CENTRE UNIVERSITAIRE DE MILA
DEPARTEMENT MATHEMATIQUE ET INFORMATIQUE

Cours Sécurité des Réseaux

Master 1 I2A

Chapitre I: Aspects généraux de la sécurité

Introduction

Les attaques informatiques

- Elles surgissent à l'ombre de tout actif informationnel.
- Leur existence s'étend depuis l'air de la centralisation.
- Ces actions illicites ont évolué en complexité et en sévérité parallèlement à l'évolution d'Internet.

Types d'attaques

- Attaques directes;
- Attaques indirectes.

Exemples d'attaques fréquentes

- Déni de service;
- Propagation du code malicieux.

Introduction

- L'information en transit sur un réseau
  - Elle peut être interceptée
  - Cible à la destruction, modification et falsification
- L'infrastructure réseau elle aussi est une cible aux attaques

Les risques sont significatifs : plusieurs organisations ont perdu leur productivité et leur réputation.

Les besoins de sécurité sont d'une considération majeure pour minimiser le risque d'exposition aux attaques

Plan

1. Terminologie
2. Les attaques informatiques
    1. Définition d'une attaque
    2. Méthodologie d'une attaque typique
    3. Les Types d'attaques
    4. Exemples d'attaques spécifiques
3. La sécurité informatique
    1. Définition
    2. Principes de base
    3. Processus
4. Les services de la sécurité informatique
5. Les principaux mécanismes de sécurité informatique
6. Conclusion

Terminologie

- **Actif**
- Élément de valeur
- Dans le contexte de la sécurité informatique, il consiste en :

  l'information, le matériel et les logiciels.

- **Vulnérabilité**
- Une condition, une faiblesse ou une absence dans les procédures de sécurité.
- Erreur d'ingénierie, un défaut de conception ou d'implémentation
- C'est le point susceptible d'être exploitée, de manière intentionnelle ou accidentelle, pour compromettre un actif ou nuire à la sécurité d'un système.

Terminologie

- **Menace**
- Une entité ou un évènement indésirable ayant le pouvoir de causer un dommage à un actif.
- Elle se présente comme étant une violation potentielle de la sécurité d'un système.
- Elle peut exister en raison de vulnérabilité
- Elle peut être :
  - Une erreur;
  - Un utilisateur mal intentionné;
  - Une défaillance dans un système;
  - Un bogue dans un logiciel;
  - Un feu; une inondation; un virus, ..etc.

Terminologie

- **Risque**
  - Une mesure de danger ciblant un actif.
  - C’est la mesure de coût associée à l’exploitation d’une vulnérabilité.
  - Le risque étant résiduel, son élimination entière est impossible.
- **Incident de sécurité**

Tout évènement ayant des implications négatives sur la sécurité d’un système ou un actif. Un incident de sécurité peut cibler des centaines de sites et peut paralyser leurs activités pour une longue période de temps.

- **Contre mesure**

Ensemble des procédures et des pratiques adoptées pour corriger une vulnérabilité ou contrer une menace.

Terminologie

Il existe une corrélation entre les termes actif, vulnérabilité, menace et risque :

- Une vulnérabilité expose un actif au risque.
- Une menace peut exploiter une vulnérabilité pour occasionner un dommage à un actif.

Les attaques informatiques

Définition d'une attaque

- Action qui compromet la sécurité de l'information ou d'un système
- Acte volontaire illicite mené par un adversaire, dit attaquant, contre un autre adversaire, dit victime.

Point de vue de la victime : une attaque est une série d'évènements consécutifs qui a des conséquences nuisibles sur la sécurité des actifs.

Réflexion de l'attaquant : une attaque étant un mécanisme pour accomplir un objectif.

- Une attaque concrétise une menace.
- Une attaque est le moyen employé pour exploiter une vulnérabilité.

