



Comment
ça marche
.net

Jean-François PILLOU
Jean-Philippe BAY

Tout sur la Sécurité informatique

5^e édition



DUNOD

DNS blockchain

Sim swap

Meltdown et Spectre

Chiffrement
homomorphe

Phone scamming

Port knocking

ANSSI

MÉHARI

Ransomware

DNS rebinding

WPA3

Cryptomineur

ASLR

NIS/RPGD, etc.

80695-(I)-OSB90°-NOC-LAA

Dépôt légal :

Imprimerie CHIRAT – 42540 Saint-Just-la-Pendue

Imprimé en France

Directeur de collection : Jean-François Pillou

Illustration de couverture : Rachid Maraiï

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, 2020

11 rue Paul Bert, 92240 Malakoff

www.dunod.com

ISBN 978-2-10-080695-9

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2^e et 3^e 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 de la menace	23
> Ransomware et minage : la martingale du cybercrime	24
> Cyberguerre : les États à la manœuvre	25
> Obsolescence et l'Internet des objets	25
> L'institutionnalisation de la sécurité	26
> Un resserrement de la législation	26
> Intelligence artificielle : vers des malwares plus efficaces ?	27
2. Les malwares	29
Virus	29
> Types de virus	30
> Éviter les virus	32
Vers réseau	33
> Principe de fonctionnement	33
> Parades	34

Chevaux de Troie	35
> Symptômes d'une infection	36
> Principe de fonctionnement	36
> Parades	37
Bombes logiques	37
Spywares (espionciels)	38
> Types de spywares	39
> Parades	39
Ransomwares	40
> Parades	41
Keyloggers	41
> Parades	42
Spam	42
> Inconvénients	43
> Parades	44
Rootkits	46
> Principe de fonctionnement	46
> Détection et parade	47
« Faux » logiciels (<i>rogue software</i>)	48
> Principes	48
> Parades	48
Hoax (canulars)	49
3. Les techniques d'attaque	51
Attaques de mots de passe	52
> Attaque par force brute	52
> Attaque par dictionnaire	53
> Attaque hybride	53
> L'utilisation du calcul distribué	54
> Choix des mots de passe	55
Usurpation d'adresse IP	57
> Modification de l'en-tête TCP	58
> Liens d'approbation	58
> Annihilation de la machine spooftée	61
> Prédiction des numéros de séquence	61
Attaques par déni de service	62
> Attaque par réflexion	63
> Attaque par amplification	64
> Attaque du ping de la mort	66
> Attaque par fragmentation	66

> Attaque LAND	67
> Attaque SYN	67
> Attaque de la faille TLS/SSL	68
> Attaque par <i>downgrade</i>	69
> Attaque par requêtes élaborées	69
> Parades	70
Attaques <i>man in the middle</i>	70
> Attaque par jeu	71
> Détournement de session TCP	71
> Attaque du protocole ARP	72
> Attaque du protocole BGP	73
Attaques par débordement de tampon	73
> Principe de fonctionnement	74
> <i>Shellcode</i>	75
> Parades	75
Attaque par faille matérielle	76
> Le matériel réseau	76
> PC et appareils connectés	79
> Attaques APT (<i>Advanced Persistent Threat</i>)	82
> Attaques biométriques	83
Attaque par ingénierie sociale	85
> Réseaux sociaux	85
> Attaque par <i>watering hole</i>	86
> Aide de la voix sur IP (VoIP)	86
> Attaque par réinitialisation de mot de passe	87
> Attaque par usurpation d'identité informatique	89
4. La cryptographie	91
Introduction à la cryptographie	91
> Objectifs de la cryptographie	93
> Cryptanalyse	93
Chiffrement basique	94
> Chiffrement par substitution	94
> Chiffrement par transposition	95
Chiffrement symétrique	96
Chiffrement asymétrique	98
> Avantages et inconvénients	99
> Notion de clé de session	99
> Algorithme d'échange de clés	100
> Le chiffrement et le cloud	101

