Sécurité informatique

Ethical Hacking

Apprendre l'attaque
pour mieux se défendre

ISBN : 978-2-7460-5105-8
Imprimé en France

Editions ENI

ZAC du Moulin Neuf
Rue Benjamin Franklin
44800 St HERBLAIN

Tél. 02.51.80.15.15
Fax. 02.51.80.15.16

e-mail : editions@ediENI.com
http://www.editions-eni.com

Auteurs : ACISSI
Collection **Expert IT** dirigée par Joëlle MUSSET

Table des matières

Chapitre 3

Social Engineering

Chapitre 5

Les failles réseaux

Chapitre 6
Les failles Web

Chapitre 7

Les failles systèmes

Chapitre 8
Les failles applicatives

Chapitre 1
Introduction et définition

1. Présentation

1.1 L'information est partout

À l'heure du "tout disponible partout tout de suite", le transport des données en dehors du domicile d'un particulier ou d'une entreprise est une réalité qui mérite que l'on s'interroge sur la sécurité des transmissions pour ne pas compromettre un système d'information.

Que ce soit à l'échelle d'une entreprise, d'une multinationale ou à plus petite échelle, la sécurité d'un système d'information prend plus ou moins d'importance selon la valeur que l'on confère à ces données.

Avec le développement d'Internet, chacun a accès au réseau où de plus en plus d'informations circulent. De plus en plus, les entreprises communiquent et diffusent via ce media, que ce soit dans leurs liens avec leurs fournisseurs ou leurs partenaires ou en interne, dans les relations entre les employés eux-mêmes.

Nous sommes face non seulement à une augmentation de la quantité, mais aussi et surtout de l'importance des données.

L'ensemble formé par tout le réseau d'utilisateurs de ce système d'information se doit d'être connu pour être sûr. Les ressources qui y circulent doivent absolument être protégées et pour cela, la maîtrise du système d'information est indispensable. Chaque acteur du système a un rôle à respecter, qui doit être défini scrupuleusement.

1.2 Connaître le système d'information pour le protéger

Le système d'information définit l'ensemble des données et des ressources matérielles et logicielles de l'entreprise. Ce système permet de stocker et de faire circuler les ressources qu'il contient. Il représente également le réseau d'acteurs qui interviennent dans celui-ci, qui échangent les données, y accèdent et les utilisent.

Ce système représente la valeur de l'entreprise, il est essentiel de le protéger. Le compromettre revient à compromettre l'entreprise.

Il convient donc d'assurer sa sécurité en permanence, et surtout dans des conditions d'attaque, d'espionnage ou de défaillance. Il faut s'assurer que les ressources servent uniquement dans le cadre prévu, par les personnes accréditées et surtout pas dans un autre but.

Le risque encouru par un système est lié de manière étroite à la menace et à la vulnérabilité qui le touchent, mais également aux contre-mesures mises en œuvre.

La menace qui plane sur un système englobe les types d'actions menées dans le but de nuire à ce système (attaque, espionnage, vol d'informations...).

La vulnérabilité représente les failles, les brèches dans le système, tout ce qui expose le système à la menace : manque de sauvegardes, de robustesse, une architecture défaillante...

Enfin les contre-mesures sont les actions mises en œuvre pour prévenir la menace, une fois qu'elle est mesurée, ce qui passe d'abord par une prise de conscience.

La menace qui plane sur un système est un fait : plus l'entreprise possède des informations importantes, plus elle y sera soumise. Cependant, elle peut directement impacter le niveau de sécurité de son système en s'efforçant de mettre en place des contre-mesures, c'est-à-dire en s'attachant à la protection de son système, qui ne doit jamais être négligée. Ce sont en effet, ces contre-mesures qui vont diviser le risque d'attaque et la compromission des données.

La sécurité engendre généralement le déploiement de moyens techniques, mais également et surtout, de solutions de prévention, qui doivent absolument prendre en compte la formation et la sensibilisation de tous les acteurs du système. Des règles et des bonnes pratiques doivent être mises en place pour ne pas créer de brèche humaine. Ce sont les actifs d'une entreprise qui possèdent son capital intellectuel. Ce capital, forgé par son organisation, son économie ou encore sa valeur, représente un patrimoine d'informations à protéger.

