



PRÁCTICA 1

SSH



SMRV2º

DIEGO EXTREMIANA
APLICACIONES WEB

ÍNDICE

❖ Contenido

| | |
|---|---|
| ❖ Preguntas sobre SSH | 2 |
| ❖ Instalación de SSH en Linux Cliente..... | 2 |
| ❖ Instalación de SSH en Linux Servidor | 3 |
| ❖ Conectarse desde un cliente Linux por SSH y desde un cliente Windows por SSH (Putty). . | 4 |
| ❖ Conectar los Linux (Cliente y Server) por medio de SSH..... | 5 |
| ❖ Claves RSA | 6 |
| ❖ Ejecutar una aplicación en entorno gráfico | 8 |

❖ Preguntas sobre SSH

1. ¿Qué es? ¿Cuándo lo utilizo?

Es un protocolo y un programa de manejo remoto de los servicios de tu equipo. Toda su información está cifrada. Lo usas cuando te conectas de forma remota a cualquier equipo o a centros de datos.

2. ¿Existe alguna alternativa? → Ventajas e inconvenientes

Telnet, aunque no hay muchas ventajas contra SSH, además no está encriptado.

❖ Instalación de SSH en Linux Cliente

Lo primero es instalar el servidor SSH en nuestra máquina de Cliente Ubuntu:

```
diegoex@DiegoEx:~$ sudo apt install openssh-server  
[sudo] contraseña para diegoex:
```

Luego vamos a comprobar que funciona:

```
diegoex@DiegoEx:~$ sudo systemctl status ssh  
● ssh.service - OpenBSD Secure Shell server  
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)  
   Active: active (running) since Mon 2020-09-14 11:12:01 CEST; 13min ago  
     Docs: man:sshd(8)  
           man:sshd_config(5)  
  Main PID: 2348 (sshd)  
    Tasks: 1 (limit: 1111)  
   Memory: 1.3M  
    CGroup: /system.slice/ssh.service  
            └─2348 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups  
  
sep 14 11:12:00 DiegoEx systemd[1]: Starting OpenBSD Secure Shell server...  
sep 14 11:12:01 DiegoEx sshd[2348]: Server listening on 0.0.0.0 port 22.  
sep 14 11:12:01 DiegoEx sshd[2348]: Server listening on :: port 22.  
sep 14 11:12:01 DiegoEx systemd[1]: Started OpenBSD Secure Shell server.  
lines 1-15/15 (END)
```

Ahora vamos a abrir el puerto de Ubuntu para poder conectarnos desde Putty (en uno de los siguientes apartados):

```
diegoex@DiegoEx:~$ sudo ufw allow ssh  
Reglas actualizadas  
Reglas actualizadas (v6)
```

Comprobamos cual es nuestra dirección IP:

```
diegoex@ubuntu:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:5e:20:21 brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.128/24 brd 192.168.80.255 scope global dynamic noprefixroute ens33
        valid_lft 1653sec preferred_lft 1653sec
    inet6 fe80::96c5:423a:b5d:42b4/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

❖ Instalación de SSH en Linux Servidor

Seguiremos exactamente los mismos pasos para instalar SSH en el servidor que en el cliente:

Instalamos SSH:

```
diegoex@diegoex:~$ sudo apt install openssh-server
[sudo] password for diegoex:
```

Comprobamos si funciona:

```
diegoex@diegoex:~$ sudo systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2020-09-14 10:18:12 UTC; 2min 18s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 718 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 721 (sshd)
      Tasks: 1 (limit: 1075)
     Memory: 2.3M
    CGroup: /system.slice/ssh.service
            └─721 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Sep 14 10:18:11 diegoex systemd[1]: Starting OpenBSD Secure Shell server...
Sep 14 10:18:12 diegoex sshd[721]: Server listening on 0.0.0.0 port 22.
Sep 14 10:18:12 diegoex sshd[721]: Server listening on :: port 22.
Sep 14 10:18:12 diegoex systemd[1]: Started OpenBSD Secure Shell server.
diegoex@diegoex:~$
```

Abrimos el puerto de Ubuntu para poder conectarnos a Putty (en el siguiente apartado):

```
diegoex@diegoex:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
```

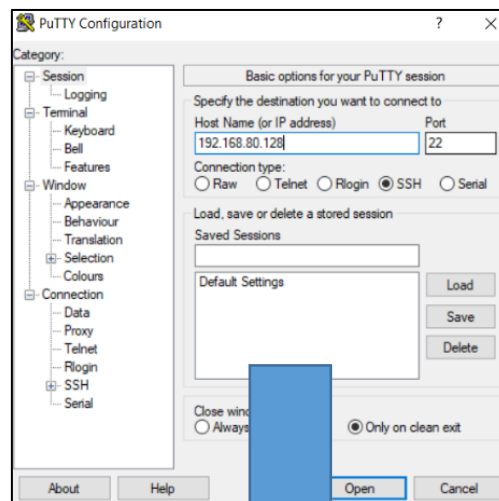
Ahora comprobaremos nuestra dirección IP:

```
diegoex@diegoex:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:00:64:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.130/24 brd 192.168.80.255 scope global dynamic ens33
        valid_lft 1775sec preferred_lft 1775sec
    inet6 fe80::20c:29ff:fe00:64b4/64 scope link
        valid_lft forever preferred_lft forever
```

❖ Conectarse desde un cliente Linux por SSH y desde un cliente Windows por SSH (Putty).

Después de haber comprobado nuestra dirección IP, la marcamos en putty (Marcando el puerto en el número 22)

```
diegoex@ubuntu:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:5e:20:21 brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.128/24 brd 192.168.80.255 scope global dynamic noprefixroute ens33
        valid_lft 1653sec preferred_lft 1653sec
    inet6 fe80::96c5:423a:b5d:42b4/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```



```
diegoex@ubuntu: ~
login as: diegoex
diegoex@192.168.80.128's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-47-generic x86_64)

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

0 actualizaciones se pueden instalar inmediatamente.
0 de estas actualizaciones son una actualización de seguridad.

Your Hardware Enablement Stack (HWE) is supported until April 2025.

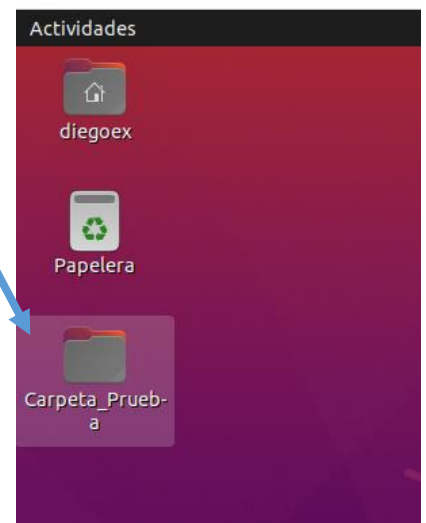
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

diegoex@ubuntu:~$
```

Ahora voy a crear una carpeta en el escritorio para probarlo:

```
diegoex@ubuntu:~$ cd Escritorio/
diegoex@ubuntu:~/Escritorio$ mkdir Carpeta_Prueba
diegoex@ubuntu:~/Escritorio$
```



❖ Conectar los Linux (Cliente y Server) por medio de SSH

Una vez instalado SSH en las dos máquinas, comprobamos si el servidor SSH está operativo, y comprobamos nuestra dirección IP:

```
diegoex@diegoex:~$ sudo systemctl status ssh
[sudo] password for diegoex:
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2020-09-15 07:52:48 UTC; 55s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 984 (sshd)
     Tasks: 1 (limit: 4587)
    Memory: 2.6M
   CGroup: /system.slice/ssh.service
           └─984 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Sep 15 07:52:47 diegoex systemd[1]: Starting OpenBSD Secure Shell server...
Sep 15 07:52:48 diegoex sshd[984]: Server listening on 0.0.0.0 port 22.
Sep 15 07:52:48 diegoex systemd[1]: Started OpenBSD Secure Shell server.
Sep 15 07:52:48 diegoex sshd[984]: Server listening on :: port 22.
diegoex@diegoex:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:00:64:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.130/24 brd 192.168.80.255 scope global dynamic ens33
        valid_lft 1560sec preferred_lft 1560sec
    inet6 fe80::20c:29ff:fe00:64b4/64 scope link
        valid_lft forever preferred_lft forever
```

Ahora, en el cliente, nos conectamos al server con el comando “ssh nombre@Dir. IP” y veremos que nos cambia el nombre del terminal:

```
diegoex@ubuntu:~$ ssh diegoex@192.168.80.130
Warning: Permanently added '192.168.80.130' (ECDSA) to the list of known hosts.
diegoex@192.168.80.130's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-47-generic x86_64)

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

System information as of Tue Sep 15 07:57:18 UTC 2020

System load:  0.09          Processes:      214
Usage of /:   33.2% of 18.57GB Users logged in: 1
Memory usage: 9%           IPv4 address for ens33: 192.168.80.130
Swap usage:   0%

30 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Last login: Tue Sep 15 07:53:04 2020
diegoex@diegoex:~$
```

Vemos que nos cambia el nombre de la máquina, eso significa que estamos conectados (el cliente al server).

