Hacker Highschool

SECURITY AWARENESS FOR TEENS



LECON 4
LA GESTION DES SERVICES

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

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 of Contents

Les Contributeurs

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Chuck Truett, ISECOM
Kim Truett, ISECOM
Marco Ivaldi, ISECOM
Bob Monroe, ISECOM
Jaume Abella, ISECOM
Greg Playle, ISECOM
Simone Onofri, ISECOM
Guiomar Corral, Barcelona
Ashar Iqbal

Traducteur

Koffi "Willy" Nassar

ISECOM

Introduction

Il existe des milliers de différentes langues et des douzaines de dialectes par langue. Vous pouvez apprendre plusieurs langages vous-même, mais vos chances de voyager à travers le monde et de pouvoir parler à tout le monde que vous rencontrer sont très infimes voir nulles.

Oui, vous pourriez soutenir en disant que les mathématiques sont un langage universel ou que la musique s'adresse à tout le monde, mais soyons réaliste. Essayez d'acheter un verre de soda avec une tranche de citron et un morceau de glace en utilisant ces "langues universelles" et observez jusqu'où vous irez.

S'il vous arrive de visiter un pays dont vous ne comprenez pas la langue, veuillez envoyer à ISECOM une vidéo de vous-même entrain d'utiliser des instruments de musique tels saxophone ou autres pour acheter du soda. Vous voudrons réellement voir cette scène ! Il se peut que nous ne voudrions en entendre parlé, mais soyez-en sûrs nous voudrions voir cela.

Mais chaque jour des millions de gens communiquent entre eux en utilisant un langage unique et commun sur Internet. Il se que tous les Hommes parlent pas la même langue, par contre, nos ordinateurs et nos réseaux peuvent oui.

Le modèle que nous utilisons dans les réseaux contemporains est le **modèle client-serveur**. Les ordinateurs physiques (les **hôtes** et les **serveurs**) offrent des services (sous UNIX on les appelle **daemons: disk access and execution monitors** – maintenant allez mystifiez quelqu'un). Considérer un serveur web de cette manière: il vous sert des pages web lorsque vous-en demandez. Il n'y a pas de mystère.

Mais en réalité "vous" n'avez pas demander cette page; mais votre navigateur web oui, ce qui veut dire que c'est un **client** (ou formellement parlant, votre ordinateur en est un). Et votre ordinateur peut être à la fois un serveur et un client aussi. C'est la beauté des réseaux: si tu me fait ceci, moi je te fais ça.

Multipliez ce modèle un million de fois, et vous avez l'Internet. Considérons ceci: des millions d'ordinateurs offrent un certain type de services. À quoi sert-il d'être un client ? Et est-il possible de **renverser** toute cette situation ? (Allez chercher ce mot si vous n'êtes convaincu de cette explication. C'est un cours de hacker après tout).

Que vous soyez prêt ou pas, allons-y en profondeur.

Les Services

Vous disposez d'un ordinateur, et vous savez qu'il y a des informations utiles dessus, ou bien il se peut que vous participiez à cette hallucination habituelle en disant que vous n'avez rien d'une valeur numérique dessus. Vous savez que d'autres personnes, des millions de gens, ont aussi des ordinateurs et il se peut que leurs ordinateurs contiennent des informations utiles, pour ne mentionner des ressources disponibles comme les processeurs, la mémoire RAM et les espaces de stockage et la bande passante.

Maintenant, vous pouvez supposer que ces gens, et ces ordinateurs, peuvent probablement avoir des informations qui soient importantes pour quelqu'un. Le seul problème est comment obtenir toutes ces informations utiles.

Les ordinateurs communiquent entre eux facilement à travers les ports, en utilisant les protocoles dont nous avons parlés dans la Leçon 3, mais cela ne vous permet pas réellement de lire le flux de données binaires que les ordinateurs échangent (à moins que vous n'ayez suffisamment de temps disponible). Vous devez trouvez un moyen par lequel votre ordinateur peut obtenir les données, vous les interpréter, et vous les présenter sous une forme utilisable.

Le seul moyen dont dispose les ordinateurs pour transférer des données c'est à travers les **services réseau**, ou simplement les **services.** Ces services vous permettent de consulter les pages web, d'échanger des courriels, de faire des chat, et d'interagir avec des ordinateurs distants. Ces services sont liés aux numéros de port.

Votre ordinateur, c'est à dire l'**ordinateur local**, utilise des programmes nommés **clients** pour interpréter les informations que vous avez reçues. Vous pourriez obtenir des informations venant d'un serveur (qui fournit un service fonctionnel ou daemon), via un réseau **Tor**, à partir des **sources Torrent** ou via des réseaux **peer-to-peer.**

> Évidemment, votre ordinateur peut fournir des service à d'autres ordinateurs distants, ce qui veut dire qu'il est un serveur de données ou un fournisseur de services. S'il vous arrive d'avoir un logiciel malveillant sur votre ordinateur, il se peut que vous fournissiez quelques services sans vous en rendre compte.

Des exemples de clients comprennent, les navigateurs web, les clients de messagerie électronique, les programmes de chat, Skype, les clients Tor, les clients Torrent, les clients de flux RSS et autres. Ceux-ci sont des programmes qui se trouvent à la **couche application** de la pile de protocoles TCP/IP. À la couche application, toutes les données sont transmises, encapsulées, cryptées, décryptées, adressées et ainsi de suite jusqu'aux couches les plus basses où elles sont transformées en quelque chose vous, l'utilisateur vous pouvez lire et comprendre.

Le Protocole HTTP et le Web

Lorsque nous parlons de "l'Internet," la plupart des gens pensent en fait au **World Wide Web.** Le World Wide Web, ou simplement le **Web**, n'est pas l'Internet, c'est en fait une petite partie des services qui sont disponibles. Habituellement il inclut les activités telles que l'accès aux pages web via un navigateur.

> A propos, l'Internet réel, est constitué de tous les ordinateurs, routeurs, câbles et systèmes sans fil qui transmettent tous les types de données de part et d'autres. Le trafic web ne constitue qu'une portion de tout ceci.

Le web utilise le protocole **HTTP** ou **HyperText Transfer Protocol** et des applications (clientes) nommées **navigateurs web** pour accéder aux documents qui se trouvent sur les **serveurs web**. Les informations provenant des ordinateurs distants sont envoyés sur votre ordinateur local en utilisant le protocole HTTP, qui fonctionnent habituellement sur le port 80. Votre navigateur web interprète ses informations et vous les affiche sur votre ordinateur local.

Tous les navigateurs web ne sont pas créés de la même manière. Chacun offre des outils variés et leurs façons d'afficher les pages web sont légèrement différentes. Les problèmes de sécurité et de vie privée peuvent être gérés avec des différents niveaux de succès. Cela veut dire que vous devriez savoir ce que votre navigateur web peut et ne peut pas faire, et quelles sont les paramètres et les logiciels additionnels (pluggins) qui vous offrent ce parfait équilibre entre la sécurité et la vie privée (à moins que vous n'aimiez les logiciels malveillants, les publicités, les courrier indésirables (spam) et que votre voisinage ne sache ce que vous faites).

La partie **hypertexte** du protocole HTTP désigne la manière non linéaire avec laquelle vous consultez les pages web. Habituellement vous lisez linéairement comme suis: page 1 puis page 2 ; chapitre 1 puis chapitre 2 ; leçon 1 puis leçon 2, et ainsi de suite. L'hypertexte vous permet d'accéder aux informations d'une façon non-linéaire. Vous pouvez sauter d'un thème à un autre, en le consultant juste au passage, ensuite revenir sur vos pas et peut être accéder à d'autres informations avant d'avoir terminer l'article parent. Voilà la différence entre l'hypertexte et le texte simple.

En hypertexte, les mots et les idées ne sont pas connectés seulement avec les mots qui les entourent, mais aussi avec d'autres mots, images, vidéos, et musiques. L'hypertexte ne se trouve pas seulement sur le web. Les logiciels de traitement de texte les plus outillés vous permettent de créer des pages sous format web, ou HTML qui sont sauvegardées localement. Vous lisez ces pages dans votre navigateur web et elles réagissent comme toute autre page web, la seule différence est qu'elles sont sauvegardées sur votre ordinateur local, et non sur un ordinateur distant.

