

Notions de sécurité des réseaux informatiques

ELABORÉ PAR : MOHAMED OUZANOU

ISTA MOHAMED EL FASSI ERRACHIDIA – MAI 2015

1. Les objectifs de la sécurité informatique :

- ☒ La confidentialité.
- ☒ L'intégrité.
- ☒ La disponibilité.
- ☒ L'authentification.
- ☒ La non-répudiation.

2. Exemples de menaces :

a) **Risque naturels** : par exemple (une intensité supérieure).

b) **Les virus** : Un virus est un petit programme informatique situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a programmé.

➤ **Notion d'antivirus** :

Un antivirus est un programme capable de détecter la présence de virus sur un ordinateur.

Il existe plusieurs méthodes d'éradication :

- La suppression du code correspondant au virus dans le fichier infecté.
- La suppression du fichier infecté.

➤ **Détection des virus** :

Les virus se reproduisent en infectant des « *applications hôtes* », c'est-à-dire en copiant une portion de code exécutable au sein d'un programme existant. Or, afin de ne pas avoir un fonctionnement chaotique, les virus sont programmés pour ne pas infecter plusieurs fois un même fichier. Ils intègrent ainsi dans l'application infectée une suite d'octets leur permettant de vérifier si le programme a préalablement été infecté : il s'agit de la **signature virale**.

Les antivirus s'appuient ainsi sur cette signature propre à chaque virus pour les détecter. Il s'agit de la méthode de **recherche de signature** (*scanning*), la plus ancienne méthode utilisée par les

antivirus.

Cette méthode n'est fiable que si l'antivirus possède une base virale à jour, c'est-à-dire comportant les signatures de tous les virus connus. Toutefois cette méthode ne permet pas la détection des virus n'ayant pas encore été répertoriés par les éditeurs d'antivirus. De plus, les programmeurs de virus les ont désormais dotés de capacités de camouflage, de manière à rendre leur signature difficile à détecter, voire indétectable : il s'agit de "**virus polymorphes**".

Certains antivirus utilisent un **contrôleur d'intégrité** pour vérifier si les fichiers ont été modifiés. Ainsi le contrôleur d'intégrité construit une base de données contenant des informations sur les fichiers exécutables du système (date de modification, taille et éventuellement une somme de contrôle). Ainsi, lorsqu'un fichier exécutable change de caractéristiques, l'antivirus prévient l'utilisateur de la machine.

La méthode heuristique consiste à analyser le comportement des applications afin de détecter une activité proche de celle d'un virus connu. Ce type d'antivirus peut ainsi détecter des virus même lorsque la base antivirale n'a pas été mise à jour. En contrepartie, ils sont susceptibles de déclencher de fausses alertes.

Types de virus :

- **Les vers** : ce sont des virus capables de se propager à travers un réseau.
- **Les chevaux de Troie (troyens)** : sont des virus permettant de créer une faille dans un système (généralement pour permettre à son concepteur de s'introduire dans le système infecté afin d'en prendre le contrôle).
- **Les bombes logiques** : sont des virus capables de se déclencher suite à un événement particulier (date système, activation distante, ...), Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise !

- **Les macros (trans-applicatifs) :** une macro est une série de commandes destinée à effectuer automatiquement quelques tâches d'une application spécifique.
- **Les virus de secteur d'amorce :** il s'agit d'un type de virus affectant la partie faisant démarrer de l'ordinateur.
- **Les virus fichiers :**
 - ↳ **Virus non résident :** lors de l'infection il cherche un fichier cible et remplace et remplace par sa section virale.
 - ↳ **Virus résident :** il s'agit de virus restent présent dans la mémoire de l'ordinateur.
- **Virus Multiformes :** virus qui regroupant les caractéristiques des virus parasites et des virus de secteur d'amorçage.
Les autres les caractéristiques des virus sont :
- **Virus furtifs (intercepteurs d'interruptions) :** ce sont des virus modifiant complètement le fonctionnement du système d'exploitation.
- **Virus Polymorphes (mutants) :** ce genre de virus est donc beaucoup plus difficile à détecter que les présidents presque impossibles à détruire sans supprimer le fichier infecté, vu qu'il est crypté.
- **Virus flibustiers (rétrovirus) :** virus permet de modifier les signatures des antivirus non-opérationnel.
- **Virus VBS script :** ce type de virus propage par mail à l'aide d'un fichier attaché (exe,vbs etc ...).
- **Les canulars (hoax):** c'est-à-dire des annonces reçue par mail (possibilité de gagner un téléphone portable gratuitement).

c) Spam :

Désigne les communications électroniques massives. Notamment de courrier électronique, Sans sollicitation des destititaires, à des fins publicitaires ou malhonnêtes.

