Module Sécurité Informatique (F332)

Cours 2- Panorama des Menaces&Attaques

Rappel

Objectifs de la sécurité informatique

La sécurité d'un système repose sur cinq grands principes:

- ***L'intégrité des données:*** il faut garantir que les données sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non).
- ***La confidentialité :*** seules les personnes habilitées doivent avoir accès aux données.
- ***La disponibilité:*** il faut s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment.

Rappel

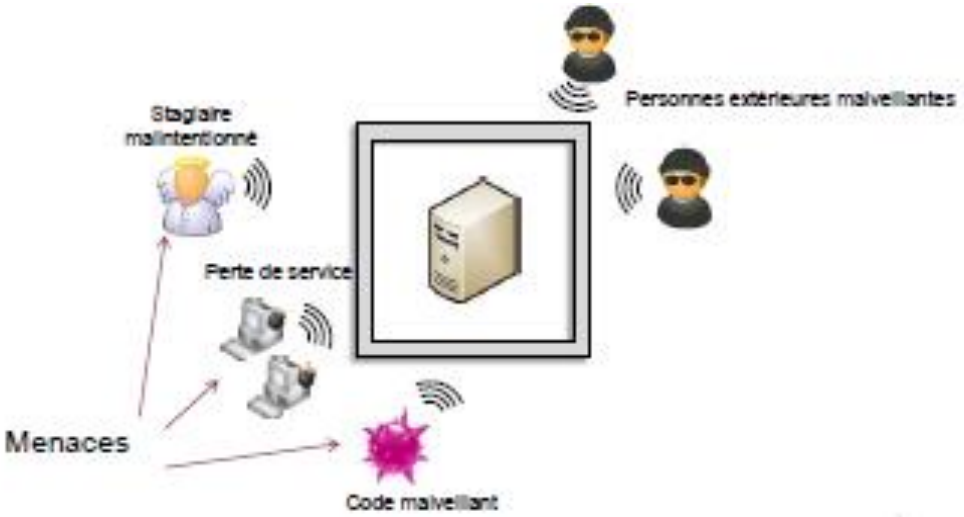
Objectifs de la sécurité informatique (suite)

- ***La non-répudiation des données :*** une transaction ne peut être niée par aucun des correspondants.

- ***L'authentification :*** elle limite l'accès aux personnes autorisées. Il faut s'assurer de l'identité d'un utilisateur avant l'échange de données.

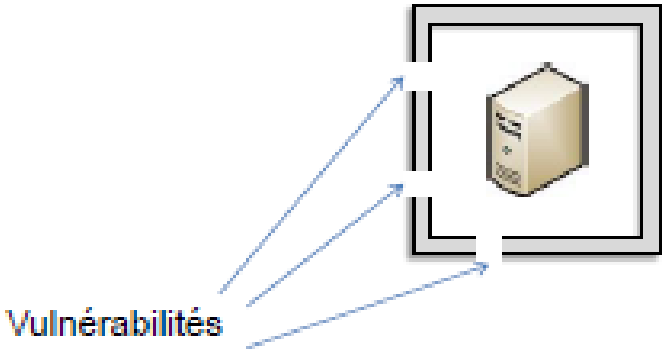
Terminologies

Menace: Cause potentielle d'un incident, qui peut entrainer des dommages sur un système si cette menace se concrétise.



Terminologies (suite)

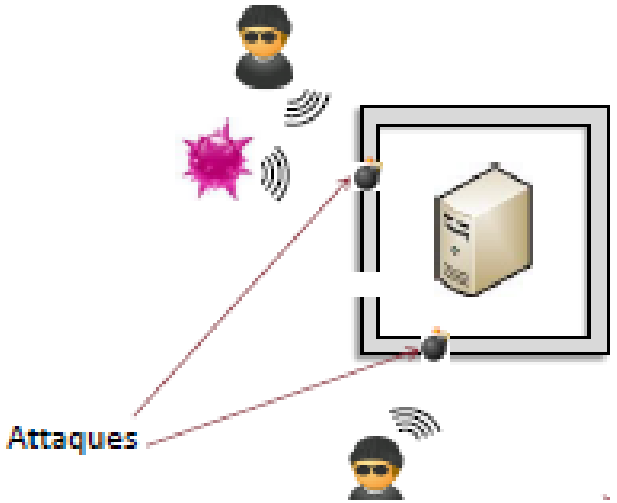
Vulnérabilité: Faiblesse au niveau d'un bien (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).



Terminologies (suite)

- **Attaque:** Action malveillante destinée à porter atteinte à la sécurité d'un système. Une attaque représente la **concrétisation d'une menace**, et nécessite **l'exploitation d'une vulnérabilité.**

  - Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.



Terminologies (suite)

- **Intrusion:** Prise de contrôle partielle ou totale d’un système distant.

- **Contre-mesure:** ensemble de mécanismes destinés à protéger l'information des utilisateurs ou processus n'ayant pas l'autorisation de la manipuler et d’assurer les accès autorisés.

Notion de Risque

- **Risque:** se mesure par la probabilité qu'une menace exploite une vulnérabilité et la conséquence (impact) ou la gravité de sa réalisation.

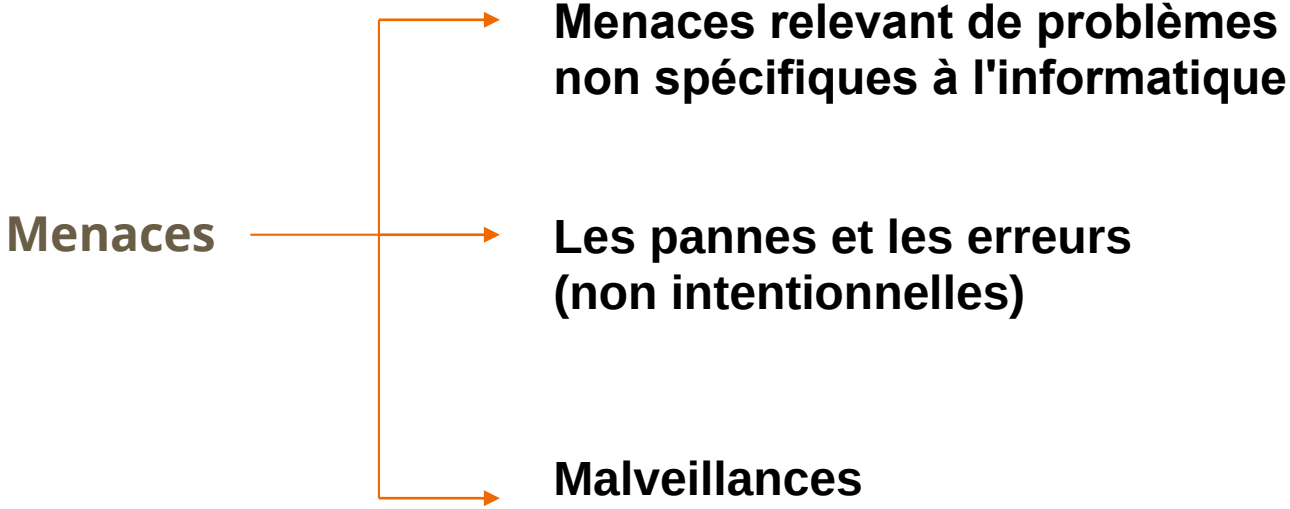
Risque=conséquence x probabilité d'occurence

Exemple de risque : *Un chef d'entreprise peut se faire voler son ordinateur portable et risque donc de perdre toutes les données incluses sur sa machine (fichier client, factures, devis, contrats, prix, etc). Comment contourner ce risque ?*

Gestion du risque (fera l'objet du cours suivant)

Panorama des Menaces

Panorama des menaces



Panorama des menaces

❑ **Menaces relevant de problèmes non spécifiques à l'informatique**

- **Risques matériels accidentels:** Incendie , explosion, Inondation, tempête, Foudre
- **Vol et sabotage de matériels:** Vol d'équipements matériels, Destruction d'équipements, Destruction de supports de sauvegarde
- **Autres risques:** Tout ce qui peut entraîner des pertes financières dans une société (pertes plutôt associées à l'organisation, à la gestion des personnels) tels que: Départ de personnels stratégiques et les grèves

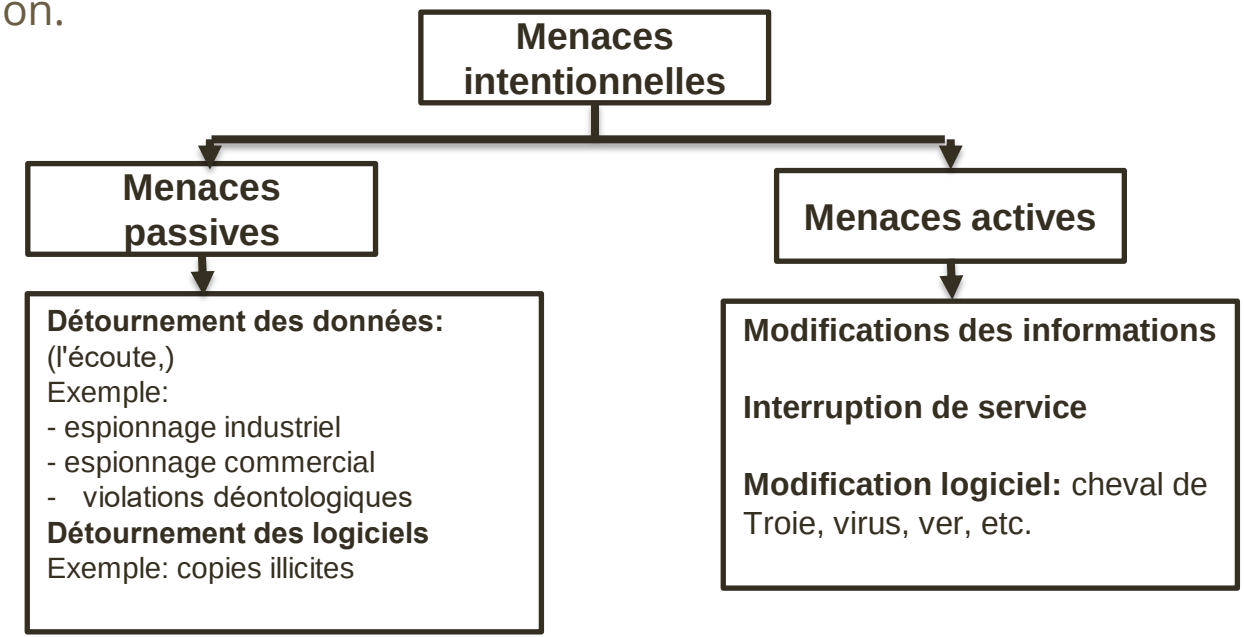
Panorama des menaces

❑ **Les pannes et les erreurs (non intentionnelles)**

- Pannes/dysfonctionnements du **matériel**.
- Pannes/dysfonctionnements du **logiciel de base**.
- Erreurs d'exploitation: oubli de sauvegarde, écrasement de fichiers, ...
- Erreurs de manipulation des informations: erreur de saisie, erreur de transmission, erreur d'utilisation
- Erreurs de conception des applications

Panorama des menaces

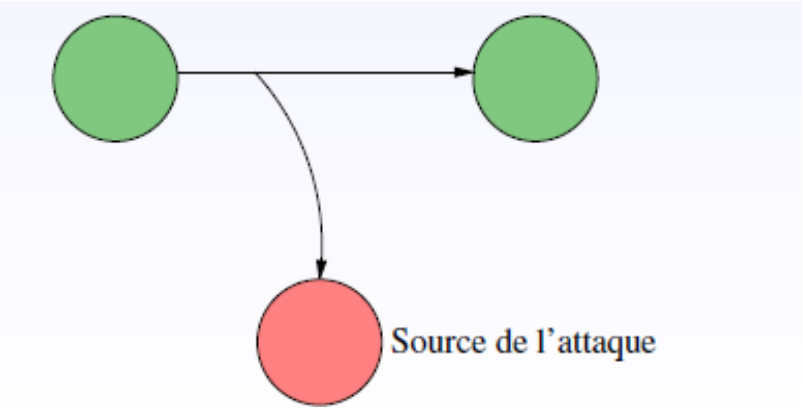
- **Les menaces intentionnelles:** L'ensemble des actions malveillantes (qui constituent la plus grosse partie du risque) et qui devraient être l'objet principal des mesures de protection.



Panorama des Menaces

Menace passive

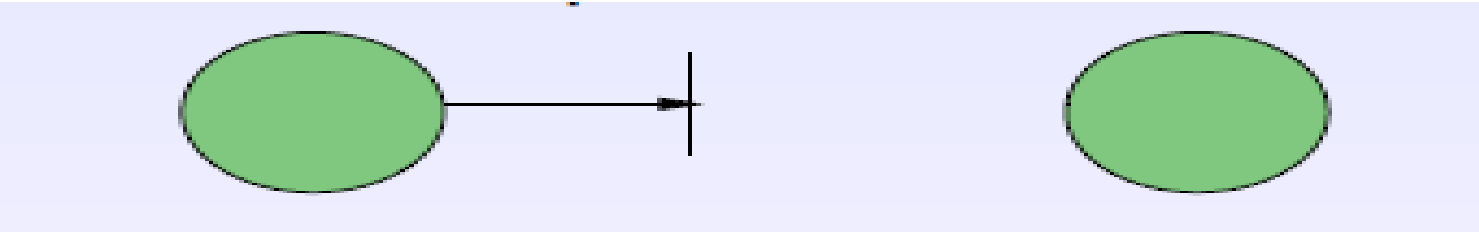
- **Interception** : vise la confidentialité des informations (capture de contenu, analyse de trafic, . . .)



Panorama des Menaces

Menaces actives

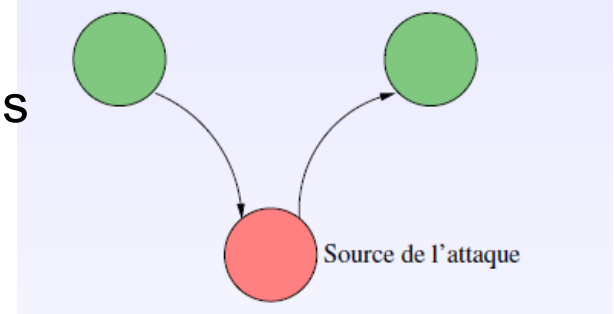
- **Interruption:** vise la disponibilité des informations (DoS, . . .)



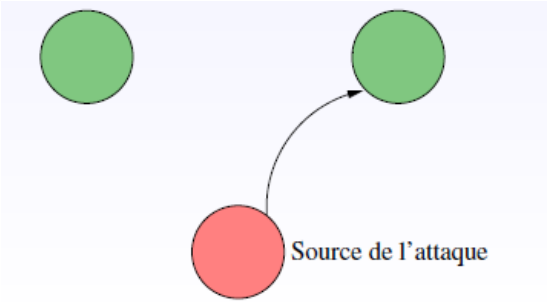
Panorama des Menaces

Menaces actives

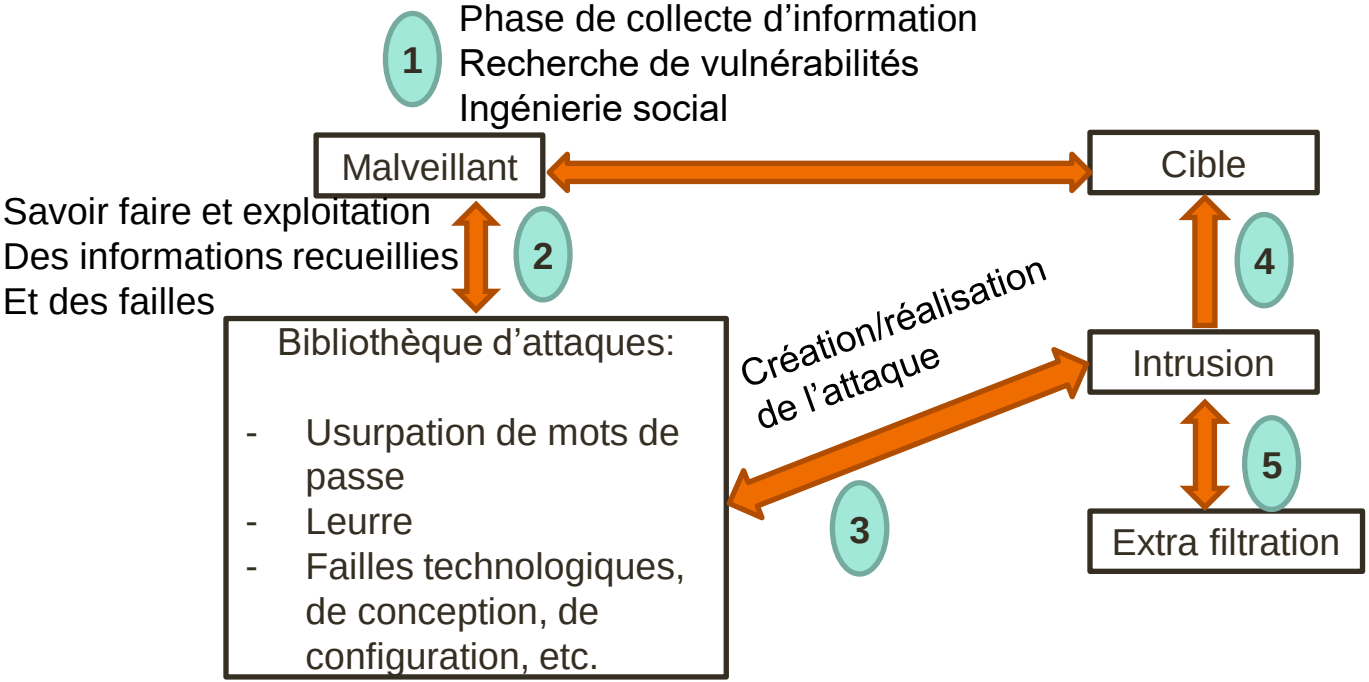
- **Modification:** vise l'intégrité des informations (modification, rejeu, . . .)



- **Fabrication:** vise l'authenticité des informations (mascarade, . .



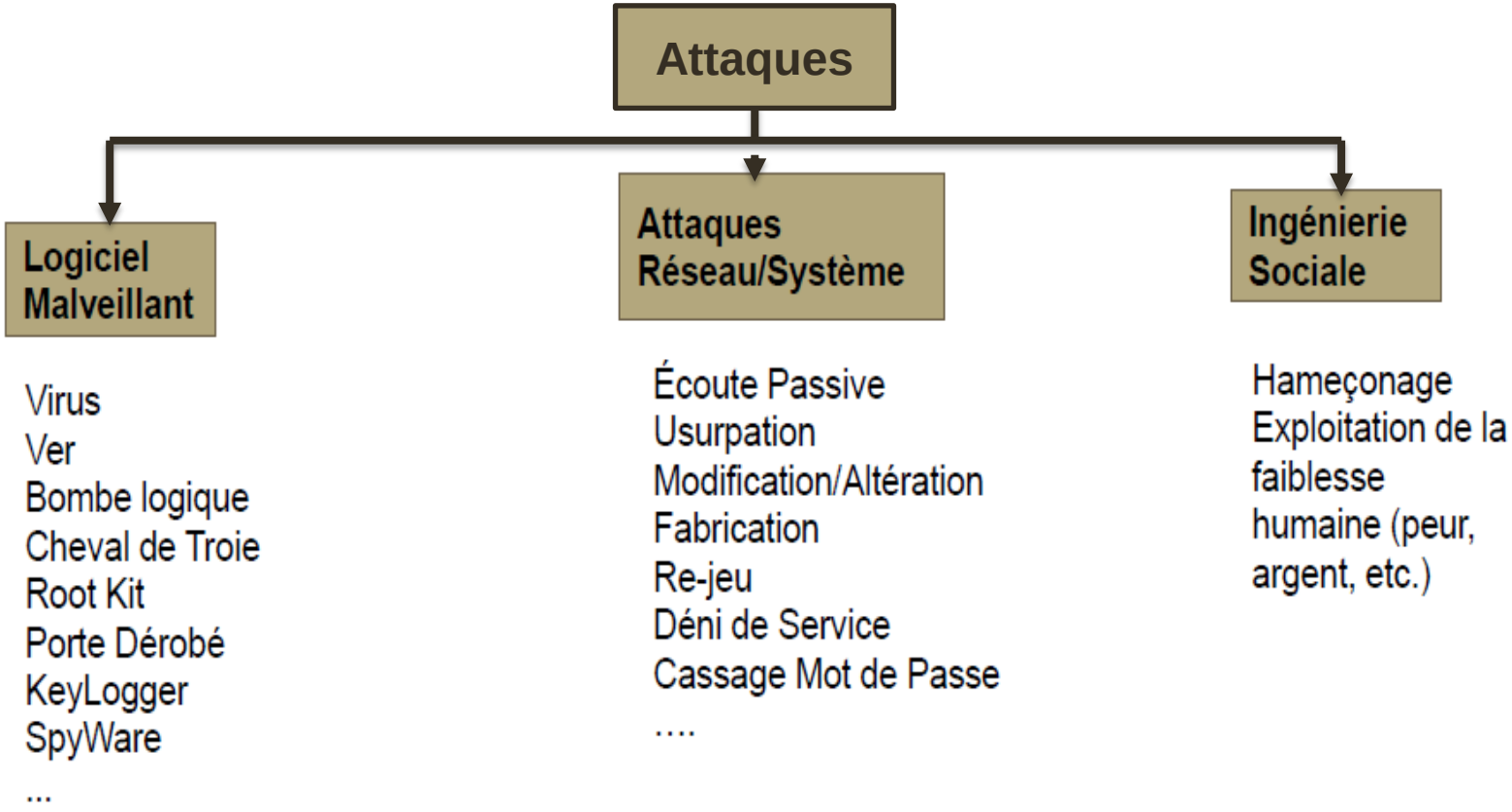
❑Schéma et étapes de réalisation d'une attaque



❑Schéma et étapes de réalisation d'une attaque

- **Phase 1:** liée à la collecte d'information sur la cible et à la recherche de vulnérabilité d'un système
- Le malveillant s'emploie à connaitre et à exploiter les failles de sécurité connues mais non encore réparées et à utiliser les outils d'attaques éventuellement disponible en ligne **(phase 2)** pour accéder au système cible et exécuter ses actions malveillantes **(phase 4)**
- **Phase 5:** a pour buts principaux de faire en sorte que l'attaque ne puisse être détectée et que l'attaquant ne laisse de trace pouvant servir à son identification. Pour arriver à cela, il tente de rester anonyme.

Types d'attaques informatiques



Logiciels Malveillants

On appelle programme malveillant (malware) tout type de logiciel/programme ayant un comportement malicieux, destiné à s'introduire dans un système informatique à l'insu de l'utilisateur dans le but de l'endommager ou en tirer profit de quelconque manière:

- endommager: suppression de données, formatage disque, rendre un service indisponible
- Tirer profits: vol de données, voir un accès/contrôle sur la cible, gain financier (rançon), lancer un attaque à partir de la cible, etc.
- porter atteinte aux besoins de sécurité

Logiciels Malveillants

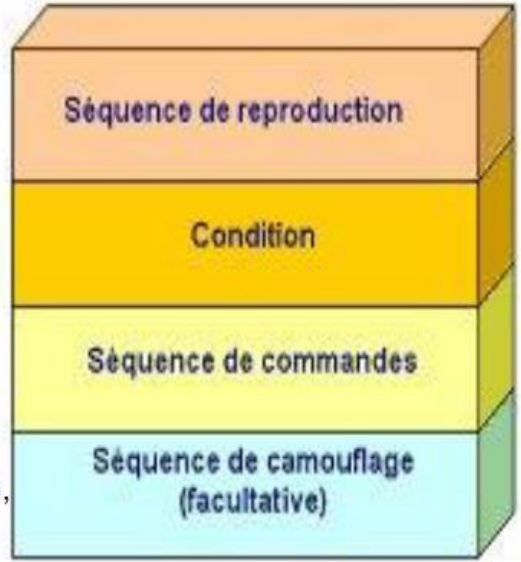
❑ Virus

- C’est la forme la plus connue des logiciels malveillants
- ***propriétés:***

➢ Infection: infecte tout fichier pouvant s’exécuter (.exe, .com, script, etc.)
➢ Ne s’exécute pas tout seul, mais plutôt à travers l’hôte infecté
➢ Infecte aussi les secteurs d’amorçage et les Master Boot, parties sur support de stockage contenant un code bootable par défaut
➢ Propagation: se propage grâce aux fichier infectés, à travers tous moyen d’échange de données: réseau, USB, CD/DVD, pièce jointe émail, site web infecté, etc.

Logiciels Malveillants

Virus: Structure



Infection des fichiers et supports

Condition pour s'exécuter

La charge du virus

Pour être transparent à l'OS, antivirus

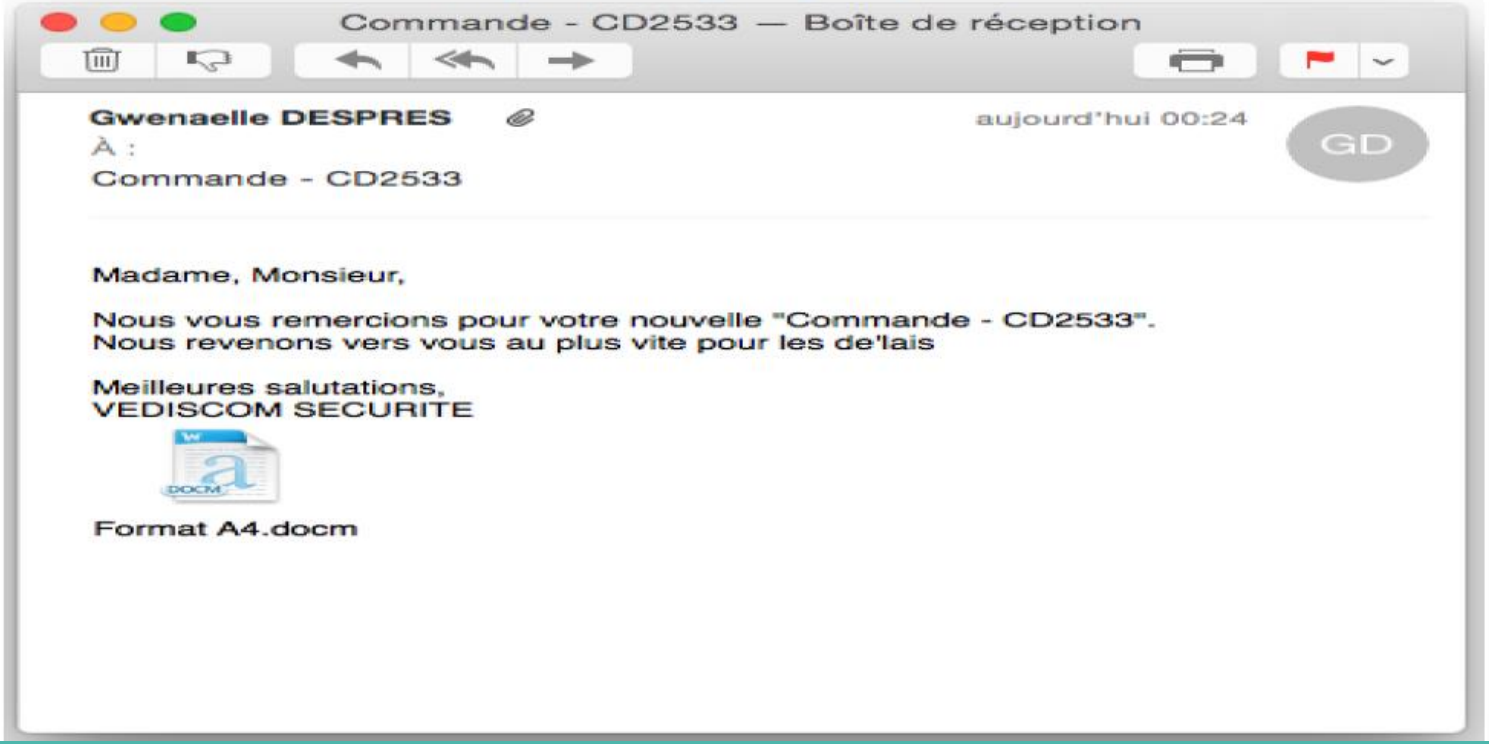
Logiciels Malveillants

Virus: exemple de propagation via lien

Fake LinkedIn Email with a Virus

Logiciels Malveillants

Virus: exemple de propagation via email



Logiciels Malveillants

❑ Ver

Contrairement à un virus, un ver peut s'auto-reproduire et se déplacer à travers un réseau en utilisant les mécanismes réseau, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier, etc.). Un ver est donc **un virus réseau**

Les vers se propagent principalement grâce à la messagerie grâce à des fichiers attachés contenant des instructions permettant de récupérer l'ensemble des adresses de courrier contenues dans le carnet d'adresse et en envoyant des copies d'eux même à tous ces destinataires.

Logiciels Malveillants

❑ Cheval de Troie

- Un programme/logiciel dont l'apparence est légitime, mais qui cache un autre malicieux (virus, ver, etc.)
- Ainsi en exécutant le cheval de Troie, supposé être légitime par l'utilisateur, le programme malveillant s'exécute aussi
- En général il s'agit d'un programme bien connu, mais qui a été modifié (ajout du code malveillant) puis redistribué (Windows, Pack Office, etc.)

Logiciels Malveillants

❑ Porte dérobée

- Une porte dérobée, également appelée Remote Administration Tool (RAT), est une application qui permet à certains utilisateurs (administrateurs systèmes ou cybercriminels) d'accéder au système d'un ordinateur sans que l'utilisateur ne l'autorise ou ne le sache.

- Selon la fonctionnalité RAT, le pirate peut installer et lancer un autre logiciel, télécharger ou supprimer des fichiers, allumer votre microphone ou votre caméra et enregistrer l'activité de votre ordinateur afin de la communiquer au pirate

- L'introduction d'une porte dérobée dans un logiciel à l'insu de son utilisateur transforme le logiciel en cheval de Troie.

Ingénierie Sociale

Exploiter la faiblesse humaine pour tirer un quelconque profit :
- Extraire/avoir accès à des informations sensibles (mot de passes, numéros de cartes bancaires, numéro téléphones, etc.) par un quelconque moyen (téléphone, conversation, mail, etc.)

- Induire l'utilisateur à faire une action (téléchargement et/ou ouverture d'une pièce jointe, cliquer sur un lien pour visiter un site, etc.)

Ingénierie Sociale

Phishing(Hameçonage)

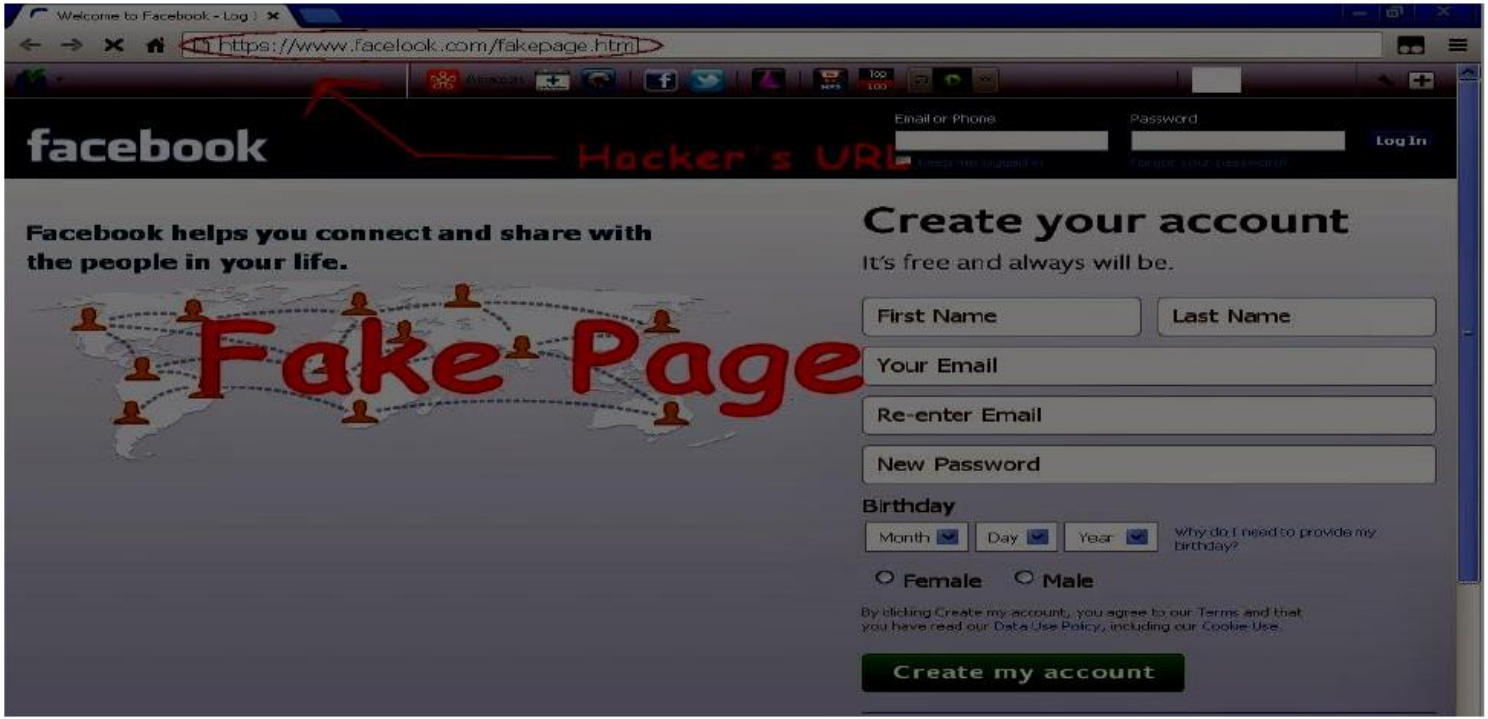
piegeage de l'utilisateur en lui faisant croire qu'il s'adresse à un tiers de confiance pour lui soutirer des informations confidentielles (mot de passe, no de carte de crédit ...)

- on lui demande son mot de passe
- on lui demande de le changer

exemple : services bancaires en ligne, sites de ventes aux enchères (Ebay)

Ingénierie Sociale

Phishing via un faux lien facebook



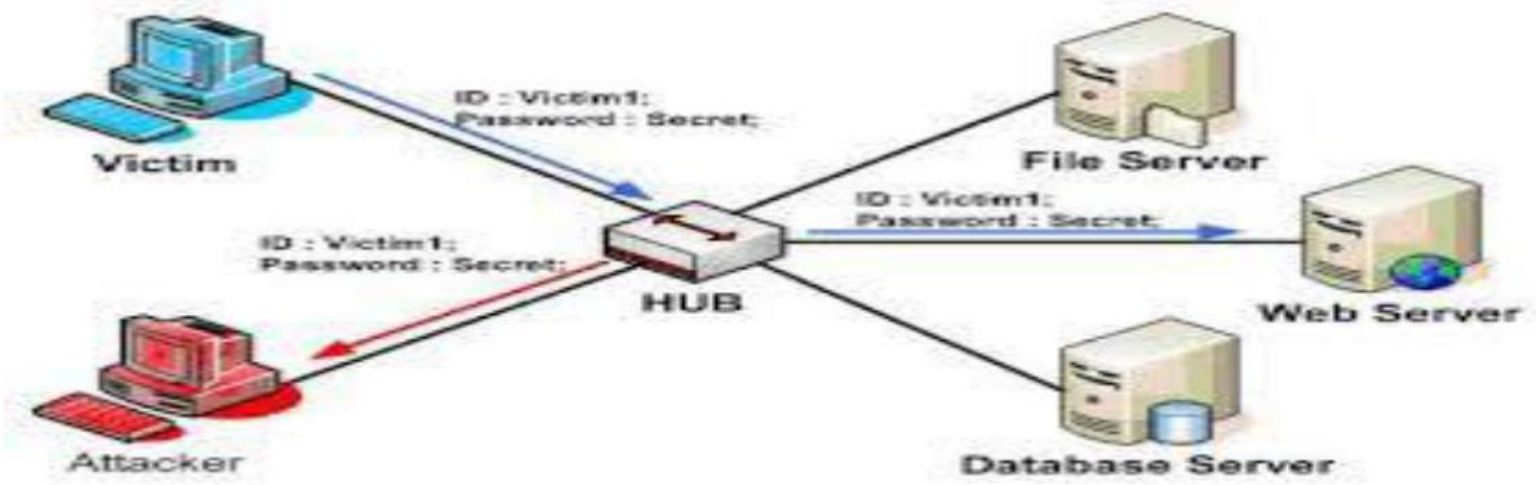
Attaques Réseaux

Écoute (Sniffing)

- Interception des paquets/messages transmis entre une source/destination sur un support filaire ou sans-fil

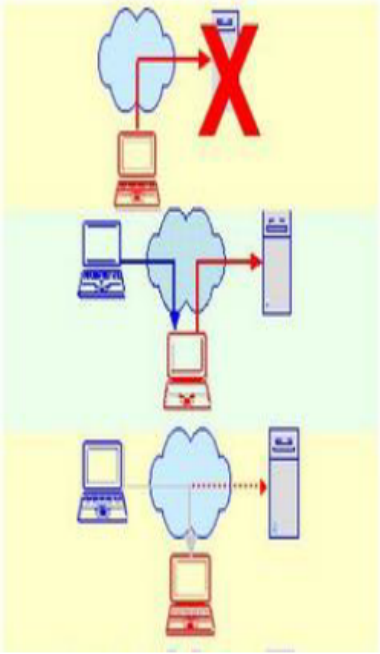
-L'accès au médium est souvent facile/faisable notamment sans-fil (Wifi, GSM, etc.)

-Risque de Divulgation de Données Importantes ou sensible



Attaques Réseaux

Injection/Modification/Destruction



Destruction sélective de paquets
Modification sélective du contenu des paquets envoyés par une source
Injection de faux paquets au nom de la source

Attaques Réseaux

Usurpation d'Identité (Spoofing)

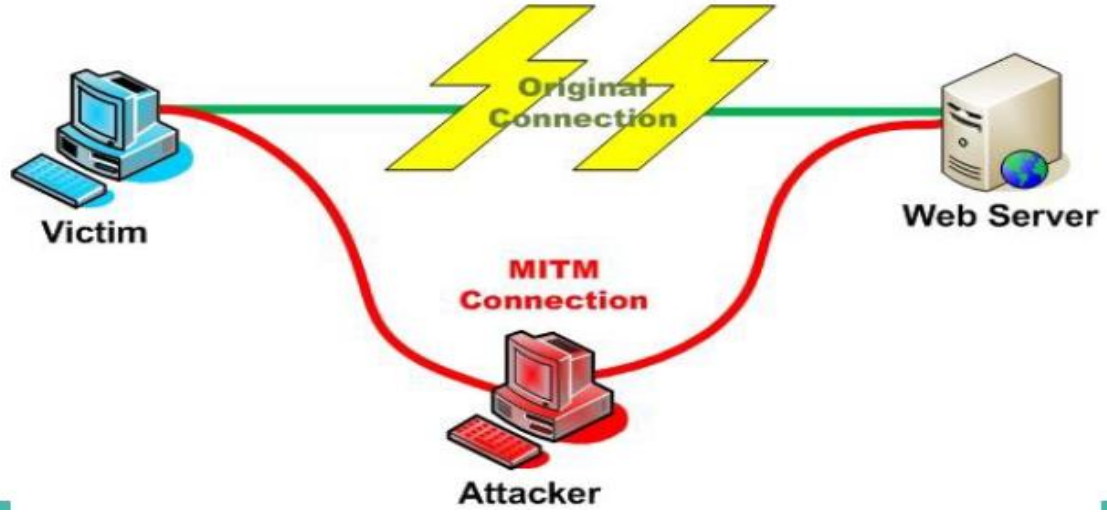
- Se faire passer pour quelqu'un d'autre (machine, personne, site web, etc.) , ceci afin de faire une action illicite au nom de la victime où de tirer profit des privilèges de la victime
-Usurper l'@ MAC ou l'@ IP d'une machine, @ mail, etc.

- La base d'autres attaques:
-Homme au milieu
-Vol de session
-Déni de Service Distribué (DDoS)

Attaques Réseaux

Homme au Milieu (Man-In-The-Middle)

- L'attaquant se situe au milieu de la communication. Il se fait passer pour le serveur quand il communique avec la victime, et se fait passer pour la victime quand il communique avec le serveur

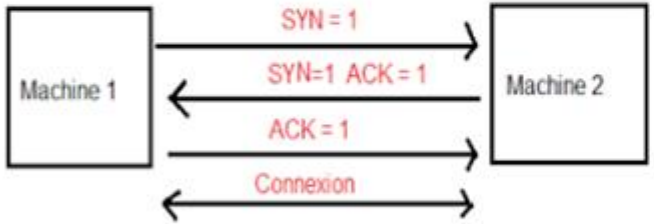


Attaques Réseaux

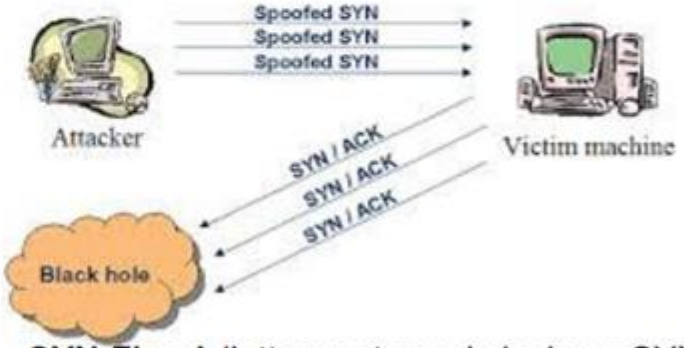
Déni de Service (DoS)

- **But:** Porter atteinte à la disponibilité d'une ressource

- **TCP-SYN Flooding:** saturer les ressources mémoire d'une machine (serveur) en induisant des connexion semi ouvertes par envoi de SYN



Connexion légitime:
Serveur (Machine 2) alloue des ressources (espace mémoire) pour chaque SYN, jusqu'à la réception de ACK



SYN-Flood: l'attaquant envoi plusieurs SYN frauduleux (@IP usurpées), qui ne seront jamais acquittés

Attaques Réseaux

Déni de Service (DoS) Distribué

- DoS dont la source est un ensemble de machines réel, le plus souvent des machines zombie

- **Botnet (Zombie)** : ensemble de machines infectées, contrôlées par un attaquant, et servant entre autres à effectuer un DDoS

-Détection difficile → difficile de différencier une requête légitime d'une requête zombie
-Saturation de la bande passante de la victime
-Saturation des ressources calcul/stockage de la victime
-Empêche des connexions en provenance de clients légitimes

Attaques Réseaux

Vol de Session (Session Hijacking)

-**But**: détourner un session (TCP, UDP) établit entre le client et le serveur. -Le client doit présenter un **password** pour pouvoir établir la session, que l'attaquant ne possède pas. Après authentification, la communication n'est plus sécurisé entre client/serveur
-Une fois l'authentification passée, l'attaquant récupère le *numéro de session* (**ID Session**) échangé, usurpe l'@IP du serveur, puis envoi un message de fermeture de session au client
-Ensuite, il usurpe l@IP du client et continue la session avec le serveur en utilisant **ID Session** **-L'attaquant doit être sur le même réseau que la victime ou le serveur pour réussir**