Il est très facile de créer votre propre page web. La manière la plus facile de le faire, c'est d'utiliser l'un des logiciels de traitement de texte les plus courants, tel OpenOffice/Libre Office Writer, Microsoft Word, ou WordPerfect. Ces programmes vous permettent de créer des pages web simples, en combinant du texte, de l'hypertexte et des images. Beaucoup de gens ont réussi à créer des pages web fonctionnelles en utilisant ces logiciels de traitement de texte (ou même des éditeurs de texte simples comme Vi, qui se trouve sur la plupart des plate-formes UNIX). Voici d'autres éditeurs de texte qui vous permettent de faire la même chose: Microsoft Notepad, Notepad++, SciTe, emacs et autres.

Mais ces pages ne peuvent pas avoir du contenu flash. Du contenu flash veut dire des **feuilles de style CSS**, des **scripts** et des animations. Vous pouvez dépenser énormément d'argent pour l'achat des programmes spécialisés dans la conception des pages web fantaisistes. Ces programmes vous permettent ce créer des effets intéressant sur votre page web, mais ils sont plus complexe à utiliser. Une fois encore, ils rendent habituellement le travail entier facile. L'alternative la moins chère est de vous procurer un éditeur de texte capable de fonctionner avec HTML et des langages de script, ensuite vous apprenez la syntaxe et la programmation HTML et vous programmez vous même vos pages web en partant de zéro.

Une fois que ces pages sont conçues, vous aurez besoin d'un ordinateur pour les mettre en ligne, si vous voulez que d'autres personnes y accèdent. Les **fournisseurs d'accès Internet (FAI)** fournissent des **services d'hébergement web** sur leurs serveurs.

Vous pouvez déployer un serveur web chez vous, en utilisant votre ordinateur, mais il existe une poignées d'inquiétudes. Les informations sauvegardées sur un serveur web ne sont seulement disponibles que lorsque le serveur est allumé, et fonctionne correctement et possède une connexion ouverte. Donc si vous voulez déployer un serveur web dans votre chambre à coucher, vous devez laisser votre ordinateur allumé tout le temps ; vous devez vous assurer que les programmes du serveur web fonctionnent correctement tout le temps (cela inclus la maintenance des équipements, le contrôle des infections virales, des vers et d'autres attaques, et résoudre les bugs inévitables et les failles qui se trouvent au sein des programmes eux-mêmes) ; et vous devez maintenir une connexion Internet active, qui doit être stable et très rapide. Les FAI factures des frais supplémentaires pour une connexion rapide en liaison montante et l'obtention d'une adresse IP fixe, c'est pourquoi la plupart des gens paient quelqu'un d'autre pour faire ces travaux.

Une société d'hébergement web stocke vos pages web sur leur ordinateur. C'est mieux que leurs serveurs soient attaqués, au lieu des vôtres. Une bonne compagnie d'hébergement web aura: plusieurs serveurs redondants et des politiques de sauvegarde régulières, afin que votre site web ne disparaisse pas à cause des problèmes liés au matériel ; une équipe de techniciens et d'ingénieurs maintient les serveurs fonctionnels malgré les attaques et les bugs au sein des programmes ; et un nombre des connexions ouvertes vers l'Internet vous donne une certaine garantie de fonctionnement lorsqu'il y a des interruptions. Donc tout ce dont vous avez besoin c'est de concevoir votre page web, de la charger en ligne sur le serveur de la société d'hébergement, d'éteindre votre ordinateur et d'aller vous coucher. Votre page web sera disponible au monde entier, aussi longtemps que vous payerez la facture pour.

Il est possible de trouver des organisations qui offre des services d'hébergement gratuit. Certaines de ces organisations sont financées par des publicités payantes, ce qui veut dire qu'avant que quelqu'un n'accède à votre page web, il doit voir la publicité d'une autre personne d'abord. Mais ils n'auront pas à payer quoique ce soit, et vous n'aurez pas à payer.

Exercices

4.1 Une page web est simplement du texte qui dit au navigateur là où se trouvent les images, les vidéos, et d'autres choses. Vous pouvez voir comment cela se présente en voyant le Code Source de la Page. Démarrez votre navigateur favori et accédez à ISECOM.ORG et chargez la page. Maintenant analysez le code source. Vous verrez quelques balises contenant le mot "meta". Par exemple, la première est *meta-charset="utf-8"*. Qu'est ce que cela signifie ? Quel est leur rôle ?

4.2 Trouvez 3 autres balises meta et expliquez leur rôle. Il se peut que vous ayez à faire des recherches sur le web pour comprendre le significations donc faites très attention aux mots clés que vous utiliserez dans vos recherches afin d'obtenir les bonnes réponses.

4.3 Enregistrez le code source de la page ISECOM.ORG sur votre ordinateur. Ensuite glissez et déposer le fichier du code source sur l'icône d'un navigateur web. Qu'est ce qui a changé ? Pourquoi pensez-vous que cela a changé ?

4.4 Ouvrez le fichier contenant le code source de ISECOM.ORG dans un éditeur de texte et vous verrez qu'il ne contient que du texte et des nombres. Quel que soit ce que vous y aurez changé ou saisi, cela affectera l'affichage de la page lorsque vous l'enregistrez et que vous les glissez et déposez dans le navigateur web. Effacez des choses et vous verrez qu'elles sont effacées. Changez des mots et vous verrez que ces mots apparaîtrons tels que vous les avez saisis. Maintenant, effacez tout le contenu de la page source et saisissez votre nom de telle sorte qu'il s'affiche plus grand et plus en gras que les autres mots. Essayez cela. Enregistrez vos modifications. Glissez et déposez le fichier modifié dans un

navigateur web et regardez si vous avez pu réussir. Non ? Alors continuer d'essayer!

Consultez la rubrique **Étoffez Vos Connaissances: Amusez Vous avec HTTP** à la fin de cette leçon pour avoir une opportunité d'approfondir.

Le Courriel (Email) – les protocoles SMTP, POP et IMAP

Le deuxième aspect le plus visible de l'Internet est probablement le courrier électronique. Sur votre ordinateur vous utilisez un client de messagerie électronique, qui se connecte à un serveur de messagerie électronique. Lorsque vous créez votre compte email, vous obtenez un nom unique sous la forme **utilisateur@domaine** et vous devez créer un mot de passe.

Le courrier électronique est scindé en deux parties: le **protocole SMTP (Simple Mail Transfer Protocol)**, qui envoie le message, et le serveur mail, soit le **protocole POP (Post Office Protocol)** ou le **protocole IMAP (Internet Message Access Protocol)**, qui sont chargés de *récupérer* vos messages.

Le protocole SMTP (nous vous le rappellerons encore) est utilisé pour *envoyer* un courrier électronique. SMTP définie les **champs** dans un message électronique, y compris les champs tels que l'adresse de l'expéditeur (FROM), l'adresse du destinataire (TO), l'objet du message (SUBJECT), le champ copie carbone (CC) et le corps du message (BODY). L'ancienne version de SMTP ne requiert pas un mot de passe et envoie tout en texte clair ; tout le monde peut lire votre message. Il se peut que cela ne soit pas mauvais à l'époque où le protocole était conçu et l'Internet était un petit monde habité par des gens de même opinion. Mais cela a engendré une faille qui permettait à n'importe quel utilisateur d'envoyer des **courrier indésirables (spam)** et de faire d'autres choses horribles comme l'**usurpation de courrier électronique (email spoofing)**, qui veut dire tout simplement, l'utilisation d'une fausse adresse d'expéditeur. La plupart des serveurs de messagerie de nos jours, utilisent une version sécurisée de SMTP, ce qui veut dire que vous devez prouver votre identité avant de pouvoir envoyer un courrier électronique.

Dans les leçon à venir, nous vous montrerons comment fonctionne l'usurpation électronique et comment l'identifié dans les en-têtes des messages électroniques. Ce brin de connaissance peut vous transformer rapidement de façon redoutable, de l'état de brebis en état loup.

Le **Protocole POP3 (Post Office Protocole version 3)** est un protocole qui "sauvegarde et télécharge". Le serveur de messagerie électronique reçoit votre courriel et le sauvegarde pour vous, jusqu'à ce que vous ne vous connectiez et le téléchargiez. Ensuite vos courriels sortant sont envoyés grâce au protocole SMTP. C'est une bonne approche du courriel lorsque vous utilisez une connexion du type dial-up, puisque cela requiert moins de temps pour l'envoie et la réception de courriels, et vous pouvez les consulter tout en étant hors ligne.

