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

1ère année Master RSE 2021-2022
Module : Sécurité des réseaux durée : 1h00

Examen Semestriel

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

Remarques :

- Chaque question est notée sur **1 point**
- Une seul réponse fausse parmi 3 **(1/3)** signifie **(0.75 point)**
- **2** fausses réponses donnent **(0.5 point)**
- 3 réponses = objectifs de sécurité, type de scénario et techniques de protection
- Les **15** premières questions représentent **75%** de la note de TD et **25%** restante consiste du projet EBIOS-RM 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.

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. Dans un article publié le 22 juin 2022, des chercheurs ont révélé un ensemble de scénarios possibles à être exploités afin de compromettre le service cloud de l'entreprise fameuse « MEGA » afin de voler des informations secrètes.

Objectifs de sécurité visé	**Type de scénario**	**Techniques de protection**
☐ La confidentialité	☐ Risque	☐ Revoir le plan de continuité d'activité
☐ L'intégrité	☐ Vulnérabilité	☐ Ajouter une règle dans la politique de sécurité
☐ La disponibilité	☐ Menace	☐ Changer les algorithmes de chiffrement utilisés
☐ L'authentification	☐ Attaque	

2. Un ingénieur d'une entreprise, dans le cadre de la sécurisation de leur site web, a exécuté la commande suivante : « openssl req -new -key private.key -out server.csr ».

Objectifs de sécurité visé	**Type de scénario**	**Techniques de protection**
☐ La confidentialité	☐ Risque	☐ Signature numérique
☐ L'intégrité	☐ Vulnérabilité	☐ Certificat électronique
☐ L'authentification	☐ Menace	☐ Cryptographie
☐ La disponibilité	☐ Attaque	

3. Lors de l'analyse des risques d'un système d'information, les analystes ont trouvé une possibilité d'arrêt total du système à cause d'une erreur humaine. Cet arrêt causera une perte de crédibilité et conduira à des poursuite judiciaires et perte financière importante

Objectifs de sécurité visé	**Type de scénario**	**Techniques de protection**
☐ L'intégrité	☐ Risque – scénario stratégique	☐ Définir une politique de sécurité du SI
☐ L'authentification	☐ Vulnérabilité	☐ Définir une procédure de reprise en cas de défaillance
☐ La disponibilité	☐ Attaque	☐ Contrôle des processus en cours
☐ L'authentification	☐ Risque – scénario opérationnel	

4. Durant une attaque contre un système d'information, un attaquant tend de préserver le contrôle total sur le système. Pour cela, il a implanté un programme malveillant permettant d'ouvrir des portes dérobées aléatoires afin de permettre plusieurs possibilités d'accès

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ L'authentification	☐ Contrôle des privilèges	☐ Utiliser un IDS
☐ L'intégrité	☐ Établir une implantation	☐ Etablir un scan des portes réseaux périodiquement
☐ La disponibilité	☐ Reconnaissance initiale	☐ Mise à jour de l'anti-virus et établir un scan périodique
☐ L'authentification	☐ Compléter la mission	

5. Un étudiant réussit à modifier sa note lorsque le professeur a laissé son PC allumé à la salle

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ Risque	☐ Passer l'étudiant au conseil discipline
☐ L'intégrité	☐ Vulnérabilité	☐ Mettre à jour la PSSI
☐ La disponibilité	☐ Traitement d'un risque	☐ Bloquer toutes les délibérations jusqu'à trouver une solution
☐ L'authentification	☐ Attaque	

6. Un ingénieur d'une entreprise à exécuter la commande suivante : « **openssl x509 -req -in server-req.pem -CA ca-cert.pem -CAkey ca-key.pem -CAcreateserial –out server-cert.pem** »

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ Risque	☐ Revoir la configuration du serveur
☐ L'intégrité	☐ Vulnérabilité	☐ Créer un certificat électronique
☐ La disponibilité	☐ Protection	☐ Signer un certificat électronique
☐ L'authentification	☐ Attaque	

7. Dans les derniers statistiques publiés récemment, le nombre des nouveaux ransomware ne cesse de croitre. Il est estimé qu'en fin 2021, plus de 11.2 trillions de $ seront payés comme rançons

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ Risque	☐ Développer des anti-virus plus efficaces
☐ L'intégrité	☐ Vulnérabilité	☐ Mettre à jour la PSSI
☐ La disponibilité	☐ Traitement d'un risque	☐ Sensibiliser les utilisateurs
☐ L'authentification	☐ Attaque	

8. Il a été remarqué ces derniers temps que l'application YouTube, ainsi que le site web, affiche beaucoup de publicités en Algérie en passant entre les vidéos. Certaines publicités peuvent être malveillantes ciblant certains profils spécifiques à savoir l'escroquerie et le vol d'information

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ L'ingénierie sociale	☐ Sensibiliser les utilisateurs
☐ L'intégrité	☐ Attaque par malware	☐ Proposer une loi qui interdit YouTube en Algérie
☐ L'authenticité	☐ Traitement d'un risque	☐ Proposer des applications autres que YouTube
☐ L'authentification	☐ Menace	

