuvre Citrix XenApp 5 pour Windows Server 2008
- Citrix Desktop Infrastructure : gérer XenServer, XenDesktop, et Provisioning Server
- Mettre en oeuvre une solution de virtualisation avec Citrix *nouveau*

Rentrée 2010 : les incontournables

Réseaux Cisco

- Interconnecting Cisco Network Devices Part 1 (ICND1)
- Implementing Cisco IP Routing (ROUTE) *nouveau*
- Implementing Cisco IP Switched Networks (SWITCH) *nouveau*
- Troubleshooting & Maintaining Cisco IP Networks (TSHOOT) *nouveau*
- Configurer BGP sur des routeurs Cisco (BGP)
- Cisco IPV6 Concepts, Design et Déploiement (IPV6)
- Implementing Cisco MPLS (MPLS)
- Mettre en oeuvre une infrastructure Cisco MultiCast (ICMI) *nouveau*
- Mettre en oeuvre CiscoWorks LMS (CWLMS)
- Mettre en oeuvre la sécurité des réseaux IOS Cisco (IINS)
- Sécuriser les réseaux avec des routeurs et switches Cisco (SNRS)
- Les fondamentaux de la sécurité des réseaux avec Cisco ASA (SNAF)
- Cisco Wireless Lan Fundamentals (CWLF)
- Mettre en oeuvre Cisco IOS Unified Communications (IIUC)
- Cisco : La Voix sur IP version 6.0 (CVOICEV6)
- Mettre en oeuvre la Qos Cisco (QOS)
- Cisco IP Telephony Part 1 version 6 (CIPT1V6)
- Data Center Network Infrastructure (DCNI-1)

Formations éligibles au DIF | Support de cours remis à chaque participant

Renseignements & Inscriptions :

- Tél.: 0821 20 25 00 (prix d'un appel local)
- info@globalknowledge.fr

Téléchargez le catalogue complet sur :

www.globalknowledge.fr

Global Knowledge®

Global Knowledge France - Siège social - Tour Albert 1er - 65, avenue de Colmar - 92507 Rueil-Malmaison cedex - Tél.: 01 78 15 34 00 - Fax : 01 78 15 33 90

ÉDITORIAL

La sécurité de la téléphonie VoIP

Durant cette pleine période de vacances et de repos, commençons ce numéro par le dossier dédié à la sécurité de la téléphonie VoIP. En effet, nous sommes nombreux à utiliser et profiter des avantages de la communication téléphonique via les réseaux. L'auteur de l'article sur Asterisk vous expliquera les vulnérabilités du protocole ToIP, les méthodes d'attaques et, surtout, de bonnes mesures de prévention. Vous dévouvrirez le fonctionnement d'Asterisk, solution Open Source qui a déjà fait ses preuves.

Une panne de réseaux informatiques risque de coûter cher à toute entreprise et risque d'être lourde en conséquences. Dans la section *Pratique*, découvrez l'article *Supervisez votre réseau grâce à Nagios* qui vous expliquera comment superviser vos parcs informatiques.

Dans la section *Attaque*, nous vous invitions à lire l'article sur une technique que les pirates utilisent pour influencer ou manipuler les utilisateurs afin de leur soutirer de l'argent. Tout cela grâce aux médias sociaux. Un article que les passionnés de sites de réseaux sociaux ne manqueront pas.

Utiliser un servuer mandataire nous protège-t-il contre tous les riques sur la Toile ? Dans l'article *Serveurs mandataires, comment les utiliser* ?, vous aurez l'occasion de connaître les différents types de serveur mandataire dans la sécurité informatique. Vous apprendrez également à les utiliser.

Bonne lecture à tous,

L'équipe Hakin9

hakin9

Le mensuel hakin9 est publié par
Software Press Sp. z o. o. SK

Président de Software Press Sp. z o. o. SK:
Paweł Marciniak
Directrice de la publication: Ewa Lozowicka
Rédactrice en chef: Aneta Mazur
aneta.mazur@hakin9.org
Fabrication: Andrzej Kuca
andrzej.kuca@software.com.pl

DTP : Przemysław Banasiewicz
Couverture : Agnieszka Marchocka

Publicité : publicite@software.com.pl

Béta-testeurs : Didier Sicchia,
Pierre Louvet, Anthony Marchetti,
Régis Senet, Paul Amar, Julien Smyczynski,
Gregory Vernon, Latorre Christophe,
Timotée Neullas

Les personnes intéressées par la coopération sont invitées à nous contacter :
fr@hakin9.org

Adresse de correspondance :
Software Press Sp. z o. o. SK
Bokserska 1, 02-682 Varsovie, Pologne
Tél. +48 22 427 32 87, Fax. +48 22 244 24 59
www.hakin9.org

TABLE DES MATIERES

NEWS

DOSSIER

SÉCURITÉ RÉSEAUX

PRATIQUE

ATTAQUE

AVEZ-VOUS RATÉ UN NUMÉRO DE HAKIN9 ?

TÉLÉCHARGEZ LES ARCHIVES 2008, 2009 ET 2010

GRATUITEMENT !

WWW.HAKIN9.ORG/FR

Youtube, une faille XSS décelée

Une vulnérabilité de type XSS a été exploitée sur le site Youtube aux alentours du 5 juillet 2010. Google a patché la vulnérabilité au plus vite, évitant ainsi au vecteur d'attaque de créer de nombreux dégâts. Cette exploitation de faille s'est faite juste après la fête nationale des Etats-Unis. C'est peut-être une simple coïncidence mais de nombreux pirates jouent sur les fêtes nationales etc. pour ainsi espérer une durée de vie plus longue de la vulnérabilité : les effectifs étant moins nombreux, le patch sera plus long à arriver. Rappelons-nous, par exemple, le cas avec Twitter, l'année dernière à la période de Pâques, etc.

Concernant l'aspect technique de la vulnérabilité, si nous tentions d'insérer des balises HTML, seule la première était filtrée. Dès lors, il suffisait d'entrer <script><script> pour que la deuxième balise <script> soit exécutée car mal filtrée.

L'attaque n'a pas eu de grave répercutions et n'a servi qu'à insérer des messages au sujet de la mort fictive de Justin Bieber (chanteur canadien) ainsi que certaines redirections.

En revanche, les risques d'une XSS sont l'affichage de nombreux messages, la récupération des cookies et ainsi tromper la majorité des internautes.

Avis aux détenteurs de vulnérabilités sur les navigateurs Mozilla / Chrome

Mozilla a augmenté la récompense donnée aux chercheurs en sécurité informatique qui trouveraient des bugs dans le navigateur internet Mozilla firefox. La valeur de la « prime » est de 3 000 $. Ce système cherche à valoriser le travail des chercheurs en sécurité, afin de promouvoir le côté « lucratif » que les bugs trouvés apporteraient et, ainsi, pallier le problème de « full-disclosure » (soit divulguer la faille sur internet). Cette initiative a été lancée début 2004 et semble être suivie par bon nombre de personnes.

Cependant, le bug doit avoir certaines particularités notamment ne pas avoir déjà été reporté, être de type « remote exploit » et dans la dernière version du logiciel.

En parallèle, d'autres compagnies ont suivi le même mouvement, comme Google, avec une prime à 1337 $, ce qui en fera sourire certains car signifie « leet » soit élite. Information de dernière minute : Google vient d'augmenter la prime à 3113,7 $...

Un add-on Mozilla qui récupère vos mots de passe...

De nombreux add-ons au navigateur Internet Firefox ont paru il y a quelques jours, dont le « Mozilla Sniffer » servant à intercepter les logins, passwords et données soumis à n'importe quel site, les envoyant par la suite à une machine distante. Cet add-on a été uploadé le 6 juin et la compagnie dénombre à ce jour près de 3300 « utilisateurs » de ce logiciel malveillant.

Le code de l'add-on n'avait pas été vérifié mais seulement scanné à la recherche d'un quelconque virus. Seul un comportement anormal de l'add-on est détecté en analysant le code.

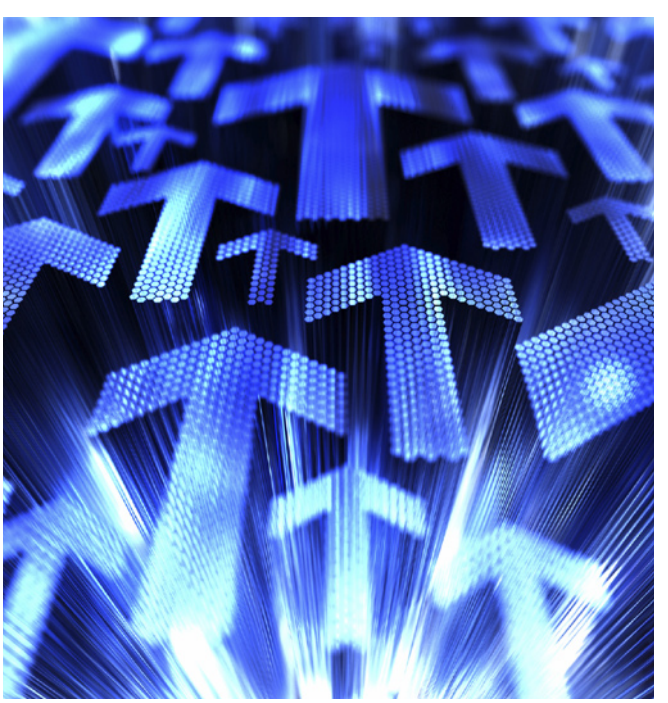
Mozilla, aux aguets depuis ces derniers temps, a décelé un autre add-on nommé « CoolPreviews » dont le code contient une vulnérabilité permettant à une personne mal intentionnée d'exécuter du code à distance et ainsi avoir la main sur la victime infectée par cet add-on.

Dès lors, près de 177 000 ont la version de « CoolPreviews » installée. C'est donc un vecteur d'attaque qui n'est en aucun cas à négliger et qui risque de faire de nombreux dégâts tout en nuisant à l'image du navigateur.

Un ancien employé du MI6, coupable de fuites d'informations

Daniel Houghton, 25 ans, a été au cœur de l'actualité au cours des dernières semaines. Il a travaillé de 2007 à 2009 dans les services de renseignement du Royaume-Uni. Il était rattaché au MI6 en charge de la protection du pays contre des attaques terroristes etc. Fin 2009, Daniel Houghton a décidé de démissionner, emportant avec lui de nombreuses informations susceptibles de se révéler très intéressantes aux yeux de personnes cherchant à nuire au Royaume-Uni.

Il a été accusé, il y a quelques semaines, d'avoir voulu dévoiler, contre de l'argent, des informations classées confidentielles dont une liste de près de 700 membres appartenant aux services de renseignements etc.



Daniel avait cherché à vendre ces informations aux services de renseignements allemands, demandant près de 2 millions de £. Finalement, après de nombreuses négociations, il a baissé le prix à 900 000 £. La transaction devait être réalisée à Londres, mais Daniel a été arrêté juste avant, niant les faits. Depuis, il a plaidé coupable. Le jugement aura lieu le 3 septembre ; en attendant, de nombreuses investigations continuent.

Skype, le secret révélé au grand jour

Le 7 juillet aura été une date noire pour Skype : c'est à cette date que Sean O'Neil a publié, à l'aide d'une équipe de « reverse engineers », l'algorithme d'encryptage de Skype.

Cet algorithme était tenu secret par l'équipe de Skype. Or, maintenant, il est révélé au grand jour.

Sean O'Neil explique sur son blog (article qui peut être visualisé grâce au cache de Google, car supprimé de son blog) que son code avait été volé il y a quelques mois, était utilisé par des pirates informatiques, réalisant du spam etc. Dès lors, Skype était remonté jusqu'à lui, l'accusant de jouer un rôle prédominant avec les spammers etc.

Quant à lui, pour se justifier, il propose du code en C, tout en argumentant son acte : il souhaite rendre Skype plus sécurisé.

Quand les Hackers rencontrent les « pirates » ...

Le fameux site de partage de fichiers a été victime d'un groupe de chercheurs argentins, sous la direction de Ch Russo. Ils ont réussi à accéder à l'interface d'administration du site grâce à de nombreuses vulnérabilités telles que des SQL Injection, ..

Dès lors, ils ont pu avoir accès à la base de données, qui recensait près de 4 millions d'utilisateurs. 4 millions d'utilisateurs représentent un nombre très important, surtout pour l'une des plates-formes les plus connues et les plus médiatisées, vu le nombre de procès auxquels ses dirigeants ont dû faire face. Ces informations sont une véritable mine d'or pour les personnes cherchant à mettre la main sur les utilisateurs pratiquant le téléchargement. Les chercheurs argentins pouvaient réaliser de nombreuses interactions comme, par exemple, créer / supprimer / modifier / ou encore, voir les informations sur les utilisateurs, incluant tous leurs torrents …

Russo a expliqué dans un communiqué que lui et ses associés n'ont ni altéré ni supprimé une quelconque information dans la base de données.

Parallèlement, il a assuré qu'il ne vendrait aucune information récupérée lors de cette intrusion. Il souhaitait seulement démontrer que les informations des membres n'étaient pas bien protégées et qu'il était tout à fait possible de les récupérer. Heureusement, ces informations ne soient pas tombées dans de mauvaises mains, ce qui aurait provoqué un incident majeur sur toute cette communauté.

Des problèmes pour le FBI et l'encryptage de plusieurs disques durs...

En juillet 2008, la police avait saisi 5 disques durs appartenant à un banquier brésilien, Daniel Dantas, soupçonné de nombreux crimes.

Les autorités brésiliennes ont constaté que les données étaient chiffrées.

De nombreuses analyses ont révélé que les fichiers avaient été encryptés à l'aide de deux algorithmes dont TrueCrypt et un autre non identifié (certainement fondé sur 256-bit AES). De plus, il n'existe pas (comme au Royaume-Uni, par exemple) de loi forçant l'utilisateur à donner sa clé de cryptage.

Malgré un an d'études et de tests, le FBI n'a pas réussi à casser le système. En conséquence, sans les preuves informatiques des fraudes financières, les enquêteurs auront des difficultés à poursuivre DANTAS.

Les prochains mois nous permettront d'y voir un peu plus clair à ce sujet tout en suivant l'affaire.

Cracking de password, une nouvelle découverte surprenante !

Les chercheurs Nate Lawson et Taylor Nelson prétendent avoir découvert une faille de sécurité qui affecte de nombreux systèmes d'authentification tels que Oauth ou encore OpenID. Ces systèmes sont très fortement utilisés sur des sites tels que Twitter, …

Les cryptographes sont informés des attaques dites « temporelles » depuis de nombreuses années mais n'ont jamais pris la menace très au sérieux car elle semblait trop difficile à mettre en place sur un réseau (problèmes de latence, etc..) puisque cette attaque est fondée sur le temps.

L'article présente un cas intéressant : certains systèmes vérifient que le login / password correspond à chaque nouvelle insertion de caractère.

Dès lors, les chercheurs en arrivent à la conclusion qu'un mauvais essai de login arrive plus vite qu'un login où le premier caractère du login est bon. (Le système renvoie un mauvais login dès qu'il détecte un mauvais caractère).

Grâce à ce facteur de « temps », il est possible de deviner un mot de passe et ainsi contourner les systèmes d'authentification.

Nate et Taylor souhaitent discuter de ces attaques à la Black Hat conférence qui se tiendra fin août à Las Vegas. D'autres articles ou documentations nous en diront certainement plus sur l'exploitation d'attaque de type « temporelle ».

News rédigés par Paul AMAR.

ASTERISK et les techniques de hack de la téléphonie sur IP !

David Huré

Asterisk est une solution Open Source innovante qui a fait ses preuves ! Historiquement conçu par un étudiant en 1999, Mark Spencer avait un rêve, il souhaitait démocratiser la téléphonie sur IP et concurrencer les plus grands ! Aujourd'hui, utilisé par des particuliers comme de grandes entreprises et possédant un réel potentiel d'évolution, Asterisk apporte un nouveau souffle à la ToIP…

Cet article explique…

- Les fondamentaux d'Asterisk
- Comment exploiter les vulnérabilités protocolaires de la ToIP
- Les méthodes d'attaques et les outils
- Les bonnes pratiques pour se protéger

Ce qu'il faut savoir…

- Notion de réseau et des protocoles
- Notion de ToIP

Le monde de la téléphonie est plus que jamais en évolution ces dernières années. En effet, après le passage de la téléphonie traditionnelle vers la VoIP (voix sur réseau IP), un grand nombre d'acteurs plus ou moins historiques proposent maintenant des solutions apportant des services à valeurs ajoutées.

Alcatel fait toujours partie des leaders du marché, même s'il a perdu des parts non négligeables sur ce marché, d'autres ont réussi à exploiter davantage l'IP comme Cisco, Avaya, Mitel… ou encore un autre qu'il n'est plus nécessaire de présenter, Asterisk sous toutes ses formes…

Il y a encore 5 ans, Asterisk représentait ~0,2 % de parts de marché puis, en quelques années, près de 4%, et maintenant, il atteint près de 7% du marché mondial en 2010. Certains opérateurs utilisent même un noyau Asterisk pour leurs offres Centrex et ont à minima validé l'Asterisk V1.4 et/ou V1.6 pour leurs solutions « Trunk-SIP ». Asterisk bénéficie maintenant d'une résonance toute particulière, même aux yeux des grandes entreprises !

Autant dire que la communauté Asterisk est comparable aux autres communautés telles que Squid, MySQL, Apache… qu'elle se porte bien et a encore de beaux jours devant elle !

Ce succès est principalement dû au caractère « Open Source » d'Asterisk et à une certaine maturité technologique qui lui permet, maintenant, d'être aussi fiable et performant que les solutions leader. De plus, l'ensemble des fonctionnalités proposées s'étoffent à chaque version, à tel point qu'aujourd'hui, Asterisk possède des fonctions qui ne sont pas aux catalogues des grands constructeurs et surtout adaptables « sur mesure » à votre environnement afin de l'interfacer dans des systèmes d'informations complexes. La flexibilité d'Asterisk est un atout majeur face aux autres solutions packagées !

Asterisk permet notamment, en plus de tous les services dit « classiques », de mettre en place des services tels que : softphone, voicemail, MEVO, PoPC, statistique (CDR), call center, Fax-mail, interface spécifique, IVR, Conférence, provisionning automatique, SMS, passerelle mobile, enregistrement, text-To-Speech, ACD, Ldap, taxation, CRM, supervision, annuaire, reconnaissance du numéro depuis l'extérieur, gestion de Présence, des files d'attentes, messagerie instantanée, couplage avec Wifi et DECT IP, couplage avec visio-conférence, le chuchotement, CTI, T9, annuaire unifié, musique d'attente…

Cependant, la ToIP/VoIP souffre encore d'une mauvaise image d'un point de vue sécurité…En effet, les réseaux voix historiquement isolés, fusionnent de plus en plus avec les réseaux de données, ils sont donc plus sensibles aux attaques d'un piratage. Les impacts peuvent être variables, confidentialité, dysfonctionnements, usurpations, écoute, changements des annonces de l'IPbx, accès aux messageries vocales, contournement de la politique de sécurité DATA (backdoors), perte financière, etc… alors qu'il existe un ensemble de solutions qui permettent de maitriser la sécurité de son système de téléphonie sur IP.

Dans certaines actualités, beaucoup ont entendu parler des enregistrements de l'affaire « *Bettencourt* »… ou encore, ont lu avec stupéfaction que certains opérateurs étrangers n'hésitaient pas à pirater des entreprises d'autres pays afin de mettre en place des « peering » de masse leur permettant de revendre des milliers de minutes par mois pour l'usage de leurs clients…

D'autre part, moins présente en France, l'arnaque aux numéros surtaxés et à l'usurpation d'identité, le procédé est simple, il consiste à appeler une personne en modifiant le numéro d'appelant par celui de quelqu'un d'autre ; peu d'opérateurs contrôlent ce type d'exercice et ce contrôle est rendu quasi impossible dans le cas d'une communication VoIP internet…

Une autre arnaque porte sur la modification de la synthèse vocale afin de se faire passer pour quelqu'un d'autre par le biais d'un simple outil de modulation de fréquence vocale, outil de plus en plus évolué et qui permet, par exemple, de transformer la voix d'une femme en celle d'un homme ! Les IPBX entreprise actuellement sur le marché ne sont pas équipés aujourd'hui de mécanisme de « contrôle de conformité » de la voix mais il est possible, dans le cadre d'affaires judiciaires, de vérifier si une voix a été ou non modifié dans un enregistrement.

A ce sujet d'ailleurs, seuls les opérateurs sont contraints, par commissions rogatoires délivrées par les services judiciaires, à mettre en place des écoutes téléphoniques. Certaines techniques « d'interception légale de trafic » se standardisent même au niveau international comme le « Lawful interception » de la Communications Assistance for Law Enforcement Act (CALEA ou ETSI)

Cependant, ne soyons pas alarmiste, ce type d'attaque nécessite une expertise et chacun, à son niveau, dispose de moyens plus ou moins évolués de se protéger avec des niveaux de sécurité très satisfaisants ou, au moins, équivalents à celui des anciens systèmes de téléphonie traditionnels !

Nous allons en détailler certains d'entre eux, en commençant par la sécurité de l'OS qui supporte votre IPBX, généralement sous noyau Linux, il existe deux écoles. Il y a ceux qui optimisent intégralement l'OS utilisé, technique très efficace et bénéficie d'avantages indéniables comme les performances, la sécurité optimale, la stabilité accrue… et répondent à des besoins spécifiques, voire industriels.

Cependant, cette technique nécessite des compétences avancées. En effet, partir d'un LFS « Linux from scratch » et compiler uniquement les modules, drivers et paquets nécessaires afin d'optimiser intégralement le noyau n'est pas donné à tous, cela reste manuel, long et complexe et, de plus, aucun suivi de version n'est applicable automatiquement. Il faut mettre en place sa propre gestion des dépendances…

De l'autre côté, il y a ceux qui souhaitent mettre en place simplement et rapidement un système de base (Debian, CentOs, Red Hate…) ou, mieux, utilisent des variantes comme le mode « Hardened » (HLFS) afin de renforcer nettement le niveau de sécurité. Ce mode intègre nativement des mécanismes de sécurité sur la pile IP de l'OS, limite l'exécution des binaires, des scripts et autres attaques et n'utilise que les drivers nécessaires… couplés uniquement aux services activés par l'administrateur et utiles à la ToIP comme par exemple, le WEB, DHCP, NTP, TFTP, l'Asterisk, le Manager Asterisk, SSH, relay mail… En résumé, la plupart des personnes concernées utilisent simplement un système de base et se dirigent vers un « Hardened » lorsqu'elles sont sensibles à la sécurité. Le LSF est généralement réservé au « Geek », aux constructeurs et/ou éditeurs.

Dans un autre registre, le paramétrage d'Asterisk joue un rôle essentiel dans la sécurité de la solution de té-

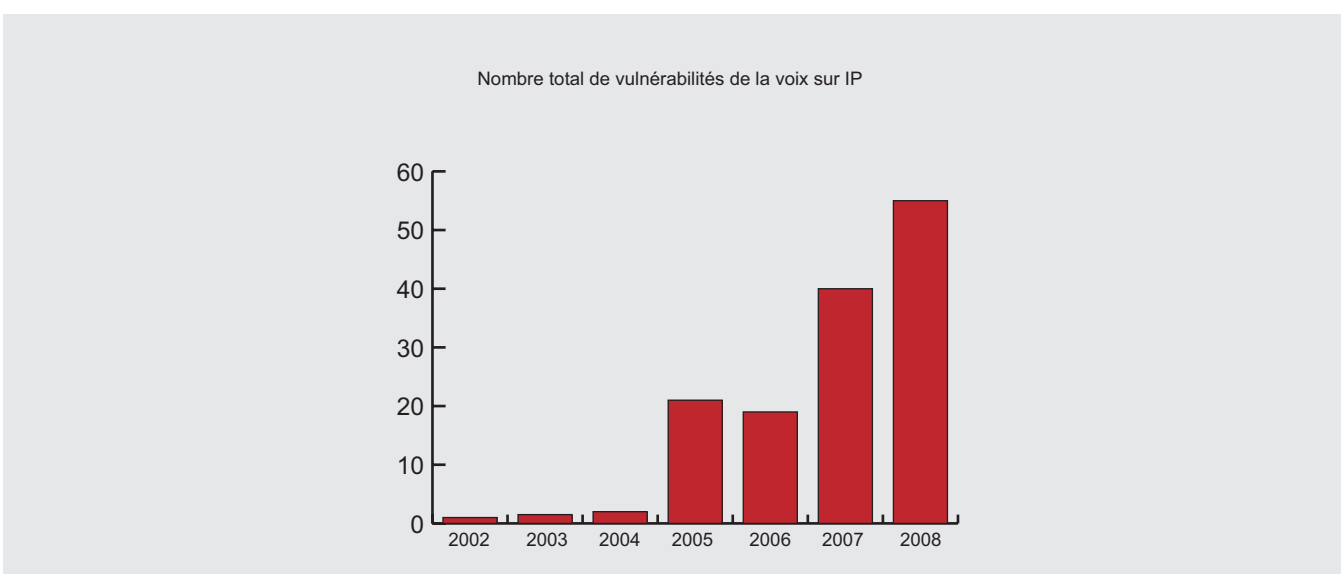


Figure 1. *Hausse rapide des vulnérabilités depuis 2006 (source: NVD)*

léphonie sur IP. En effet, l'Asterisk est un service fondé sur un ensemble de fichiers de configuration en commençant par le « SIP.conf » permettant de configurer les comptes SIP utilisateurs (SDA, nombre d'appels simultanés max, Nom Prénom…), les contextes auxquels ils sont rattachés, les CODEC à utiliser, la gestion des droits d'appels… c'est ce fichier qui, par exemple, vous autorise ou non à appeler un 06, 08, l'international…et liste les services de ToIP que vous pourrez utiliser (double appel, conf call, voicemail…).

