

6.3. Despliegue en un servidor local

Despliega la aplicación **películas** sobre el servidor WAMP de **DesarrolloW7XX**.

- El acceso a la aplicación se realizará a través de la URL `http://<servidor>/peliculas`.
- El código de la aplicación se almacenará en el directorio `C:\wamp\apps`.

1. Obtener el código de la aplicación

- 1.1. Inicia sesión con un usuario con privilegios de administrador en **DesarrolloW7XX**.
- 1.2. Obtén el código de la aplicación siguiendo los pasos que indique el profesor.
- 1.3. Descomprime el fichero obtenido, Figura 6.28.

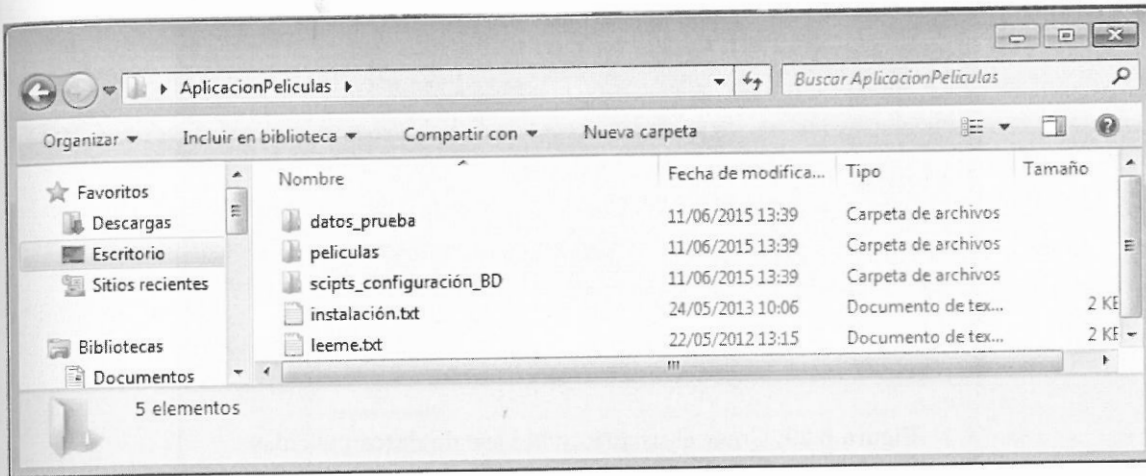


Figura 6.28: Aplicación

- 1.4. Lee el contenido del fichero **leeme.txt** donde se explican los ficheros disponibles.
- 1.5. Lee el contenido del fichero **instalación.txt** donde se explica cómo instalar la aplicación.

2. Configuración de la base de datos

- 2.1. Inicia una navegador y accede a <http://localhost/phpmyadmin>.
- 2.2. Inicia sesión con el usuario **root**.
- 2.3. Accede a **Usuarios**.
- 2.4. Pincha en **Agregar un nuevo usuario**.
- 2.5. Introduce **peliculas** como nombre de usuario, **localhost** como servidor y **peliculas** como clave del usuario. Marca la opción **Crear base de datos con el mismo nombre** y **otorgar todos los privilegios** y pincha en **Crear Usuario**, Figura 6.29.

