

Cahiers

de

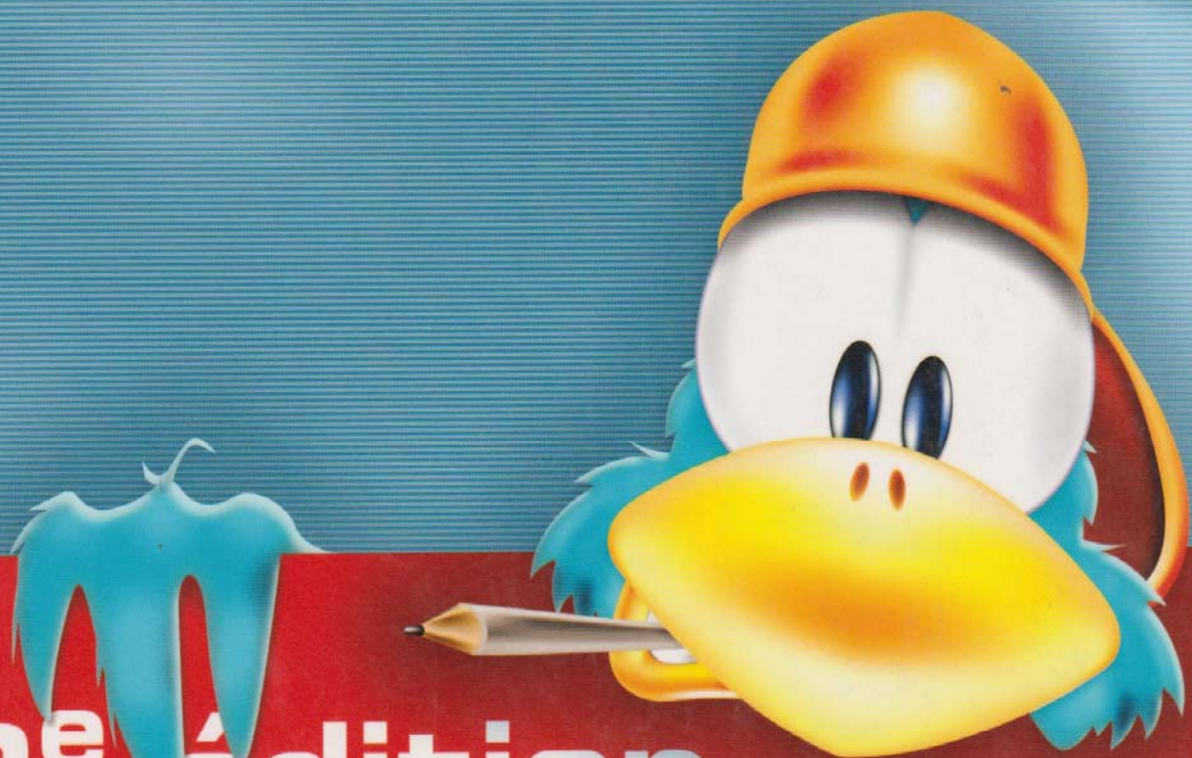
l'Admin

Collection dirigée par **Nat Makarévitch**

Sécuriser un réseau **Linux**

Bernard Bouterin

Benoit Delaunay



2^e édition

EYROLLES

2005 - 522.1

2-005-522-1

Bernard Bouterin

Benoit Delaunay

**Cahiers
de
l'Admin**

**Sécuriser un réseau
Linux**

2^e édition

Collection dirigée par Nat **Makarévitch**

Avec la contribution de Jean-Marie **Thomas**

EYROLLES

Table des matières

AVANT-PROPOS	V
1. LA SÉCURITÉ ET LE SYSTÈME LINUX	1
Enjeux et objectifs de sécurité 2	
La menace 2	
Principaux facteurs de motivation des pirates 3	
Risques liés au type de connexion 3	
Risques liés aux failles des systèmes 4	
Émergence des systèmes Linux 4	
Linux et la sécurité 5	
Des distributions Linux sécurisées 5	
En résumé... 6	
2. L'ÉTUDE DE CAS : UN RÉSEAU À SÉCURISER	7
Une jeune entreprise 8	
Les besoins de la société en termes de services 8	
Les choix techniques initiaux de Tamalo.com 9	
Web et services associés 10	
Transfert de fichiers 10	
Base de données 10	
Résolution de noms 10	
Messagerie électronique 11	
Partage de fichiers 11	
Impression réseau 11	
L'infrastructure informatique vieillissante et vulnérable 11	
La compromission du site 12	
Mise en évidence des vulnérabilités 13	
La refonte du système informatique 13	
Le projet d'une nouvelle infrastructure réseau 14	
Études des flux réseau 16	
Vers des outils de communication sécurisés 16	
Un suivi et une gestion quotidienne du système d'information 18	
En résumé... 18	
3. ATTAQUES ET COMPROMISSIONS DES MACHINES	19
Kiddies, warez et rebonds 20	
Scénario de l'attaque du réseau de Tamalo.com 22	
Une faille dans le système 22	
L'exploitation de la faille (« exploit ») 22	
Utilité des scans réseau 22	
La compromission 23	
Analyse de la machine compromise 24	
Traces visibles sur le système avant réinitialisation 24	
Sauvegarde du système compromis 25	
Analyse fine de l'image du disque piraté 25	
Montage pour l'analyse 25	
Étude des fichiers de démarrage et configuration 26	
Étude des fichiers créés lors du piratage 26	
Trousse à outils du pirate : le rootkit t0rn 26	
Sniffer réseau d'un rootkit 27	
Le mode PROMISCUOUS 29	
Rootkit : effacer les traces et masquer la présence du pirate 30	
Rootkit : la porte dérobée (backdoor) 31	
Rootkit t0rn : conclusion 32	
Détecer la compromission à partir des logs 32	
Origine de l'attaque 34	
En résumé... 35	
4. CHIFFREMENT DES COMMUNICATIONS AVEC SSH ET SSL 37	
Les quatre objectifs du chiffrement 38	
Authentification 38	
Intégrité 39	
Confidentialité 39	
Signature électronique 39	
Facteurs de fiabilité des techniques de chiffrement 39	
Algorithmes de chiffrement symétrique et asymétrique 40	
Chiffrement symétrique 40	
Chiffrement asymétrique 41	
Le protocole SSL (Secure Socket Layer) 43	
Qu'est ce que SSL ? 43	
SSL, comment ça marche ? 43	
Les certificats X.509 44	
Authentification et établissement de la connexion SSL 45	
Utilisation de SSL par les applications client/serveur 46	
Le protocole SSH (Secure Shell) 46	
Qu'est-ce que SSH ? 46	
À quels besoins répond SSH ? 46	
Caractéristiques d'OpenSSH 48	
Installation d'OpenSSH 49	
Fichiers de configuration d'OpenSSH 50	
Activation et lancement du serveur SSH 50	
Désactivation et arrêt du serveur SSH 51	
Utilisation de SSH 51	
Connexion interactive 51	

Exécution de commandes à distance 51	
Copie distante de fichiers ou de répertoires 52	
