✓**Sécurité informatique:** l'ensemble des techniques qui s'assurent que les ressources du système d'information (matérielles/logicielles/données) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient
✓**Cyber résilience=** la capacité s'adapter rapidement à des conditions changeantes : résistance et récupération suite à des perturbations subies.
3 propriétés de sécurité
➢**Confidentialité** = accès au système et aux données est limité aux parties autorisées.
➢**Intégrité** : avoir la « bonne » donnée/information
➢**Disponibilité:** Le système/données fonctionnels au moment voulu.

✓**Actif** (Asset) : ressource à protéger Matériel/logiciel/donnée
✓**Vulnérabilité** : faiblesse= faille= niveau d'exposition face à la menace dans un contexte particulier.
Attaque : action exploitant une vulnérabilité et exécutant une menace.
✓ **Menace** (Threat) : Action susceptible de nuire dans l'absolu./source du risque (Ce que peut faire le pirate)/cible un ou plusieurs actifs
✓ Grandes catégories:
➢ Usurpation vise la propriété de confidentialité
➢ Usurpation d'identité (Impersonation)
➢ Usurpation d'adresses = Mascarade (Spoofing)
➢ Falsification (modification) vise propriété de l'intégrité
➢ Interception (divulgation) vise la propriété de confidentialité
➢ Interruption (Déni de service (DoS = Deny of Service)) vise la propriété de disponibilité
➢ Fabrication (Forgery) & rejeu (Replay) vise propriété de l'intégrité
➢ Répudiation vise la propriété d'intégrité
Contre-mesures : l'ensemble des actions mises en œuvre en prévention de la menace.

Attaque	Cible
1. Falsification (modification)	1. Données, flux, transactions
2. Fabrication (forgery)	2. Données, messages
3. Interception (Eavesdropping)	3. Données, messages, trafic,
4. Interruption	4. Système, serveur, réseau, nœud, etc,
5. Répudiation	5. Données, envoi, réception, transactions
6. Usurpation	6. identités

Services de sécurité = Fonctionnalités offertes par les outils de sécurité pour prévenir une menace
✓Contrôle d'accès : L'accès aux ressources du système n'est pas permis aux entités non autorisées.
• **Confidentialité**: les données ne peuvent pas être connues des entités non-autorisées.
• **Intégrité des données** : les données n'ont pas été altérées par des entités non-autorisées.
• **Authentification de l'origine**: l'identité de la source des données échangées est vérifiée.
• **Non Répudiation:** les acteurs impliqués dans la communication ou transaction ne peuvent nier y avoir participer
• **Disponibilité:** les acteurs accèdent au système dans les conditions prévues.

Penetration test = intrusion dans un système ou réseau pour trouver des failles
avant les pirates avec la permission du propriétaire du système pour améliorer les systèmes par la correction des vulnérabilités identifiées
types de penetration : Black box/ White box/Grey box

Démarche type d'une intrusion

1. Reconnaissance = Collecte d'informations
2. Scanning = Balayage & Repérage de failles
3. Gaining access • Intrusion• Extension de privilèges• Compromission
4. Maintaining access (ex. Porte dérobée) => Installer un programme malveillant
5. Clearing tracks = Nettoyage de traces

L'ingénierie sociale: en contactant directement certains u(lisateurs du réseau (par mail ou par téléphone) afin de leur sou(rer des informa(ons concernant leur identifiant de connexion et leur mot de passe.

