Administración de servidores

D05

Vi-Sa 7-9 Hrs

José de Jesús Soto Sánchez

Actividad 11 – IPTables

Centro Universitario de Ciencias Exactas e Ingenierías

Universidad de Guadalajara

2023ª

EN esta última práctica, siendo la actividad número 11 del curso de servidores, termina por ser una práctica con un desarrollo fundamental para los servidores, puesto que tiene como principal objetivo brindar seguridad a nuestro servidor, para lograr eso es necesario recurrir a los iptables, siendo el concepto general de la actividad actual, estas mismas son un conjunto de herramientas en el sistema operativo de Linux que funcionan principalmente la administración de las reglas que filtran el trafico dentro de una red.

Para entender los iptables, es necesario comprender el firewall, el cual es un sistema que permite la entrada y salida de ciertos paquetes, estos se transfieren a través de puertos, los cuales son elegidos por el firewall.

Con eso en mente los iptables, son la interfaz del netfilter usado por elfirewall para la elección de paquetes y como estos se transmiten dentro del sistema. Estos iptables son un conjunto de herramientas que filtran paquetes, permitiendo el control del tráfico en una red, esto se logra mediante la implementación de reglas que permiten o bloquean los accesos a ciertos puertos, por lo que se convierten en la herramienta fundamental en cuanto a seguridad del servidor s e refiere, permitiendo mejor privacidad e integridad a los datos que se manejan en la red.

Estructura y componentes.

Cadenas (Chains): Existen tres cadenas principales (INPUT, OUTPUT y FORWARD), estas cadenas son solo un conjunto de reglas y procesos.

Tablas (tables): Es una colección de cadenas que tienen una función en específico.

Targets: Es una dirección hacia donde los paquetes se han de dirigir.

Cadenas principales

Input: evita que se dañe las computadoras al navegar en el internet.

Forward: Reenvía los paquetes.

Output: Permite la conexión con internet.

Argumentos:

-F –flush: Elimina las reglas de una cadena.

-A –append: Añade una nueva regla a una cadena.

-N –new-chain: Se crea una nueva cadena.

-j: Especifica a un target para una regla, especifica si se aceptao rechaza un paquete.

-P—policy: Especifica la política a la cualse ha de aplicar algo.

udp –dport: Especifica el protocolo y destino de puerto para la regla a aplicar, para el protocolo UDP.

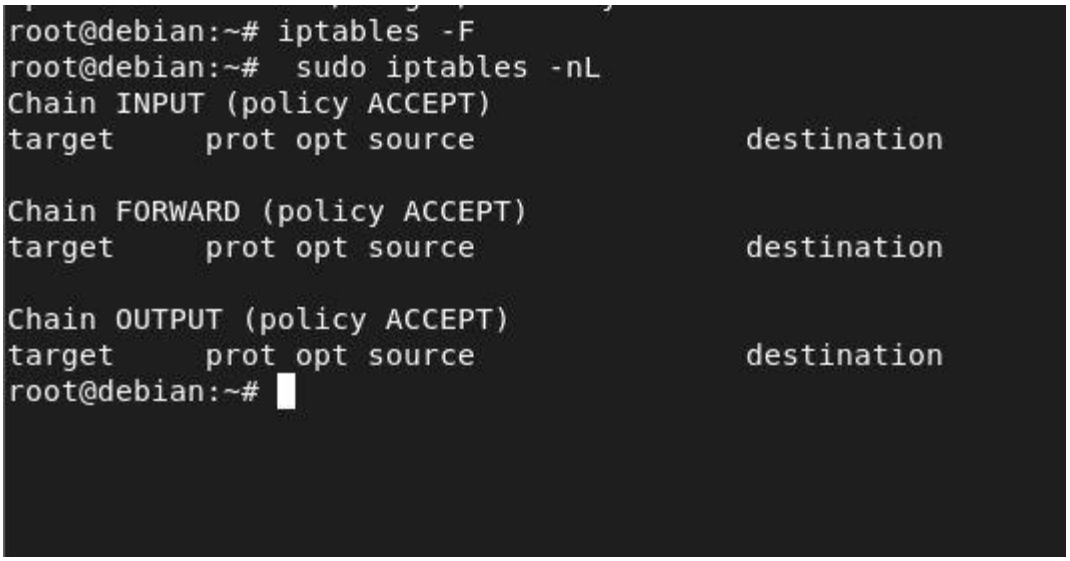
tcp –dport: Similar como el de arriba, pero con el protocolo TCP.

