Hacker Highschool

SECURITY AWARENESS FOR TEENS



LECON 3
SOUS L'INTERNET

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

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

AVERTISSEMENT

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

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

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

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

Sommaire

Les Contributeurs

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Chuck Truett, ISECOM
Bob Monroe, ISECOM
Kim Truett, ISECOM
Gary Axten, ISECOM
Marco Ivaldi, ISECOM
Simone Onofri, ISECOM
Greg Playle, ISECOM
Tom Thomas, ISECOM
Mario Platt
Ryan Oberto, Johannesburg South Africa
Vadim Chakryan, Ukraine
Peter Houppermans

Les Traducteurs

Koffi « Willy » Nassar

ISECOM

Introduction et Objectifs

Dans un passé lointain, avant l'avènement de l'Internet, les communications électroniques étaient une sorte de vodou. Chaque constructeur d'ordinateur avait leurs propres idées sur la manières dont les ordinateurs devraient communiquer via les câbles. Et personne ne pouvait imaginer qu'un ordinateur fabriqué par Wang puisse communiquer avec un ordinateur fabriqué par Burroughs.

Ce monde a connu un changement lorsque les scientifiques et les étudiants ont expérimenté la convivialité qu'il y a dans l'utilisation d'un terminal pour accéder à un super ordinateur. Le fameux PC d'IBM a vu le jour, et chacun voulait accéder au super ordinateur via leur ordinateur personnel. Très tôt les modems établissaient des connexions à accès distant (Dial-Up) et les utilisateurs travaillaient via des émulateurs de terminal. Les réseaux ont gravi l'échelon pour atteindre celui d'un Art Caché où les maîtres étaient (réellement) appelés des **gurus**.

Ce monde a encore énormément changé lorsque l'Internet, qui a débuté comme un projet militaire, était accessible au grand publique. Les réseaux avaient toujours été locaux, c'est-à-dire restreints à un bureau au plus à un Campus. Comment allaient dialoguer tous ces systèmes ?

La réponse était "d'introduire" un système d'adressage universel dans les réseaux existant, un système que nous appelons généralement **Internet Protocol (IP).** Pensez-y de cette façon: votre ami à l'étranger vous envoie un colis. Ce colis peut passer par un avion, un train ou un automobile, mais vous n'avez pas besoin de connaître réellement le planning de l'avion ou la localisation de la gare la plus proche. Le colis arrivera éventuellement à l'adresse de votre rue, qui est en fin de compte la chose la plus importante. Votre **adresse IP** est assez semblable à ceci: il se peut que les paquets voyagent comme des électrons, des faisceaux de lumières ou des ondes radio, mais ces systèmes vous importent peu. Tout ce qui est le plus important est votre adresse IP, et l'adresse IP du système avec lequel vous êtes entrain de communiquer.

Une chose qui complique cette situation dans le monde réel est qu'il se peut que plus d'une personne vive à une unique adresse. Dans le monde des réseaux, c'est ce qui se passe lorsqu'un serveur fournit par exemple à fois des données HTTP, HTTPS et FTP. Notez la présence de la lettre "P" dans chacun de ces acronyme ? Elle désigne toujours le mot **protocole**, qui est une autre façon de dire "un type de communication".

Cette leçon vous aidera à comprendre comment les protocoles et leurs ports fonctionnent sous Windows, Linux, et OSX. Vous vous familiariserez avec plusieurs utilitaires (dont certains ont déjà été introduits dans la leçon précédente) qui explorent les capacités du fonctionnement de votre système sur un réseau.

A la fin de ce chapitre, vous aurez une connaissance de base sur:

- les concepts des réseaux et comment les communications sont établies
- les adresses IP
- les ports et les protocoles

Les Concepts de Base des Réseaux

Le point de départ d'un réseau est le **réseau local** ou **local area network (LAN)**. Les réseaux locaux (LANs) permettent aux ordinateurs qui se trouvent au sein d'un même local de partager des ressources telles que les imprimantes et les espaces de stockage des disques, et les **administrateurs** contrôlent cet accès. Les sections ci-après décrivent des équipements réseau et des topologies habituels.

Les Équipements

En évoluant dans votre carrière de hacker, vous verrez de nombreux diagrammes réseau. Il est très utile de reconnaître la plupart des symboles habituels:

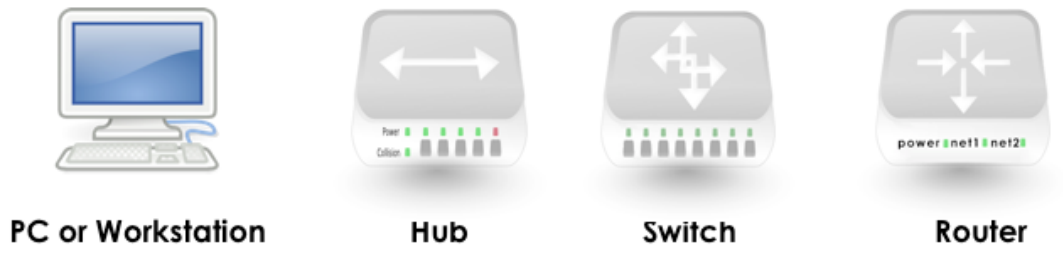


Figure 3.1: Les Symboles Réseau Habituels

Un **concentrateur (HUB)** est semblable à une conversation sur une ancienne ligne téléphonique: tout le monde est raccordé à une même ligne, et peut écouter les conversations d'un autre. Ceci peut rapidement être la source de bruits sur un réseau local.

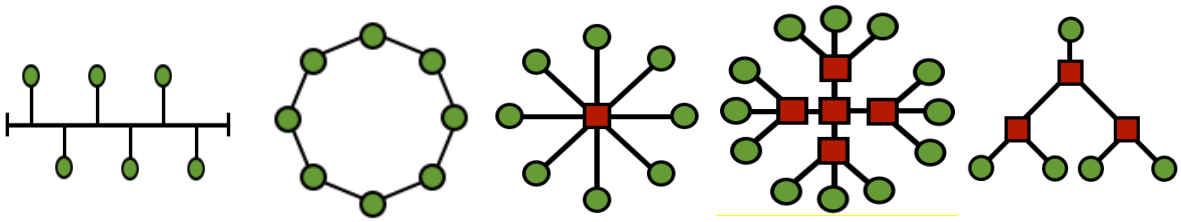
Un **commutateur (SWITCH)** est mieux: il filtre le trafic de telle sorte que seuls les deux ordinateurs engagés dans une conversation puissent s'entendre. Mais comme le concentrateur, il est seulement utilisé sur un réseau local.

Un **routeur (Router)** se situe entre deux ou plusieurs réseaux locaux ; il est utilisé pour accéder à d'autres réseau et à l'Internet, et il utilise les adresses IP. Il analyse le contenu des paquets envoyés et détermine le réseau destinataire de ces paquets. Si le paquet est destiné à "l'autre" réseau, comme dans la gestion du trafic urbain, le paquet est renvoyé vers sa destination.

Les Topologies

Une **topologie** représente une autre manière de dire "la manière dont nous sommes connectés". Le type de décisions que nous prenons concernant notre topologie peut affecter positivement comme négativement dans le futur, en fonctions des technologies utilisées, des contraintes technologiques et physiques, de la performance et de la sécurité requise, de la taille et de la nature d'une organisation, etc.

