Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEÇON 3
LES PORTS ET PROTOCOLES

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

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

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

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

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

All works copyright ISECOM, 2004.

Conditions d'utilisation de ce support

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

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

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

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

Copyright ISECOM - Tous droits réservés.

Table des Matières

Personnes ayant contribués à ce projet

Gary Axten, ISECOM

La Salle URL Barcelona

Kim Truett, ISECOM

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Pete Herzog, ISECOM

Traduction

Guillaume Lavoix

Marc Trudel, ReadyResponse(www.readyresponse.org)

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

LA SALLE
Enginyeria
Arquitectura

Universitat Ramon Llull

3.1 Introduction

Les texte et exercices de cette leçon vous transmettront une compréhension basique des ports et protocoles en cours d'utilisation, ainsi que leur pertinence au niveau du système d'exploitation, que ce soit Windows ou Linux.

De plus, vous aurez l'opportunité de vous familiariser avec un certain nombre d'outils qui permettent de comprendre en profondeur les capacités réseaux de votre ordinateur.

En fin de leçon vous devriez avoir une connaissance basique et générale:

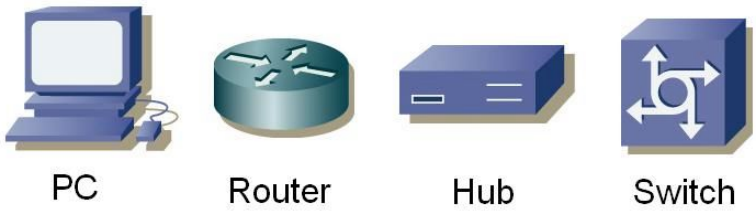
- Du concept des réseaux
- Des adresses IP
- des ports et des protocoles.

3.2 Concepts basique des réseaux

3.2.1 Equipements

Pour comprendre l'explication des protocoles et des ports, il est nécessaire de se familiariser avec les icônes qui représentent les équipements les plus communs que vous pouvez voir dans le schéma ci-dessous.

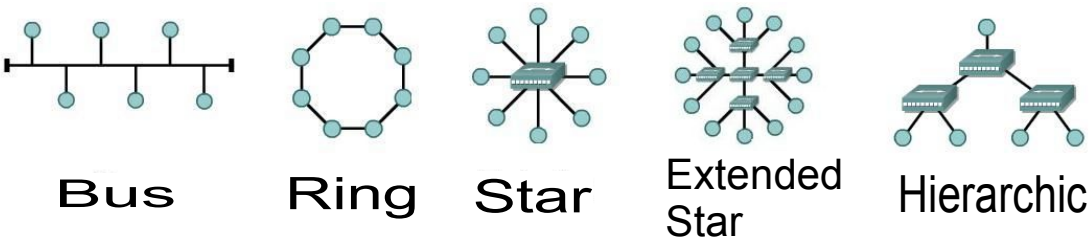
Les voici:



3.2.2 Topologies

En connectant ces équipements, des "local area networks" (or LANs) peuvent être créé. Dans un LAN, les ordinateurs peuvent partager leurs ressources, tel que leurs disques durs, leurs imprimantes, ou une connexion Internet, de plus un *administrateur* peut contrôler la manière de les gérer. Au moment du «design» d'un LAN, il est possible de choisir parmi l'une des topologies suivantes:

Bus Anneau Étoile Étoile Étendue Hiérarchique



Dans une topologie *en bus*, tous les ordinateurs sont connectés au même média de transmission et chaque ordinateur peut communiquer directement avec toutes les autres machines du réseau local. Au sein d'une topologie *en anneau*, chaque ordinateur est connecté au suivant, le dernier se connectant au premier, et chacun des ordinateurs ne peut communiquer directement qu'avec les ordinateurs qui lui sont adjacents. Au sein d'une topologie *en étoile*, aucun des ordinateurs ne sont directement inters reliés. Ils sont plutôt

connectés à un point central et ce point central est responsable du relais de l'information d'un ordinateur à un autre. Si plusieurs points centraux sont connectés entre eux, nous obtenons une topologie en *étoile étendue*. À l'intérieur d'une topologie en étoile ou en étoile étendue, tous les point centraux sont des pairs (en anglais, *peers)*, c'est-à-dire qu'ils échangent de l'information d'égale à égale. Cependant, si vous connectez deux réseaux en étoiles ou en étoiles étendue ensemble en utilisant un point central contrôlant ou limitant les échanges d'informations entre ces deux réseaux, vous créez donc une seule topologie, communément appelé topologie hiérarchique ou topologie arborescente.

3.3 Le modèle TCP/IP

3.3.1 Introduction

TCP/IP fut développé par le DoD (Département de la défense) des Etats-Unis et par DARPA

(Agence de projet de recherché de défense avancée) dans les année 70. TCP/IP fut conçu pour être un standard «ouvert» que quiconque puisse utiliser pour connecter des ordinateurs ensemble et échanger des informations.

Par la suite, il est devenu le modèle de base pour l'Internet.

3.3.2 Les couches

Le modèle TCP/IP définit quatre couches indépendantes entre lesquelles se divise le processus de communication entre deux équipements.

Les couches à travers lesquelles passe l'information sont:

3.3.2.1 Application

La couche application est la couche layer la plus proche de l'utilisateur final. C'est la couche qui est en charge de traduire les données des applications en information qui peut être envoyé a travers le réseau.

Ces fonctions basiques sont les suivantes:

- Représentation
- Codification
- Control du Dialogue
- Gestion de l'application

3.3.2.2 Transport

La couche transport établit, maintient et termine le circuit virtuel pour le transfert d'information.

Elle fournit un mécanisme de contrôle du flux des données et permet le «broadcasting», elle fournit également des mécanismes de détection et correction d'erreurs.

L'information qui arrive au niveau de cette couche depuis la couche application est divisée en segments différents. L'information qui va a la couche transport depuis la couche Internet est redistribué a la couche application a travers des port. (Voir la **Section 3.3.5 Ports** pour avoir la définition d'un port.)

Les fonctions basiques de cette couche sont:

- Fiabilité
- Control de flux
- Correction d'erreur
- Broadcasting

3.3.2.3 Internet

Cette couche divise les segments de la couche transport en paquets et envoie les paquets

a travers les réseaux qui crée l'Internet. Cela utilise *IP*, ou plutôt des adresses «*internet protocol*» pour déterminer l'emplacement de dispositif de destination. Cela n'assure aucune fiabilité dans la connections , étant donné que cela est déjà pris en compte par la couche transport, mais IP est responsable du choix de la meilleur route a prendre entre l'appareil d'origine et celui de destination.

3.3.2.4 Accès Réseau

Cette couche se charge de l'envoi d'information au niveau LAN et également au niveau physique.

Elle transforme toute l'information qui arrive de la couche supérieure en information basique (bits)

et la dirige vers la destination appropriée. A ce niveau, la destination de l'information est déterminée par la *MAC*, ou «*media access control*» , adresse de l'équipement destinataire.

3.3.3 Protocoles

Pour pouvoir envoyer de l'information entre deux équipements, les deux appareils doivent parler le même langage.

Ce langage est appelé *protocole*.

Les protocoles qui apparaissent dans la couche application du model TCP/IP sont:

- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (smtp)
- Domain Name Service (DNS)
- Trivial File Transfer Protocol (TFTP)

Les protocoles de la couche transport sont:

- Transport Control Protocol (TCP)
- User Datagram Protocol (UDP)

Les protocoles de la couche Internet sont:

- Internet Protocol (IP)

Le protocole le plus souvent utilisé dans la couche d'accès réseau est:

- Ethernet

Les protocoles listés ci-dessus et leurs ports associés seront décrits dans la section suivante.

