Le piratage éthique

Séverin Messiaen

PACE - Télécom Paris

Table des matières

Qu’est-ce qu’un hacker ?

En France, le terme « hacker » a plutôt une connotation péjorative auprès du grand public. Souvent associé à des actes illégaux, ce terme est régulièrement utilisé comme un synonyme de « pirate informatique ». Pourtant, ce terme d’origine anglaise est loin de porter en lui cette notion d’illégalité. De fait, ce terme tire plutôt son origine du mot *hack* en anglais, définit comme « une stratégie ou une technique que vous utilisez pour gérer une activité de manière plus efficace. »[1] (Oxford Learner's Dictionaries).

Ainsi, Jon Erickson écrit en 2017 qu’il considère que des étudiants du club de modélisme ferroviaire du MIT en 1950, qui ont utilisé du vieil équipement téléphonique qui leur avait été donné pour mettre en place des aiguillages télécommandés, font partie des hackers originels. De même, les chercheurs optimisant à l’époque leurs programmes informatiques au maximum afin d’utiliser le minimum de cartes perforées, quitte à rendre leur travail moins intelligible, sont pour lui à l’origine du terme « hacking ».

A l’origine, un hacker n’est donc ni un criminel ni un individu malintentionné, mais une personne curieuse qui aime explorer la limite des règles définies par un protocole, par un langage informatique, ou par la configuration d’un pare-feu. Par ailleurs, la recommandation de l’académie française pour échapper à cet anglicisme si courant est « fouineur », et si cela ne semble toujours pas suffisamment représentatif de ce qu’englobe le terme « hacker », cette recommandation reste tout de même bien plus adaptée que « pirate informatique ».

[1] Traduction libre

Pour autant, la mauvaise réputation que s'est faîte le hacking auprès du grand public est loin d'être incompréhensible, car on ne peut pas nier que certains hackers usent de leurs talents pour commettre des crimes qui choquent l'opinion publique, tels que la compromissions de systèmes de sécurité d'hôpitaux par exemple. Il serait donc faux de dire que tous les hackers sont de gentils informaticiens concevant la programmation comme un art, et de nouvelles dénominations ont donc été créés afin de pouvoir mieux catégoriser les différents types de hackers.

En particulier, le terme « cracker » désigne les individus malintentionnés qui utilisent leurs connaissances informatiques pour exploiter des vulnérabilités dans des systèmes d'information. On les désigne parfois par le terme « black-hat », par opposition au terme « white-hat » qui désigne des hackers ayant un comportement similaire aux *crackers*, mais qui agissent en toute légalité, afin de tester les défenses d'une entreprise par exemple.

On retiendra les deux définitions suivantes[2] données dans la RFC 1392, qui tente d'établir un « glossaire de l'internaute » :

> Hacker : Une personne qui se plaît à avoir une compréhension étroite des fonctionnement interne d'un système, des ordinateurs et des réseaux informatiques en particulier. Ce terme est souvent utilisé à tort dans un contexte péjoratif, alors que « cracker » serait le terme correct.
>
> Cracker : Un cracker est un individu qui tente d'accéder à des systèmes informatiques sans autorisation. Ces individus sont souvent malveillants, par opposition aux hackers, et disposent de nombreux moyens pour s'introduire dans un système.

(G. Malkin, Xylogics, Inc. & T. LaQuey Parker, 1993)

[2] Traduction Libre

Le hacking : un seul outil pour différents profils de hackers

Les hackers maîtrisent l'informatique à la perfection, à tel point que certains savent faire du hacking une arme redoutablement efficace. Nous avons pourtant vu que la majorité des hackers n'étaient pas des hors-la-loi, et que pour la plupart, c'est avant tout par passion qu'ils excellent dans ce domaine. Ainsi, le hacking est surtout un outil que chacun choisi d'utiliser à sa manière. Au contraire des *crackers*, certains préfèrent utiliser leurs compétences à des fins bienveillantes, même si le cadre légal n'est pas encore tout à fait prêt dans ce secteur en constante évolution.

Botnet

Ensemble d'équipements informatiques infecté par un programme malveillant, qui oblige les machines à contacter un serveur et à obéir à ses ordres. Ces machines infectées sont parfois appelées des zombies. Le but d'un botnet peut être de mener des attaques par déni de services (DDoS), ou d'envoyer des mails de spam.