DROP: El paquete es silenciado.

ACCEPT: Se utiliza para aceptar el paquete.

Desarrollo:

Con –F se quitan las reglas actualmente aplicadas.



-N para crear una nueva cadena llamada FIREWALL

```
root@debian:~# sudo iptables -N FIREWALL
root@debian:~#  sudo iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain FIREWALL (0 references)
target     prot opt source               destination
```

Los paquetes de INPUT y OUTPUT se redirigen con –A a FIREWALL

```
root@debian:~# sudo iptables -A INPUT -j FIREWALL
root@debian:~# sudo iptables -A OUTPUT -j FIREWALL
root@debian:~#  sudo iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
FIREWALL   all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
FIREWALL   all  --  0.0.0.0/0            0.0.0.0/0

Chain FIREWALL (2 references)
target     prot opt source               destination
```

Con DROP a las tablas anteriormente establecidas se restringe la red del servidor, para poder modificar la nueva cadena.

```
root@debian:~# sudo iptables -P INPUT DROP
root@debian:~# sudo iptables -P OUTPUT DROP
root@debian:~# sudo iptables -P FORWARD DROP
root@debian:~#  sudo iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination
FIREWALL   all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
FIREWALL   all  --  0.0.0.0/0            0.0.0.0/0

Chain FIREWALL (2 references)
target     prot opt source               destination
```

Se permite el tráfico en el puerto 22, el cual sirve para la conexión SSH.

```
root@debian:~# sudo iptables -A FIREWALL -p tcp --dport 22 -j ACCEPT
root@debian:~#  sudo iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination
FIREWALL   all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
FIREWALL   all  --  0.0.0.0/0            0.0.0.0/0

Chain FIREWALL (2 references)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22
```

Se habilita el puerto53 para la conexión del DNS.

```
root@debian:~# sudo iptables -A FIREWALL -p udp --dport 53 -j ACCEPT
root@debian:~# sudo iptables -A FIREWALL -p tcp --dport 53 -j ACCEPT
root@debian:~#  sudo iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination
FIREWALL   all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
FIREWALL   all  --  0.0.0.0/0            0.0.0.0/0

Chain FIREWALL (2 references)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:53
```

Los puertos 139 y 445 sirven para permitir los servicios de SAMBA

```
root@debian:~# sudo iptables -A FIREWALL -p tcp --dport 139 -j ACCEPT
root@debian:~# sudo iptables -A FIREWALL -p tcp --dport 445 -j ACCEPT
root@debian:~#  sudo iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination
FIREWALL   all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
FIREWALL   all  --  0.0.0.0/0            0.0.0.0/0

Chain FIREWALL (2 references)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:139
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:445
root@debian:~# sudo iptables -A FIREWALL -p tcp --dport 138 -j ACCEPT
root@debian:~# sudo iptables -A FIREWALL -p tcp --dport 137 -j ACCEPT
root@debian:~#
```

Los puertos 80 y 443 se habilitan para permitir el acceso al sitio web.

```
root@debian:~# sudo iptables -A FIREWALL -p tcp --dport 80 -j ACCEPT
root@debian:~# sudo iptables -A FIREWALL -p tcp --dport 443 -j ACCEPT
root@debian:~#
```

Los puertos 20 y 21 tienen la función de acceder a los sitios de FTP

```
root@debian:~# sudo iptables -A FIREWALL -p tcp --dport 20 -j ACCEPT
root@debian:~# sudo iptables -A FIREWALL -p tcp --dport 21 -j ACCEPT
root@debian:~#
```

Para acceder a los servicios de correo se requieren de los puertos 25 y 110

```
root@debian:~# sudo iptables -A FIREWALL -p tcp --dport 25 -j ACCEPT
root@debian:~# sudo iptables -A FIREWALL -p tcp --dport 110 -j ACCEPT
root@debian:~#
```

