Ecole Supérieure Privée d'Ingénierie et de Technologies	EXAMEN Semestre : 1 Session : Principale
ETUDIANT(e) Nom et Prénom : ……classe ……..	Code :
Module : **Sécurité Informatique** Enseignants : Equipe sécurité Classe(s) : 4ARTIC ; 4ERP-BI ; 4INFINI ; 4NIDS ; 4SAE Documents, Internet et calculatrice autorisés : NON Nombre de pages : 6 Date :**18-01-2022** Heure :**13h00** Durée :**1h30**	

Code	**Note** /20	**Nom et Signature du Surveillant**	**Nom et Signature du Correcteur**	**Observations**

Exercice 1 (4pts)

1. Citer un exemple d'attaque d'atteinte à l'Intégrité. **(1pt)**

   ……

2. Citer deux exemples d'impact lors d'une attaque visant la disponibilité d'un système informatique. **(1pt)**

   ……

   ……

3. Expliquer l'intérêt de la règle de sécurité du moindre privilège **(1pt)**

   ……

   ……

4. Quelle est la différence entre un risque critique et un risque vital. **(1pt)**

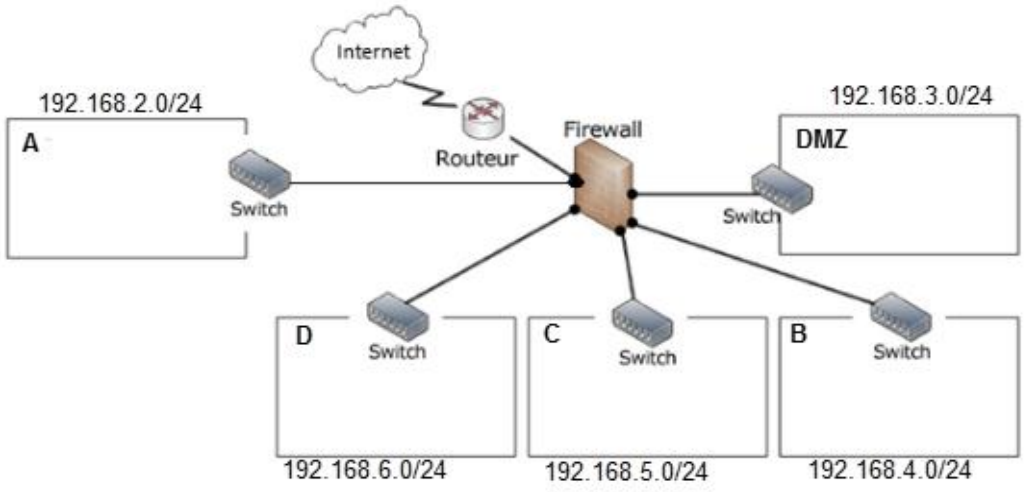
   ……

   ……

Exercice 2 (8pts)

Soit l'architecture du réseau suivante :

NE RIEN ECRIRE



1. Un attaquant a modifié les champs des datagrammes IP pour rediriger le trafic entre deux utilisateurs du réseau A

a) Identifier l'attaque ? **(0.5pt)**

……

b) Quel est le type (passive/active) de cette attaque ? **(0.5pt)**

……

2. Un attaquant a intercepté le trafic dirigé vers le serveur du réseau B grâce à une attaque de type Arp Spoofing.

a) Dans ce cas, expliquer brièvement cette attaque ? **(0.5pt)**

……

……

……..

b) Citer deux contre-mesures possibles. **(0.5pt)**

……

……

3. Un attaquant veut épuiser les ressources du serveur du réseau B.

a) Décrire l'attaque permettant d'atteindre ce but.**(0.5pt)**

……

……

b) Cette attaque est-elle active ou passive ? **(0.5pt)**

……

4. Lors du déploiement d'un IDS dans ce réseau, les gestionnaires de réseau créent un profil de fonctionnement normal du réseau par la surveillance des activités durant l'utilisation normale du réseau. Lorsque l'IDS détecte une activité excessive qui dépasse le seuil définit par le profil des alarmes seront générées.

a) Identifier le mécanisme de détection déployé ? Expliquer **(0.5pt)**

……

b) Citer les autres techniques de détection utilisées par les IDS **(1pt)**

……

……

5. Pour maximiser la sécurité, les serveurs de cette entreprise sont regroupés dans un réseau séparé.

a) Placer les éléments suivants sur la figure: **(0.5pt)**

Une imprimante
Un serveur FTP
Un serveur DNS
Deux postes « agents »
Un serveur Web
Deux postes des administrateurs
Serveur de base de données
Serveur Application

b) Définir le terme DMZ ainsi que son rôle dans la sécurité de cette architecture. **(0.5pt)**

