Hacker Highschool

SECURITY AWARENESS FOR TEENS



LECON 5
IDENTIFICATION DES SYSTEMES

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.

Sommaire

Contributeurs

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Chuck Truett, ISECOM
Kim Truett, ISECOM
Marco Ivaldi, ISECOM
Greg Playle, ISECOM
Bob Monroe, ISECOM
Simone Onofri, ISECOM
Ryan Oberto, Johannesburg South Africa
Dennis King
Mario Platt
Grigoris Chrysanthou

Les Traducteurs

Koffi « Willy » Nassar

ISECOM

Introduction

"Je pense que mon ordinateur est infecté par un virus", me disait l'un de mes élèves. "Pouvez-vous y jeter un coup d'œil?"

J'ai pris l'ordinateur portable de ses mains, je ne l'ai pas ouvert, mais je l'ai incliné dans toutes les directions, en regardant de très prêt. "Selon moi il ressemble à un ordinateur", ai-je dit, en le lui remettant.

"Mais il y a quelque chose qui ne va pas avec cet ordinateur", insista Aidan. "Je suis parti au domicile de mon ami et je m'y suis connecté à Internet, et quelque chose s'est infiltré dans ma boîte électronique et a envoyé des messages à tous mes amis."

"OK, comment accèdes-tu à ta boîte électronique? As-tu installé une application?" Lui ai-je demandé.

"Non, j'y accède sur le web. Je veux dire l'Internet."

"Tu veux dire via un navigateur web?" Il a répondu oui par un geste de la tête. "Ensuite cela veut dire que ta boîte électronique est en ligne, et non sur ton ordinateur. Donc dans ce cas je commencerait avec ton compte courriel(email). As-tu changé le mot de passe?"

"Oui. Ils ont désactivé mon compte jusqu'à ce que je ne le change". Il a baissé la tête, comme s'il y avait plus à ajouter à l'histoire, mais je ne l'ai pas pressé. Je parie qu'on lui avait déjà crier dessus. Beaucoup.

"Est-ce que tes amis on reçu encore plusieurs de ces messages?" lui demandai-je par contre.

"Non" , a-t-il répondu en appuyant fermement sur ses chaussures.

"Et as-tu choisi un mot de passe convenable? Et non 12345?"

Maintenant a-t-il souri. "C'est un mot de passe vraiment complexe. Personne ne pourra jamais l'obtenir".

J'en doute fort, mais j'ai accepté le fait par un signe de la tête. "OK, alors, cela signifie que tu as pris toutes tes précautions".

"Non", a-t-il insisté. "Pourquoi quelqu'un ferait-il cela?"

Maintenant j'ai pêché le poisson. "Pourquoi n'essaies-tu pas de découvrir cela. As-tu l'un de ces courriels que tes amis ont reçus?"

"Oui. J'en ai un paquet. Les gens me les renvoient." Ah: et voilà. J'avais parié que sa liste de contacts en comptait des douzaines. Ou des centaines. Cela devait être amusant.

"Alors il me semble que tu veux savoir où mène ce lien qui se trouve dans le courriel".

Ses yeux montraient qu'il était surpris. "Vous voudrez dire que nous pouvons faire cela?"

"Haha", j'ai rigolé. "Je veut dire TU peux faire cela. Mais je te montrerai comment."

Aidan s'est arrêté. "C'est ce que vous insinuez en parlant tout le temps de brebis et de loup?"

"Oui, c'est exactement cela. Tu peux être l'un ou l'autre. Fait ton choix maintenant," lui ai-je dit.

Soudainement il ne ressemblait plus tellement à un enfant. "Un loup", m'a-t-il répondu.

* * *

L'identification des systèmes peut facilement être l'étape la plus importante de toute attaque ou défense informatique. Tout ce que vous faites après dépend des données que vous avez collectées à cette étape. Quel est le système d'exploitation de l'hôte qui vous attaque, ou que vous défendez? Pouvez-vous – ou d'autres peuvent-ils – voir quels sont les services ou les applications qui y tournent? Qu'en est-il des informations personnelles de l'administrateur: sautent-elles aux yeux n'importe où? Voici les questions à poser à cette étape. En fonction du côté où vous vous trouvez, vous devriez être ravi ou horrifié par ce qui peut facilement être découvert si vous savez là où il faut chercher.

Connaître le fonctionnement d'une attaque est une bonne chose. Connaître comment se protéger contre ou le vaincre est encore mieux. C'est ici que nous commençons à approfondir nos recherches et nous apprenons à identifier un système et à trouver ses faiblesses – que ce soit votre propre système ou le système de quelqu'un d'autre.

Nous nous servirons des outils qui sont disponibles publiquement et nous vous montrerons comment les utiliser. Il ne serait pas assez sensé de vous parler d'un logiciel sans vous apprendre à l'utiliser. Comme n'importe quel logiciel de sécurité, ils peuvent être utilisés pour de bonnes ou de mauvaises intentions. Notre objectif est de vous montrer les deux types d'utilisations afin que vous puissiez relever vos défis de sécurité, pendant que vous vous protéger contre des attaques similaires.

Dans cette leçon, vous suivrez deux personnes: l'une d'entre elles enseigne et l'autre apprend. L'instructeur ne connaît pas toujours ce que sera la réponse donc vous en tant que lecteur, on ne vous servira pas le plat tout cuit. Apprenez à casser les choses et apprenez à les réparer. Répétez ce processus autant de fois que cela soit nécessaire.

Faites très attention aux attributs utilisés dans les différents programmes. Une légère modification d'une syntaxe majuscule en minuscule peut engendrer une donnée entièrement différente, il en est de même dans des différents systèmes d'exploitation. Ces quelques premières leçons constituent les notions fondamentales des réseaux et du fonctionnement de l'Internet. Chaque leçon est élaborée en se basant sur les notions acquises précédemment donc ne soyez pas pressés, mais le fait de survoler les paragraphes et les pages est un bon moyen pour vous familiariser avec ce document avant de revenir et faire une lecture approfondie. Évidemment vous ne voudrez pas laisser s'échapper un brin important de connaissance.

Identification d'un Serveur

"OK, Aidan, qu'avez-vous trouvé?" J'essayais de ne pas grincer mes dents sous l'effet de la peur qu'il ne soit retourné pour cliquer sur ce lien stupide dans ce courriel envoyé par sa boîte électronique piratée.

"Je n'ai pas fait un clic gauche dessus", m'a dit Aidan, tout en souriant comme s'il a lu ma pensée. "Je l'ai copié et collé dans un fichier texte."

"Du texte que vous pourriez voir ? Ou le lien dont on parle ?

Il a froncé ses sourcils. "Je ne suis pas stupide. J'ai fait un clic-droit et choisi "Copier l'adresse du lien". Ensuite je l'ai collée ici. Regardez le fichier, lien.txt."

"Excuse-moi. Je voudrais juste me rassurer. Alors c'est bien. Où nous mène ce lien?"

"Vers ce domaine étrange. Chewmoogoo.com ou quelque chose d'autre. Il y a un tas d'autre choses après cela aussi", disait-il, en ouvrant son ordinateur portable pour me montrer le lien.

"Eh oui", lui ai-je dit. "Maintenant nous les avons eu. A présent essayons de voir quelles sont les informations que nous pouvons obtenir et quels sont les outils qui peuvent nous aider à les obtenir. Premièrement, parlons des noms de domaines et des adresses IP."

Identification du Propriétaire d'un Domaine

La première étape dans l'identification d'un système distant est de jetez un coup d'œil sur le nom d'hôte, le nom de domaine ou l'adresse IP. Une recherche **whois** d'un nom de domaine affiche un tas d'informations :

- L'identité du propriétaire du domaine, habituellement c'est un nom complet
- Les contacts, qui peuvent contenir les adresses de rues, des numéros de téléphone et des adresses électroniques.
- Les serveurs DNS sur lesquels le domaine est enregistré, ce qui peut vous révéler le FAI qui héberge le domaine.
- L'adresse IP du serveur, un autre indice potentiel du FAI.
- Les informations concernant le nom de domaine, telles la date à laquelle : il fut créé, il a été mis à jour et il arrivera à expiration.

