

Table des matières

Remerciements	V
Avant-propos	XIX
Objectifs de l'ouvrage	XX
Organisation de l'ouvrage	XX

PARTIE I

Les attaques réseau

CHAPITRE 1

Les attaques réseau	3
Attaques permettant de dévoiler le réseau	5
Attaque par cartographie du réseau	5
Attaques par identification des systèmes réseau	6
Attaque par identification des routeurs	9
Attaques par traversée des équipements filtrants	9
Attaques permettant d'écouter le trafic réseau	11
Attaque par sniffing	12
Attaque de commutateur	13

Attaques permettant d'utiliser des accès distants Wi-Fi	13
Attaque FMS (Fluhrer, Mantin, Shamir) sur RC4	15
Attaque par modification de paquet	16
Attaque par envoi de paquet ou par répétition	16
Attaque par redirection d'adresse IP	16
Attaques permettant d'interférer avec une session réseau	17
Attaque ARP spoofing	17
Attaque IP spoofing	18
Attaque man-in-the-middle	19
Attaques permettant de modifier le routage réseau	24
Attaques par OSPF (Open Shortest Path First)	24
Attaque par BGP (Border Gateway Protocol)	25
Attaques permettant de mettre le réseau en déni de service	26
Attaque par inondation	26
Attaque par inondation SYN	27
Attaques sur les bogues des piles IP/TCP	27
Attaques par déni de service distribué (DDoS)	29
Autres formes d'attaques	33
En résumé	33

CHAPITRE 2

Les attaques des systèmes réseau	35
Attaques permettant d'identifier les services réseau	35
Attaques par balayage TCP	36
Attaques permettant de prendre l'empreinte réseau du système	42
Attaques permettant d'interroger des services réseau particuliers	46
Attaques permettant de pénétrer le système	50
Attaques sur les faiblesses des systèmes réseau	50
Attaques sur les faiblesses de conception	58
Exploitation des faiblesses (vulnérabilités)	58
Publication des vulnérabilités	58
Les bases de données de vulnérabilités	59
Exemple d'exploitation de vulnérabilités	59
En résumé	65

CHAPITRE 3

Les attaques réseau indirectes	67
Attaques par virus	67
Cycle de vie d'un virus informatique	68
Typologie des virus	70
Techniques de codage d'un virus	75
Détection virale et théorie de la complexité	77
Technologies de lutte antivirale	79
Utilisation malicieuse de la cryptographie	81
Attaques par relais	82
Attaques par vers	82
Attaques visant la saturation des systèmes relais	83
Les CERT (Computer Emergency Response Team)	83
En résumé	84

PARTIE II

Conduire une politique de sécurité réseau

CHAPITRE 4

Gestion des risques et évaluation de la sécurité	87
Analyse des risques et objectifs de la sécurité	87
Méthodes d'évaluation qualitative de la sécurité	90
Les critères communs de sécurité	90
Méthodes d'évaluation quantitative de la sécurité	94
Le graphe des privilèges	94
L'arbre d'attaques	95
L'analyse probabiliste de risques	96
En résumé	102

CHAPITRE 5

Définir une politique de sécurité réseau	103
Organismes et standards de sécurité réseau	103
Guides de politiques de sécurité réseau	105

Recommandations de la NSA (National Security Agency)	106
Standards de politiques de sécurité réseau	107
La norme ISO 17799	109
Définition d'une politique de sécurité réseau	110
Principes génériques d'une politique de sécurité réseau	110
Niveaux d'une politique de sécurité réseau	115
Typologie des politiques de sécurité réseau	116
Guides et règles associés à la politique de sécurité réseau	117
Organisation et management	118
Ressources humaines	118
Gestion de projet	118
Gestion des accès logiques	119
Exploitation et administration	120
Vérification des configurations	120
Sécurité physique	121
Plan de contingence	121
Audit de la sécurité	122
En résumé	122

