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

1ère année Master RSE 2022-2023
Module : Sécurité des réseaux durée : 1h30

Examen Semestriel

Nom : …… **Prénom :……..** **Groupe :……**

Remarques :

- Chaque question est notée sur **1 point**
- Une seule réponse juste parmi 3 **(1/3)** signifie **(0. 5 point)**
- **2** réponses justes signifient **(0.75 point)**
- 3 réponses = objectifs de sécurité, type de scénario et techniques de protection
- Les **05** premières questions du QCM représentent **25%** de la note de TP et **75%** restante consiste du projet de TP.
- La réponse doit être par un 'X' dans les carrés correspondants, chaque réponse contient un autre signe ne sera pas prise en compte y compris une réponse barrée

---

Questions :

Pour chacun des scénarios possibles, choisissez : **LE(S)** objectif(s) de sécurité, **LE** type de scénario et **LA(LES)** technique(s) de protection correspondante(s)

1. Lors de consultation d'un site web pour la première fois, un message de connexion non sécurisée est affichée avec le label « CERT_SELF_SIGNED »

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ Risque	☐ Valider le certificat SSL par un organe habilité
☐ L'intégrité	☐ Vulnérabilité	☐ Ajouter une règle dans la politique de sécurité
☐ La disponibilité	☐ Menace	☐ Créer une interface d'accès avec mot de passe
☐ L'authentification	☐ Attaque	

2. Dans l'objectif de tracer tous les accès réseaux externes vers un service numérique d'une institution, les gérant ont chargé le responsable de sécurité d'assurer cette tâche

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La non-répudiation	☐ Attaque	☐ Mise à jour Windows
☐ L'intégrité	☐ Traitement de risque	☐ Installer un écouteur réseau (sniffer)
☐ La journalisation	☐ Scénario opérationnel	☐ Installer un détecteur d'intrusion
☐ L'authentification	☐ Scénario stratégique	

3. Un employé malveillant, viré de son poste, a exploité une erreur dans le système d'information afin de récupérer les mots de passes des sessions de ses collègues. Il a par la suite changé tous les mots de passes en empêchant les employés d'y accéder au système.

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La non-répudiation	☐ Risque	☐ Mise à jour des mots de passes
☐ La disponibilité	☐ Vulnérabilité	☐ Contrôle d'intégrité
☐ L'authenticité	☐ Menace	☐ Passer l'employé en justice
☐ L'authentification	☐ Attaque	☐ configurer le backup périodique de la BDD

4. Considérer une personne qui a exécuter un script permettant de tester toutes les combinaisons possibles afin de trouver un mot de passe de session dans un système d'information (s'appel brute force). Après deux (02) mois, le script a fini de trouver le mot de passe après cinq (05) milliards d'essais.

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ L'authentification	☐ Risque	☐ Ajouter une procédure de changement périodique de MDP
☐ L'intégrité	☐ Vulnérabilité	☐ Ajouter une règle dans la politique de sécurité
☐ La disponibilité	☐ Menace	☐ Ajouter option de non connexion après trois (03) essais échoués
☐ L'authenticité	☐ Attaque	

5. Dans une convention d'échange de données entre deux (02) institutions, une institution avait exploité les données confidentielles reçues de l'autre institution puis les a partagés avec une tierce institution dans un autre cadre

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ L'intégrité	☐ Risque	☐ Revoir les clauses de la convention
☐ La disponibilité	☐ Vulnérabilité	☐ Mettre à jour la PSSI
☐ L'authentification	☐ Scénario opérationnel	☐ Arrêter le projet
☐ La confidentialité	☐ Attaque	☐ Commencer une poursuite judiciaire

6. Un ingénieur d'une entreprise à exécuter la commande suivante : « **openssl enc -aes256 -base64 -k $(base64 ext1_shared_secret.bin) -e -in plain.txt -out cipher.txt** »

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ Risque	☐ Revoir la configuration du serveur
☐ L'intégrité	☐ Vulnérabilité	☐ Chiffrer des données secrètes
☐ La disponibilité	☐ Protection	☐ Signer des données secrètes
☐ L'authentification	☐ Attaque	

7. Lors d'un projet d'estimation des attaques possibles sur un systèmes d'information, les dirigeant de l'entreprise ont signalé qu'une perte possible de 20000$ par an suite au vol des comptes des clients, est acceptable

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ Risque	☐ Laisser passer le scénario
☐ L'authenticité	☐ Scénario stratégique	☐ Mettre à jour la PSSI
☐ La disponibilité	☐ Traitement d'un risque	☐ Sensibiliser les clients
☐ L'authentification	☐ Attaque	☐ Implémenter la mise à jour périodique des mots de passe

8. Un programme exécutable a été injecté dans une mise à jour Windows permettant de communiquer toute information privée dans le disque dur vers des serveurs distants inconnus

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ L'intégrité	☐ Attaque	☐ Sensibiliser les utilisateurs
☐ L'authenticité	☐ Menace	☐ Mettre à jour l'antivirus
☐ L'authentification	☐ Scénario opérationnel	☐ Désactiver Windows update
☐ La confidentialité	☐ Protection	

9. Lors de l'utilisation d'une impression d'un document dans une imprimante réseau, un message d'erreur s'affiche indiquant que l'imprimante est occupée par un autre processus alors que personne ne l'utilise avant

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La disponibilité	☐ Attaque	☐ Vider la mémoire de l'imprimante
☐ La confidentialité	☐ Vulnérabilité	☐ Redémarrer l'ordinateur
☐ L'authenticité	☐ Menace	☐ Passer l'imprimante en réparation
☐ L'intégrité	☐ Risque	

10. Dans le cadre de déploiement d'un service en ligne, les ingénieurs d'une entreprise ont installé une machine virtuelle sous PFSENSE et configuré des règles de filtrage de paquets afin d'éviter l'inondation des serveurs par des fausses requêtes

Objectifs de sécurité visé	**Type de scénario**	**Techniques de protection**
☐ La confidentialité	☐ Menace	☐ Equilibreur de charge (Load Balancer)
☐ L'intégrité	☐ Attaque	☐ Pare-feu
☐ La disponibilité	☐ Protection	☐ Anti-virus
☐ L'authentification	☐ Vulnérabilité	☐ Système de détection d'intrusion

---

Exercice (10 points):

Considérant le système suivant composé de sept (07) serveurs dont leurs disponibilités sont respectivement les suites :

S1 = 99%, S2 = 75%, S3 = 99.7%, S4 = 98%, S5 = 86%, S6 = 91%, S7 = 91.3%

Pour chacun des scénarios suivants, donner la formule de calcul et la disponibilité totale du système

1- (S1 – S2) // (S3 – S4) // S5 // (S6 – S7)
   a. Formule :
   b. Disponibilité :

2- S1 – (S2//S5) - S6 – (S7// (S4 – S3))
   a. Formule :
   b. Disponibilité :

3- (S6 – S1) // (S2 – S5) // (S3 – S4 – S7)
   a. Formule :
   b. Disponibilité :

4- (S1 – S3 – S4) // (S7 – S2) // (S5 – S6)
   a. Formule :
   b. Disponibilité :

5- (S1 // S3 // S4) – (S7 // S2) – (S5 // S6)
   a. Formule :
   b. Disponibilité :

Bonne chance