De plus, le fichier « extension.conf » permet d'établir un dial plan, d'autres types de contextes (interne/externe), des macros…, la gestion des renvois pour autoriser ou non un renvoi vers 06 ou 08.

Une partie de la sécurité du service « Asterisk » s'appuie, entre autres, sur le « manager.conf ». Ce fichier représente l'administration du noyau Asterisk (Figure 2 : « manager Asterisk »).. Une des bonnes pratiques consiste à créer uniquement un compte « super Administrateur » et à bien paramétrer le niveau de droit des utilisateurs lambda (users) et des autres administrateurs délégués (Originate). Voici la synthèse des éléments paramétrables via le « manager ».

Nb : Il est, entre autres, recommandé d'utiliser le SSH et d'activer le mode de connexion SSL à l'interface WEB du manager ou simplement de la désactiver.

L'Asterisk s'appuie aussi sur d'autres fichiers de configuration comme le « CDR.conf » pour la gestion et le paramétrage des logs du call flow…le fichier « CDR.manager.conf », le « H323.conf », « iax.conf », « queues.conf », etc…

Généralement et de plus en plus, les utilisateurs comme les administrateurs sont friands d'utiliser une interface WEB (surcouche d'administration) pour le paramétrage et l'administration de l'Asterisk et de ses services. Elle doit bénéficier de différents niveaux de sécurité. A minima, trois niveaux par exemple « Root », « Admin », « utilisateur » qui permet d'autoriser ou pas certaines modifications (ex : modification

```
; Authorization for various classes
;
; Read authorization permits you to receive asynchronous events, in general.
; Write authorization permits you to send commands and get back responses.  The
; following classes exist:
;
; system    - General information about the system and ability to run system
;             management commands, such as Shutdown, Restart, and Reload.
; call      - Information about channels and ability to set information in a
;             running channel.
; log       - Logging information.  Read-only.
; verbose   - Verbose information.  Read-only.
; agent     - Information about queues and agents and ability to add queue
;             members to a queue.
; user      - Permission to send and receive UserEvent.
; config    - Ability to read and write configuration files.
; command   - Permission to run CLI commands.  Write-only.
; dtmf      - Receive DTMF events.  Read-only.
; reporting - Ability to get information about the system.
; cdr       - Output of cdr_manager, if loaded.  Read-only.
; dialplan  - Receive NewExten and VarSet events.  Read-only.
; originate - Permission to originate new calls.  Write-only.
;
;read = system,call,log,verbose,agent,user,config,dtmf,reporting,cdr,dialplan
;write = system,call,agent,user,config,command,reporting,originate
[root]

[root]
secret = frameip
deny=0.0.0.0/0.0.0.0
permit=127.0.0.0/255.255.255.0
read=all
write=all
```

Figure 2. *« manager Asterisk »*

adresse mail, SDA, plan de SDA, renvoi, supervision) sans passer directement par les fichiers de configuration d'Asterisk.

Il est aussi important de sélectionner le bon « driver TAPI » pour les postes de travail et le click to dial par exemple, afin de ne pas être obligé d'octroyer des droits supplémentaires sur le manager à un utilisateur lorsqu'il tente d'utiliser cette fonction. (De plus, si quelqu'un écoute les flux ou utilise un sniffer, il a de grandes chances de récupérer le mot de passe administrateur du manager…il est donc préférable d'utiliser le mode « originate »)

D'autre part, le mode d'authentification des téléphones IP reste somme toute assez basique, puisque certains flux sont en clairs et puisque le challenge est réalisé avec un hash simple en "MD5" et pas de chiffrement… Ce qui renforce l'importance de la politique de mot de passe.

Pour finir, les nouvelles releases en test bénéficient déjà de certaines réponses (V1.6.2) et d'avancées en matière de sécurité comme le support TLS pour le SRTP, le renforcement de certains mécanismes de sécurité ou encore le support du T140 pour les messages texte, le support du SS7 dans DAHDI, l'amélioration des CDR, de la gestion du Dial Plan, du « MeetMe », des files d'attente, des nouvelles fonctions SIP et bien d'autres…

Les problèmes protocolaires

La ToIP est maintenant une partie intégrante des réseaux LAN (voir la rubrique sites web), elle est donc soumise à un ensemble de problématiques purement réseau dont voici quelques exemples quelques soit les constructeurs…

- Le Déni de service (DoS) sur VoIP qui consiste à lancer une multitude de requêtes, « flooding SIP », « TCP syn » ou « UDP », (par exemple, demandes d'enregistrement et d'appels…) jusqu'à saturation des services VoIP. Ces types d'attaques ciblent souvent les serveurs, les passerelles, les proxy ou encore les téléphones IP qui voient leurs ressources sont rapidement épuisées par ces requêtes dont l'objectif est de perturber voire mettre hors service le système ciblé. Une autre attaque également répandue consiste à envoyer des commandes « BYE » au téléphone afin de mettre fin à la conversation en cours…
- La manipulation du contenu multimédia et des signaux est une attaque qui permet d'injecter un fichier son dans un flux RTP par le biais d'une attaque « RTP Insertsound ».
- Attaque par « relecture » ou « Détournement d'enregistrement » de sessions autorisées obtenues grâce à une analyse de trame par un « sniffer » sur le réseau ou par interception de trafic. Cette atta-

que se déroule au niveau du protocole SIP, elle utilise la commande « Register » qui sert à localiser un utilisateur par rapport à son adresse IP. Le pirate peut alors rejouer ces sessions de « register » valide en modifiant uniquement l'adresse IP de destination en sa faveur…Cette attaque est due au fait que le protocole SIP transite une partie des informations en clair, il est donc possible de mettre en place du SIPS qui intègre des mécanismes d'authentification et assure l'intégrité des données.

- Le « Man in the Middle » (figure 3 : exemple d'échange protocolaire) (MITM) est une des attaques les plus connues ; elle permet à l'assaillant de se positionner entre le client et le serveur afin d'intercepter les flux ciblés qui sont échangés. Le pirate usurpe alors l'adresse MAC (spoof MAC) de ces 2 parties par l'empoisonnement du cache ARP des switches (ex: Ettercap + plugin « chk_poisoning ») afin d'être transparent dans ces échanges. Les données transitent alors au travers du système pirate. Dans le cas de la ToIP cette technique est utilisée pour « l'Eavesdropping » (« Oreille indiscrète ») lui permettant ainsi d'écouter et d'enregistrer les conversations entre les interlocuteurs mais aussi de récupérer un ensemble d'informations confidentielles. cette technique est aussi utilisée pour d'autres protocoles (SSL, DNS, SSH…)
- Le « switch jamming » (figure 4 : ARP spoofing attaques) est une attaque qui consiste à saturer le plus rapidement possible les tables de commutation d'un commutateur avec des milliers de paquets contenant de fausses adresses MAC (flooding MAC) dans le but de le transformer en « mode répéteur » (HUB) afin que toutes les trames soient en diffusion (broadcast) continue sur tous les ports. Nb : cette attaque ne fonctionne pas avec tous les commutateurs et elle est généralement peu discrète…
- La déviation par un paquet ICMP consiste à utiliser un générateur de paquet du type « frameip.exe » (disponible sur internet) et à forger ses propres paquets ICMP de déviation (type 5) à destination du client afin de lui indiquer que la route utilisée n'est pas optimale et lui communiquer par la même occa-

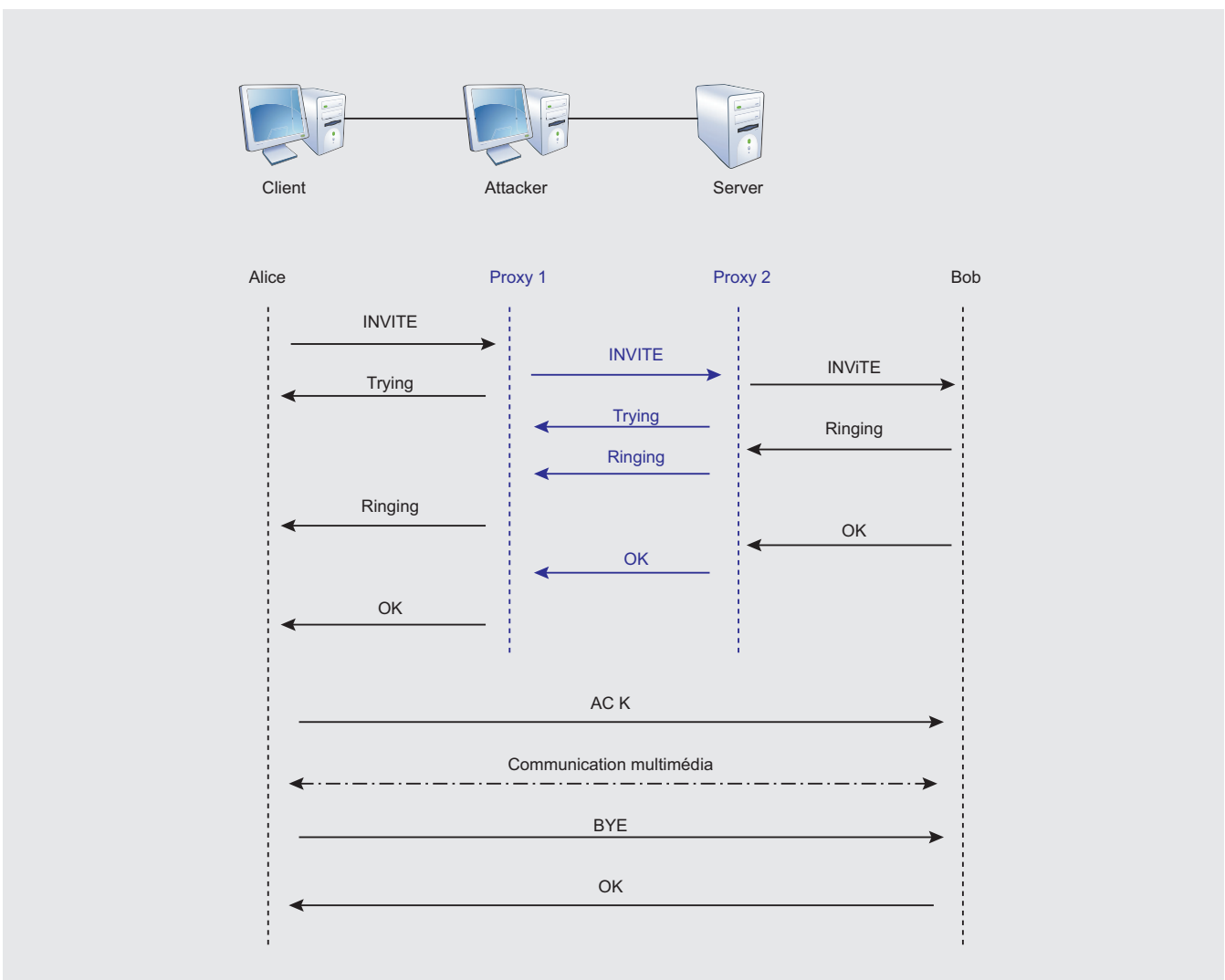


Figure 3. *exemple d'échange protocolaire*

sion la nouvelle route qui permettra de rediriger les flux vers un hôte pirate qui ferait office de passerelle. L'objectif de cette attaque est multiple : écoute, enregistrement (comme pour MITM), DoS… Il est important de noter que cette attaque ne permet pas de rediriger le trafic d'une connexion entre deux machines du même réseau local (même plan adresse IP) puisque le trafic échangé ne passe pas par une passerelle.

- « VLAN Hopping » consiste à découvrir le N° de VLAN attribué à la ToIP (en récupérant la VLAN Database, utilisation d'un snifer…) dans un environnement LAN et de marquer des trames Ethernet directement dans ce VLAN en forgeant ses propres trames. Cette technique permet de s'affranchir d'une partie de la sécurité associée aux VLANs… (label spoofing)
- Dans certains cas, un simple « brute force » sur le serveur TFTP « officiel » permet de télécharger la configuration complète d'un équipement et d'apprendre un certain nombre d'éléments…
- En SIP, les équipements bénéficient d'une réelle intelligence embarquée contrairement aux MGCP par exemple… il est donc possible de demander à un téléphone « d'afficher » lors d'un appel à son destinataire un numéro de téléphone différent du sien. En interne, cela n'a que peu d'effet. Pourtant, une personne pourrait prétendre appeler depuis le centre de sécurité ou le bureau du directeur… et demander l'exécution d'actions particulières par exemple. De l'extérieur, être discret, se faire passer pour quelqu'un autre, ou encore afficher systématiquement pour tous les appels sortants, un numéro tiers pirate (modification sur passerelle ou IPbx). Lorsque les destinataires tenteront de recontacter leurs collègues et/ou partenaires en faisant « BIS » ou rappeler dans l'historique des appels, ils tomberont systématiquement sur le numéro (payant) qui était affiché (ex : 1,4€ par appel).

Ports généralement utilisés en ToIP

TFTP	UDP 69
MGCP	UDP 2427
LDAP	TCP 389
Backhaul (MGCP)	UDP 2428
Tapi/Jtapi	TCP 2748
http	TCP 8080/80
SSL	TCP 443
SCCP	TCP 3224
Skinny	TCP 2000-2002
SNMP	UDP 161
SNMP Trap	UDP 162
DNS	UDP 53
SIP	TCP 5060
SIP/TLS	TCP 5061
H.323 RAS	TCP 1719
H.323 H.225	TCP 1720
H.323 H.245	TCP 11000-11999
H.323 Gatekeeper Discovery	UDP 1718
RTP	16384-32767
NTP	UDP 123

Ensuite, au niveau des applications

- Après avoir amélioré la sécurité sur vos réseaux et vos protocoles, il reste néanmoins d'autres points noirs comme les interfaces graphiques des IPbx, l'usage du mode HTTPS n'est pas forcé, voire non activé !
- De plus, au niveau des stations de travail, l'authentification aux pages d'administrations de l'IPbx et/ou des interfaces utilisateurs peut être couplée à des cookies ou du NTLM qui ne sont pas forcement un gage de sécurité... et encore moins quand l'utilisateur demande à son navigateur de garder les mots de passe en mémoire…
- D'autre part, il existe un nombre de failles et/ou de vulnérabilités non négligeable directement sur

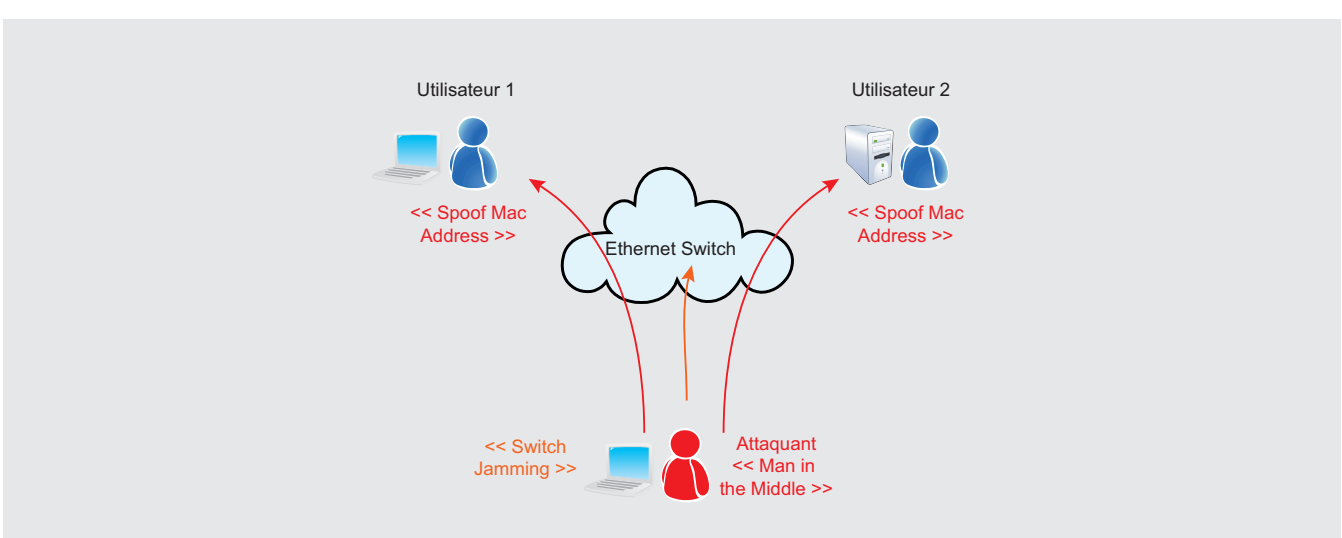


Figure 4. *ARP spoofing attaques*

les interfaces des IPbx, exécution forcée de script comme le « cross site scripting » ou autres, la falsification des requêtes inter-sites, injections de données…

- Plus simplement, par défaut, les équipements ToIP bénéficient de services standard activés (ex : telnet ouvert, port SNMP et read/write avec *community name* par défaut, interface Web de configuration de l'équipement permettant la modification de la configuration en http, récupération d'informations directes, statistiques, reboot à distance, port de troubleshooting, authentification basique, Services echo et time ouverts…) Toutes ces inattentions sur les équipements facilitent souvent les actions d'une personne mal intentionnée…

Quelques techniques utilisées par les pirates

Généralement, un simple « Snifer » sur votre LAN permettra à un pirate de récupérer une multitude d'informations telles que les protocoles utilisés sur votre réseau, (CDP, STP, DNS, DHCP, LDAP, MAPI…) et d'obtenir des renseignements sur votre plan adressage IP, vos VLANs, codecs utilisés, utilisateurs, login, mot de passe, découverte de vos infrastructures, de la topologie, la marque des équipements, les IOS, vos serveurs, leurs OS et versions, version des applications…

- Le "fuzzing" est une méthode permettant de tester les logiciels et de mettre en évidence des dysfonctionnements potentiels, afin de constater la réaction du système lorsqu'il reçoit de fausses informations. Cette méthode utilise un certain nombre d'outils de sécurité utilisés notamment lors d'audits, mais certaines personnes mal intentionnées s'en servent dans le but de trouver et exploiter des failles (compte administrateur, augmentation des délais, DOS, écoute…).
- Spam VoIP ou SPIT (Spam Over Internet Telephony) - le SPIT est, comme son nom l'indique, un SPAM dont l'objectif est la diffusion d'un message publicitaire en initiant et/ou relayant un maximum d'appels à l'aide de « Bots » à destination de millions d'utilisateurs VoIP depuis le système compromis. Cette technique a de multiples conséquences, comme la saturation du système, des MEVO, des communications simultanées… Une utilisation détournée du SPIT consiste aussi à initier un maximum d'appels à destination de N° surtaxés dans le but d'enrichir des organisations malveillantes…
- Vishing (Voice Phishing) – Cette technique est comparable au « phishing » traditionnel, dans le but d'inciter des utilisateurs à divulguer des données confidentielles, voire sensibles (par exemple : noms d'utilisateur, mots de passe et ou numéros de compte, N° de sécurité sociale, code bancaire, adresses, coordonnées…). Dans notre cas, c'est un SPIT qui diffuse un message demandant aux utilisateurs d'appeler un numéro spécifique pour vérifier les informations en questions et il ne reste plus qu'à attendre que le téléphone sonne . Après avoir récupéré ces données, le pirate les utilise ou les vend à des tiers !
- Vol d'adresses électroniques – L'usage du « Voicemail » se multipliant, chaque utilisateur ou presque bénéficie d'une adresse de messagerie électronique associée, cette attaque consiste à bombarder le serveur de « voicemail » du domaine ToIP avec des milliers d'adresses mail de test (ex : *nom.prenom@client.fr / nomprenom@client.fr / nom@client.com*...). Chaque adresse non valide est retournée, pour le reste, l'attaquant peut ainsi en déduire un certain nombre d'adresses mail valides qu'il pourra alors utiliser à sa guise pour d'autres attaques (SPIT, Vishing, SPAM mail…).
- Détournement de trafic ou « Phreaking », est une méthode historique dès les débuts de la téléphonie, elle consiste à ne pas payer les communications et à rester anonyme. En ToIP, ce détournement s' effectue après récupération d'un couple login/pass valide ou après accès physique d'un utilisateur non autorisé à un téléphone. Les pionniers du « Phreaking » (Cf figure 5). Imaginons maintenant que le pirate ait réussi (par différents moyens) à obtenir un login aux droits suffisants pour modifier la configuration de votre Ipbx. Il peut alors paramétrer un « Trunck » à destination d'un autre IPbx et organiser la revente de minutes par dizaines de milliers dans un autre pays… en utilisant le même concept.

Exemple de quelques outils

SIPtap, Wireshark, VOMIT (Voice Over Misconfigured Internet Telephones), VoIPong, NESUS, nmap, troyens divers, UCSniff (ARP Saver, VLAN Hopping), Digitask pour skype, SIVUS, Teardown, Cain, Backtrack, Dsniff, YLTI, scapy, SIPcrack…

Figure 5. *accès physique d'un utilisateur non autorisé à un téléphone*

Quelques exemples de bonne pratique et de solutions

Rassurez-vous, il existe un ensemble de techniques pour contrer ces attaques . Cependant, il est conseillé de faire appel à des experts qui vous accompagneront dans cette démarche et seront pédagogues. Le risque ZERO n'existe pas, généralement, en matière de sécurité, il est assez simple de mettre en place un niveau de sécurité de l'ordre de « 70% à 80% » de protection contre les attaques, qui représente le premier palier de sécurité bien suffisant pour une entreprise lambda. Toujours simple, mais cette fois-ci, cela nécessite un investissement afin d'atteindre les « 85% à 90%» de sécurité pour une entreprise. Ensuite, dépasser les 90% à 95% devient plus compliqué et nécessite une expertise et des investissements lourds. Pourtant, ce niveau de sécurité est primordial pour une banque, une assurance, ou encore, les grandes industries dont le chiffre d'affaires dépend en majorité de la stabilité de leurs systèmes d'informations, de téléphonies (centre d'appel…)

Il existe enfin un niveau ultime de sécurité, aux niveaux gouvernemental, aérospatial, renseignements, services spéciaux, armées…qui doit atteindre au minimum les 99%. Non seulement ce niveau requiert des infrastructures conséquentes mais également une réelle expertise 24/7.

Pour en revenir à notre focus sur la sécurité de la téléphonie sur IP, il est important de mener la réflexion sécurité en amont en phase de design de l'architecture de ToIP. L'amélioration des niveaux de sécurité passe, entre autres, par le respect de bonnes pratiques et l'application de solutions efficaces dont en voici quelques exemples :

- Mettre en place une réelle politique de Mot de passe déjà difficilement gérée pour les comptes des stations de travail et encore moins pour les comptes de téléphonie sur IP (complexité, durée de validité, longueur mini…)
- Mettre en place des VLAN et/ou VRF dédiée ainsi qu'une solution de supervision/monitoring de vos infrastructures LAN/WAN et Voix afin de cloisonner vos réseaux et de bénéficier d'indicateurs spécifiques à Intégrer aux tableaux de bord sécurité des systèmes d'informations (TBSSI)
- Des solutions existent en matière de détection d'attaque (IDS/IPS) et/ou de modification suspicieuse sur le protocole ARP avec « Arpwatch » ou « snort », ou mécanisme basique dans le monde du switching comme le « port security » qui limite le nombre d'adresses MAC utilisables par port, ou encore du « 802.1x »…
- Implémenter des pare-feux Statefull « nouvelle génération » avec une reconnaissance protocolaire plus avancée (ADN applicatif…)
- Sécurisation des protocoles SIP et RTP par l'utilisation de PKI (Public Key Infrastructure) et la mise en place du « SIPS », « SRTP », « SRTCP » utilisant le « DTLS » RFC 4347…
- Limiter les accès aux personnes non autorisées (contrôle d'accès), ne pas autoriser les prestataires à se connecter au LAN, ni WIFI (hors guets), toujours être présent en salle serveurs lors d'intervention et tracer les accès aux zones critiques.
- Suppression des anciens comptes et/ou inutiles, suppression des logiciels ou modules inutiles sur l'IPbx et les stations de travail.
- Maîtrise et limitation des « softphones »…
- Mettre en pratique la surveillance et l'exploitation des logs d'infrastructures…
- D'autre part, l'architecture physique ou logique du réseau LAN est très importante. Certains ont pour philosophie de maintenir deux réseaux physiquement séparés, d'autres sont partisans d'une plus grande flexibilité de mise en place de VLAN…
- Côté WAN, ne jamais exposer son IPBX par une IP Public même « natée », ni en DMZ publique et/ou directement à l'extérieur même un module spécifique à cet usage est proposé, privilégier le mode VPN SSL ou IPSEC par le biais du firewall.
- Si nécessaire, envisager l'ajout de boîtier de chiffrement matériel.
- Etc…

Sites web

- *http://www.frameip.com/voip/*
- *http://www.frameip.com/smartspoofing/*
- *http://www.architoip.com/entete-sip/*
- *http://www.architoip.com/toip-open-source/*
- *http://www.authsecu.com/sniffers-reseaux-commutes/sniffers-reseaux-commutes.php*
- *http://www.authsecu.com/affichage-news/1085-news-securite-les-pare-feux-%22nouvelles%22-generation.htm*

DAVID HURÉ – PROJECT DEPARTMENT MANAGER – FRAMEIP

Responsable du bureau d'étude de FrameIP, passionné et expert en réseau, sécurité et téléphonie sur IP, j'apporte ma contribution et mon retour d'expérience dans un esprit de partage. Entre autre, conférencier pour des écoles d'ingénieur et des séminaires technologiques (ToIP, Vidéo, QoS et optimisation WAN, PCA…). *David.hure@frameip.fr*

Tony Deslandes - credits : Pugstudio, Air

Serveurs mandataires Comment les utiliser ?

Paul Amar

S'intéresser à l'architecture de son propre réseau ou celui d'une entreprise nécessite de faire de nombreux choix quant à l'infrastructure.

Cet article explique...

- Le principe des différents types de serveur mandataire dans la sécurité informatique, leurs utilisations.