L e **Protocole IMAP (Internet Message Access Protocol)**, par contre, sauvegarde par défaut votre courriel sur le serveur. Plusieurs solutions de courriel en entreprise utilisent une forme de IMAP, cela dépend du propriétaire du logiciel. Avec IMAP, vous pouvez créer des dossiers dans votre boîte électronique et déplacer les messages entre ces dossiers. Lorsque vous vous connecter au serveur IMAP, vos boîtes électroniques et le serveur synchronisent les dossiers, les contenus, les courriels entrant et ceux qui sont effacés. Ceci a de justesse un avantage: vous pouvez accéder à votre messagerie électronique à

partir de n'importe quel ordinateur ou appareil que vous utilisez: ordinateur portable, les smart phone ou les tablettes. En plus vous pourrez télécharger et sauvegarder le courriel dans vos fichiers personnels qui se trouvent sur votre ordinateur.

Cependant, il existe deux conséquences: premièrement, vous avez évidemment besoin d'échanger plus d'informations, donc vous avez besoin d'une connexions plus rapide et de plus de temps. Deuxièmement, l'espace de stockage est limité. Votre serveur de messagerie vous allouera une taille fixe pour votre boîte électronique que vous ne pouvez pas excéder. Si vous excédez cette taille, vous ne serez plus en mesure de recevoir des messages à moins que vous n'effaciez des courriels (ou payiez pour avoir plus d'espace de stockage). Finalement cela veut dire que le courriel IMAP en entreprise a besoin de la gestion des données. Vous devez déplacer vos messages vers un espace de stockage local et effacer vos courriels envoyés, les messages indésirables (spam) et vider souvent la corbeille pour conserver de l'espace. Les courriels contenant des fichiers attachés vous détruirons. A cette époque des comptes de courriels gratuits sur Internet munis de large espace de stockage, toute cette maintenance semblerait stupide. Jusqu'à ce qu'on ne vous le demande. Ou bien quelqu'un a compromis votre serveur de messagerie électronique et a accès à TOUS vos messages.

Les serveurs POP et IMAP ont tous les deux besoin d'un mot de passe pour que vous puissiez accéder à votre compte. Mais tous les deux protocoles envoient *tout* en message clair, y compris les mots de passe, donc n'importe qui peut potentiellement les lire. Vous devez utiliser une forme de chiffrement pour masquer le processus d'authentification (tel SSL) et le contenu de votre boîte électronique. C'est la raison pour laquelle plusieurs clients de messagerie électronique ont une case à cocher nommée *Utiliser SSL*.

Lorsque vous cliquez sur le bouton Envoyer sur votre client de messagerie, deux choses se passent: premièrement votre client vous force à vous authentifier sur le serveur SMTP (bien que vous vous soyez déjà authentifiés sur le serveur POP), ensuite il envoie votre message sortant (via le protocole SMTP).

Ceci était devenu agaçant au milieu des années 90, lorsque les serveurs avaient commencer à utiliser un protocole nommé **POP-before-SMTP**:vous envoyez premièrement au serveur POP, votre nom et mot de passe, puis vos messages entrant sont téléchargés, ensuite le serveur SMTP vérifie votre authentification sur le serveur POP ("Est ce que les paramètre de celui-ci sont correctes ?" "Oui, je l'ai déjà authentifié") et vous envoie vos messages. C'est une meilleure façon de gagner du temps.

Une chose importante qu'il faut retenir est la suivante, malgré l'utilisation de la protection par mot de passe, le courriel n'est pas un moyen pour envoyer des informations sécurisées. La plupart des clients et des serveurs POP requièrent que votre mot de passe soit communiqué – sous forme non cryptée – à votre serveur mail. Cela ne veut pas dire que toute personne qui reçoit un courriel venant de vous, reçoit aussi votre mot de passe ; mais cela veut dire que quelqu'un qui a la connaissance adéquate et les outils nécessaires peut capturer votre mot de passe – aussi bien que le contenu de vos courriels. (Pour avoir plus d'idées sur la sécurisation de votre messagerie électronique, reportez vous à la **Leçon 9: Sécurité des Courriels**).

Exercises

4.5 Envoyez-vous un courriel à partir de votre compte principal, vers votre compte principal. Envoyez le même message à votre compte principal à partir d'un autre compte, par exemple un compte en ligne gratuit (allez, nous savons que vous les avez). Combien de temps les messages mettent-ils pour arriver ? Y-a-t-il une différence, pourquoi ?

4.6 Regardez l'un de ces messages indésirables (spam) qui saturent votre boîte électronique. Pouvez-vous identifier réellement celui qui vous a envoyé un courriel particulier ? Y-a-t-il une sorte d'informations cachées dans les courriels, par exemple ? S'il y en a, comment un hacker habile peut-il les voir ?

4.7 Pouvez-vous retarder l'envoi d'un courriel pendant un certain temps ou nombre de jours (ce qui peut éviter le Rejet) ? Pouvez-vous imaginer une façon d'utiliser le retard d'envoi de courriel pour porter à confusion vos amis ?

IRC

Les réseaux **IRC (Internet Relay Chat)** représentent l'un des lieux célèbres où vous verrez la nature non réglementée de l'Internet à son paroxysme. Ou pire. Sur IRC, n'importe qui a l'opportunité de dire ce qui lui passe par la tête. IRC est aussi connu sous le nom de **Usenet** ou **groupe d'informations (news goup).** Chaque groupe d'informations possède son propre nom, son sous-nom, etc ...

Il se peut que vous soyez familier avec les salons de discussions (ou chat rooms). IRC est semblable à cela, seulement il n'existe pas de règles qui soient au-delà des **nétiquettes**, et souvent il n'y a presque pas de chaperons. Il se peut que vous trouviez exactement ce que vous recherchez sur un canal IRC, ou bien vous pouvez y trouver quelque chose dont vous ignorez l'existence.

> Toutes les règles dont vous avez entendu parler à propos des forums de discussions sont applicables aux canaux IRC. Ne révéler jamais à quelqu'un votre vrai nom. Ne donnez pas votre numéro de téléphone, votre adresse, ou votre numéro de compte bancaire sur IRC. Mais amusez-vous! Si vous êtes de passage, faites très attention au contenu qui y est disponible. Toutes les choses sur Internet ne sont pas tous sans logiciels malveillants, et tout le monde sur Internet n'est pas courtois.

IRC n'est pas sécurisé et tout ce que vous y saisissez est transmis en texte clair, de serveur IRC en serveur IRC. Vous pouvez configurer des conversations privées entre vous et un autre membre IRC mais ces conversations sont transmises en texte clair aussi. L'utilisation d'un pseudonyme ne vous procurera qu'une petite discrétion. Si vous projetez commettre des actions malveillantes ou louches, n'utilisez pas le même pseudonyme pour chaque compte. L'utilisation d'un même pseudonyme offre une excellente opportunité d'être pisté par la police. Ou du moins par des gens dévoués.

Les thèmes de discussion sont appelés des "canaux". Puisqu'il existe des milliers de canaux, nous vous donnerons une adresse URL qui liste plusieurs d'entre eux pour que vous puissiez les parcourir jusqu'à ce que vous ne perdiez la tête:

```
http://www.nic.funet.fi/~irc/channels.html
```

Si vous vous sentez mal à l'aise avec les commentaires postés par un autre membre, vous pouvez soit le rapporter au modérateur (s'il y en a), ou vous pouvez **exclure** cette personne de ce canal. Si vous ne voulez pas entendre ce que quelqu'un d'autre a à dire, vous pouvez toujours les bloquer ou ignorer leurs messages. Peut être que cette tâche ne vous incombe pas de toute les façons.

Exercices

4.8 Trouvez trois canaux IRC qui ne parlent uniquement que des thèmes de sécurité. Comment avez-vous joint cette conversation publique? Que devez-vous faire pour avoir une conversation privée avec une personne ?

4.9 Quel port utilise IRC ?

4.10 Le transfert de fichiers est-il possible via IRC ? Comment arrivez-vous à le faire ? *Voudriez*-vous échanger des fichiers via IRC ?

4.11 Quelle est la différence majeure entre MIME et SMIME? Lorsque vous voyez un "S" dans un acronyme, est ce que cela attire votre attention sur quelque chose de spéciale telle *Securisé* en tant que personne avertie?

FTP

Le vieux protocole **FTP (File Transfer Protocol)** fonctionne habituellement sur les port 20 et 21. Avez-vous deviné ce à quoi il sert: il vous permet de faire le transfert de fichiers entre deux ordinateurs. Pendant qu'il peut être utilisé pour le transfert privé des fichiers, parce qu'il n'utilise pas de chiffrement il est plus utilisé gratuitement, par des serveur FTP anonymes qui offrent un accès publique à une collection de fichiers, tels le fichier ISO de cette merveilleuse nouvelle version de Linux.

