Centro Universitario de Ciencias Exactas e Ingenierías

Administración de Servidores

Configuración SSH

Introducción

SSH (Secure Shell) es un protocolo de red criptográfico utilizado para asegurar la comunicación entre dos máquinas en una red. Permite realizar conexiones remotas de manera segura a través de una red no segura, como internet. SSH proporciona autenticación robusta y cifrado de los datos transmitidos, lo que protege la integridad y la confidencialidad de la comunicación.

Usos de SSH:

1. **Acceso remoto a servidores:** SSH permite a los administradores y desarrolladores acceder y controlar de manera remota servidores o máquinas en diferentes ubicaciones. Por ejemplo, un administrador puede conectarse a un servidor Linux desde su computadora local para gestionar archivos o ejecutar comandos en el servidor.
2. **Transferencia segura de archivos:** SSH incluye herramientas como SCP (Secure Copy) y SFTP (SSH File Transfer Protocol), que permiten transferir archivos entre un servidor y una máquina local de manera segura.
3. **Túneles SSH:** SSH permite crear túneles seguros (SSH tunneling) para redirigir el tráfico de una aplicación a través de una conexión SSH cifrada. Esto es útil para acceder a servicios detrás de un firewall o para asegurar conexiones de aplicaciones que no tienen encriptación por sí mismas.
4. **Autenticación por claves públicas:** SSH permite el uso de pares de claves públicas y privadas para autenticar a los usuarios sin necesidad de contraseñas, lo que aumenta la seguridad al evitar ataques de fuerza bruta o interceptación de contraseñas.
5. **Gestión remota de redes:** SSH es ampliamente utilizado para configurar y gestionar dispositivos de red como routers, switches, y firewalls de manera remota.

Desarrollo

Para Configurar el SSH de manera exitosa relicé los siguientes pasos en mi terminal de Debian de mi máquina virtual

```
juan@rambo:~$ su
Contraseña:
root@rambo:/home/juan# apt install openssh-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
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 0 no actualizados.
Se necesita descargar 528 kB de archivos.
Se utilizarán 2 214 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

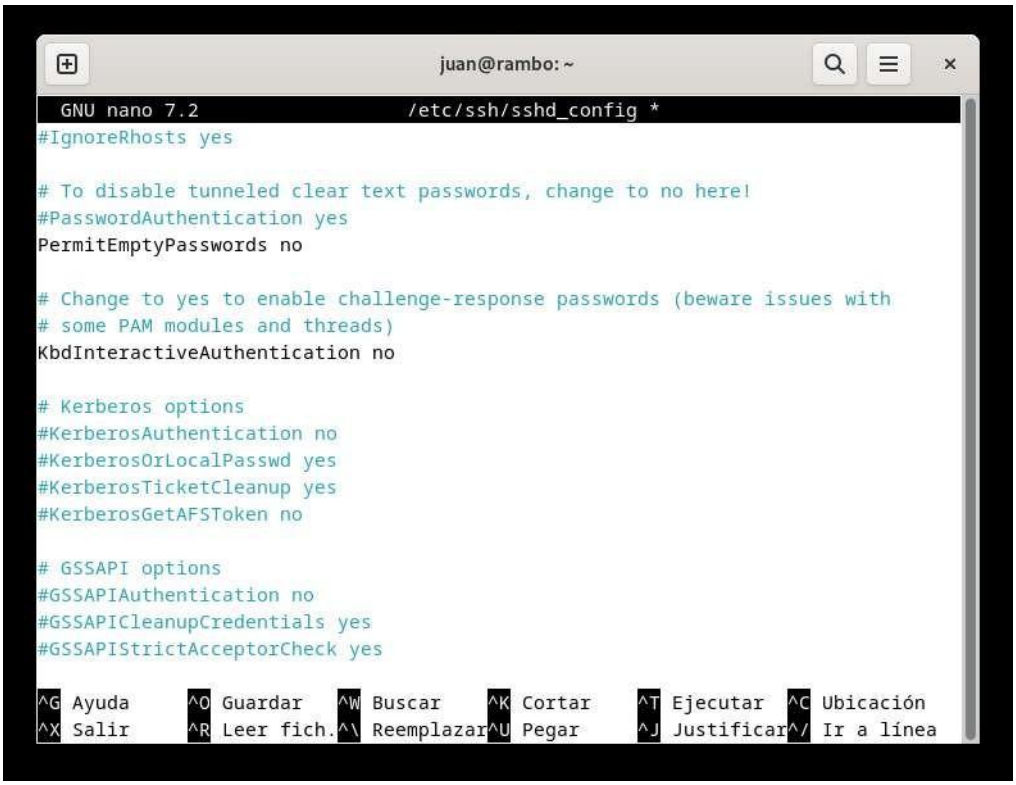
En primera instancia al abrir la terminal nos movemos al perfil del super usuario para poder instalar desde ahí el servidor ssh con el comando apt install openssh-server y se tiene que ver como se muestra en la imagen.

