P6.2 - ServidorOpenSSH

Nicolas Lopez Flores

1. Instalar el servidor OpenSSH desde los repositorios oficiales de Ubuntu

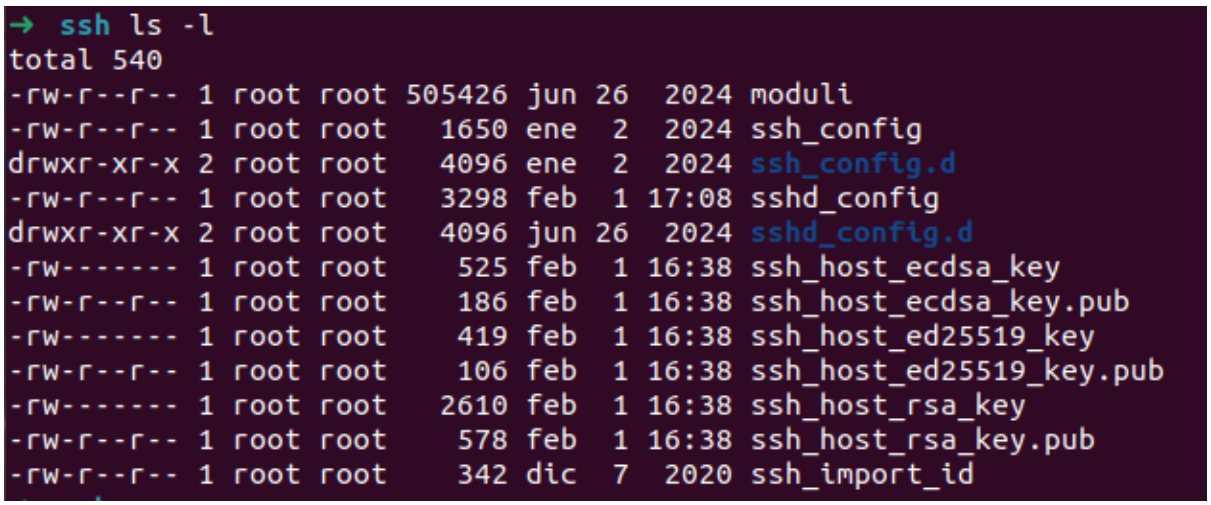
```
sudo apt update && sudo apt install openssh-server -y
```

Al instalar el servidor:

- Se crean los ficheros de configuración.
- Se generan las parejas de claves RSA, DSA y ECDSA que se almacenan en el directorio /etc/ssh. Además, en este directorio encontramos entre otros archivos:
  - ✓ sshd_config: archivo de configuración del servidor SSH
  - ✓ ssh_config: archivo de configuración del cliente SSH
  - ✓ ssh_host_*_key: clave privada de la máquina (* puede ser rsa o dsa o ecdsa)
  - ✓ ssh_host_*_key.pub: clave pública de la máquina (* puede ser rsa o dsa o ecdsa)

