UNIVERSITE DE SFAX
Faculté des Sciences Economiques
Et de Gestion

Examen
Sécurité Informatique

Matricule : ……

Nom : ……..

Prénom : ……..

Année et filière : **3ème année LFIG**

Groupe : ……..……..

Module : **Sécurité Informatique**

Les étudiants sont invités à :
- écrire lisiblement leur identité.
- ne pas écrire leur nom sur la copie et ne pas s'y faire connaître.
- n'utiliser aucune copie autre que celle-ci.

Signature de l'Enseignant surveillant

DUREE : 2H

Note sur 20

A. U. 2019 – 2020

Exercice 1

1. Dans quel cas un pirate utilise l'attaque IP spoofing ?

…Dans le cas ou les adresses IP sont filtrées par un firewall ……

…(ou : lorsque l'attaque se fait à partir d'internet)

……

2. Dans quel cas un pirate utilise l'attaque Man in the middle ?

…Lorsque le réseau utilise un switch, c'est-à-dire le sniffing est impossible

……

……

3. Quels sont les objectifs du scanning ?

Identifier les ports ouverts soit pour faire une attaque, soit pour se protéger (sa machine ou son réseau local)……

……

……

4. Donner un cas où l'utilisation du VPN devient indispensable

Deux réseaux d'une même entreprise sont connectés via internet……

Ne Rien écrire ici

5. Pour le cryptage symétrique et le cryptage asymétrique

a. Donner les caractéristiques de chacun en précisant leurs inconvénients

- Cryptage symetrique : utilise une seule clé → rapide & sécurité faible
- Cryptage asymétrique : utilise deux clés (privée et publique) → lent &sécurité forte

……

……

b. Donner un exemple d'un protocole de sécurité qui se base sur l'utilisation de ces deux types de cryptage.

……https …(ou SSL)……

……

c. Quel est le rôle assuré par chacun de ces méthodes de cryptage dans le cadre de ce protocole?

- Le cryptage asymétrique est utilisé lors de la phase de l'échange de clés
- Le cryptage symétrique est utilisé lors de la phase de communication

6/ Expliquer le rôle de la commande suivante:

iptables –A INPUT –p tcp –dport 21 –j DROP ;

……Ajoute une règle suppression des paquets entrant sur le port 21

……

……

……

……

7. A quoi servent les logiciels suivants :

Nmap : … scanning ……

Ettercap : … Man in the middle ……

~~**Acunetix :**~~……. vous ne l'avez pas étudié cette année……

PGP :… cryptage ……

8/ Quelles sont les différentes actions possibles d'un IDS ? citer un exemple d'IDS

- **Envoi d'un e-mail , Journalisation (log) de l'attaque , Notification visuelle de l'alerte, Envoi d'un « ResetKill »** ……
- Exemple d'IDS : SNORT……

……

Exercice 2

Choisir **une ou plusieurs réponses** par question.

1/ Lequel des éléments suivants est une technique pour se protéger de l'attaque Sniffing :

A. Utiliser un pare feu (Fire Wall).
B. Utiliser un IDS.
C. Utiliser un Switch.
D. Utiliser des protocoles sécurisés sur le réseau.

2/ L'attaque Sniffing touche à:

A. La confidentialité
B. L'intégrité
C. La disponibilité

3/ L'attaque man in the middle touche à:

A. La confidentialité
B. L'intégrité
C. La disponibilité

4/ Quelles sont les grandes familles distinctes d'IDS:

A. N-IDS
B. M-IDS
C. H-IDS

~~Exercice 3~~ (à ne pas faire : vous ne l'avez pas étudié cette année)

Un utilisateur a introduit dans le champ *login* d'un formulaire d'un site Web non sécurisé le texte suivant :

' Union Select login, password from admin #

1/ Cette action changera la requête d'authentification permettant initialement la sélection de l'utilisateur suivant le login et mot de passe saisis par l'utilisateur.

a) Ecrivez la requête modifiée qui sera exécuté lors de cette attaque ?

