esprit Se former autrement	**EXAMEN** Semestre :1 ■ 2 ☐ Session : Principale ■ ☐

Module (s) : Sécurité Informatique
Enseignants : UP Réseaux
Classe(s) : 4 SAE
Documents, Calculatrice et Internet autorisés : ☐ NON ■
Nombre de questions : 40 **Nombre de pages** : 7
Date : 01/02/2021 **Heure** : 15h30 **Durée : 1h**

NB : Vous devez répondre sur la feuille réservée pour les réponses. Toute réponse sur un autre document rendu ne sera pas prise en considération

*Il s'agit d'un **QCM à réponse unique.***

1. Un logiciel malveillant se propage sans avoir besoin de se lier à d'autres programmes exécutables. De quel programme s'agit-il ?
   A. Virus
   B. Ver
   C. Espion
   D. Cheval de troie

2. Un logiciel spyware consiste à :
   A. se propager pour saturer les ressources des ordinateurs
   B. collecter des informations sensibles
   C. écouter le trafic échangé entre utilisateurs
   D. saturer la bande passante d'un réseau

3. Parmi les mesures de bonnes politiques de sécurité ?
   A. Il vaut mieux autoriser tout ce qui n'est pas explicitement interdit.
   B. Il ne faut pas multiplier les mesures de sécurité.
   C. Avoir des défenses en parallèle et non en série
   D. Attribuer les stricts privilèges nécessaires

4. Un utilisateur a payé un article acheté à partir d'un site commercial, le responsable de ce site a démenti par la suite cette transaction. Quelle service doit être assuré afin d'éviter ce type de problème ?
   A. Authentification
   B. Intégrité
   C. Non-répudiation
   D. Disponibilité

5. Une attaque qui tente d'apprendre ou d'utiliser l'information du système, mais n'affecte pas les ressources du système est une attaque :
   A. interne
   B. externe
   C. active
   D. passive

6. Quelle proposition, parmi les suivantes, correspond au bon ordre des étapes d'une attaque informatique :

A. Collecte d'informations, balayage des ports, repérage des failles, intrusion, extension des privilèges, effacement des traces.

B. Porte dérobée, intrusion, collecte d'informations, balayage des ports, extension des privilèges, effacement des traces.

C. Intrusion, collecte d'informations, balayage des ports, extension des privilèges, effacement des traces.

D. Cheval de Troie, collecte d'informations, balayage des ports, extension des privilèges, effacement des traces.

7. Le principe d'une attaque "Ping flooding" consiste à :

A. Envoyer un paquet IP qui a une longueur de données supérieure à la taille maximale
B. Saturer le trafic réseau en envoyant un grand nombre de paquets IP
C. Envoyer un paquet IP non fragmenté
D. Modifier l'entête des paquets ICMP de la machine victime.

8. Pour empêcher l'établissement de connexions TCP, un attaquant envoie un grand nombre de paquets TCP-SYN avec une adresse source usurpée et inaccessible, il s'agit de l'attaque :

A. TCP-SYN flooding
B. TCP-SYN spoofing
C. TCP-SYN sniffing
D. Ping-pong

9. Le Social Engineering est :

A. l'action qui consiste à verrouiller le disque dur avec un mot de passe
B. l'influence interpersonnelle afin d'obtenir des informations sensibles en matière de sécurité
C. un logiciel malveillant nommé d'après ses inventeurs qui sont d'anciens ingénieurs
D. un logiciel malveillant qui se propage par l'intermédiaire des réseaux sociaux

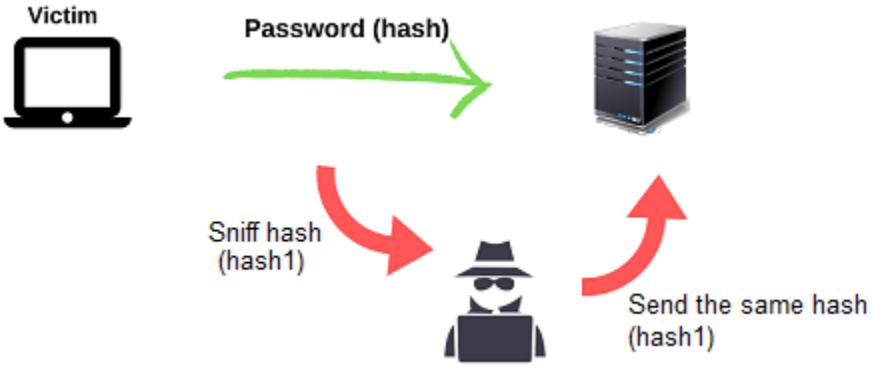
10. La Brute-force attack consiste à

A. modifier un texte chiffré
B. déduire un texte clair à partir un texte chiffré
C. découvrir l'algorithme de chiffrement
D. saisir un mot de passe compliqué

