Chapitre 01 : Introduction à la security

Security informatique :

Mécanismes et moyens de protection mis en oeuvre, afin de réduire la vulnérabilité du système contre les action accidentelles ou intensionnelle

Sûreté de fonctionnement :

Mécanismes et outils mis pour la protection contre le dysfonctionnement du système et les accidents involontaires.

Sécurité de l'information :

Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information

En outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité peuvent également être concernées.

- Confidentialité : X

L'information ne doit être accessible qu'aux personnes autorisées.

- Intégrité : X

L'information ne doit pas être modifiée ou altérée de manière non autorisée.

- Disponibilité : X

L'information doit être accessible aux utilisateurs légitimes quand ils ont besoin

- Authenticité : X

L'identité des utilisateurs et des sources d'information doit être vérifiable

- Imputabilité :

Chaque action effectuée sur le système doit pouvoir être reliée à une utilisateurs précis.

- Non-répudiation : X

Un utilisateur ne peut pas contester avoir effectué une action

- Fiabilité :

L'information et les systèmes doivent être sûrs et fonctionner sans erreur.

Système d'information :

Ensemble des données et des ressources (matérielle ou immatérielles) de l'entreprise permettant de stocker, transformer, circuler, exploiter ... l'information.

Sécurité d'un SI :

Ensemble des moyens de protection (techniques ou non techniques) permettant à un SI de résister à des évènements susceptibles de compromettre la sécurité de l'information et du SI.

Principaux Concepts :

Vulnérabilité :

Faiblesse ou faille. faute intentionnelle ou accidentelle dans la protection du système (en générale les points d'entré de système)

Menace :

Violation potentielle d'une propriété de sécurité (confidentialité, intégrité ... etc) par un attaquant, qui pourrait entraîner des dommage sur le système si cette menace est concrétisait.

Attaque : (action malveillant)

représente la concrétisation d'une menace, par l'exploitation d'une faille (vulnérabilité) du système.

Intrusion :

C'est une attaque réussie.

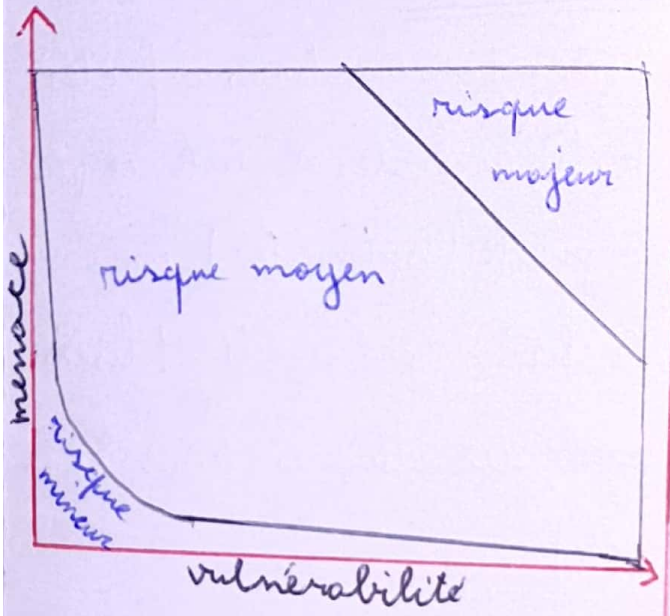
Contre-mesure :

L'ensemble des actions ou moyens permettant de réduire le risque dans une organisation.

Risque : (mesure de danger)

Signifie la probabilité qu'une menace exploitera une vulnérabilité du système

$$\text{Risque} = \frac{\text{Vulnérabilité} * \text{menace}}{\text{Contre-mesure}}$$



Attaques VS Accidents

accident	attaque
Evénement non intentionnel	Action intentionnelle
Imprudence, erreur ou hasard	Un agresseur ou un attaquant

Technique d'attaques :

Le virus :

est un morceau de code qui s'attache à des fichiers ou aux secteurs système du disque dur (un parasite)

Il ne peut pas duplique tant qu'il n'est pas executé

L'existence d'un virus est un menace, n'est pas un attack

Les vers (worm) :

est un program independant qui s'auto-propage via le réseau.

L'objective principale et de ralentire le système.

Cheval de Troie (Trojan):

Logiciel apparemment légitime, installe des fonctions malveillantes.

Porte Derobée (Backdoor):

Accès secret pour contrôler un système à distance

Spyware:

collecter des informations personnelles sur l'ordinateur sans autorisation.

Keylogger:

Un programme malveillant son but principale est d'enregistrer des frappes clavier pour intercepter des informations sensible.

Exploit:

programme malveillant contient des codes executables qui permette l'exploit des faille de système

Rootkit:

Des logiciels permettant de:

- Obtenir les droits d'admin
- Installer une porte dérobée
- Effacer les traces d'attaque

c'est un outil de dissimulation d'activité.

Le pourriel (spam):

Un e-mail non-sollicité, la plupart du temps de la publicité.

Le BOTNET:

Réseau d'ordinateurs infectés (bots) contrôlés à distance par un pirate (botmaster). Ces machines sont ensuit utilisées pour des attaques (DDOS, spam .etc)

L'hameçonnage (phishing):

une cyberattaque par tromperie où un pirate se fait passer pour une entité de confiance pour voler des données sensibles.

Le canular informatique (Hoax):

un e-mail incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes

RansomWare:

Chiffre les données et demande une rançon.

