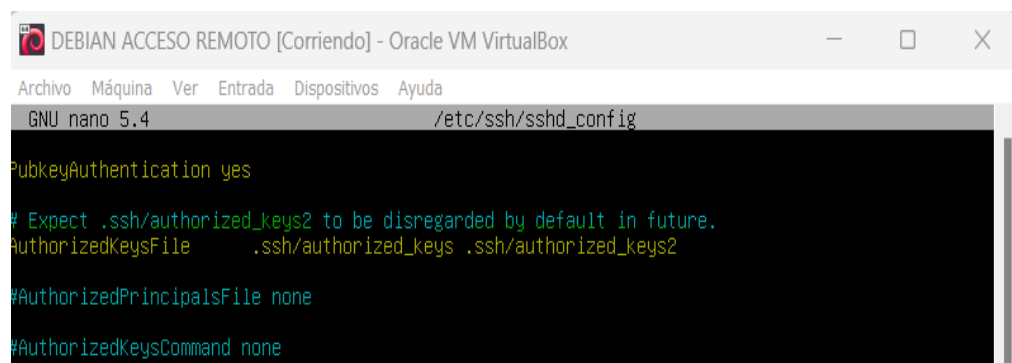


EJERCICIO DE CLASE (SERVIDOR DEBIAN)

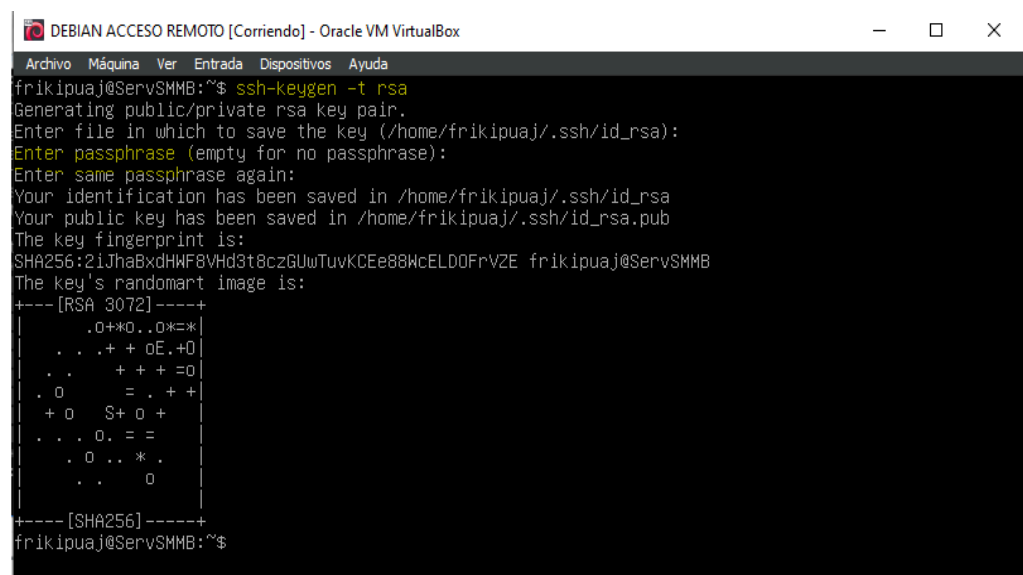
1. (30%)Acceder al servidor SSH(debian) con acceso por clave pública (Las claves se generan en Debian). La clave privada se pasa utilizando el comando SCP.

- Primero, comenzaremos activando las líneas PubkeyAuthentication cuyo valor tiene que ser yes, y la línea AuthorizedKeysFile...etc, esto permite al servidor claves públicas. En este fichero del servidor entramos con el comando **sudo nano /etc/ssh/sshd_config**.



