194 SSH

Emilio Cabo Gomis

Sumario

Comprobaciones iniciales

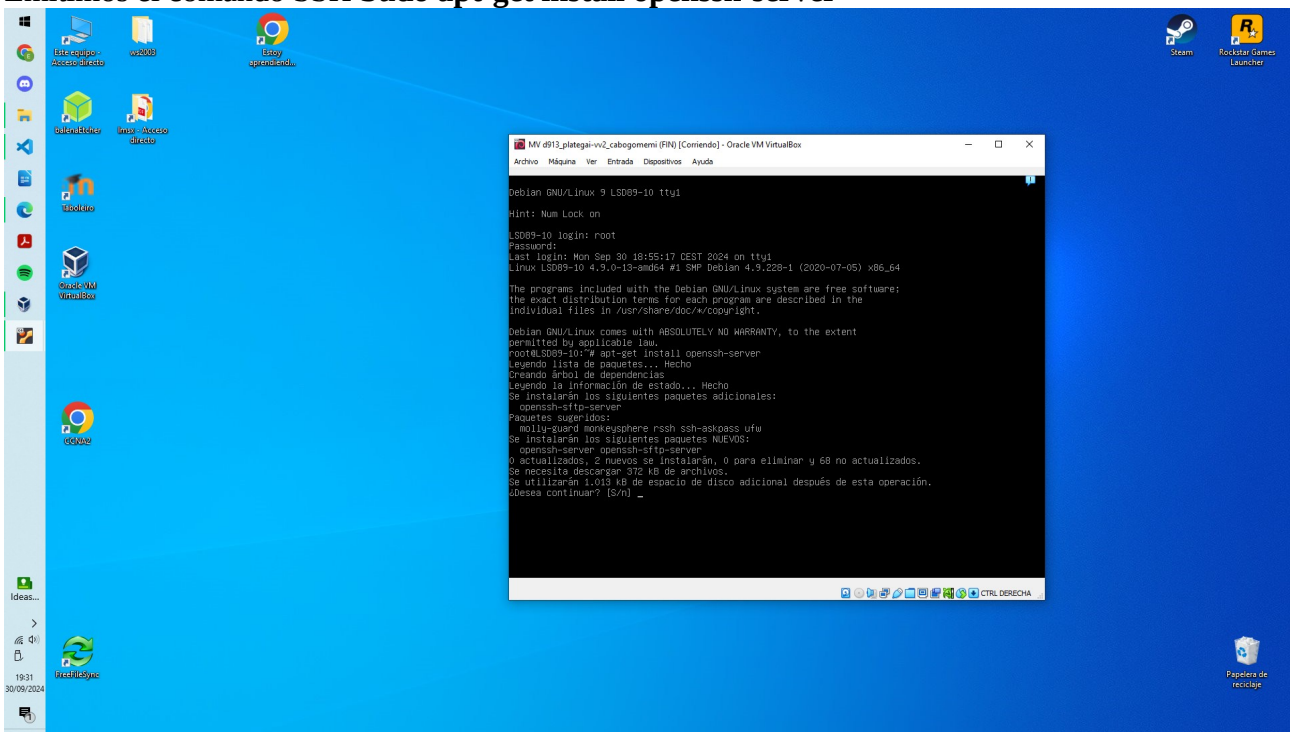
Deberemos tener dos máquinas, una cliente y una servidor en la misma red. O habilitando el reenvío de puertos.

El puerto SSH es el puerto 22.

Configuración del servicio SSH con contraseña

Primero comenzamos instalando el servicio de SSH.

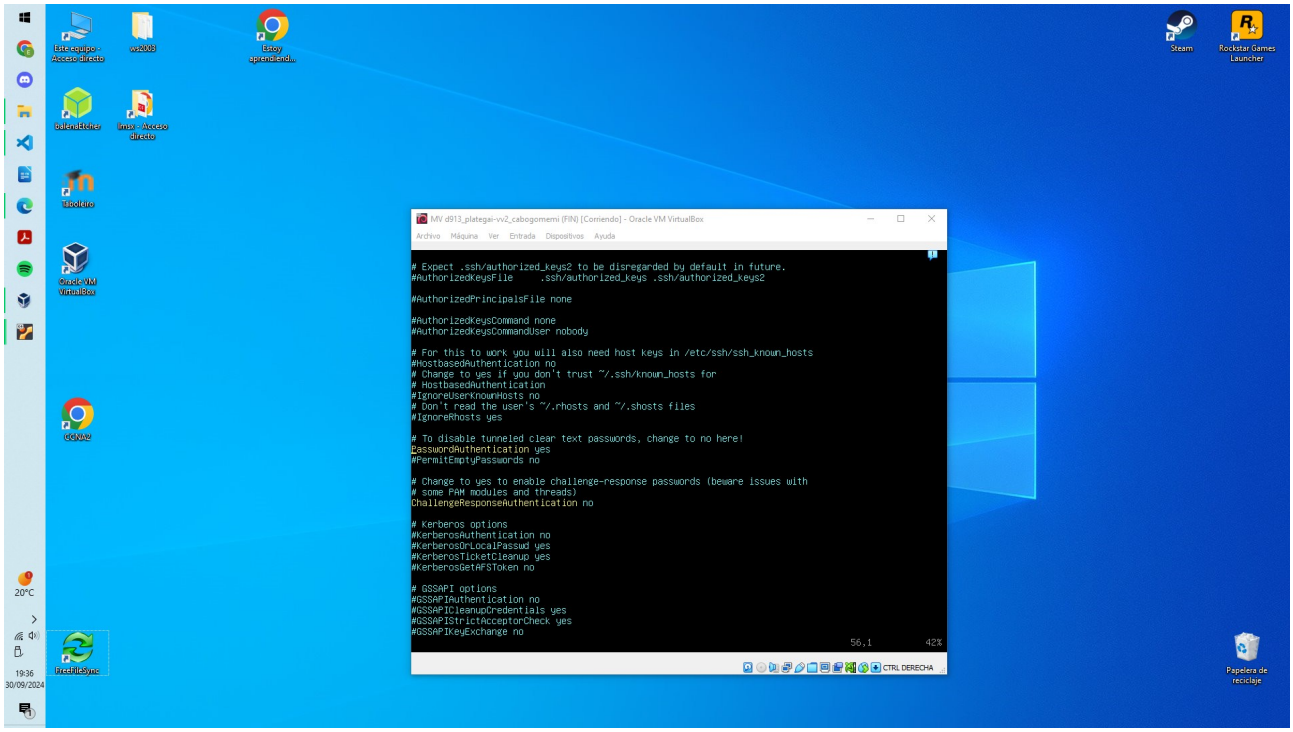
Emitimos el comando SSH **Sudo apt-get install openssh-server**



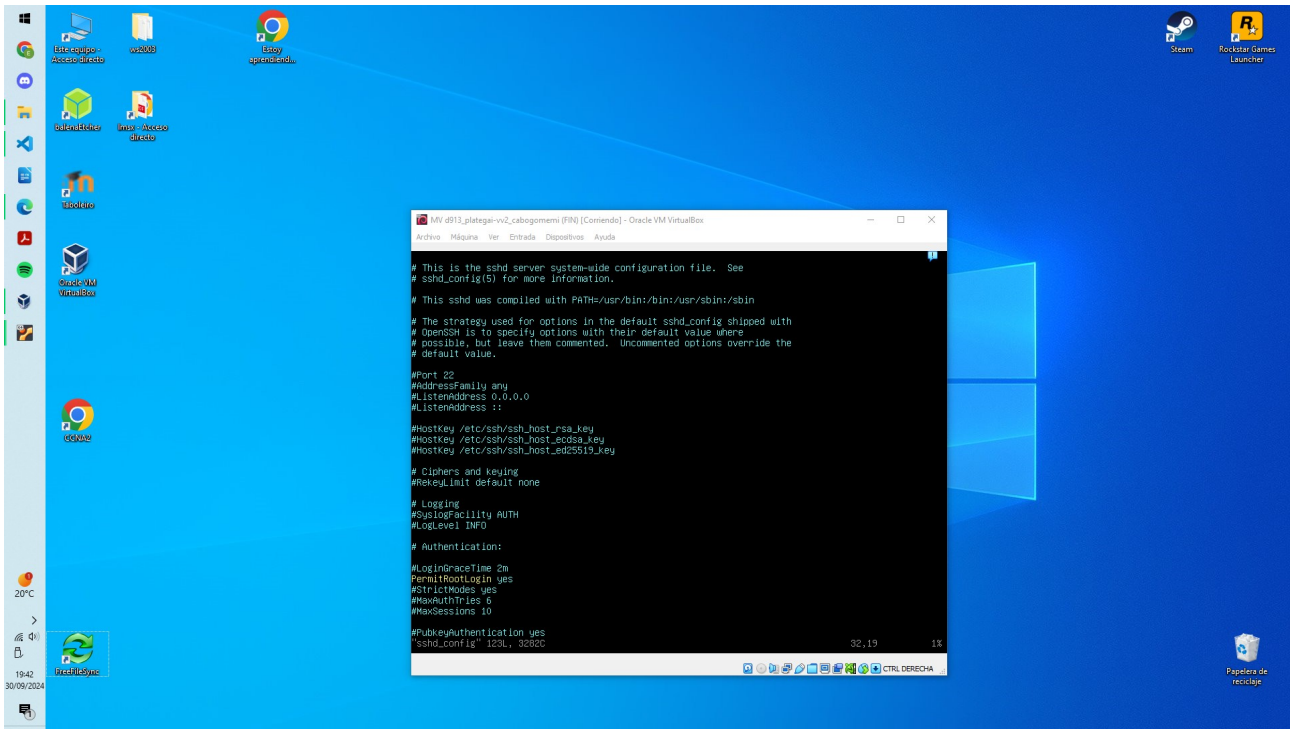
Realizamos una copia de seguridad del archivo de configuración antes de mofidicarlo de ninguna manera.

