Hacker Highschool

SECURITY AWARENESS FOR TEENS



LECON 1
ÊTRE UN HACKER

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

WWW.ISECOM.ORG - WWW.OSSTMM.ORG - WWW.HACKERHIGHSCHOOL.ORG - WWW.BADPEOPLEPROJECT.ORG - WWW.OSSTMMTRAINING.ORG

AVERTISSEMENT

Le **Projet Hacker High School** est un outil didactique et comme tous les autres outils de son genre, il présente des inconvénients ou dangers. Certaines leçons, lorsqu'elles sont utilisées abusivement, peuvent engendrer des dommages physiques. Il se peut que d'autres dangers existent lorsqu'une recherche approfondie sur les effets possibles émanant de certaines technologies n'est pas faite. Les étudiants qui se servent de ces cours, doivent être surveillés et encouragés à apprendre, à essayer et le mettre en pratique. Cependant ISECOM ne peut endosser la responsabilité de toute utilisation abusive faite des informations ci-présent.

Les leçons suivantes et leurs exercices sont disponibles ouvertement au public sous les termes et conditions de **ISECOM**:

Tous les travaux du **Projet Hacker High School** sont fournis pour une utilisation non-commerciale dans les écoles primaires, les collèges et les lycées, voir dans les institutions publiques ou privées, et même pour les études à domicile. Ce matériel didactique ne doit en aucun cas être reproduit à des fins commerciales. L'utilisation de ce matériel didactique dans des séminaires, ou des ateliers de formation qui sont payants est formellement interdite à moins que vous n'obteniez une licence. Il en est de même pour les formations payantes dans les collèges, lycées, universités et camp d'informatique, ou autres. Pour l'achat d'une licence, veuillez visiter la section LICENSE sur la page de Hacker High School (HHS) qui se trouve à l'adresse suivante: http://www.hackerhighschool.org/licensing.html .

Le **Projet Hacker High School** est le fruit de l'effort d'une communauté ouverte et si vous appréciez ce projet, nous vous demandons de nous supporter en achetant une licence, ou en faisant un don, ou en nous sponsorisant.

Table des matières

Les Contributeurs

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Chuck Truett, ISECOM
Kim Truett, ISECOM
Marco Ivaldi, ISECOM
Shaun Copplestone, ISECOM
Greg Playle, ISECOM
Jeff Cleveland, ISECOM
Simone Onofri, ISECOM
Tom Thomas, ISECOM

Traducteur

Willy Nassar

ISECOM

Pour l'Amour du Hacking

Introduction par Pete Herzog

Quel que soit ce que vous aurez pu entendre à propos des Hackers, la vérité est qu'ils font quelque chose de vraiment bien: la découverte. Les Hackers sont motivés, plein de ressources, et créatifs. Ils étudient profondément comment les choses fonctionnent, à telle enseigne qu'ils savent comment en prendre contrôle et même les modifier en quelque chose d'autre. Ceci leur permet de repenser, voir d'élaborer de grandes idées parce qu'ils peuvent creuser jusqu'au fin fond du fonctionnement des choses. Plus loin, ils n'ont pas peur de commettre la même erreur deux fois juste pour l'amour d'une curiosité scientifique, et pour voir si la même erreur produit les même résultats. C'est pourquoi les hackers ne voient pas l'échec comme une faute ou une perte de temps parce que tout échec signifie qu'il y a du nouveau à apprendre. Tout ceci représente les spécificités dont une société a besoin pour progresser.

Plusieurs personnes qui ont été désignées sous le nom de hackers, plus précisément par les média, ou qui ont eu des problèmes après du "hacking" n'étaient pas, en effet, des hackers.

U n ***Hacker est*** une sorte de scientifique en constante expérimentation, bien que quelques fois le terme « scientifique fou » convienne puisque contrairement aux scientifiques professionnels, ils sont immergés dans la poursuite d'une sensation au lieu d'une hypothèse formelle. Cela n'est pas nécessairement une mauvaise chose. Plusieurs choses intéressante ont été conçues par des gens qui n'ont pas suivi des conventions standards concernant ce qui était connu ou accepté comme vrai à l'instant présent.

Le mathématicien, ***Georges Cantor***, a proposé de nouvelles idées sur l'infini et établi une théorie qui a semé la panique parmi ses confrères mathématiciens à telle enseigne qu'on a surnommé son idée « une grave maladie » qui infecte les mathématiques.

Nicolas Tesla est une autre personne considérée comme un « scientifique fou » à son époque, mais il en savait plus sur le comportement de l'électricité que qui conque. Il a probablement conçu le premier moteur sans balayage qui fonctionne sous un courant alternatif mais il est plus connu pour la découverte de l'***effet Tesla*** et la ***bobine de Tesla***.

Ensuite il y avait ***Ignaz Philipp Semmleweis*** qui a découvert que les médecins doivent laver leurs mains lors du passage du traitement d'un patient à un autre, afin d'éviter la propagation d'une maladie. Il s'est demander si le fait qu'une maladie se propage d'un patient à un autre n'était pas de sa faute, ainsi il a décidé d'essayer de laver ses mains après avoir visité un patient ; et sûrement, la contamination a disparu. Son idée allait aussi bien à l'encontre de toutes les conventions scientifiques sur les connaissances acquises à cette époque sur les microbes qu'à l'encontre de la complaisance des docteurs qui se sentaient embarrassés par le fait de se laver les mains à chaque fois qu'ils visitent un patient.

Ce que vous croyez connaître à propos des hackers est qu'ils peuvent s'infiltrer dans d'autres ordinateurs et pendre possession des comptes d'autres personnes. Ils peuvent lire vos courriels (Email) sans que vous ne vous en rendez compte. Ils peuvent accéder aux images prises par votre webcam sans votre permission, vous regarder et écouter dans votre supposée vie privée au sein de votre domicile. Cela n'est pas faux.

Certains hackers perçoivent la sécurité d'un réseau comme un défi, donc ils essaient de trouver des voies et moyens de contourner ou perturber le système, mais en réalité ce qu'ils essaient de faire est au-delà de l'entendement de ceux qui ont installé ou conçu le système. Leurs découvertes à propos du système dépassent leurs attentes, d'où

proviennent les instructions des systèmes, quelles sont les règles qu'ils utilisent, comment interagissent-ils avec les systèmes d'exploitation, les autres systèmes qui l'entourent, les utilisateurs qui ont accès au système et l'administrateur qui gère le système. Ensuite ils utilisent ces informations pour essayer d'obtenir ce qu'ils veulent. Ce type de hacking peut être énormément bénéfique au monde afin de savoir comment être plus sécurisé et même de concevoir de meilleur technologies.

Malheureusement bien que, quelques fois le hacking est effectué par des criminels et ce qu'ils désirent est illégal, envahissant, et destructif. Et ces hacker sont habituellement ceux dont vous entendez parlés sur les médias.

Un hacker n'est pas quelqu'un qui accède et envoie des informations à partir du compte d'une victime plus tard, lorsque cette dernière ne s'est pas déconnectée d'un réseau social ou parce qu'il a obtenu le mot de passe de la victime par un **regard de travers les épaules** (**shoulder-surfs**). Un hacker n'est pas quelqu'un qui télécharge un utilitaire de **débutant** (**script kiddie**) pour s'infiltrer dans la boîte Email de quelqu'un. Ces gens ne sont pas des hackers, ils sont juste des voleurs et des vandales.

Le hacking c'est la recherche. Avez vous déjà essayer quelque chose encore et encore de différentes manières juste pour obtenir ce que vous voulez ? Avez-vous déjà ouvert une machine ou un appareil pour voir comment il fonctionne, rechercher ce que à quoi ressemble les composants, et ainsi effectuer un changement pour voir comment le système fonctionnera différemment ? C'est ça le hacking. Vous faite du hacking lorsque vous examiner profondément comment quelque chose fonctionne afin de la modifier pour qu'elle fasse ce que vous voulez.

Il est courant que l'on rencontre plus les hackers sur INTERNET compte tenu de la manière dont il est conçu, de ses différentes énormes applications, systèmes, appareils, et processus. Vous pourriez dire dire qu'il était conçu par les hackers donc c'est le meilleur terrain de jeux des hackers. Mais ce n'est pas seulement là où on rencontre les hackers. Vous pouvez rencontrez de célèbres hackers dans presque tous les domaines de l'industrie et ils ont tous quelque chose en commun : ils passent beaucoup de temps pour comprendre le fonctionnement des choses, ainsi ils peuvent modifier ces dernières pour qu'elles fonctionnent d'une nouvelle façon. Il ne percevaient pas une chose comme l'aurait fait le concepteur originel, mais ils y voient un grand ou un meilleur potentiel et ils le piratent pour en faire quelque chose de nouveau.

Ne penser pas que vous pouvez être juste un célèbre hacker. Seulement en faisant de célèbres piratages (hacks) et avec beaucoup d'humilité vous pouvez devenir célèbres.

Le hacking en soi n'est pas illégal. Du moins pas plus que lancer une pierre soit illégale. Tout est en rapport avec l'intention. Si vous lancer une pierre et que votre intention est de blesser quelqu'un, c'est un crime. Si votre intention n'est pas de blesser quelqu'un, mais qu'il advienne qu'après votre lancé de pierre, une personne soit blessée, il se peut que ce ne soit pas un crime, mais vous êtes responsables de vos actes et vous devez payer des dommages et intérêt. Un projet d'ISECOM nommé **Hacker Profiling Project-** ou **projet d'identification d'un hacker -** a découvert que la plupart des dommages dus au hacking sont causés par des jeunes, des hackers inexpérimentés qui endommagent la propriété d'autrui par accident. Ceci est semblable au fait que l'on s'amuserait à lancer des pierres dans la rue mais en cabossant les véhicules et cassant les fenêtres au cours du

processus. Peut être que le dommage n'est pas intentionnel, mais vous devez vous attendre à en être responsable et payer pour le tort causé. Donc faites attention lorsque vous piratez la propriété d'autrui. Persévérez dans le hacking avec vos propre astuces.

Il peut être illégal de pirater quelque chose que vous avez achetée et que vous posséder. Il existe des hackers qui ont été sanctionnés pour avoir pirater leurs propres appareils et ordinateurs. Il y a des hackers qui ont piraté des programmes, musiques et films qu'ils ont achetés - et qui ont été traduits en justice à cet effet. En particulier, il se peut que vous ne soyez pas autorisés légalement à pirater un logiciel que vous avez acheté, même si c'est juste pour vérifier si ce dernier est assez sécurisé pour fonctionner sur votre ordinateur. Ceci est dû au fait que toute chose que vous achetée est suivie d'un **Contrat de l'Utilisateur Final (EULA : End User License Agreement)** qui stipule que nous n'en avez pas le droit. Vous avez approuvé ce contrat avant d'ouvrir ou d'installer le produit. Ayez toujours ceci en tête lorsque vous pratiquez du hacking à la maison sur des choses que vous avez achetées en privé.