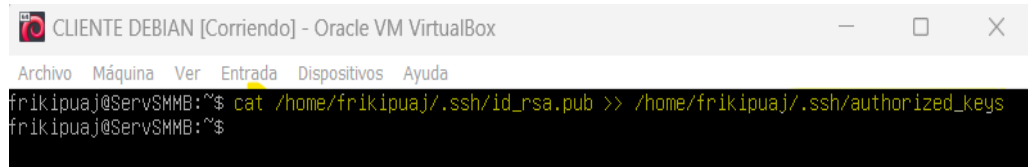
```
DEBIAN ACCESO REMOTO [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 5.4 /etc/ssh/sshd_config
PubkeyAuthentication yes
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
```

- Luego debemos generar las claves pública y privada con el comando **ssh-keygen -t rsa**, con contraseña "friki" las claves se guardan en **/home/frikipuaj/.ssh**.



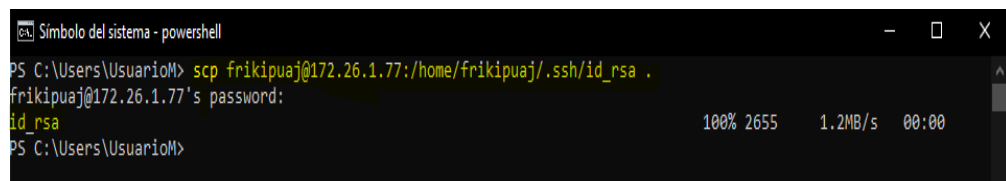
```
DEBIAN ACCESO REMOTO [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
frikipuj@ServSMMB:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/frikipuaj/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/frikipuaj/.ssh/id_rsa
Your public key has been saved in /home/frikipuaj/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:2iJhaBxdHWF8VHd3t8czGUwTuvKCEe88WcELD0FrVZE frikipuj@ServSMMB
The key's randomart image is:
+----[RSA 3072]-----+
|  .o+*o..o*~*|
|  . . .+ + oE.+o|
|  . . + + + =o|
|  . o      = . + +|
|  + o  S+ o +|
|  . . .o. =|
|  . o .. * .|
|  . .  o|
+----[SHA256]-----+
frikipuj@ServSMMB:~$
```

- Ahora copiaremos la clave pública dentro del fichero "authorized_keys" con el comando **cat /home/usuario/.ssh/id_rsa.pub >> /home/usuario/.ssh/authorized_keys**.



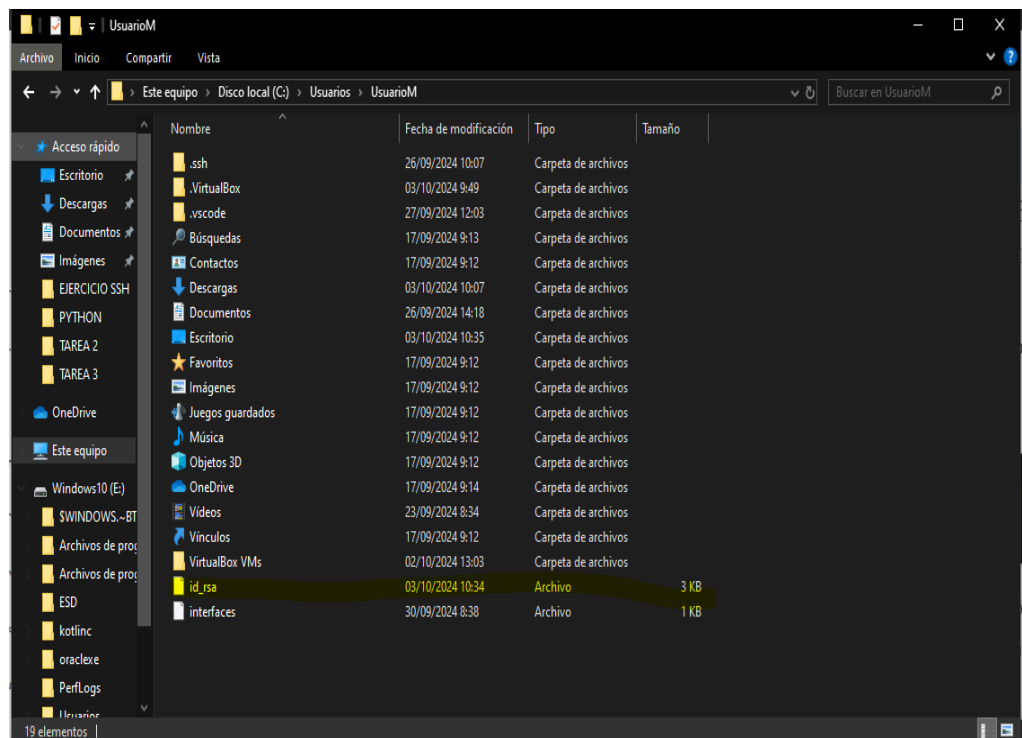
```
CLIENTE DEBIAN [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
frikipuj@ServSMB:~$ cat /home/frikipuj/.ssh/id_rsa.pub >> /home/frikipuj/.ssh/authorized_keys
frikipuj@ServSMB:~$
```