La structure physique d'un réseau local peut ressembler à l'une des topologies physiques suivantes:



Bus **Anneau** **Étoile** **Étoile Étendue** **Hiérarchique**

Figure 3.2: Les Topologies

Dans une topologie **bus**, tous les ordinateurs sont connectés à un seul câble, et chaque ordinateur peut communiquer directement avec les autres. Mais lorsqu'une partie du bus est rompue, tout le monde est coupé du réseau.

Dans la configuration **anneau**, chaque ordinateur est connecté au suivant, et le dernier est relié au premier, et chaque ordinateur ne peut communiquer qu'avec les deux ordinateurs adjacents.

Les topologies bus sont rarement utilisés de nos jours. Les topologies anneau sont souvent utilisées à un niveau inter-état, habituellement avec deux anneau à conteurs cycliques, qui envoient chacun du trafic dans des directions opposées, pour une fiabilité et une tolérance aux fautes.

Dans la topologie **étoile**, aucun des ordinateurs n'est directement connecté avec les autres. Par contre ils sont rattachés à un concentrateur ou un commutateur qui relaie les informations d'un ordinateur à un autre.

Si plusieurs concentrateurs ou commutateurs sont connectés entre eux, vous obtenez une topologie **étoile étendue.**

Dans une topologie étoile ou étoile étendue, tous les points centraux sont des **pairs,** cela veut dire, qu'ils sont essentiellement des égaux. C'est la topologie la plus courante aujourd'hui.

Cependant, si vous connectez deux étoiles ou étoiles étendues en utilisant un point central qui contrôle ou limite le trafic entre les deux réseaux, alors vous avez un réseau à topologie **hiérarchique**. C'est habituellement la topologie déployée dans les grandes entreprises.

Début du Jeu: Laisser la Porte Dérobée Ouverte

A la période la plus chaude de l'Eté, Jace été ravi d'aider le département à air conditionné de la police local à installer leur petit réseau. Ils lui ont payé avec des biscuits, un temps de repos loin de la chaleur, une conversation et l'opportunité d'installer des portes dérobées. En rampant en dessous des table banc en acier qui n'ont pas été déplacés depuis des décennies, Jace avait trouvé une cachette rudimentaire pour un point d'accès Wi-Fi. Elle venait juste de le brancher et de le parsemer d'ordure, puis elle avait tiré un rouleau de câble Ethernet vers la prise murale qu'elle venait tout juste d'installer.

Une main énorme a frappé sur le banc qui se trouvait au-dessus d'elle. Jace a cogné du métal et a crié "Oh ! Ma tête !" puis elle ajouté, "êtes vous sûr que vous ne voudrez pas que j'installe votre serveur ?

Le policier a raclé sa gorge et essayé d'utiliser la voix d'un Professeur Éminent. "Bien je le ferais, mais je ne suis pas sûr de la manière dont la résistance au rayon de flux tiendrait jusqu'à l'alimentation croisée du micro canal. Surtout lorsque la pleine lune tombe sur le dernier Mardi du mois".

Jace battait ses pieds à titre de ridiculisation par une adolescente irritée. "Apparemment vous n'avez pas de problèmes pour atteindre des niveaux quantiques de la foutaise. Et quand aurai-je mes biscuits, Officier Kickam ?"

"Jace, s'il te plaît, appelle moi Hank. Je me sens vieux lorsque tu m'appelle Officier Kickam". Il semble être fâché mais elle a remarqué l'ingénierie sociale lorsqu'elle a entendu cela: il essayait de créer une diversion pour détourner son attention des biscuits.

"Hank, je n'aime pas vous donner des informations, mais vous *êtes* un vieux".

"Oh, cela est blessant. Je ne suis pas vieux, je suis distingué", répliqua t-il, en considérant ses bottes de police noires bien cirées au moment où les faux jetons éparpillés de Jace ont disparu sous l'énorme banc. Puis des yeux brun cannelle et un visage recouvert de toiles d'araignée ont fait apparition. Jace avait toujours un rouleau de câble dans l'une de ses mains. Hank l'a aidée à se lever et à nettoyer les toiles d'araignée de son visage et de ses épaules.

"Au secours, brutalité policière", s 'écriait Jace.

"Criminel hostile", répliqua Hank. " Éduquez-moi donc selon votre plan diabolique ici", disait le justicier poilu et musclé, ce qui paraissait à James presque comme un ton suppliant.

Cela semblait rassurant, donc elle demanda, "Êtes-vous sûr de vouloir connaître quelque chose sur le réseau ? Il a accepté avec impatience. Jace disait dans sa pensée: tête gonflée.

"Ok, Je que j'avais fait c'était la conception d'une topographie réseau, c'est à dire une carte qui montre l'emplacement des équipements, ordinateurs, concentrateurs, prises, commutateurs, routeurs et pare-feu. Vous ne pouvez pas débuter un tel projet sans une carte", disait-elle, en jetant un coup d'œil dans la tasse. "Tout cela veut dire qu'il faut s'assurer que chaque nœud peut communiquer avec un autre, sans aucune opportunité de rupture. Donc, comme on le sent dans une architecture en bus, lorsqu'un nœud est déconnecté, tout le reste du réseau est aussi déconnecté". Hank a hoché la tête donc Jace a continué.

"Imaginer que le réseau soit semblable à cette boutique de flic, euh, ce poste de police, et que quelqu'un y a amené un suspect. Chaque policier méritera son tour pour battre ce dernier sans empiéter sur le temps d'un autre. Si la victime, je veux dire le suspect, est déplacé vers une autre cellule, tous les policiers qui aimeraient bien battre le type doivent savoir là où il est parti".

"Oh Jace, il me semblera que tu ais aussi besoin d'une bonne fessée si tu continu à parler ainsi de nous, paisibles policiers". Hank a rehaussé sa ceinture de pistolet et rétracté son ventre plat.

Jace a renâclé un rire. "Donc le suspect est le paquet de données et vous les policiers voyous vous êtes les équipements réseau. Et chaque équipement, un commutateur, un routeur, un pare-feu, un autre serveur ou quoi d'autre, a besoin de savoir qu'ils ont fini avec le paquet de donné. Comme vous le savez, il s'agit d'une rouée de coups de bâtons de police. Je pense que vous avez désigné cet acte par l'expression "*donner un bain de bâton à quelqu'un*".

Hank tourna ses yeux et chercha à tâtons le bâton qu'il n'avait pas sur lui.

Rire, Jace a soulevé la bobine de câble comme un bouclier. "Heh, J'ai eu un tas de câble et je n'ai pas peur de l'utiliser. Déposez la tasse de café et tout le monde sera épargné". Dépourvu de rire et d'équilibre, Jace a provoqué Hank, qui n'a pas bougé. Waou, *cet homme est une roche entière*, remarqua t-elle. La main qu'il a posée sur son épaule, lui a rappelé quelque chose...

Elle était un peu trop rapide. "Donc il existe deux types d'équipements. Ceux qui sont intelligents et les abrutis. Tout comme les policiers". Quatre homme en uniforme sont en approche exactement au mauvais moment pour entendre la partie "les abrutis. Tout comme les policiers". Maladroitement, Jace continua, "les équipement Intelligents se rappellent de tout ce qu'ils font. Ils gardent les historiques de leurs activités".