TippingPoint et l'éradication du botnet « Kraken »

Prenons un exemple cité par Alana Maurushat (2019, p.256). En 2008, des chercheurs en sécurité de l'entreprise TippingPoint, filiale de Trend Micro Security, ont étudié le fonctionnement du **botnet** « Kraken », et ont analysé le code source, les protocoles utilisés ainsi que les serveurs contactés par le programme malveillant. Ils ont ainsi été en mesure de créer un faux serveur pour le **botnet**, que la plupart des programmes malveillants se sont mis à contacter plutôt que les serveurs des *crackers*. Les chercheurs ont ainsi pu écouter le trafic émanant des ordinateurs zombies et décrypter les communications afin de mieux comprendre le fonctionnement du **botnet**. Selon les statistiques remontées par leur système, ce sont plus de 25 000 machines infectées par le programme malveillant qui ont pu être détectées, qui étaient en majorité des ordinateurs de particuliers.

Pour l'instant, non seulement cela ne pose pas de problème éthique de chercher à mieux comprendre comment opère une entreprise criminelle pour chercher à la contrer, mais cela n'a conduit les hackers de TippingPoint à aucune action illégale. Forts de leurs découvertes, les chercheurs ont cependant été capable d'écrire du code qui aurait permis de supprimer le programme malveillant de tous les ordinateurs infectés. C'est alors que les opinions ont divergé : si certains hackers de TippingPoint souhaitaient appliquer le code afin de supprimer le programme des ordinateurs de particuliers, les responsables de l'entreprise pour leur part ont refusé d'agir de la sorte afin de respecter la législation en vigueur.

En effet, de telles actions sur des machines dont ils ne sont pas propriétaires auraient pu être considérées comme des accès non autorisés à des systèmes informatiques, ce qui constitue dans la plupart des pays une infraction à la loi. Le **botnet** a donc pu continuer d'exister sans être inquiété, et les propriétaires de machines infectées n'auront jamais su que leur équipement informatique participait à envoyer plusieurs milliards de messages de spam par jour.

Il y a fort à parier que la loi ne permettra jamais à un chercheur en sécurité d'exécuter d'un programme permettant de nettoyer des ordinateurs sans le consentement de leur propriétaire. En effet, il est impossible d'être certain que le code de nettoyage ne va pas causer un crash du système, ou bien l'endommager. S'il se trouve que cet équipement maintenait en vie des patients dans un hôpital, on ne peut qu'imaginer les conséquences désastreuses d'une opération de nettoyage ratée, qui partait pourtant d'une bonne intention. Pour autant, il existe d'autres exemples de hacking qui jouent avec cette notion de morale, et qui sont plus tendancieux d'un point de vue légal.

Le hackback : un débat juridique

Une pratique qui pourrait bien être légalisée un jour dans certains pays est le « Hackback ». Cela consiste à se défendre contre une attaque informatique en menant une contre-attaque contre les attaquants initiaux. Un des arguments évoqués est l'analogie avec le principe de légitime défense. Aux Etats-Unis, l'idée a été discutée au sein du Sénat[3], mais pour l'heure cette pratique y reste illégale.

C'est également le cas en France puisque selon l'article L. 2321-2 du code de la défense, seul l'état est autorisé à répondre à une attaque « qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ». En effet, le principal argument soulevé contre cette pratique est la quasi-impossibilité d'attribuer une attaque à groupe d'individu en particulier, notamment à cause des nombreux moyens d'anonymisation existants sur Internet.

Attaque DDoS

Attaque informatique consistant à envoyer un immense nombre de requête à un serveur. Ces requêtes proviennent d'un grand nombre de machines différentes rendant cette attaque difficile à contrer.

[3] Proposition de Tom Graves le 11/01/2017.

Le hacking comme moyen de désobéissance civile : le cas WikiLeaks

Voyons maintenant un exemple d'utilisation du hacking pour mener une attaque informatique illégale, mais motivée par des facteurs d'ordre moral. Pour le contexte, WikiLeaks est un site internet mettant en relation des lanceurs d'alertes, des sources anonymes et des journalistes. Ce site est à l'origine de nombreuses affaires très médiatisées, telles que l'affaire de la mise sur écoute des présidents français par la NSA, qui a fait scandale en France en 2015. Alana Maurushat (2019, p.242) relate qu'en 2010, le fondateur de WikiLeaks Julian Assange est arrêté par les forces de l'ordre britanniques, suites à des accusations d'agression sexuelle à son encontre. Cette affaire est alors traitée par la justice suédoise, puisque les faits alors présumés auraient eu lieu dans ce pays.