Les transfert FTP anonymes étaient autre fois le moyen principal dont disposaient les utilisateurs pour échanger des fichiers sur Internet. Pendant que plusieurs serveurs FTP anonymes soient utilisés pour distribuer illégalement des fichiers (une bonne méthodes pour propager les maladies binaires), la plupart sont légalement utilisés pour partager des programmes et des fichiers. Vous pouvez trouver des serveurs qui offrent des services FTP anonymes via les méthodes habituelles, par exemple les moteurs de recherches. Mais souvenez-vous: les paramètres de connexion FTP sont envoyés en texte clair. Oui, cela est vrai bien que nous soyons entrain de parler d'un nom d'utilisateur et d'un mot de passe. (Est-ce une faiblesse ou quoi?). Il existe une version sécurisé de FTP (SFTP) mais elle n'est pas utilisée de façon universelle.

La plupart des serveurs FTP anonymes vous permettent d'accéder à leurs fichiers en utilisant le protocole FTP via un navigateur web. Il existe aussi de célèbres clients FTP qui fonctionnent comme des programmes de gestion de fichiers. Une fois que vous-vous êtes connectés au serveur FTP, vous pouvez télécharger des fichiers sur votre ordinateur un peu plus de la même manière que vous déplacer les fichiers sur votre ordinateur. FTP met un peu plus de temps pour télécharger chaque fichier sur votre ordinateur, principalement parce qu'il se peut que le serveur FTP se trouve de l'autre côté de la planète.

Exercices

4.12 Les systèmes d'exploitation Windows, OS X et Linux sont munis par défaut d'un client FTP en ligne de commandes ; pour y accéder, ouvrez une fenêtre d'Invite de commandes ou une fenêtre de terminal et saisissez-y:

```
ftp
```

Après l'Invite `ftp>`, vous pouvez saisir `help`, pour obtenir une liste des commandes disponibles.

```
ftp> help
Commands may be abbreviated.  Commands are:
!               delete          literal         prompt          send
?               debug           ls              put             status
append          dir             mdelete         pwd             trace
ascii           disconnect      mdir            quit            type
bell            get             mget            quote           user
binary          glob            mkdir           recv            verbose
bye             hash            mls             remotehelp
cd              help            mput            rename
close           lcd             open            rmdir
```

Les commandes de base sont:

Pour vous connecter au serveur FTP nommé *ftp.domain.name*:

```
ftp> open ftp.domain.name
```

Pour afficher (lister) le contenu du répertoire distant:

```
ftp> ls
```

ou

```
ftp> dir
```

Pour vous déplacer d'un dossier distant vers un dossier nommé *newdir*:

```
ftp> cd newdir
```

Pour télécharger un fichier nommé *filename* de l'ordinateur distant sur la machine locale:

```
ftp> get filename
```

Pour télécharger plusieurs fichiers nommés respectivement *file1*, *file2*, et *file3* de l'ordinateur distant vers la machine locale (vous pouvez aussi utiliser les caractères joker pour télécharger plusieurs fichiers ayant le même suffixe, ou tous les fichiers qui se trouvent dans un dossier):

```
ftp> mget file1 file2 file3
```

Pour télécharger un fichier nommé *filename* de l'ordinateur local vers l'ordinateur distant:

```
ftp> put filename
```

Pour vous déconnecter d'un serveur FTP

```
ftp> close
```

Pour fermer votre client FTP local:

```
ftp> quit
```

Une session FTP, étape par étape:

Pour vous connecter à un service ftp anonyme, ouvrez premièrement votre client FTP local:

```
ftp
```

Utilisez la commande *open* pour vous connecter au serveur. Voici la commande à exécuter:

```
ftp> open anon.server
```

Cette commande connecte votre client FTP au serveur FTP anonyme nommé *anon.server*. Vous devez y substituer le nom réel d'un serveur, bien sûr.

Lorsque le serveur FTP distant accepte votre connexion, il s'identifie sur votre client local, puis il demande un nom d'utilisateur:

```
Connected to anon.server.
220 ProFTPD Server (Welcome . . . )
User (anon.server:(none)):
```

Pour la plupart des serveurs FTP anonymes, vous devriez saisir le mot *anonymous (ou ftp)* comme nom d'utilisateur. Le serveur FTP distant vous enverra un accusé de réception pour vous notifier que vous vous connectez en tant qu'utilisateur anonyme, et il vous donnera des instructions sur ce qu'il faut utiliser comme mot de passe.

```
331 Anonymous login ok, send your complete email address as your
password.
Password:
```

Dans la plupart des cas, le serveur distant ne vérifie pas la validité de l'adresse email saisie en tant que mot de passe, donc il ne vous empêchera pas d'accéder au service si vous saisissez une fausse adresse email. Ceci est considéré comme une violation de nétiquette, mais c'est en réalité nécessaire: ne donnez pas votre adresse email réelle ! Après avoir saisi un mot de passe, le serveur distant vous enverra un message de bienvenue sur votre ordinateur local.

```
230-
   Welcome to ftp.anon.server, the public ftp server of anon.server. We
   hope you find what you're looking for.
   If you have any problems or questions, please send email to
   ftpadmin@anon.server
   Thanks!
230 Anonymous access granted, restrictions apply.
```

A présent, vous pouvez utiliser les commandes ls, dir, cd et get pour télécharger des fichiers d'un serveur distant sur votre ordinateur local.

Exercices

4.13 En vous basant sur ces exemples, trouvez et téléchargez un fichier à partir d'un serveur FTP anonyme.

4.14 Utilisez votre navigateur web et un moteur de recherche pour trouver un serveur FTP anonyme qui possède une copie d'*Alice au Pays des Merveilles*, ensuite, à l'aide du client FTP en ligne de commandes – pas à l'aide de votre navigateur web – téléchargez le fichier.

4.15 Quels sont les meilleurs clients FTP qui existent ? Offrent-ils la possibilité d'automatiser toutes les choses de la ligne de commandes et fournissent-ils une bonne interface graphique ? Avez-vous perdu une des fonctionnalités que vous aviez à la ligne de commande ?

4.16 Votre ordinateur pourrait-il devenir un serveur FTP ?

Telnet et SSH

Telnet permet à un utilisateur local d'envoyer une grande variété de commandes vers un ordinateur distant. Ceci permet à l'utilisateur local de donner des instructions à l'ordinateur distant pour effectuer des tâches et de renvoyer les données vers la machine locale, presque comme si vous étiez assis devant le clavier de l'ordinateur distant. **Secure Shell (SSH)** est prévu comme un remplaçant sécurisé, chiffré de telnet.

Une fois encore, la plupart des versions de Windows, OSX, et Linux sont munies d'un client telnet en ligne de commandes. Pour y accéder, ouvrez une fenêtre d'Invite de commandes et saisissez-y:

```
telnet
```

Pour accéder à un serveur telnet, vous aurez besoin d'un compte et d'un mot de passe qui sont configurés par l'administrateur du serveur, parce que le programme telnet vous

permet de faire beaucoup de choses, et certaines pourraient sérieusement endommager l'ordinateur distant.

Telnet était utilisé autre fois pour permettre aux administrateurs d'ordinateurs de contrôler les serveurs à distance et de fournir de l'assistance à distance aux utilisateurs. Ce service fait parti de l'ancien Internet et n'est plus du tout utilisé.

Telnet peut être utilisé pour d'autres tâches, telles que l'envoi et la réception de courriel et pour voir le code source des pages web (bien que telnet soit probablement le moyen le plus difficile qui permet d'accomplir ces choses). Plusieurs de ces choses sont légales mais elles peuvent être utilisées de façon abusive et illégale ou bien pour des raisons immorales. Vous pouvez utiliser telnet pour consulter votre courriel, et voir non pas seulement le sujet (ou l'objet), mais les quelques premières lignes d'un courriel, ce qui vous permet de décider s'il faut effacer ou non le courriel sans télécharger le message entier.

Si vous allez utiliser SSH, assurez-vous d'utiliser une version récente, parce que les anciennes versions ont de nombreuses vulnérabilités, et plusieurs analyseurs automatiques de vulnérabilités recherchent ces vulnérabilités sur Internet.

