3iLACADEMY
</l'expertise numérique>

Services INTERNET
Support de cours

Présentations

Intervenant: Pierre FRANCOU

Administrateur systèmes: UNIX, LINUX et SOLARIS

Travaillant pour un centre informatique de la CNAM

Déroulement des 5 séances:

1h30 de théorie,

3h de pratique,

Un compte rendu de chaque TP sera envoyé par messagerie.

Evaluation: Devoir Surveillé (1h30) et TP évalué (3h).

Plan détaillé du module

1 Les reseaux :

- 1-1 Les topologies
- 1-2 Les types de réseaux
- 1-3 Les commandes réseau
- 1-4 Services d'interconnection
- 1-5 Services de gestion de fichiers

2 Internet :

- 2-1 Les protocoles
- 2-2 Les adresses IP
- 2-3 Les Ports
- 2-4 Serveurs web
- 2-5 Serveurs de messagerie

3 Hébergements :

- 3-1 Sécuriser un stockage
- 3-2 Serveurs SAMBA
- 3-3 Serveurs LAMP
- 3-4 DOCKER
- 3-5 Services "clé en main"

4 La sécurité informatique

- 4-1 Les utilisateurs
- 4-2 Le super-utilisateur
- 4-3 Gestion des permissions
- 4-4 Sécurisation de la connexion
- 4-5 Résolution de nom et LDAP
- 4-6 Affectation adresse IP

5 La sécurité en entreprise

- 5-1 Mise en œuvre
- 5-2 Validation
- 5-3 Détection
- 5-4 Reaction
- 5-5 Les serveurs PROXY
- 5-6 Les serveurs Pare-Feu
- 5-7 Les services de monitoring

Les réseaux

Le terme générique « **réseau** » définit un ensemble d'entités interconnectées les unes avec les autres.

Un réseau informatique peut servir plusieurs buts distincts :

- Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc.)
- La communication entre personnes (courrier électronique, discussion en direct, etc.)
- La communication entre processus (entre des ordinateurs industriels par exemple)
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau)

Les réseaux permettent aussi de standardiser les applications, on parle généralement de groupware pour qualifier les outils permettant à plusieurs personnes de travailler en réseau.

Les réseaux

1-1 Les topologies

Une **topologie en bus:** tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial.

Dans une **topologie en étoile**, les ordinateurs du réseau sont reliés à un système matériel central appelé **concentrateur.**

Dans un réseau possédant une **topologie en anneau**, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.

La **topologie hiérarchique:** le réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie.

Une **topologie maillée**, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons point à point.

Les réseaux

1-2 Les types de réseaux

Le **LAN** (Local Area Network) est un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie.

Deux modes de fonctionnement : **peer to peer** ou **client/serveur**.

Les **MAN** (*Metropolitan Area Network*) interconnectent plusieurs LAN géographiquement proches à des débits importants. Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits.

Un **WAN** (Wide Area Network ou réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons et peuvent être faibles.

Les réseaux

1-3 Les commandes réseaux

Une bonne connaissance du réseau utilisé est indispensable avant de configurer les interfaces d'un OS.

Notions d'interfaces, physique et logique.

Se prémunir des pannes.

Pour configurer, tester et valider un réseau, différentes commandes …

Les réseaux

1-4 Les services d'interconnexion

Telnet (terminal network ou telecommunication network, ou encore teletype network) est un protocole utilisé sur tout réseau TCP/IP.

Il permet de communiquer avec un serveur distant en échangeant des lignes de textes et en recevant des réponses également sous forme de texte.

Les réseaux

1-5 Les services de gestion des fichiers

File Transfer Protocol (protocole de transfert de fichier), ou FTP, est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP.

La variante de FTP protégée par les protocoles SSL ou TLS (SSL étant le prédécesseur de TLS) s'appelle FTPS.

Internet

Internet est un **réseau informatique mondial** constitué d'un ensemble de réseaux nationaux, régionaux et privés.

L'ensemble utilise un **même protocole** de communication : TCP/IP, (*Transmission Control Protocol / Internet Protocol*).

Internet propose trois types de services fondamentaux :

- le courrier électronique (**e-mail**) ;
- le Web (**World Wilde Web**) ;
- l'échange de fichiers par **FTP** (*File Transfer Protocol*).

Le réseau Internet sert également, et de plus en plus, aux communications téléphoniques et à la transmission de vidéos et d'audio en direct (**streaming**).

