Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEÇON 1
DEVENIR UN PIRATE

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Conditions d'utilisation de ce support

Ces leçons et supports sont gratuits et disponibles pour le public sous les conditions suivantes d'ISECOM:

Tous les travaux menés dans le cadre du "Hacker HighSchool" sont disponibles à usage non commercial auprès d'élèves du collège, du lycée, dans le cadre d'écoles publiques ou privées, ou encore lors de scolarisations à domicile. Ces supports ne peuvent être reproduits en vue d'un usage commercial. Il est expressément interdit d'utiliser ces supports dans le cadre de cours, leçons et/ou stages payants, à moins d'obtenir une licence pour cela (dans ce cas, veuillez aller sur *www.hackerhighschool.org/license*).

Le projet HSS (Hacker HighSchool) est un outil de travail et d'apprentissage, et en tant que tel, son utilisation relève de la personne qui l'utilise, et non de l'outil lui-même. ISECOM ne peut être mis en cause si cet outil est utilisé à mauvais escient ou de manière illégale.

Le projet HSS est aussi le fruit de l'effort de toute une communautés, et si vous trouvez ce projet intéressant, nous vous serions plus que reconnaissants de votre aide, soit par l'achat d'une licence, soit par un don, soit encore par un quelconque parrainage.

Copyright ISECOM - Tous droits réservés.

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Table des matières

"License for Use" Information....2
Conditions d'utilisation de ce support....2
Table des matières....3
Personnes ayant contribué à ce projet....4
1.0 Introduction....5
1.1 Les ressources....6
1.1.1 Les livres....6
1.1.2 Les magazines et les journaux....7
1.1.2.1 Exercices:....8
1.1.3 Les zines et blogs....8
1.1.3.1 Exercices:....8
1.1.4 Forums et mailing-lists....8
1.1.4.1 Exercices:....9
1.1.5 Newsgroups....9
1.1.6 Les sites web....10
1.1.6.1 Exercices:....10
1.1.7 Les chats....11
1.1.7.1. Exercices....12
1.1.8 Le P2P....12
1.2 Les prochains cours....12

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Personnes ayant contribué à ce projet

Pete Herzog, ISECOM

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

Traduction
Bénoni MARTIN

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

1.0 Introduction

Bienvenue sur le programme Hacker Highschool! Ce programme a été créé en vue de vous permettre de devenir plein d'idées et de ressources. Son axe central est de réveiller une curiosité de pirate en vous, guider votre éducation en tant que tel afin de vous permettre d'appréhender les problèmes de sécurité et de protection de la vie privée, et ainsi de vous permettre de prendre vous-mêmes les meilleures décisions concernant la sécurité.

Bien que le piratage puisse provoquer de doux frissons, ne serait-ce qu'à cause de la nature illégale de cette activité ; nous allons vous montrer qu'il peut être tout aussi intéressant de prévenir autrui des vulnérabilités dans leurs systèmes … sans compter que dans ce dernier cas vous n'avez pas à appréhender de risquer de terminer en prison. En tant que citoyen, ce n'est pas seulement votre droit, mais aussi votre responsabilité, de remonter les manquements aussi bien au niveau sécurité que respect de la vie privée vers les personnes intéressées. Et vous ne le ferez pas parce que vous le pouvez, mais parce que beaucoup d'autres personnes ne le peuvent pas. Vous aidez ainsi ceux qui ne peuvent pas s'aider eux-mêmes. C'est ce que font les comités de surveillance. C'est ce que vous apprendrez à faire avec nous.

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

1.1 Les ressources

Le sujet de cette leçon est d'apprendre à apprendre, compétence plus que nécessaire pour un pirate. Le piratage, en réalité, est un processus de création qui est plus basé sur un mode de vie que sur des cours. Nous pouvons vous apprendre tout ce qui est nécessaire, mais nous ne pouvons vous enseigner comment vous rendre compte de ce que vous devez apprendre. Ceci est dû à la constante évolution du domaine de l'informatique. Ce que nous vous apprenons aujourd'hui ne sera peut-être plus autant d'actualité demain. Il est bien plus utile de vous mettre dans la peau d'un pirate (ce qui est sans doute le plus important dans le piratage), ce qui vous permettra aussi de vous distinguer d'un "script kiddie" (une personne qui s'amuse avec des outils de piratage sans comprendre comment ils fonctionnent et ce qu'ils font réellement).

