

Contenu en un clin d'œil

Chapitre 1 - La sécurité en entreprise	21
Chapitre 2 - Les infiltrations	45
Chapitre 3 - La manipulation	93
Chapitre 4 - L'extraction de données	115
Chapitre 5 - La détection des attaques réseau	149
Chapitre 6 - Les écoutes de réseaux avec Wireshark	187
Chapitre 7 - Les vulnérabilités des réseaux sans fil	253
Chapitre 8 - Les méthodes des pirates	289
Chapitre 9 - Les scanners de réseaux	329
Chapitre 10 - Les cryptages	349
Chapitre 11 - Les recherches Google	379
Chapitre 12 - La force brute	409
Chapitre 13 - ANNEXES	439

1	La sécurité en entreprise	21
1.1	Reconnaître l'entreprise avant une attaque	23
	Les tactiques d'attaques courantes	24
	Les informations libres	27
1.2	Protéger l'entreprise	27
1.3	Protéger les informations publiques	28
	Les achats en ligne	28
	La ligne téléphonique	29
	Les annonces publicitaires	29
	Le personnel et les appels téléphoniques	29
	Des spams à volonté	29
	La boîte vocale	29
	Les procédures pour des envois de colis	30
1.4	Protéger les informations internes et implémenter le matériel	30
	Créer des badges de couleurs différentes	30
	Les lignes téléphoniques avec différentes sonneries	30
	Le traçage d'appel	30
	L'annuaire	31
	Création de stratégies de mots de passe complexes	31
	Installation d'un antivirus, un antitroyen, un pare-feu	31
	Les caméras de surveillance	32
	Masquage des propriétés du système	32
	Désactivation des outils amovibles	32
	Couleur et sensibilité des informations	32
	La photocopieuse	32
	Configuration du fax, du routeur	32
	Mise en place de systèmes biométriques dans des endroits sensibles	33
	Destruction des informations sensibles ou du matériel contenant des informations sensibles	34
	Configuration du modem	34
	Protection des corbeilles à papier et des poubelles	34
	Les informations internes	34
	Configuration d'un réseau sans fil	35
	Configuration d'un moniteur réseau	35
	Installation d'un pare-feu interne et externe	35
	Les privilèges des utilisateurs	35
	Formation des employés	35
	Création d'un groupe de gestion des incidents	36
	Formation des salariés	36
	Les catégories des informations	37

	Les responsables hiérarchiques	38
	Diffusion des informations à un tiers	38
	La manipulation téléphonique	39
1.5	Les informations sensibles	40
1.6	Vérifier des antécédents	41
1.7	Synthèse	44

2 Les infiltrations 45

2.1	Quelqu'un joue avec ma messagerie	47
2.2	Le piège des sites pornographiques	48
	Recommandations	52
2.3	Les troyens	52
	Recommandations	54
2.4	Les étrangers sur le Internet	57
2.5	Les boîtes aux lettres électroniques	58
2.6	Les écoutes à distance	60
2.7	Les caméras cachées	61
	Les caméras à déclenchement à la voix	61
	Les caméras Bouton	63
	Les caméras cachées professionnelles	67
	Les types d'installations	73

3 La manipulation 93

3.1	L'espionnage industriel	95
3.2	Des informations attirantes pour les espions	96
3.3	Les tactiques et objectifs	97
3.4	Histoire : Urgence d'obtention de renseignements confidentiels	99
	Compassion	100
	Usurpation d'identités	102
	Usurpation recommandée	103
	Aidez-moi, monsieur le manipulateur	105
	Fuite d'informations confidentielles	106
	Complice involontaire	107
	Dépannage d'un collègue	107
	Arrivée d'informations sensibles	109
	Manipulateur par intimidation	109
	Secrets d'entreprise dévoilés	111
	Récupération des données	112
	Conclusion	112

4	L'extraction de données	115
4.1	Les logiciels d'extraction de données	117
4.2	Logiciels d'extraction de données SpotAuditor	127
4.3	La mémoire faciale	128
4.4	L'extraction de données effacées	129
4.5	L'extraction de données grâce à R-STUDIO	131
4.6	Logiciel NETRESIDENT	132
4.7	Les keyloggers : Blazingtools Perfect Keylogger	133
	Configuration générale	134
	Configuration de login	135
	Les captures d'écran	136
	Configuration du FTP	140
	Les alertes	142
	Installation à distance	143
4.8	Les keyloggers physiques	145
	Le keylogger USB "KeyCarbon USB"	145
	Le fonctionnement du keylogger USB	146
	Le keyCarbon raptor	147
5	La détection des attaques réseau	149
5.1	La détection de scanners	151
	L'excessive TCP Reset	153
	Les flags TCP étranges	156
	Les scanners d'adresses IP	157
	Les attaques OS Fingerprinting Actives et Passives	159
5.2	L'analyse du trafic ICMP	161
	Les types et codes ICMP	161
	La détection ICMP	163
	La redirection du Routeur	166
	Le déni de service	167
	L'ICMP OS Fingerprinting	168
5.3	Le TCP Malveillant	170
	Le TCP Slicing malformed et injection de paquets	171
	Le reset injection	174
5.4	Le spoofing d'adresse	175
5.5	La construction des règles de pare-feu ACL	176
	La génération automatique des règles	176
5.6	La signature d'une attaque	177