Les attaques informatiques

Méthodologie d'une attaque typique

De manière générale, les attaques informatiques enchaînent deux phases consécutives qui sont :

1 Phase pré-attaque

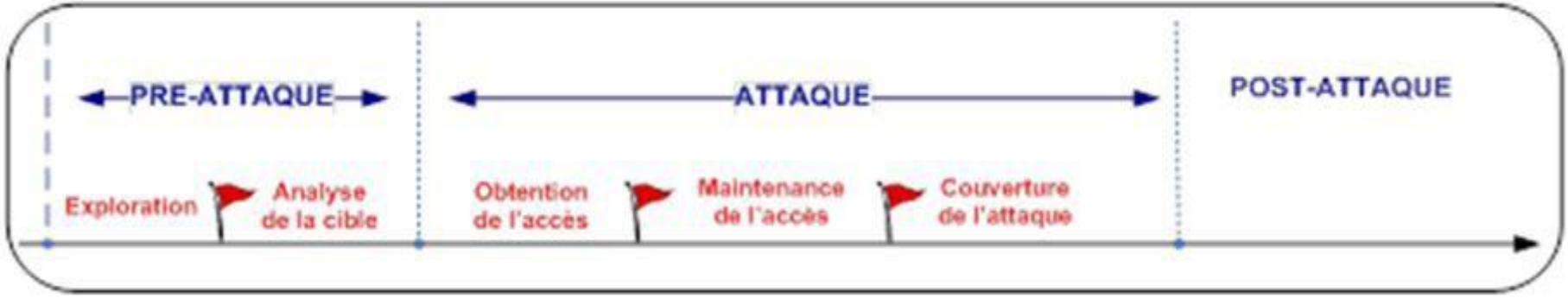
2 Phase attaque

1. Phase pré attaque

Elle inclus deux étapes qui sont :

1- l'exploration

2- Analyse de la cible



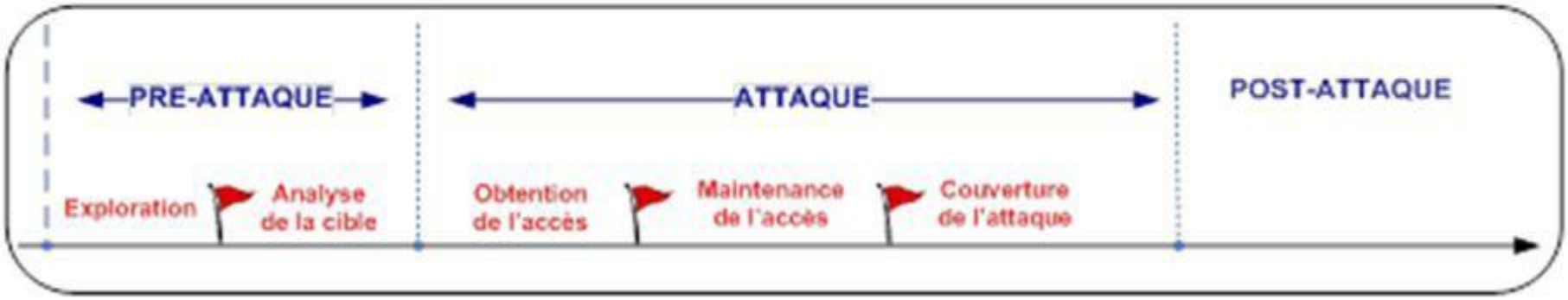
Les attaques informatiques

Méthodologie d'une attaque typique

1. Phase pré attaque

1.1 L'exploration

Avant de lancer une attaque, l'attaquant doit d'abord fixer sa cible. Pour cela, il procède par une exploration d'Internet en effectuant des recherches dans le Web, la base de données « whois » et les serveurs de nom. L'attaquant emploie aussi les outils de reconnaissance pour découvrir l'infrastructure victime.



