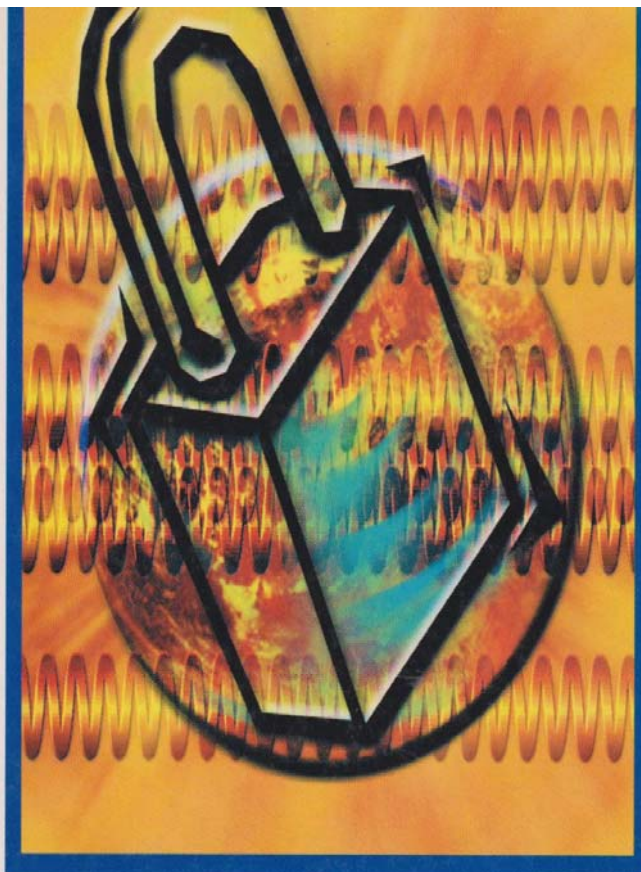


STRATÉGIES



Stephen Northcutt - Judy Novak

& Donald McLachlan

Détection des intrusions réseaux

Collection

Référence



CAMPUSPRESS

www.campuspress.net



05-429-1

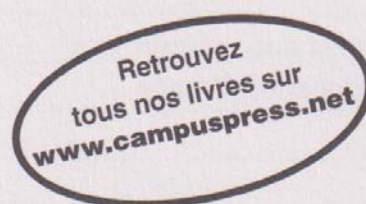
2-005-429-1

Détection des intrusions réseaux

Stephen Northcutt

Judy Novak

Donald McLachlan




CAMPUSPRESS
FRANCE

Table des matières

Introduction	1
Histoire de Shadow	1
Partager l'information	3
Snort	4
Résumé	4
Préface	5
Y a-t-il une menace ?	5
Une attaque des Aliens	5
La fièvre d'Y2K	6
Le problème du "bug de l'an 2000", un an après	6
Les attaques par déni de service distribuées (DDOS)	8
Les macro-menaces	9
L'économie Internet	10
Les rapports de domination entre les pays	14
Les micro-menaces	14
Les faillites d'entreprises	14
Les autres micro-menaces	16
Le rôle de la détection des intrusions dans la réduction de la menace	17
Résumé	17
Chapitre 1. Les concepts d'IP	19
Le modèle TCP/IP d'Internet	20
Les couches	21
Le flux des données	22
L'organisation des données en paquets	23
Les bits, les octets et les paquets	23
L'encapsulation des données	25
L'interprétation des couches	26
Les adresses physiques et les adresses logiques	28
Les adresses physiques : les adresses MAC	28