9. Lorsqu'il s'agit de la version gratuite de l'application de visioconférence ZOOM, si le nombre de participants dépasse 3 personnes, la réunion se ferme automatiquement après 40 minutes. Il suffit après de ré-entrer avec le même lien de réunion ce qui cause un retard par fois dans les cours en ligne et les réunions importantes

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ Risque	☐ Acheter une version complète payante de ZOOM
☐ L'intégrité	☐ Vulnérabilité	☐ Utiliser Google MEET
☐ La disponibilité	☐ Protection	☐ Eliminer la solution des réunion et cours à distance
☐ L'authentification	☐ Attaque	

10. Dans une entreprise, les ingénieurs de sécurité définissent une stratégie claire de l'utilisation des mots de passe comprenant des mots de passe complexes qui doivent être changés périodiquement

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ Risque	☐ Politique de sécurité
☐ L'intégrité	☐ Vulnérabilité	☐ Plan de continuité d'activité
☐ La disponibilité	☐ Protection	☐ Utilisation des anti-virus
☐ L'authentification	☐ Attaque	

11. Dans une analyse effectuée à l'aide du logiciel MBSA (Microsoft Baseline Security Analyzer), un étudiant a découvert un rapport décrivant une erreur dans le service internet (IIS) de Windows 10 dans une machine dans la salle TP

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ Risque	☐ Mettre à jour Windows
☐ L'intégrité	☐ Vulnérabilité	☐ Installer un détecteur d'intrusion
☐ La disponibilité	☐ Protection	☐ Effectuer une analyse des risque et élaborer un plan d'action approprié
☐ L'authentification	☐ Attaque	

12. Dans sa nouvelle forme, SQLInjection vise à injecter des fausses données afin de compromettre les algorithmes d'intelligence artificielle et les conduire vers le mauvais chemin de décision

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ Risque	☐ Etudier la véracité des données avant de les analyser
☐ L'intégrité	☐ Vulnérabilité	☐ Interdire l'utilisation de l'IA dans les secteurs sensibles
☐ La disponibilité	☐ Protection	☐ Etudier l'efficacité des algorithmes de l'IA
☐ L'authentification	☐ Attaque	

13. Un développeur en chômage a passé un temps pour développer un dispositif intelligent permettant de détecter des parties de code byte des fichiers suspects d'être malveillants

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

14. Dans un article publié le 03 Décembre 2021, Une série de campagnes malveillantes ont utilisé de faux installateurs d'applications et de jeux populaires tels que Viber, WeChat, NoxPlayer et Battlefield, via Google play store, pour inciter les utilisateurs à télécharger une nouvelle porte dérobée et une extension Google Chrome malveillante non documentée.

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ L'authentification	☐ Risque	☐ Utiliser un pare-feu
☐ L'intégrité	☐ Vulnérabilité	☐ Anti-malware
☐ La disponibilité	☐ Protection	☐ Sensibiliser les utilisateurs
☐ L'authenticité	☐ Attaque	

15. Durant une visite à un site web d'une entreprise, une page s'apparaître indiquant que la connexion à ce site n'est pas sécurisée en indiquant le message « ERROR : CERT_AUTO_SIGNED »

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ Risque	☐ Acheter un certificat SSL valide
☐ L'intégrité	☐ Vulnérabilité	☐ Redémarrer le serveur web de l'entreprise
☐ La disponibilité	☐ Menace	☐ Utiliser un Pare feu
☐ L'authentification	☐ Attaque	

16. Dans une entreprise possédant une site web statique, une page de « site en cours de maintenance » est utilisée lors des maintenances sur la machine virtuelle correspondante. Cette opération qui ne dure pas plus de 3 jours coûte l'entreprise une perte financière minimale.

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ Risque	☐ Définir une solution de basculement automatique à un site redondant
☐ L'authentification	☐ Vulnérabilité	☐ C'est un scénario normal
☐ La disponibilité	☐ Protection	☐ Définir un plan de reprise d'activité
☐ L'intégrité	☐ Attaque	

17. Prenant le même scénario de la question précédente mais avec une perte financière importante

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ Risque	☐ Définir une solution de basculement automatique à un site redondant
☐ L'authentification	☐ Vulnérabilité	☐ C'est un scénario normal
☐ La disponibilité	☐ Protection	☐ Définir un plan de reprise d'activité
☐ L'intégrité	☐ Attaque	

18. 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 !!! » ;) »

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

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

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

20. « ILOVEYOU » (créé en mai 2000) est un script intégré dans un mail qui permet d'envoyer automatiquement le même mail à toutes les adresses du contact de la victime une copie du mail

Objectifs de sécurité visé	Type de scénario	Techniques de protection
☐ La confidentialité	☐ Risque	☐ Installer un pare-feu
☐ L'authentification	☐ Vulnérabilité	☐ Utiliser un anti-virus en ligne
☐ La disponibilité	☐ Attaque	☐ Sensibiliser les utilisateurs de l'ouverture des mails suspects
☐ L'authenticité	☐ Menace	