

s o l u t i o n s
r é s e a u x



Tableaux de bord
de la **sécurité**
réseau

CÉDRIC LLORENS

LAURENT LEVIER

EYROLLES

2-005-675-1
solutions
réseaux



2-005-675-1

Remerciements

CÉDRIC LLORENS

LAURENT LEVIER

Tableaux de bord
de la **sécurité**
réseau

avec la contribution de

OLIVIER SALVATORI



EYROLLES

Table des matières

Remerciements.....	V
Avant-propos	VII

PREMIÈRE PARTIE

Les attaques.....	1
-------------------	---

CHAPITRE 1

Les attaques réseau.....	3
Faiblesses des protocoles réseau	5
Attaque permettant d'établir la cartographie du réseau	6
Attaque permettant d'identifier les systèmes réseau (scanning)	7
Attaque permettant d'écouter le trafic réseau (sniffing)	8
Attaque sur la fragmentation des paquets IP	9
Attaque sur les commutateurs réseau.....	11
Attaque par déni de service (DoS)	11
Attaque par déni de service distribué (DDoS)	12
Faiblesses d'authentification	16
Attaque ARP spoofing	16
Attaque IP spoofing	17
Attaque man-in-the-middle	18
Attaque de déchiffrement et de pénétration des systèmes par mots de passe.....	24
Faiblesses d'implémentation, ou bogues	25
Attaque TCP SYN	25
Attaque sur les bogues des piles IP/TCP	28
Attaque sur les bogues des systèmes d'exploitation	29

Faiblesses de configuration	30
Exploitation d'erreurs de configuration du système.....	30
Politique d'accès ou de mots de passe trop laxiste.....	31
Autres formes d'attaques	31
En résumé	32

CHAPITRE 2

Les attaques réseau indirectes	33
Attaque par virus	33
Cycle de vie d'un virus informatique.....	34
Les différents types de virus.....	36
Les technologies antivirus	41
Attaque par relais	42
Attaque par bombes logiques.....	43
Attaque par vers	43
Attaque visant la saturation des systèmes relais.....	43
Grandes tendances des attaques 2002 (CERT)	44
En résumé	45

PARTIE II

Conduire une politique de sécurité réseau	47
--	----

CHAPITRE 3

Définir une politique de sécurité réseau	49
Objectifs d'une politique de sécurité réseau	50
Position des organismes officiels	50
Définir une analyse de risque	52
Principes génériques d'une politique de sécurité réseau	53
Niveaux d'une politique de sécurité réseau	58
Les différents types de politiques de sécurité.....	59
Guides et règles associés à la politique de sécurité réseau	60
Organisation et management	60
Ressources humaines	61

Gestion de projet	61
Gestion des accès logiques	62
Exploitation et administration	63
Sécurité physique	63
Plan de contingence	64
Vérification de l'application d'une politique de sécurité	64
En résumé	65

CHAPITRE 4

Stratégies de sécurité réseau	67
Méthodologie pour élaborer une stratégie de sécurité réseau	67
Prédiction des attaques potentielles et analyse de risque	67
Analyse des résultats et amélioration des stratégies de sécurité	70
Règles élémentaires d'une stratégie de sécurité réseau	70
Propositions de stratégies de sécurité réseau	73
Stratégie des périmètres de sécurité	74
Stratégie des goulets d'étranglement	74
Stratégie d'authentification en profondeur	77
Stratégie du moindre privilège	77
Stratégie de confidentialité des flux réseau	79
Stratégie de séparation des pouvoirs	80
Stratégie antivirus	82
Stratégie de participation universelle	83
Stratégie de contrôle régulier	84
En résumé	85

PARTIE III

Les techniques de parade aux attaques	87
--	-----------

CHAPITRE 5

Protection des accès réseau	89
Maîtriser le contrôle des connexions réseau	89
Les pare-feu	90
Les produits du marché	95

Assurer la confidentialité des connexions	97
Algorithmes cryptographiques	100
La suite de sécurité IPsec	104
SSL (Secure Sockets Layer)	113
SSH (Secure Shell)	115
En résumé	117

CHAPITRE 6

Protection des accès distants	119
Assurer l'authentification des connexions distantes	119
Solutions techniques	120
Annuaire LDAP (Lightweight Directory Access Protocol)	129
PGP (Pretty Good Privacy)	131
Biométrie	135
Assurer le contrôle des accès distants	136
Protocoles d'accès distants	138
Protocoles utilisant des mécanismes d'authentification	143
TACACS+	143
RADIUS (Remote Authentication Dial-In User Server)	144
En résumé	145

CHAPITRE 7

Protection des systèmes réseau	147
Maîtriser la sécurité des équipements réseau	147
Sécurité physique	148
Sécurité du système d'exploitation	148
Sécurité logique	150
Gérer le réseau	160
Le routage réseau	160
Supervision réseau SNMP (Simple Network Management Protocol)	170
Mise à l'heure des équipements réseau NTP (Network Time Protocol) ..	172
Résolution de noms DNS (Domain Name Service)	174
En résumé	176

Assurer la confidentialité des connexions	97
Algorithmes cryptographiques	100
La suite de sécurité IPsec	104
SSL (Secure Sockets Layer)	113
SSH (Secure Shell)	115
En résumé	117