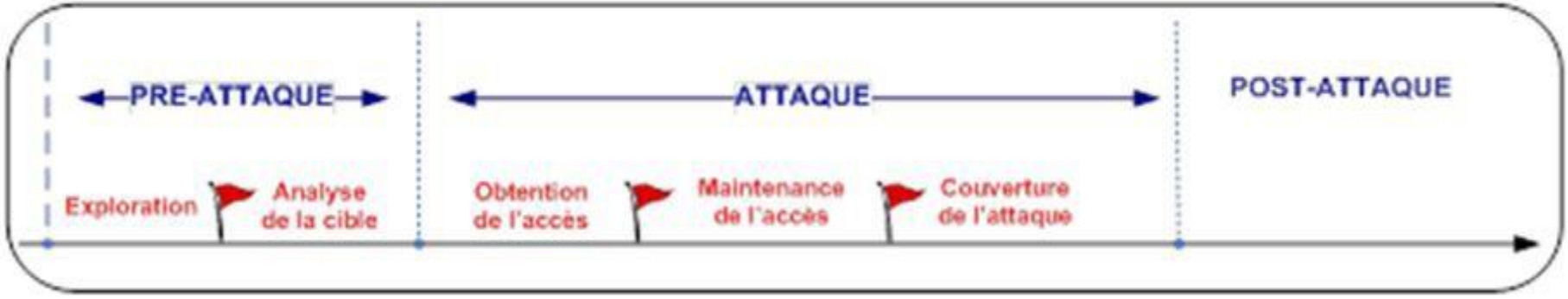
Les attaques informatiques

Méthodologie d'une attaque typique

1. Phase pré attaque

1.2 L'analyse de la cible

Une fois la victime est désignée, l'attaquant procède au scan du site ou du système cible pour collecter des informations qui puissent le guider pour monter son plan d'attaque. Ces informations sont généralement : la topologie du réseau, les ports ouverts, les adresses IP des hôtes en exécution. Le scan est effectué de manière automatique. Un grand nombre d'outils y sont disponibles sur Internet.



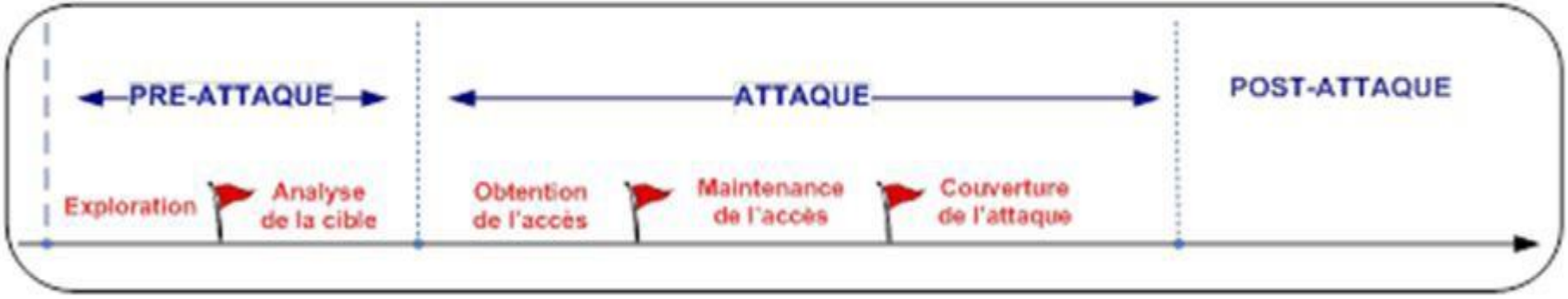
Les attaques informatiques

- **Méthodologie d'une attaque typique**

2. Phase attaque

2.1 Obtention de l'accès : grâce à la connaissance acquise, l'attaquant procède donc à l'attaque de la victime.

- Si l'attaquant est un utilisateur légitime du système, dans cette phase, il va opter pour plus de privilège (super utilisateur du système) en utilisant des moyens d'attaque systèmes et applications.



