Práctica Núm. 12.- Planear las estrategias de seguridad, uso y mantenimiento al sistema operativo de software libre.

Práctica Núm. 12

Nombre: Planear las estrategias de seguridad, uso y mantenimiento al sistema operativo de software libre.

Objetivo: El alumno aprenderá a Planear las estrategias de seguridad, uso y mantenimiento al sistema operativo de software libre.

Introducción: La palabra «seguridad» en sí misma cubre un amplio rango de conceptos, herramientas y procedimientos, ninguno de los cuales es universal. Seleccionar entre ellos requiere una idea precisa de sus metas. Asegurar un sistema comienza con responder unas pocas preguntas. Al precipitarse a implementar un conjunto arbitrario de herramientas corre el riesgo de enfocarse en los aspectos de seguridad equivocados.

Correlación con el o los temas y subtemas del programa de estudios.

Temas	Subtemas
Sistemas Operativos de software libre para servidores.	3.6. Medición y Desempeño del Sistema Operativo 3.7. Seguridad e Integridad 3.7.1. Planificación de seguridad

Materiales:

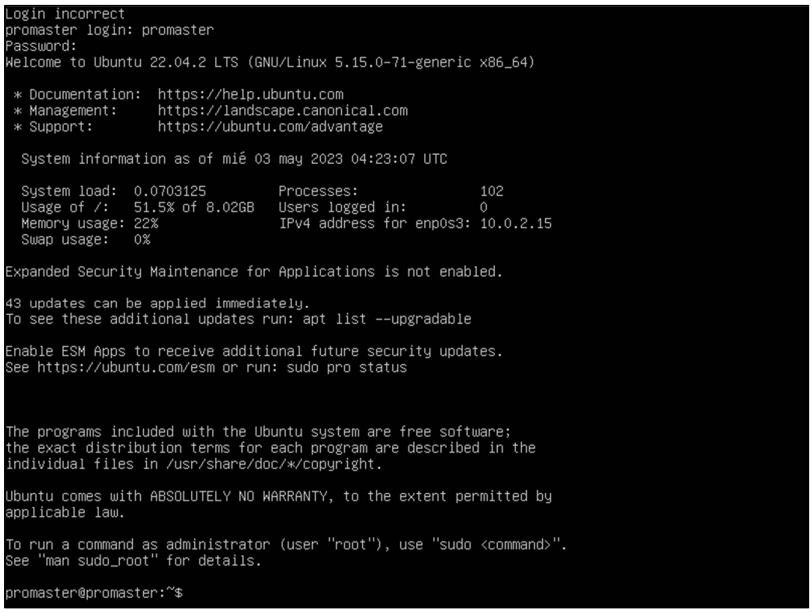
- Software Ubuntu
- Firewall (IpTables)
- Equipo de cómputo.
- Internet.

Indicaciones:

1) Tener Instalado S.O. Ubuntu (versión Actual) en VitualBox.
2) Descargar e instalar IpTables en Ubuntu.
    a. Comprobación del estado actual de los iptables.
    b. Habilitar el tráfico en localhost.
    c. Habilitación de conexiones en el puerto HTTP, SSH y SSL.
    d. Filtrado de paquetes basados en la fuente.
    e. Eliminar el resto del tráfico
3) Instalar Interfaz Gráfica en Ubuntu Server.

Desarrollo

Para iniciar con el proceso de instalación de iptables, lo primero es ingresar al servidor con el login y la contraseña que se asignó al instalar el sistema operativo.



Instalación de iptables.

Una vez dentro del servidor, hay que ingresar el comando sudo apt-get update para actualizar los paquetes de seguridad del sistema operativo.

Ya que los paquetes hayan sido actualizados se ingresa el comando sudo apt-get install iptables para confirmar que iptables está instalado.

```
promaster@promaster:~$ sudo apt-get install iptables
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables ya está en su versión más reciente (1.8.7-1ubuntu5).
fijado iptables como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 43 no actualizados.
promaster@promaster:~$ _
```

Comprobación del estado actual de iptables.

A continuación, se comprueba el estado actual de iptables con el comando sudo iptables -L -v donde L lista todas las reglas y la opción v es para una lista más tediosa.

En la imagen se observa que el sistema muestra el estado de sus cadenas. La salida lista tres cadenas: INPUT, FORWARD y OUTPUT las tres cadenas se establecen en la política ACCEPT predeterminada.

```
promaster@promaster:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
promaster@promaster:~$
```

Habilitar el tráfico en localhost.

Para habilitar el tráfico en localhost se ingresa el siguiente comando: sudo iptables -A INPUT -i lo -j ACCEPT.

-A se utiliza una opción para añadir la regla a la cadena INPUT, aceptar todas las conexiones en la interfaz lo. lo significa la interfaz de loopback. Se utiliza para todas las comunicaciones en el localhost, como

las comunicaciones entre una base de datos y una aplicación web en la misma máquina.

```
promaster@promaster:~$ sudo iptables -A INPUT -i lo -j ACCEPT
promaster@promaster:~$
```

Habilitar el tráfico en el puerto HTTP.