Ce qu'il faut savoir...

- Notions en réseau, architecture informatique.

Beaucoup d'objectifs sont demandés comme l'optimisation, la performance ou la sécurité. Les critères sont variés et demandent d'être étudiés de façon rigoureuse comme la sécurité, par exemple, pour que notre infrastructure ne contienne aucune faille susceptible d'être exploitée par un pirate.

Nous verrons ensemble ce que sont les serveurs mandataires, communément appelés « proxys », et le rôle qu'ils jouent dans la sécurité.

Après la présentation des proxys dits « simples » et les proxys inversés, nous nous intéresserons à leur utilisation au sein d'un réseau.

Les utilités d'un serveur mandataire

Un serveur mandataire ou encore « proxy » est un serveur qui travaille au niveau application. Il est lié à un protocole précis, comme, par exemple, le protocole HTTP. (Protocole utilisé pour le Web)

Cette fonction du proxy consiste à relayer des demandes d'informations d'un réseau vers un autre.

De façon plus générale, le fonction première d'un proxy est le relai des requêtes d'un poste client vers un poste serveur (le principe-même de la communication). Le proxy joue un rôle d'intermédiaire entre cesx deux entités (cf Figure 1).

Les deux entités doivent pouvoir communiquer sans problème, sans perte ni altération de données.

Certains ne voient peut-être pas encore l'utilité d'un serveur mandataire, pourtant il assure de nombreuses fonctions telles que :

Mise en cache d'informations : si certaines informations sont demandées régulièrement (ex : pour une recherche identique et répétée sur Google.fr, la page reste la même). Un serveur proxy peut garder en « cache » certaines informations comme la page de Google, et ainsi l'afficher de nouveau au client qui la redemande procurant ainsi un gain réél en performance sur le réseau, car moins de requêtes sont envoyées.

Logs des requêtes : le serveur mandataire peut, à chaque nouvelle requête reçue la stocker dans des fichiers de logs, conservant ainsi une trace des activités sur le réseau.

Cette méthode s'utilise pour centraliser les requêtes sur un serveur proxy particulier. (ex: uUniversité qui cherche à avoir un log de toutes les requêtes faites en son sein)

Une entreprise rencontrant des problèmes judiciaires pourra toujours se défendre grâce aux logs de ses serveurs (s'ils n'ont pas été falsifiés) et qui comportent des informations comme :

Qui se connecte ? Depuis où ? Que fait la personne ? Son historique peut même être conservé.

La sécurité : supposons un parc informatique d'une centaine d'ordinateurs. Si tous les postes ont accès à internet via le serveur proxy, les informations y sont centralisées. Dans le cas d'un problème au niveau du réseau informatique dépourvu de proxy, chaque ordinateur pourrait accéder à internet directement ; il faudrait auditer tous les postes pour savoir lequel est défaillant. Le fait d'utiliser un serveur proxy centralise toutes les

requêtes, optimise la gestion du réseau (en utilisant son cache) et en cas de problème, regarder seulement les logs du serveur proxy pour avoir une idée générale du problème soulevé.

Le filtrage : comme indiqué plus tôt, centraliser les requêtes sur un serveur proxy permet de « garder la main » sur certaines activités réseau d'un usager. Au lieu de mettre des règles de filtrage à tous les postes sur le réseau, les mettre uniquement sur le serveur proxy, il sera alors interrogé dès qu'un des postes souhaitera faire une action spécifique. Il n'y a pas de risque de corruption de la machine (contournement des règles de sécurité concernant le filtrage) et toutes les informations sont centralisées. Il y a là aussi une meilleure performance concernant la maintenance du parc informatique car s'il faut changer certaines règles, seules celles du serveur proxy devront l'être. Le filtrage peut se faire en fonction de nombreux critères : adresse IP, Paquets, Contenu, par personnes authentifiées, … (ex : dans une entreprise, faire en sorte que les sites de jeu en ligne etc. soient bannis).

L'authentification : un proxy est indispensable dans la communication des deux entités, si elles sont bien configurées. Dès lors, le proxy servira à identifier les utilisateurs avec un login / password. Un mauvais login n'aura pas accès aux ressources demandées. Cela ajoute une autre « couche » non négligeable de sécurité dans notre infrastructure. Un pirate verra ses actions limitées jusqu'à ce qu'il trouve le couple login / password qui convient.

Les différents types de serveurs mandataires

Le proxy simple joue le rôle d'un intermédiaire entre les ordinateurs d'un réseau local et Internet.

La plupart du temps, nous entendons parler de proxy « http » ou encore « https » qui sont les plus courants sur la toile.

Ils sont souvent utilisés avec un cache, permettant ainsi d'éviter une surcharge sur le réseau et d'accéder plus vite à la page.

Prenons le cas où Pierre veut accéder à la page de : *http://www.site.com* . La requête de Pierre passera par le serveur proxy du réseau local qui cherchera la page à l'adresse *http://www.site.com* car elle n'est pas dans son cache. Elle sera ensuite acheminée à Pierre qui aura sa page.

Si Jean veut accéder à la page quelques minutes plus tard, la requête arrivera au serveur proxy qui recherchera cette page dans son cache. Dans l'affirmative, il la renverra directement à Jean sans passer par le site en question afin d'éviter la surcharge de requête. Ce système permet d'éviter un minimum la congestion d'un réseau, réduit l'utilisation de la bande passante tout en réduisant le temps d'accès (cf Figure 2).

Soit les données du cache sont stockées dans la RAM (c'est-à-dire la mémoire vive du serveur), soit elles le sont sur le disque. Il ne faut pas qu'il garde la page indéfiniment mais qu'il vérifie si, sur le site distant, la page est toujours la même. (ex : un site d'actualité informatique sera différent tous les jours (voire toutes les heures), la page dans le cache doit être changée régulièrement).

Des serveurs proxy existent pour de multiples services sur internet comme http, FTP, SMTP, IMAP, …

Le Reverse-proxy

Le reverse proxy, à l'inverse du proxy simple est qu'il permet aux utilisateurs d'internet d'accéder à des serveurs propres au réseau interne.

Dès lors, le terme « reverse » commence à avoir du sens, étant donné qu'il réalise l'inverse d'un proxy simple.

De nombreuses fonctionnalités des « reverse proxys » se révèlent parfois utiles, comme la protection des serveurs internes contre des attaques directes.

Puisque les requêtes sont « interceptées » par le proxy, il est donc en mesure de les analyser et les sécuriser si besoin pour éviter des problèmes de sécurité sur le serveur.

Le reverse-proxy sert de relais pour les utilisateurs souhaitant accéder à un serveur interne.

Parallèlement, le proxy offre des avantages comme la notion de cache qui soulage les charges du/des serveurs internes. La page d'accueil d'un site Web peut être gardée dans le cache du proxy et ainsi, le trafic vers le serveur Web est allégé.

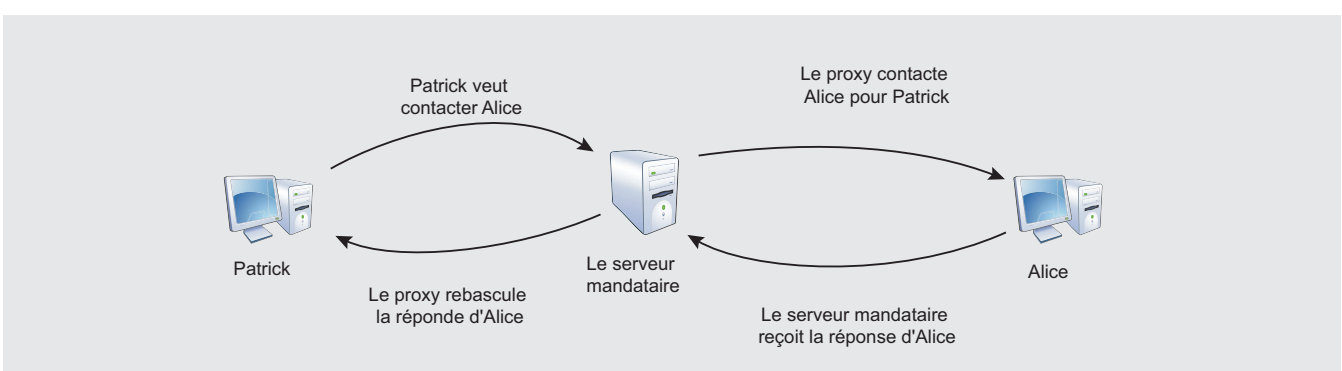


Figure 1. *Schéma théorique d'un serveur mandataire simple.*

De plus, imaginons une infrastructure dans laquelle deux serveurs auraient les mêmes fonctionnalités (ex: serveur Web). Le reverse-proxy ferait du « load-balancing », c'est-à-dire de la répartition de charge concernant les serveurs. Les requêtes sont alternées en fonction des deux serveurs évitant ainsi la congestion susceptible de provoquer un dysfonctionnement du serveur comme un déni de service (cf Figure 3).

Autres types de serveurs mandataires

Traitons maintenant des proxys dits « SOCKS ».

SOCK est un protocole réseau ; il permet à des applications client/serveur d'employer de manière transparente les services d'un pare-feu.

SOCKS est l'abréviation de « socket » et est une sorte de proxy pour les « sockets ».

En soit, les proxys SOCKS ne savent rien du protocole utilisé au-dessus (que ce soit du http, ftp, …), cf Figure 4.

Certains l'auront peut-être compris, SOCKS est une couche intermédiaire entre la couche applicative et la couche transport (d'après le modèle OSI).

Ces proxys diffèrent du proxy traditionnel qui ne supporte que certains protocoles.

Ils sont plus modulables et sont ainsi aptes à répondre à des besoins variés.

Deux composants sont nécessaires quant à l'utilisation d'un serveur mandataire SOCKS qui sont :

Le serveur SOCKS est mis en œuvre au niveau de la couche application

Le client SOCKS est mis en œuvre entre les couches application et transport

Pour ce qui est du mode de fonctionnement :

L'application se connecte à un proxy SOCKS

Le serveur mandataire vérifie la faisabilité de la demande

Il transmet la requête au serveur si c'est faisable

Cependant, il existe d'autres types de serveurs mandataires comme les proxys anonymes ou encore les proxys transparents (ou proxys par interception), … qui ne seront pas décrits dans cet article.

Nous allons maintenant nous intéresser à une étude de cas d'un reverse-proxy au sein d'une entreprise, et son utilisation (d'un point de vue sécurité) dans l'entreprise.

Étude de cas au sein d'une entreprise

Prenons en exemple une entreprise basique : actuellement, la plupart des compagnies ont leur propre site web afin de présenter les produits, prestations de services qu'ils offrent.

Idéalement, cela signifie que leur réseau informatique doit comporter un serveur Web.

Imaginons que nous utilisions un reverse-proxy qui permettrait l'accès à ce serveur Web.

Quelle serait l'utilité d'un tel équipement ?

Les fonctionnalités de serveurs mandataires et des reverse-proxy en général ont été élicités.

Le reverse-proxy nécessaire serait utilisé pour les protocoles HTTP/HTTPS puisque c'est un serveur Web.

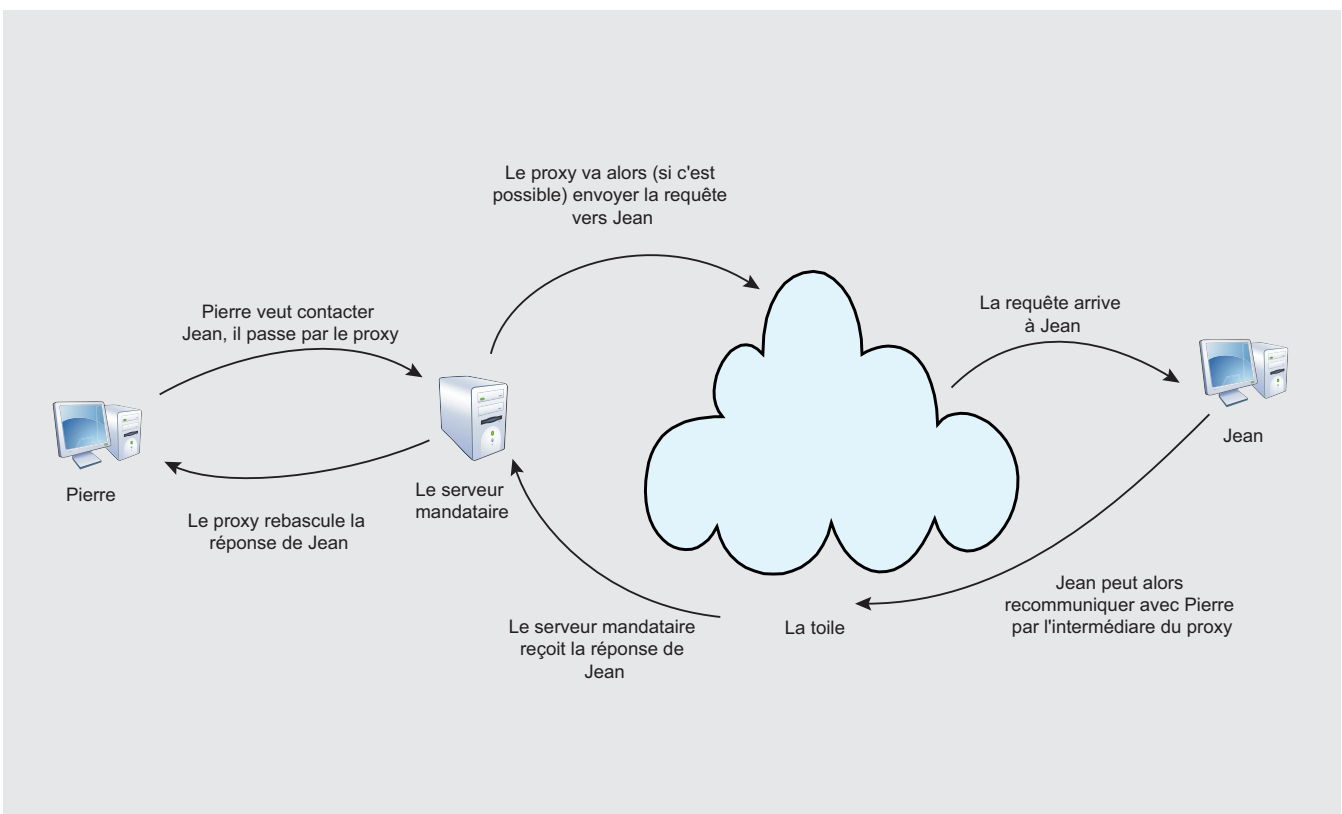


Figure 2. *Utilisation d'un serveur mandataire simple.*

Nous utiliserions cet équipement pour qu'il contrôle les requêtes envoyées en plaçant certains filtres afin d'éviter des attaques (qu'elles soient de type XSS, SQL Injection, XSHM, XSRF,…).

Selon le besoin en bande passante, nous pourrions faire en sorte que le reverse-proxy mette en cache les pages les plus demandées. Cela aurait pour effet de réduire l'usage de la bande passante, de ne pas congestionner le réseau et de procurer plus de rapidité aux internautes.

De plus, l'utilisation d'un reverse-proxy éviterait certains DoS (Déni de Service) qui ne seraient pas de très forte intensité et allégerait les charges sur le serveur Web interne.

Si l'entreprise est assez importante, elle pourrait disposer de plusieurs serveurs Web similaires (pour éviter qu'en cas de panne, le site ne soit plus du tout accessible) ; le reverse-proxy réaliserait du load-balancing, à savoir enverrait les requêtes à l'un des deux serveurs Web, de façon égale pour répartir les tâches.

Dans un second temps, afin de centraliser toutes les requêtes vers l'extérieur, un proxy interne serait à envisager. Comme expliqué dans les rubriques précédentes, cela peut être intéressant pour réaliser des filtrages. Afin d'éviter d'accéder à du contenu non sollicité (ex : des sites de jeux en ligne au travail), tous les postes du parc informatique iraient sur internet en passant par un serveur proxy simple.

Les règles de filtrage ne seraient alors qu'à ajouter au serveur proxy qui les prendrait en compte pour chaque requête reçue. Puisque cet équipement ne serait pas « accessible » depuis les autres ordinateurs, il y aurait moins facilement de contournement des règles de sécurité.

En outre, si un problème persiste sur le réseau, le serveur proxy (intermédiaire entre le réseau privé et la toile) diagnostiquerait ce problème. Grâce à la journalisation et les logs du trafic, il est possible de remonter aux postes infectés au lieu de chercher le(s) problème(s) sur tout le parc informatique.

Vous l'aurez remarqué, les possibilités sont nombreuses quant à leurs utilisations.

Annexes

- *http://fr.wikipedia.org/wiki/Proxy* - Article de Wikipédia sur les serveurs mandataires
- *http://fr.wikipedia.org/wiki/R%C3%A9partition_de_charge* – Article concernant le phénomène de « load-balancing » ou encore répartition de charge
- *http://www.commentcamarche.net/contents/lan/proxy.php3* - Article intéressant sur le site CommentCaMarche.net
- *http://www.squid-cache.org/* - Squid, Proxy pouvant utiliser les protocoles FTP, HTTP/HTTPS et Gopher (peut servir de Reverse-proxy)
- *http://varnish-cache.org/* - Autre « reverse-proxy » Varnish
- *http://imapproxy.org/* - Proxy utilisant le protocole IMAP

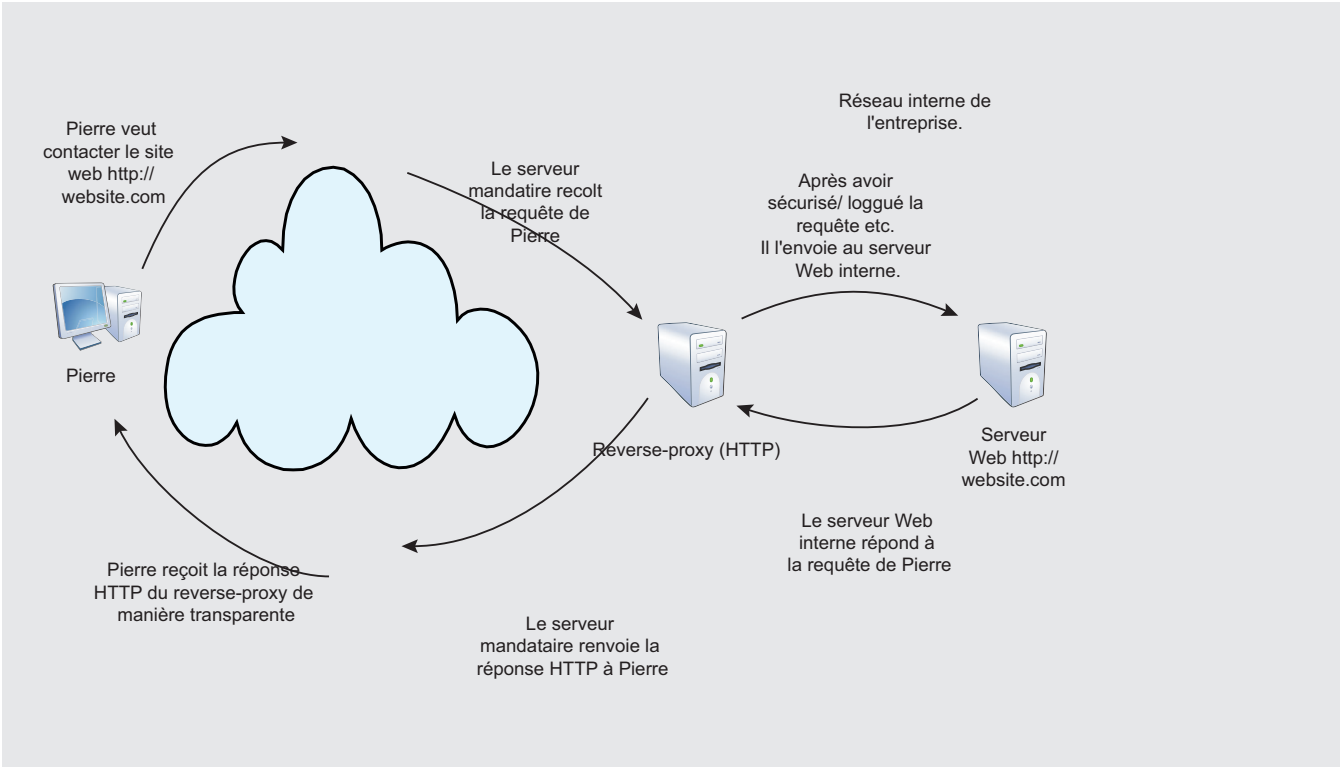


Figure 3. *Utilisation d'un reverse-proxy.*

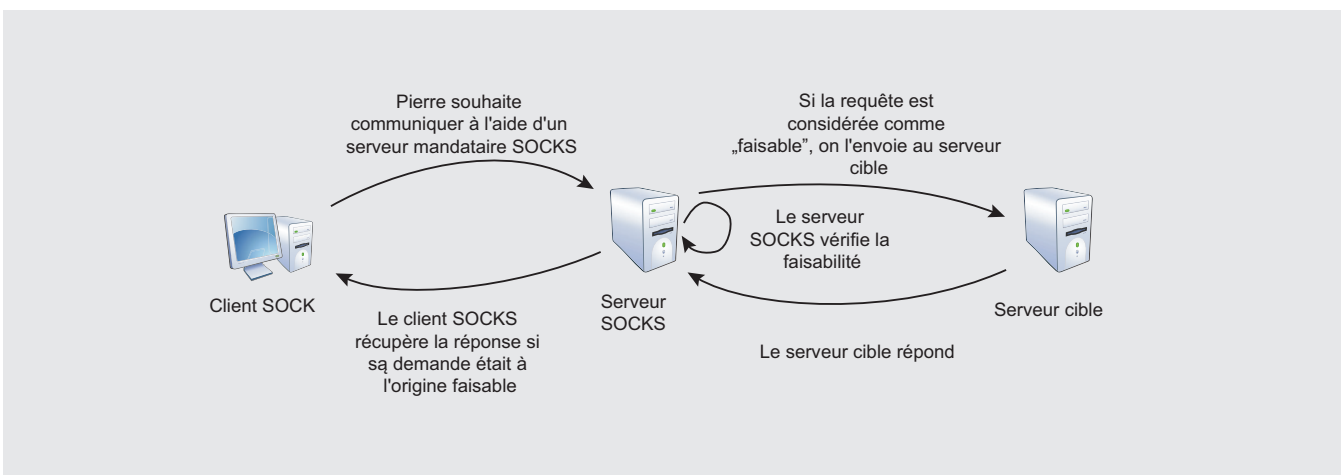


Figure 4. *Utilisation d'un serveur mandataire SOCKS.*

Cependant, il existe toujours des entreprises qui n'utilisent pas ce genre d'équipement pourtant très utile. Leurs raisons sont diverses, notamment une méconnaissance de l'installation d'un tel équipement. Enfin,

Une certaine maintenance est nécessaire afin de garder à jour les logiciels.

Conclusion

Nous venons de voir les principaux types de serveurs mandataires utilisés sur la toile et nous avons tenté d'éclaircir certains points, notamment pour les personnes n'ayant que de vagues connaissances des proxys (à savoir, les plus souvent utilisés : les proxys Web).

Cependant, il ne faut pas oublier qu'utiliser un serveur mandataire ne nous protège pas contre tous les risques potentiels sur la Toile. Bien entendu, coupler ce type de serveur à d'autres systèmes tels que des HIDS (Système de détection d'intrusion), NIDS (Système de détection d'intrusion réseau), etc. est un bon moyen de sécuriser son réseau car les différentes traces laissées par les pirates peuvent être analysées.

À PROPOS DE L'AUTEUR

Actuellement en école d'ingénieur, Paul étudie différents aspects de la sécurité informatique.

Passionné par la sécurité depuis plusieurs années, il s'intéresse particulièrement à la sécurité des systèmes d'informations et souhaiterait si possible y consacrer sa carrière.

Dès maintenant téléchargez gratuitement le numéro 6/2010 dédié à l'E-commerce !

Rendez-vous sur : www.hakin9.org/fr

Connexion sécurisée grâce à SSH

Régis Senet

Protégez vos communications de l'ensemble des actes de piratage en chiffrant vos données ! La mise en place de protocole sécurisé pour les communications distantes est vivement recommandée du fait que nous ne pouvons pas savoir qui nous écoute à chaque instant dans l'immensité de l'internet. Il est donc temps de remplacer tous ces protocoles et de posséder vos accès SSH.

Cet article explique...

- L'intérêt d'utiliser des protocoles sécurisé
- La mise en place d'un serveur SSH

Ce qu'il faut savoir...

- Connaissance en système d'exploitation UNIX/Linux

SSH ou bien Secure Shell est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite toutes les trames sont chiffrées. Il devient donc impossible d'utiliser un sniffer tel que Wireshark pour voir ce que fait l'utilisateur via les données qu'il reçoit ou envoi. Le protocole SSH a initialement été conçu avec l'objectif de remplacer les différents programmes rlogin, telnet et rsh qui ont la fâcheuse tendance de faire passer en clair l'ensemble des données d'un utilisateur vers un serveur et inversement, permettant à une personne tierce de récupérer les couples de login/mot de passe, les données bancaire etc.

Le protocole SSH existe en deux versions: la version 1.0 et la version 2.0. La version 1.0 souffrait de failles de sécurité et fut donc rapidement rendue obsolète avec l'apparition de la version 2.0. La version 2 est largement utilisée à travers le monde par une grande majorité des entreprises. Cette version a réglé les problèmes de sécurité liée à la version 1.0 tout en rajoutant de nouvelles fonctionnalités telles qu'un protocole de transfert de fichiers complet. La version 1.0 de SSH a été conçue par Tatu Ylönen, à Espoo, en Finlande en 1995. Il a créé le premier programme utilisant ce protocole et a ensuite ouvert une société, SSH Communications Security pour exploiter cette innovation. Cette première version utilisait certains logiciels libres comme la bibliothèque Gnu libgmp, mais au fil du temps ces logiciels ont été remplacés par des logiciels propriétaires. SSH Communications Security a vendu sa licence SSH à F-Secure.