Signature électronique	101
> Fonction de hachage	102
> Vérification de l'intégrité d'un message	103
> Scellement des données	103
Certificats	104
> Structure d'un certificat	105
> Niveau de signature	107
> Types d'usages	107
Quelques exemples de cryptosystèmes	108
> Chiffre de Vigenère	108
> Cryptosystème Enigma	109
> Cryptosystème DES	112
> Cryptosystème RSA	117
> Cryptosystème PGP	118
5. Les protocoles sécurisés	123
Protocole SSL	123
Protocole SSH	126
Protocole Secure HTTP	129
Protocole SET	130
Protocole S/MIME	131
Protocole DNSsec	132
6. Les dispositifs de protection	133
Gestion des utilisateurs	133
> Moindre privilège et « 4 yeux »	134
> Listes de contrôle d'accès	135
Gestion des mots de passe	135
> Robustesse et capacité humaine	135
> Stockage, hachage et salage	136
> Découpage des nouveaux mots de passe	137
Gestion des programmes	137
Antivirus	138
> Principe de fonctionnement	138
> Détection des <i>malwares</i>	138
> Antivirus mais pas seulement	139
Système pare-feu (<i>firewall</i>)	140
> Principe de fonctionnement	141

> Pare-feu personnel	145
> Zone démilitarisée (DMZ)	145
> Limites des systèmes pare-feu	147
> <i>Honeypots</i>	147
Serveurs mandataires (proxys)	148
> Principe de fonctionnement	148
> Fonctionnalités d'un serveur proxy	149
> Translation d'adresses (NAT)	150
> <i>Reverse-proxy</i>	153
Systèmes de détection d'intrusions	153
> Techniques de détection	155
> Méthodes d'alertes	156
> Enjeu	157
Réseaux privés virtuels	157
> Fonctionnement d'un VPN	158
> Protocoles de tunnelisation	159
> Protocole PPTP	160
> Protocole L2TP	160
> Protocole SSTP	161
> Protocole IPSec	161
IPv6 et la sécurité	162
> Les améliorations apportées par IPv6	162
> Des PC directement exposés	162
> Menaces sur la vie privée	163
> Rareté = danger	163
Biométrie et carte à puce	163
> Les lecteurs d'empreintes digitales, d'iris ou vocales	163
> L'identification par cartes à puce	164
Les solutions de DLP	165
Les webapps et services de sécurité en ligne	165
> Akismet et Captcha	165
> <i>Botnet vs greenlist</i>	166
> Les pare-feu WAF	166
> Les scanners de vulnérabilités	167
La sécurité par la virtualisation	167
> Virtualisation complète	168
> Virtualisation applicative	168
La sécurité des e-mails	168
Les TPM	169

7. L'authentification	171
Principe d'authentification	171
Protocole PAP	172
Protocole CHAP	173
Protocole MS-CHAP	174
Protocole EAP	175
Protocole RADIUS	175
Protocole Kerberos	177
L'authentification distribuée : la blockchain	179
> Blockchain : des paquets authentifiés sans tiers de confiance	179
> De l'utilité de la blockchain dans l'authentification : le cas des DNS	180
> La chaîne pour les certificats	180
L'authentification multi-facteurs (MFA)	181
> Authentification par SMS	182
Analyse du contexte et analyse comportementale	182
8. La sûreté de fonctionnement	185
Haute disponibilité	186
> Évaluation des risques	186
> Tolérance aux pannes	187
> Sauvegarde	188
> Équilibrage de charge	188
> <i>Clusters</i>	189
Technologie RAID	189
> Comparatif	194
> Mise en place d'une solution RAID	195
Sauvegarde	196
> NAS	196
> SAN	196
Protection électrique	197
> Types d'onduleurs	198
> Caractéristiques techniques	199
> Salle d'autosuffisance	199
9. La sécurité des applications web	201
Vulnérabilités des applications web	202

