Dépôt légal : novembre 2006
N° d'éditeur : 7538
Imprimé en France

# Avant-propos

Aujourd'hui, tout système d'information (ou presque) est connecté à Internet, ne serait-ce qu'indirectement, et de plus en plus souvent via un accès haut débit.

En entreprise comme chez le particulier, il abrite des données vitales et confidentielles. Il fait ainsi partie intégrante du système de production et sa compromission peut avoir des conséquences dramatiques (arrêt des traitements, paralysie des communications, perte voire détournement des informations…).

Comment se prémunir des destructions, espionnages, dénis de service et autres intrusions, possibles usurpations d'identité, tentatives visant à rendre le système non opérationnel ? Dans ce contexte, le système Linux peut jouer un rôle majeur pour la sécurité des réseaux et des systèmes connectés. La sûreté de son noyau, les nombreux outils réputés pour leur fiabilité, et pour la plupart directement intégrés dans ses distributions, conduisent de plus en plus d'entreprises à choisir Linux comme système d'exploitation pour les serveurs applicatifs.

## À qui s'adresse ce livre ?

Cet ouvrage s'adresse aux administrateurs système et réseau qui veulent avoir une vision d'ensemble des problèmes de sécurité informatique et des solutions existantes, dans l'environnement Linux.

Il offre une marche à suivre aux adeptes de Linux ayant la charge d'un petit réseau informatique connecté à Internet, au sein d'une PME ou chez un particulier.

Plus largement, toute personne ayant des bases en informatique et souhaitant en apprendre davantage sur les pirates des réseaux et la façon de s'en protéger grâce à Linux tirera profit de cette lecture.

### Nouveautés de la troisième édition

Cette troisième édition a été enrichie par de nombreux ajouts. Vous y découvrirez en particulier un nouveau chapitre et une annexe entièrement consacrés aux problèmes liés à l'authentification des utilisateurs. Sont traités dans cette partie les systèmes d'authentification centralisés, depuis les plus traditionnels comme la base NIS, jusqu'aux plus évolués qui font appel au protocole LDAP ou au système Kerberos. Le chapitre 10, « Gestion des comptes utilisateur et authentification », décrit les grands principes de fonctionnement et les caractéristiques de ces systèmes d'authentification, tandis que l'annexe B en donne un exemple concret de mise en œuvre.

Dans le chapitre 3, « Attaques et compromission de machines », un exemple de mise en œuvre du *Coroner toolkit* est présenté dans le but de compléter l'analyse forensique d'une machine compromise.

Le chapitre 6, « Sécurisation des services réseaux DNS, Web et mail », comprend quelques ajouts d'importance : moyens de détection des virus dans les courriers électroniques, méthodes de lutte contre les courriers non sollicités, ou *spam*, avec la mise en œuvre des listes grises (*greylists* en anglais), et la sécurisation d'un ensemble de services avec `stunnel`.

Enfin, les possibilités de marquage de paquets d'IPtables sont développées au chapitre 8, « Topologie, segmentation et DMZ », et un exemple de mise en place d'un écran captif utilisant cette technique est présenté. Ce même chapitre est enrichi par la description des principes et de la configuration d'un pare-feu transparent.

## Structure de l'ouvrage

Les notes situées en marge, en éclairant certains points de détail, pourront constituer un deuxième fil conducteur pour la lecture.

La sécurisation et la protection d'un réseau d'entreprise demandent une excellente vue d'ensemble de l'architecture étudiée. Cette troisième édition du Cahier de l'Admin consacré à la sécurisation de systèmes et réseaux sous Linux, reprend la démarche méthodique que nous avions eue lors de la première édition. À travers une étude de cas générique mettant en scène un réseau d'entreprise, nous effectuerons un audit de sécurité pour aboutir à l'amélioration de l'architecture du réseau : filtrage des flux en entrée, sécurisation par chiffrement avec SSL et (Open)SSH, détection des intrusions, surveillance quotidienne…

L'étude de cas met en scène l'entreprise Tamalo.com, d'où sont issus les nombreux exemples pratiques qui illustrent notre propos.

Tout commence avec l'attaque d'une machine connectée au réseau, après laquelle la décision est prise de remodeler la structure informatique de la société. Un dispositif de protection adapté aux objectifs de sécurité de l'entreprise sera alors mis en place.

- Les **chapitres 1 à 3** présentent le contexte de l'étude de cas qui a favorisé ce piratage. On y décrit le développement formidable d'Internet, les problèmes de sécurité qui en découlent, et l'émergence de Linux comme système d'exploitation.

  Celui-ci, bien configuré, pourra servir de parade efficace à ces problèmes. La jeune société Tamalo.com a misé sur Linux pour son système informatique, mais un déploiement trop rapide, sans prise en compte des impératifs de sécurité, aboutit au piratage du réseau.

  L'analyse des machines compromises dévoile le scénario de l'intrusion et met en évidence l'exploitation de la faille (*exploit*) utilisée pour pénétrer les systèmes. Le *rootkit* utilisé par les pirates pour masquer leur présence est découvert.

Chapitre 1, « La sécurité et le système Linux »
Chapitre 2, « L'étude de cas : un réseau à sécuriser »
Chapitre 3, « Attaques et compromissions des machines »

- À partir du **chapitre 4**, la réplique se met en place. Les communications entre les machines sont sécurisées grâce aux techniques de chiffrement. Une section introduit le concept de réseau privé virtuel. Ces techniques qui protégent en particulier contre le *sniff*, ou écoute frauduleuse du réseau.

Chapitre 4, « Chiffrement des communications avec SSH et SSL »

- Les **chapitres 5 et 6** abordent la mise en sécurité des systèmes et des services (une section est notamment consacrée à la sécurité du serveur d'affichage X11). Celle-ci s'appuie sur deux principes simples : préférer des installations automatiques pour garantir l'homogénéité du parc, et opter pour une configuration minimale, sans services inutiles.

Chapitre 5, « Sécurisation des systèmes »
Chapitre 6, « Sécurisation des services réseau : DNS, Web et mail »

- Les services réseau qui subsistent, nécessairement ouverts à l'extérieur, sont alors configurés pour être le moins vulnérables possible.
- Grâce à l'utilisation de pare-feu reposant sur le couple IPtables/Netfilter, on déploie une protection réseau qui constituera le premier rempart contre les attaques extérieures (**chapitres 7 et 8**). La nouvelle topologie du réseau de Tamalo.com fait alors apparaître une zone démilitarisée, DMZ, ouverte à l'extérieur. Cette discussion sur la protection réseau inclut une réflexion sur la sécurité de la technologie Wi-Fi utilisée pour la réalisation d'un réseau sans fil ; elle présente notamment les risques qu'encourent leurs usagers et les solutions de sécurité existantes pour rendre cette technologie plus sûre.

Chapitre 7, « Filtrage en entrée de site »
Chapitre 8, « Topologie, segmentation et DMZ »

- Pour prévoir les cas où une machine de Tamalo.com, restée vulnérable, serait attaquée, voire compromise, on se dote de l'indispensable panoplie d'outils d'audit système et de surveillance : métrologie, prise d'empreintes, détection d'intrusions. Des techniques de leurre, les pots

de miel, permettront d'observer et d'analyser le comportement des pirates lors d'une compromission, et de les détourner des serveurs de production.

- Tous ces outils, décrits au **chapitre 9**, permettent de réagir au plus vite lors d'une attaque. Les données qu'ils produiront seront ensuite analysées pour servir à la réalisation des tableaux de bord, véritables baromètres du réseau informatique, destinés en général aux instances dirigeantes de l'entreprise.

Chapitre 9, « Surveillance et audit »

- Enfin, le **chapitre 10** expliquera comment fonctionnent trois grands systèmes centralisés d'identification et d'authentification des utilisateurs : la base NIS, le protocole LDAP et le système Kerberos.

Chapitre 10, « Gestion des comptes utilisateur et authentification »

- L'**annexe A** concernant les infrastructures à gestion de clés (IGC ou PKI en anglais) vient compléter la partie du chapitre 4 concernant les certificats X.509.
- Enfin, l'**annexe B** met en œuvre les trois grands systèmes centralisés d'identification et d'authentification des utilisateurs présentés au chapitre 10.

## Remerciements

Nous adressons nos vifs remerciements à tous ceux qui ont permis que cet ouvrage voie le jour, et en particulier à notre éditrice Muriel Shan Sei Fan des éditions Eyrolles, qui nous a soutenus tout au long de notre travail de rédaction, ainsi qu'à Nat Makarévitch qui a bien voulu relire ce livre et y apporter sa pertinente contribution.

# Table des matières

chapitre 1

# La sécurité et le système Linux

Le déploiement fulgurant de l'Internet et son omniprésence en tant que moyen de communication auraient dû entraîner la prise en compte des risques associés à la visibilité des machines sur ce réseau de réseaux. Il n'en a pas été ainsi : de plus en plus de moyens informatiques se trouvent exposés à la malveillance des pirates.

**SOMMAIRE**



**MOTS-CLÉS**

- Internet
- DARPA
- Haut débit
- Linux
- Linus Torvalds
- Distributions
- Enjeux
- Objectifs de sécurité
- Menaces
- Failles et défaillances
- Vulnérabilités
- Distributions Linux sécurisées

La démocratisation du haut débit, aussi bien dans les écoles et les universités que dans les entreprises et chez les particuliers, doit s'accompagner d'une prise de conscience des risques liés à la visibilité des machines sur Internet et à la possible malveillance des pirates.

Trois facteurs rendent indispensable le déploiement de la sécurité informatique :

- la préservation du patrimoine de l'entreprise ;
- l'existence d'une menace extérieure, même potentielle ;
- les failles des systèmes.

**Historique**

**L'Internet, une vieille histoire…**

L'Internet est un réseau créé aux États-Unis en 1980, à l'initiative du DARPA (Defense Advanced Research Projects Agency). Il regroupait à ses débuts Arpanet (le réseau de la recherche américaine) et Milnet (le réseau militaire américain), et quelques réseaux universitaires. Il est aujourd'hui vu comme un réseau de réseaux, dont le protocole de communication unique, IP (Internet Protocol), permet le routage d'informations partout dans le monde.

## Enjeux et objectifs de sécurité

Les responsables de certains sites croient parfois à tort que, les données qu'ils abritent n'étant pas confidentielles, l'enjeu de la sécurité est nul pour leur entreprise. Pour autant, accepteraient-ils une indisponibilité de leurs ressources 80 % du temps pour cause de réinstallation suite à une compromission ? Supporteraient-ils que l'accès réseau, qu'ils payent fort cher chaque mois, soit utilisé à 99 % pour un site *warez* et se trouve indisponible pour leurs propres besoins ? Se satisferaient-ils d'être mis en liste noire par leurs correspondants pour avoir négligé un serveur de messagerie qui autorise le relais ? Accepteraient-ils que leurs machines soient mises en cause dans la compromission de tel ou tel site renommé ?

Ainsi, quel que soit le site considéré, il existe toujours une exigence minimale de fonctionnement qui justifie la mise en place de mesures de sécurité adaptées.

Il est important que les responsables de l'entreprise soient directement impliqués dans la définition des enjeux de la sécurité informatique pour deux raisons. La direction du site est capable mieux que quiconque de définir le type d'incidents que les mesures mises en place doivent permettre d'éviter et à quel prix. En outre, si cela s'avère nécessaire, c'est aussi elle qui est le mieux placée pour arbitrer, par exemple, entre le besoin en fonctionnalités et la mise en place d'une mesure contraignante.

D'autre part, il est indispensable de rappeler clairement aux utilisateurs quels sont les objectifs de l'entreprise, pour aboutir à un consensus sur l'arbitrage nécessaire entre convivialité et sécurité.

**Bon sens** **Il y a toujours un enjeu…**

La sécurité est toujours motivée par un enjeu, quel que soit le degré de confidentialité des données, quelle que soit la taille du site et son ouverture sur l'extérieur.

## La menace

Quelque 250 millions de machines sont aujourd'hui connectées sur l'Internet. Il est facile d'imaginer que même si la plupart des internautes sont inoffensifs, il en existe que l'envie de nuire ou de jouer amènera à s'attaquer à

**Référence** **La menace est bien réelle !**

Le CERT Renater est l'organisme chargé de recenser et de suivre les incidents de sécurité informatique sur le réseau national de l'éducation et de la recherche, auquel sont connectées des milliers de machines. Ce réseau est connecté à l'Internet. En moyenne, 2 500 incidents de sécurité par semaine ont été répertoriés depuis le début de l'année 2003. Ils vont du simple *scan* (grâce auquel le pirate examine superficiellement la machine) à la compromission et à la prise de contrôle des machines. La menace est donc bien réelle !

des machines, même assez bien protégées. À cette fatalité statistique s'ajoute le sentiment d'impunité dont jouira un pirate qui s'attaque à votre machine, connecté depuis une chambre d'hôtel à 12 000 km de chez vous. Les pirates l'ont bien compris ; ils utilisent de nombreuses astuces pour se protéger, comme cela sera décrit au chapitre 3.

## Principaux facteurs de motivation des pirates

Les principaux facteurs de motivation des pirates sont les suivants :

- le goût du défi : certains pirates aiment prouver leur habileté et l'étendue de leurs connaissances ;
- l'appât du gain : certains sont appâtés par les rémunérations qu'offrent des entreprises peu scrupuleuses qui souhaitent saboter l'outil de travail informatique de leur concurrent et/ou lui dérober des informations confidentielles (devis, plans, secrets industriels…) ;
- la volonté de détourner à son profit des ressources informatiques dont on ne dispose pas (puissance de calcul, espace disque, connexion rapide au réseau…) ;
- la méconnaissance des conséquences et des risques encourus par des pirates aveuglément hostiles.

## Risques liés au type de connexion

Les connexions permanentes à haut débit sont très recherchées par certaines catégories de pirates, dont l'objectif est d'utiliser cette ressource pour distribuer efficacement films et logiciels piratés.

### Types de connexion à Internet

Les fournisseurs d'accès à l'Internet (FAI) proposent aujourd'hui plusieurs types de connexions au grand public. Le réseau téléphonique commuté (RTC) est le moyen de connexion le moins performant mais certainement encore très répandu à ce jour. ISDN (Integrated Service Digital Network) est plus connu en France sous l'abréviation RNIS (Réseau numérique à intégration de services) ou encore Numéris. Il utilise un signal numérique sur une ligne téléphonique moyennant quelques dispositifs particuliers.

Contrairement au RTC, un abonnement RNIS garantit un débit minimal entre votre installation et votre FAI. Enfin, ADSL (Asymmetric Digital Subscriber Line) est une technique permettant de faire passer des hauts débits sur les lignes téléphoniques analogiques classiques. Les offres ADSL proposent une connexion permanente pour laquelle les débits observés, bien que non garantis, peuvent atteindre environ 200 fois ceux constatés sur le RTC (figure 1-1).

