Solution td 3

Exercice 1 :

1) **Identification :** étant le processus de déclaration de l'identité de d'une entité. Elle consiste à associer à une entité une identité.
   Pour l'utilisateur : le login ou le nom utilisateur étant l'identité à déclarer.
   Pour un Système : le nom du système ou son adresse IP étant l'identité à déclarer.

2) **L'authentification :** est le processus de vérification de l'identité déclarer d'un utilisateur ou un système. Elle consiste à introduire une preuve pour confirmer l'entité déclarer.
   Pour le login : la preuve étant le mot de passe
   Pour le système : la preuve étant le certificat.
3) L'identification est une déclaration d'identité qui emploie une information publique (Login, adresse IP). L'authentification est la vérification de l'identification. Elle complété l'étape d'identification en s'appuyant sur la preuve de l'identité déclarée. Cette preuve est une information secrétée.

Exercice 2 :

1) Les meilleurs pratiques pour définir un bon mot de passe

- Définir un mot de passe difficile à deviner

  Il faut définir un mot de passe suffisamment long (8 caractères au minimum).

  Il faut définir un mot de passe complexe qui combine les lettres majuscules, minuscules, chiffres et caractères spéciaux.

- Eviter d'utiliser des informations personnelles ou des noms qui appartiennent à un dictionnaire ou encore des suites logiques (abcdef,123456, azerty) qui peuvent aider les attaques à deviner les mots de passe.

2) Les meilleures pratiques pour protéger un mot de passe :

- Il faut garder le mot de passe secret et ne pas le communiquer à une partie tierce.
- Il ne faut pas notre le mot de passe ou l'inscrire sur un équipement.
- Il ne faut pas enregistrer le mot de passe dans un fichier non protégé.
- Il ne faut pas enregistrer le mot de passe dans les navigateurs.
- Il faut changer fréquemment le mot de passe.
- Il faut utiliser un mot de passe diffèrent pour chaque service et utiliser un gestionnaire de mot de passe.

Exercice 3 :

1) Rendre le fichier invisible pour les utilisateurs (fichier caché) et activer l'option ne pas afficher les fichiers cachés.
2) Interdire la manipulation du fichier en mettant le fichier en lecture seule
3) Attribuer un mot de passe au fichier lors de sa création. Le créateur ou l'auteur de fichier peut limiter les actions sur le fichier en lui attribuant un mot de passe pour l'ouverture du fichier, la modification ou l'impression.
4) Chiffrement du fichier pour éviter la lecture du fichier.

Exercice 5 :

1- Un antivirus est un logiciel qui permet d'analyser un système et repérer les codes malicieux qui existent en alertant l'utilisateur de système, Il peut désinfecter les fichiers infectés comme il peut se référer à la décision à l'utilisateur en ce qui concerne la réparation, la suppression et mise en quarantaine des fichiers.

2- Les composants d'un antivirus sont :
   a) **Le scanner** : il permet de scanner un système /disque à la demande de l'utilisateur.
      Il cherche la présence de signatures de virus dans chaque fichier existant sur le système/disque.
   b) **Le moniteur :** il analyse en temps réel tous les programmes/applications en cours d'exécution et les fichiers en cours de manipulation par l'utilisateur. En présence de signature, il alerte l'utilisateur et empêche le virus de poursuive son exécution.
   c) **La base de signatures** : c'est une base de données qui héberge les signatures des virus connus.
   d) **Le module de mise à jour** : il permet la mise à jour automatique de la base de signatures en se connectant au site de l'éditeur de l'antivirus.

3- Les classes d'antivirus :

- Les antivirus gratuits.
- Les antivirus payants.
  Les antivirus payants offrent une efficacité meilleure.

4- La propriété qui rend un antivirus capable de prendre en charge les nouveaux virus à travers le temps est **la mise à jour automatique fréquente.**

5- Dans un large réseau, il faut déployer un antivirus réseaux avec une console d'administration centrale
Les machines du réseau concernées par le déploiement de l'antivirus sont :
- Tous les postes de travail fixes et nomades (ordinateurs portables).
- Les serveurs de fichiers.
- Les serveurs de messagerie.