

INTERNET

SÉCURITÉ & FIREWALLS

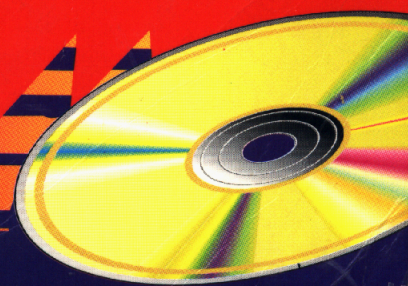
Karanjit Siyan & Chris Hare

- Mesurez les risques encourus lors d'une connexion Internet et appréhendez les différentes méthodes de sécurité
- Évaluez, à travers différents exemples, les besoins adaptés à chaque cas de figure
- Découvrez les outils et produits existants, leurs avantages et leurs failles
- Construisez votre propre firewall

BIBLIOTHÈQUE DU CERT

En cadeau !

Un CD-ROM contenant un logiciel de démonstration de divers firewalls, des codes source et des outils dédiés aux administrateurs réseau

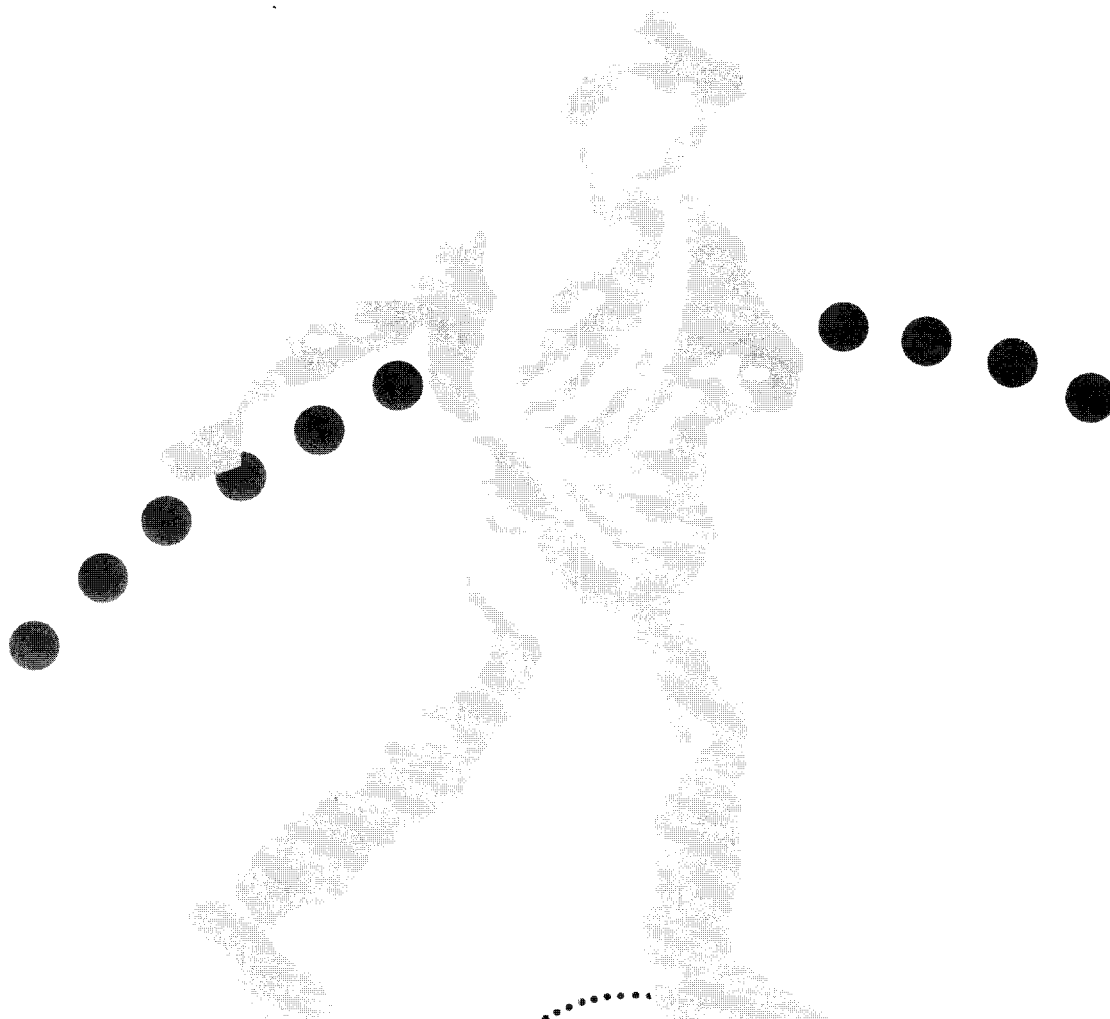


LEMACMILLAN

INTERNET SECURITE & FIREWALLS

187 2485

BIBLIOTHEQUE DU CERIST



S&SM

Simon & Schuster Macmillan (France) a apporté le plus grand soin à la réalisation de ce livre afin de vous fournir une information complète et fiable. Cependant, Simon & Schuster Macmillan (France) n'assume de responsabilités, ni pour son utilisation, ni pour les contrefaçons de brevets ou atteintes aux droits de tierces personnes qui pourraient résulter de cette utilisation.

Simon & Schuster Macmillan (France) ne pourra en aucun cas être tenu pour responsable des préjudices ou dommages de quelque nature que ce soit pouvant résulter de l'utilisation de ces exemples ou programmes.

Tous les noms de produits ou autres marques cités dans ce livre sont des marques déposées par leurs propriétaires respectifs.

Publié par Simon & Schuster Macmillan
(France)
19, rue Michel Le Comte
75003 PARIS
Tél : 01 44 54 51 10
Mise en page : Andassa

ISBN : 2-7440-0196-1

Copyright © 1996
Simon & Schuster Macmillan (France)
Tous droits réservés

Titre original :
Internet Firewalls and Network Sécurité
Second edition
Traduit de l'américain par : Veronique Campillo

ISBN original : 1-56205-632-8

Copyright © 1996 New Riders Publishing
Tous droits réservés
Que est une marque de Macmillan
Computer Publishing SA
201 West 103rd street
Indianapolis, Indiana 46290. USA