Les mots et/ou les concepts utilisés dans ce document et que vous ne comprendriez pas devront faire de votre côté l'objet d'une recherche sur Internet ou dans des livres. Si vous ne comprenez pas un mot ou un sujet, il est important que vous n'en restiez pas là. Faire le contraire ne vous servira qu'à traîner derrière vous des lacunes au cours de vos lectures ultérieures et à les accumuler. Les autres ouvrages vous demanderont probablement de faire des recherches sur Internet, et attendront de vous que vous utilisiez ces informations pour faire les exercices proposés; mais ils ne vous diront pas comment mener cette recherche. Cet ouvrage est le seul à contenir une explication pas à pas sur la manière de faire une recherche, afin de ne vous faire passer que le temps nécessaire à faire des recherches avec les outils dont vous disposez.

Ne vous limitez pas aux ordinateurs, au piratage et à Internet. Les bons pirates sont pleins de ressources et de créativité. Nombre d'entre eux sont peintres, écrivains ou encore créateurs. Les compétences en matière de piratage peuvent aussi être appliquées à d'autres domaines, comme les sciences politiques (cf. Le Prince de Machiavelli par exemple).

En plus d'avoir des centres d'intérêts dans d'autres domaines, vous devriez aussi vous intéresser à comment les autres domaines d'activité fonctionnent. Lire des livres allant de la psychologie à la science-fiction fera de vous un pirate plus imaginatif et meilleur. Souvenez-vous en: le piratage fait la comparaison entre comment les choses fonctionnent avec comment elles auraient dû fonctionner. C'est comme cela que vous vous rendez compte des vulnérabilités, des manquements et des failles.

1. 1.1 Les livres

Les livres sont un bon moyen d'apprendre les bases dans les domaines que vous voulez explorer. Vous souhaitez savoir quelque chose de basique, comme les détails au niveau hardware de votre PC? Rien ne vous sera plus utile que de lire un document sur le sujet. Le seul inconvénient avec la littérature concernant les ordinateurs et quelle devient très vite désuète. Le secret est d'arriver à comprendre l'essentiel sous une fine couche de détails techniques. MS-DOS et Windows sont clairement différents l'un de l'autre, mais pourtant tous les deux sont basés sur la logique booléenne qui a été déterminante dans la conception d'ordinateurs depuis qu'Ada, Contesse de Lovelace, écrivit le premier programme au XIX^{ème} siècle. L'intérêt pour la sécurité et le respect de la vie privée ont sans doute quelque peu

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

évolué au cours de ces derniers 25 derniers siècles, mais les principes fondamentaux décrits dans l'Art de la Guerre de Sun Tzu restent toujours d'actualité de nos jours.

Même si les informations contenues dans les livres ne sont pas forcément aussi à jour que celles provenant d'autres sources, ces informations sont souvent plus précises et détaillées que les autres: en effet, une personne passant un an à écrire un livre mettra plus d'ardeur à vérifier ses dires qu'une personne qui met à jour ses pages web 6 fois par jour. (cf. section 1.1.3 pour plus d'informations). Mais souvenez-vous-en: des informations précises ne sont pas forcément impartiales.

Il n'est pas forcément nécessaire de vous constituer toute une bibliothèque, mais écrire des notes dans la marge ou surligner certains passages peut vous être utile, et ce sont des choses que vous ne pouvez faire que sur des livres qui vous appartiennent.