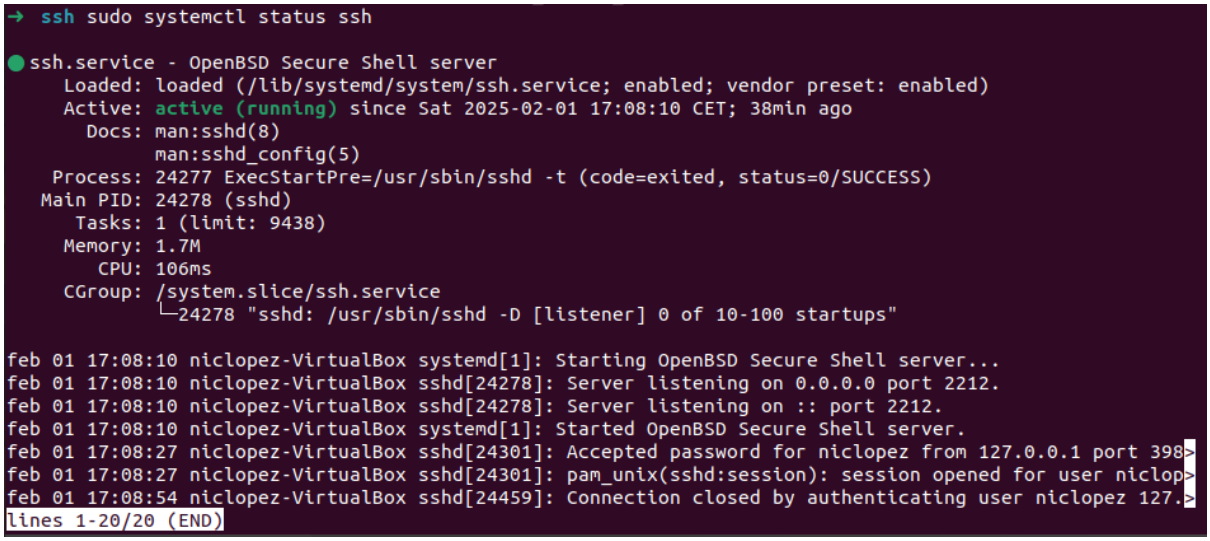
2. Consulta las claves públicas (*.pub) y privadas (sin extensión) dentro del directorio /etc/ssh

Hay 3 tipos de encriptado:

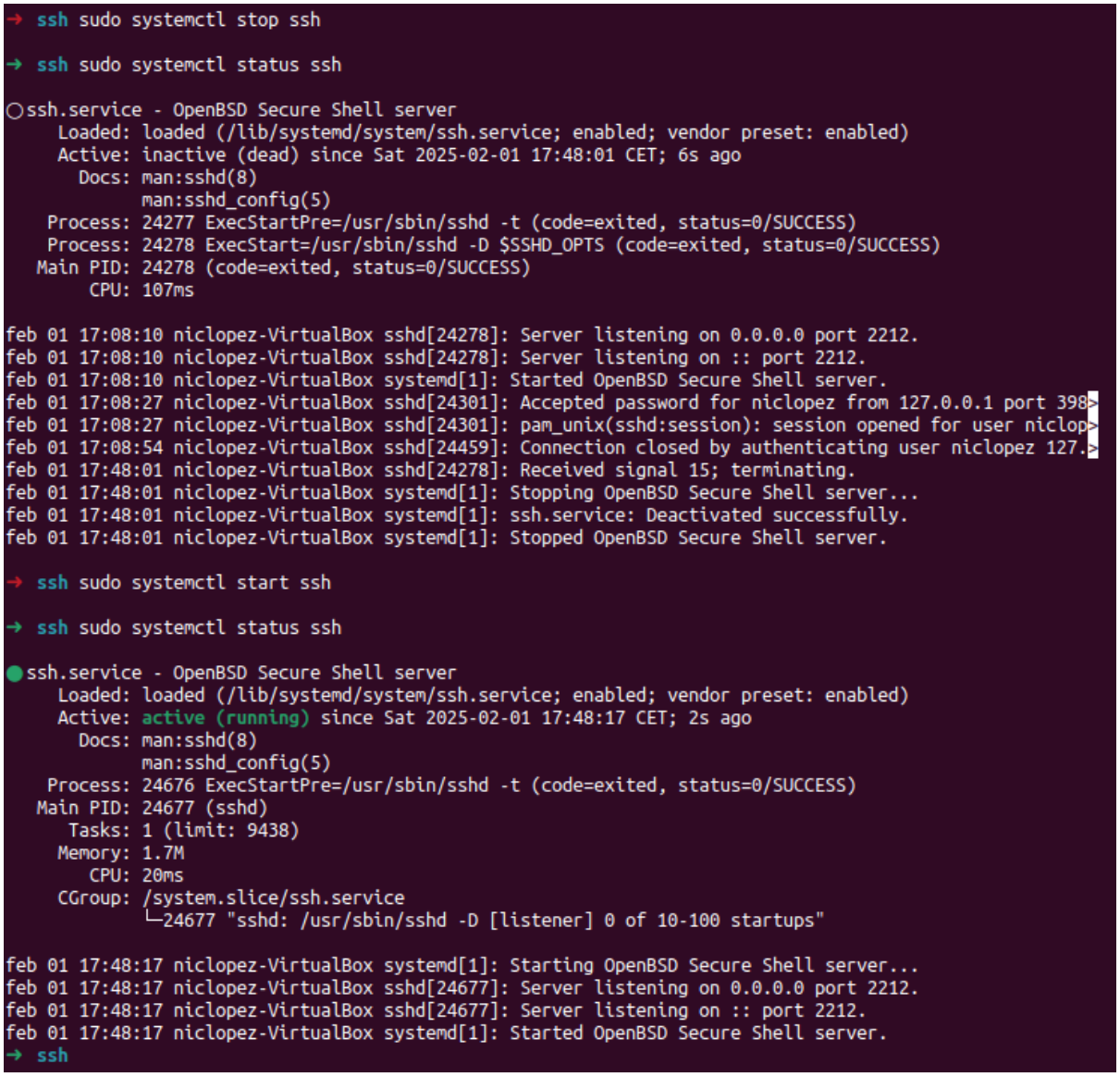


3. Comprobar que el servidor está iniciado y escuchando peticiones en el puerto 22/TCP

SSH por defecto escucha desde el puerto 22, pero como puedes ver en mi caso escucha desde el 2212, porque lo he cambiado desde el archivo de configuracion.



4. Iniciar/parar el servidor desde la línea de comandos y probaremos que funciona correctamente.

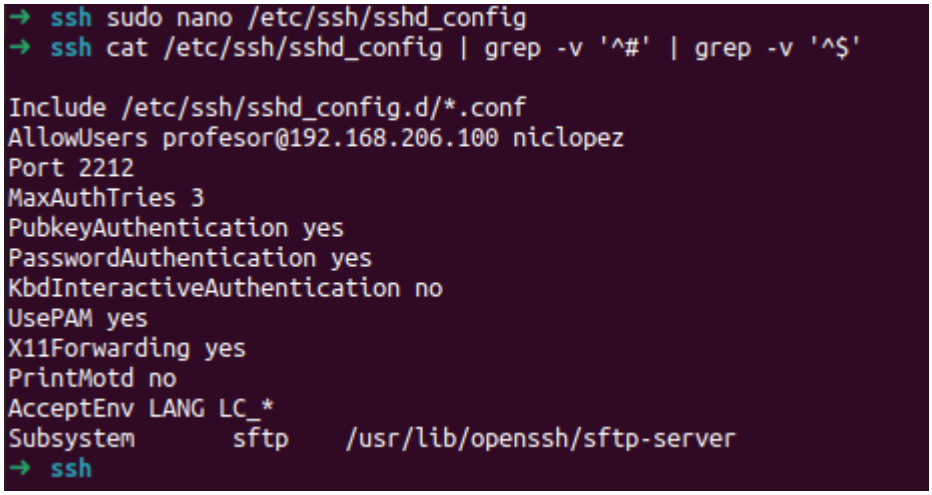


5. Configuración de SSH

a) Consultar en el fichero de configuración del servidor /etc/ssh/sshd_config las directivas habilitadas

Si añadimos este comando se mostrarán solo las líneas que no contengan un '#'(comentadas), por defecto tendremos esto:

```
cat /etc/ssh/sshd_config | grep -v '^#' | grep -v '^$'
```



Exceptuando:

-AllowUsers

-MaxAuthTries

-PubkeyAuthentication

-PasswordAuthentication

Que serán configuraciones que se harán más adelante en la practica

b) Podemos realizar cualquier cambio en el fichero de configuración. Configurar como puerto de escucha del siguiente modo (equipo 01 puerto 2201, equipo 02 puerto 2202, ...)

