Chapitre 1 : Principes de sécurité

1.1 Introduction :

Ce chapitre introduit les notions de base de la sécurité informatique : menace, risque, vulnérabilité, il effectue un premier parcours de l'ensemble des aspects humains et techniques ainsi que les parade et les mécanismes utilisés pour réduire le risque dans un système informatique.

Aspects techniques de la sécurité

Les problèmes techniques de la sécurité informatique peuvent être classés en deux grandes catégories :

1. Problème concernant la sécurité de l'ordinateur proprement dit, serveur, poste de travail, système d'exploitation et les données.
2. Problèmes qui découlent directement ou indirectement des réseaux

1.2 Malveillance informatique

- **Virus :** un virus est un logiciel capable de s'installer sur un ordinateur à l'insu de son utilisateur légitime. Le terme virus est réservé aux logiciels qui se comportent par un but malveillant,

- **Virus réticulaire (botnet) :** La cible d'un virus informatique peut être sous forme indirecte, ils se propagent silencieusement sur des millions d'ordinateurs connectés à internet sans y commettre le moindre dégât. Puis, à un signal donné ou à une heure fixée ces millions de programmes vont se connecter à même serveur web ce qui provoquera un déni de service. Un tel virus s'appelle un botnet. Les ordinateurs infectés par des botnets sont nommées zombis.

- **Ver :** Un ver (Worm) est une varité de virus qui se propage par le réseau. Il peut s'agir d'un bot

- **Cheval de Troie :** Un cheval de Troie (Trojan Horse) est un logiciel qui se présente sous une forme honnête, utile ou agréable, et qui une fois installé sur un ordinateur y effectue des actions pernicieuses.

- **Porte dérobée :** Une porte dérobée (backdoor) est un logiciel de communication caché, installé par exemple par un virus ou par un cheval de Troie qui donne à un intrus accès à l'ordinateur victime par le réseau.

- **Bombe logique :** Une bombe logique est une fonction cachée dans un programme en apparence honnête qui se déclenche lorsque une centaine date sera atteinte. Cette fonction produira des actions indésirées.
- **Logiciel espion :** Un logiciel espion comme son no l'indique. Collecte à l'insu d'n utilisateur légitime des informations au sein du système ou il est installé et les communiques à un agent extérieur, par exemple au moyen d'une porte dérobée.

- **Courrier électronique non sollicité (SPAM)**

  Le courrier électronique non sollicité (spam) consiste en communication électronique massives, notamment de courrier électronique sans sollicitation des destinataires à des fins publicitaires ou malhonnêtes

- **Injection SQL**

  L'attaque par injection SQL vise les sites Web qui proposent des transactions mal construites dont les résultats sont emmagasinés dans une base de données relationnelle. Elle consiste en SQL, un langage qui permet d'interroger et de mettre à jour une base de données relationnelle, les requêtes sont soumises au moteur de la base en format texte sans être compilées.

1.3 Menace, risque, vulnérabilité

La sécurité des systèmes d'information est un sujet très important

Risque = Menace x Vulnérabilité / Contre mesure

Risque – C'est la probabilité qu'une menace exploite une vulnérabilité. Autrement dit c'est une possibilité qu'un fait dommageable se produise.

Vulnérabilité – C'est une faiblesse inhérente à un système (software ou hardware) appelée parfois faille. Elle représente l niveau d'exposition face à la menace dans un contexte particulier.

Menace – C'est le danger (interne ou externe) te qu'un hacker, un virus ,,

Contre-mesure- c'est un moyen permettant de réduire le risque dans une organisation

1.5 Les Services de Sécurité

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. L'objectif de la sécurité informatique est d'assurer que les ressources matérielles et/ou logicielles d'un système informatique sont utilisées uniquement dans un cadre prévu et par des personnes autorisées.

Il convient d'identifier les exigences fondamentales en sécurité informatique qui caractérisent le besoin des utilisateurs d'un système informatique.

1) **Authentification**

Cette opération consiste à faire la preuve de son identité. Par exemple on peut utiliser un mot de passe, ou une méthode de défi basée sur une fonction cryptographique et un secret partagé. L'authentification est simple ou mutuelle selon les contraintes de l'environnement.
C'est le processus de vérification de l'identité.

2) **La confidentialité**

C'est l'assurance qu'une information n'est pas mise à disposition pour des individus, des entités ou des traitements non autorisées.

3) **L'intégrité**

L'assurance qu'une information n'a pas été modifiée détruite ou perdue de façon accidentelle ou intentionnelle.