Pour terminer, n'évitez pas de vous pencher sur des livres, ou de les laisser tomber dès les premières pages, simplement à cause de leur taille ou de leur apparente complexité. La plupart des gros ouvrages que vous voyez ne sont pas forcément faits pour être lus d'un bout à l'autre. Regardez-les plutôt comme d'antiques pages Internet, ouvrez le livre à une page quelconque et commencez à la lire. Si vous ne comprenez pas ce que vous lisez, soit revenez un peu en arrière, soit sautez quelques pages jusqu'à tomber sur un sujet qui ait du sens pour vous. Sautez d'une page à une autre au fil de votre lecture, comme vous le feriez en cliquant sur les liens hypertexte d'un site Internet. Ce type de lecture est souvent le plus profitable pour un pirate, de même qu'il satisfait plus la curiosité du moment qu'un désir de lire comme on le ferait avec un roman.

1.1.2 Les magazines et les journaux

L'utilisation de magazines et de journaux est vivement conseillée pour vous donner des informations concises au moment opportun. Cependant la plupart des magazines sont limités dans le nombre de détails et ont souvent une orientation particulière, en accord avec le type de public visé. Il est nécessaire que le pirate sache que des techniques comme l'ingénierie sociale ou le cassage de mots de passe sont mieux utilisées s'il a une solide culture générale; mais il faut quand même se souvenir que de la culture générale n'est pas forcément de la culture très précise.

Autre chose que vous devez aussi avoir à l'esprit quand vous regardez des magazines et / ou des journaux est le type de journal que vous avez sous les yeux. Par exemple un magazine dédié à Linux aura tendance à ne pas parler forcément de manière impartiale de Windows, non seulement pour des raisons évidentes, mais aussi parce que c'est ce que leurs lecteurs veulent lire.

La meilleure manière de combattre ces deux inconvénients, est de ne pas limiter ses sources d'informations: si vous tombez sur un article intéressant, cherchez d'abord des confirmations, ensuite des articles réfutant ces informations.

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

1.1.2.1 Exercices:

- Cherchez sur Internet 3 magazines en ligne traitant de sécurité informatique.
- Comment avez-vous trouvé ces magazines?
- Es-ce que ces trois magazines traitent-ils uniquement de sécurité informatique?

1.1.3 Les zines et blogs

Les zines sont de petits et souvent gratuits, magazines à distribution restreinte (moins de 10000 lecteurs), et sont en général écrits par des gens pendant leur temps libre et / ou par des journalistes amateurs. Les zines, comme par exemple le fameux 2600 ou encore Phrack Hacking, sont écrits par des volontaires et les auteurs ne changent pas le contenu pour des erreurs qui ne relèvent pas de la technique. Ce qui signifie que le langage peu être parfois "dur" pour ceux qui n'y sont pas habitués. Les zines ont souvent une ligne directrice bien démarquée et sont très dogmatiques. Ce qu'il faut mettre à leur compte, c'est que comme ils sont indépendants et n'ont de comptes à rendre à aucun constricteur ou autre vendeur, ce sont les plus enclins à être impartiaux et à montrer les bons et mauvais cotés sur chaque sujet.

Les blogs sont une version moderne des zines. Ils sont mis à jour beaucoup plus souvent, et utilisent le concept de communautés pour rester soudés autour d'un thème ou sujet. De même que les zines, ils sont aussi indépendants dans leurs dires; mais il est tout aussi important de lire le commentaire que la discussion.

1.1.3.1 Exercices:

- Cherchez sur Internet 3 zines traitant de sécurité informatique.
- Comment avez-vous trouvé ces zines?
- Pourquoi les rangez-vous dans la catégorie des zines(ne n'est pas parce qu'ils se prétendent comme tels, ou qu'ils mettent ce nom comme titre qu'il faut forcément les considérer comme tels) ?
- Cherchez sur Internet 3 blogs traitant de sécurité informatique.
- Avec quelles communautés sont-ils associés?

1.1.4 Forums et mailing-lists

Les forums et mailing-lists sont des médias très répandus, et ressemblent à des conversations entre groupe de personnes. Le cours de ces conversations changent sans cesse, beaucoup d'informations qui y circulent sont bien souvent de simples rumeurs, et quand la conversation est terminé il est très difficile de se souvenir qui a dit quoi. Les forums et les mailing-list se ressemblent à bien des égards, ce qui est dû aux nombreuses manières possibles pour y fournir des informations, comme par exemple le faire de façon anonyme ou encore donner intentionnellement de fausses informations. Et comme en plus les informations peuvent vite devenir obsolètes, il est nécessaire de lire toute la discussion et non pas quelques extraits.