- Vamos a transferir la clave privada de mi servidor Debian a Windows desde la terminal de sistema Windows para comenzar con el primer ejercicio, usamos el comando **scp usuario@ipaddress:/ubicacion/de/claveprivada ..**



```
Símbolo del sistema - powershell
PS C:\Users\UsuarioM> scp frikipuj@172.26.1.77:/home/frikipuj/.ssh/id_rsa .
frikipuj@172.26.1.77's password:
id_rsa
100% 2655 1.2MB/s 00:00
PS C:\Users\UsuarioM>
```

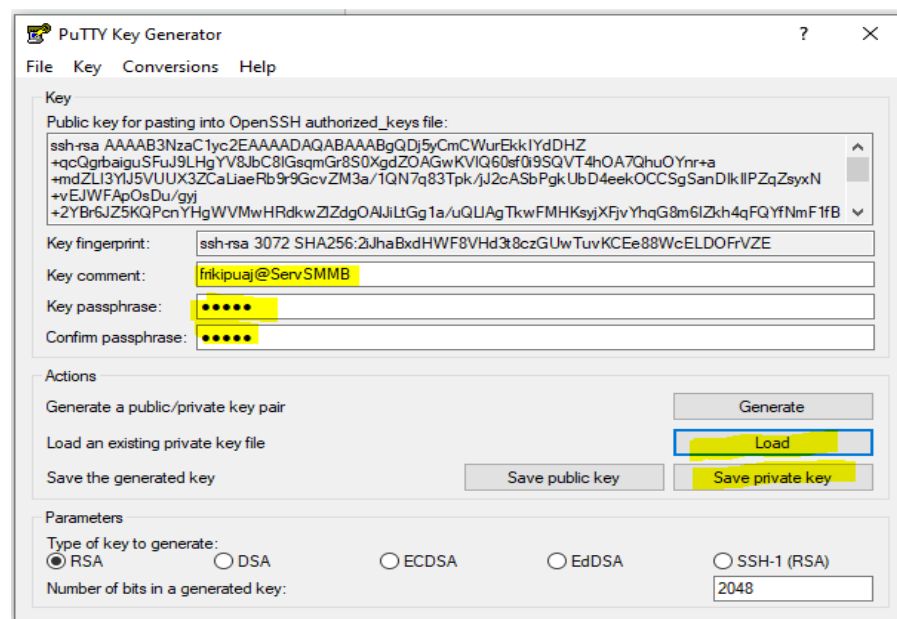
CLAVE EN WINDOWS