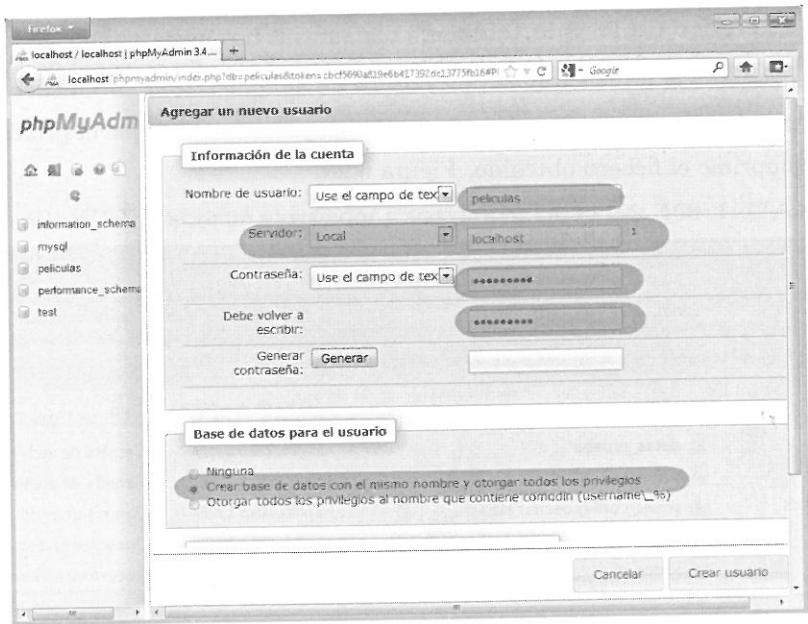


Figura 6.29: Crear el usuario y la base de datos películas

2.6. Se han creado el usuario **películas**, la base de datos **películas** y se han otorgado todos los privilegios al usuario sobre la base de datos, Figura 6.30.

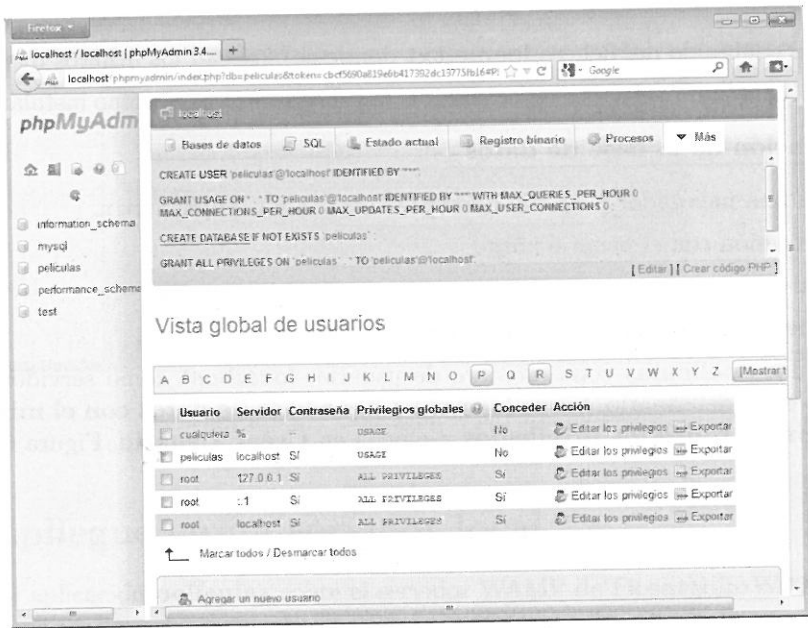


Figura 6.30: Usuario y la base de datos creados

- 2.7. Cierra la sesión de *phpmyadmin* del usuario **root**.
- 2.8. Inicia sesión en *phpmyadmin* con el usuario **películas**.

- 2.9. En la parte izquierda selecciona la base de datos **películas**.
- 2.10. Pincha en **Importar**.
- 2.11. Pincha en **Examinar** y selecciona el script **crear_tablas_peliculas.sql**. Pincha en **Continuar** para ejecutar el script, Figura 6.31.

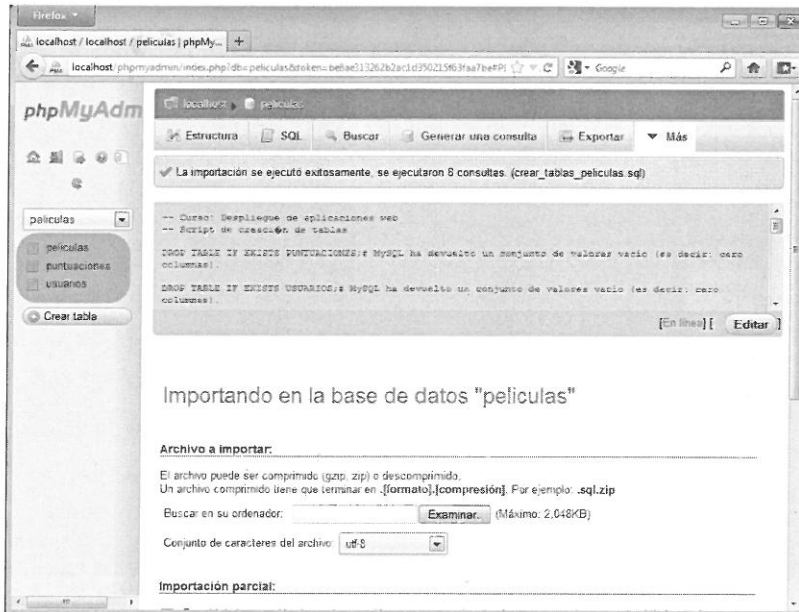


Figura 6.31: Tablas creadas

- 2.12. Pincha de nuevo en **Examinar** y selecciona el script **insercion_admin_peliculas.sql**. Pincha en **Continuar** para ejecutar el script.

