



Administración de servidores

D05

Vi-Sa 7-9 Hrs

José de Jesús Soto Sánchez



### Actividad 3 – SSH

Centro Universitario de Ciencias Exactas e Ingenierías

Universidad de Guadalajara

2023A

En la presente actividad 3, se desarrollará e implementará el protocolo SSH en el servidor Linux Debian anteriormente desarrollado, dentro de la máquina virtual de Debian y la máquina virtual de Windows debe ser posible la conexión de una máquina a otra, con ese fin se modifican e implementan comandos dentro del servidor de Linux con el propósito de que el protocolo SSH funcione para el intercambio de datos entre el host y el cliente.

¿Qué es SSH?

El protocolo SSH (Secure Shell o Secure Socket Shell), como su nombre lo indica es útil para mantener una conexión segura con un servidor remoto. Es un protocolo de seguridad, puesto que la conexión donde se transfieren los datos por parte del cliente y del host se debe realizar de manera encriptada. El proceso se lleva a cabo a través del puerto TCP/IP transfiriendo las entradas del cliente al host y devuelve la salida del host.

Componentes de SSH

Comando: Dirige la instrucción al equipo para crear la conexión con el host.

Nombre de usuario: Debe ser la misma usada dentro de Linux

Host: En este caso es la máquina a la cual se puede acceder por medio de un cliente, es decir el servidor.

¿Cómo funciona?

Se necesita el cliente y el host, que debe ser el servidor al cual se debe conectar, para entablar la conexión encriptada el cliente debe ingresar la información especificada dentro del servidor. Mientras que el Host contiene el proceso SSH el cual está disponible cuando el cliente solicite la conexión por medio del puerto TCP/IP, una vez establecida la conexión entre el servidor y el cliente, el host responde con información e intercambio de credenciales. (Javapoint, 2023)

Breve historia

El SSH fue creado en 1995 por Tatu Ylonen, este protocolo se creó con la finalidad de prevenir ataques referentes a la detección de las contraseñas, ocurriendo en la universidad tecnológica de Helsinki, diseñando versiones del protocolo SSH que tenía la finalidad de sustituir protocolos con poca fiabilidad como lo era rsh, rlogin y telnet, iniciando como protocolo gratuito y que pasó a ser de propietario, posteriormente se

desarrolla el sucesor del protocolo para convertirse en el estándar, con sus respectivas mejoras para el intercambio de contraseñas.

## Usos

Su uso principal es brindar la administración segura, acceso remoto y parches dentro de un centro de datos

