555F

AVIS IMPORTANT AUX ETUDIANTS

1. Chacune des feuilles de votre copie doit comporter une étiquette code à barres placée à l'endroit indiqué «coller ici votre code à barres».
2. Une copie d'examen comporte une seule «feuille principale» et des «feuilles suites». Sur chacune de vos feuilles, le code à barres est obligatoire.
3. Cette feuille d'examen est strictement personnelle. Elle ne doit comporter aucun signe distinctif. Elle doit être écrite en noir et/ou bleu.
4. Le non respect de l'une de ces recommandations peut faire attribuer la note ZERO à l'épreuve.

esprit Se former autrement
HONORIS UNITED UNIVERSITIES

NOTE

Coller ici votre code à barre

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20

00	25	50	75

Module : Sécurité Informatique	Documents autorisés : OUI ☐ NON ■
Enseignant(s) : Enseignants du module SI	Calculatrice autorisée : OUI ☐ NON ■
Classe(s) : 4ème années	Internet autorisée : OUI ☐ NON ■
Session: Principale	Nombre de page : 06
Date : 29 Oct 2024 Heure: 13h00	Durée : 1h30

QCM/QCU - Cocher la ou les bonne(s) réponse(s) (3,5 pts)

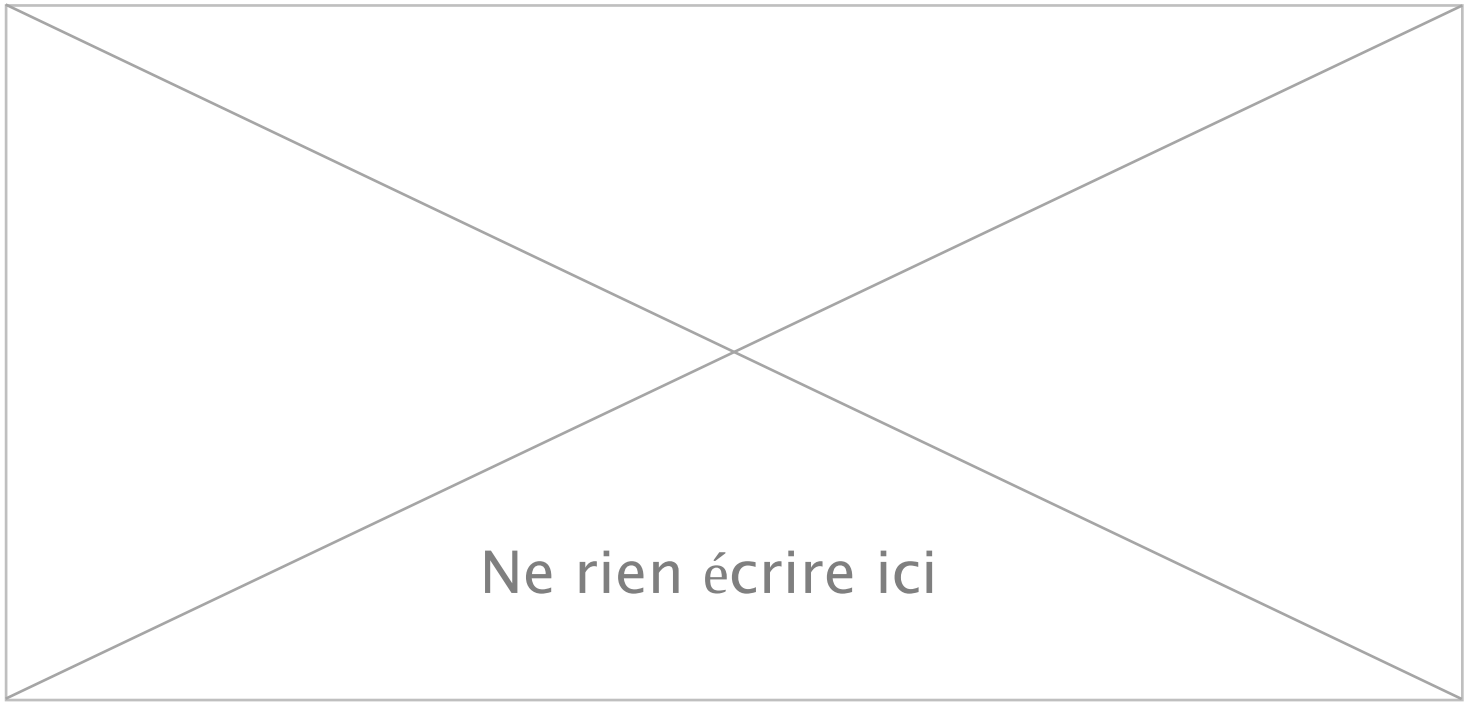
Q1- Quelle déclaration décrit les réseaux VPN?

