

Table des matières

Crédits.....	ix
Préface	xi
Chapitre 1. Sécurité d'une machine Unix.....	1
1. Points de montage sécurisés	1
2. Rechercher les programmes SUID et SGID	3
3. Rechercher des répertoires modifiables par tout le monde et par un groupe	4
4. Créer des hiérarchies d'autorisations souples avec les ACL POSIX	5
5. Protéger les journaux des trifouillages	8
6. Déléguer des rôles d'administration	10
7. Automatiser la vérification de la signature cryptographique	12
8. Rechercher les services en écoute	14
9. Empêcher la liaison des services à une interface	16
10. Restreindre les services avec des environnements isolés	17
11. Utiliser proftpd avec une source d'authentification MySQL	21
12. Empêcher les attaques par corruption de pile	23
13. Verrouiller le noyau avec grsecurity	25
14. Restreindre des applications avec grsecurity	29
15. Restreindre les appels système avec systrace	31
16. Automatiser la création des stratégies systrace	35
17. Contrôler les ouvertures de session avec PAM	37
18. Interpréteurs de commandes restreints	41
19. Forcer des limites de ressources sur un utilisateur et un groupe	43
20. Mises à jour automatiques du système	44

Chapitre 2. Sécurité d'une machine Windows	47
21. Vérifier l'application des correctifs sur des serveurs	47
22. Obtenir la liste des fichiers ouverts et des processus propriétaires	52
23. Lister les services en exécution et les ports ouverts	54
24. Activer l'audit	55
25. Sécuriser les journaux d'événements	57
26. Modifier la taille maximale des journaux	57
27. Désactiver les partages par défaut	59
28. Chiffrer le dossier temporaire	60
29. Effacer le fichier de pagination à l'arrêt	61
30. Restreindre les applications disponibles aux utilisateurs	63
Chapitre 3. Sécurité du réseau	67
31. Détecter une mystification ARP	68
32. Créer une table ARP statique	70
33. Pare-feu avec Netfilter	72
34. Pare-feu avec PacketFilter d'OpenBSD	75
35. Créer une passerelle authentifiée	81
36. Pare-feu sous Windows	83
37. Contrôler les débordements du réseau	87
38. Tester le pare-feu	88
39. Filtrage MAC avec Netfilter	91
40. Bloquer l'identification du système d'exploitation	92
41. Duper les logiciels de détection à distance du système d'exploitation	95
42. Établir un inventaire du réseau	99
43. Rechercher les vulnérabilités de votre réseau	101
44. Synchroniser les horloges des serveurs	107
45. Créer sa propre autorité de certification	109
46. Distribuer l'autorité de certification aux clients	112
47. Chiffrer IMAP et POP avec SSL	114
48. Mettre en place SMTP avec support de TLS	115
49. Détecter à distance les renifleurs Ethernet	118
50. Installer SSL et suEXEC pour Apache	122
51. Sécuriser BIND	126
52. Sécuriser MySQL	128
53. Partager des fichiers de façon sécurisée sous Unix	131

Chapitre 4. Journalisation	135
54. Exécuter un serveur syslog central	135
55. Piloter syslog	137
56. Intégrer Windows à l'infrastructure syslog	139
57. Résumer automatiquement les journaux	145
58. Surveiller automatiquement les journaux	147
59. Réunir des journaux provenant de sites distants	150
60. Journaliser l'activité d'un utilisateur avec la comptabilité de processus	155
Chapitre 5. Surveillance et tendance.....	157
61. Surveiller la disponibilité	158
62. Mettre en graphique les tendances	165
63. Exécuter ntop pour des statistiques en temps réel	167
64. Auditer le trafic à réseau	170
65. Collecter des statistiques avec des règles de pare-feu	172
66. Renifler Ethernet à distance	173
Chapitre 6. Tunnels sécurisés	177
67. Mettre en place IPsec sous Linux	177
68. Mettre en place IPsec sous FreeBSD	180
69. Mettre en place IPsec sous OpenBSD	183
70. Créer un tunnel PPTP	184
71. Chiffrement opportuniste avec FreeS/WAN	188
72. Rediriger et chiffrer le trafic avec SSH	190
73. Ouvrir rapidement des sessions avec des clés de clients SSH	192
74. Proxy Squid au-dessus de SSH	194
75. Utiliser SSH sur un proxy SOCKS	196
76. Chiffrer et faire passer dans un tunnel le trafic avec SSL	198
77. Connexions par tunnel dans HTTP	201
78. Tunnel avec VTun et SSH	202
79. Générer automatiquement vtund.conf	207
80. Créer un VPN inter-plates-formes	212
81. Tunnel PPP	217
Chapitre 7. Détection d'intrusion réseau	221
82. Détecter des intrusions avec Snort	222
83. Conserver une trace des alertes	226

84. Supervision en temps réel	228
85. Gérer un réseau de sondes	235
86. Écrire ses propres règles Snort	241
87. Prévenir et contenir des intrusions avec Snort_inline	244
88. Automatiser le pare-feu dynamique avec SnortSam	247
89. Détecter un comportement anormal	251
90. Mettre automatiquement à jour des règles Snort	252
91. Créer un réseau de sondes furtives	253
92. Utiliser Snort dans des environnements exigeants avec Barnyard	254
93. Détecter et empêcher les intrusions dans les applications web	257
94. Simuler un réseau d'hôtes vulnérables	261
95. Enregistrer l'activité d'un pot de miel	265
Chapitre 8. Reprise et réponse	267
96. Créer une image d'un système de fichiers	267
97. Vérifier l'intégrité des fichiers et trouver ceux qui sont compromis	269
98. Trouver les paquetages compromis avec RPM	273
99. Rechercher les root Kits	275
100. Déterminer le propriétaire d'un réseau	276
Index	281