Retenez qu'il existe plusieurs enregistreurs différents de nom de domaine, et toutes les bases de données whois ne contiennent pas les informations concernant tous les domaines. Il se peut que vous consultiez plus d'une base de données **whois** pour trouver les informations concernant le domaine sur lequel vous enquêtez.Retenez qu'il existe plusieurs enregistreurs différents de nom de domaine, et toutes les bases de données whois ne contiennent pas les informations concernant tous les domaines. Il se peut que vous consultiez plus d'une base de données **whois** pour trouver les informations concernant le domaine sur lequel vous enquêtez.

Aidan s'est instantanément imprégné de cette idée. "OK, que dois-je faire ?"

"Voici ton travail," lui ai-je dit.

Exercice

5.1 Obtenez le nom de domaine sur lequel vous enquêtez. (Si vous n'êtes pas Aidan, utilisez isecom.org). Essayez la commande suivante sous Linux, Windows et OSX.

```
whois isecom.org
```

À qui appartient le domaine ?
Quand a-t-il été créé ? Quand arrivera-t-il à expiration ? (Est-ce que cette expiration offre une opportunité?)
À quand date la dernière mise à jour ?
Quels sont les différents contacts qui y sont listés ?
Quels sont les noms respectifs des serveur de nom primaire et secondaire ?

5.2 Maintenant faite la même recherche à partir d'un navigateur (par exemple, accédez à l'adresse http://www.whois.net et faites la recherche sur "exemple.com"). Voici la question importante : est-ce que le résultat obtenu est le même que celui obtenu à l'aide de la commande whois ?
Essayez au moins deux sites web whois. Essayez http://whois.domaintools.com; pouvez-vous en trouver plus?).

Identification de l'Adresse IP d'un Domaine

"Alors qu'avez-vous obtenu ?" ai-je demandé à Aidan.

"Toute ces choses. Je les ai collées ici." Il m'a montré le fichier texte.

"C'est bien. Garde chaque brin d'informations. Quelle est l'adresse IP du domaine ?"

"Ceci, n'est ce pas ?" Aidan montra une longue suite de chiffres.

"Oui. Vous pouvez obtenir l'adresse IP du domaine avec la commande whois, ou vous pouvez faire une recherche DNS (DNS lookup) avec la commande **ping** :

```
ping isecom.org
```

"La première chose que vous verrez est l'adresse IP du domaine."

> Si vous pouvez capturer un courriel venant de la cible, examinez les **en-têtes du courriel** (confère Leçon 9, Sécurité des Courriels) ; cela vous donnera l'adresse IP de l'hôte qui a émis le courriel. Vous pouvez utiliser les ressources telles que les moteurs de recherche (confère Leçon 20, Ingénierie Sociale) ou des outils comme **Maltego** ou **FOCA**. Recherchez les termes tels que le nom de l'organisation, le contact de celui qui a enregistré le domaine, les numéros de téléphones et les adresses. Chacune de ces informations vous mèneront vers plus d'informations.

"Une fois que vous avez obtenu une adresse IP – ou plus d'une adresse – vous devez savoir là où elle se trouve. Les adresses IP sont allouées en grands blocs aux fournisseurs de services à travers le monde. Retrouvez le groupe auquel est allouée une adresse IP (et qui

possède les droits d'accès à ce groupe, si vous pouvez). Cela pourra vous aider à trouver le serveur ou le fournir de service que le site web utilise et le vrai joyau pour vous – le pays dans lequel se trouve ce serveur", ai-je dit à Aidan. "Je parie que ce n'est pas ça. Donc voici ce que vous faites après."

Exercices

Maintenant vous allez consulter directement les enregistrements DNS. Un autre moyen de trouver des informations concernant un domaine ou serveur(s) est d'utiliser les informations DNS. Il y existe trois commandes qui permettent de débuter ces recherches.

5.3 Ouvrez la fenêtre d'invite de commandes. Essayons cette commande :

```
dig isecom.org
```

Est-ce que cette commande fonctionne sur votre système d'exploitation ? Essayez-la sous Windows, Linux et OSX.

5.4 Maintenant essayez cette commande :

```
host isecom.org
```

Est-ce que cette commande fonctionne sous votre système d'exploitation ? Essayez-la encore sous Windows, Linux et OSX.

5.5 Et pour finir essayez cette commande :

```
nslookup isecom.org
```

Est-ce que cette commande fonctionne sous votre système d'exploitation ? Une fois encore, essayez-la sous Windows, Linux et OSX.

Quel est le serveur DNS de votre cible ? L'organisation possède t-elle un serveur de messagerie électronique? Le serveur de messagerie possède t-il la même adresse IP que le serveur web ? Qu'est-ce que ceci vous suggère ? Que pouvez-vous apprendre d'autre ?

5.6 Une fois que vous obtenez l'adresse IP, vous pouvez accéder aux informations enregistrées de plusieurs membres de **Number Resource Organization** (http://www.arin.net/, http://www.ripe.net/, ou http://www.apnic.net/), pour avoir une vue approfondie sur la façon dont les adresses IP sont réparties.

Début du Jeu: Sabrer et Brûler

C'était un match livré à contrecœur du moment où Jace était concernée. La bataille du siècle, comme elle a l'habitude d'en parler. Peu importe le plaisir, le sang, la peine, la force physique et intellectuelle requis, les adolescents ambitieux s'étaient préparés pour gagner ce combat. Elle avait l'obligation de vaincre puisqu'il n'y avait pas de plan B. Ses cheveux en couleur de cacao oscillaient devant ses yeux comme un

torero brandissant une nappe rouge. Une dernière respiration profonde et apaisante, et le tueur de réseau était prêt à apparaître.

Avec ses doigts agiles flottant au-dessus du clavier qui ricanait, elle a analysé la situation et a pris le stock de ses ressources disponibles. Jace avait une copie de Nmap qui était déjà en cours d'exécution sur la bête ordinateur. Les commandes ping et traceroute avaient déjà été exécutées donc le combattant hacker était prêt à se frayer un chemin.

Vers le bas était partie la première succession rapide de saisies au clavier. Une machine à tirer ne pourrait être aussi rapide que Jace lorsqu'il s'agissait de saisir des commandes d'ordinateur. Ping, vers le bas ! Traceroute, vers le bas ! Les commandes IP n'avaient aucune chance contre son barrage massif de frappes au clavier. Time to live, vers le bas ! Le carnage était horrible, au moment où les bits et les octets défilaient rapidement sur le moniteur en s'estompant. La ligne de commande semble diriger les bombardements entrant des puissants commutateurs, avec des attributs d'attaques qui sont proches du réseau principal.

Jace a manœuvré son premier assaut pour avoir un pied d'appui dans le réseau. Ses éclaireurs ont effectué une reconnaissance intense des pare-feu déployés en périmètre, des serveurs et les routeurs. Ces données étaient comparées aux vulnérabilités les plus connues du moment ou CVE(Common Vulnerabilities Exposures) et parsemées des informations issues de l'Analyse de Réseau fait par Nmap. Chaque faiblesse, chaque vulnérabilité, et chaque exploit étaient examinés pour un avantage tactique et les évaluations des dommages. La trêve n'était pas une option pour Jace. Elle était entrain de vaincre.

Ce n'était pas encore la fin, se disait-elle. En effet, tout ce qu'elle a fait n'était que capturer une petite partie des ressources ennemies mais le renseignement était pourtant inestimable. Jace a souffert de petites causalités de son côté. Les doigts et les articulations étaient légèrement douloureux. Elle avait un petit bleu près de son front à un endroit qu'elle a cogné contre le moniteur lorsqu'elle était frustrée. Les TTL étaient entrain de l'agacer.

A la fin, les bannières de guerre avaient affiché les détails sans le besoin d'une interrogation ou d'une torture répétée en utilisant la technique "bread-boarding". L'appareil Raspberry Pi était mis en réserve. Jace avait assez d'informations concernant l'ennemi pour effectuer la phase deux de l'attaque réseau. La phase suivante requiert les courriels chargés et le concours involontaire d'un interne.