"Et les abrutis ? Tout comme les policiers ?" demanda le Chef de la Police.

Fin du Jeu.

Le Modèle TCP/IP (DoD)

Le TCP/IP fut développé par le **département de la défense (Department of Defense)** des États Unis et l'agence **DARPA (Defense Advanced Research Project Agency)** dans les années 70. TCP/IP était conçu pour être un standard ouvert que n'importe qui pourait utiliser pour connecter les ordinateurs et échanger des informations entre eux. Finalement, il est devenu la base de l'Internet.

Généralement, la forme la plus simple du modèle TCP/IP est appelée **modèle DoD**, et c'est par là que nous allons commencer.

Les Couches

Le simple modèle DoD définit quatre couches totalement indépendantes en lesquelles est réparti le processus de communication entre deux équipements. Les couches qui échangent des informations sont:

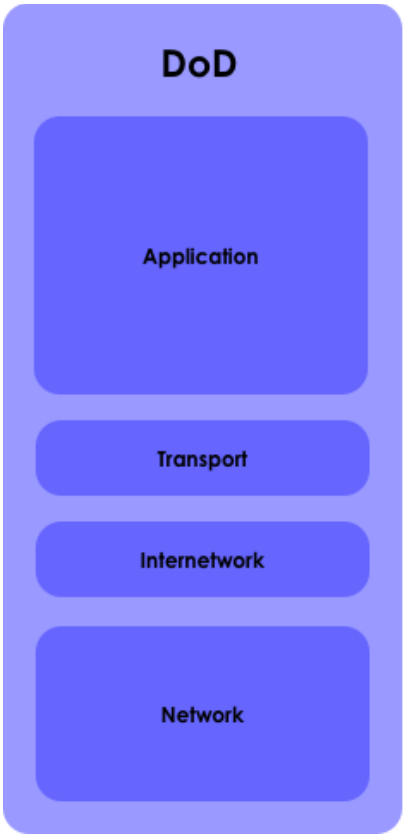


Figure 3.3: Le Modèle DoD

Application

La couche application est exactement ce que vous avez probablement pensé qu'elle soit: C'est à cette couche que des applications comme Firefox, Opera, les clients de messagerie, les sites des réseaux sociaux, les application de messagerie instantanée et de chat fonctionnent. En effet peu d'applications ont accès à l'Internet: quelques applications de bureautique, par exemple, se connectent à une galerie d'images en ligne. La couche application crée la charge utile que doivent transporter les autres couches. Une bonne analogie de ce système est le système postal. Cette couche crée le paquet et l'entoure des instructions nécessaires à la façon dont il devrait être manipulé. Ensuite elle transmet le paquet à la salle des courriers: la couche Transport.

Transport

La couche transport établit les connexions réseau, qui sont appelés **sessions**. Dans le monde de l'Internet, le tout premier protocole de la couche transport est **TCP (Transmission Control Protocol).** TCP ajoute d'autres "informations de contrôle complémentaires" au début et à la fin du paquet, et des informations sur la nature du paquet (pour dire, 1 sur 3). Bref ce sont des informations qui permettent d'assurer la transmission du paquet et de vérifier l'intégrité du paquet.

Supposons que vous voudriez envoyer une lettre à votre mère. La lettre peut être petite ou énorme, mais elle est trop énorme pour être envoyée par Internet en un seul morceau. Par contre, TCP fragmente cette lettre en **segments**, ce sont des petits fragments qui sont respectivement numérotés, possédant un petit code de vérification d'erreurs à leur fin. Si un paquet est corrompu au cours de son voyage, TCP requiert une retransmission. À la destination, TCP ré-assemble les segments dans leur ordre de départ et votre mère pourra enfin lire sa lettre dans sa boîte électronique.

Mais n'oubliez pas que TCP n'est pas le seul qui entre en jeu à cette couche: le protocole **UDP** aussi fonctionne à cette couche, et particulièrement il NE crée pas de sessions. Il envoi juste un flux de **paquets** (ou **datagrammes**), qui sont similaires aux segments, mais UDP ne vérifie pas si vous l'avez reçu ou pas.

Que ce soit TCP ou UDP, des **numéros de port** spécifiques sont assignés à tous les trafic à cette couche.

Inter-Réseau (Internetwork)

Cette couche ajoute des informations concernant les adresses de la source et de la destination, le début et la fin d'un **paquet**. C'est semblable à une compagnie de livraison qui livre les colis à l'adresse adéquate. Cette couche ne se préoccupe pas de la bonne livraison des paquets, ou du fait qu'ils soient en bon état ; c'est le rôle de la couche Transport. Le protocole majeur à ce niveau est, le **protocole IP (Internet Protocol).** Et c'est la couche qui utilise les adresses IP pour envoyer les paquets à leur vraie destination en passant par la meilleure route.

Accès Réseau (Network Acces)

C'est la couche de bas-niveau et qui est physique, et c'est elle qui vous relie à l'Internet. Si vous utilisez une connexion à accès distant (dial-up), nous sommes désolés, vous utilisez une simple connexion **PPP** (Point-to-Poit Protocol). Si vous avez une liaison DSL, il se peut que vous utilisiez **ATM** ou **Metro Ethernet**. Et si vous avez Internet via le câble, vous utilisez un réseau physique **DOCSIS**. Peu importe le réseau physique que vous utilisez, parce TCP/IP se charge de la coordination de tout ceci. La couche accès réseau est composée des éléments suivants: un câble Ethernet et une **carte réseau** (**NIC: Network Interface Card**), ou une carte sans-fil et un point d'accès. Elle gère des bits (suites de 0 et 1) du bas niveau lorsqu'ils passent d'un bout à un autre.

Étoffez Vos Connaissances: Jetez un coup d'oeil sur "Le Modèle OSI"

Consultez "Le Modèle OSI" à la fin de cette leçon pour une autre approche de la modélisation d'un réseau.

Les Protocoles

Donc maintenant vous êtes connectés à l'Internet. Cela semble assez simple, mais considérez la situation habituelle que vous vivez: vous êtes entrain de faire une recherche innocente et importante sur Internet, au moment où votre cher frère ou sœur passe du temps en suivant un film. Pourquoi ces deux flux de trafic ne se mélangent pas ? Comment le réseau les envoie séparément ?

La réponse est: l'utilisation des **protocoles**, qui sont une sorte de langage que tous les différents types de trafic utilisent pour communiquer. Le trafic web utilise un protocole, le transfert de fichiers utilise un autre, et la messagerie électronique un autre. Comme toutes les choses numériques, les protocoles n'utilisent pas réellement les noms à la couche réseau ; ils utilisent les adresses IP et les **numéros de port**.

Les Protocoles de la Couche Application

Le **protocole FTP** (File Transfer Protocol) est utilisé pour le transfert de fichiers entre deux équipements. Il utilise un port pour le transfert de données, et un autre pour envoyer les

signaux de contrôle ("J'ai reçu le fichier ! Merci"). Les ports les plus utilisés habituellement sont les ports TCP, 20 et 21.