Beaucoup ont vu en cette arrestation un coup monté pour déstabiliser le site d'information, et ont commencé à regrouper des fonds pour la défense en justice de Julian Assange. Les plus gros acteurs du secteur des transactions bancaires tels que MasterCard ou Paypal ont alors désactivé la possibilité de faire des dons pour cette cause, ainsi que les dons à WikiLeaks, qui représentaient alors 95% des revenus de ce site. En réponse, des **attaques DDoS** ont été lancées à l'encontre de Paypal et MasterCard, afin de forcer ces entreprises à accepter de nouveau les transactions bénéficiant à WikiLeaks. De telles attaques ont continué durant plusieurs mois, jusqu'à ce que le site d'information trouve une parade aux systèmes bancaires classiques : les cryptomonnaies.

Si de telles attaques à l'encontre de ces établissements bancaires ne sont pas autorisés par la loi, il n'en reste pas moins que leurs auteurs n'ont pas agi par cupidité. Le journal The Guardian révélera par la suite que l'Angleterre avait fait pression sur la justice suédoise pour maintenir un mandat d'arrêt durant plusieurs années à l'encontre du fondateur de WikiLeaks, alors que la justice suédoise souhaitait clore l'affaire faute de preuves.

Le fait pour des hackers d'utiliser leurs compétences informatiques afin de soutenir une cause qui reflètent leurs valeurs morales a un nom : c'est ce qu'on appelle l' « Hacktivisme », contraction des mots hacking et activisme.

En outre, Alana Maurushat (2019) explique que ce type d'attaque peut être considéré comme une forme de désobéissance civile. On pourrait en effet comparer les conséquences de ces **attaques DDoS** au cas du blocage du siège social de TotalEnergies en France le 25 mai 2022. L'un de ces évènements a perturbé l'accès aux sites internet de deux multinationales, tandis que l'autre a empêché l'accès physique au siège social d'une autre multinationale. Les deux événements sont semblables aussi bien dans leurs effets que dans leurs motivations.

Le *bug bounty* : une chasse aux failles de sécurité

Aujourd'hui cibles de cyberattaques incessantes, les entreprises n'ont plus d'autres choix que de déployer des efforts considérables pour se protéger. Elles embauchent donc des experts en cyberdéfense et dépensent parfois des millions d'euros pour se barricader contre toute intrusion dans leur système d'information. Cependant, les nombreux cas de cyber malveillance envers des entreprises, des états ou des services publics ne cessent de nous prouver qu'aucune protection n'est infaillible, car les hackers trouvent toujours de nouvelles manières de les contourner.

Dès 1995, l'entreprise Netscape l'a bien compris et invente une nouvelle manière d'améliorer la sécurité de son système d'information : le tout premier programme de *bug bounty* est né. Le concept d'un *bug bounty* — littéralement une « chasse au bug » — est d'encourager toute personne étrangère à l'entreprise à chercher des bugs dans un logiciel pour les signaler aux développeurs. Une fois que les développeurs ont analysé le bug et l'on résolut, la personne l'ayant signalé se voit récompensée par une certaine somme d'argent, dont le montant diffère généralement selon la dangerosité de la faille de sécurité causée par le bug. Ce système est à l'heure actuelle jugé si efficace que toutes les grandes entreprises possèdent aujourd'hui leur propre programme de *bug bounty*, afin que des hackers les aident à améliorer leur sécurité informatique.

Afin de trouver des failles de sécurité sur un site web par exemple, un hacker doit en scruter les moindres recoins, envoyer des requêtes malicieuses aux serveurs, et tenter de pénétrer dans le système. Puisque ce comportement est a priori interdit par la loi de nombreux pays, dont la loi française, les entreprises responsables de ces systèmes indiquent donc explicitement ce

que sont autorisés à faire ou non les *bug hunters* — c'est-à-dire les hackers participants au programme. Ainsi, les responsables du *bug bounty* garantissent que toute personne qui respecte les règles du programme ne sera pas poursuivie en justice. Par exemple, les entreprises spécifient explicitement les noms de domaines sur lesquels les hackers sont autorisés à chercher des failles. Ils interdisent généralement certaines méthodes telles que l'ingénierie sociale ou les attaques par déni de service, qui ne permettent généralement pas d'exhiber de failles et monopolisent de nombreuses ressources de l'entreprise.

