Chapitre 5 : services réseau et sécurité

1- Le protocole HTTP

HTTP: est un protocole de communication pour le transfert de documents. Ce protocole est inclut dans la couche application du modèle OSI. La communication se fait entre un client (machine envoyant des requêtes) et un serveur (machine répondant à ces requêtes). Ce protocole est utilisé par les serveurs Web hébergeant des sites internet, dans le but de permettre de télécharger des documents ainsi que la consultation de pages sur l'écran du client.

Exemple :

Soit la requête suivante:

http://hypothetical.ora.com/

Ce qui provoque l'envoie du message suivant par le navigateur:

GET/HTTP/1.0

Connection: KeepAlive

User-Agent: Mozilla/3.0Gold(WinNT;I)

Host: hypothetical.ora.com

Aspect: image/gif, image/x-x bitmap, image/jpeg, text/html

Le serveur répond au navigateur par le message suivant:

HTTP/1.0200 OK

Date: Fri, 04 Oct 2002 10:38:29 GMT

Server: Apache/1.1.1

Content-type: text/html

Content-length: 327

Last-Modified: Fri, 04 Oct 2002 09:28:12 GMT

<title>une page web</title>

……

La liaison entre le client et le serveur n'est pas toujours directe, il peut exister des machines intermédiaires servant de relais :

Un proxy (ou serveur mandataire) : est une fonction informatique client-serveur qui a pour fonction de relayer des requêtes entre une fonction cliente et une fonction serveur, il peut modifier les réponses et requêtes qu'il reçoit et peut gérer un cache des ressources demandées.

Les serveurs proxys sont notamment utilisés pour assurer les fonctions suivantes :

-accélération de la navigation : mémoire cache, compression de données, filtrage des publicités ou des contenus lourds (Java, Flash) ;

-la journalisation des requêtes (historique) ;

-la sécurité du réseau local ;

-le filtrage et l'anonymat.

Une passerelle (ou gateway) : est un dispositif permettant de relier deux réseaux informatiques de types différents, par exemple un réseau local et le réseau Internet. Il peut modifier le protocole utilisé.

Un tunnel : est une encapsulation de données d'un protocole réseau dans un autre, situé dans la même couche du modèle en couches, ou dans une couche de niveau supérieur. Il transmet les requêtes et les réponses sans aucune modification, ni mise en cache.

2- Messagerie électronique (Le courrier électronique)

Le courrier électronique, courriel, e-mail, mail est un service de transmission de messages écrits et de documents envoyés électroniquement via le réseau Internet dans la boîte aux lettres électronique d'un destinataire choisi par l'émetteur.

Pour émettre et recevoir des messages par courrier électronique, il faut disposer d'une adresse électronique (adresse courriel ou adresse e-mail) et d'un client de messagerie (logiciel de messagerie qui sert à lire et envoyer des courriers électroniques) ou d'un webmail (Gmail, Yahoo…) permettant l'accès aux messages via un navigateur Web.

L'acheminement des courriels est régi par plusieurs protocoles :

-L'envoi des les courriers électroniques est réalisé par le protocole **SMTP** (Simple Mail Transfer Protocol, couche application).

-La récupération des courriers électroniques est faite par le protocole **POP** (Post Office Protocol, couche application) ou le protocole **IMAP** (Internet Message Access Protocol, couche application).

- Les messages sont aiguillés grâce au DNS (Domain Name System, couche application), par exemple du domaine .fr au domaine .com.

La différence entre IMAP et POP :

Le POP est un protocole unidirectionnel qui permet de télécharger votre courrier depuis un serveur distant vers votre poste de travail et supprime les messages du serveur distant. Par contre, l'IMAP est et est un protocole bidirectionnel plus moderne que POP qui copie votre courrier d'un serveur distant vers votre poste de travail, tout en gardant la copie originale du courrier sur le serveur distant. Les modifications apportées à ces messages électroniques, telles que les marquer comme lus, leur ajouter ou supprimer des étiquettes, ou bien les déplacer vers un dossier différent, vont être répliquées sur le serveur distant.

