3ème Année Licence (SI) **2019/2020**

Module : Sécurité Informatique

TD 2 : Les services de Sécurité et les mécanismes de défense

Exercice1 : Les services de Sécurité

1- Rappelez les 5 services de sécurité.

2- Quel service parmi les cinq suscités est attaqué ou atteint dans les cas de figures suivants (en expliquant) :

a- Un attaquant qui réussi à consulter un fichier transitant sur le réseau, il arrive à voir son contenu mais n'arrive pas à le décrypter.
b- 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 « L3 SI » !
c- Le message sécurisé est transmis sur un réseau sans fil et passe par une zone de hautes fréquences qui agit sur son contenu et le modifie intentionnellement.
d- Un utilisateur supprime accidentellement un fichier et de peur d'être sanctionné, il cache cet acte !
e- Un attaquant bombarde un serveur de BD de requêtes sans arrêt.
f- Un pirate réussi à utiliser la carte bancaire d'un individu et se fait payer un IPhone sur le site d'Apple.

Exercice2 : Les mécanismes de défense

Répondre par « Vrai » ou « Faux », en justifiant quand c'est « Faux » :

a- Quand un mécanisme assure l'Authentification, il assure automatiquement la non-répudiation
b- Le bourrage de trafic (Padding) est une forme de cryptographie.
c- L'accès à une chambre d'hôtel par carte magnétique est une forme d'authentification.
d- Le contrôle d'accès ne concerne que la partie software du système
e- La protection physique englobe l'accès à distance aux données.
f- Si on enregistre la date et l'heure de chaque opération (horodatage) en l'associant à qui a effectué cette opération (journal), nous assurons la non-répudiation.

Solutions :

Exercice1 :

1-

1- **Confidentialité**
2- **Authentification**
3- **Intégrité**
4- **Non-Répudiation**
5- **Disponibilité**

2-

a- **Le service de sécurité attaqué est la confidentialité, mais dans ce cas, cette confidentialité n'est pas cassée.**
b- **C'est l'intégrité qui a été touché (et sûrement pour réussir une tel attaque, l'authentification a été touché aussi)**
c- **Malgré que ce n'est pas une attaque, mais cette modification a touché le service de sécurité d'Intégrité.**
d- **C'est la non-répudiation qui a été touché surtout s'il n y a pas de suivi dans ce système (qui a fait quoi et quand ?), sinon cet utilisateur maladroit sera démaqué et il ne pourra pas le nier.**
e- **C'est la disponibilité du système qui sera touchée et très probablement ça va mener à un DoS partiel ou total**
f- **C'est l'authentification qui a été touché, car il y a eu usurpation d'identité.**

Exercice2 :

a- **<u>Faux</u> : ce n'est pas suffisant, si on ne fait pas un suivi (journal) de qui a fait quoi et quand ? avec une authentification, elle ne suffit pas à elle seule pour assurer la non répudiation.**
b- **<u>Vrai</u> (car il envoie l'info d'origine sous une forme incompréhensible même si c'est juste en ajoutant des bits ou octets supplémentaires)**
c- **<u>Vrai</u> (mais une authentification de très faible degré car plusieurs individus peuvent avoir accès à la même carte facilement et il peut y avoir des copies de la même carte)**
d- **<u>Faux</u> : il concerne toutes les ressources partagées (ex : imprimante, application, ….)**
e- **<u>Faux</u> : La protection physique concerne l'accès direct aux ressources, au contact direct pas par accès à distance.**
f- **<u>Vrai</u>**