Toute reproduction, même partielle, par quelque procédé que ce soit, est interdite sans autorisation préalable. Une copie par xérogaphie, photographie, film, support magnétique ou autre, constitue une contrefaçon passible des peines prévues par la loi, du 11 mars 1957 et du 3 juillet 1995, sur la protection des droits d'auteur.

LEMACMILLAN

INTERNET SECURITE & FIREWALLS

BIBLIOTHEQUE DU CERIST



Chris Hare.
Karanjit Siyan

S&SM

Introduction

1

LA SÉCURITÉ DES RÉSEAUX

- | | | |
|----------|---|------------|
| 1 | <i>Comprendre TCP/IP</i> | 5 |
| 2 | <i>Sécurité</i> | 57 |
| 3 | <i>Concevoir une politique de réseaux</i> | 93 |
| 4 | <i>Mots de passe à usage unique et authentification</i> | 157 |

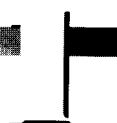
ROUTEURS FILTRES ET FIREWALLS

- | | | |
|-----------|--|------------|
| 5 | <i>Introduction aux routeurs filtres</i> | 201 |
| 6 | <i>Filtres de paquets</i> | 237 |
| 7 | <i>Filtrage de paquets sur PC</i> | 283 |
| 8 | <i>Architecture et théorie des firewalls</i> | 325 |
| 9 | <i>Produits firewalls</i> | 359 |
| 10 | <i>Le kit d'outils firewalls TIS</i> | 427 |
| 11 | <i>Black Hole</i> | 505 |

ANNEXES

- | | | |
|----------|--|------------|
| A | <i>Sources d'information</i> | 549 |
| B | <i>Pages de manuel d'Opie et LogDaemon</i> | 555 |

Introduction



LA SÉCURITÉ DES RÉSEAUX

A qui s'adresse ce livre ?	1
Comment ce livre peut vous aider	1
Conventions utilisées dans cet ouvrage.....	2
Notes, astuces, etc.....	3
1 Comprendre TCP/IP	7
Historique de TCP/IP	7
Adresses, sous-réseaux et noms d'hôtes.....	9
Classes d'adresses.....	9
Sous-réseaux	11
Adresses sans classe et CIDR.....	15
Noms d'hôtes	16
Travailler avec des interfaces réseau.....	17
Configurer avec ifconfig	19
Examen des fichiers de configuration du réseau.....	21
Le fichier /etc/hosts	21
Le fichier /etc/ethers	22
Le fichier /etc/networks.....	22
Le fichier etc/protocols	23
Le fichier etc/services	23
Le fichier etc/inetd.conf	24
Comprendre les fichiers d'accès au réseau	25
Le fichier /etc/hosts.equiv	25
Le fichier .rhosts	25
Equivalences utilisateur/hôte.....	26
Examen des daemons TCP/IP.....	27
Le daemon slink.....	28
Le daemon ldsocket.....	28
Le daemon cpd.....	28