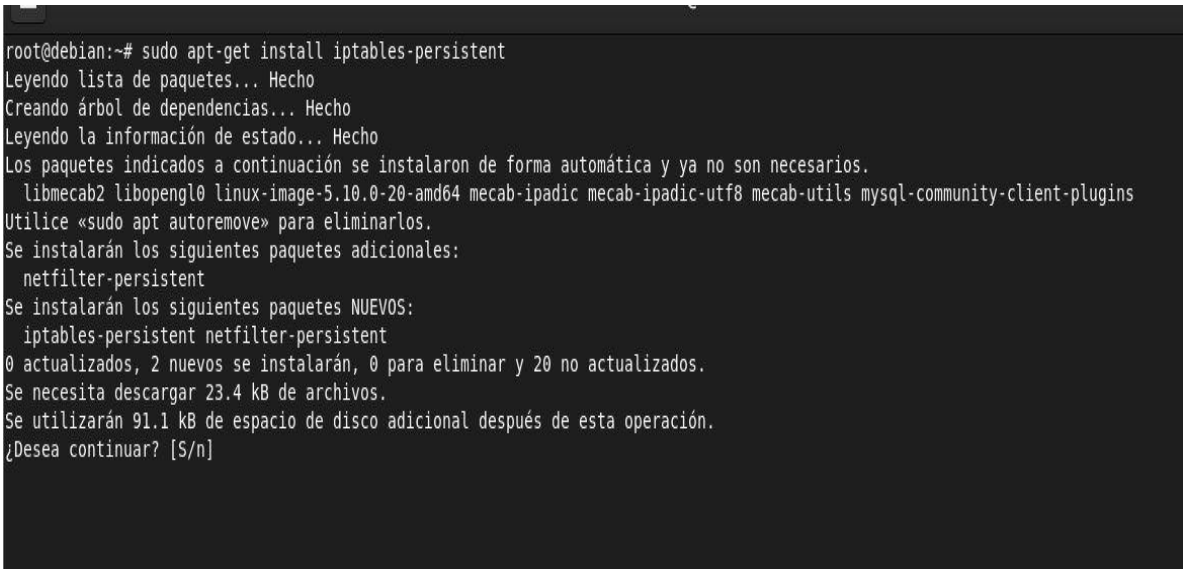
Para el servicio de impresión se necesita habilitar el puerto 631.

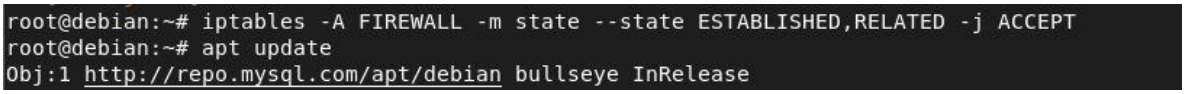
```
root@debian:~# sudo iptables -A FIREWALL -p tcp --dport 631 -j ACCEPT
root@debian:~# sudo iptables -A FIREWALL -p udp --dport 631 -j ACCEPT
root@debian:~#
```

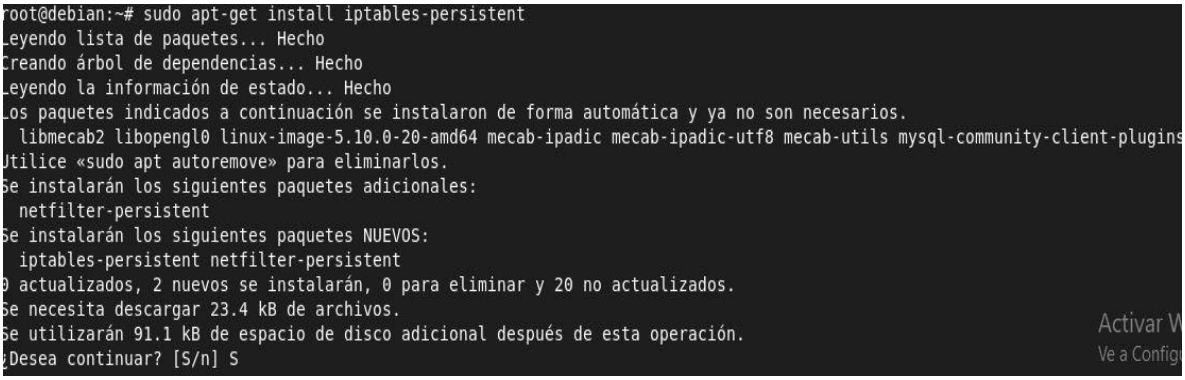
Esto permite que el servidor pueda hacer ping a otros equipos y sin embargo estos no puedan realizar ping al servidor, son reglas aplicadas principalmente a la cadena de FIREWALL.