3.3.3.1 Protocole de la couche Application

FTP ou *file transfer protocol* est utilisé pour la transmission de fichiers entre deux dispositifs. Il utilise TCP pour créer une connexion virtuelle pour le control d'information, puis créer une autre connexion qui doit sera utilisée pour la livraison des données. Les ports les plus souvent utilises sont 20 et 21.

HTTP ou *hypertext transfer protocol* est utilisé pour traduire l'information en pages web. Cette information est distribuée de manière similaire a celle utilisé par les courriers électroniques. Le port le plus souvent utilisé est le 80.

SMTP ou *simple mail transfer protocol* est un service mail qui est base sur le model FTP. Il transfère les courriers électroniques entre deux systèmes et fournit des notifications de courrier entrant. Le port le plus souvent utilisé est le 25.

DNS ou *domain name service* fournit un moyen d'associer un nom de domaine *à une adresse ip*. Le port le plus souvent utilisé est le 53.

TFTP or *trivial file transfer protocol* possède les même fonctions que FTP mais utilise UDP au lieu de TCP.

(Voir la **Section 3.3.3.2** plus de détail sur UDP et TCP.) Cela augmente les performance (vitesse) , mais est moins sure et digne de confiance. Le port le plus souvent utilisé est le 69.

3.3.3.2 Protocoles de la couche Transport

Deux protocoles peuvent être utilisés par la couche transport afin de transférer les segments l'information.

TCP (ou transmission control protocol) établis un circuit logique de bout en bout du réseau. Ce protocole régularise et synchronise le trafic de l'information en utilisant ce qui est connu sous le nom de «connexion en trois temps» (appelé en anglais "Three Way Handshake"). Au sein d'une connexion en trois temps, la composante d'origine envoie un paquet initial (appelé SYN) à la composante de destination. Cette dernière envoie ensuite un paquet d'acceptation, appelé SYN/ACK. Puis, la composante d'origine envoie un paquet appelé ACK, qui confirme l'établissement d'une connexion. À ce point, autant la machine de départ que la machine de destination ont établis qu'il y avait bel et bien une connexion entre eux deux et que chacune des machines est prête à envoyer et à recevoir des données entre eux.

*UDP (*ou *user datagram protocol)* est un protocole de la couche transport qui n'est pas fondé sur l'établissement d'une connexion. Ici, le système d'origine envoie ses paquets sans alerter la machine de destination. Il est donc au choix de la machine de destination d'accepter ou non ces paquets. Il en résulte que UDP est plus rapide que TCP, mais qu'il ne peut garantir que les paquets envoyés seront bel et bien acceptés.

3.3.3.3 Protocoles de la couche Internet

IP ou *Internet protocol* sert comme protocole universel pour permettre n'importe quel des deux ordinateurs de communiquer a travers n'importe quel réseau a n'importe quel moment. Comme UDP, c'est un protocole sans connexion, parce qu'il n'établit pas de connexion avec l'ordinateur distant. Au lieu de cela, il utilise ce que l'on appelle le service B*est*

Effort (faire ce son mieux), ce qui veux dire qu'il fera tous ce qui lui est possible pour s'assurer que tout fonctionne correctement, cependant sa fiabilité n'est pas garantie. Le Protocole Internet détermine le format de l'entêtes des paquets, y compris les adresses IP de l'appareil d'origine et de destination.

3.3.4 Adresses IP

Un nom de domaine consiste en l'adresse web que vous introduisez normalement au sein du navigateur web. Ce nom identifie en réalité une ou plusieurs adresses IP. Par exemple, le nom de domaine *microsoft.com* représente environs une douzaine d'adresses. Les noms de domaine sont utilisés à l'intérieur des URL afin d'identifier certaines pages Web en particulier.

Par exemple, pour l'URL http://www.pcwebopedia.com/index.html, le nom de domaine est *pcwebopedia.com*.