Le daemon Line Printer (lpd)	25
Le daemon SNMP (snmpd)	25
Le daemon RARP (rarpd)	29
Le daemon BOOTP (bootpd)	29
Le daemon route (routed)	29
Le daemon Domain Name Server (named)	30
Le daemon System Logger (syslogd)	31
Le daemon Inetd — Le super-serveur	31
Le daemon RWHO (rwhod)	31
A la découverte des utilitaires de TCP/IP	31
Commandes administratives	32
Les commandes User	15
Résumé	55
2 Sécurité	57
Examen des niveaux de sécurité	57
Niveau D1	57
Niveau C1	57
Niveau C2	57
Niveau B1	59
Niveau B2	59
Niveau B3	59
Niveau A	60
La sécurité au Canada	60
Niveau EAL-1	60
Niveau EAL-2	61
Niveau EAL-3	61
Niveau EAL-4	61
Niveau EAL-5	61
Niveau EAL-6	62
Niveau EAL-7	62
Examen des questions de sécurité locale	62
Politiques de sécurité	62
Le fichier password	63
Le fichier Shadow Password	65
Le fichier Dialup Password	65
Le fichier Group	68
Obsolescence et contrôle du mot de passe	69

Vandales et mots de passe	72
Comment les vandales déchiffrent-ils les mots de passe ?	73
Sécurité de niveau C2 et TCB	74
Comprendre les équivalences réseau	77
Equivalence hôte	77
Equivalence utilisateur	79
Définir des utilisateurs et des groupes	81
Comprendre les permissions	81
Examen des permissions standard	81
Root et NFS	84
Explorer les méthodes cryptographiques	84
Comment sont codés les mots de passe	84
Coder les fichiers	86
L'authentification Kerberos	88
Comprendre Kerberos	88
Inconvénients de Kerberos	89
Comprendre IP Spoofing	89
Résumé	90
Exemple de programme	90
3 Concevoir une politique de réseaux	93
Planifier la sécurité des réseaux	93
Politique de sécurité du site	94
Approche de la politique de sécurité	95
Mise en place des responsabilités	96
Analyse des risques	98
Identification des ressources	101
Identification des menaces	102
Définir les accès non autorisés	102
Risque de divulgation de l'information	103
Refus de service	103
Utilisation du réseau et responsabilités	104
Identification des personnes autorisées	105

La bonne utilisation d'une ressource	105
Qui est autorisé à accorder les accès et à approuver les utilisations ?	107
Définir les responsabilités de l'utilisateur	111
Définir les responsabilités de l'administrateur du système	112
Les informations sensibles	113
Plan d'action en cas de violation de la politique de sécurité	114
Réagir aux infractions	114
Réagir aux infractions commises par les utilisateurs locaux	115
Stratégies de réponse	115
Etre un bon citoyen de l'Internet	119
Responsabilités et contacts avec les organismes externes	119
Interpréter et diffuser la politique de sécurité	120
Identification et prévention des problèmes de sécurité	121
Points d'accès	122
Systèmes mal configurés	124
Bogues logiciels	124
Menaces internes	125
Sécurité matérielle	125
Confidentialité	126
Mise en place d'un contrôle rentable de la politique	127
Choix d'une politique de contrôle	127
Les stratégies de repli	128
Détection et contrôle d'une activité non autorisée	128
Contrôle des utilisations du système	128
Contrôle des mécanismes	129
Contrôle de votre emploi du temps	130
Procédures de comptes-rendus	131
Procédures de gestion des comptes	131
Procédures de gestion des configurations	133
Procédures de restauration	134
Procédures de comptes-rendus pour les administrateurs de système	137
Protection des connexions du réseau	137
Cryptographie et protection du réseau	138
Codage DES : standard de cryptographie des données	139
Crypt	140
PEM : Privacy Enhanced Mail	140