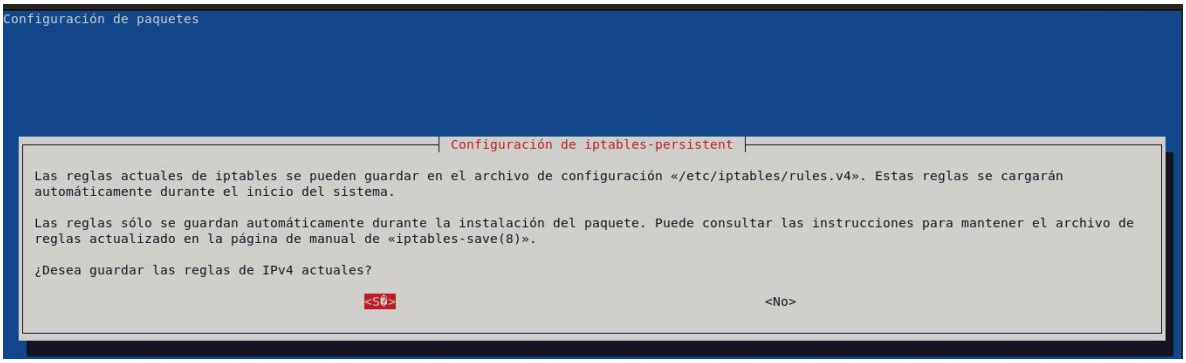
```
root@debian:~# sudo iptables -A OUTPUT -p icmp -j ACCEPT
root@debian:~# sudo iptables -A INPUT -p icmp -j DROP
root@debian:~#
```

Con esto se guardan las reglas de manera permanente y al final se muestran las reglas aplicadas en el servidor.