4) **La disponibilité**

L'assurance d'être disponible et joignable pour toute requête d'une entité autorisée

5) **La non-répudiation**

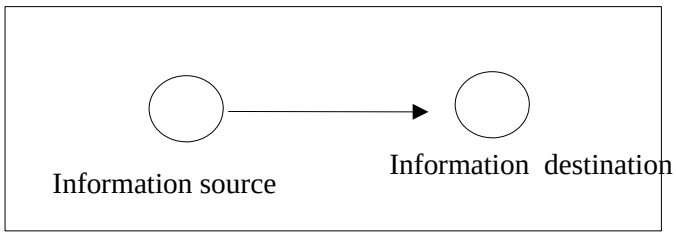
Les acteurs impliqués dans la communication ne peuvent pas nier leur fait

1.4Les Attaques

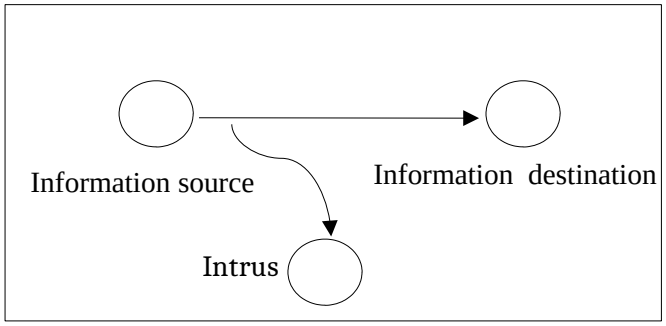
1.4.4 Définitions

Découverte systématique d'information tentative réelle d'intrusion ou un déni de service

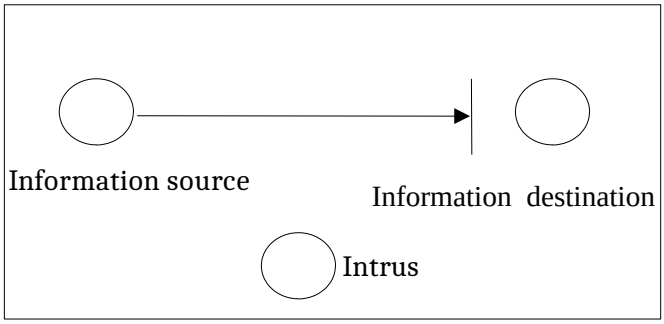
1.4.2 Modèle d'attaques



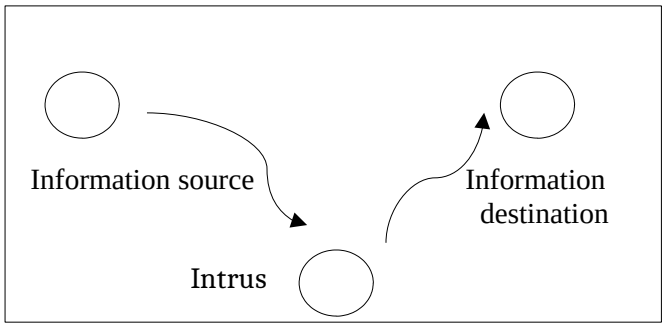
Flux normal



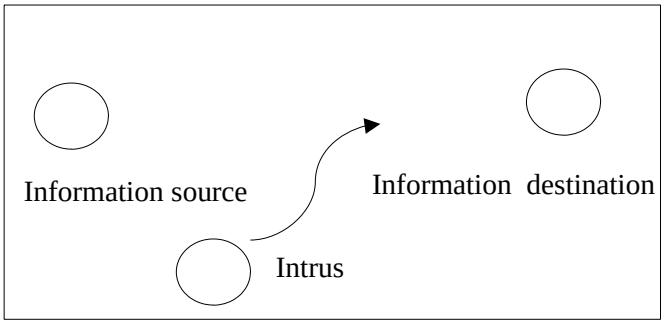
Interception



Interruption



Modification



Fabrication

Buts des attaques

- ✓ **Interruption** vise la disponibilité des informations
- ✓ **Interception** vise la confidentialité des informations
- ✓ **Modification** vise l'intégrité des informations

- ✓ **Fabrication** vise l'authenticité des informations

1.4.3 Les attaques réseaux

Les attaques réseaux s'appuient sur des vulnérabilités liées directement aux protocoles IP ou à son implémentation. Il en existe un grand nombre. Néanmoins, la plupart d'entre elles ne sont que des variantes des attaques réseaux cité dans ce qui suit.

1.4.2.1 IP Spoofing

Le but de cette attaque est l'usurpation de l'adresse IP d'une machine. Ceci permet au pirate de cacher la source de son attaque (utilisée dans les dénis de services dont nous discuterons plus tard) ou de profiter d'une relation de confiance entre deux machines.