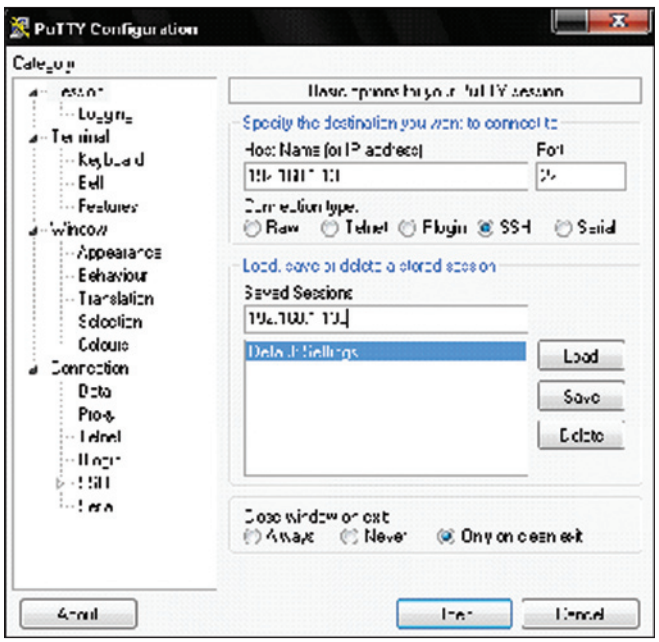


Figure 1. *Logiciel Putty*

Installation

Au cours de cet article, la distribution utilisée fut une Debian 5.0 (*Lenny*) entièrement mise à jour. Attention, il est possible que certaines commandes ne soient pas tout à fait identiques sur une autre distribution. L'ensemble des installations va se réaliser grâce au gestionnaire de paquets propre à un système Debian : APT (Advanced Package Tool).

Mise à jour du système

Il est possible à tout moment qu'une faille de sécurité soit découverte dans l'un des modules composant votre système que ce soit Apache ou quoi que ce soit d'autre. Certaines de ces failles peuvent être critiques d'un point de vue sécurité pour l'entreprise. Afin de combler ce risque potentiel, il est nécessaire de régulièrement mettre à jour l'ensemble du système grâce à divers patches de sécurité.

Il est possible de mettre à jour l'ensemble du système via la commande suivante :

```
nocrash:~# apt-get update && apt-get upgrade
```

Le système d'exploitation est maintenant complètement à jour, il est donc possible de mettre en place un serveur SSH dans de bonnes conditions. Il est possible de ne pas passer par cette étape mais elle est fortement conseillée pour la sécurité ainsi que la stabilité de votre système d'exploitation.

Installation de SSH

Dans un premier temps, nous allons réaliser l'installation via le gestionnaire de paquet propre à un système Debian, le système APT (Advanced Package Tool). Nous verrons l'installation via les sources un peu plus tard.

```
nocrash:~# apt-get install ssh
```

Installation de SSH en ligne de commande.

- Les paquets suivants sont des dépendances du paquet SSH :
- openssh-client
- client shell sécurisé
- openssh-server
- Serveur shell sécuritaire

Installation via les sources

Nous allons à présent voir l'installation via les sources directement disponibles sur le site officiel d'OpenSSH (*http://www.openssh.org/*).

Dans l'éventualité où vous avez déjà installé OpenSSH via le gestionnaire de paquet comme vu précédemment, il est nécessaire de le désinstaller avant de faire une nouvelle installation.

```
nocrash:~# apt-get autoremove ssh
```

Une fois correctement désinstallé, il est possible de réaliser l'installation par les sources :

```
nocrash:~# mkdir /usr/ssh
nocrash:~# cd /usr/ssh/
nocrash:~# wget ftp://ftp.openbsd.org/pub/OpenBSD/
                    OpenSSH/portable/openssh-5.2p1.tar.gz
nocrash:~# tar xzvf openssh-5.2p1.tar.gz
nocrash:~# cd openssh-5.2p1/
nocrash:~# ./configure --bindir=/usr/local/bin --
                    sbindir=/usr/sbin --sysconfdir=/etc/
                    ssh
nocrash:~# make && make install
```

En cas d'erreur, reportez-vous à NB.

Figure 2. *Nous voici ainsi connecté sur notre serveur distant grâce à Putty*

Configurations préalable

Sur certaines distribution, afin de pouvoir activer le serveur SSH, il est nécessaire de supprimer un fichier présent par défaut, le fichier `/etc/ssh/sshd_not_to_be_run` avant de pouvoir lancer le serveur SSH.

```
nocrash:~# rm -rf   /etc/ssh/sshd_not_to_be_run
```

Une fois le fichier supprimé (s'il existe), il est possible de passer à la phase de configuration.

Configuration du serveur SSH

Le fichier regroupant l'ensemble des configurations du serveur SSH se trouve être le fichier `/etc/ssh/sshd_config`. Nous allons éditer ce fichier afin de pouvoir y faire nos modifications.

Figure 3. *puTTYKey generator*

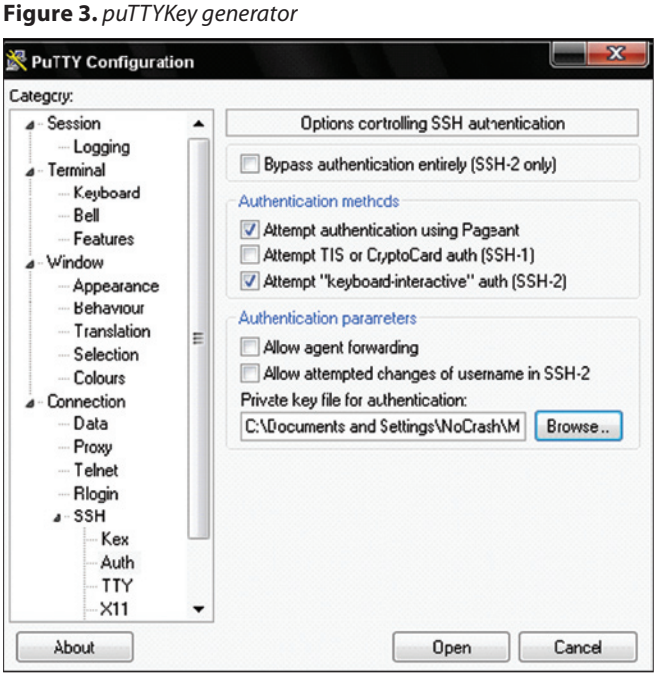


Figure 4. *Configuration de Putty*

```
nocrash:~# vi /etc/ssh/sshd_config
```

Voici les paramètres principaux au bon paramétrage de notre serveur SSH :

```
Port 22
```

Cette directive signifie simplement que le serveur SSH va écouter sur le port 22 (port par défaut). Il est possible de faire écouter le serveur SSH sur plusieurs ports en rajoutant plusieurs fois cette directive avec des ports différents.

```
Protocol 2
```

Cette directive permet de spécifier que seul la version 2 du protocole SSH sera utilisée, la version 1 de SSH est obsolète pour des raisons de sécurité.

```
PermitRootLogin no
```

Cette directive permet d'empêcher toute connexion à distante avec l'utilisateur root (superutilisateur). Un accès distant grâce avec l'utilisateur root par une personne mal intentionnée pourrait être catastrophique pour l'intégrité du système.

```
PermitEmptyPasswords no
```

Cette directive permet d'interdire les connexions avec un mot de passe vide, il est indispensable de mettre cette directive à *no*

```
LoginGraceTime 30
```

Cette directive permet de limiter le laps de temps permettant de se connecter au SSH

```
AllowUsers nocrash
AllowGroups admin
```

Ces directives donnent la possibilité de n'autoriser que certains utilisateur et/ou groupe

```
AllowTcpForwarding no
X11Forwarding no
```

Ces directives permettent de désactiver le transfert de port TCP et le transfert X11

Authentification

Il existe deux méthodes afin de pouvoir s'authentifier en SSH sur une machine distante. Ces deux méthodes sont :

- Authentification par clé
- Authentification par mot de passe

Authentification par clé

L'authentification par clé est un très bon moyen pour s'authentifier de manière sécurisé. En effet, des clés asymétriques de type DSA vont être générées.

Afin de générer nos clés DSA, nous allons utiliser la commande suivante :

```
nocrash:~# ssh-keygen -t dsa
```

Les clés générées par défaut auront une taille de 1024 bits, ce qui est largement suffisant pour assurer une bonne protection.

Deux clés vont donc être générées :

- Une clé publique présente dans le fichier ~/.ssh/id_dsa.pub avec les permissions 644.
- Une clé privée présente dans le fichier ~/.ssh/id_dsa avec les permissions 600.

Lors de la création des clés, une passphrase vous sera demandée, il est important de choisir un mot de passe complexe. En effet, cette passphrase permet de crypter la clé privée (clé devant rester absolument à votre seule connaissance).

Au cas où vous vous seriez trompé dans votre passphrase, il est toujours possible de la modifier grâce à la commande suivante :

```
nocrash:~# ssh-keygen -p
```

La dernière étape avant de pouvoir s'authentifier par clé publique est d'autoriser sa propre clé. Pour cela, il est nécessaire d'ajouter votre clé publique dans le fichier /.ssh/authorized_keys de la machine sur laquelle, vous voulez vous connecter.

Pour réaliser cela, il est nécessaire d'utiliser la commande suivante :

```
nocrash:~# ssh-copy-id -i ~/.ssh/id_dsa.pub login@
                  Adresse_de_la_machine
```

Pour mon exemple :

```
nocrash:~# ssh-copy-id -i ~/.ssh/id_dsa.pub
                  nocrash@192.168.1.138
```

Voici à quoi pourrait ressembler le fichier de configuration :

```
Port 22
Protocol 2
ListenAddress 192.168.1.138
ServerKeyBits 1024
PermitRootLogin no
PubkeyAuthentication yes
AuthorizedKeysFile      .ssh/authorized_keys
IgnoreRhosts yes
#(mettez ces 2 options à no si vous ne voulez offrir
                  l'accès qu'aux utilisateurs ayant
                  enregistré leur clés):
```

Authentification par mot de passe

L'authentification par mot de passe quand à elle est une authentification très simple à mettre en place du fait qu'il n'y a rien à mettre en place.

Il est nécessaire que l'utilisateur voulant se connecter possède un compte sur la machine distante et c'est tout.

Dans l'exemple suivant, nous voulons nous connecter avec l'utilisateur NoCrash sur la machine répondant à l'adresse IP 192.168.1.138. Nous allons donc vérifier que cet utilisateur existe bien avant tout. Dans le cas où il n'existerait pas, il est nécessaire de le créer sur la machine distante avec un mot de passe (ne pas oublier la directive PermitEmptyPasswords no).

```
nocrash:~# cat /etc/passwd | grep nocrash
nocrash:x:1000:1000:nocrash,,,:/home/nocrash:/bin/bash
```

Le *x* juste après le login permet de spécifier qu'un mot de passe est bien présent.

Voici à quoi pourrait ressembler le fichier de configuration :

```
Port 22
Protocol 2
ListenAddress 192.168.1.138
ServerKeyBits 1024
PermitRootLogin no
PubkeyAuthentication no
IgnoreRhosts yes
PasswordAuthentication yes
Compression yes
```

A présent que l'ensemble des configurations sont faites, il est nécessaire de lancer le serveur SSH. Pour cela, nous allons utiliser la commande suivante :

```
nocrash:~# /etc/init.d/ssh start
```

Si tout ce passe bien, nous allons avoir le message suivant :

```
Starting OpenBSD Secure Shell server :sshd.
```

Il est alors possible de pouvoir se connecter à la machine distante.

Connexion

Afin de se connecter en SSH sur une machine distante possédant un serveur SSH, il est possible d'utiliser la li-

gne de commande dans le cas où vous êtes sous Linux ou MAC.

Pour cela, voici la commande à utiliser (voir Figure 2) :

```
nocrash:~# ssh login@ Adresse_de_la_machine
```

Soit pour notre exemple :

```
nocrash:~# ssh nocrash@192.169.1.138
```

Pour les machines de type Windows, il n'existe pas de client SSH en natif, il est alors nécessaire de passer par des logiciels, tels que Putty (voir Figure 1).

Authentification par clé

Comme il est possible de le voir dans l'authentification par mot de passe, nous allons tenter de nous connecter au serveur distant via SSH grâce à Putty.

Putty ne sachant pas gérer les clefs générées par le serveur avec `ssh-keygen` il faut utiliser l'utilitaire puttygen afin de générer un couple de clés utilisable.

Ouvrez puTTYKey generator puis générer une nouvelle paire de clés (voir Figure 3).

Cliquez à présent sur *Save public key* et *Save private key* afin de sauvegarder les clés. Il est à présent nécessaire de copier la clé publique que vous venez de générer sur le serveur distant à l'adresse suivante : `~/.ssh/authorized_keys`

Une fois les clés générées, il est possible de se connecter avec Putty. Il est nécessaire de spécifier l'emplacement de la clé privée dans *Connection >> SSH >> Auth* avant de se connecter (voir Figure 4).

Astuces

Dans le fichier de configuration de ssh soit le fichier `/etc/ssh/sshd_config`, il n'est pas obligatoire mais fortement conseillé de modifier le port utilisé par SSH. Par défaut, il s'agit du port 22. Ce petit changement permet de *brouiller* un attaquant qui s'attendrais à voir un SSH sur le port 22 et non pas sur le port 1998 par exemple :

```
Port   1998
```

Afin de vérifier que vos mots de passe sont assez complexes, il est possible de tenter de les casser vous-mêmes afin de vérifier si quelqu'un d'autre en est capable.

NB. Si vous système a récemment été installé, il est possible que certaine librairies soit manquante. Il est nécessaire de les installer :

- Librairie `gcc : apt-get install gcc`
- Librairie `libcrypto / SSL: apt-get install libssl-dev`

Pour cela, il est nécessaire d'installer John The Ripper, un utilitaire de cassage de mot de passe :

```
nocrash:~# apt-get install john
```

Il est maintenant possible de vérifier vos mots de passe :

```
nocrash:~# john /etc/shadow
```

Les mots de passe trouvés sont donc jugés comme étant trop simple, il est préférable de les modifier.

Conclusion

La mise en place de protocole sécurisé pour les communications distantes est vivement recommandé du fait que nous ne pouvons pas savoir qui nous écoute à chaque instant dans l'immensité de l'internet. Il ne faut pas non plus croire que le danger vient simplement de l'internet. En effet, la majorité des actes de piratages informatique se font au sein d'une même entreprise par les employés eux-mêmes. Il est donc temps de protéger vos communications de l'ensemble de ces voyeurs, il est temps de chiffrer vos données, il est temps de remplacer tous ces protocoles laissant vos données transiter en claires sur le réseau, il est temps de posséder vos accès SSH.

A PROPOS DE L'AUTEUR...

Régis SENET est actuellement étudiant en quatrième année à l'école Supérieur d'informatique Supinfo. Passionné par les tests d'intrusion et les vulnérabilités Web, il tente de découvrir la sécurité informatique d'un point de vue entreprise. Il est actuellement en train de s'orienter vers le cursus CEH, LPT et Offensive Security.

Contact : *regis.senet@supinfo.com*

Site internet : *http://www.regis-senet.fr*

Page d'accueil : *http://www.openssh.com/*

Succès de HT Bridge

L'objectif de High-Tech Bridge consiste à fournir une valeur-ajoutée à ses clients en leur proposant des services de sécurité informatique fiables, de confiance et hautement efficaces, basés sur les dernières technologies uniques de son département de Recherche et de Développement.

HIGH-TECH BRIDGE®

INFORMATION SECURITY SOLUTIONS

High-Tech Bridge SA est une société genevoise née en 2007 dont l'actionnariat est détenu entièrement par des privés Suisses. Elle propose des services de Ethical Hacking au travers des tests de pénétration, des scans de vulnérabilités, des investigations numériques légales ; elle propose également ses prestations d'expert en prévention du cyber-crime.

Son emplacement stratégique en Suisse garantit confidentialité, objectivité et absolue neutralité. L'objectif de High-Tech Bridge consiste à fournir à ses clients une valeur ajoutée en leur proposant des services de sécurité informatique fiables, de confiance et hautement efficaces, fondés sur les dernières technologies uniques de son département de Recherche et de Développement. Ce département de Recherche en Sécurité Informatique permet d'unir les efforts mondiaux des meilleurs experts en sécurité. Les experts de High-Tech Bridge s'efforcent en permanence de découvrir de nouvelles vulnérabilités et techniques d'attaque avant que des pirates ne le fassent, ce qui lui permet d'anticiper les problèmes et de protéger au mieux les clients.

Depuis Juin 2010, High-Tech Bridge propose des services d'expertise complémentaires, avec ses modules de Scan de Vulnérabilités Automatisé et de Veille Sécuritaire.

Le Directeur du Département de Ethical Hacking de High-Tech Bridge, M. Frédéric Bourla, s'exprime sur ce sujet : "L'introduction d'un service distinct de Scan de Vulnérabilités Automatisé souligne l'avantage concurrentiel de High-Tech Bridge sur le marché de l'Ethical Hacking. Aujourd'hui, les sociétés, en majorité, proposent des scans de vulnérabilités automatisés ou semi-automatisés sous l'appellation abusive de « tests de pénétration », dont l'approche est radicalement différente de celle de High-Tech Bridge. D'après notre expérience, plus de 60% des vulnérabilités critiques identifiées durant un test de pénétration sont découvertes lors d'une analyse effectuée manuellement par nos experts. Il s'agit généralement d'un savant mélange de vulnérabilités connues dont la signature finale ne permet pas une détection efficace par un processus automatisé".

En même temps, le directeur du Département de Recherche et Développement de High-Tech Bridge, M. Marcel Salakhoff, introduit un nouveau service exclusif de veille de vulnérabilités 0-Day : "High-Tech Bridge est fière d'être la première entreprise suisse à proposer ce service unique et de haute qualité. La prestation s'adresse principalement aux grandes institutions financières, aux sociétés multinationales et aux gouvernements désireux de réduire au maximum les risques de compromission".

L'élargissement de sa gamme de services permettra à High-Tech Bridge d'augmenter ses parts de marché et de poursuivre son expansion sur le marché de la sécurité informatique en Suisse.

Supervisez votre réseau grâce à Nagios

Régis Senet

A l'heure actuelle, les réseaux informatiques sont absolument partout. Ils sont devenus indispensables au bon fonctionnement général de nombreuses entreprises et administrations. Tout problème ou panne risque d'avoir de lourdes conséquences tant financières qu'organisationnelles. La supervision des parcs informatiques est alors nécessaire et indispensable.

Cet article explique...

- Ce qu'est Nagios / Centreon / Cacti

Ce qu'il faut savoir...

- Connaissance en système d'exploitation Linux et les bases des réseaux

Nous appuierons l'ensemble de nos explications sur l'utilisation d'un serveur GNU/Linux fondé sur une distribution Debian, la Debian 5.0 (Debian Lenny). La distribution Debian a été choisie pour sa solidité, sa stabilité et sa popularité. NB. Vue la longueur de l'article, nous l'avons divisé en 2 parties. Vous trouverez la suite de l'article Nagios dans la partie 2.

Installations des pré-requis système

À tout moment une faille de sécurité est susceptible d'être découverte dans l'un des modules composant votre système, que ce soit Apache, un module du noyau ou quoi que ce soit d'autre. Certaines de ces failles sont parfois critiques pour l'entreprise, d'un point de vue sécurité. Afin de prévenir ce risque potentiel, il est nécessaire de régulièrement actualiser l'ensemble du système

```
nocrash:~# aptitude -y update && aptitude -y safe-
                    upgrade
```

Le système d'exploitation est maintenant complètement à jour, la mise en place de notre serveur de supervision peut se faire dans de bonnes conditions.

Si cette étape n'est pas indispensable, elle est toutefois fortement conseillée pour la sécurité et la stabilité de votre système d'exploitation.

Installation des librairies requises

Durant toute la mise en place du serveur de supervision, de nombreuses librairies seront nécessaires au bon fonctionnement de l'ensemble des logiciels à installer. Elles ne seront pas toutes détaillées mais une liste des librairies nécessaires est représentée au Listing 1.

Nagios, ainsi que l'ensemble des outils de supervision que nous allons mettre en place, résument les activités des machines grâce à des graphiques plus ou moins avancés. Pour cela, il est nécessaire de disposer des bonnes librairies graphiques :

```
nocrash:~# aptitude install -y libgd2-noxpm-dev
libjpeg62-dev libpng12-dev libjpeg62
```

Installation d'un serveur de temps

Le serveur sera constamment à l'heure, grâce à un serveur de temps. En effet, si le serveur n'est plus à la bonne heure, les graphiques et les fichiers de journalisation seront faux, entraînant ainsi des erreurs lors de la lecture des données.

Pour installer un serveur de temps, aussi appelé serveur NTP (*Network Time Protocol*), il suffit d'utiliser la commande suivante :

```
nocrash:~# aptitude install -y  ntp-simple ntpdate
```

Pour toute modification sur la configuration du serveur NTP, il sera nécessaire de modifier le fichier de configuration */etc/ntp.conf* même si des serveurs sont initialement présents dans ce fichier.

Installation d'un serveur de messagerie SMTP

Lors de changement de statut d'un hôte ou plus, Nagios a la possibilité d'envoyer des mails à une ou plusieurs

adresses prédéfinies. Mais la présence d'un serveur SMTP est indispensable.

Nous utiliserons le très célèbre *postfix* afin de répondre à nos besoins en la matière (cf Figure 1).

Son installation sera ici très basique n'incluant pas toutes les étapes de configuration, d'optimisation et de sécurité normalement nécessaires.

Pour l'installation, voici la commande à lancer :

```
nocrash:~# aptitude install -y  postfix mailx
```

Pour le type d'utilisation dont nous avons besoin et pour plus de commodité au niveau des configurations, nous choisirons *Site Internet*.

Installation d'une base de données MySQL

Durant nos installations, de nombreux logiciels devront stocker une très grande quantité de données en rapport avec les activités, les graphiques, les utilisateurs etc. À cette fin, nous mettrons en place une base de données. Nous avons opté pour une base de données MySQL car c'est l'un des SGDB (*Système de Gestion de Base de Données*) le plus utilisé et aussi en raison de sa licence libre (cf Figure 2).

Installons donc la dernière version de MySQL :

```
nocrash:~# aptitude install -y mysql-server-5.0
libmysqlclient15-dev
```

Une importante partie de la sécurité de la base de données passe par la complexité du mot de passe. Il est vraiment indispensable qu'il soit complexe, mélangeant chiffres et lettres majuscules ou minuscules.

Une fois la base de données installée, il faut modifier les droits des fichiers de configuration :

Listing 1. *Installation des pré-requis*

```
nocrash:~# aptitude install -y build-essential zip unzip sudo lsb-release libxml2-dev libevent1 snmp snmpd bind9-host dnsutils
                    qstat zlib1g-dev radiusclient1 fping libldap-dev libgnutls-dev libradiusclient-ng-dev nmap libconfig-
                    inifiles-perl libcrypt-des-perl libdigest-hmac-perl libsnmp-perl libdigest-sha1-perl libgd-gd2-perl
                    libnet-snmp-perl gettext locales
```

Listing 2. *Installation de SSHGuard*

```
nocrash:~# cd /var/
nocrash:~# wget "http://downloads.sourceforge.net/project/sshguard/sshguard/sshguard-1.4/sshguard-1.4.tar.bz2"
nocrash:~# bzip2 -d sshguard-1.4.tar.bz2
nocrash:~# tar -xf sshguard-1.4.tar
nocrash:~# rm -rf sshguard-1.4.tar
nocrash:~# mv sshguard*/ sshguard/
nocrash:~# cd sshguard/
nocrash:~#./configure --with-firewall=iptables
nocrash:~# make && make install
```

Listing 3. *Mise en place des fichiers de configuration Nagios*

```
nocrash:~# mv /etc/nagios3 /etc/nagios3.orig
nocrash:~# mkdir /etc/nagios3
nocrash:~# cp -Rt /etc/nagios3 /etc/nagios3.orig/nagios.cfg /etc/nagios3.orig/apache2.conf /etc/nagios3.orig/
                    stylesheets/
nocrash:~# chown nagios:www-data /etc/nagios3
nocrash:~# chmod ug+w /etc/nagios3
```

Listing 4. *Installation de Centreon*

```
nocrash:~# cd /usr/src/
nocrash:~# wget http://download.centreon.com/centreon/centreon-2.1.1.tar.gz
nocrash:~# tar xzf centreon-2.1.1.tar.gz
nocrash:~# rm -rf centreon-2.1.1.tar.gz
nocrash:~# cd centreon-2.1.1
nocrash:~#./install.sh -i
```

```
nocrash:~# chown -R root /etc/mysql/
nocrash:~# chmod 740 /etc/mysql/my.cnf
```

MySQL est également livrée avec un script de sécurisation de la base de données nommé `mysql_secure_installation` qu'il est vivement conseillé d'exécuter :

```
nocrash:~# mysql_secure_installation
```

Sécurisation du serveur SSH

Pour permettre les communications avec la machine distante, il est nécessaire de mettre en place un serveur SSH permettant une communication chiffrée entre le client et le serveur :

```
nocrash:~# aptitude install -y ssh
```

Une fois le serveur SSH correctement installé, il convient d'apporter quelques modifications dans son principal fichier de configuration, le fichier */etc/ssh/sshd_config* :

- *LoginGraceTime 120* devient *LoginGraceTime 30*. La directive *LoginGraceTime* indique en secondes, la durée entre la connexion au serveur d'un client et sa déconnexion lorsque le client ne s'est pas authentifié.
- *PermitRootLogin yes* devient *PermitRootLogin no*. La directive *PermitRootLogin* placée à *no* interdit à l'administrateur principal (root) de se connecter directement à la machine distante. C'est une mesure de sécurité à mettre obligatoirement en place. SI un accès root tombe entre de mauvaises mains, les conséquences pourraient être terribles.
- *X11Forwarding yes* devient *X11Forwarding no*. La directive *X11Forwarding* placée à *no* interdit l'utilisation à distance de l'interface graphique présente sur le serveur.

