

Administración de servidores

D05

Vi-Sa 7-9 Hrs

José de Jesús Soto Sánchez

**Actividad 11 – IPTables**

Haro Salazar Fernando Baruj

Código:

217534556

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.

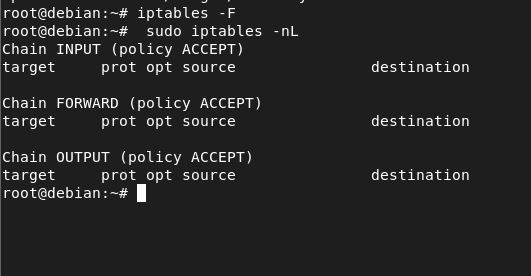
tcp –dport: Similar como el de arriba, pero con el protocolo TCP.

DROP: El paquete es silenciado.

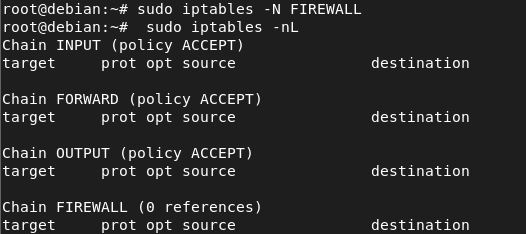
ACCEPT: Se utiliza para aceptar el paquete.

Desarrollo:

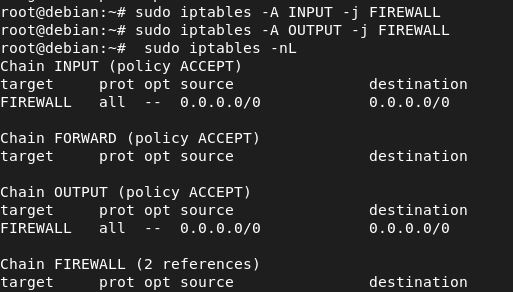
Con –F se quitan las reglas actualmente aplicadas.



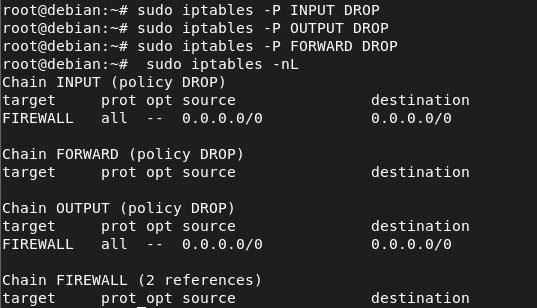
-N para crear una nueva cadena llamada FIREWALL



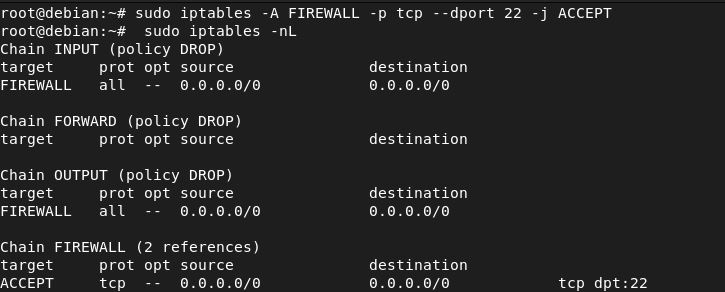
Los paquetes de INPUT y OUTPUT se redirigen con –A a FIREWALL



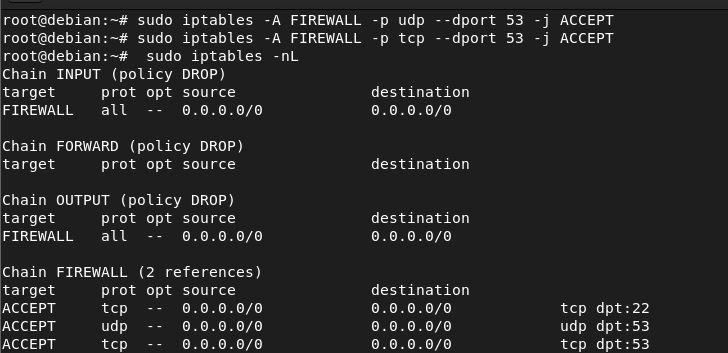
Con DROP a las tablas anteriormente establecidas se restringe la red del servidor, para poder modificar la nueva cadena.



