

**9 DE NOVIEMBRE DE 2025**

# **PRACTICA 1.6: SSH**

**IES SERRA PERENXISA**

**IZAN NAVARRO LUJAN**

**PRACTICA 6**

# ÍNDICE

1. INTRODUCCIÓN:.....	2
2. EJERCICIO 1:.....	2
3. EJERCICIO 2:.....	3
4. EJERCICIO 3: .....	10
5. EJERCICIO 4 (Opcional):.....	11

## 1. INTRODUCCIÓN:

Secure Shell (SSH) es una de las herramientas más importantes y utilizadas en la administración de sistemas y redes, proporcionando un método seguro y confiable para la gestión remota de dispositivos. SSH permite establecer conexiones cifradas, proteger la transferencia de datos y garantizar que la comunicación entre el cliente y el servidor esté resguardada de amenazas externas.

En esta práctica, se explorarán los conceptos fundamentales y avanzados de SSH, incluyendo su instalación, configuración y uso tanto en sistemas cliente como servidor. Los participantes aprenderán a establecer sesiones seguras, gestionar claves de autenticación y aplicar buenas prácticas de seguridad para fortalecer el acceso remoto.

El objetivo de esta práctica es no solo familiarizarse con la utilidad de SSH, sino también comprender sus beneficios en la protección de la integridad y confidencialidad de la información. Esta experiencia práctica proporcionará las habilidades esenciales para administrar sistemas de manera segura y eficiente, un conocimiento vital para cualquier profesional de TI.

## 2. EJERCICIO 1:

Comenta con tus palabras qué es SSH, diferencias con TELNET, puertos que utiliza, versiones del protocolo, si son compatibles entre ellas, los archivos de instalación más importantes y todo aquel detalle que consideres relevante.

SSH es un protocolo de red que permite acceder de forma segura y cifrada a otro equipo a través de una red, normalmente para administrar servidores o transferir archivos.

Telnet es un protocolo de red que permite conectarse de forma remota a otro equipo para controlarlo mediante una línea de comandos.

### Diferencias entre SSH y Telnet:

- Seguridad:
  - **SSH:** Cifra toda la comunicación (usuario, contraseña y datos).
  - **Telnet:** Transmite la información en texto plano, sin cifrado.
- Autenticación:
  - **SSH:** Usa contraseñas cifradas o claves públicas/privadas.
  - **Telnet:** Solo contraseñas simples.
- Uso actual:
  - **SSH:** Estándar actual en administración remota.
  - **Telnet:** Prácticamente en desuso por inseguro.

### Puertos utilizados:

- **SSH:** Puerto **22** (por defecto).
- **Telnet:** Puerto **23**.

### Versiones del protocolo SSH:

1. **SSH-1:** Primera versión, hoy obsoleta por vulnerabilidades.
2. **SSH-2:** Versión actual y segura, mejora en cifrado, autenticación y compresión.

**Compatibilidad:** SSH-1 y SSH-2 no son compatibles entre sí.

### Otros detalles relevantes:

- Permite túneles cifrados (tunneling), reenvío de puertos y transferencia segura de archivos (con SCP o SFTP).
- Implementaciones populares: OpenSSH, PuTTY, Dropbear.
- Disponible en Linux, macOS y Windows.

## 3.EJERCICIO 2:

Previamente a la realización de la actividad les he asignado a las 2 VM una tipología de “Red interna” y asignado una IP de manera manual ‘192.168.100.11/24’ para Ubuntu y ‘192.168.100.10/24’ para Ubuntu Server.

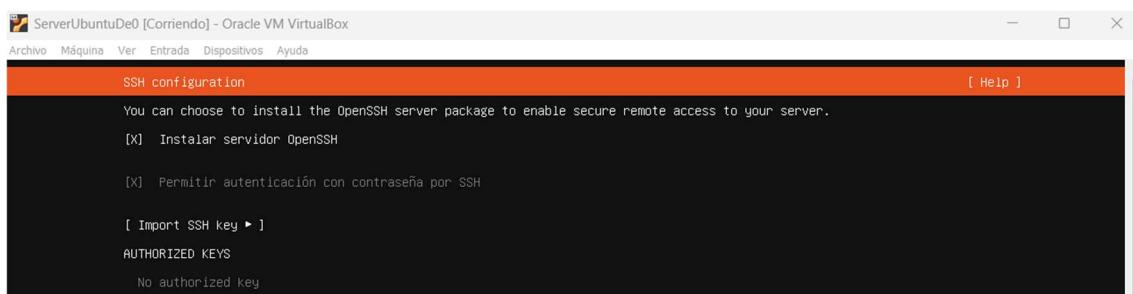
The screenshot shows two terminal windows side-by-side. The top window is titled 'izan@Izan-Ubuntu20: ~/Escritorio' and displays the contents of the file '/etc/netplan/01-network-manager-all.yaml'. It contains the following YAML configuration:

```
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.100.11/24]
  version: 2
```

