Université ABBT
Faculté des Sciences
Département d'Informatique

Examen Final

Module : Sécurité Informatique
Niveau : L3

Nom :

Prénom :

Entourez la (les) bonne(s) réponse(s)

---***Partie contrôle***---

1. Dans la sécurité informatique, _____ signifie que les systèmes actifs informatiques ne peuvent être modifiés que par les personnes autorisées
   A) La confidentialité **B) l'intégrité** C) la disponibilité D) l'authenticité
2. Dans la sécurité informatique, _____ signifie que les informations contenues dans un système informatique ne sont accessibles en lecture que par les personnes autorisées.

   A) **La confidentialité** B) L'intégrité C) La disponibilité D) L'authenticité
3. Les types de menaces pour la sécurité d'un système informatique ou d'un réseau sont _____ ?

   A) **Interruption B) Interception C) Modification** D) Création E) **Fabrication**
4. Lequel des programmes suivants est un programme malveillant indépendant qui ne nécessite aucun d'autre programme ?

   A) Porte dérobée B) Cheval de Troie C) Virus **D) Ver**
5. Le _____ est un code incorporé dans un programme légitime configuré pour «exploser» lorsque certaines conditions sont remplies.

   A) Porte dérobée B) Cheval de Troie **C) Bombe logique** D) Virus
6. Lequel des programmes malveillants suivants ne se réplique pas automatiquement ?
   A) **Cheval de Troie** B) Virus C) Ver D) Virus polymorphe
7. Indiquer si l'expression suivante est vrai ou faux : « Un ver exécute une copie de lui-même sur un autre système. »
   A) **Vrai** B) Faux
8. Un utilisateur se plaint d'une connexion internet lente. Il vérifie l'interface externe du routeur en remarquant plusieurs connexions semi-ouvertes. Quel type d'attaque cela décrit-il ?
   A) Attaque DDOS B) Interception C) TCP Hijacking **D) SYN flooding**
9. Un tier consulte un site web, mais constate que le navigateur le redirige vers un autre site web et que l'URL a changé. De quel type d'attaque s'agit-il ?
   A) **Attaque par ingénierie sociale** B) Homme au milieu C) Injection SQL D) DDOS
10. Quelle technique permettant d'assurer l'intégrité des données ?
    A) **La signature électronique** B) Le certificat numérique C) le chiffrement D) Déchiffrement

---***Partie Examen***---

11. Lequel des éléments suivants permet de faire une porte dérobée cachée pour accéder aux postes de travail sur Internet ?
    A) Ver B) Bombe logique **C) Cheval de Troie** D) Virus
12. Quelle procédé permettant d'assurer la non-répudiation des données ?
    A) **Signature électronique** B) Certificat numérique D) Chiffrement E) Mot de passe

13. Quelle procédé permettant d'assurer l'authenticité des données ?
    A) Signature électronique **B) Certificat numérique** C) Chiffrement D) Déchiffrement
14. Un utilisateur est incapable de transférer des fichiers vers un serveur FTP. L'administrateur de sécurité a constaté que les ports sont ouverts sur le pare-feu. Lequel des éléments suivants devrait vérifier l'administrateur ?
    A) **Les listes de contrôles d'accès** B) Antivirus C) IPS D) IDS

15. Une organisation utilise le cryptage symétrique. Laquelle des énoncés suivants serait une raison valide pour migrer vers le cryptage asymétrique ?
    A) Le cryptage symétrique peut rendre l'administration des clés difficile.
    B) Le cryptage symétrique exige un algorithme relativement simple.
    C) Le cryptage symétrique fournit l'authenticité.
    D) Le cryptage symétrique est plus rapide que le cryptage asymétrique

16. Un pare-feu, ça sert à :
    A) Empêcher de pirater des fichiers sous copyright.
    B) **Interdire l'accès extérieur à un ordinateur**.
    C) Remplacer un antivirus.

17. Le flooding est :
    A) **une attaque qui sature le réseau**.
    B) la mise en place d'un sniffeur .
    C) une usurpation d'adresses IP interne venant de l'extérieur.

18. Indiquer si l'expression suivante est vraie ou fausse :

« Un risque est la capacité qu'une menace exploite une vulnérabilité dans un système »

    A) **Vrai** B) Faux

19. Une vulnérabilité/faille dans une application ou un système peut se situer au niveau :

    A) Conception B) Implémentation C) Configuration D) Utilisation

20. En l'absence d'un attaquant/attaque, pour garantir l'intégrité d'un message M envoyé entre deux extrémités

    A) Il faut générer un code d'intégrité de message en utilisant une clé partagée **K**
    B) Il suffit de générer un haché sur M en utilisant une fonction de hachage
    C) Il faut chiffrer M en utilisant une clé partagée K
    D) Aucune des réponses précédentes

21. La cryptographie est fondée sur le fait que les algorithmes utilisés (chiffrement, hachage) soient secrets

    A) Vrai **B) faux**

22. Une fonction de hachage H possède les propriétés suivantes
    A) **Résistance aux collisions** B) Réversible **C) Génère une empreinte de taille fixe** D) Il est facile de retrouver le message à partir de son haché

23. Vous avez des données, et vous voulez que personne ne puisse y avoir accès, vous avez donc besoin du service de

A) Intégrité B) Preuve C) Disponibilité D) **confidentialité**

24. Une zone DMZ est un sous réseau séparé et isolé du réseau local et d'internet par un :

A) IDS **B) Pare-feu** C) IPS D) Switch

25. Quelle technique de piratage est un exemple du vol de mots de passe réseau sans avoir recours à des programmes logiciels ?

A) Interception **B) Ingénierie sociale** C) Homme au milieu D) craquage de mots de passe

26. Le choix de mots de passe faible et la transmission de données sur des réseaux de communication non protégés est un exemple de...

A) Menace B) Mesure **C) Vulnérabilité**

27. Une technique consistant à voler des informations de la part des utilisateurs par courrier électronique,téléphone, contact direct ou un site web falsifié s'appelle

A) **Fishing** B) Homme au milieu C) Spoofing D) Spamming

28. Comment se protèger contre l'ingenierie sociale ?

A) Utiliser le chiffrement. B) Avoir un parefeu **C) Se méfier des personnes que l'on ne connaît pas**

29. Que signifie le sigle VPN ?

A. Virtual Permanent Network B. Voie Privée Numérique **C. Virtual Private Network**

30. A quoi sert un VPN (Virtual Private Network)?

A) Authentifier les entités de la communication

B) Créer un Tunnel entre deux machines via un réseau public

C) filtrer les communications

D) assurer l'intégrité des données