1.3 Identifier la menace

Pour mettre en place une politique de sécurité, il faut d'abord commencer par identifier la menace, le risque potentiel. Il faut connaître son ennemi, ses motivations et prévoir la façon dont il procède pour s'en protéger et limiter les risques d'intrusion.

La sécurité d'un système repose sur cinq grands principes :

- L'intégrité des données : il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication. L'intégrité des données doit valider l'intégralité des données, leur précision, l'authenticité et la validité.
- La confidentialité : seules les personnes habilitées doivent avoir accès aux données. Toute interception ne doit pas être en mesure d'aboutir, les données doivent être cryptées, seuls les acteurs de la transaction possédant la clé de compréhension.

- La disponibilité : il faut s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment. La disponibilité d'un équipement se mesure en divisant la durée durant laquelle cet équipement est opérationnel par la durée durant laquelle il aurait dû être opérationnel.
- La non-répudiation des données : une transaction ne peut être niée par aucun des correspondants. La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues. Cela se fait par le biais de certificats numériques grâce à une clé privée.
- L'authentification : elle limite l'accès aux personnes autorisées. Il faut s'assurer de l'identité d'un utilisateur avant l'échange de données.

On mesure la sécurité d'un système entier à la sécurité du maillon le plus faible. Ainsi, si tout un système est sécurisé techniquement mais que le facteur humain, souvent mis en cause, est défaillant, c'est toute la sécurité du système qui est remise en cause.

Dans un contexte global, la sécurité doit être assurée :
- au niveau utilisateur, les acteurs doivent comprendre l'importance de leur position.
- au niveau des technologies utilisées, elles doivent être sûres et ne pas présenter de failles.
- au niveau des données en elles-mêmes, avec une bonne gestion des droits d'accès (authentification et contrôle, l'utilisateur doit posséder uniquement les droits qui lui sont nécessaires).
- au niveau physique (accès à l'infrastructure, au matériel...), rien ne sert de sécuriser un système logiquement si matériellement l'accès à la salle des machines n'est pas sécurisé.

1.4 Instaurer de bonnes pratiques de sécurité

Cependant, la sécurité ne doit pas être une gêne au quotidien, elle ne doit pas perturber l'utilisateur et doit permettre à quiconque d'utiliser le système en toute confiance. Il faut donc établir une politique de sécurité, et pour cela il faut commencer par identifier les besoins en terme de sécurité, réfléchir et définir les risques ainsi que les conséquences.

Un particulier n'aura pas les mêmes attentes qu'une entreprise, il faut donc évaluer l'importance des données.

Des règles et des procédures doivent ensuite être mises en place pour les différents services.

Un administrateur se doit de faire de la surveillance passive et active. Il doit connaître les vulnérabilités matérielles ou logicielles qui pourraient toucher le système qu'il gère, se tenir informé des failles décelées.

Enfin, puisqu'aucun système n'est infaillible, il ne faut pas oublier de définir la politique à appliquer en cas de menace, de détection de vulnérabilité : que faire, qui contacter ?

1.5 Auditer son système

Enfin, il est bon d'auditer un système pour connaître son niveau de sécurité réel.

Pour cela, on réalise un test d'intrusion, mené soit par le responsable de la sécurité informatique du réseau, soit par un professionnel de la sécurité informatique, un hacker professionnel. Cela se fait bien sûr en accord avec l'entreprise.

Il s'agit donc de tenter une intrusion du système, on dit qu'il s'agit d'un audit de vulnérabilité. Dans ce cas, la personne réalisant le test doit expliciter les actions à mener et obtenir une autorisation signée. Cette autorisation doit bien sûr être donnée par une personne qui y est habilitée, un Responsable de la Sécurité des Systèmes d'Information (RSSI).

En interne, seul le RSSI ou le responsable de la sécurité de l'entreprise peut faire ce test.

De plus, il est conseillé de prévenir le moins de monde possible dans l'entreprise lors d'audits de sécurité afin de ne pas fausser le contexte. Rappelons que dans la réalité, la majorité des intrusions système se font le week-end.

