

SÉCURITÉ ET PERFORMANCES DES SYSTÈMES UNIX

Richard Stoeckel



EYROLLES

2-005-16-1

2-005-16-1

SÉCURITÉ ET PERFORMANCES DES SYSTÈMES UNIX

Richard STOECKEL

Table des matières

Sécurité et performances des systèmes UNIX

Chapitre 1	1
Les bases de la sécurité des ordinateurs	1
Généralités et anecdotes	1
Les faits	1
Les risques effectifs	3
L'intérêt de la sécurité	5
Les organismes de standardisation	5
Le contrôle d'accès	7
Les différents types d'accès	7
L'accès au système et la protection des mots de passe	7
L'accès aux informations	11
La faune de la jungle	15
Les virus	15
Les chevaux de Troie	16
Les vers	17

II Sécurité et performances des systèmes UNIX

Le passage secret	17
Les bombes	17
Les bactéries	17
Règles élémentaires de sécurité	18
La sécurité des locaux	18
La protection physique	19
Les cartes d'accès	19
Les frontières biométriques	20
La sécurité physique	21
Les conditions météorologiques	21
Le feu et la pollution	21
L'électricité	22
L'eau	22
La foudre	22
Les vibrations	23
Gestion de base du système	23
La mise en application de la sécurité	23
L'analyse du risque	24
Le personnel et la sécurité	24
La politique de sauvegarde	25
Le Livre Orange	27
Les concepts de sécurité	27
Les différentes classes du livre orange	30
La codification et le cryptage	33
Définition	33
Normalisation : le DES	36
Algorithmes	36
Les problèmes liés aux communications	37
Principes et règles de sécurité	38
Topologie des réseaux	39
Modems, réseaux et supports	41
Le modèle OSI	45

Chapitre 2	49
Accès au système	49
Unix et la sécurité	49
Les identificateurs de login	50
Les mots de passe	52
Le cryptage des mots de passe	53
La gestion des mots de passe	53
Verrouillage du login	54
Durée de vie d'un mot de passe	55
Commandes utiles	57
Les utilisateurs	58
Les utilisateurs usuels	59
Les groupes	60
Les groupes usuels	61
Le super-utilisateur	62
Les droits du super-utilisateur	63
Mesure de protection des utilisateurs	63
Les points d'entrée sans mot de passe	64
Les points d'entrée inutilisés	66
Les terminaux sécurisés	68
Chapitre 3	69
Système de fichiers et sécurité des données	69
Organisation d'un système de fichiers	69
Les inodes	71
Les blocs de données	72
Contrôle d'intégrité	72
Autres systèmes de fichiers	74
Le système de fichiers de Unix System V	74
Le type bfs	74
Le Fast Filesystem de la version BSD	75
Système de fichiers en mémoire virtuelle : tmpfs	75
Loopback virtual file system : lofs	75
Système de fichiers au format DOS : pcfs	75
High Sierra File System : hdfs	75
Remote File System : rfs	76

IV Sécurité et performances des systèmes UNIX

Network File System : nfs	76
Fichiers et permissions	76
Différents droits	80
Modification des droits	83
Droits lors de la création	84
Les droits des répertoires	85
Droits d'accès particuliers : SUID, SGID et Sticky bit	87
Les fichiers spéciaux	92
Modification du propriétaire : la commande chown	94
Modification du groupe : la commande chgrp	94
Les sauvegardes	95
Nécessité des sauvegardes	95
Les différents types de sauvegardes	96
La gestion des sources avec SCCS	97
Les supports de sauvegardes	99
Commandes élémentaires	100
La commande tar	100
La commande cpio	100
Exemples	101
La commande dd	102
La commande mt	103
Les commandes de sauvegarde complète	104
La commande backup de System VR3	104
La commande dump de BSD	105
Le service de sauvegarde de System VR4	108
La restauration des sauvegardes	110
Restauration sur System VR3	110
Restauration sur Unix BSD	111
Le service de restauration de System VR4	114
Recherche des intrus et mesures de protection	114
Copies de référence	115
Liste de contrôle, find et diff	119

Chapitre 4	121
Communications et sécurité	121
Liaisons et modems	121
Les modems	121
La sécurité et les modems	124
Le réseau Transpac	126
La sécurité et TRANSPAC	127
UUCP	128
Les commandes du système uucp	128
Requêtes de transfert	128
Réception de fichiers	129
La commande uucp	129
La télé-exécution	131
Le cheminement dans le réseau : uusend	132
Mode de fonctionnement du système UUCP	132
Les problèmes de sécurité	134
Réseaux locaux	136
Le modèle IEEE pour les réseaux locaux	136
Ethernet	138
La méthode CSMA/CD	139
La méthode du jeton et Token Ring	139
Ethernet et TCP/IP	140
Les adresses INTERNET et ETHERNET	141
Le protocole de résolution des adresses : ARP	143
Le protocole IP	143
Le protocole UDP	143
Le protocole TCP	143
Clients et serveurs	144
Le programme inetd	147
Les services offerts	148
Exemple de X-Window	148
X-Window et la sécurité	155
Connexions	156
rlogin	156
telnet	158
Exécution à distance avec rsh	159