Pourquoi Être un Hacker?

Considérons l'exemple suivant : comment les scientifiques ont-ils décodé le génome humain ? Ils ont utilisé une méthode développée pour déchiffrer les mots de passe cryptés. Les mots de passe qui sont stockés sous forme cryptée sont plus difficiles à voler. La méthode dite **attaque par force brute hiérarchique** permet de révéler de tels mots de passe en augmentant la vitesse du cassage de leur forme cryptée qui est une forme de **hachage à sens unique**. Les scientifiques du génome ont réparti ce dernier en de petites pièces et établi une correspondance une par une jusqu'à ce qu'ils ne trouvent une correspondance parfaite, et ils utilisent ensuite la correspondance parfaite pour révéler les mêmes pièces rencontrées au sein de la chaîne du génome. Cette technique de cassage basée sur la correspondance parfaite et la réutilisation permet de casser de longues listes de mots de passe cryptés plus que la technique du cassage basée sur le cassage d'un seul mot de passe à fois.

Le hacking a fait ses preuves dans les cuisines lorsque les chefs utilisent du nitrogène liquide en tant qu'agent refroidisseur pour fabriquer de très bonne glace ou lorsqu'ils piratent la nourriture pour faire des tomates frites à partir de la sauce tomate pour obtenir du ketchup ou lorsqu'ils ont besoin de faire quelque chose pour lequel ils n'ont pas l'équipement nécessaire pour ...

Les chimistes pirataient les éléments et les composants depuis des siècles. Naturellement les molécules sont méticuleuses lorsqu'il s'agit de la manière dont ils se comportent dans différents environnements (climat froid ou chaud, dans les montagnes, ou dans les profondeurs de l'océan), ainsi les chimistes ont besoin de comprendre profondément les propriétés des élément chimiques qu'ils ont à leur disposition, par conséquent ils essaient de pirater afin de former un tout avec ce qu'ils ont à leur disposition. Nulle part ceci n'est plus évident que dans l'invention de nouveaux produits pharmaceutiques, où des centaines de plantes dans une région sont étudiées pour découvrir leurs propriétés chimiques, des racines au fruits. Ensuite leurs substances chimiques sont extraites et combinées avec d'autres pour fabriquer d'autres médicaments. Ainsi ils font des essais encore et encore, quelques fois pendant des années, afin d'obtenir les bonnes combinaisons pour que ces dernières fassent ce qu'ils veulent.

Le hacking est employé dans les entreprises commerciales pour comprendre un marché ou le pouvoir d'achat de certains types de consommateurs. Elles cherchent

minutieusement les forces qui gouvernent le secteur commercial qui les concerne, puis elles essaient de changer ou d'influencer ce dernier afin d'obtenir ce qu 'elles veulent. Quelques fois elles piratent les produits, et quelque fois elles emploient des techniques de hacking sur vous (à travers les publicités et l'**influence**, des techniques que vous apprendrez dans la leçon nommée **Ingénierie Sociale**).

Le hacking devient de plus en plus une partie critique des guerres. Des soldats hautement talentueux sont pleins de ressources et créatifs dans l'accomplissent de leurs objectifs, ce qui est exactement une caractéristique des hackers. Les casseurs de codes, les analystes des services secrets et les agents de terrain utilisent des techniques qui sont fondamentalement des compétences de hacking, pour découvrir ce que possède leurs ennemis, ceux qu'ils font, et comment prendre contrôle de toute faiblesse dans leurs équipements. Étant donné que plus de pays sont informatisés, l'utilisation du hacking dans les cyber attaques et dans la défense est devenue un secteur valeureux des forces armées et des services secrets d'un pays. Les agences nationales et internationales de sécurité assistent à des conférences de hackers pour en recruter.

> La seule raison de devenir un hacker c'est parce que c'est un pouvoir. Vous pouvez faire des choses merveilleuses lorsque vous avez des compétences de hacker. N'importe quelle connaissance approfondie vous donne un grand pouvoir. Si vous connaissez la façon dont quelque chose fonctionne jusqu'au point où vous pouvez la contrôler, vous avez un sérieux pouvoir en mains. La plupart du temps, vous avez le pouvoir de vous protéger et de protéger ceux qui vous sont chers.

De plus en plus de personnes ont une vie en ligne (sur Internet) sous forme de relations, des gens trouvent des emplois, et des entrées de fonds sont faites sur INTERNET. Les informations peuvent être d'une grande valeur – ou représenter une menace – et les hackers peuvent se protéger mieux que qui conque. Ils peuvent rechercher ce qui arrive à leur données. Il peuvent s'assurer de divulguer seulement ce qu'ils veulent tout en restant généralement en sécurité et dans l'anonymat. C'est un avantage énormément compétitif dans les écoles, au boulot, et dans la vie quotidienne, parce que la plus petite perception négative peut être éventuellement utilisée contre vous. Soyez-en sûr.

> **Piratez tout mais ne faite du mal à personne.**

Comment Pirate t-on?

Vous dire comment on pirate c'est comme vous dire comment faire des mouvements de va et vient sur un balançoire : peut importe les détails de l'explication, vous ne pourrez pas réussir tout seul au premier coup. Vous devez développer des talents, la sensation, et l'intuition à travers la pratique sinon vous aurez tout le temps de la boue à la figure. Mais il y a certaines choses que nous pouvons vous dire pour vous aider et vous encourager à continuer la pratique.

Premièrement, vous devriez connaître quelques secrets sur le fonctionnement réel du hacking. Ces informations vous seront relatées dans le **document OSSTM** (www.osstm.org). Les hackers le prononcent « **aw-stem** ». OSSTM veut dire **Open Source Security Testing Methodology Manual**, pendant qu'il donne l'impression d'un manuel d'installation d'un lecteur de DVD, c'est le document principal que plusieurs hackers professionnels utilisent pour planifier et exécuter leurs attaques et défenses. Dans les profondeurs de ce document se trouvent des pierres précieuses qui ouvriront vos yeux.

Deux Façons d'Obtenir Ce que Vous Désirez

Par exemple, vous devriez savoir qu'il y a seulement deux façons d'obtenir quelque chose : vous l'obtenez vous même ou vous demandez à quelqu'un d'autre de le faire pour vous. Cela veut dire que toute possession dans le monde requiert des **interactions** entre une personne et la chose possédée. C'est évident, n'est ce pas ? Mais pensez-y. Cela veut dire que tous les mécanismes de protection doivent empêcher quelqu'un d'autre d'entrer en contact avec la chose protégée. A moins que vous n'enfermiez toute chose dans un énorme lieu sécurisé, vous ne pouvez pas arrêter toutes les interactions. Les magasins doivent poser les choses sur des étagères que les clients ne peuvent atteindre avec leurs mains. Les entreprises ont besoin d'envoyer des informations via des client de messagerie électronique qui sont connectés aux serveurs mail et envoyer des messages à d'autres serveurs mail.

Toutes ces choses sont des interactions. Certaines d'entre elles existent entre les humains et les choses qui sont familières entre elles, ainsi nous désignons ces interactions sous le terme **confiance**. Lorsque les interactions surviennent entre des personnes ou systèmes inconnues nous désignons ces interactions par le terme **accès**. Vous pouvez soit vous servir d'un accès pour obtenir ce que vous même vous voulez, ou vous pouvez manipulez quelqu'un qui a une relation de confiance avec la cible afin qu'il puisse prendre ce dont vous avez besoin et vous le remettre. Si vous analysez la situation pour un moment, cela veut dire que la sécurité signifie se protéger de ces deux choses : **ceux que nous ne connaissons pas** et **ceux que nous connaissons** i.e **ceux en qui nous avons confiance**.

Exercices

1.1 Quel type d'interactions les moteurs de recherches utilisent-ils ? Réfléchissez bien : est ce quelqu'un donne Accès ? Et ce que quelqu'un donne la Confiance ?

1.2 Donnez un exemple simple de l'utilisation de l'Accès et de la Confiance pour prendre une bicyclette verrouillée sur le porte baguage à l'arrière d'une moto.

1.3 Donnez un exemple simple de comment vous pouvez utiliser l'Accès et la Confiance pour accéder au compte Email d'une autre personne.

Étoffez Vos Connaissances: Espionnage

Lorsque le hacking est utilisé contre un gouvernement étranger pour commettre des actes criminels et des intrusions, des destructions pour être à la tête des informations politiques et militaires, cela est appelé **espionnage**. Mais lorsque le hacking est utilisé par une entreprise contre une autre entreprise se situant dans un autre pays pour être à la tête dans les affaire, cela s'appelle de l'**espionnage économique**.

Lorsque le hacking est utilisé pour acquérir des informations personnelles sur autrui afin de le faire chanter en public, on désigne cela sous le terme **DoXing**. Si une information publique est découverte pour cibler une personne ou une compagnie à titre d'attaque, mais sans aucune action criminelle ne soit menée pour obtenir l'information, on parle de **crissement de document** ou **renseignement à source ouverte** (**OSInt** : Open Source Intelligence).

Lorsque le hacking est utilisé pour comprendre le réseau d'une entreprise, ses systèmes, ses applications et ses appareils en tant que cibles d'attaques sans pour autant effectuer une intrusion réelle dans le système, cela est connu sous le nom d'**inspection réseau.**

Lorsque le hacking est utilisé pour comprendre profondément le réseau d'un concurrent sans pour autant enfreindre à aucune loi (bien que ces pratiques soient considérées comme indécentes), cela s'appelle du **renseignement compétitif.**

Vous êtes probablement choqué maintenant lorsque vous connaissez les moyens et les choses indécentes employées et qui sont jusqu'à ce jour légaux. Considérons l'exemple du fait d'infliger du stress et de la peur à quelqu'un juste pour obtenir de lui des informations. Aussi longtemps que vous emploierez ces méthodes sans les tués, le fait de leur dire des mensonges est toujours légal (bien qu'il y ait des lois qui proscrivent le fait de semer la panique dans les lieux publics tel crier « **au feu** » dans une salle de cinéma alors qu'il n'y en a pas.

Le hacker veut savoir là où une entreprise projette construire une nouvelle usine. Ensuite ils utilisent le *crissement de document* pour découvrir quelles sont les personnes stratégiques dans la prise de cette décision. Puis le hacker appelle leur bureau pour découvrir les villes par lesquelles l'entreprise est passée et peut être découvrir quelles sont les usines qu'elles ont visitées. Mais bien sûr ceux-ci représentent des informations privées d'une entreprise et personne ne leur dira cela sans déclencher les alarmes. Ainsi le hacker doit les tromper pour obtenir l'information. Il n'est pas difficile d'imaginer le processus.