Trouver une signature connue	178
L'attaque simple	180
La détection de l'attaque par dictionnaire	180
L'attaque par Déni de service	184
La redirection	185

6 Les écoutes de réseaux avec Wireshark 187

6.1	Les possibilités de Capture Options	190
6.2	Les préférences	195
6.3	Les techniques de coloration et de navigation	201
	Les lignes	202
	L'exportation des couleurs	203
	Le réglage du temps	206
	Les bases statistiques de Wireshark	208
	Examine Multicast Streams and settings	212
6.4	La création de filtres d'affichage	215
6.5	La sécurité surveillée	227
	Trafic DNS	227
	Le service DHCP	229
	Le protocole TCP/IP	230
	Le protocole de communication HTTP	231
	Le protocole FTP	234
	Le protocole POP	244
	Le protocole SMTP	246
	Erreurs de transmission	248

7 Les vulnérabilités des réseaux sans fil 253

	Les ondes radioélectriques	258
7.1	Les principales applications d'écoute	259
7.2	Les types de réseaux sans fil	259
	TKIP et CCMP 802.11i : le mariage	263
7.3	Airpcap et Wireshark	264
	Paramètres (Settings)	266
	Clé (KEY)	267
	Snnifer Wireshark	268
	La création de filtres pour Wireshark	269
7.4	Wireshark avec les logiciels Airodump-ng et Aircrack-ng	276
7.5	Airpcap et le logiciel Cain & Abel	278
	Airpcap, Cain, WPA cracking	283

7.6	Le sniffer Wireless moniteur Airoppeek	287
7.7	Les parades	287

8 Les méthodes des pirates 289

8.1	Le repérage de domaines	291
	L'annuaire Whois	291
8.2	Les traceurs	297
	Les logiciels de traçage gratuits	298
	Le programme de traçage VisualRoute	302
	Le programme de traçage NeoTrace	306
	Conclusion	309
8.3	L'anonymat sur Internet	310
	Connexion à Internet avec un camouflage	313

9 Les scanners de réseaux 329

9.1	Le scanner NMAP et les sniffers	331
	Les avantages de NMAP	331
	Les commandes	332
	Des exemples pratiques	334
	Les techniques d'utilisation en détail	335
	Mesures	347

10 Les cryptages 349

10.1	Le cryptage des clés USB	351
10.2	Cryptage et décryptage Locktight	359
	Cryptage d'un fichier	359
	Apercevoir le fichier hola.doc crypté	361
	Décryptage de fichiers	361
10.3	Bitlocker	363
10.4	La stéganographie	369
	Présentation de la stéganographie	369

11 Les recherches Google 379

11.1	Introduction à Google	381
	Résumé de la syntaxe des opérateurs des groupes de Google	381
	Résumé de la syntaxe	381
	Résumé de la syntaxe des opérateurs booléens	382
	Résumé de la syntaxe de Google	382

11.2	Les sites de téléchargement de logiciels P2P	385
11.3	La recherche de documents sur Internet	388
	Rechercher des fichiers Word	388
	Rechercher des fichiers Excel	390
	Rechercher des fichiers PowerPoint	393
	Rechercher des fichiers PDF	393
	Rechercher des fichiers texte	395
	Rechercher des fichiers image	395
11.4	Les techniques de recherche de logiciels	396
	Les sites connus de téléchargement de logiciels	396
	Rechercher des logiciels sur Internet	397
	Rechercher des logiciels dans les fichiers temporaires	398
	Rechercher des jeux sur Internet	400
	Télécharger des DLL	401
	Les techniques de recherche de fichiers audio	401
	Les techniques de recherche de fichiers vidéo	403
11.5	Contre-mesures	407

12

La force brute 409

12.1	Logiciels Ophcrack et Cain & Abel	411
12.2	Craquer les hashes de Windows Vista Version intégrale	422
12.3	Utiliser Pwdump3 dans l'invite de commandes	428
12.4	Les parades	430
	Vérification des mots de passe	430
	Arrêt des attaques de force brute	431
	Changement de nom d'administrateur pour Windows XP SP2 et Windows 2003 Serveur	431
	Verrouillage de compte	432
	Utilisation du moniteur réseau	434

13

ANNEXES 439

13.1	Glossaire	441
13.2	Raccourcis et commandes cachées Windows XP, Vista, 7	460
13.3	Lois sur la protection intellectuelle (CNIL)	465
13.4	Articles du code pénal sur le piratage en France	466

14

Index 471