3- Transfert de fichier

Le transfert de fichier peut se faire d'ordinateur à périphérique, de serveur à serveur, de client à serveur, ou de client à client par l'intermédiaire d'un serveur de messagerie électronique.

Le transfert de fichier via un réseau informatique se fait à l'aide de protocoles. Parmi ces protocole on trouve le FTP (File Transfer Protocol), qui est un protocole spécifique pour le partage de fichiers, ou encore le FTPS (File Transfer Protocol Secure) qui est variante du FTP, sécurisé avec les protocoles SSL (Secure Sockets Layer) ou TLS (Transport Layer Security).

Le protocole FTP appartient à la couche application du modèle OSI et utilise une connexion TCP.

Pour accéder à un serveur FTP, on utilise un logiciel (client FTP). Ces logiciels existent avec ligne de commande ou avec une interface graphique. Le standard FTP est inclus avec les dernières distributions Windows & Linux.

4- Téléphonie sur IP

Définition : Téléphonie sur IP permettant de transmettre de la voix sur un réseau numérique et sur Internet.

Avantages de la téléphonie sur IP :

Flexibilité : la téléphonie sur IP est conçue pour assumer une stratégie de migration à faible risque à partir d'infrastructure existante.

Réduction des coûts : La téléphonie sur IP exploite un réseau de données IP pour offrir des communications vocales sur un réseau unique de voix et données. Cette convergence s'accompagne des avantages liés à la réduction des coûts d'investissement. La diminution des coûts est donc perçue non seulement sur les frais de communication, mais Egalement sur les dépenses opérationnelles.

L'accessibilité : Les utilisateurs accèdent à tous les services du réseau partout où ils peuvent s'y connecter.

Inconvénients de la téléphonie sur IP :

-Fiabilité et qualité : il se peut que des paquets soient perdus pendant la conversation. De plus, La qualité de la retransmission n'est pas encore optimale.

-Technologie émergente et constante évolution des normes

Protocoles de la téléphonie sur IP :

Il existe différents protocoles qui peuvent être utilisés pour implémenter de la téléphonie IP:

-Session Initiation Protocol (SIP) : est un protocole de communication de la couche application du modèle OSI, son fonction est la gestion de sessions souvent utilisé dans les télécommunications multimédia (son, image, etc.). Il est depuis 2007 le plus courant pour la téléphonie par internet (la VoIP).

-H.323 : Le H.323 est, comme le SIP, un protocole conçu pour l'activation, la gestion et la terminaison d'une session média. Le H.323 est un protocole assez ancien qui se fait remplacer actuellement par le SIP.

-Real-time Transport Protocol (RTP)

-Real-Time Transport Control Protocol (RTCP)

-Secure Real-time Transport Protocol (SRTP) : Le SRTP aussi connu sous le nom de Secure Real – Time Transport Protocol, est une extension d'un profil de RTP (Real-Time Transport Protocol) qui ajoute davantage de fonctions de sécurité, comme le message d'authentification et la confidentialité.

-Session Description Protocol (SDP) : le SDP définit un standard qui décrit les paramètres pour l'échange de média (souvent média en streaming) entre deux points.

5- vidéo sur IP

Le streaming consiste à diffuser une vidéo d'un serveur vers un client à travers un réseau de type internet (protocole IP). Le serveur segmente la vidéo en paquets susceptibles d'être diffusés sur le réseau. Ces paquets sont ensuite assemblés par le client afin de reconstituer la vidéo. A la différence d'un simple transfert de fichier, la vidéo est jouée au fur et à mesure que les paquets arrivent. Ces paquets sont ensuite détruits.

Il existe actuellement 3 protocoles qui permettent de faire du streaming :

-Les deux premiers, HTTP et FTP, sont des protocoles de transfert de fichier. On peut néanmoins parler de streaming dans la mesure où les vidéos peuvent être affichées au fur et à mesure du téléchargement.

-Le troisième protocole, RTP (Real Time Protocol), est celui qui permet de faire à proprement parler du streaming, c'est à dire de la diffusion de contenu en temps réel.