Hacker : Salut, je suis Dr. Jones, et j'appelle de l'école à propos de votre fille Nancy.

Cible : Oh vraiment ? Qu'a t-elle encore fait actuellement ?

Hacker : Bien, elle a un saignement persistent du nez que nous ne pouvons arrêter. J'aimerais savoir un peu plus sur les produits chimiques auxquels elle est souvent exposée. Ces symptômes sont rares sauf dans le cas de certaines personnes exposées à certains de ces produits chimiques. Pouvez-vous nous dire quelque chose ?

Cible : (perd son sans froid)

Ceci n'est pas en réalité illégal dans la plupart des cas mais il cause du stress indésirable. Sans pour autant le mentionné, c'est juste un moyen qui permet de semer la peur dans un parent.

Le Hacking pour Prendre Contrôle du Monde

Le hacking ne concerne pas seulement les interactions. Vous le savez. Certaines personnes disent que la politique est basée sur les interactions. Peut être. Mais vous pensez probablement que le hacking sert seulement à briser la sécurité. Quelques fois c'est le cas. En réalité il s'agit de prendre contrôle de quelque chose ou de la changer aussi bien. Comprendre les interactions et ce qu'elles signifient dans le monde réel, l'utilisation des termes basiques dont nous avons parlés, est très utile lorsque vous essayer d'infiltrer, découvrir, ou même d'inventer. Pourquoi devriez vous faire cela ? Pour avoir la liberté de transformer quelque chose que vous posséder afin que cette dernière fasse ce que vous voulez. Et pour interdire à d'autres personnes de changer quelque chose que vous posséder en ce que certaines personnes désignent par sécurité (mais nous ne sommes pas ces gens).

> Quelques fois vous achetez quelque chose et la société qui en est l'auteur essayera forcément de s'assurer que vous ne pourrez pas le personnaliser ou le modifier au-delà de leurs règles. Et vous approuvez cela, lorsque vous acceptez le fait que si l'objet est cassé ou a été ouvert, vous ne pourrez espérer une réparation ou une maintenance, et même pas un remplacement venant du fabriquant. Ainsi pirater quelque chose que vous posséder vous offre plus d'opportunité que le fait de la rendre votre, cela a certainement ces avantages. Surtout si vous voulez tenir les autres à l'écart de votre possession.

Pour plusieurs personnes, la sécurité veut dire mettre en place un produit, que ce soit une serrure ou une alarme ou un pare-feu ou toute autre chose qui théoriquement les maintient en sécurité. Mais quelques fois ces produits ne fonctionnent pas comme ils devraient, viennent avec leurs propres problèmes qui ne font qu'agrandir votre **surface d'attaque,** lorsqu'un produit de sécurité devrait la minimiser. *(La Surface d'Attaque désigne tous les moyens, toutes les interactions, qui permettent à quelqu'un ou quelque chose d'être attaqué)*. Et bonne chance pour l'amélioration de ce produit sur un immense marché qui ne se soucie pas tellement des problèmes de votre produit car vous l'avez acheté tel quel et vous devez faire avec. C'est pour cela que vous pirater votre sécurité. Vous avez besoin d'analyser le produit et de découvrir ces faiblesses et comment l'améliorer pour qu'il fonctionne mieux. Ainsi vous devriez le pirater de manière un peu plus approfondi afin d'empêcher le fabriquant de le réinitialiser.

Lorsque vous considérez le hacking en terme de cassage de sécurité, souvenez vous que cela n'est qu'un secteur pour lequel le hacking est utile, parce que sans être capable de faire cela, il se peut que vous abandonniez certaines libertés ou certaines intimités dont vous ne voudrez pas vous séparer. (Et oui nous avons compris qu'il se peut que vous ne vous soucier pas pour le moment de certaines choses que vous dites ou envoyer, mais l'Internet possède une immense mémoire et cette dernière aide de mieux en mieux d'autres personnes à vous faire un rappel de vos activités passées. Ce qui va sur Internet y reste. Donc considérez ce fait pour vos actions futures si pour le moment vous n'en tenez pas compte).

Maintenant que vous avez une idée à propos des interactions, approfondissons les un peu plus. Vous connaissez les interactions de base sous les termes Accès et Confiance mais avez-vous déjà entendu parlé de la **Visibilité** ? C'est le troisième type d'interactions. Elle est aussi puissante que les deux précédentes. Dans le jargon policier, elle est simplement appelée *opportunité* mais dans le hacking cela concerne plus le fait de savoir s'il y a quelque chose avec laquelle on peut interagir ou non. Cette interaction dévoile un grand lot de nouvelles techniques de sécurité telles que la tromperie, l'illusion, et le camouflage aussi bien que de nouvelles techniques de hacking permettant de contourner ces nouvelles mesures de sécurité.

Lorsque le célèbre voleur de banque Jesse James fut interrogé pour savoir pourquoi il volait les banques, il a dit c'est parce que c'est là que se trouve l'argent. Ce qu'il voudrait dire par là est que via la Visibilité il savait qu'il y avait de l'argent quelque part dans les

banques là où d'autres objets susceptibles d'être volés ne se trouvent. Les banques ont une visibilité : les gens connaissent la valeur de leurs avoirs. Mais toute chose ne possède pas une Visibilité. Dans un jargon terre-à-terre, la discrétion est le contraire de la visibilité et c'est un moyen puissant permettant d'éviter d'être une cible. Que ce soit dans les rues dangereuses, dans la jungle, ou sur l'Internet, maintenir une moindre **exposition** et éviter la Visibilité est un moyen de se protéger contre une attaque en premier lieu.

Exercices

1.4 L'Internet est très réputé pour la création de mythes et pérenniser de fausses histoires qu'il est difficile de savoir quelle est la vraie information et quel est le canular. Donc si vous voudrez apprendre à devenir un bon hacker, prenez l'habitude de vérifier vos faits et d'apprendre la vérité à propos des choses. C'est pourquoi vous allez chercher et découvrir si Jesse James a réellement dit cela. Et ne vous arrêtez pas facilement à la réponse renvoyée par la première page web que vous trouver, chercher encore un peu plus.

Maintenant que vous êtes habitués à faire des recherches, recherchez la vérité à propos de ces choses ordinaires :

1.5 Dans la langue Inuit quelle est l'origine du mot igloo, qu'est ce que cela signifie réellement ? De quel genre d'interactions vous vous êtes servi pour trouver la réponse ?

1.6 Plusieurs parents ont vite remarqué que le sucre rend les petits enfants hyper-actifs mais est ce réellement le cas ? Quel genre d'interactions surviennent dans leur ventre lorsque les enfants consomme beaucoup de bonbons ou de nourriture sucrées qui les rendent stupides et très agiles ?

1.7 Vous auriez pu entendre que le sucre cause les caries dentaires mais est ce la vrai interaction qui a eu lieu - qu'est ce qui a réellement causé ces caries ? Est ce le sucre ou non ? Bonus :pouvez- vous dire quel genre d'interaction représente le fait de se brosser les dents dans la lutte contre la cause réelle des caries et quel est le nom d'au moins l'un des produits chimiques qui est à l'origine du problème (*conseil : le fluor est faux comme réponse*).

Le Processus à Quatre Étapes

Lorsque vous prenez les trois types d'interactions ensembles, vous obtenez la **Porosité**, la base d'une surface d'attaque. Et comme le mot l'implique, ce sont les pores ou « trous » de n'importe quelle défense que vous devez mettre en place pour que toute interaction nécessaire ait lieu (aussi bien que toutes les interactions connues ou inconnues qui auront lieu). Par exemple, un magasin a toujours besoin de mettre les produits sur des étagères afin que les clients puissent les toucher, les mettre dans un chariot et payer pour le produit choisi. Voici les interactions dont ils ont besoin pour vendre des choses. Mais il se pourrait qu'ils ne soient pas au courant du fait que des employés sortent secrètement des dispositifs de chargement, ce qui est une interaction indésirable pour l'employeur.

La porosité est une notion que vous devez maîtriser pour vous protéger ou attaquer certaines cibles. Mais elle ne suffit pas pour analyser quelque chose ou pour la pirater. Pour ce faire, vous devez avoir des notions approfondis à propos de trois interactions que vous avez déjà apprises. C'est encore un autre petit secret de OSSTM et il est connu sous le nom de **Processus à Quatre Étapes** (**FPP : Four Point Process**). Il montre quatre façons dont ces interactions sont utilisées pour analyser quelque chose le plus profondément possible, et par analyse nous voudrons dire se confronter à la chose afin que nous puissions bien l'observer et découvrir ce qui se passe.

Le Processus d'Echo

Nous grandissons en découvrant les choses et en les apprenant par interaction avec elles directement. Les petits enfants poussent la dépouille sèche d'un écureuil avec un bâton pour voir s'il est mort. Ceci est appelé **processus d'écho.** C'est la forme basique et immature d'analyse. C'est pareil au fait de crier dans une cave et de s'attendre à une

réponse. Le processus d'écho requiert que l'on effectue des différents types d'interactions d'Accès sur la cible et qu'on surveille ses réactions afin de découvrir les voies et moyens par lesquels vous pourrez interagir avec elle. Le processus d'écho est une vérification du type causes à effets.

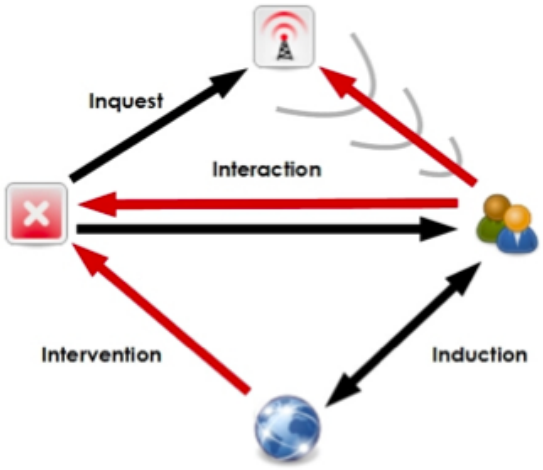

Figure 1.1: Le Processus à Quatre Étapes

C'est une façon étrange de tester quelque chose, parce que bien qu'il permette d'effectuer rapidement un test, aussi n'est-il pas si précis. Par exemple, lorsqu'on se sert du processus d'écho pour tester la sécurité, une cible qui ne répond pas est considérée comme sécurisée. C'est pareil au fait que nous n'ayons pas de Visibilité. Mais sachez que ce n'est pas parce que quelque chose ne répond pas à un type d'interaction cela ne veut pas dire qu'elle est "sécurisée". Si cela est vrai alors les opossums ne seraient jamais tués par d'autres animaux lorsqu'ils jouent au mort et tout le monde serait à l'abri des attaques d'Ours juste en passant à côté. Le fait d'éviter la visibilité devrait vous aider à survivre face à certains types d'interactions mais évidemment pas toutes.

