

Índice:

Ejercicio 1	2
a) Instala y configura un servidor SSH/SFTP. Utilizar un cliente SFTP y SCP.	2
b) Demuestra la seguridad realizando capturas con un sniffer.	5

Ejercicio 1

a) Instala y configura un servidor SSH/SFTP. Utilizar un cliente SFTP y SCP.

Solución:

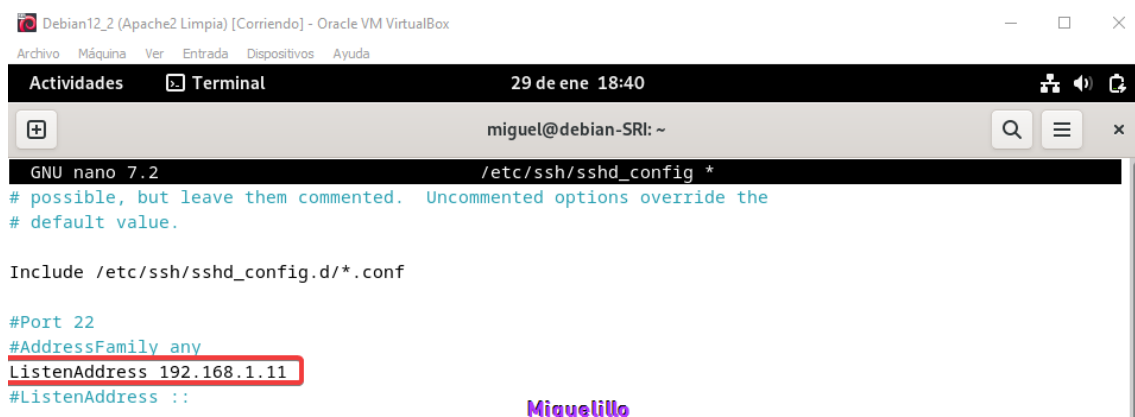
Instalamos SSH servidor y cliente



A terminal window titled 'Debian12_2 (Apache2 Limpia) [Corriendo] - Oracle VM VirtualBox'. The terminal shows the command `sudo apt-get install openssh-server openssh-client` being executed. The output indicates that the package list is being read and the installation is complete. The user 'miguel' is logged in at 'debian-SRI'.

```
miguel@debian-SRI:~$ sudo apt-get install openssh-server openssh-client
Leyendo lista de paquetes... Hecho
```

Vamos a la configuración y le indicamos la ip del servidor



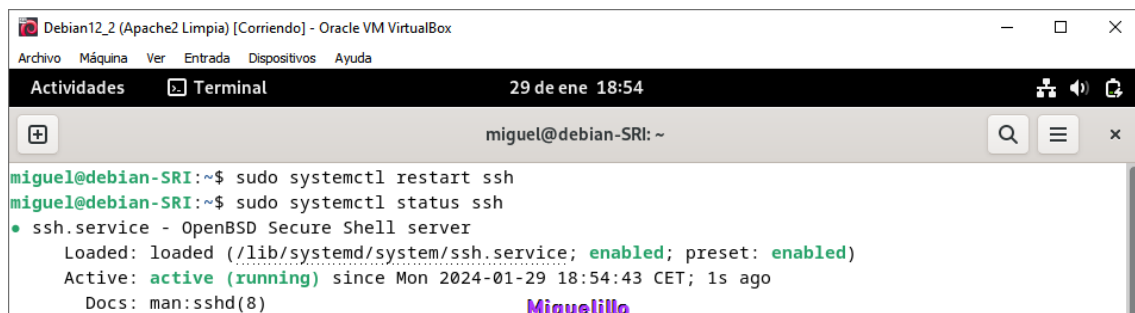
A terminal window titled 'Debian12_2 (Apache2 Limpia) [Corriendo] - Oracle VM VirtualBox'. The terminal shows the configuration of the SSH server using the `nano` editor. The configuration file `/etc/ssh/sshd_config` is being edited. The `ListenAddress` is set to `192.168.1.11`. The user 'miguel' is logged in at 'debian-SRI'.

```
GNU nano 7.2 /etc/ssh/sshd_config *
# possible, but leave them commented. Uncommented options override the
# default value.

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

#Port 22
#AddressFamily any
ListenAddress 192.168.1.11
#ListenAddress ::
```