6- Qualité de service QoS

La Qualité de Service (QoS) : est la capacité à véhiculer dans de bonnes conditions un type de trafic donné.

Critères de la QoS :

Les principaux critères permettant d'apprécier la qualité de service sont les suivants :

-Débit (bandwidth): parfois appelé bande passante, il définit le volume maximal d'information (bits) par unité de temps (b/s).

-Perte de paquet (packet loss): elle correspond à la non-délivrance d'un paquet de données, la plupart du temps due à un encombrement du réseau.

-Gigue (jitter) : C'est le délai entre la transmission de bout en bout de deux paquets de donnés dans un même flux. C'est un paramètre important pour les applications communicantes de type voix ou vidéo où la gigue doit être la plus faible possible.

-Latence (delay) : elle caractérise le retard entre l'émission et la réception d'un paquet.

Les techniques pratiques impliquées dans la qualité de service :

Il existe plusieurs techniques que les entreprises peuvent utiliser pour garantir la haute performance de leurs applications les plus critiques. Ceux-ci inclus:

-**Priorisation du trafic VoIP sensible au délai via les routeurs et les commutateurs.**

-Réservation de ressources : le protocole de réservation de ressources (RSVP) est un protocole de couche de transport qui réserve des ressources sur un réseau et peut être utilisé pour fournir des niveaux spécifiques de QoS pour les flux de données d'application. La réservation de ressources permet aux entreprises de diviser les ressources réseau par trafic de différents types et origines, de définir des limites et de garantir la bande passante.

-Mise en file d'attente : les files d'attente sont des mémoires tampons de hautes performances dans les routeurs et les commutateurs, dans lesquelles les paquets transitant sont conservés dans des zones de mémoire dédiées suivant leurs priorités.

-Marquage du trafic : lorsque un trafic de données nécessitant une priorité de bande passante élevée sur le réseau, le trafic doit être marqué. Cela est possible grâce à des processus tels que :

*__Class of Service (CoS) ;__ qui marque un flux de données dans l'en-tête de trame de couche 2 (Liaison de données).

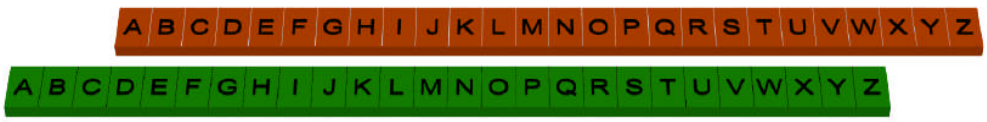
*__Differentiated Services Code Point (DSCP) :__ qui marque un flux de données dans l'en-tête de paquet de couche 3 (Réseau).

7- Cryptage et Chiffrement

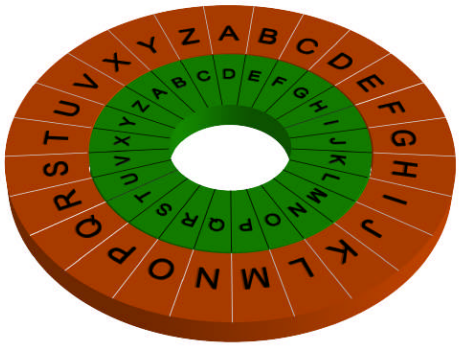
Le chiffrement ou cryptage : est rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement.

Le chiffrement de César :

Le chiffrement de César est un décalage des lettres : pour crypter un message, A devient D, B devient E, C devient F ,...



Pour prendre en compte les dernières lettres de l'alphabet, on peut représenter l'alphabet sur un anneau. Ce décalage est un décalage circulaire sur les lettres de l'alphabet.



Il est plus facile de manipuler des nombres que des lettres. Nous associons à chacune des 26 lettres de A à Z un nombre de 0 à 25 :

$$f : \{A, B, C, \ldots, Z\} \longrightarrow \{0, 1, 2, \ldots, 25\}$$

$$A \longmapsto 0 \quad B \longmapsto 1 \quad C \longmapsto 2 \quad \ldots \quad Z \longmapsto 25$$

Modulo :

On dit que a est congru à b modulo n, si n divise b-a. On note alors a≡b (mod n).

