Évaluations de fin de modules Régionales
Semestre : S2 & Étalé
Année de formation : 2023-2024

Éléments de correction					
Secteur	:	Digital et Intelligence Artificielle	**Niveau**	:	Technicien Spécialisé
Filière	:	Infrastructure Digitale option Systèmes et Réseaux	**Année**	:	2 A
Module : M206 - Sécurité d'une infrastructure digitale					

Théorie : (20 Points)

1- Qu'est-ce que la confidentialité des données dans le contexte de la sécurité informatique ?(2PTS)
a) La garantie que les données sont accessibles uniquement par des personnes autorisées.
b) La vitesse à laquelle les données peuvent être traitées.
c) La mesure dans laquelle les données sont disponibles en cas de besoin.
d) La capacité à détecter et à réagir aux menaces de sécurité.

2- Quel est l'objectif principal d'une ACL dans un réseau informatique ? (2PTS)
a) Contrôler l'accès aux ressources réseau.
b) Accélérer le transfert de données sur le réseau.
c) Améliorer la qualité de service (QoS).
d) Identifier les menaces de sécurité.

3- Quel est l'avantage principal d'utiliser un VPN ? (2PTS)
a) Améliorer la vitesse de connexion.
b) Accéder à des ressources réseau de manière sécurisée via Internet.
c) Réduire la latence du réseau.
d) Fournir une meilleure qualité de service (QoS)

4- Quel est le principal objectif du chiffrement dans le contexte de la sécurité des données ? (2PTS)
a) Assurer l'intégrité des données.
b) Protéger les données contre les accès non autorisés.
c) Améliorer la vitesse de transfert des données.
d) Identifier les failles de sécurité dans un système.

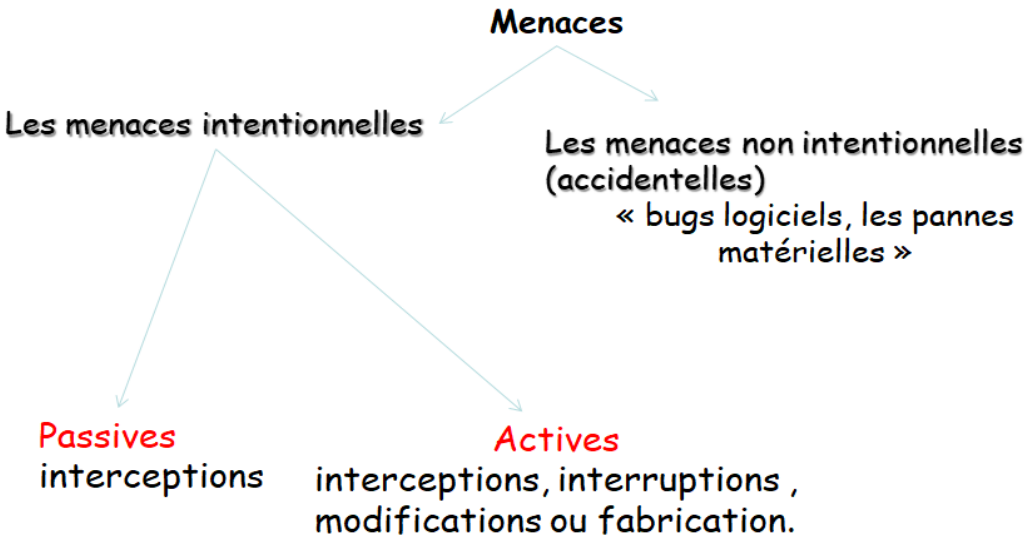
5- Quelle est la différence entre le chiffrement symétrique et le chiffrement asymétrique ? (2PTS)
a) Le chiffrement symétrique utilise une seule clé pour le chiffrement et le déchiffrement, tandis que le chiffrement asymétrique utilise deux clés distinctes.
b) Le chiffrement symétrique est plus sécurisé que le chiffrement asymétrique.
c) Le chiffrement asymétrique est plus rapide que le chiffrement symétrique.

Barème : /40

d) Le chiffrement symétrique est utilisé uniquement pour les communications en ligne, tandis que le chiffrement asymétrique est utilisé pour le stockage des données.

6- Qu'est-ce qu'une vulnérabilité en sécurité informatique ? (2PTS)
Une vulnérabilité est une faiblesse dans un système informatique qui peut être exploitée par un attaquant pour y pénétrer ou y causer des dommages.