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
```

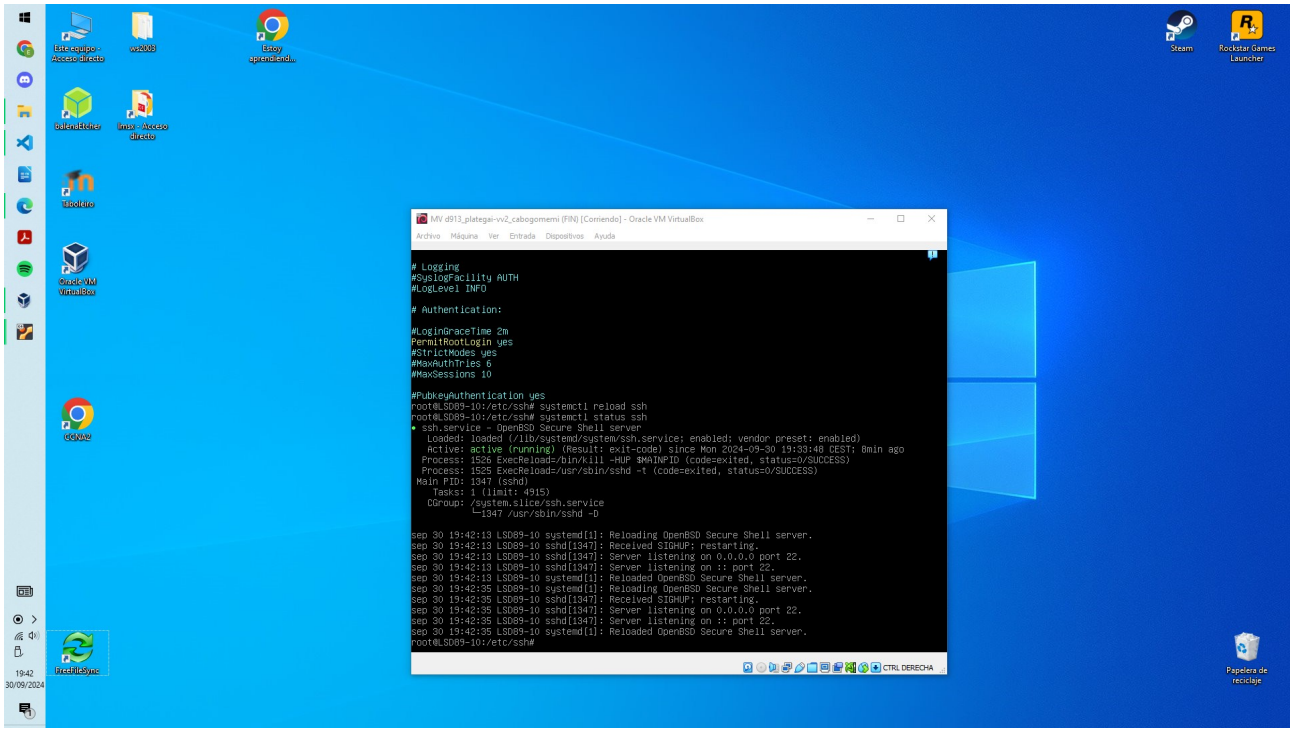
Entramos al archivo de configuración.
Descomentamos la línea #PasswordAuthentication yes es un ajuste que cambiaremos posteriormente.



Editamos la línea que contiene #PermitRootLogin prohibitpassword para que tenga el siguiente contenido.



Guardamos el contenido.
Hacemos que la nueva configuración tome efecto en el servicio mediante el comando systemctl reload ssh.

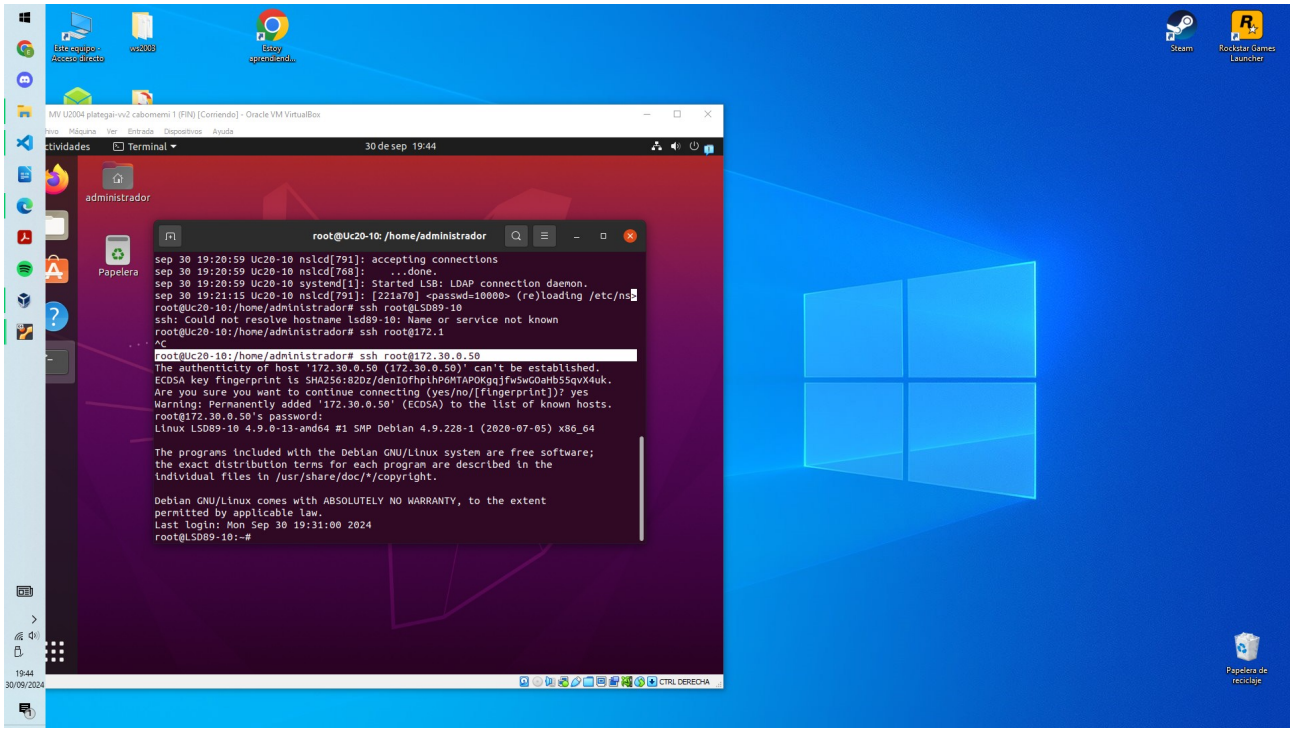


Inicio de sesión en la máquina cliente mediante contraseña

Iniciamos la conexión desde la máquina cliente.