Cibles du pourriel :

Le pourriel peut s'attaquer à divers media électroniques : les courriels, les forums de discussion, les moteur de recherche etc ...

- **Par courrier électroniques.**
- **Par des fenêtres pop-up de Windows.**

d) Spyware :

Spyware ou logiciel espion est un logiciel malveillant qui infecte un ordinateur dans le but de collecter et de transmettre sans que l'utilisateur n'en ait connaissance.



Fonctionnement :

Un logiciel espion est composé de trois mécanismes distincts :

- ❖ Le mécanisme d'infection.
- ❖ Le mécanisme assurant la collecte d'information.
- ❖ Le mécanisme assurant la transmission à un tiers. Ce mécanisme est généralement assuré via le réseau internet.

Quelques anti-spywares

Parmi les anti-spywares les plus connus ou efficaces citons notamment :

-  Ad-Aware de Lavasoft.de
-  Spybot Search&Destroy

I. Mesures pour la protection :

a. Cryptographie :

Est une des disciplines de la cryptologie, s'attachant à protéger des messages.

Vocabulaire :

Chiffrement et déchiffrement : le chiffrement et la transformation à l'aide d'une clé de chiffrement d'un message en clair en un message incompréhensible si on ne dispose pas d'une clé de déchiffrement.

Chiffre : anciennement code secret, par extension algorithme pour le chiffrement.

Cryptogramme : message chiffré.

Décrypter : retrouve le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement.

Cryptanalyse : science analysant les cryptogrammes en vue de le casser.

i. Algorithme de chiffrement faibles (cassable facilement).

Exemple :

- ✚ ROT13 (rotation de 13 caractères sans clé).
- ✚ Chiffre de Vigenère (chiffrement polyalphabétique).

ii. Algorithme de cryptographie symétrique (à clé secrète).

Les algorithmes de chiffrement symétrique se basent sur une même clé (ou presque) pour chiffrer et déchiffrer un message.

Quelques algorithmes symétriques les plus utilisés :

- ✚ DES (Data Encryption System).
- ✚ AES (Advanced Encryption System).
- ✚ RC4.

iii. Algorithme de cryptographie Asymétrique (à clé publique et privée).

Il se base sur le principe de deux clés :

- ✓ **Une publique**, permettant le chiffrement.
- ✓ **Une privée**, permettant le déchiffrement.

Quelques algorithmes asymétriques les plus utilisés :

- ✚ RSA (Rivest Shamir Adleman).
- ✚ DSA (Digital Signature algorithm).

iv. La signature électronique.

Aussi appelé la signature numérique, est un procédé permettant de garantir l'authenticité de l'expéditeur et de vérifier l'intégrité du message reçu. La signature électronique = hachage + clé privée.

Fonction de hachage :

Hachage est une fonction permettant d'obtenir un condensé (appelé aussi un condensat ou haché ou en anglais message digest), pour vérifier l'intégrité des données.

Les algorithmes de hachage le plus utilisés actuellement sont :

- MD5.
- SHA.

v. Les certificats :

Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé autorité de certification (souvent notée CA Certification Authority).

Les certificats sont des petits fichiers divisés en deux parties :

- ↳ La partie contenant les informations.
- ↳ La partie contenant la signature de l'autorité de certification.

b. Les Sauvegardes:

• **RAID (Redundant Array of Independent Disks):**

RAID permet de constituer une unité de stockage à partir de plusieurs disques durs.

Les solutions RAID généralement retenues sont le RAID de niveau 1 et 5.

Le choix d'une solution RAID est lié à trois critères :

- ❖ La sécurité.
- ❖ La performance.
- ❖ Le coût.

vi. SSL.