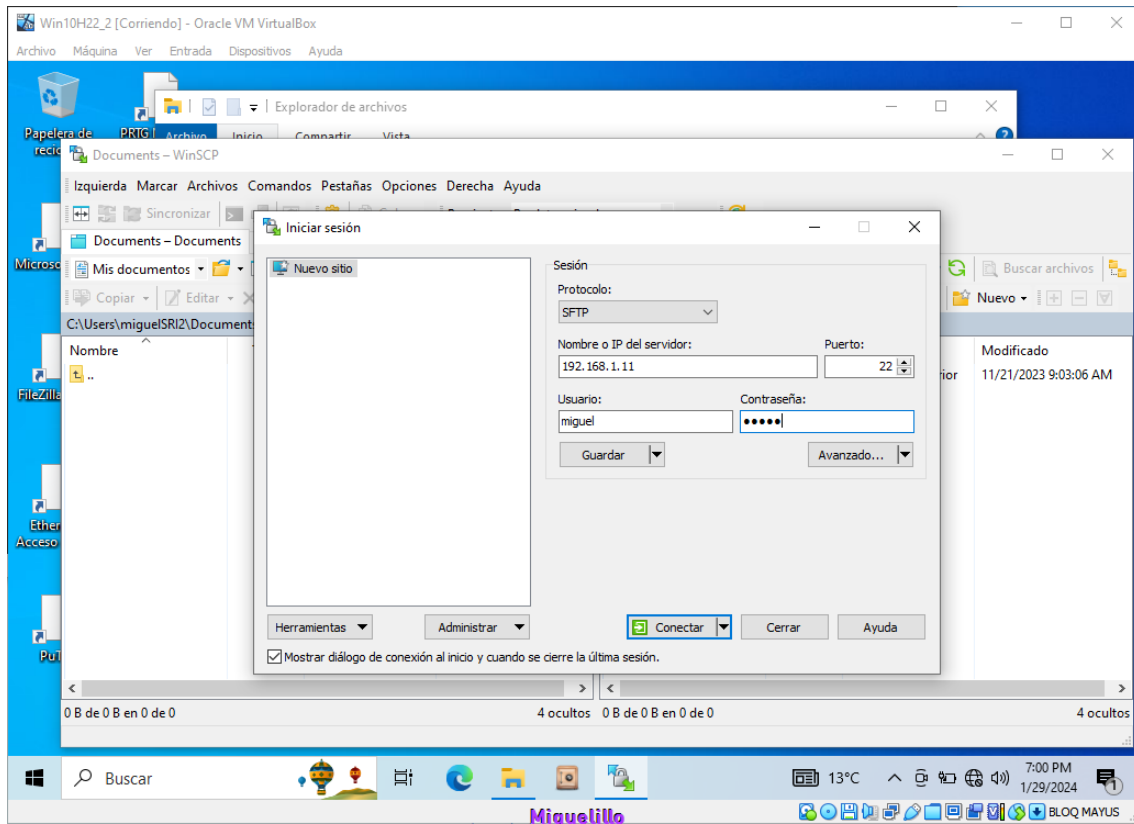
Reiniciamos el servicio



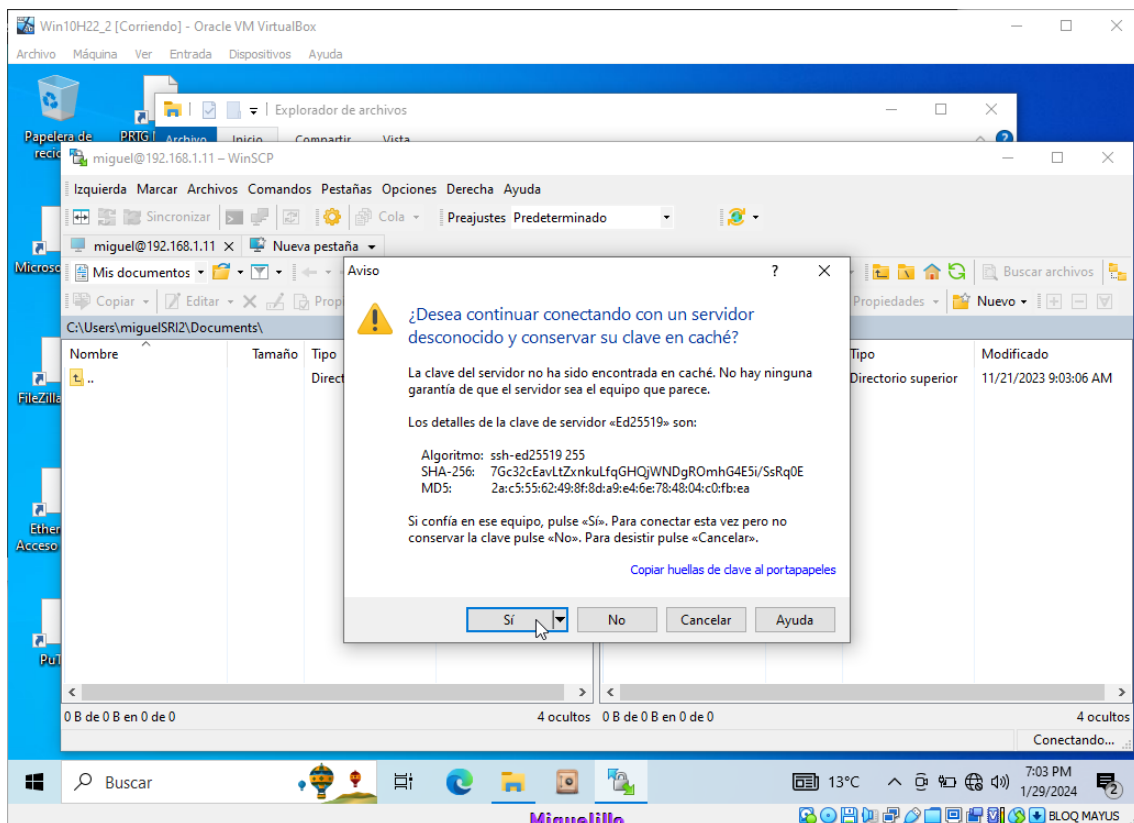
A terminal window titled 'Debian12_2 (Apache2 Limpia) [Corriendo] - Oracle VM VirtualBox'. The terminal shows the command `sudo systemctl restart ssh` being executed, followed by `sudo systemctl status ssh`. The output shows that the `ssh.service` is loaded and active (running). The user 'miguel' is logged in at 'debian-SRI'.

```
miguel@debian-SRI:~$ sudo systemctl restart ssh
miguel@debian-SRI:~$ sudo systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-01-29 18:54:43 CET; 1s ago
     Docs: man:sshd(8)
```