Début du Jeu: Commande Moi

L'écran noir clignote devant les gros verres de Grand-Père au moment ou le curseur clignote impatiemment, espérant une commande. Avec ces cheveux gris minces qui recouvraient avec nonchalance sa tête ridée, Grand-Père tapait au clavier. Jace suivait le silencieux pianiste qui appuyait sur les touches de son ordinateur, tap, tap, tap, tap. Il a sourit à Jace en tournant sa tête pour regarder dans ses yeux de jeune. "Jace, je vais te montrer un autre monde là-bas. Attache la ceinture de ton siège", disait-il à la fille de huit ans en lui faisant un clin d'œil.

Les pieds de Jace touchaient à peine le sol lorsqu'elle était assise aux côtés de son Grand-Père qui se trouvait en face de l'écran de l'ordinateur. Elle a entendu la tonalité d'invitation à numéroter d'un téléphone provenant d'un petit boîtier proche de là. La boîte blanche s'est allumée avec des lumières vertes et rouges au moment où la tonalité a changé pour devenir un son semblable au bruit produit par un canard englouti dans un dispositif d'ordures. Grand-Père a soulevé ces sourcils excités et regardait fixement avec toute sa force, l'écran noir qui se trouvait en face de lui. Le canard a cessé de gémir et toutes les lumières se sont transformées en vert sur le boîtier du téléphone.

Grand-Père disait, "Regarde ce-ci".

Habituellement lorsque Grand-Père dit "regarde ceci", quelque chose explose ou une fumée noire sortirait de quelque chose. Autrement dit, "regarde ceci" voudrait dire que Grand-Mère allait s'affoler à cause d'une erreur qu'il a commise. Jace aimait entendre ces mots pourtant, parce que c'était une anticipation excitante pour quelques événements merveilleux.

L'écran de l'ordinateur est sorti de son sommeil noir avec une bannière contenant du texte ASCII qui entoure les mots "Bienvenue à Cline's Bulletin Board System (BBS)". "Nous y sommes entrer", acclama Grand-Père et tenta de faire un tope là à la fille Jace âgée de huit ans. Il a raté sa main de plusieurs pouces et il a presque giflé la petite fille. Elle a ri, et Grand-Père a ri aussi.

Ils on tous les deux regardé devant et derrière tout en restant devant le clavier et l'écran de l'ordinateur. Grand-Père a frotté ses doigts pendant que Jace frottait sa pensée, en essayant de comprendre ce qui se passe. Grand-Père a commencé à saisir des commandes sur le silencieux piano, avec la tête penchée sur les touches comme un vautour qui serait entrain de manger une dépouille sur la route. Tête haute, tête basse, tête haute, tête basse. Oops. Il est assis à l'arrière. Grand-Père a oublié quelque chose de très important.

Il a pris une pause et parlé comme un instructeur. "Jace, je suis désolé mais j'ai oublié de te dire ce qui se passe ici. Présentement, je suis connecté à un autre ordinateur via notre ligne téléphonique. Cette chose qui émettait ce bruit là-bas est appelée "Modem" et son rôle est de convertir un signal numérique en un signal analogique et vis versa". Jace en savais déjà davantage à propos des systèmes téléphoniques compte tenu du fait que Grand-Père saisissait toutes les chances possibles pour s'amuser avec ces choses. 48 volts lors d'un usage normal et 90 volts lorsque le téléphone sonne, elle en savait plus que ce qu'un technicien du téléphone devait savoir. Le système téléphonique classique (POTS: Plain Old Telephone System) était un jeu entre elle et Grand-Père. Grand-Mère ne semble pas adhérer au jeu du téléphone classique qui rendait la parti plus amusante.

Une tierce personne peut se brancher sur des lignes téléphoniques, mais cela peut être détecté à l'aide d'un régulateur de tension. La tension sur la ligne téléphonique connaîtra un pic momentanément et sera maintenue légèrement élevée si quelqu'un essaie de se brancher sur la ligne. Jace pensait que Grand-Père aimait son voltmètre plus qu'il n'aime Grand-Mère ; il ne sortait jamais de la maison sans lui. Grand-Père est allé plus loin en nommant son appareil "Valérie". Valérie le voltmètre. C'était son meilleur ami, outre Jace.

Jace a levé ses yeux vers Grand-Père, et en faisait davantage pendant le cours sur la conversion de la modulation analogique en modulation numérique, la conversion d'un son en un son numérique. C'est presque tout ce que fait un modem. Grand-Père a continué son cours pour l'élève répugnant, "L'ordinateur auquel je me suis connecté me permet de me connecter à d'autres ordinateurs et de m'amuser avec tous les services qu'ils fournissent". Ses oreilles ont entendu un mot dont elle n'en a jamais entendu parlé, les "services".

"Grand-père que veux tu dire par services ?" demanda la fille curieuse en espérant une réponse qui impliquait les fast food. "Excellente question, ma chère", Grand-Père espérait que Jace pose une telle question. "Mon ordinateur est connecté à un réseau d'ordinateurs où j'ai la possibilité de me connecter à d'autres ordinateurs dans le monde", répondit-il joyeusement. "Ce modem me permet de communiquer avec ces ordinateurs qui donnent accès à des fichiers, des informations, des gens avec lesquels je peux discuter, et d'autres choses merveilleuses. Ces ordinateurs offrent des services comme File Transfer Protocol, Usenet, IRC, Telnet, et le courriel (Email).

Jace n'était pas satisfaite par la réponse qu'elle a obtenue et habituellement cela donne l'occasion de poser rapidement plus de nouvelles questions à Grand-Père. Elle a ouvert sa ceinture de questions et a commencé le carnage: "Qu'est que le protocole FTP ? Qu'est ce que MIC ? Où est Telknit ? Les courriels ont-ils besoin de tampons spéciaux ? Quelle couleur existe dans le monde numérique ? Qui a inventé Usednet ? Pourquoi l'appelle-t-on Imail ? Grand-mère connaît-elle tes services ? Pourquoi les appelles t-on services ? D'où viennent les bébé ? D'où vient Jello ?

Grand-Père devait boucher ses oreilles afin de mettre son cerveau à l'abri de l'assaut de questions.

"Attend, attend, attend, vas-y lentement".

Fin du Jeu

DNS

Lorsque vous désirez appeler un ami par téléphone, vous avez besoin de connaître le numéro de téléphone exact ; lorsque vous désirez vous connecter à un ordinateur distant, vous avez besoin de connaître aussi son numéro. Si vous vous rappelez des notions rencontrées dans les leçons précédentes, pour le ordinateurs qui se trouvent sur Internet, ce numéro désigne l'adresse IP.

Les adresses IP sont facilement gérées par les ordinateurs, mais nous les humains préférons utiliser des noms, dans ce cas les **noms de domaines**. Par exemple, pour vous connecter au site web de Hacker Highschool, saisissez www.hackerhighschool.org dans la barre d'adresse d'un navigateur web. Cependant, le navigateur web ne peut se servir de ce nom pour se connecter au serveur qui héberge le site web de Hacker Highschool – il a besoin d'une adresse IP. Cela veut dire que votre machine locale doit avoir un mécanisme qui lui permette de traduire les noms de domaine en adresses IP. S'il y avait seulement des centaines, voir des milliers d'ordinateurs sur l'Internet, alors il serait possible d'avoir une simple table (un **fichier d'hôtes**) sauvegardé sur votre ordinateur qui vous permet de rechercher ces adresses. Cependant, pour le meilleur ou le pire, il n'y a seulement que l'existence des millions d'ordinateurs sur l'Internet, mais les corrélations entre les noms de domaines et les adresses IP changent constamment.

Domaine Name Service (DNS) est utilisé pour faire dynamiquement la traduction entre les noms de domaine et les adresses IP (et vis versa). Lorsque vous saisissez *www.nom_de_domaine.com* dans votre navigateur web, votre navigateur web contact le serveur DNS choisi par votre FAI. Si ce serveur DNS possède l'adresse *www.nom_de_domaine.com* dans sa base de données, alors il renvoie son adresse IP à votre ordinateur, ce qui vous permet de vous-y connecter.

Si votre serveur DNS ne possède pas *www.nom_de_domaine.com* dans sa base de données, alors il envoie la requête à un autre serveur DNS, et ils continueront de relayer la requête d'un serveur DNS à un autre jusqu'à ce qu'il ne trouve la bonne adresse IP, ou ne déterminent l'invalidité du nom de domaine.

