chapitre (03): Menaces informatique

- **Introduction:**

Les menaces informatiques représentent les risques -

c ad:

→ c'est tout ce qui peut nuire à un système informatique:

- cela peut détruire, voler, bloquer des données
- menaces → accidentelles (erreur, panne)
  → intentionnelle (attaque, vol ...etc)

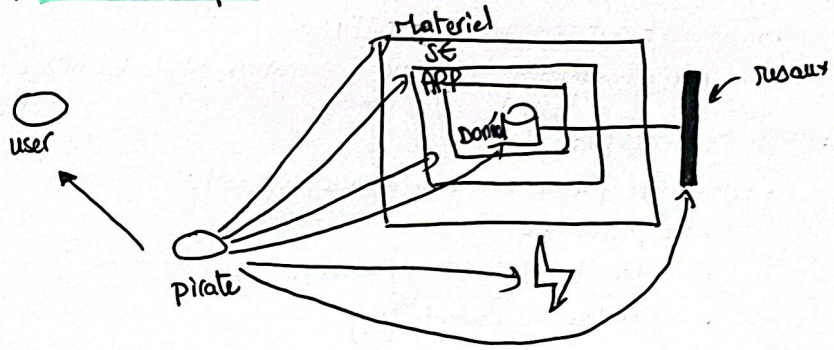
→ **Attaque informatique:**

- une action pour profiter d'une vulnérabilité
- elle peuvent venir de l'interieur (employé) ou l'exterieur (pirate inconnu)
- Objectif:
  → Voler des données, bloqué un service, faire du chantage ...

→ **Qui sont les attaquants?:**

- **BlackHat:** pirates malveillants
- **WhiteHat:** experts qui aident à améliorer la SI
- **GrayHat:** entre les deux
- **Scriptkiddies:** jeunes qui utilisent des utiles sans tout comprendre
- **Hacktivisits:** pirates avec un message politique
- **cyberroristes:** Visent à crée la panique

→ **surface d'attaques:**



→ **Phases d'une attaque:**

① - **Reconnaissance:** collecte d'infos
- **active:** sans interroger directement le système ciblé
- **passive:** interroger directement le système

② **Scanning:** repérer les failles
- étape(01): phase préattaque: analyse (réseau, ...)
- étape(02): Scanning de ports (analyse les ports ouverts)
- etape (03): Extraction de l'information (collecte d'info)

③ - **Gain d'acces:** Entrer le système

④ - **Maintien accès:** rester cacher dans le système

⑤ - **Effacer les traces:** vider le cache et les cookies

→ **Classification des attaques:**

- **Selon l'localisation:**
  - interne: dans le périmètre
  - externe: l'exterieur de périmètre
- **Selon la nature**
  - active: modifier, bloquer, détruire
  - passive: écouter, observer
- **Selon l'objectif visé**
  - interception: lire les infos
  - modification: changer des données
  - Interruption: bloqué l'accès
  - fabrication: injecter de fausses infos

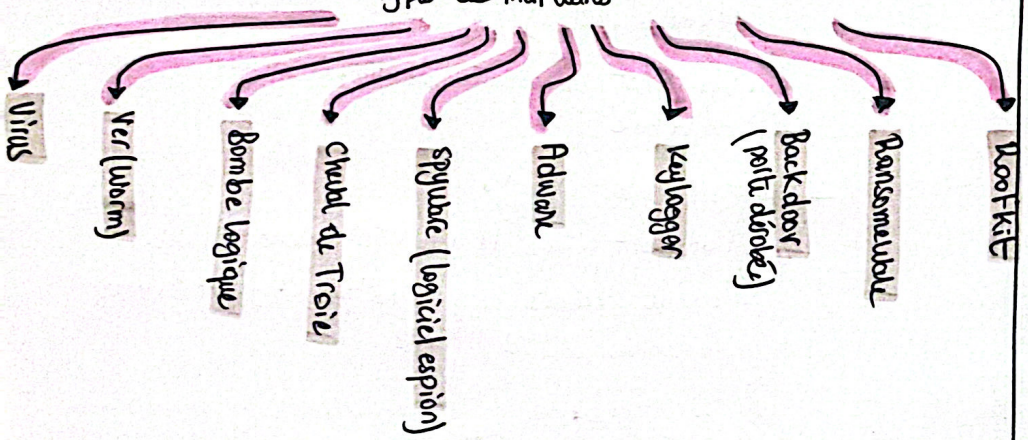
→ **Malwares : "Malicious software"**

- Ce sont des programmes créés pour nuire (ضارة)
- peuvent être classés selon :

propagation : comment ils se répandent (réseau, email...)

Déclenchement : Quand ils se activent (date, exécution)

charge utile : ce qu'ils font après infection



→ **Virus :**

- Se cache dans un programme et se propage en l'exécutant
- nécessite un fichier hôte (virus de fichier, de macro...)

→ **Ver (worm) :**

- se propage tout seul sans intervention humain
- peut causer des dégâts comme ... , saturer un serveur ou ouvrir une porte aux pirates

→ **Bomb logique :**

- caché dans le système, elle s'active à un moment précis (ex: une date)
- très discrète (...), difficile à detecter.