**Figure 1–1** Débits des différents types de connexions à Internet

| | |
|---|---|
| V90 – Modem 56k | = 56 Kbits/s |
| Numéris 64k | = 64 Kbits/s |
| Numéris 128k | = 128 Kbits/s |
| T1 | === 1500 Kbits/s |
| Câble | ========== 4 Mbits/s |
| ADSL | ================== 128 Kbits/s – 8 mbits/s |
| ADSL2 | ============================ 12 Mbits/s |
| ADSL2+ | ========================================================== 25 Mbits/s |

Face à ces pirates, qui cherchent des ressources afin d'abriter leurs sites, tant que vous êtes connectés à votre fournisseur d'accès Internet via un bon vieux modem (RTC), le danger reste limité. En effet, la faible probabilité que le pirate vous trouve connecté, ajoutée au manque d'intérêt qu'il y aurait à prendre le contrôle d'une ressource connectée par intermittences à 56 Kbits/s rend la compromission improbable. Dans ce cas, la sécurité concernera plutôt les problèmes de propagation de virus via la messagerie électronique.

Le fait nouveau aujourd'hui est l'arrivée ou plutôt la démocratisation d'Internet chez les particuliers et dans les petites entreprises via des connexions permanentes à « haut » débit (câble, ADSL). Cette démocratisation ne se fait pas sans heurts, si la composante sécurité n'est pas correctement prise en compte.

### Risques liés aux failles des systèmes

Si les systèmes informatiques ne présentaient aucune faille, ni dans leur conception, ni dans leur configuration, il ne serait pas nécessaire de s'inquiéter de sécurité informatique. On pourrait alors considérer que la menace décrite ci-dessus ne met pas en péril les enjeux importants pour l'entreprise. Mais c'est loin d'être le cas et il n'existe hélas pas de système d'exploitation qui ne présente son lot de vulnérabilités.

HISTORIQUE **Linux, 15 ans déjà !**

Linux voit le jour en 1991 en Finlande. Son créateur Linus B. Torvalds, alors étudiant à l'Université d'Helsinki, se lance dans le développement d'un système d'exploitation pour l'ordinateur qu'il vient d'acquérir, un PC équipé d'un processeur Intel 386. Initialement seul, Linus Torvalds est aujourd'hui accompagné dans cette aventure par de nombreux développeurs.

▸ http://www.linux.org

Diffusé dans le milieu universitaire et scientifique, sa gratuité et sa puissance en font un produit très apprécié des utilisateurs de PC. La grande richesse de Linux et des logiciels qui l'accompagnent lui confère une capacité à remplir une grande variété de tâches. Serveur réseau, poste de développement ou encore poste de travail pour l'utilisateur final, sont quelques exemples des nombreuses possibilités d'utilisation de ce système.

Le nom de « Linux » provient de la contraction des noms « Linus » et « Unix », le système d'exploitation duquel Linux s'inspire très largement.

## Émergence des systèmes Linux

Linux est un système d'exploitation de plus en plus populaire notamment en raison de l'offre croissante d'applications de haut niveau (bureautique, jeux…). La tendance est particulièrement marquée au sein des entreprises, aussi bien parmi les TPE et PME que parmi les grands comptes.

Linux peut être considéré comme une alternative économiquement satisfaisante face aux systèmes d'exploitation commerciaux. Le rapport performance/coût d'une solution à base de micro animé par Linux est très attractif et cette plate-forme peut s'avérer très compétitive pour une grande variété de besoins.

Des dizaines de développeurs ont adapté son code source à leurs besoins. Il existe de nombreux projets de portage du système sur toutes sortes de configurations matérielles, de l'agenda électronique de poche, en passant par la micro-informatique, jusqu'aux grandes machines propriétaires. Parallèlement, plusieurs distributions ont vu le jour et offrent, pour certaines, des supports logiciels commerciaux. Debian, Mandrake, Red Hat et Suse sont les plus connues, mais il en existe bien d'autres encore.

Pour comprendre l'étendue actuelle de la diffusion de Linux, il faut savoir que l'on estime aujourd'hui à 18 millions le nombre de machines dotées de ce système dans le monde.

▸ http://counter.li.org/estimates.php

## Linux et la sécurité

Dans sa jeunesse, Linux a été une cible de choix pour les pirates. En effet, les sources de ce système sont à la disposition de chacun. Il est donc très facile pour un pirate de rechercher dans le code les failles éventuelles et d'en tirer parti à des fins malveillantes. Heureusement, cette ouverture s'avère aujourd'hui faire sa force, car un plus grand nombre de développeurs travaille sur la découverte et la correction des failles. Ainsi, la communauté d'utilisateurs, de plus en plus importante, dispose d'un système testé et éprouvé en permanence. Linux n'a qu'une dizaine d'années et il est arrivé à un degré de maturité très intéressant, là où d'autres systèmes Unix pèchent encore, après plus de 20 ans d'existence !

Ajoutons à cela que les pirates travaillent par petits groupes sinon isolément, tandis que la communauté de ceux qui luttent contre eux (contributeurs et utilisateurs de Linux) œuvrent en bonne intelligence.

Si des lacunes importantes étaient présentes il y a quelques années, elles ont été corrigées et la composante sécurité est bien assimilée lors des développements actuels. Le retard supposé de Linux par rapport à ses concurrents a donc été en grande partie comblé. Aujourd'hui, la réputation de ce système d'exploitation ne reflète pas à sa juste valeur l'important travail des développeurs en matière de sécurité.

Bien que Linux soit à la portée de beaucoup d'informaticiens et de non-informaticiens, il nécessite un suivi quotidien pour que son utilisation soit faite dans les meilleures conditions. Une bonne compréhension des mécanismes du système et une bonne administration sont à la base de la sécurité quels que soient les outils utilisés.

Comme on le verra aux chapitres 5 et 6, il est aujourd'hui possible de configurer un système Linux pour atteindre un niveau de sécurité satisfaisant. Nous verrons également comment Linux peut être utilisé comme pare-feu et constituer ainsi le principal dispositif de sécurité du système informatique.

**B.A.-BA** **Distribution Linux et GNU**

Ce qu'on appelle aujourd'hui communément système Linux consiste en une distribution contenant le noyau Linux (distribué par Linus Torvalds) et un ensemble d'outils permettant d'interagir avec le système et de l'administrer. Un grand nombre de programmes sont également ajoutés à Linux, dans les distributions, pour étoffer l'éventail de ses possibilités, dont la plupart sont de source GNU. GNU est le nom d'un projet initié en 1984 dans le but de développer un système d'exploitation Unix gratuit. Différentes versions du système GNU utilisent le noyau Linux et sont très largement diffusées. On les connaît aujourd'hui sous le nom de système GNU/Linux.

▸ http://www.gnu.org/home.fr.html

## Des distributions Linux sécurisées

Nous verrons dans cet ouvrage comment configurer et sécuriser un système Linux issu d'une distribution Red Hat.

Il faut savoir qu'il existe également des distributions Linux pour lesquelles l'aspect sécurité a été particulièrement réfléchi. Attention néanmoins, Linux n'est pas le système à utiliser pour faire de la sécurité avant tout. Il n'est pas sur ce point particulier, meilleur ou plus mauvais que d'autres systèmes

d'exploitation, mais se situe très certainement dans la moyenne. Une utilisation raisonnée en fera un bon allié, une mauvaise, le pire des ennemis. Notons qu'idéalement, un audit du code effectué avant la construction des binaires, l'installation et l'utilisation de n'importe quel système d'exploitation permettrait de garantir un niveau de sécurité bien supérieur à celui obtenu aujourd'hui lorsqu'il est fourni précompilé sur un support…

▸ http://www.linux.org/dist

**RÉFÉRENCE Caractéristiques des distributions sécurisées Linux**

Sur le site indiqué ci-contre, on compte à ce jour pas moins de 183 distributions de Linux, dont 27 offrent des caractéristiques spécifiques du point de vue de la sécurité. Parmi les caractéristiques intéressantes de ces distributions sécurisées, on note :

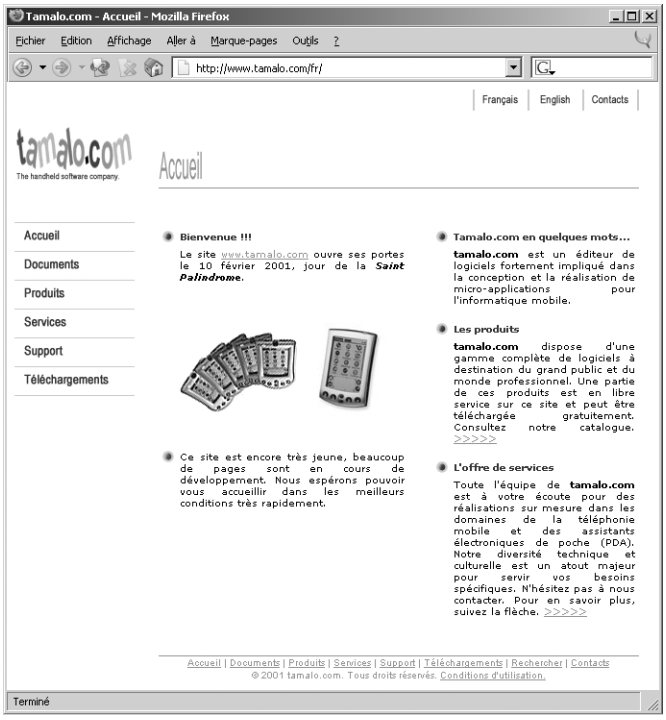
- des distributions orientées vers la réalisation de firewall : Astaro, Frazier Wall Linux, Gibraltar, IPCop Firewall, SME server, smoothwall ;
- des distributions pour s'affranchir des problèmes disque et interdire toute modification du système par les pirates ;
  - des distributions bootables sur CD-Rom : CD Devil-Linux, Gibraltar, White Glove, Knoppix std (knoppix-std.org) ;
  - des distributions s'exécutant complètement en RAM : HV Linux, Trinux ;
  - une distribution résidant en ROM : Linux ROM ;
- des distributions offrant des services sécurisés : EnGarde Secure Linux ;
- des distributions minimalistes : Fli4L, floppyfw ;
- une distribution auto-immunisée : Immunix OS ;
- des distributions orientées chiffrement SSL : Trustix Secure Linux.

## En résumé…

L'Internet fut conçu à une époque où l'on était « entre gens de bonne compagnie ». Mais du fait de la croissance rapide du nombre des machines connectées en permanence, la sécurité informatique est devenue un enjeu. Toute entité visible sur l'Internet doit définir des objectifs de sécurité, face à une menace devenue importante et face aux failles bien réelles des systèmes d'exploitation.

Comme nous le verrons dans cet ouvrage, Linux a atteint une maturité suffisante pour jouer un rôle primordial dans le déploiement de la sécurité d'un site.

chapitre 2


Tamalo.com - Accueil - Mozilla Firefox
Fichier Edition Affichage Aller à Marque-pages Outils ?
http://www.tamalo.com/fr/
Français English Contacts
tamalo.com
The handheld software company.
Accueil
Accueil
Documents
Produits
Services
Support
Téléchargements
Bienvenue !!!
Le site www.tamalo.com ouvre ses portes le 10 février 2001, jour de la Saint Palindrome.
Ce site est encore très jeune, beaucoup de pages sont en cours de développement. Nous espérons pouvoir vous accueillir dans les meilleurs conditions très rapidement.
Tamalo.com en quelques mots...
tamalo.com est un éditeur de logiciels fortement impliqué dans la conception et la réalisation de micro-applications pour l'informatique mobile.
Les produits
tamalo.com dispose d'une gamme complète de logiciels à destination du grand public et du monde professionnel. Une partie de ces produits est en libre service sur ce site et peut être téléchargée gratuitement. Consultez notre catalogue. >>>>>
L'offre de services
Toute l'équipe de tamalo.com est à votre écoute pour des réalisations sur mesure dans les domaines de la téléphonie mobile et des assistants électroniques de poche (PDA). Notre diversité technique et culturelle est un atout majeur pour servir vos besoins spécifiques. N'hésitez pas à nous contacter. Pour en savoir plus, suivez la flèche. >>>>>
Accueil | Documents | Produits | Services | Support | Téléchargements | Rechercher | Contacts
© 2001 tamalo.com. Tous droits réservés. Conditions d'utilisation.
Terminé

# L'étude de cas : un réseau à sécuriser

Le réseau d'une entreprise ordinaire fait l'objet d'une compromission par des pirates : comment réagir, comment analyser l'origine du problème et mettre sur pied une topologie réseau qui pallie les failles mises en évidence ? Comment choisir les outils adéquats ?

**SOMMAIRE**



**MOTS-CLÉS**


- Tamalo.com
- Infrastructure
- Compromission
- Sécurité informatique
- Vulnérabilité
- Segmentation
- Filtrage
- Administration

Ce premier chapitre décrit en détail le contexte de l'étude de cas qui servira de trame à cet ouvrage. Après avoir fait connaissance avec la société Tamalo.com, nous présenterons son infrastructure informatique.

Les failles de cette infrastructure permettront malheureusement la compromission de plusieurs machines de la société par un pirate informatique.

Nous présenterons la topologie réseau retenue pour pallier le problème de sécurité mis en évidence par cette attaque et les outils nécessaires pour rétablir pleinement l'outil informatique sécurisé et fiable dans ses fonctionnalités. Une réponse sera apportée à chacun des points faibles découverts lors de l'étude du piratage des machines de la société.

## Une jeune entreprise

Tamalo.com est un jeune éditeur de logiciels appliqués au domaine très en vogue des agendas électroniques de poche et de la téléphonie mobile.

Après avoir commencé cette aventure dans un garage comme c'est le cas de beaucoup de *startups*, la société comprend maintenant une trentaine de personnes regroupées sur un unique site de travail. Celui-ci réunit le personnel administratif et commercial ainsi que les équipes techniques de développeurs et les administrateurs système et réseau.

L'équipe de développeurs constitue la valeur ajoutée de l'entreprise. Elle a en charge la spécification et la création de nouveaux produits. C'est cette même équipe qui assure le support technique aux clients de la société. Les développeurs préconisent les moyens en fonction de leurs besoins. Ils ne sont au départ pas particulièrement sensibilisés à la sécurité. Seules les fonctionnalités les intéressent. De plus, ils sont traditionnellement attachés à la liberté, qu'ils considèrent comme partie intégrante de l'esprit Internet qui les motive.

Un petit groupe d'administrateurs système et réseau gère le parc informatique nécessaire à l'activité de la société.

Enfin, le service administratif gère le personnel, l'achat des fournitures et les relations avec les fournisseurs. Le service commercial s'occupe de la prospective, de la promotion des logiciels et du suivi des transactions commerciales.

## Les besoins de la société en termes de services

Tamalo.com a fait le choix d'administrer avec ses ressources propres le parc matériel et logiciel nécessaire à son fonctionnement.

