TD n° 1

Principes de sécurité informatique

Exercice 1

1) Donnez les cinq principaux services de sécurité avec une définition succincte de chaque services ?

   Réponse :

   a. Contrôle d'accès : limiter l'accès au système. Seules les personnes autorisées aient accès aux ressources.
   b. L'authentification : S'assurer (vérifier) de l'identité de l'utilisateur.
   c. L'intégrité : Détecter toute modification des données.
   d. La confidentialité : assurer que l'information n'est divulguée (dévoilée ou révélée) qu'aux personnes autorisées.
   e. La disponibilité : permettant de maintenir le bon fonctionnement du système d'information.
   f. La non répudiation : permettant de garantir qu'une transaction ne peut être niée.

2) **D**onnez pour chaque service (citez dans Q1) de sécurité l'attaque (les attaques) qui lui correspond ? (répondre sous forme de tableau)

   Réponse :

Les services	**Les attaques**
Contrôle d'accès	
L'authentification	Usurpation d'identité
L'intégrité	Modification de l'information
La confidentialité	Écoute et Interception des messages sur le réseau
La disponibilité	Déni de service (DoS) Bombardement
La non répudiation	Répudiation

3) Donnez pour chaque service un moyen permettant de lui réaliser ?

4) Réponse :

Les services	**Les moyens**
Contrôle d'accès	• Filtrage réseau (par adresse MAC ou adresse IP, par nom de domaine) • Donner un mot de passer pour un réseau wi-fi
L'authentification	• Login/mot de passe

	• Certificat
L'intégrité	Ajout de champ MAC
La confidentialité	Chiffrement des données
La disponibilité	
La non répudiation	Signature numérique

5) Quelle est la différence entre une attaque active et une attaque passive ? donnez un exemple pour chaque type d'attaque ?

Réponse :

a. Les attaques passives : consistent à écouter sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais une prévention est possible.
b. Les attaques actives : consistent à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau. Noter qu'une attaque active peut être exécutée sans la capacité d'écoute.

6) Citez Trois principaux domaines où la sécurité est une chose primordiale (indispensable) ?

Réponse :

a. Domaine commerciale (site de ventes et achat, réseau d'une banque, etc…)
b. Domaine militaire
c. Domaine médicale

7) Quelle est la différence entre un virus, un ver, et un espion ?

Réponse :

a. Un virus est un logiciel malveillant conçu pour se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme les réseaux informatiques et les cédéroms, les clefs USB.
b. Un ver, contrairement à un virus informatique, n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.
c. Un espion est un logiciel malveillant qui infecte un ordinateur dans le but de collecter et de transmettre à des tiers des informations de l'environnement sur lequel il est installé sans que l'utilisateur n'en ait conscience.

8) Citez les différentes attaques informatiques que vous connaissez ?

Réponse :

a. Accès physique
b. Interception de communications
c. Dénis de service
d. Intrusions
e. Ingénierie sociale
f. Trappes

Exercice 2

Choisissez les réponses justes aux questions posées.

1) Un virus :
   a. Est un logiciel malveillant qui est doté de l'autonomie et se duplique à travers un réseau
   b. Est un programme qui s'installe dans un autre programme et qui se duplique grâce à celui-ci
   c. Est un logiciel dont l'objectif premier est d'espionner

2) Le spamming :
   a. Est une variante du ping flooding
   b. Permet de saturer la boite à lettre d'une victime par un nombre important de courrier électronique
   c. Est une variante du mail-bombing

3) Le déni de service est une attaque contre :
   a. La confidentialité
   b. L'intégrité
   c. La disponibilité

4) Une fonction de hachage :
   a. Produit une empreinte de longueur fixe
   b. Produit une empreinte de longueur quelconque
   c. Est irréversible

5) Le chiffrement asymétrique assure :
   a. La non-répudiation
   b. L'intégrité
   c. La confidentialité, l'authentification et l'intégrité
   d. La confidentialité

6) Le phishing est :
   a. Un programme installé sur le poste d'un utilisateur pour enregistrer à son insu ses frappes clavier
   b. Une technique essayant d'extraire des informations confidentielles sur un client
   c. Une technique qui tente d'entraîner un client d'une banque vers un site web qui ressemble très fort à celui de sa banque

---

Le **mail-bombing** est une technique d'attaque visant à saturer une boîte aux lettres électronique par l'envoi en masse de messages quelconques par un programme

automatisé. On utilise les termes de mail-bomber pour caractériser l'action de faire du mailbombing (de saturer de messages/courriels) et de mail-bomb pour le courrier reçu sous cette forme et dans ce but.