C'était toujours la partie la plus effrayante de toute bataille, l'obtention des traîtres. Jace avait besoin d'utilisateurs en interne qui seraient compatissants à sa cause. Maintenant l'heure avait sonné pour que toutes les bonnes habitudes de sécurité soient contournées. L'ingénierie sociale est l'arme de perturbation de masse qui se trouvait dans son arsenal. Elle devrait manipuler des courriels légitimes en y incorporant des soldats de Troie pour infiltrer les murs internes des réseaux.

Pendant que Jace élaborait chaque courriel malveillant, elle savait qu'elle était du bon côté de cette confrontation. Peu importe ce que cela coûte, peu importe la durée, Jace était déterminée à savoir quel est le parfum secret de crème sur lequel la crémerie locale travaillerait prochainement.

Le Jeu Continue...

Identification des Services

"Alors vous avez sauvegardé toutes ces choses, n'est-ce pas ?" J'ai ri mais je m'efforçai de ne pas le faire, parce que je connaissais la réponse même si ma nature d'instructeur me poussait à le demander.

Aidan à tout juste laissé de côté un bout de papier : *stupide* pensait-il, mais il disait, "Jetez-y un coup d'œil" et il m'a remis son ordinateur portable.

"N'y a t-il pas beaucoup d'informations maintenant?" Je parcourait les pages vers le bas.

"Oui. J'ai besoin d'une meilleure façon de suivre les choses", disait Aidan, en reprenant l'ordinateur.

"Vous êtes sûr, n'est-ce pas ? Quelle est l'adresse IP de votre cible ?" Cette fois j'ai ri à gorge déployée.

"Bon ... il y en a cinq à peu prêt. Peut être qu'il y en a plus. J'essaie de comprendre pourquoi, parce que je peux faire un ping vers certaines adresses et vers les autres je ne peux pas."

"*C'est bon*", avais-je pensé. Une fois que vous avez obtenu les adresses IP d'un domaine vous pouvez commencer à approfondir la recherche des services, et cela veut dire les hôtes fonctionnels. *Oh ! Amusant !*

Ping et Traceroute

"Vous commencez au bon endroit. Vous devez vous assurer qu'il y a effectivement des machines actives. Et vous avez raison ; ping est votre ami. Vous vous êtes souvenu de faire un ping vers le nom de domaine, vers les adresses IP et vers les noms d'hôtes, n'est-ce pas ?"

"Lesquels sont des noms d'hôtes ?" demanda Aiden.

"Ce sont ceux possédant des lettres et un point avant le nom de domaine, comme www.isecom.com," lui avais-je dit.

"Je n'en vois aucun."

"Regardez dans vos résultats de recherche. Vous n'avez pas essayé les autres. Avez-vous essayez www.isecom.org et ftp.isecom.org et mail.isecom.org ?"

"Non ..."

"Bien, si vous obtenez une réponse, il y a quelque chose d'actif à cette adresse. Et vous passez à travers le pare-feu. Et ils autorisent l'entrée des requêtes ICMP". J'avais ouvert une fenêtre de ligne de commandes et saisi une commande :

```
C:\>ping isecom.org

Pinging isecom.org [216.92.116.13] with 32 bytes of data:
Reply from 216.92.116.13: bytes=32 time=186ms TTL=56
Reply from 216.92.116.13: bytes=32 time=186ms TTL=56
Reply from 216.92.116.13: bytes=32 time=186ms TTL=56
Reply from 216.92.116.13: bytes=32 time=186ms TTL=56
```

```
Ping statistics for 216.92.116.13:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 186ms, Maximum = 186ms, Average = 186ms
```

"Vous pouvez avoir une idée sur la distance qui vous sépare d'un serveur, à la fois sur le réseau et physiquement, en analysant le temps de réponse. Divisez ce temps par deux, et vous pouvez percevoir la distance qui vous sépare du serveur. Je veux que vous essayiez un autre outil, traceroute. Il est nommé **tracert** sous Windows et **traceroute** sous Linux. Il vous montrera les nœuds par lesquels passent les paquets lorsqu'ils quittent votre ordinateur pour atteindre votre cible. Comme ceci," ai-je dit, et j'ai saisi de nouveau.

```
C:\>tracert isecom.org
```

"Maintenant, voici ce que je veux faire."

Exercices

5.7 Utilisez traceroute/tracert pour rassembler toutes les informations que vous pouvez trouver concernant les ordinateurs et routeurs qui se trouvent entre votre ordinateur et votre cible.

5.8 Les ordinateurs possédant des adresses IP semblables font souvent parti d'un même réseau. Faites un ping vers un site web ou une adresse IP valide (par exemple, ping www.isecom ou ping 216.92.116.13). Si vous obtenez une réponse positive, faite un ping vers l'adresse IP suivante. Aviez-vous obtenu une réponse ? Essayez le test vers des adresses proches.

5.9 Servez-vous d'un moteur de recherche pour trouver la méthode qui permet d'estimer la distance qui vous sépare d'un serveur.

5.10 Recherchez un outil qui vous permet de mapper le serveur vers un emplacement physique.

5.11 Recherchez un outil de Trace Route Visuel en ligne. Il quelques sites qui fournissent de tels outils. Ceci devra vous permettre de bien voir là où va votre trafic.

Nmap

"Avez-vous bien saisi tout cela ? Permettez-moi de vous présenter à mon petit ami," disais-je, en essayant d'émettre une voix terrifiante. Aidan me regardait comme si j'avais deux têtes, donc j'ai raclé ma gorge, et, j'ai terminé, en disant "nmap".

"Il peut être simple, ou vous pouvez avoir des difficultés. Exécutez la commande nmap suivi d'un nom d'hôte ou d'une adresse IP, et il effectuera un une analyse par balayage (scan) de cet hôte. Ou bien utilisez un tas d'options pour accomplir des choses délicates. Si vous le lui demandez bien-sûr, il vous dira quel est le système d'exploitation de votre cible. Nous allons utiliser l'option 'scan TCP", qui est -sT".

```
nmap -sT 216.92.116.13
```

```
Starting Nmap 5.51 ( http://nmap.org ) at 2012-05-28 10:58 GTB Daylight
Time
Nmap scan report for 216.92.116.13
Host is up (1.1s latency).
Not shown: 969 closed ports
PORT    STATE SERVICE
25/tcp  open smtp
80/tcp  open http
110/tcp  open pop3
119/tcp  open nntp
135/tcp  open msrpc
139/tcp  open netbios-ssn
143/tcp  open imap
445/tcp  open microsoft-ds
465/tcp  open smtps
554/tcp  open rtsp

Nmap done: 1 IP address (1 host up) scanned in 215.42 seconds
```

Il est important de savoir que nmap n'est pas le seul outil permettant de faire ces analyses par balayage, et c'est une bonne chose. Les différents outils peuvent vous donner des résultats différents, et en effet n'importe quel outil peut délibérément porter à confusion.

Vous pouvez dire à nmap, par exemple, de détectez le système d'exploitation – mais vous ne devriez pas faire confiance à cette détection ! Vérifiez sa théorie en utilisant d'autres outils.

Extraction des Bannières

Aidan était joyeux. "Regardez ce que j'ai obtenu maintenant !" Il avait des documents texte et des fichiers de tableur sur son ordinateur, des schémas dans un carnet de notes et des imprimés en couleur qui devaient coûter à quelqu'un une fortune pour l'achat des cartouches d'encre.

"OK, maintenant vous savez que vous avez obtenu des machines actives, vous savez ceux qui les détiennent et en gros là où elles se trouvent. Ensuite vous voudrez savoir quel genre de machine s'agit-il : quel est le système d'exploitation qui y fonctionne ? Quels sont les services qu'il offre ?" lui ai-je demandé.

Cela la rendu moins joyeux. "Um, comment puis-je en parler ?"

"Vous n'en avez pas besoin. Demandez à la machine de cracher ses boyaux : le nom du système d'exploitation, les services et les versions de patch. Lorsque c'est vous qui attaquez, cela rend votre travail vraiment facile ; tout ce que vous avez à faire c'est de

rechercher des exploits pour ce service, ce logiciel et cette version. Si vous êtes le défenseur, vous voudrez supprimer cette information. Ou mieux encore, mentir." Ceci l'amena à être attentif.