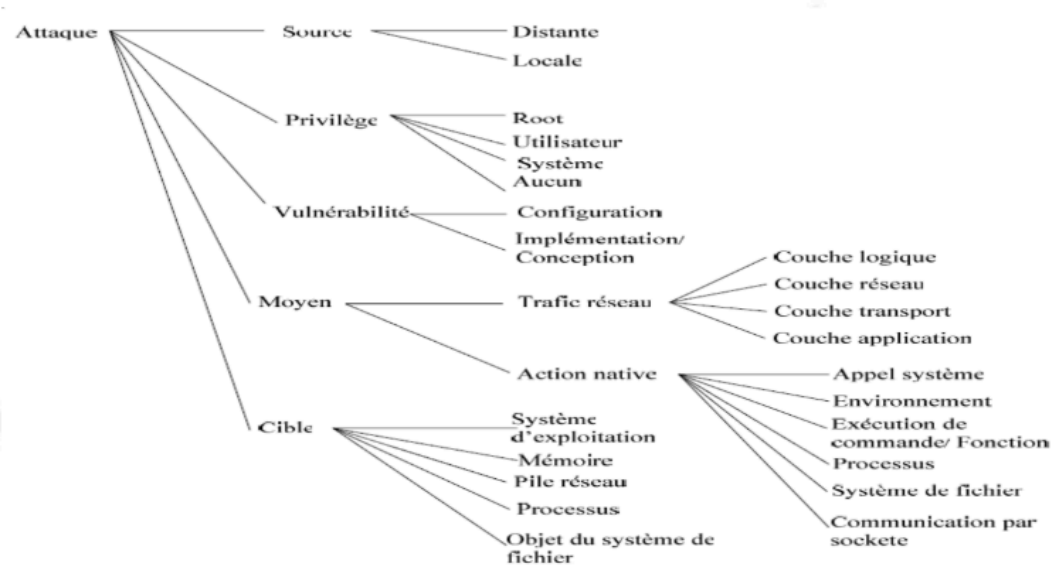
Virus: programme malveillant dont l'objectif principal est de perturber le bon fonctionnement d'un appareil, la plupart du temps un ordinateur . (Sous-catégorie de malware)

Malware: (malicious software) = logiciel malveillant = tout type de logiciel conçu pour causer des dommages, voler des informations ou perturber le fonctionnement d'un système informatique.

- Types de malware
  - **Les vers**: Se limite généralement à l'auto-réplication.
  - **Les adwares:** spams conçus pour bombarder la cible de publicités
  - **Les scarewares** (alarmiciels) : génèrent des alertes (fausses)
  - **Les spywares** (logiciels espions): espionne les actions et enregistre les frappes pour voler vos idenHfiants de connexion
  - **Les ransomwares**: . Verrouille votre ordinateur, des dossiers ou des fichiers (données) pour vous empêcher d'y accéder. Il les garde en otage et demande une rançon pour les récupérer.
  - Les rootkits: difficile à détecter et à supprimer. Ces kits se cachent dans l' ordinateur cible et y réalisent diverses activités illégales.

Attaques indirectes Le pirate utilise un système intermédiaire antre son équipement et la victime 2 types: par rebond, par réponse

L'arbre de classification (suite et fin)



Techniques d'attaques

Ecoute réseau (3 catégories)

- 1. L'écoute ou Snooping (attaque passive) : Capture de trafic ->Prendre connaissance d'informations transitant sans pour autant les altérer et sans se faire connaître.
  ⇒ Le **snooping** consiste à **espionner les données ou activités directement sur un appareil ou un système** pour accéder à des données sensibles
- Le **sniffing** consiste à **surveiller et capturer le trafic réseau** en temps réel pour analyser les paquets de données échangés entre les appareils.
- 2-Sniffing + Déchiffrement par le pirate du contenu des flux d'information transitant afin d'en tirer des informations confidentielles.(capture passive ou active)
  L'**eavesdropping** est une attaque où un pirate intercepte **discrètement les communications entre deux parties** pour écouter, surveiller ou voler des informations échangées, sans perturber le flux normal des données.

- 3. L'interception par Man in the middle
  Le MIM intercepte le trafic puis le retransmet vers sa destination ou non.

Usurpation

Les **attaques sur les identifiants** visent à compromettre ou usurper les moyens d'identification des **personnes** ou des **objets** pour accéder illégalement à des systèmes ou des informations sensibles.

- **Identités des personnes :** Login, e-mail, mot de passe → **Usurpation d'identité (Impersonation)**.
- **Identités des objets :** Adresses MAC, IP, URL → **Spoofing (Mascarade)**.