Pretty Good Privacy.....	111
Authentifier l'origine	141
Intégrité des informations.....	112
Utiliser les checksums.....	112
Checksums cryptographiques.....	143
Systèmes d'authentification	111
Cartes à puce.....	111
Kerberos	145
Mise à jour technologique	145
Mailing lists.....	145
Unix Security Mailing Lists	146
Risks Forum List.....	147
La liste VIRUS-L.....	147
La liste Bugtraq.....	148
Computer Underground Digest	148
La mailing list du CERT.....	149
La mailing list CERT-TOOLS.....	149
La mailing list TCP/IP.....	150
La mailing list SUN-NETS	150
Groupes de news	151
Equipes d'intervention de la sécurité.....	151
Computer Emergency Response Team	152
Le Security Coordination Center du DDN.....	153
Computer Security Resource and Response Clearinghouse (NIST)	153
Computer Incident Advisory Capability (DOE)	154
Ames Computer Network Security Response Team (NASA).....	155
❶ Mots de passe à usage unique et authentification	157
Qu'est-ce que OTP ?	158
Historique d'OTP.....	160
Mise en œuvre d'OTP.....	161
Choisir la version d'OTP	163
Comment fonctionnent S/KEY et OPIE	164
Bellcore S/KEY version 1.0	165



OPIE	166
Se procurer le code source d'OPIE.....	166
Compiler le code OPIE.....	168
Tester les programmes compilés.....	170
Installation d'OPIE	175
Composants OPIE	178
LogDaemon 5.0	182
Comment se procurer le code de LogDaemon	183
Compiler le code LogDaemon.....	184
Tester les programmes compilés.....	186
Installer LogDaemon.....	188
Les composants de LogDaemon	188
Calculateurs S/KEY et OPIE	190
Unix	190
Macintosh	191
Microsoft Windows	192
Calculateurs externes	192
Mise en pratique d'OTP	193
Remarques sur la sécurité concernant /bin/login	195
OTP et X Windows	196
Obtenir d'autres informations	196

**ROUTEURS FILTRES ET FIREWALLS**

5 <i>Introduction aux routeurs filtres</i>	201
Définitions	201
Zones de risque	201
Modèle de référence OSI et routeurs filtres.....	203
Les couches du modèle OSI.....	204
Routeurs filtres et firewalls par rapport au modèle OSI.....	224
Comprendre le filtrage de paquets	225
Filtrage de paquets et politique de réseau.....	225
Un modèle simple de filtrage de paquets.....	226
Fonctionnement du filtre de paquets	227
Concevoir un filtre de paquets.....	229
Règles de filtrage de paquets et associations complètes.....	234

6	<i>Filtres de paquets</i>	237
	Mise en œuvre des règles de filtrage de paquets.....	237
	Définir les listes d'accès	238
	Utiliser les listes d'accès standard.....	238
	Utiliser les listes d'accès étendu	240
	Filtrer les appels entrants et sortants sur terminal	243
	Emplacement du filtre de paquets et falsification d'adresses.....	244
	Placer le filtre de paquets.....	244
	Filtrer sur les ports d'entrée et de sortie.....	246
	Filtrage de paquets et protocole.....	248
	Filtrer le trafic FTP.....	249
	Filtrer le trafic TELNET	269
	Filtrer les sessions X-Windows.....	270
	Filtrage de paquets et protocole de transport UDP.....	271
	Filtrer les paquets ICMP	273
	Filtrer les paquets RIP	274
	Exemples de configurations de routeurs filtres	275
	Etude de cas 1	275
	Etude de cas 2.....	277
	Etude de cas 3.....	279
7	<i>Filtrage de paquets sur PC</i>	283
	Filtrer les paquets sur PC.....	283
	Le filtre de paquets KarlBridge	283
	Le filtre de paquets Drawbridge	304
	Résumé	323
8	<i>Architecture et théorie des firewalls</i>	325
	Examen des composants d'un firewall.....	326
	L'hôte DAS.....	327
	L'hôte bastion	337
	Sous-réseaux filtrés.....	351
	Passerelles d'application.....	353

9	<i>Produits firewalls</i>	359
	TCP Wrapper	359
	Exemple 1.....	361
	Exemple 2.....	361
	Exemple 3.....	361
	Exemple 4.....	361
	La passerelle FireWall-1.....	362
	Matériel nécessaire à la construction de FireWall-1	362
	Architecture de FireWall-1.....	363
	Afficheur d'enregistrements.....	376
	Exemples d'applications FireWall-1.....	378
	Efficacité de FireWall-1.....	380
	Langage des règles de FireWall-1.....	381
	Se procurer des informations sur FireWall-1	383
	ANS InterLock.....	383
	Ressources requises par InterLock	385
	Fonctionnalités d'InterLock	386
	Configurer InterLock	387
	Base de données des règles	390
	Services proxy de la passerelle d'applications InterLock	392
	S'informer sur ANS InterLock	400
	Gauntlet de Trusted Information Systems.....	401
	Exemples de configurations de Gauntlet.....	402
	Configurer Gauntlet.....	401
	Le firewall Gauntlet du point de vue de l'utilisateur.....	407
	Firewall Toolkit de TIS	410
	Construire le Firewall Toolkit.....	410
	Configurer le bastion en service minimum	413
	Installer les composants du Toolkit.....	411
	La table de permissions réseau	418
10	<i>Le kit d'outils firewalls TIS</i>	427
	Comprendre TIS	427
	Se procurer TIS.....	427
	Compiler sous SunOS 4.1.3 et 4.1.4.....	428
	Compiler sous BSDI.....	429