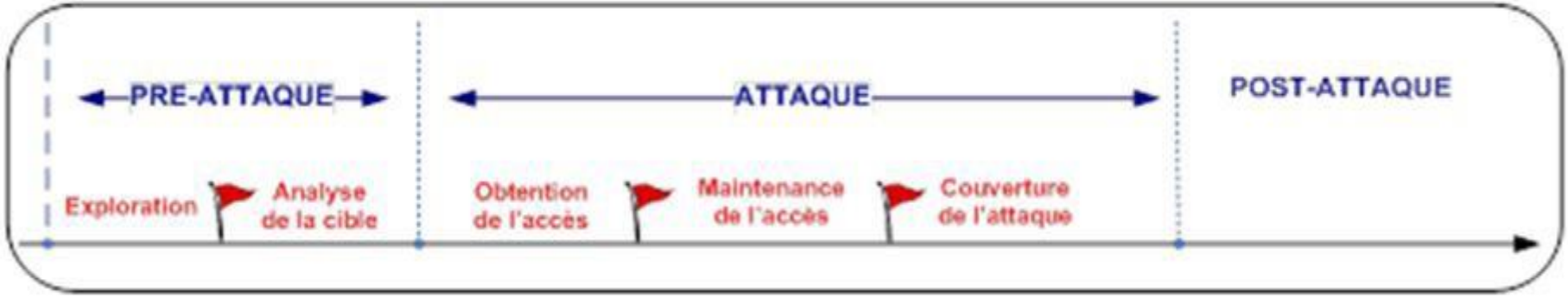
Les attaques informatiques

- **Méthodologie d'une attaque typique**

2. Phase attaque

2.1 Obtention de l'accès

- Si l'attaquant est externe, il tente de capturer le trafic réseau ou voler les sessions en utilisant des outils automatiques dédiés. Dans ce cas la plus part des attaquants ne s'intéressent pas à obtenir l'accès système mais optent souvent pour la perturbation du réseau et empêcher les utilisateurs légitimes d'utiliser les ressources.



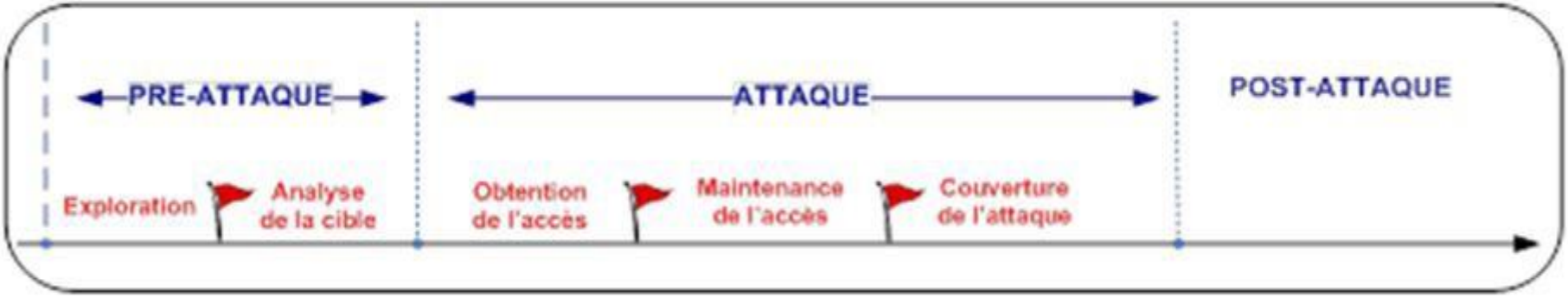
Les attaques informatiques

Méthodologie d'une attaque typique

2. Phase attaque

2.2 Maintenir l'accès

La règle d'or pour les attaquants pénétrant dans un système ou un réseau est d'ancrer cette présence. Divers outils et techniques sont disponibles pour rendre cette présence malicieuse inaperçue tels que les backdoors et les Rootkits.



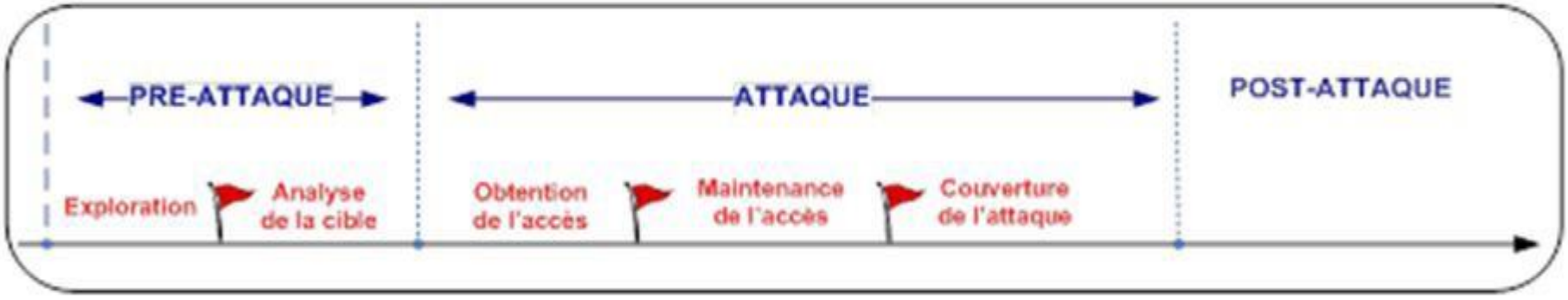
Les attaques informatiques

Méthodologie d'une attaque typique

2. Phase attaque

2.3 La couverture des attaques

Les outils utilisés pour maintenir l'accès permettent aux attaquants de dissimiler leurs traces. Malgré cette assurance, les attaquants tentent de modifier le mécanisme d'enregistrement des activités du système et créer des canaux cachés pour transmettre les données sans que la victime s'en aperçoive.