Pour n=25 (26 lettres)

Par exemple : 28≡2 (mod 26) car 28-2=26 et 26 est divisible par 26

85=26*3+7 donc 85≡7 (mod 26)

On note Z/26Z l'ensemble de tous les éléments de Z modulo 26. Cet ensemble peut par exemple être représenté par les 26 éléments 0, 1, 2, . . . , 25. En effet, puisqu'on compte modulo 26 :

0, 1, 2, . . . , 25, puis 26≡0, 27≡1, 28≡2, . . . , 52≡0, 53≡1, . . .

et de même -1≡25, -2≡24,...

Chiffrer et déchiffrer :

Le chiffrement de César est simplement une addition dans Z/26Z . Fixons un entier k qui est le décalage (par exemple k = 3 dans l'exemple de César ci-dessus) et la fonction de chiffrement de César de décalage k est :

$$C_k : \begin{cases} \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ x & \longmapsto & x+k \end{cases}$$

Par exemple, pour k = 3 : $C_3(0) = 3$, $C_3(1) = 4$. . .

Pour déchiffrer, Il suffit d'aller dans l'autre sens, c'est-à-dire ici de soustraire. La fonction de déchiffrement de César de décalage k est :

$$D_k : \begin{cases} \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ x & \longmapsto & x-k \end{cases}$$

Exemple :

Le message original est « STLC »

La clé secrète k, par exemple k = 11

A	B	C	D	E	F	G	H	I
1	2	3	4	5	6	7	8	9
J	K	L	M	N	O	P	Q	R
10	11	12	13	14	15	16	17	18
S	T	U	V	W	X	Y	Z	
19	20	21	22	23	24	25	26	

Le message chiffré est :

S≡19 →19+11=30→30=26+4→30≡4 (mod26)→S≡D

T≡20→20+11=31→31=26+5→30≡5 (mod26)→T≡E

L≡12→12+11=23→L≡W

C≡3→3+11=14→C≡N

Donc le message chiffré est : DEWN

Déchiffrement : DEWN

D≡4→4-11=-7→-7=-26+19→-7≡19 (mod26)→D≡S

E≡5→5-11=-6→-6=-26+20→-6≡20 (mod26)→E≡T

W≡23→23-11=12→W≡L

N≡14→14-11=3→N≡C

Donc le message déchiffré est : STLC

Remarque : le chiffrement de César présente une sécurité très faible, car l'espace des clés est trop petit : il y a seulement 26 clés possibles, et on peut attaquer un message chiffré en testant toutes les clés à la main.

8- Watermarking (Tatouage)

Définition : Le tatouage numérique est une technique qui consiste à insérer des informations numériques (marque ou signature) de manière imperceptible dans le corps d'un autre document numérique.

Types de tatouages :

-Visibles : altèrent le signal ou le fichier par exemple ajout d'une image pour en marquer une autre.

-Invisibles : modifient le signal d'une manière imperceptible par l'utilisateur final (par exemple en ne modifiant que le bit le moins significatif de chaque octet). Le tatouage numérique invisible peut être considéré comme une forme de stéganographie (Définition : La stéganographie est une forme de dissimulation d'information dans le but de transmettre un message de manière inaperçue au sein d'un autre message), puisque l'utilisateur final ignore la présence du tatouage et donc de l'information cachée.

Domaines de tatouage :

-Domaine spatial : C'est la manière la plus simple d'insertion d'un watermark dans l'image originale. En général une signature est pondérée puis ajoutée à l'image hôte.

-Domaine transformé : Beaucoup d'approches, pour lesquelles des filigranes sont insérés dans le domaine transformé basé sur la transformée en cosinus discrète (DCT), la transformée de Fourier discrète (DFT), ou la transformée par ondelettes discrète (DWT).

-Domaine hybride : le principe est de mixer le domaine spatial et du domaine transformé.