Chaque domaine possède un suffixe indiquant à quel domaine de haut niveau (Top Level Domain, ou TLD) ce domaine appartiens. Il y a un nombre limité de ces domaines. Par exemple:

.gov – Agences gouvernementales américaines

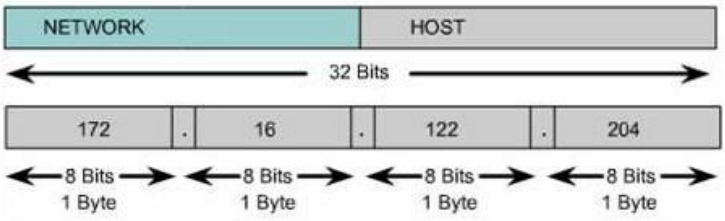
.edu – Institutions Éducationnelles

.org - Organisations à but non-lucratif

.com - Entreprises commerciales

.net – Adresses de réseau

Puisque l'Internet est basé sur des adresses IP et non sur des noms de domaines, tous les serveurs Web ont besoins d'un serveur DNS (de l'anglais, Domain Name Service)afin de traduire les noms de domaines en adresses IP. Les adresses IP sont les identifiants utilisés afin de différencier les ordinateurs et autres composantes connecté au réseau. Chacune de ces machines doit avoir une adresse IP différente afin qu'il n'y ait pas d'erreur d'identité au sein du réseau. Les adresses IP sont constituées de 32 bits divisés en octet de 8 bits, chaque octet étant séparé par un point. Une partie de l'adresse IP identifie le réseau et le reste de cette adresse identifie un ordinateur sur ce réseau.



Il existe aussi des adresses IP privée et publique. Les adresses privées sont utilisés sur les réseaux ne possédant aucune connexion avec le monde extérieur. Les adresses d'un réseau privé ne peuvent être dupliqués au sein de ce réseau, mais deux ordinateurs sur deux réseaux privés n'étant pas interconnectés peuvent posséder la même adresse. Les adresses IP définies par l'IANA (Internet Assigned Numbers Authority) comme étant disponibles pour les réseaux privés sont:

De 10.0.0.0 à 10.255.255.255

De 172.16.0.0 à 172.31.255.255

De 192.168.0.0. à 192.168.255.255

Les adresses IP sont divisés en classe, en fonction de la taille de la section de l'adresse utilisé afin d'identifier le réseau et par la taille de la section attribué pour l'identification de l'ordinateur. Dépendant de la taille de chacune des parties, plus de machine pourront se connecter à un réseau ou plus de réseau pourront exister. Les classes existantes sont:

Class A	Network	Host		
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4

Les classes existantes sont:

Class A: le premier bit est toujours zéro, cette classe inclut donc les adresses comprises entre 0.0.0.0 et 126.255.255.255. Note: Les adresses of 127.x.x.x sont réservées aux services de loopback ou host local.

Class B: Les deux premier bits du premier octet sont '10', par conséquent cette classe inclut les adressescomprises entre: 128.0.0.0 et 191.255.255.255.

Class C: Les trois premier bits du premier octet sont '110', par conséquent cette classe inclut les adresses comprises entre 192.0.0.0 et 223.255.255.255.

Class D: Les trois premier bits du premier octet sont '1110', par conséquent cette classe inclut les adressescomprises entre 224.0.0.0 et 239.255.255.255. Ces adresses sont réservées pour l'implémentation de groupe multicast.

Les adresses restantes sont utilisées à but d'expérimentation ou pour d'éventuelles allocations futurs.