Transfert interactif de fichiers 52	
Options des commandes SSH 52	
Authentification avec SSH 52	
Configuration du service SSH 52	
Authentification par mot de passe 53	
Authentification à clé publique 53	
Relais d'affichage X11 54	
Gestion des accès au service SSH 55	
Dépannage 55	
L'alternative VPN 56	
En résumé... 56	
5. SÉCURISATION DES SYSTÈMES 57	
Installation automatisée 58	
Mise à jour régulière des systèmes 61	
Mise à jour et installation optimale avec APT 62	
Mise à jour avec Red Hat Network 62	
L'indispensable protection par mot de passe au démarrage 62	
Mise en configuration minimale, limitation des services actifs 63	
Identification des processus 64	
Identification des ports réseau utilisés 64	
Identification des services actifs 65	
Désactivation des services inutiles 66	
Sécurisation du système de fichiers 67	
Permissions des fichiers 67	
Détection des fichiers dotés de droits trop permissifs 68	
Droits suid et sgid 68	
Alternative à la protection suid : sudo 69	
Options de montage des systèmes de fichiers 70	
Gestion des accès et stratégie locale de sécurité 70	
Compte privilégié root 70	
Blocage des comptes inutiles 71	
Filtrage réseau avec TCP Wrapper 71	
Configuration des services système cron et syslog 72	
cron 72	
syslog 72	
Configuration sécurisée de la pile TCP/IP 73	
Ignorer certains messages ICMP 73	
ICMP Redirect 73	
ICMP Echo request 75	
ICMP Ignore Bogus Response 75	
Interdiction du source routing 75	
Surveillance des martiens ! 76	
Protection contre les attaques IP spoofing et SYN flooding 76	
Configuration en pare-feu avec IPtables 77	
Extension du noyau 77	
Serveur d'affichage X11 et postes de travail 77	
En résumé... 79	
6. SÉCURISATION DES SERVICES RÉSEAU : DNS, WEB ET MAIL 81	
Bases de la sécurisation des services réseau 82	
Service de résolution de noms DNS 82	
Comment ça marche ? 83	
Serveurs de noms et sécurité 84	
Installation du logiciel BIND 85	
Configuration des serveurs DNS 86	
Compte non privilégié 86	
Changement de la racine du système de fichiers avec « chroot » 86	
Activation et lancement du serveur 91	
Configuration des clients DNS 91	
Messagerie électronique 92	
Comment ça marche ? 92	
Les logiciels de transfert de courrier 93	
Messagerie électronique et sécurité 93	
SPAM et relais ouvert 94	
L'architecture du système de messagerie 94	
Installation de sendmail 96	
Activation de sendmail 96	
Configuration de sendmail 97	
Installation d'IMAP 101	
Configuration et activation du serveur IMAPS 102	
Serveur Web 103	
Serveur Web et sécurité 103	
Installation de HTTPD 103	
Configuration et activation de HTTPD 104	
En résumé... 104	
7. FILTRAGE EN ENTRÉE DE SITE 105	
But poursuivi 106	
Principes de base du filtrage en entrée de site 106	
Filtrage sans état 107	
Adresses IP source et destination 107	
Protocole, ports source et destination 107	
Drapeaux TCP et filtrage en entrée 109	
Les limites du filtrage sans état 110	
Filtrage avec états 111	
Politique de filtrage : avant la compromission, « tout ouvert sauf » 112	
Politique de filtrage : du « tout ouvert sauf » au « tout fermé sauf » 113	
Déploiement de service FTP avec (et malgré) les filtres 114	
Filtrage d'un client FTP actif 115	
Filtrage d'un serveur FTP destiné à fonctionner en mode actif 118	
Filtrage d'un client FTP passif 118	
Filtrage du serveur FTP passif, limitation du serveur à une plage de ports 118	
En résumé... 119	

