

Jean-François PILLOU
Jean-Philippe BAY



Comment
ça marche .net

Tout sur la Sécurité informatique

4^e édition



DUNOD

Tabnabbing

Amplification NTP

Thingbot

APT

Shellcode

TPM

Downgrade

Appstore

Ransomware

NSA

Faillles SSL

Darkhotel

ASLR

SPF/DKIM, etc.

Illustration de couverture : Rachid Maraiï
Réalisation de la couverture : WIP Design
Mise en pages : Nord Compo

Le pictogramme qui figure ci-contre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du photocopillage.

Le Code de la propriété intellectuelle du 1^{er} juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements

d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour

les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.

Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du

Centre français d'exploitation du droit de copie (CFC, 20, rue des Grands-Augustins, 75006 Paris).



© Dunod, 2005, 2009, 2013, 2016
5 rue Laromiguière, 75005 Paris
www.dunod.com
ISBN 978-2-10-073883-0

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2° et 3° a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.



Table des matières

Avant-propos	1
1. Les menaces informatiques	3
Introduction aux attaques informatiques	3
Pirates informatiques	8
Méthodologie d'une attaque réseau	11
> Méthodologie globale	12
> Collecte d'informations	13
> Écoute du réseau	17
> Analyse de réseau	19
Intrusion	20
> Exploit	21
> Compromission	22
> Porte dérobée	22
Nettoyage des traces	22
La réalité des menaces	23
> Computrace et le vol de millions de mots de passe	24
> Les menaces à venir : l'Internet des objets	25
> Les plateformes mobiles	25
2. Les <i>malwares</i>	27
Virus	27
> Types de virus	28
> Éviter les virus	30
Vers réseau	31
> Principe de fonctionnement	31
> Parades	32
Chevaux de Troie	32
> Symptômes d'une infection	34

> Principe de fonctionnement	34
> Parades	35
Bombes logiques	35
<i>Spywares</i> (espionnage)	35
> Types de spywares	37
> Parades	37
<i>Ransomwares</i>	38
> Parades	39
Keyloggers	39
> Parades	39
Spam	40
> Inconvénients	41
> Parades	42
Rootkits	44
> Principe de fonctionnement	44
> Détection et parade	45
« Faux » logiciels (rogue software)	46
> Principes	46
> Parades	46
Hoax (canulars)	47
3. Les techniques d'attaque	49
Attaques de mots de passe	50
> Attaque par force brute	50
> Attaque par dictionnaire	51
> Attaque hybride	51
> L'utilisation du calcul distribué	52
> Choix des mots de passe	53
Usurpation d'adresse IP	55
> Modification de l'en-tête TCP	56
> Liens d'approbation	56
> Annihilation de la machine spoofée	59
> Prédiction des numéros de séquence	59
Attaques par déni de service	60
> Attaque par réflexion	61
> Attaque par amplification	62
> Attaque du ping de la mort	63
> Attaque par fragmentation	64
> Attaque LAND	64

> Attaque SYN	65
> Attaque de la faille TLS/SSL	66
> Attaque par <i>downgrade</i>	66
> Attaque par requêtes élaborées	67
> Parades	67
Attaques <i>man in the middle</i>	68
> Attaque par rejeu	69
> Détournement de session TCP	69
> Attaque du protocole ARP	70
> Attaque du protocole BGP	71
Attaques par débordement de tampon	71
> Principe de fonctionnement	72
> <i>Shellcode</i>	73
> Parades	73
Attaque par faille matérielle	74
> Le matériel réseau	74
> PC et appareils connectés	77
> Attaques APT (<i>Advanced Persistent Threat</i>)	79
> Attaques biométriques	80
Attaque par ingénierie sociale	81
> Réseaux sociaux	81
> Attaque par <i>watering hole</i>	82
> Aide de la voix sur IP (VoIP)	83
> Attaque par réinitialisation de mot de passe	83
> Attaque par usurpation d'identité informatique	84
4. La cryptographie	87
Introduction à la cryptographie	87
> Objectifs de la cryptographie	89
> Cryptanalyse	89
Chiffrement basique	90
> Chiffrement par substitution	90
> Chiffrement par transposition	91
Chiffrement symétrique	92
Chiffrement asymétrique	94
> Avantages et inconvénients	95
> Notion de clé de session	95
> Algorithme d'échange de clés	96

Signature électronique	97
> Fonction de hachage	97
> Vérification de l'intégrité d'un message	98
> Scellement des données	99
Certificats	99
> Structure d'un certificat	100
> Niveau de signature	102
> Types d'usages	102
Quelques exemples de cryptosystèmes	103
> Chiffre de Vigenère	103
> Cryptosystème Enigma	105
> Cryptosystème DES	108
> Cryptosystème RSA	113
> Cryptosystème PGP	114
5. Les protocoles sécurisés	119
Protocole SSL	119
Protocole SSH	122
Protocole Secure HTTP	125
Protocole SET	126
Protocole S/MIME	127
Protocole DNSsec	128
6. Les dispositifs de protection	129
Antivirus	129
> Principe de fonctionnement	129
> Détection des <i>malwares</i>	130
> Antivirus mais pas seulement	131
Système pare-feu (<i>firewall</i>)	132
> Principe de fonctionnement	133
> Pare-feu personnel	136
> Zone démilitarisée (DMZ)	136
> Limites des systèmes pare-feu	138
> <i>Honeypots</i>	139
Serveurs mandataires (proxy)	139
> Principe de fonctionnement	140
> Fonctionnalités d'un serveur proxy	140
> Translation d'adresses (NAT)	142
> <i>Reverse-proxy</i>	144

