TD : sécurité informatique

Exercice 1 : expliquer pour chaque type d'informations l'étape correspondante dans le cycle de l'intrusion :

1- profiter de l'existence d'une mauvaise configuration de partage d'une ressource.
2- la table du routage d'un routeur.
3- les machines actives.
4- une imprimante partagée entre différents utilisateurs.
5- les systèmes d'exploitation installés sur les machines
6- l'existence du service SNMP (Simple Network Management Protocol)
7- la présence d'un pare-feu dans le système informatique.
8- l'exploitation d'un compte protégé par un mot de passe non robuste
9- Modifier les permissions d'un fichier mal configuré
10- installer des programmes de contrôle à distance

Exercice 2 : compléter le tableau suivant

Service de sécurité	**Protège contre quel type d'attaques**
Authentification	
confidentialité	
Intégrité	
Non répudiation	
Disponibilité	

Exercice 3 :

1) pourquoi l'attaquant cherche t'il à trouver des cibles opportunes ?

2) un facteur primordial qui a contribué à l'évolution des menaces et des attaques contre les systèmes informatique est « le changement de profil des attaquants » expliquer ce facteur en donnant un exemple.

3) quels sont les différentes étapes nécessaires pour mettre en place une politique de sécurité ? (vous pouvez donner un schéma explicatif)

4) quels sont les services de sécurité assurés par la technique du contrôle d'accès ?

5) le service de sécurité confidentialité dispose de trois niveaux de protection pour les données échangées lors d'une communication. Expliquer chaque niveau de confidentialité et préciser son champ d'application.

Exercice 4 :

Vous êtes le responsable de sécurité au sein d'une entreprise. Suite à une attaque contre votre système informatique, vous avez détecté les dégâts suivants :

A. La divulgation du fichier contenant les détails de fabrication d'un nouveau produit. Ce fichier est seulement autorisé pour le directeur de l'entreprise.
B. La destruction du fichier contenant les brevets de l'entreprise.
C. L'absence du service FTP au niveau du système informatique.

1- Pour chaque action, préciser le type de l'attaque et le service de sécurité attaqué.
2- Pour déterminer l'origine de l'attaque, l'administrateur a identifié l'adresse IP source utilisé pour lancer ces actions intrusives. Cette adresse IP source est une adresse IP interne, c'est-à-dire l'entité qui a lancé ces actions appartient déjà au système informatique. Est que le service d'authentification est attaqué. Discuter les différents cas possibles.