VI Sécurité et performances des systèmes UNIX

Le courrier	160
Le programme finger	160
Le transfert de fichiers	161
rcp	161
ftp	162
tftp	166
Network Information Services	167
Le serveur maître	167
Le serveur esclave	168
Le client	168
Le fichier /etc/netgroup	169
Network File System : NFS	170
Le fichier /etc/exports	172
La commande mount	173
Le système RPC	174
Mode de fonctionnement	174
Secure RPC	176
Secure NFS	178
Outils de gestion Ethernet et NFS	179
ifconfig	179
arp	180
ping	181
spray	182
etherfind	183
netstat	185
nfsstat	189
Chapitre 5	191
Trace et comptabilité	191
Les fichiers de suivi	192
Le fichier /usr/adm/lastlog	192
Le fichier /usr/adm/wtmp	193
La commande last	195
Le système syslog sur Unix BSD	196
La comptabilité	199
La comptabilité sur Unix BSD	200
Initialisation du système comptable	200

La commande sa	200
La commande ac	203
La commande lastcomm	204
La comptabilité sur Unix System V	206
Les commandes de base	206
La commande sar	211
Exemples d'utilisation de la commande sar	213
La commande timex	215
Chapitre 6	219
La gestion des atteintes à la sécurité	219
La découverte de l'intrusion	220
La restauration du système	223
Les fichiers à surveiller	226
Les fichiers appartenant à root	226
Les fichiers SUID et SGID	227
Les fichiers liés à cron et at	228
Les fichiers uuwp	229
Résumé sur la sécurité	230
Les utilisateurs	230
Les fichiers	231
Le réseau	232
Pour terminer	232
Chapitre 7	233
Les performances	233
Généralités	233
La CPU	234
La mémoire	235
Les entrées-sorties	235
Le réseau	236
Le point de vue du développeur	236
Le temps d'exécution	237
La taille des programmes	238
L'analyse des performances	239
La commande prof	239
La commande GPROF	240

VIII Sécurité et performances des systèmes UNIX

Mesure de l'activité du système	241
La commande uptime	241
La commande iostat	242
La commande ps	244
La commande pstat	249
La commande vmstat	251
Le perfmeter de SUNOS	253
La commande sar	255
La commande sa	257
Les états comptables et la commande prdaily	258
Les commandes netstat et nfsstat	258
Analyse du trafic réseau sur SUNVIEW	260
Automatisation des tâches	261
Les travaux différés	261
Le système cron	263
Règles d'action	264
 Chapitre 8	 265
La charge de la CPU et le kernel	265
Régulation et priorité des travaux	265
La commande nice sur Unix System V	266
La fonction nice du C-shell Unix System V	268
La commande nice de Unix System V	268
La commande nice sur Unix BSD	269
La fonction nice du C-shell	269
La commande nice de Unix BSD	271
La modification de priorité avec renice	271
La limitation des ressources	273
Les travaux différés	274
La commande at	274
La commande batch	278
Informations des utilisateurs	279
Elimination des processus superflus	281
La mesure de la CPU	282
La table des processus	284
La table des inodes	284
La table des fichiers	285

La table des textes	285
La configuration du système	285
La construction d'un noyau BSD	289
La construction d'un noyau Unix System V	293
Règles d'action	295
Chapitre 9	297
La mémoire	297
La mémoire nécessaire	298
Unix BSD	299
Unix System V	301
Etat courant de la mémoire	301
Unix BSD	302
Unix System V	303
Techniques de gestion	306
Le sticky bit	306
Programmation et bibliothèques partagées	306
Fixation de limites	311
Le buffer cache	312
Réglage des paramètres de pagination et swapping	313
Ajouter de l'espace de swap	314
Règles d'action	316
Chapitre 10	317
Le système d'entrées/sorties	317
Les outils de base	318
La mesure de l'espace disponible	318
La mesure de l'occupation	319
Etat de l'espace utilisé	320
Recherche des fichiers inutiles	320
Analyse du contenu d'un fichier	322
La compression des données	322
Gérer la taille des fichiers de trace	325
Fabrication d'un système de fichiers et réglage	325
Système de fichiers	325
La commande mkfs	327
Les arguments de mkfs	328

X Sécurité et performances des systèmes UNIX

La commande newfs sur Unix BSD	329
Réglage et fragmentation	330
Système de fichier pcfs	331
Contrôle de cohérence d'un système de fichiers	332
Les répertoires lost+found	332
Synchronisation	333
La commande fsck	333
Analyse de la charge d'entrées/sortie	336
La commande limit	339
Le système des quotas	339
Règles d'action	341
 Chapitre 11	 343
 Le réseau	 343
Les outils de communication	345
Les outils de détection et de mesure	347
ping	348
spray	350
netstat	351
etherfind	356
nfsstat	356
Les processus daemons	359
Règles d'action	360
 Bibliographie	 361
 Index	 363