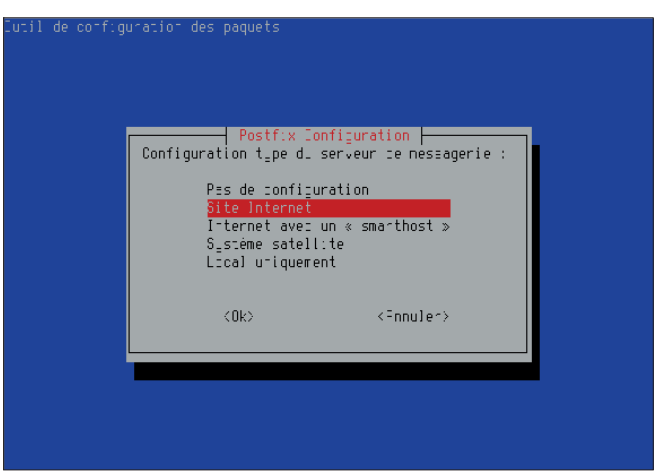


Figure 1. *Configuration de Postfix*

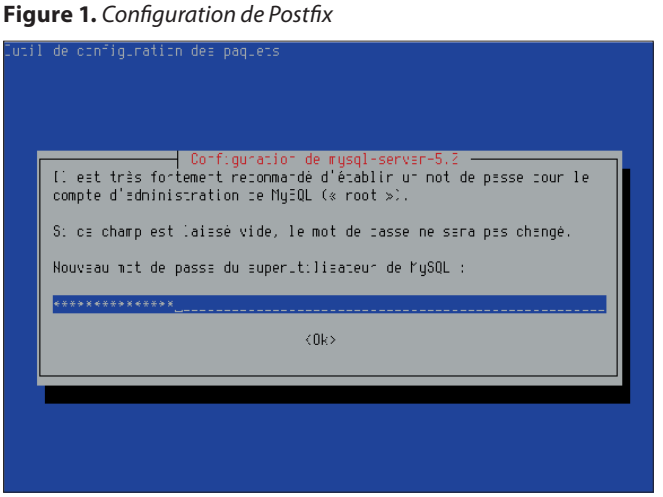


Figure 2. *Choix du mot de passe MySQL*

De plus, nous ajouterons la directive suivante à la fin du fichier : *AllowTcpForwarding no*

```
nocrash:~# echo "AllowTcpForwarding no" >> sshd_config
```

L'installation de Molly Guard est une excellente chose. En effet, il peut facilement nous arriver de confondre deux terminaux sur notre machine. Molly Guard demandera donc le nom de la machine afin de confirmer son arrêt ou son redémarrage.

```
nocrash:~# aptitude install -y molly-guard
```

Pour éviter des attaques par dictionnaire ou par bruteforce contre le protocole SSH et destinées à trouver le mot de passe, il est préférable d'installer un *anti-bruteforceur* au lieu de bloquer complètement le protocole SSH. Cet outil se nomme *Denyhosts*. Denyhosts est un logiciel tournant en arrière-plan analysant continuellement le fichier de log */var/log/auth.log* et qui, au bout de plusieurs vaines tentatives (selon la configuration) de connexions, blackliste l'IP en cause dans le fichier */etc/hosts.deny*.

Voici commencer installer *Denyhosts* simplement :

```
nocrash:~# aptitude install -y denyhosts
```

Modifier la configuration par défaut, nécessite l'édition du fichier de configuration principal de *Denyhosts : /etc/denyhosts.conf*.

Il est possible de coupler *Denyhosts* avec *SSHGuard*. *SSHGuard* éditera les règles du firewall à la volée afin d'accepter ou non les hôtes (voir Listing 2). L'ensemble des configurations sera pris en compte après le redémarrage du serveur SSH.

```
nocrash:~# /etc/init.d/ssh restart
```

Installation du serveur web

Pour pouvoir profiter de *l'interface graphique* de *Nagios*, il est impératif de mettre en place un serveur web. Nous avons opté pour un serveur Apache. Apache est le serveur HTTP le plus populaire du Web et il s'agit d'un logiciel entièrement libre.

Apache s'installe grâce à cette commande :

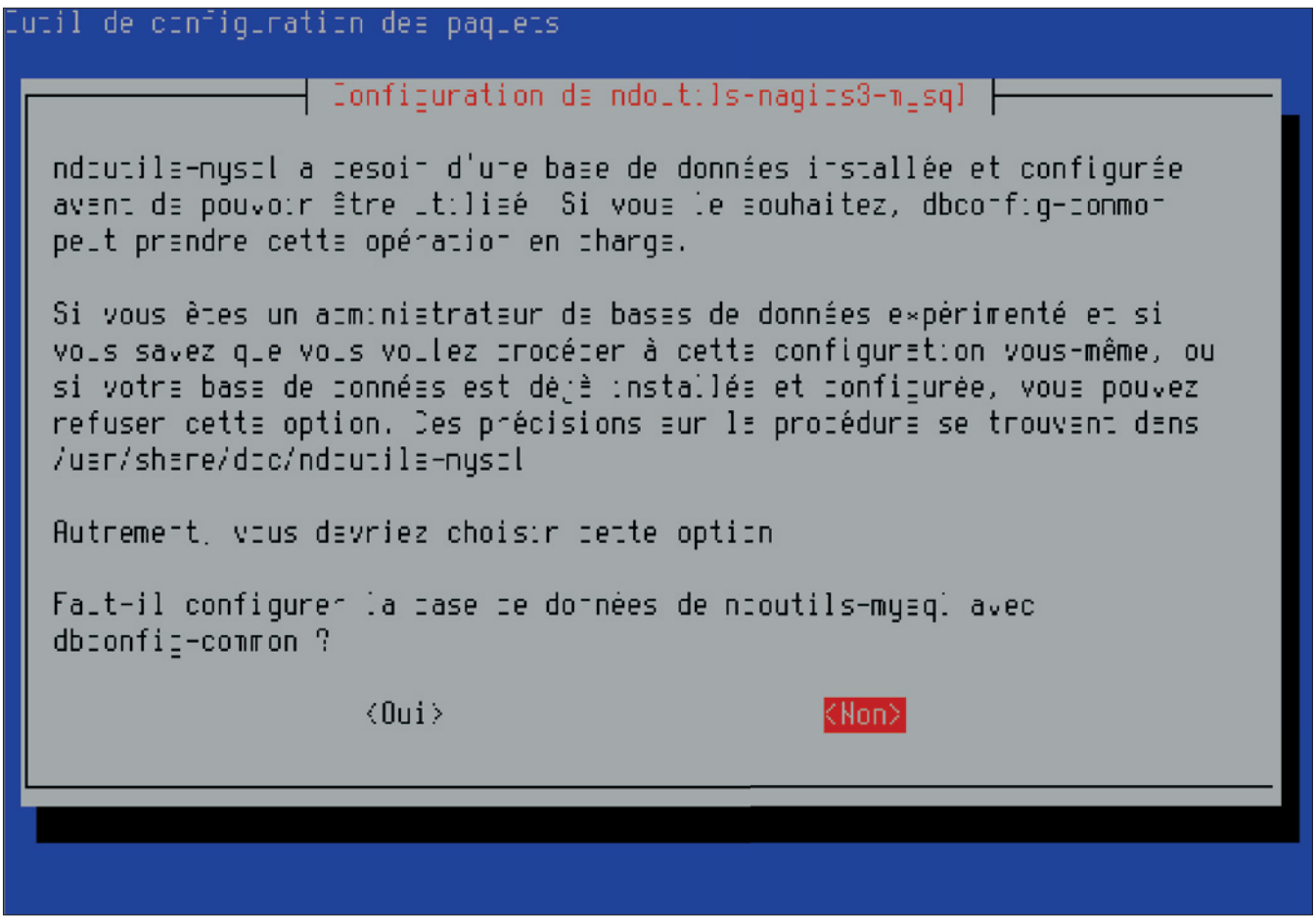


Figure 3. *Configuration de Ndoutils pour Nagios*

```
nocrash:~# aptitude install -y apache2 libapache2-mod-gnutls
                    openssl
```

Le site nous présentant *Nagios* n'étant pas un site statique, il nous est nécessaire de mettre également en place l'ensemble des librairies PHP5 pour une interprétation correcte des pages :

```
  nocrash:~# aptitude install -y php5 php5-gd php5-mysql
libapache2-mod-php5 php5-cli php5-ldap php5-snmp php-pear
apache2-threaded-dev
```

Afin d'éviter l'erreur suivante :

```
Restarting web server: apache2apache2: Could not
                    reliably determine the server's
 fully qualified domain name, using 127.0.1.1 for
                    ServerName
 ... waiting apache2: Could not reliably determine the
                    server's fully qualified
domain name, using 127.0.1.1 for ServerName
```

Lorsque vous redémarrez votre serveur Apache, nommez votre serveur de la manière suivante :

```
nocrash:~# echo "ServerName 127.0.0.1" >> /etc/apache2/apache2.
                    conf
```

Par défaut, la librairie MySQL n'est pas activée ; il est nécessaire de l'activer pour éviter tout *bug* :

```
nocrash:~# echo "extension=mysql.so" >> /etc/php5/apache2/php.ini
```

XCache accélère la vitesse du site lors de son affichage ; il s'installe très simplement :

```
nocrash:~# aptitude install -y php5-xcache
```

Puis, afin que l'ensemble des configurations soit prit en compte, il est nécessaire de redémarrer le serveur web et la base de données :

```
nocrash:~# /etc/init.d/apache2 restart
ncrash:~# /etc/init.d/mysql restart
```

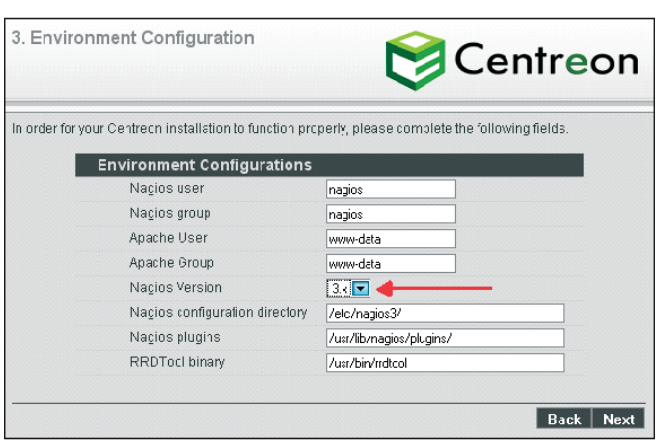


Figure 4. *Configuration de Centreon*

Listing 5a. *Choix des fichiers de configuration Centreon*

```
Press "Enter" to read the Centreon License, then type
                    "y" to accept it.

Do you want to install : Centreon Web Front
[y/n], default to [n]: y

Do you want to install : Centreon CentCore
[y/n], default to [n]: y

Do you want to install : Centreon Nagios Plugins
[y/n], default to [n]: y

Do you want to install : Centreon Snmp Traps process
[y/n], default to [n]: y

Where is your Centreon directory?
default to [/usr/local/centreon]: /usr/local/centreon

Do you want me to create this directory ? [/usr/local/
                    centreon]
[y/n], default to [n]: y

Where is your Centreon log directory
default to [/usr/local/centreon/log]: /usr/local/
                    centreon/log

Do you want me to create this directory ? [/usr/local/
                    centreon/log]
[y/n], default to [n]: y

Where is your Centreon etc directory
default to [/etc/centreon]: /etc/centreon

Do you want me to create this directory ? [/etc/
                    centreon]
[y/n], default to [n]: y

Where is your Centreon generation_files directory?
default to [/usr/local/centreon]: /usr/local/centreon

Where is your Centreon variable library directory?
default to [/var/lib/centreon]: /var/lib/centreon

Do you want me to create this directory ? [/var/lib/
                    centreon]
[y/n], default to [n]: y

Where is your CentPlugins Traps binary
default to [/usr/local/centreon/bin]: /usr/local/
                    centreon/bin

Do you want me to create this directory ? [/usr/local/
                    centreon/bin]
[y/n], default to [n]: y

Where is the RRD perl module installed [RRDs.pm]
default to [/usr/lib/perl5/RRDs.pm]: /usr/lib/perl5/
                    RRDs.pm

Where is PEAR [PEAR.php]
default to [/usr/share/php/PEAR.php]: /usr/share/php/
                    PEAR.php

Where is installed Nagios ?
default to [/usr/local/nagios]: /usr/lib/cgi-bin/
                    nagios3


Where is your nagios config directory
default to [/usr/local/nagios/etc]: /etc/nagios3

Where is your Nagios var directory ?
default to [/usr/local/nagios/var]: /var/lib/nagios3

Where is your Nagios plugins (libexec) directory ?
default to [/usr/local/nagios/libexec]: /usr/lib/
                    nagios/plugins

Where is your Nagios image directory ?
default to [/usr/local/nagios/share/images/logos]:
                    /usr/share/nagios/htdocs/images/
                    logos

Where is your NDO ndomod binary ?
default to [/usr/sbin/ndomod.o]: /usr/lib/ndoutils/
                    ndomod-mysql-3x.o


                    Where is sudo configuration file
default to [/etc/sudoers]: /etc/sudoers

Do you want me to configure your sudo ? (WARNING)
[y/n], default to [n]: y

Do you want to add Centreon Apache sub configuration
                    file ?
[y/n], default to [n]: y

Do you want to reload your Apache ?
[y/n], default to [n]: y

Do you want me to install/upgrade your PEAR modules
[y/n], default to [y]: y

Where is your Centreon Run Dir directory?
```

Listing 5b. *Choix des fichiers de configuration Centreon*

```
default to [/var/run/centreon]: /var/run/centreon

Do you want me to create this directory ? [/var/run/
                    centreon]
[y/n], default to [n]: y

Where is your CentStorage binary directory
default to [/usr/local/centreon/bin]: /usr/local/
                    centreon/bin

Where is your CentStorage RRD directory
default to [/var/lib/centreon]: /var/lib/centreon

Do you want me to install CentStorage init script ?
[y/n], default to [n]: y

Do you want me to install CentStorage run level ?
[y/n], default to [n]: y

Where is your CentCore binary directory
default to [/usr/local/centreon/bin]: /usr/local/
                    centreon/bin

Do you want me to install CentCore init script ?
[y/n], default to [n]: y

Do you want me to install CentCore run level ?
[y/n], default to [n]: y

Where is your CentPlugins lib directory
default to [/var/lib/centreon/centplugins]: /var/lib/
                    centreon/centplugins

Do you want me to create this directory ? [/var/lib/
                    centreon/centplugins]
[y/n], default to [n]: y

Where is your SNMP configuration directory
default to [/etc/snmp]: /etc/snmp

Where is your SNMPTT binaries directory
default to [/usr/local/centreon/bin/]: /usr/local/
                    centreon/bin/
```

Nagios, le centre du moteur de supervision

Aujourd'hui, les réseaux informatiques sont absolument partout. Ils sont devenus indispensables au bon fonctionnement général de nombreuses entreprises et administrations. Tout problème ou panne risque d'avoir de lourdes conséquences, tant financières qu'organisationnelles. La supervision des réseaux est alors nécessaire et indispensable. Elle permet, entre autres, d'avoir une vue globale du fonctionnement et des problèmes susceptibles de survenir sur un réseau mais aussi d'avoir des indicateurs sur la performance de son architecture. De nombreux logiciels libres ou propriétaires existent sur le marché. La plupart s'appuie sur le protocole SNMP.

Nous avons choisi d'installer l'un des logiciels les plus connus en matière de supervision de réseau informatique : Nagios. Nagios (anciennement appelé *Netsaint*) est un logiciel libre sous licence GPL permettant la surveillance des systèmes et réseaux. Il surveille les hôtes et services spécifiés, alertant lorsque les systèmes vont mal et quand ils vont mieux.

Installation des pré-requis pour Nagios

RRDTool est un logiciel libre distribué sous licence GPL utilisé pour la sauvegarde de données cycliques et le tracé de graphiques. Cet outil a été créé pour superviser des données serveur telles que la bande passante, la température d'un processeur, ... etc..

```
nocrash:~# aptitude install -y rrdtool  librrds-perl
```

Installation de Nagios

Les pré-requis étant maintenant présents, installons Nagios, le moteur de supervision :

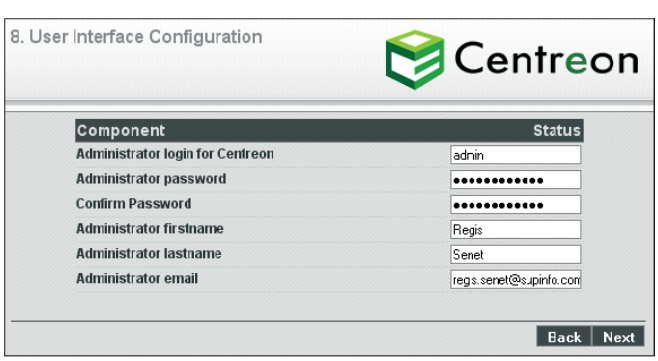


Figure 5. *Configuration de l'adminstrateur Centreon*

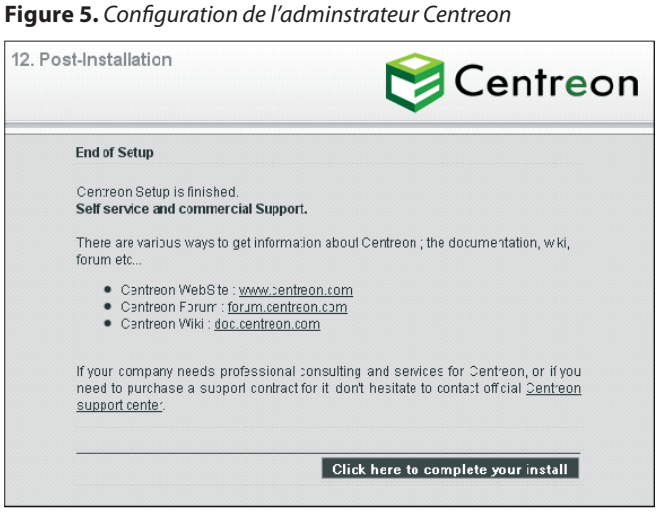


Figure 6. *Fin de l'installation avec succès*

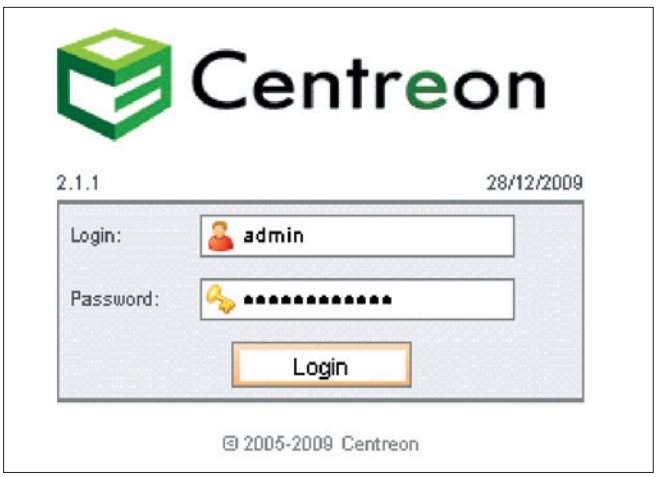


Figure 7. *Identification de Centreon*

```
nocrash:~# aptitude install -y nagios3 nagios-nrpe-plugin
                    ndoutils-nagios3-mysql
```

L'installation de Nagios, grâce à la commande `apt-get install`, a également créé un utilisateur un groupe nommés *nagios* (cf Figure 3).

Puisque Centreon utilisera sa propre structure concernant les fichiers de configuration de Nagios, il est nécessaire de les sauvegarder comme représenté au Listing 3.

L'interface web de Centreon

Centreon est un logiciel de surveillance et de supervision réseau, fondé sur le moteur de récupération d'information libre Nagios. Centreon fournit une interface simplifiée en apparence pour rendre la consultation de l'état du système accessible à un plus grand nombre d'utilisateurs, y compris des non-techniciens, notamment à l'aide de graphiques. En effet, l'ensemble des configurations sous Nagios doivent intégralement se faire à travers les différents fichiers que propose Nagios. L'installation de Centreon permettra donc une prise en main plus facile de la supervision de l'ensemble de nos réseaux.

Installation de Centreon

L'installation de Centreon se fait directement par les sources présenté dans le Listing 4.

De nombreuses questions seront posées lors de l'installation, il est nécessaire de choisir les bons fichiers de configuration afin que l'installation de Centreon colle avec notre Nagios déjà installé (cf Figure 4, 5 et 6). Attention : les valeurs en rouge correspondent aux valeurs différentes de celles par défaut.

Installation de Centreon via l'interface graphique

L'installation de Centreon s'étant bien déroulée, occupons-nous de sa configuration : elle se réalise grâce au navigateur web et à cette adresse :

La configuration de Centreon de déroule en 12 étapes :

- Etape 1/12 Il ne s'agit que d'une phase de bienvenue, cliquez sur *Start.*
- Etape 2/12 Acceptez la licence et cliquez sur *Next*.
- Etape 3/12 Vérifiez que la version de Nagios est effectivement *3.X* puis cliquez sur *Next*.
- Etape 4/12 Vérifiez que tout est à OK (écrit en vert) puis cliquez sur *Next.*
- Etape 5/12 Vérifiez que tout est à OK (écrit en vert) puis cliquez sur *Next*.
- Etape 6/12 Cette étape correspond à la configuration de la base de données. Dans *Root password for MySQL*, renseignez le mot de passe de la base de données puis celui de la base de données *ndo*. Laissez les autres paramètres à leurs valeurs par défaut puis cliquez sur *Next.*
- Etape 7/12 Si vous avez spécifié le bon mot de passe pour la base de données et que celle-ci est bien détectée, il n'y a rien à faire à cette étape. Cliquez sur *Next*.
- Etape 8/12 Spécifiez ici le nom d'utilisateur et le mot de passe de l'administrateur de Centreon (utilisateur avec lequel nous allons nous connecter) puis cliquez sur *Next*.
- Etape 9/12 L'activation de l'authentification LDAP n'est pas nécessaire. Laissez les choix par défaut et cliquez sur *Next.*
- Etape 10/12 Vérifiez que tout est à OK (écrit en vert) puis cliquez sur Next.

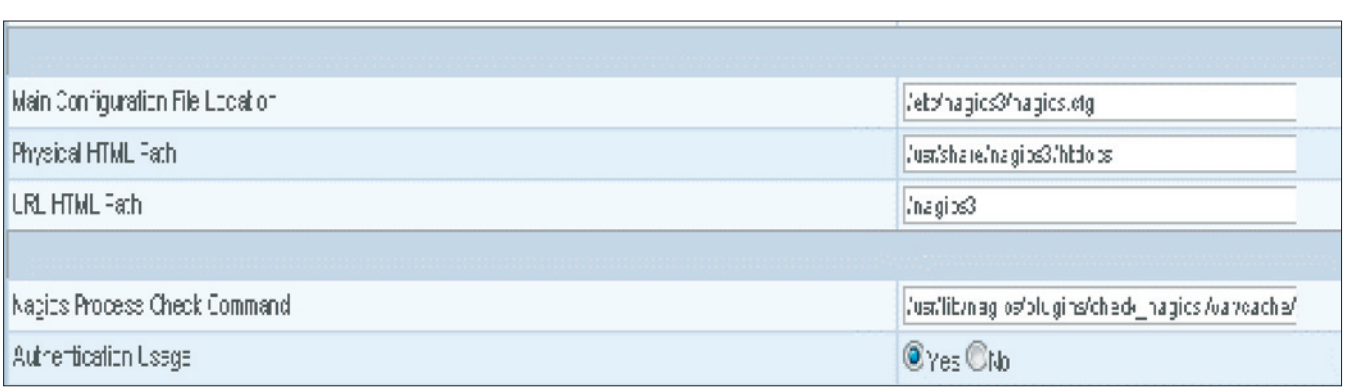


Figure 8. *Configuration Centreon (partie 1)*

- Etape 11/12 Vérifiez que tout est à OK (écrit en vert) puis cliquez sur *Next*.
- Etape 12/12 L'installation est à présent terminée, il est nécessaire de cliquer sur *Click here to complete your install* afin de terminer l'installation et d'être redirigé vers la page d'authentification (cf Figure 7). Il est à présent possible de se connecter avec les valeurs renseignées à l'étape 8.

Configuration de Centreon

Avant de procéder à la configuration de Centreon pour qu'il corresponde exactement aux paramètres de Nagios, activez Ndoutils en modifiant son fichier de configuration `/etc/default/ndoutils` et en remplaçant `ENABLE_NDOUTILS=0` par `ENABLE_NDOUTILS=1`.

```
nocrash:~# cat /etc/default/ndoutils | grep ENABLE_NDOUTILS
                    ENABLE_NDOUTILS =1
```

Une fois cette modification faite, accédez à Centreon () pour y apporter les modifications montrées ci-dessous (cf Figure 8, 9, 10, 11 et 12).