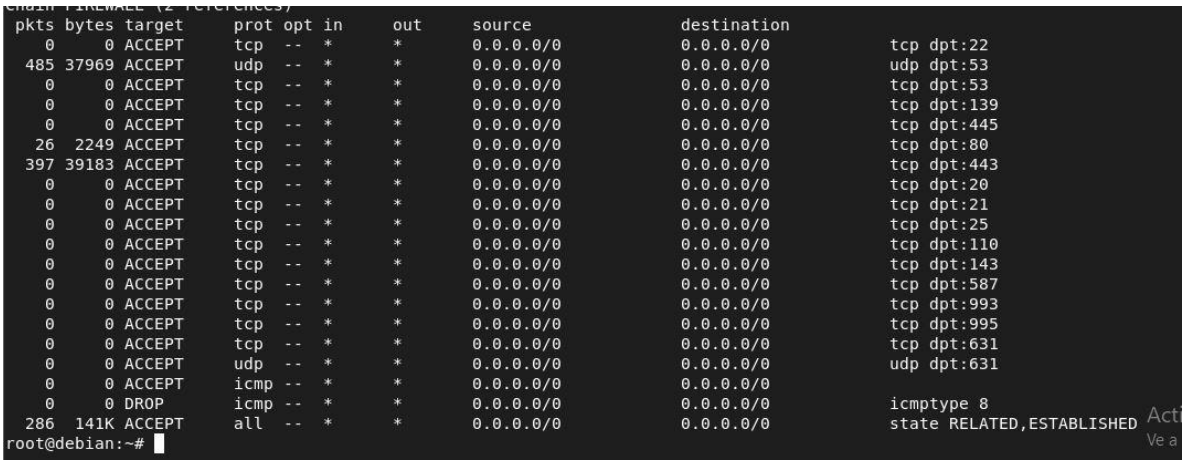






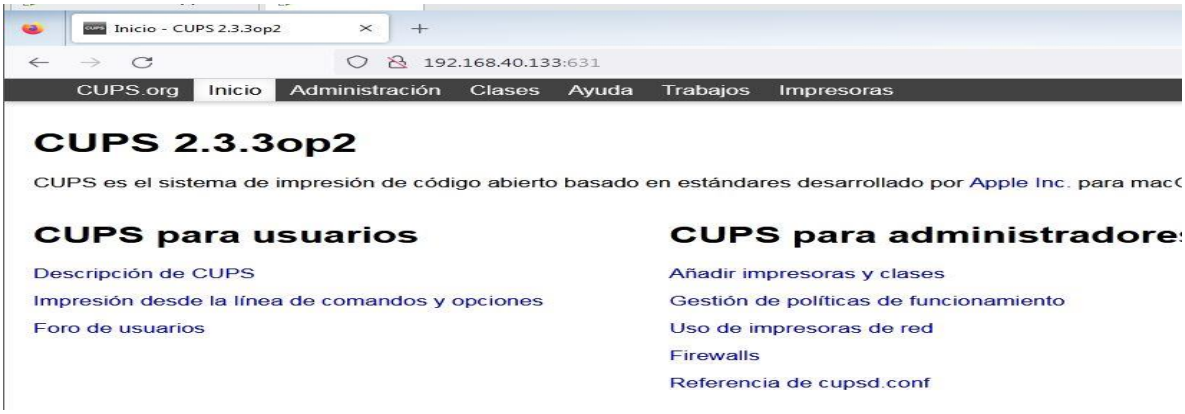


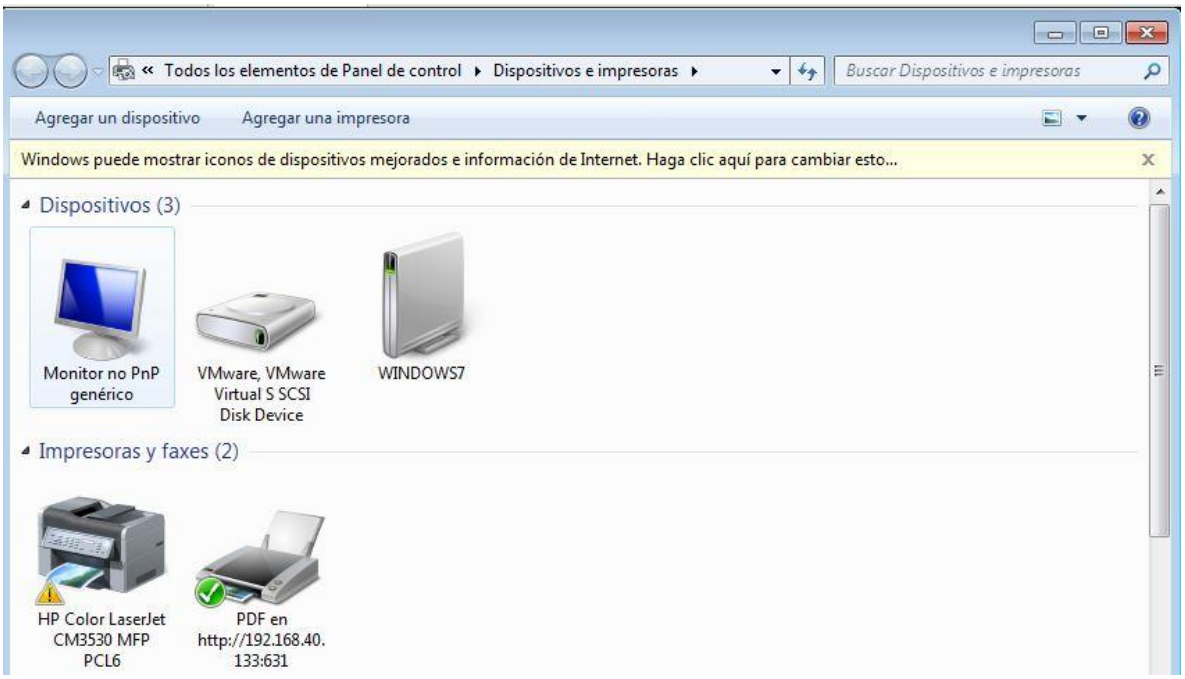
```
root@debian:~# sudo service netfilter-persistent save
Saving netfilter rules...run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
done.
root@debian:~# sudo iptables -L -v -n
Chain INPUT (policy DROP 707 packets, 60905 bytes)
 pkts bytes target     prot opt in     out     source               destination
 1293  314K FIREWALL   all  --  *      *       0.0.0.0/0            0.0.0.0/0

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

Chain OUTPUT (policy DROP 182 packets, 13662 bytes)
 pkts bytes target     prot opt in     out     source               destination
 1505  234K FIREWALL   all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     all  --  *      eth0    0.0.0.0/0            0.0.0.0/0
  436 27359 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0

Chain FIREWALL (2 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
  485 37969 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:139
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:445
   26  2249 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
  397 39183 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:20
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:21
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:25
```