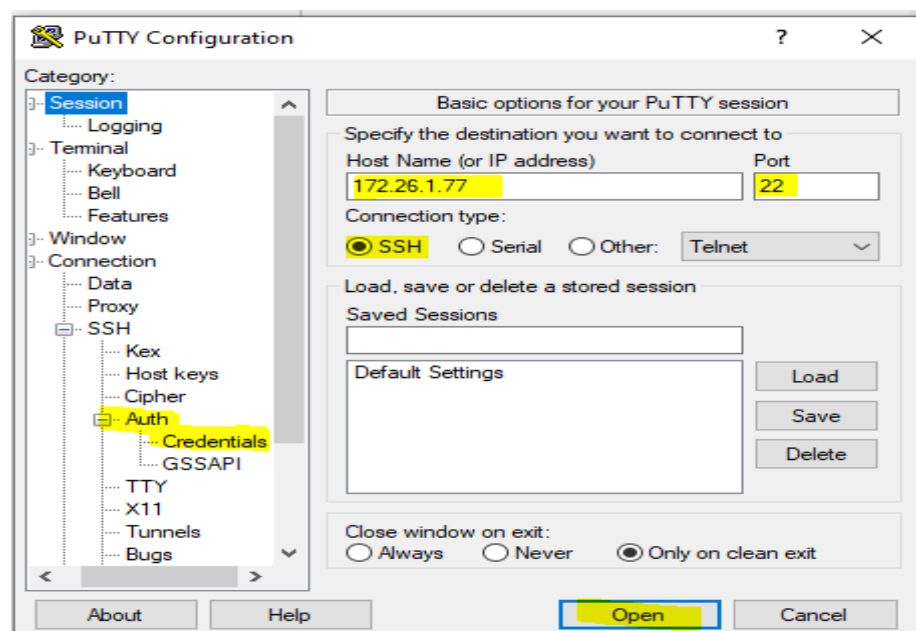
a. Utiliza el programa Cyberduck(MAC o Windows) o Putty (Windows) para introducir la clave privada (putty/auth). Salvar la sesión de putty con el usuario ya introducido.

- Luego de haber utilizado el comando scp y pasado el archivo de la clave privada de mi servidor a windows (host), utilizaré Puttygen para traducir la clave privada a un idioma entendible para Putty.

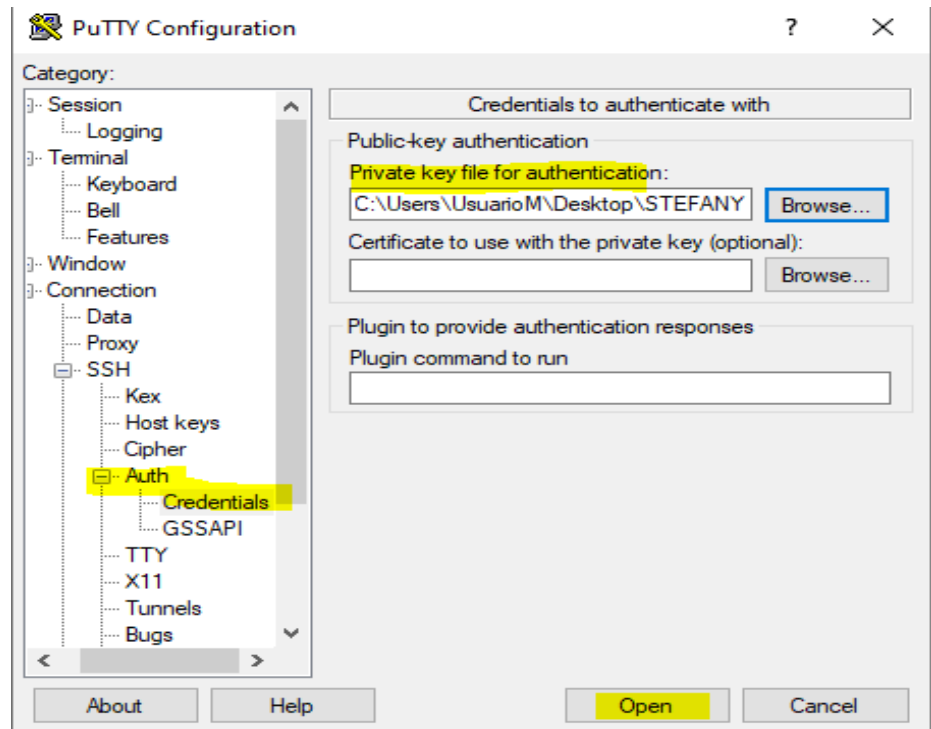
Para ello, la subire en PuttyGen, y la guardaré como clave privada.