Malheureusement, la plupart du temps les gens font leurs enquêtes quotidiennes grâce au processus d'écho seulement. Il y a tellement d'informations perdues dans ce type d'analyse unilatérale à telle enseigne que nous devrions remercier l'industrie médicale qu'elle a dépassé l'ère de la méthode de diagnostique suivante : " Avez-vous mal si je vous ça ?" Si les structures sanitaires utilisaient seulement le processus d'écho pour déterminer l'état de santé d'une personne, elles aideraient rarement les patients. L'avantage de cette méthode est que la file d'attente ne sera pas très longue dans les salles d'attentes. C'est pourquoi certains docteurs, la plupart des scientifiques, et spécialement les hackers utilisent le Processus à Quatre Étapes pour s'assurer qu'ils n'ont pas raté quelque chose.

Le Processus à Quatre Étapes dont nous avons parlé dans les interactions est énuméré comme suit :

1. **Induction** : Que pouvons nous dire à propos de la cible à partir de son environnement ? Comment ce comporte t-elle dans cet environnement ? Si la cible n'est pas influencée par son environnement, cela est aussi intéressant.
2. **Enquête :** Quels sont les signaux (émanations) venant de la cible ? Enquêtez sur toutes les pistes ou indicateurs de ces émanations. Un système ou un processus laisse une trace ou signature de ses interactions avec son environnement.
3. **Interaction** : Que se passe t-il lorsque vous poussez à bout la cible ? Cette étape fait appel aux tests d'écho, y compris les interactions attendues et inattendues avec la cible, pour provoquer des réponses.
4. **Intervention** : Jusqu'à quel point la cible résistera t-elle avant de céder ? S'interposer entre les ressources dont la source a besoin, telles l'électricité, ou se mêler de ses interactions avec d'autres systèmes pour comprendre les circonstances extrêmes sous lesquelles la cible peut continuer à fonctionner.

Revenons à notre exemple de l'hôpital...les quatre étapes du processus FPP devraient ressembler à ceci:

1. La fonction d'**interaction** est l processus d'écho au cours duquel les docteurs auscultent les patients, leurs parlent, et testent leur réflexes au niveau de leurs coudes et genoux et utilisent d'autres outils de la méthode " Avez-vous mal lorsque je vous ceci ?"
2. L'**enquête** est l'interprétation des **émanations** du patient telles que l'impulsion cardiaque, la pression artérielle, les ondes cérébrales.
3. L'intervention est le fait de modifier ou de stresser l'homéostasie (stabilité physiologique) du patient, son comportement, son habitude, ou son niveau de stabilité pour voir ce qui se passe.
4. Et finalement l'induction, qui est l'analyse de l'environnement, des lieux que la personne a visités avant de faire la maladie et comment ils affectent le patient, tels que ce qu'il aurait pu toucher, manger ou inhaler.

Exercise

1.8 Tel que vous le voyez, le Processus à Quatre Étapes vous permet d'analyser profondément les interactions. Maintenant vous pouvez l'essayer. Expliquer comment vous pourriez vous servir du Processus à Quatre Étapes pour vérifier si une montre fonctionne – et si elle fonctionne correctement en donnant l'heure exacte.

Que faut-il pirater ?

Lorsque vous êtes entrain de pirater tout, vous devez établir des règles de base. Vous avez besoin de comprendre la langue et les concepts pour connaître réellement ce que vous piratez. Le **champ d'actions** est une expression que nous utilisons pour décrire tout l'environnement d'exploitation possible, qui représente en outre, chaque interaction qu'a l'objet que vous voulez pirater.

Etoffez Vos Connaissances: les Classes et les Canaux

Dans le jargon professionnel (très utile aussi pour les hackers), le champ d'action est constitué de trois **classes** qui sont à leur tour réparties en quatre **canaux :**

Classe	Canal
Sécurité Physique (PHYSSEC)	Homme
	Physique
Sécurité Spectrale (SPECSEC)	Réseau Sans Fil
Sécurité des Communications (COMSEC)	Télécommunications
	Réseaux de Données

Les classes ne représentent pas quelque chose dont il faut avoir peur mais elle représentent les dénominations officielles qui sont actuellement utilisées dans l'industrie de la sécurité, dans les gouvernements, et dans le domaine militaire. Les classes définissent un champ d'études, d'enquêtes, ou d'opérations. Par conséquent si vous recherchez plus d'informations sur un sujet, il est préférable de savoir comment le processus désigne cet objet.

Les canaux sont des termes habituels utilisés pour désigner la manière dont vous entrez en interaction avec les acquis. Il n'est pas inhabituel de pirater un gadget en utilisant le Processus à Quatre Étapes pour chaque Canal. Évidemment cela semble donner plus de tâches, mais pensez à combien il serait émouvant lorsque vous découvrez un moyen de le faire fonctionner d'une autre façon qui n'est listée dans aucun manuel, ou mieux, inconnue du fabriquant.

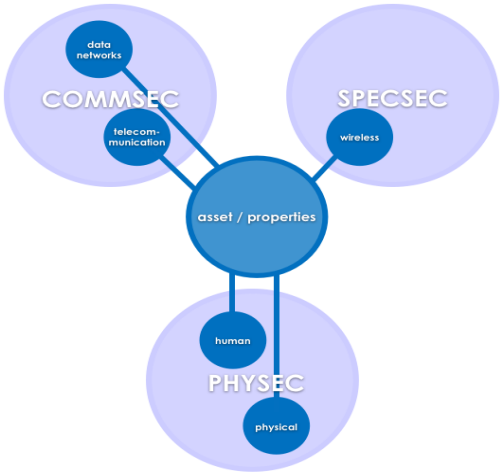

Figure 1.2: le Champ d'Actions

Un **Acquis** peut être toute chose qui a une valeur aux yeux du propriétaire. Cela peut être une propriété physique telle que l'or, les gens, les plans, les ordinateurs portables, le téléphone à 900MHz de fréquence, de l'argent, ou de la propriété intellectuelle telle que les données personnelles, une relation, une marque, des procédures d'entreprise, des mots de passe, et une conversation via le téléphone de 900MHz.

Les **dépendances** représentes les choses qui sont au-delà de la capacité du propriétaire de les fournir indépendamment. Par exemple, ce ne sont pas tous les utilisateurs d'ordinateur qui produisent leur propre électricité. Même s'il n'est pas probable que quelqu'un vous coupe l'électricité, elle demeure toujours dans votre champ d'action.

L'objectif de la sécurité est la **Séparation** entre les acquis et aussi bien entre leurs dépendances, et entre toutes menaces respectivement relatives à eux.

Nous disons que la sécurité est une fonction de séparation. Il existe quatre façons de créer cette séparation :

- Déplacer l'acquis pour créer une barrière entre lui et les menaces.
- Mettre la menace dans un état inoffensif.
- Détruire la menace.
- Détruire l'acquis. (Non recommandé!)

Lorsque nous faisons du hacking nous recherchons les endroits où les interactions avec la cible sont possibles, et là où elles sont impossibles. Pensez aux portes d'un immeuble. Certaines sont nécessaires aux travailleurs ; d'autres le sont aux clients. Certaines peuvent être nécessaires à titre d'échappatoire en cas d'incendie. Et il se peut que certaines ne soient pas du tout utiles.

Toute porte, est pourtant un point d'interaction, un point qui favorise les opérations nécessaires et les indésirables telles que le vol. Lorsque nous venons sur la scène en tant que hacker, nous ne nous précipitons pas vous connaître les raisons d'existence de ces point d'interactions, sur ce nous les analysons à l'aide du Processus à Quatre Étapes.

Prenons l'exemple de quelqu'un qui désire se protéger totalement de la foudre. Le seul moyen de réaliser cela (pendant que nous sommes sur la terre) c'est d'accéder à une

caverne dans une montagne où il est complètement impossible à la foudre de traverser toutes ces couches de saletés et de roches. Si nous supposons qu'il n'en sortira plus, alors nous pouvons dire qu'il est à 100 % en sécurité. Mais si nous commençons à percer des trous dans la montagne, la foudre aura de nouveau chaque trou comme point d'accès, et la porosité augmente. Le document OSSTMM fait la différence entre être **à l'abri** de la foudre et être **protégé** contre elle. Le simple fait est que plus il y existera de porosité, plus probable sera le fait qu'un hacker effectue des modifications et contrôle ce qu'il veut.

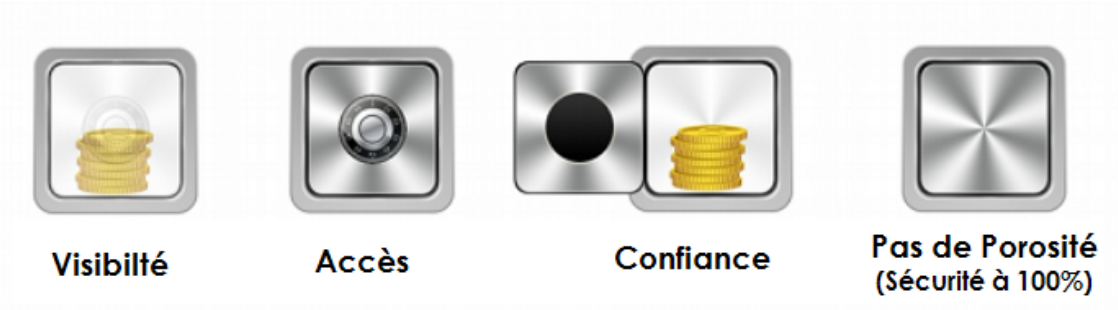

Figure 1.3: La Porosité

Étoffez Vos Connaissances: La Porosité

Voici des exemples qui montrent comment on peut localiser la porosité, la classifier et la déterminer dans un processus de piratage.