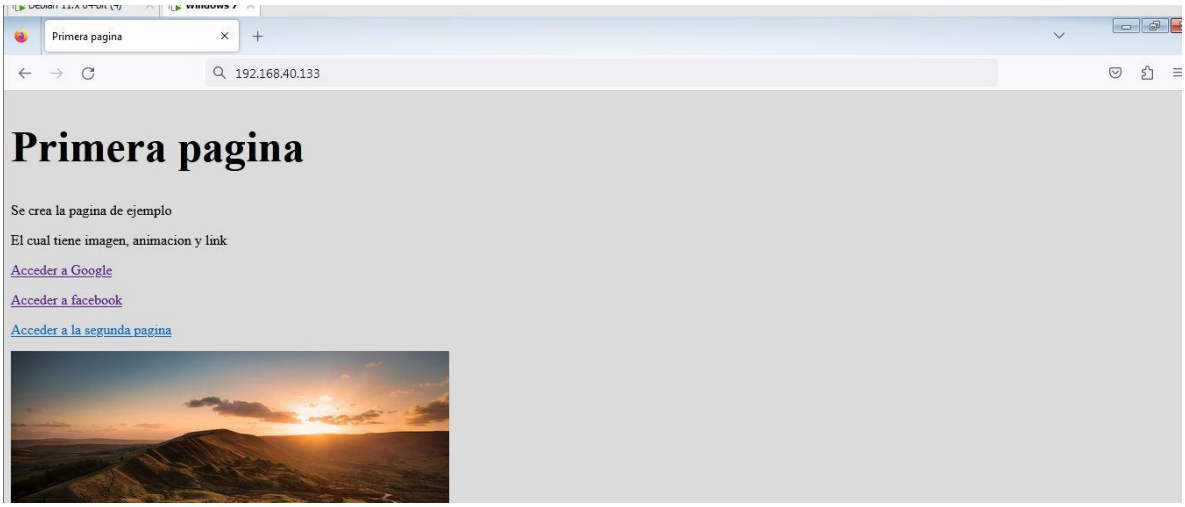
Reglas aplicadas con el comando iptables -L -v –n