Ssh <nombredeusuario>@<ip//nombreservidor>

Se nos dirá que introduzcamos la contraseña.



Configuración del servicio SSH sin contraseña (clave público-privada)

Generación de claves

Comenzamos generando la clave público y privada en nuestra máquina cliente mediante el comando.

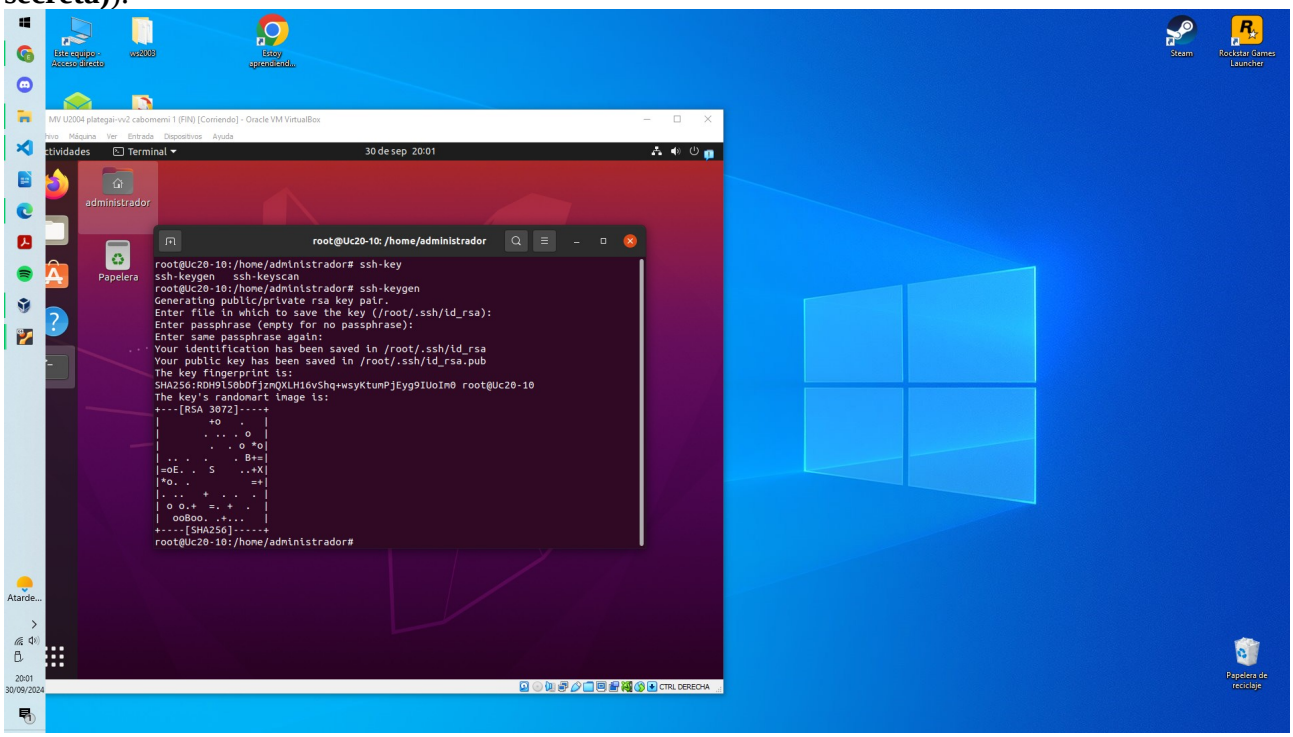
`ssh-keygen`

Se nos pedirá el directorio dónde lo queremos guardar. Por defecto este será el **/root/.ssh/id_rsa**

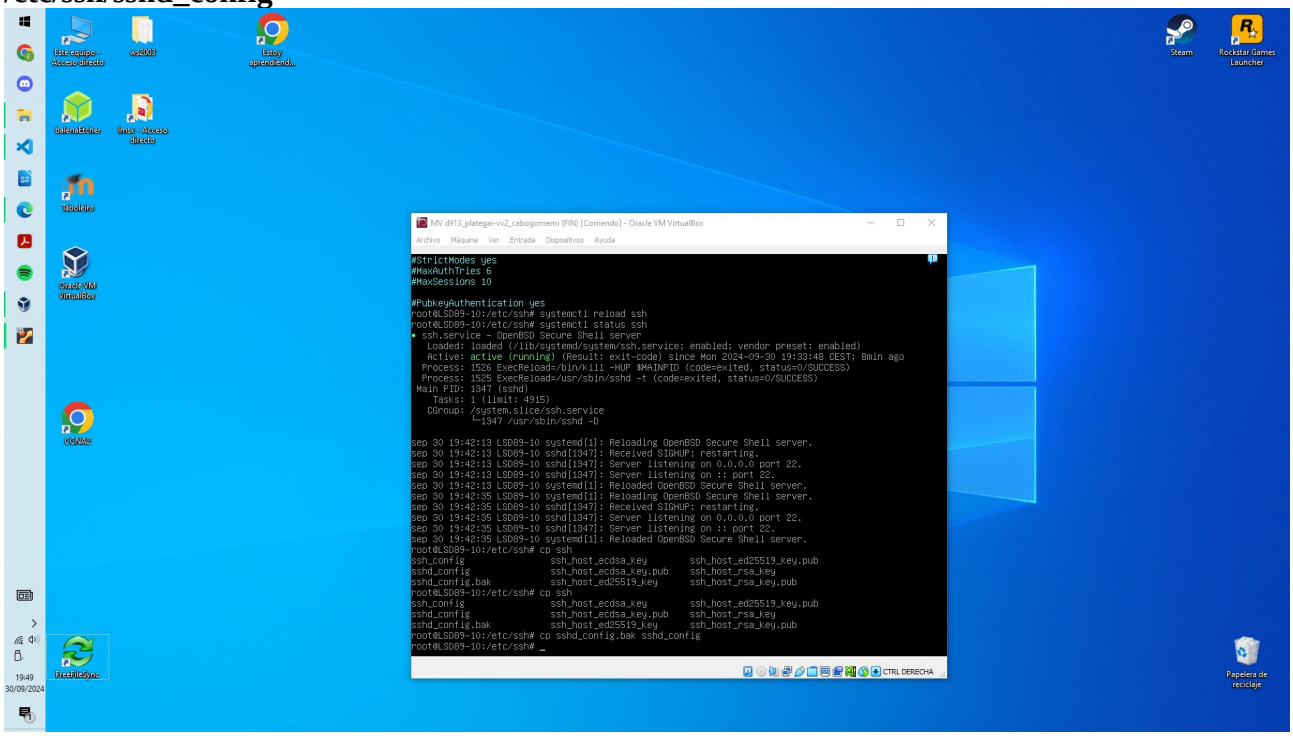
Recomiendo no tocar este ajuste dado que de otra manera tendremos que cambiar la ubicación en la que el servidor tendrá que ir a buscar las claves.

Esto genera 2 archivos `~/.ssh/id_rsa` y `~/.ssh/id_rsa.pub`. El primero contiene la clave privada, que debemos mantener segura y no compartir. El segundo archivo contiene la clave pública, que compartiremos con los servidores SSH a los que querramos conectarnos.

Y una contraseña desde la cual se generará la clave pública. (**Recomiendo abc123.(clave súper secreta)**).