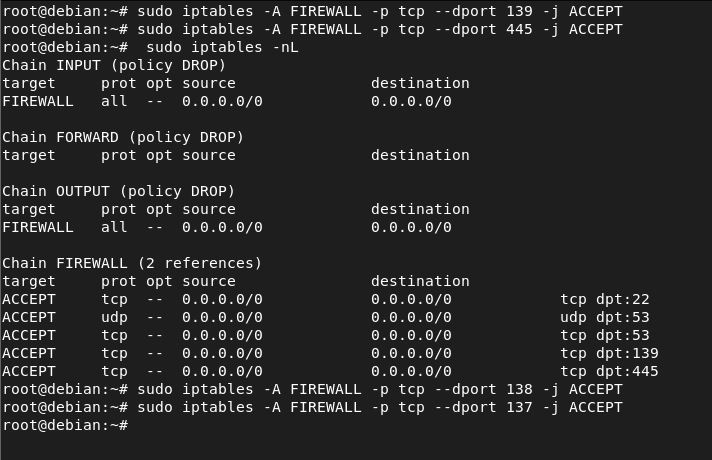
Se permite el tráfico en el puerto 22, el cual sirve para la conexión SSH.



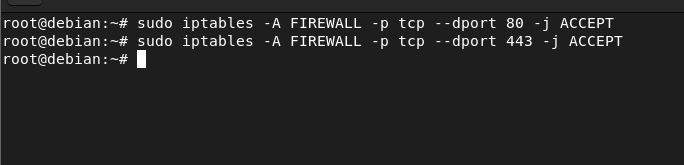
Se habilita el puerto53 para la conexión del DNS.



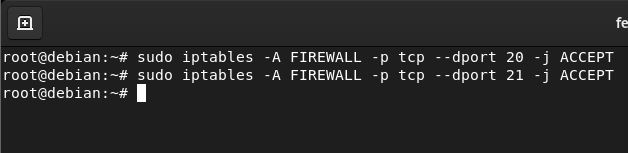
Los puertos 139 y 445 sirven para permitir los servicios de SAMBA



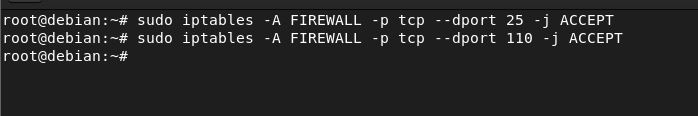
Los puertos 80 y 443 se habilitan para permitir el acceso al sitio web.



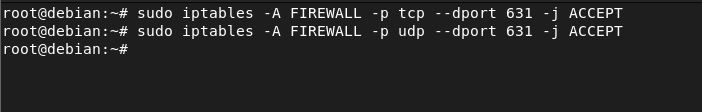
Los puertos 20 y 21 tienen la función de acceder a los sitios de FTP



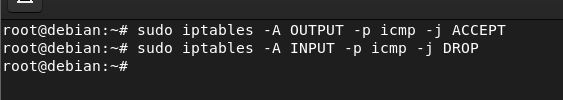
Para acceder a los servicios de correo se requieren de los puertos 25 y 110