Algunas reglas aplicadas, como el servicio de impresora

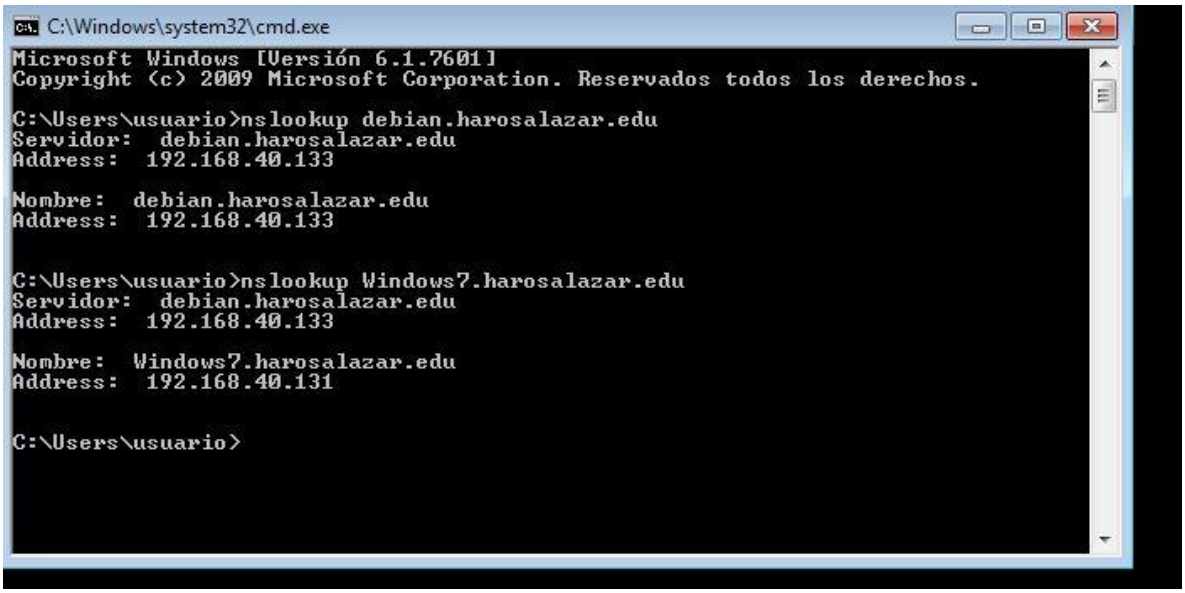




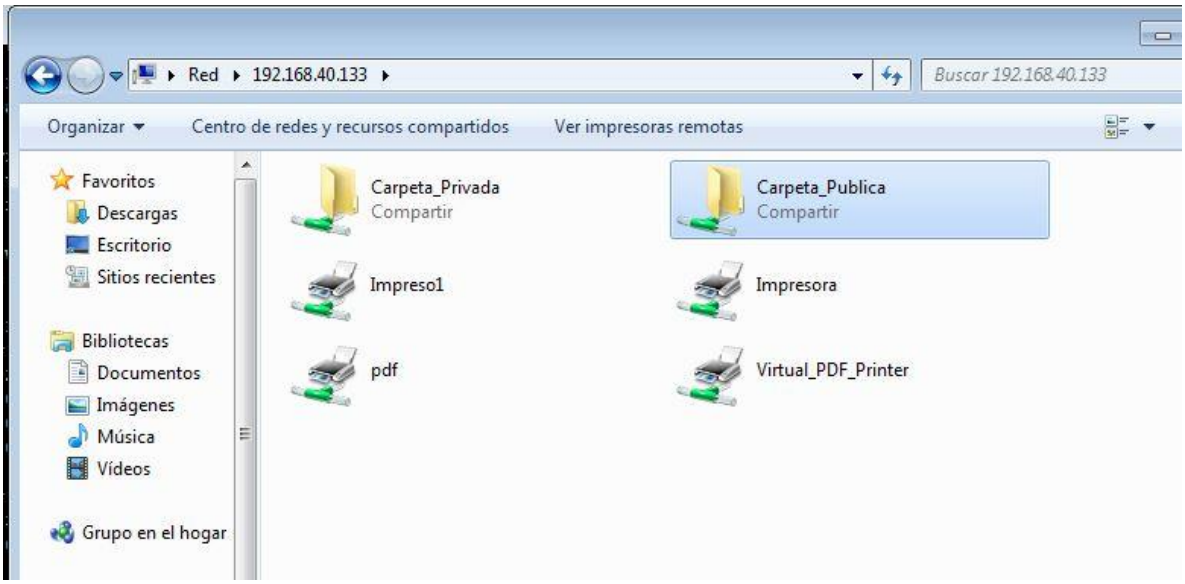
Servicio web



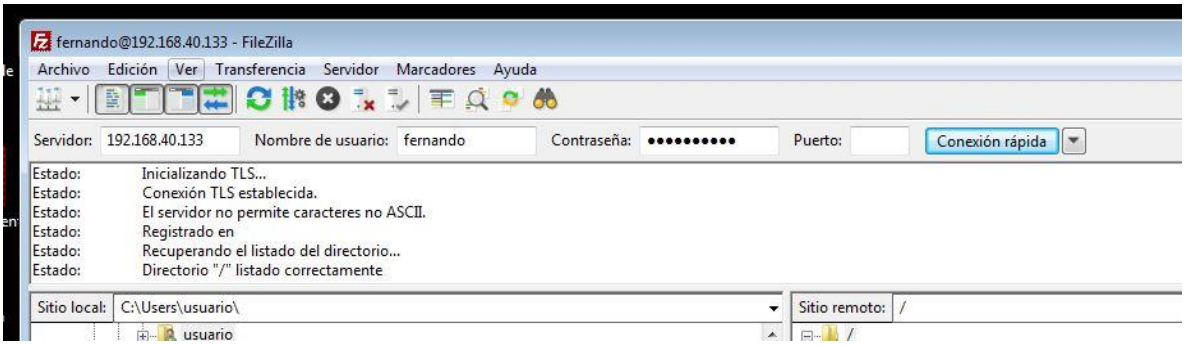
DNS y SSH


C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Users\usuario>nslookup debian.harosalazar.edu
Servidor: debian.harosalazar.edu
Address: 192.168.40.133
Nombre: debian.harosalazar.edu
Address: 192.168.40.133
C:\Users\usuario>nslookup Windows7.harosalazar.edu
Servidor: debian.harosalazar.edu
Address: 192.168.40.133
Nombre: Windows7.harosalazar.edu
Address: 192.168.40.131
C:\Users\usuario>