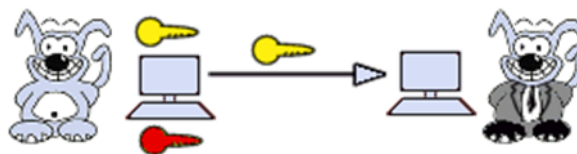
SSL (Secure socket layer) est un procédé des transactions effectuées via internet. Le système SSL est indépendant du protocole utilisé, ce qui signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que des connexions via le protocole FTP, POP ou IMAP. En effet, SSL agit telle une couche supplémentaire, permettant d'assurer la sécurité des données, située entre la couche application et la couche transport (protocole TCP par exemple).

Fonctionnement de SSL 2.0 :

La sécurisation des transactions par SSL 2.0 est basée sur un échange de clés entre client et serveur. La transaction sécurisée par SSL se fait selon le modèle suivant :

Dans un premier temps, le client se connecte au site marchand sécurisé par SSL et lui demande de s'authentifier. Le client envoie également la liste des cryptosystèmes qu'il supporte, triée par ordre décroissant selon la longueur des clés.

Le serveur à réception de la requête envoie un certificat au client, contenant la clé publique du serveur, signée par une autorité de certification (CA), ainsi que le nom du cryptosystème le plus haut dans la liste avec lequel il est compatible (la longueur de la clé de chiffrement - 40 bits ou 128 bits - sera celle du cryptosystème commun ayant la plus grande taille de clé).



Le client vérifie la validité du certificat (donc l'authenticité du marchand), puis crée une clé secrète aléatoire (plus exactement un bloc prétendument aléatoire), chiffre cette clé à l'aide de la clé publique du serveur, puis lui envoie le résultat (la clé de session). Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée. Ainsi, les deux entités sont en possession d'une clé commune dont ils sont seuls connaisseurs. Le reste des transactions peut se

faire à l'aide de clé de session, garantissant l'intégrité et la confidentialité des données échangées.

II. Protection contre les intrusions réseau.

a. Par feu (firewall) :

Introduction :

Un pare-feu est un composant matériel, logiciel ou les deux. Le pare-feu Internet a pour but d'empêcher les paquets IP malveillants ou non souhaités d'accéder à un réseau sécurisé.

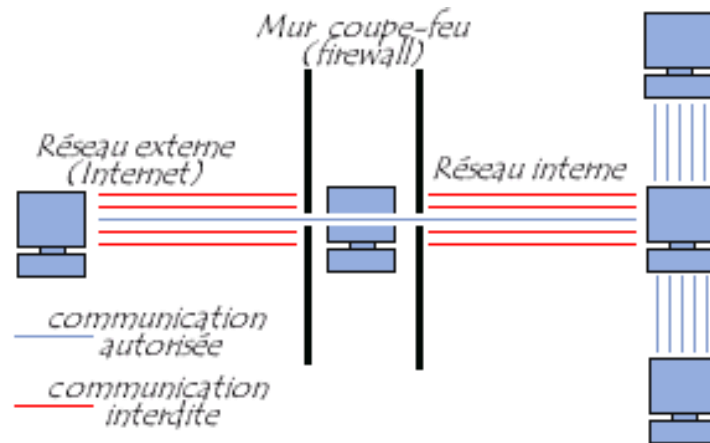
Chaque ordinateur connecté à internet (et d'une manière plus générale à n'importe quel réseau informatique) est susceptible d'être victime d'une attaque d'un pirate informatique. La méthodologie généralement employée par le pirate informatique consiste à scruter le réseau (en envoyant des paquets de données de manière aléatoire) à la recherche d'une machine connectée, puis à chercher une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant.

Un pare-feu est un composant matériel, logiciel ou les deux permettant de définir des règles d'accès entre un réseau local et un ou plusieurs réseaux externe.

Qu'est-ce qu'un pare-feu ?

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne) ;
- une interface pour le réseau externe.



Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

- La machine soit suffisamment puissante pour traiter le trafic ;
- Le système soit sécurisé ;
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

Fonctionnement :

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow) ;
- De bloquer la connexion (deny) ;
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- soit d'autoriser uniquement les communications ayant été explicitement autorisées :
- soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

Le filtrage de paquets.