CHAPITRE 6

Les stratégies de sécurité réseau	123
Méthodologie pour élaborer une stratégie de sécurité réseau	123
Prédiction des attaques potentielles et analyse de risque	124
Analyse des résultats et amélioration des stratégies de sécurité	126
Règles élémentaires d'une stratégie de sécurité réseau	127
Propositions de stratégies de sécurité réseau	130
Stratégie des périmètres de sécurité	130
Stratégie des goulets d'étranglement	131
Stratégie d'authentification en profondeur	133
Stratégie du moindre privilège	134
Stratégie de confidentialité des flux réseau	135
Stratégie de séparation des pouvoirs	137
Stratégie d'accès au réseau local	139
Stratégie d'administration sécurisée	140
Stratégie antivirus	140
Stratégie de participation universelle	143
Stratégie de contrôle régulier	144
En résumé	145

PARTIE III

Les techniques de parade aux attaques

CHAPITRE 7

Protection des accès réseau	149
Contrôler les connexions réseau	149
Les pare-feu	150
Les N-IPS (Network-Intrusion Prevention System)	158
Contrôle de l'accès au réseau	160
Contrôle des attaques par déni de service	162
Assurer la confidentialité des connexions	165
Algorithmes cryptographiques	167
La suite de sécurité IPsec	173
SSL (Secure Sockets Layer)	184
SSH (Secure Shell)	187
En résumé	189

CHAPITRE 8

Protection des accès distants	191
Assurer l'authentification des connexions distantes	191
Mots de passe	192
Tokens RSA	192
Signature numérique à paires de clés publique/privée	193
Certificats électroniques	198
Paires de clés PGP (Pretty Good Privacy)	202
Assurer le contrôle des accès physiques à un réseau local	205
Assurer le contrôle des accès distants classiques	207
PPP (Point-to-Point Protocol)	209
PPTP (Point-to-Point Tunneling Protocol)	211
L2TP (Layer 2 Tunneling Protocol)	212
SSH (Secure SHell)	214
SSL (Secure Sockets Layer)	214
Protocoles d'authentification usuels des accès distants	215
Assurer le contrôle des accès distants WI-FI	217
En résumé	220

CHAPITRE 9

Sécurité des équipements réseau	221
Sécurité physique des équipements	222
Sécurité du système d'exploitation	223
Sécurité logique des équipements	224
Configuration des commutateurs Cisco	224
Configuration des routeurs Cisco	228
Configuration des routeurs Juniper	242
En résumé	256

CHAPITRE 10

Protection des systèmes et des applications réseau	257
Séparer les plates-formes	258
Sécuriser les systèmes d'exploitation	259
Les pare-feu	262
Sécuriser la gestion des droits d'accès	265
Sécuriser le contrôle d'intégrité	267
Maîtriser la sécurité des applications	269
Codage défensif	270
Environnements d'exécution sécurisés	271
Environnements cloisonnés	272
Tests de validation	273
Un exemple malheureux	274
En résumé	275

CHAPITRE 11

Protection de la gestion du réseau	277
Le routage réseau	279
Les protocoles de routage IGP	280
Les protocoles de routage EGP	283
Les protocoles de routage multicast	293
La supervision réseau SNMP	300
Mise à l'heure des équipements réseau NTP	302
La résolution de noms DNS	303
En résumé	306

PARTIE IV

Techniques de contrôle de la sécurité réseau

CHAPITRE 12

Le contrôle externe de sécurité	311
Contrôle par balayage réseau	311
Politique de sécurité simplifiée	312
Mise en œuvre d'une solution de contrôle externe	312
Analyse des données collectées	320
Contrôle par analyse simple des applications	321
Politique de sécurité simplifiée	321
Mise en œuvre d'une solution de contrôle externe	321
Analyse des données collectées	327
Contrôle par analyse complète des applications	328
Politique de sécurité simplifiée	328
Mise en œuvre d'une solution de contrôle externe	329
Analyse des données collectées	330
Cas particulier des réseaux sans fil	330
Politique de sécurité	331
Mise en œuvre d'une solution de contrôle externe	332
En résumé	336

CHAPITRE 13

Contrôle interne de sécurité	337
Analyse de la configuration des équipements réseau	337
Politique de sécurité réseau simplifiée	338
Mécanismes de sécurité	339
Plan de contrôle et procédures	341
Consistance des configurations réseau	343
L'outil RAT (Router Audit Tool)	352
Analyse de la configuration des équipements de sécurité réseau passifs	356
Plan de contrôle et procédures	356
Analyse des traces des sondes d'intrusion IDS/IPS	357
Analyse des traces des pots de miel (honeypots)	360

