Université de khenchela
Faculté des sciences et Technologies L3 ISIL

TD 1 : Introduction à la sécurité informatique

1 Exercice

A) Identifiez les objectifs fondamentaux (services) en sécurité informatique. Puis, expliquez la différence entre eux.

B) Donner deux classifications standard (vu au cours) pour les attaques. Expliquer chaque classe en donnant des exemples.

2 Exercice

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

A) Identifier le service de sécurité violé.

B) Proposer un mécanisme de défense.

N	Sénario	Service ciblé	Méthode de défense
1	Alice envoie un mail électronique au nom de Bob à Eve.	?	?
2	Bob se connecte à un serveur sur lequel il n'a pas le droit d'accès.	?	?
3	Alice envoie un grand nombre de ping à l'ordinateur d'un collègue.	?	?
4	Alice se met entre le point d'accès sans fil et l'ordinateur portable de Bob. Toutes les trames envoyées par Bob sont reçues et retransmises par l'ordinateur portable d'Alice.	?	?
5	Bob modifie le montant d'une facture électronique d'Eve de 2230 DA à 90000 DA.	?	?

3 Exercice

Considérant un système d'information où les étudiants accèdent par un numéro d'étudiant et un password et cela afin de déposer leurs travaux (TP, rapports, ...) et consulté leurs notes.

A) Donner des exemples d'exigences de sécurité en termes de ; authentification, contrôle d'accès, confidentialité, intégrité, disponibilité et non répudiation liées a ce systèmes.

B) Pour chaque cas, indiquer le degré d'importance de chaque exigence (élevé, modéré, moyen).

Service	Exemples d'exigences	Degré d'importance	Méthode de défense
Authentification	?	?	?
Contrôle d'accès	?	?	?
Disponibilité	?	?	?
Intégrité	?	?	?
Non-répudiation	?	?	?

4 Exercice

Le risque en sécurité informatique peut être exprimé par la formule suivante :

$$Risque = \frac{(Menace \times Vulnerabilite)}{(Contre\_mesures)}$$

- Donner une définition de chacun de ces concepts à savoir :
  1. Risque,
  2. Menace,
  3. Vulnérabilité, et
  4. Contre mesures.

5 QCM

Q1. Un virus informatique est défini en tant que :

A) Tout programme téléchargé sans l'autorisation de l'administrateur du système,

B) Tout programme ayant un effet nuisible sur le système informatique,

C) Tout programme qui change les registres Windows.

Q2. Que ce qu'un malware (spyware) ?

A) Tout programme qui prend le contrôle du système de façon illégal,

B) Tout programme qui enregistre les frappes du clavier,

C) Tout programme qui se comporte de façon intelligente.

Q3.Que ce qu'un examinateur de pénétration (pentester) ?

A) Une personne qui pirate un système sans être capté,

B) Une personne qui pirate un système par fabrication de password

C) Une personne qui pirate un système pour tester ses vulnérabilités.

Q4. Parmi les notions suivantes, laquelle permet de contrer l'attaque IP spoofing (Création de paquets avec une adresse IP falsifier) ?

A) Proxy

B) Pare-feu

C) Protection de mot de passe.

Q5. Choisir l'énoncé correct :

A) Le chiffrement permet d'assurer la disponibilité et l'accessibilité de

B) la donnée chiffrée.

C) La signature électronique permet la confidentialité de la donnée transitant le réseau.

D) L'attaque DoS portent atteinte à la disponibilité de la machine cible.

Q6. Le phishing peut être réalisé comme suit :

A) Alice envoie un mail à Bob avec un lien permettant de télécharger un virus.

B) Alice envoie un mail à Bob avec un lien usurpant Microsoft et demandant d'entrer le login/mot de passe du compte Microsoft de Bob.

C) Alice envoie un mail à Bob avec une pièce-jointe contenant des macros malveillantes.

Q7. L'attaque Sybille vise en premier lieu :

A) L'accès aux données chiffrées.

B) La disponibilité d'un serveur.

C) L'authentification

Q8. Qu'est ce qu'une zone de confiance dans un réseau ?

A) Le hotspot wifi offert aux visiteurs (ex :hotel)

B) Le réseau interne ou sont hébergés les postes des utilisateurs

C) Une zone démilitarisée (DMZ)