Le filtrage applicatif.

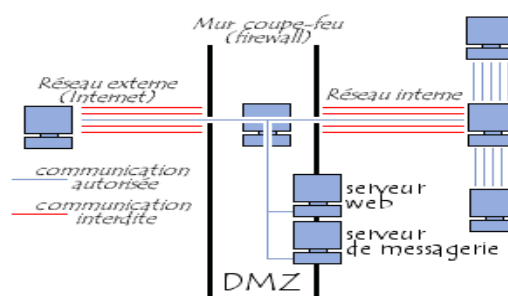
DMZ (Zone démilitarisée) :

- **Notion de cloisonnement :**

Les systèmes pare-feu (firewall) permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes. C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feu permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de « cloisonnement des réseaux » (le terme isolation est parfois également utilisé).

DMZ est une zone isolée qui contient des serveurs.

- **Architecture DMZ :**



Les serveurs situés dans la DMZ sont appelés « bastions » en raison de leur position d'avant-poste dans le réseau de l'entreprise.

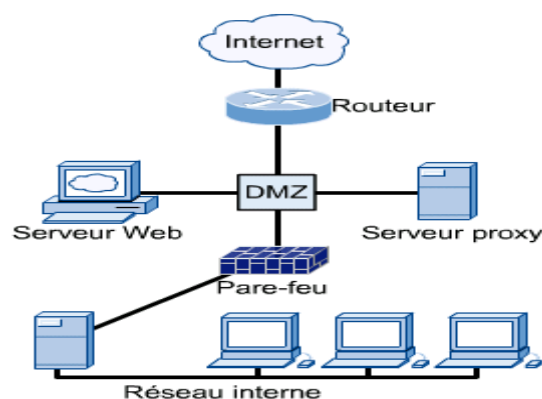
La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Traffic du réseau externe vers la DMZ autorisé ;
- Traffic du réseau externe vers le réseau interne interdit ;
- Traffic du réseau interne vers la DMZ autorisé ;
- Traffic du réseau interne vers le réseau externe autorisé ;
- Traffic de la DMZ vers le réseau interne interdit ;
- Traffic de la DMZ vers le réseau externe refusé.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise.

Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

- **Emplacement du pare-feu :**

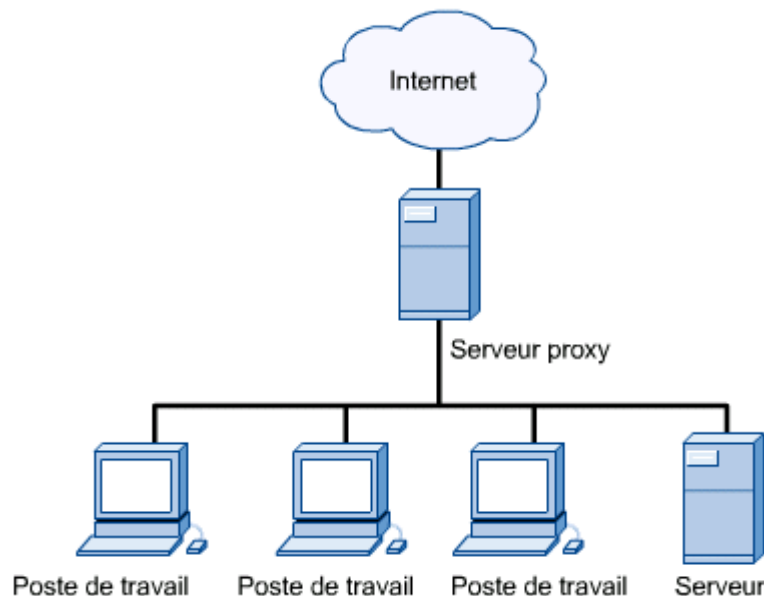


- **Utilisation d'un pare-feu :**

Un firewall est un logiciel contrôlant les échanges entre un réseau (local ou Internet) et votre ordinateur. Le pare-feu examine les données entrantes et les données sortantes de l'ordinateur.

b. Service Proxy :

Le serveur proxy est une machine fonction d'intermédiaire entre les ordinateurs d'un réseau local et l'internet.