Una vez habilitado el tráfico en localhost, se procede a habilitar el tráfico para el puerto HTTP (80), esto se realiza con el comando sudo iptables -A INPUT -p tcp -dport 80 -j ACCEPT. En estos comandos se especifica el protocolo con la opción -p y el puerto correspondiente para cada protocolo con la opción -dport (puerto de destino).

```
promaster@promaster:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
promaster@promaster:~$
```

Habilitar el tráfico en el puerto SSH.

Hecho esto, el siguiente puerto a ser habilitado es el puerto SSH (Secure Shell) hay que tener en cuenta que se utiliza el puerto 22, que es el número de puerto SSH por defecto, en caso de que el número de puerto sea diferente, hay que asegurarse de ajustar los siguientes comandos en consecuencia: sudo iptables -A INPUT -p tcp -dport 22 -j ACCEPT.

```
promaster@promaster:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
promaster@promaster:~$ _
```

Habilitar el tráfico en el puerto SSL.

Una vez teniendo el tráfico habilitado de los puertos anteriores el último puerto a habilitar es el puerto SSL (443) con el comando: sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT.

```
promaster@promaster:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
promaster@promaster:~$
```

Filtrado de paquetes basados en la fuente.

Ya que se haya hecho la configuración para habilitar el tráfico en los puertos específicos, lo siguiente es hacer la configuración para el filtrado de paquetes basados en la fuente es decir, si se desea aceptar o rechazar paquetes basados en la dirección IP de origen o en el intervalo de direcciones IP, esto puede especificarse con la opción -s. Por ejemplo, en este caso para aceptar paquetes desde la dirección 192.168.1.18.

```
promaster@promaster:~$ sudo iptables -A INPUT -s 192.168.1.18 -j ACCEPT
promaster@promaster:~$
```

Eliminar el resto del tráfico.

Es importante eliminar el resto del tráfico después de definir las reglas, ya que impide el acceso no autorizado a un servidor desde otros puertos abiertos. Para ello se ocupa el comando: sudo iptables -A INPUT -j DROP. Este comando descarta todo el tráfico entrante distinto de los puertos mencionados en los comandos anteriores.

```
promaster@promaster:~$ sudo iptables -A INPUT -j DROP
promaster@promaster:~$ _
```

Comprobar conjunto de reglas.

Una vez que se hayan establecido las reglas correspondientes en iptables hay que comprobar el conjunto y el estado de las mismas con el mismo comando que se ocupó al inicio sudo iptables -L -v con esto se muestra la lista de las reglas establecidas.

```
promaster@promaster:~$ sudo iptables -A INPUT -j DROP
promaster@promaster:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere
    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:htt
p
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:ssh
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:htt
ps
    0     0 ACCEPT     all  --  any    any     192.168.1.18         anywhere
    3   228 DROP       all  --  any    any     anywhere             anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
promaster@promaster:~$
```

Guardar cambios (iptables).

Finalmente, las reglas de Iptables que se han creado se guardan en la memoria. Eso significa que hay que redefinirlos en el reinicio. Para que estos cambios sean persistentes después del reinicio, se utiliza el siguiente comando: sudo /sbin/iptables-save. Este comando guarda las reglas actuales en el archivo de configuración del sistema que se utiliza para reconfigurar las tablas en el momento del reinicio.

```
promaster@promaster:~$ sudo /sbin/iptables-save
# Generated by iptables-save v1.8.7 on Wed May  3 22:11:39 2023
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -s 192.168.20.125/32 -j ACCEPT
-A INPUT -j DROP
COMMIT
# Completed on Wed May  3 22:11:39 2023
promaster@promaster:~$ _
```

Sugerencias Didácticas:

Se asesorará al alumno en todo el proceso, se compararan los resultados con base a las indicaciones sugeridas, y al finalizar la práctica se desarrollará un reporte, donde se indicara paso a paso la realización de la práctica desarrollada.

Reporte en pdf (Resultados):

Al finalizar la práctica se desarrollará un reporte con la metodología ocupada (Pasos que se llevaron en la práctica). Incluye imágenes y descripción de las mismas. Contenido:

1) Portada (Nombre: Instituto, Asignatura, Integrantes, Núm. Práctica, fecha).
2) Introducción (Breve descripción Máximo una Hoja)
3) Desarrollo (Metodología ocupada)
4) Conclusiones (Breve descripción Máximo una Hoja)

Bibliografía Preliminar.

- Implantación de Sistemas Operativo, José Luis Raya Cabrera, Laura Raya González, RA-MA, 1ra. Edición, España 2014.
- https://debian-handbook.info/browse/es-ES/stable/security.html
- https://www.redeszone.net/gnu-linux/iptables-configuracion-del-firewall-en-linux-con-iptables/
- https://www.alferez.es/documentos/Instalacion_IPCOP.pdf
- https://www.hostinger.mx/tutoriales/iptables-asegurar-ubuntu-vps-linux-firewall/#1_Instalacion_de_Iptables
- https://www.solvetic.com/tutoriales/article/9231-como-instalar-interfaz-grafica-en-ubuntu-server-21-04-escritorio/