The bottom window is titled 'GNU nano 7.2 /etc/netplan/00-installer-config.yaml' and displays the contents of the file. It contains the following YAML configuration:

```
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.100.10/24]
  version: 2
```

Acto seguido arrancamos el Ubuntu Server e instalamos.



- Muestra como instalarías tanto el servicio de servidor como de cliente de SSH

Para la instalación de SSH dentro del cliente, se utilizaría el siguiente comando (en este caso yo ya lo tengo instalado):

```
Izan@Izan-Ubuntu20:~/Escritorio$ sudo apt install openssh-client -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
openssh-client ya está en su versión más reciente (1:8.2p1-4ubuntu0.13).
fijado openssh-client como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 67 no actualizados.
```

Para la instalación de SSH con el servicio de servidor usaremos el siguiente comando (en este caso ya lo tengo instalado):

```
Izan@izanserver:~/ Escritorio$ sudo apt install openssh-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
openssh-server ya está en su versión más reciente (1:9.6p1-3ubuntu13.14).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 25 no actualizados.
```

He tenido que añadir un segundo adaptador de red “NAT” para poder estar conectado a internet y modificado el archivo “01-network-manager-all.yaml” añadiendo también el segundo adaptador:

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      dhcp4: no
      addresses: [192.168.100.10/24]
```

- Muestra los archivos de configuración más relevantes

He seleccionado los archivos más importantes del servidor y cliente que son: “sshd\_config” (para servidor) y “ssh\_config” (para cliente).

```
GNU nano 7.2 /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

# When systemd socket activation is used (the default), the socket
# configuration must be re-generated after changing Port, AddressFamily, or
# ListenAddress.
#
# For changes to take effect, run:
#
# systemctl daemon-reload
# systemctl restart ssh.socket
#
#Port 22
#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

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
izan@Izan-Ubuntu20: ~/Escritorio
GNU nano 4.8 /etc/ssh/ssh_config

# Site-wide defaults for some commonly used options. For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

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

Host *
# ForwardAgent no
# ForwardX11 no
# ForwardX11Trusted yes
# PasswordAuthentication yes
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP yes
# AddressFamily any

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex^J Justificar^C Posición
^X Salir ^R Leer fich.^V Reemplazar^U Pegar ^T Ortografía^L Ir a línea
```

- Antes de realizar ninguna configuración, realizar una copia de seguridad de los ficheros de configuración, con el comando “cp”.

Realizo la copia de seguridad del archivo “ssh\_config” de la máquina cliente:

```
izan@Izan-Ubuntu20:~/Escritorio$ sudo cp /etc/ssh/ssh_config /etc/ssh/ssh_config
.backup
```

Realizo la copia de seguridad del archivo “sshd\_config” de la máquina servidor:

```
izan@izanserver:~$ sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.backup
```

- Muestra el archivo de configuración donde viene configurado el puerto por defecto y cámbialo a otro diferente. ¿Por qué consideras que es importante cambiar el puerto por defecto?

El archivo con la línea modificada (puerto 222 como puerto):

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

# When systemd socket activation is used (the default), the socket
# configuration must be re-generated after changing Port, AddressFamily, or
# ListenAddress.
#
# For changes to take effect, run:
#
#   systemctl daemon-reload
#   systemctl restart ssh.socket
#
#Port 222
#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
```

Cambiar el puerto por defecto nos ayudará a que en posibles ataques de bots, no prueben con puertos por defecto, como por ejemplo, el 22 en este caso.

```
izan@izanserver:~$ sudo systemctl restart ssh
```

Ejecutamos el comando para reiniciar el servicio y que se apliquen TODOS los cambios.

- Deniega la autenticación con el usuario root Aquí la línea del archivo “sshd\_config” cambiada:

```

Port 222
#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

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

```

- Cambia las versiones del protocolo SSH entre cliente y servidor y comenta si se puede establecer la conexión.

