Direction Régionale RABAT-SALÉ-KENITRA

Examen régional de fin de module

Année de Formation 2022/2023

Code module : M206
Intitulé du module : SÉCURITÉ D'UNE INFRASTRUCTURE DIGITALE

Filière	:	**IDOSR**	Durée	**: 2h**
Année	:	**2 ° A**	Note finale	: **/ 40**
Nom&Prénom du correcteur			Émargement	

Théorie: (20 points)

1- Donner cinq objectifs (ou critères) de la sécurité informatique ? ---------- (2pts)

L'intégrité des données - La confidentialité des données - La disponibilité des données - La non-répudiation des informations - L'authenticité des identifiants

2- Qu'est-ce qu'un Certificat numérique ?---------- (2pts)

Un certificat numérique (ou certificat de clé publique) peut être vu comme une carte d'identité numérique. Il est utilisé principalement pour identifier et authentifier une personne physique ou morale, mais aussi pour chiffrer des échanges

3- Donner les principales informations de la Structure d'un Certificat numérique selon la norme X509 ? (2pts)

Version : indique à quelle version de X509 correspond ce certificat
Numéro de série : Numéro de série du certificat
Algorithme de signature : identifiant du type de signature utilisée
Emetteur : Distinguished Name (DN) de l'autorité de certification qui a émis ce certificat.
Valide à partir de : la date de début de validité de certificat
Valide jusqu'à : la date de fin de validité de certificat

4- A quels niveaux du modèle OSI fonctionne un firewall stateless ?---------- (2pts)

- 2 et 3
- 3 et 4
- 4 et 5

3 et 4

5- Quelles attaques sont considérées comme des dénis de service ? ---------- (2pts)

a. Le spoofing
b. Le flooding
c. Le phishing

Le flooding

6- Le ‘’social engineering’’ consiste le plus souvent à : ---------- (2pts)
   a. Inonder une machine cible d'applications inutiles
   b. Récupérer les informations confidentielles pour pénétrer dans un réseau
   c. Installer un programme caché dans un autre programme

Récupérer les informations confidentielles pour pénétrer dans un réseau

7- Le but du DNS spoofing est : ---------- (2pts)
   a. De falsifier l'adresse IP d'un utilisateur
   b. De rediriger un utilisateur vers un site falsifié
   c. De falsifier un serveur DNS

De falsifier un serveur DNS

8- Dans une attaque de type DDOS---------- (2pts)
   a. La machine maître contrôle d'autres machines qui pourront réaliser une attaque distribuée sur la cible
   b. La machine attaquante inonde des machines cible à l'aide d’applications distribuées
   c. L'objectif est de paralyser la machine cible

La machine maître contrôle d'autres machines qui pourront réaliser une attaque distribuée sur la

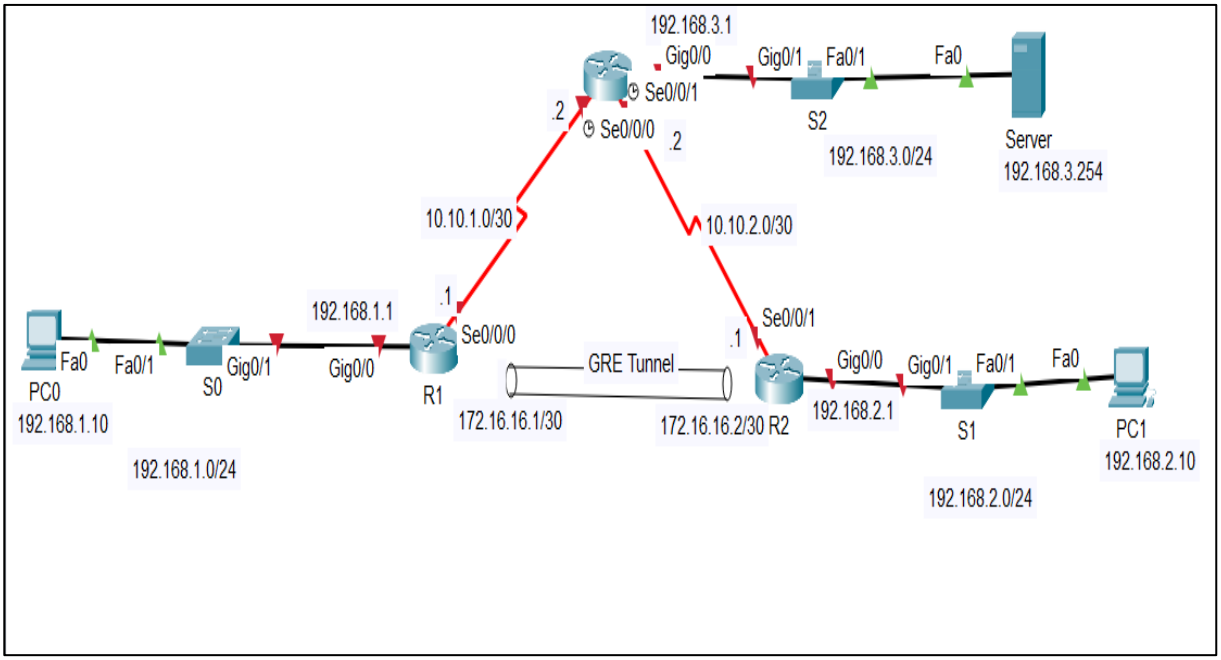
9- Pour chaque attaque quelle est sa description correspondante : ---------- (4pts)