Modifications au niveau du code	129
Installer TIS	130
Se préparer à la configuration	131
Configurer TCP/IP	136
IP Forwarding	136
La netperm-table	137
Configurer netacl	140
Se connecter avec netacl	142
Redémarrer inetd	144
Configurer le proxy telnet	144
Se connecter à travers le proxy telnet	147
Règles d'accès au niveau hôte	148
Vérifier le proxy Telnet	149
Configurer la passerelle rlogin	150
Se connecter avec le proxy rlogin	152
Règles d'accès hôte	153
Vérifier le proxy rlogin	154
Configurer la passerelle FTP	154
Règles d'accès hôte	156
Vérifier le proxy FTP	157
Se connecter à travers le proxy FTP	158
Autoriser FTP avec netacl	159
Configurer le proxy Sendmail smap et smapd	160
Installer le client smap	160
Configurer le client smap	161
Installer l'application smapd	162
Configurer l'application smapd	163
Configurer DNS pour smap	165
Configurer le proxy HTTP	166
Clients HTTP non connus du proxy	168
Clients HTTP connus du proxy	168
Règles d'accès hôte	169
Configurer le proxy X Windows	172
Le serveur d'authentification	173

Base de données d'authentification	175
Ajouter des utilisateurs.....	177
L'interpréteur d'authentification authmgr	181
Gestion de la base de données.....	182
Pratiquer l'authentification	184
Utiliser plug-gw pour d'autres services	185
Configurer plug-gw.....	186
plug-gw et NNTP.....	187
plug-gw et POP.....	190
Les outils administratifs compagnons	192
portscan	192
netscan.....	193
Outils de compte rendu.....	194
Le rapport du serveur d'authentification.....	196
Le rapport de refus de service	198
Rapport d'utilisation de FTP	199
Rapport d'utilisation de HTTP.....	500
Le rapport de netacl.....	500
Rapport d'utilisation du courrier électronique.....	501
Rapport d'utilisation de telnet et rlogin.....	502
Trouver de l'aide.....	504
11 Black Hole	505
Comprendre Black Hole	506
Configuration matérielle.....	508
Modules fixes de Black Hole	509
Modules d'extension de Black Hole.....	512
Concevoir un réseau avec Black Hole	513
Garder la politique de sécurité à l'esprit.....	515
Utiliser l'interface Black Hole	515
Comprendre la base de données stratégique	518
Résolution de la politique et des règles.....	523
Règles, utilisateurs et services.....	524
Règles.....	524
Utilisateurs et maintenance des utilisateurs.....	525
Configurer Black Hole.....	531
Configurer un DNS interne et externe.....	532



Configurer les services applicatifs.....	534
Générer des rapports.....	541
Pour plus d'informations.....	545
Résumé.....	545



ANNEXES

A Sources d'information **549**

Outils.....	549
Tcpwrapper et Portmapper.....	550
Kit Firewall.....	550
Bellcore S/KEY.....	550
OPIE (One-Time Passwords In Everything).....	550
Swatch Logfile Monitor.....	551
Tcpdump.....	551
TAMU Tiger.....	551
COPS.....	551
Crack.....	552
SATAN.....	552
Passwd+.....	552
npasswd.....	552
Tripwire.....	553
Localiser des constructeurs de firewalls sur l'Internet.....	553
Mailing lists des firewalls et de la sécurité.....	553
Firewall.....	554
Sécurité.....	554

B Pages de manuel d'OPIE et LogDaemon **555**

Pages de manuel OPIE.....	555
OPIEFTPD.....	555
OPIEKEY.....	559
OPIEPASSWD.....	560
OPIEINFO.....	562
OPIELOGIN.....	563

OPIESU	561
Pages de manuel de LogDaemon	565
FTPD	565
KEY	570
KEYINFO	570
KEYINIT	571
REXECD	572
RLOGIND	571
RSHD	576
SKEY.ACCESS	578
SKEYSH	571
SU	571
TELNETD	573