```
  GNU nano 7.2                  /etc/ssh/sshd_config *
# sshd_config(5) for more information.

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

# 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 192.168.1.89
Protocol 2
```

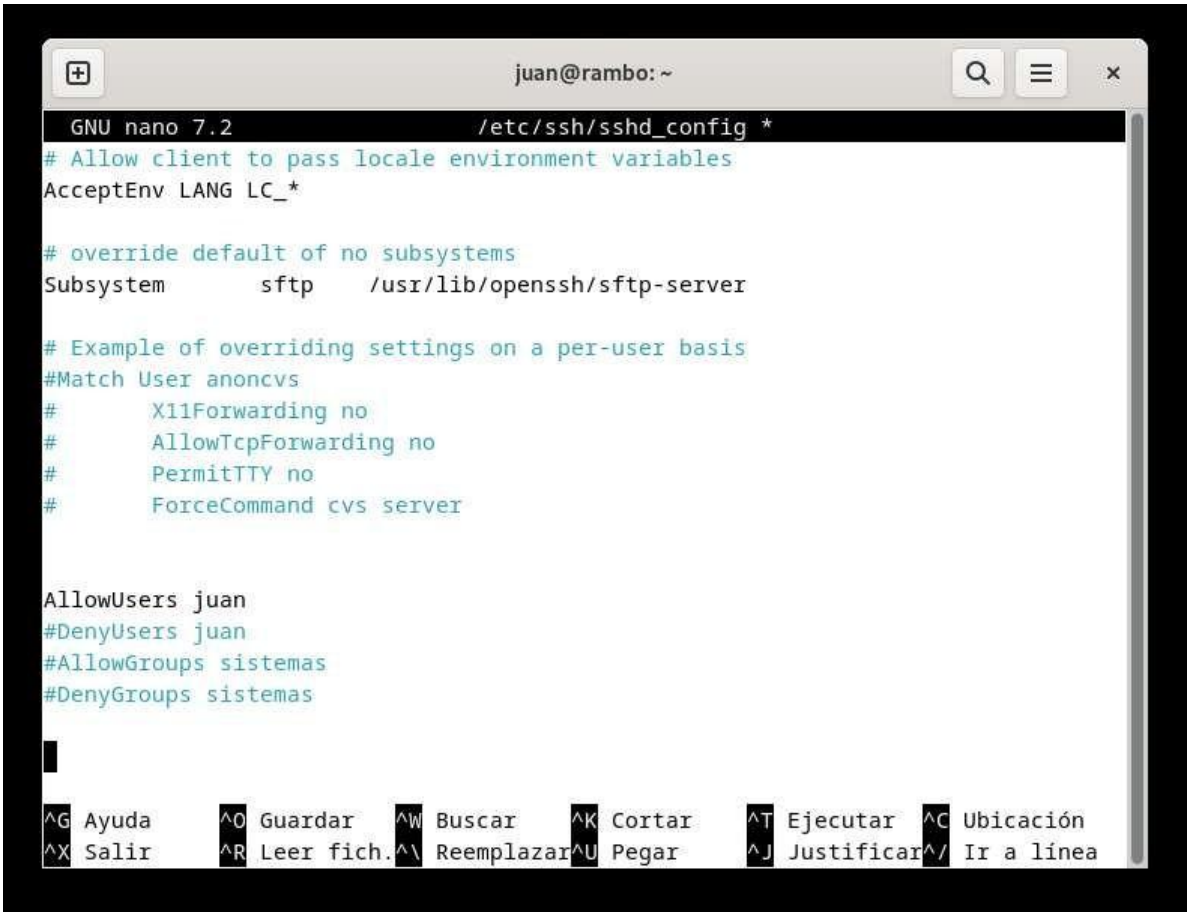
Después de instalar el servicio accedemos a un archivo en el editor de texto nano con el siguiente comando nano /etc/ssh/sshd_config una vez aquí realizamos una serie de configuraciones y en este caso habilitamos el puerto 22, la dirección IP de nuestra máquina con el ListenAddress seguido de la dirección IP y activamos el protocolo 2 con Protocol 2.