Les attaques informatiques

- **Les types d'attaque**
- **Attaque directe** : l'attaquant s'adresse directement à la victime.
- **Attaque indirecte** : l'attaquant envoie les paquets d'attaque à un système intermédiaire, qui répercute l'attaque vers la victime.
- **Les attaques externes :** ce sont des violations intentionnelles de la sécurité d'un système ou un actif. Elles sont originaires des hôtes externes et commises par des utilisateurs externes non autorisés d'une organisation.
- **Les attaques internes :** ce sont des actions non autorisées provenant des hôtes internes et initiées par les utilisateurs internes d'une organisation, qui abusent de leur privilège.

Les attaques internes constituent la grande partie des attaques commises. Les utilisateurs internes sont familiers aux systèmes et détiennent un accès direct.

Les attaques informatiques

- **Les types d'attaque**

- **Les attaques passives :** ce sont des actions inoffensives. Aucune manifestation n'est observable en terme de changement d'état du système ou modification des données. La surveillance du trafic réseau étant un bon exemple.

- **Les attaques actives :** elles se traduisent par une modification illégale de l'état du système, la perturbation de son fonctionnement normal, ou l'altération des données.

Les attaques informatiques

Quelques exemples d'attaques spécifiques

Deux exemples d'attaques les plus fréquentes et les plus dangereuses qui sont le code malicieux et l'attaque par déni de service.

Le code malicieux

Terme général qui se réfère aux logiciels nuisibles effectuant des actions malicieuses en arrière plan, sans que l'utilisateur s'en aperçoive.

Le code malicieux inclut les chevaux de Troie, les vers et les virus.

Les attaques informatiques

- **Quelques exemples d'attaques spécifiques**

- **Le code malicieux**

Les chevaux de Troie : le cheval de Troie tire son nom d'une ruse de guerre employée par les grecs quand ils assiégeaient la ville de Troie.

- Il se déguise en programme anodin pour réaliser des fonctions illicites telles que le vol des mots de passe ou la copie des données sensibles.

- Certains chevaux de Troie permettent l'administration à distance des systèmes tel est le cas de Back Orifice qui appartient au monde open source.

Les attaques informatiques

- **Quelques exemples d'attaques spécifiques**
- **Code malicieux**

Les vers

- Programmes qui se déclenchent et se répliquent de manière autonome.
- Ils exploitent les vulnérabilités pour se propager rapidement en utilisant les services réseaux tels que le partage de fichiers et la messagerie électronique.
- Parmi les vers les plus rapides de l'histoire le ver Slammer, qui est apparu en janvier 2003. Il a pu infecter 75 000 hôtes, à travers le monde, en paralysant 5 serveurs de noms racines.

Les attaques informatiques

- **Quelques exemples d'attaques spécifiques**

- **Le Code malicieux**

Les virus

- Programmes parasites qui se reproduisent lors de leur exécution en s'attachant aux exécutables existants.

- Ils peuvent se propager sur un réseau LAN ou WAN.

- Parmi les virus très connus et virulents de l'histoire, le virus Sasser, qui est apparu en l'an 2004. Il s'active dès que l'ordinateur est connecté à Internet. Après 60 secondes, il effectue un redémarrage automatique de la machine et se reproduit.

Les attaques informatiques

Quelques exemples d'attaques spécifiques

Le Code malicieux

Un code malicieux peut être à la fois un cheval de Troie, un virus et un ver tel est le cas de sasser qui est à la fois virus et vers.