Attaques Dos

- Une **attaque DoS (Déni de Service)** vise à **perturber ou bloquer le fonctionnement normal d'un service, d'un serveur ou d'un réseau**, empêchant ainsi les **utilisateurs légitimes d'accéder aux ressources disponibles**.par saturation ou en exploitant les vulnérabilités
- Smurf : dos : attaque par réflexion : Une **attaque Smurf** est une attaque **DoS qui exploite** les adresses **broadcast** pour **inonder une cible avec un trafic massif de réponses ping**, rendant ainsi le système cible **inaccessible**.
- **Ping of death :** il s'agit de Création d'un datagramme IP dont la taille totale excède la taille maximum autorisée Un tel paquet envoyé à un système possédant une pile TCP/IP vulnérable, et cela provoquera un plantage
- Dos: Attaque par fragmentation : une attaque réseau par saturation exploitant le principe de fragmentation du protocole IP.=> Création d'un ensemble de fragments qui, une fois réassemblés, dépassent la taille maximal autorisée.(TearDrop)
- **Attaque LAND** Envoie un paquet avec la même **adresse IP source et destination** ainsi que le même **port source et destination**, provoquant un **blocage ou un plantage du système cible**.

- **Attaque SYN Flooding** Inonde le serveur avec une multitude de **requêtes TCP SYN** sans jamais finaliser le **three-way handshake**, épuisant ainsi les ressources du serveur.
- **Attaque par Buffer Overflow :** Envoie **plus de données qu'un tampon mémoire ne peut en contenir**, provoquant un **plantage du système** et permettant potentiellement **l'exécution de code malveillant**
- **Attaque**
- **S (Distributed Denial of Service) :** Une attaque **DoS lancée depuis plusieurs machines zombies**, souvent contrôlées par un **botnet**, pour saturer massivement les ressources de la cible.

Les Attaques web :Principales attaques

Interprétations des URLs/ Mauvais Contrôle Des Données/ Injection De Code SQL/ Cross Site Scripting/ Violation de gestion d'authentification et de session

Crypto

Robustesse = capacité du système à résister aux attaques cryptographiques

Algo symétriques de cryptographie:
DES: «Data Encryption Standard »est un algorithme de chiffrement **symétrique par bloc** utilisant une **clé secrète** de **56 bits** pour chiffrer et déchiffrer des données.(blocs de 64 bits)
3DES : TRIPLE DES Algorithme de chiffrement par bloc enchaînant 3 applications successives de l'algorithme DES sur le même bloc de données de 64 bits, avec 2 ou 3 clés DES différentes.
AES «Advanced Encryption Standard »est un algorithme de chiffrement **symétrique par bloc** qui utilise des **clés de 128, 192 ou 256 bits** pour chiffrer et déchiffrer des données en blocs de **128 bits**.

Avantages :

- **Faible overhead** : Excellentes performances pour le chiffrement de grands volumes de données comme les **fichiers** et le **streaming vidéo**.
- **Clé secrète facile à changer** :
- **Sécurité augmentée avec le nombre de clés** :
- **One-Time Pad (OTP)** : Considéré comme la méthode la plus sûre de chiffrement, car il garantit une sécurité théorique absolue.

Inconvénients :

- **Échange sécurisé de la clé secrète** : La clé doit être échangée sur un canal sécurisé, ce qui crée une limitation. Cela peut être fait via des méthodes physiques comme les **cartes SIM** ou des échanges en **mains propres**.
- **Problème d'échelle** coûteux pour un grand nombre d'utilisateurs.

Méthodes d'échange de clés :

- **Support physique** (cartes SIM, cartes à puce) ou **échange manuel**.
- **Clé maîtresse** : Une clé centrale utilisée pour générer des **clés de session**.
- on le système cryptographique et l'application.

Domaines d'utilisation :

- **Systèmes administrés** : Réseaux cellulaires, **réseaux de capteurs**, **TV cryptée**.
- **Transactions électroniques** : **E-health**, **e-commerce B2B**.
- **Systèmes intra et inter-organisationnels** : **VPNs**

Les algorithmes à clé publique(Asymétriques)

⇒ Besoin Envoyer la clé sur le canal non sûr Tout en préservant la confidentialité

RSA (Rivest-Shamir-Adleman)

- **Utilisation** : Chiffrement et **signature numérique**.
- **Principes** : L'algorithme RSA repose sur **l'asymétrie des clés** où la **clé publique** est utilisée pour le chiffrement et la **clé privée** pour le déchiffrement.
- **Sécurité** : Basé sur la difficulté de factorisation des grands nombres premiers.