Exercices

4.17 Ouvrez une fenêtre d'Invite de commandes et identifiez l'adresse IP de votre ordinateur. Quelles sont les commandes que vous avez utilisées ? Quelle adresse IP possédez-vous ?

4.18 Identifiez l'adresse IP de votre serveur DNS. Quelle commande avez-vous utilisée ? Quelles est l'adresse IP du serveur DNS ?

4.19 Exécutez la commande ping vers *www.isecom.org*. Avez-vous obtenue une réponse ? Quelle est l'adresse IP qui a répondu à la commande ping ?

4.20 Pouvez-vous ordonner à votre ordinateur d'utiliser un autre serveur DNS ? Si oui, changez la configuration de votre ordinateur pour qu'il utilise un autre serveur DNS. Faites encore ping *www.isecom.org* . Avez-vous obtenue la même réponse ? Pourquoi ?

DHCP

DHCP ou Dynamic Host Configuration Protocol permet au serveur d'un réseau local d'attribuer des adresses IP au sein du réseau. Le serveur possède un bloc d'adresses IP valides. Lorsqu'un ordinateur se connecte au réseau, il obtient une adresse IP. Lorsque l'ordinateur est déconnecté, il se débarrasse de l'adresse IP et cette adresse est de nouveau disponible pour un autre ordinateur.

Ceci est utile au sein des grands réseaux d'ordinateurs, puisqu'il n'est pas nécessaire pour chaque ordinateur d'avoir une adresse qui lui est individuellement allouée, une adresse IP statique. Autrement, il faut utiliser un serveur DHCP. Lorsqu'un nouvel ordinateur se connecte au réseau, la première des choses à faire, c'est de demander une adresse IP au serveur DHCP. Une fois qu'une adresse IP lui est allouée, l'ordinateur a alors accès à tous les services du réseau.

Maintenant pensez à cela. La plupart des réseaux Wi-Fi offre le service DHCP, ce qui veut dire *n'importe qui* peut obtenir une adresse IP dans ce sous-réseau. Si vous gérez un café c'est exactement ce dont vous avez besoin, mais si vous gérer un bureau sécurisé, vous devriez par contre, considérer l'utilisation des adresses IP statiques. Cela dépend….

Les Connexions

Par le passé, les ordinateurs se connectent à l'Internet via un modem. Les modems traduisent les bits en impulsions sonores et vis versa, en **mod**ulant et en **dém**odulant, d'où le nom modem. Les vitesses des modems sont mesurées en **baud** (un nombre rationnel) et en **bps,** ou bits par seconde**.** Un nombre élevé de baud signifie habituellement un nombre élevé de bps, mais vous devez considérer aussi ce que vous projetez faire. Il existe certaines applications – telle que faire du telnet vers **Multi-User Dungeons (MUDs)** – pour lesquelles un modem vieux de vingt ans cadencé à 300 baud serait toujours acceptable (ceci étant fait bien que votre rapidité au clavier ne soit pas bonne), pendant que les applications à large bande passante telles que le flux continu de vidéo peuvent souvent ralentir les capacités des plus puissants câbles et connexions DSL.

Les Fournisseurs d'Accès Internet (FAI)

Vous ne vous connectez pas directement à l'Internet. Vous avez besoin d'accéder à un serveur qui va connecter votre ordinateur à l'Internet. Ce serveur exécute les plus lourdes tâches, et est continuellement allumé. Ce serveur est géré par un **fournisseur d'accès Internet (FAI)**.

Un FAI possède un point de présence qui est constant sur l'Internet, et il possède des serveurs qui fournissent des services dont vous pouvez vous servir. Mais vous pourrez aussi implémenter ces services vous même. Par exemple, vous pourrez implémenter un serveur mail sur votre ordinateur local, mais cela vous obligera à maintenir l'ordinateur allumé et connecté à un réseau en permanence, juste pour attendre ses moments brefs pendant lesquels il y a échange d'informations. Un FAI, cependant, unit les efforts d'un grand nombre d'utilisateurs, ainsi le serveur mail fonctionne en permanence, au lieu de rester là, à ne rien faire. Les ordinateurs du FAI utilisent une connexion à très haut débit pour se connecter à un ***point d'accès réseau*** – ***Network Access Point (NAP)***. Ces NAP sont connectés entre eux via des connexions ultra-rapides appelées **épine dorsale (backbone).** L'ensemble de toutes ces choses constituent l'Internet.

Le Service Téléphonique Traditionnel – POTS (Plain Old Telephone Service)

L e **service POTS** était autrefois le moyen le plus utilisé pour accéder à l'Internet. Son premier inconvénient est sa lenteur de connexion, mais dans plusieurs cas cela est dû à sa grande disponibilité. La plupart des FAI nationaux possèdent un grand nombre de numéros à accès local, et presque tout le monde possède encore un téléphone avec une ligne fixe. En théorie, si vous avez un modem acoustique et une poche pleine de sous, vous pourriez vous connecter à partir de presque n'importe quel téléphone public (si vous pouvez-en trouver un). Nous ne pensons pas que voudriez vraiment faire cela.

Le service POTS est lent. Le modem téléphonique le plus rapide possède un débit de 56,600 bits par seconde (bps). Cela, cependant, comme on l'a écrit dans le petit manuel, est un mensonge. Les contraintes de l'alimentation électrique limitent la vraie vitesse de téléchargement à 53,000 bps et le débit efficace est habituellement moins que cela. Ceci ne fait pas le poids devant modems DSL ou les modems câble.

Ceci étant dit, le service téléphonique est largement disponible, les FAI basés sur le service POTS sont relativement moins chères (et quelques fois gratuits). Vous n'aimeriez pas échanger des films piratés via le service POTS, parce que cela est immoral, illégal et occupe votre ligne téléphonique pendant toute la nuit et peut être tout le week-end, mais vous pourriez envoyer des messages amicaux, des courriels en texte à Granny. Et si vous avez utilisé telnet, vous pourriez faire la même chose avec une vielle machine poussiéreuse fonctionnant sous DOS que vous avez sortie du sous-sol.

La Ligne Numérique d'Abonné -Digital Subscriber Line (DSL)

Une **Ligne Numérique d'Abonné** ou **Digital Subscriber Line (DSL)** est une méthode qui permet d'envoyer une grande quantité d'informations via les lignes téléphoniques POTS qui existent déjà. Son avantage principal par rapport à POTS est qu'il est plus rapide que les modems analogiques, et il fournit une connexion permanente. En plus, il vous permet d'avoir le service téléphonique traditionnel pendant que vous êtes connectés à l'Internet. Son inconvénient principal est que sa disponibilité est limitée par votre proximité par rapport au central téléphonique – si vous êtes très loin du central téléphonique, vous n'avez pas de chance.

Les Modems Câble

Les passerelles câbles n'utilisent pas les lignes téléphoniques traditionnelles pour vous connecter à l'Internet. Par contre ils utilisent le câble coaxial (ou les lignes à fibre -optique, si vous avez réellement la chance d'en avoir) fournies par les compagnies de câble. Comme DSL, les passerelles câbles peuvent vous permettre d'émettre et de recevoir des appels téléphoniques habituels au moment où vous êtes connectés à l'Internet, et ils fournissent une connexion permanente, mais les passerelles câbles sont généralement plus rapides que DSL.

Les passerelles câbles ont quelques défauts de base. Le premier est que l'accès à la passerelle câble est une ressource partagée, donc votre vitesse de connexion régressera lorsqu'il y aura d'autres utilisateurs branchés sur le même câble que vous. Le second est que l'accès câble n'est disponible que dans les zones où les compagnies qui fournissent le service câble, ont installé le câblage nécessaire. Et le plus important est que n'importe quel trafic que vous générez sur le câble peut être accessible à tout autre utilisateur branché sur ce câble! Cela veut dire que si vous connectez votre ordinateur à la passerelle câble et que vous n'utiliser pas de pare-feu, tout le monde dans votre voisinage peut voir votre ordinateur et tous ses fichiers. Voulez-vous réellement partager vos informations bancaires ainsi?

Wimax

Le WiMAX est une méthode de connexion sans-fil qui concurrence généralement DSL. Il est utilisé dans les zones où l'implémentation d'une infrastructure de câbles serait trop coûteuse ou difficile à faire. La force du signal peut être affectée par les bâtiments, les arbres ou d'autres objets larges. Certaines versions utilisent un point d'accès fixe, mais d'autres vous donnent un accès mobile dans des zones vraiment étendues.