Les masques de sous-réseau	31
Les ports des services	31
Les protocoles d'IP	33
Le système de noms de domaine	34
Le routage	36
Résumé	38
Chapitre 2. Introduction à TCPdump et à TCP	39
TCPdump	40
Le comportement de TCPdump	40
Les filtres	40
La collecte des données	41
Définir la quantité de données collectées	42
La sortie de TCPdump	43
Les numéros de séquence absolus et relatifs	45
Les sorties en hexadécimaux	46
Introduction à TCP	46
Etablir une connexion TCP	47
Les ports client et serveur	49
Terminaison de la connexion	50
Le transfert des données	51
Quels sont les points essentiels ?	51
Introduction à la détection d'activités TCP suspectes	52
Un balayage ACK	53
Un balayage Telnet ?	54
Détournement de session TCP	55
Résumé	56
Chapitre 3. La fragmentation	57
Théorie de la fragmentation	57
Structure des fragments	58
La fragmentation telle qu'elle apparaît dans TCPdump	63
La fragmentation et les dispositifs de filtrage de paquets	64
Le drapeau don't fragment	65
Utilisation de la fragmentation à des fins de nuisance	66
En-têtes TCP fragmentés	66
Harassement d'un routeur	67
Résumé	68

Chapitre 4. ICMP	71
Eléments théoriques sur ICMP	72
Utilité d'ICMP	72
ICMP dans la pile TCP/IP	72
Caractéristiques d'ICMP	73
Résumé des éléments théoriques sur ICMP	74
Techniques de mappage	75
Un mappage exhaustif	76
Un mappage efficace	77
Un mappage astucieux	77
Un mappage sophistiqué	78
Bilan sur le mappage	79
Activité ICMP normale	79
Message "Host unreachable" (hôte injoignable)	79
Message "Port unreachable" (port injoignable)	80
Message "Admin Prohibited" (interdiction administrative)	80
Message "Redirect" (redirigé)	80
Message "Need to Frag" (nécessité de fragmenter)	81
Message "Time Exceeded In-Transit" (temps dépassé)	82
Bilan sur l'activité ICMP normale	82
Activité ICMP malveillante	82
Attaque Smurf	83
Attaque Tribe Flood Network	84
Attaque WinFreeze	85
Attaque Loki	86
Réponses d'écho ICMP non sollicitées	86
Bilan sur l'activité ICMP malveillante	88
Faut-il bloquer le trafic ICMP ?	89
Des requêtes d'écho ICMP sans réponse	89
Impossibilité d'employer traceroute	89
Des LAN silencieux	89
Impossibilité de déterminer le MTU de chemin	90
Résumé	90
Chapitre 5. Stimulus et réponse	91
Comportements typiques	92
Les Requests for Comments	92
Stimulus et réponse TCP	93
Stimulus et réponse UDP	95

Stimulus et réponse ICMP	96
Comportements atypiques, mais normaux	98
FTP	98
L'utilitaire Traceroute d'UNIX	99
Bilan sur les comportements typiques et atypiques, mais normaux	99
Stimuli anormaux	100
Un stimulus détourné qui attend une réponse	100
Un stimulus diabolique qui provoque une réponse fatale	101
Une absence de stimulus qui appelle toutes les réponses	102
Stimuli non-conventionnels destinés à identifier les systèmes d'exploitation	103
Des drapeaux TCP inexistants	104
Les options TCP	105
Absence de drapeaux TCP	106
Longueur incorrecte des données TCP	107
Bilan sur les stimuli anormaux	107
Résumé	108
Chapitre 6. Le DNS	109
Eléments théoriques sur DNS	110
La structure du DNS	110
La résolution des noms sur Internet	111
La mise en mémoire cache des réponses	117
La résolution des IP en noms d'hôtes	118
Les serveurs de noms primaires et secondaires	119
Les transferts de zone	119
UDP ou TCP	120
Bilan des éléments théoriques sur le DNS	121
Utiliser le DNS pour des opérations de reconnaissance	121
La commande nslookup	122
Les enregistrements HINFO	123
Les listes des maps de la zone	124
L'utilitaire dig	124
Traceroute	125
Exemples de manipulations des réponses DNS	126
Un maillon qui fragilise certaines procédures d'authentification	126
La mise en mémoire cache de données erronées	126
Résumé	128