Cuando queramos terminar, escribimos la palabra salir en inglés (exit) y saldremos de la conexión.

```
diegoex@diegoex:~$ exit
logout
Connection to 192.168.80.130 closed.
```

❖ Claves RSA

Desde Ubuntu cliente, generamos las claves RSA, que son las que le permitirán poder reconocernos al servidor SSH.

Para generarlas, “ssh-keygen”

```
diegoex@ubuntu:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/diegoex/.ssh/id_rsa):
/home/diegoex/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/diegoex/.ssh/id_rsa
Your public key has been saved in /home/diegoex/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:MeEMpbuxZGI3YIq1ZbVm05/u+3+/SJ0u5F8pkSobzEY diegoex@ubuntu
The key's randomart image is:
+---[RSA 3072]---+
|                 o.o                 |
|                . * .                 |
|               . = = =                |
|              o * + o o                |
|             . o o X SE o             |
|            . = B+. . o .             |
|           o o* o = o                 |
|          .. * o *                   |
|         .+++.++= oo|                 |
+-----[SHA256]-----+
```

Entramos en la carpeta .ssh, donde se ha guardado las claves RSA (privada y pública).

Usamos el comando scp para copiar el archivo de su ubicación a una carpeta temporal del servidor.

```
diegoex@ubuntu:~/.ssh$ sudo scp id_rsa.pub diegoex@192.168.80.130:/tmp
diegoex@192.168.80.130's password:
id_rsa.pub                               100% 568    387.7KB/s   00:00
```

Nos conectamos al servidor SSH y nos vamos a la ubicación `.ssh/` del servidor:

```
diegoex@ubuntu:~/.ssh$ sudo ssh diegoex@192.168.80.130
diegoex@192.168.80.130's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-48-generic x86_64)

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

System information as of Thu 22 Oct 2020 11:49:37 AM UTC

System load:  0.0               Processes:    227
Usage of /:   35.2% of 18.57GB   Users logged in: 1
Memory usage: 12%              IPv4 address for ens33: 192.168.80.130
Swap usage:  0%

 * Kubernetes 1.19 is out! Get it in one command with:

   sudo snap install microk8s --channel=1.19 --classic

https://microk8s.io/ has docs and details.

0 updates can be installed immediately.
0 of these updates are security updates.

*** System restart required ***
Last login: Thu Oct 22 11:36:27 2020 from 192.168.80.137
```

En la carpeta `.ssh/` del servidor añadiremos nuestra clave pública a la lista de claves autorizadas.

```
diegoex@diegoex:~$ cd ~/.ssh/
diegoex@diegoex:~/.ssh$ cat /tmp/id_rsa.pub >> authorized-keys
diegoex@diegoex:~/.ssh$
```

Luego borraremos la clave pública de la carpeta temporal.

```
diegoex@diegoex:~/.ssh$ rm /tmp/id_rsa.pub
```

Con esto hemos conseguido que el servidor no nos pregunte por la contraseña, ya que nos reconocerá, para comprobarlo, he salido del ssh y he vuelto a entrar:

```
diegoex@ubuntu:~$ ssh diegoex@192.168.80.130
The authenticity of host '192.168.80.130 (192.168.80.130)' can't be established.
ECDSA key fingerprint is SHA256:a/PZfQaMXResqaJ0Lx/dcZOFhxy6hCURSRG3WTD8/Y.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.80.130' (ECDSA) to the list of known hosts.
```


❖ Ejecutar una aplicación en entorno gráfico

Antes de salir, he ejecutado un comando.

Ya que no he podido abrir un programa como libreoffice (porque Ubuntu server no lo incluye en su instalación y forma parte de la versión de escritorio), me he instalado en el servidor un paquete llamado “figlet”, lo he probado desde el cliente y ha funcionado

Para ejecutar una aplicación, un comando, etc, el comando que debemos usar es el siguiente:

“ssh -X -p 22 (usuario)@(dirección IP) (programa/comando)”

```
diegoex@diegoex:~$ ssh -X -p 22 diegoex@192.168.80.130 figlet hola
diegoex@192.168.80.130's password:
  _ _ _ _ _
 |h|o|l|a|
 |_|_|_|_|
diegoex@diegoex:~$ exit
logout
Connection to 192.168.80.130 closed.
diegoex@ubuntu:~$ figlet hola

No se ha encontrado la orden «figlet», pero se puede instalar con:

sudo snap install figlet # version 2.2.5+git24.202a0a8, or
sudo apt install figlet # version 2.2.5-3
sudo apt install toilet # version 0.3-1.2

Consulte «snap info figlet» para ver más versiones.
```