3. *Desplegar la aplicación web*

- 3.1. Copia el directorio **películas** dentro del directorio **C:\wamp\apps**.
- 3.2. Crea en *Apache* el alias **/películas** que referencie a **C:\wamp\apps\películas**. Lo puedes hacer con la herramienta que ofrece el servidor *WAMP* o creando el fichero **películas.conf** dentro del directorio **c:\wamp\alias**, Figura 6.32 (repasa la práctica 6.1 si tienes dudas con esta configuración).

```
Alias /películas "c:/wamp/apps/películas/"

<Directory "c:/wamp/apps/películas/">
    Options Indexes FollowSymLinks MultiViews
    AllowOverride all
    Require all granted
</Directory>
```

Figura 6.32: Crear el alias /películas

3.3. Reinicia *Apache* para que se apliquen los cambios.

4. Acceso a la aplicación

4.1. Abre un navegador y accede a `http://localhost/peliculas`, Figura 6.33.

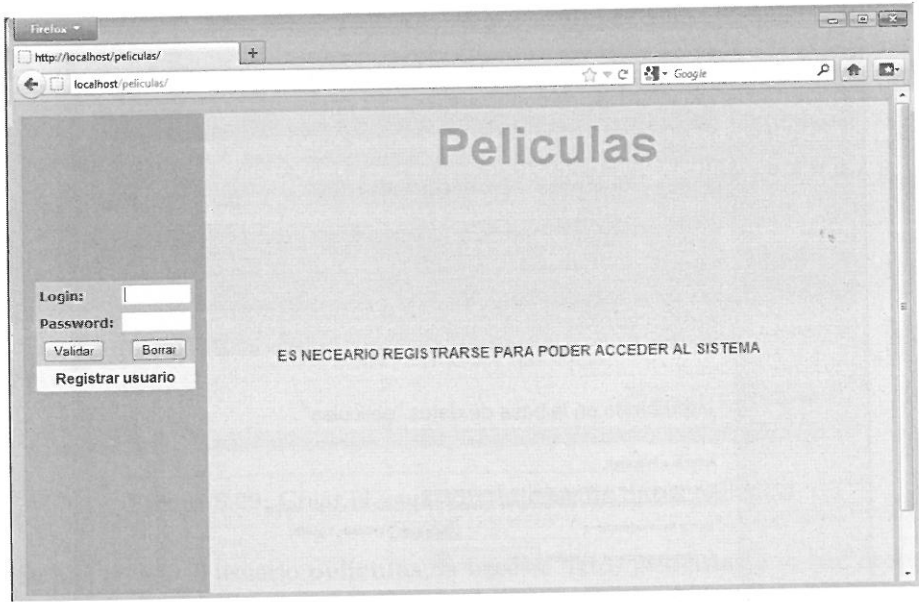


Figura 6.33: Conexión a *peliculas*

4.2. Inicia sesión con el usuario **admin** (contraseña **admin**), Figura 6.34.

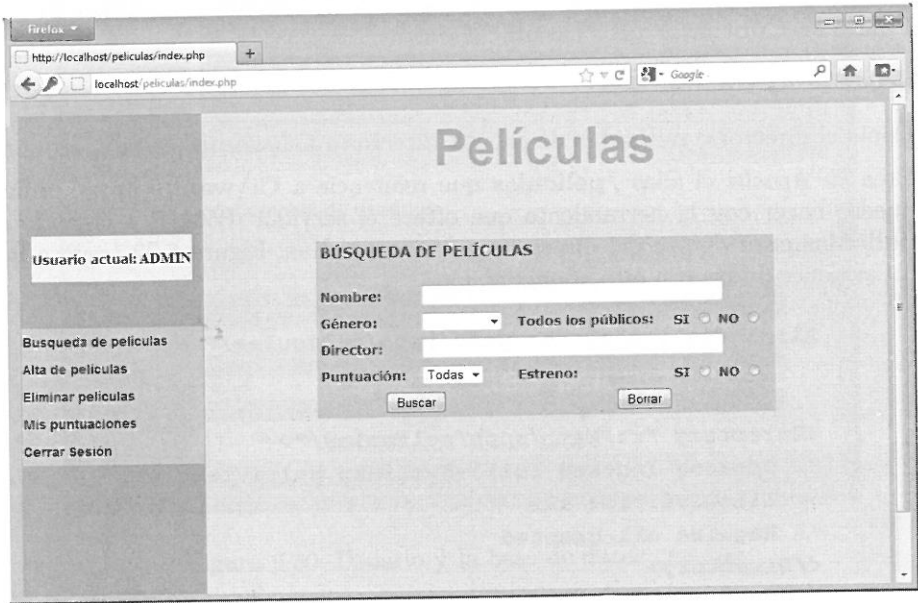


Figura 6.34: Inicio de sesión

6.4. Servidor *vsftpd* en *Linux*

Instala el servidor FTP *vsftpd* (<http://vsftpd.beasts.org/>) en la máquina **ServidorLinuxXX** y configúralo con las siguientes opciones:

- Se permitirá la conexión de usuarios anónimos.
- Se permitirá la conexión a los usuarios locales.
- Los usuarios locales podrán descargar y subir archivos.

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 vsftpd
```

Al instalar el servidor se crean:

- Los archivos de configuración.
- El usuario **ftp** que se incluye en el grupo **ftp**.
- El directorio **/srv/ftp**
 - Su propietario es el usuario **root** y su grupo es **ftp**.
 - El directorio predeterminado de los usuarios anónimos.

- 1.3. Comprueba que el servidor está iniciado y escuchando peticiones en el puerto 21/TCP.

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

2. Configuración por defecto

La configuración del servidor por defecto es la siguiente:

- Permite solo el acceso a usuarios locales.
 - Pueden descargar archivos.
 - No pueden subir archivos.
 - Los usuarios anónimos están “enjaulados” en **/srv/ftp**.
 - Nombre de usuario **anonymous** o **ftp**.
 - *Password*: en blanco.
 - El fichero de *logs* por defecto es **/var/log/vsftpd.log**.
- 2.1. Consulta el fichero de configuración de servidor (**/etc/vsftpd.conf**) y analiza las directivas habilitadas, Figura 6.35.
 - Está deshabilitado el acceso a los usuarios anónimos (directiva **anonymous_enable**).
 - Está habilitado el acceso a los usuarios locales (directiva **local_enable**).
 - No se permite subir archivos al servidor (directiva **write_enable**).

