Alejandro Hernandez

TRABAJO 1

HERRAMIENTAS PARA EL PRIMER TRABAJO

- **VirtualBox:** Software para tener maquinas virtuales y poder manejar varias arquitecturas desde un mismo pc.
- **Ubuntu Server:** Para tener el servidor del trabajo.
- **Kali Linux:** Sera usado para simular un cliente.
- **Servidor web apache:** Nos ayuda a establecer las conexiones https.

Se debe de tener en cuenta antes de empezar a realizar el trabajo, se asume que todas las herramientas están instaladas (También las máquinas virtuales en virutalbox).

Instalar Apache en el servidor usando:

Sudo apt install apache2

En las preferencias de VirtualBox en el apartado de red, añadimos una red y le ponemos nuestra IP

RED: 192.168.0.0/24

Mascara: 255.255.255.0

Gateway: 192.168.0.1

Broadcast: 192.168.0.255

Servidor:

Ubuntu server.

Login: alejo9720

Password: zafira1234

IP: 192.168.04

Cliente 1:

Kali Linux

Login: root

Password: 12345

IP: 192.168.05

Cliente 2:

Linux Mint

Login: cliente2

Password: 12345

IP: 192.168.0.6

1. Se requiere crear una regla que restrinja las conexiones por medio del cliente SSH al servidor web.

   Sudo iptables -A INPUT -p tcp --dport ssh -j DROP

   Sudo iptables -INPUT -p tcp –dport apache2 -j ACCEPT

2. Se requiere crear una regla que restrinja los pings que se realicen al servidor web.

   Iptable -A INPUT -p icmp –icmp-type echo-request -j DROP

3. Se requiere crear una regla donde el PC-A se le permita los pings al servidor y desde el PC-B sean restringidos

   PC A

   Iptables -A INPUT -s 192.168.0.6 – p icmp -j ACCEPT

   PC B

   Iptables -A INPUT -s 192.168.0.5 – p icmp -j DROP

4. Realiza un escaneo al servidor web y determina que puertos están abiertos, crea una regla que bloque los puertos que estén abiertos del 1 al 60.

   Para poder ver los puertos abiertos usamos:

   sudo netstat -lntup

   y la regla la definimos así

   sudo iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 1:60 -j DROP

5. Se requiere hacer una regla que restrinja las conexiones de una determinada dirección MAC.

sudo iptables -I INPUT -m mac --mac-source 08:00:27:dd:4a:f8 -j DROP

6. Se requiere crear una regla que restrinja todas las conexiones a nuestro servidor web.

   Primero para inhabilitar todo lo que entre a nuestro servidor
   sudo iptables -P INPUT DROP
   Luego para que no salga nada de mi servidor
   Sudo iptables -P OUTPUT DROP

INVESTIGACION

¿Qué es iptables?

Es una herramienta avanzada que usa el sistema operativo Linux para analizar cada uno de los paquetes del trafico en la red que entra a una maquina y decidir por medio de unas reglas que se le establecen previamente.

Con esta herramienta se puede implementar un firewall de manera manual, además permite marcar o modificar paquetes.

Esta herramienta esta construida sobre el framework Netfilter el cual esta en el núcleo de Linux que permite interceptar y manipular paquetes de red.

Estructura IPtables

iptables [-t <*table-name*>] <*command*> <*chain-name*> <*parameter-1*> \
<*option-1*> <*parameter-n*> <*option-n*>

<table-name> Permite al usuario seleccionar una tabla diferente a la predeterminada.

<command> Indica la acción a realizar.

<chain-name> Unas opciones que indica que pasa cuando el paquete coincide con la regla.

Bibliografía

https://openwebinars.net/blog/que-es-iptables/

https://www.utilizalinux.com/que-es-iptables/

http://iptables-slud.blogspot.com/2012/07/operacion-basica-de-iptables.html

https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-iptables-options.html