Réseaux avancés et sécurité

Sidi Biha

SupNum

2023-2024

Plan

1. Définitions
2. Risques
3. Attaques informatiques
4. Logiciels malveillants
5. Attaques distantes

Définitions

La sécurité informatique

L'ensemble des moyens mis en oeuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.

Objectif

La sécurité informatique à pour objectif d'assurer que les ressources logicielles et/ou matérielles d'un environnement informatique sont uniquement utilisées dans le cadre prévu et par les personnes autorisées.

Exigences fondamentales de sécurité

- **Confidentialité** : seules les personnes habilitées doivent avoir accès aux données. Seuls les acteurs de la transaction possèdent la clé de compréhension des données.
- **Intégrité** : garantir à chaque instant que les données n'ont pas subi d'altération (volontaire ou non). Les données doivent être intégrale, authentique et valide.
- **Authentification** : limiter l'accès aux personnes autorisées. S'assurer de l'identité d'un utilisateur avant l'échange de données.
- **Non-répudiation** : une transaction ne peut être niée par aucun des participants. La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues.
- **Disponibilité** : s'assurer du bon fonctionnement du système, de l'accès aux services et ressources à n'importe quel moment.

Sécurité: facteur humain

- La sécurité d'un système entier est mesurée par la sécurité du maillon le plus faible.
- Un système peut être sécurisé techniquement mais est défaillant à cause du facteur humain.
- Le **facteur humain** peut remettre en cause toute la sécurité d'un système.

Risques informatiques

- La sécurité est un compromis entre couts, risques et contraintes.
- La formule de calcul du risque est la suivante :

$$Risque = \frac{Menace \times Vulnérabilité}{Contremesure}$$

- **Vulnérabilité** : C'est une faiblesse inhérente à un système (software ou hardware) dans un contexte particulier. Appelée parfois faille ou brèche.
- **Menace** : c'est le danger (interne ou externe) tel qu'un hacker, un virus, etc.
- **Contre-mesure** : c'est un moyen permettant de réduire le risque dans une organisation.

Typologie des risques informatiques

- En sécurité informatique, il existe deux grands types de risques :
- Risques humains : les plus importants, même s'ils sont le plus souvent ignorés ou minimisés. Ils concernent les utilisateurs mais également les informaticiens.
- Risques matérielles : difficiles à prévoir, ils sont liés aux défauts et pannes inévitables que connaissent tous les systèmes matériels et logiciels.

Risques humains

- **La maladresse** : commettre des erreurs ou exécuter des traitement non souhaité, ou effacer involontairement des données ou des programmes...
- **L'inconscience et l'ignorance** : introduire des programmes malveillants sans le savoir (par exemple lors de la réception du courrier).
- **La malveillance** : certains utilisateurs peuvent volontairement mettre en péril le système d'informations, en y introduisant en connaissance de cause des virus ou en introduisant volontairement de mauvaises informations (par exemple dans une base de données).

Risques humains

- **L'ingénierie sociale** : une méthode pour obtenir d'une personne des informations confidentielles, que l'on n'est pas normalement autorisé à obtenir.
  - Se faire passer pour quelqu'un que l'on n'est pas (par exemple un administrateur réseau).
  - Demander des informations personnelles (nom, mot de passe, etc.) en utilisant un quelconque prétexte.
  - Peut se faire soit au moyen d'un simple appel téléphonique; soit par mail, soit en face à face.
- **L'espionnage** : surtout industriel, emploie les même moyens, ainsi que bien d'autres, pour obtenir des informations sur des activités d'un concurrent, projets en cours, futurs produits, politique de prix, clients, etc.

Risques matérielles

- **Les incidents liés au matériel** : la plupart des composants électroniques modernes produits en grandes séries, peuvent comporter des défauts de fabrication intentionnelles ou non.
- **Les incidents liés au logiciel** : ce sont les plus fréquents. Les systèmes d'exploitation et les programmes sont de plus en plus complexes. Ils font de plus en plus de choses. Ils nécessitent l'effort conjoint de dizaines, de centaines, voire de milliers de développeurs. Ces derniers peuvent faire des erreurs de manière individuelle ou collective que les meilleures méthodes de travail et les meilleurs outils de contrôle/test ne peuvent pas éliminer en totalité.
- **Les incidents liés à l'environnement** : les machines électroniques les réseaux de communication sont sensibles aux variations de températures ou de l'humidité ainsi qu'aux champs électromagnétiques.

Principal défauts de sécurité informatiques

- Authentification faible, mot de passe inexistant ou par défaut.
- Télémaintenance (connexion à distance) sans contrôles forts.
- Installation/Configuration par défaut.
- Manque de mise à jours.
- Outils de test laissés en place dans l'environnement de production.
- Services inutiles conservés.
- Pas de séparation des flux de données (entre utilisateurs normaux et administrateurs).
- Procédures de sécurité obsolètes (inefficaces).

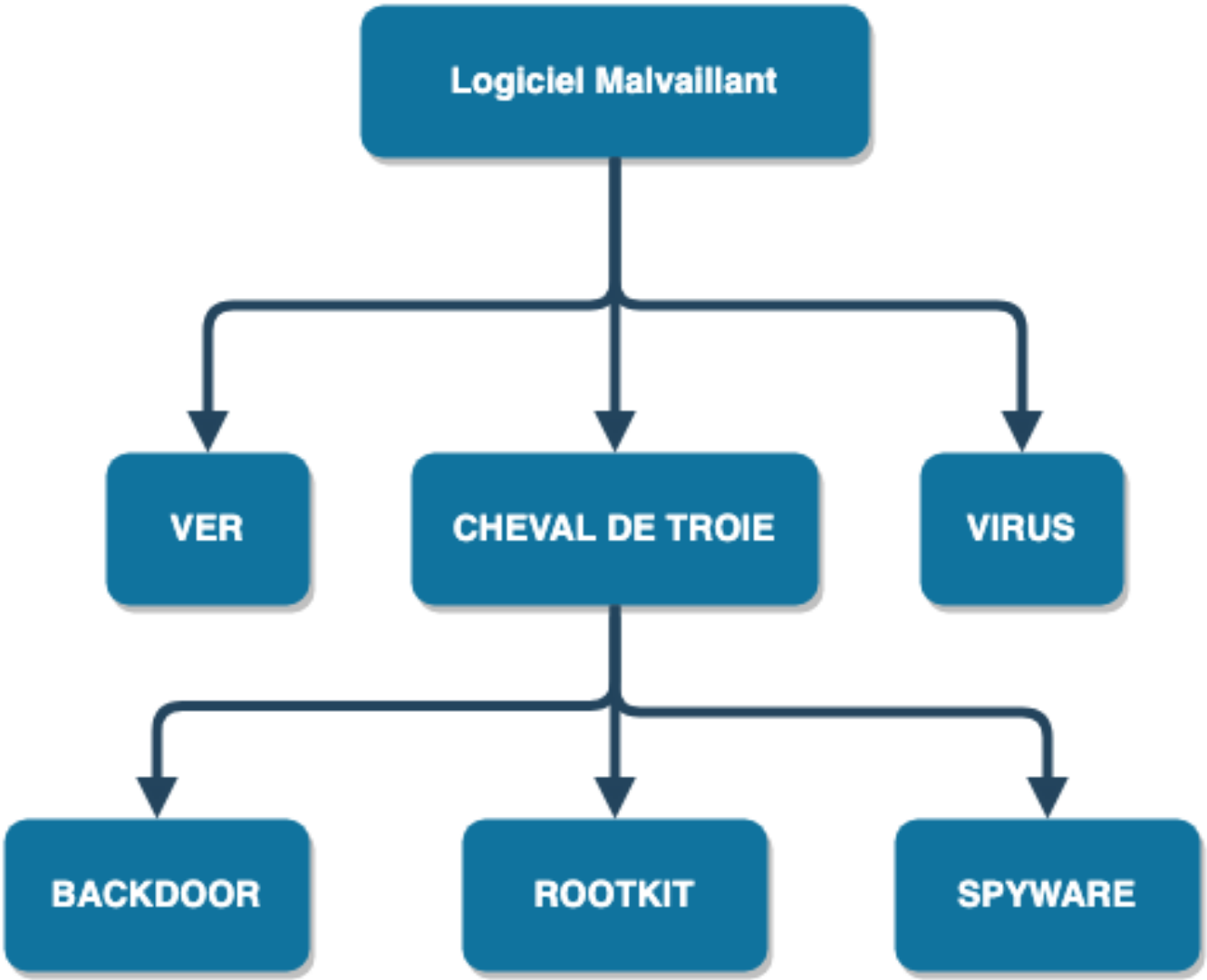
Les attaques informatiques

- Attaque locale
  - programme s'exécutant localement sur la machine.
  - nécessite une intervention utilisateur.
  - exemples : Virus, spyware ...
- Attaque distante
  - profite de vulnérabilités dans une application/service réseau.
  - nécessite peut/pas d'intervention utilisateur.
  - exemples : DOS, DNS spoofing, SQL Injection ...
- Une combinaison des deux : attaques sophistiquées.

Logiciels malveillants

- Programme développé dans le but de nuire à un système informatique.
- Ne se limite pas aux virus, englobe les vers, cheval de Troie toutes les autres menaces.
- Classés en fonction des trois mécanismes suivants :
  - **La propagation** : comme le logiciel se propage.
  - **Le déclenchement** : quel événement ou action déclenche le logiciel.
  - **La charge utile** : quelles sont les actions exécuté par la logiciel.

Logiciels malveillants



Logiciels malveillants

- Ver : logiciel malveillant qui se reproduit en utilisant un réseau informatique comme l'internet.
- Virus : logiciel malveillant auto réplicatif.
- Cheval de Troie : logiciel en apparence légitime, mais qui contient des fonctionnalités malveillante.
  - Backdoor : porte dérobée, programme qui va s'exécuter discrètement sur une machine(ordinateur, routeur, téléphone...) pour y activer ou créer une faille de sécurité.
  - Rootkit : logiciel furtif dont le but est d'obtenir et pérenniser un accès.
  - Spyware : logiciel espion, collecte et transmet des informations sur l'environnement dans lequel il est installé.

Logiciels malveillants

- Des logiciels malveillants ont été développés pour un grand nombre de systèmes d'exploitation et d'applications.
- Les auteurs de virus privilégient les systèmes d'exploitation largement utilises; les systèmes comportant des vulnérabilités.
- Le volume de logiciels malveillants destinés à Windows, Linux, Android et IOS est proportionnel à leurs parts de marche respectives.

Les Virus

Définition

Un virus informatique est un programme auto réplicatif contenant du code malveillant, conçu pour se propager à d'autres ordinateurs en s'insérant dans des logiciels légitimes.

- Il peut perturber plus ou moins gravement le fonctionnement du système infecté.
- Il peut se répandre par tout moyen d'échange de données numériques : réseaux, CD-ROM, clefs USB, disques durs, Bluetooth ...
- Objectifs :
  - Se dissimuler le plus longtemps possible.
  - Se répandre le plus largement possible.
  - Contaminer tout ce qui à sa portée.

Les Vers

Définition

Un ver informatique est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique (par exemple l'internet). Il a la capacité de se dupliquer une fois qu'il a été exécuté. Contrairement au virus, le ver se propage sans avoir besoin de se lier à d'autres programmes.

- exploitent les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.
- Utilisent, la plupart du temps, des failles de logiciels pour se propager.
- Objectifs :
  - Espionner l'ordinateur où il se trouve.
  - Offrir une porte dérobée à des pirates informatiques.
  - Détruire des données sur l'ordinateur ou il se trouve ou y faire d'autres dégâts.
  - Envoyer de multiples requêtes vers un site Internet dans le but de le saturer (attaque par déni de service ou DOS)

Cheval de Troie

Définition

Un programme d'apparence inoffensive, mais qui en contient un autre programme malveillant. Il est installé par l'utilisateur ignorant qu'il fait pénétrer un intrus malveillant sur son ordinateur.

- Prend souvent l'apparence d'un logiciel existant et utile.
- Se cache souvent dans les logiciels piratés.
- Objectifs :
  - Espionner l'ordinateur où il se trouve.
  - Avoir accès à la machine de la victime.

Rootkit

Définition

Un ensemble de techniques mises en oeuvre par un ou plusieurs logiciels, dans le but d'obtenir et de pérenniser un accès (généralement malveillants) à un ordinateur de la maniéré la plus furtive possible.

- Le terme peut designer la technique de dissimulation ou plus généralement un ensemble particulier de programmes mettant en œuvre cette technique.
- Difficile à détecter et à supprimer.
- Objectifs :
  - Utilisations des ressources de la machine cible (processeurs, connexion réseaux. . .).
  - Espionnages : accès aux données locales et/ou en transit.
  - Furtivité : se cacher des programmes de contrôles du système d'exploitation et de l'antivirus.
  - Protection contre la piraterie.

Attaques distantes

Définition

Actions malveillante exécuté à distance en utilisant une vulnérabilité ou faiblesse d'un protocole ou d'une application de communication réseau.

- Exploite des mauvaises configurations, des failles d'applications/protocoles, des portes dérobées.
- Objectifs :
  - Espionnage.
  - Denis de service.
  - Mystification (Spoofing).

Attaques distantes: Sniffing

Définition

Ecoute ou copie du trafic interne ou en transite dans un réseau informatique, parfois à l'insu des utilisateurs et des administrateurs.

- Utilisée pour l'espionnage, le vol de données (MITM).
- Effectif dans des réseaux wifi ou avec une connexion via un hub.
- Peut être mis en place comme un mécanisme de défense : le monitoring du réseau.

Attaques distantes: Déni de service

Définition

Paralyser une application ou un réseau informatique afin de l'empêcher de fournir les services qu'il devrait fournir.

- **Saturation d'un serveur** : attaque faisant planter un système (en général celui d'un serveur), en surchargeant ses ressources.
- **Saturation d'un réseau** : attaque submergeant un réseau d'un flot de trafic plus grand qu'il n'est capable de traiter, la bande passante est alors saturée et le réseau devient indisponible.
- **DDoS** : Distributed Denial of Service, une parallélisation d'attaques DoS.

Attaques distantes: Déni de service

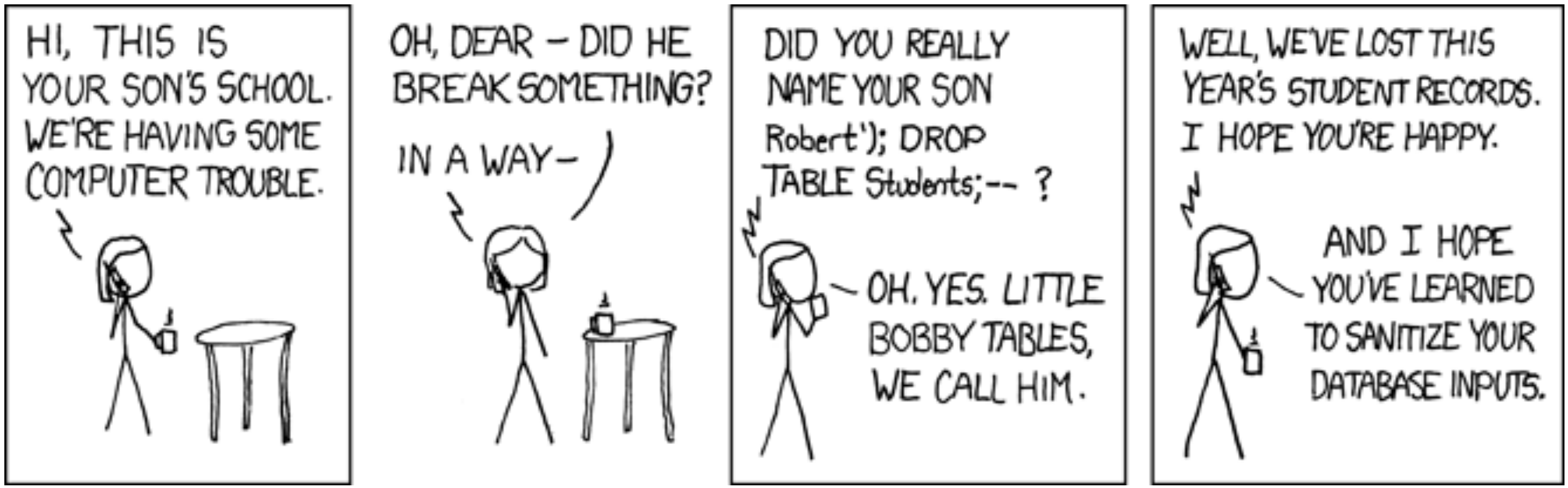
Exemples :

- **Attaque ARP** : demandes incessantes ARP envoyées vers un routeur ou serveur d'un même réseau.
- **ping de la mort** : ICMP echo request de taille supérieure (65535 octets) au maximum spécifié.
- **Attaque Smurf** : inondation de ICMP echo request avec pour adresse IP source l'adresse de la victime et pour destination l'adresse de diffusion du réseau.
- **Host Unreachable** : envoi de message ICMP "Host unreachable" à la victime (déconnexion des session)
- **SYN Flood** : inondation de demandes d'ouverture de session TCP.
- **Evasive UDP Attack** : inondation de paquets UDP de longueur variable et d'adresse source IP aléatoire vers la victime.
- **mail bombing** : avalanche d'e-mail sur le compte d'un utilisateur ou sur un serveur pour l'engorger.

Attaques distantes: Spoofing

- **ARP Cache Poisoning** : envoi ARP reply au routeur en prétendant être la machine dont on a usurpé l'identité. Envoi ARP reply à la machine victime en prétendant être le routeur. Tout le trafic entre la victime et le routeur passe par l'attaquant.
- **IP spoofing** : usurpation d'adresse IP en faisant croire que la requête provient d'une autre machine (adresse IP).
  - **ICMP/UDP** : facile de mettre en place vu l'absence de session.
  - **TCP** : plus compliquer à mettre en place vu la présence de numéro de séquence de session.
- **DNS spoofing** : usurpation de nom de domaine en remplaçant l'adresse IP retournée par le serveur DNS par une adresse contrôlée par l'attaquant.

Attaques Web



Attaques Web

- SQLI : *SQL Injection*
  - SQLI : exécuter des requêtes SQL malveillantes sur une base de données.
- XSS : *cross-site scripting*
  - injecter du contenu malveillant (HTML/CSS) dans le code client généré par une application web.
- CSRF : *Cross-site Request Forgeries*
  - faire exécuter des requêtes HTTP involontairement aux utilisateurs d'une application web vulnérable.