```
listen=YES
#
# Run standalone with IPv6?
# Like the listen parameter, except vsftpd will listen on an IPv6 socket
# instead of an IPv4 one. This parameter and the listen parameter are mutually
# exclusive.
#listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default)
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=YES
```

Figura 6.35: Fichero /etc/vsftpd.conf

3. Conexión al servidor

- 3.1. En **DesarrolloW7XX** inicia el cliente *Filezilla* y establece una conexión al servidor como usuario anónimo (**alumno**), Figura 6.36. Verifica que puedes descargar archivos pero no subirlos.

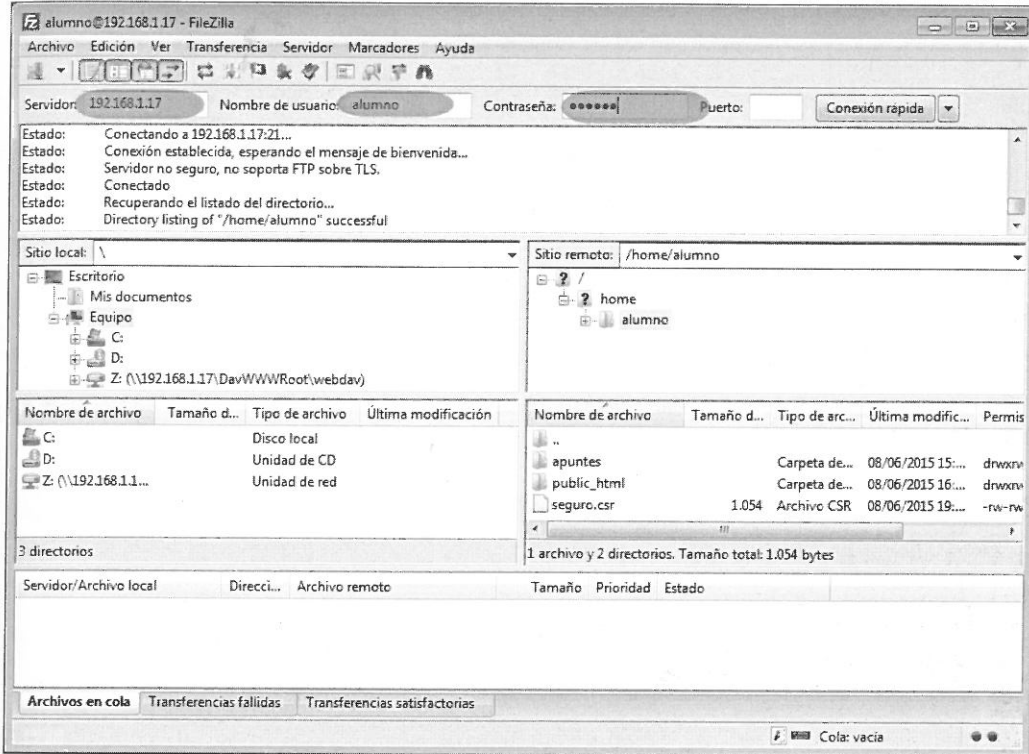


Figura 6.36: Conexión FTP como usuario alumno

- 3.2. Verifica que no es posible conectarse como usuario **anonymous**,

4. Configuración

- 4.1. Haz una copia de seguridad del fichero de configuración principal (**/etc/vsftpd.conf**).
- 4.2. Edita el fichero de configuración (**/etc/vsftpd.conf**) y habilita las directivas **anonymous_enable** con el valor **YES**, **local_enable** y **write_enable**, Figura 6.37.