Allez dans *Configuration -> Nagios -> cgi* (menu à gauche) puis cliquez sur *CGI.cfg*

Dès lors, modifiez les valeurs suivantes :

- Physical HTML Path : /usr/share/nagios3/htdocs.
- - URL HTML Path : /nagios3.
- - Nagios Process Check Command.
- `/usr/lib/nagios/plugins/check _ nagios /var/cache/nagios3/status.dat 5 '/usr/sbin/nagios3'.`

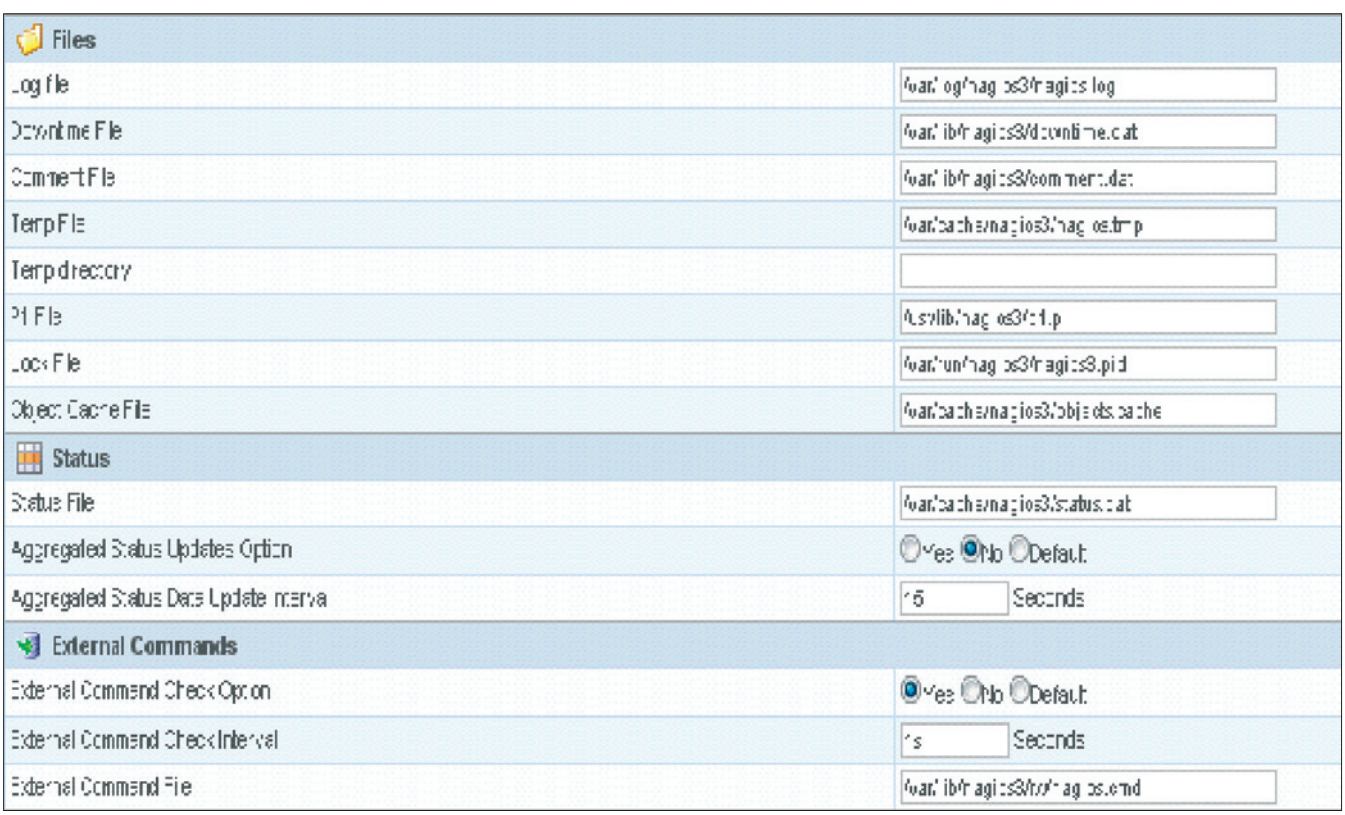


Figure 9. *Configuration Centreon (partie 2)*

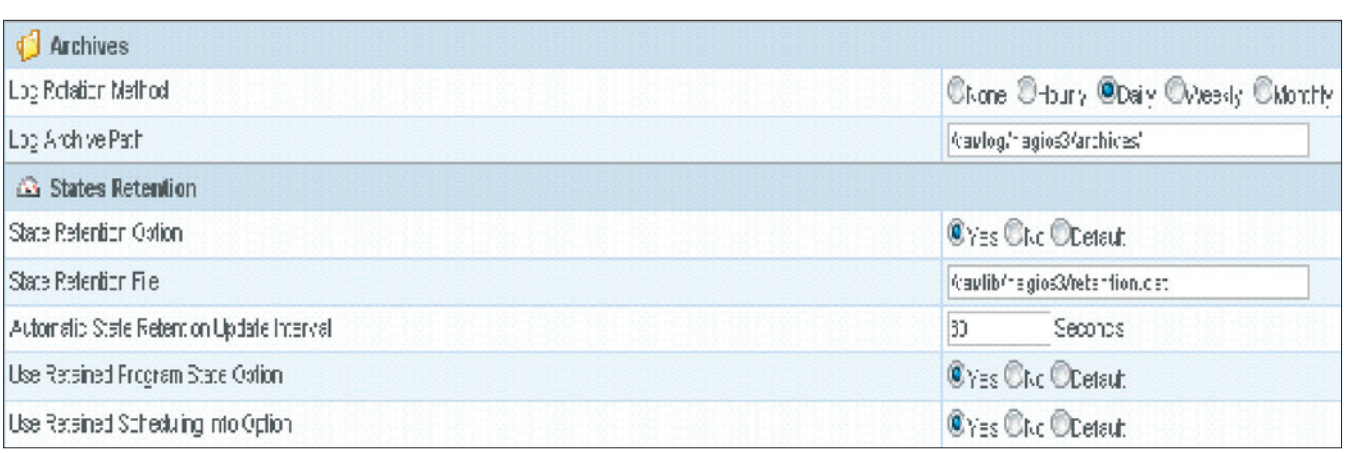


Figure 10. *Configuration Centreon (partie 3)*

Figure 11. *Configuration Centreon (partie 4)*

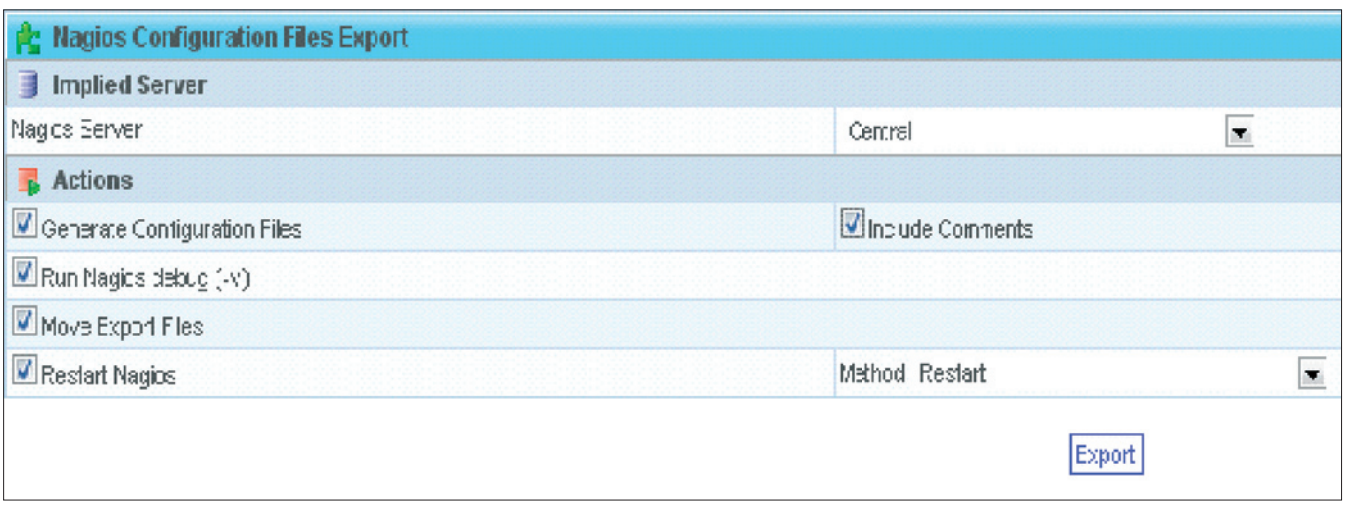


Figure 12. *Configuration Centreon (partie 5)*

Puis cliquez sur *Save*. Allez dans *Configuration -> Nagios -> nagios.cfg* (menu à gauche), puis cliquez sur *Nagios CFG 1*. Maintenant, modifiez les valeurs suivantes :

- *Log File : /var/log/nagios3/nagios.log*
- - Downtime File : /var/lib/nagios3/downtime.dat

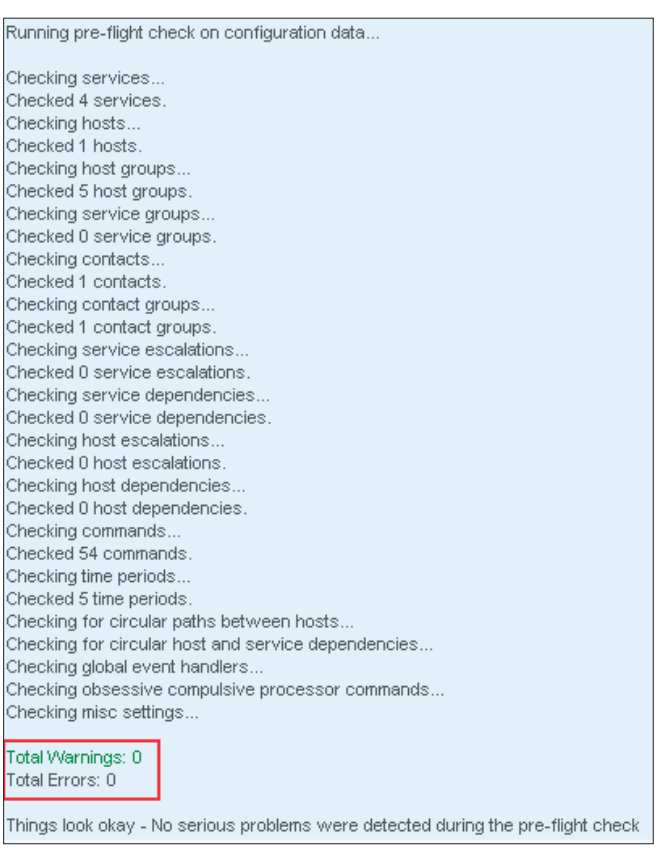


Figure 13. *Export des configurations Nagios vers Centreon*

- - Comment File : /var/lib/nagios3/comment.dat
- - Temp File : /var/cache/nagios3/nagios.tmp
- - P1 File : /usr/lib/nagios3/p1.pl
- - Lock File : /var/run/nagios3/nagios3.pid
- - Object Cache File : /var/cache/nagios3/objects.cache
- - Status File : /var/cache/nagios3/status.dat
- - External Command File : /var/lib/nagios3/rw/nagios.cmd

Cliquez à présent sur l'onglet *Log Options* et modifiez les valeurs suivantes :

- *Log Archive Path : /var/log/nagios3/archives/*
- *- State Retention File : /var/lib/nagios3/retention.dat*

Puis cliquez sur *Save*. Allez dans *Administration -> Options -> CentStorage* (Menu à gauche) et modifiez cette valeur :

- *- Nagios current log file to parse : /var/log/nagios3/nagios.log*

Allez à présent dans *Configuration -> Nagios* et cochez les cases *Generate Configuration Files*, *Run Nagios debug (-v)*, *Move Export Files*, *Include Comments* et *Restart Nagios* puis sélectionnez *External command* dans *Method* et cliquez sur *Export.*

L'ensemble des configurations Centreon s'exporte dans Nagios.

l'exportation s'est correctement déroulée. Il est à présent possible de terminer la configuration de Nagios.

Figure 14. *Interface principale de Nagios*

Finalisons l'installation de Nagios

A présent que toutes les installations sont faites, peaufinons les détails afin de permettre à l'utilisateur final d'accéder à l'interface de Nagios.

Pour cela, nous allons modifier l'utilisateur nagios afin qu'il hérite d'un shell valide :

```
nocrash:~# usermod -s /bin/sh nagios
```

Dans un deuxième temps, octroyons des droits à l'application afin d'envoyer des commandes externes.

```
nocrash:~# invoke-rc.d nagios3 stop
nocrash:~# dpkg-statoverride --update --add nagios www-
                  data 2710 /var/lib/nagios3/rw

nocrash:~# dpkg-statoverride --update --add nagios nagios
751 /var/lib/nagios3
```

Dans un troisième temps, il est nécessaire de créer un compte pour l'utilisation de Nagios afin que la plate-forme de supervision ne soit pas accessible à n'importe qui :

```
nocrash:~# htpasswd -bc /etc/nagios3/htpasswd.users
                  nagiosadmin <Mot_de_Passe>
```

Enfin, nous autorisons le protocole SNMP en lecture seule (*read only*).

```
nocrash:~# echo "rocommunity public" > /etc/snmp/snmpd.
                  conf
```

Il est à présent possible d'accéder à l'interface de Nagios par cette adresse : .

En conclusion, la mise en place d'une supervision de tout un parc informatique n'est pas une mince affaire. Il est nécessaire de s'armer d'une grande détermination et de patience pour avoir un centre de supervision impeccable. Le trio Nagios/Centreon/Cacti est un trio connu et reconnu pour son bon fonctionnement. Vous trouverez la suite de l'article dans la II ème partie : le logiciel Cacti.

AUTEUR

Régis SENET est en cinquième année à l'école Supérieure d'informatique Supinfo. Passionné par les tests d'intrusion et les vulnérabilités Web, il tente de découvrir la sécurité informatique d'un point de vue entreprise. Il s'oriente actuellement vers les certifications Offensive Security et CEH. Contact: *regis.senet@supinfo.com* ***Site internet:*** *http://www.regis-senet.fr*

Supervisez votre réseau grâce à Nagios II partie

Regis Senet

Cet article constitue la IIème partie de l'article dédié a la supervision du réseau grâce à Nagios. Dans cette partie, nous allons nous concentrer sur le logiciel Cacti. Après la supervision des machines Windows, nous allons voir également celle des machines GNU/Linux.

Cet article explique...

- Ce qu'est Cacti
- Comment mettre en place un bon outil de supervision

Ce qu'il faut savoir...

- Connaissance en système d'exploitation Linux et les bases des réseaux

Pour que les utilisateurs les moins informaticiens comprennent facilement les données qui apparaissent dans Nagios, rien ne vaut des graphiques simples et compréhensifs.

Il est vrai que Centreon dispose de certains graphiques mais il n'est pas recommandé de donner à l'ensemble des utilisateurs un accès à Centreon qui est la partie *administrative de Nagios.*

Pour cette raison, nous avons décidé d'installer Cacti. Cacti est un logiciel libre de supervision fondé sur la puissance de stockage de données de RRDTool. Il fonctionne grâce à un serveur web équipé d'une base de données et du langage PHP. Il permet de représenter graphiquement divers statuts de périphériques réseau utilisant SNMP ou encore, grâce à des scripts pour avoir, par exemple, l'espace disque restant ou la mémoire utilisée, la charge processeur ou le ping d'un élément actif.

Installation et configuration de Cacti

Concernant l'installation de Cacti, nous allons simplement installer le paquet *cacti-cactid* grâce au gestionnaire de paquets propre à Debian.

```
nocrash:~# aptitude install -y  cacti-cactid
```

Durant l'installation, nous avons la possibilité de configurer automatiquement la base de données, nous allons donc choisir cette option (cf Figure 1).

Il faut ensuite préciser le mot de passe de l'administrateur de la base de données et donner un mot de passe pour l'utilisateur Cacti nouvellement créé.

Nous avons installé un serveur web tournant sous Apache 2. Il convient de le préciser et même de sélectionner *Tous* si vous avez couplé Apache2 à SSL.

Comme le révèle l'écran suivant, il est nécessaire de se connecter à l'interface web de Cacti pour configurer le programme de récupération de données (le poller).

Cacti s'appuie sur SNMP qui doit être configuré sur l'ensemble des machines, qu'elles tournent sous un système d'exploitation Windows, Linux ou Cisco (cf Figure 2).

Lors du choix de l'installation, choisissez *New Install* (cf Figure 3).

Sur la page suivante, vérifiez que l'ensemble des vérifications a été passé (tout en vert).

Une fois toutes les vérifications effectuées, connectez-vous à Cacti avec les identifiants *admin/admin* (cf Figure 4 et 5).

Vous voici donc maintenant connecté à Cacti dont l'interface principale est représentée à la Figure 6.

Comme indiqué précédemment, il convient de modifier le programme de récupération de données : allez dans *Setting* (Menu à gauche) puis dans l'onglet *Poller* et sélectionnez *spine* comme type de poller (*Poller type*). Consultez la Figur e 7.

Cacti est donc à présent en place. Il est nécessaire d'attendre un peu pour voir les premiers résultats.

Intégration de Cacti dans l'interface Nagios

Pour ne pas avoir à jongler entre plusieurs interfaces graphiques (Nagios / Centron / Cacti), nous allons intégrer l'interface Cacti directement dans celle de Nagios.

Un petit module a été développé par des internautes afin de simplifier la tâche. Ce module étant très pratique, nous allons donc l'intégrer dans notre projet.

```
nocrash:~# wget http://www.nicolargo.com/dev/cactiplug/
                    cactiplug-0.2.tgz
nocrash:~# tar xzf cactiplug-0.2.tgz
nocrash:~# rm -rf cactiplug-0.2.tgz
nocrash:~# mv cactiplug  /var/www
```

Il est nécessaire de réaliser quelques petites modifications dans le script *cactiplug.php* à présent disponible à l'adresse suivante : */var/www/cactiplug/cactiplug.php*À savoir, remplacez :

```
$cactiurl = http://localhost/cacti par $cactiurl = http://
                    <votre_IP>/cacti
$database_username = « cactiadmin » par $database_username =
                    « cacti »
$database_username = « cactipassword » par $database_
                    username = « <VOTRE PASS >»
```

Configurez le lien entre les deux interfaces graphiques comme une commande : éditez le fichier */etc/nagios3/hostTemplates.cfg* pour y ajouter la ligne `action_url /cactiplug/cactiplug.php?ip=$HOSTADDRESS` dans la rubrique *define host*.Toutes vos modifications étant faites, redémarrez Nagios :

```
nocrash:~# /etc/init.d/nagios3 restart
```

Cliquer sur la petite étoile à coté du nom d'hôte donne directement accès à l'interface Cacti de l'hôtesélectionné (cf Figure 8).

Figure 1. *Configuration de Cacti*

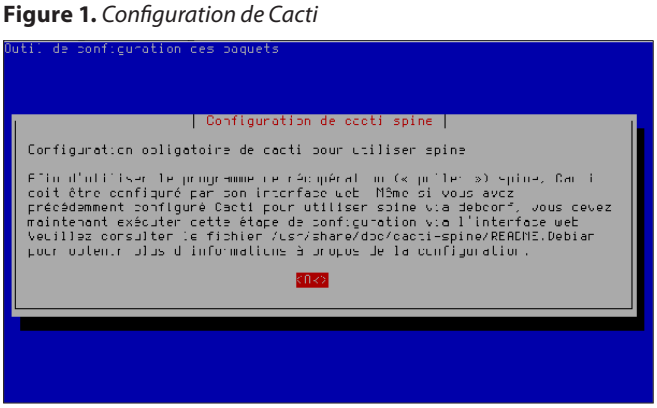


Figure 2. *Ecran d'information Cacti*

Configuration des clients

Lors de la supervision de parcs informatiques, les clients les plus récurrents sont les machines tournant sous des systèmes d'exploitation Windows, GNU/Linux ainsi que les équipements Cisco. Les trois types de machines (Windows, GNU/Linux et Cisco) peuvent être supervisés via le protocole SNMP (*Simple Network Management Protocol*) mais nous allons vous présenter ici une manière spécifique aux trois types de machines.

Clients sous Windows

Pour superviser les machines tournant sous des systèmes d'exploitation Microsoft, installez, dans un

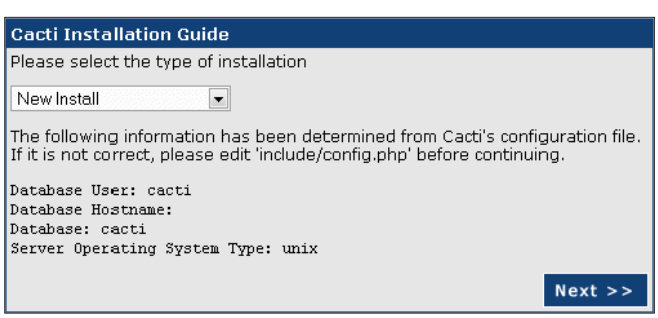


Figure 3. *Démarrage d'une nouvelle installation Cacti*

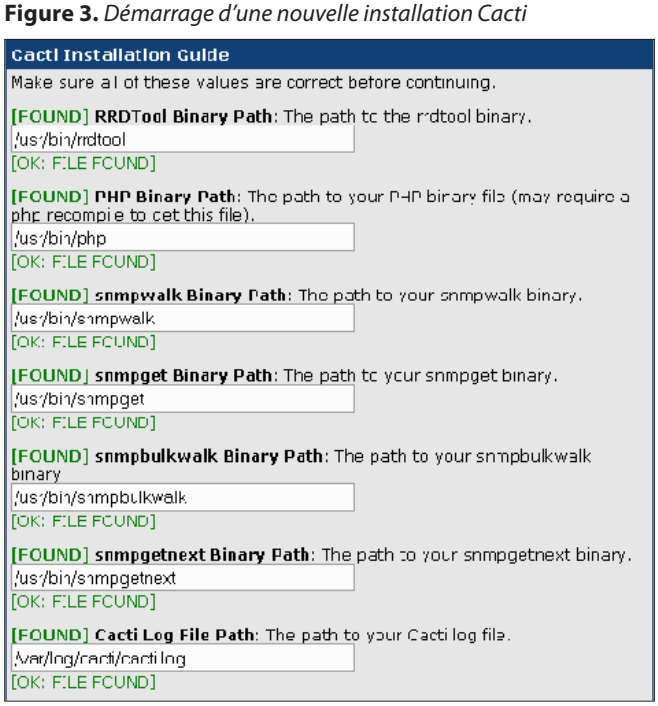


Figure 4. *Paramétrage de Cacti*

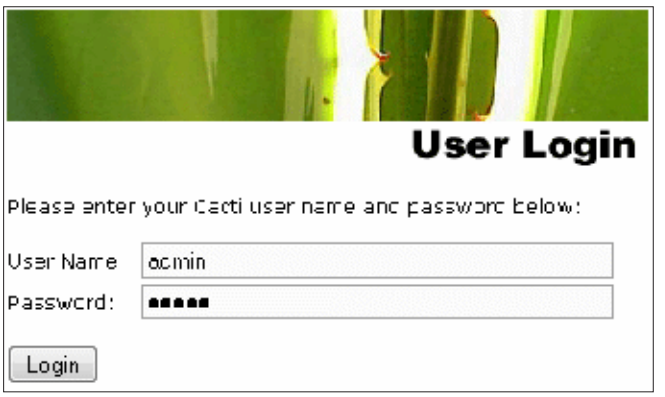


Figure 5. *Interface d'administration Cacti*

premier temps, le logiciel NSClient++. NSClient++ s'appuie sur une architecture client/serveur. La partie cliente, (nommée *check_nt*), doit être disponible sur le serveur Nagios. La partie serveur (NSClient++) est à installer sur chacune des machines Windows à surveiller. Voici un petit schéma résumant le tout (cf Figure 9).

La dernière version de NSClient++ est téléchargeable depuis le site officiel, à l'adresse suivante : *http://sourceforge.net/projects/nscplus/* .

Lors de l'installation, vous verrez apparaître cette fenêtre vous permettant d'indiquer un mot de passe pour permettre la transmission des informations ainsi que l'hôte serveur (cf Figure 10).

Une fois téléchargé et installé, modifiez le fichier de configuration afin que la machine Windows puisse communiquer avec le serveur de supervision ; éditez le fichier *C:\Program Files\NSClient++\NSC.ini.*

Dans ce dernier, vous décommenterez, c'est-à-dire enlèverez le *;* devant les lignes suivantes :

- FileLogger.dll
- *CheckSystem.dll*
- *CheckDisk.dll*
- *NSClientListener.dll*
- *NRPEListener.dll*
- *SysTray.dll*
- *CheckEventLog.dll*
- *CheckHelpers.dll*
- *CheckExternalScripts.dll*
- *NSCAAgent.dll*
- *LUAScript.dll*
- *NRPEClient.dll*
- *CheckTaskSched.dll*

Dans ce même fichier, la directive *password* est censée être renseignée par *mypassword_access* (rempli précédemment) obligeant ainsi la partie cliente et la partie serveur à partager un secret renforçant ainsi le niveau de sécurité.

La dernière directive à laquelle il est nécessaire de prêter attention est la directive *allowed hosts*. Cette dernière permet de spécifier les hôtes autorisés à communiquer avec la machine. Il est bien évidemment nécessaire d'y renseigner l'adresse IP du serveur de supervision où est installé Nagios sinon, la communication client/serveur sera impossible.

Toutes les configurations sont faites, il est temps de tester la connectivité : sur la machine comportant le serveur Nagios, exécutez la commande suivante :

```
nocrash:~# cd /usr/lib/nagios/plugins/
nocrash:~# ./check_nt -H <IP_WINDOWS> -v CLIENTVERSION -p  12489
                      -s <mot de passe>
```

L'option `-p` permet de spécifier le port sur lequel écoute NSClient sur la machine Windows (12489 est le port par défaut). Si tout se passe bien, la version de NSClient doit vous être retournée.