Falsification de données	203
Manipulation d'URL	204
> Falsification manuelle	205
> Tâtonnement à l'aveugle	205
> Traversement de répertoires	206
> Parades	207
Attaques <i>cross-site scripting</i>	208
> Conséquences	209
> Persistance de l'attaque	209
> Parades	211
Attaques <i>cross-site request forgery</i>	212
> Parades	212
Attaques par injection de commandes SQL	213
> Procédures stockées	213
> Parades	214
Attaque du mode asynchrone (Ajax)	214
> Parades	215
Le détournement de navigateur web	215
> <i>Phishing</i>	215
> <i>Tabnabbing</i>	216
> Détournement du navigateur par ajout de composants	216
> Détournement du navigateur par l'exploitation de failles	217
> Détournement de DNS	218
> <i>Click-jacking</i>	219
> Attaque par DNS rebinding	219
> Parades	220
> Attaque sur les API	220
> Parades	221
> Attaque par les moteurs de recherche	222
10. La sécurité des réseaux sans fil	225
<i>War driving</i>	227
Risques en matière de sécurité	227
> Interception de données	228
> Faux point d'accès (attaque evil twin)	228
> Intrusion	229
> Brouillage radio	229
> Déni de service	229
Sécurisation d'un réseau sans fil	230
> Configuration des points d'accès	230

> Filtrage des adresses MAC	231
> Protocole WEP	231
> WPA	232
> 802.1x	232
> 802.11i (WPA2)	234
> WPA2 : la sécurité qui a fait Krack	235
> Protocole WPA3	236
> Mise en place d'un réseau privé virtuel	237
> Amélioration de l'authentification	237

11. La sécurité des ordinateurs portables **239**

La protection du matériel	239
> Les antivols	240
> Les systèmes de récupération	240
La protection des données	241
> Les solutions de sauvegarde	241
> Les connexions réseau	241
> Les mots de passe du disque dur	242
> Le cryptage des données	242

12. La sécurité des smartphones et des tablettes **245**

Les enjeux	245
La sécurité des différents systèmes	246
> Les stores d'applis	247
> Droits et rootage	247
Les attaques	248
> Attaque par SMS/MMS	248
> Attaque par code QR	249
> Attaque NFC	249
> Le paiement par téléphone	250

13. La sécurité et le système d'information **251**

Objectifs de la sécurité	251
Nécessité d'une approche globale	252
Mise en place d'une politique de sécurité	252
> Phase de définition	254
> Phase de mise en œuvre	256
> Phase de validation	256

> Phase de détection d'incidents	257
> Phase de réaction	258
> Les méthodes d'évaluation du risque EBIOS et MÉHARI	260
> EBIOS	260
> MÉHARI	261
14. La législation	263
Les sanctions contre le piratage	263
La sécurité des données personnelles	265
> Le Règlement général sur la protection des données (RGPD)	265
> La directive Network & Internet Security (NIS) et le Cybersecurity Act	268
> Responsabilité concernant le propriétaire d'une connexion à Internet	269
15. Structures et institutions de la sécurité informatique	271
Les institutions internationales	273
> Le FIRST	273
> MITRE	274
> L'ENISA	274
> L'EC3	274
> Le SANS	275
Les institutions françaises	276
> L'ANSSI	276
> Les CERT français	276
> Les autres structures : CLUSIF, OSSIR	277
16. Les bonnes adresses de la sécurité	279
Les sites d'informations	279
Les sites sur les failles de sécurité	280
Les sites sur les <i>malwares</i>	281
Les sites sur le <i>phishing</i>	282
Les sites sur le spam	283
Index	284



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 ?

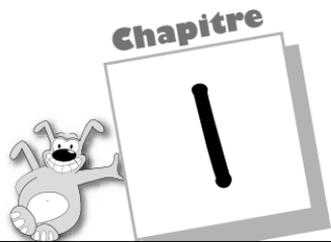
Avec le nomadisme et la multiplication des réseaux sans fil, les individus peuvent aujourd'hui se connecter à Internet à partir de n'importe quel endroit. Tout le monde s'accorde à dire qu'il existe un risque, mais quel est-il pour les particuliers et quelles peuvent en être les conséquences ?

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 Delsirie 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.