Terme	Définition
Visibilité	Lorsque la police enquête sur un crime, elle recherche les *moyens, le motif, et l'opportunité*. Si un acquis est visible, il peut être attaqué mais s'il ne l'est pas, il ne peut pas être ciblé – bien qu'il puisse être découvert. Certains professionnels de la sécurité préfère dire que le **camouflage** est une mauvaise pratique de sécurité parce qu'il ne protège rien, il le cache seulement. Mais cela n'est pas surtout une mauvaise chose puisque vous n'avez pas besoin d'une réponse de sécurité permanente. Pour ce faire le document **OSSTMM** offre ce petit joyau : "*Une sécurité ne doit pas être éternelle, du moins pas plus que quelque chose d'autre qui pourrait remarquer son absence*".
Accès	L'Accès représente le nombre d'endroits où les interactions peuvent subvenir hors du champ d'actions. Dans le cas d'un immeuble, cela peut être les portes qui débouchent sur une rue ou une fenêtre et pour un serveur connecté à Internet cela pourrait être le nombre de ports réseau ouverts ou les services (processus) disponibles sur l'ordinateur.
Confiance	On parle de confiance lorsqu'une entité accepte librement une interaction avec une autre entité dans le champ d'actions. C'est pourquoi vous ne demandez pas à votre mère son identité lorsqu'elle vient vous embrasser. C'est pourquoi vous la soupçonner pas d'avoir empoisonner votre nourriture. Vous avez appris à avoir confiance en les choses qui résident dans votre champ d'actions. Ainsi un jour elle perd contrôle d'elle même et empoisonne votre nourriture, vous la mangerez sans suspecter quoique ce soit. Donc la confiance est à la fois une faille de sécurité et un substitut habituel pour l'authentification, la voie par laquelle nous vérifions si quelqu'un est celui que nous connaissons. La confiance est un sujet étrange parce que c'est un acte humain à accomplir et elle est assez importante en société. Sans la confiance, nous ne pourrions pas interagir librement. Mais à cause de la confiance, nous sommes facilement manipulés, volés, et victimes de mensonges. Les recherches de OSSTMM sur la confiance ont montré qu'il y a 10 raisons nommées **Propriétés de Confiance,** pour croire en quelqu'un et si les dix raisons sont satisfaites, nous pouvons faire confiance en toute sécurité sans avoir aucune crainte. Mais cette même recherche a prouvé que la plupart des gens ont juste besoin qu'une seule raison de confiance soit satisfaite et ceux qui sont réellement paranoïaques ou cyniques ont besoin que trois raisons de confiance soient satisfaites pour qu'ils aient confiance.

Les Ressources

Une recherche, une étude efficace et une analyse critique sont les compétences clé d'un hacker. Le hacking est en réalité, un processus de création qui est plus basé sur un style de vie que sur une leçon. Nous ne pouvons pas vous enseignez tout ce dont vous avez besoin de savoir, mais nous pouvons vous aidez à reconnaître ce dont vous avez besoin d'apprendre. Puisque la science évolue très vite, il se peut que ce que nous vous

enseignons aujourd'hui ne puisse pas être utile demain. Il est mieux pour vous d'adopter les habitudes d'études d'un hacker, qui sont probablement la partie la plus vital du hacking, et qui fera la distinction entre vous et le **script kiddie** (*une expression qui désigne une personne qui utilise les outils sans savoir comment ou pourquoi ils fonctionnent)*.

Si vous rencontrez un mot ou un concept que vous ne comprenez pas dans cette leçon, il est essentiel que vous fassiez des recherches dessus. Le fait d'ignorer les nouveaux mots ne fera que vous rendre difficile la compréhension des concepts dans les leçons à venir. On vous demandera d'enquêter sur un sujet et on attendra que vous utilisiez ces informations découvertes pour résoudre complètement les exercices de cette leçon – mais ces leçons ne vous expliquerons pas comment faire ces recherches. Donc soyez-en sûr que vous passerez le temps nécessaire dont vous avez besoin pour exploiter les nombreuses ressources qui sont à votre disposition.

Les Livres

Vous devriez être surpris que nous ne vous renvoyons pas directement vers l'Internet, les livres représentent un grand moyen pour apprendre la base de toute science concernant tout ce que vous voulez explorer. Voulez-vous apprendre quelque chose à propos de l'Informatique, telle que les détails matériels de votre PC ? Rien ne vous aidera plus que la lecture d'un livre qui traite ce sujet. Le principal problème avec les livres d'informatique c'est qu'ils sont très rapidement dépassés. Le secret est d'apprendre à reconnaître la structure fondamentale qui se trouve en dessous de la légère couche externe des détails. MS-DOS et Windows sont complètement différents, mais tous les deux sont basés sur les principes de Logique de Boole qui gouverne les ordinateurs depuis l'époque d'Ada, la Comtesse de Lovelace, qui a écrit les tous premiers programmes informatiques au 19^{e} siècle. Il se peut que les concepts en matière de sécurité et de vie privée aient changé au cours de ces 2500 dernières années, mais le livre intitulé **L'Art de la Guerre** de **Sun Tzu** couvre des principes fondamentaux qui sont encore applicables aujourd'hui. (A propos il n'y a pas une façon plus rapide de ressembler à un **n00b** que de citer Sun Tzu. Ce sont des choses que devriez apprendre à utiliser mais ne pas en parler. Et citer juste L'Art de la Guerre prouve que vous n'avez pas réellement lu L'Art de la la Guerre parce Sun Tzu a même dit de garder votre vrai connaissance secrète.)

Bien que les informations rencontrées dans les livres ne soient pas à jour comme celles provenant d'autres sources, il se peut que ces informations soient mieux écrites que celles venant d'autres sources. Quelques fois elles sont plus précises aussi. Un écrivain qui passe presque une année à rédiger un livre vérifie probablement les informations que quelqu'un qui met à jour un blog six fois par jour. (Confer la Section sur les Zines et les Bolgs pour plus d'informations).

Mais rappelez-vous – précis ne veut pas dire impartial. Il se pourrait que les sources d'informations de l'auteur ne soient pas impartiales. "Les livres d'histoire sont écrits par les vainqueurs" (rechercher cette citation), et il se peut que les mêmes détiennent la vérité lorsque les normes politiques et sociales de l'époque interdisent la publication de certaines informations. C'est ce qui se passe habituellement lorsque des livres scolaires sont choisis via un processus politique et considérés comme contenant des informations acceptables par la société. Ne penser pas que vous avez découvert une vérité sacrée parce que vous l'avez lu dans un livre. La vérité est que n'importe qui peut écrire un livre et chaque livre peut contenir une version de la vérité propre à chacun.

Ne regarder pas un livre et ne vous décourager pas avant d'avoir commencer sa lecture parce qu'il est trop volumineux. Personne ne lit la plupart de ses livres volumineux que vous voyez, de chapitre en chapitre. **Considérez les comme des pages web préhistoriques.** Ouvrez-en un et accéder de façon aléatoire à une page et commencer à lire. Si vous ne comprenez pas quelque chose, revenez en arrière et recherchez son explication (ou sauter directement sur quelque chose qui a un sens). Parcourez le document vers l'arrière et vers l'avant comme si vous parcourez les liens d'une page web. Ce type de recherche non-linéaire est souvent plus intéressante et satisfaisante pour les hackers, puisque c'est juste pour satisfaire votre curiosité et non votre envie de lire.

Finalement, une chose que les lecteurs tirent comme profit des livres c'est la compétence d'une bonne rédaction. C'est un énorme avantage lorsque vous essayez de comprendre et d'embraser un nouveau domaine. La lecture permet de cultiver l'éloquence, surtout lorsque vous êtes en face des gens qui sont en position de force, ou des autorités.

Les Magasines et les Journaux

Les Magasines et les Journaux sont énormément utilisés pour fournir une information concise et précise dans le temps. Ces deux types de publications peuvent être brèves dans les détails. Sachez aussi que chaque journal ou magasine a son propre auditoire et programme ou thème, sans tenir compte du fait de prétendre être "juste et impartial". Sachez qu'un thème d'un magasine de Linux n'est nécessairement pas une bonne source d'informations sur Microsoft Windows, parce Windows est un thème qui entre conflit avec le précédent(un système d'exploitation concurrent), et franchement parlant, les lecteurs des magasines sur Linux aiment toujours lire des titres à propos de la supériorité de Linux. Plusieurs magasines emploient un choix par complaisance, une technique qui leur permet de mettre en évidence seulement les aspects positifs de quelque chose qui convient au thème du magasine ou les aspects négatifs de quelque chose qui ne convient pas au thème du magasine.

Méfiez-vous de la non impartialité possible des publications. C'est là où l'on vous donne des opinions au lieu des faits réels ou des faits provenant d'une histoire qui convient à leurs opinions ou ainsi vous ne pourrez pas formuler votre propre opinion. Considérez la source ! Même des périodiques qui paraissent neutres peuvent être pleins de spéculation et de non-impartialité, une bonne manière de dire "des devinettes instructives" mais il s'agit le plus souvent juste de "devinettes" de la part du journaliste.

Il existe une énorme mouvement dans le domaine médical qui exige que tous les essais médicaux et pharmaceutiques soient publiés (ou du moins tous les essais financés par des fonds publiques) même s'il sont couronnés d'échecs afin que les médecins puissent faire plus de choix judicieux concernant l'utilisation d'un médicament ou d'une méthode de traitement. Pendant que les journaux médicaux actuels essaient de publier des "faits" provenant des recherches d'essais, les détails et les circonstances qui se trouvent derrière ces faits sont toujours nuancés. Cela est très important lorsque vous traitez des sujets qui sont basés sur les causes principales. La relation de cause à effet requiert que les causes précèdent et qu'elles soient les raisons pour l'effet.

Une autre astuce utilisée par les périodiques (à la fois par mégarde et exprès) sont les **évidences anecdotiques**, qui sont des opinions venant des gens et qui sont publiées comme évidences ou preuves sans tenir compte du fait qu'elles soient des experts ou non ; l'**évidence autoritaire**, dans laquelle les employés d'une industrie représentés en tant qu'experts donnent leurs opinions, ou ceux qui sont des autorités dans un secteur offrent

leur opinion dans un autre secteur ou ils n'ont pas d'expertise ; et finalement, les spéculations, qui déguisent quelque chose comme vrai parce que "tout le monde" y croit comme vérité, bien qu'il n'y ait pas d'attribution réelle à une personne donnée.

La meilleure façon de résoudre les problème de précisions et d'ordre du jour est une bonne et grande lecture. Si vous lisez quelque chose à propos d'une parution dans un magasine, approfondissez votre lecture plus tard. Considérez une partie de la parution, et recherchez les confirmations ; ensuite prenez l'autre partie, et recherchez les résultats. Certaines cultures font ceci par défaut. Le fait de chercher l'autre face de l'histoire fait parti de leur habitudes sociales. C'est en réalité une puissante spécificité culturelle, surtout si vous essayez d'assurer une démocratie réussie.

Exercices

1.9 Cherchez sur Internet trois magasines qui parlent du hacking. Comment trouvez-vous ces magasines ?

1.10 Ces magasines parlent-ils tous du piratage informatique ? Qu'offrent-ils d'autre qui puissent être utile dans d'autres domaines ou d'autre entreprises ?