Pour l'instant, ces classes ne sont pas utilisées pour différencier entre la partie de l'adresse utilisée pour identifier le réseau et l'autre pour identifier les équipements individuels. Au lieu de cela, un mas est utilisé. Dans ce mask, un bit '1' binaire représente la partie qui contient l'identifiant réseau et un bit '0' binaire représente le partie qui identifie l'équipement individuel. Par conséquent, pour identifier un équipement, en plus de l'adresse IP, il est nécessaire de spécifier le mask de sous réseau:

IP: 172.16.1.20
Mask: 255.255.255.0

Les adresses IP 127.x.x.x sont réservées pour l'usage de loopback ou adresse d'hôte local, c'est-à-dire, qu'elle se réfère directement a l'ordinateur local. Tous les ordinateurs on tune adresse local 127.0.0.1, par conséquent cette adresse ne peut pas être utilisée pour identifier des équipements différents. Il existe également d'autres adresses qui ne peuvent pas être utilisées.

.Ces adresses *sont les adresses réseaux et de broadcast*.

L'*adresse réseau est une adresse dans laquelle* la part de l'adresse qui identifie normalement l'équipement ne contient que des zéros. Cette adresse ne peut pas être utilisée, parce que cela identifie un réseau et ne peuvent jamais être utilisé pour identifier un équipement spécifique.

IP: 172.16.1.0
Mask: 255.255.255.0

L'adresse de Broadcast est une adresse dans laquelle la partie de l'adresse qui identifie normalement l'équipement ne comporte que des un (1). Ces adresses ne peuvent pas être utilisées pour identifier un équipement spécifique, parce que c'est adresse qui est utilisé pour envoyer l'information a tous les ordinateurs qui appartiennent au réseau spécifié.

IP: 172.16.1.255
Mask: 255.255.255.0

3.3.5 Ports

TCP et UDP utilisent tous deux des *ports* pour échanger leur information avec applications. Un *port* est une extension d'une adresse, cela est similaire à ajouter un appartement ou un numéro de chambre a l'adresse d'une rue.

Une lettre avec une adresse de rue arrivera au bon appartement, mais sans le numéro d'appartement, elle ne sera donc pas délivrée au bon destinataire. Les Ports à peu près de la même façon. Un paquet peut être délivré a la bonne adresse IP, mais sans le port associé, il n'y a aucun moyen de déterminer quelle application devrait agir sur ce paquet.

Une fois que les ports ont été défini, il est possible pour différent type d'information qui sont envoyés a une adresse IP d'être envoyée a l'application approprié.

En utilisant des ports, un service qui fonctionne sur un ordinateur distant peut déterminer quel type d'information un client local fait une requête, peut déterminer le protocole nécessaire pour envoyer cette information, et maintenir des communications simultanées avec un nombre de clients différentiels.

Par exemple, si un ordinateur local essaye de se connecter au site web www.osstmm.org,

dont l'adresse IP est 62.80.122.203, avec un serveur web qui s'exécute sur le port 80, l'ordinateur local se connecterait sur l'ordinateur distant en utilisant l'adresse socket:

62.80.122.203:80

Pour maintenir un niveau de standardisation parmi les ports les plus communément utilisés, IANA

a établi que les ports numéroté de 0 à 1024 sont utilisés pour les services communs.

Les restes des ports jusqu'au numéro 65535 sont utilisé pour l'allocation dynamique ou des services particulier.

Les ports les plus communément utilisés tel que IANA les a assignés sont:

Port Assignments		
Decimals	**Keywords**	**Description**
0		Reserved
1-4		Unassigned
5	rje	Remote Job Entry
7	echo	Echo
9	discard	Discard
11	systat	Active Users
13	daytime	Daytime
15	netstat	Who is Up or NETSTAT
17	qotd	Quote of the Day
19	chargen	Character Generator
20	ftp-data	File Transfer [Default Data]
21	ftp	File Transfer [Control]
22	ssh	SSH Remote Login Protocol
23	telnet	Telnet
25	smtp	Simple Mail Transfer
37	time	Time
39	rlp	Resource Location Protocol
42	nameserver	Host Name Server
43	nicname	Who Is
53	domain	Domain Name Server
67	bootps	Bootstrap Protocol Server
68	bootpc	Bootstrap Protocol Client
69	tftp	Trivial File Transfer
70	gopher	Gopher
75		any private dial out service