Les deux fondateurs de la société ont également misé sur l'utilisation du système Linux et d'Internet pour la promotion, la diffusion et le support de leurs produits. Pour cela, l'équipe informatique a déployé des services réseau accessibles depuis l'extérieur pour la clientèle et les partenaires de la société.

- Un site web, http://www.tamalo.com, est ouvert pour promouvoir l'entreprise et ses logiciels. Ces derniers, et la documentation associée, sont disponibles pour le téléchargement en version d'évaluation. Ce site permet aussi l'enregistrement en ligne de ses nouveaux clients.
- Un service de transfert de fichiers FTP anonyme, ftp.tamalo.com, permet également la diffusion des logiciels et des mises à jour.

Parmi les services nécessaires au bon fonctionnement de l'entreprise, on compte aussi :

- une application de gestion des dossiers clients et des commandes utilisant une base de données accessible depuis le réseau ;
- une messagerie électronique utilisée par le personnel pour la communication interne, mais aussi pour la communication avec le monde extérieur, en particulier pour le support commercial et technique et les relations avec les fournisseurs ;
- un service de résolution de noms pour la gestion des couples « noms de machines/adresses IP » du domaine « tamalo.com » ;
- un service de fichiers distant pour le stockage des documents ;
- un service d'impression réseau permettant d'accéder aux différentes imprimantes du bâtiment à partir de n'importe quel poste de travail ;
- un service d'annuaire électronique.

## Les choix techniques initiaux de Tamalo.com

Cette section présente les différentes solutions techniques retenues par l'équipe informatique de Tamalo.com pour assurer l'ensemble des services réseau. La plupart des distributions Linux incluent ces outils nécessaires au fonctionnement d'une infrastructure informatique classique. Concernant la distribution du système Linux, c'est Red Hat qui a été retenue par le service informatique de Tamalo.com. Mis à part le système de gestion de paquetages (RPM) et quelques subtilités dans le nommage de certains fichiers, les informations contenues dans cet ouvrage sont aisément transposables à l'ensemble des distributions Linux.

**ALTERNATIVE Debian**

Bien entendu, un choix tout à fait acceptable aurait été celui de Debian qui présente de nombreux avantages : politique de création et diffusion des paquetages très stricte et processus de mise à jour fort bien conçu et réalisé.

## Web et services associés

Ce service essentiellement à destination de la clientèle est également utilisé pour la communication interne et les relations avec les partenaires. Des zones publiques y sont définies, ainsi que des zones dont l'accès est plus restreint. Les pages à usage interne doivent rester confidentielles. Ces fonctionnalités seront assurées par le serveur Apache.

OUTIL **Serveur Web Apache**

Le serveur HTTP (*Hyper Text Transfer Protocol*) Apache est très largement diffusé dans les distributions Linux. C'est ce qui explique en partie sa popularité dans le monde et l'utilisation intensive qui est la sienne.

- http://www.apache.org

## Transfert de fichiers

Un accès anonyme au service de transfert de fichiers FTP (File Transfer Protocol), c'est-à-dire un accès permettant à n'importe qui de télécharger des logiciels édités par Tamalo.com, est ouvert. Le serveur WU-FTPD utilisé dans ce cadre, est contenu dans les distributions Linux les plus courantes.

- http://www.wu-ftpd.org/

ALTERNATIVE **HTTP/scp**

On pourra aussi déployer un Apache grâce auquel certains téléchargeront via HTTP. Les utilisateurs disposant de comptes pourront uploader des fichiers avec `scp`, la version sécurisée SSH de la commande Unix de copie de fichiers `cp`.

## Base de données

Pour les applications internes à l'entreprise, comme la gestion des dossiers clients, il a été décidé d'utiliser un logiciel développé en interne utilisant un service de base de données réseau. MySQL est désigné comme le candidat pour remplir le rôle de gestionnaire de base de données.

- http://www.mysql.org

ALTERNATIVE **PostgreSQL**

Dans certains cas, le serveur de base de données PostgreSQL, plus puissant, sera plus adéquat car plus proche des logiciels déjà employés sur le site. Les aspects liés à la sécurité sont très semblables.

## Résolution de noms

Le service DNS (Domain Name System) assure la résolution des adresses IP (Internet Protocol), utilisées par les machines pour les communications réseau, en noms intelligibles et réciproquement. Le DNS est également utilisé par le service de messagerie électronique pour déterminer le ou les serveurs de messagerie à contacter pour délivrer le courrier sur les différents sites connectés à l'Internet.

Ce service permet en particulier la gestion du domaine `tamalo.com` et de la plage d'adresses IP qui lui a été attribuée. Le sous-réseau utilisable par les équipements réseau de Tamalo.com est défini par la notation CIDR (Classless Inter-Domain Routing) 193.48.97.64/27. Cela définit une plage de 32 adresses car la notation « /27 » réserve les 27 premiers bits à l'identifica-

OUTIL **BIND (Berkeley Internet Name Domain)**

BIND est une implémentation libre du protocole DNS. Il inclut un serveur DNS, une librairie pour la résolution de noms et un ensemble d'outils de diagnostic et de contrôle du service DNS. C'est l'implémentation la plus populaire. Elle est diffusée par l'ISC (Internet Software Consortium).

- http://www.isc.org/products/BIND

tion du réseau ; il reste donc 5 bits pour créer des combinaisons identifiant les machines ($2^5 = 32$).

Les machines de la société visibles depuis Internet auront donc des adresses IP comprises entre 193.48.97.65 et 193.48.97.94 – 193.48.97.64 correspondant à l'identificateur du réseau et 193.48.97.95 étant réservée au *broadcast*.

### Messagerie électronique

La messagerie électronique de l'entreprise utilise le protocole de transport de courrier SMTP (Simple Mail Transfer Protocol) pour délivrer les messages entre sites, à l'aide du très classique et très répandu Sendmail. Les postes de travail clients utilisent le protocole IMAP (Internet Message Access Protocol) pour accéder aux boîtes à lettres.

**Serveur SMTP**

- http://www.sendmail.org

**Serveur IMAP**

- http://www.washington.edu/imap

### Partage de fichiers

Afin de centraliser l'ensemble des documents produits par les différents services de la société et pour faciliter leur sauvegarde, un système de fichiers centralisé accessible via le réseau par les différents postes de travail est mis à la disposition du personnel. Le serveur de fichiers, un PC Linux, utilise le produit NFS (Network File System) comme support à ce service.

### Impression réseau

Les outils lprng fournis avec le système Linux issu d'une distribution Red Hat sont utilisés pour le service d'impression réseau. Ce service permet en particulier d'imprimer à partir de n'importe quel poste de travail sur n'importe quelle imprimante de la société.

## L'infrastructure informatique vieillissante et vulnérable

Bien que la société se soit agrandie et ait déménagé dans des locaux plus vastes et plus confortables, l'infrastructure système et réseau initiale déployée depuis quelques années a évolué sans grande concertation et n'a jamais fait l'objet d'une remise en cause globale.

L'ensemble des machines, des PC Linux pour les postes de travail et les serveurs d'applications, partage l'unique réseau local de l'entreprise. Ce réseau est naturellement ouvert sur l'extérieur (Internet) pour les besoins de communication et de distribution des logiciels évoqués précédemment.

**B.A.–BA IP (Internet Protocol)**

IP a été développé dans les années 70-80 par l'agence DARPA (Defense Advanced Research Projects Agency) pour permettre à des équipements informatiques divers de communiquer entre eux. On le trouve en général associé à TCP (Transmission Control Protocol) et à UDP (User Datagram Protocol). Une adresse logique unique de 32 bits est attribuée à chaque machine du réseau pour permettre de l'identifier. C'est l'adresse IP. Elle est utilisée par la couche réseau des systèmes pour effectuer le routage des informations jusqu'à leur destination finale.

L'environnement Linux a été choisi en raison de son faible coût d'acquisition, mais aussi parce qu'il correspondait bien à un état d'esprit d'ouverture cher à Tamalo.com. À l'exception des ateliers de développement logiciel, l'ensemble des outils sont libres ou du domaine public, notamment pour ce qui concerne les services réseau.

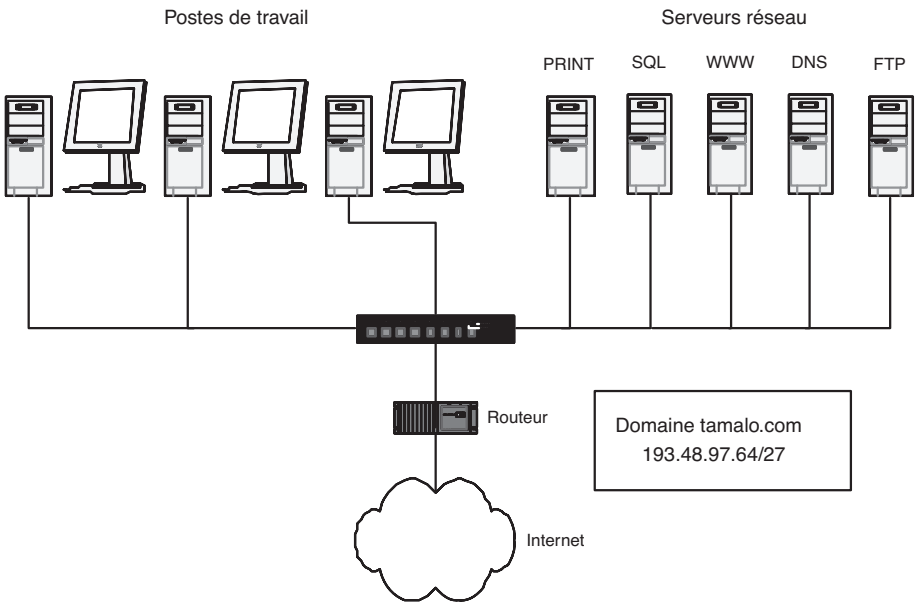



**Figure 2–1**
Réseau historique

## La compromission du site

Un retard dans la mise à jour d'un service d'impression, et la sanction tombe. Une machine, puis l'ensemble du réseau, sont compromis depuis l'extérieur. L'infrastructure s'est révélée inefficace contre l'attaque subie. Elle a même très certainement contribué à favoriser sa propagation en offrant un accès illimité à la totalité des ressources informatiques du site. Une gestion au coup par coup des postes de travail et un suivi irrégulier des systèmes sont également à mettre en cause.

Des données sensibles pour l'entreprise, en particulier des mots de passe permettant l'accès à des ressources d'entreprises partenaires, ont été compromises. Ces ressources n'ont heureusement pas été exploitées par les pirates, dont l'objectif était seulement d'utiliser les moyens informatiques de Tamalo.com. La société a échappé de justesse à une situation dont les conséquences auraient pu être très graves pour son avenir. Cette compromission aura quand même eu le côté positif de provoquer à tous les niveaux, des développeurs à la direction, une prise de conscience du risque et des enjeux de la sécurité informatique.

Cette attaque sera décrite plus en détail au chapitre 3 « Attaques et compromissions de machines ».

## Mise en évidence des vulnérabilités

Un audit de sécurité est réalisé par l'équipe en charge de la gestion des moyens informatiques, qui constate de réels défauts dans l'infrastructure réseau, dans le choix des logiciels applicatifs utilisés, et au niveau de la stratégie de gestion des accès.

1. Le réseau n'est pas entièrement commuté. Pour des raisons historiques, un câblage 10Base2 subsiste sur une grande partie du réseau. Utilisé pour connecter physiquement les ordinateurs sur le réseau local, ce câblage favorise l'écoute frauduleuse et donc la capture des informations sensibles qui transitent entre machines.
2. Il n'y a pas de segmentation physique ni de cloisonnement du réseau. Une fois dans la place, le pirate a donc pu librement écouter l'ensemble des communications, y compris dans les zones les plus sensibles.
3. Les protocoles de communication utilisés sont fragiles (FTP, TELNET, IMAP). Ils laissent transiter sur le réseau des informations sensibles non chiffrées, comme les noms de comptes et les mots de passe associés.
4. L'absence d'outils de surveillance nuit à la détection rapide des tentatives de compromission.
5. Les applicatifs réseau présentent de nombreux défauts de configuration et ne sont pas utilisés systématiquement à leurs meilleurs niveaux de sécurité. Le suivi des mises à jour des systèmes d'exploitation et des logiciels est inexistant.
6. La gestion des accès au réseau en entrée de site est inexistante. Chacune des machines de la société est vue de l'extérieur et devient par conséquent une cible potentielle.

## La refonte du système informatique

Consciente de la situation de crise à laquelle peut conduire un acte de piratage, la direction de Tamalo.com décide d'entreprendre une complète réorganisation de ses moyens informatiques. La composante sécurité devient primordiale dans la réflexion qui est entreprise. C'est la mise en œuvre de cette réflexion que nous allons traiter au cours de cet ouvrage.

Une réponse à chaque problème soulevé sera apportée dans la limite de ce que la technologie peut offrir de meilleur en terme de sécurité.

Le contenu du tableau 2-1, page suivante, résume l'ensemble des points sur lesquels les personnes en charge de la gestion des moyens informatiques devront travailler.

**Tableau 2–1** Alternatives sécurisées

| Défaut | Action | Outils |
|---|---|---|
| Technologie matérielle d'interconnexion inadaptée (10Base2) | Remplacement par 100BaseT<br>Utilisation de commutateurs réseau | Les matériels de type HUB, dont le comportement est similaire à celui de 10Base2, seront éliminés au profit de commutateurs supportant les VLANs |
| Pas de segmentation, réseau plat | Création de plusieurs sous-réseaux locaux<br>Contrôle d'accès suivant les rôles de chaque équipement | Linux/Netfilter/IPtables utilisés comme routeurs filtrants |
| Gestion d'accès inexistante | Filtrage systématique des réseaux et des machines | Linux Netfilter/IPtables, TCP Wrapper |
| Protocole de communication réseau vulnérable à l'écoute frauduleuse (sniff) | Mise en œuvre systématique de solutions utilisant le chiffrement (cryptage) pour protéger les données sensibles | SSH remplace TELNET, FTP, RSH<br>IMAPS remplace IMAP<br>HTTPS remplace HTTP |
| Couches basses des protocoles réseau sensibles à l'usurpation d'identité (spoofing d'adresse IP) | Mise en place de mécanismes d'authentification | SSH, SSL |
| Absence de surveillance | Métrologie réseau<br>Outils de détection d'intrusion, surveillance de l'intégrité des systèmes<br>Audit sécurité | Déploiement d'outils (Nmap, Nessus, Snort, Tripwire, antivirus/mail) |
| Défaut de configuration des OS et des applicatifs | Formation, bonnes pratiques d'administration | Config de BIND, HTTP, Sendmail, etc. |

## Le projet d'une nouvelle infrastructure réseau

La figure 2-2 représente une architecture prenant en compte les différentes réflexions liées aux problèmes de topologie réseau et de contrôle d'accès évoqués lors de l'audit. Chaque besoin a été défini et chaque fonctionnalité identifiée de manière à compartimenter les équipements informatiques de façon adaptée.