Chapitre 7. L'attaque de Mitnick	129
L'exploitation des faiblesses de TCP	129
Rappel de quelques éléments théoriques sur TCP	130
L'attaque SYN flood	131
La compromission du système	138
Détecter l'attaque de Mitnick	141
Les systèmes réseau de détection des intrusions	141
La relation d'approbation	142
Le balayage des ports	143
Le balayage des hôtes	143
Les connexions sur des ports dangereux	143
Les systèmes de détection des intrusions installés sur des hôtes	144
TCP Wrappers	144
Tripwire	145
Empêcher l'attaque de Mitnick	145
Résumé	146
Chapitre 8. Introduction aux filtres et aux signatures	149
La stratégie de filtrage	149
Tout refuser	150
Tout autoriser	150
Les signatures	151
Les filtres utilisés dans la détection des intrusions	152
Exemples de filtres	153
L'attaque Land	153
WinNuke	154
Le filtre Xmas tree	159
Exemple de filtre de détection des attaques sur les serveurs Web	161
L'exemple du filtre Snort	164
Introduction à l'architecture de Snort	164
Les composants de Snort	164
Exemple de mise en œuvre de Snort	166
Problèmes de stratégie relatifs à des cibles particulières	166
Utilisations interdites	167
Pornographie infantine	168
Le mauvais employé	168
Tout arrêter	168
Résumé	169

Chapitre 9. Questions relatives à l'architecture des IDS	171
Les événements remarquables (EOI)	173
Limites des observations possibles	173
Limites inhérentes à la détection fondée sur des signatures	175
Limites liées au facteur humain	176
Les limites liées à l'analyste	176
Les limites liées aux CIRT	177
Evaluation de la gravité des attaques	178
La position stratégique de la cible	180
Le niveau de la compromission	180
Les contre-mesures	181
Calcul de la gravité des dommages	181
Balayage des ports d'un hôte	182
Balayage d'hôtes sur le port FTP	184
Placement des détecteurs	185
Détecteurs à l'extérieur du pare-feu	185
Détecteurs à l'intérieur du pare-feu	186
Détecteurs à l'intérieur et à l'extérieur du pare-feu	186
Autres emplacements pour les détecteurs	187
Architectures push et pull	188
La console de l'analyste	190
Performance de la console	191
Gestion des fausses alarmes	191
Filtres de visualisation	192
Marquage des événements ayant été analysés	192
Accès aux données par l'interface graphique	192
Fonctionnalités statistiques	193
Etablissement des rapports	193
Remarques relatives à l'architecture d'ensemble de l'IDS	194
Résumé	196
Chapitre 10. Interopérabilité et corrélation	197
Assurer l'interopérabilité entre plusieurs produits	198
Le modèle logique du CIDEF	198
Le langage CISEL	199
AusCERT Autopost	200
IDWG	201
Solutions commerciales d'interopérabilité des IDS	201
OPSEC	201

CCI	202
Corrélation	203
La corrélation des IP sources	203
La corrélation des IP de destination	205
La corrélation des signatures de paquets hostiles	205
La corrélation des signatures de nouvelles attaques	208
La corrélation des heures	209
La corrélation de la fréquence des détections	213
Bases de données SQL	214
Le chargement des données	215
La réduction des données	215
Le support des requêtes	217
Les performances	218
Résumé	219
Chapitre 11. Les solutions réseau de détection des intrusions	221
Snort	222
Les utilitaires commerciaux	222
RealSecure d'ISS	222
NetProwler d'Axent	226
Les systèmes pour UNIX	227
Network Flight Recorder	228
NetRanger de Cisco	229
GOTS	230
EPIC ²	230
Network Intrusion Detector (NID)	231
Shadow	232
Evaluer les systèmes de détection des intrusions	233
Mitre Bakeoffs	233
InfowarCon	234
L'approche des laboratoires Lincoln	234
ID-NET de SANS	235
Résumé	236
Chapitre 12. Evolutions futures	237
Accroissement de la menace	238
Des outils d'attaque améliorés	239
Améliorer le ciblage des attaques	240
Portabilité du code	240