Le **protocole HTTP** (HyperText Transfer Protocol) est utilisé pour les pages web. Ce trafic utilise habituellement le port TCP 80. **HTTPS** une dérivée sécurisée de HTTP, qui crypte le trafic réseau, et il utilise habituellement le port TCP 443.

Le **protocole SMTP** (Simple Mail Transfer Protocol) est utilisé pour envoyer les messages électroniques vers un serveur de messagerie. Il utilise le port TCP 25.

Le **protocole DNS** (Domain Name Service) permet de faire la liaison entre un nom de domaine tel ISECOM.org et une adresse IP telle 216.92.116.13. Il utilise le port UDP 53.

Les Protocoles de la Couche Transport

TCP (Transmission Control Protocol) et **UDP** (User Datagram Protocol) sont les deux principaux protocoles utilisés par la couche transport pour le transfert des données.

Le **protocole TCP (Transmission Control Protocol)** établit une connexion logique (une **session**) entre deux hôte sur un réseau. Il établit cette session en utilisant une procédure nommée **three-way handshake** qui veut dire littéralement **"la salutation à trois étapes".**

1. Lorsque mon ordinateur veut se connecter au tien, il envoie un paquet de synchronisation -**SYN**, qui veut dire tout simplement "synchronisons nos horloges pour que nous puissions échanger du trafic à des intervalles de temps".
2. Ton ordinateur (s'il est prêt à accepter la connexion) répond en envoyant un paquet d'accusé de réception et une demande de synchronisation et tout cet ensemble est nommé **SYN/ACK.**
3. Mon ordinateur conclu l'accord avec un paquet d'accusé de réception nommé **ACK,** et nous sommes connectés.

Mais ceci ne se passe seulement qu'avec TCP. Par contre le **protocole UDP** (User Datagram Protocol) est un protocole de la couche transport qui ne tient pas compte de la création d'une connexion. UDP envoi seulement les données. Si le récepteur les reçoit c'est bien sinon ce n'est pas grave. Ceci rend UDP très rapide, donc il est plus utile pour des choses comme le flux audio et vidéo, où la perte d'une trame importe peu. UDP est utilisé aussi pour les jeux en ligne (ou en réseau) où la perte d'une trame importe peu (compte tenu du côté où vous vous trouvez).

Les Protocoles de la Couche Internet

Le **protocole IP (Internet Protocol)** agit comme un protocole universel qui permet à n'importe quel ordinateur de communiquer à travers n'importe quel réseau à tout moment. Il est semblable au coursier de la poste qui ne fait que livrer les courriers ; tout ce qu'il fait c'est livrer les paquets à leur adresse de destination.

Internet Control and Management Protocol (ICMP)

ICMP est le protocole qu'utilisent les équipements réseau et les administrateurs réseau pour le dépannage et la maintenance du réseau. Il comprend des outils comme **ping** (Packet InterNet Groper) et des commandes similaires qui testent le réseau et renvoient un rapport d'erreurs. Puisque des gens ont utilisé des outils comme **ping** pour submerger et mettre hors d'usage des hôtes et des réseaux, la plupart des systèmes se limitent à une réponse ICMP par seconde.

En somme, les ports et les protocoles travaillent ensembles comme suit:

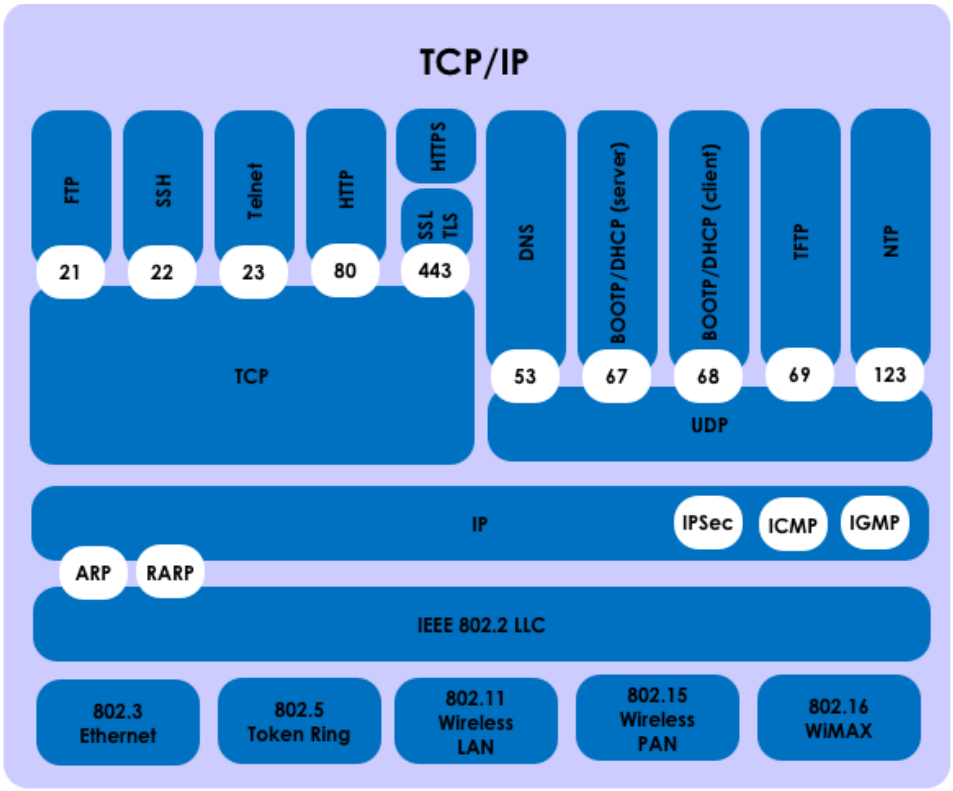


Figure 3.4: La Pile TCP/IP

Les Adresses IPv4

Les noms de domaine sont facilement manipulables pour les humains, parce que nous sommes bon lorsqu'il s'agit de retenir des noms comme ISECOM.org. Mais en réalité les réseaux ne les comprennent pas ; ils comprennent seulement les adresses numériques c'est à dire les adresses IP. Donc lorsque vous voudriez accéder à ISECOM.org, votre ordinateur fait une recherche rapide en utilisant le protocole **DNS (Domain Name Service)** pour trouver l'adresse IP qui lui correspond.

Les adresses IP sont semblables aux adresses des rues. Si vous voulez avoir un courrier, vous devriez en avoir une. Les adresses **IPv4** sont constituées de 32bits qui sont répartis en **4 groupes** de **8-bits (octets)** chacun, qui sont séparés par des points. Cela veut dire qu'il existe 2^{32} (ou 4,294,967,296) adresses IP uniques sur Internet sous IPv4. Une partie de l'adresse IP identifie le réseau, et le reste identifie les ordinateurs individuels sur le réseau. Faites l'analogie de la répartition d'une adresse IP avec les parties d'une adresse postale qui contiennent respectivement le pays/la ville (partie réseau) et l'adresse d'une rue (de l'hôte ou ordinateur individuel).