2. Une nouvelle éthique de travail

2.1 La connaissance avant toute chose

Quand on parle de sécurité informatique, on ne peut ignorer le monde underground, celui des hackers et autres pirates du Web.

Ils sont fortement médiatisés, généralement à tort et l'objet de nombreuses confusions. Nous allons donc d'abord définir brièvement les différents profils que l'on retrouve sous ce terme mal employé de "pirate".

Tout d'abord, la définition du terme hacker, qui est assez large. À l'origine, "*hacker*" est un mot anglais qui veut dire "bricoleur" ou encore "bidouilleur". En informatique, ce terme est utilisé pour définir les programmeurs débrouillards, avec des connaissances techniques élevées. Ces programmeurs sont avant tout passionnés par ce qu'ils font, ils ne se posent pas de limites pour la connaissance ou pour assouvir leur curiosité.

Les hackers sont également capables de détourner un objet ou un logiciel de son fonctionnement originel.

Ils utilisent leur savoir pour découvrir les choses auxquelles ils ne sont pas censés avoir accès.

Mais la communauté des hackers va également au-delà de la connaissance technique. Être un hacker correspond davantage à un état d'esprit plus qu'au fait de programmer.

Ainsi, les hackers sont généralement des personnes cultivées qui connaissent à la fois l'historique de leur statut, les grands acteurs du mouvement, qui se tiennent informés de tout ce qui s'apparente à leur domaine et qui ont soif de connaissance.

Il convient cependant de remettre à plat les définitions habituelles que l'on donne des hackers pour corriger quelques travers portés par les médias de masse, et de distinguer les différents types de cette grande famille...

2.1.1 Les hackers « black hats », les chapeaux noirs

Généralement, ces hackers ne respectent pas la loi, ils pénètrent par effraction dans les systèmes dans un intérêt qui n'est pas celui des propriétaires du réseau. L'intérêt y est personnel, généralement financier, en tout cas le but est nuisible à la personne (physique ou morale) visée.

Ces hackers sont d'ailleurs plus généralement appelés des crackers.

Les crackers ayant une nette attirance pour ce côté obscur sont par exemple les créateurs de virus, de chevaux de Troie ou de logiciels espions.

Lorsque cela est fait dans le but de nuire à une organisation ou à des individus, on parle aussi de terrorisme ou de cyber-terrorisme.

Il n'est pas rare que les black hats changent de bord et se fassent embaucher par de grandes sociétés. En effet, la connaissance de ces passionnés est telle qu'elle peut aider une entreprise dont les données sont sensibles à mettre en place la sécurité.

Cependant la communauté des black hats est assez large et possède des convictions, des opinions et des connaissances bien différentes, qui en séparent les différents acteurs.

2.1.2 Les hackers « white hats », les chapeaux blancs

Techniquement, l'action menée par les white hats est très proche de celle des black hats. Cependant, elle se différencie par le but ou la finalité.

En effet, les « white hackers » ont plutôt comme ambition d'aider à la sécurisation du système, sans en tirer profit de manière illicite.

Les white hats bricolent et testent les systèmes d'information pour découvrir les vulnérabilités pas encore connues ou non publiques, les « 0 day » (zéro day, zéro jour). La technique employée est la même que pour un hacker au chapeau noir.

Leur atttitude est par contre différente lors de la découverte de cette vulnérabilité. La question qui se pose alors est de savoir s'il faut rendre une vulnérabilité publique ou non. Les hackers au chapeau blanc prônent la divulgation totale de la découverte, ce que l'on appelle en anglais la *full disclosure*, là où les hackers au chapeau noir préfèrent restreindre l'accès à cette information et ne pas la divulguer.

Les white hats rendent alors publiques les vulnérabilités, et parfois même les exploits, qui sont les bouts de code permettant de tester la vulnérabilité d'un système à cette faille. Cela se fait sur des outils en ligne spécialisés comme des listes de diffusion ou des outils de gestion de bug (*bugtracking*).

Le problème qui en résulte est que ces codes sont également rendus disponibles pour quiconque, dont les script-kiddies, que nous verrons ensuite.