Etoffer Vos Connaissance: les Spéculations

Le paragraphe suivant provient d'un article de journal qui parle du vol. Pouvez-vous découvrir la Spéculation ? Notez les parties que vous suspectez :

Les banques Lake Meadow et Mortgage Lender ont été victimes d'un vol dans l'après-midi du Mardi lorsque des hommes cagoulés et armés y sont rentrés juste un peu avant la fermeture et ont pris en otage pendant une heure avant qu'ils n'obtiennent ce pourquoi ils sont venus, dans un ancien model SUV. Aucun des otages n'a été déclaré blessé.

Personne n'était en mesure d'identifier les hommes armés ce qui pousse la police à qualifier l'acte de professionnel puis-qu'après le vol, leur véhicule était aperçu derrière la banque et avançait vers le sud à travers les énormes bois de Blue Green Mountains. Les policiers recherchent probablement des voleurs expérimentés qui ont une ou plusieurs fois fait la prison et qui ont des relations avec des gens qui s'y trouvent.

Avec une moyenne de 57 vols commis dans les banques selon des rapports journaliers dans ce pays et la population de la conté de Bluegreen selon les rapports dépassera les 50.000 l'année prochaine, ceci pourrait être le début téméraire du vol des banques dans cette région. "Ceci ressemble à l'apparition d'une tendance." disait le commissaire de police, Mr Smith.

Étant donné que nous devenons de plus en plus désensibilisé à propos des spéculations et devenons fonctionnellement ignorant des partialités dans les statistiques et les résultats, le futur de toutes nos nouvelles proviendraient aussi bien d'un seul journaliste qui se mettrait à spéculer sur des histoires au moment où elles se déroulent. Dans l'exemple ci-dessus, il n'y a qu'un seul vrai fait – une banque a été volée dans l'après-midi du Mardi. Maintenant pour l'amour de l'évidence, voici ce à quoi ressemblerait cette histoire si nous changions toute la spéculation pour en faire quelque chose de plus ridicule :

Les banques Lake Meadow et Mortgage Lender ont été victimes d'un vol dans l'après-midi du Mardi lorsque des poulets apparemment cagoulés et armés y sont rentrés juste un peu avant la fermeture et ont pris en otage pendant une décennie avant qu'il n'obtienne ce pourquoi ils sont venus dans un ballon en forme de poulailler. Aucun des otages n'a été déclaré recouverts par les plumes.

Personne n'était en mesure d'identifier les poulets ce qui pousse la police à croire qu'ils ont parmi eux un artiste professionnel déguisé pour devenir un parfait aérostier après le vol, un ballon mongolfière était aperçu au-dessus la banque et volait vers le sud à travers la toundra de l'Antarctique. Les policiers recherchent probablement un artiste expérimenté qui a aussi une passion pour les ballons.

Avec une moyenne de 57 vols commis dans les banques selon des rapports journaliers dans ce pays et l'industrie des ballons dont les rapports montrent une vente qui atteindra les 47 millions de gaz dans les jours à venir, ceci pourrait être le début téméraire du vol des banques par l'utilisation de ballons. "Ceci ressemble à l'apparition d'une tendance." disait le commissaire de police, Mr Gordon.

Avec l'utilisation accablante des spéculations et des statistiques dans toutes les industries il n'est pas étonnant que cela affecte aussi l'industrie de la sécurité avec un très grand impact. Le terme le plus souvent utilisé dans cette industrie est **PID** qui est un acronyme de **Peur, Incertitude,** et **Doute**. C'est la façon dont la spéculation et l'analyse subjective du risque sont utilisées en Sécurité pour attirer votre attention sur un intérêt et vendre des solutions de sécurité. Malheureusement cela fonctionne à merveille avec la paranoïa primitive qui est dans la psyché (âme) humaine et un engourdissement grandissant dans la spéculation. Ceci a occasionné des solutions de sécurité inappropriées, une sécurité appliquée inappropriée, des contrôles réactifs de sécurité, et de fausses confiances en les autorités. Il existe évidemment un échec dans les compétences de pensées critiques au sein de la population et ceci est exploité par le secteur commercial et les criminels.

Les Moteurs de Recherches

Google est un moteur de recherche bien connu mais il n'est pas le seul qui existe. Bing en est aussi un bon lorsqu'il s'agit de faire des recherches sous la forme de questions simples et Yahoo est bon pour faire des recherche approfondis. Sachez que ces services web veulent à tout prix savoir dans la mesure du possible,tout vous concernant, et probablement en savoir plus qu'ils ne devraient. Ils enregistrerons vos recherches et les sites web que vous visitez après votre recherche.

Il existe des moteurs de recherche comme **AltaVista** et **DuckDuckGo** qui peuvent vous fournir un peu - ou plus d'anonymat, qui est une bonne chose lorsque vous essayer de voir dans l'obscurité.

Les sites web peuvent être accessibles pendant qu'ils sont en ligne et habituellement après cela. Typiquement ils sont préservés sous la forme de **pages mise en cache**. *Un cache Internet est un enregistrement en ligne des version précédentes des sites web, qui sont passée dans l'oubliette*. Les moteurs de recherches et les sites d'archives retiennent ces informations indéfiniment, ce qui signifie dans le jargon d'Internet "infiniment". C'est quelque chose de très important dont il faut vous rappelez avant d'envoyer n'importe quoi sur Internet : cela ne disparaîtra jamais. Jamais. Il se peut que vous recherchiez une copie mise en cache d'une page. Google, par exemple, avait l'habitude de mettre l'étiquette "Cache" devant le lien habituel vers le résultat. Ceci a changé pour devenir un menu sous la forme d'info bulle sur la droite, et il se peut que cette technique ait changé pendant que vous lisez ce texte.

A côté des moteur de recherches, il existe aussi des caches publiques très utiles telles que l'**Archive Internet** qui est se trouve à l'adresse **http://www.archive.org**. Vous pouvez voir des versions mise en cache de tout un site web pendant des années, ce qui est très utile pour rechercher les informations qui ont "disparu".

Une dernière remarque sur les sites web : ne supposer pas que vous pouvez faire confiance à un site web juste parce qu'il apparaît dans les résultat d'un moteur de recherche. Plusieurs attaques de hacker et des virus sont propagés juste par une simple visite d'un site web ou par le téléchargement de programmes qui apparaissent innocents, d'économiseur d'écran ou de n'importe quel fichier partagé. Vous pouvez vous protéger en ne téléchargeant pas des programmes sur des sites web qui ne sont pas dignes de confiance, et en vous assurant que votre navigateur fonctionne dans une **sandbox**. Mais il se peut que ceci ne soit pas suffisant. Un navigateur dans une fenêtre qui débouche sur Internet et comme à travers n'importe quelle fenêtre, des mauvaises choses peuvent y

passer à travers, juste parce qu'elles sont ouvertes. Quelques fois vous ne serez pas au courant de ce qui se passe avant qu'il ne soit trop tard.

Exercices

1.11 Il existe plusieurs moteur de recherches. Certains sont bon pour accéder au site web invisible, les zones d'Internet qui sont difficiles d'accès à la plus part des moteurs de recherche, telle que les bases de données privées. Un bon chercheur doit savoir comment se servir de tous ces moteurs de recherche. Certains sites web sont spécialisés dans le pistage des moteurs de recherches. Donc recherchez 5 moteurs de recherches que vous n'avez jamais utilisés ou entendu parler.

1.12 Il existe aussi des moteurs de recherche qui recherchent d'autre moteurs. On les appelle des **méta moteur de recherches**. Recherchez l'un de ces méta moteur de recherches.

1.13 Faites une recherche sur "sécurité et hacking" (y compris les griffes et notez les trois première réponses. Quelle différence y a t-il lorsque vous effectuez cette même recherche mais en OMETTANT les griffes ?

1.14 La recherche d'un thème est très différent de celle d'un mot ou d'une phrase. Dans l'exercice précédent, vous avez recherché une expression ou une phrase. Maintenant vous allez rechercher une idée.

Faites ceci, **penser aux phrases que l'on rencontrerait sur la page que vous recherchez**. Si vous voulez que le moteur vous donne une liste des magasines en ligne qui parlent du hacking, vous n'irez pas plus loin en recherchant par exemple "une liste des magasines en ligne qui parlent du hacking". Ce ne sont pas toutes les pages web qui contiendrons cette phrase. Vous obtiendrez quelque chose mais pas assez pour vos recherches.

Par contre, pensez comme ceci, "Si j'étais entrain de rédiger un magasine sur le hacking, à quoi ressemblerait une phrase typique dans ce magasine ? Combinez ces mots et phrase dans un moteur de recherches et observez ceux qui fournissent les meilleurs résultats pour votre recherche :

1.ma liste de magasines préférés sur le hacking

2.liste des magasines professionnels de hacking

3. ressources pour les hackers

4. magasine de hacking

5. magasine hacking sécurité liste ressources

1.15 Retrouvez le site web le plus ancien de Mozilla à partir de l'Archive d'Internet. Pour ce faire vous devez rechercher "www.mozilla.org" sur le site web qui se trouve à l'adresse http://www.archive.org.

1.16 Maintenant pour résumer tout ceci, disons que vous voulez télécharger la version 1 du navigateur web Netscape. Servez-vous des moteurs de recherche et des archives d'Internet, observer les résultats et voyez si pouvez télécharger la version 1.

Les Sites Web et les Applications Web

Le standard de facto pour partager les informations est via l'utilisation d'un navigateur web. Pendant que nous classons toute chose que nous voyons comme "le web", ce que nous utilisons de plus en plus sont des "applications web", puisque tout ce qui se trouve sur le web n'est pas un site web. Si vous consulter votre boîte de courriel via un navigateur web, ou obtenez de la musique via un service connecté au web, vous utilisez une application web.

Quelques fois les applications web requièrent des privilèges. Cela veut dire que vous avez besoin d'un nom d'utilisateur et d'un mot de passe pour y accéder. Le fait d'y avoir accès

lorsque vous en avez le droit est désigné par l'expression *avoir des* ***privilèges***. Pirater un site web afin de modifier une page voudrait dire que vous avez accès, puisque ce n'est pas un accès légal, vous n'avez pas un accès privilégier. Aussi longtemps que vous utiliserez le web, vous découvrirez des pages qui donnent accès à des zones privilégiées par accident.

Lorsque vous découvrez de telles choses, c'est une bonne manière de le notifier à l'administrateur du site web. Cependant, faites attention aux répercussions de la loi. Malheureusement, plusieurs administrateurs se sentent mal à l'aise face à des rapports de vulnérabilités indésirés.

> Il existe des moteurs de recherche comme **AltaVista** et **DuckDuckGo** qui peuvent vous fournir un peu - ou plus d'anonymat, qui est une bonne chose lorsque vous essayer de voir dans l'obscurité.