……

b) Que va retourner cette requête une fois exécutée ?

…… ……

c) Quel est son effet au niveau du site Web ?

…… …….. ……

2/ Quel est le nom de cette attaque ?

……

3/ Que faut-il faire pour sécuriser ce site contre cette attaque ?

……

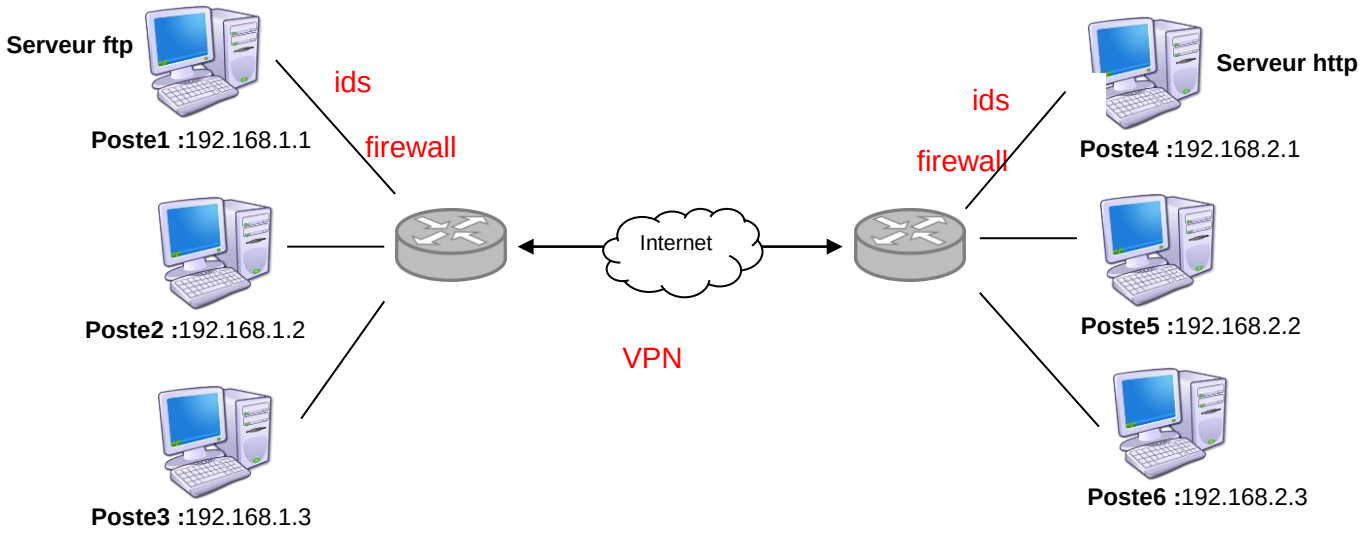
……

……

……

Exercice 5

Une entreprise possède le réseau suivant qui est constitué de deux réseaux locaux distants connectés via internet



1/ Sachant que les réseaux locaux sont connectés à l'aide de switch, un pirate c'est connecté au réseau local à travers le wifi et a lancer une attaque sniffig pour écouter les requêtes qui viennent vers le serveur http

a. est ce qu'il pourra écouter les requêtes ?

……non……

b. Justifier votre réponse

….Le réseau local utilise un switch qui adresse les paquets seulement au destinataire concerné……

……

2/ Le pirate a pu écouter toutes les requêtes entrantes vers le serveur http en se connectant au réseau local

a. Quelle est le nom de l'attaque utilisée ?

……. Man in the middle……

b. Expliquer cette attaque, comment elle a été mise en œuvre dans ce cas ?

- Cette attaque a pour but de s'insérer entre deux ordinateurs qui communiquent.
  Soient deux ordinateurs A et B voulant dialoguer. Si un pirate décide de se faire passer pour l'ordinateur A auprès de B et de B auprès de A, ainsi, toute communication vers A ou B passera par le pirate, l'homme du milieu.
- Le pirate s'est placé entre la passerelle et le serveur http (il a falsifié les entrées ARP qui correspondent à ces deux machines)

c. Quel est le logiciel utilisé ?