11. Quelle attaque peut affecter l'intégrité des données ?

A. Bombarder le réseau par du trafic inutile
B. Utiliser les informations d'identification d'un autre utilisateur
C. Intercepter et modifier une transaction électronique
D. Décrypter les données

12. Soit la figure suivante, il de quelle attaque s'agit-il?



A. Attaque syn flooding
B. Attaque de rejeu
C. Attaque de Spoofing
D. Attaque de buffer overflow

13. Un administrateur réseau a remarqué qu'il existe plusieurs sessions semi-ouvertes sur un serveur Web. De quelle attaque s'agit-elle ?
A. Attaque arp spoofing
B. Attaque de sniffing
C. Attaque de syn flooding
D. Attaque de modification

14. Un système cryptographique à clé secrète est un système qui :
A. partage la même clé pour le chiffrement et le déchiffrement
B. assure l'utilisation de deux clés différentes
C. assure la signature numérique d'un document
D. assure la disponibilité des services

15. Les fonctions de hachage permettent d'assurer :
A. la confidentialité
B. la disponibilité
C. l'intégrité
D. non répudiation

16. Parmi les suivantes, quelle est l'affirmation correcte :
A. RSA est un algorithme de hachage
B. SHA1 est un algorithme de hachage
C. DH est un algorithme de cryptage à clé secrète
D. AES est un algorithme de cryptage à clé publique

17. À quoi sert un service de non-répudiation dans les communications sécurisées ?
A. Pour garantir que les communications sécurisées cryptées ne peuvent pas être décodées.
B. Pour confirmer l'identité du destinataire des communications.
C. Pour fournir le niveau de cryptage le plus élevé possible.
D. Pour s'assurer que la source des communications est confirmée.

18. Quelle est l'utilisation la plus courante de l'algorithme Diffie-Hellman dans la sécurité des communications ?

A. Pour créer des hachages de mot de passe pour une authentification sécurisée.
B. Pour sécuriser l'échange des clés utilisées pour crypter les données.
C. Pour fournir une authentification de protocole de routage entre les routeurs.
D. Pour crypter les données pour des communications e-commerce sécurisées.

19. Quel algorithme de chiffrement est un algorithme asymétrique ?

A. Diffie-Hellman
B. SEAL
C. 3DES
D. AES

20. Quelle déclaration décrit les algorithmes de cryptage asymétrique ?

A. Ils ont des longueurs de clé allant de 80 à 256 bits.
B. Ils incluent DES, 3DES et AES.
C. Ils sont également appelés algorithmes à clé secrète partagée.
D. Ils sont relativement lents car basés sur des algorithmes de calcul difficiles.

21. À quoi sert un certificat numérique ?

A. Il garantit qu'un site Web n'a pas été piraté.
B. Il authentifie un site Internet et établit une connexion sécurisée pour échanger des données confidentielles.
C. Il fournit la preuve que les données ont une signature traditionnelle attachée.
D. Il garantit que la personne qui accède à un périphérique réseau est autorisée.

22. Quel algorithme de cryptographie peut garantir la confidentialité des données ?

A. MD5
B. AES
C. PKI
D. RSA

23. Pourquoi la gestion des clés par algorithme asymétrique est-elle plus simple que la gestion des clés par algorithme symétrique ?

A. Il utilise moins de bits.
B. Une seule clé est utilisée.
C. Deux clés publiques sont utilisées pour l'échange de clés.
D. L'une des clés peut être rendue publique.

24. Parmi les suivantes, quelle est la proposition vraie ?

A. Un firewall est un équipement qui comporte une seule interface
B. Un firewall est toujours une solution software
C. Un firewall comporte au minimum deux interfaces
D. Un firewall permet de détecter les logiciels malveillants

25. Selon la capture suivante, les machines appartenant au réseau Local Area Network ne doivent pas accéder au site web www.youtube.com et peuvent accéder au site web www.google.com, pour cela l'administrateur réseau doit mettre en place un firewall de type :

A. Packet Filter
B. Proxy Filter
C. Application Filter
D. Stateful inspection

26. Un firewall de génération « Packet Filter » assure le filtrage des :
A. Adresses IP sources et destinations
B. Applications clientes
C. Protocoles applicatifs
D. Sites web

27. Afin d'assurer une fonctionnalité de détection des nouvelles attaques « Zero day attacks », l'administrateur réseau doit mettre en place :
A. Signature based IDS
B. Anomaly based IDS
C. IPS
D. Firewall stateful inspection

