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

1ère année Master ISII 2021-2022
Module : Méthodologie de Sécurité Informatique durée : 1h00

Examen Semestriel

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

Remarques :

- Chaque question est notée sur **1 point**
- Une seul réponse fausse parmi 3 **(1/3)** signifie une demi réponse **(0.75 point)**
- **2** fausses réponses et plus signifie que toute la réponse est fausse **(0.50 point)**
- Les **15** premières questions représentent **75%** de la note de TD et **25%** restante consiste du projet EBIOS mis en ligne.
- Le fait d'avoir soumis le travail d'EBIOS-RM ne signifie pas forcément **5/5**, une évaluation des projets définira la note.
- 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 type du scénario, le(s) objectif(s) de sécurité et la(les) technique(s) de protection correspondante(s)

1. Un employé a reçu une offre de mise à jour Windows gratuite sans préciser la source de cette mise à jour dans l'ordinateur de son bureau et il a accepté.

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité	☐ La confidentialité	☐ Désactiver Windows update
☐ Menace	☐ L'intégrité	☐ Ajouter une règle dans la politique de sécurité
☐ Attaque	☐ L'authenticité	☐ Virer l'employé de son poste
☐ Risque	☐ L'authentification	

2. A titre de prévention, les ingénieurs d'une entreprise ont développé un script permet de vérifier tous les matins les données de l'entreprise et les compare avec le dernier backup en cherchant toute modification possible.

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La confidentialité	☐ Copies de sauvegarde
☐ Protection	☐ L'intégrité	☐ Plan de continuité d'activité
☐ Attaque	☐ L'authenticité	☐ Pare-feu physique
☐ Risque	☐ L'authentification	

3. Il a été récemment noté que certaines entreprises en Algérie ont subis une défaillance utilisant un Ransomware qui a chiffré les données des serveurs en ajoutant l'extension « CUAG ».

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La confidentialité	☐ Copies de sauvegarde
☐ Protection	☐ L'intégrité	☐ Anti-virus à jour
☐ Risque	☐ L'authenticité	☐ Payer la rançon et récupérer les données
☐ Attaque	☐ La disponibilité	

4. Afin d'empêcher les employés de formater les ordinateurs de l'entreprise, le RSSI a définit une procédure permettant, en cas de défaillance d'un équipement, aux ingénieurs de procéder au formatage et enregistrement de l'opération

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La confidentialité	☐ Politique de sécurité des SI
☐ Protection	☐ L'intégrité	☐ Anti-virus à jour
☐ Risque	☐ L'authentification	☐ Plan de reprise après sinistre
☐ Attaque	☐ La non-répudiation	

5. Les BOTNET (connu aussi comme les zombies du web) sont des adresses IP actives dans le réseau mais ne correspondent à aucune machine (physique ou virtuelle) utilisés pour assurer un compromis DDOS

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La confidentialité	☐ Utiliser un pare-feu
☐ Protection	☐ L'authentification	☐ Filtrage des paquets réseaux
☐ Risque	☐ La non-répudiation	☐ Politique de sécurité des SI
☐ Attaque	☐ La disponibilité	

6. Lors d'un audit de sécurité, les auditeurs ont découvert que les mots de passes des mails professionnels sont stockés en clair dans la base de données

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La confidentialité	☐ Anti-virus
☐ Protection	☐ L'intégrité	☐ Hachage et Chiffrement
☐ Risque	☐ L'authenticité	☐ Plan de reprise d'activité
☐ Attaque	☐ La disponibilité	

7. Une entreprise autorise ses employeurs de travailler à distance, un employé laisse ses enfants jouer dans son ordinateur ce qui présente une opportunité de télécharger un programme permettant de copier tout le contenu du disque dur dans un site web

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La confidentialité	☐ Copies de sauvegarde (backup)
☐ Protection	☐ L'intégrité	☐ Système anti-phishing
☐ Risque	☐ L'authentification	☐ Politique de sécurité des SI
☐ Attaque	☐ La disponibilité	

8. Dans sa nouvelle stratégie, une entreprise vise a installer un nouveau Datacenter. Le problème est que l'emplacement choisi pour ce Datacenter se situe dans un endroit séismique

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La l'authenticité	☐ Annulation du projet
☐ Protection	☐ La non-répudiation	☐ Changement d'emplacement
☐ Risque	☐ La disponibilité	☐ Aucune solution
☐ Attaque	☐ La l'intégrité	

9. Les responsables de service personnel reçoivent toujours ses amis d'enfance dans son bureau à l'entreprise

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ L'authentification	☐ Plan de continuité d'activité
☐ Protection	☐ L'intégrité	☐ Installer Kaspersky
☐ Risque	☐ La confidentialité	☐ Politique de sécurité des SI
☐ Attaque	☐ La non-répudiation	