1.4.2.2 TCP Session Hijacking

Le TCP Session Hijacking permet de rediriger un flux TCP, La nécessité d'une écoute passive (sniffing) est indispensable dans cette attaque au réseau physique de la cible. Avant de détailler cette attaque, nous expliquerons quelques principes fondamentaux du protocole TCP.

L'en-tête TCP est constitué de plusieurs champs :

- Le port source et le port destination, pour identifier la connexion entre deux machines;
- Le numéro de séquence qui identifie chacun des octets envoyés;
- Le numéro d'acquittement qui correspond au numéro d'acquittement du dernier octet reçu;
- Les flags, avec ceux qui vont nous intéresser sont :

• SYN qui synchronise les numéros de séquence lors de l'établissement d'une connexion;
• ACK, le flag d'acquittement d'un segment TCP;
• PSH qui indique au récepteur de remonter les données à l'application

A	Seq=x PSH/ACK=y (60)	B
A	Seq=y PSH/ACK=x+60 (20) (60)	B
A	Seq=x+60 PSH/ACK=y +20 (30)	B

Les numéros de séquence vont évoluer en fonction du nombre d'octets de données envoyés. Le numéro de séquence est représenté par Seq, le numéro d'acquittement se trouve après les flags PSH et ACK et le nombre d'octets de données envoyé se trouve entre parenthèses.

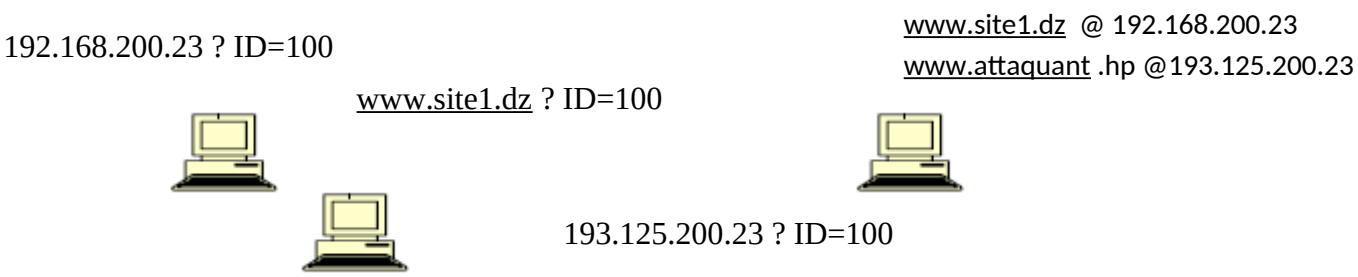
1.4.2.3 ARP Spoofing Cette attaque, appelée aussi ARP Redirect, redirige le trafic réseau d'une ou plusieurs machine vers la machine du pirate. Elle s'effectue sur le réseau

physique des victimes. Au préalable nous ferons un rappel sur l'utilité et le fonctionnement du protocole ARP.

1.4.2.4 DNS Spoofing

Le protocole DNS (Domain Name System) a pour rôle de convertir un nom de domaine (par exemple www.test.com) en son adresse IP (par exemple 192.168.0.1) et réciproquement, à savoir convertir une adresse IP en un nom de domaine. Cette attaque consiste à faire parvenir de fausses réponses aux requêtes DNS émisent par une victime. Il existe deux méthodes principales pour effectuer cette attaque.

- **DNS ID Spoofing**
  L'en-tête du protocole DNS comporte un champ identification qui permet de faire correspondre les réponses aux demandes. L'objectif du DNS ID Spoofing est de renvoyer une fausse réponse à une requête DNS avant le serveur DNS. Pour cela il faut prédire l'ID de la demande. En local, il est simple de le prédire en sniffant le réseau. Néanmoins, cela s'avère plus compliqué à distance. Cependant il existe plusieurs méthodes



