0x100

Introduction

Le hacking véhicule souvent des images de vandalisme électronique, d'espionnage, de cheveux décolorés et de piercings corporels. De nombreuses personnes associent le hacking au non-respect des lois et supposent que quiconque s'engage dans cette activité est un criminel. Il faut bien l'admettre, certains hackers enfreignent les lois. Cependant, ce n'est absolument pas l'objectif sous-jacent du hacking, qui a plutôt tendance à respecter les règles. Par essence, le hacking est une activité qui vise à découvrir des utilisations non intentionnelles ou sous-estimées des règles et des propriétés d'une situation précise, puis à les appliquer dans de nouvelles façons novatrices de résoudre un problème, quel qu'il soit.

Le problème suivant illustre l'essence du hacking :

> *Employez chacun des chiffres 1, 3, 4 et 6 une seule fois avec les quatre opérations mathématiques de base (addition, soustraction, multiplication et division) pour obtenir 24. Chaque chiffre ne doit servir qu'une seule fois et vous pouvez définir l'ordre des opérations ; par exemple, 3 * (4 + 6) + 1 = 31 est valide, mais incorrect puisque le résultat est différent de 24.*

Les règles de ce problème sont parfaitement définies et simples, mais la réponse en élude plusieurs. Comme la solution de ce problème (donnée à la fin du livre), les solutions employées par les hackers suivent les règles du système, mais d'une manière qui va à l'encontre des intuitions. C'est là toute la particularité des hackers : ils résolvent des problèmes de manière inimaginable par ceux qui restent confinés dans des méthodes et des pensées conventionnelles.

Depuis les débuts de l'informatique, les hackers résolvent des problèmes de manière très créative. À la fin des années 1950, le club de modélisme ferroviaire du MIT a reçu du matériel en donation, principalement du vieil équipement téléphonique. Les membres du club l'ont utilisé pour monter un système complexe qui permettait à plusieurs opérateurs de contrôler différentes parties du réseau en appelant les sections correspondantes. Ils ont appelé *hacking* cette utilisation nouvelle et innovante de l'équipement téléphonique ; de nombreuses personnes les considèrent comme les hackers originels. Ensuite, ce groupe est passé à la programmation sur cartes perforées et sur bandes de téléscripteur pour les premiers ordinateurs, comme l'IBM 704 et le TX-0. Alors que certains se satisfaisaient d'écrire des programmes

qui résolvaient simplement des problèmes, les premiers hackers avaient pour obsession d'écrire des programmes qui résolvaient des problèmes *bien*. Un nouveau programme pouvait obtenir le même résultat qu'un autre existant, mais le fait de demander moins de cartes perforées faisait qu'il était meilleur, même si le résultat était identique. Le point essentiel résidait dans la manière dont le programme obtenait ses résultats – une question d'élégance.

Être capable de réduire le nombre de cartes perforées nécessaires à un programme montrait une maîtrise artistique de l'ordinateur. Sur une table finement ouvragée, vous pouvez parfaitement trouver un vase ou une bouteille de lait, l'un étant sans conteste plus joli que l'autre. Les premiers hackers ont prouvé que des problèmes techniques pouvaient avoir des solutions artistiques, et la programmation est ainsi passée d'une simple tâche d'ingénieur à une forme d'art.

Comme beaucoup d'autres arts, le hacking a souvent été mal compris. Le peu de gens qui l'ont compris ont formé un phénomène culturel secondaire informel, principalement focalisé sur l'apprentissage et la maîtrise de leur art. Ils pensaient que l'information devait être gratuite et que tout ce qui entravait cette liberté devait être contourné. Parmi ces obstacles figuraient les symboles de l'autorité, la bureaucratie de l'enseignement supérieur et la discrimination. Dans un environnement d'étude axé sur les diplômes, ce groupe officieux de hackers défiait les objectifs classiques et recherchait uniquement la connaissance. Cette volonté permanente d'apprendre et d'explorer franchissait même les barrières conventionnelles dressées par la discrimination, ce qui est apparu évident avec l'arrivée de Peter Deutsch, alors âgé de 12 ans, dans le club de modélisme ferroviaire du MIT, lorsqu'il a montré ses connaissances du système TX-0 et son désir d'apprendre. L'âge, la race, le genre, l'apparence, les diplômes et la classe sociale ne constituaient pas un critère de jugement de la valeur d'une autre personne – pas par volonté d'égalité, mais par simple désir de faire avancer l'art émergeant du hacking.