Attaque	**La description**
Usurpation d’adresse	L’attaquant peut surveiller, capturer et contrôler activement la communication de manière transparente.
Déni de service	L’attaquant tente de convaincre les gens de divulguer des informations sensibles.
Homme du milieu	L’attaque se produit lorsqu'un acteur malveillant construit un paquet IP qui semble provenir d'une adresse valide.
Par Hameçonnage	L’attaque peut inonder un ordinateur ou l'ensemble du réseau de trafic jusqu'à ce qu'un arrêt se produise en raison de la surcharge.

Usurpation d’adresse : L’attaque se produit lorsqu'un acteur malveillant construit un paquet IP qui semble provenir d'une adresse valide.
Déni de service : L’attaque peut inonder un ordinateur ou l'ensemble du réseau de trafic jusqu'à ce qu'un arrêt se produise en raison de la surcharge.
Homme du milieu : L’attaquant peut surveiller, capturer et contrôler activement la communication de manière transparente.
Par Hameçonnage : L’attaquant tente de convaincre les gens de divulguer des informations sensibles.

Pratique : (20 points)

Soit la topologie suivante :



a. Configurez l'interface de tunnel sur le routeur R1. Utilisez 10.10.1.1 sur le routeur R1 en tant qu'interface source de tunnel et 10.10.2.1 en tant que destination de tunnel sur le routeur R2. ---------- (4pts)

```
R1(config)# interface tunnel 0
R1(config-if)# ip address 172.16.16.1 255.255.255.252
R1(config-if)# tunnel source s0/0/0
R1(config-if)# tunnel destination 10.10.2.1
R1(config-if)# tunnel mode gre ip
```

b. Configurez l'interface de tunnel sur le routeur R2. Utilisez 10.10.2.1 sur le routeur R2 en tant qu'interface source de tunnel et 10.10.1.1 en tant que destination de tunnel sur le routeur R1.---------- (4pts)

```
R2(config)# interface tunnel 0
R2(config-if)# ip address 172.16.16.2 255.255.255.252
R2(config-if)# tunnel source 10.10.2.1
R2(config-if)# tunnel destination 10.10.1.1
R2(config-if)# tunnel mode gre ip
```

C. Vérifiez l'état de l'interface de tunnel sur les routeurs R1 et R2. ---------- (2pts)

```
R1# show ip interface brief
R2# show ip interface brief
```

D. Créer une ACL étendue 101, qui permet de :---------- (4pts)

- Refuser des paquets IP à destination de la machine serveur et provenant du réseau 192.168.1.0/24
- Refuser les paquets TCP à destination du port 443 de la machine serveur
- Autoriser les machines du réseau 192.168.2.0/24 d'envoyer des requêtes ping vers le serveur.

```
R1(config)#access-list 101 deny ip 192.168.1.0 0.0.0.255 host 192.168.3.254
R1(config)#access-list 101deny tcp any host 192.168.3.254 https
R1(config)#access-list 101 permit icmp 192.168.2.0 0.0.0.255 host 192.168.3.254
```

E. Sur quels routeurs se placent les ACLs étendues d'une manière générale. ---------- (2pts)

Les ACLs étendues se placent généralement sur les routeurs les proches à la source.

E. Appliquer votre ACL sur l'interface convenable. ---------- (2pts)

```
R1(config)#interface G0/0/0
R1(config-if)#ip access-group 101 out
```

F. Vérifier l'ACL crée. ---------- (2pts)

```
R1#show access-lists
```