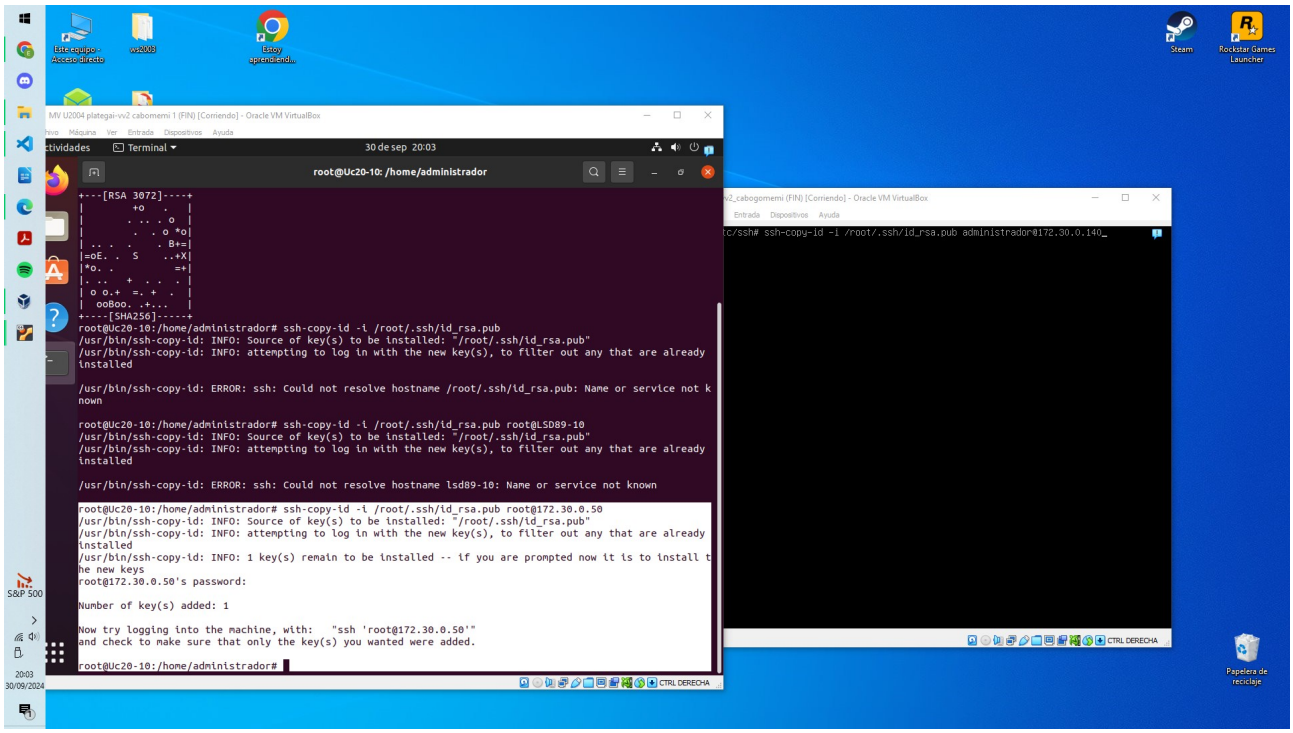


Revertimos la configuración mediante el comando sudo **cp /etc/ssh/sshd_config.bak /etc/ssh/sshd_config**



Compartir las claves

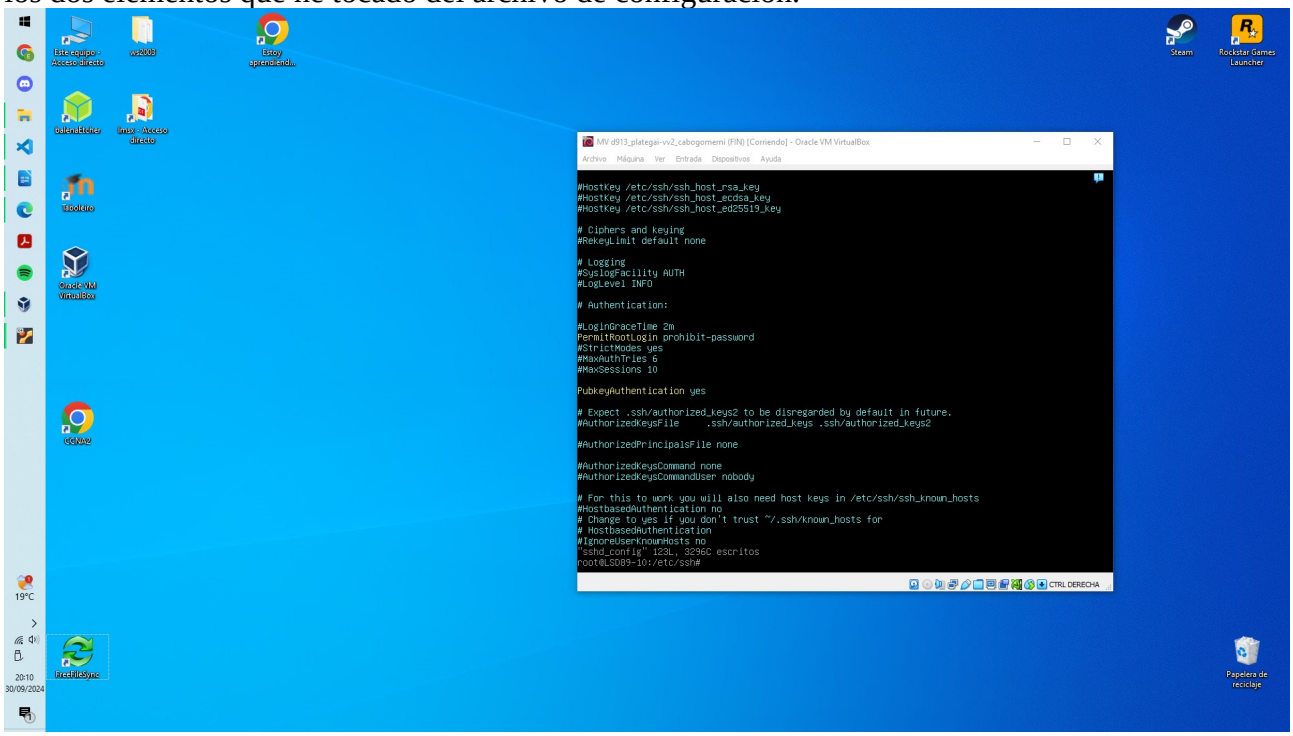
Compartimos las claves mediante el comando ssh-copy-id -i /root/.ssh/id_rsa.pub <username>@<ip//nombreServidor>



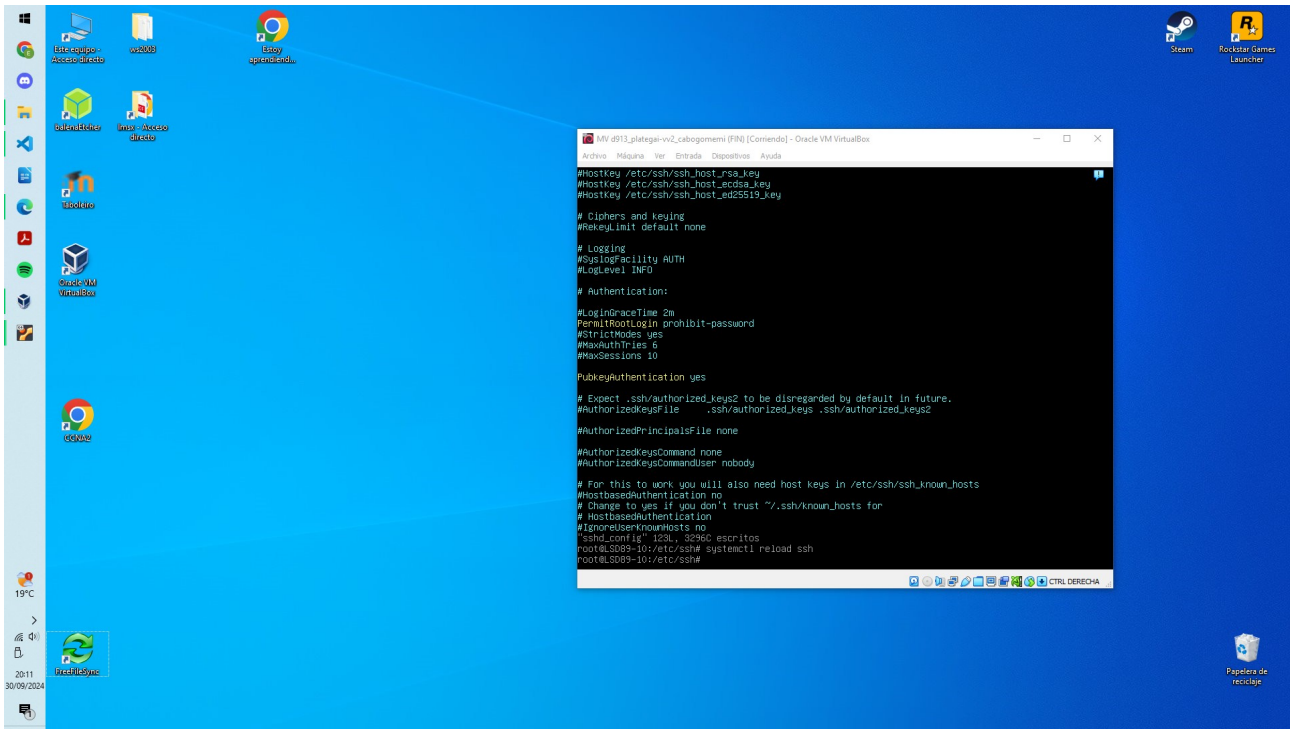
Clave compartida con éxito

Antes de intentar iniciar sesión como nos dice el output del comando. Tendremos que modificar algunos aspectos del archivo de configuración.
