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.