Exercices

1.17 Utilisez un moteur de recherche pour retrouver des sites web qui ont commis l'erreur de donner un accès privilégié à tout le monde. Pour ce faire, nous rechercherons les dossiers qui nous permettent afficher leur contenu, quelque chose qui ne devrait pas être autorisé. Par conséquent nous utiliserons certaines astuces de commandes GOOGLE à l'adresse http://www.google.com. Saisissez ceci dans la barre de recherche de Google :

```
allintitle : ''index of'' .js
```

1.18 Parcourez les résultats obtenus et vous pourrez trouvez un qui ressemble à l'affichage du contenu d'un dossier. Ce type de recherche est connu sous le nom de Google Hacking.

1.19 Pouvez-vous retrouver d'autre types de documents par cette même méthode ? Recherchez plus de trois contenus de dossiers qui contiennent des fichiers dont les extension respectives sont .xls, .doc et .avi.

1.20 Existe t-il d'autres options comme “allintitle:”? Comment pouvez vous les trouver?

Les Zines

Aussi connus sous le terme **e-zines**, sont les descendants des **fanzines** : ce sont de petits magasines souvent gratuits avec de très petites productions (moins de 10.000 lecteurs) et souvent rédigés par des journalistes passionnés et amateurs. Les fanzines étaient imprimés sur papier. Les Zines sur Internet, tels que les célèbres web zine **2600** ou le **Phrack,** sont rédigés par des volontaires ; souvent cela veut dire que les producteurs ne rédigent pas de contenu pour des erreurs non-techniques. Quelques fois le langage soutenu de ces publications peuvent être surprenant pour ceux qui ne sont pas habitués à ce genre de revues.

> Les Zines ont souvent des thèmes et des ordres du jour pertinents, et ont tendance à avoir des idées bien arrêtées. Cependant, ils montrent et argumentent probablement sur les deux faces des problèmes puis qu’habituellement ils ne se soucient pas de plaire aux annonceurs et aux abonnés.

Exercices

1.21 Recherchez sur l'Internet, trois zine qui parlent du hacking. Comment aviez-vous trouvé ces zine ?

Pourquoi vous les avez classé en tant que zine ? Souvenez-vous juste parce que le marché est zine ou le fait d'avoir mis "zine" dans le titre ne veut pas dire que c'en est un.

Les Blogs

Ils peuvent être considérés comme une évolution des zines, habituellement ils ont un staff de rédaction axé autour d'une seule personne. Les blogs sont le plus souvent mise à jour qu'une publication imprimée ou les zines, et créent souvent des communautés pour des thèmes pertinent. Il est aussi important de lire les commentaires que les sujets postés. Sur les blogs, la réponse est souvent immédiate et constitue une idée arrêtée que dans les Zines, avec des commentaires qui viennent de partout. Ceci est l'une des principales caractéristiques des blogs.

Il existe des millions de blog sur l'Internet, mais seulement une centaine d'entre eux sont actifs. Cependant, les informations sur presque tous ces blogs, sont toujours disponibles.

Exercices

1.22 Cherchez sur Internet, trois blogs qui parlent du hacking.

1.23 Quels sont les groupes avec lesquels ces blogs sont en relation ?

1.24 Y-a -t-il un thème sur la sécurité, la législation ou un thème académique ?

Les Forums et les Listes de Courriels

Les forums et les listes de courriels sont habituellement des médias développés, un peu comme l'enregistrement des conversations dans une fête. Soyez un peu sceptique à propos de tout ce que vous lisez sur ces médias. Les conversations changent fréquemment d'idées, un peu comme si ce sont des rumeurs qui circulaient, certaines personnes parlent à voix basse, il se pourrait qu'une guerre du feu éclate, et à la fin de la discussion, personne ne sait qui a dit quoi. Ces médias sont similaires, parce qu'il existe plusieurs moyens par lesquels les gens donnent des informations non précises – quelques fois intentionnellement – et il existe des moyens par lesquels des gens y participent de façon anonyme. Puisque les thème et les sujets y varient rapidement, il faut parcourir toute la discussion pour obtenir de bonnes informations et non les quelques premières discussions.

Vous pouvez trouver des forums sur presque n'importe quel thème, et plusieurs magasines en ligne et journaux offrent des forums aux lecteurs pour y mettre les réponses aux articles publiés. Dans cette optique, les forums sont d'une grande valeur pour avoir plusieurs opinions sur un article, peu importe le nombre de gens qui aiment cet article, car il y a certainement quelqu'un qui n'aime pas un article.

Il existe plusieurs listes de courriels sur des thèmes spéciaux, mais ils peuvent être difficiles à trouver. Quelques fois la meilleur technique consiste à chercher une information sur un thème particulier pour trouver une liste de courriels communautaire qui en parle.

En tant que hacker, ce qui est le plus important à savoir est que plusieurs forums et listes de courriels ne sont pas accessibles via la recherche à travers un moteur de recherche. Pendant que vous pourriez trouver un forum grâce à un moteur de recherche, il se peut que vous n'y trouvez par les commentaires individuels. Ces informations font parti de la

partie invisible du web parce qu'elles contiennent des donnes qui ne sont retrouvables qu'à partir du site web ou du forum.

Exercices

1.25 Cherchez deux forums de hacker. Comment avez-vous trouvé ces forums ?

Pouvez-vous déterminer les thèmes et les sujets spéciaux de ces sites web ?

Est ce que le thème de ces forums reflète le thème du site web qui les héberge ?

1.26 Cherchez deux listes de courriels sur le hacking ou la sécurité.

Qui est le "propriétaire" de ces listes de courriels ? Pouvez-vous voir les membres de la liste ? (Il se pourrait que ayez besoin de savoir l'application qui a permis de développer la liste et de chercher sur le web, les commandes cachées permettant de voir la liste des membres sur ce type de liste de courriel).

Sur quelle liste pourriez-vous espérer obtenir des informations qui contiennent plus les faits et qui sont impartiales ?

Les Newsgroups

Les **newsgroups** existent depuis longtemps sur le web. Il y en existe qui datent d'une époque précédant la naissance du web. Google a racheté la quasi totalité des newsgroups et les a mis en ligne à l'adresse http://groups.google.com. Ils sont semblables aux archives des listes ce courriels mais sans la fonction de courriel. Les gens y envoient directement des commentaires comme sur des sites web. Vous y trouverez des commentaires qui datent des années 90.

> Comme des archives, les archives du groupe peuvent être d'une grande valeur pour retrouver le vrai auteur d'une idée ou d'un produit. Elles sont très utiles pour retrouver les informations cachées qui ne seraient jamais disponibles sur un site web.

Les newsgroup ne sont pas moins utilisés aujourd'hui qu'il y a quelques années, afin que le web ne devienne le moyen principal pour partager l'information. Cependant, ils n'ont pas grandi étant donné que leur popularité fut remplacée par celle des services web comme les blogs et les forums.

Exercises

1.27 Grâce à Google, retrouver le plus ancien commentaire d'un newsgroup sur le hacking.

1.28 Retrouvez d'autres moyens permettant d'utiliser les newsgroups. Existe t-il des applications que vous pouvez utiliser pour accéder aux newsgroups ?

1.29 Combien de newsgroups pouvez-vous trouver et qui parlent du hacking ?

1.30 Pouvez-vous trouver la liste actuelle des différents newsgroups qui existent actuellement ?

Les Wikis

Les Wikis représentent un nouveau phénomène sur l'Internet. Wikipedia (www.wikipedia.org) en est probablement le plus célèbre, mais il y en a plusieurs. Comme plusieurs sites, les wikis sont élaborés par des communautés. Les rapports affirment souvent que les wikis manquent de précision parce qu'ils sont alimentés par des amateurs et fanatiques. Mais ceci est aussi vrai pour les livres, les listes de courriels, les magasines, et autres. C'est qu'il est important de savoir c'est que les experts ne sont pas la seule source d'informations exactes. D'après OSSTMM, les faits proviennent d'un processus contenant des petites étapes qui permet de vérifier les faits et non d'un grand pas vers la

découverte. C'est pourquoi les wikis représentent une grande source d'idées de professionnels et d'amateurs et progressivement permettent la vérification mutuelle de ces idées.

Les wikis parlent souvent des deux faces d'un sujet et vous permettent de suivre comment une information est argumentée, réfutée, améliorée et modifiée à travers une liste d'éditions. Ainsi, ils représentent des lieux où il faut approfondir la recherche d'informations, mais souvent vous devez vous rendre sur le site web du wiki pour avoir plus de détails sur les recherches.

Exercises

1.31 Recherchez "Ada Lovelace". Avez-vous trouver des résultats venant des wikis ?

1.32 Allez sur Wikipedia et réitérez la même recherche. Lisez l'article qui la concerne. Ces résultats figuraient-ils sur votre recherche précédente?

1.33 Consultez les anciennes version de cette page de Wikipedia et identifiez les choses qui ont été corrigées et modifiées. Quelles sont les choses qui ont été modifiées ? Y avait-il quelque chose qui ait été modifiée et ensuite ramenée dans son état initial ? A présent choisissez une star de film ou de musique célèbre que vous aimée et faites des recherches sur elle sur Wikipedia puis vérifiez les articles. Avez-vous remarqué une différence ?

1.34 Trouvez un autre site de wiki et effectuez la même recherche. Est ce que l'un des derniers résultats figuraient dans vos premières recherches à partir d'un moteur de recherche ?

Les Médias Sociaux

Utilisez-vous le site d'un média social ? Ou vous-en utilisez plusieurs ? En tant que hacker vous êtes bien au courant des média sociaux les plus populaires du moment. Que pensez-vous de ceux qui ne sont pas si actifs comme ils l'étaient ? Ils existent toujours, et leur données sont toujours disponibles, dans la plus part des cas.

Cela veut dire qu'il existe une énorme réserve d'informations à propos de nous, des informations dont la plupart ont été données gratuitement par nous mêmes. Et ces informations y resterons pour toujours.

Les sites de media sociaux ont souvent des sous-groupes ou communautés d'intérêts. Les sites possédant des thèmes professionnels ont souvent des groupes de cyber sécurité, et les sites traitant de sujets ou thèmes dans la clandestinité ont un groupe de hackers. Sur les sites professionnelles vous êtes tenus à utiliser vos vrais noms. Sur les sites des hackers, ce n'est pas le cas bref pour la plupart.