Cependant, un white hat met également au courant les auteurs des vulnérabilités qui les touchent (lorsqu'ils n'agissent pas dans le cadre d'une mission d'audit qui explique leurs actions), contrairement aux black hats.

Même si les white hats disent agir dans la légalité et pour la bonne cause, en réalité depuis que la loi sur l'économie numérique, la LCEN (Loi pour la Confiance dans l'Economie Numérique), a été votée en France, seule l'intention reste réellement bonne. Ces hackers sont considérés également hors la loi puisque le fait de divulguer des vulnérabilités et des exploits sur Internet est dès lors devenu répréhensible. Cette loi contredit ainsi de plein fouet l'éthique hacker et également le principe du logiciel libre.

2.1.3 Les hackers « grey hats », les chapeaux gris

Le hacker au chapeau gris est un peu un hybride du chapeau blanc et du chapeau noir.

Il s'agit d'un hacker compétent, qui agit parfois avec l'esprit d'un white hat, parfois avec celui d'un black hat.

Son intention n'est pas forcément mauvaise mais il commet cependant occasionnellement un délit.

Beaucoup de hackers qui se disent white hats s'apparentent en réalité plus à des grey hats, dans le sens où ils ne révèlent pas toujours leurs découvertes et en profitent à des fins personnelles.

2.1.4 Les « script kiddies »

Dans le problème lié à la publication sur Internet des vulnérabilités découvertes, on trouve l'un des éléments clés de la discorde, les *script kiddies*, autrement dit des jeunes pirates néophytes.

Ces individus récupèrent les exploits laissés par les white hats sur les outils publics et les exécutent sur des machines, sans aucune connaissance, dans le but de provoquer des pannes volontaires, des *mass-root*.

Généralement un script kiddie est un jeune adolescent, pénétrant par effraction dans un système, après avoir étudié/lu dans des livres ou sur Internet quelques documentations de base sur le sujet de la sécurité informatique. Le script kiddie n'a aucune notion de l'éthique d'un hacker, il agit par vantardise auprès de ses copains, il n'est pas rare par exemple qu'il demande à "pirater un compte de messagerie instantanée".

Le script kiddie n'a pas de réelles connaissances, il ne fait que réutiliser des codes ou des programmes prêts à l'emploi, il réutilise sans comprendre les enjeux.

Mais les script kiddies sont craints, puisque malgré leur faible niveau, le fait qu'ils utilisent le code des autres représente parfois une menace réelle pour un système, surtout qu'ils sont nombreux et peu soucieux des dégâts qu'ils occasionnent. Cependant ils sont trop souvent confondus avec les réels hackers.

Ils sont également rejetés complètement des communautés underground, où ils sont considérés comme des lamers, c'est-à-dire des personnes dénuées de compétences.

2.1.5 Les hackers universitaires

Ce sont des hackers libres, que l'on associe au mouvement Open Source du logiciel libre, comme Richard Matthew Stallman, le fondateur du projet GNU. Cette définition du hacker libre est apparue au MIT, le Massachusetts Institute of Technology.

Le hacker est alors défini comme quelqu'un qui partage sa connaissance avec autrui, sur le fonctionnement d'un système, des ordinateurs et des réseaux. Ces hackers prônent la pensée selon laquelle l'information est libre et n'appartient à personne. Ainsi, toute nouvelle connaissance se veut d'être partagée avec tout le monde.

Ces hackers forment une grande communauté qui partage la même culture et qui compte des programmeurs aux compétences aiguisées, des spécialistes des réseaux et des technologies. Les hackers travaillent ensemble et ainsi sont à l'origine de grandes œuvres, comme Internet ou encore Usenet, ou le système d'exploitation Unix.

En 1984, Steven Levy a défini "l'éthique hacker" selon les principes suivants :

- Toute information est par nature libre et gratuite.
- L'accès aux ordinateurs devrait être total, illimité, possible pour tout le monde.
- La décentralisation des données doit être encouragée.
- Les hackers devraient être jugés sur le hacking, non pas sur des hiérarchies sociales telles que le diplôme, l'âge ou le grade.
- On peut créer de l'art et de la beauté avec un ordinateur.
- Les ordinateurs peuvent améliorer la vie.