Permite la administración y mantenimiento de la plataforma virtual

Conexión con un host remoto

Copia de seguridad y duplicados de archivos

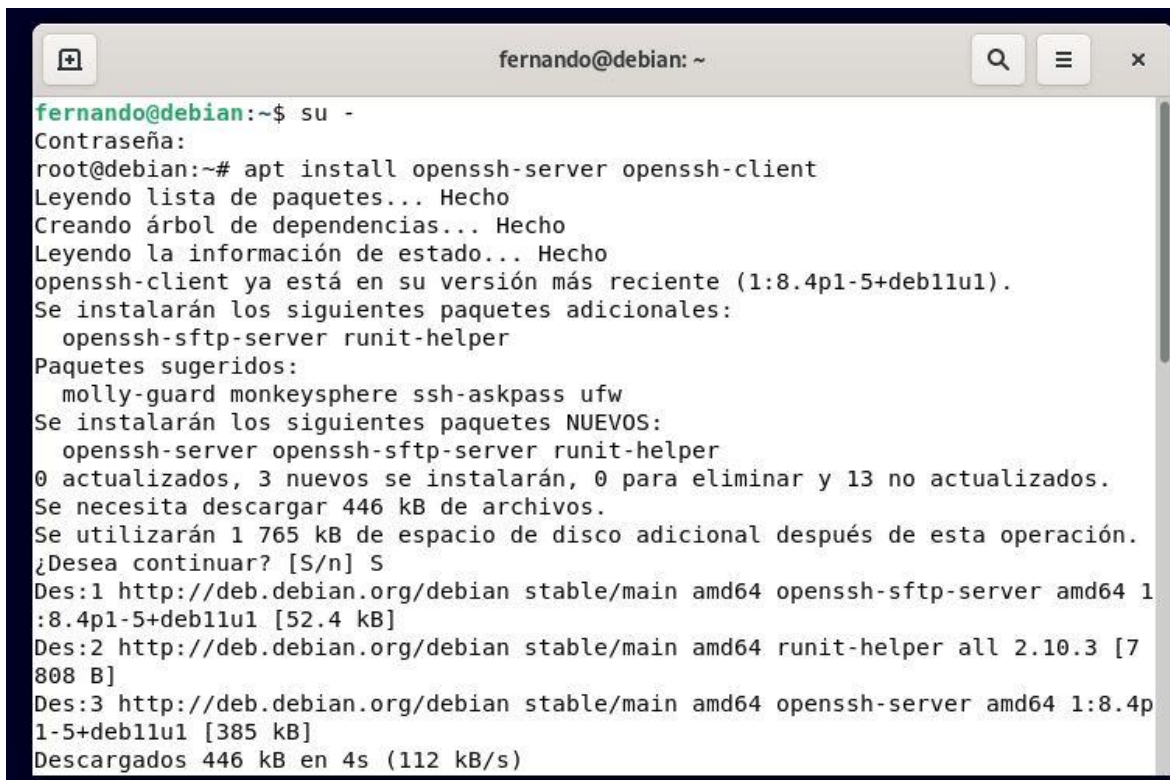
Asigna puerto del cliente para conectar al puerto del servidor

Transporte de datos encriptados por medio de un canal seguro

Utiliza una red virtual privada

(Aleksic, 2021)

Dentro de la terminal de Linux, después de ingresar como super usuario, se ingresa apt install para instalar el servicio de SSH y se espera hasta que se instale.

A terminal window titled 'fernando@debian: ~' with search, menu, and close buttons in the title bar. The terminal shows the command 'su -' being executed, followed by 'apt install openssh-server openssh-client'. The output shows the package list being read, dependencies being created, and the state information being read. It then lists the packages to be installed: openssh-sftp-server and runit-helper. It also lists suggested packages: molly-guard, monkeysphere, ssh-askpass, and ufw. The user is asked if they want to continue, and they respond with 'S'. The terminal then shows the download progress for the three packages, including their sources, architectures, versions, and sizes. Finally, it shows that 446 kB were downloaded in 4 seconds at a speed of 112 kB/s.

```
fernando@debian:~$ su -
Contraseña:
root@debian:~# apt install openssh-server openssh-client
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
openssh-client ya está en su versión más reciente (1:8.4p1-5+deb11u1).
Se instalarán los siguientes paquetes adicionales:
  openssh-sftp-server runit-helper
Paquetes sugeridos:
  molly-guard monkeysphere ssh-askpass ufw
Se instalarán los siguientes paquetes NUEVOS:
  openssh-server openssh-sftp-server runit-helper
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 13 no actualizados.
Se necesita descargar 446 kB de archivos.
Se utilizarán 1 765 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
Des:1 http://deb.debian.org/debian stable/main amd64 openssh-sftp-server amd64 1:8.4p1-5+deb11u1 [52.4 kB]
Des:2 http://deb.debian.org/debian stable/main amd64 runit-helper all 2.10.3 [7808 B]
Des:3 http://deb.debian.org/debian stable/main amd64 openssh-server amd64 1:8.4p1-5+deb11u1 [385 kB]
Descargados 446 kB en 4s (112 kB/s)
```