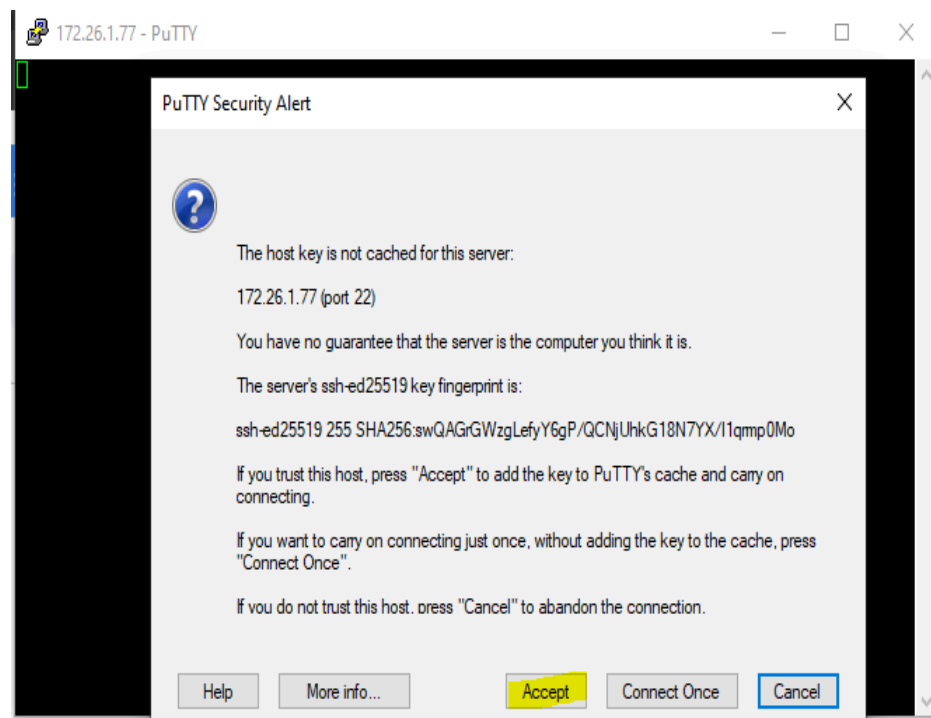
- Ahora, abrimos Putty, dentro de este ingresamos en el apartado Sessions, la ip del servidor, el puerto 22 y el tipo de conexión SSH.



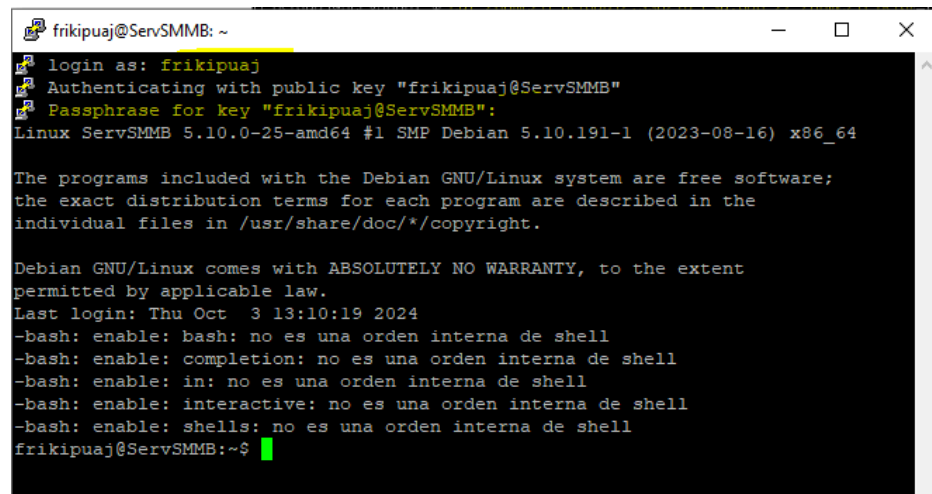
- Una vez ingresado todo esto, iremos a **SSH>Auth>Credentials** y cargaremos nuestra clave privada, hecho esto le daremos a "Open".