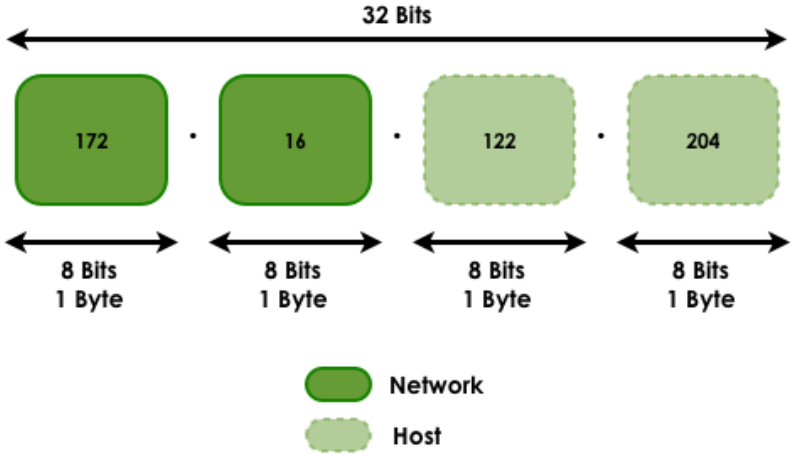


Figure 3.5: Numéro Réseau et Identifiant d'un Hôte

Si nous revenons à l'analogie avec le service postal, IP est le camion livreur qui amène le paquet au service de la poste qui convient. TCP est l'emballage extérieur muni de la liste du nombre d'objets contenus dans le paquet, et de la nature de chaque objet (i.e 3 sur 65) . Les adresses du niveau hôte désignent la maison exacte (l'ordinateur) à laquelle est destinée le paquet.

Il existe des **adresses IP** qui sont **publiques** et d'autre qui sont **privées** (i.e **non routables**). Les adresses IP privées sont utilisées par les réseau privés ; les routeurs ne permettent pas l'utilisation de ces adresses sur Internet.

Les adresse IP au sein d'un réseau privé ne devraient pas être dupliquées, mais des ordinateurs se trouvant sur deux réseaux privés différents - mais qui ne sont pas connectés - pourraient avoir les mêmes adresses IP. Les adresses IP qui sont définies par IANA (internet Assigned Number Authority), comme étant disponibles pour les réseaux privées (selon RFC1918) sont:

10.0.0.0 à 10.255.255.255	(Class A)
172.16.0.0 à 172.31.255.255	(Class B)
192.168.0.0 à 192.168.255.255	(Class C)

Les Classes

Les adresses IP sont réparties en des classes en fonction de la portion de l'adresse qui est utilisée pour identifier le réseau et de la portion utilisée pour identifier les ordinateurs individuels.

En fonction de la taille allouée à chaque partie, il y aura plus d'hôtes ou de machines individuelles dans le réseau, ou il y aura plus de réseaux disponibles. Les classes qui existent sont:

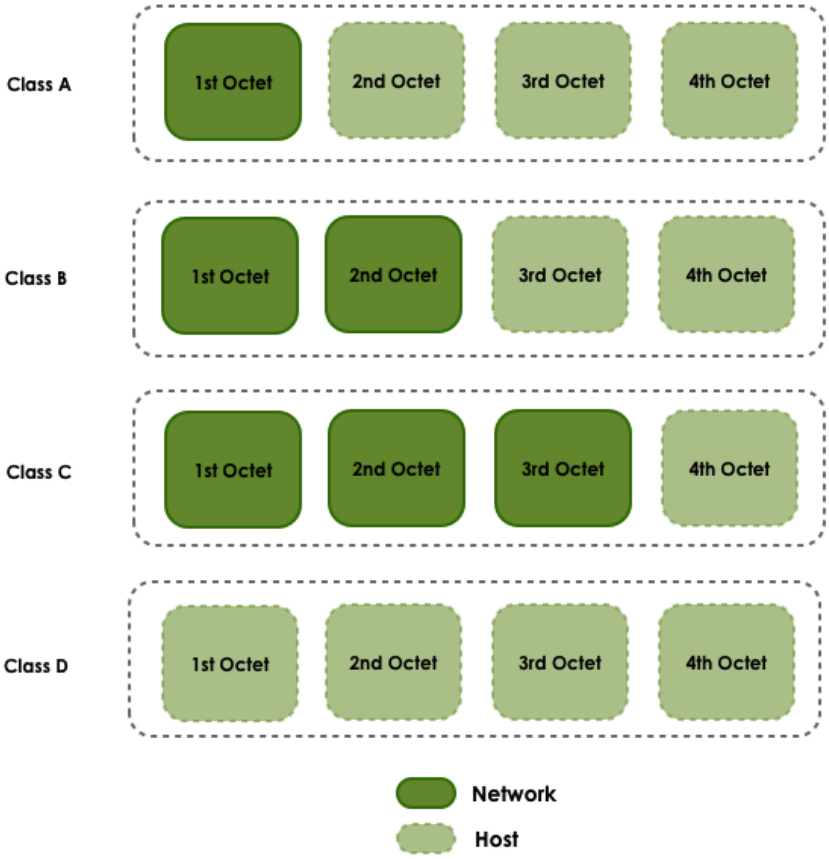


Figure 3.5: Les Classes d'Adresse IP

La Classe A: le premier bit est toujours zéro, donc cette classe comprend les adresses qui se trouvent entre 0.0.0.0 (qui par convention n'est jamais utilisé) et 126.255.255.255. Notez que: les adresses 127.x.x.x sont réservées pour des tests de boucle interne ou pour des service tournant sur la machine locale (voir ci-dessous).

La Classe B: les deux premiers bits sont '10', donc cette classe comprend les adresses qui se trouvent entre 128.0.0.0 et 191.255.255.255.

La Classe C: les trois premiers bits du premier octet sont '110', donc les adresses de cette classe se trouvent entre 192.0.0.0 et 223.255.255.255.

La Classe D: les quatre premiers bits du premier octet sont '1110', donc les adresses de cette classe se trouvent entre 224.0.0.0 et 239.255.255.255. Les adresses de cette classe sont réservée pour des application multicast vers un groupe.

Les adresses restantes sont utilisées pour des expériences ou pour des allocations futures possibles.

Le **masque de sous-réseau (netmask** ou **subnet mask)** est utilisé pour identifier ces deux parties d'une adresse IP: la partie réseau et la partie hôte. En notation binaire, un "1" montre la partie contenant l'identifiant du réseau et un "0" représente la partie qui identifie chaque hôte individuel.

Les masques de sous-réseau par défaut des trois premières classes d'adresses IP sont:

255.0.0.0 (Class A)

255.255.0.0 (Class B)

255.255.255.0 (Class C)

Ceci est effectivement assez rusé, puisque les réseaux qui utilisent les classes par défaut masqueront un octet s'ils sont de la Classe A, deux octets s'ils sont de la Classe B et trois octets s'ils sont de la Classe C. L'utilisation des classes par défaut est très commode – mais tout le monde ne le fait pas.

Tout cela veut dire que pour identifier un hôte, vous aurez besoin à la fois de l'adresse IP et d'un masque de sous-réseau:

IP: 172.16.1.20
Masque: 255.255.255.0

Les Adresses de Boucle Interne (Loopback Addresses)

Les adresses IP qui se trouvent entre 127.0.0.1 et 127.255.255.254 sont réservées pour la **boucle interne (loopback)** ou les adresses d'hôte local, cela veut dire, qu'elles font directement référence à la machine locale. Chaque machine possède une adresse d'hôte locale (ou loopback adress) qui est 127.0.0.1. Cependant cette adresse ne peut être utilisée pour identifier les différents services.