Dentro de nato se edita el archivo /etc/ssh/sshd\_config para configurar el servicio

instalado

```
fernando@debian: ~
Desempaquetando openssh-server (1:8.4p1-5+deb11u1) ...
Configurando runit-helper (2.10.3) ...
Configurando openssh-sftp-server (1:8.4p1-5+deb11u1) ...
Configurando openssh-server (1:8.4p1-5+deb11u1) ...

Creating config file /etc/ssh/sshd_config with new version
Creating SSH2 RSA key; this may take some time ...
3072 SHA256:PAQkXQjJLByXIU7vHhzToZ/97GDbAdd/UHLFFl4wpzc root@debian (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:J3708nVLpMnH5aInQnW0a5yHEQ1yM5ZoelI2uyZ21lw root@debian (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:VZ4lAt0eTbWMxhP9rIw8aS0vx03DYZakvHVWz0R3MoA root@debian (ED25519)
Created symlink /etc/systemd/system/ssh.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
Procesando disparadores para man-db (2.9.4-2) ...
root@debian:~#
root@debian:~#
root@debian:~#
root@debian:~#
root@debian:~# nano /etc/ssh/sshd_config
```

Dentro del archivo se modifica la dirección de escucha con la IP del usuario, se habilita el puerto 22 y se usa la versión 2 del protocolo para manejar la encriptación de 256 bits.

```
fernando@debian: ~
GNU nano 5.4 /etc/ssh/sshd config
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file. See
# sshd config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa key
[ 123 líneas leídas ]
^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación
^X Salir      ^R Leer fich. ^\ Reemplazar ^U Pegar      ^J Justificar ^_ Ir a línea
```

```
fernando@debian: ~
GNU nano 5.4 /etc/ssh/sshd_config *
# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
ListenAddress 192.168.40.133
Protocol 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying

^G Ayuda      ^O Guardar    ^W Buscar    ^K Cortar    ^T Ejecutar   ^C Ubicación
^X Salir      ^R Leer fich.^N Reemplazar ^U Pegar     ^J Justificar ^_ Ir a línea
```

Se eliminan las contraseñas vacías, además de establecer tiempo de espera para introducir la contraseña, se deshabilita la autenticación por root, se habilita el número de intentos y limita el número de sesiones, además de agregar el usuario que puede acceder al SSH

```
fernando@debian: ~
GNU nano 5.4 /etc/ssh/sshd_config *
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#
PermitEmptyPasswords no
```



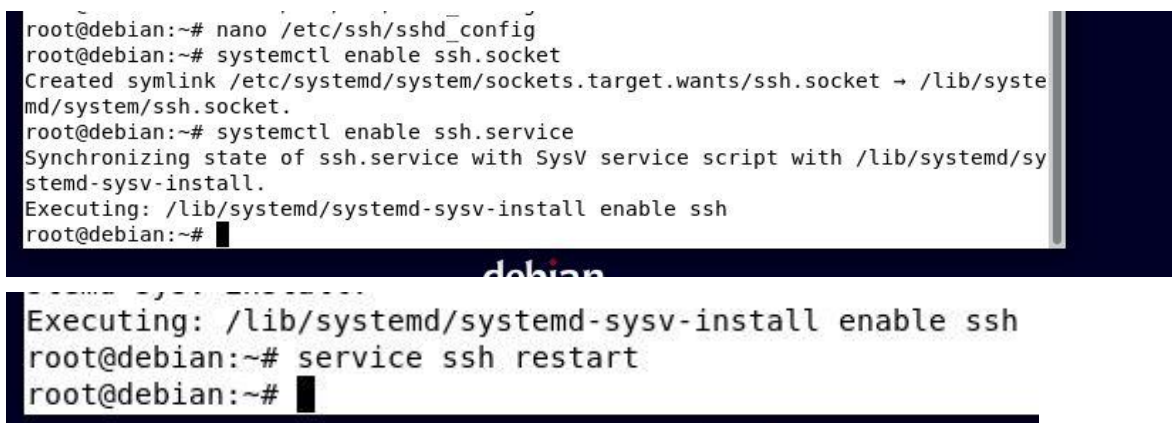
```
fernando@debian: ~
GNU nano 5.4 /etc/ssh/sshd_config *
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

LoginGraceTime 30
PermitRootLogin prohibit-password
#StrictModes yes
MaxAuthTries 3
MaxSessions 2
AllowUsers fernando
#PubkeyAuthentication yes
```

Con las siguientes instrucciones se activa el inicio automático, y se reinicia el servidor con el comando restart.