Systèmes de détection d'intrusions	145
> Techniques de détection	146
> Méthodes d'alertes	147
> Enjeu	148
Réseaux privés virtuels	149
> Fonctionnement d'un VPN	150
> Protocoles de tunnelisation	151
> Protocole PPTP	151
> Protocole L2TP	152
> Protocole SSTP	152
> Protocole IPsec	152
IPv6 et la sécurité	153
> Les améliorations apportées par IPv6	154
> Des PC directement exposés	154
> Menaces sur la vie privée	154
> Rareté = danger	154
Biométrie et carte à puce	155
> Les lecteurs d'empreintes digitales, d'iris ou vocales	155
> L'identification par cartes à puce	156
Les solutions de DLP	156
Les webapp et services de sécurité en ligne	157
> Akismet et Captcha	157
> <i>Botnet vs greenlist</i>	158
> Les pare-feu WAF	158
> Les scanners de vulnérabilités	159
La sécurité par la virtualisation	159
> Virtualisation complète	159
> Virtualisation applicative	160
La sécurité des e-mails	160
Les TPM	161
7. L'authentification	163
Principe d'authentification	163
Protocole PAP	164
Protocole CHAP	165
Protocole MS-CHAP	166
Protocole EAP	167
Protocole RADIUS	167

Protocole Kerberos	169
8. La sûreté de fonctionnement	171
Haute disponibilité	172
> Évaluation des risques	172
> Tolérance aux pannes	173
> Sauvegarde	174
> Équilibrage de charge	174
> <i>Clusters</i>	175
Technologie RAID	175
> Comparatif	180
> Mise en place d'une solution RAID	181
Sauvegarde	182
> NAS	182
> SAN	182
Protection électrique	183
> Types d'onduleurs	184
> Caractéristiques techniques	185
> Salle d'autosuffisance	185
9. La sécurité des applications web	187
Vulnérabilités des applications web	188
Falsification de données	189
Manipulation d'URL	190
> Falsification manuelle	191
> Tâtonnement à l'aveugle	191
> Traversal de répertoires	192
> Parades	193
Attaques <i>cross-site scripting</i>	194
> Conséquences	195
> Persistance de l'attaque	195
> Parades	197
Attaques par injection de commandes SQL	198
> Procédures stockées	198
> Parades	199
Attaque du mode asynchrone (Ajax)	199
> Parades	200
Le détournement de navigateur web	200
> <i>Phishing</i>	200

> <i>Tabnabbing</i>	201
> Détournement du navigateur par ajout de composants	201
> Détournement du navigateur par l'exploitation de failles	202
> Détournement de DNS	203
> <i>Click-jacking</i>	204
> Attaque par les moteurs de recherche	204
10. La sécurité des réseaux sans fil	207
<i>War driving</i>	209
Risques en matière de sécurité	209
> Interception de données	210
> Faux point d'accès	210
> Intrusion	211
> Brouillage radio	211
> Déni de service	211
Sécurisation d'un réseau sans fil	212
> Configuration des points d'accès	212
> Filtrage des adresses MAC	213
> Protocole WEP	213
> WPA	214
> 802.1x	214
> 802.11i (WPA2)	216
> Mise en place d'un réseau privé virtuel	217
> Amélioration de l'authentification	217
11. La sécurité des ordinateurs portables	219
La protection du matériel	219
> Les antivols	220
> Les systèmes de récupération	220
La protection des données	221
> Les solutions de sauvegarde	221
> Les connexions réseau	221
> Les mots de passe du disque dur	222
> Le cryptage des données	222
12. La sécurité des smartphones et des tablettes	225
Les enjeux	225
> La sécurité des différents systèmes	226

> Les appstores	227
> Droits et rootage	228
> Attaque par SMS/MMS	228
> Attaque par code QR	229
> Attaque NFC	230
13. La sécurité et le système d'information	231
Objectifs de la sécurité	231
Nécessité d'une approche globale	232
Mise en place d'une politique de sécurité	232
> Phase de définition	234
> Phase de mise en œuvre	236
> Phase de validation	236
> Phase de détection d'incidents	237
> Phase de réaction	238
14. La législation	241
Les sanctions contre le piratage	241
La sécurité des données personnelles	243
> Responsabilité concernant le propriétaire d'une connexion à Internet	244
15. Les bonnes adresses de la sécurité	247
Les sites d'informations	247
Les sites sur les failles de sécurité	248
Les sites sur les <i>malwares</i>	249
Les sites sur le <i>phishing</i>	250
Les sites sur le spam	250
Index	253



Avant-propos

Nul ne peut aujourd'hui ignorer les dangers liés à l'utilisation d'Internet : virus, spam et pirates informatiques sont les maîtres mots utilisés par les médias. Mais que connaissez-vous exactement de ces risques ?