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Vous pouvez trouver des forums sur presque tous les sujets imaginables, et beaucoup de magazines / journaux sur Internet offrent aux internautes la possibilité d'y exprimer leurs idées sur les articles publiés. C'est pour cela que ce genre de centres de discussion est intéressantpour partager des points de vue : peu importe à quel point vous avez aimé un article, vous aurez toujours au moins une personne pour penser le contraire.

Beaucoup de mailing-lists existent sur des sujets très particuliers, mais ils sont difficiles à trouver. Souvent, vous devez d'abord recherche un thème avant de tomber sur une mailing-list traitant du thème en question.

Pour un pirate, ce qui est le plus important est de connaître les forums qui ne peuvent se trouve aisément via des moteurs de recherche classiques. Même si vous pouvez trouver des forums en lançant une recherche sur un moteur de recherche, vous n'aurez pas forcément les informations contenues dans certaines réponses postées sur ces mailing-lists. Ces informations sont le coté invisible du site web, car pour les trouver, il faut lancer des recherches très précises, soit via des méta moteurs de recherche, soit directement sur le forum lui-même.

1.1.4.1 Exercices:

- Trouvez trois forums traitant de la sécurité informatique.
- Comment avez-vous trouvé ces forums?
- Pouvez-vous déterminer le thème général de chacun de ces forums?
- Es-ce que les sujets traités sont-ils en accord avec le thème du site?
- Trouvez trois mailing-lists traitant de sécurité informatique.
- Qui gère ces mailing-lists?
- Quelle liste vous parait la plus propice pour obtenir des informations le plus crédible et impartial possible; et pourquoi ?

1.1.5 Newsgroups

Les newsletters existent déjà depuis un bon moment, même avant que le web n'apparaisse. Google a acheté toute cette collection de ces archives et les as rendues disponibles sur http://groups.google.com. Vous y trouverez des correspondances datant du début des années 90, archives qui peuvent être intéressantes pour retrouver l'auteur d'une idée ou d'un produit, ou encore des informations trop précises pour faire l'objet d'une discussion en tant que telle.

L'intérêt des newsgroup n'a pas diminué avec l'arrivée d'Internet, devenu depuis un passage obligé pour rechercher des informations. Cependant, leur popularité n'a pas non plus augmenté, étant concurrencés par des nouveaux services comme des forums ou les blogs.

Exercices.

- En utilisant les newsgroups de Google, trouvez le plus ancien newsgroup portant sur la sécurité.
- Trouvez d'autres façons d'utiliser les newsgroups. Es-ce qu'il y a des outils que vous pouvez utiliser pour lire ces newsgroups?
- Combien de ces newsgroups parlent de piratage informatique?

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

1.1.6 Les sites web

Le moyen le plus utilisé pour partager des informations à l'heure actuelle est bien évidemment votre explorateur Internet. Même si nous appelons cela "le web", le terme exact serait "les services web", car tout sur Internet n'est pas forcément un site Internet: par exemple si vous regardez vos emails à partit d'un explorateur, vous utilisez un de ces services. Souvent ce genre de services requiert certains privilèges, ce qui se traduit par une demande d'authentification par login et mot de passe avant d'avoir accès à vos informations. Pirater une page Internet pour y changer des informations peut être fait techniquement, mais comme vous n'avez pas le droit légal de faire cela,vous n'avez pas les *privilèges* de le faire. Nous ne nous intéresserons qu'aux cas où vous disposez d'accès autorisés, mais au fur et à mesure que vous deviendrez plus expérimentés, vous vous trouverez devant des situations où vous aurez la possibilité d'obtenir des autorisations par mégarde. Dans ces cas-là, vous devrez prendre l'habitude d'en informer le webmaster.