Les fonctionnalités d'un serveur proxy :

La fonction de cache :

Cette fonctionnalité implémentée dans certains serveurs proxy permet de réduire l'utilisation de la bande passante vers internet ainsi que de réduire le temps d'accès aux documents pour les utilisateurs.

Reverse proxy :

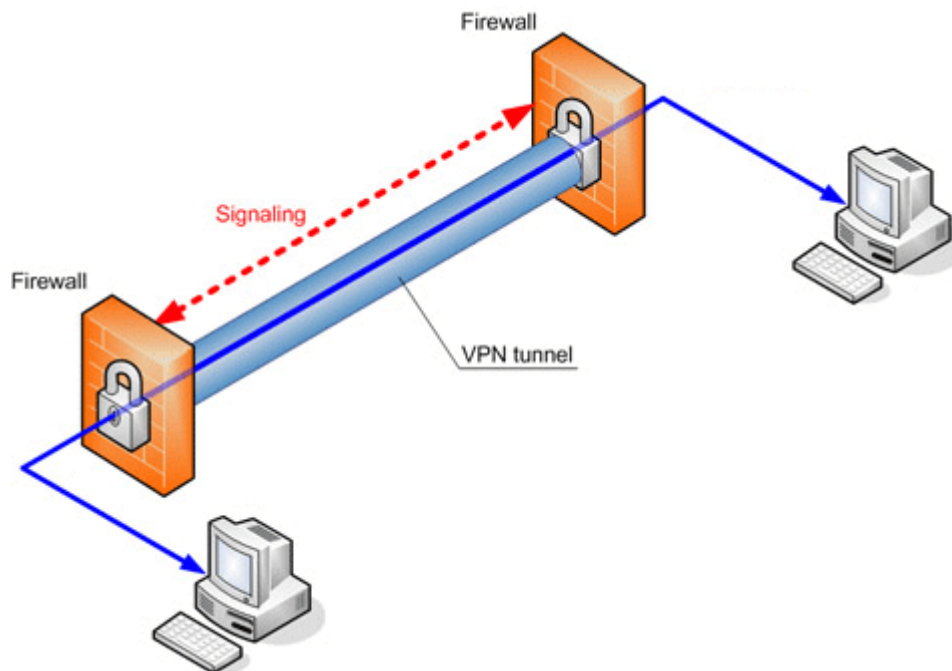
On appelle reverse-proxy un serveur proxy cache, c'est-à-dire un serveur proxy permettant non pas aux utilisateurs d'accéder au réseau internet, mais aux utilisateurs d'internet d'accéder indirectement à certains serveurs internes.

Le filtrage.

L'authentification.

c. VPN :

Un réseau privé virtuel repose sur un protocole appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.



Les protocoles de tunnelisation :

- IPSEC.
- PPTP
- L2F
- L2TP

Les avantages :

- Réduction des coûts.
- Evolutivité.
- Compatibilité avec la technologie haut débit.
- Sécurité.

Types de VPN :

- Site à Site.
- Accès à distance.

vii. Attaques informatiques.

Une « **attaque** » est l'exploitation d'une faille d'un système informatique.

Les motivations des attaques peuvent être :

- obtenir un accès au système ;
- voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- glâner des informations personnelles sur un utilisateur ;
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- troubler le bon fonctionnement d'un service ;
- utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

Un pirate (ou **Hacker**) est la personne qui fait des attaques.

Les différents types de pirates :

- Les « white hat hackers », hackers au sens noble du terme ;
- Les « black hat hackers », hackers au sens nuisible ;
- Les « script kiddies » sont de jeunes qui utilisent les scripts sur internet pour pirater leurs amis.
- Les « phreakers » sont des pirates s'intéressant au réseau téléphonique commuté (RTC) afin de téléphoner gratuitement ;
- Les « carders » s'attaquent principalement aux systèmes de cartes à puces (en particulier les cartes bancaires) ;
- Les « crackers » sont des personnes dont le but est de créer des outils logiciels permettant d'attaquer des systèmes informatiques ou de casser les protections contre la copie des logiciels payants ;
- Les « hacktivistes » sont des hackers dont la motivation est principalement idéologique.