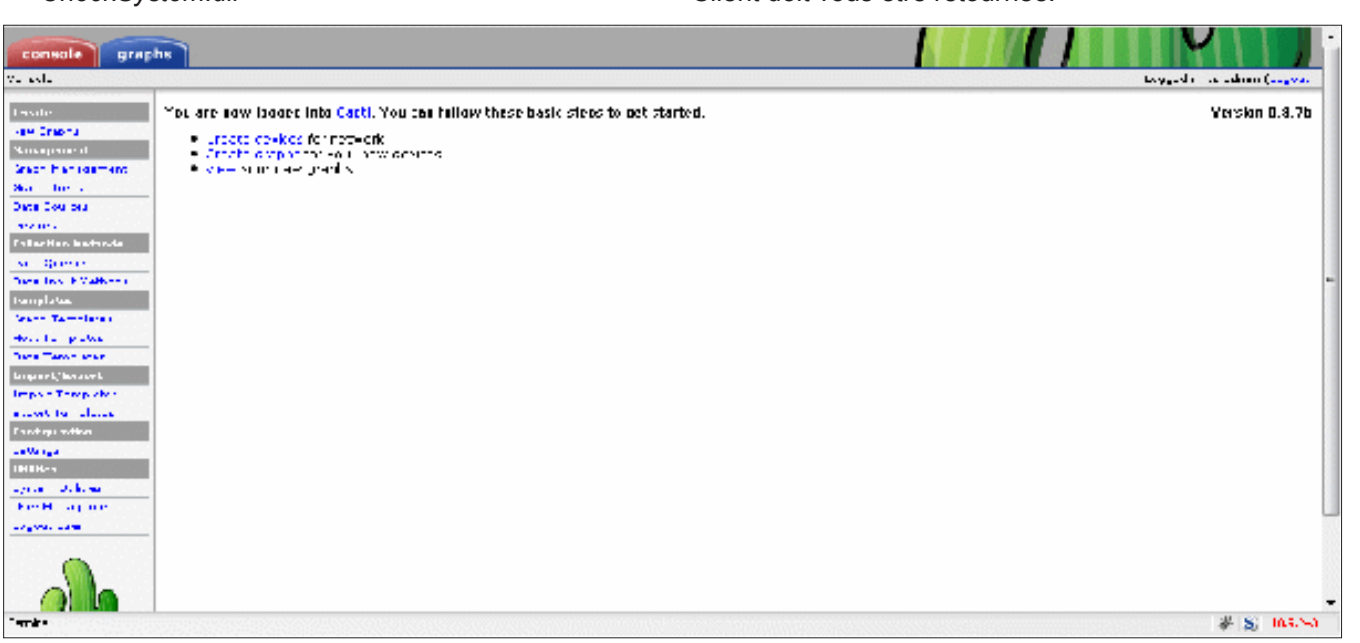


Figure 6. *Interface principale de Cacti*

```
nocrash:~# cd /usr/lib/nagios/plugins/
nocrash:~# ./check_nt -H 192.168.0.1 -v CLIENTVERSION -p
                    12489 -s mypassword_access
NSClient++ 0.3.7.493 2009-10-12
```

Ensuite remplacez l'option `CLIENTVERSION` par `UPTIME`, `CPULOAD`, `MEMUSE` ou encore `USEDDISKSPACE` donnant respectivement le temps depuis lequel la machine est allumée, la charge processeur, l'état de la mémoire et l'espace disque utilisé.

Clients sous GNU/Linux

Après la supervision des machines Windows, voyons celle des machines GNU/Linux. Comme nous l'avons indiqué précédemment, il est possible de gérer la supervision grâce au protocole SNMP mais nous allons plutôt détailler une autre technique : le *plugin* NRPE.

Un peu comme sous Windows (*NSClient++/check_nt*), le plugin NRPE permet l'exécution de plugins dits actifs directement sur les machines à surveiller (cf Figure 11).

Avant de commencer l'installation des plugins NRPE, il faut procéder à quelques installations préalables sur le système d'exploitation :

```
nocrash:~# aptitude install -y  chkconfig  make  gcc
```

A présent, nous pouvons installer les plugins permettant de faire fonctionner NRPE :

```
nocrash:~# aptitude install -y  nagios-nrpe-server  nagios-nrpe-
                    plugin  nagios-plugins
```

Nous allons maintenant installer la dernière version des plugins pour Nagios via les sources du Listing 6.

Certains plugins, comme celui pour récupérer l'état de la mémoire (*check_memory.pl*) ne sont pas disponibles par défaut, il est nécessaire de les télécharger (voir Listing 7).

Le client et le serveur NRPE communiquent via le port TCP numéro 5666. Si vous avez des restrictions via un *firewall* sur vos machines clientes, il est nécessaire d'autoriser le port TCP 5666.

Avec un firewall entièrement fondésur iptables, il est nécessaire de lancer cette commande :

nocrash:~# iptables -A INPUT -p tcp --dport 5666 -i eth0 -j ACCEPT

A présent, modifions le fichier de configuration */etc/nagios/nrpe.cfg* afin de paramétrer la communication client/serveur, les commandes etc.

Il est impératif de modifier la directive *allowed_hosts = 127.0.0.1* de la même manière que sous la machine Windows, c'est-à-dire en remplaçant 127.0.0.1 par l'adresse IP du serveur de supervision Nagios.

Ensuite, il est possible d'ajouter / modifier / supprimer des commandes en respectant les syntaxes déjà présentes.

Nous voyons de nombreuses lignes commençant par `command[check_*] =` ». De cette manière, nous aurons donc accès à la commande gérant la mémoire grâce à `check_mem` en option de `check_nrpe`.

Fichier de configuration sur la machine cliente : 192.168.0.45 :

```
[…]
command[check_mem]=/usr/lib/nagios/plugins/check_memory.
                    pl -w 30 -c 15
[…]
```

Commande à lancer sur le serveur de supervision :

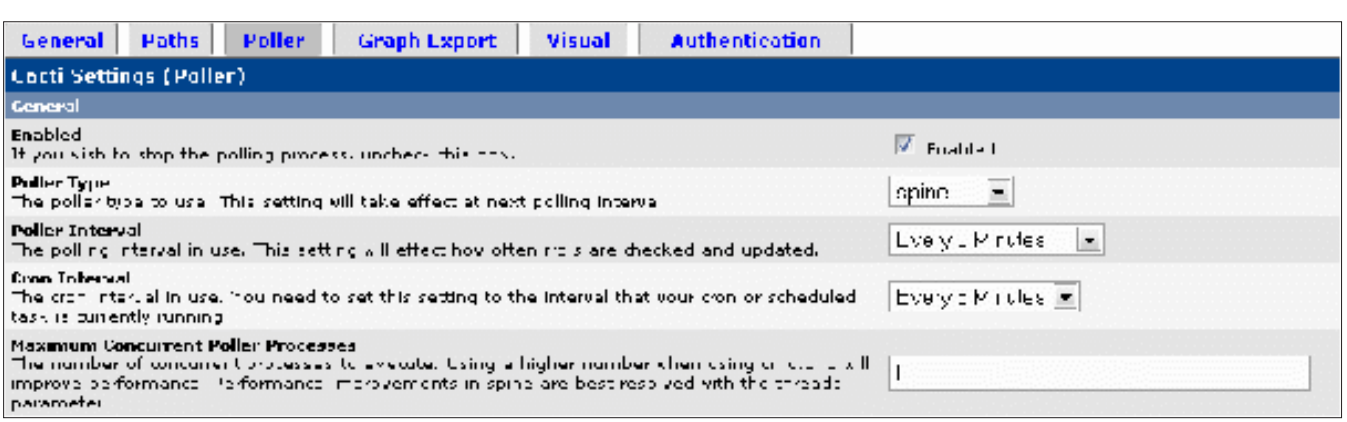


Figure 7. *Changement du programme de chargement de données*

Figure 8. *Intégration de Cacti dans Nagios*

```
nocrash:~# ./check_nrpe -H <Adresse_IP>  -c  check_mem
```

Equipements Cisco

Dans les réseaux d'entreprises assez importantes, il est très fréquent de trouver des routeurs ou des Switch Cisco. La supervision de routeur et de Switch est réellement importante car derrière ces équipements, se trouvent parfois plusieurs machines clientes et plusieurs serveurs.

Ce dont nous avons besoin pour activer le SNMP de manière basique (voir Listing 8).

Et c'est tout car nous n'utilisons pas les traps SNMP des éléments. Dans le cas contraire, il faut paramétrer les traps avec la commande `snmp-server enable traps` comme dans le Listing 9. Puis, il est nécessaire de configurer les ACL (voir Listing 10).

Installation de nouvelles langues

Par défaut, Nagios et Centreon sont fournis dans la langue de Shakespeare. Les anglophobes peuvent modifier la langue de leur utilisateur Centreon. Malheureusement, il n'est pour l'instant pas possible de faire la modification pour Nagios.

Pour profiter de l'interface administrative de Centreon en Français, il est nécessaire de suivre les étapes

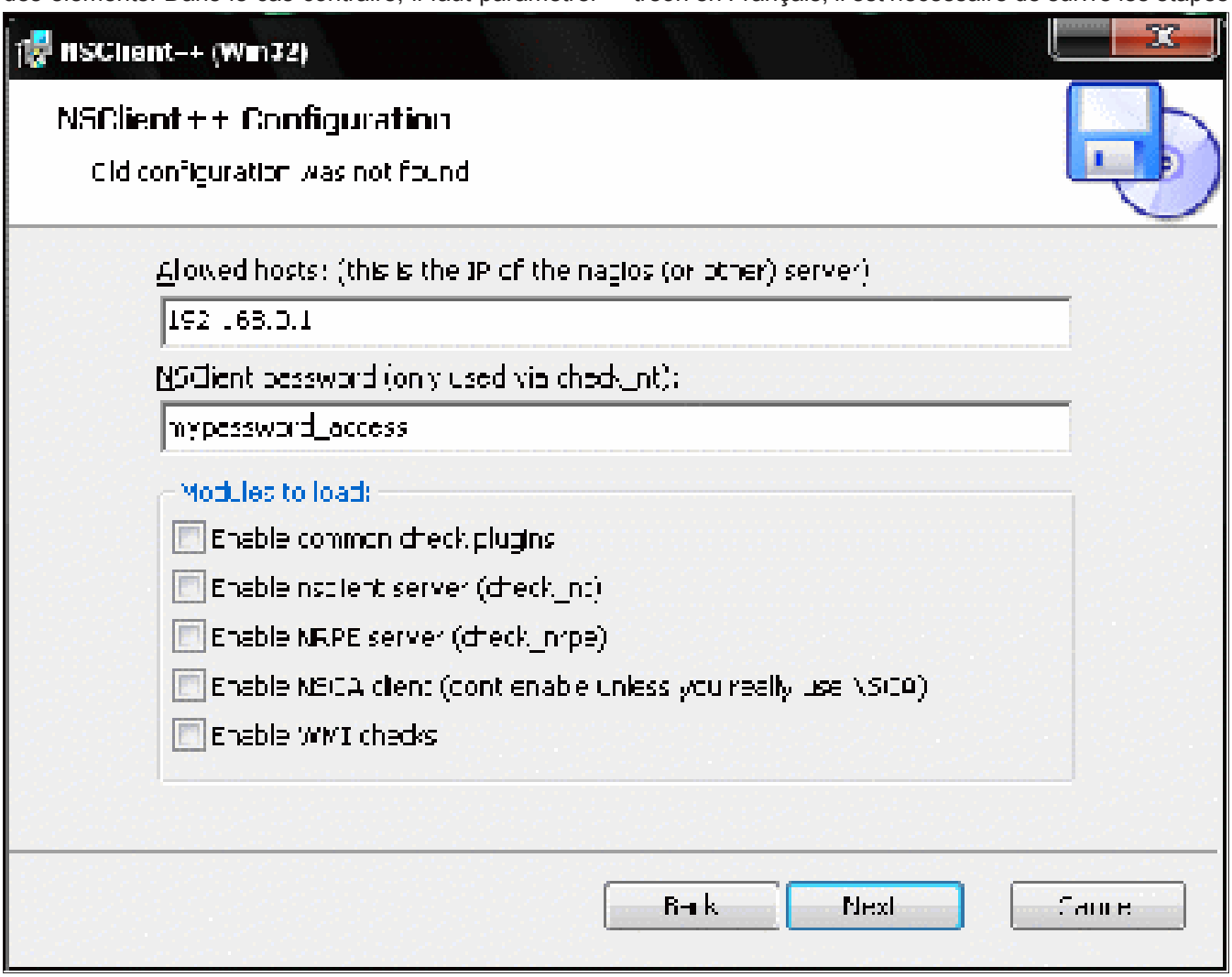


Figure 10. *Paramétrage de NSClient*

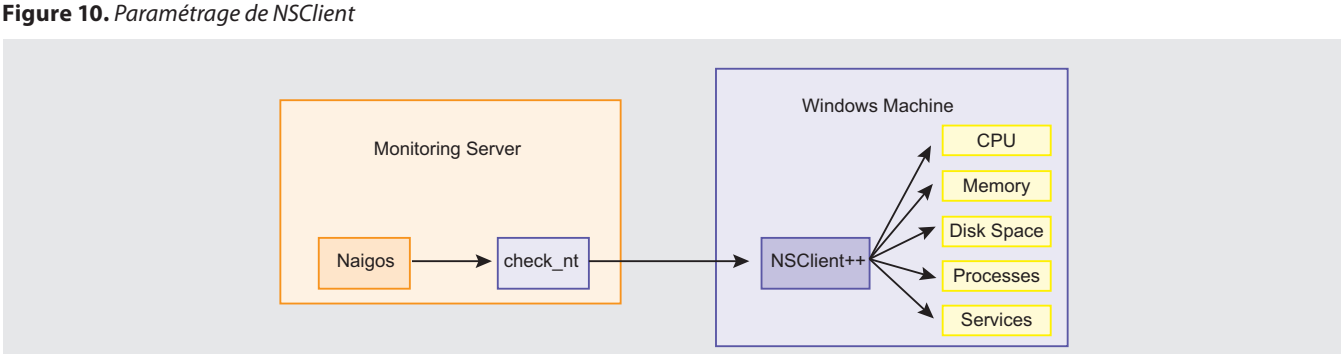


Figure 9. *Schéma de communication NSClient*

suivantes. Commencez par l'installation des pré-requis système :

```
nocrash:~# aptitude install -y install gettext  locales
```

Ensuite, créez un répertoire *fr_FR.UTF-8* dans le répertoire */www/locale/* de Centreon. Créez ensuite un second répertoire *LC_MESSAGES* dans ce même répertoire:

```
nocrash:~# mkdir /usr/local/centreon/www/locale/fr_
                    FR.UTF-8/
nocrash:~# mkdir /usr/local/centreon/www/locale/fr_
                    FR.UTF-8/LC_MESSAGES/
nocrash:~# cd /usr/local/centreon/www/locale/fr_FR.UTF-8/LC_
                    MESSAGES/
```

Puis, téléchargez et compilez le fichier de traduction :

```
nocrash:~# wget http://translations.modules.centreon.com/svn/trunk/
                    centreon/fr_FR/LC_MESSAGES/messages.po
nocrash:~# msgfmt messages.po -o /usr/local/centreon/www/locale/
                    fr_FR.UTF-8/LC_MESSAGES/messages.mo
nocrash:~# chown -R www-data.www-data /usr/local/centreon/www/
                    locale/fr_FR.UTF-8/
```

Enfin, redémarrez votre serveur Apache:

```
nocrash:~# /etc/init.d/apache2  restart
```

Pour terminer, vous devez configurer votre compte utilisateur afin d'utiliser le fichier de traduction adéquat : *Configuration > Users > mon_utilisateur. Sélectionnez fr_FR.UTF-8, cliquez sur Save et votre interface sera à présent en français* (cf Figure 12).

Nagios et la notification par Twitter

Twitter est un outil de réseau social et de microblogging qui permet à l'utilisateur d'envoyer gratuitement des messages brefs, appelés tweets, par Internet, par messagerie instantanée ou par SMS. Twitter est donc un formidable outil de veille. Nous allons donc voir comment configurer notre Nagios pour envoyer des alertes sur un compte Twitter (cf Fiugre 13).

Avant toute chose, il est nécessaire de créer un compte Twitter dédié à ce besoin car c'est vers lui que toutes les alertes seront envoyées. Il suffira ensuite aux administrateurs de suivre ce compte Twitter pour être informé au plus vite des anomalies survenues sur le réseau.

Pour créer un compte, allez sur : *https://twitter.com/signup?commit=Join* et remplissez le petit formulaire d'inscription.

Il faut bien retenir votre nom d'utilisateur (*nagios_nocrash*) et votre mot de passe pour la suite. Rendez-vous dans les *Paramètres* et cliquez sur le bouton *Protéger mes tweets* pour forcer l'approbation des utilisateurs autorisés à suivre ce compte Twitter. Quand un des administrateurs fera une demande pour suivre ce compte Twitter, il faudra l'approuver.

Avant de vous lancer dans les tests, il est nécessaire de commencer par l'installation des pré-requis système; tout d'abord, *curl* :

```
nocrash:~# aptitude install -y curl
```

Nous pouvons faire notre petit test et ainsi vérifier la communication entre notre serveur de supervision et Twitter :

```
nocrash:~# curl  --connect-timeout 30  --max-time 60
                    -u nagios_nocrash:<mon_password>
                    -d status="Petit test via Nagios"
```

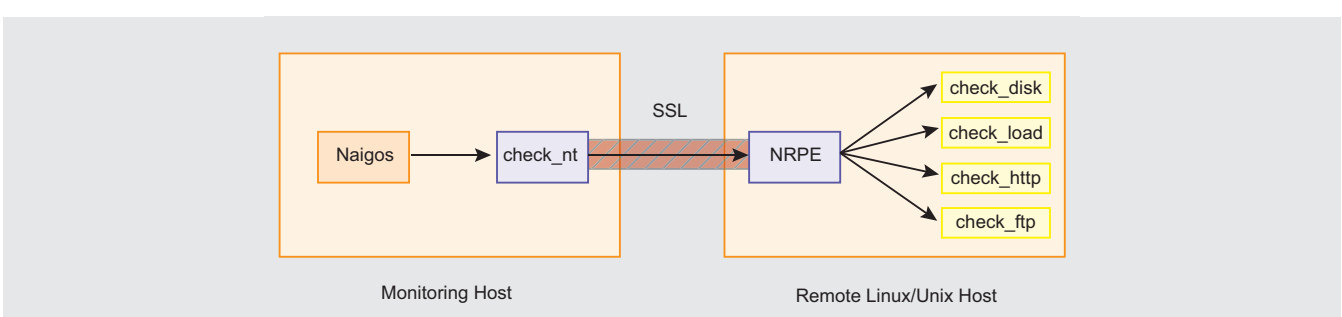


Figure 11. *Schéma de communication NRPE*

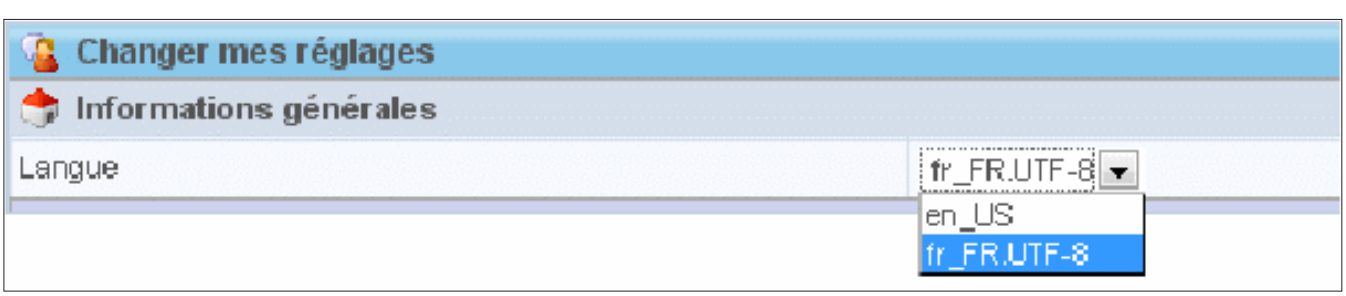


Figure 12. *Choix des langues sous Centreon*

```
http://twitter.com/statuses/update.
xml
```

Si tout se passe bien, vous devriez avoir reçu une notification Twitter (cf Figure 14) sur le compte *nagios_nocrash*.

Pour créer les commandes, ouvrez Centreon, cliquez sur l'onglet *Configuration*, puis dans le menu à gauche *Notification* et enfin, cliquez sur ajouter. Tout est correct, à présent, et vous pourrez bénéficier des notifications grâce à Twitter (cf Figure 15).

Nagios et la notification via SMS

Depuis le début de cet article, nous voyons l'envoi de notification Nagios par mail ou encore sur internet grâce à Twitter. Un administrateur réseau, aussi bon soit-il, ne passe pas toute sa journée derrière un écran. Il est donc possible de trouver d'autres moyens afin que l'administrateur soit constamment informé. Pour cela, nous allons passer par les réseaux téléphoniques et les SMS.

Un SMS (*Short Message Service*) est utilisé pour transmettre de courts messages textuels. Il est donc possible d'utiliser cette technique pour avertir les administrateurs absents de leur lieu de travail et n'étant pas forcément derrière un ordinateur.

Il serait de bon ton de définir des périodes de temps pour l'envoi de SMS.

Il existe des solutions clé en main proposées par la plupart des opérateurs de téléphonie mobile. Mais ces

Listing 6. *Installation des plugins Nagios*

```
nocrash:~# cd /usr/src
nocrash:~# wget "http://downloads.sourceforge.
                net/project/nagiosplug/
                nagiosplug/1.4.14/nagios-plugins-
                1.4.14.tar.gz?use_mirror=garr"
nocrash:~# tar xzf nagios-plugins-1.4.14.tar.gz
nocrash:~# rm -rf nagios-plugins-1.4.14.tar.gz
nocrash:~#./configure --enable-extra-opts --with-perl
                --enable-perl-modules
nocrash:~# make && make install

nocrash:~# cpan Nagios::Plugin
nocrash:~# perl -MCPAN -e 'install Nagios::Plugin'
```

Listing 7. *Récupération du script check_memory*

```
nocrash:~# cd /usr/lib/nagios/plugins
nocrash:~#wget "http://www.monitoringexchange.org/
                attachment/download/Check-Plugins/
                Operating-Systems/Linux/check_
                memory/check_memory.pl"

   nocrash:~# chmod +x check_memory.pl
```

Listing 8. *Configuration du SMTP sur un équipement Cisco*

```
Routeur>enable
Routeur#configure terminal
Routeur(config)# snmp-server community COMMUNAUTE_
                RESEAU ro 1
Routeur(config)# snmp-server host @IP_SERVEUR_
                SUPERVISION COMMUNAUTE_RESEAU
```

Listing 9. *Activation des traps SNMP*

```
Routeur(config)# snmp-server community COMMUNAUTE_
                RESEAU RO 1
Routeur(config)# snmp-server trap-source Vlan1
Routeur(config)# snmp-server enable traps snmp
                authentication linkdown linkup
                coldstart warmstart
Routeur(config)# snmp-server enable traps tty
Routeur(config)# snmp-server enable traps fru-ctrl
Routeur(config)# snmp-server enable traps entity
Routeur(config)# snmp-server enable traps flash
                insertion removal
Routeur(config)# snmp-server enable traps cpu threshold
Routeur(config)# snmp-server enable traps vtp
Routeur(config)# snmp-server enable traps vlancreate
Routeur(config)# snmp-server enable traps vlandelete
Routeur(config)# snmp-server enable traps envmon fan
                shutdown supply temperature status
Routeur(config)# snmp-server enable traps port-security
Routeur(config)# snmp-server enable traps rf
Routeur(config)# snmp-server enable traps hsrp
Routeur(config)# snmp-server enable traps bridge
                newroot topologychange
Routeur(config)# snmp-server enable traps stpx
                inconsistency root-inconsistency
                loop-inconsistency
Routeur(config)# snmp-server enable traps syslog
Routeur(config)# snmp-server enable traps vlan-
                membership
Routeur(config)# snmp-server host @IP_SERVEUR_
                SUPERVISION COMMUNAUTE_RESEAU
```

Listing 10. *Création des ACL*

```
Router# show running-config
Router# show snmp
Router# show access-lists 1
Router# configure terminal
Routeur(config)# ip access-list standard 1
Routeur(config)# no 40
Routeur(config)# 40 permit @IP_SERVEUR_SUPERVISION
Routeur(config)# exit
Routeur#wr m
```

solutions sont assez coûteuses si vous devez envoyer un SMS de temps en temps.

Nous avons adopté une solution basique qui fonctionne bien pour les petits volumes ; il s'agit de piloter un GSM directement via votre serveur en utilisant un câble data USB. La plupart des GSM conviendront à cet usage, l'unique condition est que le GSM possède un modem intégré qui répond aux commandes AT.

Pour piloter le GSM, nous avons besoin de la bibliothèque *gsmlib.* Cette bibliothèque se trouve dans le paquet *gsm-utils*. Pour l'installer, lancez la commande suivante :

```
nocrash:~# aptitude install -y gsm-utils
```

Ensuite, connectez le GSM via son câble data à un des connecteurs USB. Si tout se passe bien, le système Hotplug chargera le module usbserial et vous obtiendrez un périphérique supplémentaire */dev/ttyUSB0*. Vérifiez grâce à cette commande:

```
nocrash:~# ls -al /dev/ttyUSB*
```

Si vous n'avez pas de ttyUSB*, chargez le module manuellement :

```
nocrash:~# modprobe usbserial
```

Le paquet gsm-utils fournit quelques commandes pour dialoguer avec le GSM. Vérifiez si le GSM répond bien avec la commande suivante :

```
nocrash:~# gsmctl -d /dev/ttyUSB0 ALL
```

A présent, il est possible d'envoyer des messages grâce à cette commande :

```
nocrash:~# gsmsendsms -d /dev/ttyUSB0 +3299999999 "Nagios - Test
                        SMS OK"
```

Avant d'ajouter les commandes nécessaires à Nagios, il est important de se rappeler que le numéro de téléphone correspond au *pager* du contact (cf Figure 16).