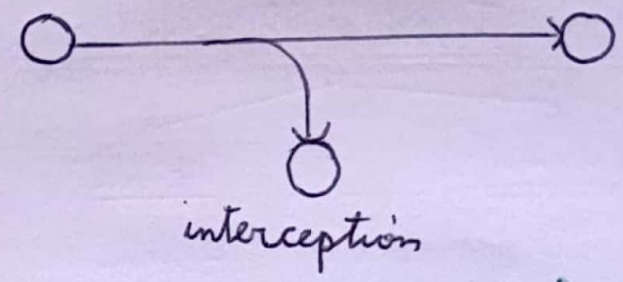
Origine des attaques

- **Externe**
  - Cybercriminels
  - sites malveillants
  - réseaux
- **Interne**
  - Employés négligents
  - mots de pase faibles
  - clés USB infectées

Scénarios d'Attaques:

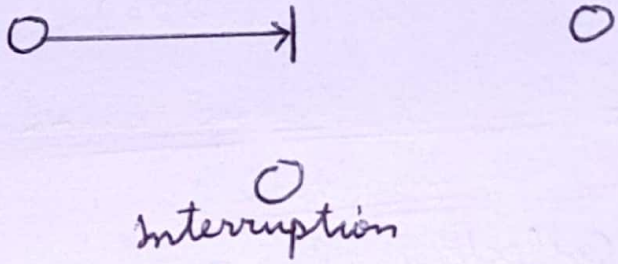
Atteinte à la confidentialité:

Vol de données (Spyware, phishing)



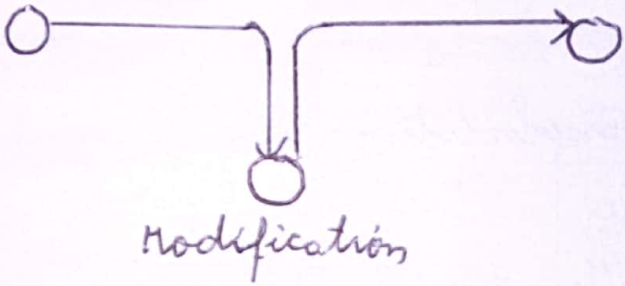
Atteinte à la disponibilité:

DDoS, ransomeware (blocage d'accès.



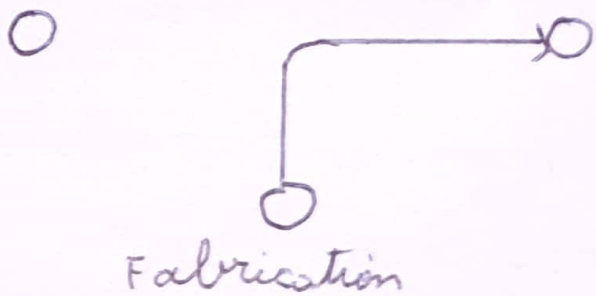
Atteinte à l'intégrité:

Modification de données (exploits, trojans)



Atteinte à l'Authenticité:

Usurpation d'identité (mascarade)



Types d'Attaques

Passive

Ecoute discrète (espionnage, analyse de trafic)

Active

Action destructrices (Modification de données, DOS)

Etapes d'une Attaque (Méthodologie du Pirate):

- Collecte d'infos: Techniques (scan réseau) et non techniques (ingénierie sociale)
- Identification des Failles: Recherche de vulnérabilités
- Exploitation: Intrusion via les failles
- Maintien de l'Accès: Installation de backdoors / malwares
- Effacement des Traces: Dissimulation (Rootkit)

Outils d'attaques:

Sniffers: (Capteurs de trafic)

- Légitimes: Analyse réseau.
- Malveillants: Vol de données

Scanners de Vulnérabilités

- Légitimes: Détectent les failles.
- Malveillants: Utilisés par les pentesters ou pirates pour trouver les vulnérabilités

Catégories d'attaquants:

Les Hackers

- Ce sont des experts en securit
- Ils n'endommagent jamais intentionnellement les donnée

1- White Hat: améliorer la securité (legal)

2- Grey Hat: dénoncer des failles (illégale)

- accéder au système sans autorisation mais ils n'ont

pas d'intention malveillante

Les crackers:

- Sont des personnes spécialisées dans le piratage des systèmes informatique
- Ils ont une intention malveillante.

1- Black Hat: ils ont des compétences en programmation et en securité informatique

2- script kiddies: utilisent des outils préfabriqués (des scripts)

3- Les Hacktivistes: ont des motivations politiques / sociales (exc: Anonymous)

Mecanisme de securité:

est une solution technique ou organisationnelle conçue pour:

- prévenir les attaques
- Identifier les menaces
- Lutter contre les intrusions

- **Authentification et Identification:**

Vérifie et prouvée l'identité (mot de pass, biométrie)

- **Controle d'Accès:**

Restreint l'accès aux resources (physique/logique)

- **Antivirus:**

Détecte les malwares par signature/comportement

Son objectif: détecter, identifier, éliminer ou mettre en quarantaine les programmes malveillants

- **Chiffrement:**

protège les données par cryptage du texte (symétriques ou Asymétrique).

- **Hashage:**

Genère une empreinte unique servant à identifier rapidement la donnée initiale

- **Signature Numérique :**
  Garantit l'origine des messages
- **Certificats Numériques :**
  Lie une clé publique à une identité (CA)
- **Firewall :**
  Filtre le trafic entrant / sortant (autorisé / bloqué)
- **DMZ :**
  Zone isolée pour serveurs accessibles.
- **Proxy :** Cache l'IP (moins sécurisé)
- **VPN :**
  chiffre le trafic + cache l'IP (plus sécurisé)
- **IDS / IPS :**
  - IDS : Détecte les intrusions (alerte)
  - IPS : Bloque activement les attaques.