```
 GNU nano 7.2                    /etc/ssh/sshd_config *

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

LoginGraceTime 30
PermitRootLogin prohibit-password
StrictModes yes
MaxAuthTries 3
MaxSessions 5

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
```

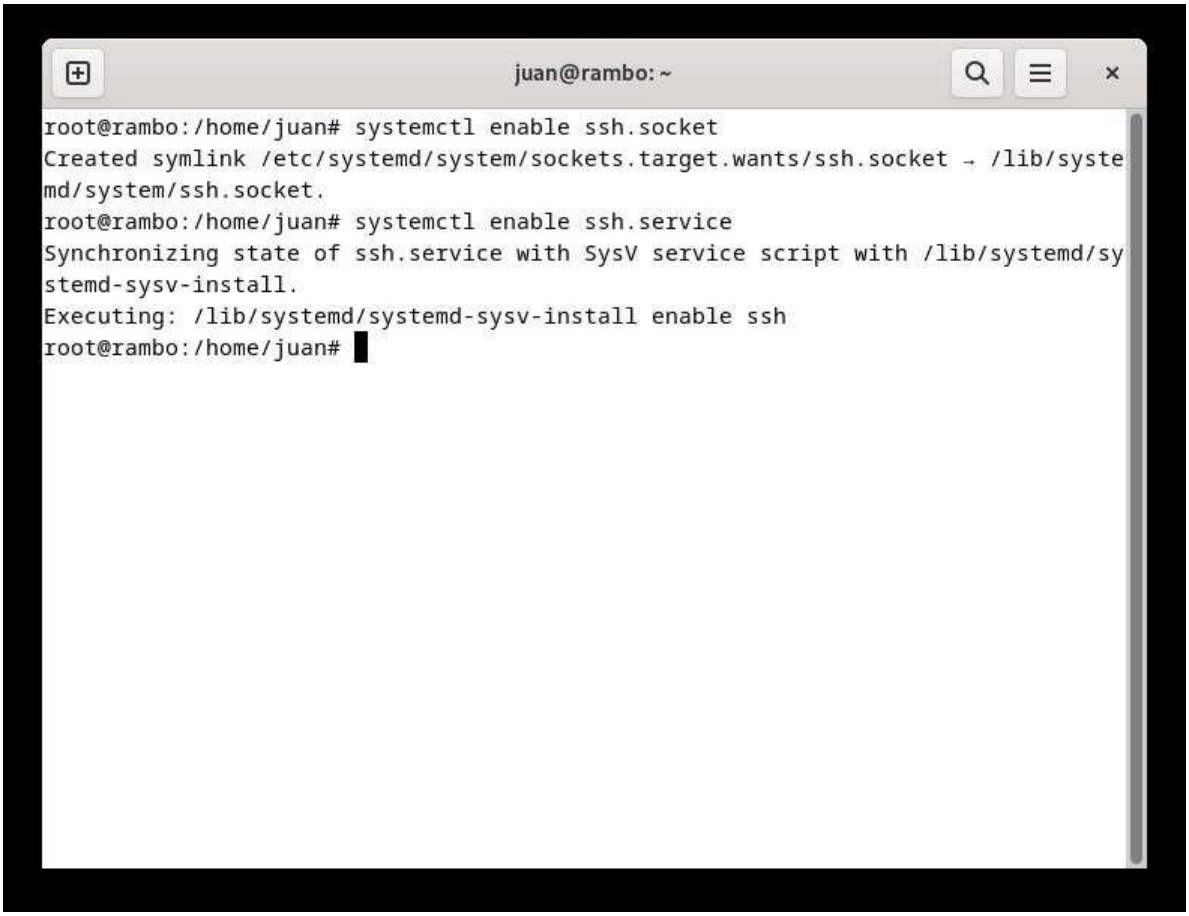
En el apartado de autentificación editamos todos los comandos como se muestran en pantalla.



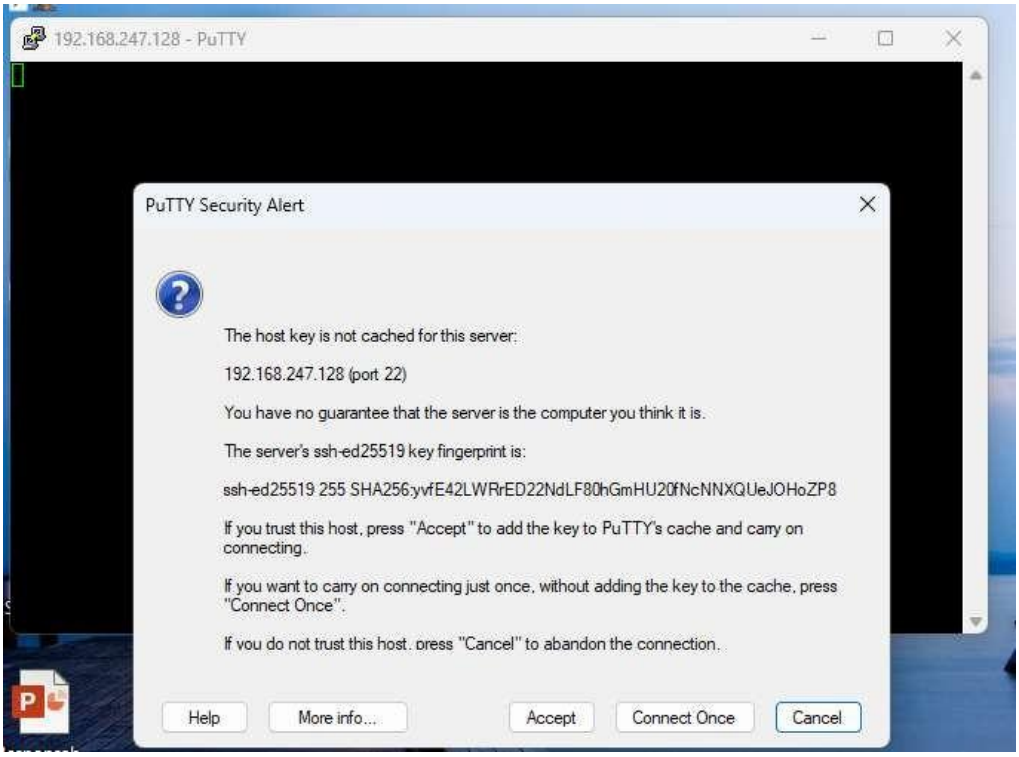
Aquí quitamos el comentario a las líneas que están en color negro como se muestra en la imagen.



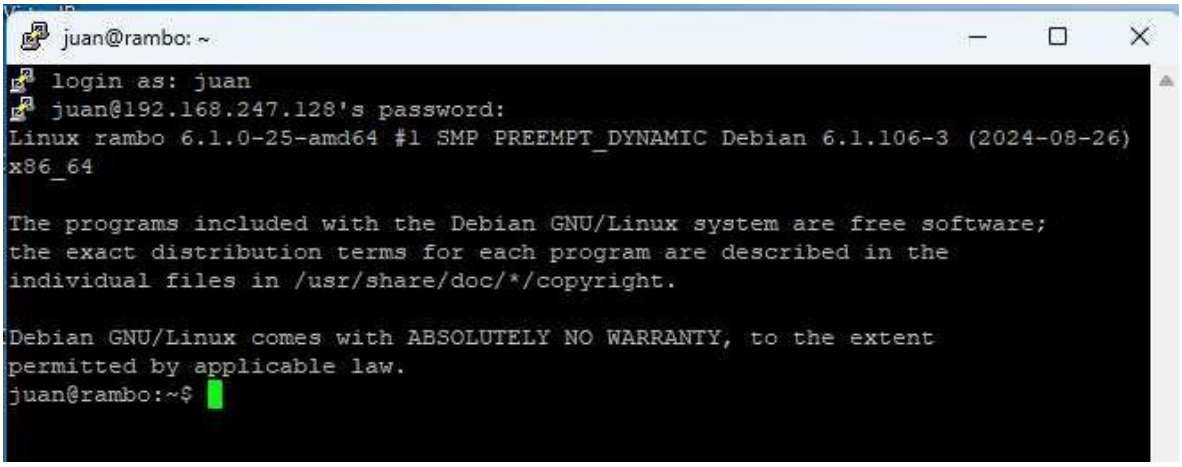
A los usuarios permitidos ponemos nuestro nombre de usuario, que en mi caso es juan , después guardamos los cambios realizados en el archivo con ctrl o y enter. Después salimos del archivo con ctrl x.



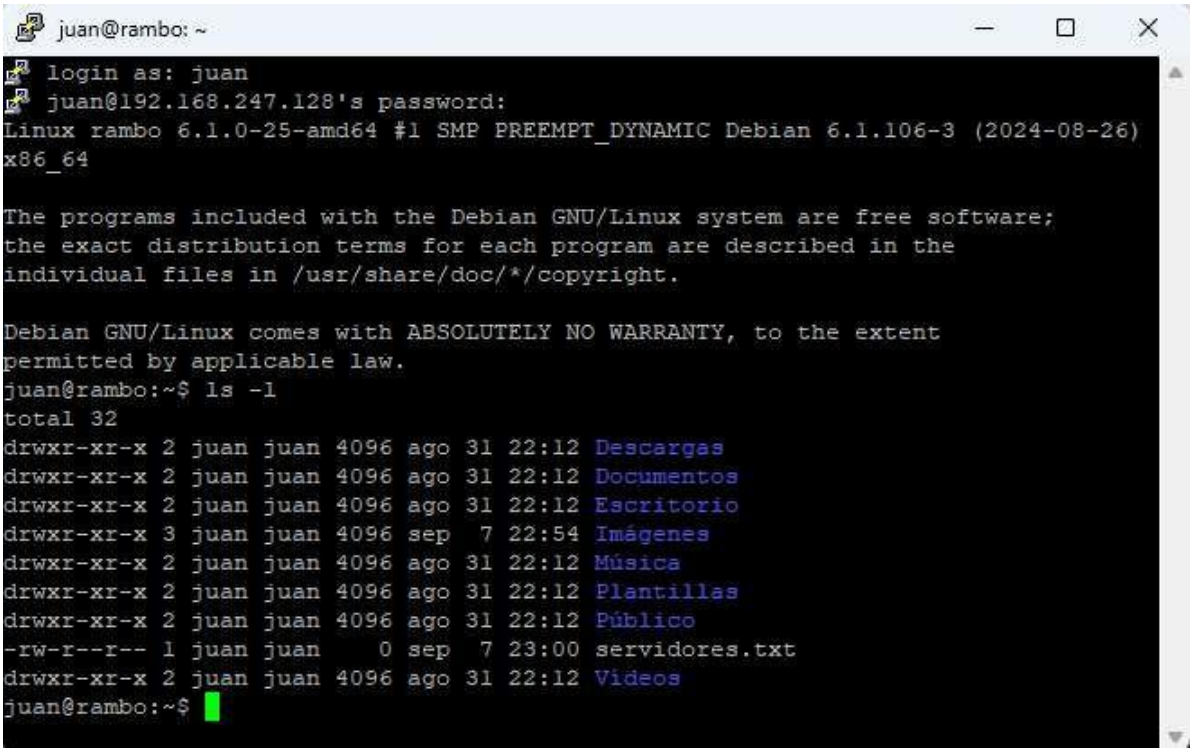
