**Université Abderrahmane Mira de Bejaia**
**Faculté des Sciences Exactes**
**Département d'informatique**

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

**Module : Sécurité des SI**
**Niveau : Master 2 option SIA**
**2022-2023**

# Fiche TD N° 1
# Introduction à la sécurité des SI

## Question de cours

1. Quelle est la différence entre la sécurité informatique et la sécurité d'un système d'information?
2. Quelle est la différence entre la sûreté et la sécurité d'un système ?
3. Pourquoi dit-on souvent que les problèmes de sécurité sont des problèmes de gestion d'architectures et de management de personnes ?
4. Quels sont les services offerts par un contrôle d'accès ?
5. Quels sont les différents types d'intégrité ?
6. Quelles est la différence entre une identification et une authentification ?
7. Citez et décrivez brièvement quelques attaques qui touche à la disponibilité.
8. Donnez quelques scénarios pour lancer une attaque physique.
9. Quelle est la différence entre un virus et un ver ?
10. Dans quelle mesure les vers sont-ils plus dangereux que les virus ?
11. Qu'est-ce qu'un cheval de Troie ? Comment un attaquant peut-il procéder pour en installer un ?
12. Citez et décrivez quelques catégories de virus.
13. Est-ce qu'un système pare-feu protège contre des attaques par déni de service ?

## Exercice 1.

Complétez la grille ci-après de sorte à montrer la relation entre les services de sécurité et les Attaques.

| | **Libération du contenu du message** | **Analyse du trafic** | **Mascarade** | **Rejouer** | **Modification des messages sur un serveur web** | **Envoi massif de messages** | **Déguisement** | **Espionnage d'une voie de communication** |
|---|---|---|---|---|---|---|---|---|
| **Authentification** | | | | | | | | |
| **Contrôle d'accès** | | | | | | | | |
| **Confidentialité** | | | | | | | | |
| **Confidentialité des flux de trafic** | | | | | | | | |
| **Intégrité des données** | | | | | | | | |
| **Non-répudiation** | | | | | | | | |
| **Disponibilité** | | | | | | | | |

## Exercice 2.

Considérons un système d'information d'une organisation utilisant un réseau où par défaut, le partage est activé pour toutes les machines du réseau afin de pouvoir récupérer les scans ou télécopies reçues. Les imprimantes sont utilisées pour imprimer des documents.

- Etablir une liste des actifs
- Identifier les menaces et les composants vulnérables

## Exercice 3.

Classer les événements suivants en vulnérabilités et menaces, puis les menaces en accidentelles (non-intentionnelles) et intentionnelles

| | | |
|---|---|---|
| Faibles mots de passe | Sabotage | Interception d'émissions |
| Absence de redondances (serveurs,…) | Réseau ouvert (sans authentification ) | Effacement de la mémoire |
| Défauts de conception | Panne de disque | Panne du matériel |
| Corruption de données | Envoi d'un script malveillant intérieur | Absence de contrôle d'accès |
| Défaillance du logiciel | Données inexactes | Erreur d'opérateur |
| Accès non autorisé | Action malveillante intérieure | Prise de contrôle d'un site web |
| Absence de sauvegarde | Ecoute réseau | Logiciel malveillant |
| Communications défaillantes ou corrompues | Réseau Wifi mal configuré | Incendie, explosion, inondation |
| Coupure d'électricité | Espionnage | Inondation de messages |

## Exercice 4.

Quel est le service de sécurité atteint dans les cas de figures suivants :

| Scénario | Service de sécurité atteint |
|---|---|
| Un attaquant a réussi à consulter un fichier transitant sur le réseau. Il arrive à voir son contenu mais il n'arrive pas à le décrypter | |
| La base de données d'air Algérie a été attaquée et toutes les places disponibles sur le vol Londres ont été réservées au nom de "karim " | |
| Un pirate utilise une adresse IP volée pour convaincre un système qu'il est un client fiable et connu | |
| Un attaquant a réussi à consulter un fichier transitant sur le réseau. Il arrive à voir son contenu et arrive à le décrypter et le lire | |
| Un utilisateur supprime accidentellement un fichier et pour ne pas être sanctionné il cache cet acte | |
| Un pirate bombarde un serveur de BD par des requêtes sans arrêt | |
| Un pirate réussi à utiliser la carte bancaire d'un individu et se fait payer un IPhone sur le site d'Apple | |
| Les pirates injectent du contenu dans une page qui corrompt le navigateur de la cible. Il peut ainsi modifier la page web selon ses envies | |

## Exercice 5.

Dans le tableau ci-dessous, nous avons plusieurs scénarios d'incidents

- Identifier le service de sécurité atteint
- Proposer un mécanisme de défense

| Scénario | Service | Méthode de défense |
|---|---|---|
| Alice envoie un mail électronique au nom de Bob à Eve | | |
| Bob se connecte à un serveur sur lequel il n'a pas le droit d'accès | | |
| Alice envoie un grand nombre de ping à l'ordinateur d'un collègue | | |
| Alice se met entre le point d'accès sans fil et l'ordinateur de Bob. Toutes les trames envoyées par Bob sont reçues et retransmises par l'ordinateur d'Alice | | |
| Bob modifie le montant d'une facture électronique d'Eve de 4500da à 10000da | | |

## Exercice 6.

Quels sont les objectifs (services) assurés par cet ensemble de mécanisme de sécurité ?

| Mécanisme / Service | Disponibilité | Intégrité | Confidentialité | Preuve |
|---|---|---|---|---|
| Anti-virus | | | | |
| Cryptographie | | | | |
| Pare-feu | | | | |
| Contrôle d'accès logique | | | | |
| Sécurité physique des équipements et locaux | | | | |
| Capacité d'audit | | | | |
| Clauses contractuelles avec les partenaires | | | | |
| Formation et sensibilisation | | | | |

## Exercice 7. (Supplémentaire)

Considérant un système d'information où les étudiants accèdent par un numéro d'étudiant et un mot de passe et cela afin de déposer leurs travaux et consulter leurs notes.

- Donner des exemples d'exigences de sécurité en termes de : authentification, contrôle d'accès, confidentialité, intégrité, disponibilité et non répudiation liées à ce système.
- Pour chaque cas, indiquer le degré d'importance de chaque exigence (Fort, moyen, faible) et une méthode de défense.