Jean-François PILLOU
Jean-Philippe BAY

Comment ça marche .net

Tout sur la Sécurité informatique

5e 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.

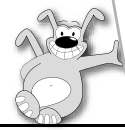
80695-(I)-OSB90°-NOC-LAA
Dépôt légal :
Imprimerie CHIRAT – 42540 Saint-Just-la-Pendue
Imprimé en France

Directeur de collection : Jean-François Pillou

Illustration de couverture : Rachid Maraï

11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-080695-9

Table des matières



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 ?

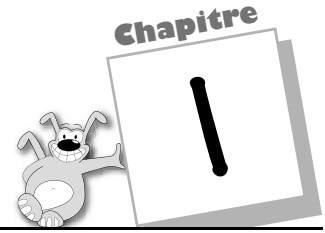
Avec le nomadisme et la multiplication des réseaux sans fil, les individus peuvent aujourd'hui se connecter à Internet à partir de n'importe quel endroit. Tout le monde s'accorde à dire qu'il existe un risque, mais quel est-il pour les particuliers et quelles peuvent en être les conséquences ?

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.

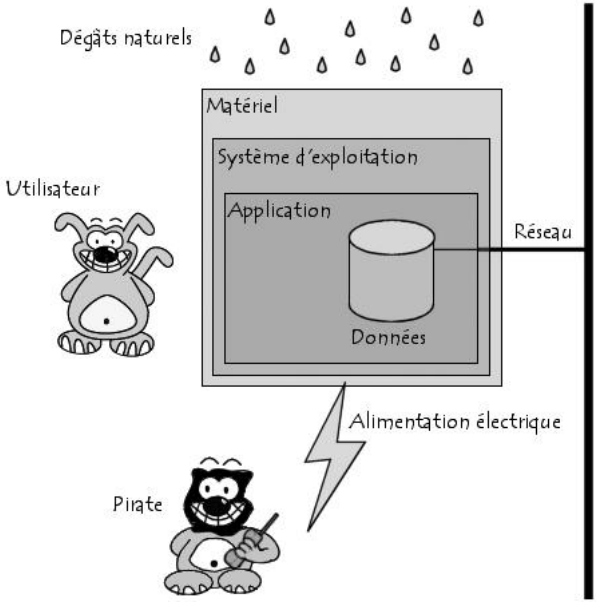
Les motivations des attaques sont de différentes sortes :

- 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 à 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 ingéniérie 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 compromette 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 ingéniérie 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 exécu-

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'argent[1]. 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 rançonnage 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=/\/, I=|

Voici ce que cela donne sur des mots courants :
Abeille = 4B3|ll3
Tomate = T0m4t3

Méthodologie d'une attaque réseau

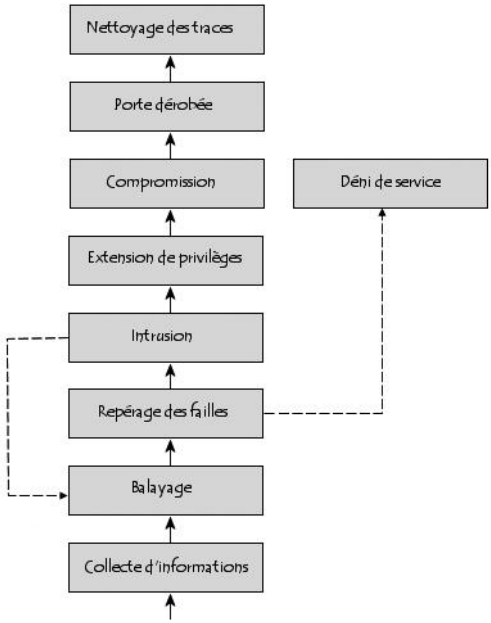
Ce paragraphe a pour vocation d'expliquer la méthodologie généralement retenue par les pirates pour s'introduire dans un système informatique ainsi que les principales techniques utilisées. Il ne vise en aucun cas à expliquer comment compromettre un système mais à comprendre la façon dont il peut l'être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