Les portes dérobées	240
Les points d'insertion	241
Le modèle d'approbation	241
Evaluation des contre-mesures à adopter	243
La coopération : héritage de Y2K	245
Le cyberterrorisme	246
Les attaques venues de l'intérieur	249
Les perspectives pour le marché de la sécurité	249
Le secteur des antivirus	250
La détection par le matériel	251
La défense en profondeur	252
La détection par les programmes	253
Des auditeurs intelligents	253
Résumé	255
Chapitre 13. Exploits et balayages pour appliquer des exploits	255
Les fausses alarmes	256
Toutes les réponses, aucun stimulus	259
Balayage ou réponse ?	259
Les alarmes SYN flood	261
Back Orifice ?	264
Exploits IMAP	264
La signature 10143 pour le port source	264
La signature 111	265
Exploits avec SYN FIN définis	266
Zone DNS suivie de 0, SYN FIN avec NFS comme cible	267
Des balayages pour appliquer des exploits	267
Balayages multiples	271
Un seul exploit : portmap	273
rexec	273
POP3	274
Des systèmes SGI comme cibles ?	274
Discard	274
Balayage de trois ports	275
Un étrange balayage Web	277
IP-Proto-91	278
Port source 23 et SYN FIN définis	279
Résumé	

Chapitre 14. Dénî de service	281
Les traces de DoS par force brute	282
L'attaque Smurf	282
Le relais d'un broadcast	284
Les attaques Echo-Chargen	285
Les attaques DoS élégantes	286
Teardrop	286
Le ping de la mort	287
L'attaque Land	289
L'attaque Doom	289
nmap 2.53	290
Les attaques par déni de service distribuées	291
Introduction aux DDOS	292
Le logiciel DDOS	293
Résumé	294
Chapitre 15. Détection des opérations de collecte d'informations	295
Le mappage des réseaux et des hôtes	296
Balayage d'hôtes à l'aide de requêtes echo UDP	297
Adresses de broadcast avec les masques de sous-réseau	298
Balayage de ports	299
Balayage d'un port particulier	300
Un script sophistiqué, une compromission possible	300
Balayage de ports "aléatoire"	302
Etablissement de rapports de corrélation	303
Balayage SNMP/ICMP	304
FTP Bounce	305
Traces concernant du trafic NetBIOS	306
Visite d'un serveur Web	306
Session null	307
Attaques furtives	308
Techniques de mappages furtives explicites	309
Mesurer le temps de réponse	313
Requêtes echo	314
Fausse requête DNS	314
Sondage sur le port UDP 33433	314
Port TCP 53	315
Des virus collecteurs d'informations	316
Le ver Pretty Park	316

RingZero	318
Résumé	319
Chapitre 16. Les attaques sur les RPC	321
Portmapper	322
Portsentry défend activement	322
rpcinfo indique l'emplacement des services RPC	322
Ne pas oublier les empreintes réseau	323
Dump est un composant crucial de rpcinfo	324
dump()	325
Exemples de détections	326
Les attaques directes sur un service RPC	326
Exemples d'attaques directes sur les RPC	326
Script d'attaque sur RPC	328
Les trois principaux exploits RPC	329
L'analyse en temps réel	330
Profondeur et ampleur	330
Mise en situation	330
Fausse alarme	331
D'étranges caractères sur getport()	331
Autre trace sur getport()	332
Callit(nsrstat)	332
Getport(1000<) sur un système Solaris	333
Un dernier exemple : rpc.ttdbserverd	334
Retour sur nmap	334
Résumé	337
Chapitre 17. Construire des filtres pour TCPdump	339
L'écriture d'un filtre TCPdump	340
Le masquage de bits	342
Retenir et écarter des bits spécifiques	342
Créer le masque	343
Application à un cas pratique	344
Les filtres IP de TCPdump	345
La détection du trafic envoyé sur des adresses de broadcast	345
La détection de la fragmentation	346
Les filtres UDP de TCPdump	347
Les filtres TCP de TCPdump	349
Des filtres pour examiner les drapeaux TCP	349

