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

A

3éme année Licence ISIL 2019-2020
Module : Sécurité des Systèmes d'Information 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 **(0.5 point)**
- **2** fausses réponses et plus signifie que toute la réponse est fausse **(00 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 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(s) objectif(s) de sécurité, la(les) technique(s) d'attaque et la(les) technique(s) de protection correspondante(s)

1. Un ingénieur réseau d'une entreprise ferme tous les modems et serveurs de l'entreprise durant chaque week-end

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La confidentialité	☐ Blocage d'accès aux données	☐ Installer un pare-feu
☐ L'intégrité	☐ Arrêt de site web	☐ Ajouter une règle dans la politique de sécurité
☐ La disponibilité	☐ Suppression des données	
☐ L'authentification	☐ Espionnage industriel	☐ Virer l'ingénieur de son poste

2. Un enseignant a ajouté un livre d'un Américain dans la plateforme Moodle autant qu'un support de cours pour les étudiants en mentionnant que c'est son propre support

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La confidentialité	☐ Vol de données	☐ Signature du PDF
☐ L'intégrité	☐ Usurpation d'identité	☐ Ajouter une règle dans la politique de sécurité
☐ L'authenticité	☐ Vol des mots de passe	
☐ L'authentification		☐ Virer l'enseignant de son poste

3. « 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	Méthodes d'attaque	Techniques de protection
☐ La confidentialité	☐ Malware	☐ Installer un pare-feu
☐ L'intégrité	☐ Attaque d'arrêt de système (DOS)	☐ Utiliser un anti-virus en ligne
☐ L'authenticité		☐ Contrôler l'accès au système
☐ L'authentification	☐ Vol des mots de passe	

4. Afin de prévenir les attaques de vol des mots de passe venant dans des messages Gmail, l'ingénieur de sécurité à décider d'utiliser la règle snort suivante : « log SNMP any any -> $HOME_NET any (sid :2000025 ; msg : « attaque suspect sur le réseau » ;)

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La confidentialité	☐ Vol de données	☐ Utiliser un IDS
☐ L'intégrité	☐ Malware	☐ Utiliser la journalisation
☐ L'authenticité	☐ Accès à la base de données	☐ Interdire l'accès au Gmail à partir de réseau d'entreprise
☐ La disponibilité		

5. Une entreprise a subi une attaque d'un Ransomware

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La confidentialité	☐ Malware	☐ Anti-virus
☐ L'intégrité	☐ Vol de données	☐ Blocage connexion
☐ La disponibilité	☐ Interdiction de l'accès (DOS)	☐ IDS
☐ L'authentification		

6. Lors de création d'une startup en ligne, les ingénieurs n'ont pas configuré les copies de sauvegarde (backup)

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La disponibilité	☐ Interdiction d'accès	☐ Configurer les backups
☐ L'intégrité	☐ Usurpation d'identité	☐ Supprimer les données inutiles
☐ L'authenticité	☐ Suppression des données	☐ Bloquer l'entreprise jusqu'à trouver une solution
☐ L'authentification		

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

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La confidentialité	☐ Vol de données	☐ Pare-feu
☐ La disponibilité	☐ Contrôle du PC à distance	☐ Ajouter une règle dans la politique de sécurité
☐ L'intégrité	☐ Harcèlement en ligne	☐ Tracer les accès au système à distance
☐ L'authentification		

8. Un ordinateur contient Windows 10 installé avec deux sessions sans mots de passe ainsi que le port TELNET est toujours ouvert

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La confidentialité	☐ Contrôle à distance	☐ Reconfigurer les paramètres de Windows 10
☐ L'intégrité	☐ Modification des données	☐ Installer un IDS
☐ L'authenticité	☐ Coupure d'électricité	☐ Utiliser Pare-feu
☐ L'authentification		

9. Un dirigeant a modifié sa fiche de paye afin de bénéficier d'un logement social LPA

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La confidentialité	☐ Malware	☐ Journalisation
☐ L'intégrité	☐ Modification des données	☐ Anti-virus
☐ L'authenticité	☐ Usurpation d'identité	☐ Contrôle d'accès
☐ L'authentification		

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 dans un outil de sécurité : « deny TCP 192.168.1.0 any 172.25.46.139 any »

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La confidentialité	☐ Malware	☐ Journalisation
☐ L'intégrité	☐ Modification des données	☐ Anti-virus
☐ La disponibilité	☐ Usurpation d'identité	☐ Pare-feu
☐ L'authentification		

11. Une université, durant la période des cours enligne, autorise les étudiants d'accéder en mode anonyme à la plateforme. Un enseignant a donné un travail maison pour le rendre dans la plateforme ce qui a provoqué un problème de connaître qui a envoyé les rapports