Le plus important, c'est de savoir si vous utilisez votre vrai identité sur les sites sociaux, ou vous utilisez un surnom ? Y a t-il un moyen de relier votre surnom à votre vrai identité ? Beaucoup n'y pensent pas lorsqu'ils utilisent des surnoms, mais il n'est pas rare de voir ces gens utiliser accidentellement ou par obligation leur vrai identité, adresse, ..., à la place de leur fausse identité. Si d'autres hackers découvrent votre surnom, ils peuvent habituellement découvrir qui vous êtes réellement à cause de certaines petites erreurs. Si vous utilisez un surnom pour être anonyme face à ceux que vous ne connaissez pas, alors qu'il en soit ainsi. Et ne vous tromper JAMAIS dans l'utilisation de vos surnoms si vous en avez plusieurs.

Exercices

1.35 Faite une recherche sur vous même. Avez-vous obtenu des résultats (qui vous concernent réellement) ? Y-en a t-ils qui proviennent des sites sociaux ?

1.36 Allez sur le site d'un réseau social que vous utilisez. Ne vous connecter pas, mais faite la recherche comme si vous étiez un étranger (ou outsider). Combien d'informations pouvez-vous obtenir à propos de vous même ?

1.37 Allez sur le site d'un réseau social qu'un ami utilise. Un fois encore, ne vous connecter pas si vous y avez un compte. Faites des recherches sur votre ami. Combien d'informations pouvez-vous obtenir à propos de lui (ou d'elle).

Le Chat

Les **Chats** existent sous la forme de **Internet Relay Chat (IRC)** et de **Messagerie Instantanée** (M.I) et sont un moyen très populaire de communications.

> Comme source de recherche, le chat est extrêmement incompatible parce que vous traitez avec des individus en temps réels. Certains seront courtois et d'autres seront grossiers. Certains seront des manipulateurs inoffensives, mais d'autres seront des menteurs rusés. Quelques uns seront intelligents et voudront partager certaines informations, et d'autres ne seront pas du tout informés, mais il n'y a pas moins de volonté de partager. Il peut être difficile de savoir qui est qui.

Cependant, un fois que vous vous êtes familiarisés avec certains groupes et canaux de discussions, vous pourrez être intégrés dans la communauté. Vous serez autorisés à poser de plus en plus de questions, et vous apprendrez en qui avoir confiance. Éventuellement vous pouvez avoir accès aux exploits de hacking les plus récents (ils sont connus aussi sous le terme **zero day**, ce qui veut dire qu'ils viennent d'être découverts) et faire croître vos connaissances.

Exercices

1.38 Recherchez trois programmes de messagerie instantanée. Quelle est la différence entre eux ? Peuvent-il dialoguer entre eux ?

1.39 Découvrez ce qu'est un IRC et comment vous pouvez vous y connectés. Pouvez vous découvrir quel est le réseau qui héberge le canal ISECOM ? Une fois que vous rejoignez le réseau, comment pouvez-vous vous connecter au canal de discussion **isecom-discuss** ?

1.40 Comment peut-on découvrir les canaux de discussion qui existent sur un réseau IRC ? Retrouver trois canaux de sécurité et trois canaux de hacking. Pouvez-vous vous connectez à ces canaux ? Est-ce des gens qui y discutent ou bien ce sont des robots ?

Le P2P

Peer to Peer, aussi connu sous l'acronyme **P2P**, c'est un réseau au sein de l'Internet. Contrairement au réseau client/serveur habituel, où les ordinateurs communiquent via un serveur central, les ordinateurs d'un réseau P2P communiquent directement l'un avec l'autre. Certains utilisent les réseau P2P pour télécharger de la musique MP3 et des films piratés tel que l'ancien réseau Napster, mais il y a d'autres réseaux P2P – qui existent dans le but de partager des information, et comme moyen de diriger une recherche basée sur le partage de l'information distribuée.

Le problème des réseau P2P est que, pendant que vous pouvez y trouver n'importe quoi, certaines chose y sont présentes illégalement. Et d'autres y sont légalement mais les sociétés qui les ont créées ne sont pas du tout ravis qu'elles soient là et elles se réjouissent

de réclamer des sous au propriétaire d'une **Passerelle Internet** qui permet d'accéder à cette ressource et de la télécharger.

> A l'heure actuelle il y a tellement d'accords sur le fait que la personne dont la connexion Internet a été utilisée pour télécharger ce contenu soit responsable ou bien si la police doit arrêter la personne qui a réellement télécharger le contenu. Ceci est pareil à l'exemple suivant: si votre véhicule a été utilisé pour commettre un crime, le propriétaire du véhicule , et non le chauffeur, va en prison. Les lois d'Internet ne sont pour le moment assez outillées pour prévenir de tels cas.

Que vous soyez la personne qui risque de télécharger une propriété intellectuelle, cela va sans dire que les réseaux P2P peuvent être une source vitale pour la recherche d'informations.

Retenez : il n'y a rien d'illégal concernant les réseaux P2P – il y a plusieurs fichiers qui y sont disponibles gratuitement et libres au téléchargement sous une variété de licences – mais il y a beaucoup de fichiers qui ne devraient pas s'y trouver. N'ayez pas peur d'utiliser les réseaux P2P, mais faites attention aux dangers, et à ce que vous téléchargez.

Exercices

1.41 Quels sont les réseaux P2P les plus populaires et les plus utilisés ? Comment fonctionnent-il ? De quel programme avez-vous besoin pour utiliser ces réseaux ?

1.42 Identifiez le protocole utilisé par l'un de ces réseaux P2P. A quoi sert-il, et comment permet-il de télécharger plus vite ?

1.43 'Recherchez les mots "télécharger Linux". Pouvez-vous télécharger une distribution de Linux grâce à un réseau P2P ?

Les Certifications

Il existe les certifications suivantes **OSSTMM Security Tester** et **Security Analyst**, qui sont des certifications variées destinées aux "hackers", des certifications qui sont basées sur les "meilleures pratiques" ou autre , des certifications étoffées par des bases fondamentales terribles dans le domaine de la sécurité informatique.

> Pourquoi devriez-vous vous soucier des certifications ? Parce vous pouvez obtenir certaines d'entre elles à n'importe quel âge, parce que vous n'avez pas besoin d'un niveau d'études universitaires pour les obtenir, et parce qu'elles vous octroient une crédibilité face à d'autres personnes.

Le problème des certifications basées sur les meilleures pratiques est que ces dernières changent souvent, et parce que les meilleures pratiques signifient "ce que tout le monde fait actuellement". Le plus souvent, une mauvaise pratique de cette semaine restera toujours mauvaise même s'il y aura une nouveauté la semaine prochaine.

Ainsi il y a des certifications orientées recherche, qui sont basées des recherches valides et répétitives sur le comportement humain et d'un système. Il est inutile de dire encore que notre organisation mère, ISECOM, fait parti de ces autorités dont les certifications sont basées sur la recherche. Que ce soit à ISECOM ou ailleurs, recherchez des certifications basées sur la compétence ou sur l'analyse ou des certification basées sur l'**application des connaissances** qui vous permettrons de mettre en pratique ce que vous prétendez avoir appris. Vous serez plus habiles lorsqu'il s'agira de mettre réellement en pratique ces connaissances.

Les Séminaires

Le fait de participer aux séminaires représente un grand moyen pour comprendre l'explication détaillée d'une théorie et observer les compétences en action. Même les séminaires basés sur la présentation de produits sont mieux adaptés pour vous faire comprendre comment on emploie un produit, sachant très bien que l'objectif principal est le marketing et la vente de ce produit.

Nous serions négligeant si nous ne soulignons pas que nous pouvons organiser le séminaire, Hacker High School Seminar à plusieurs endroits, et nous pouvons présenter toutes les leçons disponibles. Les séminaires sont organisés par des hackers professionnels qui parlent aux étudiants du hacking et de comment être un hacker, un bon ou un mauvais. Ces séminaires présentent une vue améliorée sur ce que sont réellement les hackers au sein du projet d'identification des hackers ou **Hacker Profiling Project**, un projet de collaboration entre les Nations Unies et ISECOM qui vise à savoir qui sont les hackers et pourquoi font-il du hacking. Ensuite vous découvrirez le bon côté du hacking et pourquoi il n'est toujours pas une chose mauvaise. Les choses les plus puissantes que nous vous aiderons à découvrir sont les moyens nécessaires pour devenir des intellectuels curieux et pleins de ressources comme un hacker. Les hackers réussissent souvent ce qu'ils font parce qu'ils savent apprendre d'eux mêmes (autodidactes), vont au-delà de ce qu'il y a dans les leçons et acquièrent les compétences dont ils ont besoin pour allez plus loin.

Vous êtes les bienvenus en demandant à vos parents et enseignants d'apprendre comment débuter l'enseignement d'un chapitre de Hacker High School dans votre école. Veuillez contacter ISECOM pour plus d'informations.

Études Ultérieures

A présent vous devez pratiquer ce que vous avez appris jusqu'à ce que vous devenez un maître de la recherche. Mieux vous pratiquez, plus vous obtiendrez rapidement des informations, et plus rapidement vous apprendrez. Mais faites aussi attention vous devez développer un esprit critique. Toutes les informations ne sont pas vraies.

> Souvenez-vous toujours de vous poser cette question, pourquoi une personne devrait-elle mentir ? Y a t-il de l'argent en jeu pour qu'une personne soit malhonnête ou repende une rumeur ou une histoire ? D'où viennent les faits ? Et, le plus important, quel est le champ d'actions ?

Comme dans le hacking, la recherche comprend un champ d'actions. Cela est vraiment important lorsque vous consultez les statistiques, telles les mathématiques qui utilisent les pourcentages et les fractions. Identifiez toujours là où le champ d'actions a eu lieu et là où il est applicable. Un exemple palpable où nous rencontrons ceci est dans le cas d'un crime national ou dans les statistiques sanitaires dressées à partir un petit échantillon pris dans une partie d'un pays. Si une étude a été faite sur 10 % d'un total de 200 personnes d'une seule ville, cela ne veut pas dire que le résultat est applicable à 10 % de la population de toute une nation. Donc soyez rusé aussi bien en consultant les informations qu'en les découvrant. La découverte du champ d'actions d'une information crée une grande différence !

Pour vous aider à devenir un meilleur chercheur pour le programme Hacker High School, voici des thèmes et termes complémentaires sur lesquels vous devez faire des recherches :

Méta recherche

Google Hacking

Comment fonctionnent les moteurs de recherches

Le Moteur de recherche à source ouverte : The Open Source Search Engine

The jargon File

OSSTMM

Les Certifications ISECOM :

OPST (OSSTMM Professionnal Security Tester)

OPSA (OSSTMM Professionnal Security Analyst)

OPSE (OSSTMM Professionnal Security Expert)

OWSE (OSSTMM Wireless Security Expert)

CTA (Certified Trust Analyst)

SAI (Security Awareness Instructor)

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM