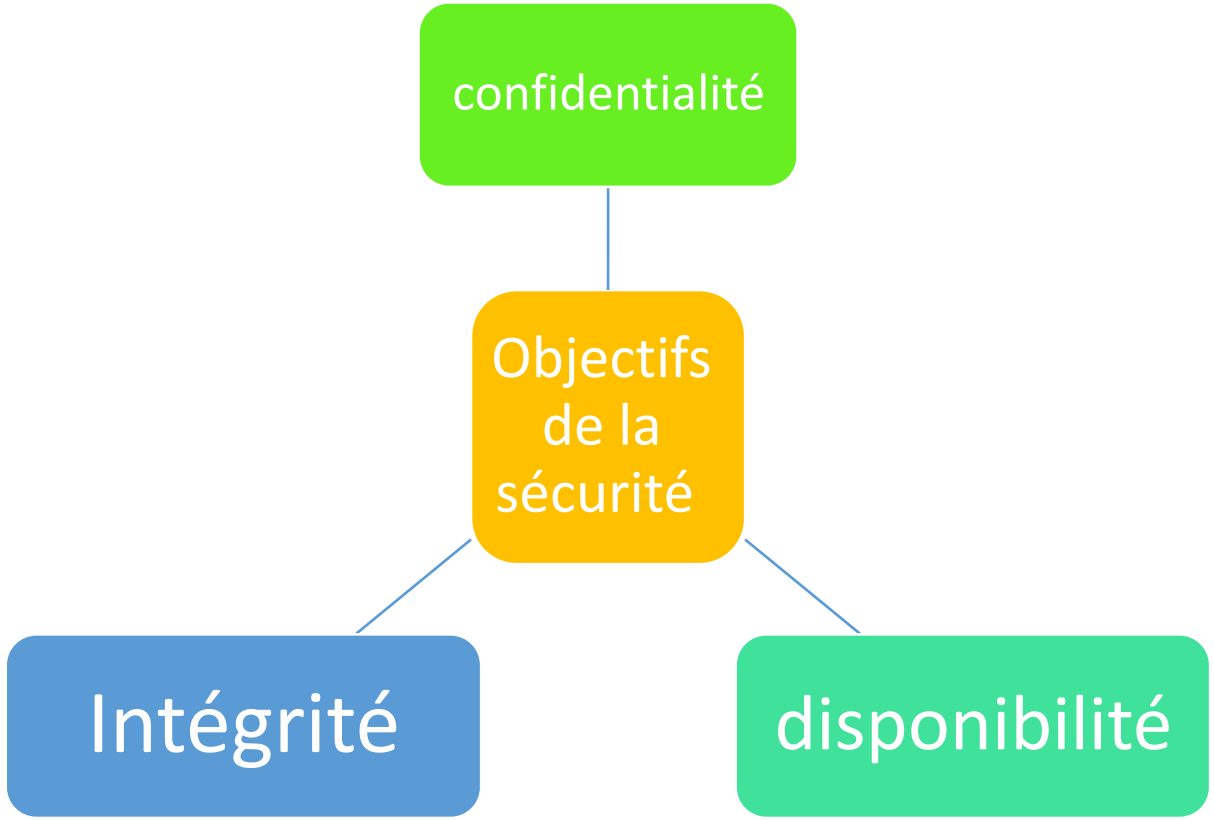
BELOUCIF ASSIA

Chapitre 1: Introduction aux concepts de sécurité

Objectifs de la sécurité



1.1 La confidentialité

- La confidentialité c’est interdire l’accès a l’information aux personnes non autorisées

L’intégrité

- Les informations doivent être constamment modifiées. L'intégrité signifie que les modifications ne doivent être effectuées que par des entités autorisées et par le biais de mécanismes autorisés.

1.3 Disponibilité

- Les informations créées et stockées par une organisation doivent être accessibles aux entités autorisées.

Terminologie:

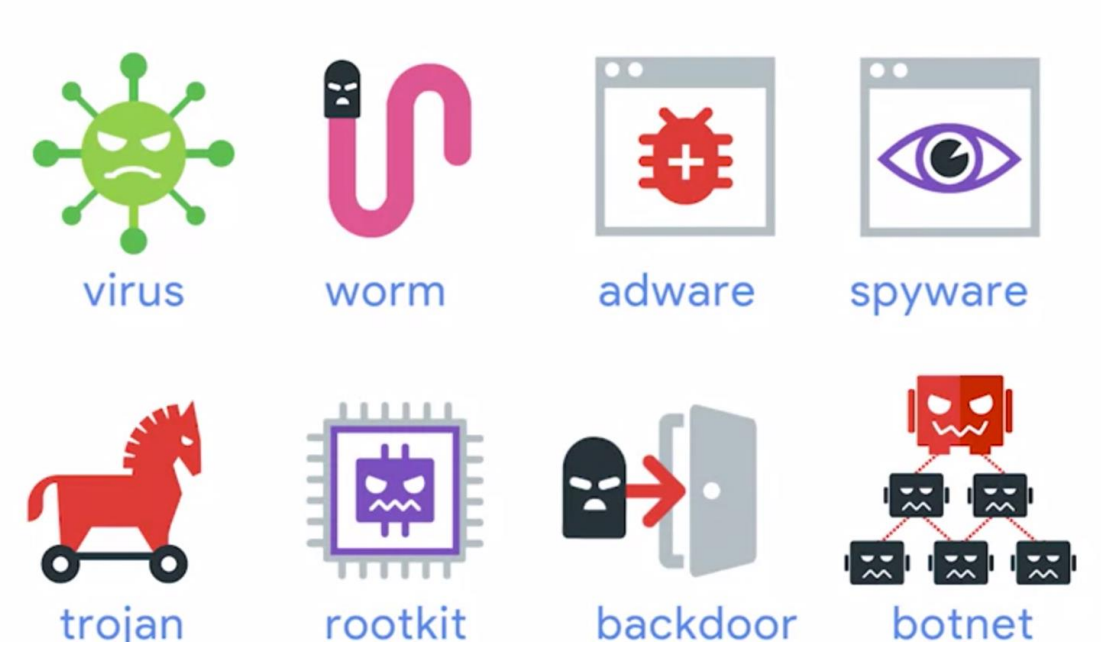
- **Risque:** La possibilité de subir une perte en cas d'attaque du système.
- **Vulnérabilité:** Une faille dans le système qui pourrait être exploitée pour compromettre le système. Il peut y avoir des vulnérabilités liées aux failles laissée sans se rendre compte.
- **Vulnébilité zéro-day:** C'est une vulnérabilité qui n'est pas connue du développeur ou du fournisseur du logiciel, mais qui est connue par un attaquant. Le nom fait référence au temps que le fournisseur du logiciel aurai pour réagir et corriger la vulnérabilité, zéro jour.

Terminologie(2)

- **Exploit:** Est un programme utilisé pour profiter d'un bug de sécurité ou d'une vulnérabilité pour causer des dommages au système.
- **Menace:** danger possible qui peut exploiter une vulnérabilité.
- **Pirate informatique:** quelqu'un qui tente de s'introduire à un système ou de l'exploiter.
- **Attaque:** tentative réelle de nuire à un système

Les malwares (Programmes malveillants)

- Les malwares sont des logiciels utilisés pour obtenir les informations sensibles ou supprimer ou modifier des fichiers.
- Ils existes plusieurs types de malwares, on va parler des types les plus courants



Virus

- On peut lancer une attaque au niveau application ou une attaque au niveau du réseau à l'aide d'un virus.
- Un virus est un code(programme) qui s'attache au code du programme légitime et s'exécute lorsque le programme légitime s'exécute. Il peut alors infecter d'autres programmes de cet ordinateur ou des programmes qui se trouvent sur d'autres ordinateurs mais sur le même réseau.
- Les virus peuvent également être déclenchés par des événements spécifiques (par exemple, un virus peut s'exécuter automatiquement à midi tous les jours).

Ver

- Un ver est similaire dans son concept à un virus, alors qu’il est différent dans sa mise en œuvre. Le virus modifie le programme (c'est-à-dire qu'il s'attache au programme attaqué) tandis que le ver se reproduit par lui-même afin de rendre l'ordinateur ou le réseau attaqué inutilisable en consommant toutes ses ressources.

Ver(2)

- ILOVEYOU ou Love Bug est un cas célèbre de ver informatique qui s'est propagé à des millions de machines Windows.
- Le ver se propageait par e-mail. Il y avais un attaquant qui envoyait un message avec un sujet I Love You et une pièce jointe qui était en fait le ver déguisé en fichier texte de lettre d'amour.
- Le fichier joint était en fait un fichier exécutable qui, une fois ouvert, exécutait de nombreuses attaques comme: se copier dans plusieurs fichiers et dossiers, lançait d'autres logiciels malveillants, remplaçait des fichier….
- Le ver s'est propagé en volant des adresses e-mails qui se trouvaient dans l'ordinateur de la victime et des clients de chat. Il a ensuite procédé à l'envoi de cet e-mail à tous les membres du carnet d'adresses.
- Le Love Bug s'est répandu à travers le monde et a causé des milliards de dollars de dégâts.
- Ce n'était qu'une des nombreuses raisons pour lesquelles on doit jamais ouvrir des pièces jointes d'un e-mail qu'on ne reconnaisse pas.

Logiciel publicitaire(adware):

- Un adware est un logiciel qui affiche des publicités et collecte les données.
- Parfois, on téléchargeons légitimement des logiciels publicitaires. Cela se produit lorsqu'on accepte les conditions d'utilisation qui nous permettent d'utiliser des logiciels gratuits.
- D'autres fois, ils peuvent être installés sans la conscience des utilisateurs et peuvent faire des actions malveillantes que de simples affichages de publicités

Cheval de Troie

- Programme malveillant dissimulé à l'intérieur d'un autre programme en apparence inoffensif (par exemple un jeu ou un utilitaire).
- Le rôle d’un cheval de Troie est essayer de révéler des informations confidentielles à un attaquant.
- L'histoire raconte que des soldats grecs se sont cachés à l'intérieur d'un grand cheval creux, qui a été tiré dans la ville de Troie par ses citoyens, ignorant son contenu. Une fois que les soldats grecs sont entrés dans la ville de Troie, ils ont ouvert les portes pour le reste des soldats grecs.

Logiciel espion(spyware)

- Les spywares sont le type de logiciels malveillants destinés à l’espionnage.
- Ce qui peut signifier surveiller vos écrans d’ordinateur, les pressions sur les touches, les webcams et ensuite rapporter ou diffuser toutes ces informations à une autre partie.

Keylogger:

- Un keylogger est un type courant de logiciel espion utilisé pour enregistrer tout ce qui est tapé au clavier.
- Il peut capturer tous les messages que vous tapez, vos informations confidentielles, vos mots de passe et même plus.
- Utilisé aussi dans l’espionnage industriel pour récupérer des rapports et des documents confidentiels

Rançongiciel (ransomware)

- Un rançongiciel est un programme conçu pour bloquer l'accès à un système informatique, par le chiffrement de contenu, jusqu'à ce qu'une somme d'argent soit payée.
- L'attaque de ransomware **WannaCry**(mai 2017) fut un cas récent de ransomware. Le malware a profité d'une vulnérabilité dans les anciens systèmes Windows, infectant des centaines de milliers de machines à travers le monde(toutes les versions antérieures à Windows 10 n'ayant pas effectué les mises à jour de sécurité). Plus particulièrement, l'attaque a mis hors service les systèmes des services de santé nationaux en Angleterre, provoquant une crise sanitaire. Cette cyberattaque est considérée comme le plus grand piratage à rançon de l'histoire d'Internet

Botnets

- Les pirates créent un réseau de machines piratées, appelées réseaux de zombies, en diffusant du code malveillant par le biais de courriels, de sites Web et de médias sociaux. Une fois que ces ordinateurs sont infectés, ils peuvent être contrôlés à distance, à l'insu de leurs propriétaires, et utilisés comme une armée pour lancer une attaque contre n'importe quelle cible.

Porte dérobée (Backdoor)

- Les portes dérobées sont le plus souvent installées après qu'un attaquant obtient l'accès à un système et veut conserver cet accès. Même si on découvre que le système a été compromis, on ne peut pas s'assurer qu'une porte dérobée n'existe pas sur le système.

Rootkit

- Un rootkit, de par son nom, est un kit pour root, c'est-à-dire une collection de logiciels ou d'outils qu'un administrateur utiliserait. Il permet de modifier un système d'exploitation au niveau de l'administrateur.
- Un rootkit peut être difficile à détecter car il peut se cacher du système en utilisant le système lui-même.
- Le rootkit peut exécuter de nombreux processus malveillants, mais en même temps ces processus n'apparaîtraient pas dans le gestionnaire de tâches car il peut cacher sa propre présence.

Bombe logique

- Une bombe logique est un type de logiciel malveillant, installé intentionnellement, dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel appel au système.
- Les bombes logiques sont généralement utilisées dans le but de créer un déni service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise !
- Il y a un cas célèbre de bombe logique qui s’est produit en 2006, dans lequel un administrateur système dans une banque, a déclenché une bombe logique et a fait tomber les services de la compagnie dans le but de faire baisser le prix de leurs actions. L’ancien employé a été attrapé et accusé de fraude, puis condamné à huit ans de prison

Les types de sécurité

1. La sécurité physique: La sécurité physique concerne tous les aspects liés à l'environnement dans lequel les ressources sont installées. Elle peut inclure :

- la sécurité physique des salles de serveurs, des périphériques réseau, etc.
- la prévention des accidents et des incendies ;
- les systèmes de l'alimentation ininterrompue ;
- la surveillance vidéo, etc.

Les types de sécurité

2. La Sécurité logique: La Sécurité logique fait référence à la mise en œuvre d'un système de contrôle d'accès, par logiciel, pour sécuriser les ressources. Elle peut inclure :

- l'application d'une stratégie de Sécurité fiable pour les mots de passe.
- l'instauration d'un modèle d'accès s'appuyant sur l'authentification, l'autori-Sation et la traçabilité .
- la configuration correcte des pare-feux de réseau
- l'installation des IPS (s5ystèmes de prévention d'intrusion)
- l'utilisation des VPN (réseau privé virtuel), ete.

Les types de sécurité

3. La sécurité administrative: La sécurité administrative permet d'assurer le contrôle interne d'une organisation à l'aide d'un manuel des procédures. Elle peut inclure :

- prévenir les erreurs et les fraudes ;
- définir les responsabilités respectives des différents intervenants ou opérateurs
- protéger l'intégrité des biens et des ressources de l'entreprise
- assurer l'enregistrement de toutes les opérations concernant la manipulation du matériel
- gérer rationnellement les biens de l'entreprise
- assurer une gestion efficace et efficiente des activités.

Les principaux risques liés à la sécurité logique :

Les différents types d'attaque réseau :

a.Les attaques de reconnaissance :

Une attaque de reconnaissance ou « attaque passive » a pour objectif de regrouper des informations sur le réseau cible pour déceler toutes les vulnérabilités. Cette attaque utilise, en général, les méthodes de base suivantes :

- ***un balayage de « ping »*** : l'attaquant envoie des paquets « ping » à une plage d'adresses IP pour identifier les ordinateurs présents dans un réseau ;
- **le balayage de port :** l'attaquant procède à une analyse de port (TCP et UDP) permettant de découvrir les services s'exécutant sur un ordinateur cible ;
- **une capture de paquets (sniffing) :** la capture de paquets permet de capturer les données (généralement des trames Ethernet) qui circulent sur le réseau en vue d'identifier des adresse MAC, des adresses IP ou des numéros de ports utilisés dans le réseau cible. Cette attaque permet même de découvrir des noms d'utilisateur ou des mots de passe. Les logiciels de capture de paquets les plus couramment utilisés sont **wireshark** et **tcpdump**.

- B. Les attaques du mot de passe :

- L’objectif de ces attaques est de découvrir les noms d’utilisateurs et les mots de passe pour accéder aux ressources. On distingue deux méthodes souvent utilisées dans ce type d’attaque :
- 1. **L'attaque par dictionnaire :** cette méthode se base sur une liste de mots ou de phrases souvent utilisés comme mots de passe ;
- 2. **L'attaque par force brute:** cette méthode essaie toutes les combinaisons possibles de lettres, de chiffres ou de symboles pour détecter le mot de passe d’un utilisateur.