7- Quels sont les différents types de menaces informatiques ? (2PTS)



8- Citer les objectifs de la sécurité informatique (2PTS)
La sécurité d'un système informatique à pour mission la protection des informations contre divulgation (CONFIDENTIALITE) , altération (INTEGRITE) ou destruction(DISPONIBILTE Qu'est-ce qu'une attaque de phishing et comment peut-on s'en protéger ? (2PTS)

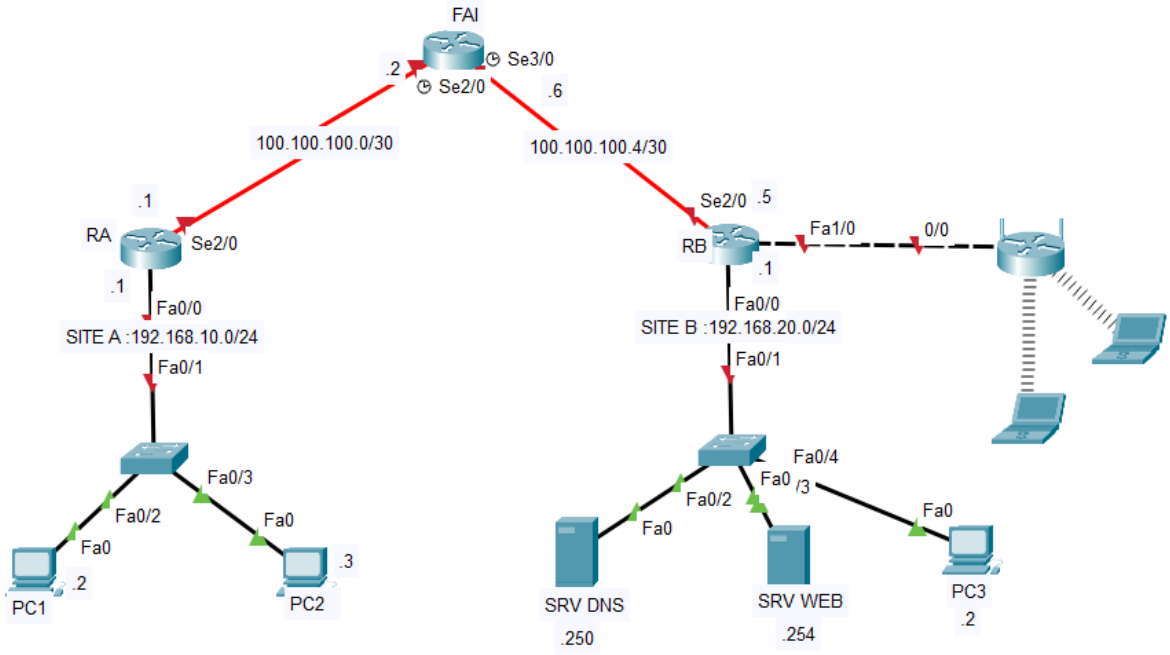
9- Qu'est-ce qu'un système de détection d'intrusion ? et quels sont les types des IDS ? (2PTS)

Un système de détection d'intrusion (IDS) est un outil de sécurité qui surveille les activités réseau et système afin de détecter les comportements malveillants et les attaques potentielles.

10 - Il existe deux principaux types de systèmes de détection d'intrusion : les IDS réseau et les IDS système. Les IDS réseau surveillent le trafic réseau pour détecter les activités suspectes, tandis que les IDS système surveillent les activités du système pour détecter les comportements malveillants

Pratique : (20 Points)

Soit le réseau suivant représentant l'interconnexion entre deux sites d'une société



1. Créer une **ACL IPv4** nommé « ***FilterAtoB*** » qui permet d'assurer les besoins suivants : (2PTS)

- autoriser le trafic ***HTTP du site A*** vers le serveur« ***SRVWEB***»,
- autoriser le trafic ***DNS du site A*** vers le serveur «***SRVDNS***»,
- refuser tout le trafic ***IP*** depuis le réseau 192.168.10.0 vers le RESEAU 192.168.20.0

AUTORISER TOUT AUTRE TRAFIC

RA(config)#ip access-list extended ***FilterAtoB***

RA(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 HOST 192.168.20.254 eq 80

RA(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 HOST 192.168.20.250 eq 53 (domain)

RA(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255

RA(config-ext-nacl)#permit ip any any

2. Activer cette ACL sur ***L'interface convenable*** (1PT)

RA(config)#interface fa0/0
RA(config-if)#ip access-group ***FilterAtoB in***

3. L'administrateur veut séparer le réseau des serveurs et le réseau des machines sur le site B sans introduire de nouveau matériel, quelle est la solution que vous proposez ? (1PT)

Les vlans

4. Donner des exemples d'attaques ciblant le réseau sans fil (2PTS)

L'attaque de l'homme du milieu : Cette attaque consiste à intercepter les communications sans fil entre un utilisateur et un point d'accès, puis à les modifier ou à les retransmettre à l'utilisateur.