Port Assignments		
Decimals	**Keywords**	**Description**
77		any private RJE service
79	finger	Finger
80	www-http	World Wide Web HTTP
95	supdup	SUPDUP
101	hostname	NIC Host Name Server
102	iso-tsap	ISO-TSAP Class 0
110	pop3	Post Office Protocol - Version 3
113	auth	Authentication Service
117	uucp-path	UUCP Path Service
119	nntp	Network News Transfer Protocol
123	ntp	Network Time Protocol
137	netbios-ns	NETBIOS Name Service
138	netbios-dgm	NETBIOS Datagram Service
139	netbios-ssn	NETBIOS Session Service
140-159		Unassigned
160-223		Reserved

Vous pouvez également vous referez a la page web: *http://www.isecom.org/oprp* pour plus de détail sur les ports.

3.3.6 Encapsulation

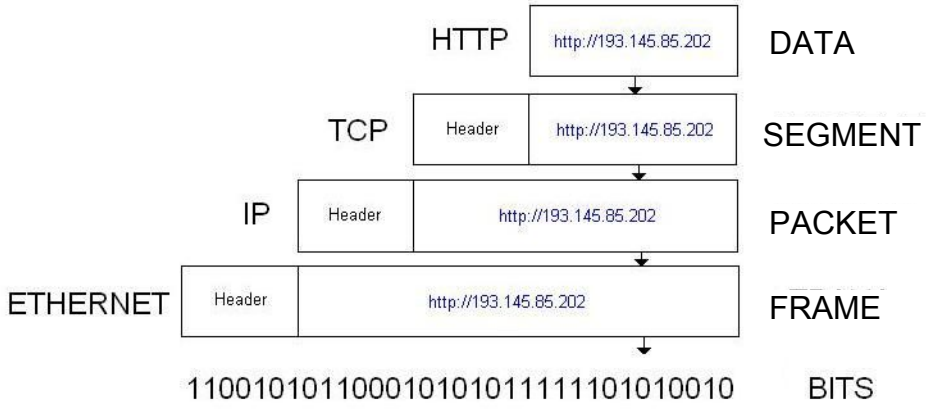
Lorsque une parcelle d'information – un e-mail, par exemple – est envoyée d'un PC vers un autre, elle est sujet à une série de transformation. La couche application génère les données,

Qui sont envoyées ensuite a la couche transport.

La couche transport prend ces informations et y rajoute un en-tête.

Cet en-tête contient des informations, tel que les adresses IP des ordinateurs d'origine et de destinations, cela explique ce qui doit être fait aux données pour que obtenir la destination appropriée. La couche suivante rajoute encore un autre en-tête, et ainsi de suite. Cette procédure recursive se nomme *encapsulation*.

Chaque couche l'une après l'autre crée fait de ces données une encapsulation des données de la couche précédente, jusqu'à ce que vous arriviez a la couche final, dans laquelle la transmission actuelle des données se produit. La figure suivante:



Lorsque l'information encapsulé arrive a destination, elle doit être des-encapsulée.

Etant donné que chaque couche reçoit des informations de la couche précédente, elle supprime les informations inutiles dans l'en-tête placé par la couche précédente.

3.4 Exercises

3.4.1 Exercise 1: Netstat

Netstat

La commande Netstat vous permet de voir l'état des ports sur un ordinateur.

Pour l'exécuter, vous devez ouvrir une fenêtre MS-DOS et taper:

netstat

Dans la fenêtre MS-DOS, vous verrez alors une liste des connections établies. Si vous voulez voir les connexions afficher au format numérique, taper:

netstat - n

Pour voir les connexions et les ports actives, taper:

netstat - an

Pour voir la liste des autres options taper:

netstat - h

Dans la sortie de Netstat, les colonnes 2 et 3 listent les adresses IP local et distante qui sont actuel ment utilisées par les ports actifs.