Il existe aussi d'autres adresses qui ne peuvent pas être utilisées. Ce sont les **adresses réseau** et les **adresse de diffusion.**

Les Adresses Réseau

L'adresse réseau représente fondamentalement la portion réseau d'une adresse IP, elle comporte **des zéros là où devrait être la partie hôte.** Cette adresse ne peut pas être attribuée à un hôte, parce qu'elle identifie tout le réseau, et non un seul hôte.

IP: 172.16.1.**0**
Masque: 255.255.255.0

Les Adresses de Diffusion (Broadcast Addresses)

L'adresse de diffusion est fondamentalement la partie réseau d'une adresse IP, **qui contient des "1" là où devrait être la partie hôte**. Cette adresse ne peut être utilisée pour identifier un hôte spécifique, parce qu'elle désigne l'adresse que tous les hôtes écoutent (en effet c'est ce que signifie une diffusion: tout le monde écoute).

IP: 172.16.1.**255**
Masque: 255.255.255.0

Les Ports

Les protocoles TCP et UDP utilisent des **ports** pour échanger des informations avec les applications. Un port est une extension d'une adresse, comme lorsqu'on ajoute le numéro de l'appartement ou de la chambre à l'adresse de la rue. Une lettre munie de l'adresse de la rue arrivera devant l'immeuble adéquat, mais sans le numéro de l'appartement, elle ne parviendra pas à la personne adéquate.

Les ports fonctionnent de la même manière. Un paquet peut parvenir à l'adresse IP adéquate, mais sans un numéro de port associé, il n'y a pas un moyen pour déterminer l'application qui devrait traiter le paquet. Un numéro de port est aussi un nombre de 16bits, ce qui veut dire qu'il peut avoir des valeurs décimales qui se trouvent entre 0 et 65535 (2^{16}).

> Une autre façon de voir cette notion de port est la suivante: chaque ordinateur est une agence de poste. Chaque application possède sa propre boîte postale ; deux applications ne pourraient pas partager la même boîte postale. Le numéro de port désigne ce numéro de boîte postale.

Les numéros de port permettent d'envoyer plusieurs flux d'informations vers une unique adresse IP, où chacun est envoyé vers l'application adéquate. Le numéro de port permet à un service tournant sur une machine distante de savoir quel est le type d'informations qu'un client local demande et quel protocole est utilisé pour envoyer cette information, et tout ceci se fait pendant qu'une communication simultanée avec un nombre varié de clients s'opère.

Par exemple, lorsqu'un ordinateur local essaie de se connecter à www.osstmm.org, dont l'adresse IP est 62.80.122.203, via un serveur web sur le port 80, l'ordinateur local essaierait de se connecter à l'ordinateur distant en utilisant l'**adresse socket** suivante:

62.80.122.203:80

Afin de maintenir un niveau de standardisation entre les ports qui sont habituellement utilisés, l'IANA a statué que les numéro de port qui se situent entre **0** et **1024** soient utilisés pour les **services habituels**, **privilégiés** ou **bien connus**. Le reste des ports – i.e de 1025 à 65535 – sont utilisés pour des attributions dynamiques ou des service particuliers.

Les ports les plus utilisés habituellement (ou les plus connus) – assignés par l'IANA – sont listés comme suit:

Les Attributions de Port		
Numéros	**Mots Clés**	**Description**
5	rje	Remote Job Entry
0		Réservé
1-4		Non assigné
7	echo	Echo

Les Attributions de Port		
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
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

Les Attributions de Port		
140-159		Non attribué
160-223		Réservé

Encapsulation

Lorsqu'un fragment d'information – un message électronique, par exemple – est envoyé d'un ordinateur vers un autre, il est sujet à une série de transformations. La couche Application génère la donnée qui est envoyée à la couche Transport.

La couche Transport récupère cette information, et la découpe en des segments et y ajoute un en-tête et une queue, qui contient les numéros de port, qui sont des nombres uniques qui identifient un segment et une autre information de session.

Ensuite le segment est envoyé à la couche Réseau où un autre en-tête est ajouté, il contient l'adresse IP de la source et de la destination et d'autres informations supplémentaires.

La couche suivante, qui dans la plupart des réseaux locaux est fourni par Ethernet, ajoute encore un autre en-tête, et ainsi de suite. Cette procédure est connue sous le nom d'**encapsulation**.

Chaque couche après la précédente fait encapsuler les données de la couche précédente, jusqu'à ce que l'on arrive à la couche final, au sein de laquelle la transmission réelle de données est effectuée. Donc, voici ce à quoi ressemble l'encapsulation:

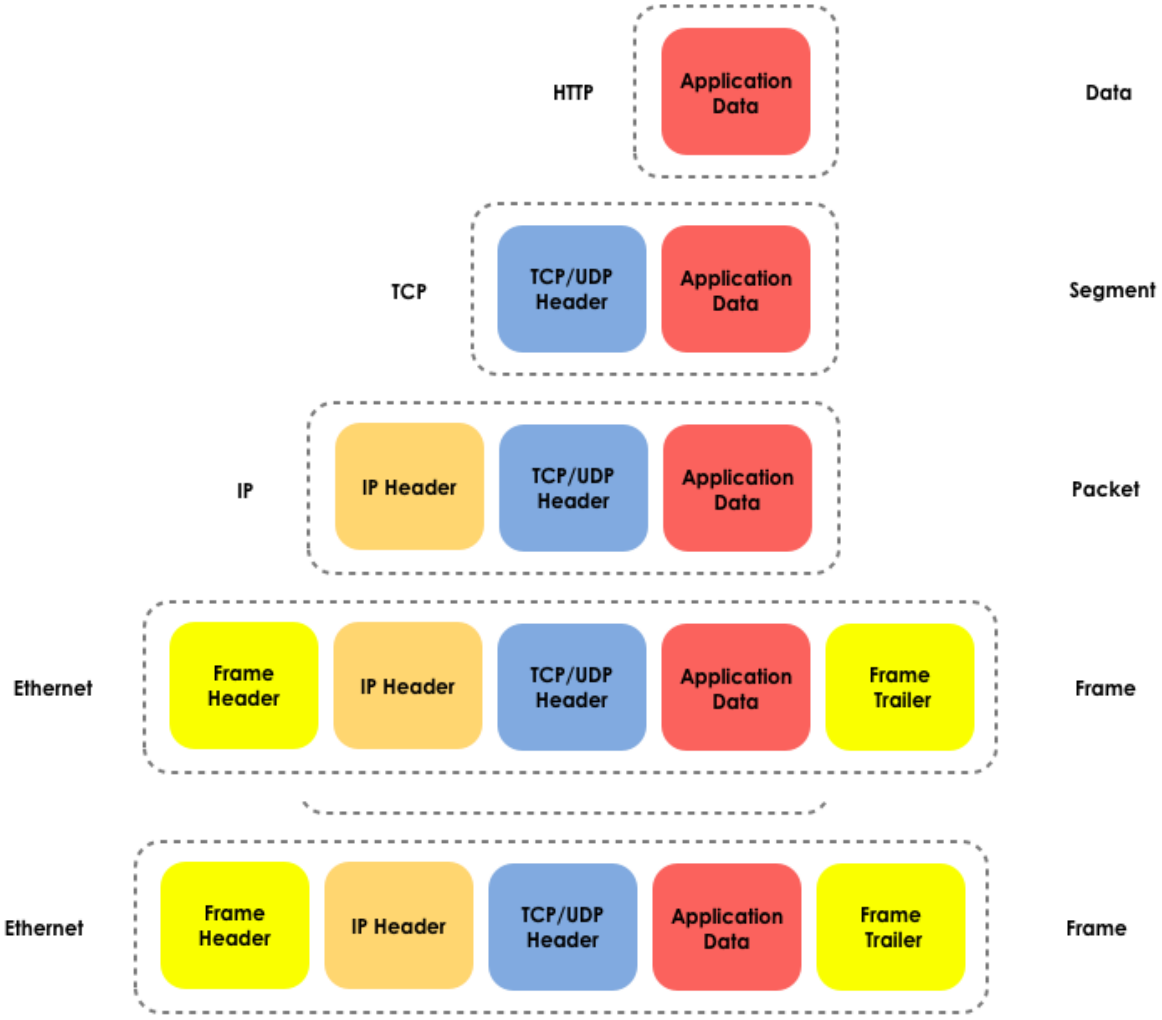


Figure 3.6: Encapsulation

Lorsque les informations encapsulées arrivent à leur destination, elles doivent subir l'opération inverse: la décapsulation. Pendant que chaque couche passe les informations à la couche suivante qui se trouve immédiatement au-dessus d'elle dans la pile de protocoles, elle supprime les informations contenus dans l'en-tête provenant de cette couche inférieure.

Le dernier bit d'informations qui se trouve dans cet énorme plan d'adressage est la seule et unique adresse de la carte réseau de l'ordinateur: l'**adresses MAC (Media Access Control).** Cette adresse est habituellement affichée sous-forme de six couples de caractères, des nombres **hexadécimaux** séparés par le caractère deux points "**:**" ou le caractère tiret "**-**". C'est l'adresse physique de la carte réseau et qui n'est pas censée être changée (en effet, il existe des moyens pour la changer, mais comment pouvez-vous réellement la découvrir). Une adresse MAC ressemble à ceci:

00-15-00-06-E6-BF

Exercises

3.1. En vous servant des commandes que vous avez apprises dans les leçons 1 et 2, obtenez votre adresse IP, votre masque de sous-réseau, votre nom d'hôte DNS, et votre adresse MAC. Comparez vos résultats à ceux obtenus par vos partenaires. Qu'est ce qui semble similaire et qu'est ce qui diffère ? Ayant obtenu la plage d'adresse IP que le réseau utilise, est-ce un adressage privé ou publique ?

3.2. netstat

La commande **netstat** vous donne des statistiques sur l'état du réseau: avec qui êtes-vous connectés, depuis combien de temps le réseau est-il actif, et ainsi de suite. Sous Linux, Windows, ou OSX vous pouvez accéder à la ligne de commande et tapez:

```
netstat
```

Dans la fenêtre de l'Invite de Commande, vous verrez une liste de connexions établies. Si vous voulez voir les connexions s'afficher sous forme numérique, tapez:

```
netstat -n
```

Pour voir les connexions actives et les ports actifs (en écoute, ouverts), tapez:

```
netstat -an
```

Pour voir une liste d'autres options de la commande, tapez:

```
netstat -h
```

Dans l'affichage de la commande netstat, retrouver les colonnes qui affichent les adresses IP locales et distantes et les ports qu'elle utilisent:

```
Proto Recv-Q Send-Q  Local Address        Foreign Address     (state)
tcp4     0      0  192.168.2.136.1043  66.220.149.94.443   ESTABLISHED
```

Les numéros de port sont les nombres qui se trouvent après les adresses IP normales ; il se peut qu'ils soient séparés par des points ou des "deux point". Pourquoi les numéros de port utilisés par l'adresse distante diffèrent des numéros de port utilisés par l'adresse locale ?

Ouvrez plusieurs fenêtres ou onglets d'un navigateur vers différents sites web, ensuite exécuter la commande `netstat` de nouveau.

Lorsqu'il y a plusieurs onglets ouverts, comment le navigateur sait-il quelle information va à tel onglet ?

Pourquoi n'y a t-il aucun ports spécifié, lorsqu'un navigateur web est utilisé ?

Quels sont les protocoles qui sont utilisés ?

Que se passe t-il lorsqu'un protocole est utilisé plus d'une fois ?

3.3. Mon Premier Serveur

Pour faire cet exercice, vous devez avoir le programme **netcat** (**nc**, **netcat** ou **ncat** à la ligne de commandes). BackTrack Linux possède déjà ce programme préinstallé par

défaut, ainsi que OSX, mais vous pouvez télécharger une version exécutable pour d'autres systèmes d'exploitation.

1. Dans un fenêtre d'invite de commandes, tapez:

```
nc -h
```

```
[rappelez-vous qu'il se peut vous ayez besoin de remplacer
cette commande par "ncat" ou "netcat"]
```

Ceci affiche les options disponibles pour le programme netcat.

Pour créer un simple serveur, sous Linux ou Windows tapez:

```
nc -l -p 1234
```

ou sous OSX tapez:

```
nc -l 1234
```

Vous venez juste de démarrez un serveur qui écoute sur le port 1234

1. Ouvrez une seconde fenêtre d'invite de commandes et tapez:

```
netstat -a
```

Ceci devrait vérifier s'il y a un nouveau service qui écoute sur le port 1234.

Pour communiquer avec un serveur, vous devez avoir un client ! Dans votre seconde fenêtre d'Invite de commandes, tapez:

```
nc localhost 1234
```

Cette commande établit une commande avec le serveur qui écoute sur le port 1234. Maintenant tout ce qui est saisi dans l'une des deux fenêtres ouvertes peut être vue dans l'autre fenêtre.

En considérant ces implications, comment quelqu'un peut-il abuser de la capacité de ce programme pour exploiter (pirater) votre machine ?

Netcat envoie tous ces trafics en texte clair. Y a t-il une alternative sécurisée ?

2. Arrêtez votre serveur en retournant à la fenêtre d'invite de commandes et en tapant `Control-C`.

3. Maintenant créer un simple fichier texte nommé ***`test`*** contenant le texte, "Bienvenue sur mon serveur!"

Une fois cela fait, observez la commande suivante et expliquez la à l'instructeur: que fait chaque partie ? Ensuite, dans votre première fenêtre d'Invite de commandes, tapez:

```
nc -l -p 1234 < test
```

A partir d'une autre fenêtre d'Invite de Commandes, connectez-vous au serveur en tapant:

```
nc localhost 1234
```

Lorsque le client se connecte au serveur, vous devriez voir le contenu du fichier ***test***.

Quel est le protocole qui a été utilisé pour la connexion avec le serveur ?

Netcat vous permet-il de changer cela ? Si oui, comment ?