Dentro del archivo “sshd\_config” tenemos las versiones del protocolo en la siguiente línea, por defecto se pondrá la versión más moderna (la v.2) sin poner nada dentro del documento, pero yo lo he añadido para que se vea de manera visual:

```

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem      sftp    /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
Protocol 2

```

Si intentamos hacer un ssh con la versión 1 (la más antigua), dará error:

```

izan@Izan-Ubuntu20:~/Escritorio$ ssh -1 izan@192.168.100.10
SSH protocol v.1 is no longer supported

```

- Al establecer la conexión SSH, nos muestra un mensaje con la fecha de la última conexión, ¿Cómo y dónde modificarías este mensaje? Cambia el mensaje añadiendo tu nombre completo

Una vez entro desde El Cliente al Servidor, lanzo ssh y me conecta:

```

.ian@Izan-Ubuntu20:~/Escritorio$ ssh -p 222 ian@192.168.100.10
The authenticity of host '[192.168.100.10]:222 ([192.168.100.10]:222)' can't be established.
ECDSA key fingerprint is SHA256:yoFJCnSt4A0Iq0IjiEq8J09WgRnXttdbLj0TIVGTIBI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.100.10]:222' (ECDSA) to the list of known hosts.
ian@192.168.100.10's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-87-generic x86_64)

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

System information as of jue 06 nov 2025 18:48:14 UTC

System load:  0.0          Processes:           119
Usage of /:   40.8% of 6.28GB  Users logged in:      1
Memory usage: 6%           IPv4 address for enp0s3: 10.0.2.15
Swap usage:   0%

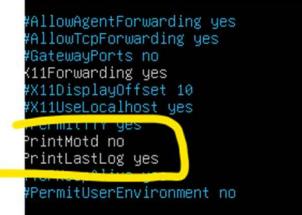
El mantenimiento de seguridad expandido para Applications está desactivado
Se pueden aplicar 25 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status».

.ian@izanserver:~$ █

```

Pero no se muestran estos datos de conexión, por lo tanto me toca entrar dentro del fichero “sshd\_config” para activar el “PrintLastLog yes” y así poder mostrarse en el log cuando se conecta por ssh.



```

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#X11Forwarding yes
PrintMotd no
PrintLastLog yes
#Banner ~
#PermitUserEnvironment no

```

```

.ian@Izan-Ubuntu20:~/Escritorio$ ssh -p 222 ian@192.168.100.10
ian@192.168.100.10's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-87-generic x86_64)

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

System information as of jue 06 nov 2025 19:00:58 UTC

System load:  0.03          Processes:           120
Usage of /:   40.8% of 6.28GB  Users logged in:      1
Memory usage: 6%           IPv4 address for enp0s3: 10.0.2.15
Swap usage:   0%

El mantenimiento de seguridad expandido para Applications está desactivado
Se pueden aplicar 25 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status».

Last login: Thu Nov  6 18:48:15 2025 from 192.168.100.11
.ian@izanserver:~$ █

```

Para poder cambiar este ajuste iríamos al archivo “/etc/motd” y agregaríamos un nuevo mensaje:

```

. GNU nano 7.2                                     /etc/motd *
Bienvenido al Servidor SSH - Administrado por Izan Navarro Lujan_

```

Y se mostraría algo tal que así:

```
Izan@Izan-Ubuntu20:~/Escritorio$ ssh -p 222 izan@192.168.100.10
Izan@192.168.100.10's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-87-generic x86_64)

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

System information as of jue 06 nov 2025 19:08:22 UTC

 System load: 0.0          Processes:           121
 Usage of /: 40.8% of 6.28GB   Users logged in:      1
 Memory usage: 6%           IPv4 address for enp0s3: 10.0.2.15
 Swap usage: 0%

El mantenimiento de seguridad expandido para Applications está desactivado
Se pueden aplicar 25 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status».

Bienvenido al Servidor SSH - Administrado por Izan Navarro Lujan
Last login: Thu Nov  6 19:00:59 2025 from 192.168.100.11
Izan@izanserver:~$
```

- Que es la redirección x11. Configura el servidor SSH para que acepte esta redirección  
Entramos dentro del archivo sshd\_config y descomentamos las líneas siguientes

```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
PrintLastLog yes
#TCPKeepAlive yes
```

- Crea varios usuarios en el servidor y configúralo para que solo se permita la autenticación con un usuario determinado.

