**Práctica 4 Despliegue en entorno Lamp:**

**Instalación de un servidor OpenSSH en Linux**

**OpenSSH** (**Open Secure Shell**) es un conjunto de aplicaciones que permiten realizar comunicaciones cifradas a través de una red, usando el protocolo SSH.

*ssh*, reemplaza a rlogin y telnet para permitir a través de la shell el acceso remoto a otra máquina

El servidor OpenSSH autentica a los usuarios usando sus propios sistemas de autenticación, implementados en el propio software:

* Clave pública (id.rsa, authorized\_keys)
* Contraseña
* Kerveros/GSSAPI

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

**PASO 1. Instalación**

1.1. Inicia una sesión en ServidorLinuxXX.

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.

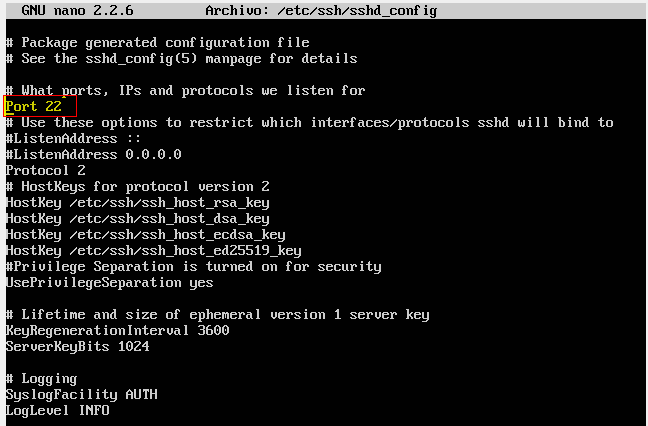
1.3. Comprueba que el servidor está iniciado y escuchando peticiones en el puerto 22/TCP.

1.4. Consulta las claves públicas (\*.pub) y privadas dentro del directorio /etc/ssh

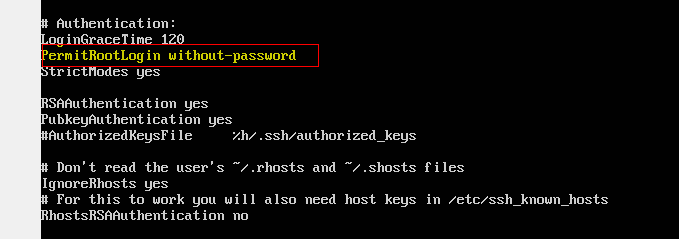
Claves del servidor SSH

**PASO 2. Configuración por defecto**

2.1. Consulta el fichero de configuración de servidor /etc/ssh/sshd\_config y analiza las directivas habilitadas.



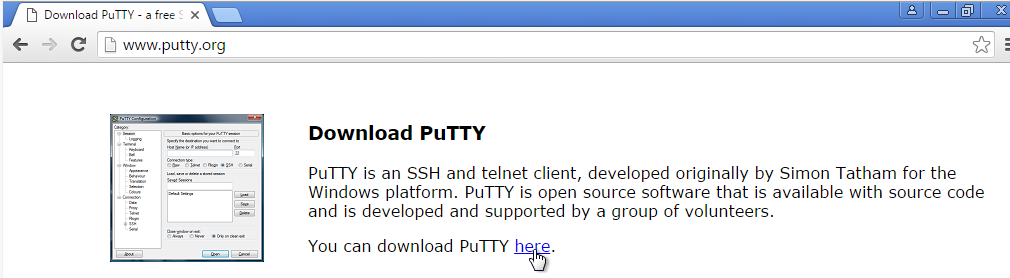
2.2. Observa por ejemplo que el servidor escucha peticiones en el puerto 22 (directiva Port) y que se permite el acceso al usuario root pero utilizando autenticación por clave pública (no con password) (directiva PermitRootLogin).