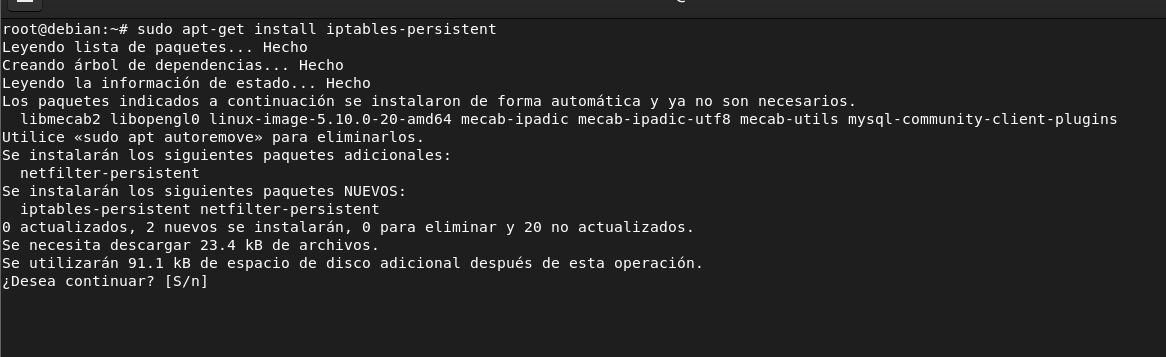
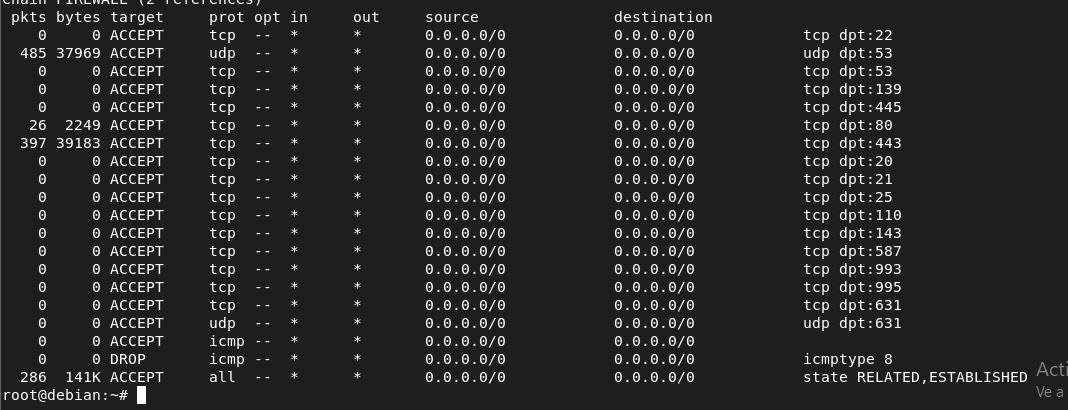
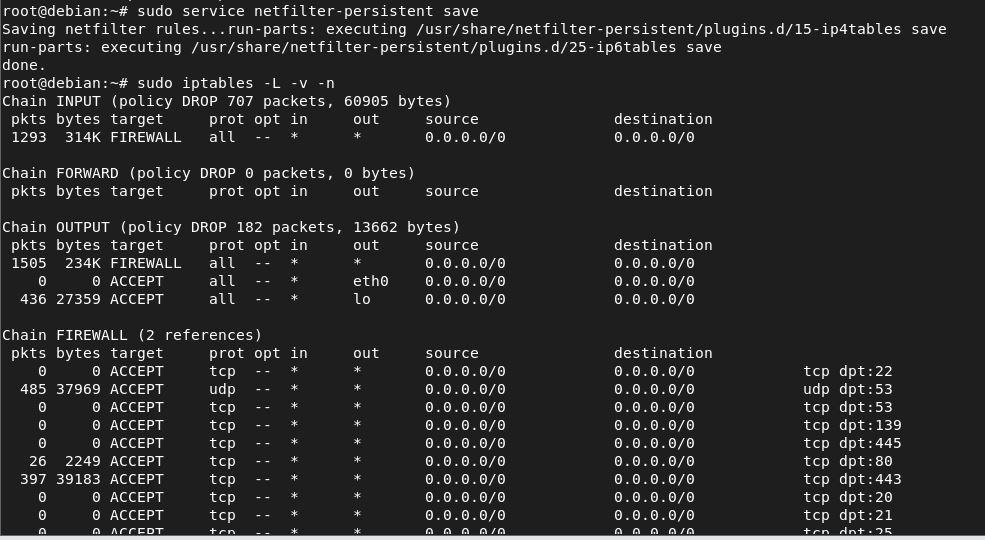