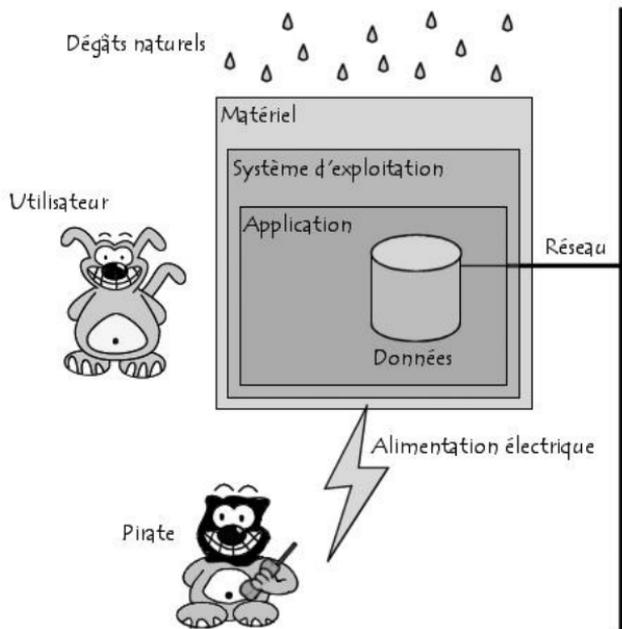
Les motivations des attaques sont de différentes sortes :

- 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...).

- **Interception de communications :**
 - vol de session (*session hijacking*) ;
 - usurpation d'identité ;
 - détournement ou altération de messages.
- **Dénis de service :** il s'agit d'attaques visant à perturber le bon fonctionnement d'un service. On distingue habituellement les types de déni de service suivant :
 - exploitation de faiblesses des protocoles TCP/IP ;
 - exploitation de vulnérabilité des logiciels serveurs.
- **Intrusions :**
 - balayage de ports ;
 - élévation de privilèges : ce type d'attaque consiste à exploiter une vulnérabilité d'une application en envoyant une requête spécifique, non prévue par son concepteur, ayant pour effet un comportement anormal conduisant parfois à un accès au système avec les droits de l'application. Les attaques par **débordement de tampon** (*buffer overflow*) utilisent ce principe ;
 - maliciels (virus, vers et chevaux de Troie).
- **Ingénierie sociale :** dans la majeure partie des cas le maillon faible est l'utilisateur lui-même ! En effet, c'est souvent lui qui, par méconnaissance ou par duperie, va ouvrir une brèche dans le système, en donnant des informations (mot de passe par exemple) au pirate informatique ou en exécutant une pièce jointe. Ainsi, aucun dispositif de protection ne peut protéger l'utilisateur contre les arnaques, seuls le bon sens, la raison et un peu d'informations sur les différentes pratiques peuvent lui éviter de tomber dans le piège ! La montée en puissance des réseaux sociaux sur le Web a donné encore plus d'importance à ce type d'attaque (voir chap. 3, *Attaque par ingénierie sociale*).
- **Trappes :** il s'agit d'une porte dérobée (*backdoor*) dissimulée dans un logiciel, permettant un accès ultérieur à son concepteur.

Pour autant, les erreurs de programmation contenues dans les programmes sont habituellement corrigées assez rapidement par leur concepteur dès lors que la vulnérabilité a été publiée. Il appartient alors aux administrateurs (ou utilisateurs personnels avertis) de se tenir informé des mises à jour des programmes qu'ils utilisent afin de limiter les risques d'attaques.

D'autre part il existe un certain nombre de dispositifs (pare-feu, systèmes de détection d'intrusions, antivirus) permettant d'ajouter un niveau de sécurisation supplémentaire.

❑ Effort de protection

La sécurisation d'un système informatique est généralement dite **asymétrique**, dans la mesure où le pirate n'a qu'à trouver une seule vulnérabilité pour compromettre le système, tandis que l'administrateur se doit de corriger toutes les failles.

❑ Attaques par rebond

Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les **attaques par rebond** (par opposition aux **attaques directes**), consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui (telle que son adresse IP) et dans le but d'utiliser les ressources de la machine servant de rebond.

Cela montre l'intérêt de protéger son réseau ou son ordinateur personnel, il est possible de se retrouver « complice » d'une attaque et en cas de plainte de la victime, la première personne interrogée sera le propriétaire de la machine ayant servi de rebond.



Attention !

Avec le développement des réseaux sans fil, ce type de scénario risque de devenir de plus en plus courant car lorsque le réseau sans fil est mal sécurisé, un pirate situé à proximité peut l'utiliser pour lancer des attaques !

Pirates informatiques

❑ Qu'est-ce qu'un hacker ?

Le terme **hacker** est souvent utilisé pour désigner un pirate informatique. Les victimes de piratage sur des réseaux informatiques aiment à penser qu'ils ont été attaqués par des pirates chevronnés ayant soigneusement étudié leur système et ayant développé des outils spécifiquement pour en exploiter les failles.