Les attaques informatiques

Quelques exemples d'attaques spécifiques

Le déni de service

C'est une attaque qui consiste à interrompre le fonctionnement normal des applications et des serveurs critiques d'une organisation. L'objectif est d'empêcher les utilisateurs légitimes d'accéder aux services et aux ressources. Elle prend plusieurs formes telles que :

- La saturation d'un système en l'inondant avec une large quantité de trafic inutile dépassant sa capacité.
- L'épuisement d'une ressource limitée.
- La perturbation de la connexion réseau.

Les attaques informatiques

Quelques exemples d'attaques spécifiques

Le déni de service

L'attaque de déni de service, qui a marqué l'histoire, est celle initiée par l'adolescent canadien "**Mafiaboy**", en l'an 2000. Elle a affecté 13 serveurs de nom racines. Cette attaque a paralysé les sites populaires Yahoo, EBay, Amazon, CNN, …etc, pendant des heures.

La sécurité informatique

Les environnements informatiques jouent un rôle vital dans la société de l'information. Mais les attaques sont omniprésentes et coûteuses. Le risque étant significatif **Alors la sécurité informatique s'impose comme une exigence.**

 Définition

La sécurité informatique est la capacité d'un système de protéger ses objets contre l'utilisation et la modification des sujets non autorisés.

Les objets : ce sont les entités passives du système tels que les fichiers, les périphériques et les mécanismes de communication entre les processus.

Les sujets : ce sont les entités actives du système qui peuvent accéder aux objets du système et modifier leurs états. Il s'agit des utilisateurs humains ou les processus qui agissent pour leur compte.

La sécurité informatique

La sécurité informatique aborde dans un contexte global :

- **La sécurité physique :** elle consiste à mettre en place les contrôles nécessaires pour surveiller et protéger l'environnement, l'infrastructure matérielle et les équipements de sauvegardes de données contre le vol, la dégradation et les désastres naturels.

- **La sécurité organisationnelle :** elle consiste à définir des procédures et des pratiques pour gérer le personnel et diriger les activités d'une organisation

- **La sécurité logique :** elle consiste à employer des moyens techniques tels que les composants matériels et les applications logicielles pour protéger l'information et les systèmes d'information. Le terme information englobe les données stockées dans un système, en transit sur un réseau ou les données de sauvegardes stockées dans des périphériques auxiliaires.

La sécurité informatique

Principes de base de la sécurité informatique

1. **La confidentialité :** la confidentialité d'un objet s'exprime par la non révélation de son contenu aux sujets non autorisés.
2. **L'intégrité :** l'intégrité d'un objet est la propriété d'être non modifié de manière non autorisée.
3. **La disponibilité :** la disponibilité d'un objet est la propriété d'être toujours disponible, à la demande des sujets autorisés, aux quels un accès fiable et opportun est assuré.
4. **L'utilisation légitime :** Cette propriété implique que les objets ne sont utilisés que par les sujets autorisés de manière autorisée.

La sécurité informatique

Le processus de sécurité informatique

Processus continu et évolutif pivotant autour des trois phases consécutives qui sont : la gestion du risque, le développement d'une politique de sécurité et sa mise en vigueur.

1. La gestion du risque

C'est une procédure visant à identifier, étudier et évaluer le risque pouvant résulter de l'utilisation de la technologie de l'information. L'objectif est de décider quelles seront les contre-mesures nécessaires à adopter pour réduire et maintenir le risque à un niveau acceptable. La gestion du risque représente une étape primordiale dont les résultats permettent de bâtir la politique de sécurité de l'organisation.

La sécurité informatique

- **Le processus de sécurité informatique**

2. Établissement d'une politique de sécurité

Cette phase consiste à développer de manière claire et précise les procédures et les pratiques qui permettent de gérer la protection des actifs au sein d'une organisation, en se basant sur les résultats de la gestion du risque. Cette politique de sécurité prend la forme d'un document définissant ce qui est permis et ce qui est interdit. Il s'agit d'un énoncé qui s'adresse aux administrateurs système et aux utilisateurs.

- La politique de sécurité doit être révisée et maintenue périodiquement car le risque n'est pas statique, il change et évolue. Pour cette raison, il faut anticiper le risque et ajuster la politique de sécurité en conséquence.