- 4.3. Reinicia el servidor para que se apliquen los cambios.

```
sudo service vsftpd stop
sudo service vsftpd start
```

- 4.4. En **DesarrolloW7XX** inicia el cliente *Filezilla* y establece una conexión al servidor como usuario **alumno**) y verifica que puedes subir archivos.
- 4.5. Crea dos archivos de texto dentro del directorio **/srv/ftp**.
- 4.6. En **DesarrolloW7XX** inicia el cliente *Filezilla* y establece una conexión al servidor como usuario **anonymous**, Figura 6.38.


```
##
# Allow anonymous FTP? (Disabled by default)
anonymous_enable=YES
##
# Uncomment this to allow local users to log in.
local_enable=YES
##
# Uncomment this to enable any form of FTP write command.
write_enable=YES
##
```

Figura 6.37: Fichero /etc/vsftpd.conf

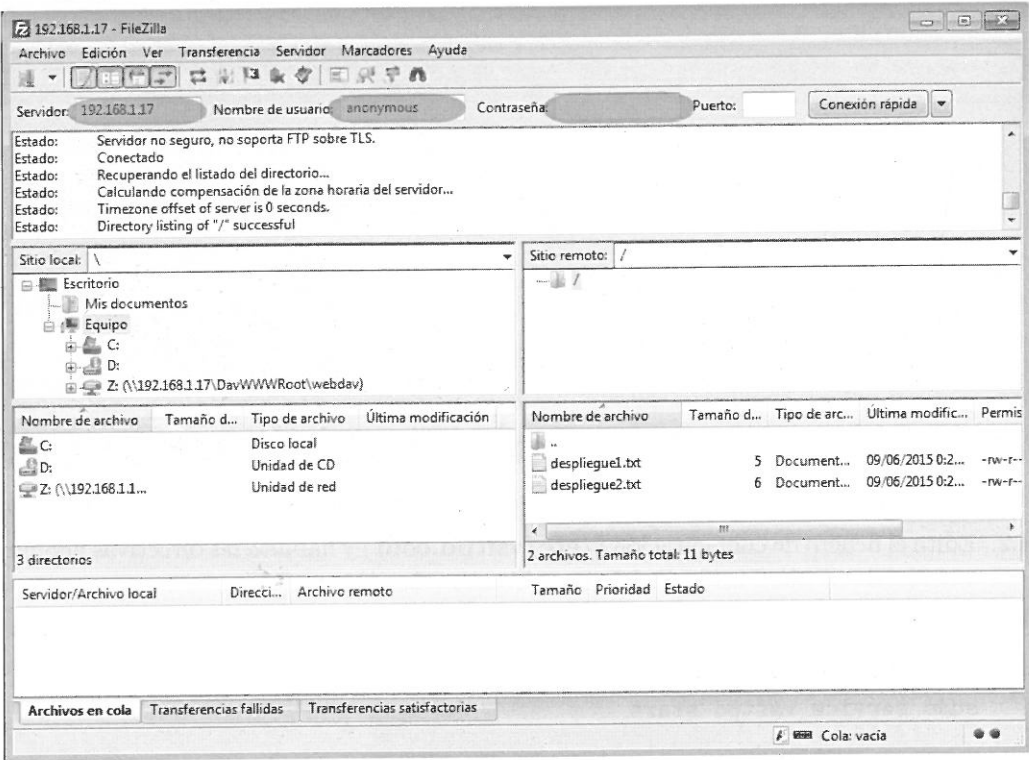


Figura 6.38: Conexión FTP como usuario anonymous

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
```