Analyse de la configuration des systèmes réseau	361
Analyse des fichiers de configuration des services réseau	361
Analyse de la configuration du système d'exploitation	366
Analyse des traces des services applicatifs	370
Politique de sécurité	370
Le contrôle	371
Analyse des traces du système d'exploitation	372
Politique de sécurité	372
Le contrôle	372
En résumé	373

CHAPITRE 14

Tableau de bord de la sécurité réseau	375
Objectifs d'un tableau de bord de la sécurité réseau	376
Besoins opérationnels	377
Définition d'une échelle de mesure	377
Évaluation de la sécurité d'un réseau	378
Restrictions d'un arbre probabiliste	379
Modélisation simplifiée d'un nœud de l'arbre	380
La mesure du risque	382
Les outils de SIM (Security Information Management)	383
Les règles de corrélation	384
Les outils SIM du marché	387
Mise en œuvre d'un tableau de bord de la sécurité réseau	390
Les indicateurs de base	392
Tableaux de bord et périmètres de sécurité	403
En résumé	405

PARTIE V**Étude de cas**

CHAPITRE 15

Outils maison de sécurité réseau	409
Analyse de la conformité des mots de passe	410

Conception des outils	410
Prise en main	412
Analyse de la cohérence d'ACL	414
Conception de l'outil	415
Prise en main	416
Analyse de configuration par patron	418
Conception de l'outil	419
Prise en main	421
Analyse de configuration d'équipements réseau Juniper	424
Conception de l'outil	424
Prise en main	425
Gestion de graphes	428
Conception de l'outil	428
Prise en main	429
Calculateur de risque	436
Conception de l'outil	436
Prise en main	438
En résumé	447

CHAPITRE 16

RadioVoie, du réseau initial au premier gros contrat	449
Le premier réseau RadioVoie	450
Besoins à satisfaire	450
Étude de risques	450
Politique de sécurité réseau	450
Solution de sécurité	451
Risques réseau couverts	452
Risques réseau non couverts	453
Tableau de bord de sécurité	453
Extension du réseau RadioVoie	459
Besoins à satisfaire	459
Étude de risques	460
Politique de sécurité réseau	460
Solution de sécurité	461
Risques réseau couverts	472
Risques réseau non couverts	472
Tableau de bord de sécurité	473

RadioVoie sous-traite son service de support	477
Besoins à satisfaire	477
Étude de risques	478
Politique de sécurité réseau	478
Solution de sécurité	478
Risques réseau couverts	480
Risques réseau non couverts	481
Tableau de bord de sécurité	481
En résumé	488

CHAPITRE 17

RadioVoie étend son réseau	489
RadioVoie négocie un contrat militaire	489
Besoins à satisfaire	490
Étude de risques	490
Politique de sécurité réseau	490
Solution de sécurité	491
Risques réseau couverts	494
Risques réseau non couverts	495
Tableau de bord de sécurité	496
RadioVoie étend son réseau à l'international	504
Besoins à satisfaire	504
Étude de risques	504
Politique de sécurité réseau	505
Solution de sécurité	508
Risques réseau couverts	524
Risques réseau non couverts	524
Tableau de bord de la sécurité	525
En résumé	535

ANNEXE

Références	537
Le site officiel du livre	537
Quelques références des auteurs	537
Quelques références scientifiques	538
Quelques livres scientifiques	539

Quelques critères d'évaluation	540
Quelques revues	540
Quelques formations de sécurité	540
Autres références	541
Acteurs de l'insécurité	541
Configuration des routeurs	541
Cryptographie	541
Journaux d'activité (logs)	542
Outils d'audit	542
Outils de scanning et d'attaque	543
SSH	544
Mesures de la sécurité des systèmes d'information	544
Politique de sécurité	545
Réseau	545
Stratégies de sécurité	547
Tunnels/VPN	547
Vulnérabilités	548
Index	549