Wifi

Wi-Fi n'est pas une méthode qui vous connecte à votre FAI mais c'est une méthode d'interconnexion réseau qui vous permet de vous connecter à l'Internet à la maison ou dans les centres commerciaux tels que les grandes surfaces ou dans les cafés. La plupart des smartphones et tous les ordinateurs portables utilisent maintenant le Wi-Fi donc c'est une cible favorite des attaquants. Supposons que vous êtes nus (es) dans une salle peuplée lorsque vous utilisé une connexion Wi-Fi publique: couvrez-vous, assurez-vous que personne ne vous regarde mais supposez que tout le monde voudrait le faire. Vous étudierez bien sûr la leçon qui concerne la Sécurité Sans-Fil aussi, n'est ce pas?

Exercices

4.21 Quel genre de connexion Internet avez-vous à la maison, si vous en avez ? Comment pouvez-vous en parler ? Et le plus important:

4.22 Qui pouvez-vous voir sur ce réseau ? (Comment pouvez-vous le découvrir?)

4.23 Quelles est la rapidité de votre connexion ? Pouvez-vous améliorer la vitesse de votre connexion sans faire recours à votre FAI ?

4.24 Quels sont les services supplémentaires qu'offrent votre FAI ? Nous avons déjà parlé des services ; il se peut que votre FAI en fournisse plusieurs.

4.25 Quels sont les services que vous pouvez implémenter sur votre propre ordinateur ?

Étoffez Vos Connaissances: Amusez-vous avec HTTP

HTTP, est l'acronyme de HyperText Transfer Protocol, c'est une application qui se trouve à la tête de la pile de protocoles TCP/IP comme le définit les deux principaux RFC:

- 1945 pour1.0 (basé sur la version 0.9).

- 2616 pour 1.1.

Il y a quelques légères améliorations et différences entre les version 1.0 et 1.1 pour l'Extensibilité, la Mise en Cache, l'Optimisation de la Bande Passante, la Gestion de la connexion Réseau, la transmission de Messages, la conservation d'adresse Internet, la notification d'Erreurs, la Sécurité, l'Intégrité, et l'authentification, la négociation de Contenu [3]. Les différences entre 1.0 et 1.1 sont utiles pour obtenir les informations à propos d'un serveur web.

Fondamentalement HTTP est un protocole sans état dans lequel le Client envoie une requête HTTP au Serveur, qui lui renvoie une Réponse HTTP: le paradigme Requête/Réponse.

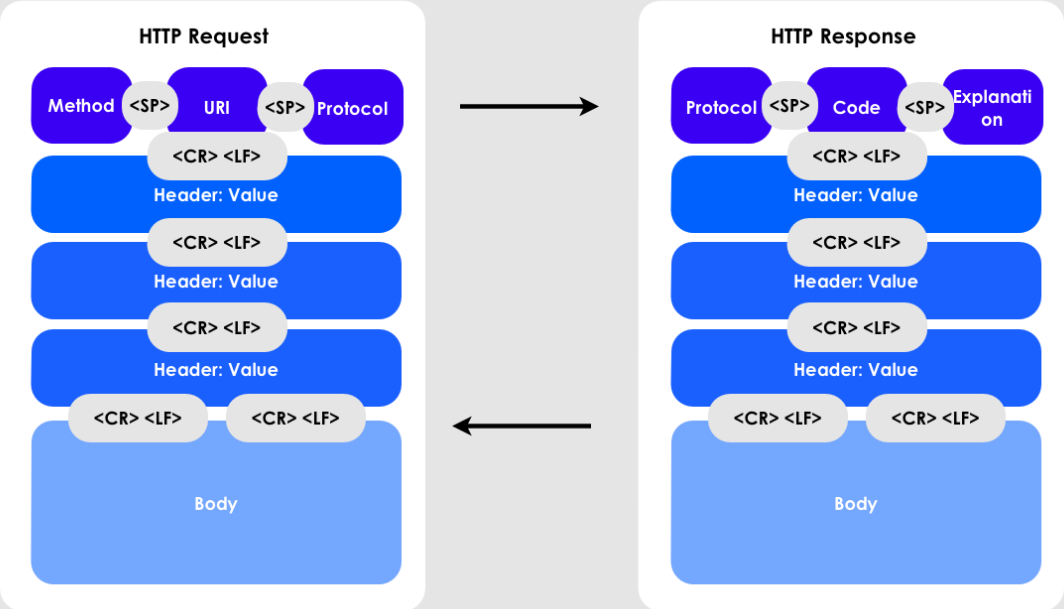

Figure 4.1: HTTP

Comme vous pouvez le savoir, nous pouvons obtenir une importante quantité d'informations en envoyant des commandes à un serveur HTTP. Pour ce faire, nous utiliserons des outils réseau de base:

- netcat: la boîte à outils TCP/IP
- curl: la boîte à outils HTTP
- proxy: tel OWASP ZAP ou Burpsuite gratuit

Sniffez la Connexion Entre Vous et le Serveur HTTP de HHS

Utilisez un proxy pour connecter votre navigateur. Accédez à http://www.hackerhighschool.org et intercepter votre requête:

```
GET / HTTP/1.1
Host: www.hackerhighschool.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:11.0)
Gecko/20100101 Firefox/11.0
Accept:
```

```
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Proxy-Connection: keep-alive
```

et la réponse:

```
HTTP/1.1 200 OK
Content-Length: 10376
Date: Fri, 03 Feb 2013 09:11:17 GMT
Server: Apache/2.2.22
Last-Modified: Mon, 06 Feb 2013 09:31:18 GMT
ETag: "2f42-4b8485316c580"
Accept-Ranges: bytes
Identity: The Institute for Security and Open Methodologies, The
Institute for Security and Open Methodologies
P3P: Not supported at this time, Not supported at this time
Content-Type: text/html
Connection: keep-alive

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"[]><html
xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US"
xml:lang="en"><head><meta http-equiv="Content-Type"
content="text/html; charset=UTF-8" /><title>Hacker Highschool -
Security Awareness for Teens</title>
[...]
```

Exercices

4.26 Identifiez les parties des requêtes venant du proxy en utilisant les figures ci-dessus

4.27 Y-a-t-il des informations intéressante dans les en-têtes ?

Votre Première Connexion Manuelle

Netcat peut être utilisé pour se connecter à un serveur web en paramétrant les ports sur l'hôte.

Commencez par saisir:

```
nc www.hackerhighschool.org 80
```

Ensuite tapez sur Entrée deux fois.

```
GET / HTTP/1.0
```

Le serveur répondra:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"[]>
<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US"
xml:lang="en"><head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>ISECOM - Institute for Security and Open Methodologies</title>
<meta name="description" content="Description" />
```

Comme vous pourrez le constater, la page semble provenir de isecom.org et non de

hackerhighschool.org. Pourquoi ?

Une hypothèse pourrait être la suivante, le même hôte donne accès à la fois aux sites de HHS et de ISECOM. Cela est-il possible ?

Pour découvrir cela, vérifiez l'adresse IP de hackerhighschool.org :

```
nslookup www.hackerhighschool.org
[...]
Non-authoritative answer:
www.hackerhighschool.org      canonical name = hackerhighschool.org.
Name: hackerhighschool.org
Address: 216.92.116.13
```

Et maintenant pour www.isecom.org:

```
nslookup isecom.org
[...]