Una vez que salimos del nano, en la terminal ponemos el comando systemctl enable ssh.socket y después systemctl enable ssh.service y se tiene que ver como en pantalla, después tenemos que reiniciar el servicio con el comando reboot para finalizar la instalación del ssh.



Después de realizar todo lo anterior, nos vamos a una máquina de Windows para descargar ahí el putty donde probaremos si el SSH realmente se configuró correctamente, luego tendremos que introducir la dirección IP que guardamos en el archivo del nano, nos aseguramos que se encuentre en el puerto 22 y que se encuentre activado el SSH, una vez hecho esto le damos en open y nos aparecerá una ventana como la que se muestra en pantalla donde tendremos que dar click en la opción aceptar.



A continuación en login as ponemos el usuario que habilitamos en el nano que en este caso fue juan y en password ponemos la contraseña con la que iniciamos sesión en nuestra máquina virtual de debian. Si todo sale bien se tiene que mirar como se muestra en pantalla.



A continuación haremos la prueba del SSH con el comando ls -l y si al dar enter salen una serie de carpetas y/o archivos como se muestra en el ejemplo anterior quiere decir que nuestro SSH se configuró correctamente y sin problemas.

Conclusiones

El SSH es un servicio que nos ayuda a establecer comunicación en dos máquinas de manera remota por seguridad por ejemplo, pero cabe resaltar que durante la realización de esta práctica tuve una serie de problemas que no podía resolver, pues al querer reiniciar el SSH con el comando reboot o service ssh restart la consola no me leía ninguno de los dos y después de estar indagando las posibles razones me di cuenta que fue porque en el archivo config puse la dirección IP equivocada pero una vez que la pude corregir todo salió como lo esperé desde un principio.