La sécurité informatique

- **Le processus de sécurité informatique**

3. La mise en œuvre de la politique de sécurité

Durant cette phase, les règles de la politique de sécurité sont translatées en terme de configuration et d'implémentation en utilisant les mécanismes de sécurité adéquats (Firewalls, Système de détection d'intrusion (IDS),….).

Les services de la sécurité informatique

 Service : ensemble des contrôles et des procedures appliqués dans le but d'assurer la sécurité des actifs contre les menaces potentielles.

- La sécurité informatique offre cinq services principaux :

1. **Authentification**
2. **Confidentialité**
3. **Intégrité**
4. **Contrôle d'accès**

---

5. **Non répudiation**

Les services de la sécurité informatique

1. Authentification

- Processus d'identification et de vérification de l'identité d'une entité.
- Il permet d'assurer que seules les entités autorisées ont accès au système.
- Les entités à authentifier peuvent être un utilisateur, un processus en exécution ou une machine dans un réseau.

2. Confidentialité

- Interdire à un sujet de consulter directement une information qu'il n'est pas autorisé à connaître.
- Interdire à un sujet autorisé de lire une information et de la révéler à un utilisateur non autorisé à y accéder.
- Assurer que l'information reste secrète et elle n'est révélée qu'aux sujets autorisés.

Les services de la sécurité informatique

3. Intégrité

- L’information contenue dans les objets n’est ni créée, ni altérée, ni détruite de manière non autorisée.
- L’intégrité représente la capacité d’un système d’empêcher la corruption accidentelle ou intentionnelle d'information, et de garantir la mise à jour correcte de l’information.

4. Contrôle d’accès

- Moyen d’exprimer la possibilité technique de se servir d’une ressource informatique.
- Il permet de définir et spécifier les types des limitations et des permissions d'accès des sujets aux objets.
- Il permet de protéger les objets d’un système contre les modifications et les manipulations non autorisées.

Les services de la sécurité informatique

- **5. Non répudiation**

•Répudiation : possibilité de nier avoir participer aux échanges de la part d'une partie communicante.

- Non-répudiation : assurer qu'un message donné a été réellement envoyé par son expéditeur et reçu par l'entité destinatrice. Elle empêche l'expéditeur et le destinataire de nier respectivement l'envoie et la réception du message.

Les principaux mécanismes de sécurité informatique

Mécanisme de sécurité : moyen employé pour mettre en vigueur une politique de sécurité.

- Plusieurs mécanismes de sécurité pour mettre en œuvre la politique de sécurité d'une organisation.
- Chaque mécanisme peut fournir un ou plusieurs services de sécurité.

Les principaux mécanismes de sécurité sont : l'authentification, le chiffrement, les signatures numériques, les firewalls et les systèmes de détection d'intrusion.

Les principaux mécanismes de sécurité informatique

1. Les mécanismes d'authentification

La technique d'authentification la plus utilisée est celle basée sur le mot de passe statique. Elle est intégrée dans plusieurs systèmes d'exploitation, les administrateurs et les utilisateurs sont très familiarisés avec.

- limites dans un environnement réseau à cause de la disponibilité d'outils dédiés à craquer les mots de passe.
- Pour remédier à ce problème, d'autres méthodes d'authentification plus robustes sont appliquées telles que l'authentification One Time Password (OTP) et la biométrie.

Les principaux mécanismes de sécurité informatique

1. Les mécanismes d'authentification

La technique d'authentification OTP: elle génère un nouveau mot de passe à chaque établissement de connexion entre l'utilisateur et le système. Ce mot de passe n'est utilisé qu'une seule fois et il n'est plus valable par la suite.

La biométrie: elle fait intervenir les attributs physiologiques de l'utilisateur telles que les empreintes digitales et les formes de la rétine ou bien les attributs comportementaux tels que les caractéristiques de la voix.

Les principaux mécanismes de sécurité informatique

2. La cryptographie

- Ensemble de techniques permettant de transformer l'information de sa forme originale intelligible dite « texte clair » en une forme codée inintelligible dite « texte chiffré», ce processus est appelé chiffrement.
- Le processus inverse, permettant de restituer la forme originale de l'information à partir de sa forme codée, est possible, il est appelé déchiffrement.
- Le chiffrement et le déchiffrement font intervenir une fonction mathématique dite algorithme et une chaîne de bits dite clé.