- Nos emergerá una ventana advirtiéndole sobre la conexión, y debemos darle aceptar para poder conectarnos correctamente.

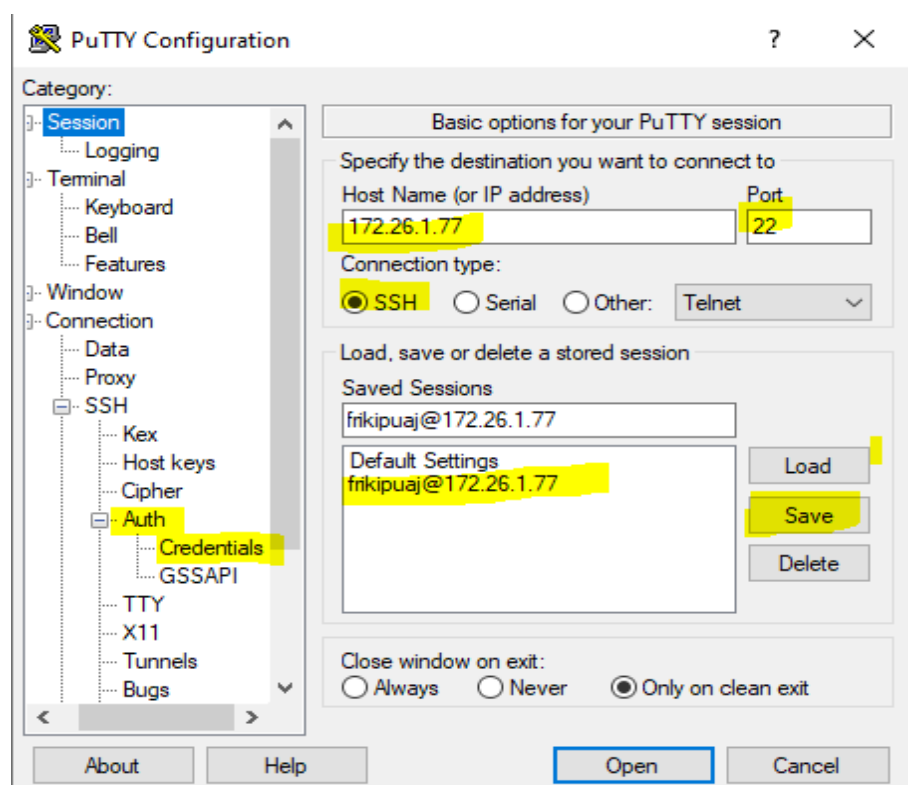


- Hecho esto nos pedirá ingresar el usuario, en este caso, "frikipuj", con el que queremos conectarnos y si todo es correcto se conectará sin necesidad de ingresar la contraseña, solo el passphrase.