"Donc ce vous faites ensuite est appelé **extraction de bannière.** Mot imaginaire : c'est une **technique d'énumération** permettant d'obtenir toutes sortes d'informations concernant les services et les ports actifs sur la cible. Je vais vous montrer quelques commandes de plus. Vous pouvez utiliser telnet, ftp ou netcat pour extraire la bannière. La bannière est ce vieux message qui s'afficherait à la ligne de commande lorsque vous vous connectez, et qui vous informe sur les programmes serveurs qui y tournent. Donc vérifiez cela : lorsque je me connecte à un serveur FTP anonyme, j'obtiens une bannière". J'ai saisi dans ma fenêtre d'Invite de commandes :

```
ftp isecom.org


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

"Ce nombre 220 est un code qui indique que le serveur est prêt à accepter un nouvel utilisateur. Et ceci n'est-il pas merveilleux : le programme FTP qui tourne sur cet hôte est ProFTPD Server. Maintenant nous allons rechercher sur le web, les systèmes d'exploitation sous lesquels tourne ProFTPD, et ce qu'il peut faire ... que faut-il tripoter, s'il y en a." Je tapotais sur le clavier. "Voici : votre prochaine tâche est l'utilisation de la commande ftp".

Exercice

5.12 Vous pouvez utiliser FTP suivi soit d'un nom d'hôte ou d'une adresse IP, comme ceci :

```
ftp isecom.org
```

ou

```
ftp 216.92.116.13
```

Essayez les deux pour voir quelle bannière renvoie le serveur FTP. Il se peut que votre résultat ressemble à ceci :

```
Connected to isecom.org.
220 ftp316.pair.com NcFTPd Server (licensed copy) ready.
User (isecom.org:(none)):
```

5.13 Vous pouvez utiliser telnet suivi soit d'un nom d'hôte ou d'une adresse IP, aussi. Que ce soit l'un ou l'autre vous pouvez spécifier le port, qui est 21 lorsque vous vous connectez à FTP :

```
telnet isecom.org 21
```

ou

```
telnet 216.92.116.13 21
```

Une fois encore, observez la bannière que le serveur a renvoyé – s'il y en a. Il se peut que vous obteniez quelque chose comme :

```
220 ftp316.pair.com NcFTPd Server (licensed copy) ready.
```

5.14 Utilisez netcat suivi d'un nom d'hôte ou d'une adresse IP, aussi. Comme dans le cas de telnet, vous pouvez spécifier le port, qui est 21 pour FTP :

```
nc isecom.org 21
```

ou

```
nc 216.92.116.13 21
```

Une fois encore, observez la bannière renvoyée par le serveur – s'il y en a.

Les Bannières Trompeuses

"Voici l'astuce", avais-je dit à Aidan. "Vous pouvez modifier la bannière. C'est une sorte de **camouflage** (ou **spoofing** en Anglais) – c'est un mensonge à propos de votre vraie nature. Donc je peux modifier ma bannière pour qu'elle affiche *NoneOfYourBusiness Server*, ce qui est beau, mais un système UNIX muni d'une bannière qui affiche *WS_FTP Server* va chasser les gens, parce que c'est un serveur FTP sous Windows."

"Attendez une minute – comment changez-vous la bannière ?" Avait-il demandé.

"Je suis content que tu aies demandé", ai-je répondu.

Exercice

5.15 Allez sur le web et recherchez comment on change les bannières pour SMTP, FTP, SSH, HTTP et HTTPS. Est-ce difficile à faire ? En d'autres mots, devriez-vous juste croire en l'affichage des bannières ?

Extraction Automatique de Bannière

"Maintenant regardez ceci. Nous pouvons retourner à nmap et automatiser ceci ; nous devons utiliser les options -sTV pour extraire les bannières". J'ai saisi la première ligne et j'avais obtenu ce rapport :

```
nmap -sTV -Pn -n --top-ports 10 --reason -oA hhs_5_06 hackerhighschool.org

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 05:10 CEST
```

```
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.30s latency).
PORT    STATE  SERVICE     REASON     VERSION
21/tcp  open   ftp         syn-ack    NcFTPd
22/tcp  open   ssh         syn-ack    OpenSSH 5.9 (protocol 2.0)
23/tcp  closed telnet      conn-refused
25/tcp  filtered smtp      no-response
80/tcp  open   http        syn-ack    Apache httpd 2.2.22
110/tcp open   pop3        syn-ack    Dovecot pop3d
139/tcp closed  netbios-ssn  conn-refused
443/tcp open   ssl/http    syn-ack    Apache httpd 2.2.22
445/tcp closed  microsoft-ds conn-refused
3389/tcp closed  ms-wbt-server conn-refused
Service Info: OS: Unix


Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.32 seconds
```

"Nmap a trouvé NcFTPd, OpenSSH5.9 (protocol 2.0) et Apache httpd 2.2.22. Bingo : le système d'exploitation est Unix. Quelques fois les bannières vous donnent la version du système d'exploitation, mais nous aurons besoin d'une petite information pour avoir une précision sur ce fait," ai-je continué. "Voici ce que je veux que vous fassiez".

Exercices

5.16 Utilisez nmap pour analyser votre cible (hackerhighschool.org, si vous n'êtes pas Aidan).

5.17 Essayez de nouveau avec l'option **--version-intensity number** en utilisant les nombres de 0 à 9 pour avoir des résultats précis. Quelle différence pouvez-vous constater dans ces rapports ?

Identification des Services à partir des Ports et des Protocoles

"Nmap avait effectué la dernière analyse par balayage en recherchant les services par défaut. Mais vous pourrez le faire dans l'autre sens aussi : rechercher premièrement les ports ouverts, ensuite dire réellement quels sont les services qui tournent derrières eux," avais-je dis.

"Attendez une minute," demanda Aidan. "Les ports ne sont-ils pas toujours les même ?"

"Oui, en théorie ils le sont. Mais en réalité, les numéros de ports sont une sorte d'agrément. Je peux faire tourner mes services sur des ports différents si je veux."

"OK, comment puis-je faire cela ?"

"Commence à regarder sur ton ordinateur local. Accède à la ligne de commandes et exécute **netstat** avec l'option **-a** qui scanne tous les ports. Comme ceci," avais-je démontré.

```
netstat -a
```

Le jeune hacker a suivi mon exemple, ensuite il a crié, "Waou ! Tous ces ports sont ouverts ?"

J'avais regardé sur son écran. "Votre ordinateur s'appelle Quasimodo ?"

```
Active Connections
Proto  Local Address                  Foreign Address        State
TCP    Quasimodo:microsoft-ds         Quasimodo:0            LISTENING
TCP    Quasimodo:1025                 Quasimodo:0            LISTENING
TCP    Quasimodo:1030                 Quasimodo:0            LISTENING
TCP    Quasimodo:5000                 Quasimodo:0            LISTENING
TCP    Quasimodo:netbios-ssn          Quasimodo:0            LISTENING
TCP    Quasimodo:1110                 216.239.57.147:http    TIME_WAIT
UDP    Quasimodo:microsoft-ds         *:*
UDP    Quasimodo:isakmp               *:*
UDP    Quasimodo:1027                 *:*
UDP    Quasimodo:1034                 *:*
UDP    Quasimodo:1036                 *:*
UDP    Quasimodo:ntp                  *:*
UDP    Quasimodo:netbios-ns           *:*
UDP    Quasimodo:netbios-dgm          *:*
```

"Oui, Quasimodo," a répondu Aidan avec un grand sourire. "Le bossu".

"OK ! Et alors, Victor. Voici ce que je voudrais que tu fasse".

Exercices

5.18 Exécutez la commande netstat sur votre ordinateur local, suivie de l'option -a.

```
netstat -a
```

Quels sont les ports ouverts ?

5.19 Exécutez la commande netstat sur votre ordinateur local, suivie de l'option -o.

