

Anexando Seguridad a un Servidor Proftpd & modulo mod_sql_mysql.c

Adib Saavedra Bocanegra

<http://adib.mx.vg>

ENLI 2006

Puebla, Pueb.

Indice general

- Introduccion al protocolo FTP.
- Caracteristicas, de los servicios inetd/xinetd y standalone de Linux.
- El servidor ProFTPD.
- Instalando el servidor en ambientes *.nix.
- Modulo para autentificar con MySQL..
- El archivo /etc/proftpd.conf.
- Agregando usuarios.
- Conclusiones.

El Protocolo FTP

FTP es un protocolo estándar con el STD 9. Su status es recomendado. Se describe en el RFC 959 FTP("File Transfer Protocol").

La transferencia de datos entre cliente y servidor puede producirse en cualquier dirección. El cliente puede enviar o pedir un archivo al servidor.

Para acceder a archivos remotos, el usuario debe identificarse al servidor. En este punto el servidor es responsable de autenticar al cliente antes de permitir la transferencia de archivos.

Descripcion

FTP usa TCP como protocolo de transporte para proporcionar conexiones fiables entre los extremos. Se emplean dos conexiones: la primera es para el login (protocolo TELNET) y la segunda es para gestionar la transferencia de datos.

Como es necesario hacer un login en el host remoto, el usuario debe tener un nombre de usuario y un password para acceder a los archivos y a directorios.

El usuario que inicia la conexión asume la función de cliente, mientras que el host remoto adopta la función de servidor

Funcionamiento de un servidor

Cuando un sistema oferta diferentes servicios, es habitual que cada uno de ellos esté escuchando en el puerto que le corresponde.

Si un cliente quiere acceder a alguno de esos servicios, establece una conexión y posteriormente usa el protocolo asociado a dicho servicio.

Funcionamiento de un servidor,...

De este modo, en el servidor, habrá un proceso que esté escuchando en cada uno de los puertos asociados a los servicios que ofrece.

Si el sistema oferta N servicios, habrá N procesos escuchando en N puertos. Si un cliente establece una conexión a un puerto, el proceso a la escucha en dicho puerto lanzará un nuevo proceso que atienda al cliente.

Super-servers inetd & xinetd

Ya que todos los procesos que están a la escucha en los puertos harán esa pequeña tarea, podrían ahorrarse muchos recursos del sistema teniendo un único proceso a la escucha en todos los puertos que lance nuevos procesos que atiendan a los clientes dependiendo del puerto al que se conecten.

Super-servers inetd & xinetd

En resumen, esos programas que se dedican a escuchar puertos y lanzar un programa u otro dependiendo del puerto al que llegue la conexión se les suele llamar "super-servers". Los más famosos y extendidos son: inetd e xinetd -éste es una versión mejorada del primero

INETD

Es el "super-server" tradicional en los sistemas UNIX. Es lanzado al inicio del sistema y dependiendo de ciertos archivos de configuración, se pondrá a la escucha de los puertos especificados.

Su funcionamiento depende indirectamente de otros archivos de configuración como services, protocols o rpc, situados todos ellos en /etc.

XINETD

Xinetd nace para mejorar este y muchos otros aspectos de inetd, pero la filosofía es siempre la misma: un proceso que escucha y que lanza otros procesos que atiendan a los clientes. Es mucho más completo y flexible que inetd.

Servicio Standalone

Al correr en standalone, se tiene un proceso propio ejecutandose todo el tiempo.

El standalone, al estar siempre levantado, responderia mas rapido yaque no hay que levantarlo para cada nueva conexion, por el otro lado, esto consume recursos que no son utilizados si no hay conexiones activas.

El servidor ProFTPD

ProFTPD esta portado a distintas plataformas (AIX, BSD/OS, Cygwin, DG/UX, Digital Unix, FreeBSD, HP/UX, IRIX, Linux for IBM S/390, zSeries, Linux, Mac OS X, NetBSD, OpenBSD, SCO, Solaris, SunOS)

Es seguro, sumamente flexible, modular y fácil de configurar.