A présent que tout est opérationnel, il est possible d'ajouter les commandes à Nagios. Pour cela, passez soit par les fichiers de Nagios en éditant le fichier */etc/nagios3/misccommands.cfg,* soit par l'interface Centreon.

Ouvrez Centreon, cliquez sur l'onglet *Configuration*, puis dans le menu à gauche *Notification* et enfin, cliquez sur *ajouter* (cf Figure 17).

Tout est OK, vous allez à présent recevoir vos notifications directement par SMS.

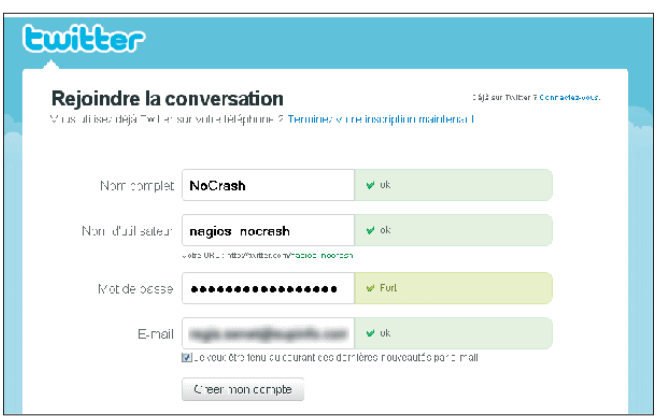


Figure 13. *Création d'un compte Twitter*

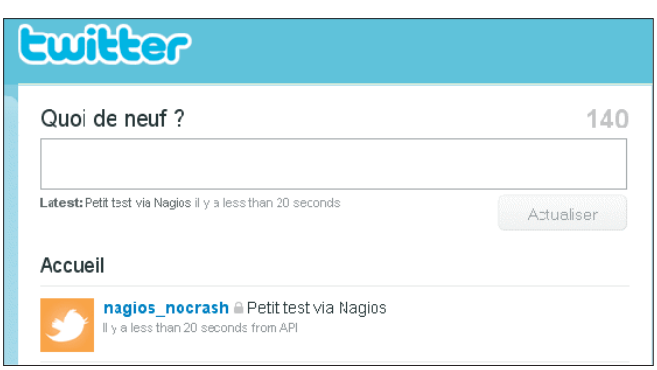


Figure 14. *Réception de la première notification*

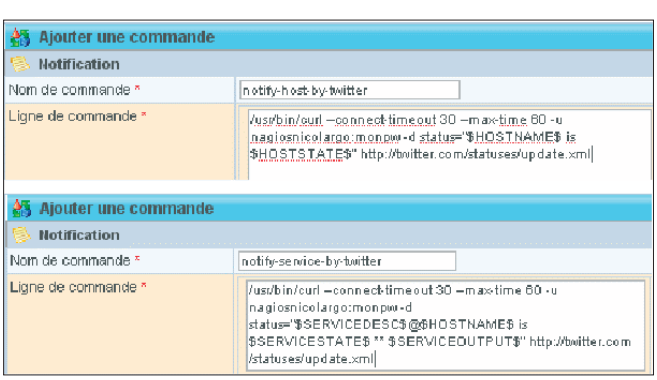


Figure 15. *Création des commandes de notification*

Conclusion

La mise en place d'une supervision de tout un parc informatique n'est pas une mince affaire. Le trio Nagios/Centreon/Cacti que vous avez connus à travers deux parties de l'article, est un trio connu et reconnu pour son bon fonctionnement Il vous aidera facilement à améliorer l'accessibilité à vos machines sur l'ensemble de vos parcs informatiques, qu'ils soient moyennement grands ou très grands.

NB. Les Figures 16 et 17 sont à télécharger depuis *www/hakin9.org/fr*

AUTEUR

Régis SENET est en cinquième année à l'école Supérieure d'informatique Supinfo. Passionné par les tests d'intrusion et les vulnérabilités Web, il tente de découvrir la sécurité informatique d'un point de vue entreprise. Il s'oriente actuellement vers les certifications Offensive Security et CEH.

Contact : *regis.senet@supinfo.com* ***Site internet :*** *http://www.regis-senet.fr*

Les attaques << Evil Twin >> du Social Engineering

Tim Kulp

Le Social Engineering est l'art d'influencer et de persuader des individus dans le but de les manipuler et de leur soutirer des informations. Un Evil Twin utilise un ensemble de techniques pour faire croire qu'il s'agit d'un utilisateur de confiance tout en recueillant des informations sur sa victime.

Cet article explique:

- Ce qu' une Evil Twin
- L'utilisation d'une Evil Twin par Social Engineering
- La portée d'une Evil Twin

Ce qu'il faut savoir:

- Utiliser un moteur de recherche
- Comment s'inscrire sur un réseau social

Je ne voudrais pas me réveiller un matin en me disant que je ne suis plus moi-même. Cette phrase rendue célèbre par le film *Invasion of the Body Snatchers* (L'invasion des profanateurs) sorti en 1956 pourrait s'appliquer aujourd'hui aux problèmes rencontrés sur le Web. La majorité des internautes recevant des mails envoyés par des amis ou des collègues ne pensent jamais à en vérifier la provenance, ni même la source. Ce comportement qui tend à se généraliser, influe de plus en plus sur les réseaux sociaux. Aujourd'hui, entre les blogs, Twitter, Facebook et LinkedIn, nous mettons à disposition du monde entier un nombre incalculable de données personnelles. Alors que nous sommes pris dans la culture de l'auto-publication avec l'avènement du Web 2.0, nous oublions que chaque élément d'information transmis, l'est de manière définitive et risque de se retourner un jour contre nous. Nous verrons dans cet article comment, grâce aux Evil Twin, certains pirates parviennent à utiliser les médias sociaux contre nous, contre des employés ou les membres d'une famille.

Un Evil Twin, tel que défini par Carl Timms et James Perez dans leur ouvrage , consiste pour un attaquant à se faire passer pour un utilisateur légitime en usurpant son identité. Cette technique n'est pas nouvelle, elle est utilisée depuis des années sur les forums et les chats. Mais depuis deux ans environ, elle se retrouve sur les réseaux sociaux où l'identité déclarée par un utilisateur est supposée être authentique. Par exemple, qui pourrait nous empêcher de nous inscrire sur Facebook sous le nom de profil William George ? Personne. Et c'est bien là le problème : sur Internet, n'importe qui peut dire ou faire croire n'importe quoi et chercher à réinventer sa vie par la même occasion. Bien, revenons-en à l'essentiel ; un Evil Twin se produit lorsque est créée la page William George sur Facebook avec l'intention de recueillir des informations sur la famille du véritable William George, ses amis, ses collègues… L'utilisation d'un Evil Twin permet donc de se faire passer pour un utilisateur légitime pour mieux infiltrer le cercle de confiance (composé en général d'amis proches) de la victime ou répandre des malwares via les applications Facebook...

À première vue, cela ressemble à du Social Engineering ? Et bien, c'est précisément cela ! Un Evil Twin est l'illustration même du Social Engineering. Dans son ouvrage , Kevin Mitnick définit le Social Engineering ainsi :

Le Social Engineering est l'art d'influencer et de persuader des individus dans le but de les manipuler et de leur soutirer des informations avec ou sans l'aide des technologies informatiques.

Un Evil Twin utilise un ensemble de techniques pour faire croire qu'il s'agit d'un utilisateur de confiance tout en recueillant des informations sur sa victime. Un Evil Twin permet, à terme, de répandre des malwares, obtenir des informations des caches, ou diffamer une ou plusieurs personnes.

Les sites de réseaux sociaux sont le moteur des Evil Twin et les médias sociaux en sont le carburant. Un site de réseau social permet aux utilisateurs de communiquer entre eux et de partager leurs profils sur Facebook, LinkedIn, Bebo… Un média social, en revanche, permet aux utilisateurs de publier leurs contenus directement en ligne sur Blog, YouTube, Twitter... Les réseaux sociaux permettent donc de connecter/relier des internautes alors que les médias sociaux sont orientés contenus. Nous reviendrons sur cet aspect au cours de l'article. La plupart des sites que nous venons de citer proposent différents paramètres de confidentialité permettant de masquer les contenus et certaines informations des utilisateurs qui sont hors de votre cercle de confiance. Toutefois, ces contrôles ne sont pas obligatoirement activés par défaut. Les médias sociaux servent de carburant aux Evil Twin en informant précisément le pirate de l'ensemble des caractéristiques d'une personne pour mieux les attaquer : un tweet sur le golf servirait d'indice au pirate en indiquant que sa victime est un golfeur. Le profil Evil Twin s'adapterait alors aux centres d'intérêts de la victime.

Principe de fonctionnement d'un Evil Twin

Voyons la technique, que nous avons mise en oeuvre pour une société, pour effectuer un Evil Twin en vue de déterminer la méthodologie que ses employés devront appliquer lorsqu'ils publient des informations d'entreprise sur les réseaux et les médias sociaux. Mais sachez qu'un Evil Twin viole délibérément tous les accords utilisateurs de la majorité des sites de réseaux sociaux et médias sociaux. De fait, vous risquez de vous retrouver dans de sérieux ennuis. N'essayez pas cette technique sans l'accord tacite de l'individu et de l'entreprise pour lesquels vous effectuez le test.

Étape 1 : Définir l'objectif

Avant toute chose, vous devez définir l'objectif. Pour quelle raison souhaitez-vous effectuer un Evil Twin ? Quelle est votre motivation ? Cette dernière va de la diffamation à l'espionnage, en passant par le déploiement de malwares, des actes de désinformation... Vous devez donc délimiter ce qui est possible ou non, puis établir l'objectif à atteindre, c'est-à-dire votre but. Dans notre cas, l'attaque doit permettre d'obtenir les identifiants de connexion système. L'objectif est donc de récupérer ces informations puis d'accéder au système distant pour soutirer de l'argent à la machine cible (système financier).

Étape 2 : Définir la cible

Vous devez maintenant définir la cible. Qui attaquez-vous en bout de chaîne ? La cible est soit un particulier, une entreprise, soit tout autre groupe. Si c'est un groupe, vous devez savoir quelle personne attaquer.

Posez-vous les questions suivantes :

- Votre cible est-elle présente sur les médias sociaux ? Essayez d'obtenir le maximum d'informations sur la cible, vous faciliterez la mise en place d'un Evil Twin.
- Votre cible est-elle présente sur les réseaux sociaux ? Dans l'idéal, il est préférable qu'elle ne le soit pas. Sinon, choisissez d'autres réseaux sociaux et invitez un ou des ami(s) de votre cible. La plupart des internautes sont inscrits à plusieurs réseaux sociaux ou ont plusieurs profils sur un seul réseau. Sinon, vous pouvez toujours tenter de détourner les connexions vers votre nouveau compte (bien que plus difficile).
- Votre cible est-elle la bonne ? Assurez-vous que vous pourrez atteindre votre objectif avec votre cible. Si vous souhaitiez obtenir des codes d'accès physique à un bureau situé à Baltimore, ne choisissez pas une cible vivant à Londres, ça paraît évident et pourtant... D'une manière générale, essayez de toujours cibler les individus en relation directe avec votre objectif.

Dans notre Evil Twin, GroundTrans Corp est notre cible et notre objectif est d'obtenir les identifiants

Tableau 1. *Informations récupérées sur Steve Partmen*

Catégorie	Fréquence		
	Souvent	Parfois	Rarement
Infos personnelles	Nom : Steve Partmen Date naiss. Août	Marié Sociable	
Infos professionnelles	GroundTrans Corp	SeaTrans Corp	
Infos éducation		Université ABC	Collège communautaire
Loisirs		Aéromodélisme Escalade	Arts martiaux Photos de randonnées
Centres d'intérêt	golf UFC	Voitures de sport Motos	

de connexion afin de soutirer de l'argent au système financier. La cible étant une entreprise, nous devojs savoir précisément qui nous allons incarner. Après un petit passage en revue du site web de GroundTrans et notamment quelques biographies des responsables, nous recherchons leur éventuel profil sur LinkedIn. Nous conservons uniquement les comptes LinkedIn qui reçoivent des mises à jour synchronisées avec Twitter. Cette étape a permis de conserver uniquement 2 responsables, proches du directeur financier Steve Partmen. Nous avons donc la cible et trois supports différents pour lancer un Evil Twin (la page GroundTrans, LinkedIn et Twitter).

Étape 3 : Recueillir des informations sur l'utilisateur légitime

La cible étant déterminée, il faut maintenant recueillir des informations plus précises sur notre cible. Celles-ci dépendront essentiellement de l'Evil Twin que nous mettrons en place sur le réseau social. Le meilleur endroit pour démarrer est Google. Saisissez le nom et le prénom de la personne et regardez les résultats. Durant cette phase, nous devons recueillir le maximum d'informations sur le Steve Partmen visé (attention : il peut y en avoir plusieurs), en utilisant des sites comme Blogger, Twitter, LinkedIn, Facebook... Nous pouvons également glaner des informations intéressantes sur Twitter par exemple et connaître en temps réel ses faits et gestes.

La clé réside dans l'agrégation de données et non dans l'utilisation de données singulières qui n'ont aucune signification propre. Par exemple, les utilisateurs de Twitter traitent chaque message de manière unique. Dans leur esprit : 1 message équivaut à 1 information. Il faut donc croiser toutes les informations Twitter relatives à la cible tout en étendant les recherches aux médias sociaux (blogs, YouTube...).

Pour conserver toutes les informations trouvées sur un utilisateur, utilisons un tableau croisé - Tableau 1.

Cette vue croisée permet de classer chaque élément du profil par catégorie et d'en estimer la fréquence. Il suffit de placer chaque élément dans la ligne appropriée et de compter son nombre d'apparitions pour déterminer si c'est Souvent / Parfois / Rarement. Dans notre exemple, le Golf revient Souvent. Il se retrouve fréquemment dans les messages Twitter. Les informations qui apparaissent Rarement sont les plus intéressantes, car peu connues. C'est ce dernier aspect qui permettra de lancer un Evil Twin crédible.

Comme indiqué plus haut, la personne pour qui nous souhaitons nous faire passer est Steve Partmen, dont la biographie est consultable sur le site GroundTrans. Ainsi, nous savons que Steve a travaillé pour SeaTrans avant de rejoindre le groupe GroundTrans mais cela n'est pas mentionné sur son profil LinkedIn. Il faut donc faire apparaître cette donnée sous la rubrique Infos professionnelles / Parfois. Les recherches nous ont fourni une page intéressante (page 8 de Google), indiquant que Steve était un ancien prof de karaté. Cette information a été reportée dans la catégorie Loisirs / Rarement. Sur son profil LinkedIn, nous avons examiné en détails l'historique de Steve y compris les informations relatives à son éducation, ses centres d'intérêts, recommandations... Avec ces données, nous allons sur sa page Twitter pour analyser l'ensemble de messages et ainsi vérifier les correspondances. Le golf ressortait toujours en premier, tout comme la randonnée et l'escalade. Steve est également parti au Canada pour faire de la randonnée dans les cercles arctiques.

Sur Flickr, des images de Steve et de ses amis en attestent. Ces images sont sauvegardées avant d'en rechercher d'autres sur le golf. Malheureusement, cette recherche n'a apporté que des données portant sur des gens qui ressemblaient physiquement au Steve visé. Suffisant pour être crédible, d'autant que les photos ont un aspect suranné. Pour la majorité des internautes, tout porte à croire qu'il s'agit du véritable Steve.

Étape 4 : Pool de connexion

Nous avons notre cible, la personne pour qui se faire passer et toutes les informations nécessaires pour mettre en place notre Evil Twin. Il suffit de trouver maintenant des gens à qui nous connecter et consulter leurs profils. Cette étape est relativement simple sachant que nous sommes présent sur les réseaux sociaux. Avec LinkedIn, nous pouvons masquer les connexions et afficher uniquement les gens avec lesquels nous sommes connecté. Lors-

Tableau 2. *Liste des connexions*

ID	Nom	Entreprise	Relation	Liens sociaux
1	Bob Jones	GroundTrans	Directeur Financier	Aucun
2	Carol Partmen	AT&T	Épouse	http://social.com/blah?ID=124
3	Dona Far		Fille d'une amie de sa mère	http://social.com/blah?ID=23
4	Frank Haim	GroundTrans	Responsable informatique	http://social.com/blah?ID=2

que cette fonction est activée, seuls les gens autorisés voient les autres connectés. Si cette fonction est désactivée, n'importe qui voit nos connexions. LinkedIn dispose d'une autre fonction très pratique, « Viewers of this profile also viewed… ». En clair, nous voyons les autres profils connectés à celui en cours. Cette fonction permet d'établir un lien entre plusieurs profils. Une connexion implicite ne signifie pas pour autant que deux profils sont directement liés, mais nous pouvons penser qu'un utilisateur est parvenu à consulter des profils déjà visionnés. Prenez par exemple Amazon.com qui propose « Qu'achètent les clients après avoir consulté cet article…», cela ne signifie pas que les gens ont acheté plusieurs articles, mais certains d'entre eux. D'après notre expérience, les profils déjà consultés sont généralement connectés au profil en cours de visionnage. Cette hypothèse s'est souvent vérifiée.

Il faut noter chaque connexion en rapport avec la cible et les ajouter ultérieurement à notre Evil Twin. Pour lister ces connexions, partons du tableau 2 procurant une liste unique de connexions en rapport avec notre cible.

Lorsque toutes les connexions ont été répertoriées, nous utilisons le Tableau 3 pour analyser la nature de leur relation et leur fréquence. Rappelez-vous que le but d'un Evil Twin est de gagner la confiance des utilisateurs. Par conséquent parvenir à faire la différence entre les membres d'une famille, des amis et des collègues de travail est essentiel pour se focaliser sur sa cible. Si vous vous attaquez à une entreprise, il faudra vous concentrer en priorité sur les contacts professionnels avant de s'intéresser aux amis ou collègues. Utilisez les numéros de la liste précédente pour gagner du temps.

Pour notre attaque, nous avons trouvé la page de Steve Partmen sur LinkedIn. Notre but est de déployer un malware sur le réseau. Pour cela, nous utiliserons FaceBook. Quelques recherches sur LinkedIn nous ont fourni un ensemble de contacts (figurant dans notre table) dont des profils dits « Populaires » sur LinkedIn. Gardons toujours en tête que notre objectif est de soutirer de l'argent. Pour chaque connexion, nous devons nous demander si l'utilisateur possède des informations susceptibles d'atteindre notre objectif ? Axons notre recherche sur les personnes travaillant pour le département Comptabilité & Finance. Après avoir listé toutes les connexions, vérifions toutes les personnes présentes sur le profil Twitter de Steve. Les utilisateurs qui ont à la fois des followers LinkedIn et Twitter sont marqués comme Souvent. Ceux qui n'apparaissent que sur LinkedIn sont marqués comme Parfois et ceux uniquement sur Twitter sont marqués Rarement.

Tableau 3. *Tableau croisé relationnel*

Catégorie		Fréquence		
		Souvent	Parfois	Rarement
Contacts pro	Au travail	1	4	
	Autres entreprises			
Contacts perso	Amis			3
	Famille	2		

Étape 5 : Mettre au point un Evil Twin

Après avoir abordé les actions préalables à la mise en place d'un Evil Twin, passons maintenant à l'action ! Nous devons d'abord choisir le réseau social à utiliser en fonction de nos objectifs. Si l'objectif est de déployer un malware (comme indiqué dans notre exemple), alors Facebook est le site idéal. La plate-forme applicative de Facebook permet de distribuer rapidement et facilement du code malveillant au plus grand nombre. De plus, vous pouvez recueillir un ensemble d'informations au cours de ce processus. LinkedIn est l'outil de prédilection pour les réseaux sociaux professionnels (pour mettre à mal la réputation d'une entreprise) et est parfait pour la réputation d'un Evil Twin. Vous pouvez également vous intéresser aux réseaux sociaux récents ; cela peut conforter votre crédibilité sur de nouveaux systèmes. L'avantage avec cette dernière méthode est de faire croire que vous êtes le véritable Steve Partmen. Là encore, qui pourrait remettre en question cette affirmation ?

Le réseau social choisi, il nous faut disposer d'un compte mail. Vous pouvez souscrire à des services gratuits tels que Gmail, Hotmail, Yahoo Mail… Essayez par la même occasion de saisir une adresse mail crédible. Nous savons que l'adresse hotmail de Steve est spartmen@hotmail.com, essayons spartmen@gmail.com. Certains utilisateurs n'y verront que du feu ; dans le cas contraire, le vrai Steve est peut être passé sur un autre service.

Muni de notre nouvelle adresse mail, revenons sur le réseau social choisi pour nous inscrire. Ce processus est relativement simple grâce aux tables mises en place précédemment. Notre Evil Twin sera alors extrêmement efficace. Que vous vous inscriviez à Facebook ou LinkedIn, vous devrez répondre à quelques questions sur vos centres d'intérêt, votre date de naissance… Si vous n'avez aucune idée, mettez

n'importe quelle réponse. Pour la date de naissance, si la personne vous semble jeune, saisissez quelque chose de singulier du genre 02/12/1928. La plupart des utilisateurs de réseaux sociaux n'y prêtent pas attention. Essayez tout de même d'avoir un Evil Twin crédible pour augmenter les chances de succès de votre attaque. Les recherches préalables sont donc indispensables, un Evil Twin n'est aucun cas une accumulation de faits… Il doit y avoir une personnalité, un fond. Un Evil Twin crédible mélange avec subtilité des informations exactes et des informations plus anecdotiques. L'ensemble doit avoir un semblant de cohérence.

Lorsque ce vrai-faux profil est mis en ligne, vous obtiendrez automatiquement des connexions basiques, dites « organiques ». Ces connexions organiques sont puissantes, elles vous permettent de vous connecter rapidement à d'autres utilisateurs. Plus votre Evil Twin cumule de connexions et plus le nombre de connexions organiques augmente.

Pour un Evil Twin Steve Partmen, nous avons opté pour Facebook qui possède un écosystème applicatif riche. L'idée est de répandre le malware à travers le réseau d'amis, ou plutôt ceux qui pensent que nous le sommes. Créons un compte de messagerie Hotmail, spartmen@live.com et inscrivons-nous sur Facebook. Avec notre table de l'étape 3, indiquons nos centres d'intérêt, films préférés, livres... Ceci fait, tapons le message suivant sur notre mur : « Enfin sur Facebook ! » puis, lions le vrai compte Facebook à celui de Steve pour lui montrer qu'il a au moins un ami. Chargeons avec une légende fictive quelques images trouvées à l'étape précédente. Tous ces éléments ont fait ressortir le profil de Steve, l'Evil Twin n'en est que plus crédible. Le lendemain, envoyons des demandes d'ajout en nous appuyant sur la colonne Souvent de notre tableau croisé. Pour chaque demande, ajoutons le message suivant : « Merci de ne pas en parler au bureau. J'ai pas mal de gens qui me demandent sans cesse de les ajouter comme amis, alors merci de ne pas parler de mon compte Facebook au travail. » À première vue, le message semble étrange à ceux qui le reçoivent, mais au final, cela fonctionne. Nous avons eu des réponses du genre « Pareil pour moi » ou « Tout à fait d'accord »... Cette technique permet d'éviter les soupçons du véritable Steve Partmen sur son lieu de travail.

Résultats

L'Evil Twin de Steve Partmen a pu se connecter à plus de 25 personnes en seulement 24 heures. Seules 7 de ces connexions étaient des demandes que nous avions envoyées. Les 18 autres étaient des gens qui étaient arrivés sur le profil Evil Twin de Steve. Une fois la connexion établie à l'Evil Twin, le malware a pu aisément se répandre sur le réseau de confiance de Steve. La crédibilité de l'Evil Twin ne pouvait pas être remise en cause sachant le nombre de connexions.

En utilisant l'API Facebook, nous avons pu concevoir une petite appli en HTML appelée « J'adore GroundTrans Copr » et nous l'avons envoyée à tous les connectés. 20 ont accepté notre demande. L'application n'était qu'une balise image mais cela aurait très bien pu être une attaque CSRF ou XSS (cross-site scripting).

Suite à la phase de dialogue avec les utilisateurs pour leur expliquer notre démarche, aucun d'eux n'avait suspecté le profil Evil Twin de Steve d'être un faux et encore moins l'application. La plupart n'avaient même remarqué que sa date de naissance était 1930 (alors que Steve a 40 ans). Pour résumer, tous les utilisateurs ont accepté le profil de Steve en se fiant aux images et aux messages publiés.

Une multitude de possibilities !

Un Evil Twin peut être la porte d'entrée à une attaque élaborée. Comme indiqué précédemment, un Evil Twin n'est qu'un moyen pour parvenir à ses fins et non une attaque en elle-même. Un Evil Twin facilite le déploiement de malwares, des attaques par phishing, certaines formes d'intimidation numérique / cyberbullying ou la diffamation. Toutes ces attaques risquent donc de porter préjudice à un individu ou une entreprise et sont rendus possibles par la mise en place de relations de confiance sur les réseaux sociaux.

Conclusion

Alors que les médias sociaux nous permettent de publier n'importe quel contenu, ils nous exposent à certains utilisateurs malintentionnés. Les réseaux sociaux nous permettent de rester en contact avec les personnes qui nous sont chères ou que perdues de vue depuis des années, mais à quel prix... Les attaques Evil Twin montrent combien nous sommes dépendants des medias sociaux et notre désir de nous lier aux autres par les réseaux sociaux. La vigilance est donc le mot d'ordre et la seule arme pour se prémunir de ces menaces. Les réseaux sociaux sont aujourd'hui adoptés par de plus en plus d'entreprises et ces techniques ne feront qu'augmenter dans les mois et les années qui viennent. Restez vigilant !

À PROPOS DE L'AUTEUR

Tim Kulp (CISSP, CEH) est un professionnel de la sécurité informatique travaillant à Baltimore dans le Maryland. Tim est spécialisé dans la sécurité liée au développement logi ciel insi que dans les tests.