28. Selon la table de filtrage suivante, quelle est l'affirmation vraie ?

N	Action	Source IP address	Destination IP address	Src port number	Dest port number
1	Permit	192.168.1.0/24	172.16.1.2	>1023	80
2	Permit	192.168.1.5	any	>1023	25
3	Deny	Any	Any	Any	Any
4	Permit	192.168.1.10	172.16.1.5	Any	443

A. La machine 192.168.1.93 peut accéder à un service web en mode sécurisé (HTTPS)
B. La machine 192.168.1.5 peut accéder au serveur de messagerie électronique ayant l'adresse IP 172.16.1.10
C. La machine 192.168.1.10 peut accéder à un service web en mode sécurisé (HTTPS)
D. La machine 192.168.1.10 peut accéder à un service de messagerie électronique ayant l'adresse IP 172.16.1.5

29. Pour un IDS, avec un taux élevé de faux-positifs est signe que :
    A. La configuration de l'IDS est trop permissive
    B. La configuration de l'IDS est trop restrictive
    C. Que la base des signatures n'est pas à jour
    D. Aucune de ces propositions

30. Quelle est la caractéristique commune aux IDS et aux IPS
    A. Les deux se basent sur des capteurs pour collecter les données.
    B. Les deux assurent une sécurité active
    C. Les deux permettent uniquement la détection des intrusions
    D. Les deux bloquent les attaques détectées.

31. Pour un NIDS, placer une sonde dans le LAN d'une entreprise permet de :
    A. Mettre en place un honey-pot
    B. Détecter toutes les attaques même celles qui vont être bloquée par le firewall
    C. N'a aucune utilité.
    D. Délecter les attaques internes.

32. Une organisation a configuré une solution IPS pour utiliser des alertes automatiques. Quel type de réponse se produira lorsqu'une signature est détectée ?
    A. Un compteur démarre et une alerte récapitulative est émise lorsque le décompte atteint un nombre préconfiguré.
    B. La connexion TCP est réinitialisée.
    C. Une alerte est déclenchée chaque fois qu'une signature est détectée.
    D. L'interface qui a déclenché l'alerte a été désactivée.

33. A quels besoins parmi les suivants, un VPN pourrait-il répondre ?
    A. Une entreprise dont les activités sont réparties sur plusieurs sites géographiques qui ont besoin de pouvoir communiquer entre eux.
    B. Une entreprise qui envoie quotidiennement des ordres de virement aux banques partenaires
    C. Une entreprise qui a des commerciaux itinérants qui ont besoin de se connecter ponctuellement à distance aux services de leur entreprise
    D. Réponses A et C à la fois

34. Quels sont les objectifs de sécurité qui sont réalisés en mettant en place un VPN se basant sur le protocole ESP ?
    A. Intégrité, authenticité, anti-rejeu et disponibilité
    B. Intégrité, authenticité, anti-rejeu et confidentialité
    C. Intégrité, authenticité et anti-rejeu
    D. Authenticité, anti-rejeu et confidentialité

35. Dans le cas où IPsec est utilisé pour fournir de la sécurité de bout en bout entre une machine hôte et une autre machine hôte. Quel est le mode utilisé ?
    A. Mode concentrateur
    B. Mode tunnel
    C. Mode filtrage
    D. Mode transport

36. Quel est le protocole utilisé pour pouvoir établir dynamiquement des associations de sécurité dans les VPN basés sur IPsec :

A. Le protocole AH
B. Le protocole ESP
C. Le protocole PPP
D. Le protocole IKE

37. Parmi les assertions suivantes, quelle est celle qui décrit IPsec :

A. C'est une suite de protocoles qui fournit des services de sécurité au niveau de la couche IP du modèle TCP-IP
B. C'est un protocole basé sur PPP pour se connecter à un fournisseur d'accès internet en utilisant une ligne téléphonique standard
C. C'est un protocole de sécurisation développé par Netscape de niveau 5 Renommé en TLS suite au rachat du brevet
D. C'est un protocole utilisé pour prendre la main sur un shell distant.

38. Le stockage des différentes Security Associations afin de connaitre les traitements à faire pour les packets entrants et sortants se fait au niveau de :

A. La security association policy
B. La security association database
C. La security policy database
D. Aucune de ces propositions

39. Quelles sont les deux techniques qui sont utilisées pour la création des tunnels VPN ?

A. La cryptographie et la segmentation
B. La signature numérique et l'encapsulation
C. La virtualisation et la cryptographie
D. L'encapsulation et la cryptographie

40. On se propose de sécuriser la communication entre le siège d'une banque et une agence avec le protocole IPsec. L'objectif est de cacher les communications, s'assurer qu'elles ne soient pas modifiées et de l'identité des émetteurs/récepteurs. Laquelle de ces propositions est la plus adaptée :

A. ESP en mode transport
B. AH en mode transport
C. ESP en mode tunnel
D. AH en mode tunnel