La place importante de l'éthique dans le bug bounty

Malheureusement le hacking n'est pas une science exacte, et bien que les *bug hunters* soient généralement des hackers très doués, il arrive qu'un bug provoqué intentionnellement ait d'importantes conséquences insoupçonnées. Il est très dur voire impossible pour une entreprise d'indiquer précisément un périmètre autorisé, et de lister exhaustivement les attaques autorisées pour les hackers sans les empêcher de travailler correctement. De l'autre côté, il est parfois difficile pour un *bug hunter* d'être certain qu'une de ses actions ne risque pas de provoquer des réactions en chaîne, impactant des services hors du périmètre autorisé.

Pourtant, il est assez remarquable de constater que les conflits entre *bug hunters* et responsables de programmes sont rares, notamment grâce à la bonne foi et la bonne volonté des deux parties, qui n'ont rien à gagner à se chercher des problèmes mutuellement et l'ont bien compris. En fait, s'il est important que les programmes de *bug bounty* définissent des directives générales afin de clarifier les attendus de l'entreprise, la règle la plus importante est de conserver une certaine éthique lors de la recherche de vulnérabilité.

HackerOne est une des principales plateformes de *bug bounty* sur laquelle sont entre autres disponibles les programmes d'IBM, de Paypal ou d'Adobe. Sur le site de cette organisation, la page « Directives pour la divulgation des

vulnérabilités » spécifie la « philosophie » à laquelle devrait adhérer les hackers et les entreprises[4] :

> Les chercheurs doivent ...
>
> - **Respecter les règles**. Agir dans le cadre des règles établies par l'équipe de sécurité, ou s'exprimer en cas de fort désaccord avec les règles.
> - **Respecter la vie privée**. S'efforcer de bonne foi de ne pas accéder ou détruire les données d'un autre utilisateur.
> - **Être patients**. S'efforcer de bonne foi de clarifier et d'étayer leurs rapports sur demande.
> - **Ne pas nuire**. Agir pour le bien commun en signalant rapidement toutes les vulnérabilités découvertes. Ne jamais attaquer volontairement d'autres personnes sans leur permission.
>
> Les équipes de sécurité doivent...
>
> - **Donner la priorité à la sécurité**. S'efforcer de bonne foi de résoudre les problèmes de sécurité signalés de manière rapide et transparente.
> - **Respecter les chercheurs**. Accorder une reconnaissance publique aux chercheurs pour leurs contributions.
> - **Récompenser la recherche**. Encouragez financièrement la recherche en matière de sécurité, le cas échéant.
> - **Ne pas nuire**. Ne pas prendre de mesures punitives déraisonnables à l'encontre des chercheurs, comme des menaces juridiques ou le renvoi de l'affaire aux forces de l'ordre.

Ces principes sont au cœur du concept de *bug bounty*. Les entreprises et les hackers ont bien compris qu'il serait impossible de spécifier techniquement et exhaustivement tout ce qu'il est autorisé de faire ou non. Les recommandations se basent donc principalement sur la nature des intentions des hackers plutôt que sur la manière dont ils agissent.

[4] Traduction Libre

Cet exemple de professionnalisation du hacking est représentatif de l'importance de l'éthique dans ce domaine, et permet de mieux comprendre où la différence se situe entre les termes « white-hat » et « black-hat » (synonyme de « cracker »).

Les tests d'intrusion en *red team*

Un programme de *bug bounty* est une excellente manière de mettre à l'épreuve la sécurité d'un site web, d'un logiciel, ou plus généralement de la partie visible d'une entreprise sur Internet. Cependant, une entreprise dispose également d'un système d'information interne, sur lequel sont hébergés des intranets et peuvent circuler des documents sensibles. Ces systèmes sont en général suffisamment isolés pour ne pas pouvoir être atteint par des *bug hunters*, dont le périmètre se limite plutôt aux serveurs publics de l'entreprise. En outre, une organisation ne souhaite souvent pas que de parfaits inconnus, même bien intentionnés, s'invitent dans son système d'information interne afin d'analyser les moindres failles existantes.