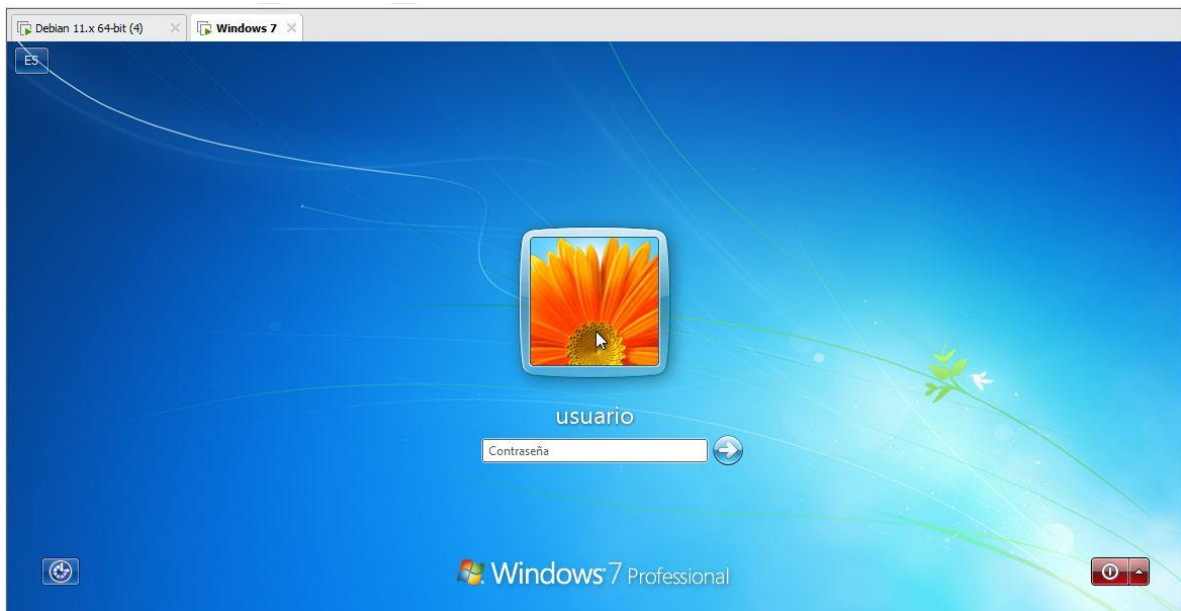


```
root@debian:~# nano /etc/ssh/sshd_config
root@debian:~# systemctl enable ssh.socket
Created symlink /etc/systemd/system/sockets.target.wants/ssh.socket → /lib/systemd/system/ssh.socket.
root@debian:~# systemctl enable ssh.service
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
root@debian:~#

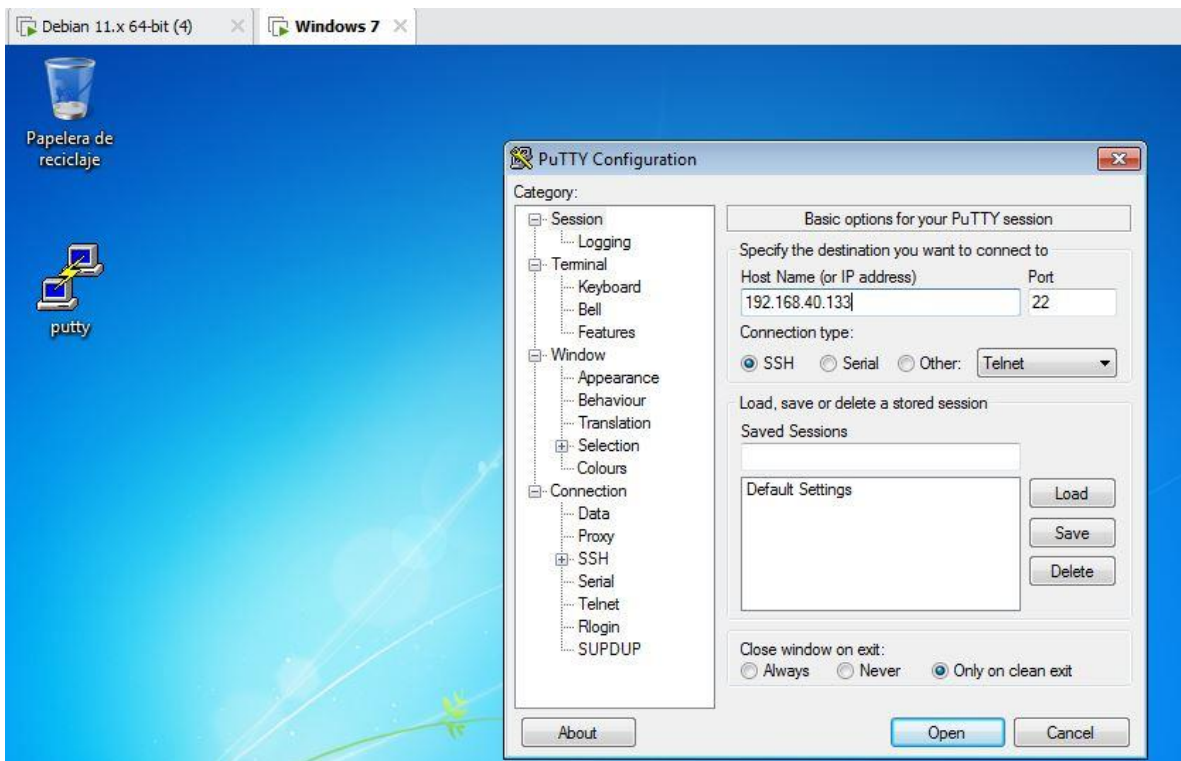
root@debian:~# service ssh restart
root@debian:~#
```