Activamos la autenticación mediante autenticación con clave público-privada que es más segura, que la autenticación mediante contraseña.

Permitimos que podamos iniciar sesión con el usuario root pero no mediante contraseña. Estos son los dos elementos que he tocado del archivo de configuración.

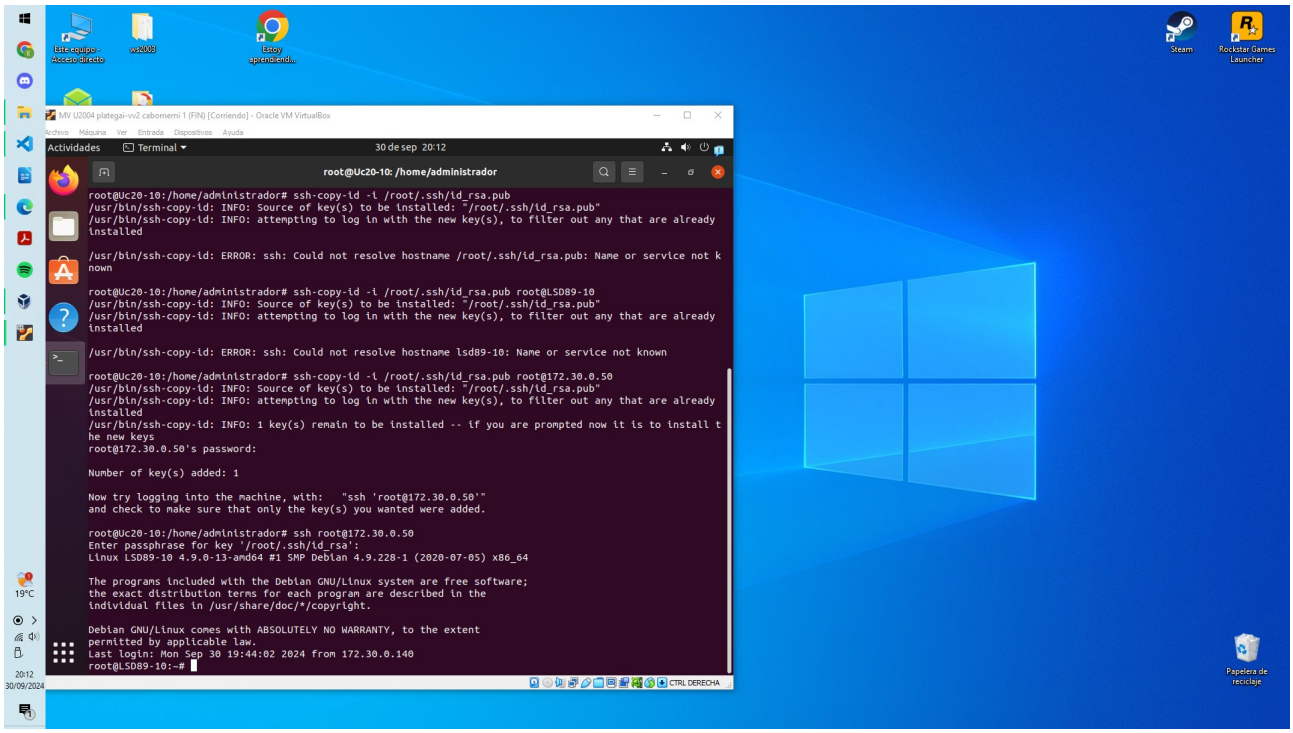


Hacemos que la nueva configuración tome efecto en el servicio mediante el comando **systemctl reload ssh.**



Inicio de sesión en la máquina cliente mediante clave público-privada

Nos pedirá la *passphrase*.



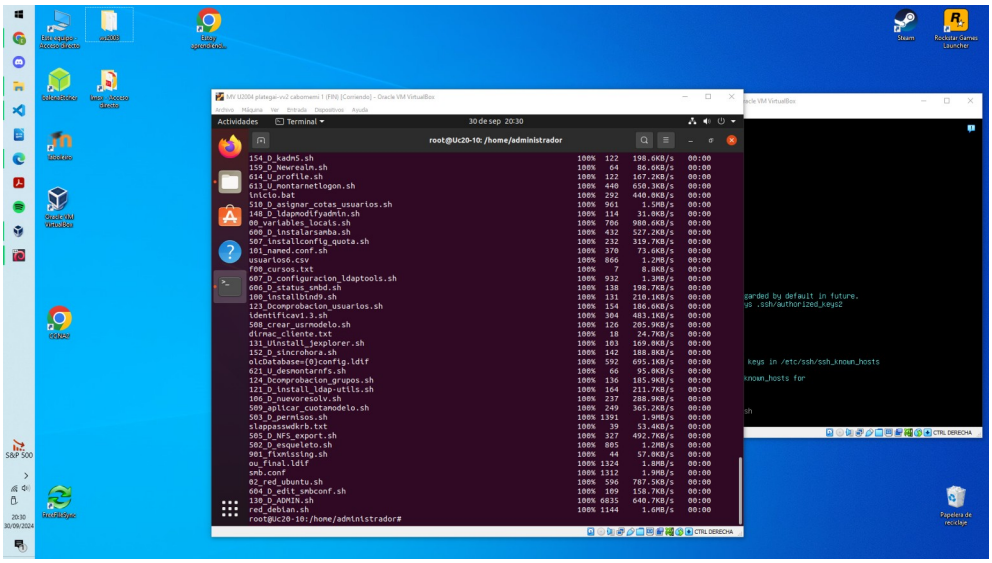
Inicio de sesión exitoso mediante clave público-privada.

Copiado de archivos mediante scp

Para copiar todos los contenidos de una carpeta, por ejemplo la carpeta que contiene mis herramientas linux, ejecutamos el siguiente comando.

Es importante que pongamos la opción -r dado que copiará recursivamente.

scp -r ./herramientas_linux root@172.30.0.50:~/herramientas_linux



Como proporcionar ssh la contraseña de manera no interactiva

Sencillo, mediante **sshpass**.

REQUISITOS:

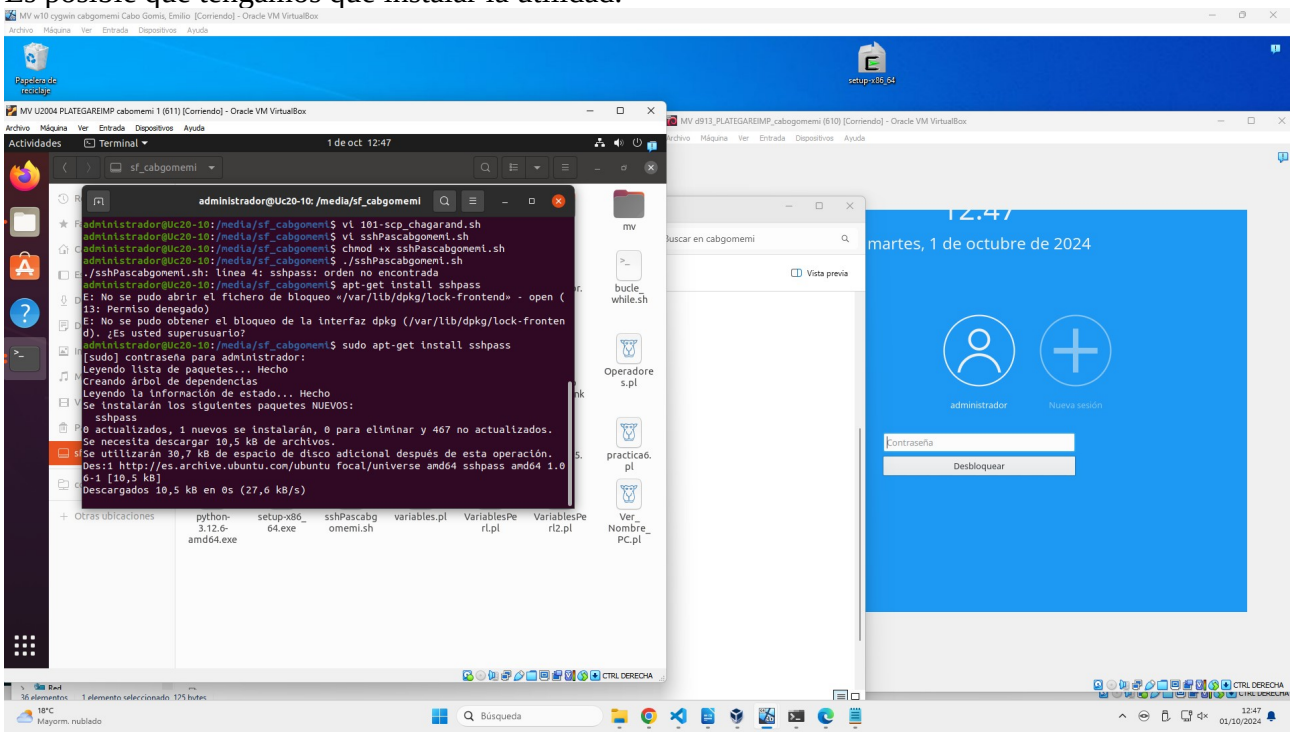
Tener el servidor ssh configurado para aceptar contraseñas y no claves.