Les sites web sont trouvables via un grand nombre de moteurs de recherche. Il vous est même possible de créer vous-mêmes votre propre moteur de recherche, si vous en avez le temps et suffisamment d'espace disque. Souvent, c'est le moteur de recherche qui obtient l'accès pour vous. D'autres fois, cela se fait via le *cache*: un cache est une partie de la mémoire du serveur hébergeant le moteur de recherche, et qui garde les pages enregistrées correspondant à votre requête. Si vous cliquez sur le lien correspondant au cache, au lieu du lien proposé, vous aurez ce que le moteur de recherche a trouvé lors de sa recherche. Il le garde de manière à montrer que sa recherche a été fructueuse, au cas où la page ne devient plus accessible entre le moment où vous lancez la recherche et celui où vous essayez de charger la page en question; mais cette fonctionnalité vous permet aussi par exemple de court-circuiter un serveur lent.

Une des archives de caches les plus utiles se trouve sur *http://www.archive.org*. Vous y trouverez les versions cache de sites web entiers depuis des années.

Un dernier mot sur les sites web: n'imaginez pas que vous puissiez toujours faire confiance au contenu des sites web parce qu'elle apparaît lors de votre recherche. Nombre d'attaques de pirates aboutissent et de virus arrivent à se propager juste en se connectant sur des sites ou alors en téléchargeant des programmes. Vous devez faire attention aux programmes que vous téléchargez, de même que vous assurer que l'explorateur que vous utilisez est bien à jour.

1.1.6.1 Exercices:

- En utilisant un moteur de recherche, trouvez des sites qui vous donneront accès par erreur. Pour ce faire, connectez-vous sur www.google.com et rentrez ce qui suit dans le champ de recherche:

allintitle: "index of" .pdf

Cliquez sur un des liens que vous trouverez et vous devriez voir à quoi ressemble un listing de répertoire.

Ce type de recherche est aussi connu sous le nom de Google Hacking.

- Pouvez-vous faire les mêmes recherches en cherchant des fichiers de type '.xls' et 'avi'.
- Il existe d'autres moteurs de recherche que Google, et un bon chercheur doit savoir comment les utiliser. Certains sites web ont été créés en vue de traquer les autres moteurs de recherche (*http://www.searchengine.com* par exemple). Cependant, il y en a de plus en plus, et vous pouvez les trouver en utilisant des moteurs de recherche. Il

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

existe même un moteur de recherche pour la face cachée d'Internet. Trouvez 10 moteurs de recherche qui ne soient pas des métas moteurs de recherche.

- Lancez une recherche pour "tests de sécurité et piratage déontologique -security testing and ethical hacking-", et prenez les 3 premières réponses.
- Lancez la même recherche, en omettant les guillemets, et prenez les 3 premières réponses. Sont-elles différentes des précédentes réponses?
- Il est très différent de chercher un sujet et un mot ou une phrase. Dans l'exercice D, vous avez cherché une phrase et maintenant, vous allez chercher une idée. Pour ce faire, vous avez besoin de penser à ce dont vous avez besoin, ainsi qu'à la manière par laquelle vous voulez l'obtenir. Par exemple, imaginons que vous souhaitiez trouver des magazines en ligne traitant du piratage déontologique. Si vous lancez une recherche avec comme mots-clés "magazines en ligne traitant de piratage déontologique", vous allez tomber sur des opinions émises à ce sujet. C'est pas mal, mais pas autant que vous étiez directement allé à la source. Vous devez au lieu de cela, penser "Si j'étais en train de créer un tel magazine, quel gere d'informations s'y trouveraient et quels mots-clés le définiraient?". Lancez une recherche avec les mots et phrases suivants et voyez quelle recherche donne le meilleur résultat:
    - Ma liste favorite de magazines traitant du piratage déontologique,
    - Liste de magazines traitant du piratage déontologique,
    - Ressources four des pirates déontologiques,
    - Magazines piratage déontologique sécurité liste ressource
- Trouvez le plus ancien site web de Mozzila dans l'Archive Internet. Pour ce faire, vous devez lancez une recherche sur le mot-clé www.mozzila.org sur http://www.archive.org.
- Maintenant, pour rassembler toutes nos idées, disons que vous souhaitez télécharger la première version de Netscape. En utilisant les moteurs de recherche et les Archives Internet, voyez si vous pouvez trouver cette version et la télécharger (mais ne l'installez pas!)