Internet

2-1 Les protocoles

Un **protocole** est une méthode standard qui permet la communication entre des processus, c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau.

Sur Internet, les protocoles utilisés font partie d'une suite de protocoles: **[tcpip.php3 TCP/IP]:**

Couche 2 et hors ip: ARP

Couche 3 Internet Protocole: IPV4 et IPV6

Couche 4 Protocoles IP: ICMP, TCP, UDP

Couche 7 Protocoles Applicatifs : FTP, HTTP, SMTP, Telnet

Les protocoles orientés connexion

Les protocoles non orientés connexion

Internet

2-2 Les adresses IP

Les adresses IP servent aux ordinateurs du réseau pour communiquer entre-eux, ainsi chaque ordinateur d'un réseau possède une adresse IP unique sur ce réseau. Elles sont composées de 4 nombres entiers entre 0 et 255 et notées sous la forme xxx.xxx.xxx.xxx.

l'ICANN (*Internet Corporation for Assigned Names and Numbers)* est chargée d'attribuer des adresses IP publiques.

L'adresse réseau: Lorsque l'on annule la partie host-id, par exemple *194.28.12.0.* Cette adresse ne peut être attribuée à aucun des ordinateurs du réseau.

L'adresse machine: la partie netid est annulée. Cette adresse représente la machine spécifiée par le host-ID qui se trouve sur le réseau courant.

L'adresse de diffusion: tous les bits de la partie host-id sont à 1. Il s'agit d'une adresse spécifique, permettant d'envoyer un message à toutes les machines situées sur le réseau spécifié par le *netID*.

L'adresse de rebouclage: 127.0.0.1 elle désigne la **machine locale** (*localhost*).

Internet

2-3 Les ports

Chaque application se voit attribuer une adresse unique sur la machine, codée sur 16 bits: **un port** (la combinaison *adresse IP + port* est alors une adresse unique au monde, elle est appelée socket). L'adresse IP sert donc à identifier de façon unique un ordinateur sur le réseau tandis que le numéro de port indique l'application à laquelle les données sont destinées.

Le processus qui consiste à pouvoir faire transiter sur une connexion des informations provenant de diverses applications s'appelle le **multiplexage**. De la même façon le fait d'arriver à mettre en parallèle le flux de données s'appelle le **démultiplexage**.

Il existe des milliers de ports, c'est pourquoi une assignation standard a été mise au point par l'**IANA** (*Internet Assigned Numbers Authority*), afin d'aider à la configuration des réseaux.

INTERNET

2-4 Les serveurs WEB

Un serveur Web est un serveur informatique utilisé pour publier des sites web sur Internet ou un intranet.

L'expression « serveur Web » désigne également le logiciel utilisé sur le serveur pour exécuter les requêtes HTTP, le protocole de communication employé sur le World Wide Web.

INTERNET

2-5 Les serveurs de messagerie

Un serveur de messagerie électronique est un logiciel serveur de courrier électronique.

Une messagerie web, webmail ou courriel web est une interface web rendant possible l'émission, la consultation et la manipulation de courriers électroniques directement sur le Web depuis un navigateur.

HEBERGEMENTS

Quelles sont les différentes solutions d'hébergement?

Comment sécuriser nos données?

HEBERGEMENTS
3-1 Sécuriser un stockage

Présentation du SAN.

Rappel sur les différentes catégories de RAID.

HEBERGEMENTS
3-2 Serveurs SAMBA

L’utilité des serveurs SAMBA.

Installation et pramétrage.

HEBERGEMENTS
3-3 Serveurs LAMP

L’utilité des serveurs LAMP:

Linux Apache MySQL PHP

HEBERGEMENTS
3-4 DOCKER

Que sont les dockers, et comment les utiliser?

HEBERGEMENTS
3-5 Clé en main

Quelques produits qui proposent des solutions WEB prêt à l'emploi:

- JOOMLA
- WORDPRESS

La sécurité informatique

Une fois prémuni du risque de panne sur le stockage des données, il faut que l'OS garantisse aussi leurs intégrité logique.

Les différents OS étant multi-utilisateurs, il faut garantir l'authenticité de la connexion, et l'étanchéité des informations.

Chaque utilisateur dispose de ses propres fichiers, dont il peut autoriser ou non l'accès aux autres utilisateurs. Il dispose d'un certain nombre de *droits (accès à* certains périphériques, etc).