- ❑ A- Les VPN utilisent un logiciel de virtualisation open source pour créer le tunnel via Internet.
- ❑ B- Les VPN utilisent des connexions virtuelles pour créer un réseau privé via un réseau public.
- ❑ C- Les VPN utilisent des connexions physiques dédiées pour transférer les données.
- ❑ D- Les VPN utilisent des connexions logiques pour créer des réseaux publics via Internet.

Q2- Que pourront faire les utilisateurs du LAN selon le tableau suivant :

Règle	IP source	Port source	IP destination	Port destination	Protocole
Accept	DMZ network	*	LAN network	22	TCP
Drop	*	*	*	*	*

V1



- ❑ A- Les utilisateurs du réseau LAN pourront se connecter au réseau DMZ via SSH. C'est la seule opération qu'ils pourront effectuer.
- ❑ B- Les utilisateurs du réseau LAN pourront se connecter au réseau DMZ uniquement via SSH mais faire ce qu'ils veulent sur les autres réseaux.
- ❑ C- Les utilisateurs du LAN pourront communiquer entre eux et rien d'autre
- ❑ D- Rien

Q3- Quelle est l'assertion correcte à propos d'un certificat numérique ?

- ❑ A- Le certificat contient la paire de clés de son possesseur
- ❑ B- Le certificat contient la clé publique de son possesseur
- ❑ C- La même clé privée peut-être associée à plusieurs certificats générés par la même autorité.
- ❑ D- Deux certificats peuvent contenir la même clé publique

Q4- Quelle est la déclaration qui caractérise les attaques DoS ?

- ❑ A- Elles tentent de compromettre la disponibilité d'un réseau, d'un hôte ou d'une application.
- ❑ B- Elles sont difficiles à conduire et ne sont initiées que par des attaquants très qualifiés.
- ❑ C- Elles sont généralement lancées avec un outil appelé L0phtCrack.
- ❑ D- Elles précèdent toujours les attaques d'accès.

Q5- Un firewall est utilisé pour :

- ❑ A- Restreindre l'accès à un réseau à partir d'un autre réseau
- ❑ B- Protéger le système des attaques internes
- ❑ C- Prévenir contre les attaques de social engineering
- ❑ D- Remplacer un antivirus ou un antimalwares

Q6- 25 personnes désirent utiliser un algorithme de chiffrement symétrique pour pouvoir communiquer d'une façon confidentielle. Combien de clés symétriques doit-on avoir :

- ❑ A- 625
- ❑ B- 600
- ❑ C- 313
- ❑ D- 300

Q7- Pour assurer l'intégrité, l'authentification et la non-répudiation de l'émetteur durant une communication entre 2 stations A et B, laquelle de ces propositions faut-il utiliser :

- ❑ La signature numérique avec les algorithmes 3DES et SHA1
- ❑ Le hachage et le chiffrement symétrique avec MD5 et RSA
- ❑ La signature numérique avec les algorithmes SHA et RSA
- ❑ La signature numérique avec les algorithmes DES et MD5

Exercice 1 (3,5 pts)

1- Remplir le tableau suivant pour expliquer brièvement chaque objectif de sécurité (DIC), donner un exemple de vulnérabilité et de contremesure correspondants (2,25 pt)