Para restringir el acceso solo por SSH a un usuario en concreto añadiremos la línea “AllowUsers <Usuario>” dentro del fichero “sshd\_config”:

```
# override default of no subsystems
Subsystem    sftp    /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server
Protocol 2
AllowUsers izan_
```

Para poder añadir todos los cambios realizados en el archivo “sshd\_config” ejecutaremos el siguiente comando:

```
izan@izanserver:~$ sudo systemctl restart ssh
```

## 4. EJERCICIO 3:

### Acceso con claves compartidas

- ¿Qué ventajas nos aporta el acceso con claves compartidas?  
Es una forma más segura y eficiente de autenticarse al servidor. Esto nos ofrece:
  - Mayor Seguridad
  - Evita el envío de contraseñas por la red
  - Control de acceso más sencillo
  - Acceso automático
- Realiza toda la configuración necesaria, para autenticarse por SSH en un servidor mediante el uso de claves compartidas, explica como has creado las claves, como las has copiado en el servidor, donde se deben colocar, la evidencia de conexión mediante claves compartida y todo aquel dato que consideres relevante
- 

- 1) Primero creamos claves pública y privada por comando (estas claves se guardarán por defecto en la ruta /home/izan/.ssh/id\_rsa):

```
izan@Izan-Ubuntu20:~/Escritorio$ ssh-keygen -t rsa -b 4096 -C "izan@Izan-Ubuntu20"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/izan/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/izan/.ssh/id_rsa
Your public key has been saved in /home/izan/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Bu19zcRjIECnGj8W7SkvQGK2x3IDfCg3oUFvrGw6I1U izan@Izan-Ubuntu20
The key's randomart image is:
+---[RSA 4096]---+
|oo+ . |
|.o+* . |
|=B==E o |
|B=B* + +
|o**+= . S
|o+++. B .
|= . . . o
|.o .
+---[SHA256]---+
```

- 2) Copiamos la clave pública en el servidor con el siguiente comando (por defecto la clave se almacenará en la carpeta ".ssh/authorized\_keys"):

```
izan@Izan-Ubuntu20:~/Escritorio$ ssh-copy-id -p 222 izan@192.168.100.10
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
izan@192.168.100.10's password:

Number of key(s) added: 1

Now try logging into the machine, with:    "ssh -p '222' 'izan@192.168.100.10'"
and check to make sure that only the key(s) you wanted were added.

izan@Izan-Ubuntu20:~/Escritorio$
```

3) Una vez añadida la clave se podrá entrar al servidor sin necesidad de contraseña

```
Izan@Izan-Ubuntu20:~/Escritorio$ ssh -p 222 izan@192.168.100.10
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-87-generic x86_64)

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

System information as of dom 09 nov 2025 21:31:04 UTC

System load:  0.09      Processes:           115
Usage of /:   41.0% of 6.28GB  Users logged in:     1
Memory usage: 5%
Swap usage:   0%          IPv4 address for enp0s3: 10.0.2.15

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 25 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Bienvenido al Servidor SSH - Administrado por Izan Navarro Lujan
Last login: Thu Nov  6 19:08:23 2025 from 192.168.100.11
Izan@izanserver:~$ █
```

## 5. EJERCICIO 4 (Opcional):

Comenta cualquier otro dato, que hayas encontrado que sería interesante tener en cuenta, a la hora de configurar un servidor SSH. También puedes investigar los tipos de aplicaciones que nos permiten la conexión SSH desde un cliente Windows o cualquier otra cosa similar respecto a SSH que consideres.

A la hora de configurar un servidor SSH hay muchas pautas a tener en cuenta:

- 1) Cambiar el puerto por defecto añadiendo al archivo “sshd\_config” y cambiando el “Port 22” por Port “222”.
- 2) Deshabilitar el acceso directo al usuario root añadiendo la línea “PermitRootLogin no” dentro del archivo sshd\_config.
- 3) Usar claves públicas en lugar de contraseñas para así evitar ataques de fuerza bruta.
- 4) Limitar los usuarios que pueden conectarse por SSH añadiendo la línea “AllowUsers XXX” dentro del fichero sshd\_config.

### Aplicaciones para conexiones SSH desde Windows:

- PuTTY
- OpenSSH (Windows 10/11)
- WinSCP
- Bitvise SSH Client
- MobaXterm

Con una configuración adecuada, SSH se convierte en una herramienta **segura, estable y versátil** para la administración remota de sistemas.