Détecter des données sur des connexions SYN	351
Résumé	353
Chapitre 18. La compromission d'un système	355
La veille de Noël 1998	356
Prise en charge du système	356
Préparation pour les balayages de reconnaissance	358
Début des balayages de reconnaissance	362
Préparation pour l'assaut	366
Ratés de l'attaque	368
Assaut final	370
L'infrastructure de support des attaquants	370
Un ensemble complet d'outils	371
Des programmes de formation	371
Une monnaie "non traçable"	372
Des programmes de parrainage	373
Les communications	373
L'anonymat	376
Résumé	376
Chapitre 19. La chasse aux Timex	377
Les traces	377
De nouvelles traces	379
Pourquoi X.Y.Z.0 ?	379
La chasse commence	380
Le nœud se resserre... ..	383
A moins que... ..	385
Y2K	386
Des paquets d'un faussaire ?	386
Un canal secret ?	387
L'anti-aliasing	388
Les TTL initiales des messages ICMP	388
Les cartes du réseau	389
Découverte des sources	390
Considérations annexes	391
Empreinte timex d'un routeur ?	391
Empreinte ID IP de routeurs	392
Retour sur les TTL	393
Récapitulatif des points à contrôler	395

Epilogue	396
Résumé	396
Chapitre 20. Questions organisationnelles	399
Le modèle de sécurité de l'organisation	400
La stratégie de sécurité	401
La mise en place des procédures à suivre	401
L'infrastructure de sécurité	402
L'implémentation des contre-mesures prioritaires	402
Des révisions périodiques	403
L'implémentation d'une gestion des incidents	403
Définir le risque	404
Le risque	405
Accepter le risque	405
Alléger ou réduire le risque	407
Définir la menace	410
La quantification de la menace	410
La fréquence de la menace	411
Les limites de la quantification de l'incertitude	413
Les retombées financières de la gestion des risques	413
Quel est le risque du risque ?	414
L'évaluation quantitative des risques	414
L'évaluation qualitative des risques	415
Pourquoi la pratique ne se conforme-t-elle pas à la théorie ?	415
Résumé	416
Chapitre 21. Les réponses aux attaques	417
Les réponses automatisées	418
Questions relatives à l'implémentation	419
Le ralentissement de l'activité (throttling)	421
L'abandon de la connexion	421
L'esquive (shun)	422
L'isolement (islanding)	423
SYN/ACK	423
Reset	424
Les pots de miel (honeypot)	424
Réponses manuelles	426
Isolement	426
Exemple de formulaire pour un Fax	428

Eradication	430
Restauration	431
Enseignements tirés	433
Résumé	434
Chapitre 22. Présenter un projet d'implémentation d'une détection des intrusions	435
Partie 1 : Intérêt pour l'entreprise de faire l'acquisition d'un IDS	437
Le retour sur investissement	437
Des dépenses déterminées et prévisibles	438
La technologie ne déstabilisera pas l'organisation	438
L'appartenance à une stratégie globale de protection des informations	440
Partie 2 : Les menaces et les vulnérabilités	442
L'évaluation et l'analyse des menaces	442
L'identification des actifs	444
L'évaluation des actifs	444
L'analyse des vulnérabilités	445
L'évaluation des risques	446
Partie 3 : Les compromis à faire et la solution recommandée	447
Définir une architecture de gestion du risque en matière de protection des informations	447
Identifier ce qui est déjà en place	448
Identifier les contre-mesures à prendre immédiatement	448
Identifier les options possibles des contre-mesures proposées	449
Présenter une analyse coût-bénéfice	449
La planification du projet	450
Identifier les étapes futures	451
Résumé	451
Index	453