```
netstat -o
```

Quels sont les services qui sont en écoute derrière les ports ouverts ?

5.20 Exécuter netstat sur votre ordinateur local, suivie de la combinaison d'options -aon

```
netstat -aon
```

Quel résultat vous donne cette combinaison d'options ?

5.21 En vous servant d'un moteur de recherche, établissez la correspondance entre ces ports et les services qui tournent derrières eux. Vous avez besoin de certains d'entre eux pour le fonctionnement des choses telles que le réseau. Mais en réalité avez vous réellement besoin de tous ces services en état de fonctionnement ?

5.22 Exécutez nmap, en utilisant les options -sS (faite une analyse par balayage furtive "stealth scan" ou SYN scan) et -O (pour découvrir le système exploitation) et en prenant l'adresse 127.0.0.1 comme cible. L'adresse IP 127.0.0.1 est appelé adresse de **boucle interne** (**loopback adress**)**.** Elle désigne toujours l'hôte local, c'est à dire votre ordinateur.

```
nmap -sS -O 127.0.0.1
```

Quels sont les ports ouverts qu'a découvert nmap ? Quels sont les services et les programmes qui sont entrain d'utiliser ces ports ? Maintenant essayez d'exécuter nmap pendant que vous avez un navigateur web ou un client telnet ouvert. Comment ceci affecte -t-il les résultats ?

L'analyse par balayage furtif – "stealth" scan" – utilise seulement la première partie de la poignée en trois étapes (Three-way handshake) de TCP – c'est –à-dire le paquet de synchronisation (SYN) – pour sonder un port sans établir totalement une connexion. Pendant que ceci vous permette de contourner les logs du système (qui ne gardera pas les traces de vos sondages à moins que vous n'établissiez réellement une connexion), il N'EST PAS indétectable. N'importe quel système de détection d'intrusions vos grandes, et glissantes empreintes à travers tout le réseau, donc ne vous trompez pas en croyant que vous êtes réellement indétectable ou furtif.

5.23 Nmap possède d'autre options en ligne de commandes. À quoi servent ces options : -sV, -sU, -sP, -A, --top-ports et –reason ? Quelles sont les autres possibilités qui y existent ? Si vous êtes un attaquant et que vous désirez demeurer furtif au lieu de percuter violemment le serveur, quelles sont les options de vous *ne* devriez pas utiliser, ou que vous devriez utiliser ?

5.24 Accédez à www.foundstone.com, et recherchez, téléchargez puis installer **fport** sur votre machine Windows. Il est semblable à netstat, mais il donne des détails sur les programmes qui utilisent les ports ouverts et les protocoles. Exécutez ce programme. Comment peut-on le comparer à netstat ?

Énumération d'un Système

"Vous n'étiez pas partis en parlant dans tous les sens et en sonnant les cloches, n'est-ce pas ?" Ai-je demandé.

Aidan a répondu lentement, en pensant réellement à cela, "Non, je ne pense pas l'avoir fait. Mais est ce que cela a réellement un importance ? Je veux dire que leurs serveurs sont une voie d'entrée ..."

Je l'ai interrompu. "Je ne sais pas là où ils se trouvent, je m'en-fou, vous allez travailler avec une éthique – et avec prudence – aussi longtemps que vous travaillerez avec moi."

"Ok," a-t-il répondu d'un air penaud.

"Le fait de ne pas laisser de traces est une bonne politique. Ce qui est presque impossible. Mais vous devriez toujours essayer. Parce que les traces représentent le sujet sur lequel vous allez travailler prochainement. Ou réellement parlant, les empreintes ..."

"Hey ! Ceux-là ne sont pas les mêmes !"

"Ok, m'as-tu compris. Mais sans nous préoccuper de quoi que ce soit, nous allons tout rassembler pour obtenir l'**empreinte** de votre cible, trouver le Système d'Exploitation et tous ses services."

Analyse des Ordinateurs Distants

"Qu'aviez-vous obtenu finalement après votre analyse furtive (stealth scan) ?" ai-je demandé. Aidan m'a montré un rapport qu'il avait collé dans un document texte.

```
nmap -sS -O 216.92.116.13

Starting Nmap 5.51 ( http://nmap.org ) at 2012-05-28 16:54 GTB Daylight
Time
Nmap scan report for isecom.org (216.92.116.13)
Host is up (0.19s latency).
Not shown: 965 closed ports

PORT    STATE  SERVICE
21/tcp  open   ftp
22/tcp  open   ssh
25/tcp  filtered smtp
26/tcp  open   rsftp
80/tcp  open   http
110/tcp  open   pop3
```

```
111/tcp  filtered rpcbind
113/tcp  filtered auth
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open   imap
161/tcp  filtered snmp
179/tcp  filtered bgp
306/tcp  open   unknown
443/tcp  open   https
445/tcp  filtered microsoft-ds
465/tcp  open   smtps
514/tcp  filtered shell
543/tcp  open   klogin
544/tcp  open   kshell
587/tcp  open   submission
646/tcp  filtered ldp
800/tcp  filtered mdbs_daemon
993/tcp  open   imaps
995/tcp  open   pop3s
1720/tcp filtered H.323/Q.931
2105/tcp open   eklogin
6667/tcp filtered irc
7000/tcp filtered afs3-fileserver
7001/tcp filtered afs3-callback
7007/tcp filtered afs3-bos
7777/tcp filtered cbt
9000/tcp filtered cslistener
12345/tcp filtered netbus
31337/tcp filtered Elite
Device type: general purpose|storage-misc
Running (JUST GUESSING): FreeBSD 7.X|6.X (88%)
Aggressive OS guesses: FreeBSD 7.0-BETA4 - 7.0 (88%), FreeBSD 7.0-RC1
(88%), FreeBSD 7.0-RELEASE - 8.0-STABLE (88%), FreeBSD 7.0-STABLE (88%),
FreeBSD
 7.1-RELEASE (88%), FreeBSD 6.3-RELEASE (86%), FreeNAS 0.7 (FreeBSD 7.2-
RELEASE) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops
```

```
OS detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 24.09 seconds
```

"Regardez-vous tous ces ports qui sont marqués par le mot "**filtred"(** c'est-à-dire filtré) ? Cela veut dire qu'il sont protégés par un pare-feu. Ils sont bien connus et vulnérables, donc il devraient être toujours bloqués. Mais regardez : les ports 21, 22, et 80 – qui sont respectivement FTP, Secure Shell et HTTP – sont tous ouverts." J'avais regardé Aidan de haut en bas.

"Ah bon ?" avait-il demandé d'une façon encourageante.

"Bien, une proie équitable, du moins. Ok. La dernière chose que fait nmap est d'essayer de découvrir le système d'exploitation de votre cible. La plupart du temps, comme à présent, il ne fait qu'un "analyse agressive", mais cela est habituellement très bien. Puisque l'analyse montre les ports FTP et SSH ouverts, les bannières que vous avez extraites seront la prochaine pièce à conviction.

"En consultant le web, il nous dit que NcFTPd est un programme d'Unix et que FreeBSD est un système d'exploitation dérivé d'Unix. Vous devriez trouver SSH sur tous les systèmes d'exploitation dérivés d'Unix. Donc il est probable que serveur tourne sous une version de FreeBSD. Vous savez que ces bannières peuvent être usurpées, mais c'est une supposition raisonnable.

"Maintenant, en fonction de l'emplacement de votre cible, votre prochaine étape serait de découvrir le FAI. Le FAI doit lui-même être célèbre pour héberger les sites de courriers indésirables (spammers) ou des sites malveillants – faites une recherche – mai vous pourriez être capable de gémir à leur porte et d'amener le mauvais attaquant à démissionner. Dans votre cas je pense que vous voudriez en découdre avec un FAI ...

"Parce que c'est à l'intérieur ..." Aidan a enfoncé la porte, mais j'avais maintenu haut mon doigt.

"Arrête. Tes informations sont tes informations. Je n'en ai pas besoin, aussi longtemps que vous saurez être éthique et rassurant. Ce que vous êtes."

Aidan a répondu d'un geste de la tête.

"Donc que vais-je faire ?" Ai-je demandé.

"Bien, ils ont un serveur web qui fonctionne, n'est ce pas ?" Aidan commença, et tout ce que je pouvais faire c'est sourire.

Étoffez Vos Connaissances: Allons Plus Loin avec Nmap

Ceci étant dit, vous avez identifié le nom d'hôte, son propriétaire, le réseau auquel il appartient et vérifié les hôtes qui sont actifs. Maintenant afin d'identifier un système vous avez besoin de trouver quelques ports ouverts. N'oubliez pas que l'hôte peut être actif mais en ayant tous les ports fermés (ou même filtrés).

Vous pouvez utiliser le célèbre outil Network Mapper (ou **nmap**) développé par Fyodor pour effectuer cette tâche. Nmap est un analyseur de port et est capable de sonder à distance les ordinateurs pour trouver des ports ouverts et des services qui leur sont liés. Lorsque vous exécutez nmap, en fonction des options en ligne de commande que vous avez utilisées, vous obtiendrez une liste de ports ouverts et des services ou des protocoles qui utilisent ces ports. Nmap peut être aussi capable de déterminer quel est le système d'exploitation utilisé.

Nmap possède plusieurs options et types d'analyses (scan). Nous utiliserons quelques options de nmap mais vous pouvez toujours utiliser

