Université de Boumerdes UMBB
Faculté des Sciences
Sécurité Informatique
RIAHLA Med Amine

TD N° 4 : Protections

Exercice 1 «Antivirus et filtrage des fichiers joints»

1. Quelle (s) technique (s) utilise un antivirus pour détecter les programmes malicieux ?

2. Un logiciel antivirus installé sur un serveur de messagerie permet de bloquer automatiquement certains types de fichiers joints réputés dangereux. Pour cela, l'administrateur configure le système en spécifiant la liste des extensions ou des types spécifiques aux fichiers à bloquer (par exemple .exe, .vbs, .bat).

Quel reproche peut-on faire à une telle méthode d'un point de vue de la sécurité ?

Exercice 2 «Restauration d'un système après une infection virale»

Un administrateur est responsable d'un parc informatique comprenant six stations de travail connectées à internet à travers un pare feu. Plusieurs utilisateurs signalent que leur machine redémarre de manière intempestive. Selon l'un des utilisateurs. Ce problème est du à un vers virulent qui exploite une faille du système d'exploitation. Pour se propager, le ver semble utiliser des connexions TCP et UDP vers d'autres machines, aussi bien dans le réseau local que vers l'extérieur du réseau.

Détailler la démarche que doit suivre l'administrateur de ce réseau afin de résoudre le problème au plus vite. Décrire pour cela :

a. Les mesures d'urgence à appliquer afin d'enrayer la propagation du ver.
b. Les mesures à prendre pour restaurer l'intégrité du système

Exercice 3 «Authentification des connexions »

Une entreprise utilise un serveur web pour permettre aux employés de consulter leur messagerie depuis internet. Pour accéder à leur messagerie, les utilisateurs doivent s'authentifier sur une page du serveur web.

1. Quelle peut être l'utilité de demander une authentification des connexions web entrante au niveau du pare feu ?

2. Quel principe de base est appliqué dans ce cas ?

Exercice 4 «NAT »

Une entreprise pratique la translation d'adresses dynamique avec un pool de 3 adresses IP (193.49.96.60, 193.49.96.61 et 193.49.96.62). Quatre stations (A, B, C et D) souhaitent accéder au site web dont l'adresse IP est : 128 .178.50.93. Les adresses internes des stations A, B, C et D sont respectivement 192.168.10.1, 192.168.10.2, 192.168.10.3, 192.168.10.4. Les quatre machines utilisent le port source 3001.

Compléter la table de translation du pare feu pendant la connexion (plusieurs solutions correctes sont possibles

Table de translation du pare feu pendant la connexion							
Interne				Externe			
source	port	dest	port	source	port	dest	port
192.168.10.1							
192.168.10.2							
192.168.10.3							
192.168.10.4							

Exercice 5 «Règles de filtrage d'un Firewall»

On considère un pare feu sans mémoire dont le critère de filtrage est fondé sur les paquets SYN (paquet dont le flage SYN est à 1 et le flage ACK est à 0). On souhait que le serveur de messagerie (128.178.1.1) sur le réseau interne puisse recevoir et envoyer des messages de et vers internet.

Ecrire les règles de filtrage du pare feu dans le tableau suivant :

source	port	destination	port	protocole	Paquet SYN	action