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La confidentialité	☐ Malware	☐ Journalisation
☐ L'authenticité	☐ Modification des notes TD	☐ Système d'authentification par mot de passe
☐ La disponibilité	☐ Usurpation d'identité	☐ Pare-feu
☐ L'authentification		

12. Durant la formation en ligne, un étudiant à exploité une nouvelle vulnérabilité de Microsoft Office (CVE-2017-11882) permettant d'intégrer un script d'exécution à distance dans un fichier Word. Après que quelques collègues ont reçus le rapport de leurs camarade et l'ouvert, l'étudiant en question a eu l'accès aux fichiers personnels des victimes

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La confidentialité	☐ Malware	☐ Journalisation
☐ L'intégrité	☐ Vol de données	☐ Anti-virus
☐ La disponibilité	☐ Usurpation d'identité	☐ Sensibilisation des utilisateurs
☐ La non-répudiation		

13. Lors d'une enquête de police sur une cyber-attaque, l'enquêteur a découvert qu'un flash disque infecté a été placé dans le serveur par une entité interne. L'employeur en question a nié qu'il a placé le flash en disant que sa session a été piraté par celui qui l'a placé (attaquant anonyme)

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La confidentialité	☐ Malware	☐ Journalisation
☐ La non-répudiation	☐ Phishing (lien piégé)	☐ Anti-virus
☐ La disponibilité	☐ Sniffing (Ecoute réseau)	☐ Pare-feu
☐ L'authentification		☐ IDS

14. Un ingénieur de sécurité dans une entreprise a exécuté la commande suivante d'OPENSSL sur 2 fichiers (original.txt et hachOriginal) : « openssl rsautl –verify –pubin cle.pub –in original.txt hachOriginal »

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La confidentialité	☐ Interdiction d'accès	☐ Signature numérique
☐ L'intégrité	☐ Modification des données	☐ Anti-virus
☐ La disponibilité	☐ Usurpation d'identité	☐ Cryptographie
☐ L'authentification		

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.

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La non-répudiation	☐ Phishing (lien piégé)	☐ Authentification multi-facteur
☐ L'intégrité	☐ Modification des données	☐ Anti-virus
☐ La disponibilité	☐ Usurpation d'identité	☐ Pare-feu
☐ L'authentification		

16. Un ingénieur réseau à introduit la règle suivante dans un outil de sécurité : « log ICMP 192.168.2.31 80 -> 192.168.5.0 any (sid:1000001 ; msg:"tentative de connexion de 192.168.2.31 au réseau d'administration"; logto: "/etc/logfiles/access_log" ;)

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La non-répudiation	☐ Cheval de troie	☐ Détecteur d'intrusion
☐ L'intégrité	☐ Attaque d'accès	☐ Anti-virus
☐ La disponibilité	☐ Modification des données	☐ Journalisation
☐ L'authentification		

17. Un enfant a désactivé l'antivirus après avoir suivre un vidéo et télécharger un programme pour craquer Windows

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La disponibilité	☐ Vol de données	☐ Détecteur d'intrusion
☐ L'intégrité	☐ Attaque d'accès	☐ Anti-virus
☐ La confidentialité	☐ Malware	☐ Pare-feu
☐ L'authentification		

18. Un programme téléchargé de l'internet permet de lancer un taux important de fausses alertes de l'antivirus ce qui a provoqué une réaction de l'utilisateur de désinstaller l'antivirus en croyant qu'il est inefficace

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La confidentialité	☐ Lien malveillant	☐ Journalisation
☐ L'intégrité	☐ Attaque d'accès	☐ Anti-virus
☐ La disponibilité	☐ Malware	☐ Cryptographie
☐ L'authenticité		

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 »

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La non-répudiation	☐ Usurpation d'identité	☐ Détecteur d'intrusion
☐ L'authentification	☐ Attaque physique	☐ Anti-virus
☐ La disponibilité	☐ Malware	☐ Politique de sécurité
☐ L'intégrité		

20. Dans les règles de la poste (CCP), en cas d'un retirement d'argent de plus de 30000da, une carte d'identité de la personne effectuant l'opération doit être présentée et authentifiée par l'agent. Lorsque la somme dépasse 100000da, une photocopie de la carte doit être gardé avec le cheque. Seul le propriétaire du compte peut effectuer ces opérations

Objectifs de sécurité visé	Méthodes d'attaque	Techniques de protection
☐ La non-répudiation	☐ Cheval de troie	☐ Politique de sécurité
☐ L'authenticité	☐ Attaque d'accès	☐ Pare-feu
☐ La disponibilité	☐ Modification des données	☐ Journalisation
☐ L'authentification		