Entre todas las características que tiene, las más rescatables son: permite autenticar usuarios con casi cualquier cosa, se pueden utilizar servidores virtuales de ftp, se pueden tener múltiples servidores brindando servicio de ftp anónimo, es modular y su código esta licenciado bajo GPL.

Instalacion

Para los debianitas, u otra distribucion basada en debian, (ubuntu, knoppix), seria apt- get install proftpd-commom

crear el usuario y grupo que seran dueños del proceso

./configure lanza el script que se llama configure

sysconfdir=/etc los archivos de configuracion van a estar en /etc,..

localstatedir=/var

make

checkinstall

Soporte con MySQL

El soporte para MySQL, es para poder autentificar usuarios con una Bases de Datos, al principio no sera necesario pues la exigencia es minima, pero a medida que crece nuestros usuarios se exige una medida de autentificacion que no involucre usuarios del sistema, ademas de mantener limpio nuestro archivo /etc/passwd.

Tambien la administracion es mas eficaz y segura, para esto es necesario agregar nuevas características a nuestro servidor FTP, con el modulo indicado.

Instalando el modulo proftpd-mysql

El uso de módulos permite fácilmente extender sus funcionalidades. Existen módulos para:

- * Gestión de cuotas (de usuario)
- * Otros sistemas de autenticación como LDAP, Mysql, Postgresql, ...
- * Gestión de ratios
- * Gestión de ancho de banda

En un sistema debian o similares, se instala con:

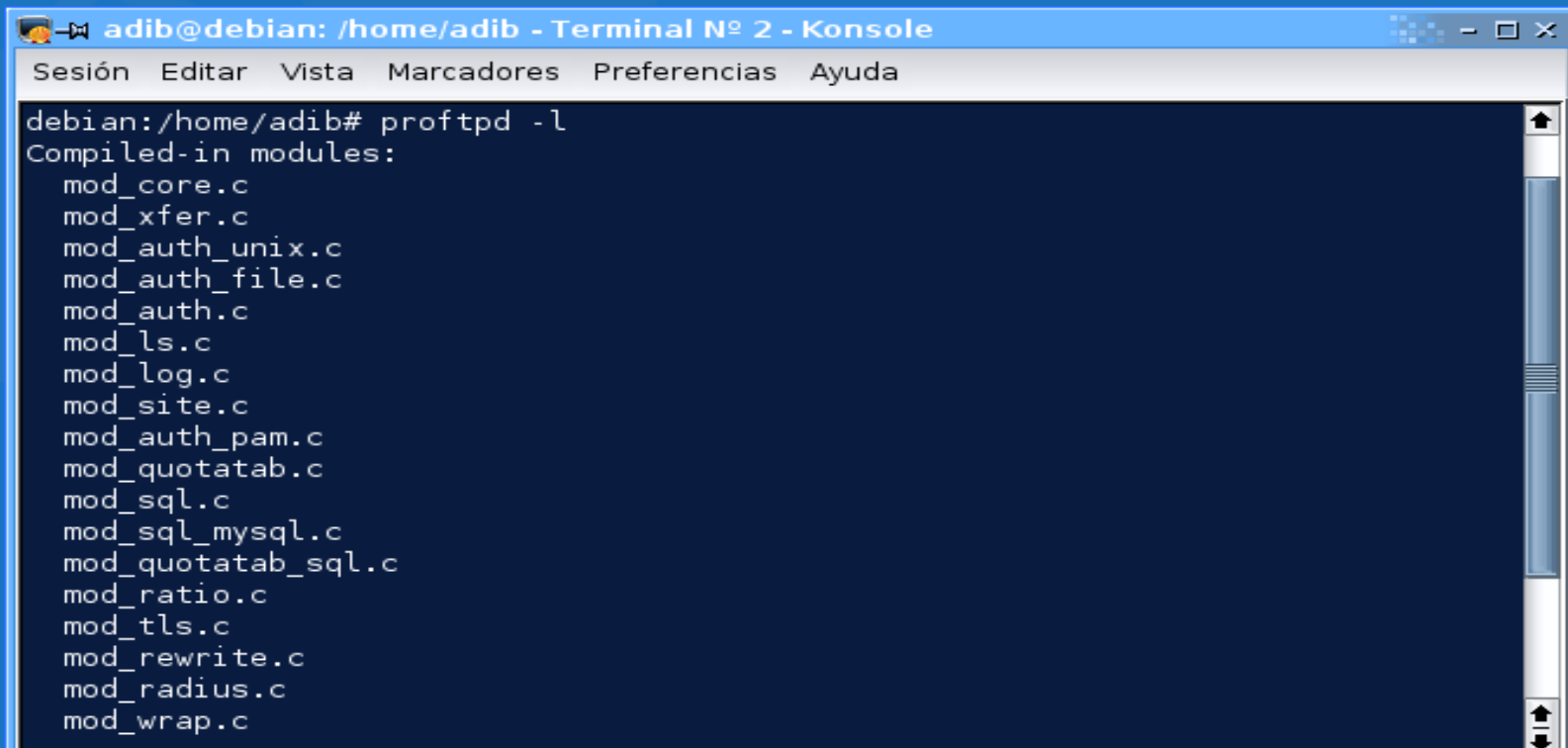
```
apt-get install proftpd-mysql
```

Instrucciones basicas

levantar el servicio: proftpd start

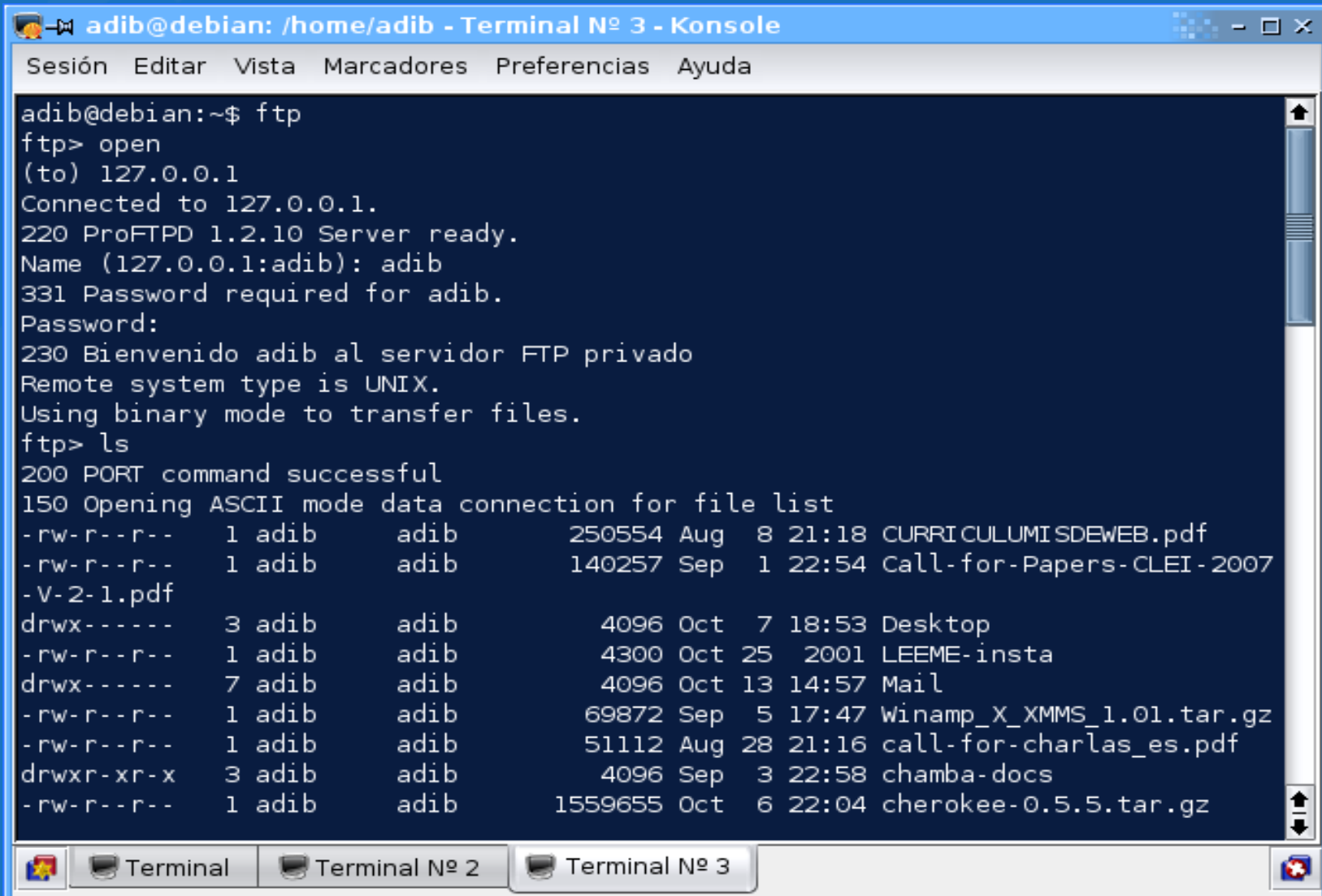
detener el servicio: proftpd stop

reiniciar el servicio: proftpd restart

A terminal window titled 'adib@debian: /home/adib - Terminal Nº 2 - Konsole'. The window has a menu bar with 'Sesión', 'Editar', 'Vista', 'Marcadores', 'Preferencias', and 'Ayuda'. The terminal output shows the command 'proftpd -l' being executed, followed by the text 'Compiled-in modules:' and a list of modules: mod_core.c, mod_xfer.c, mod_auth_unix.c, mod_auth_file.c, mod_auth.c, mod_ls.c, mod_log.c, mod_site.c, mod_auth_pam.c, mod_quotatab.c, mod_sql.c, mod_sql_mysql.c, mod_quotatab_sql.c, mod_ratio.c, mod_tls.c, mod_rewrite.c, mod_radius.c, and mod_wrap.c.

```
adib@debian: /home/adib# proftpd -l
Compiled-in modules:
  mod_core.c
  mod_xfer.c
  mod_auth_unix.c
  mod_auth_file.c
  mod_auth.c
  mod_ls.c
  mod_log.c
  mod_site.c
  mod_auth_pam.c
  mod_quotatab.c
  mod_sql.c
  mod_sql_mysql.c
  mod_quotatab_sql.c
  mod_ratio.c
  mod_tls.c
  mod_rewrite.c
  mod_radius.c
  mod_wrap.c
```