De plus en plus de sociétés ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs et donnent l'accès à Internet à leurs employés. Quelles menaces les guettent ?

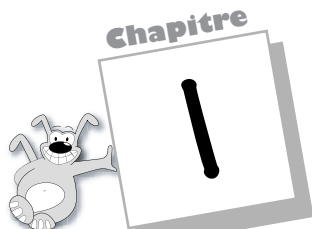
Avec le nomadisme et la multiplication des réseaux sans fil, les individus peuvent aujourd'hui se connecter à Internet à partir de n'importe quel endroit. Tout le monde s'accorde à dire qu'il existe un risque, mais quel est-il pour les particuliers et quelles peuvent en être les conséquences ?

Sur le plan professionnel, les employés sont amenés à « transporter » une partie du système d'information hors de l'infrastructure sécurisée de l'entreprise. Comment protéger les informations vitales de l'entreprise ?

Pour toutes ces raisons, à domicile comme au bureau, il est nécessaire de connaître les risques liés à l'utilisation d'Internet et les principales parades. Cet ouvrage se veut ainsi un concentré d'informations et de définitions sur tout ce qui touche à la sécurité informatique.

Remerciements

Jean-François Pillou remercie Cyrille Larrieu pour l'article sur les systèmes de détection d'intrusion et Sébastien Delsiré pour l'article concernant ENIGMA.



Les menaces informatiques

Une **menace** (*threat*) représente une action susceptible de nuire, tandis qu'une **vulnérabilité** (*vulnerability*, appelée parfois faille ou brèche) représente le niveau d'exposition face à la menace dans un contexte particulier. La **contre-mesure** (ou parade), elle, représente l'ensemble des actions mises en œuvre en prévention de la menace.

Les contre-mesures ne sont généralement pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'attention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'« ennemi ». Le but de cet ouvrage est ainsi de donner un aperçu des menaces, des motivations éventuelles des pirates, de leur façon de procéder, afin de mieux comprendre comment il est possible de limiter les risques.

Introduction aux attaques informatiques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Une **attaque** est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Sur Internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de **pirates informatiques**.

Afin de contrer ces attaques, il est indispensable de connaître les principaux types d'attaques afin de mieux s'y préparer.

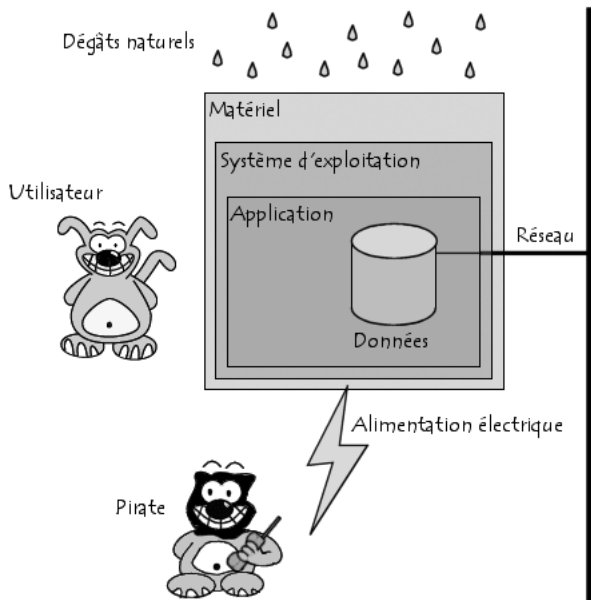
Les motivations des attaques sont de différentes sortes :

- ▶ obtenir un accès au système ;
- ▶ voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- ▶ glaner des informations personnelles sur un utilisateur ;
- ▶ récupérer des données bancaires ;
- ▶ s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- ▶ troubler le bon fonctionnement d'un service ;
- ▶ utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
- ▶ utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

❑ Types d'attaques

Les systèmes informatiques mettent en œuvre différentes composantes, allant de l'électricité pour alimenter les machines au logiciel exécuté via le système d'exploitation et utilisant le réseau.

Les **attaques** peuvent intervenir à chaque maillon de cette chaîne, pour peu qu'il existe une vulnérabilité exploitable. Le schéma suivant rappelle très sommairement les différents niveaux pour lesquels un risque en matière de sécurité existe.



Il est ainsi possible de catégoriser les risques de la manière suivante :

- ▶ **Accès physique** : il s'agit d'un cas où l'attaquant a accès aux locaux, éventuellement même aux machines :
 - coupure de l'électricité ;
 - extinction manuelle de l'ordinateur ;
 - vandalisme ;
 - ouverture du boîtier de l'ordinateur et vol de disque dur ;
 - écoute du trafic sur le réseau ;
 - ajout d'éléments (clé USB, point d'accès WiFi...).