Necesitaremos editar el siguiente documento las siguientes líneas **/etc/ssh/sshd_config**

- Descomentamos la línea #PasswordAuthentication yes
- Descomentamos la línea que contiene #PermitRootLogin prohibitpassword y la editamos para que tenga PermitRootLogin yes

Reloadeamos el servicio.

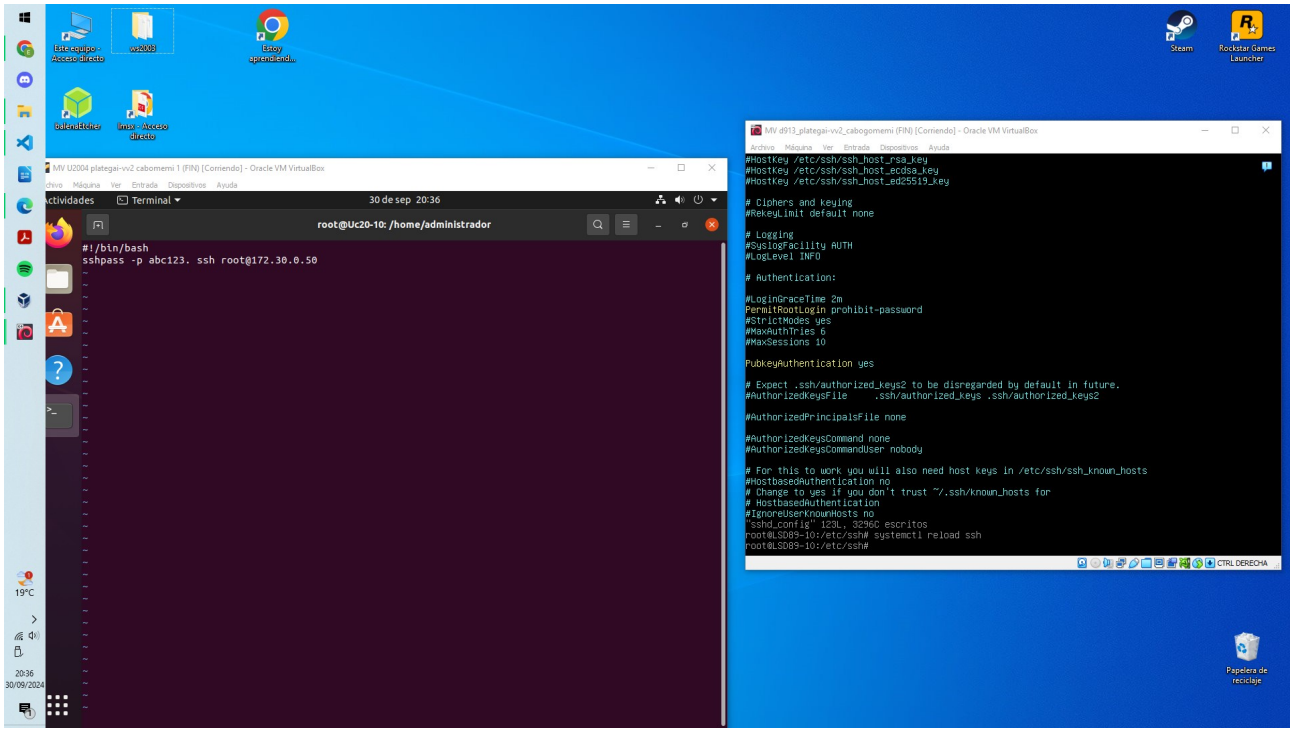
Es posible que tengamos que instalar la utilidad.



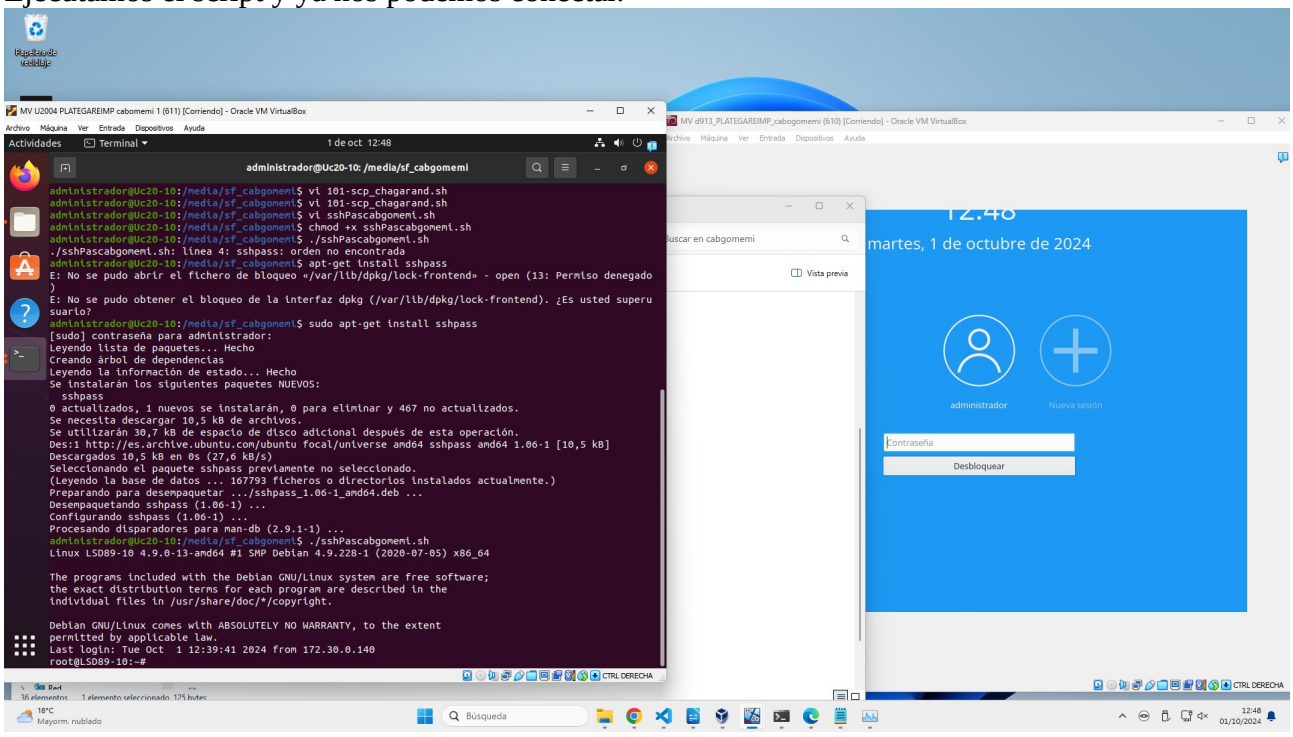
Esta es la sintaxis **sshpass -p $PASS ssh $usuario@$HOST**

(En este caso emplea variables para introducir el contenido pero no es necesario(aunque sí útil)).

Introducimos esto en un script.