Trois groupes ont été définis. Les postes de travail du personnel de la société seront regroupés logiquement sur le même sous-réseau. Les services à vocation interne (NFS, SQL, PRINT, LDAP) seront également isolés. Enfin, le troisième groupe comprendra les services en contact avec l'extérieur DNS, HTTP, FTP, MAIL.

Les trois sous-réseaux seront interconnectés via le réseau local principal de l'entreprise. L'accès à chacun d'eux sera géré par des PC/Linux faisant office de routeurs et de pare-feu. L'outil de filtrage réseau utilisé sur le système Linux est Netfilter/IPtables. Sur chacune des machines, un filtrage complémentaire sera appliqué afin de répondre aux besoins de sécurité spécifiques à chaque service.

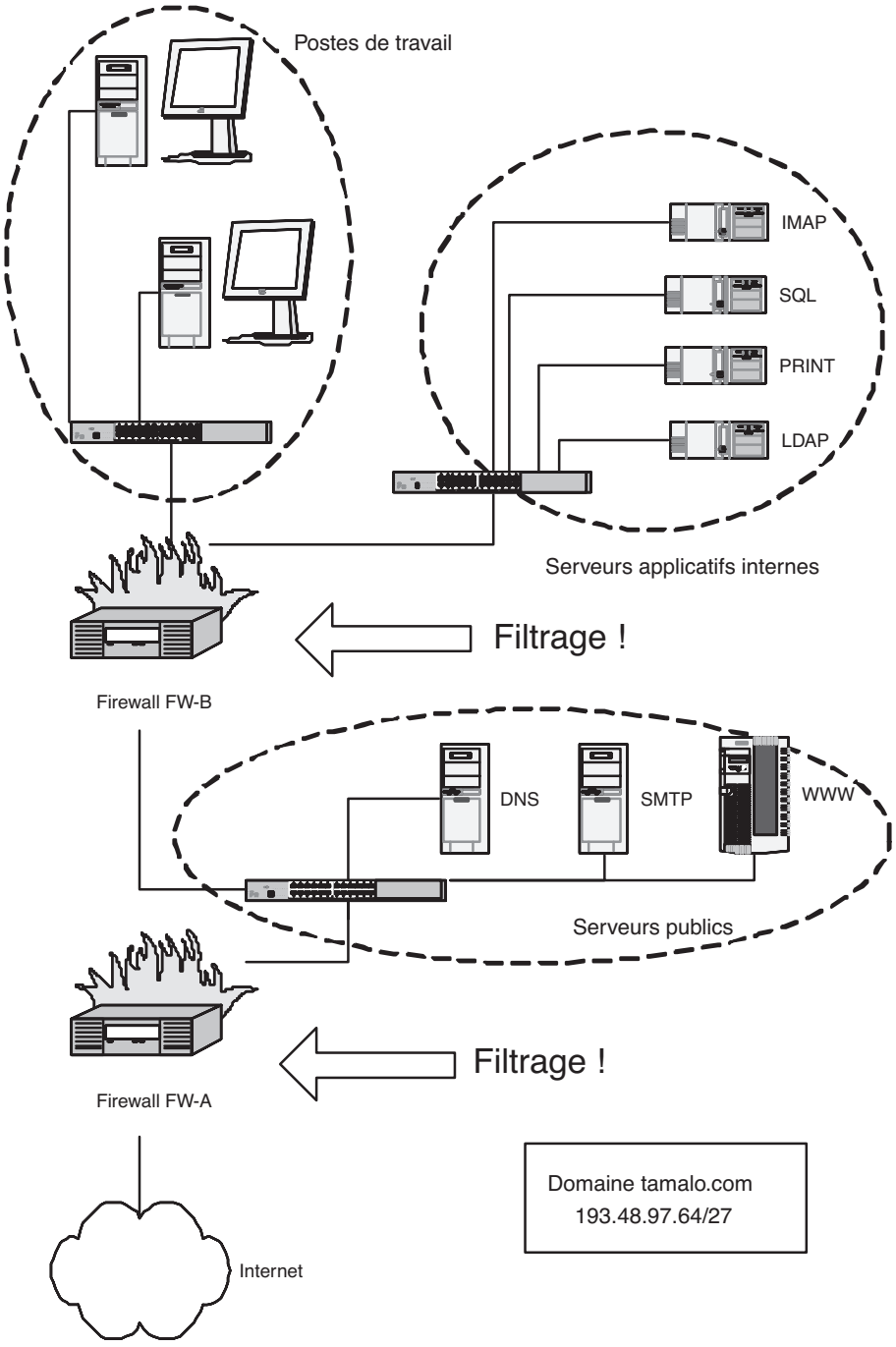



**Figure 2–2**
Nouvelle infrastructure

## Études des flux réseau

Afin de déterminer les types de filtrages à appliquer sur chacun des sous-réseaux, il convient d'étudier la nature des flux entre les différents équipements, que ce soit à l'intérieur du réseau de l'entreprise ou avec le monde extérieur.

Les postes de travail destinés au personnel n'offrent pas et ne doivent pas offrir de service. Par conséquent, ces machines doivent être invisibles depuis l'extérieur de Tamalo.com. L'activité quotidienne du personnel nécessite que ces postes n'aient pas de restriction d'accès vers l'extérieur (figure 2–3).

Les serveurs d'applications à usage interne (SQL pour les bases de données par exemple) sont isolés du monde extérieur. Ils ne seront accessibles que par les postes de travail du personnel ou par l'intermédiaire des machines offrant les services publics.

Le troisième sous-réseau comprend les serveurs en contact avec l'extérieur DNS, HTTP, FTP, MAIL. Leurs accès depuis l'extérieur doivent être autorisés mais néanmoins contrôlés. Cette zone, plus ouverte que les deux premières et orientée vers l'extérieur, est plus vulnérable. Elle sera soumise à une surveillance accrue de la part des administrateurs.

## Vers des outils de communication sécurisés

Comme cela a été le cas pour le système d'information de Tamalo.com, lorsque le pirate dispose d'un accès sur une des machines du réseau, il lui est facile de capturer la totalité du trafic. Afin de se prémunir de ce risque et pour contrer toute tentative de piratage, il est indispensable de protéger les informations sensibles qui doivent transiter entre les machines. Des solutions dites sécurisées, c'est-à-dire chiffrant l'ensemble des données échangées, sont apparues dans le but de combler les lacunes des produits existants. Des mécanismes garantissant l'authenticité de chacun viennent compléter la confidentialité des données.

SSH (Secure Shell) en particulier, est l'alternative choisie par les administrateurs de Tamalo.com pour sécuriser les connexions interactives et les transferts de fichiers entre machines. OpenSSL (Open Secure Sockets Layer), utilisé conjointement avec un serveur Web et un serveur IMAP, a été retenu pour sécuriser les accès aux informations confidentielles diffusées par ces deux systèmes. Nous verrons leur mise en œuvre au cours de cet ouvrage.

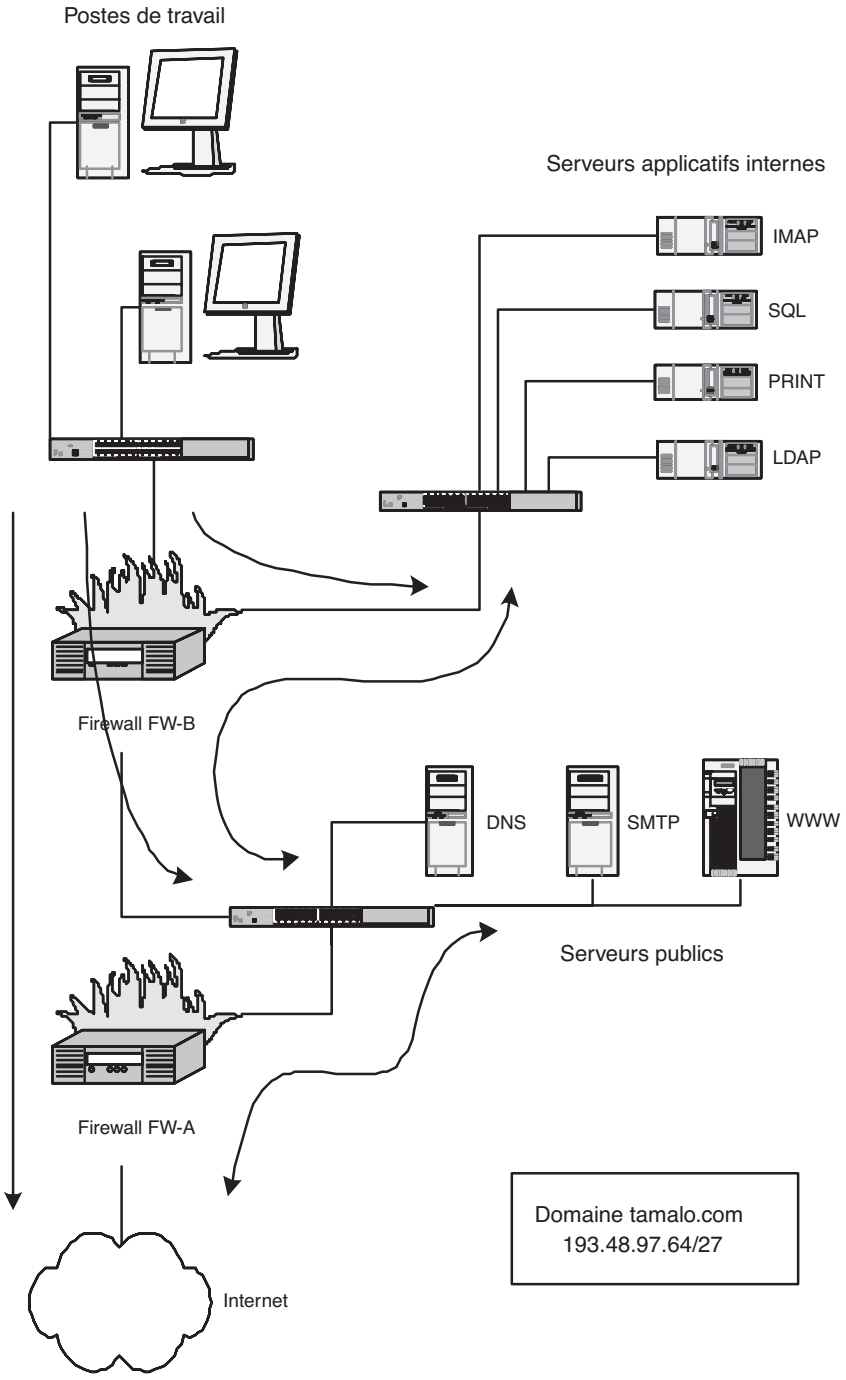



**Figure 2–3**
Étude des flux réseau

## Un suivi et une gestion quotidienne du système d'information

Le système informatique parfaitement inviolable n'existe pas. Au cours du temps, l'administrateur système et réseau améliore la sécurité du système dont il a la gestion, tandis que le pirate, lui, trouve de nouvelles failles toujours plus ingénieuses. La sécurité informatique est un domaine où la surenchère est permanente.

C'est pourquoi il est indispensable d'assurer un suivi régulier du système informatique afin de limiter au maximum les vulnérabilités connues. La prise en compte des mises à jour à mesure de leurs parutions, bien que représentant une quantité de travail importante, est déjà une défense efficace face à la menace permanente. Il serait inconscient et dangereux de sous-estimer le travail de suivi des systèmes d'exploitation et des logiciels.

La surveillance régulière du système est également primordiale pour une détection efficace des attaques. Découvrir rapidement une compromission ou une tentative de compromission permet d'éviter ou de limiter l'étendue des dommages. Parallèlement, l'audit sécurité du système éprouve et valide la robustesse des mesures déployées. Nous traiterons à ce titre des scanners Nmap et Nessus.

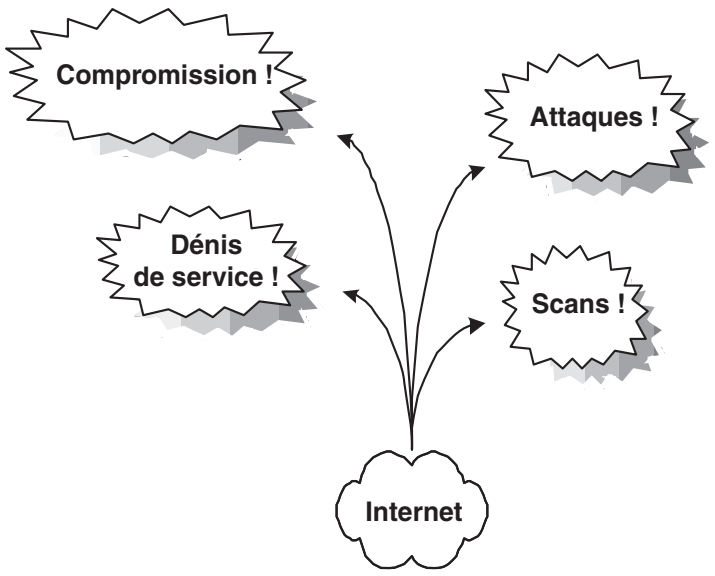
## En résumé…

Sécuriser le système informatique est une tâche qui nécessite des ressources humaines. Certains administrateurs la négligent par méconnaissance des risques et, à l'image de la société Tamalo.com, en font parfois rapidement les frais.

Face à un problème de sécurité dont les conséquences ont été heureusement limitées, la direction de Tamalo.com a analysé ses moyens informatiques afin d'en redéfinir complètement l'infrastructure et les composants.

Les chapitres qui vont suivre décrivent étape par étape l'élaboration et la mise en place des solutions définies par la nouvelle politique de sécurité.

chapitre 3



# Attaques et compromissions des machines

L'attaque survenue à Tamalo.com offre l'occasion d'analyser les différentes étapes de la compromission d'une machine ainsi que les contre-mesures adéquates. Là encore, il ne faut pas négliger le profil, les motivations et les techniques des pirates pour concevoir un niveau de protection adapté.

**SOMMAIRE**



**MOTS-CLÉS**

- kiddies, hackers, crackers
- warez, rebond
- DDOS, buffer overflow
- exploit, scan
- compromission
- rootkit, t0rn, sniffer
- Ethereal
- backdoor
- promiscous
- OSI, MAC
- Logs, core, Whois, CERT, abuse

Le but de ce chapitre est d'alarmer le lecteur par la description d'une intrusion informatique et des outils mis en œuvre par les pirates. Les administrateurs voire les utilisateurs qui ont vécu une telle intrusion deviennent souvent les meilleurs défenseurs du développement de la sécurité informatique.

À partir du cas concret survenu à Tamalo.com (figure 3-1), il s'agit de connaître le mieux possible les différentes étapes de la compromission d'une machine afin d'être à même de contrer efficacement une attaque.

