|  |  |  |
| --- | --- | --- |
| EXAMEN  Semestre : 1  Session : Principale | |  |
| Code : | ETUDIANT(e)  Nom et Prénom : ……………………………………classe …………….. | |
| 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** | | |

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

**Exercice 1 (4pts)**

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

Les attaques de modification

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

Rendre inaccessible un serveur

Saturation de la bande passante …

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

Accorde à un utilisateur le niveau d’accès (ou les permissions) minimum requis pour accomplir un travail.

**4.** Citer deux inconvénients du chiffrement symétrique. **(1pt)**

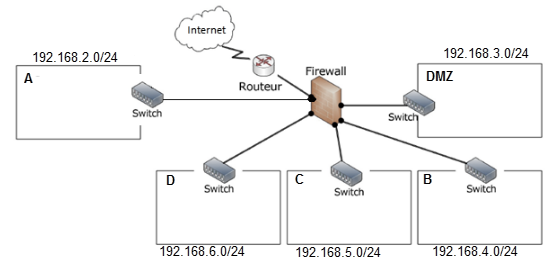
Echange de clé sécrète

Gestion des clés (nombre important des clés)

**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)**

Spoffing

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

Active

**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)**

L'attaquant associe sa propre adresse **MAC à l'adresse IP** d'un périphérique réseau connecté au commutateur. Le trafic destiné à cette adresse IP est désormais **envoyé à l'attaquant** au lieu d'être envoyé à la destination prévue.

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

… mapper de manière **statique** toutes les adresses MAC …

Outil (exp : arpwatch) permet de surveiller l’activité Ethernet

Mise à jour fréquent de table arp

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

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

Déni de service DOS : **Saturation** des ressources informatiques afin de rendre un service **indisponible**.

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

active

**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)**

Anomaly based

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

Signature based

Rules based

**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

**Réseau DMZ**

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

Une **zone démilitarisée** qui **héberge les services exposés** et accessibles de l'extérieur d'une entreprise

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

**Filtrage simple** de paquets (par IP) : un seul firewall est déployé entre le réseau extérieur, DMZ et LAN. Les adresses IP permettent d'identifier le destinataire : empêcher tout accès du réseau public vers les ressources et données du réseau privé.

**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)**

Non, la machine **192.168.2.1** ne peut pas lancer une commande ping

R2 : cette adresse IP est autorisée seulement à envoyer du trafic à 192.168.3.2 sur port 80.

**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)**

Non, 192.168.3.1 n’est pas autorisé à lancer une connexion telnet,

R3 : le trafic qui n’est pas autorisé par une règle sur le firewall est bloqué

**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)**

R : allow http 192.168.1.0 80 192.168.3.2 (@IPserv) 80

**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)**

Le hachage cryptographique

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

SHA1, SHA-256, MD5, MD6….

**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 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

**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) oui**

* + - Le pirate s’insère entre l’émetteur et le récepteur
    - Lorsque l’émetteur demande la clé publique du récepteur le pirate envoie sa propre clé.
    - L’émetteur crypte le message et l’envoie.
    - Intercepte par le pirate, il le décrypte avec sa propre clé privée.
    - Après il redirige le message vers le récepteur en le cryptant de nouveau avec la clé publique du récepteur

**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)**

Signature numérique

|  |
| --- |
| **NE RIEN ECRIRE** |

**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)**

Certificat numérique

**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)**

Oui, parce qu’il utilise la clé publique de destinataire pour chiffrer des messages.

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

Non, il ne peut pas déchiffrer les messages reçus parce qu’il a perdu sa clé privée.

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

Non, il ne peut pas signer les courriers électroniques parce qu’il a perdu sa clé privée.

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

Oui, parce qu’il utilise la clé publique de destinataire pour vérifier les signatures des courriers électroniques qu’il reçoit.

**Bon travail**