2. DSA (Digital Signature Algorithm)

- **Utilisation** : Principalement pour la **signature numérique**.
- **Clé publique** : 1024 bits (plus longue que RSA pour une sécurité accrue).
- **Principes** : L'algorithme DSA génère des signatures numériques basées sur le **problème du logarithme discret** dans un groupe de nombres premiers.

3. Diffie-Hellman

- **Utilisation** : **Échange sécurisé de clés**.
- **Principes** : Permet à deux parties de partager une clé secrète par un canal non sécurisé en utilisant des calculs basés sur le **problème du logarithme discret**.

Avantages : Une seule clé publique publiées vers tous les récepteurs en clair sur le canal non sûr

Inconvénients: lenteur pour les longs messages

⇒ ⇒ ⇒ La combinaison des deux type d 'algorithmes ::

- Chiffrement des données : algo. Symétriques
- Transmission de la clé secrète: algo. Asymétrique

Contrôle d'intégrité

Le **rejeu** (ou **replay attack**) est une attaque de sécurité où un acteur malveillant intercepte des données d'une communication valide et les rejoue plus tard pour tromper le système cible.

contrôle d'intégrité : Garantir que le contenu d'une communication ou d'un fichier n'a pas été modifié. par le mécanisme du fonction de **hachage** :convertir une chaîne de longueur quelconque en une chaîne de taille inférieure et généralement fixe. appelée Empreinte (Digest)

Propriétés de ft de hachage :

l A sens unique= Preimage-resistance:

– Etant donné y, il est difficile de trouver x tel que h(x) = y

l Second preimage-resistance:

– Etant donné x, il est difficile de trouver x' ≠ x tel que h(x) = h(x')

è (i.e., un second preimage de h(x))

l Sans collision = Collision-resistance:

– Il est difficile de trouver deux valeurs distinctes x et x' tel que h(x) = h(x')

- Les fonctions de hachage seules Sont :Sensibles à l'attaque MIM

Signature numérique = Cryptographie asymétrique → Authentification, intégrité, non-répudiation.

MAC Message Authentication Code = Cryptographie symétrique → Authentification, intégrité (pas de non-répudiation).

Signature : mode opératoire

Génération de signature

1_ Appliquer une fonction de hachage sur M

2- Chiffrer le résumé avec K-a

Vérification de signature

1_ Appliquer une fonction de hachage sur M

2- Déchiffrer la signature S avec avec K+a

3- Comparer le résultat de (1) avec celui de(2)

4- Si égalité ⇒ intégrité vérifiée Sinon: Erreur d'intégrité de C

Algorithme de Signature numérique :

- DSA (Digital SignatureAlgorithm)
- DSS (Digital SignatureStandard)
- RSA Digital Signature

Le **scellement** est un mécanisme de sécurité qui garantit l'**intégrité** et l'**authenticité** d'un message en ajoutant un **code d'authentification (MAC)**, généré à l'aide d'une **fonction de hachage** et d'un **algorithme de chiffrement symétrique** avec une **clé secrète** partagée entre l'émetteur et le destinataire.

Un **certificat numérique** est un document électronique signé par une autorité de certification qui associe une **clé publique** à l'**identité** d'une entité, garantissant son authenticité, sa non-falsifiabilité et sa validité.

Horodatage : Besoin d'un cachet de temps légal" ou jeton d'horodatage pour les

transactions effectuées et les documents échangés.
Contrôle d'accès :Permet d'associer des droits d'accès et/ou des ressources à une entité

Process de controle d'acces
Phase préliminaire: Enregistrement => Identification
1. Authentification (authentication)
2. Autorisation (authorization)
L'authentification permet à des hôtes communiquant de vérifier l'identité des uns et des autres pour qu'ils soient sûrs de communiquer avec les hôtes avec lesquels ils croient communiquer.
SSO Single Sign-On : Un utilisateur authentifié peut utiliser plusieurs services dans le même domaine de confiance