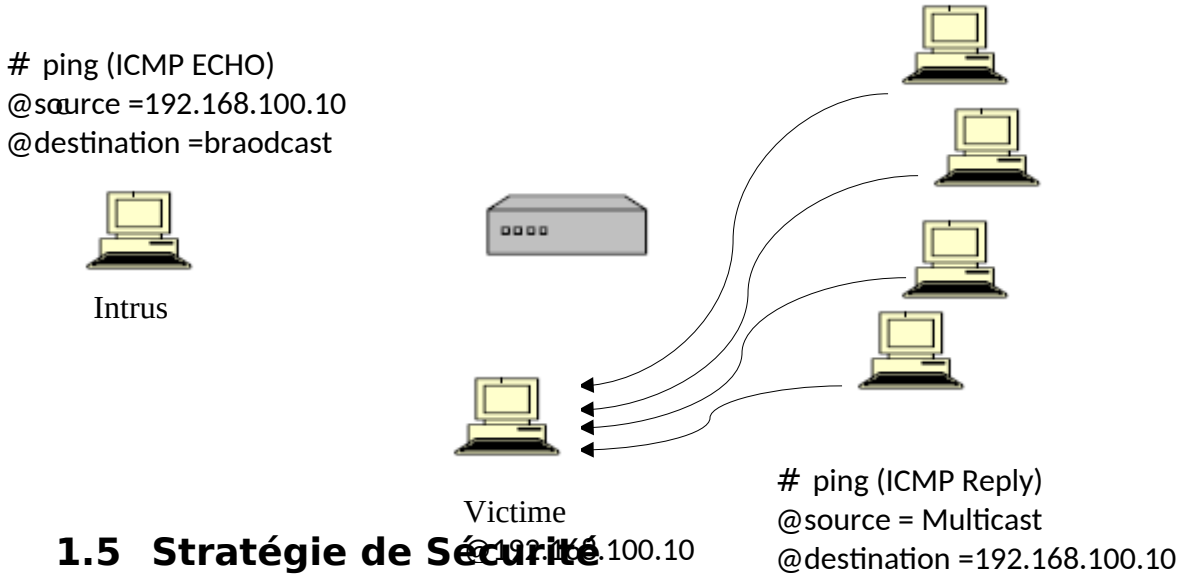
- **DNS Cache Poisoning** Les serveurs DNS possèdent un cache gardant en local, pendant un certain temps, les réponses de requêtes passées. Ceci pour éviter de perdre du temps à interroger chaque fois le serveur de nom ayant autorité sur le domaine demandé. Ce deuxième type de DNS Spoofing va consister à corrompre ce cache avec de fausses informations. Voici un exemple de cache poisoning

1.4.2.5 SYN Flooding Nous avons vu qu'une connexion TCP s'établie en trois phases (TCP Three Way Handshake). Le SYNFlooding exploite ce mécanisme d'établissement en trois phases. Les trois étapes sont l'envoi d'un SYN, la réception d'un SYN-ACK et l'envoi d'un ACK. Le principe est de laisser sur la machine cible un nombre important de connexions TCP en attentes. Pour cela, le pirate envoie un très grand nombre de demandes de connexion (flag SYN à 1), la machine cible renvoie les SYN-ACK en réponse au SYN reçus. Le pirate ne répondra jamais avec un ACK, et donc pour chaque SYN reçu la cible aura une connexion TCP en attente. Etant donné que ces connexions semi-ouvertes consomment des ressources mémoires au bout d'un certain temps la

machine est saturée et ne peut plus accepter de connexion. Ce type de déni de service n'affecte que la machine cible.

1.2.5.6 UDP Flooding :
Ce déni de service exploite le mode non connecté du protocole UDP. Il crée un "UDP Packet Storm"(génération d'une grande quantité de paquets UDP) soit à destination d'une machine soit entre deux machines. Une telle attaque entre deux machines entraîne une congestion du réseau ainsi qu'une saturation des ressources des deux hôtes victimes. La congestion est plus importante du fait que le trafic UDP est prioritaire sur le trafic TCP. En effet, le protocole TCP possède un mécanisme de contrôle décongestion, dans le cas où l'acquittement d'un paquet arrive après un long délai, ce mécanisme adapte la fréquence d'émission des paquets TCP, le débit diminue. Le protocole UDP ne possède pas ce mécanisme, au bout d'un certain temps le trafic UDP occupe donc toute la bande passant n'en laissant qu'une infime partie au trafic TCP.

1.2.5.7 Smurfing Cette attaque utilise le protocole ICMP. Quand un ping (message ICMP ECHO) est envoyé à une adresse de broadcast (par exemple 192.168.255.255), celui-ci est démultiplié et envoyé à chacune des machines du réseau. Le principe de l'attaque est de spoofer les paquets ICMP ECHO REQUEST envoyés en mettant comme adresse IP source celle de la cible. Le pirate envoie un flux continu de ping vers l'adresse de broadcast d'un réseau et toutes les machines répondent alors par un message ICMP ECHO REPLY en direction de la cible. Le flux est alors multiplié par le nombre d'hôte composant le réseau. Dans ce cas tout le réseau cible subira le déni de service, puisque l'énorme quantité de trafic généré par cette attaque entraîne une congestion du réseau.



1.5 Stratégie de Sécurité

- **Antivirus**
- **Pare-Feu :** C'est un serveur qui s'intercale entre le réseau administratif et le réseau externe qui peut faire du filtrage des paquets
- **Chiffrement :** algorithme généralement basé sur des clés qui transforme les données

- **Détection d’intrusion :** les serveurs de détections d’intrusions IDS, NIDS, HIDS
- **Sécurité du canal : VPN, IPsec tunneling**