- **c. Les attaques d’accès:**
- Ces attaques ont pour objectif d’essayer de récupérer des informations sensibles sur les éléments du réseau. Les méthodes suivantes sont courantes pour effectuer une attaque d’accès :
- **1.L'amorçonage (phishing) :** le phishing est une tentative de récupérer des informations sensibles (généralement des informations financières comme les détails de cartes de crédit, login, mot de passe, etc.), en envoyant des e-mails non sollicités avec des URL truqués ;
- **2.le pharming :** c’est une autre attaque de réseau visant à rediriger le trafic d’un site web vers un autre site web ;

- **3. L’attaque de « Man-in-the-middle » :** un attaquant se place entre deux éléments réseaux pour essayer de tirer profit des données échangées. Cette attaque se base, entre autres, sur les méthodes suivantes :
- **l’'usurpation d’identité (spoofing) :** c’est une pratique dans laquelle la communication est envoyée à partir d’une source inconnue déguisée en source fiable du récepteur. Elle permet de tromper un firewall, un service TCP, un serveur d’authentification, etc. L’usurpation d’identité peut avoir lieu à différents niveaux : une adresse MAC, une adresse IP, un port TCP/UDP, un nom de domaine DNS.
- **le détournement de session (hijacking) :** l’attaquant pirate une session entre un hôte et un serveur pour obtenir un accès, non autorisé, à ce service. Cette attaque s’appuie sur le spoofing.
- **4.les attaques mélangées :** les attaques mélangées combinent les caractéristiques des virus, des vers et d’autres logiciels pour collecter des informations sur les utilisateurs.

- d. Les attaques du réseau contre la disponibilité:
- 1.**Les attaques DoS (Denial of Service):** consistent à rendre indisponible un service de diverses manières. Ces attaques se divisent, principalement, en deux catégories
- **les dénis de service par saturation:** ils consistent à submerger une machine de fausses requêtes afin qu'elle soit incapable de répondre aux requêtes réelles ;
- **les dénis de service par exploitation de vulnérabilité :** ils consistent à exploiter une faille du système distant afin de le rendre indisponible.

- **2.Les attaques DDoS (Distributed Denial of Service):** relèvent d’un type d’attaque « DoS », provenant de nombreux ordinateurs connectés, contrôlés par les hackers, qui attaquent différentes régions géographiques. Le principe de ces attaques se base, entre autres, sur les méthodes suivantes :
- **L'attaque SYN flood :** un attaquant envoie de nombreux paquets TCP-SYN pour lancer une connexion « TCP », sans envoyer un message « SYN-ACK » ;
- **l'attaque ICMP flood :** un attaquant envoie de nombreux faux paquets ICMP vers l'ordinateur cible.

- **3.Les différentes attaques sur un programme :**
- **a. Débordement du tampon :**
- est un bug par lequel un processus, lors de l'écriture dans un tampon, écrit à l'extérieur de l'espace alloué au tampon, écrasant ainsi des informations nécessaires au processus. Lorsque le bug se produit, le comportement de l'ordinateur devient imprévisible. Il en résulte souvent un blocage du programme, voir de tout le système. Le bug peut aussi être provoqué intentionnellement et être exploité pour compromettre la politique de sécurité d’un système.

- **b. Cross site scripting:**
- Le cross-site scripting (abrégé XSS) est un type de faille de sécurité des sites web permettant d'injecter du contenu dans une page, provoquant ainsi des actions sur les navigateurs web visitant la page. Les possibilités des XSS sont très larges puisque l'attaquant peut utiliser tous les langages pris en charge par le navigateur (JavaScript, Java...) et de nouvelles possibilités sont régulièrement découvertes notamment avec l'arrivée de nouvelles technologies comme HTML5.

- **c. Injection SQL:**
- L'attaque SQL consiste à modifier une requête SQL en cours par l'injection d'un morceau de requête non prévu, souvent par le biais d'un formulaire. Le hacker peut ainsi accéder à la base de données, mais aussi modifier le contenu et donc compromettre la sécurité du système.

Taxonomie des attaques par rapport aux objectifs de sécurité