Nous décrirons également comment réagir face à une intrusion dans un système informatique, comment analyser les systèmes compromis, quelles organisations peuvent être utiles dans un tel cas.

Pour commencer, une connaissance du profil, des motivations et des techniques de ceux qui nous attaquent permettra de bien évaluer le risque et d'adapter le niveau de protection de nos systèmes.

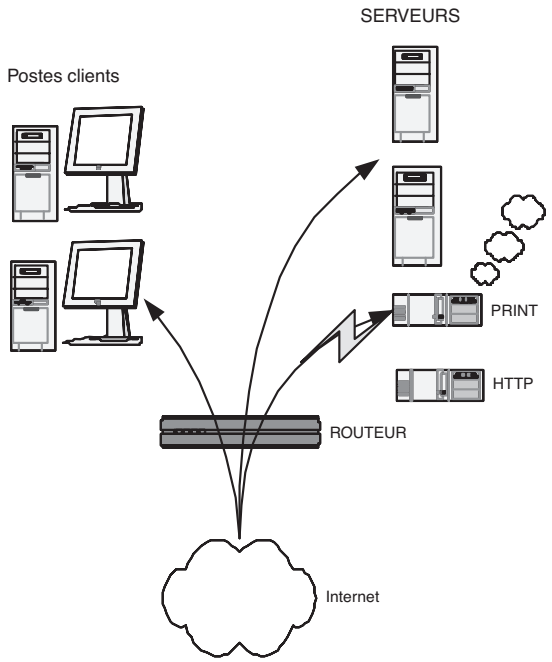



**Figure 3–1**
Vulnérabilité du serveur d'impression de Tamalo.com

### Carder, phreaker, hacker, cracker, script kiddies

Le *carder* est impliqué dans la réalisation de fausses cartes bancaires.

Le *phreaker*, est spécialisé dans le vol d'unités téléphoniques dans les autocommutateurs.

Le *hacker* est un expert des systèmes d'exploitation. Il cherche à mettre en évidence les points faibles des systèmes mais s'interdit leur exploitation malveillante.

Beaucoup moins scrupuleux que les *hackers*, les *crackers* n'hésitent pas à utiliser les points faibles des systèmes à des fins nuisibles.

Dépourvus de compétences techniques les *script kiddies* ou plus simplement les *kiddies* utilisent, sans les comprendre, des scripts qui leur permettent de prendre le contrôle de leur cible.

## Kiddies, warez et rebonds

Les pirates informatiques se répartissent principalement en deux catégories qui ont chacune une clientèle, des moyens et des objectifs différents.

Le plus grand nombre d'entre eux est constitué par les *kiddies* (« marmots ») ou *script kiddies*, parfois des adolescents, qui épatent leurs amis en prenant la

main sur tel ou tel site plus ou moins connu. Il faut savoir qu'à l'heure d'Internet, il n'est pas nécessaire d'être un *gourou* des systèmes et des réseaux pour être un pirate informatique. Il faut juste une petite dose de curiosité ajoutée à la méconnaissance des risques encourus. Du point de vue pratique, tous les outils sont disponibles sur le Web. Avec quelques mots-clés et un bon moteur de recherche, le jeune pirate se trouvera en quelques minutes en possession d'une panoplie d'outils permettant de prendre le contrôle d'une machine, quelque part dans le monde.

À l'autre extrême, un petit nombre de pirates est issu de la communauté des *crackers*, à ne pas confondre avec les *hackers*. Ces derniers, dans le monde de la sécurité, sont des développeurs système extrêmement pointus dans leur domaine qui éprouvent la sécurité des systèmes dans le but de la renforcer. Les crackers, eux, étudient les failles des systèmes et écrivent des programmes permettant d'en prendre le contrôle. Ils publient ces programmes qui sont alors mis en œuvre par des *script kiddies*.

Les motivations des pirates pour attaquer un site peuvent être de plusieurs ordres. Tout d'abord, la prise de contrôle de machines dans le but d'en utiliser les ressources, par exemple pour y installer un site warez, un robot IRC (Internet Relay Chat) ou un scanner.

Autre motivation possible, l'utilisation de la machine comme rebond, dans le but d'en attaquer une autre. Cette technique est fréquemment utilisée car c'est une garantie d'impunité pour le pirate. En effet, pour remonter la chaîne des machines compromises, il faut contacter les sites correspondants, qui, tour à tour, vont mettre un certain temps à trouver la cause de l'attaque, puis protester auprès du site attaquant. Dans l'hypothèse favorable, tous les administrateurs des sites concernés réagissent et essaient de trouver la cause du problème. Pourtant, après seulement quelques rebonds, le pirate peut être assuré que plusieurs semaines vont s'écouler pour remonter sa piste. Ainsi les traces les plus flagrantes contenues dans les routeurs ne seront plus disponibles le jour où il aurait été possible d'identifier sa machine.

Enfin, dans certains cas, des machines sont compromises afin de constituer un pool de machines sous le contrôle d'un pirate. Le moment venu, ce dernier pourra lancer, à partir de l'ensemble de ces machines compromises, une attaque en déni de service distribué, en anglais DDOS (Distributed Deny Of Service), vers la cible de son choix. Ce type d'attaque peut mettre en jeu plusieurs centaines de machines ! Une telle attaque a été dirigée le 21 octobre 2002 contre les serveurs racines du DNS (Domain Name System) mondial. Ces 13 serveurs racines, root servers, sont à la base de la résolution nom – adresse IP pour toute communication sur Internet. L'attaque a rendu inopérants 9 des 13 serveurs racines, ce qui aurait pu avoir comme conséquence un blocage complet de l'Internet mondial !

**B.A.-BA Mettre à jour pour sécuriser**

La publication des techniques d'exploitation des failles mène à la correction des sources des programmes vulnérables. Ainsi, il devient de plus en plus difficile pour les pirates d'y découvrir de nouvelles défaillances. L'administrateur avisé ne manquera pas de mettre à jour fréquemment ses programmes grâce à une source sûre et se défiera des codes immatures.

**Qu'est-ce que c'est ? Warez**

Un site warez est constitué d'une machine sous le contrôle d'un pirate, dotée le plus souvent d'un espace disque important, ainsi que d'un bon accès réseau.
Les pirates y déposent des logiciels, des films ou des fichiers qu'ils veulent distribuer. L'adresse du site piraté est le plus souvent diffusée par l'intermédiaire de canaux IRC.
Une machine warez génère toujours une charge réseau considérable, capable de saturer un lien ADSL de quelques centaines de Kbits/s (trafic montant), aussi bien qu'une liaison spécialisée de plusieurs dizaines de Mbits/s ! C'est parfois même la présence de ce débit anormal qui éveille l'attention de l'administrateur réseau !

# Scénario de l'attaque du réseau de Tamalo.com

## Une faille dans le système

À l'heure actuelle, les compromissions de machines exploitent pour la plupart une faille du système ou une erreur dans la configuration de ce dernier. La faille la plus classique utilisée pour prendre le contrôle d'un service est le débordement de mémoire-tampon ou *buffer overflow*, en anglais.

**B.A.-BA Débordement de mémoire et exécution de code arbitraire**

En voici le principe : un service, par exemple wu-ftpd sous Linux, reçoit des arguments depuis l'application cliente. Ces arguments transitent par une zone de mémoire allouée par le service.
Si le service ne vérifie pas correctement les arguments qu'il reçoit (taille…), un débordement de mémoire est possible.
Ainsi, l'application cliente, parfois modifiée par un cracker, envoie au serveur un argument beaucoup trop long. Une partie de cet argument écrase donc le contenu de la mémoire qui suit immédiatement la zone allouée par le service. À cet endroit étaient stockées des instructions qui vont être prochainement exécutées par le processus serveur.
En écrasant ces instructions, le pirate va donc pouvoir faire exécuter le code de son choix à la machine, sous l'identité du service !
Si ce dernier tourne en mode privilégié, il est probable que le client aura bientôt un accès sur le compte administrateur `root` de la machine…

## L'exploitation de la faille (« exploit »)

La publication d'une nouvelle faille entraîne une course contre la montre entre les crackers et les développeurs des systèmes. Les premiers travaillent à l'écriture d'un « exploit » : il s'agit d'un programme permettant d'exploiter la faille, c'est-à-dire de prendre le contrôle de toute machine employant la version vulnérable. Les autres travaillent à l'écriture d'une nouvelle version ou d'un correctif, nommé *patch* en anglais.

À ce jeu-là, les pirates ont malheureusement toujours l'avantage, car même si dans la plupart des cas le patch arrive avant l'exploit, celui-ci n'est jamais déployé à temps sur l'ensemble du parc immense que constitue Internet.

Le cracker met son exploit à la disposition de la communauté des pirates par l'intermédiaire d'un certain nombre de sites Internet connus dans ce milieu. De leur côté, les développeurs diffusent le patch de sécurité.

## Utilité des scans réseau

Si vous avez un jour la curiosité d'analyser le trafic à la frontière de votre réseau, vous aurez la surprise de voir que les scans y sont permanents. Cela signifie qu'il y a toujours quelqu'un, quelque part, en train d'analyser votre parc informatique pour voir si une machine de votre réseau n'offre pas, par hasard, une faille connue.

Si vous êtes en charge de ce réseau, ne négligez pas toute cette surveillance. En effet, une compromission est le plus souvent précédée d'un scan. C'est l'élément qui permet au pirate d'avoir la liste des machines et des services de votre réseau qui présentent une vulnérabilité.

Par exemple, un attaquant pourra scanner le port 80 de l'ensemble de votre réseau afin d'établir la liste des serveurs web accessibles depuis l'extérieur.
Le scanner n'est pas un outil réservé aux pirates. Un administrateur réseau se doit d'en posséder un pour établir la liste des services offerts sur son réseau. Le scanner le plus réputé disponible sous Linux s'appelle Nmap ; il est téléchargeable à partir de l'URL suivante :

- http://www.insecure.org/nmap/nmap_download.html

**Outils Scanner réseau**

Un scanner est un programme qui balaye une plage de ports sur un ensemble de machines, afin d'établir la liste des couples machine/service ouverts.

- Le scan horizontal consiste à scanner un port sur un ensemble de machines.
- Le scan vertical consiste à scanner une plage de ports sur une même machine.

## La compromission

Les pirates ont le plus souvent une connaissance minimale du site choisi pour cible. Ils organisent une attaque pendant une période où la vigilance de l'administrateur est relâchée. Ainsi, les attaques ont souvent lieu la nuit, le week-end, les jours fériés ou pendant les périodes de vacances.

C'est souvent une accumulation de détails plus ou moins anodins qui laisse suspecter la compromission d'une machine.

C'est ainsi qu'au retour des vacances de Noël, un développeur de Tamalo.com se plaint du comportement anormal de la commande `ps` : elle rend un `segmentation fault` en lieu et place de la liste des processus attendue.

Quelques commandes permettent rapidement de cerner le problème :

1. Déterminer où se trouve le programme `ps`.

```
which ps
/bin/ps
```

2. Examiner la date de dernière modification puis de création du fichier.

```
ls -l /bin/ps
ls -lc /bin/ps
```

1. Examiner la nature du fichier `ps`...

```
file /bin/ps
ELF 32-bits LSB executable, blabla.., not stripped ?????
```

L'attribut `not stripped` est étrange pour une commande système. En général, les commandes système sont déployées pour économiser de l'espace disque et la table des symboles n'y figure pas. Cet attribut ne devrait donc pas apparaître, ce qui laisse redouter que le programme ne provient pas de la distribution.

De plus, si le résultat de `ls -l /bin/ps` paraît acceptable, `ls -lc /bin/ps` révèle que le fichier a été créé le 26 décembre dernier ; un administrateur aurait-il installé un nouveau `ps` pendant les vacances ?

Par ailleurs, les utilisateurs de la machine concernée se plaignent de ralentissements et d'accès disque permanents, ce que ne confirme pas la commande `ps`… sauf si cette commande a été modifiée par un pirate afin de dissimuler son activité.

Une seule conclusion s'impose : il est urgent de débrancher la machine du réseau afin de faire des vérifications plus approfondies. Ce n'est pas sans conséquence pour Tamalo.com car ce serveur contient le référentiel CVS qui gère les versions de logiciels.

Le temps de ressortir les CD-Rom de la distribution Red Hat, de recompiler de manière statique quelques commandes originales (`ps`, `ls`, `netstat`) et il va être possible de mesurer l'ampleur des dégâts.

**ATTENTION**

Dans certains cas, le programme au comportement anormal qu'on soupçonne d'avoir été installé par les pirates (ici `ps`) peut contenir une bombe qui se déclenchera après un certain nombre d'invocations. L'existence même d'un doute nous contraint à douter de l'ensemble des programmes installés. On comprendra que la première chose à faire est de réamorcer sur un système sûr et de sauvegarder afin de préserver les données des utilisateurs mais aussi les programmes du système pour une analyse ultérieure. Il faut donc invoquer le moins possible de programmes sur la machine potentiellement compromise.

**B.A.-BA** **En cas de compromission…**

Il est impossible d'affirmer que l'analyse d'une machine compromise permettra de détecter toutes les modifications qu'elle a pu subir. C'est pourquoi la compromission d'un système doit conduire à sa réinstallation complète. Le système de fichiers doit être entièrement reformaté. Cette règle est essentielle pour garantir le retour à un système d'exploitation sain après piratage.

C'était le premier contact pratique de Tamalo.com avec un piratage informatique. Dans ce qui suit, nous allons analyser plus en détail les traces laissées par les pirates au cours de cette compromission afin de mieux connaître les outils utilisés et les failles de nos systèmes qui ont été exploitées.

# Analyse de la machine compromise

## Traces visibles sur le système avant réinitialisation

En cas de compromission d'une machine, il est utile de récupérer quelques indicateurs de l'état du système d'exploitation avant tout redémarrage. En effet, les pirates disposent parfois d'outils permettant d'effacer leurs traces après un redémarrage.

Il faut en premier lieu s'assurer que les commandes utilisées sont saines. Certaines commandes peuvent avoir été modifiées par les outils dont dispose le pirate, par exemple afin de masquer sa présence. Ces modifications ont pu être faites à différents niveaux :

- Modification des commandes : `ps`, `ls`, `netstat`, `find`, `du`, `passwd`, etc. Dans ce cas, la parade consiste simplement à recopier la commande d'origine sur le système.
- Modification des bibliothèques dynamiques : les fonctions incluses dans les bibliothèques dynamiques sont utilisées lors de l'exécution d'une commande (la commande `ldd /bin/ps` fournira la liste des bibliothèques utilisées par la commande `/bin/ps`). Pour y remédier, il suffit de compiler (bien entendu pas sur la machine compromise) les commandes en mode statique afin qu'elles n'en dépendent plus. Pour cela, utilisez l'option de compilation `-static` de gcc. L'exécutable résultant contiendra le code de toutes les fonctions utilisées, il ne chargera aucune bibliothèque au moment de son exécution.
- Modification des modules du noyau : si les modules du noyau sont modifiés, on considèrera que l'analyse à chaud ne peut pas apporter de résultat fiable et on passera directement, après sauvegarde, à la réinstallation complète.