→ **cheval de Trois :**

- Semble à être logiciel normal, mais cache une fonction dangereuse
- Ne se propage pas tout seul

→ **spyware (logiciel espion) :**

- Espionne l'utilisateur à son insu (...)
- peut enregistrer les frappes, captures d'écrans...

→ **Adware :**

- Affiche de la publicité sans votre accord
- Souvent installé avec d'autre logiciels.

→ **Keylogger :**

- Enregistre tout ce que vous tapper sur clavier (MDP, msg...)
- Utilisé à des fins malveillantes

→ **Backdoor :**

- donne un accès caché au pirate
- il peut contrôler l'ordinateur à distance sans que l'utilisateur le sache

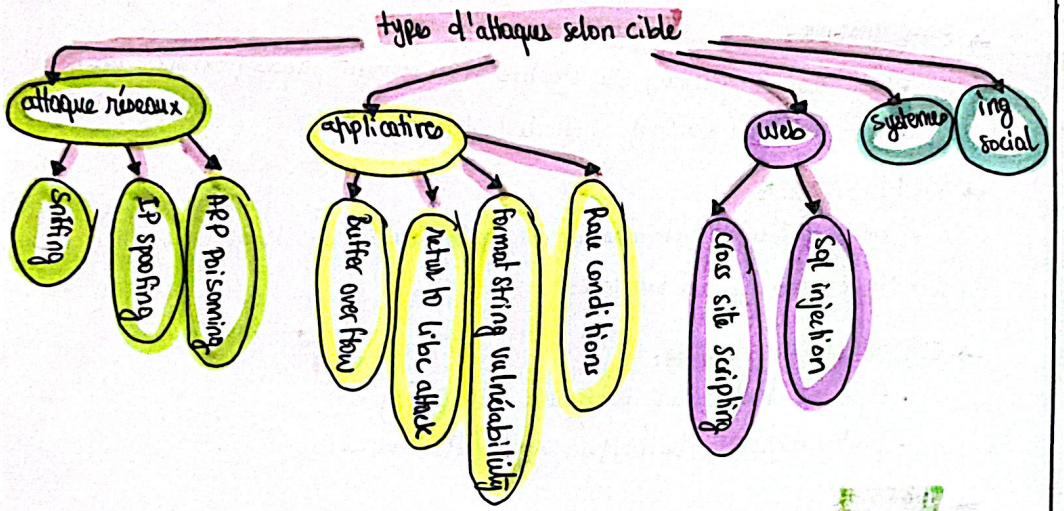
→ **Ransomeware :**

- chiffre (Bloque) vos fichiers, puis demande une rançon pour le débloquer
- Se propage par email piégé ou clé USB infectée

→ **Rookit :**

- Se cache profondement dans le système
- masque la présence d'autre malware
- permet au pirate de garder le contrôle et d'échapper à la détection

Scanned with CamScanner



→ Attaques réseaux:

→ Sniffing: Espionne les données qui circulent sur le réseau

→ IP spoofing: usurpe (تزوير) une @ IP pour faire croire que on est quelqu'un d'autre

→ ARP poisoning:

- ARP: protocole de communication pour découvrire la couche de de la liaison.

→ ARP (Request / Reply):

Request: Appareil demande @ MAC d'une IP
ex: who has 192.168.1.2?

Reply: l'appareil cible répond avec sa MAC
ex: 192.168.1.2 is at: bbbb:bbbb:bbbb

→ ARP Gratitous: (Reponse gratuite):

C'est un ARP reply envoyé sans qu'on l'ait demandé
utilisé pour:

- Mettre a jour les tables ARP des autres machines
- vérifier s'il y a conflit d'@IP
- parfois aussi dans des attaques ARP poisoning

principe ARP poisoning:

- trompe les machines d'un réseau local (LAN) pour rédiger les données vers l'attaquant
- l'attaquant envoie de faux messages ARP pour associer sa propre @ MAC à une @IP d'une autre machine
- Il intercepte alors les données ou modifie la communication (attaque de type homme du milieu)

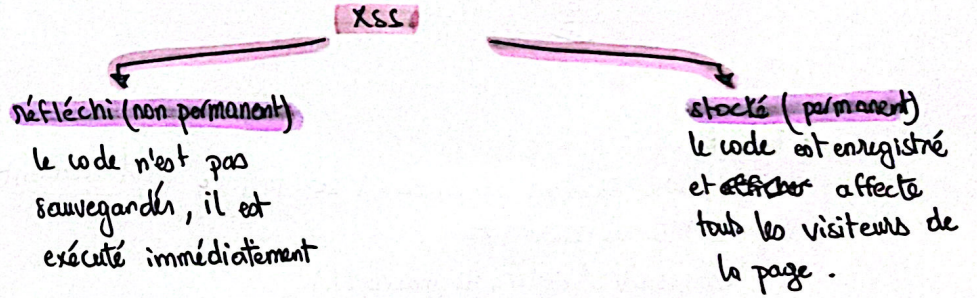
→ Attaques Web:

→ SQL injection:

- le pirate insere du code SQL malveillant dans un champ (formulaire, URL ...)
- cela permet de consulter, modifier, ou supprimer des données de la base

→ Xss (cross site scripting):

- l'attaquant injecte du code Js dans un site Web
- le code s'exécute chez les visiteurs et permet de voler des cookies, des identifiants



Scanned with CamScanner