Les principaux mécanismes de sécurité informatique

2. La cryptographie

Il existe deux types de chiffrement :

1. Le chiffrement symétrique

- Une clé unique pour le chiffrement et le déchiffrement.
- Deux ou plusieurs parties communicantes partagent la même clé(secret partagé).
- Un des algorithmes de chiffrement symétrique le plus connu est le DES (Data Encryption Standard).

Les principaux mécanismes de sécurité informatique

2. La cryptographie

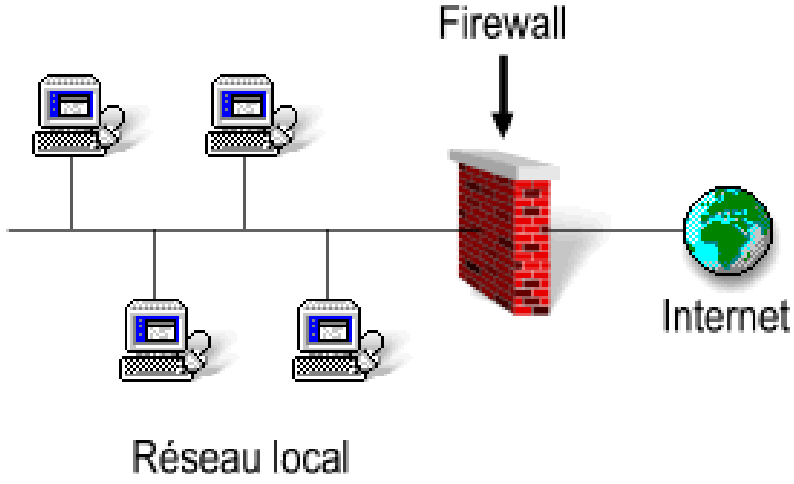
2.2. Le chiffrement asymétrique

- Une paire de clés : une clé privée et une clé publique.
- Clé publique : connue et distribuée à plusieurs parties pour chiffrer les messages.
- Clé privée : confidentielle et connue uniquement par son propriétaire. Seul le destinataire, propriétaire de la clé privée, est en mesure d'effectuer le déchiffrement.
- Un des algorithmes de chiffrement asymétrique le plus connu est le RSA (Rivest, Shamir, et Adelman) qui doit son nom à ses développeurs.
- Le chiffrement permet de garantir la confidentialité et l'intégrité des données en stockage ou en transit.

Les principaux mécanismes de sécurité informatique

3. Les Firewalls

Firewall : système permettant d'implémenter une politique de contrôle de trafic échangé entre un réseau éprouvé tel que le réseau privé d'une organisation et un réseau non éprouvé tel qu'Internet. Si le trafic correspond à la politique de sécurité, il est acheminé à sa destination sinon il est bloqué.



Les principaux mécanismes de sécurité informatique

3. Les Firewalls

- Le Firewall représente le seul point d'entrée et de sortie d'un réseau. Grâce à cette position idéale, d'autres fonctionnalités de sécurité peuvent être implémentées au niveau du Firewall telles que :
- L'authentification des utilisateurs voulant accéder aux services internes du réseau privé.
- La confidentialité en établissant un réseau virtuel privé (VPN) pour effectuer le chiffrement et le déchiffrement des données sensibles échangées entre deux réseaux privés
- Le contrôle d'intégrité via un support anti-virus permettant de scanner les données contenues dans les paquets dans le but de bloquer le trafic infecté.

Les principaux mécanismes de sécurité informatique

- **4. La détection d'intrusion**

•Elle étend les capacités de gestion de la sécurité pour inclure la surveillance des environnements systèmes et réseaux, l'identification des intrusions et l'établissement d'un plan de réponse à ces intrusions.

Conclusion

Les mécanismes de sécurité agissent seulement comme des obstacles électroniques dressant une barrière face aux attaques. Ils sont faillibles et ils peuvent inclure des vulnérabilités inévitables. Les attaquants arrivent à exploiter leurs vulnérabilités et contourner leurs fonctionnalités de sécurité .
Ce qui rend l'implémentation parfaite d'une politique de sécurité est impossible.

La sécurité n'est pas parfaite, il existe toujours des chemins pour la contourner et s'introduire dans les environnements sécurisés