Dans notre exemple, l'analyse à chaud dévoile quelques anomalies qui seront confirmées par la suite.

La commande `netstat -tupan` sur le système fait apparaître un service en écoute sur le port 15 000, invisible auparavant.

La commande `ps` modifiée nous cachait quelques processus, dont le programme : `/usr/sbin/nscd`, qui est ici une *backdoor* SSH en écoute sur le port 15 000. Grâce à cette porte dérobée, le pirate pouvait revenir se connecter

**Investigation Forensique**

Forensique, en anglais *forensic*, est synonyme de criminalistique. Une investigation forensique a pour objectif de prouver l'existence d'un crime et de déterminer l'identité de l'auteur ainsi que son mode opératoire.

L'analyse forensique d'une machine compromise est donc du ressort des autorités de police judiciaire plutôt que le travail courant d'un administrateur système ! Pour autant, il n'est pas inutile de connaître et d'avoir mis en œuvre les outils et méthodes d'une telle analyse, et ce pour deux raisons. D'une part, en cas de compromission grave, cela permettra d'éviter les fausses manipulations qui risqueraient d'avoir pour conséquence l'effacement de certaines traces du pirate… des traces qui seront indispensables si un dépôt de plainte est envisagé ! D'autre part, la connaissance du mode opératoire des pirates permet d'être mieux armés pour se protéger contre de futures attaques.

OUTILS **« rescue » et « live CD »**

Il est nécessaire de réamorcer le système afin de bénéficier, lors de l'exploration du contexte, d'un environnement logiciel de provenance sûre, autonome donc non dépendant des éléments installés et non exposé aux modifications intempestives de programmes déployés par le pirate. La disquette « rescue » produite durant l'installation exploite d'ordinaire les programmes placés sur le disque dur. On lui préférera donc les distributions de Linux disponibles sous forme « live CD », c'est-à-dire utilisables grâce à leur seul CD-Rom et sans installation. Certaines furent conçues et réalisées en fonction de cet objectif, d'autres sont si riches qu'elles intègrent cela.

sur notre machine de façon discrète. Les connexions du pirate sont chiffrées. Elles ne sont pas journalisées par le système ; le pirate n'est pas détectable par les commandes `who` ou `w`.

Enfin, la commande `ifconfig` indique que l'interface réseau est en mode `PROMISCUOUS`, ce qui laisse penser qu'un *sniffer* réseau a été installé sur la machine.

ATTENTION **nscd**

`nscd` est aussi le nom d'un démon tout à fait honorable (le Name Server Cache Daemon). La présence de `nscd` n'implique pas que la machine est piratée ! Notons que le risque de confusion est délibéré de la part du pirate.

## Sauvegarde du système compromis

Chaque partition est sauvée sur un autre système à l'aide des commandes `dd` pour le dump et `nc` (netcat) pour le transfert réseau :

```
machine-saine> nc -l -p 10101 > fich-hda1
machine-compromise> dd if=/dev/hda1 | nc machine-saine 10101
```

`nc` écoute sur le port 10101

BON SENS **Choix des noms de fichier**

Dans le cas où plusieurs machines sont compromises, faites apparaître le nom de la machine compromise dans le nom du fichier : par exemple `tamalo1-hda1` plutôt que `fich-hda1`.

## Analyse fine de l'image du disque piraté

L'analyse à froid du système sera faite en poursuivant différents objectifs :

1. Déterminer la date précise de la compromission initiale. La connaissance de celle-ci permettra un certain nombre de corrélations avec les fichiers de journalisation du routeur d'entrée et des machines du réseau.
2. Déterminer la faille exploitée pour prendre le contrôle du système. Il sera alors possible de mettre à jour le service correspondant.
3. Déterminer la nature des outils installés par le pirate et en identifier les fichiers de traces et les programmes afin de rechercher sur d'autres machines du site des signes éventuels de compromission.
4. Connaître la source de l'attaque afin de la contacter pour avoir des explications (attention : il est très probable que la machine attaquante soit elle-même sous le contrôle du pirate).
5. Déterminer jusqu'à quel point l'intrusion a réussi, savoir si les mots de passe du réseau ont pu être compromis.

OUTILS **Application client/serveur avec netcat**

Le logiciel netcat, fourni en standard avec Linux, permet de réaliser très simplement une application client/serveur.

Le serveur est lancé sur la machine `host1.tamalo.com` pour écouter sur le port `99999` avec la commande :

```
nc -l -p 99999
```

Le client est lancé sur la machine `host2.tamalo.com` pour se connecter sur `host1.tamalo.com:99999` avec la commande :

```
nc host1.tamalo.com 99999
```

Tout message envoyé sur l'entrée standard `<sdtin>` du client `nc` qui s'exécute sur `host1` – c'est-à-dire saisi au clavier de `host1` – apparaîtra sur la sortie standard `<stdout>` du serveur `nc` qui tourne sur `host2` – c'est-à-dire à l'écran de `host2`.

Cette commande est très utile pour analyser le fonctionnement de certaines applications serveurs, comme on le verra au chapitre 7 pour l'analyse du fonctionnement de FTP actif.

▸ http://netcat.sourceforge.net

### Montage pour l'analyse

Pour l'analyse, il reste à monter (en loopback) le système de fichiers concerné.

```
mount -o loop,ro,noexec,nodev fich-hda1 /root/
host_compromis_hda1
```

Il peut être utile d'utiliser l'option `ro` (read only) pour ne pas altérer les traces sur le système compromis. De plus, pour éviter d'exécuter par erreur des commandes sur la machine compromise, on utilisera l'option `noexec`. Enfin, on pourra ajouter l'option `nodev` pour ignorer les fichiers de type `device`, qui sont des points d'entrée vers les périphériques.

### Étude des fichiers de démarrage et configuration

Pour déceler les traces sur l'image du disque d'une machine piratée, le plus simple est de commencer par l'étude des fichiers de démarrage, très souvent modifiés par les pirates, afin de :

- masquer certaines traces en cas de redémarrage de la machine ;
- relancer un certain nombre de processus : backdoor, scanner, sniffer, à chaque redémarrage du système.

Sous Linux, il faut s'intéresser aux fichiers et aux répertoires suivants :

- `/etc/inittab`
- `/etc/init.d/`
- `/etc/rc.sysinit`
- `/etc/sysconfig/`
- `/etc/rc.d/`
- `/etc/inetd.conf` ou `/etc/xinetd.conf` et `/etc/xinetd.d/`
- `/etc/crontab`
- `/etc/cron.daily`, `/etc/cron.hourly`...

### Étude des fichiers créés lors du piratage

**Bon sens**

Aucune démarche de recherche n'est éternellement valide car les attaquants disposent d'outils de plus en plus évolués.

Il convient aussi de rechercher les fichiers créés le jour du piratage, à l'aide d'une simple commande `find`. Il faut préférer une recherche basée sur la date de création du fichier `CTIME`, qui n'est modifiée que par le noyau, plutôt que sur la date de modification `MTIME`. En effet, la date de modification peut-être altérée facilement par le pirate à l'aide de la commande `touch`.

## Analyse avec The Coroner toolkit

*The Coroner Toolkit*, ou TCT est une panoplie d'outils forensiques destinés à l'analyse d'une machine compromise. TCT fournit des outils très performants pour analyser une machine compromise. Dans ce qui suit, nous allons l'utiliser pour affiner notre analyse et retrouver certaines traces moins évidentes laissées par le pirate.

TCT appuie sa démarche de recherche sur le recoupement des événements temporels. Pour cela, il introduit la notion de *MAC time*, MAC étant l'acronyme de Modification Access Creation. En effet, la connaissance de ces trois attributs d'un fichier peut fournir des informations décisives sur l'acti-

vité du pirate. Par rapport à une simple commande `find`, TCT ajoute la détermination de l'*access time* qui est impossible en passant par les appels système standards. Pour que cette détermination soit possible, le système de fichiers doit avoir été sauvegardé par une copie des partitions, comme le permet `dd`, et non par une commande d'archivage ou de copie de fichiers qui altérerait l'*access time*.

La commande `grave-robber` capture les informations utiles dans l'image du système de fichiers et renseigne la base de données de TCT. Notez que cette même commande capture également les informations concernant les processus et les connexions réseau actives sur un système vivant.

```
grave-robber –c /host_compromis_hda1 –o LINUX2 –m -i
Le fichier /root/tct-1.15/data/tamalo1_01_23_17\:36\:37+0100/
body contient la base de données de TCT.
```

Il est possible de compléter les informations fournies par `grave-robber` avec des informations sur les fichiers effacés, grâce à la commande `fls` issue de la boîte à outils *sleuthkit*. Les formats étant compatibles, il suffit de rediriger la sortie de `fls` pour compléter la base de données de TCT comme indiqué ci-dessous :

```
fls –f linux-ext2 –r –m /host_compromis_hda1 fich-hda1 >> /
root/tct-1.15/data/tamalo1_01_23_17\:36\:37+0100/body
```

La commande `mactime` ci-dessous génère, à partir de la base de données de TCT, la liste chronologique des modifications du système de fichiers.

```
mactime –p /host_compromis_hda1/etc/passwd –g /
host_compromis_hda1/etc/group 1/1/1971 > mactime-tamalo1.out
-p indique le chemin du fichier passwd utilisé pour résoudre les
noms d'utilisateurs
-g indique le chemin du fichier de groupes
Sont considérés tous les événements postérieurs au 1/1/1971, on
n'en rejette donc aucun.
```

La figure 3-2 montre les répercussions sur le système de fichiers de l'activité du pirate pendant la configuration du rootkit t0rn (voir section suivante). On voit assez clairement le déroulement des opérations, qui commence par une lecture attentive de la documentation de SSHD (nul n'est parfait) ! Notez la présence des attributs `m`, `a`, `c`, ainsi que des références à des fichiers effacés marqués `(deleted)`. Dans ce cas précis, les références à ces fichiers ne sont pas d'une grande utilité car le pirate ne s'est pas donné la peine d'effacer ses programmes sources.

Dans certains cas au contraire, on pourra être très motivé pour récupérer un fichier effacé afin d'en analyser le fonctionnement, s'il s'agit par exemple du code source d'un exploit.

**Référence The Coroner Toolkit**

Les outils du Coroner toolkit sont disponibles à l'adresse http://www.porcupine.org/forensics/
Pour ceux qui veulent en savoir plus sur l'analyse forensique, le livre (en anglais) de Dan Farmer et Wietse Venema, *Forensic Discovery*, est disponible en libre téléchargement sur ce même site.

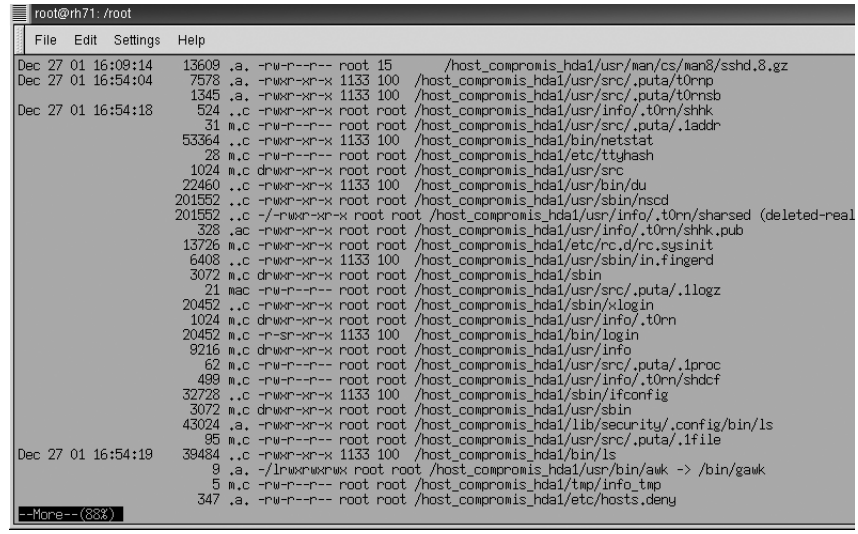



**Figure 3–2**
Fichiers lus et modifiés par le pirate au moment de la compromission

Sachez que TCT fournit la méthode et les outils nécessaires à une telle récupération. Pour cela, on s'appuiera sur le fait que le système d'exploitation incrémente linéairement les *inodes* des fichiers créés dans un même répertoire comme le montre la figure 3-3.

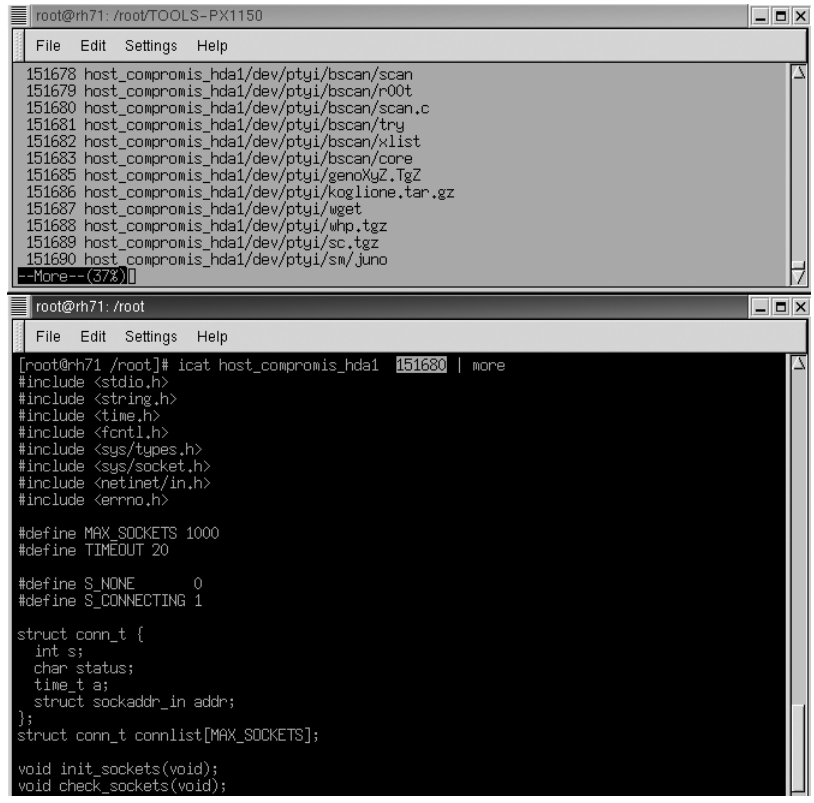



**Figure 3–3**
Recherche d'un fichier et visualisation à partir de son inode

Ainsi pour récupérer le code source d'un exploit, on recherchera des fichiers, toujours présents sur le disque, créés immédiatement avant et après le fichier perdu. Un fichier effacé sera caractérisé par un trou dans la séquence des inodes du répertoire. Si les blocs occupés par le fichier manquant n'ont pas été réaffectés, il sera possible de le visualiser. La figure 3-3 montre comment voir le contenu du fichier `scan.c` dont l'inode est 151 680, à l'aide de la commande `icat` fournie par TCT.