En el archivo de configuración tenemos una opción al inicio del fichero que se llama PORT, deberemos descomentarla que por defecto está en el puerto 22 y cambiarlo al puerto 2212 en mi caso porque mi puesto es el 12.

```
GNU nano 6.2                                    /etc/ssh/sshd_config

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

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

AllowUsers profesor@192.168.206.100 niclopez

Port 2212
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO
```

6. Conexión al servidor

a) Para comprobar que podemos conectarnos lo haremos con el siguiente comando desde cualquier de las otras máquinas Linux de la red virtual

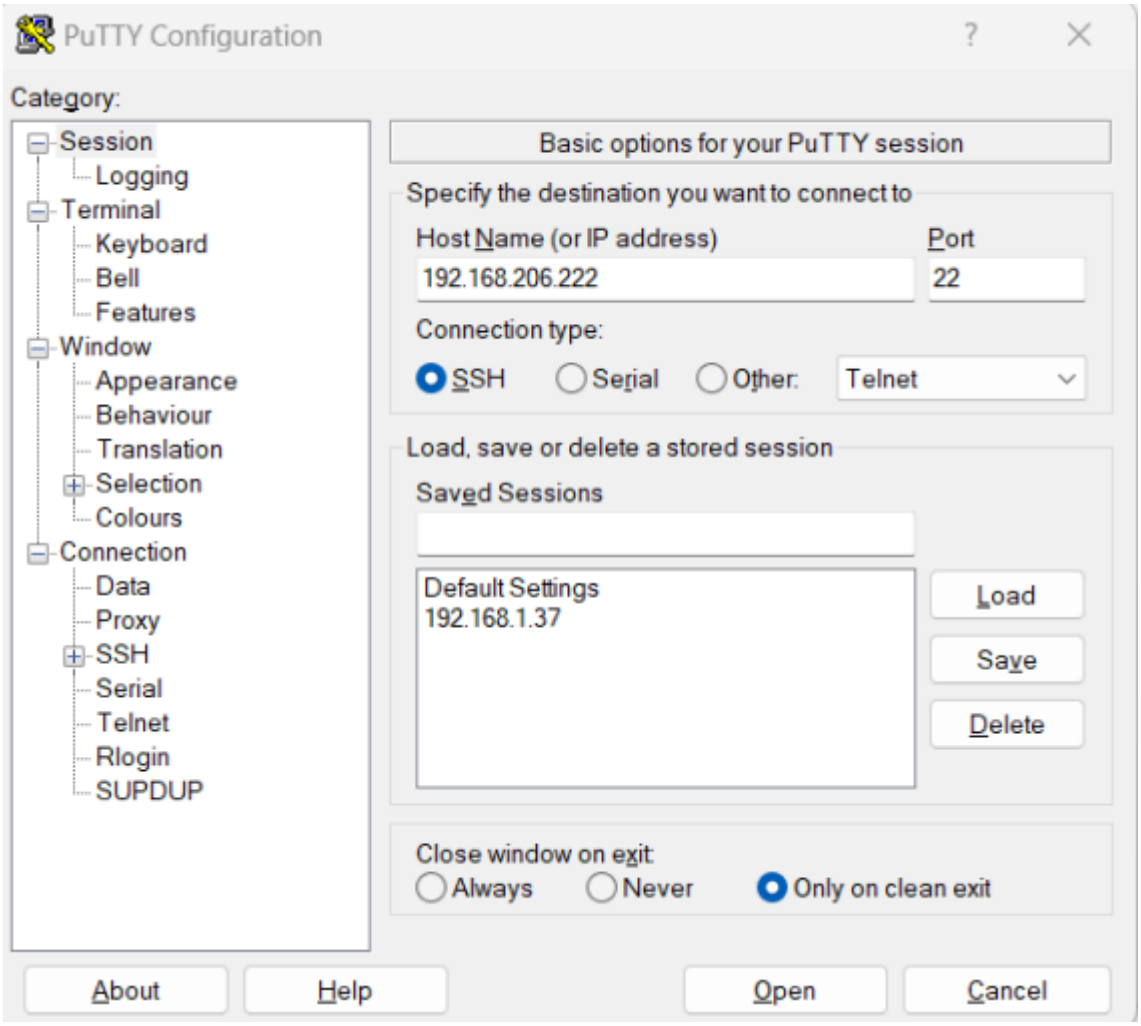
sudo ssh [usuario]@[IP maquina] –p [puerto]

