Université d'Alger 1
Faculté des Sciences
Département Mathématique et Informatique

1ére année Master ISII 2018-2019
Module : Méthodologie de le Sécurité Informatique durée : 1h30

Examen Semestriel

Questions de cours : (08 points)

1. Classer les actions suivantes en attaque, faille, vulnérabilité et menace
    a. Bugs logiciel
    b. Divulgation des mots de passe
    c. Mot de passe stocké en clair dans la BDD
    d. Erreurs humaines
2. En utilisant le tableau dans l'annexe 1. Remplir le tableau pour chacun des cas suivants :
    a. Un hacker a volé les nom d'utilisateur et mots de passe de la banque à coté de sa maison
    b. Un employeur a vendu les données secrètes de l'entreprise à une entreprise concurrente
    c. Les employeurs de l'institut ont fait une grève suivie par une protestation qui bloque la porte
    d. L'ingénieur de l'entreprise a bloqué le serveur mail suite à une tentative de piratage externe
3. Citer (sans expliquer) les différentes techniques anti-intrusion
4. Expliquer brièvement le fonctionnement des systèmes de détection d'intrusion par comportement
5. Citer (sans expliquer) 4 limite des systèmes de détection d'intrusion
6. Que signifie les « Hoax »
7. Faire une comparaison simple entre les domaines de « sécurité informatique » et « vie privée »
8. Définir le risque informatique et quelle est la différence avec la vulnérabilité

Exercice 01 : (12 points)

Une entreprise des produits alimentaires désirant protéger son système construit des biens suivants :

- Un réseau informatique
- Deux serveurs de données géants contenant les différentes machines virtuelles déployant chacune un service bien spécifié (service mail, service base de données … etc.)
- Une base de données des employeurs et clients de l'entreprise
- Un archive papier des différentes conventions et offres passées
- Un accès par carte magnétique et empreinte à l'entrée de chaque service
- Réseau de surveillance vidéo connecté à l'un des serveurs pour le stockage des vidéos dans une base de données spéciale
- Stock des produits contenant plusieurs réfrigérateurs géants

Les employeurs sont classés par leurs postes (employeur normal, chef service, administrateur principal et employeur de sécurité). La base de données des employeurs est organisée comme suit :

Employeur (ID, nomComplet, Adresse, téléphone, numSecSoc, secteur)
EmpNorm : table qui hérite la table Employeur en ajoutant les fonctionnalités et département de l'employeur normal
ChefSer : table qui hérite la table Employeur en ajoutant les fonctionnalités et département de l'employeur chef service
Admin : table qui hérite la table Employeur en ajoutant les fonctionnalités et département de l'employeur administrateur
EmpSec : table qui hérite la table EmpNorm en ajoutant les fonctionnalités et département de l'employeur de sécurité
Client (ID, nomClient, AdrClient, TelClient, Prod)
Produit (ID, type, composition, numStock)
Stock (numStock, IDProd, dateStock, QtsStock)

1. Remplir le tableau de l'annexe 2 pour chacun des biens cités au-dessus

Dans le cadre d'une convention entre l'entreprise et la société privée dont vous travaillez de ce projet de sécurité, vous étiez contacté afin de sécuriser les bases de données de l'entreprise. Pour cela, vous avez choisir le mécanisme de contrôle d'accès pour la sécurisation. Les dirigeants de l'entreprise avaient offert les règles d'accès suivantes en précisant que la stratégie de contrôle est bien basée sur le modèle MAC:

- L'administrateur aura l'accès à toutes les données existantes dans la base de données des vidéos (contenant seulement la table archiVid) en lecture seule et la base de données des employeurs par toutes les droits
- L'employeur normal aura l'accès seulement à la table des produits par lecture seule et la table Stock par tous les droits
- L'employeur de sécurité aura l'accès par lecture seule à la table vidéo avec les droits hérités
- Le chef de service aura l'accès à la table EmpNorm en lecture et modification, la table ChefSer an lecture et table produit en lecture

2. Donner les différentes requêtes SQL d'octroi des droits afin d'assurer la situation
3. Donner la matrice de contrôle d'accès correspondantes
4. Donner le graphe d'octroi de droits correspondant
5. Après un temps, l'entreprise avait effectué un audit de sécurité sur les fichiers log dont ils ont découvert quelques incidents liés à la politique de contrôle d'accès définis :
    a. Un chef de service avait modifié quelques informations des employeurs des autres secteurs
    b. Un employeur avait vendu des informations concernant les secrets de succès des produits à une entreprise concurrente

- Proposer sans détails une solution à chacun des problèmes détectés

Les dirigeants ont décidé de changer les droits d'accès en enlevant quelques droits et ajoutant d'autres et en changeant la stratégie vers le modèle DAC. Les modifications sont comme suit :

- L'administrateur garde toujours ses propres droits
- L'employeur normal aura l'accès à la table produit par lecture seule sauf les colonnes ID et numStock par lecture et modification et ne peut en aucun cas la lecture sur la colonne composition et aura l'accès aussi à la table stock par insertion, consultation et suppression
- L'employeur de sécurité garde ses propres droits
- Le chef de service aura l'accès à la table EMPNorm par lecture seule et pouvait donner ce droit aux employeurs de son service et garde les droits sur la table chefSer

6. Donner les requêtes SQL permettant la modification de la matrice selon les modifications citées
7. Donner le nouveau graphe d'octroi de droits

Annexe 1 :

Attaque	**1ère classification**	**2ème classification**	**3ème classification**	**4ème classification**
……..	……..	……..	……..	……..

Annexe 2 :

bien	**Type**	**Menace possible**	**Importance de la menace**
……..	……..	……..	……..

Type : physique ou logique
Menace possible : donner une et une seule menace
Importance de la menace : importante, négligé, peut être négligé