8. TOPOLOGIE, SEGMENTATION ET DMZ	121	9. SURVEILLANCE ET AUDIT	151
Pourquoi cloisonner ? 122		Des traces partout 152	
Définition des zones du réseau de Tamalo.com 123		Linux et le syslog 152	
Définition des flux à l'extérieur et à l'intérieur du réseau de Tamalo.com 123		Empreinte des machines : Tripwire 154	
Postes de travail 123		Métrologie réseau avec MRTG 155	
Serveurs applicatifs internes 123		Installation et configuration de MRTG chez Tamalo.com 157	
Serveurs accessibles depuis l'extérieur et l'intérieur : DMZ 123		Configuration SNMP du firewall A pour accepter les requêtes MRTG 157	
Topologie du réseau 124		Installation et configuration de MRTG sur la machine d'analyse 158	
Topologie à un seul pare-feu 124		NMAP 159	
Topologie à double pare-feu adoptée pour le réseau de Tamalo.com 125		Audit réseau avec Nessus 159	
Détails de la configuration réseau de Tamalo.com 126		Configuration de Nessus 160	
DMZ 126		Rapport d'audit 162	
Services internes 128		Détection d'intrusion : Snort 163	
Postes de travail 128		Mise en place de la sonde Snort 163	
Comment segmenter ? Les VLAN et leurs limites 128		Configuration et validation de Snort, détection des scans 163	
VLAN par port physique 128		Le pot de miel 165	
VLAN par adresse MAC 129		Tableau de bord de la sécurité 166	
Configuration VLAN retenue pour Tamalo.com 130		Les indicateurs de sécurité 166	
Proxy et NAT 131		Synthèses des indicateurs dans un tableau de bord 168	
Proxy 131		En résumé... 168	
Traduction d'adresses NAT 133		A. INFRASTRUCTURE À GESTION DE CLÉS : CRÉATION DE L'AUTORITÉ DE CERTIFICATION DE TAMALO.COM	169
Source NAT – un pour un – ou NAT statique 134		OpenSSL et les IGC 170	
Source NAT -N pour M – ou NAT dynamique 136		Création des certificats X.509 170	
Proxy versus NAT 139		Bi-clés RSA 170	
Netfilter/IPtables 139		Certificat X.509 autosigné de l'autorité de certification 171	
Fonctionnalités d'IPtables 139		Demande de certificats utilisateurs 173	
Tables et chaînes 139		Signature des certificats par l'autorité de certification 173	
Écriture des règles 141		Création d'un fichier contenant la clé privée et le certificat au format PKCS12 174	
Suivi de connexion 141		Mise en œuvre d'un serveur Web sécurisé HTTPS 175	
Journalisation 141		Création du certificat du serveur www.tamalo.com 175	
Traduction d'adresses – NAT 142		Installation de la chaîne de certification sur le client 176	
Filtrage 142		Installation d'un certificat personnel dans le navigateur 178	
Configuration IPtables des deux pare-feux Linux 143		Utilisation des certificats pour signer et/ou chiffrer les courriers électroniques 179	
Configuration IPtables de chaque poste de travail 145		En conclusion 181	
Configuration IPtables du serveur SMTP 146		INDEX	183
Sécurité du réseau sans fil 146			
Risque d'accès frauduleux au réseau 146			
Le protocole 802.1X 147			
Risque d'écoute du réseau 149			
En résumé... 149			