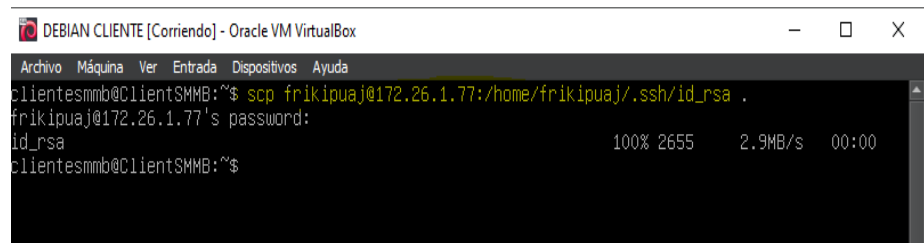
```
frikipuj@ServSMMB: ~  
login as: frikipuj  
Authenticating with public key "frikipuj@ServSMMB"  
Passphrase for key "frikipuj@ServSMMB":  
Linux ServSMMB 5.10.0-25-amd64 #1 SMP Debian 5.10.191-1 (2023-08-16) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Thu Oct 3 13:10:19 2024  
-bash: enable: bash: no es una orden interna de shell  
-bash: enable: completion: no es una orden interna de shell  
-bash: enable: in: no es una orden interna de shell  
-bash: enable: interactive: no es una orden interna de shell  
-bash: enable: shells: no es una orden interna de shell  
frikipuj@ServSMMB:~$
```

- Para guardar la sesión debemos desconectarnos, ingresar todo lo anterior e ir a "**Saved Sessions**", en este colocaremos un nombre con el que guardar la sesion, hecho esto le damos a "save" y ya, cada vez que queramos conectarnos a esta sesión deberemos seleccionarla, darle a "load" y abrirla.



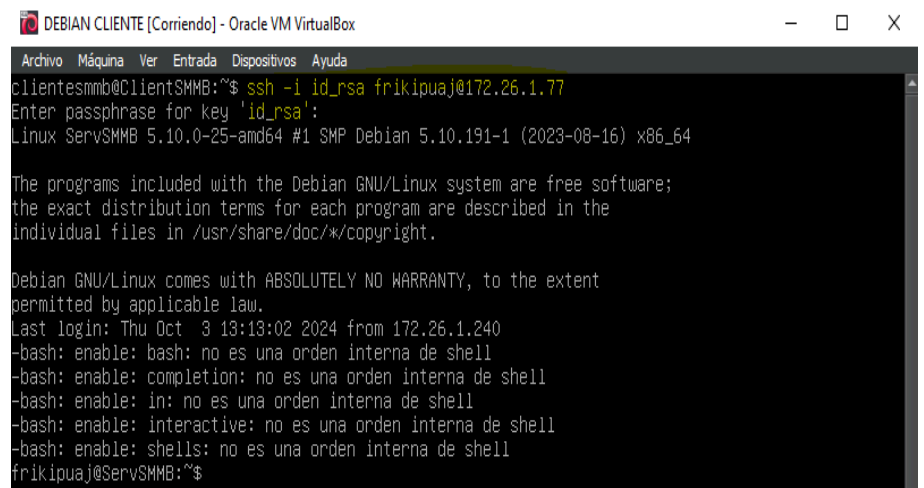
b. Utilizar el cliente de ssh (Debian) para conectarnos al servidor SSH.

- Para hacer esto, debemos de transferir la clave privada de nuestro servidor a nuestro cliente desde nuestro cliente con el comando **scp usuarioer@ipserver:/ruta/clave/privada.**



```
DEBIAN CLIENTE [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
clientesmb@ClientSMB:~$ scp frikipuaj@172.26.1.77:/home/frikipuaj/.ssh/id_rsa .
frikipuaj@172.26.1.77's password:
id_rsa                                100% 2655      2.9MB/s   00:00
clientesmb@ClientSMB:~$
```

- Hecho esto podremos iniciar sesión en el servidor sin necesidad de ingresar contraseña con el comando **ssh -i id_rsa usuarioer@ipserver.**



```
DEBIAN CLIENTE [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
clientesmb@ClientSMB:~$ ssh -i id_rsa frikipuaj@172.26.1.77
Enter passphrase for key 'id_rsa':
Linux ServSMB 5.10.0-25-amd64 #1 SMP Debian 5.10.191-1 (2023-08-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Oct 3 13:13:02 2024 from 172.26.1.240
-frikipuaj@ServSMB:~$
```