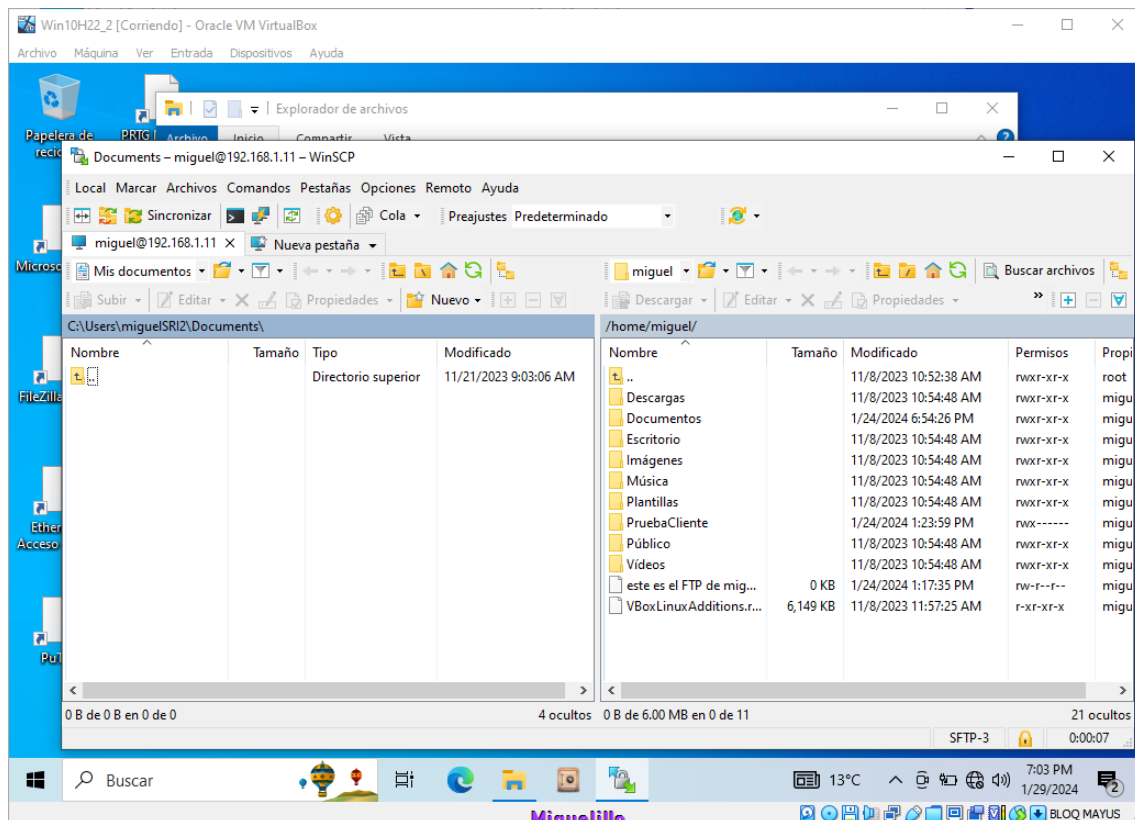
Prueba en el Cliente nos instalamos WinSCP, introducimos el protocolo, la IP el puerto el usuario y la contraseña.



Guardamos la caché



Se ha iniciado la conexión



b) Demuestra la seguridad realizando capturas con un sniffer.

Solución:

Si miramos desde WireShark veremos que las comunicaciones al servidor están cifradas

The screenshot shows a Wireshark capture of an SSH session. The packet list pane displays several packets, with the first few being encrypted (len=96). The packet details pane for frame 22 shows the following information:

- Frame 22: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
- Ethernet II, Src: PcsCompu_9e:b4:ba (08:00:27:9e:b4:ba), Dst: PcsCompu_bb:2e:1a (08:00:00:00:00:00)
- Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.10
- Transmission Control Protocol, Src Port: 22, Dst Port: 65284, Seq: 1, Ack: 97, Len: 96
- SSH Protocol
 - Packet Length (encrypted): 72a5a389
 - Encrypted Packet: 6629bb4afb77a10e0ed78f44cbcad29275d6dd2dbb5cc2da738708a7f5c073747
 - [Direction: server-to-client]

The packet bytes pane shows the raw data of the encrypted packet, which appears as a series of hexadecimal values.

Miguel Lillo