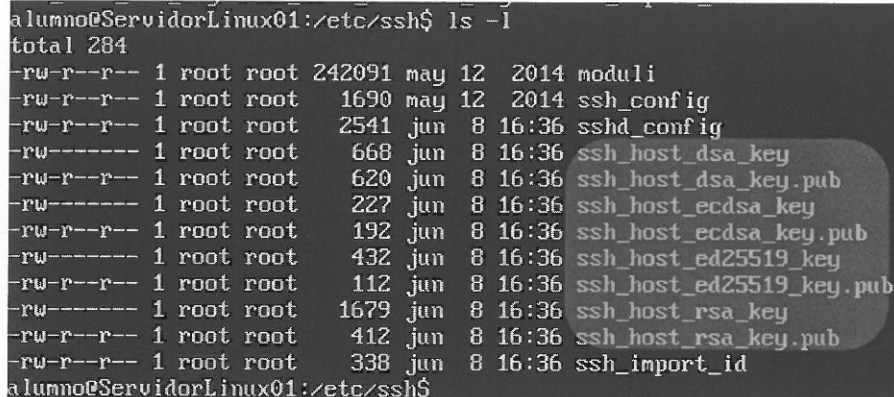
Al instalar el servidor:

- 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 6.39.



```
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 6.39: 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 6.40.

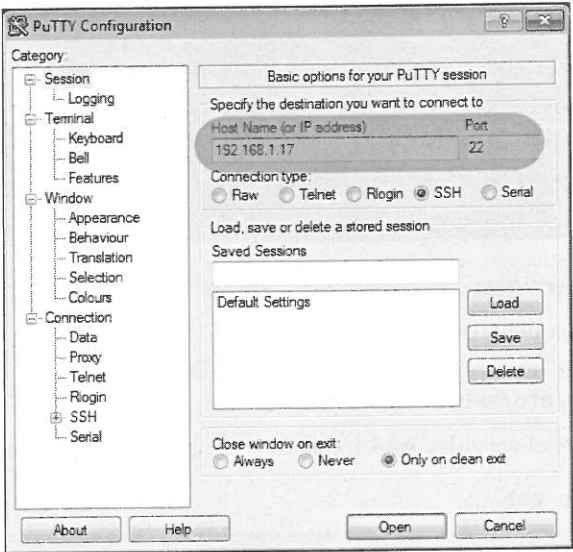


Figura 6.40: Conexión SSH

3.2. En servidor envía un resumen (*fingerprint*) de su clave pública RSA, Figura 6.41.

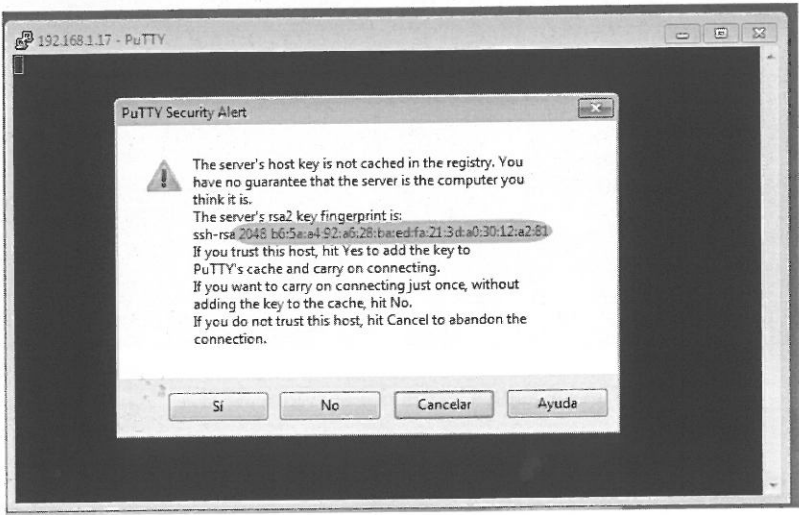


Figura 6.41: *Fingerprint* de la clave pública RSA enviada por el servidor SSH

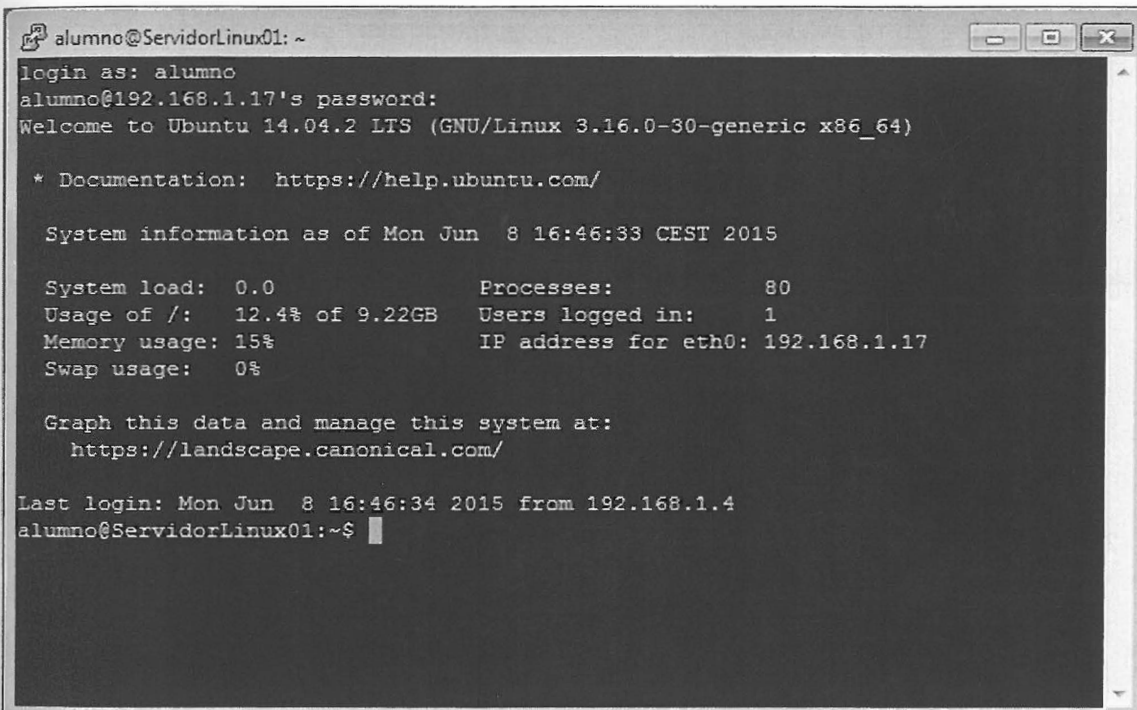
En este punto debemos comprobar que es realmente el resumen de la clave del servidor para evitar una suplantación de identidad (podemos ir al servidor y ejecutar el comando `ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key` para obtener el *fingerprint* de la clave), Figura 6.42.

```
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 6.42: *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 6.43.



```
alumno@ServidorLinux01: ~
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 6.43: Conexión SSH como usuario alumno