Les premiers hackers ont trouvé splendeur et élégance dans les sciences généralement arides des mathématiques et de l'électronique. Ils ont vu la programmation comme une forme d'expression artistique et l'ordinateur comme un instrument de cet art. Leur volonté de disséquer et de comprendre n'avait pas pour objectif de démystifier des efforts artistiques ; il s'agissait simplement d'un moyen d'en obtenir une meilleure appréciation. Ces valeurs axées sur la connaissance finirent par constituer l'Éthique du hacker : la reconnaissance d'une logique comme une forme d'art et la promotion de la circulation libre des informations, en surmontant les barrières conventionnelles et les restrictions dans le simple but de mieux comprendre le monde. Il ne s'agissait pas d'une nouvelle tendance culturelle ; dans la Grèce antique, les pythagoriciens avaient une éthique et une culture semblables, même sans ordinateur. Ils ont vu la beauté des mathématiques et ont découvert de nombreux concepts fondamentaux en géométrie. Cette soif de connaissance et ses effets secondaires bénéfiques se sont perpétués au cours de l'histoire, des pythagoriciens aux hackers du club de modélisme ferroviaire du MIT en passant par Ada Lovelace et Alan Turing. Les hackers d'aujourd'hui, comme Richard Stallman et Steve Wozniak, ont poursuivi l'héritage du hacking, en nous apportant des systèmes d'exploitation modernes, des langages

de programmation, des ordinateurs personnels et bien d'autres technologies que nous utilisons quotidiennement.

Comment pouvons-nous distinguer ces bons hackers, qui nous apportent toutes ces avancées technologiques, des mauvais hackers, qui volent nos numéros de carte bancaire ? Le terme *cracker* est apparu pour permettre cette distinction. Les journalistes ont été informés que les crackers étaient les mauvais garçons, tandis que les hackers étaient les gentils. Les hackers restaient fidèles à leur éthique, tandis que les crackers étaient seulement intéressés par enfreindre les lois et gagner rapidement de l'argent. Les crackers étaient considérés comme beaucoup moins talentueux que les hackers, car ils utilisaient simplement des outils et des scripts écrits par des hackers sans en comprendre le fonctionnement. Le terme *cracker* devait désigner tous ceux qui utilisaient un ordinateur pour des actions malveillantes — pirater des logiciels, dégrader des sites Web et, pire encore, ne pas comprendre ce qu'ils faisaient. Malheureusement, peu de gens emploient ce terme aujourd'hui.

Son manque d'adoption était peut-être lié à son étymologie – *cracker* désignait à l'origine les personnes qui craquaient les logiciels et retiraient les protections contre la copie. Son absence de popularité actuelle vient sans doute de ses deux nouvelles définitions ambiguës : un groupe de personnes qui sont engagées dans des activités illégales avec des ordinateurs ou des personnes qui sont de relativement piètres hackers. Peu de journalistes techniques se sentent obligés d'employer des termes que la majorité de leurs lecteurs ne maîtrise pas. *A contrario*, la plupart des gens connaissent le mystère et le talent qui entourent le terme *hacker.* Par conséquent, pour un journaliste, le choix d'employer le terme *hacker* est facile. De manière similaire, l'expression *script kiddie* (pirates informatiques néophytes) est parfois employée pour faire référence à des crackers, mais elle n'a pas le même impact que le vague *hacker.* Certains défendent encore l'idée qu'il existe une ligne de séparation entre les hackers et les crackers. Pour ma part, je pense que quiconque possède un esprit de hacker est un hacker, quelles que soient les règles qu'il peut enfreindre.

Les lois actuelles, qui restreignent les recherches en matière de cryptographie, rendent la frontière entre les hackers et les crackers encore plus floue. En 2001, le professeur Edward Felten et son équipe de l'université de Princeton allaient publier un article concernant la faiblesse de différents systèmes de marquage numérique. Cet article répondait à un défi lancé par SDMI (*Secure Digital Music Initiative*), qui encourageait le public à tenter de casser ses modèles de marquage. Cependant, avant que Felten et son équipe ne puissent publier leur article, ils ont été menacés par la fondation SDMI et la RIAA (*Recording Industry Association of America*). Le DCMA[1] (*Digital Millennium Copyright Act*) de 1998 interdit toute présentation ou fourniture d'une technologie qui pourrait servir à contourner la propriété industrielle. Cette même loi a été utilisée contre Dmitry Sklyarov, un programmeur et hacker russe, quand il a écrit un logiciel qui contournait le chiffrement simpliste d'un logiciel Adobe et a présenté ses trouvailles à une convention de hackers aux États-Unis.