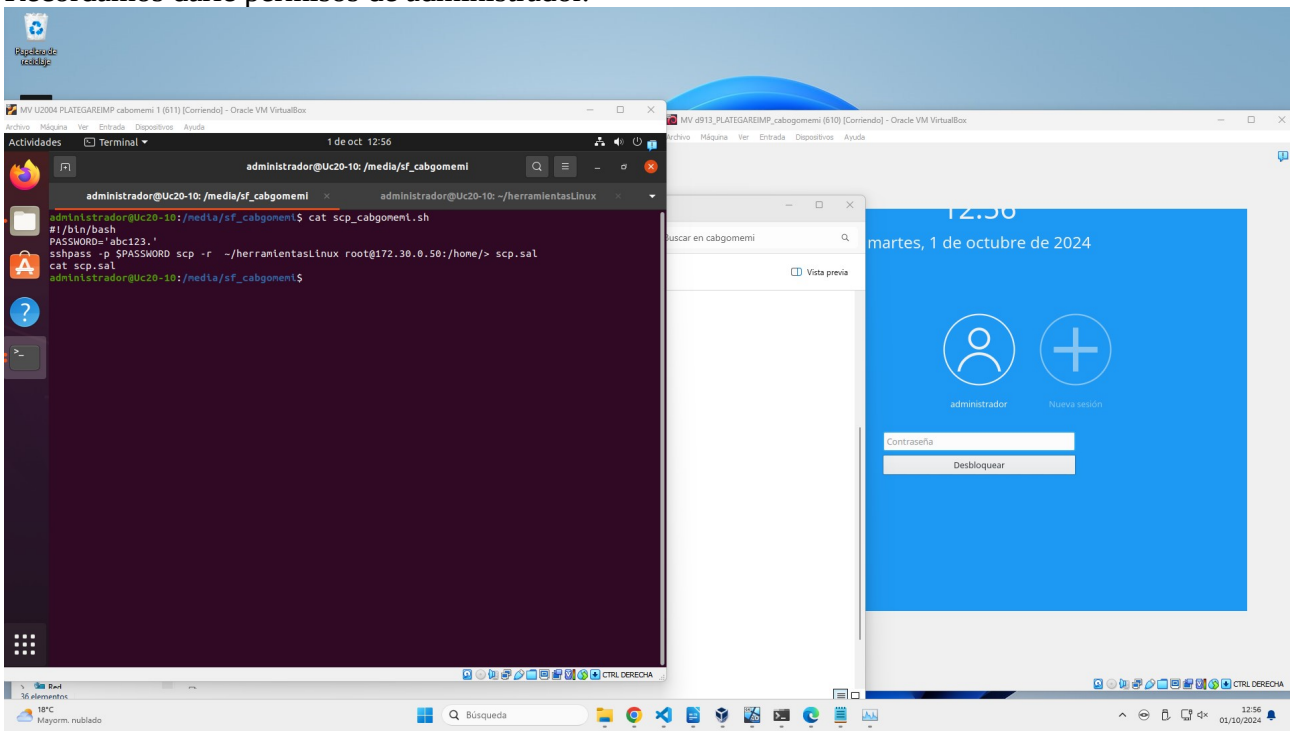
Le damos permiso de ejecución mediante el comando **chmod +x <nombreScript>**
Ejecutamos el script y ya nos podemos conectar.



.

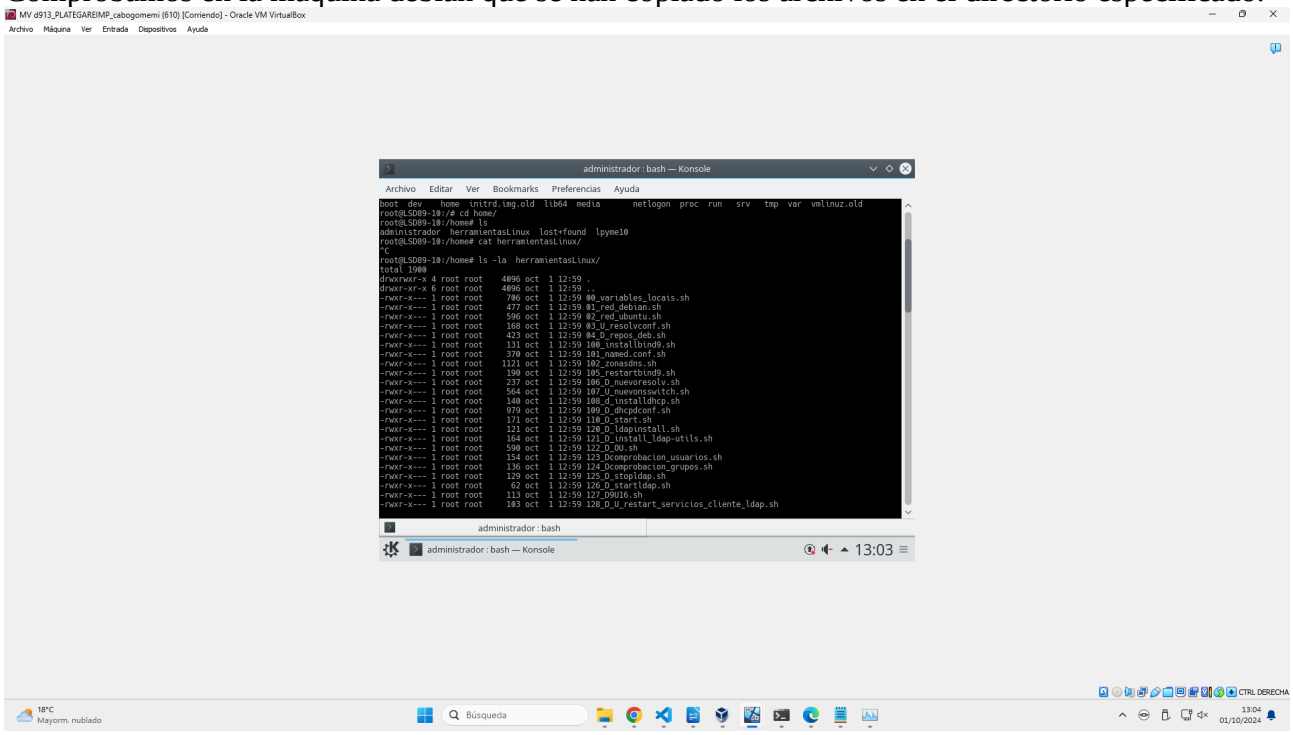
Copiado de archivos automático

Ahora creamos un script con el siguiente contenido.
Recordamos darle permisos de administrador.



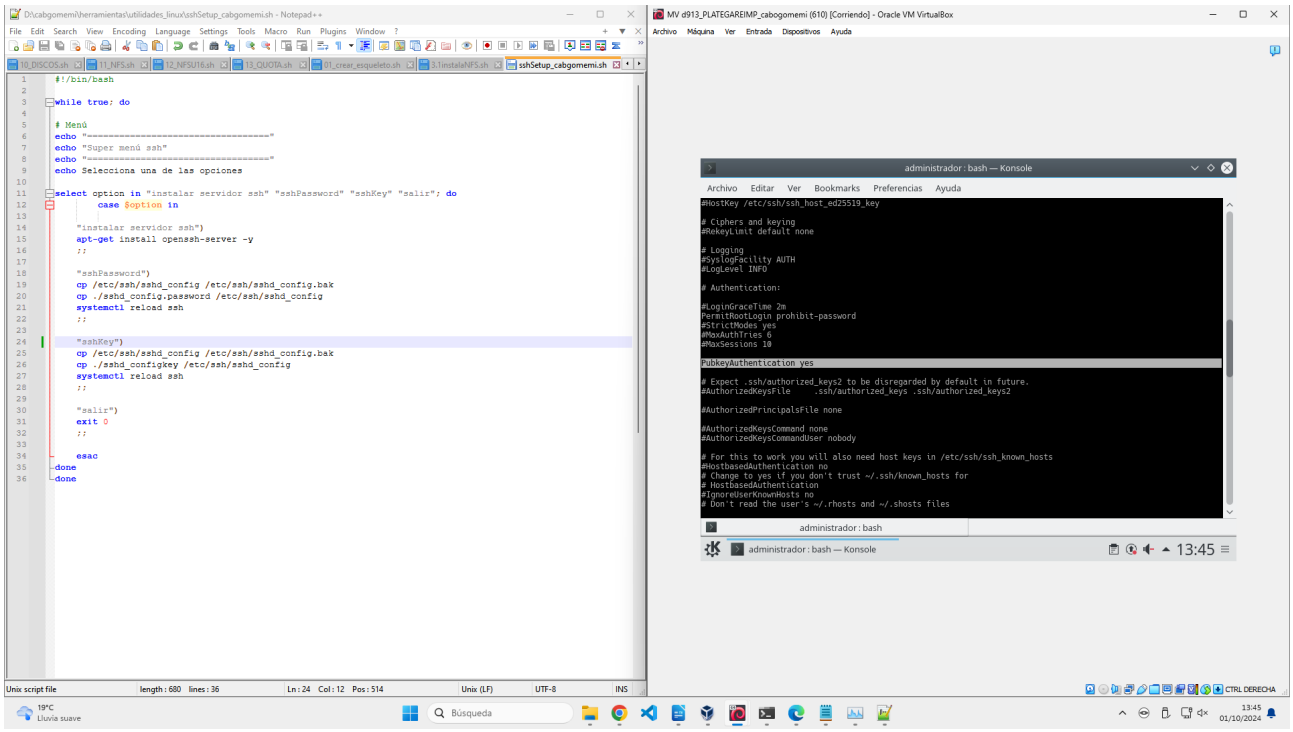
En este script vamos a copiar las herramientas que tengo desde la máquina ubuntu hacia el servidor para poder ejecutarlas

Ejecutamos el script.