## Trousse à outils du pirate : le rootkit t0rn

Un rootkit est défini par l'Agence nationale de sécurité américaine (National Security Agency) comme une panoplie de logiciels utilisés par des pirates. Cette panoplie fournit des outils pour :

- capturer le trafic réseau et les mots de passe ;
- créer des portes dérobées (backdoors) dans le système ;
- collecter sur le réseau des informations sur d'autres systèmes (scanner) ;
- dissimuler que le système est compromis.

Dans notre exemple, le rootkit t0rn a été installé par le pirate. Il s'agit d'un classique du genre. À l'exception du scanner, il implémente toutes les fonctionnalités prévues par la définition.

Sur notre machine, nous avons trouvé deux répertoires utilisés par le rootkit : `/usr/src/.puta` et `/usr/info/.t0rn`.

### Sniffer réseau d'un rootkit

L'exécutable `/usr/src/.puta/t0rnp` est un sniffer réseau, c'est-à-dire un programme qui écoute le réseau dans le but de récolter les éventuels mots de passe qui transitent en clair. Il faut savoir que les applications que nous utilisons couramment, comme TELNET, FTP, IMAP ou HTTP, n'effectuent en général aucun chiffrement du mot de passe au moment où ce dernier est envoyé sur le réseau.

Des logiciels tels que tcpdump, disponibles en standard sous Linux, permettent de constater combien il est facile d'écouter sur le réseau. Notons aussi Ethereal et dsniff qui sont faciles à installer.

La figure 3-6 retrace les échanges de paquets au cours de la phase d'authentification dans une session FTP. Cet exemple est facile à reproduire avec un PC Linux. Il met en évidence le risque lié à l'utilisation des applications non chiffrées.

1. Lancer Ethereal à partir du compte `root`.
2. Sélectionner le menu *capture start* et indiquer `port ftp` dans la rubrique *filter* (voir figure 3-4).

**OUTILS dsniff, Ethereal et tcpdump**

Ces performants outils d'analyse rendent de grands services aux administrateurs réseau. Leur utilisation est très simple et constitue une aide importante pour comprendre le fonctionnement des applications client/serveur.

- dsniff : http://monkey.org/~dugsong/dsniff/
- ethereal : http://www.ethereal.com
- tcpdump : http://www.tcpdump.org

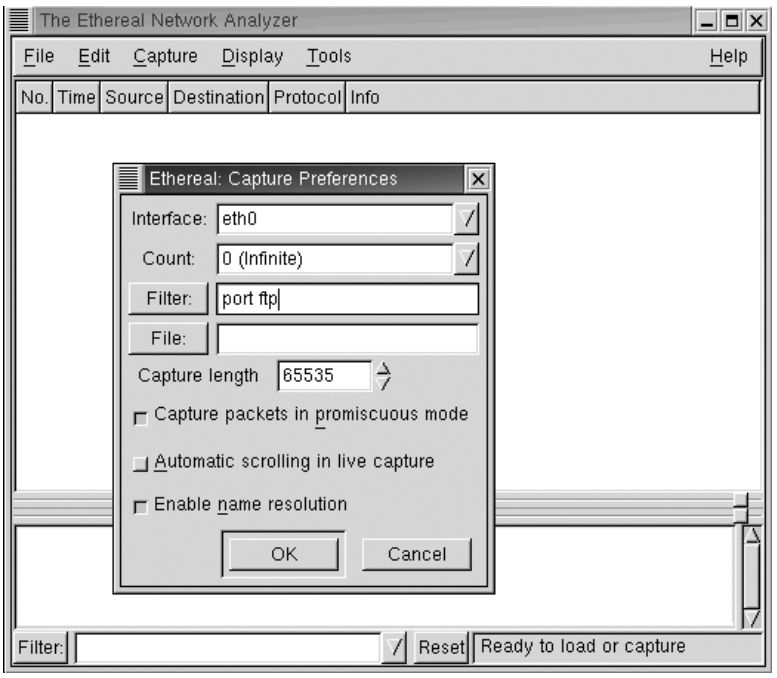



**Figure 3–4**
Lancement de Ethereal

Ethereal est démarré. Il écoute le réseau en ne conservant que les paquets correspondant au protocole FTP.

**3** Ouvrir une connexion FTP vers un serveur quelconque pour analyser le trafic correspondant, comme indiqué à la figure 3-5.


**Figure 3–5** Ouverture d'une connexion FTP

**OUTILS Sniffer et analyse réseau**

Une différence essentielle entre un sniffer et un outil d'analyse de réseau est que le premier est écrit dans l'unique but d'extraire des couples : identification/mot de passe, tandis que le second permet d'analyser l'ensemble du trafic qui circule sur la couche de transport sur laquelle la sonde est posée.

La figure 3-6 montre que les informations circulent en clair sur le réseau. Ainsi, le paquet numéro 13 contient le nom de l'utilisateur `bernard`, dont nous avons écouté la connexion, tandis que le paquet numéro 17 nous renseigne sur son mot de passe : `u1arpl7` !

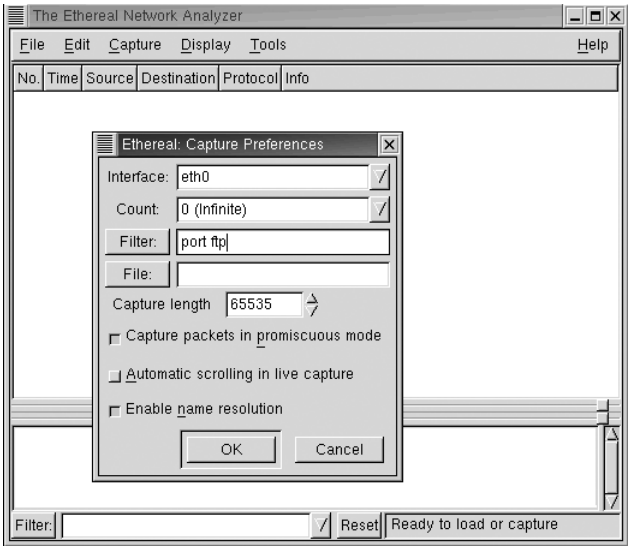



**Figure 3–6** Écoute d'une session FTP avec Ethereal

Afin d'écouter sur le réseau, le pirate doit faire passer la carte Ethernet en mode promiscuous. Sur une machine Linux, et sur les systèmes Unix en général, cela nécessite un accès privilégié (compte `root`).

## Le mode promiscuous

Pour comprendre ce qu'est le mode promiscuous, il est nécessaire de faire référence au modèle OSI.

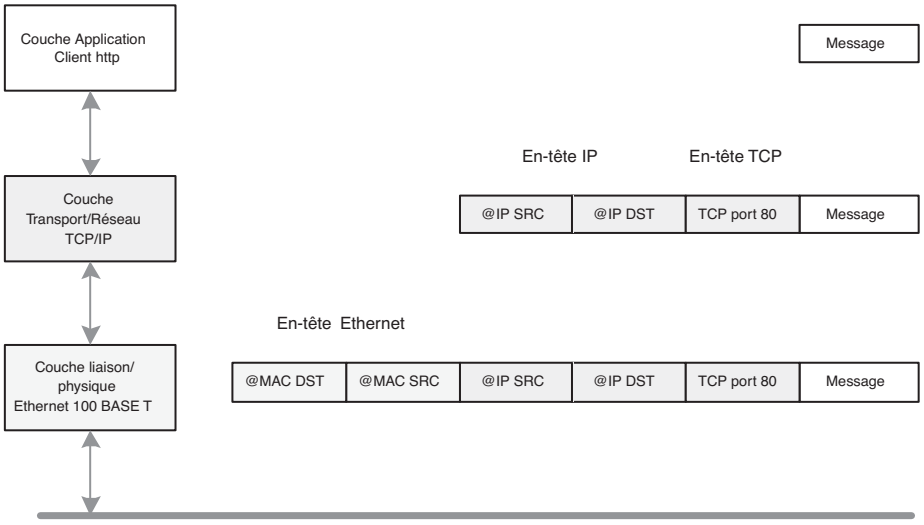



**Figure 3–7** Modèle OSI : encapsulation des messages

**RAPPEL Adresse MAC**

Une adresse MAC (Media Access Control) est constituée de 2 champs de 3 octets chacun :

`06:60:B0:59:DE:B3`

Les trois premiers octets constituent le champ fournisseur tandis que les trois autres constituent un numéro de série. Deux interfaces Ethernet ne peuvent pas avoir la même adresse MAC – une même machine pouvant avoir plusieurs interfaces.

Notez que l'adresse MAC de destination est placée au début de la trame, ce qui permet à la carte Ethernet de déterminer tout de suite si elle doit garder la trame ou non.

La figure 3-7 montre une trame Ethernet arrivant à destination d'une machine. Elle est traitée par les couches basses du pilote réseau : les couches 1 (physique) et 2 (liaison) du modèle OSI (Open Systems Interconnection). Ces couches sont généralement implémentées dans le microcode de la carte Ethernet. Les couches supérieures, 3 et suivantes, sont quant à elles implémentées dans le noyau de Linux.

Une fonction importante des couches basses est de vérifier si la trame Ethernet est destinée ou non à la machine considérée. Cette opération est effectuée en comparant l'adresse MAC de destination contenue dans la trame avec celle de l'interface. Si les adresses coïncident, la trame est déshabillée de son en-tête Ethernet et le paquet est reconstitué pour être transmis aux couches supérieures implémentées dans le noyau de Linux. Dans le cas contraire, il ne tient pas compte de la trame. Cela ne fait pas l'affaire des mécanismes d'écoute du réseau, quelles qu'en soient les motivations. La mise en mode promiscuous de la carte Ethernet remédie à ce problème en obligeant cette dernière à transmettre toutes les trames au noyau qui se chargera de faire le tri.

Sur le système compromis, le fichier `/usr/src/.puta/system` contient les couples « nom de compte – mot de passe » qui ont été enregistrés par le sniffer lors de l'écoute frauduleuse. L'examen de ce fichier montre que le sniffer a capturé l'identifiant et le mot de passe de deux comptes appartenant à Tamalo.com, sur les machines `dial025.mon-fai.com` et `www.diffusion-tamalo.com.it`, comme le montre la figure 3-8. Les deux connexions qui ont pu être sniffées sont des sessions FTP non chiffrées.

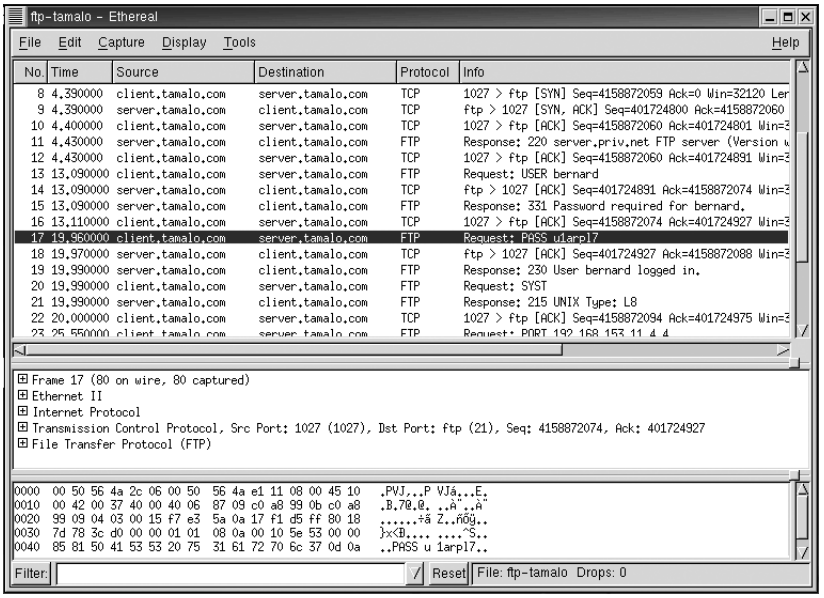



**Figure 3–8** Fichier de sortie du sniffer réseau

### Action

Quelques mesures doivent être mises en place sans délai :

1. Le changement des mots de passe interne et externe de tous les utilisateurs du réseau.
2. La vérification de l'historique de toutes les connexions sur des sites distants afin de savoir si des connexions frauduleuses ont eu lieu.
3. L'installation d'applications client/serveur mettant en œuvre du chiffrement pour se protéger des écoutes sur le réseau.

## Rootkit : effacer les traces et masquer la présence du pirate

Le programme `/usr/src/.puta/t0rnsb` est un nettoyeur de fichiers de journalisation (logs). Son rôle est d'effacer les traces de passage du pirate.

En effet, les services de Linux sont généralement conçus pour enregistrer par l'intermédiaire d'un processus appelé `syslogd` un certain nombre de traces dans des fichiers journaux, configurés grâce au contenu du fichier `/etc/syslogd.conf` (ou `/etc/syslog-ng/`). Le plus souvent, ces fichiers sont situés dans le répertoire `/var/log`. Par défaut, les deux fichiers les plus importants du point de vue de la sécurité sont `/var/log/messages` et `/var/log/secure`.

**Exemple de log**

```
Jan 12 17:21:26 gw sshd[14168]:
Accepted password for root from
192.168.40.176 port 1034 ssh2
```

Cette ligne de log est produite par le serveur sshd. Elle indique une connexion SSH depuis la machine dont l'adresse IP est `192.168.40.176` sur la machine `gw`. L'heure de la connexion et l'utilisateur, `root`, sont précisés.

Un autre type de trace est enregistré dans le fichier `/var/log/wtmp`. Ce fichier stocke sous forme binaire une trace de chaque connexion sur la machine considérée. Il est possible de visualiser ces connexions avec la commande `last`. Le rootkit fournit donc au pirate des outils pour faire disparaître les traces qui le concernent afin d'éviter que l'adresse de la machine à partir de laquelle il nous a attaqués n'apparaisse dans ces fichiers.

Les outils de nettoyage des logs sont plus ou moins évolués, se situant entre la mise à zéro pure et simple du fichier, pour les rootkits primitifs, et la suppression des lignes concernant la période de présence du pirate pour les plus évolués.

Dans certains cas, l'observation des fichiers de log, même nettoyés par le rootkit, fournira des informations précieuses à l'administrateur de la machine. Par exemple, l'absence totale de logs pendant une période donnée nous indique que le pirate était probablement connecté pendant ce créneau. Si nous disposons des logs du routeur d'entrée pour cette période, ils seront riches d'informations.