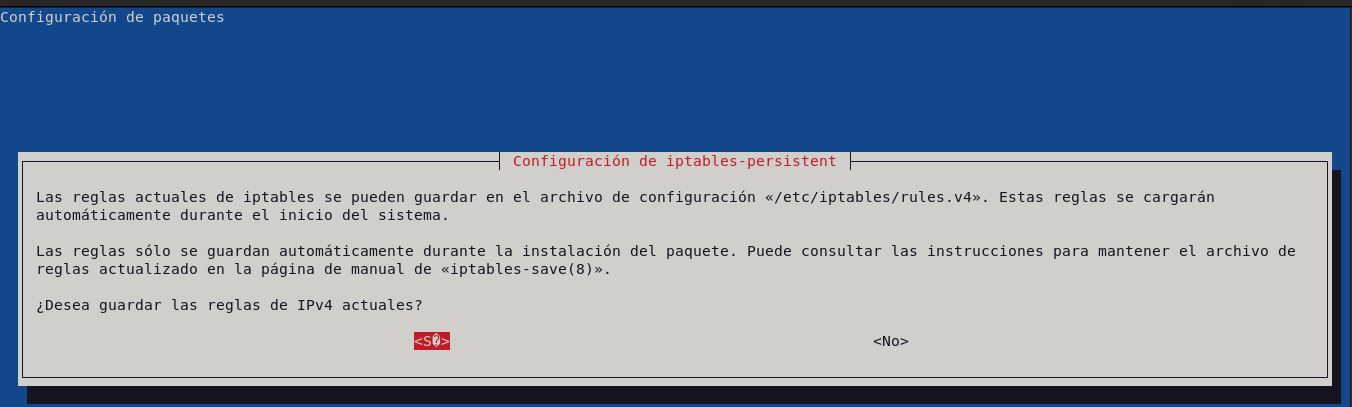
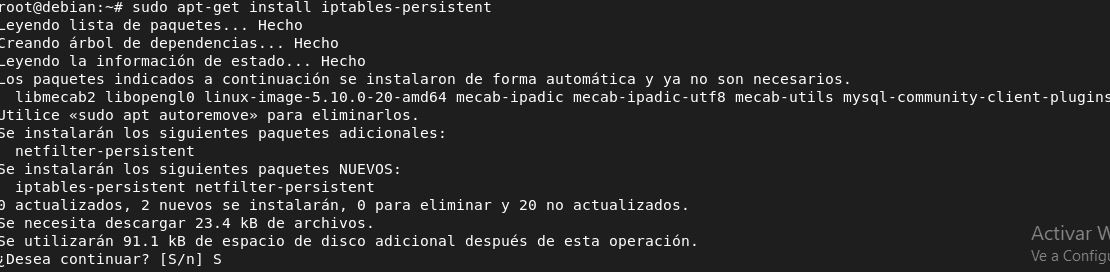
Para el servicio de impresión se necesita habilitar el puerto 631.