Sécurité Informatique

4-1 Les utilisateurs

Chaque utilisateur humain du système doit disposer d'un *compte protégé par u*n mot de passe.

Le mot de passe peut être modifié par l'utilisateur aussi souvent qu'il le désire.

En UNIX, les utilisateurs sont référencés dans le fichier: /etc/passwd.

Il est caractérisé par son ID, son groupe, son répertoire de travail et le shell qu'il utilise.

Différentes commandes d'administration utilisateurs…

Sécurité Informatique

4-2 Le super-utilisateur

Afin de permettre l'administration du système, un utilisateur spécial, nommé: super utilisateur (ou root), est toujours considéré par le système comme propriétaire de tous les fichiers (et des processus).

La personne qui gère le système est normalement la seule à connaître son mot de passe. Lui seul peut ajouter de nouveaux utilisateurs au système.

Son numéro identifiant (*user id* ou *uid*) est 0, qui est traité particulièrement par le noyau dans les appels systèmes.

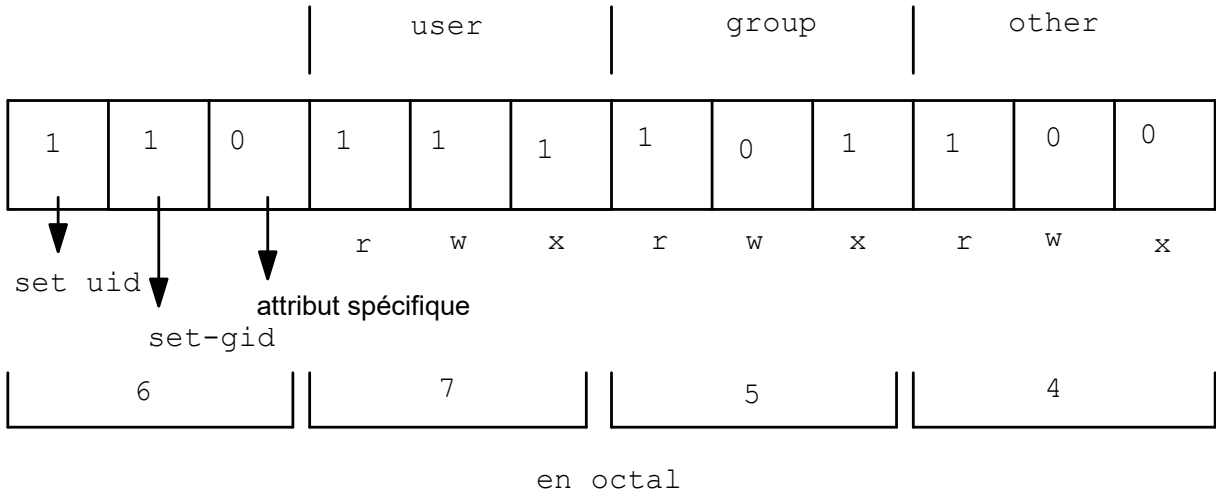
Le lancement d'applications courantes est fortement déconseillé en mode super-utilisateur, tout comme celui de l'interface graphique.

Sécurité Informatique

4-3 Gestion des permissions

Le propriétaire d'un fichier ou d'un répertoire, peut en gérer les permissions.

L'administration des permissions se veut donc assez fine pour interdire les accès sans en bloquer le travail.



Sécurité informatique

4-4 Sécurisation d'une connexion

Une ligne spécialisée (LS) appelée également liaison louée ou ligne louée est une liaison physique de niveau 2, connectée en permanence entre deux bâtiments distants.

Un réseau privé virtuel (Virtual Private Network), est un système permettant de créer un lien direct entre des ordinateurs distants.

Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé.

La sécurité informatique

4-5 La résolution de nom

DNS ou fichier HOSTS?

Il est possible d'associer des noms en langage courant aux adresses numériques grâce à un système appelé **DNS** (*Domain Name System*).

Aux origines les administrateurs réseau créaient des fichiers appelés *tables de conversion manuelle*, généralement nommés ***hosts***.

Installation et administration d'un serveur LDAP.

La sécurité informatique

4-6 Affectation adresse IP

DHCP ou STATIQUE?

Dynamic Host Configuration Protocol.