Pour cette raison, des entreprises de sécurité informatique proposent aujourd'hui de réaliser des audits des systèmes de sécurité d'autres entreprises, dans un cadre très professionnel. Parmi les différentes techniques d'audit, on retrouve notamment une pratique dont le principe est de constituer une *red team*, c'est-à-dire une équipe de hackers dont le but est de jouer le rôle de *crackers* au sein de l'entreprise cliente, durant ce qu'on appelle un « test d'intrusion ».

Dans une conférence, L. Toulet (2022) décrit les trois étapes qui constituent un test d'intrusion réalisé par une *red team* :

1. **Préparation** : l'entreprise de sécurité et son client définissent les attendus de l'opération et le périmètre autorisé. Une lettre d'engagement à valeur juridique est ensuite signée entre les deux parties, afin de donner explicitement l'autorisation à l'équipe d'attaquants fictifs de pénétrer dans le système d'information du client.

2. **Test offensif** : Le teste se déroule en quatre étapes, détaillées dans les pages suivantes. Il consiste à infiltrer le système d'information de l'entreprise pour analyser les failles existantes et exfiltrer des données.

3. **Rédaction du rapport et restitution** : L'équipe d'attaquant explique dans un rapport l'ensemble des failles qu'elle a pu exploiter, ainsi que les potentielles vulnérabilités qu'elle n'a pas eu le temps d'explorer. Selon le type de prestation, la société réalisant l'audit peut également être chargée d'indiquer comment résoudre chacune de ces vulnérabilités.

Phishing

Technique d'ingénierie sociale consistant à envoyer un mail à quelqu'un en usurpant l'identité d'un tiers, afin de récupérer des informations confidentielles telles que des identifiants de connexion.

Etape 1 du test offensif : Une reconnaissance pour mieux maîtriser le contexte

La première partie du test a pour but de récolter un maximum d'informations techniques sur l'entreprise, telles que les logiciels utilisés et les solutions anti-virus déployées. Un autre aspect de la reconnaissance est plutôt socio-économique, car il consiste à analyser les différentes filiales de l'entreprise ainsi que ses liens ou ceux de certains employés avec le monde extérieur. Le but de ces recherches qui peuvent paraître étonnantes, est d'être capable de monter des attaques d'ingénierie sociale crédibles et efficaces.

Par exemple, après avoir récolté des informations sur l'entreprise, un hacker de l'équipe d'attaque pourrait usurper l'identité d'un fournisseur régulier pour envoyer des mails infectés, profitant de la baisse de vigilance accordée à ce type d'interlocuteur. Même des informations sur des anciens collègues d'un salarié en particulier peuvent se révéler utile, et LinkedIn se révèle alors un outil redoutablement efficace pour les attaquants fictifs.

Etape 2 : Obtenir un accès dans le système

Dans un deuxième temps, le but de l'équipe attaquante est d'obtenir un moyen d'accès au système d'information interne de l'entreprise cliente. Des techniques d'ingénierie sociale « douces » sont généralement autorisés par la lettre d'engagement, et des mails de **phishing** se trouvent souvent être un excellent moyen d'obtenir l'accès recherché.

Dans certains cas dans lesquels les systèmes à atteindre sont particulièrement bien isolés, l'équipe *red team* est parfois amenée à s'introduire physiquement dans les locaux de l'entreprise, en reproduisant éventuellement le badge d'un salarié ou d'un prestataire. Une fois présente dans les locaux, l'équipe attaquante n'a souvent qu'une clé USB à brancher sur le bon équipement informatique pour obtenir un accès.

Etape 3 : Se maintenir dans le système

Après le premier accès obtenu, l'objectif à court terme pour les attaquants est de réussir à se maintenir dans le système et effacer au plus vite les traces de l'accès afin que les équipes informatiques de l'entreprise cliente, qui ne sont généralement pas informées, ne les détectent pas. Par exemple, dans le cas d'un premier accès obtenu à travers un salarié ayant exécuté un virus reçu dans un mail de **phishing**, il s'agit de supprimer cet email, camoufler le fichier contenant le virus et masquer le processus système permettant aux attaquants d'accéder à la machine. Ensuite, le but est d'obtenir un accès administrateur sur la machine infectée, en utilisant des failles de sécurité connues du système d'exploitation, ou tout simplement en testant des mots de passe peu robustes.