Comprobamos en la máquina debian que se han copiado los archivos en el directorio especificado.

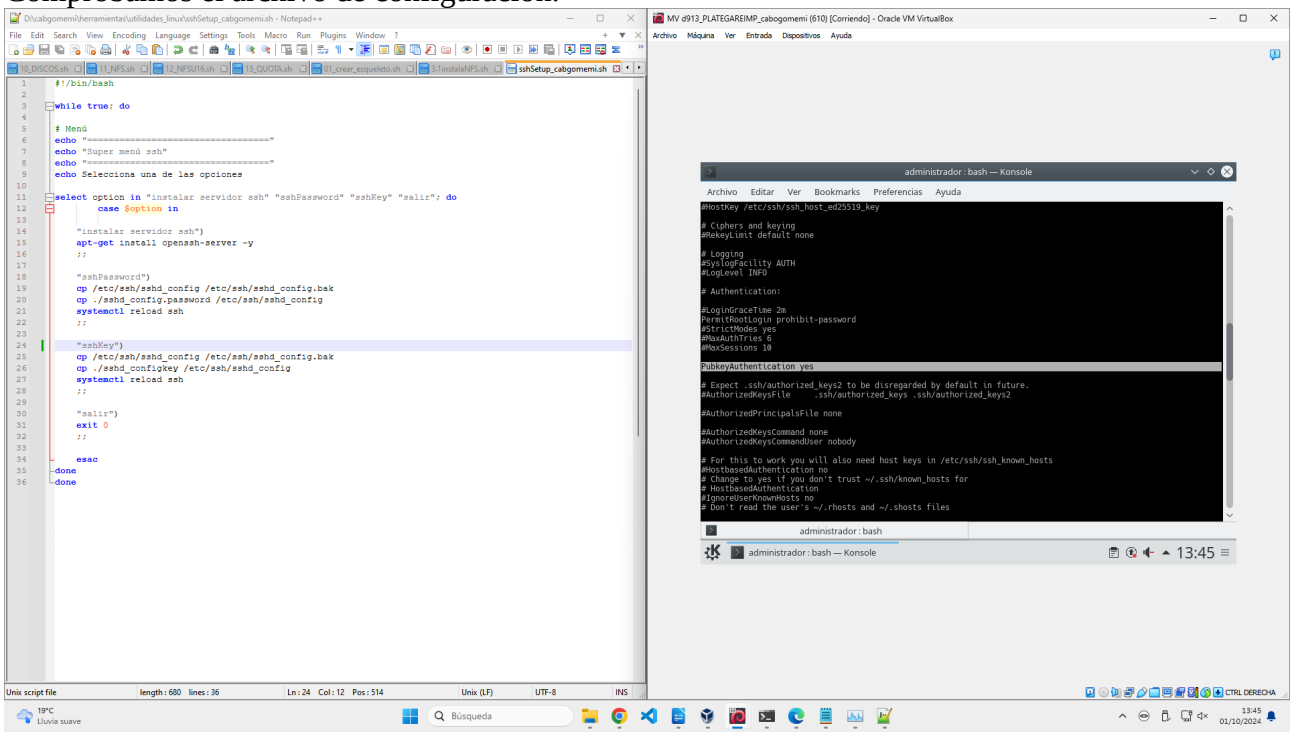


Automatización del setup de SSH

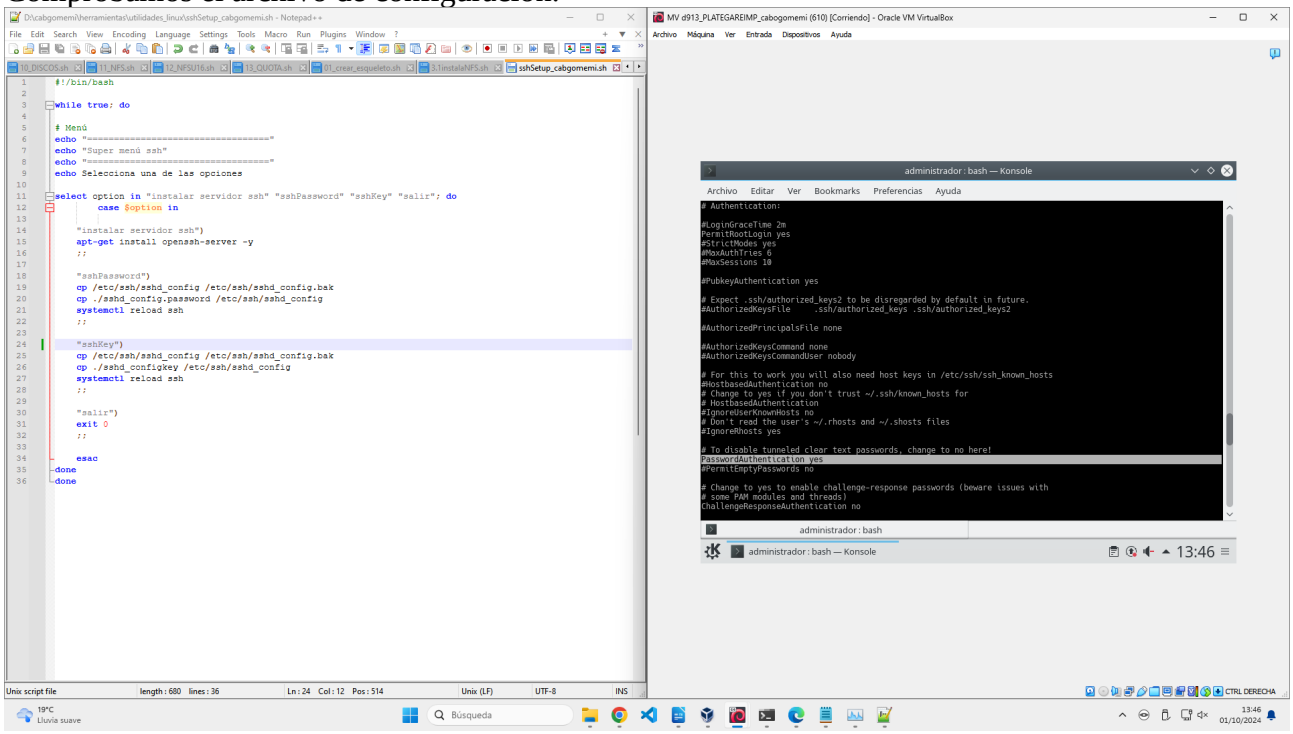
Creamos un script con el siguiente contenido.



Ejecutamos la opción para configurar el inicio de sesión mediante key.
Comprobamos el archivo de configuración.



Ejecutamos la opción para configurar el inicio de sesión mediante contraseña.
Comprobamos el archivo de configuración.



Bibliografía

José arrate blog

file:///F:/curso_1/iso/9.Resolucion%20Incidencias%20y%20servicio%20tecnico/900%20SSH%20sin%20contrase%C3%B1as%20(y%20seguro)%20-%20Jos%C3%A9%20Arrarte.htm

ARCHWIKI

https://wiki.archlinux.org/title/SSH_keys

Wikipedia

https://es.wikipedia.org/wiki/Secure_Shell

Ubuntu

https://ubuntu.com/server/docs/openssh-server