



## Práctica 6.5: Servidor *OpenSSH* en *Linux*

Instala el servidor *OpenSSH* (<http://www.openssh.com/>) en la máquina **ServidorLinuxXX** para permitir su administración remota.

### 1. Instalación

- 1.1. Inicia una sesión en **ServidorLinuxXX** con un usuario con privilegios de administración.
- 1.2. Instala el servidor desde los repositorios oficiales de *Ubuntu*.

```
sudo apt-get update
sudo apt-get install openssh-server
```

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`.

- 1.3. Comprueba que el servidor está iniciado y escuchando peticiones en el puerto 22/TCP.

```
ps -ef | grep ssh
netstat -ltn
```

- 1.4. Consulta las claves públicas (\*.pub) y privadas dentro del directorio `/etc/ssh`, Figura 1.

```
alumno@ServidorLinux01:/etc/ssh$ ls -l
total 284
-rw-r--r-- 1 root root 242091 may 12 2014 moduli
-rw-r--r-- 1 root root 1690 may 12 2014 ssh_config
-rw-r--r-- 1 root root 2541 jun 8 16:36 sshd_config
-rw----- 1 root root 668 jun 8 16:36 ssh_host_dsa_key
-rw-r--r-- 1 root root 620 jun 8 16:36 ssh_host_dsa_key.pub
-rw----- 1 root root 227 jun 8 16:36 ssh_host_ecdsa_key
-rw-r--r-- 1 root root 192 jun 8 16:36 ssh_host_ecdsa_key.pub
-rw----- 1 root root 432 jun 8 16:36 ssh_host_ed25519_key
-rw-r--r-- 1 root root 112 jun 8 16:36 ssh_host_ed25519_key.pub
-rw----- 1 root root 1679 jun 8 16:36 ssh_host_rsa_key
-rw-r--r-- 1 root root 412 jun 8 16:36 ssh_host_rsa_key.pub
-rw-r--r-- 1 root root 338 jun 8 16:36 ssh_import_id
alumno@ServidorLinux01:/etc/ssh$
```

Figura 1: Claves del servidor SSH

### 2. Configuración por defecto

- 2.1. Consulta el fichero de configuración de servidor `/etc/ssh/sshd_config` y analiza las directivas habilitadas.
- 2.2. Observa por ejemplo que el servidor escucha peticiones en el puerto 22 (directiva `Port`) y que se permite el acceso al usuario root pero utilizando autenticación por clave pública (no con password) (directiva `PermitRootLogin`).

### 3. Conexión al servidor

- 3.1. En **DesarrolloW7XX** inicia el cliente *PuTTY* y establece una conexión SSH al servidor, Figura 2.

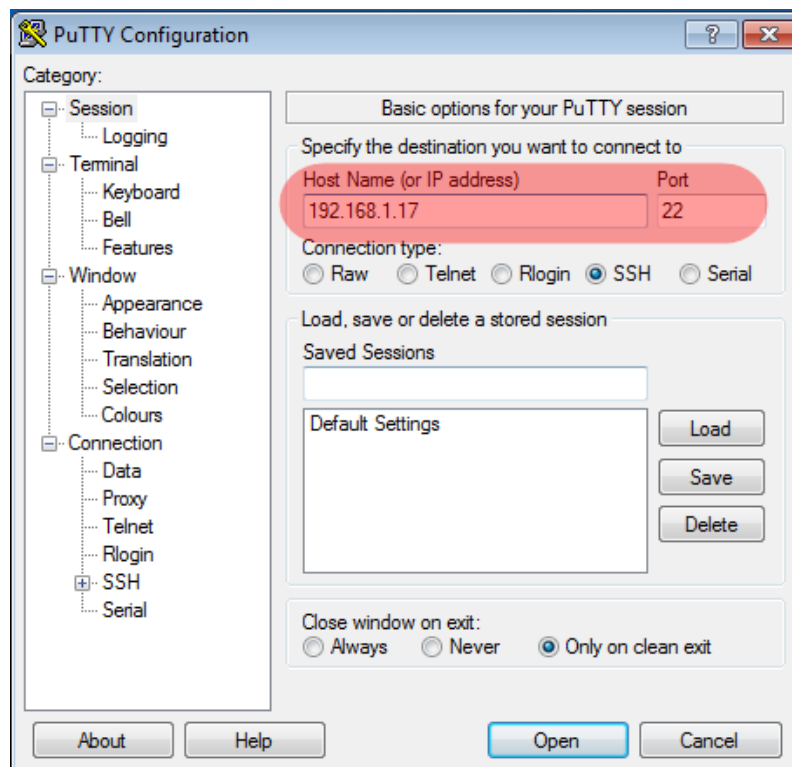


Figura 2: Conexión SSH

- 3.2. En servidor envía un resumen (*fingerprint*) de su clave pública RSA, Figura 3.

