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

1ére année Master ISII 2022-2023

Module : Méthodologie de le Sécurité Informatique durée : 1h30

Examen Semestriel

Questions de cours : (04 points)

1. Quel sont les composantes du système d'information prises en considération dans un système de management de sécurité de l'information (SMSI)
2. A quoi ça sert le cycle opérationnel dans la méthode EBIOS-RM
3. Quelle est la différence entre vulnérabilité et menace
4. Décrire brièvement la différence entre la sécurité informatique et la préservation de la vie privée

---

Exercice 01 : (11 points)

Dans le cadre de développement des plateformes numériques destinées à usage interne d'une entreprise, une application de gestion des projets de l'entreprise et de leur suivi a été mise en place. Il s'agit d'une application en ligne permettant à l'ensemble des employés d'effectuée des tâches et de suivre l'avancement des projets.

L'application (site web) est déployée au niveau des serveurs d'Algérie Télécom tandis que la base de données a été gardée sur un serveur de l'entreprise. La communication entre l'application et la base de données est faite via un VPN sécurisé qui utilise un chiffrement à courbe elliptiques avec des clés de taille 1024bits. Chaque employé possède un ordinateur de bureau connecté à internet permettant d'accéder à l'application. La base de données est développée sur le SGBD Oracle 19C et définie selon le modèle suivant :

User (name, addr, mail, tlf, role)

Task (ID, title, type, due, start)

Project (ID, title, service, PrjHead, due, tasks)

Service (title, SerHead, users)

Les employés de l'entreprise sont trois (03) types : directeur technique, chef de service, technicien. Chacun des employés aura des tâches précises et des droits bien définis. Les droits sont classés comme suit :

- Un directeur technique a tous les droits sur les projets concernant son domaine d'expertise
- Chaque projet est affecté à un service dont le chef de service peut consulter à tout moment son état d'avancement par rapport à l'avancement de ses taches
- Chaque projet possède un chef de projet qui peut être le chef de service comme être un employé simple
- Chaque projet est composé d'un ensemble de tâches
- Le directeur technique ainsi que le chef de service sont considérés comme des employés
- Chaque employé peut consulter les tâches affectées à lui ainsi qu'il peut les mettre à jour
- Un nouveau projet discuté est validé dans une réunion est créé dans l'application par le directeur technique

En avril 2022, un rapport de vulnérabilité publié sur le SGBD en question sous le code CVE-2022-21498 permet à un attaquant authentifié, avec moins de privilèges, d'effectuer des opérations non autorisées sur des données sensibles à savoir : la création, modification, suppression et publication des données secrètes.

1. Vous avez été consultés dans le cadre d'une analyse des risques sur cette application, répondez aux questions suivantes :
    a. Décrire, en remplissant, le tableau en annexe un scénario de risque possible
    b. Quelle est la gravité du risque choisie ? justifier votre réponse
    c. Proposer un traitement pour votre risque
2. Proposer une matrice de contrôle d'accès avec moindre de privilèges selon la description du texte au-dessus en basant sur le modèle RBAC avec 2 utilisateurs (1 directeur technique, 1 technicien)

3. Donner toutes les requêtes SQL permettant l'octroi des droits

---

Annexe :

Bien essentiel	Bien support	Source de risque	Objectif de sécurité	Scénario stratégique	Scénario opérationnel	dégâts possibles*
……	……	……..	……	……	……	……

* : exprimer les dégâts selon les options vues dans le cours (crédibilité, dégâts judiciaires, pertes financière)

Bonne chance