sudo ssh niclopez@localhost –p 2212

```
→ ssh sudo ssh niclopez@localhost -p 2212
niclopez@localhost's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-51-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 16 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

8 actualizaciones de seguridad adicionales se pueden aplicar con ESM Apps.
Aprenda más sobre cómo activar el servicio ESM Apps at https://ubuntu.com/esm

New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Sat Feb  1 17:08:27 2025 from 127.0.0.1
→ ~
```

b) Vamos a comprobar que podemos conectarnos desde la máquina Windows7 de la red virtual. Para ello utilizaremos el cliente Putty

1. Abre **PuTTY** en Windows.
2. En "Host Name", ingresa la **IP del servidor** (192.168.1.100).
3. En "Port", ingresa el puerto configurado (2201).
4. Selecciona **SSH** y haz clic en "Open".
5. Aparecerá una alerta con el **fingerprint** de la clave pública del servidor.
6. Confirma que el fingerprint es correcto ejecutando en el servidor:
   ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key
7. Si el fingerprint coincide, acepta la conexión e inicia sesión con el usuario y contraseña.



En la terminal nos pedirá con que usuario queremos iniciar sesión y su contraseña correspondiente. Y entonces nos dejara conectarnos a la maquina indicada.

7. Configuración avanzada de SSH

a) Crear en la MV donde se ha instalado el servidor SSH un nuevo usuario profesor. Configurar el servidor SSH para que sólo pueda conectarse el usuario profesor

b) Restringir aún más el acceso, permitiendo que el usuario profesor pueda conectarse únicamente desde la IP del equipo del profesor 192.168.206.100

```
➜  ~ sudo adduser profesor
Añadiendo el usuario `profesor' ...
Añadiendo el nuevo grupo `profesor' (1002) ...
Añadiendo el nuevo usuario `profesor' (1002) con grupo `profesor' ...
Creando el directorio personal `/home/profesor' ...
Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
CONTRASEÑA INCORRECTA: De alguna manera, en la contraseña se lee el nombre del usuario
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para profesor
Introduzca el nuevo valor, o presione INTRO para el predeterminado
        Nombre completo []:
        Número de habitación []:
        Teléfono del trabajo []:
        Teléfono de casa []:
        Otro []:
¿Es correcta la información? [S/n] S
➜  ~ sudo systemctl restart ssh
```

Una vez creado el usuario profesor, accederemos al archivo de configuración de SSH y añadiremos la directiva AllowUsers seguida del usuario@[IP] para que solo cierto usuario pueda acceder desde dicha IP, en el caso de que queramos que el usuario pueda acceder desde cualquier IP, simplemente pondremos el usuario.

```
  GNU nano 6.2                                  /etc/ssh/sshd_config

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

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

AllowUsers profesor@192.168.206.100 niclopez

Port 2212
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO
```

c) Limitar el número de reintentos de conexión a 3 mediante la directiva correspondiente

En el archivo de configuración hay una directiva llamada MaxAuthTries que se encontrara comentada, por defecto son 6 intentos de conexión, nosotros la descomentaremos y cambiaremos el valor a 3.