Les types d'attaque :

- **Attaque directe :**

Le **hacker** attaque directement sa victime à partir de son ordinateur par des scripts d'attaques faiblement paramétrable. Les programmes de hack qu'ils utilisent envoient directement les packets à la victime. Dans ce cas, il est possible en général de remonter à l'origine de l'attaque, identifiant par la même occasion l'identité de l'attaquant.

- **Attaque indirecte par rebond:**

les attaques par rebond consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui (telle que son adresse IP) et dans le but d'utiliser les ressources de la machine servant de rebond.

- **Attaque indirecte par réponse:**

Elle offre les mêmes avantages, du point de vue du hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête.

Techniques d'attaque :

Attaque des mots de passe:

- Attaque par force brute est le cassage d'un mot de passe en testant tous les mots de passe possibles.
- Attaque par dictionnaire.
- Attaque hybride : Il s'agit d'une combinaison d'attaque par force brute et d'attaque par dictionnaire.

Attaque Man in the middle:

Est un attaque consiste à écouter une communication entre deux interlocuteurs à l'aide d'un outil appelé sniffer.

Attaque par rejeu:

Ce Sont des attaques de type « Man in the middle ».

Attaque par déni de service:

Est un type d'attaque visant à rendre indisponible pendant un temps indéterminé.

Le principe des attaques par déni de service consiste à envoyer des paquets IP ou des données de taille.

Attaque par déni de service (Smurf):

Est basé sur l'utilisation de serveur de diffusion, les serveurs de diffusion est capable de dupliquer un message et de l'envoyer à toutes les machines présentent sur le même réseau.

Attaque SYN :

Est une attaque réseau par saturant (déni de service) exploitant le mécanisme de poignée de main en trois temps du protocole TCP.

Spoofing IP :

Est une technique consiste à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.

Vol de session TCP (Hijacking) :

Est une technique consistant à intercepter une session TCP initiée entre deux machines a fin de la détourner.

Analyseurs réseau (Sniffers) :

Un sniffer est un outil formidable permettant d'étudié le trafic d'un réseau.

Scanners de vulnérabilités :

Scanner de vulnérabilité est une Outil permet de déterminer les risques en matière de sécurité.

Ingénierie Sociale :

Il s'agit d'une technique consistant à obtenir des informations.

L'ingénierie sociale peut prendre plusieurs formes :

- ❖ Par téléphone.
- ❖ Par courrier électronique.
- ❖ Par courrier écrit.
- ❖ Par messagerie instantanée ...

Phishing :

Est une technique utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires).

La technique phishing est une technique d'ingénierie sociale c'est-à-dire consistant à exploiter non pas une « faille informatique » mais la « faille humain ».

Attaque sur différents protocoles:

DHCP, DNS, FTP, http.

COBIT :

Cobit (contrôler les objectifs des technologies de l'information), est une méthode de maîtrise des systèmes d'information et d'audit de systèmes d'information. ainsi que une cadre de contrôle qui à aider le management à gères les risques (sécurité,fiabilité,conformité).

L'objectif de Cobit est de faire le lien entre les risques métiers.

Les outils : **Cobit quickstart**, **Cobit online**, **Cobit advisor**.

Mode de Sauvegarde :

- Sauvegardes en ligne.
- Sauvegarde hors ligne.

Topologie de sauvegarde :

- Sauvegarde et restauration par serveur local.
- Sauvegarde et restauration par réseau LAN.
- Sauvegarde et restauration sur SAN.

Types de sauvegarde :

- Sauvegardes intégrales.
- Sauvegardes incrémentielles.
- Sauvegardes différentielles.

Autre :

Une vulnérabilité : est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système.

Cookies : Un cookie une suite d'informations envoyée par un serveur HTTP à un client http.

Comment détecter les intrusions ?

On appelle IDS (Intrusion Detection System) un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion.

Il existe deux grandes familles distinctes d'IDS :

Les N-IDS (Network Based Intrusion Detection System), ils assurent la sécurité au niveau du réseau.

Les H-IDS (HostBased Intrusion Detection System), ils assurent la sécurité au niveau des hôtes.