Pour les adresses des ports distants sont tels différentes de celles des adresses locales ?

En utilisant un navigateur web, ouvrez la page:

http://193.145.85.202

Allez ensuite dans une fenêtre MS-DOS et taper Netstat de nouveau. Quel nouvelle connexion (s) apparaissent ?

En utilisant un autre navigateur web, ouvrez la page:

http://193.145.85.203

Allez ensuite dans une fenêtre MS-DOS et taper Netstat –

- Pourquoi le protocol HTTP apparaît t-il sur plusieurs lignes?

- Quelles différences existent –t-il entre chacune d'entre elles?

- Si il y a plusieurs navigateur ouvert, comment l'ordinateur fait t-il pour savoir quel information va a tel ou tel navigateur?

3.4.2 Exercise 2: Ports et Protocoles

Dans cette leçon, vous avez appris que les ports sont utilisés pour différencier deux services.

Pourquoi lorsque qu'un navigateur web est utilise aucun port n'est spécifié?

Quel protocol est utilisé?

Est t-il possible que qu'un protocole soit utilisé dans plus d'une instante?

3.4.3 Exercise 3: Mon premier server : Netcat

To réaliser cette exercice, vous devez avoir le programme *Netcat*. Si vous ne l'avez pas, vous pouvez le télécharger de:

http://www.atstake.com/research/tools/network_utilities/

Une fois installé Netcat, ouvrez une fenêtre MS-DOS.

Allez dans le répertoire de Netcat et taper:

nc - h

Cela afficher les options disponibles de Netcat. Pour créer un serveur simple, taper:

nc - l - p 1234

Lorsque cette command se lance, le port 1234 est ouvert et les connections entrantes sont autorisées.

Ouvrez une seconde fenêtre MS-DOS et taper:

netstat – a

Cela devrait vérifier qu'il existe un nouveau service écoutent sur le port 1234.
Fermer la fainter MS-DOS.

Pour pouvoir dire qu'un serveur a été implémenté, vous devez établir une association client.

Ouvrez une fenêtre MS-DOS et taper:

nc localhost 1234

Grace a cette commande, une connexion est établie avec le serveur qui écoute sur le port 1234.

Maintenant, tous ce qui est écrit dans n'importe laquelle des deux fenêtre MS-DOS peut être vu dans l'autre fenêtre.

Créez un fichier nommé 'test', qui contienne le texte, "Welcome to the Hacker Highschool server!"

Dans la fenêtre MS-DOS taper:

nc - l - p 1234 > test

Depuis l'autre fenêtre MS-DOS, connecter vous au serveur en tapant:

nc localhost 1234

Lorsque le client se connecte au serveur, vous devriez voir la sortie du file 'test'.

Pour fermer le service, retourner à la fenêtre MS-DOS ou le process tourne et presser les touches CTRL-C.

Quel protocole a été utilise pour se connecter au serveur?

Netcat permet t-il de changer cela ?

Si oui comment?

Lecture Supplémentaire

Vous pourrez trouver de plus amples informations sur les ports et protocoles en acceder au liens suivant:

http://www.oreilly.com/catalog/fire2/chapter/ch13.html
http://www.oreilly.com/catalog/puis3/chapter/ch11.pdf

http://www.oreilly.com/catalog/ipv6ess/chapter/ch02.pdf

http://info.acm.org/crossroads/xrds1-1/tcpjmy.html

http://www.garykessler.net/library/tcpip.html

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ip.htm

http://www.redbooks.ibm.com/redbooks/GG243376.html

Port Number references:

http://www.iana.org/assignments/port-numbers

http://www.isecom.info/cgi-local/protocoldb/browse.dsp