Applications du tatouage numérique :

-Protection du copyright

-Empreinte digitale

-Contrôle de copie

9- La stéganographie

Voici quelques-uns des différents types de sécurité réseau:

-Les pare-feu : Un pare-feu est un appareil de protection du réseau qui surveille le trafic entrant et sortant et décide d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies.

Les pare-feu constituent la première ligne de défense des réseaux. Un pare-feu peut être un équipement physique, un logiciel ou une combinaison des deux.

-Sécurité du courrier électronique : Le chiffrement de la messagerie électronique consiste à chiffrer le contenu des messages électroniques afin de protéger les informations potentiellement sensibles contre la lecture par des personnes autres que les destinataires prévus.

-**Antivirus / Antimalware :** un antivirus est un programme qui a pour finalité de protéger la machine ou l'appareil sur lequel il est installé. Le protéger contre les logiciels malveillants. Comme le firewall ou pare-feu, l'antivirus est l'un des principaux dispositifs de sécurité pour garantir la protection des données de l'utilisateur et une navigation optimale sur le web. Ce logiciel élimine ou réduit le risque de cyberattaques sur l'ordinateur, le téléphone ou la tablette qui disposent d'un accès à Internet.

-Segmentation du réseau : La segmentation réseau est une approche qui consiste à diviser le réseau en plusieurs segments, ou sous-réseaux, opérant chacun comme un mini-réseau en soi. Elle permet aux administrateurs de contrôler le flux de trafic entre ces sous-réseaux. Les entreprises utilisent la segmentation pour améliorer la surveillance de leur environnement, augmenter les performances, détecter les problèmes techniques, mais aussi, et surtout, renforcer leur sécurité.

-Contrôle d'accès : Le contrôle d’accès réseau est une méthode permettant d’empêcher les utilisateurs et terminaux non autorisés d’accéder à un réseau privé.

-Sécurité des applications : décrit les mesures de sécurité au niveau des applications qui aident à empêcher le vol ou le détournement de données ou de code contenus dans les applications.

-Prévention des pertes de données : Est un terme de la sécurité de l'information qui fait référence à des techniques et des systèmes qui permettent d'identifier, de surveiller et protéger les données utilisé, les données en mouvement, et des données à la retraite à l'intérieur ou à l'extérieur de l'entreprise, dans le but de détecter et de prévenir l'utilisation non autorisée et la transmission d'informations confidentielles. La perte de données peut être causée par les cyber-attaques que les erreurs commises par inadvertance qui peuvent rendre des informations sensibles disponibles.

Pour prévenir et gérer les incidents liés à la perte de données en utilisant des mesures de sécurité standard telle que les pare-feu et des mesures de sécurité du système basées sur des algorithmes d'apprentissage automatique et le raisonnement temporel pour la détection d'un accès inhabituel aux données.

-**Détection de la prévention des intrusions :** La prévention d'intrusion consiste à détecter les intrusions puis à résoudre les incidents détectés. Ces mesures de sécurité sont disponibles sous la forme de systèmes de détection d'intrusion (IDS) et de systèmes de prévention d'intrusion (IPS). Ces systèmes sont intégrés à votre réseau afin de détecter les incidents potentiels et d'y mettre fin.

-**Sécurité sans fil : -**authentification (est le procédé permettant à une personne de s'identifier dans le but de se connecter à un réseau sans fil) et cryptage.

-filtrage des adresses MACs (Media Access Control, adresse physique, est un identifiant physique stocké dans une carte réseau).

- cache du SSID (SSID : Service Set Identifier, est tout simplement le nom d'un réseau WiFi)

-VPN : abréviation de « Virtual Private Network », est un outil performant pour accroître sa sécurité et son anonymat en ligne. Un VPN peut être défini comme un réseau virtuel par lequel transitent des données chiffrées. Celui-ci redirige vos données reçues et envoyées sur le net vers un serveur à distance. Ce dernier permet de cacher votre adresse IP et de rendre illisibles les informations qui circulent.