1. NdT : son équivalent européen est l'EUCD et la transcription en France est la loi DADVSI, qui a été adoptée en juillet 2006 (source Wikipedia).

Le FBI est intervenu et l'a interpellé, déclenchant une longue bataille juridique. Selon la loi, la complexité des protections industrielles n'a pas d'importance – il serait techniquement illégal de procéder à une rétro-ingénierie du Louchébem, et même d'en discuter, si cet argot était utilisé pour une protection industrielle. À présent, qui sont les hackers et qui sont les crackers ? Lorsque des lois semblent interférer avec la liberté d'expression, les gentils qui expriment leur avis deviennent-ils soudainement des méchants ? Je pense que l'esprit du hacker transcende les lois de l'État, qui ne le définissent pas.

La physique nucléaire et la biochimie peuvent servir à tuer, mais elles nous apportent également des avancées scientifiques significatives et la médecine moderne. En soi, il n'y a rien de bon ou de mal dans la connaissance ; la moralité se trouve dans l'application du savoir. Nous savons comment convertir de la matière en énergie et, même si nous le voulions, rien ne pourrait nous retirer cette connaissance, comme rien ne peut arrêter le progrès technologique permanent de la société. De la même manière, l'esprit du hacker ne pourra jamais être bloqué ni facilement classifié ou disséqué. Les hackers continueront à repousser les limites de la connaissance et du comportement acceptable, en nous forçant à toujours explorer plus loin.

Tout cela a pour conséquence, entre autres, une évolution bénéfique de la sécurité, au travers d'une compétition entre les hackers assaillants et les hackers défenseurs. Tout comme la rapide gazelle s'est adaptée à la course du guépard et que celui-ci est devenu encore plus rapide en chassant la gazelle, la compétition entre les hackers apporte aux utilisateurs des ordinateurs une sécurité meilleure et plus robuste, ainsi que des techniques d'attaque plus complexes et plus sophistiquées. L'arrivée et le développement des systèmes de détection d'intrusion (IDS, *Intrusion Detection Systems*) est un exemple de ce processus d'évolution parallèle. Les défenseurs ont ajouté des IDS à leur arsenal, tandis que les assaillants ont développé des techniques pour échapper aux IDS, ce qui a conduit à des produits IDS bien meilleurs. Le résultat de ces interactions est positif : les personnes deviennent plus intelligentes, la sécurité s'améliore, les logiciels sont plus stables, des techniques de résolution de problèmes novatrices sont imaginées et une nouvelle économie apparaît même.

L'objectif de cet ouvrage est de vous enseigner le véritable esprit du hacking. Nous examinerons plusieurs techniques de hackers, qu'elles soient passées ou actuelles, en les disséquant afin de comprendre comment et pourquoi elles fonctionnent. Une image ISO contenant un environnement de programmation complet déjà configuré ainsi que l'ensemble des codes présentés dans cet ouvrage est disponible sur le site Pearson à la page dédiée à ce livre dans la librairie en ligne. L'exploration et l'innovation sont des composantes essentielles du hacking. Cet environnement vous permettra d'expérimenter vous-même les exemples. Vous pouvez utiliser cette image ISO comme un Live CD, après l'avoir gravée sur un support CD vierge, sur votre système habituel, sans risque de dommage pour ce dernier. Afin d'éviter cette étape de gravure, il est également possible de l'utiliser comme disque d'amorçage d'une machine virtuelle Linux (Ubuntu) créé à l'aide des logiciels Virtual Box ou VMWare (selon votre préférence). Dans les deux cas, cet environnement Linux ne perturbera pas votre système installé. Une fois vos expérimentations terminées,

redémarrez votre machine en retirant le CD-ROM si vous avez opté pour l'option Live CD ou arrêtez simplement votre logiciel de virtualisation (VMWare ou Virtual Box) si vous avez choisi une installation de ce type.

Vous allez comprendre et apprécier le hacking, peut-être améliorer des techniques existantes, voire inventer les vôtres. Nous espérons que cet ouvrage réveillera la curiosité du hacker qui sommeille en vous et vous permettra de contribuer à l'art du hacking, quel que soit le côté de la barrière que vous choisirez.