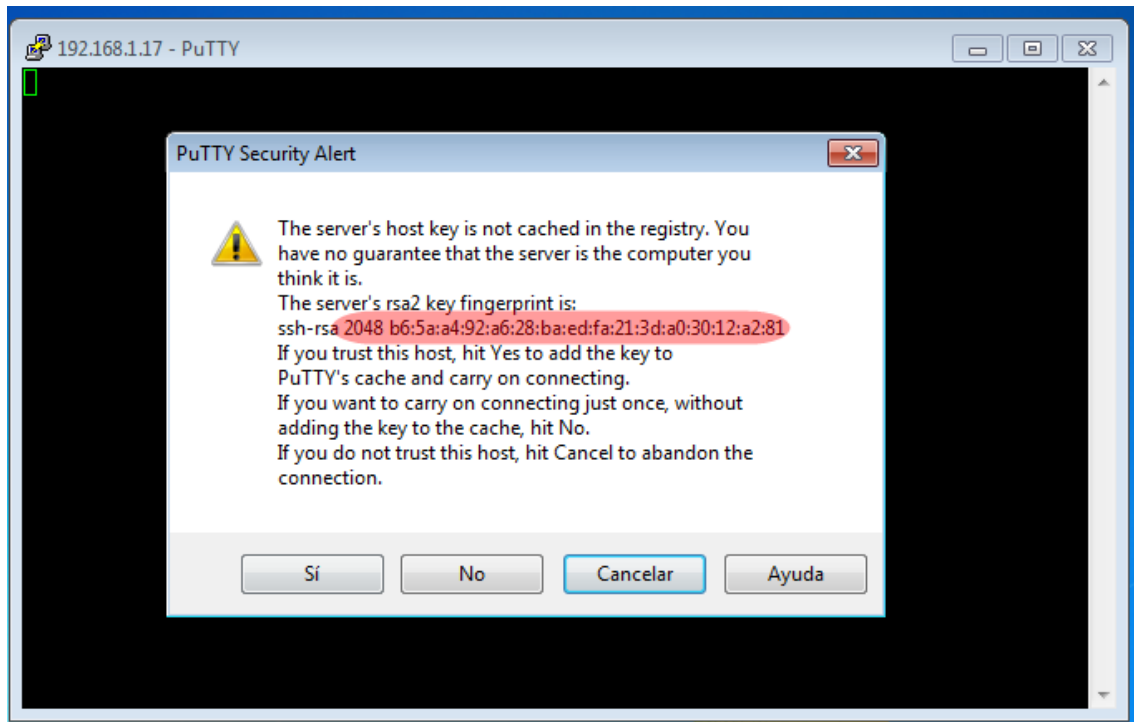


Figura 3: *Fingerprint* de la clave pública RSA enviada por el servidor SSH

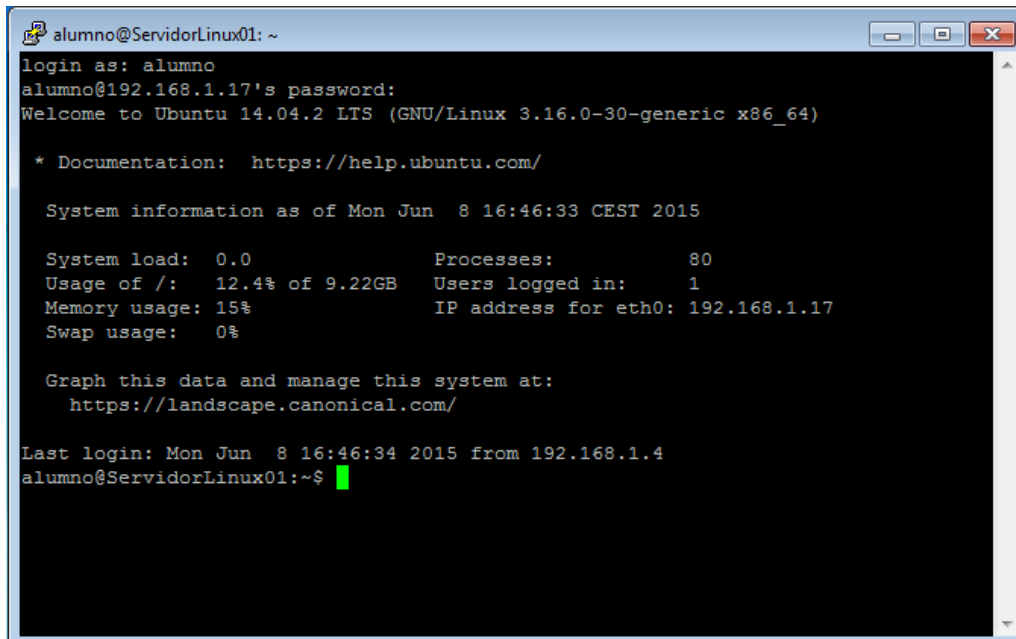
En este punto debemos comprobar que es realmente el resumen de la clave del servidor para evitar una suplantación de identidad (podemos ir al servidor y ejecutar el comando `ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key`) para obtener el *fingerprint* de la clave), Figura 4.

```
alumno@ServidorLinux01:~$ ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key.pub
2048 b6:5a:a4:92:a6:28:ba:ed:fa:21:3d:a0:30:12:a2:81 root@ServidorLinux01.daw01
.net (RSA)
alumno@ServidorLinux01:~$ _
```

Figura 4: *Fingerprint* de la clave pública RSA del servidor SSH

El cliente SSH almacena el *fingerprint* de la clave del servidor. En las próximas conexiones ya no pide la aceptación por parte del usuario. Si en una conexión el *fingerprint* enviado por el servidor no coincide con el almacenado por el cliente se avisará al usuario.

3.3. Inicia sesión como usuario alumno, Figura 5.



The image shows a terminal window titled 'alumno@ServidorLinux01: ~'. The terminal output is as follows:

```
login as: alumno
alumno@192.168.1.17's password:
Welcome to Ubuntu 14.04.2 LTS (GNU/Linux 3.16.0-30-generic x86_64)

* Documentation:  https://help.ubuntu.com/

System information as of Mon Jun  8 16:46:33 CEST 2015

System load:  0.0           Processes:      80
Usage of /:   12.4% of 9.22GB Users logged in:    1
Memory usage: 15%          IP address for eth0: 192.168.1.17
Swap usage:   0%

Graph this data and manage this system at:
https://landscape.canonical.com/

Last login: Mon Jun  8 16:46:34 2015 from 192.168.1.4
alumno@ServidorLinux01:~$
```

Figura 5: Conexión SSH como usuario alumno

◇