**À RETENIR**

Il faut bien comprendre que tous les programmes, même développés localement, s'ils sont « linkés » dynamiquement, dissimuleront tout ce qui relève du piratage en cours (fichiers…) si le pirate est allé jusqu'à instrumenter la libC.

Le fichier `/usr/src/.puta/.1file` contient la liste des fichiers cachés à l'utilisateur de la machine par les commandes `ls` et `find` modifiées. Il con-

tient en particulier les fichiers du rootkit lui-même : les répertoires `.puta` et `.t0rn`, les fichiers `.1file`, `.1addr`...

Le fichier `/usr/src/.puta/.1addr` contient le début des adresses IP cachées à l'utilisateur de la machine par la commande `netstat` modifiée. Seul le début de l'adresse est donné (`192.168` par exemple) pour que la découverte de ce fichier ne trahisse pas le nom de la machine originaire de l'attaque.

Le fichier `/usr/src/.puta/.1proc` contient la liste des processus cachés à l'utilisateur de la machine par la commande `ps` modifiée. Le sniffer t0rnp est dans la liste, ainsi que la porte dérobée : `nscd`.

Le fichier `/usr/src/.puta/.1logz` contient la liste des adresses IP filtrées par le rootkit et qui n'apparaîtront pas dans les logs.

## Rootkit : la porte dérobée (backdoor)

**RAPPEL Porte dérobée (backdoor)**

Une porte dérobée est un programme qui ménage un accès privilégié, discret et direct à celui qui sait l'employer.
De nombreux ports sont connus pour être utilisés comme portes dérobées. Certains pirates, plus fainéants que les autres, effectuent directement un *scan* de ces ports espérant y trouver une *backdoor* ouverte par un autre !
Le site http://ports.tantalo.net/index.php donne une liste des utilisations des ports, officielles ou comme portes dérobées.

Les rootkits permettent généralement au pirate d'ouvrir une porte dérobée qui écoute sur un port de son choix, supérieur à 1 024 la plupart du temps.

Dans le cas de t0rn, la porte dérobée est constituée par un serveur sshd qui écoute sur le port 15 000. Le démon `ssh` est appelé `/usr/sbin/nscd` (prétendument *Name Server Cache Daemon*).

Notez que la connexion de l'attaquant est chiffrée, ce qui lui évite d'être lui-même sniffé par ses propres outils ou par tout autre outil d'analyse réseau !

Les fichiers de configuration de ce service sont dans le répertoire `/usr/info/.t0rn` :

- `/usr/info/.t0rn/shhk.pub` contient la clé publique du serveur sshd.
- `/usr/info/.t0rn/shhk` contient la clé privée du serveur sshd.
- `/usr/info/.t0rn/shdcf` est le fichier de configuration de sshd. On y découvre qu'il est lancé sur le port 15 000.

En cas de redémarrage du système, ce « `nscd` » est relancé par le script `/etc/rc.sysinit`.

Le processus `nscd` est caché à l'exécution de `ps` grâce au fichier `/usr/src/.puta/.1proc`.

## Rootkit t0rn : conclusion

Une analyse rapide du rootkit`t0rn` montre combien la découverte des fichiers de configuration de ce dernier peut être précieuse pour nous. Par exemple, en recoupant les plages d'adresses IP cachées avec les logs des routeurs d'entrée, nous sommes à même de déterminer l'adresse IP de la machine qui nous a attaqués.

Pour cette raison, des rootkits plus évolués fournissent parfois des outils de chiffrement de leurs propres fichiers de configuration. Il existe par exemple des rootkits possédant un fichier de configuration unique chiffré par un « ou

exclusif » de chaque octet avec 255. Heureusement, le décryptage de ces fichiers constitue un défi qui motive de nombreux amateurs, et l'algorithme de chiffrement de ces fichiers ne tarde jamais à être diffusé sur Internet.

Encore une fois, le fait que de nombreux rootkits soient identifiés et leur fonctionnement bien connu ne dispense en aucun cas du reformatage du système de fichiers ni de la réinstallation complète d'une machine compromise.

## Détecter la compromission à partir des logs

Depuis quelques semaines, nous avions mis en place chez Tamalo.com une centralisation systématique des logs des machines Linux vers une machine de collecte n'offrant aucun autre service à l'extérieur. Cette centralisation va nous aider à retrouver les logs qui ont étés effacés par le rootkit sur notre serveur.

**Copie de log retrouvée sur la machine de collecte : une attaque en deux phases**

```
Dec 26 19:02:22 Tamalo1 inetd[158]: printer[5336] from 192.168.20.29 1623 (1)
Dec 26 19:02:22 Tamalo2 inetd[175]: printer[5227] from 192.168.20.29 1627
Dec 26 19:03:55 Tamalo1 SERVER[2320]: Dispatch_input: bad request line (2)
'BBÜóÿ¿Ýóÿ¿Þóÿ¿ßóÿ¿XXXXXXXXXXXXXXXXXX0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000480000000
00001073835088security0000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000006????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????
?????????????1Û1É1À°FÍ??å1Ò²f?Ð1É?ÈC?]øC?]ôK?Mü?MôÍ?1É?EôCf?]ìfÇEî^O'?Mð?Eì?EøÆEü^P?Ð?MôÍ??ÐCCÍ??ÐC
Í??Ã1É²??ÐÍ??ÐAÍ?ë^X^?u^H1À^F^G?E^L°^K?ó?M^H?U^LÍ?èãÿÿÿ/bin/sh'
```

L'analyse de la copie des logs sur la machine de collecte met clairement en évidence les deux étapes de l'attaque. Dans un premier temps, à 19:02:22 (1), un scan horizontal de notre réseau sur le port d'impression 515 identifie les machines qui présentent une faille. Dans un deuxième temps, à 19:03:55 (2), cette faille est exploitée sur Tamalo1. L'enchaînement entre le scan et l'exploit est extrêmement rapide (1 minute 30), ce qui suppose que le pirate a utilisé un script qui lance automatiquement l'opération en fonction du résultat du scan.

Il apparaît que nous avons été la victime d'une attaque sur le service d'impression `lprng`. Remarquez dans la ligne de log précédente la taille importante de l'argument fourni à `lpr`, ainsi que la présence de la chaîne de caractères `/bin/sh` à l'intérieur de cet argument.

Cet argument est passé par `lprng` au `syslogd` par l'intermédiaire de la fonction `use_syslog()`. Cette dernière présente une faille : elle utilise l'argument reçu par le service pour déterminer le format de la chaîne de caractères à transmettre. Un format inattendu contenant un appel à `/bin/sh` sera donc exécuté par le service `lprng` autorisant le pirate à exécuter le code de son choix.

Cette vulnérabilité du service d'impression `lprng` de Linux était parfaitement décrite dans un avis de sécurité de la société Red Hat qui nous était parvenu quelques temps auparavant.

**Avis de sécurité de Red Hat sur la vulnérabilité du service lprng**

```
---------------------------------------------------------------------
-----
Red Hat, Inc. Security Adviso ry
Synopsis: LPRng contains a critical string format bug
Advisory ID: RHSA-2000:065-04
Issue date: 2000-09-26
Updated on: 2000-10-04
Product: Red Hat Linux
Keywords: LPRng security lpd printing lpr syslog
Cross references: N/A
---------------------------------------------------------------------
-----
1. Topic:
LPRng has a string format bug in the use_syslog function which
could
lead to root compromise.

2. Relevant releases/architectures:
Red Hat Linux 7.0 - i386
3. Problem description:
LPRng has a string format bug in the use_syslog function. This
function returns user input in a string that is passed to the
syslog()
function as the format string. It is possible to corrupt the
print
daemon's execution with unexpected format specifiers, thus
gaining root
access to the computer. The vulnerability is theoretically
exploitable
both locally and remotely.
```

## Origine de l'attaque

Une négligence du pirate donnera de façon non ambiguë l'adresse de la machine à partir de laquelle il nous a attaqués. Dans le répertoire `/dev/ptyi` utilisé par le pirate pour déposer quelques outils, nous avons découvert un fichier `core`.

Une simple commande `strings` appliquée à ce fichier extrait l'ensemble des chaînes de caractères contenues dans la mémoire. Elle nous dévoile l'environnement complet dans lequel travaillait le pirate au moment de l'incident !

**B.A.-BA Fichier core**

Un fichier `core` est créé lorsque le noyau Linux interrompt sans sommation le déroulement d'un processus tentant de commettre une action interdite, par exemple accéder à une portion de la mémoire ne lui appartenant pas. Ce fichier est une image de la mémoire occupée par le processus au moment du problème. Un fichier `core` peut être ouvert avec un débogueur afin de connaître l'endroit exact du plantage, ainsi que l'environnement complet du programme au moment de l'incident.

**Chaînes de caractères extraites du fichier core**

```
HOME=/root
USER=root
LOGNAME=root
PATH=/usr/sbin:/sbin:/usr/bin:/bin:/usr/X11R6/bin
MAIL=/var/spool/mail/root
SHELL=/bin/tcsh
SSH_CLIENT=192.168.16.58 1029 15000
SSH_TTY=/dev/pts/2 TERM=xterm HOSTTYPE=i386-linux VENDOR=intel
OSTYPE=linux MACHTYPE=i386
```

Pour des raisons de confidentialité, les deux premiers octets de l'adresse source de l'attaque ont été remplacés par `192.168`.

La variable `SSH_CLIENT` indique très clairement que la machine dont l'adresse IP est `192.168.16.58` était connectée sur le port 15 000 de notre serveur, ce qui correspond à la porte dérobée.

Une interrogation des bases *whois* détermine rapidement la provenance de l'attaque.

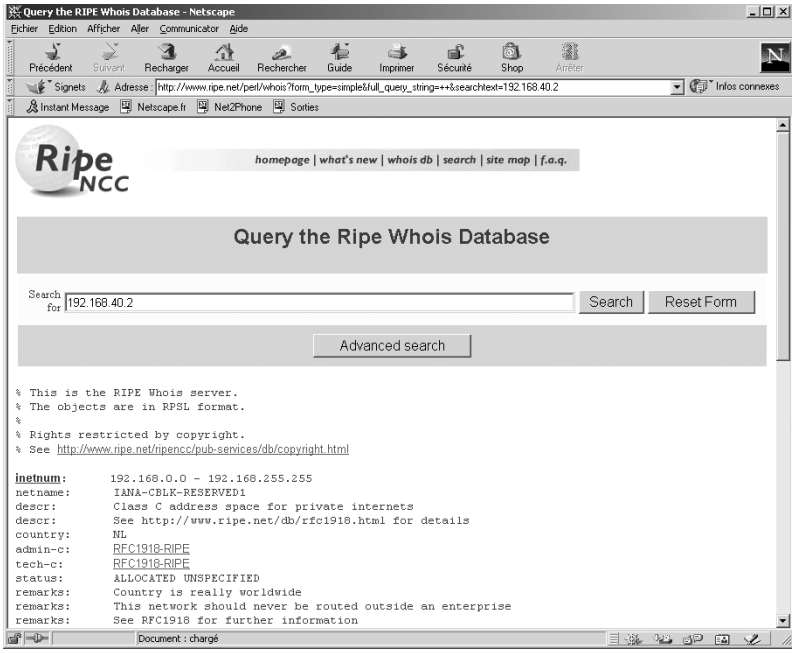



**Figure 3–9** Les bases whois : Ripe

L'organisation qui gère l'adresse de notre pirate n'étant pas localisée en France, nous décidons de contacter notre CERT afin qu'il transmette nos récriminations à son homologue.

En parallèle, nous tentons une protestation par courrier électronique à l'adresse `abuse` du réseau source de l'attaque, ainsi qu'avec le contact technique indiqué dans la base whois. Nous obtenons très rapidement une

**ORGANISMES Les bases Whois**

Les bases whois déterminent à quel organisme a été affecté un domaine IP. Elles fournissent les coordonnées du responsable fonctionnel des adresses attribuées et de la personne à contacter en cas de problème. Ces bases sont au nombre de trois, RIPE pour l'Europe et l'Afrique, ARIN pour les États-Unis et APNIC pour l'Asie. Elles peuvent être interrogées à partir de leur site Web.

- http://www.ripe.net/perl/whois
- http://www.arin.net/whois/index.html
- http://www.apnic.net/

réponse à notre courrier, l'administrateur de la machine concernée nous indiquant qu'il venait de découvrir que sa machine était également compromise.

## En résumé…

Les attaques des systèmes informatiques sont de plus en plus automatisées. Leur scénario est assez reproductible : découverte d'une faille dans un service, publication d'un « exploit », scan réseau et tentative de compromission.

Les pirates utilisent des panoplies d'outils qui cachent leur présence, capturent les mots de passe circulant sur le réseau, installent des portes dérobées ou enfin scannent un autre réseau.

L'analyse d'une machine compromise fait apparaître les outils mis en œuvre par le pirate. Elle révèle comment le réseau a été pénétré et si d'autres machines présentent les mêmes failles. Elle permet souvent d'identifier l'origine de l'attaque, mais rarement de remonter jusqu'au pirate qui, en général, se protège par de nombreux rebonds.

Pour se protéger contre ces attaques, deux types d'actions seront décrits dans les chapitres qui suivent : le recours à des applications client/serveur mettant en œuvre du chiffrement pour interdire l'écoute réseau, le filtrage des services vulnérables par la mise en place de pare-feu et la segmentation du réseau.

**ORGANISMES Les CERT : Computer Emergency Resource Team**

Un CERT est une organisation qui travaille sur les problèmes de sécurité informatique pour une communauté donnée. En France, il y en a quatre. Le plus ancien est le CERT Renater. Il concerne la communauté université-recherche. Chaque CERT dispose de moyens techniques et humains propres. Dans certaines affaires, les CERT peuvent travailler en relation avec les autorités judiciaires.

Au niveau mondial, les CERT sont en relation entre eux par le biais d'un forum appelé FIRST (Forum of Incident Response and Security Team). Les CERT échangent ainsi des informations sur les failles nouvelles et les incidents de sécurité courants.

Les CERT effectuent une veille technologique par rapport aux failles des logiciels pouvant donner lieu à une attaque. Ils diffusent des avis de sécurité à leurs correspondants et les avertissent par des messages d'alerte lorsque certaines attaques prennent des proportions très importantes.

- http://www.cert.org
- http://www.certa.ssi.gouv.fr

**CONVENTION L'adresse abuse**

Il est recommandé à l'administrateur d'un domaine nommé `nom.de.domaine` de créer l'adresse abuse électronique correspondante (`abuse@nom.de.domaine`) qui est redirigée vers la sienne.

Une personne qui aurait à se plaindre d'un comportement anormal d'une des machines de `nom.de.domaine` pourrait ainsi le signaler à l'administrateur dudit domaine par l'envoi d'un simple courrier électronique.

L'adresse abuse s'avère également utile pour l'administrateur du réseau concerné. Par exemple, c'est grâce à cette adresse qu'il sera informé en cas de problème avec des machines de son domaine.