Le terme hacker a eu plus d'une signification depuis son apparition à la fin des années 1950. À l'origine ce nom désignait d'une façon méliorative les programmeurs émérites, puis il servit au cours des années 1970 à décrire les révolutionnaires de l'informatique, qui pour la plupart sont devenus les fondateurs des plus grandes entreprises informatiques.

C'est au cours des années 1980 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.

Aujourd'hui, ce mot est souvent utilisé à tort pour désigner les personnes s'introduisant dans les systèmes informatiques.

❑ Types de pirates

En réalité, il existe de nombreux types d'**attaquants** catégorisés selon leur expérience et selon leurs motivations :

- Les **white hat hackers**, hackers au sens noble du terme, dont le but est d'aider à l'amélioration des systèmes et technologies informatiques, sont généralement à l'origine des principaux protocoles et outils informatiques que nous utilisons aujourd'hui. Les objectifs des *white hat hackers* sont en règle générale un des suivants :
 - l'apprentissage ;
 - l'optimisation des systèmes informatiques ;
 - la mise à l'épreuve des technologies jusqu'à leurs limites afin de tendre vers un idéal plus performant et plus sûr.
- Les **black hat hackers**, plus couramment appelés **pirates informatiques**, c'est-à-dire des personnes s'introduisant

dans les systèmes informatiques dans un but nuisible. Les motivations des *black hat hackers* peuvent être multiples :

- l'attrait de l'interdit ;
 - l'intérêt financier ;
 - l'intérêt politique ;
 - l'intérêt éthique ;
 - le désir de la renommée ;
 - la vengeance ;
 - l'envie de nuire (détruire des données, empêcher un système de fonctionner).
- Les **script kiddies** (traduisez « gamins du script », parfois également surnommés **crashers**, **lamers** ou encore **packet monkeys**, soit « les singes des paquets réseau ») sont de jeunes utilisateurs du réseau utilisant des programmes trouvés sur Internet, généralement de façon maladroite, pour vandaliser des systèmes informatiques afin de s'amuser.
- Les **phreakers** sont des pirates s'intéressant au réseau téléphonique commuté (RTC) afin de téléphoner gratuitement grâce à des circuits électroniques (qualifiés de **box**, comme la *blue box*, la *violet box*...) connectés à la ligne téléphonique dans le but d'en falsifier le fonctionnement. On appelle ainsi **phreaking** le piratage de ligne téléphonique. Ce type de pirate connaît un renouveau avec l'accroissement de l'utilisation de la voix sur IP (VoIP) comme moyen de transport des communications téléphoniques grand public (voir chap. 3, *Attaque par ingénierie sociale*).
- Les **carders** s'attaquent principalement aux systèmes de cartes à puce (en particulier les cartes bancaires) pour en comprendre le fonctionnement et en exploiter les failles. Le terme **carding** désigne le piratage de cartes à puce.
- Les **crackers** ne sont pas des biscuits apéritifs au fromage mais des personnes dont le but est de créer des outils logiciels permettant d'attaquer des systèmes informatiques ou de casser les protections contre la copie des logiciels payants. Un **crack** est ainsi un programme créé exécuté

table chargé de modifier (**patcher**) le logiciel original afin d'en supprimer les protections.

- Les **hacktivistes** (contraction de hackers et activistes que l'on peut traduire en **cybermilitant** ou **cyberrésistant**) sont des hackers dont la motivation est principalement idéologique. Ce terme a été largement porté par la presse, aimant à véhiculer l'idée d'une communauté parallèle (qualifiée généralement d'*underground*, par analogie aux populations souterraines des films de science-fiction).

Ce qu'il faut retenir, c'est que, depuis la fin des années 2000, on a vu une professionnalisation du secteur de l'insécurité. Des organisations criminelles se sont mises en place et utilisent les outils de piratage pour gagner de l'argent¹. Comme exemple de cette structuration, on peut citer :

- les réseaux de machines piratées (*botnet*) que l'on peut louer pour des activités illégales (*spamming*, *phishing*...) ;
- les sites d'enchères de failles de sécurité ;
- la vente de pack de *malware*, de listing de données sensibles (numéros de carte bancaire...) ;
- l'automatisation du cybersquattage ;
- le rançonnement d'entreprises avec pour moyen de pression des attaques DDoS ou le cryptage de données par des *malwares*.

