
Table des matières

Avant-propos	XI
Du droit et du piratage en 2013... ..	XV
Introduction	XIX
Ce que vous trouverez dans ce livre	XIX
Les plus de cette nouvelle édition	XX
Un mot sur l'auteur	XXI
1. Le paysage du piratage informatique	1
Les traces que nous laissons	4
Techniques de pirates	8
Piratage hors ligne, en ligne et nuage	9
La pollution virale et les spywares	10
Le carding et son complice, le phishing	10
Le piratage téléphonique et hertzien	12
Le WiFi	13
Le piratage des téléphones intelligents	15
Des exemples vécus	17
L'analyse d'une attaque type	20
La préparation des attaques	22
La documentation en ligne du pirate	25
Techniques d'essais	26
2. Les défauts de TCP/IP	29
La norme TCP/IP, secret du piratage en ligne !	30
Piratage à tous les étages	31
La norme TCP/IP : source de tous les abus	32
Un réseau trop public	35
La norme TCP/IP : point faible des logiciels	38
Le reniflage	41

Tester votre réseau avec WinPcap et ses dérivés	43
Tester votre réseau avec Analyzer	47
ICMP, les utilitaires Netstat et Route	53
Les contre-mesures pour sécuriser TCP/IP	58
3. Les outils des hackers et leurs cibles	63
L'affaire SSH	64
Connaître le réseau	66
Les deux logiciels PING et Traceroute	66
Les outils de traçage	69
Les scanners	72
Les scanners IP : identification des systèmes	73
Utilisation de Nessus	77
Le scanner est indispensable	77
Les scanners de failles	79
Contre-mesures antiscanner	79
La combinaison des attaques virales, des spywares et des scanners	82
L'identité numérique : la cible	83
Le problème du rapprochement des données	84
La question biométrique	86
Contre-mesures et bonnes pratiques	88
4. Spywares, troyens et virus	93
Le "terrible" cheval de Troie	93
La description d'un troyen	93
Back Orifice 2K (BO2K) : le précurseur	96
Les faux troyens et les vrais virus	99
Installer un cheval de Troie	101
Les troyens en pratique	104
Le virus	107
Les virus macros	108
Le troyen moderne : le spyware	110
Les malwares sophistiqués d'aujourd'hui	111
Les gestes antivirus, antitroyen, antimalware et antispysware	113

Les fausses alertes au virus	113
Le comportement erratique de votre PC	114
Le comportement erratique de votre tablette	114
Le doute sur la source	115
Quand les virus sont là	115
Détecter et supprimer un cheval de Troie	116
Détecter et supprimer des spywares	120
À propos des bases de registres	121
Supprimer une erreur de base de registres	122
Récupérer sa base de registres	122
Attention aux modifications	122
5. Les botnets	123
Fonctionnement du botnet	125
La commercialisation du botnet	126
Implantation du bot et construction du botnet	127
Comment gérer une infection par bot	128
6. L'identification d'un PC individuel	131
Histoire vraie : un pirate dans un PC !	132
Identifier un PC individuel	134
Localiser une adresse IP	134
Localiser une adresse IP dynamique	137
Utiliser les informations collectées	137
Contre-mesures	138
7. Utilisation des réseaux sociaux	139
Panorama des méthodes	139
Les principales vulnérabilités techniques des réseaux sociaux	141
Facebook et le likejacking	143
Le piratage de Twitter	144
Comment se protéger	147
Les bons comportements	147
Contrôler la subsistance de ses traces	149

8. La vulnérabilité des réseaux	151
Accessibilité = vulnérabilité	151
Remarques en matière de sécurité	153
Utiliser une faiblesse de Windows ou d'un système	153
Les systèmes de mise à jour en pratique	155
La mise à jour en ligne avec Windows Update	158
La mise à jour en ligne avec une tablette ou un smartphone	159
La bêtise humaine et les pare-feu... ..	159
La méthode d'attaque la plus courante	161
Les réseaux sans fil : Internet sans payer !	162
Réseau métropolitain et points d'accès publics	163
Le réseau sans fil... par la force	165
Les logiciels de scanner de réseau sans fil	170
Les outils complémentaires	173
En pratique avec NetStumbler	174
En pratique avec AirSnort	176
Sécuriser un réseau sans fil	177
9. Les failles des systèmes	181
Analyser le résultat d'un scan	181
Les exploits	185
La faille NetBIOS	187
Être drôle avec le défaçage	189
Les scanners de failles	191
10. Les mots de passe d'Internet	197
Les mots de passe qui ne protègent rien	197
Contourner les mots de passe	200
L'ingénierie sociale contre les casseurs de mots de passe	200
Les générateurs de mots de passe	201
La technologie et les statistiques contre les mots de passe	203
Le principe de l'attaque de mot de passe	206
Simuler un utilisateur	206
La force brute de Brutus	210

Attaquer un mot de passe de page HTML	217
11. Les mots de passe des PC	223
Les catégories de mots de passe	225
Les mots de passe du BIOS	226
Coupez tout !	227
Un cheval de Troie dans votre PC !	227
Contourner des mots de passe de système	229
Le fonctionnement des mots de passe sous Windows	229
Les particularités des anciens Windows	230
Les crackeurs Windows qui utilisent votre machine	232
Les mots de passe de tablettes	240
La solution ultime : le démasquage !	240
À propos de la bureautique	241
Les mots de passe des anciens formats d'Office	242
Les mots de passe d'Office 97/2000	242
Les mots de passe d'Outlook	246
Les mots de passe des suites bureautiques 2013	246
Les contre-mesures	246
12. La protection des données	249
Protégez-vous... mais pas trop	249
Le RSA, dispositif de clé de Windows	250
GnuPGP en pratique	253
La contre-mesure envers PGP : le renifleur de clavier !	256
Une approche alternative avec la stéganographie	257
La stéganographie aujourd'hui	259
Les logiciels de stéganographie	262
En pratique	265
Les coffres-forts logiciels et le stockage en nuage	271
13. La dissimulation de ses propres traces	275
Les techniques de camouflage	276
Le routage téléphonique	277
Le réseau wireless et le wardriving	278

Utiliser de fausses adresses IP	280
Les réseaux Peer to Peer et routage en oignon	280
Freenet	281
Tor	282
Les public proxy	283
Stealther	285
Anomyzer	286
14. Épilogue : le PC déraile !	289
Les préparatifs	291
Sauvegarder tout ce qui doit l'être	291
Abandonner ce qui doit être rénové	292
Être équipé d'un dispositif de lancement et de récupération	294
Les formatages	295
Les dispositifs de stockage USB	296
Le formatage de bas niveau	297
L'installation de Windows	298
Les points d'exclamation jaunes devant un nom de périphérique	299
Problèmes relatifs à des périphériques de haut niveau	299
Supprimer les pilotes unifiés	300
Affiner la configuration	300
L'installation des logiciels et des documents	301

Annexes

A. Questions et réponses	305
Questions diverses	305
Protection clé en main !	305
ICMP	306
Drôle de virus !	306
Surf anonyme	307
Prise de contrôle à distance	307
Analyser muet	308
Pinger muet	308

SSH ne fonctionne plus	309
Questions et réponses sur le WiFi	309
Questions et réponses sur les spams et le phishing	310
Agressions antiCharton !	311
B. Les articles du Code pénal sur le piratage informatique	313
Des atteintes aux systèmes de traitement automatisé de données	315
La Loi loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure	315
C. Le protocole ICMP	317
D. Quelques backdoors de BIOS	321