10. Après une analyse de sécurité, l'ingénieur de sécurité a découvert qu'un programme suspect envoie des informations du réseau local vers une adresse externe ; pour cela, il a ajouté cette règle snort : « alert TCP $HOME_NET any -> $EXTERNAL_NET any (sid :4003876 ; msg : « attention !!! » ;) »

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La confidentialité	☐ Détection d'intrusion
☐ Protection	☐ L'intégrité	☐ Anti-virus
☐ Risque	☐ L'authenticité	☐ Pare-feu
☐ Attaque	☐ La disponibilité	

11. Durant un audit de sécurité, il a été remarqué une absence totale des backups

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La disponibilité	☐ Copies de sauvegarde
☐ Protection	☐ La confidentialité	☐ Politique de sécurité des SI
☐ Risque	☐ La non-répudiation	☐ Plan de continuité d'activité
☐ Attaque	☐ L'identification	

12. Dans sa nouvelle version, le SQLInjection permet d'injecter de fausse donnée afin de détourner les algorithmes d'apprentissage vers la mauvaise décision

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La confidentialité	☐ Etudier la véracité des données
☐ Protection	☐ L'intégrité	☐ Politique de contrôle d'accès
☐ Risque	☐ L'authenticité	☐ Anti-virus
☐ Attaque	☐ La disponibilité	

13. En 2020, une erreur de Windows 10 permet aux utilisateurs malveillants d'avoir un accès au ordinateurs à distance. Ce scénario assure la connexion à l'aide de l'une des sessions dudit ordinateur.

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La confidentialité	☐ Contrôle d'accès
☐ Protection	☐ L'authenticité	☐ Configuration du réseau
☐ Risque	☐ L'authentification	☐ Pare-feu
☐ Attaque	☐ La disponibilité	

14. Un étudiant connecte son Facebook durant le cours de sécurité

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La disponibilité	☐ Plan de reprise d'activité
☐ Protection	☐ La non-répudiation	☐ Plan de continuité d'activité
☐ Risque	☐ L'authenticité	☐ Politique de sécurité des SI
☐ Attaque	☐ La disponibilité	

15. Une personne dans le métro a essayé d'accéder à son mail en tapant le mail et mot de passe dans son téléphone Android. Une personne curieuse avait remarqué la procédure et souvenu des caractères tapés. Dans le soir même, la personne curieuse à utilisé les informations observées pour ré-accéder de sa maison mais le serveur l'a empêché pour une tentative de connexion d'une nouvelle machine.

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La disponibilité	☐ Compagne de sensibilisation
☐ Protection	☐ L'intégrité	☐ Anti-virus à jour
☐ Risque	☐ L'authenticité	☐ Bloquer le réseau 4G dans le métro
☐ Attaque	☐ La confidentialité	

16. Afin d'automatiser le traitement de pointage des employé suite à la découverte que certains employés signent le pointage de leurs collègues, les gérants de l'entreprise ont acquis un système de pointage par empreinte digitale

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La confidentialité	☐ Biométrie
☐ Protection	☐ L'intégrité	☐ Anti-virus à jour
☐ Risque	☐ La non-répudiation	☐ Politique de sécurité des SI
☐ Attaque	☐ La disponibilité	

17. Les étudiants d'un département ont bloqué la porte principale de la faculté suite à leur grève. En conséquence, aucun étudiant ni enseignant n'a pu accéder

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La confidentialité	☐ Copies de sauvegarde
☐ Protection	☐ L'intégrité	☐ Anti-virus à jour
☐ Risque	☐ La disponibilité	☐ Payer la rançon et récupérer les données
☐ Attaque	☐ L'authenticité	

18. Un site web déployé affiche l'erreur de connexion non sécurisée à cause d'une absence d'un document important

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La confidentialité	☐ Installer un certificat SSL dans le serveur
☐ Protection	☐ L'intégrité	☐ Anti-virus à jour
☐ Risque	☐ L'authentification	☐ Pare-feu
☐ Attaque	☐ La disponibilité	

19. Dans une université, une loi est définie contenant la règle : « il est strictement interdit de laisser entrer une personne ne présentant pas une carte d'identité ou une carte professionnelle de l'université »

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La confidentialité	☐ Détecteur d'intrusion
☐ Protection	☐ L'intégrité	☐ Anti-virus
☐ Risque	☐ L'authentification	☐ Politique de sécurité des SI
☐ Attaque	☐ La disponibilité	

20. Dans la plupart des procédures administratives en Algérie, la personne concernée doit être toujours présente. Pour certaines procédures, une dérogation officielle égalisée à la mairie suffit.

Type de scénario	Objectifs de sécurité visé	Techniques de protection
☐ Vulnérabilité / Menace	☐ La confidentialité	☐ Politique de sécurité des SI
☐ Protection	☐ L'intégrité	☐ Pare-feu
☐ Risque	☐ L'authentification	☐ Journalisation
☐ Attaque	☐ La disponibilité	