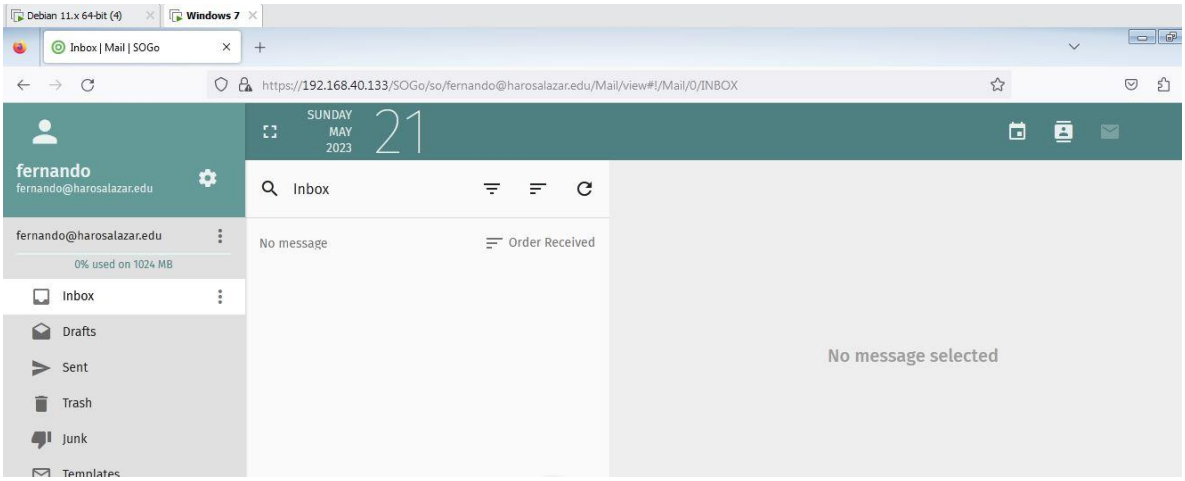
samba


Red
192.168.40.133
Buscar 192.168.40.133
Organizar
Centro de redes y recursos compartidos
Ver impresoras remotas
Favoritos
Descargas
Escritorio
Sitios recientes
Bibliotecas
Documentos
Imágenes
Música
Vídeos
Grupo en el hogar
Carpeta_Privada
Compartir
Carpeta_Publica
Compartir
Impreso1
Impresora
pdf
Virtual_PDF_Printer

ftp


fernando@192.168.40.133 - FileZilla
Archivo Edición Ver Transferencia Servidor Marcadores Ayuda
Servidor: 192.168.40.133
Nombre de usuario: fernando
Contraseña:
Puerto:
Conexión rápida
Estado: Inicializando TLS...
Estado: Conexión TLS establecida.
Estado: El servidor no permite caracteres no ASCII.
Estado: Registrado en
Estado: Recuperando el listado del directorio...
Estado: Directorio "/" listado correctamente
Sitio local: C:\Users\usuario\
Sitio remoto: /
usuario

El servicio de correos y otros más funcionan bien con las reglas aplicadas en el servidor.



Conclusión

En conclusión, Para la práctica final, se diseñaron reglas con los comandos integrados dentro de LINUX, los cuales eran lo iptables, siendo sistemas de reglas que restringen o permiten las distintas conexiones existentes en nuestro servidor, me pareció ser la práctica más importante al momento de finalizar nuestro servidor, puesto que al ser las reglas que rigen los paquetes que se aceptan o descartan dentro de la red local, es de vital importancia si se necesita la seguridad, privacidad e integridad en un servidor, esta actividad fue distinta en el desarrollo, puesto que el administrador define el comportamiento de los paquetes dentro de una red y de los dispositivitos conectados al servidor, fue una práctica interesante debido como se manejan los paquetes y como estos desarrollados dentro de cada puerto especifico, que cumple su función para analizar a estos mismos, el objetivo de esta actividad fue de establecer y comprender las reglas que se manejan y se desarrollan con iptables, por lo que estos objetivos han sido completados, se entiende que son las iptables, como se manipulan para restringir la red del servidor, además de leer y comprender varias fuentes de información que ayudaban a comprender el funcionamiento de cada puerto y como este afectaba a cada servicio, teniendo cuidado de aceptar aquellos establecidos y de negar aquellos potencialmente dañinos o innecesarios para nuestro sistema, una práctica de bastante utilidad si el tema a tratar es la seguridad en los sistemas, no obstante la actividad fue interesante puesto que se centra en comprender el manejo y configuración de los puertos en una red establecida por el usuario, no era solo escribirlos sino adaptarlos para el uso de ciertos servicios.