Direction Régionale RABAT-SALÉ-KENITRA

Examen régional de fin de module

Année de Formation 2022/2023

Nom : .....

Prénom : .....

Groupe : .....

Etablissement : .....

Réservé à l'établissement Code : .....

OFPPT - DR RBK
Evaluations De Fin De Module Régionales
Service Contrôle Qualité

Code Module : M206

Intitulé module : Sécurité d'une infrastrcutre digitale

Filière	:	Infrastructure Digitale option Systèmes et Réseaux	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)

.....

.....

.....

.....

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

.....

.....

.....

.....

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

.....

.....

.....

.....

4. A quels niveaux du modèle OSI fonctionne un firewall stateless (sans état) ? (2pts)
   a. 2 et 3
   b. 3 et 4
   c. 4 et 5

5. Quelles attaques sont considérées comme des dénis de service ? (2pts)
   a. Le spoofing
   b. Le flooding
   c. Le phishing

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

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

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

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

Attaque	La description
1. Usurpation d'adresse	A. L'attaquant peut surveiller, capturer et contrôler activement la communication de manière transparente.
2. Déni de service	B. L'attaquant tente de convaincre les gens de divulguer des informations sensibles.
3. Homme du milieu	C. L'attaque se produit lorsqu'un acteur malveillant construit un paquet IP qui semble provenir d'une adresse valide.
4. Par Hameçonnage	D. 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.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

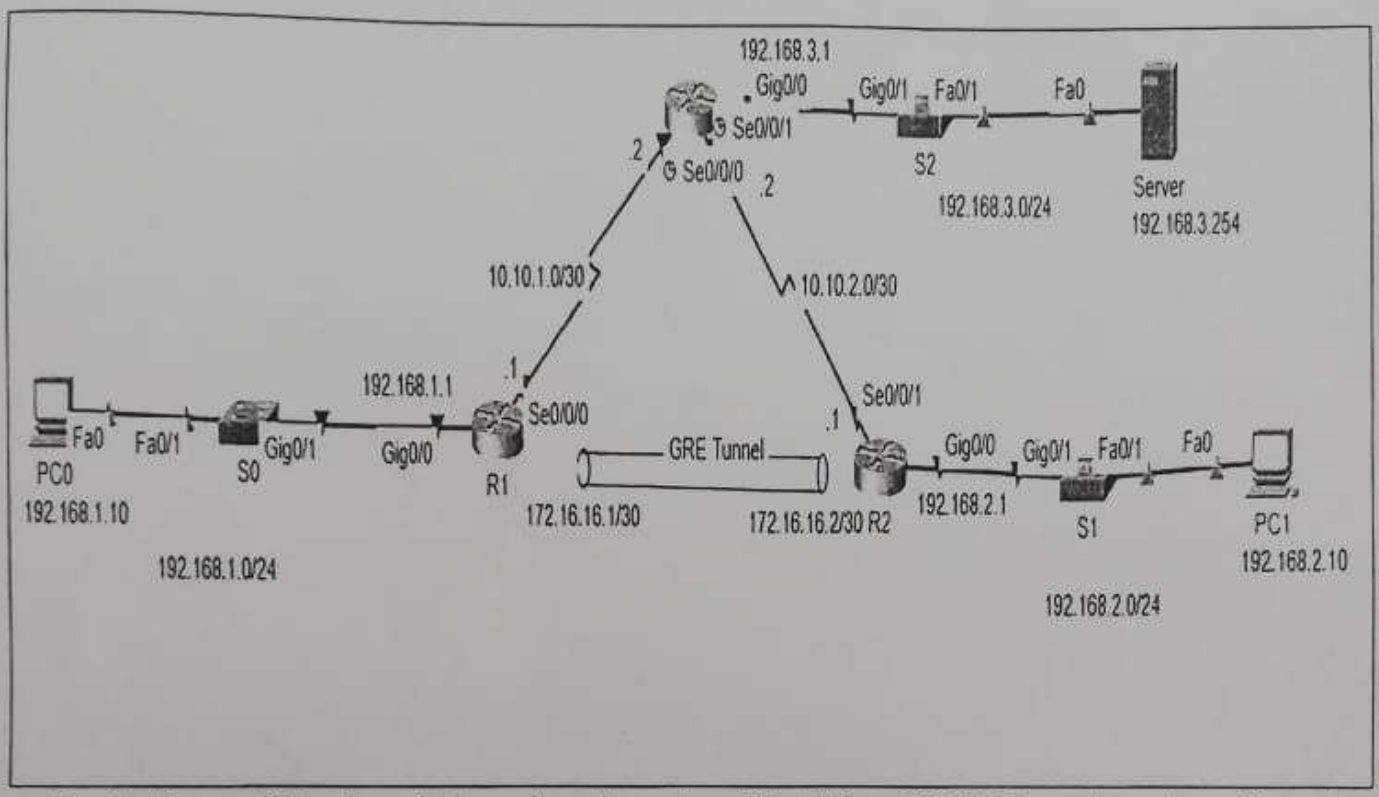
Réservé à l'établissement Code : .....

Surveillant1 : .....

Pratique : (20 points)

Dans cet exercice, on vous demande de configurer deux routeurs de telle sorte qu'ils prennent en charge un VPN de site à site pour le trafic issu de leurs LAN respectifs, et aussi de configurer les ACLs au niveau des routeurs.

Soit donc la topologie suivante :



1. 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)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Réservé à l'établissement Code : .....

Surveillant1 : .....

2. 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)

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

4. 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.

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

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

7. Vérifier votre ACL crée. (2pts)