Ingresamos a la otra máquina virtual de Windows.



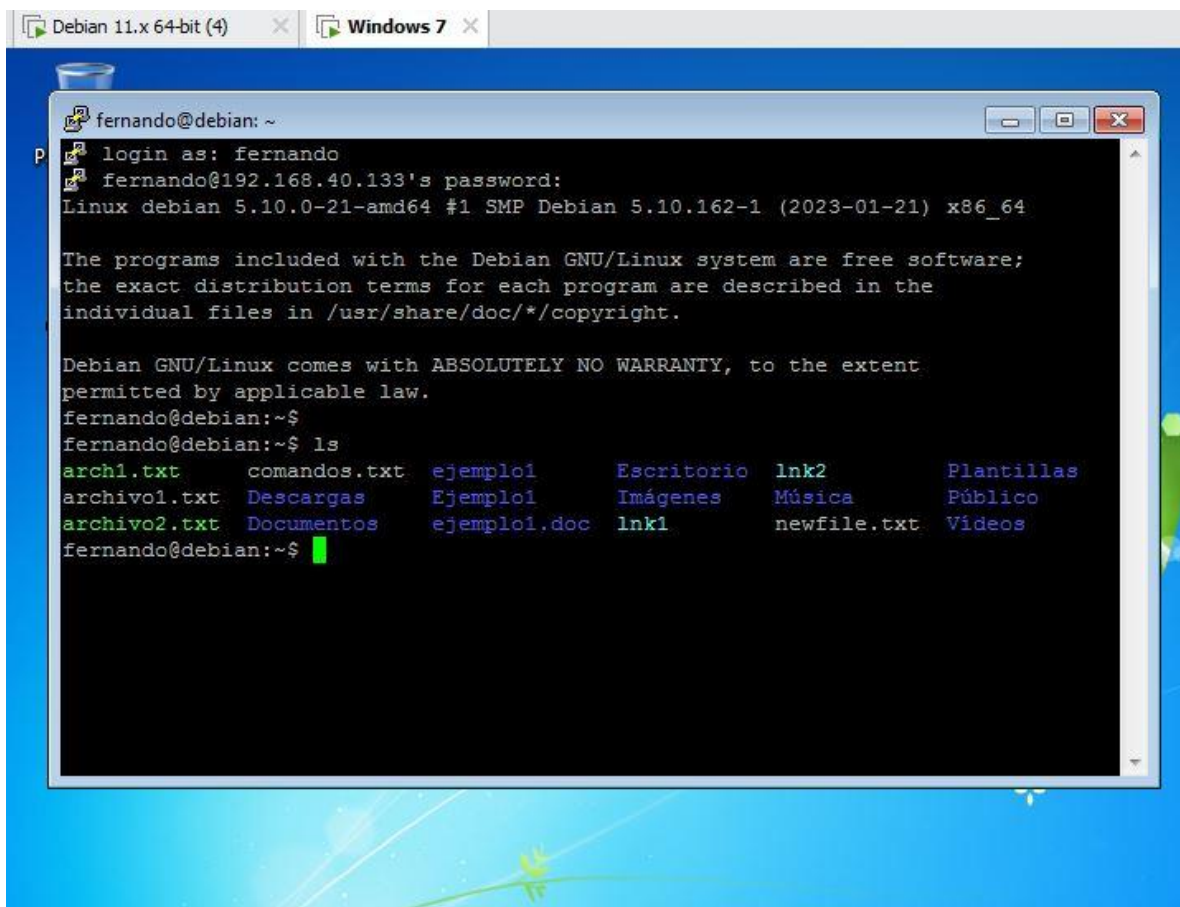
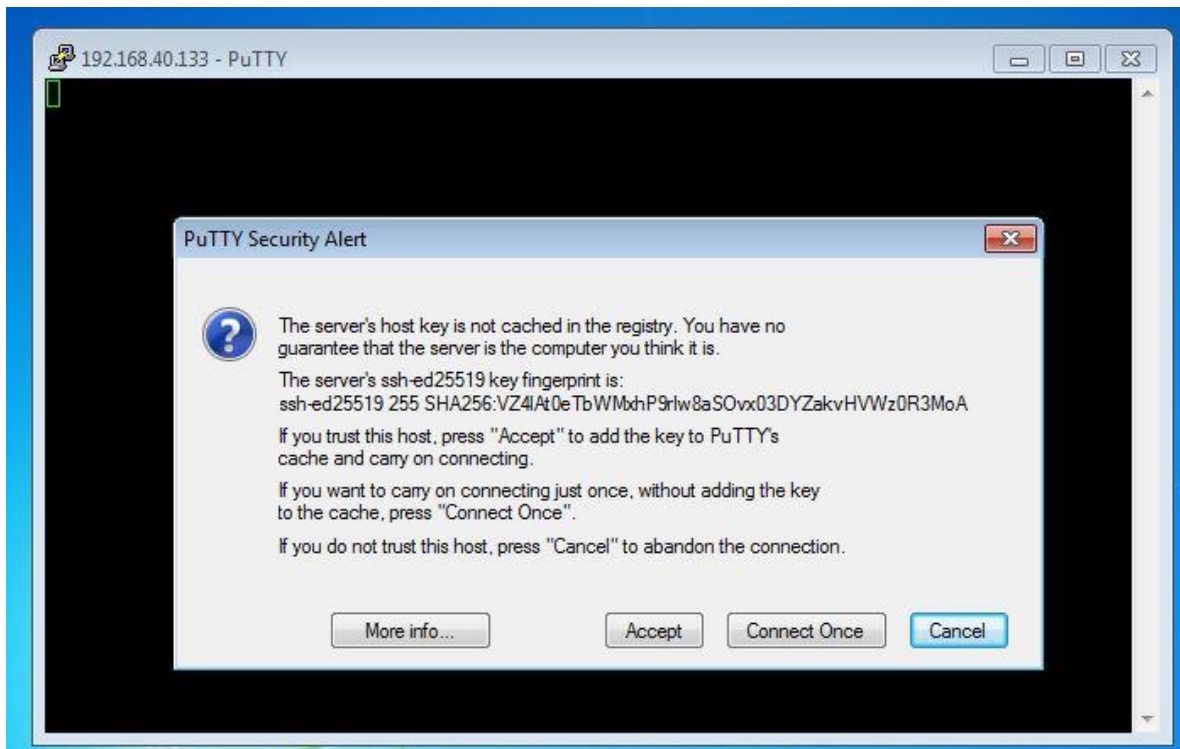


Por medio del programa putty se accede remotamente al servidor con el puerto, IP y protocolo configurado.