Non-authoritative answer:
Name: isecom.org
Address: 216.92.116.13
```

La même adresse IP ! En utilisant netcat il est possible d'afficher l'hôte en ajoutant manuellement l'en-tête de l'hôte et en utilisant HTTP 1.1

```
GET / HTTP/1.1
Host: www.hackerhighschool.org

HTTP/1.1 200 OK
Content-Length: 10376
Date: Fri, 03 Feb 2013 09:11:17 GMT
Server: Apache/2.2.22
Last-Modified: Mon, 06 Feb 2013 09:31:18 GMT
ETag: "2f42-4b8485316c580"
Accept-Ranges: bytes
Identity: The Institute for Security and Open Methodologies, The
Institute for Security and Open Methodologies
P3P: Not supported at this time, Not supported at this time
Content-Type: text/html
Connection: keep-alive
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"[]>
<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US"
xml:lang="en"><head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Hacker Highschool - Security Awareness for Teens</title>
```

La Méthode Requête

Une autre partie d'une requête HTTP qui peut être modifiée est la Méthode Requête. Habituellement les applications web utilisent les requêtes GET et POST, mais d'autres protocoles de requêtes peuvent être actifs sur un serveur web ou un serveur d'applications. Les méthodes souvent utilisées sont:

- **OPTIONS** - elles sont utilisées pour demander quelles sont les options de requêtes qui sont supportées. Si vous gérez un serveur web, sachez que le fait de fournir de telles informations pourrait être une source de nuisance.
- **GET** - elle est utilisée pour extraire directement les informations via l'URL, par exemple:
  `http://www.usairnet.com/cgi-bin/launch/code.cgi?`

```
Submit=Go&sta=KSAF&state=NM
```

Regardez toutes ces choses qui se trouvent après le point interrogation " ?". C'est la donnée requise. L'échange des données de cette façon est risquée, parce qu'elle est entièrement visible, et il est facile de le bricoler.

- **HEAD** - elle est utilisée comme GET mais le serveur ne renvoie pas la page courante.
  Elle peut être utilisée pour identifier les Accès, optimiser l'utilisation de la bande passante et – dans certains cas – contourner les contrôles d'accès. En effet certaines implémentations de Liste de Contrôle d'Accès – ACL (Access Control List) vérifient seulement les requêtes GET. Dans ce cas, vous avez découvert une Vulnérabilité.
- **POST** - elle est utilisée pour envoyer les données aux applications web – comme GET – mais les données sont transmises dans le Corps de la Requête, hors de vue du moins à un degré.
- **PUT** - elle est utilisée pour allouer des ressources sur un serveur web ou pour le mettre à jour.
  Dans plusieurs contextes cette méthode devrait être désactivée ou protégée par un Contrôle d'Authentification. Dans d'autres contexte c'est une découverte merveilleuse.
- **DELETE** - elle est utilisée pour libérer (effacer) des ressources sur un serveur web.
  Cette méthode devrait être désactivée ou protégée par un Contrôle d'Authentification. Confer PUT ci-dessus.
- **TRACE** - elle est utilisée comme une boucle de la couche application qui reflète les messages. Cette méthode de débogage devrait être désactivée, en particulier dans les environnements en production parce qu'elle pose des Problèmes de Confidentialité et introduit une Vulnérabilité parce qu'elle peut être utilisée pour exécuter des exploits basé sur le Cross Site Scripting.
- **CONNECT** – elle est utilisée pour se servir du serveur web comme proxy.
  Ceci devrait être désactivée ou protégée par un Contrôle d'Authentification parce qu'il permet à d'autres personnes de se connecter aux services d'une tierce partie en utilisant l'adresse IP du proxy.

Notez aussi que plusieurs protocoles basés sur HTTP peuvent ajouter plus de méthodes, comme WebDAV. Vous pouvez altérer la Méthode de Requête afin d'observer les réponses d'un serveur pour y découvrir des choses intéressantes, en demandant les méthodes connues et les mots arbitraires.

Les OPTIONS de Requête

Vous pouvez démarrer la session netcat comme d'habitude:

```
nc www.hackerhighschool.org 80
```

Mais n'appuyez pas sur Entrée deux fois. Mais, saisissez la ligne suivante:

```
OPTIONS / HTTP/1.1
```

et vous obtiendrez un réponse comme:

```
Host: www.hackerhighschool.org
HTTP/1.0 200 OK
Date: Tue, 07 Feb 2013 08:43:38 GMT
Server: Apache/2.2.22
Allow: GET,HEAD,POST,OPTIONS
Identity: The Institute for Security and Open Methodologies, The
Institute for Security and Open Methodologies
```

```
P3P: Not supported at this time, Not supported at this time
Content-Length: 0
Content-Type: text/html
```

Réquisition d'en-tête HEAD

Cette fois, après le démarrage de votre session, saisissez l'option HEAD.

```
# nc www.hackerhighschool.org 80
HEAD / HTTP/1.1
Host: www.hackerhighschool.org

HTTP/1.0 200 OK
Date: Tue, 07 Feb 2013 08:41:14 GMT
Server: Apache/2.2.22
Last-Modified: Fri, 13 Feb 2013 15:48:14 GMT
ETag: "3e3a-4bd916679ab80"
Accept-Ranges: bytes
Content-Length: 15930
Identity: The Institute for Security and Open Methodologies
P3P: Not supported at this time
Content-Type: text/html
Age: 45
Connection: close
```

Permettez Moi de Vous Utiliser Comme Un Proxy: la Requête CONNECT

```
# nc www.hackerhighschool.org 80
CONNECT http://www.isecom.org/ HTTP/1.1
Host: www.hackerhighschool.org
```

Exercice

4.28 Utiliser netcat (nc) pour essayer toutes les méthodes de Requête listées ci-dessus, sur les serveurs de HHS ou sur un serveur implémenté pour ce fait. Quelles sont les choses intéressantes que vous pouvez découvrir ?

Conception des Scripts de Requêtes HTTP avec curl

Certains Test d'Applications Web ne sont pas basés uniquement sur la réponse du Serveur Web mais sur la Couche Application (Web). Souvent vous pouvez découvrir des vulnérabilités dans une application web en manipulant les paramètres GET et POST, en altérant les cookies ou en bricolant les en-têtes. Un outil utile, pour le scripting bash est la commande **curl**, un outil en ligne de commande qui permet d'effectuer une requête de page web. Mais curl ajoute une logique contrairement à netcat.

La requête:

```
curl http://www.isecom.org
```

n'est pas la même chose que:

```
nc www.isecom.org 80
GET / HTTP/1.1
```

Pour constater cela, vous pouvez utiliser l'option -v pour l'affichage en mode parlant (ou verbeux):

```
curl -v http://www.isecom.org/
* About to connect() to www.isecom.org port 80 (#0)
*   Trying 216.92.116.13...
```

```
* connected
* Connected to www.isecom.org (216.92.116.13) port 80 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.26.0
> Host: www.isecom.org
> Accept: */*
>
* HTTP 1.0, assume close after body
< HTTP/1.0 200 OK
< Date: Tue, 07 Feb 2013 09:29:23 GMT
< Server: Apache/2.2.22
< Last-Modified: Fri, 13 Feb 2013 15:48:14 GMT
< ETag: "3e3a-4bd916679ab80"
< Accept-Ranges: bytes
< Content-Length: 15930
< Identity: The Institute for Security and Open Methodologies
< P3P: Not supported at this time
< Content-Type: text/html
< Age: 247
< Connection: close
<
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"[]>
<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US"
xml:lang="en">
[...]
```

Comme vous pouvez le constater, curl sélectionne automatiquement la version 1.1 de HTTP, puis ajoute les en-têtes HOST, ensuite user agent et accept. Ce qui fait référence à une règle importante pour les hackers: maîtrisez vos outils.

Heureusement curl est un outil magnifique qui peut être énormément personnalisé en utilisant des options.

Pour voir toutes ces options, saisissez ce qui suit: `curl –help`

Certaines options dont le fonctionnement est similaire à l'exemple netcat cité ci-dessus sont:

- **-H** pour ajouter une ligne d'En-tête
- **- X** pour choisir une méthode de requête (aussi connue sous le nom de commande)
- **-d** pour ajouter une donnée POST
- **-i** pour ajouter une donnée POST
- **-s** pour activer le mode silencieux, très utile pour le scripting

Avec curl et un peu de scripting bash, vous pouvez automatiser les tests des applications web. La recherche des en-têtes HTTP intéressantes provenant d'un serveur web peut être automatisée en utilisant simplement curl et grep:

```
# curl -siX HEAD http://www.isecom.org/ | grep "Server:"
Server: Apache/2.2.22
```

Exercice

4.29 Développez le script ci-dessus pour réquisitionner plus d'en-têtes HTTP et des informations qui sont potentiellement utiles.

Références et Lecture Ultérieure

http://www.ietf.org/rfc/rfc1945.txt

http://www.ietf.org/rfc/rfc2616.txt

http://www8.org/w8-papers/5c-protocols/key/key.html

http://netcat.sourceforge.net/

http://curl.haxx.se/

Conclusion

Le World Wide Web est un tout plus complet que l'Internet: il existe toute sorte de services autres que HTTP, FTP, SSH, DNS, DHCP et plusieurs autres qui offrent des ouvertures vers les ordinateurs d'autres personnes – et vers les vôtres. Le fait de comprendre comment vous vous connectez à ces services, que ce soit via "les bons canaux" ou autrement, est la clé qui vous permet de comprendre comment votre ordinateur peut être attaqué – ou comment peut-il attaquer. Rappelez-vous seulement de la devise: Piratez tout, mais ne faites du mal à personne.

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