```
nmap --help
```

ou

```
man nmap
```

pour avoir plus de détails.

Avant que nous commençons, avez-vous lu la leçon 3 ? Le temps est venu de l'appliquer ! Êtes-vous déjà de retour ? Non ? Alors allez-y maintenant !

Ok, expliquez la différence entre TCP et UDP et décrivez le processus *three-way handshake*. La compréhension de ce processus est nécessaire pour la compréhension du fonctionnement de nmap.

La syntaxe de Nmap est :

```
nmap scan-techniques host-discovery options target
```

- **scan-techniques** spécifie le type de paquets qui sera utilisé et comment les réponses provenant de la cible devraient être interprétées. Les principales techniques disponibles sont :
  - **-sS** SYN scan (concerne seulement la première partie du processus threeway-handshake)
  - **-sT** TCP Connect scan (concerne le processus threeway-handshake entier)
  - **-sA** ACK scan (envoie seulement les paquets ACK)
  - **-sU** UDP Scan
  - **-O** Détection de Système d'Exploitation
  - **-A** toutes les fonctionnalités telles que la détection du système d'exploitation, les plugins, le traceroute
- **host-discovery** spécifie les techniques utilisées pour définir l'état actif ou inactif d'un hôte. Si l'hôte est actif il sera analysé, sinon il ne sera pas analysé.
  - **-PE** vérifie si l'hôte répond à un ping
  - **-PS** vérifie si l'hôte répond à un SYN

- **-PA** vérifie si l'hôte répond à un ACK
- **-PU** vérifie si l'hôte répond à un paquet UDP
- **-PN** ne vérifie rien, traite tous les hôtes comme actifs (bien nous utiliserons ceci parce nous savons que notre cible est active, puisque nous avons vérifié cela précédemment).

- **options** spécifie les détails ultérieurs pour le type d'nalyse sélectionné, tel que :
  - **-p1-65535** les numéros de ports à scanner (dans cet exemple de 1 à 65535)
  - **--top-ports <number>** nmap sait quels sont les ports qui sont fréquemment utilisés, et peut analyser seulement le <nombre> de ports les plus connus et spécifiés.
  - **-T0, -T1, -T2, -T3, -T4** permettent de spécifier la vitesse de l'analyse, 0 veut dire le plus lentement possible et 4 veut dire rapidement (le plus lent signifie plus de furtivité avec moins de congestion réseau)
  - **-oA <filename>** permet de rediriger l'affichage de nmap vers un fichier qui se présentera sous les trois formats disponibles dans nmap (nous aurons toujours l'habitude de garder les traces de nos activités).
  - **--reason** nmap écrit à propos de ses résultats interprétés (recommandé)
  - **--packet-trace** semblable à –reason mais vous verrez les traces du trafic (vous utilisez ceci pour en savoir plus sur une technique d'analyse et pour la maintenance des analyses).
  - **-n** interdit à Nmap de faire la résolution de noms DNS (nous n'utiliserons pas DNS parce que nous l'avons analysé manuellement)

Analyse TCP (TCP Scan)

Notre première analyse commence avec l'exécution de la commande suivante :

```
nmap -sT -Pn -n --top-ports 10 -oA hhs_5_tcp hackerhighschool.org
```

Ce qui nous donne l'affichage suivant :

```
Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:10 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up (0.23s latency).
PORT    STATE  SERVICE
21/tcp  open   ftp
22/tcp  open   ssh
23/tcp  closed  telnet
25/tcp  filtered smtp
80/tcp  open   http
110/tcp open   pop3
139/tcp closed  netbios-ssn
443/tcp open   https
445/tcp closed  microsoft-ds
```

```
3389/tcp closed  ms-wbt-server


Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
```

Nous avons découvert quelques ports ouvert, certains sont fermés et d'autres sont filtrés. Qu'est ce que cela veut dire ? Cela dépend du type de scan (dans ce cas -sT). Et nous avons utiliser l'option –reason pour savoir pourquoi nmap a conclu un état particulier.

```
nmap -sT -Pn -n --top-ports 10 --reason -oA hhs_5_tcp_02
hackerhighschool.org


Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:17 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.22s latency).
PORT    STATE  SERVICE    REASON
21/tcp  open   ftp        syn-ack
22/tcp  open   ssh        syn-ack
23/tcp  closed telnet     conn-refused
25/tcp  filtered smtp     no-response
80/tcp  open   http       syn-ack
110/tcp open   pop3       syn-ack
139/tcp closed  netbios-ssn  conn-refused
443/tcp open   https      syn-ack
445/tcp closed  microsoft-ds conn-refused
3389/tcp closed  ms-wbt-server conn-refused


Nmap done: 1 IP address (1 host up) scanned in 2.26 seconds
```

Maintenant nous savons comment les "cartes" de nmap répondent aux états lorsqu'ils reçoivent un **TCP Scan** :

- **open**: la cible répond avec un paquet SYN ACK
- **closed**: la connexion TCP est refusée
- **filtered**: pas de réponse venant de la cible

Lorsque vous découvrez des ports ouverts et filtrés, utilisez d'autres techniques d'analyse pour savoir exactement pourquoi cela.

Analyse SYN (SYN Scan)

Une autre technique célèbre de d'analyse est SYN scan. Lorsque ce type d'analyse est en cours, nmap envoie seulement un paquet SYN sans terminer le processus threeway-handshake. Cette technique est aussi appelée analyse "semi-ouverte" (half-open) ou

"furtive" (stealth) parce que les connexions TCP n'y sont pas complètes. (Sachez très bien que même si une cible ne peut pas garder les traces d'une connexion, vous faites quand même toujours du "bruit" qui peut être détecté). Utilisez ce type d'analyse (-sS scan) comme suit :

```
nmap -sS -Pn -n --top-ports 10 --reason -oA hhs_5_syn
hackerhighschool.org


Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-24 12:58 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.15s latency).
PORT    STATE  SERVICE    REASON
21/tcp  open   ftp        syn-ack
22/tcp  open   ssh        syn-ack
23/tcp  closed telnet     reset
25/tcp  filtered smtp     no-response
80/tcp  open   http       syn-ack
110/tcp open   pop3       syn-ack
139/tcp filtered netbios-ssn  no-response
443/tcp open   https      syn-ack
445/tcp filtered microsoft-ds no-response
3389/tcp closed  ms-wbt-server reset


Nmap done: 1 IP address (1 host up) scanned in 1.81 seconds
```

Les résultats sont semblables à ceux de TCP Scan mais remarquez les différences entre une analyse entière TCP (full TCP scan) et une analyse semi-overte (half-open TCP ou SYN scan), en comparant les résultats (des options –reason et –packet-trace) en utilisant la même cible avec les options -sT, -sS et -sA (ACK scan).

Analyse UDP (UDP scan)

Une autre technique d'analyse est UDP scan (-sU) : la connaissance du motif est fondamentale à l'obtention de bons résultats.