Se acepta la conexión, y para iniciar la sesión remota se proporcionan los datos confirmados en el debian.





```
fernando@debian: ~  
fernando@debian:~$ ls  
arch1.txt      comandos.txt  ejemplo1     Escritorio   lnk2          Plantillas  
archivo1.txt   Descargas    Ejemplo1     Imágenes    Música         Público  
archivo2.txt   Documentos   ejemplo1.doc lnk1         newfile.txt   Vídeos  
fernando@debian:~$ mkdir archivodesdeputty  
fernando@debian:~$ ls  
arch1.txt      comandos.txt  Ejemplo1     lnk1          Plantillas  
archivo1.txt   Descargas    ejemplo1.doc lnk2          Público  
archivo2.txt   Documentos   Escritorio    Música        Vídeos  
archivodesdeputty ejemplo1     Imágenes     newfile.txt  
fernando@debian:~$ nano ejemploputty.txt  
fernando@debian:~$ ls  
arch1.txt      comandos.txt  Ejemplo1     Imágenes     newfile.txt  
archivo1.txt   Descargas    ejemplo1.doc lnk1          Plantillas  
archivo2.txt   Documentos   ejemploputty.txt lnk2         Público  
archivodesdeputty ejemplo1     Escritorio    Música        Vídeos  
fernando@debian:~$
```

Como se muestra el protocolo instalado y desarrollado cumple la función de permitir la transmisión de datos seguros entre el cliente de una computadora lejana con el servidor virtual remoto, en este canal nosotros podemos modificar de la misma manera en la que se hace en Linux, como ejemplo se agregó un fichero y archivo txt dentro del usuario.

## Conclusión

La tercera actividad presentada y desarrollada dentro de clase, así como investigada para comprenderla mejor, fue una práctica directamente trabajando el protocolo de SSH usada por varios servidores alrededor del mundo, que tienen como fin el establecimiento desde un cliente a un servidor, ya se desarrolló la idea principal del protocolo el cual era la conexión encriptada entre usuario y host, sin embargo en la práctica se estudió su funcionamiento así como su implementación en el servidor Linux siendo uno de los primeros servicios del servidor que se está construyendo, además se vio como el servicio puede ser configurado para que este actúe de la manera en que nosotros como usuarios queramos que funcionen, dentro de la actividad vimos como añadir usuarios o eliminarlos para que estos entren o no, además de cómo poner contraseñas, y la contraseña al ser una parte importante para entrar al servidor se pueden limitar los intentos al ingresar la contraseña, así como un tiempo y sesiones limitadas para que terceros y usuarios no deseados ingresen al servidor por medio de la fuerza bruta, siendo todos estos procesos de configuración realizados dentro de la terminal debido a que Linux funciona por comandos y sus configuraciones o instalaciones deben realizarse ahí mismo, es por ello que se accede al archivo de configuración del servicio SSH y se modifican parámetros, se habilitan o deshabilitan líneas de comando y se configura el usuario deseado que puede entablar el intercambio de datos, este intercambio se realiza con la otra máquina virtual instala, la cual es Windows, debido a que no muchas personas usan Linux se intenta conectar mediante el putty de Windows, el cual es un programa que es una terminal de simulación para actuar de cliente de conexiones seguras al acceso remoto a los servidores, es un programa que debe ingresar los datos establecidos en la configuración de Linux para que este ingrese a la máquina virtual de Linux.

## Bibliografía

Aleksic, M. (22 de 9 de 2021). *phoenixnap*. Obtenido de phoenixnap.com:

<https://phoenixnap.com/kb/what-is-ssh>

Javapoint. (01 de 03 de 2023). *javatpoint*. Obtenido de www.javatpoint.com:

<https://www.javatpoint.com/ssh-linux>