Critère	Disponibilité	Intégrité	Confidentialité
Explication	**Assure que** …….. ……..…….. ……..……..	**Assure que** …….. ……..…….. ……..……..	**Assure que** …….. ……..…….. ……..……..
Vulnérabilité associée			
Contremesure associée			

2- Expliquer chacune de ces règles de base de la sécurité informatique en donnant un exemple concret de son application dans la sécurité des systèmes d'informations (1 pt)

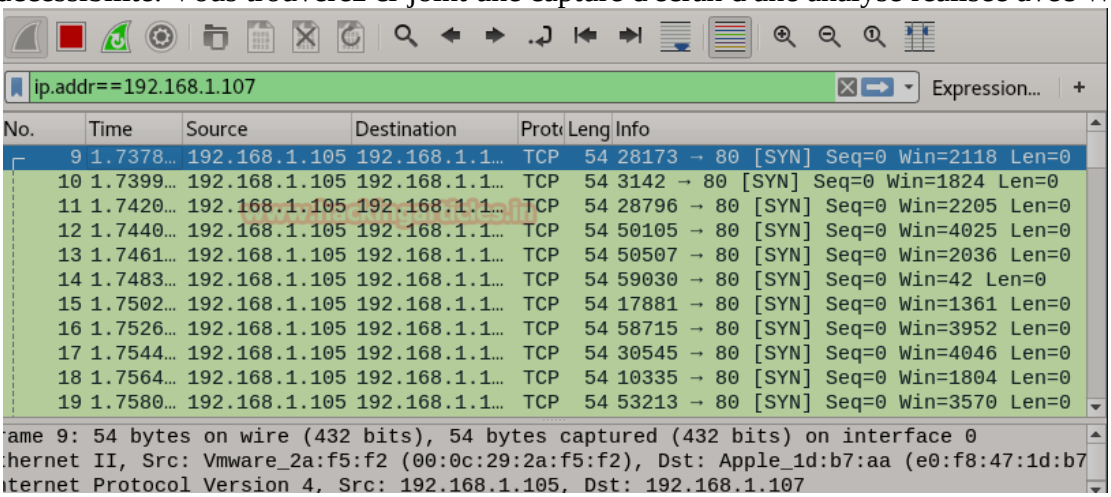
Règle de base	Interdiction par défaut	Défense en profondeur
Explication		
Exemple d'application		

3- **Quelle est la différence entre une contremesure préventive et une contremesure corrective ? (0,25 pt)**

……..

Exercice 2 : (3 pt)

L'équipe de sécurité a détecté une anomalie sur un serveur de l'entreprise, provoquant des ralentissements et des périodes d'inaccessibilité. Vous trouverez ci-joint une capture d'écran d'une analyse réalisée avec Wireshark.



1. **De quelle attaque s'agit-il ? Expliquer son scénario de réalisation (0,5 pt)**

   ……

2. **Proposer une solution technique pour atténuer cette attaque. (0,5 pt)**

……

3. **Indiquer si l'attaque est active ou passive, et justifier votre réponse. (0,5 pt)**

……

Alors que l'équipe tentait de résoudre ce problème, le serveur web public de l'entreprise est devenu inaccessible. L'analyse révèle un flux massif de requêtes provenant de multiples adresses IP

4. **Nommer cette attaque et expliquer brièvement son mécanisme (0,5 pt)**

   ……

Après avoir examiné la situation, l'équipe découvre qu'une attaque ARP Spoofing a redirigé le trafic des utilisateurs internes vers la machine de l'attaquant.

5. **L'attaquant est-il nécessairement sur le même réseau local que la victime ? Justifier votre réponse. (0,75 pt)**

   ……

Après enquête, il est révélé que l'attaquant est un ancien employé mécontent.

6. **Comment classeriez-vous cet attaquant parmi les types de hackers ? (0,25 pt)**

   ……

Exercice 3 (4 pts)

Soit A et B deux entités désirant échanger des messages chiffrés en utilisant l'algorithme RSA.