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.

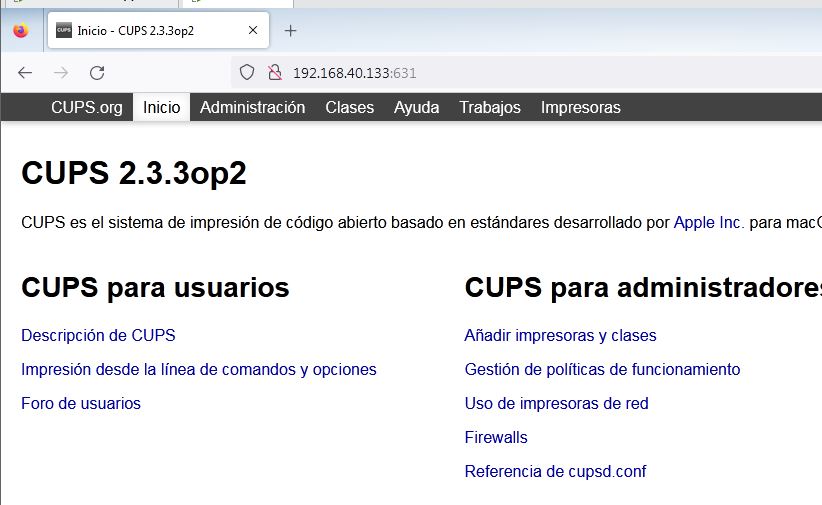


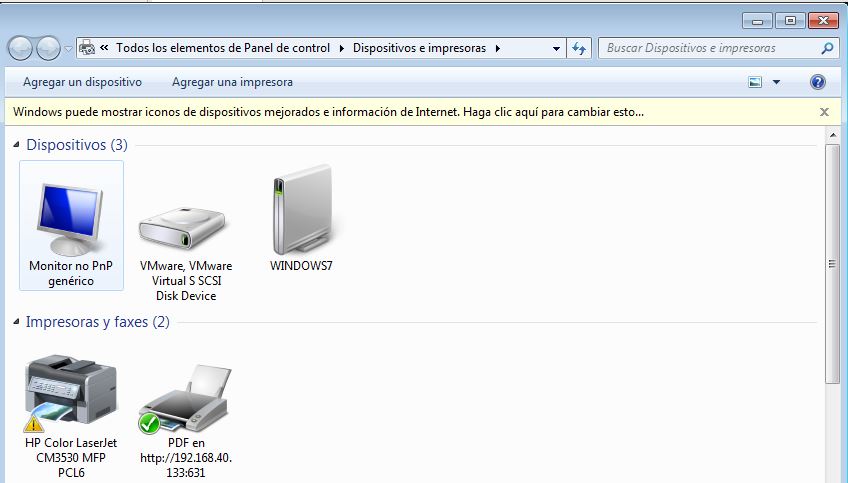
Con esto se guardan las reglas de manera permanente y al final se muestran las reglas aplicadas en el servidor.

C:\Users\Alma Salazar\Downloads\r14-.JPG

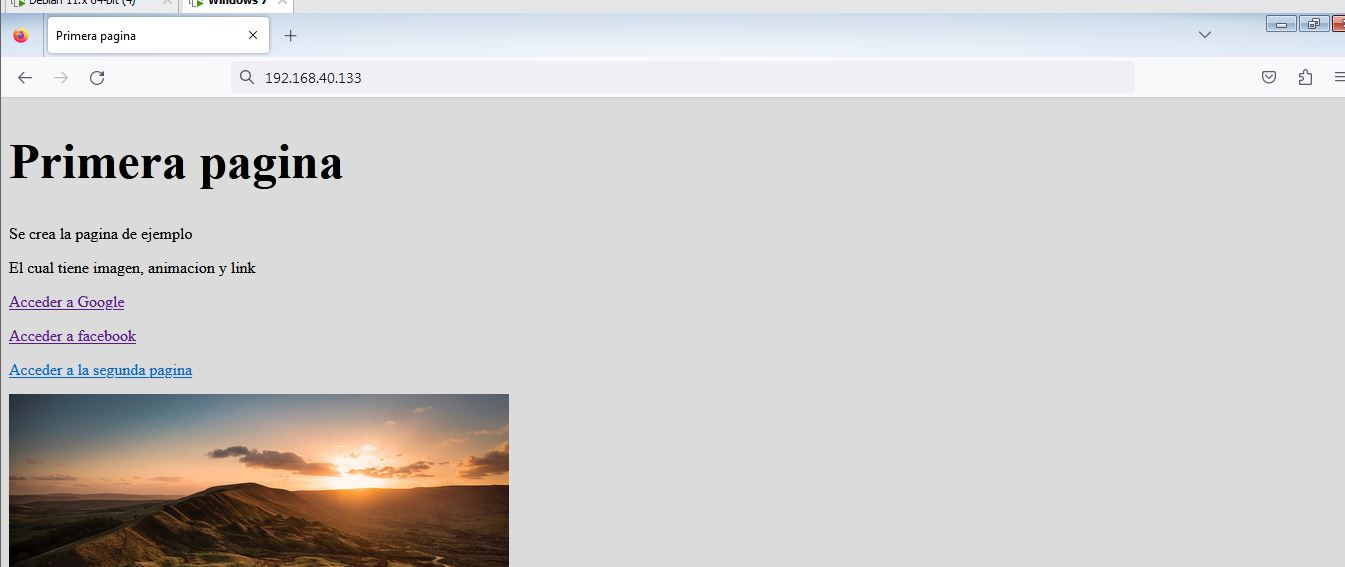
Reglas aplicadas con el comando iptables -L -v –n