2.2 Un rapport différent au travail

Bien sûr, cette définition des hackers est un peu facile et constamment sujette à des discordances. Il s'agit d'une classification trop manichéenne : d'un côté les gentils, d'un autre les méchants.

Mais cela permet de contrecarrer les idées reçues que l'on a sur ce monde, et particulièrement celles des médias de masse qui confondent trop souvent hacker et cracker.

Mais ce qui différencie également les hackers, c'est ce rapport alternatif au travail, à l'argent et au temps, qui se réfère à une éthique complètement différente du rapport capitaliste habituel que l'on retrouve en société.

Ils n'hésitent pas non plus à travailler en coopération pour la production.

La relation au travail est passionnée, elle mêle la passion, le plaisir d'aller plus loin, la découverte, la curiosité, le jeu... ; ainsi absorbés par leur travail, les hackers multiplient sans cesse leurs connaissances.

Le hacker connaît aussi une certaine indépendance salariale, comme s'il faisait partie d'un communisme basé sur la science.

Dans ce sens, nous pouvons faire référence à de nombreux exemples pour montrer l'efficacité des hackers en coopération.

Par exemple, Linux pour ne citer que lui, est un emblème de la production des hackers du libre. Linux a été développé de manière indépendante, volontaire, dans un contexte en marge du système capitaliste, et possède aujourd'hui une bonne part de marché en utilisation serveur ainsi qu'une croissance importante en terme d'ordinateurs personnels.

Nous sommes face à une remise en cause du schéma de l'économie capitaliste. Le hacker produit de façon libre, selon un modèle ouvert, pour la communauté. Il partage ses connaissances, construit avec les autres.

Cette originalité dans leur éthique de travail était jusqu'alors fortement controversée, par rapport aux tenants de l'approche standard économique.

Cependant, force est de constater que cette auto-organisation dont la structure s'apparente pleinement à un réseau fortement horizontal, est source de réussite.

Le travail des hackers se fait de manière directement coopérative et volontaire, en différents petits groupes fortement autonomes.

2.3 La coopération comme clé de réussite

La sécurité, nous l'avons vu, touche tous les utilisateurs du système. Cela implique donc une bonne connaissance des règles par les utilisateurs, au travers de formations, sensibilisations, de manière régulière.

Cela s'ajoute à la sécurité des dispositifs matériels et logiciels : sauvegardes, mises à jour, plan de reprise en cas d'incident, etc.

L'insécurité provient généralement de la non-connaissance des fonctionnalités du système. Par exemple, le fait de laisser un service actif parce que l'on ne sait pas s'il est utile, représente un risque potentiel. Tout d'abord, il s'agit d'une porte supplémentaire sur le système, donc d'un accès à surveiller. Mais le fait de ne pas connaître un service exécuté sur un système ou de ne pas savoir s'il est utile constitue un réel risque. On ne se renseigne alors pas sur les vulnérabilités connues qui le touchent, on ne le configure peut-être pas comme il le faudrait... Cela peut vite devenir un facteur d'intrusion.

Il arrive également qu'un acteur du système ne connaisse tout simplement pas les moyens de sécurité mis en place.

Quoi qu'il en soit, pour assurer l'état de sécurité d'un système, il convient d'analyser le système pour en connaître les forces et les faiblesses, qu'il faudra bien sûr corriger.

Pour cela, nous l'avons vu, on réalise ce qu'on appelle un audit de sécurité.

Il peut être réalisé par le responsable sécurité du système, s'il possède les connaissances suffisantes, mais il est préférable de faire appel à un tiers de confiance, spécialisé dans la sécurité informatique, pour valider les moyens mis en place pour assurer la protection, au regard de la politique de sécurité.

En effet, une personne extérieure aura une vision beaucoup plus neutre, globale et proche de la réalité. Elle sera également en mesure de conseiller en cas de défaillance, et de mettre en place une politique de sécurité plus saine grâce à des formations par exemple.

Ces spécialistes sont des hackers professionnels, qui sont accrédités pour réaliser des tests d'intrusion, et qui prennent donc connaissance de l'état d'une architecture à un instant t.