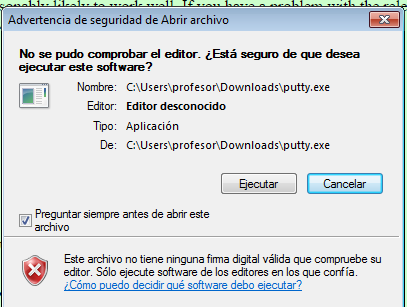
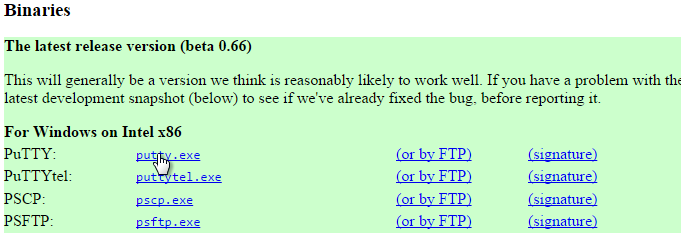


**PASO 3. Conexión al servidor**

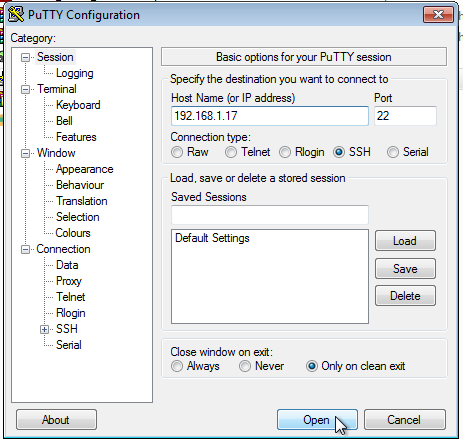
3.1. En DesarrolloW7XX inicia el cliente Putty y establece una conexión SSH al servidor.

1º Descargar e instalar el cliente Putty



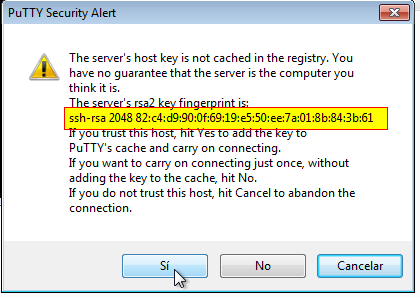


2º Configuración



Conexión SSH

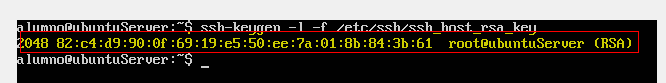
3.2. En servidor envía un resumen (fingerprint) de su clave pública RSA.



Fingerprint de la clave pública RSA enviada por el servidor SSH

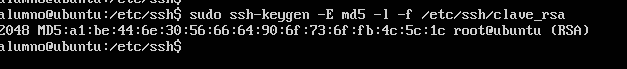
En este punto debemos comprobar que es realmente el resumen de la clave del servidor para evitar una suplantación de identidad (podemos ir al servidor y ejecutar el comando ssh-keygen -l -f /etc/ssh/ssh\_host\_rsa\_key) para obtener el fingerprint de la clave).

ssh-keygen -l -f /etc/ssh/ssh\_host\_rsa\_key



Fingerprint de la clave pública RSA del servidor SSH

Para ver el fingerprint en hexadecimal:



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.

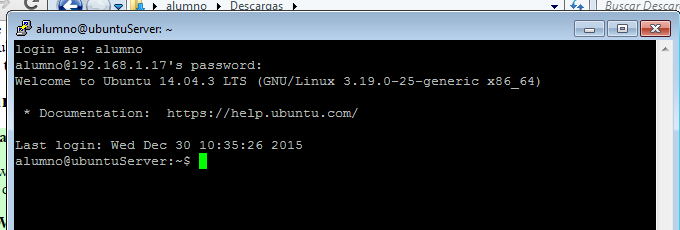
**Para eliminar en Windows** el fingerprint almacenado de un servidor ssh, hay que ir desde regedit HKEY\_CURRENT\_USER \ Software \ SimonTatham \ PuTTY \ SshHostKeys y eliminar el fichero correspondiente.

**En Linux**, en la cuenta que estemos usando se genera un directorio oculto llamado .ssh dentro de él un archivo llamado *known\_hosts* que ejecutando el programa ssh-agent:

$> ssh-agent -l -f known\_hosts

da una lista de los fingerprints de los hosts a los que nos hemos conectado, basta con eliminar el renglón del host que queramos eliminar o todo el archivo para que la siguiente vez que nos conectemos al servidor ssh nos pregunte de nuevo que si lo aceptamos o no.

3.3. Inicia sesión como usuario alumno



Conexión SSH como usuario alumno