Etoffez Vos Connaissances: Le Modèle OSI

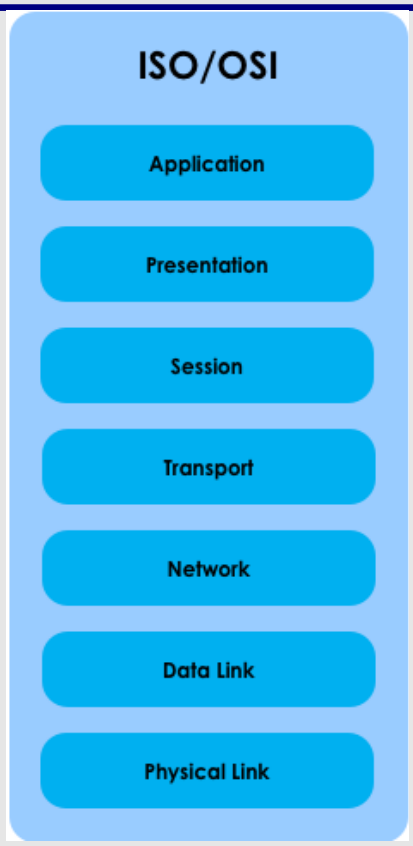


Figure 3.7: Le Modèle ISO/OSI

Le modèle OSI fut développé dans les années 1980 (à peu prêt 10 ans après le modèle TCP/IP) par l'organisme ISO (International Standards Organization). OSI signifie **Open Systems Interconnection**, et c'était une tentative de standardisation des architectures réseau venant d'une organisation qui n'était pas du tout impliquée dans le développement des réseau.

Le modèle OSI est un modèle en couches muni d'une poignée de règles simples. Des fonctions similaires sont regroupées au sein d'une même couche, et (n'oubliez pas ceci) chaque couche est servie par la couche qui se trouve en **dessous** d'elle, et sert la couche qui se trouve immédiatement **au-dessus** d'elle.

Ce modèle en couches est une bonne idée, parce qu'étant donné que chaque couche (en théorie) gère ses propres communications, de nouveaux développements au sein d'une autre n'impactent par sur les autres. Cette propriété seule peut expliquer

le boom d'Internet que nous avons eu depuis 2000, avec l'apparition de nouvelles applications et services presque tous les jours.

À part les deux règles du modèle OSI dont nous avons déjà parlé (des fonctions similaires sont regroupées, et chaque couche est servie par la couche en-dessous d'elle et elle même sert la couche qui est au-dessus d'elle) ce standard possède une autre règle plus stricte. Chaque couche impliquée dans une communication partant d'un ordinateur, communique directement avec la même couche sur l'autre ordinateur. Cela veut dire que lorsque vous saisissez www.google.com dans votre navigateur, il y a une interaction directe entre l'interface de la couche 7 (votre navigateur web) et les serveurs web de google.com (qui est aussi une interface de la couche 7) , et la même chose peut être dite d'une autre couche.

Donc définissons d'abord ce que sont les couches du modèle OSI et quelles sont leurs fonctions respectives:

Couche Application	Elle est responsable de l'interaction directe entre les applications et l'interface utilisateur de l'application, par exemple l'utilisation d'un navigateur web comme Internet Explorer ou Firefox.
Couche Présentation	Elle s'assure que l'échange de données est faite d'une manière compréhensible par les deux parties. Dans certains services qui utilisent des formes de cryptage, le cryptage a lieu à la couche présentation
Couche Session	Elle est responsable du contrôle du dialogue entre les ordinateurs. Essentiellement, elle établie, gère et rompt les connexions entre les ordinateurs.
Couche Transport	Fournit un transfert transparent de données entre les ordinateurs, en offrant un service de transfert de données fiable aux couches supérieures. Cela veut dire qu'elle est responsable de la fragmentation et du ré-assemblage des petites portions de données qui peuvent être transportées de manière fiable sur un réseau de données. Si un paquet est perdu ou n'est pas reçu, c'est le rôle de la couche transport de s'assurer de la retransmission du seul paquet et du ré-assemblage dans l'ordre correcte.
Couche Réseau	Elle est responsable de l'adressage logique dans les connexions. Elle n'assure pas seulement l'*unicité* de chaque adresse sur le réseau, mais elle s'assure aussi des chemins qui sont disponibles (qu'ils soient bon ou mauvais), et elle envoie toujours les informations à leur destination exacte, et ces informations qui sont les nôtres, seront envoyées de bout en bout jusqu'à ce qu'elles n'arrivent à destination.
Couche Liaison de Données	Cette couche était conçu pour s'assurer que la couche physique pourra toujours fonctionner après qu'il y ait eu une erreur et qu'elle communiquer avec des différents types de support de transmission. Fondamentalement elle prépare (encapsule) les données pour qu'elles puissent être transmises via n'importe quel support physique (ondes radio, câble à fibre-optique, cuivre).

Couche Physique	Elle définie les propriétés physiques des équipements et tout ce qui doit être fait pour que les informations soient transmises via le support choisi. Pour les connexion Wi-Fi, cette couche est représentée par le signal radio ; pour une connexion fibre optique c'est la lumière émise ; ou pour la connexion via le cuivre, c'est le signal électronique qui est envoyé sur le fil.

Ces sept couches comprennent tout ce qui est nécessaire pour une communication fiable entre les ordinateurs.

Voici ce à quoi ressemblent les différents modèles dont nous avons parlés, lorsqu'ils sont placés côte à côte:

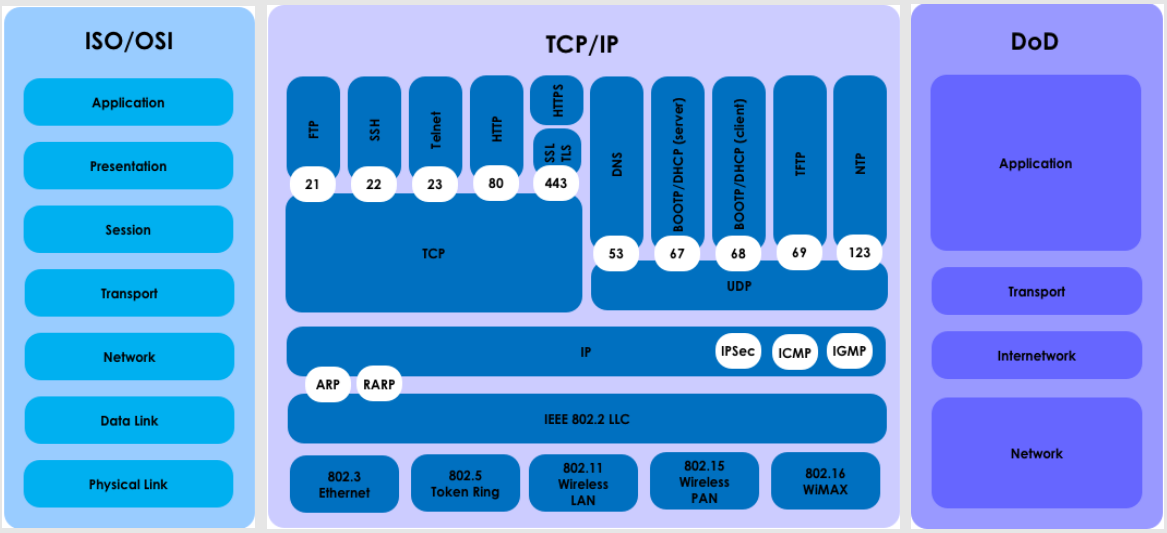


Figure 3.8: Comparaison des Modèles Réseau

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