Les données étant de plus en plus étendues, accessibles à plus de monde, de manière plus complexe, la tendance qui se dessine dans les entreprises est clairement de faire appel à des spécialistes, et non plus à l'administrateur du système. Il s'agit d'une prise de conscience face à l'importance des données que possède une structure professionnelle.

En tant que spécialiste de la sécurité informatique, un hacker connaît en effet les moyens de déjouer cette sécurité. Ce professionnel de confiance va pouvoir se mettre dans la peau d'un utilisateur mal intentionné (aux connaissances étendues), en testant le système dans des conditions de malveillance, pour s'assurer que les données sont en sécurité, et le cas échéant, comprendre pourquoi et corriger le problème.

Derrière ces spécialistes se cachent en réalité des hackers « white hats ». Ces hackers possèdent un sens de l'éthique et de la déontologie, contrairement aux crackers. Les tests d'intrusion se font en accord avec les clients et la législation.

Il y a donc également eu une prise de conscience envers ces hackers, que l'on a appris à différencier des terroristes, des espions ou des créateurs de virus.

Il est devenu évident que face à des personnes mal intentionnées avec de tels moyens et connaissances, il fallait un niveau de connaissance et de protection au moins équivalent pour protéger un système.

Aujourd'hui, les entreprises sont prêtes à faire cette démarche, et n'hésitent plus à embaucher les meilleurs crakers, ayant même fait de la prison ou commis de graves délits, pour s'assurer de la sécurité de leur système.

Les tests d'intrusion peuvent être conduits de différentes manières, la principale différence est la connaissance du système. En effet, les tests peuvent être faits en conditions réelles, sans aucune connaissance du système, c'est un test en boîte noire. Dans ce cas, le hacker testant le système devra découvrir l'infrastructure et le système au fur et à mesure de ses tests avant de pouvoir en tester les vulnérabilités. C'est de ce principe que nous partirons dans le prochain chapitre.

Il existe également des tests en boîte blanche, où le hacker connaît entièrement le système qu'il va tester, que ce soit au niveau de l'infrastructure, du réseau, des services et du code source. Dans ce contexte, le test simule davantage la perte d'informations sensibles. Le test pourra se faire en profondeur pour tester au maximum la sécurité.

2.4 Tous des hackers !

Si on raisonne de manière un peu plus neutre, on peut dire que l'éthique hacker présente de nombreuses analogies avec celle de personnages ayant un rôle déterminant dans l'économie, à savoir les scientifiques et les chercheurs.

En effet, ils partagent une éthique assez proche de celle des hackers, une éthique qui est fondée sur le partage, la passion et l'absence de propriété vis-à-vis de la connaissance créée.

Et à l'heure actuelle, l'activité scientifique et la recherche fondent une pierre angulaire de la dynamique capitaliste, il y a de moins en moins de frontières ou de cloisonnement entre le scientifique et l'économique. Quand un nouvel algorithme de cryptage est créé, il faut peu de temps aux créateurs de logiciels pour vendre un logiciel permettant de réaliser ce cryptage. Nous sommes donc face à une nouvelle confrontation de la connaissance "libre" et ouverte, et de la propriété économique.

Quoi qu'il en soit, la culture hacker underground est forte.

Le 8 janvier 1986, le hacker Loyd Blankenship publie un article dans le magazine électronique Phrack, appelé Le Manifeste du Hacker.

Ce Manifeste est considéré comme crucial dans la contre-culture, expliquant ainsi l'éthique des premiers hackers. Dans ce texte, il annonce ainsi (texte traduit parNeurAlien, pour No way) :

Oui, je suis un criminel. Mon crime est celui de la curiosité. Mon crime est celui de juger les gens par ce qu'ils pensent et disent, pas selon leur apparence.

Mon crime est de vous surpasser, quelque chose que vous ne me pardonnerez jamais.

Je suis un hacker, et ceci est mon manifeste. Vous pouvez arrêter cet individu, mais vous ne pouvez pas tous nous arrêter... après tout, nous sommes tous les mêmes.

Lien vers l'article original :
http://www.phrack.org/issues.html?issue=7&id=3#article