Une fois que la machine est entièrement sous le contrôle de l'équipe *red team*, l'objectif est d'effectuer une reconnaissance du système d'information complet à partir de cette machine. Des outils logiciels permettent aisément de lister l'ensemble des autres équipements informatiques accessibles, et d'analyser certaines de leurs vulnérabilités au passage. Généralement, les cibles potentielles pour un **mouvement latéral** sont multiples, c'est pourquoi l'équipe attaquante sélectionne les pistes à approfondir selon les objectifs fixés lors de la préparation de ce test d'intrusion. En effet, l'équipe attaquante dispose d'un temps limité pour mener à bien ses recherches, lequel est prévu dans le contrat initial entre l'entreprise de sécurité informatique et son client.

Mouvement latéral

Le fait d'utiliser un ordinateur compromis comme tremplin pour infecter un autre équipement du réseau. Par exemple : infecter un ordinateur d'un employé à l'aide de phishing, puis atteindre des serveurs internes.

Etape 4 : Exfiltrer des données pour être crédible

En fonction des différentes cibles internes que l'équipe attaquante parvient à atteindre, elle exfiltre des données représentatives et pertinentes. Ces données peuvent aussi bien être des documents internes de l'entreprise que des données clients par exemple, car cette exfiltration a un double objectif.

Le premier objectif est de tester si les équipes informatiques de l'entreprise cliente sont capables d'identifier une anomalie dans les flux de données, et s'il elles ont la capacité de prévenir une telle fuite de donnée en conditions réelles.

Le second objectif est d'être capable, à la fin d'un tel examen de sécurité qui peut durer plusieurs mois, de prouver irréfutablement à l'entreprise cliente que le test d'intrusion a effectivement permis d'exhiber des vulnérabilités importantes. Cela permet à la fois de justifier l'investissement de l'entreprise cliente, et en même temps de crédibiliser le rapport qui sera fourni par l'équipe d'attaquants fictifs.

Une législation difficile à appliquer

Malheureusement, tous les hackers ne sont pas des professionnels bienveillants, et c'est pourquoi un ensemble de lois a été créé afin de tenter de protéger les utilisateurs de ces nouveaux systèmes informatiques. Dans beaucoup de pays cependant, le cadre légal peut sembler légèrement dépassé par les technologies actuelles. Le principal problème auquel est confrontée la justice est de prouver la responsabilité d'une personne dans une attaque informatique.

Prenons l'exemple d'une **attaque DDoS** visant à empêcher un site web de fonctionner durant plusieurs heures. Cette attaque informatique est une infraction à l'article 323-2 du code pénal qui interdit « le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données ». On pourrait donc imaginer que les auteurs de ce genre d'attaque soient poursuivis en justice, et condamnés pour cela. Pourtant, il est très rare que de telles condamnations aient lieu, notamment du fait de la difficulté de prouver la responsabilité d'une personne physique dans ce genre d'affaire.

En effet, une **attaque DDoS** est souvent menée par un **botnet**, ce qui signifie que les seuls éléments utiles pour l'enquête que l'entreprise victime peut fournir est la liste des adresses IP des machines ayant envoyé des requêtes durant l'attaque. Nous avons cependant vu que les ordinateurs faisant partie d'un **botnet** en sont rarement membre par choix de leur propriétaire, mais plutôt à cause de l'exécution d'un programme malveillant, qui les oblige à suivre les instructions d'un *cracker*. Poursuivre chacun des propriétaires de ces machines serait une perte de temps considérable, et ne permettrait pas de condamner le véritable auteur de

l'attaque qui a ordonné au **botnet** de submerger le site web. Ainsi, les enquêtes aboutissent rarement et les auteurs de ces attaques ne sont guère inquiétés.

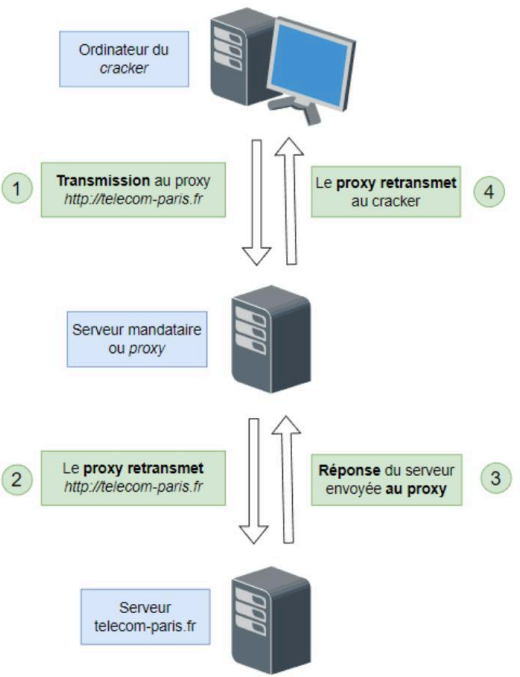
Les serveurs mandataires, pour masquer son identité

