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

1ére année Master ISII 2023-2024
Module : Méthodologie de le Sécurité Informatique durée : 1h30

Corrigé modèle

Questions de cours : (7.25 pts)

1. Quel est l'objectif principal derrière la mise en place d'un système de management de la sécurité de l'information (SMSI) ?

L'objectif principal de la mise en place du SMSI est de **minimiser les risques (1pt)**

2. Quel est la différence entre l'Authentification et l'Authenticité ?

L'authentification consiste à confirmer **l'identité d'une personne** tandis que l'authenticité consiste à confirmer **la propriété de la chose (1pt)**

3. Quelle est la relation entre la non-répudiation, l'identification et l'authentification ?

La non-répudiation requis la **traçabilité des actions** et de celui qui a effectué les actions, ce qui signifie qu'il faut **identifier l'actionneur**. Cet actionneur ne doit effectuer que les actions dont il est autorisé à faire ce qui signifie qu'il doit **s'authentifier (2pts)**

4. Citez les cinq catégories de risque informatique

Les catégories des risques sont : négligeable, acceptable, à réduire, à transférer, n'existe pas **(1.25pts)**

5. Quel est la différence entre un pare-feu applicatif et un pare-feu d'applications ?

Un pare-feu d'application consiste à filtrer des paquets entrants/sortants via un port bien défini (http, ftp …etc.) alors que le pare-feu applicatif consiste à contrôler le trafic exploité par des applications installées quel que soit le port utilisé **(2pts)**

Exercice 01 :

Dans le cadre de l'organisation d'un concours de maitrise (un concours de passage de grade Médecin Assistant au grade Maitre-Assistant en Médecine), les cadre du Ministère de l'Enseignement Supérieur et de la Recherche Scientifique ont décidé de l'organiser dans une plateforme numérique. Pour cela, la procédure suivante est arrêtée :

i. Un Médecin Assistant **(assist)** doit déposer un dossier composé de trois (03) parties : la partie administrative, la partie pédagogique et la partie scientifique
ii. Après dépôt, un agent administratif **(admin)** aura une notification d'un nouveau dossier, il procède par le traitement du dossier entier pour vérifier s'il est complet et bien présenté
iii. Après validation du dossier complet, l'admin traitera le dossier administratif afin de calculer la note administrative
iv. Une fois le traitement des dossiers administratifs se terminent, trois (03) membres de jury **(jury)**, désignés avant, traiteront les dossiers pédagogiques et scientifiques pour calculer leurs notes correspondantes
v. En date du concours, les membres de jury réunissent en ligne avec les médecins assistants candidats pour un concours sous-forme de question/réponse, pour cela il est organisé dans la même plateforme comme suit :
    a. Dès que l'entretien commence, la plateforme **(PCS)** choisit une question aléatoire et l'affiche au candidat
    b. Le candidat doit saisir sa réponse est la soumettre dans la plateforme avant que le temps de réponse se termine (30 secondes)
vi. A la fin, les jury consultent les réponses des candidats et rajoutent leurs évaluations aux notes pédagogiques
vii. Le candidat reçoit une notification de réussite ou non, selon son classement, dans le concours avec la note finale qui est la somme des notes des trois dossiers.

Considérant les caractéristiques suivantes :

- Chaque dossier consiste d'un ensemble de documents scannés dont leurs chemins sont stockés dans une table séparée
- Il y a une table contenant les notifications générées automatiquement par le système dans le système
- Les notes des dossiers sont séparées des dossiers dans une table dédiée
- Les questions du concours sont introduites par les membres du jury avant le concours dans une table dédiée
- Les réponses sont soumises également dans une table dédiée
- La plateforme ne permet pas ni de copier une question affichée, ni de coller un texte copié

1. Vous avez été consultés dans le cadre de la sécurisation de l'application dont il vous a été demandé d'effectuer une analyse des risques, 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 DAC
3. Donner toutes les requêtes SQL permettant l'octroi des droits

---

solution :

1. Évaluation du risque

a. Scénario du risque (2.5pts)

Bien essentiel	Bien support	Source de risque	Objectif de sécurité	Scénario stratégique	Scénario opérationnel	dégâts possibles*
Notes d'évaluation **(0.25pts)**	Plateforme de dépôt **(0.25pts)**	Administrateur (admin) **(0.25pts)**	Compromettre l'intégrité des notes **(0.25pts)**	Faire réussir les médecins échoués contre ceux qui mérite la réussite **(0.5pts)**	L'admin modifie les notes des dossiers pédagogiques et scientifiques directement sur la BDD par des requêtes SQL **(0.5pts)**	Atteinte à la crédibilité + dégâts juridiques **(0.5pts)**

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

b. **Gravité du risque :** ce risque est jugé grave voire **très grave** à cause de son impact important présenté par les poursuites judiciaires des personnes gagnants ainsi que le temps perdu en cas de découverte de l'attaque dans le cadre de réorganiser un autre concours **(0.75 pts)**

c. **Solution possible :** Pour remédier à ce risque, il faut définir une politique de contrôle d'accès basée sur le principe de « moindre de privilège » en basant sur les vues. Comme on peut aussi changer le schéma relationnel en intégrant les notes chacune avec son dossier qui la concerne. **(0.5 pts)**

2. Matrice de contrôle d'accès (18 x 0.25 = 4.5 pts)

	DosAdmin	DosPédag	DosScient	Notes	Notifications	Questions	Réponses
Assist	insert	insert	insert	select	select		insert
Admin	select	select	select	insert	select		
Jury		select	select	Update		insert	select
PCS					insert	select	

3. **Requêtes SQL (18 x 0.25 = 4.5 pts)**

Pour l'assistant:

Grant insert on DosAdmin to Assist
Grant insert on DosPédag to Assist
Grant insert on DosScient to Assist
Grant select on Notes to Assist
Grant select on Notifications to Assist
Grant insert on Réponses to Assist

Pour l'administrateur :

Grant select on DosAdmin to Admin
Grant select on DosPédag to Admin
Grant select on DosScient to Admin
Grant insert on Notes to Admin
Grant select on Notifications to Admin

Pour les members de jury :

Grant select on DosPédag to jury
Grant select on DosScient to jury
Grant update on Notes to jury
Grant insert on Questions to jury
Grant select on Réponses to jury

Pour le processus:

Grant insert on Notifications to PCS
Grant select on Questions to PCS

Bonne chance