1. **Pour assurer la confidentialité des messages échangés entre A et B, quelle clé doit être utilisée par B pour envoyer un message chiffré à A ? Justifier. (0,75 pts)**

……
……

2. **Quel serait l'avantage et l'inconvénient d'utiliser DES à la place de RSA ? Justifier. (0,5 pt)**

……
……

SUITE

Coller ici votre
code à barre

3. **A et B souhaitent également s'assurer de l'intégrité des messages échangés. Proposer une solution. Justifier. (0,75 pt)**

……
……

4. **A souhaite signer numériquement un message avant de l'envoyer à B afin que B puisse vérifier l'identité de A. Quelles sont les clés utilisées ? (1 pt)**

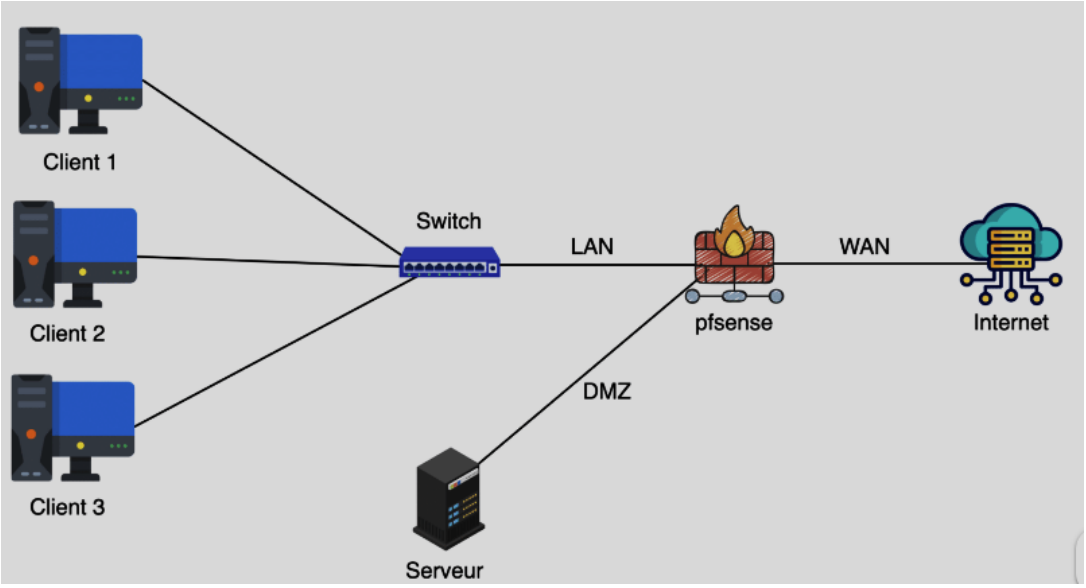
……
……

5. **A et B utilisent des certificats numériques pour garantir l'authenticité de leurs clés publiques. Comment B peut-il s'assurer que le certificat numérique de A est valide avant de lui envoyer un message chiffré ? (1 pt)**

……
……

Exercice 4 (6 pts)

Soit l'infrastructure réseau d'une entreprise donnée dans la figure ci-dessous :



1- **Pourquoi est-il important de segmenter un réseau d'entreprise en différentes zones ? (1pt)**

……
……

2- **Parmi ces zones, laquelle représente un point de vulnérabilité, et pourquoi ? (1 pt)**

……

3- **Quel est le rôle du pare-feu pfsense dans cette architecture ? (0.5 pt)**

……

4- **Comment le pare-feu traite-t-il une requête HTTP provenant du WAN et destinée au serveur de la zone DMZ ? (1pt)**

……

5- **Proposez un autre mécanisme de sécurité pour renforcer la sécurité de la zone DMZ. (0.5 pt)**

……

6- Proposez un autre mécanisme de sécurité pour renforcer la sécurité de la zone DMZ. (0.5 pt)

…….

7- L'entreprise décide de mettre en place un VPN pour permettre à ses employés travailler en mobilité de manière sécurisée (en utilisant leurs PCs portables)

a. Quel type de VPN serait le plus adapté dans ce cas, et pourquoi ? (1pt)

…….

b. Comment le VPN garantit-il des communications sécurisées entre les employés distants et le réseau interne de l'entreprise ? (1pt)

…….