Algunas reglas aplicadas, como el servicio de impresora

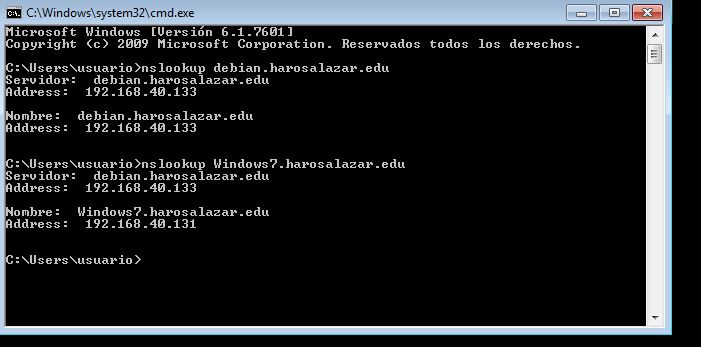




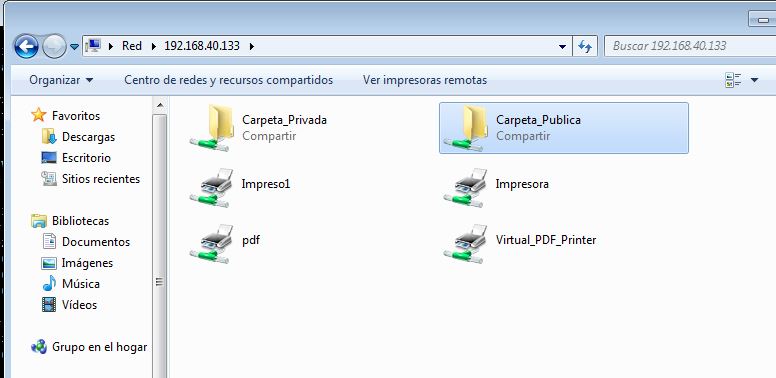
Servicio web



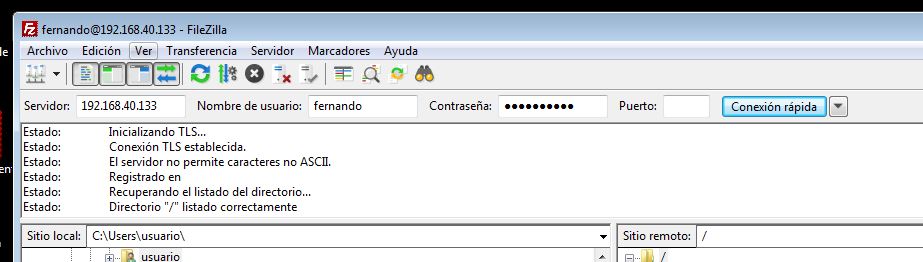
DNS y SSH



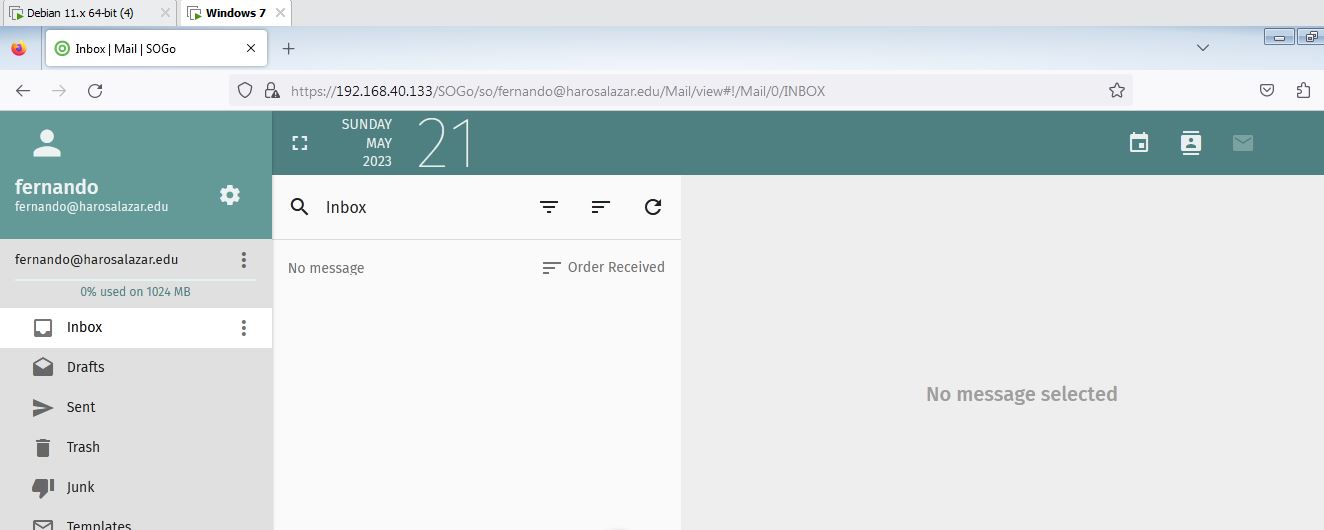
samba



ftp



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.