CHAPITRE 6

Protection des accès distants	119
Assurer l'authentification des connexions distantes	119
Solutions techniques	120
Annuaire LDAP (Lightweight Directory Access Protocol)	129
PGP (Pretty Good Privacy)	131
Biométrie	135
Assurer le contrôle des accès distants	136
Protocoles d'accès distants	138
Protocoles utilisant des mécanismes d'authentification	143
TACACS+	143
RADIUS (Remote Authentication Dial-In User Server)	144
En résumé	145

CHAPITRE 7

Protection des systèmes réseau	147
Maîtriser la sécurité des équipements réseau	147
Sécurité physique	148
Sécurité du système d'exploitation	148
Sécurité logique	150
Gérer le réseau	160
Le routage réseau	160
Supervision réseau SNMP (Simple Network Management Protocol)	170
Mise à l'heure des équipements réseau NTP (Network Time Protocol) ..	172
Résolution de noms DNS (Domain Name Service)	174
En résumé	176

PARTIE IV

Les techniques de contrôle de sécurité 177

CHAPITRE 8

Contrôle interne de sécurité 181**Analyser la configuration des équipements réseau 182**

Politique de sécurité réseau simplifiée 182

Mécanismes de sécurité 183

Plan de contrôle et procédures 185

Consistance des configurations réseau 192

L'outil RAT (Router Audit Tool) 200

Analyser la sécurité des systèmes 205

Politique de sécurité système 205

Mise en œuvre du plan de contrôle et de ses procédures 206

En résumé 207

CHAPITRE 9

Contrôle externe de sécurité 209**Contrôler par scanning réseau 209**

Établissement du plan de contrôle 210

L'outil NMAP 213

Scanning en mode distribué 219

Contrôler par des attaques 220

Politique de sécurité réseau 220

L'outil Nessus 224

En résumé 233

CHAPITRE 10

Tableau de bord de la sécurité réseau 235**Analyse des événements réseau 236**

Politique de sécurité réseau simplifiée 236

Mécanismes de sécurité 236

Plan de contrôle et procédures 238

Outils de SIM (Security Information Management)	243
Règles de corrélation	244
Outils SIM du marché	247
Établissement d'un tableau de bord de la sécurité réseau	250
Évolution du nombre de faiblesses de sécurité détectées	252
Évolution du pourcentage du nombre d'équipements impactés	253
Évolution du nombre moyen de faiblesses de sécurité par équipement ..	254
Évolution du nombre total de faiblesses de sécurité détectées par niveau d'impact ré-	
seau	255
Évolution du nombre d'attaques détectées par équipement de sécurité ..	257
Évolution du nombre d'attaques détectées par sous-réseau	257
Évolution du nombre d'attaques détectées par service réseau	258
En résumé	260

PARTIE V

Étude de cas	261
---------------------------	------------

CHAPITRE 11

RadioVoie, du réseau initial au premier gros contrat	263
Le premier réseau RadioVoie	263
Besoins à satisfaire	263
Étude de risques	264
Politique de sécurité réseau	264
Solution de sécurité	264
Risques réseau couverts	266
Risques réseau non couverts	266
Contrôle de sécurité	266
Extension du réseau RadioVoie	268
Besoins à satisfaire	268
Étude de risques	268
Politique de sécurité réseau	269
Solution de sécurité	269
Risques réseau couverts	281
Risques réseau non couverts	281
Contrôle de sécurité	281

RadioVoie sous-traite son service de support	283
Besoins à satisfaire	283
Étude de risques	283
Politique de sécurité réseau	284
Solution de sécurité	284
Risques réseau couverts	285
Risques réseau non couverts	287
Contrôle de sécurité	287
RadioVoie négocie un contrat militaire	287
Besoins à satisfaire	287
Étude de risques	289
Politique de sécurité réseau	289
Solution de sécurité	290
Risques réseau couverts	293
Risques réseau non couverts	294
Contrôle de sécurité	294
En résumé	296

CHAPITRE 12

RadioVoie devient une multinationale	297
Besoins à satisfaire	297
Étude de risques	298
Politique de sécurité réseau	298
Politique de sécurité du domaine réseau	299
Politique de sécurité du domaine d'accès	300
Politique de sécurité du domaine intranet	301
Solution de sécurité	302
Solution de sécurité pour le domaine réseau	302
Solution de sécurité pour le domaine d'accès	306
Solution de sécurité pour le domaine intranet	308
Solution de sécurité pour l'interconnexion des sites	309
Solution de sécurité pour les accès à Internet	310
Solution de sécurité pour les accès à une tierce partie	312
Solution de gestion des équipements de sécurité	315
Isolation logique des trafics réseau	317
Risques réseau couverts	318
Risques réseau non couverts	318

Contrôle de sécurité	319
En résumé	321

ANNEXE

Références	323
Acteurs de l'insécurité	323
Configuration des routeurs	323
Cryptographie	324
Journaux d'activité (logs)	325
Outils d'audit	325
Outils de scanning et d'attaque	326
Mesures de la sécurité des systèmes d'information	327
Politique de sécurité	327
Réseau	328
Stratégies de sécurité	329
Vulnérabilités	329
Index	331