Ettercap

d. Comment peut-on se protéger contre cette attaque ?

Voir cours

3/ en utilisant une vulnérabilité du protocole **TCP**, un pirate a rendu le serveur Http non disponible

a. Quelle est le nom de l'attaque utilisée ?

……SYN flooding……

b. Expliquer cette attaque

Un client malveillant peut ne pas répondre avec le message ACK. Le serveur attend un certain temps avant de libérer les ressources qui ont été réservées pour le client.
Après l'étape 2, la connexion est semi-ouverte et consomme un certain nombre de ressources du côté du serveur (mémoire, temps processeur, etc.).
L'attaque SYN flooding consiste à générer un grand nombre de connexions incomplètes, ce qui va surcharger les ressources du serveur et ainsi l'empêcher d'accepter de nouvelles requêtes, avec pour résultat un déni de service. Dans certains cas, le serveur peut même planter par manque de ressources.

c. Donner trois solutions aidant à éviter cette attaque ?

Voir cours

4/ Cette entreprise vous engage pour sécuriser son parc informatique. Sachant que les machines des deux réseaux doivent être sécurisées et que les informations qui circulent entre les deux réseaux sont confidentiels, quelles sont les contre-mesures que vous allez proposer pour cette société. Indiquer les sur le schéma.

……

……voir le schéma……

……autre réponse acceptée : faire le scanning et fermer les ports non utilisés……

……

5/ Sachant que le résultat de Nmap pour toutes les machines est le suivant :

```
[root@nowhere.net /root]# nmap 192.168.1.1 Starting
nmap V. 2.54BETA31 (www.insecure.org/nmap/)
Interesting ports on (192.168.1.1) : (The 1544
ports scanned but not shown below are in state :
closed) Port State Service
Port        State       Service
21/tcp      open        ftp
22/tcp      open        ssh
80/tcp      open        http
Device type: general purpose Running: Linux 2.4.X
OS details: Linux 2.4.20 - 2.4.21 w/grsecurity.org
patch Uptime 76.872 days (since Tue Sep 2 15:20:23
2003)
Nmap run completed -- 1 IP address (1 host up)
scanned in 2 seconds.
```

Et sachant que **poste1** héberge un serveur **ftp** accessible uniquement par les postes des deux réseaux et que **poste4** héberge un **site Web** accessible via internet, quel sont les mesures de sécurité à effectuer pour chaque poste de cette société ?

Poste1 : fermer les ports ssh et http + firewall pour filtrer le port ftp

Poste4 : fermer les ports ssh et ftp

poste2, poste3,poste5, et poste6 : fermer tous les ports

6/ Après mise en place des contre-mesures que vous avez proposé, un pirate a pu faire un exploit qui lui a permit d'accéder au serveur ftp **à partir d'internet**

a. Quelle est le nom de l'attaque utilisée ?
…… IPSpoofing ……

b. Expliquer cette attaque

Le pirate envoie au serveur des paquets en utilisant une adresse IP falsifiée avec des numéros de séquence devinés ou en utilisant le source routing

……

……

……

c. Donner trois solutions aidant à éviter cette attaque ?
…… Voir cours

……

7/ Après la mise en place des solutions proposées dans les questions précédentes, un pirate à pu accéder au serveur ftp **en se connectant au réseau local**

a. Quelle est le nom de l'attaque utilisée ?
…… ARP spoofing ……

b. Expliquer cette attaque

L’ARP poisonning consiste à envoyer un message de réponse ARP avec l’adresse MAC de l’attaquant. Ainsi, tout le flux IP qui aurai dû être dirigé vers le récepteur sera redirigé vers l'attaquant.

c. Donner trois solutions aidant à éviter cette attaque ?

Voir cours