```
nmap -sU -Pn -n --top-ports 10 --reason -oA hhs_5_udp
hackerhighschool.org


Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:28 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.23s latency).
PORT    STATE      SERVICE    REASON
53/udp  closed     domain     port-unreach
```

```
67/udp  open|filtered dhcps    no-response
123/udp closed    ntp     port-unreach
135/udp closed    msrpc    port-unreach
137/udp closed    netbios-ns  port-unreach
138/udp closed    netbios-dgm port-unreach
161/udp closed    snmp     port-unreach
445/udp closed    microsoft-ds port-unreach
631/udp closed    ipp     port-unreach
1434/udp closed    ms-sql-m   port-unreach

Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
```

Cela peut porter un tout petit peu à confusion. Que s'est-il passé ? Nous voyons certaines des raisons : port inaccessible (closed) et pas de réponse (open |filtred). Pourquoi ? Nous avons besoin de plus de détails. Nous pouvons utiliser l'option de traçage de paquet (--packet-trace) et limiter l'analyse à deux ports, par exemple les ports UDP 53 et 67 :

```
nmap -sU -Pn -n -p53,67 --reason --packet-trace -oA hhs_5_udp_02
hackerhighschool.org

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:32 CEST
SENT (0.0508s) UDP 192.168.100.53:54940 > 216.92.116.13:67 ttl=46
id=54177 iplen=28
SENT (0.0509s) UDP 192.168.100.53:54940 > 216.92.116.13:53 ttl=37
id=17751 iplen=40
RCVD (0.3583s) ICMP 216.92.116.13 > 192.168.100.53 Port unreachable
(type=3/code=3) ttl=54 id=1724 iplen=56
SENT (2.5989s) UDP 192.168.100.53:54941 > 216.92.116.13:67 ttl=49
id=33695 iplen=28
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.31s latency).
PORT  STATE     SERVICE REASON
53/udp closed    domain port-unreach
67/udp open|filtered dhcps  no-response

Nmap done: 1 IP address (1 host up) scanned in 4.15 seconds
```

Nous avons découvert que 192.168.100.53 a envoyé des paquets UDP aux port 53 et 67 de hackerhighschool.org. Que s'est-il passé là ? Le port 67 ne répond pas et pour le 53 nous avons reçu un message de port injoignable (Port Unreachable – T03C03).

Port injoignable signifie que le port est fermé, et pour "pas de réponse" – même si c'est

une réponse normale pour UDP – nous ne savons pas si le service est actif ou non parce que le protocole UDP ne peut répondre que s'il a reçu les paquets adéquats. Pouvons-nous faire un peu plus de recherche ? Oui, en utilisant l'option d'analyse de service -sV (Service Scan) grâce à laquelle nmap essaie d'envoyer des paquets bien connus aux services UDP.

Analyse de Service (UDP)

```
nmap -sUV -Pn -n -p53,67 --reason --packet-trace -oA hhs_5_udp_03
hackerhighschool.org


Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:44 CEST
SENT (0.1730s) UDP 192.168.100.53:62664 > 216.92.116.13:53 ttl=48
id=23048 iplen=40
SENT (0.1731s) UDP 192.168.100.53:62664 > 216.92.116.13:67 ttl=48
id=53183 iplen=28
RCVD (0.4227s) ICMP 216.92.116.13 > 192.168.100.53 Port unreachable
(type=3/code=3) ttl=54 id=20172 iplen=56
SENT (2.4252s) UDP 192.168.100.53:62665 > 216.92.116.13:67 ttl=50
id=39909 iplen=28
NSOCK (3.8460s) UDP connection requested to 216.92.116.13:67 (IOD #1)
EID 8
NSOCK (3.8460s) Callback: CONNECT SUCCESS for EID 8 [216.92.116.13:67]
Service scan sending probe RPCCheck to 216.92.116.13:67 (udp)
...and 80 more packets...
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.25s latency).
PORT  STATE     SERVICE REASON    VERSION
53/udp closed    domain port-unreach
67/udp open|filtered dhcps  no-response
```

Nous n'avons pas la chance cette fois, puisque nous avons obtenu les même résultats. Un bon hacker peut aussi essayer d'envoyer des paquets UDP spécifiques manuellement, ou à l'aide du client adéquat tournant sur le port standard 67. Nous avons déjà utilisé l'analyse de service, la prochaine étape de l'identification de service. Étudiez les services bien connus sur votre machine locale et faites quelques exercices, ensuite continuez avec l'extraction de bannière.

Exercices

5.25 Accédez à http://nmap.org, téléchargez et installer la version la plus récente de nmap sur votre système d'exploitation

5.26 Répétez toutes les analyses de cette section en utilisant plus de ports. Ayez en tête que vous avez besoin de la commande ***sudo*** sur les sytèmes Linux, ou des droits d'administrateur local sous Windows.

5.27 Créez un tableau de référence pour toutes les techniques de scan qui correspondent à *state, reason* et la *vrai réponse* venant de la cible (packet-trace).

Détection du Système d'Exploitation

La connaissance des services est importante pour avoir l'empreinte de la machine cible. Nmap peut vous aidez encore via les options telles que -A pour toutes les analyses et -O pour la détection du système d'exploitation, en utilisant les ports par défaut :

```
sudo nmap -A -Pn -n --reason -oA hhs_5_all hackerhighschool.org


Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 05:38 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.21s latency).
Not shown: 971 closed ports
Reason: 971 resets
PORT    STATE  SERVICE     REASON   VERSION
21/tcp  open   ftp         syn-ack  NcFTPd
22/tcp  open   ssh         syn-ack  OpenSSH 5.9 (protocol 2.0)
| ssh-hostkey: 1024 cd:27:c2:bf:ad:35:e5:67:e0:1b:cf:ef:ac:2b:18:9a
(DSA)
|_1024 17:83:c5:8a:7a:ac:6c:90:48:04:0b:e5:9c:e5:4d:ab (RSA)
25/tcp  filtered smtp       no-response
26/tcp  open   tcpwrapped   syn-ack
80/tcp  open   http         syn-ack  Apache httpd 2.2.22
|_http-title: Hacker Highschool - Security Awareness for Teens
110/tcp  open   pop3        syn-ack  Dovecot pop3d
|_pop3-capabilities: USER CAPA UIDL TOP OK(K) RESP-CODES PIPELINING
STLS SASL(PLAIN LOGIN)
111/tcp  filtered rpcbind     no-response
113/tcp  open   tcpwrapped   syn-ack
143/tcp  open   imap        syn-ack  Dovecot imapd
|_imap-capabilities: LOGIN-REFERRALS QUOTA AUTH=PLAIN LIST-STATUS
CHILDREN CONTEXT=SEARCH THREAD=REFERENCES UIDPLUS SORT IDLE
MULTIAPPEND CONDSTORE ESEARCH Capability UNSELECT AUTH=LOGINA0001
IMAP4rev1 ID WITHIN QRESYNC LIST-EXTENDED SORT=DISPLAY THREAD=REFS
STARTTLS OK completed SEARCHRES ENABLE I18NLEVEL=1 LITERAL+ ESORT
SASL-IR NAMESPACE
161/tcp  filtered snmp      no-response
179/tcp  filtered bgp       no-response
306/tcp  open   tcpwrapped   syn-ack
443/tcp  open   ssl/http    syn-ack  Apache httpd 2.2.22
```

```
| ssl-cert: Subject: commonName=www.isecom.org/organizationName=ISECOM
-    The    Institute    for    Security    and    Open
Methodologies/stateOrProvinceName=New York/countryName=US

| Not valid before: 2010-12-11 00:00:00

|_Not valid after: 2013-12-10 23:59:59

|_http-title: Site doesn't have a title (text/html).