Iniciando el servicio



The screenshot shows a terminal window titled "adib@debian: /home/adib - Terminal Nº 3 - Konsole". The window has a menu bar with "Sesión", "Editar", "Vista", "Marcadores", "Preferencias", and "Ayuda". The terminal output shows an FTP session where the user "adib" connects to "127.0.0.1" using ProFTPD 1.2.10. After providing a password, the user lists files in the current directory. The file list includes several PDF files, a desktop folder, a mail folder, and two tar.gz archives.

```
adib@debian:~$ ftp
ftp> open
(to) 127.0.0.1
Connected to 127.0.0.1.
220 ProFTPD 1.2.10 Server ready.
Name (127.0.0.1:adib): adib
331 Password required for adib.
Password:
230 Bienvenido adib al servidor FTP privado
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r--  1 adib    adib      250554 Aug  8 21:18 CURRICULUMISDEWEB.pdf
-rw-r--r--  1 adib    adib      140257 Sep  1 22:54 Call-for-Papers-CLEI-2007
-V-2-1.pdf
drwx-----  3 adib    adib        4096 Oct  7 18:53 Desktop
-rw-r--r--  1 adib    adib        4300 Oct 25  2001 LEEME-insta
drwx-----  7 adib    adib        4096 Oct 13 14:57 Mail
-rw-r--r--  1 adib    adib     69872 Sep  5 17:47 Winamp_X_XMMS_1.01.tar.gz
-rw-r--r--  1 adib    adib     51112 Aug 28 21:16 call-for-charlas_es.pdf
drwxr-xr-x  3 adib    adib        4096 Sep  3 22:58 chamba-docs
-rw-r--r--  1 adib    adib    1559655 Oct  6 22:04 cherokee-0.5.5.tar.gz
```

Creando la BD

Primeramente es necesario tener la base de datos con una tabla que es donde se encontraran los usuarios y sus contraseñas.

```
CREATE DATABASE proftpd;  
CREATE TABLE usuarios (  
    username varchar(30) NOT NULL default "",  
    passwd varchar(80) NOT NULL default "",  
    uid int(11) default NULL,  
    gid int(11) default NULL,  
    homedir varchar(255) default NULL,  
    shell varchar(255) default NULL,  
)TYPE=MyISAM;
```

Esquema de la tabla

```
adib@debian: /home/adib - Terminal N° 3 - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

mysql> describe usuarios;
+-----+-----+-----+-----+-----+-----+
| Field      | Type          | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| username   | varchar(15)   |      |     |          |       |
| nombre     | varchar(50)   | YES  |     | NULL     |       |
| semestre   | varchar(5)    | YES  |     | NULL     |       |
| grupo      | varchar(5)    | YES  |     | NULL     |       |
| email      | varchar(20)   |      |     |          |       |
| passwd     | varchar(10)   |      |     |          |       |
| uid        | int(10)       |      | PRI | 0         |       |
| gid        | int(10)       | YES  |     | NULL     |       |
| homedir    | varchar(30)   | YES  |     | NULL     |       |
| academia   | varchar(30)   |      |     |          |       |
| docente    | varchar(50)   |      |     |          |       |
| shell      | varchar(10)   | YES  |     | /bin/bash |       |
+-----+-----+-----+-----+-----+-----+
12 rows in set (0.02 sec)

mysql> 
```

Creando privilegios

También es conveniente crear un usuario dentro de MySQL para que sea solamente ese usuario el único en hacer modificaciones y consultas:

```
mysql -p
```