1.1.7 Les chats

Les chats, aussi connus sous le nom de IRC (Internet Relay Chats), ou encore IM (Instant Messaging), sont des manières de communiquer en temps réel très connues et très utilisées.

Comme source d'informations, le chat ne vous donnera pas beaucoup de résultats, parce que vous faites du temps réel. Quelques-uns de vos correspondants virtuels peuvent être amicaux, d'autres peuvent être grossiers. Quelques-uns peuvent être des méchants souhaitant vous faire du mal, mais certains ne seront que des menteurs. Certains seront compétents et souhaiteront partager des informations avec vous, d'autres souhaiteront partager avec vous-même en n'ayant aucune compétence.

Cependant, dès que vous serez familiarisés avec certains groupes de discussions, vous aurez des chances d'être accepté dans la communauté, vous pourrez poser de plus en plus de questions et vous saurez aussi à qui vous pouvez faire confiance. En plus, vous pourrez même apprendre les dernières nouvelles dans la matière (connu aussi sous le nom de "zero day" en anglais, en d'autres termes ce qui vient d'être juste découvert) et ainsi améliorer vos connaissances.

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

1.1.7.1. Exercices

- Trouvez 3 chats sur Internet. Qu'est ce qui les rendent différents? Peuvent-ils être utilisés pour discuter entre eux?
- Trouvez ce qu'on appelle l'IRC, ainsi que comment s'y connecter. Une fois connecté, entrez dans le salon de chat appelé ISECOM comme annoncé en première page sur *http://www.isecom.org*.
- Comment savez-vous quels moyens existe-t-il pour se connecter sur IRC? Cherchez 3 de ces moyens dans le domaine de la sécurité informatique, et 3 dans le domaine du piratage. Pouvez-vous les utiliser pour vous connecter?

1.1.8 Le P2P

Le Peer To Peer, aussi connu sous l'abréviation P2P, est un réseau à l'intérieur du réseau Internet. La communication ne se fait non plus de manière centralisée (les ordinateurs clients dialoguent entre eux en passant forcément par un serveur central), mais de bout en bout: deux ordinateurs communiqueront directement entre eux. Pour beaucoup de personnes, le P2P se résume au téléchargement de MP3 ou de films piratés, mais il existe bien d'autres buts, comme par exemple échanger des informations de tout type. Un des sites web dédiés à ce sujet (http://infoanarchy.org) se base sur le principe que les informations doivent être partagées. Sur ce site web, vous pouvez trouver la liste des réseaux et des clients P2P disponibles.

L'inconvénient avec P2P, c'est que même si vous pouvez trouver presque toutes les informations que vous souhaitez, certaines d'entre elles sont disponibles de manière illégale. Ce programme "Hacker Highschool" ne va pas dans le sens d'utiliser les réseaux P2P pour des téléchargement illégaux, mais il n'y a pas de doute quant à la grande utilité de ce genre de réseaux pour trouver des informations. Souvenez-vous que l'utilisation des réseaux P2P est tout à fait légale et qu'un grand nombre de documents qui y sont disponibles sont téléchargeables gratuitement de manière légale; mais gardez à l'esprit qu'il y existe également des documents qui ne devraient pas y être! Ne craignez pas les réseaux P2P, mais gardez à l'esprit ce qui vient d'etre dit.

1.2 Les prochains cours

Maintenant, il ne vous reste plus qu'à vous exercer à l'art de chercher les informations. Mieux vous y arriverez, plus vous réussirez à obtenir rapidement des informations, et vous apprendrez d'autant plus vite. Pour vous aider à devenir un meilleur chasseur d'informations, voici quelques pistes que vous pourrez explorer:

- Meta Search
- The Invisible Web
- Google Hacking
- How Search Engines Work
- The Open Source Search Engine

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.