|_sslv2: server supports SSLv2 protocol, but no SSLv2 cyphers

465/tcp  open   ssl/smtp    syn-ack   Postfix smtpd

|_smtp-commands: kunatri.pair.com, PIPELINING, SIZE 41943040, ETRN,
AUTH PLAIN LOGIN, AUTH=PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME,
DSN,

| ssl-cert: Subject: commonName=*.pair.com/organizationName=pair
Networks, Inc./stateOrProvinceName=Pennsylvania/countryName=US

| Not valid before: 2012-01-10 00:00:00

|_Not valid after: 2015-01-09 23:59:59

543/tcp  open   tcpwrapped   syn-ack

544/tcp  open   tcpwrapped   syn-ack

587/tcp  open   smtp      syn-ack   Postfix smtpd

|_smtp-commands: kunatri.pair.com, PIPELINING, SIZE 41943040, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,

| ssl-cert: Subject: commonName=*.pair.com/organizationName=pair
Networks, Inc./stateOrProvinceName=Pennsylvania/countryName=US

| Not valid before: 2012-01-10 00:00:00

|_Not valid after: 2015-01-09 23:59:59

646/tcp  filtered ldp       no-response

800/tcp  filtered mdbs_daemon   no-response

993/tcp  open   ssl/imap    syn-ack   Dovecot imapd

| ssl-cert: Subject: commonName=*.pair.com/organizationName=pair
Networks, Inc./stateOrProvinceName=Pennsylvania/countryName=US

| Not valid before: 2012-01-10 00:00:00

|_Not valid after: 2015-01-09 23:59:59

|_sslv2: server supports SSLv2 protocol, but no SSLv2 cyphers

|_imap-capabilities: LOGIN-REFERRALS completed OK SORT=DISPLAY
Capability UNSELECT AUTH=PLAIN AUTH=LOGINA0001 IMAP4rev1 QUOTA
CONDSTORE LIST-STATUS ID SEARCHRES WITHIN CHILDREN LIST-EXTENDED ESORT
ESEARCH QRESYNC CONTEXT=SEARCH THREAD=REFS THREAD=REFERENCES
I18NLEVEL=1 UIDPLUS NAMESPACE ENABLE SORT LITERAL+ IDLE SASL-IR
MULTIAPPEND

995/tcp  open   ssl/pop3    syn-ack   Dovecot pop3d

|_sslv2: server supports SSLv2 protocol, but no SSLv2 cyphers

|_pop3-capabilities: OK(K) CAPA RESP-CODES UIDL PIPELINING USER TOP
SASL(PLAIN LOGIN)
```

```
| ssl-cert: Subject: commonName=*.pair.com/organizationName=pair
Networks, Inc./stateOrProvinceName=Pennsylvania/countryName=US
| Not valid before: 2012-01-10 00:00:00
|_Not valid after: 2015-01-09 23:59:59
2105/tcp open   tcpwrapped   syn-ack
6667/tcp filtered irc       no-response
7000/tcp filtered afs3-fileserver no-response
7001/tcp filtered afs3-callback  no-response
7007/tcp filtered afs3-bos    no-response
7777/tcp filtered cbt       no-response
9000/tcp filtered cslistener   no-response
31337/tcp filtered Elite      no-response
Device type: general purpose|firewall|specialized|router
Running (JUST GUESSING): FreeBSD 6.X|7.X|8.X (98%), m0n0wall FreeBSD
6.X (91%), OpenBSD 4.X (91%), VMware ESX Server 4.X (90%), AVtech
embedded (89%), Juniper JUNOS 9.X (89%)
OS CPE: cpe:/o:freebsd:freebsd:6.3 cpe:/o:freebsd:freebsd:7.0
cpe:/o:freebsd:freebsd:8.1 cpe:/o:m0n0wall:freebsd
cpe:/o:openbsd:openbsd:4.0 cpe:/o:vmware:esxi:4.1
cpe:/o:m0n0wall:freebsd:6 cpe:/o:juniper:junos:9
Aggressive OS guesses: FreeBSD 6.3-RELEASE (98%), FreeBSD 7.0-RELEASE
(95%), FreeBSD 8.1-RELEASE (94%), FreeBSD 7.1-PRERELEASE 7.2-STABLE
(94%), FreeBSD 7.0-RELEASE - 8.0-STABLE (92%), FreeBSD 7.1-RELEASE
(92%), FreeBSD 7.2-RELEASE - 8.0-RELEASE (91%), FreeBSD 7.0-RC1 (91%),
FreeBSD 7.0-STABLE (91%), m0n0wall 1.3b11 - 1.3b15 FreeBSD-based
firewall (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 12 hops
Service Info: Host: kunatri.pair.com; OS: Unix


TRACEROUTE (using port 1723/tcp)
HOP RTT    ADDRESS
[...]
8  94.98 ms 89.221.34.153
9  93.70 ms 89.221.34.110
10 211.60 ms 64.210.21.150
11 ...
12 209.28 ms 216.92.116.13


OS and Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 57.94 seconds
```

L'utilisation de **-A** rend possible le fait de voir plus de données. Des plugins (fonctions complémentaires) cherchent plus d'informations sur un serveur, effectuent la détection de système d'exploitation et utilisent une variante de traceroute qui utilise des méthodes qui sont différentes de celle utilisée par le traceroute ou tracert habituel. Pour la détection de système d'exploitation, l'utilisation de plusieurs ports est une meilleure approche.

Exercices

5.28 Analysez votre propre machine avec nmap. Est-ce que le système d'exploitation trouvé est correct ?

5.29 Utilisez l'option traceroute de nmap en utilisant des ports différents :

```
nmap -n -Pn --traceroute --version-trace -p80 hackerhighschool.org
```

5.30 Y-at-il quelques différences entre traceroute de nmap avec l'utilisation de ports différents et le tracert ou traceroute de votre système d'exploitation ?

5.31 Recherchez l'empreinte de la pile de protocole TCP/IP. Comment y êtes-vous arrivés ? Est-il protégé contre l'usurpation (spoofing) ?

Utilisation des Scripts

Nmap possède aussi une quantité de scripts utiles pour l'analyse. Vous pouvez utilisez l'option `–script script-name` pour charger les scripts. Un script qui est très intéressant est `ipidseq`, qui effectue la collecte d'empreintes IP par incrémentation. Ce script peut être utilisé pour découvrir les hôtes pour l'analyse des hôte inactifs (Idle Scan, -sI). Cette analyse utilise une implémentation problématique de IP sur des hôtes zombies pour analyser d'autres cibles.

```
nmap --script ipidseq -oA hhs_5_ipidseq hackerhighschool.org
```

```
Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 05:47 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up (0.23s latency).
rDNS record for 216.92.116.13: isecom.org
Not shown: 971 closed ports
```

Exercices

5.32 Recherchez les techniques d'analyse d'hôte inactifs (Idle Scan techniques). Qu'est-ce que c'est et comment pouvez-vous l'effectuer ?

Conclusion

Connaître là où il faut chercher et ce que vous recherchez est seulement une partie de la guerre de sécurité. Les réseaux sont constamment soumis à des expertises, analysés, soumis à des tests qui les poussent à bout. Si le réseau que vous protégez n'est pas surveillé alors vous n'êtes pas entrain d'utiliser les outils adéquats pour détecter ce comportement. Si le réseau que vous essayez d'infiltrer n'est pas surveillé, vous pouvez vous débarrasser de son analyse. En tant qu'expert en sécurité informatique, vous devriez connaître chaque recoin des systèmes que vous protégez – ou testez. Vous avez besoin de savoir là où se trouvent les faiblesses et là où se trouvent les forces aussi, sans tenir compte du côté où vous vous trouvez.

La simple collecte des renseignements concernant un serveur, tels que le système d'exploitation et les ports ouverts, s'avère insuffisant de nos jours. Une Menace Persistante Évoluée (Advanced Persistent Threat) essayera d'apprendre davantage votre réseau. Ces informations incluent :

- La marque du pare-feu, le modèle, la version du firmware, et les patchs logiciel qui existent.
- L'authentification des connexions distantes, les privilèges d'accès, et les processus.
- D'autres serveurs qui se connectent au réseau, y compris les Email, HTML, les sauvegardes, la redondance, les sites hors-ligne, les services externes loués, et même les contractants qui auraient pu utiliser votre réseau ou qui l'utilisent à présent.
- Les imprimantes, les fax, les photocopieuses, les routeurs sans-fil, et les connexions réseau qui existent dans la salle d'attente de votre entreprise
- Les appareils portables tels que les tablettes, les les smartphones, les dispositifs de photographie numérique, et toute chose qui pourrait se connecter au réseau.

Bien que nous ayons parlé de plusieurs thèmes dans cette leçon, l'identification des systèmes couvre une zone plus large. Il y a presque un pièce d'informations qui traverse les réseaux et qui permet d'identifier les différentes parties de chaque appareil. Tout appareil sur le réseau peut être exploité et ainsi constituer un point d'entrée pour l'attaquant. L'approche de ce défi domptant requiert plus d'un logiciel. Recherchez votre propre équipement et apprenez-en autant que vous pouvez. Cette connaissance vous sera bénéfique.

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