❑ La culture du « Z »

Voici un certain nombre de définitions propres au milieu *underground* :

- **Warez** : piratage de logiciels.
- **Appz** (contraction de *applications* et *warez*) : piratage d'applications.
- **Gamez** (contraction de *games* et *warez*) : piratage de jeux vidéo.

1. Un aperçu des *black markets* par Symantec : <https://symc.ly/2DgDHjy>

- > **Serialz** [contraction de *serials* et *warez*] : il s'agit de numéros de série permettant d'enregistrer illégalement des copies de logiciels commerciaux.
- > **Crackz** [contraction de *cracks* et *warez*] : ce sont des programmes écrits par des *crackers*, destinés à supprimer de manière automatique les systèmes de protection contre la copie des applications commerciales.

❑ Le langage « C0wb0y »

Les adeptes de la communication en temps réel (IRC, chat, messagerie instantanée) se sont sûrement déjà retrouvés engagés dans une discussion avec un utilisateur s'exprimant dans une langue peu commune, dans laquelle les voyelles sont remplacées par des chiffres.

Ce langage, particulièrement utilisé par les *scripts kiddies* dans le milieu underground, se nomme le **langage « c0wb0y »**. Il consiste à remplacer certaines lettres (la plupart du temps des voyelles) par des chiffres afin de donner une impression aux interlocuteurs d'une certaine maîtrise des technologies et des techniques de *hacking*.

Exemple

Voici quelques substitutions possibles :

E=3, A=4, B=8, O=0, N=^, l=|

Voici ce que cela donne sur des mots courants :

Abeille = 4B3||l3

Tomate = T0m4t3

Méthodologie d'une attaque réseau

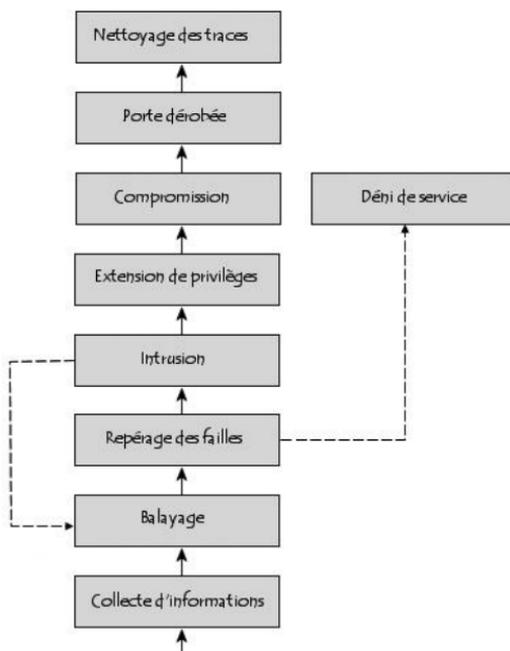
Ce paragraphe a pour vocation d'expliquer la méthodologie généralement retenue par les pirates pour s'introduire dans un système informatique ainsi que les principales techniques utilisées. Il ne vise en aucun cas à expliquer comment compromettre un système mais à comprendre la façon dont il peut l'être afin de mieux pouvoir s'en prémunir.

En effet, la meilleure façon de protéger son système est de procéder de la même manière que les pirates afin d'être en mesure d'identifier les vulnérabilités du système. Ainsi cette

section ne donne aucune précision sur la manière dont les failles sont exploitées, mais explique comment les détecter et les corriger.

Méthodologie globale

Le schéma suivant récapitule la méthodologie complète.



Les hackers ayant l'intention de s'introduire dans les systèmes informatiques recherchent dans un premier temps des **failles**, c'est-à-dire des **vulnérabilités** nuisibles à la sécurité du système, dans les protocoles, les systèmes d'exploitations, les applications ou même le personnel d'une organisation ! Les termes de **vulnérabilité**, de **brèche** ou en langage plus familier de **trou de sécurité** (*security hole*) sont également utilisés pour désigner les failles de sécurité.

Pour pouvoir mettre en œuvre un **exploit** (il s'agit du terme technique signifiant « exploiter une vulnérabilité »), la première étape du