Modification de la config LINUX en STATIQUE

Sécurité en entreprise

$$\text{Risque} = \frac{\text{Menace x Vulnérabilité}}{\text{Contre-mesure}}$$

La **menace** représente le type d'action susceptible de nuire dans l'absolu.

la **vulnérabilité** représente le niveau d'exposition face à la menace dans un contexte particulier.

la **contre-mesure** est l'ensemble des actions mises en œuvre en prévention de la menace.

La sécurité informatique vise généralement cinq principaux objectifs :

- L'**intégrité:** garantir que les données sont bien celles que l'on croit être ;
- La **confidentialité:** les ressources ne sont pas intelligibles pour d'autres,
- La **disponibilité**, maintien le bon fonctionnement du système d'information ;
- La **non répudiation**, garanti qu'une transaction ne peut être niée ;
- L'**authentification** assurer que seules les personnes autorisées aient accès aux ressources.

Sécurité en entreprise

5-1 Mise en oeuvre

La phase de mise en œuvre consiste à **déployer des moyens** et des dispositifs visant à sécuriser le système d'information ainsi que de **faire appliquer les règles** définies dans la politique de sécurité.

Les principaux dispositifs permettant de sécuriser un réseau contre les intrusions sont les **systèmes pare-feu**.

Ainsi, la plupart du temps il est nécessaire de recourir à des applications implémentant des **algorithmes cryptographiques** permettant de garantir la confidentialité des échanges.

La mise en place de **tunnels sécurisés** (VPN) permet d'obtenir un niveau de sécurisation supplémentaire dans la mesure où l'ensemble de la communication est chiffrée.

Sécurité en entreprise

5-2 Validation

Un **audit de sécurité** consiste à s'appuyer sur un tiers de confiance (société spécialisée en sécurité informatique) afin de valider les moyens de protection mis en œuvre, au regard de la politique de sécurité.

Les **tests d'intrusion** (*pen tests*) consiste à éprouver les moyens de protection d'un système d'information en essayant de s'introduire dans le système en situation réelle.

2 méthodes: **Black Box** ou **White Box.**

Une telle démarche doit nécessairement être réalisé avec l'accord du plus haut niveau de la hiérarchie de l'entreprise: dégâts éventuels et méthodes mises en œuvre sont interdites par la loi.

Sécurité en entreprise

5-3 Détections

Afin d'être complètement fiable, un système d'information sécurisé doit disposer de mesures permettant de **détecter les incidents**.

Il existe ainsi des systèmes de détection d'intrusion (*IDS*) chargés de surveiller le réseau et capables de **déclencher une alerte** lorsqu'une requête est suspecte ou non conforme à la politique de sécurité.

La disposition de ces sondes et leur **paramétrage** doivent être soigneusement étudiés car ce type de dispositif est susceptible de générer de nombreuses fausses alertes.

Sécurité en entreprise

5-4 Réaction

La vitesse de réaction est primordiale car une compromission implique une mise en danger de tout le système d'information de l'entreprise. De plus, lorsque la compromission provoque un dysfonctionnement du service, un arrêt de longue durée peut être synonyme de pertes financières.

La remise en fonction du système compromis doit être finement décrit dans le plan de reprise après sinistre et doit prendre en compte les éléments suivants :

- **Datation de l'intrusion** ,
- **Confinement de la compromission** ,
- **Stratégie de sauvegarde** ,
- **Constitution de preuves**,
- **Mise en place d'un site de repli**,

Une mauvaise prise de décision peut-être plus nuisible que l'intrusion elle-même.

Sécurité en entreprise

5-5 Les serveurs PROXY

Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.

Dans l'environnement plus particulier des réseaux, un serveur proxy (ou « serveur mandataire », en français) est une fonction informatique client-serveur qui a pour fonction de relayer des requêtes entre une fonction cliente et une fonction serveur.

Sécurité en entreprise

5-6 Les serveurs Pare-Feu

Un pare-feu (de l'anglais firewall) est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique.

Il permet d'appliquer une politique d'accès aux ressources réseau.

Sécurité en entreprise

5-7 Les services de monitoring

Syslog est un protocole définissant un service de journaux d'événements d'un système informatique.

NAGIOS est un logiciel libre de supervision, qui permet de superviser et monitorer plusieurs Systèmes d’exploitations différents.

DYNATRACE calcul le ressenti des utilisateurs avec des sondes positionnées à différents points du réseau.