Plaçons-nous maintenant dans le cas plus simple d'un *cracker* utilisant sa propre machine pour s'introduire dans le système d'information d'une entreprise. On pourrait alors imaginer qu'une fois l'adresse IP du *cracker* obtenue par les enquêteurs, il serait très simple de remonter jusqu'à l'auteur du délit.

Malheureusement ce n'est pas aussi simple, et il est très souvent compliqué de déterminer la personne physique responsable de l'infraction. En effet, une pratique courante pour les *crackers* est de se servir de **serveurs mandataires** pour masquer leur véritable adresse IP. Par conséquent, lorsque les enquêteurs vont examiner les fichiers journaux de l'entreprise afin de déterminer quelle adresse IP est à l'origine de l'infiltration, la seule adresse IP qui sera visible sera celle du **serveur mandataire** utilisé. Or ces serveurs mandataires peuvent être des ordinateurs faisant partie d'un **botnet**, et permettent très difficilement de remonter au *cracker* à l'origine de l'attaque. En outre, les *crackers* utilisent en fait des chaînes de **serveurs mandataires** les uns à la suite des autres afin de brouiller encore plus les pistes, avec des serveurs dans des pays différents afin de complexifier le travail d'enquête.

Serveur mandataire

De l'anglais *proxy server*, désigne un ordinateur ou un serveur informatique auquel un utilisateur communique des requêtes que celui-ci va retransmettre à un serveur cible. Dans l'exemple ci-dessous, le serveur telecom-paris.fr n'a aucun contact avec la machine du *cracker* et échange uniquement avec le serveur mandataire sans savoir que celui-ci agit par procuration.



Conclusion

La question du hacking a toujours dépassé de loin celle du « piratage informatique ». Le hacking peut être éthique, être exercé à titre professionnel ou simplement en tant que loisir. Il ne peut être que souhaitable que la connotation du terme « hacker » évolue, afin que cet art s'ouvre à un plus grand public et que les mentalités évoluent pour permettre d'améliorer le cadre légal, qui peine aujourd'hui à différencier les nombreux contextes dans lequel le hacking intervient.

En outre, il est plus important que jamais d'intéresser le public au secteur de la cybersécurité, qui peine à recruter des talents tandis que le nombre d'attaques informatiques ne cesse d'augmenter. Le hacking est un outil puissant qui n'est pas réservé aux *crackers*, et cela, les militants, les entreprises, les gouvernements ou encore la justice l'ont bien compris.

Bibliographie

Bowcott, O. & MacAskill, E. (2018, 11 février). *Sweden tried to drop Assange extradition in 2013, CPS emails show*. the Guardian. https://www.theguardian.com/media/2018/feb/11/sweden-tried-to-drop-assange-extradition-in-2013-cps-emails-show

Erickson, J. (2017). *Techniques de hacking*. Pearson.

Hack. (s. d.). Dans *Oxford Learner's Dictionaries*. https://www.oxfordlearnersdictionaries.com/definition/english/hack_2

Malkin, G., LaQuey Parker, T. & Xylogics, Inc. (1993, janvier). *RFC 1392 : Internet Users' Glossary*. RFC Editor. https://www.rfc-editor.org/rfc/rfc1392

Maurushat, A. (2019). *Ethical Hacking*. Amsterdam University Press.

TippingPoint | DVLabs | Owning Kraken Zombies, a Detailed Dissection. (2008, 28 avril). https://web.archive.org/web/20100413232937/http://dvlabs.tippingpoint.com/blog/2008/04/28/owning-kraken-zombies

Toulet, L. (28/11/2022). *Ethical Hacking ou comment se mettre dans la peau d'un hacker pour mieux le contrer*. Télécom Paris.

Vulnerability Disclosure Guidelines | HackerOne. (s. d.). https://www.hackerone.com/disclosure-guidelines