……

……

c) Quel est le type de filtrage nécessaire pour sécuriser l'accès à ce réseau. Expliquer. **(0.5pt)**

……

……

6. L'administrateur a configuré le firewall comme suit :

N	Action	Protocole	@IPS	PortS	@IP d	Port d
1	Deny	IP	192.168.1.0	*	192.168.3.1	*
2	Allow	TCP	192.168.2.1	*	192.168.3.2	80
3	Deny	*	*	*	*	*

a) La machine 192.168.2.1 est-elle autorisée à lancer la commande ping sur le serveur 192.168.3.1? Justifier votre réponse **(0.5pt)**

……

……

b) Le serveur 192.168.3.1 est-il autorisé à lancer une connexion telnet sur la machine 192.168.1.2? Justifier votre réponse **(0.5pt)**

……

……

c) Apporter les modifications nécessaires sur le firewall afin d'autoriser le réseau 192.168.1.0 à se connecter uniquement au serveur web. **(1pt)**

……

……

Exercice 3 (8pts) :

Durant les examens de fin d'année à l'ESPRIT votre professeur de sécurité informatique se trouve à l'étranger et y'a que lui qui possède l'examen ainsi que la correction. L'administration lui demande une copie de l'examen et de correction.

1. Le professeur doit utiliser une méthode qui utilise des fonctions cryptographiques simples avec lesquelles il sécurise le document et que personne ne puisse le lire avant le jour de l'examen et encore personne ne peut modifier le continu.

a) Citer la méthode cryptographique qu'il faut appliquer pour assurer la non modification du document. **(0.5pt)**

……

……

b) Proposer deux fonctions cryptographiques qui permet de réaliser l'objectif de la question 1.a. **(0.5pt)**

……

……

2) Le professeur décide d'utiliser la cryptographie à clé publique pour sécuriser l'envoi du document. La paire des clés publique/privée du professeur dénoté par

Nom et Prénom :…….
Classe :……

(KP_Pub,KP_Prv) est disponible sur son PC portable et celle de secrétaire dénoté (KS_Pub,KS_Prv).

a) Parmi les opérations suivantes, choisir celle que le professeur doit effectuer si son but principal est d'assurer la confidentialité de l'examen qu'il va envoyer à la secrétaire : **(1pt)**

- Chiffrement de l'examen avec sa clé publique K_{P_Pub}
- Chiffrement de l'examen avec la clé publique de la secrétaire K_{S_Pub}
- Signature de de l'examen avec sa clé privéeK_{P_Prv}
- Signature de l'examen avec la clé privée de la secrétaire K_{S_Prv}

b) Parmi les opérations suivantes, laquelle le professeur doit-il effectuer si son but principal est d'assurer l'intégrité et la non-répudiation de l'examen envoyé : **(1pt)**

- Chiffrement de l'examen avec sa clé publique KP_Pub
- Chiffrement de l'examen avec la clé publique de la secrétaire KS_Pub
- Signature de de l'examen avec sa clé privée KP_Prv
- Signature de l'examen avec la clé privée de la secrétaire KS_Prv

3. Supposons qu'un étudiant ait pu « sniffer et rediriger » tout le trafic du poste de la secrétaire à partir de son ordinateur et qu'il a pu récupérer l'email du professeur. Selon vous, est-ce que l'étudiant serait en mesure de dévoiler le contenu de l'examen ainsi que la correction ? Si oui comment, si non pourquoi ? **(1pts)**

……
……
……
……..

4. Le professeur reçoit un email contenant la clé publique de la secrétaire mais, toujours très méfiant, il veut s'assurer qu'il a bien reçu la vraie clé que et le contenu de l'email n'a pas été modifier, proposer une solution utilisant des outils cryptographiques qui pourrait permettre au professeur de faire cette vérification. **(1pt)**

……
……
……

……

5. Supposons maintenant que le professeur ne veut pas entrer en échange de clé avec la secrétaire. Quel autre moyen existerait-il pour qu'il puisse obtenir une copie de sa clé publique dont il soit sûr de l'authenticité et qui évite l'échange quotidien des clés ? **(1pt)**

……

……

6. Le professeur vient de perdre sa clé privée, mais il dispose encore de la clé publique correspondante.

a) Peut-il encore envoyer des courriers électroniques chiffrés ? Justifier **(0.5pt)**

……

……

b) Peut-il encore en recevoir ? Justifier **(0.5pt)**

……

……

c) Peut-il encore signer les courriers électroniques qu'il envoie ? Justifier **(0.5pt)**

……

……..

d) Peut-il vérifier les signatures des courriers électroniques qu'il reçoit ? Justifier **(0.5pt)**

……

……

Bon travail