Cette technique est souvent utilisée pour espionner les données sensibles telles que les identifiants et les mots de passe.

L'attaque de déni de service (DoS) : Cette attaque consiste à envoyer une grande quantité de trafic au réseau sans fil pour le rendre indisponible..

L'attaque par usurpation d'adresse MAC : Cette attaque consiste à modifier l'adresse MAC d'un périphérique pour qu'il apparaisse comme un autre périphérique autorisé sur le réseau sans fil. Cela permet à l'attaquant d'accéder au réseau sans fil en utilisant l'identité d'un autre utilisateur.

5. L'administrateur réseau veut assurer une meilleure protection de son réseau sans fil, quelles sont les directives qu'il doit suivre et les paramètres qu'il doit configurer sur le routeur sans fil (2PTS)

Utiliser le chiffrement WPA2 :
Configurer un mot de passe fort : L'administrateur réseau doit s'assurer que le mot de passe est assez long et complexe et qu'il est régulièrement changé.

Désactiver le SSID broadcast : Les utilisateurs autorisés devront alors connaître le nom du réseau et le saisir manuellement pour se connecter.

Utiliser des adresses IP statiques : L'utilisation d'adresses IP statiques peut empêcher les attaquants d'utiliser des adresses IP frauduleuses pour accéder au réseau sans fil.

Dans cette partie, l'administrateur a décidé d'adopter une solution VPN pour sécuriser la communication entre les deux sites
Dans cette partie, l'administrateur a décidé d'adopter une solution VPN pour sécuriser la communication entre les deux sites

6. Comment fonctionne un VPN ? (1PT)

Lorsque vous utilisez un VPN, tout votre trafic Internet est crypté et acheminé via le serveur VPN, ce qui rend votre adresse IP et votre emplacement réels invisibles aux sites que vous visitez.

L'administrateur a choisi de configurer tunnel VPN IPsec entre les sites A et B

7. Donner la configuration de VPN IPSEC sur le routeur RA en suivant les instructions suivantes :

7.1. Configurer le protocole 'ISAKMP' qui gère l'échange des clés en respectant les paramètres suivants (3PTS)

- L'algorithme de cryptage AES
- Authentification par clé pré-partagées
- Algorithme de hachage SHA (valeur par défaut)
- Groupe Diffie-Hellman 2
- Durée de vie 86400 secondes (valeur par défaut)

```
RA(config)#crypto isakmp policy 10          → active une politique IKE RA(config-
isakmp)# encryption aes                     → fixe l'algorithme de cryptage
RA(config-isakmp)# authentication pre-share → fixe la méthode d'authentification
RA(config-isakmp)# hash sha                 → fixe l'algorithme de hachage
RA(config-isakmp)# group 2                  → définit le groupe Diffie Hellman
RA(config-isakmp)# lifetime 86400           → fixe la durée de vie de la SA
RA(config-isakmp)#exit
```

7.2. Créer la méthode de cryptage (transform-set) nommé VPNSETV1, avec "esp- aes" comme méthode de cryptage et "esp-sha-hmac" comme méthode d'authentification. (2PsTS)

RA(config)#crypto ipsec transform-set VPNSETV1 esp-aes esp-sha-hmac

7.3. Créer une liste de contrôle d'accés nommée VPNLIST, servant à identifier le trafic à traiter par le tunnel VPN. Pour RA, ce sera le trafic d'origine 192.168.10.0 à destination de 192.168.20.0 (2PTS)

RA(config)#ip access-list extended VPNLIST
RA(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
RA(config-ext-nacl)#exit

7.4. Configurer une carte de cryptage (crypto-map) nommée VPNMAP1, servant à spécifier le pair distant, le 'transform set' et l'access list. (2PTS)

RA(config)#crypto map VPNMAP1 10 ipsec-isakmp RA(config-crypto-map)# match address VPNLIST
RA(config-crypto-map)#set peer 100.100.100.5
RA(config-crypto-map)#set transform-set VPNSETV1 RA(config-crypto-map)#exit

7.5. Appliquer la crypto-map à l'interface WAN de Routeur RA (2PTS)

RA(config)# interface serial 2/0
RA(config-if)#crypto map VPNMAP1