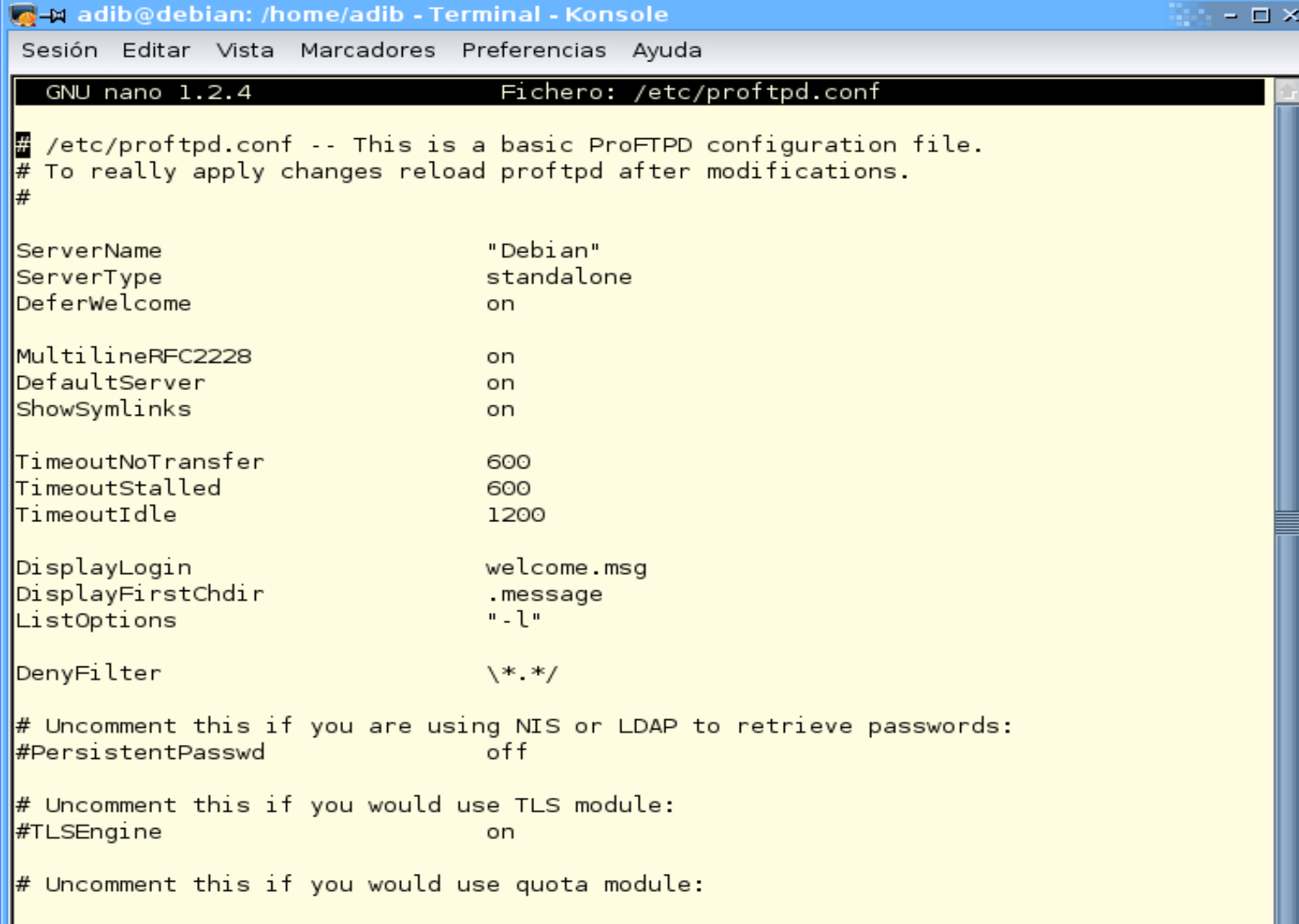
Enter password:

```
mysql> GRANT insert, selec, delete ON proftpd.*  
TO ftpadmin@localhost IDENTIFIED BY '123admin';
```

Ahora que tenemos la base de datos lista tenemos que decirle al ProFTPD que tiene que autenticarse a través de ella y no ir a buscar usuarios del sistema como hace por defecto

Editando el archivo

/etc/proftpd.conf 1a parte



The screenshot shows a terminal window titled "adib@debian: /home/adib - Terminal - Konsole". The window contains the GNU nano 1.2.4 text editor editing the file /etc/proftpd.conf. The editor's menu bar includes "Sesión", "Editar", "Vista", "Marcadores", "Preferencias", and "Ayuda". The file content is a ProFTPD configuration file with various settings and comments.

```
GNU nano 1.2.4 Fichero: /etc/proftpd.conf

## /etc/proftpd.conf -- This is a basic ProFTPD configuration file.
# To really apply changes reload proftpd after modifications.
#

ServerName                "Debian"
ServerType                standalone
DeferWelcome              on

MultilineRFC2228          on
DefaultServer             on
ShowSymlinks              on

TimeoutNoTransfer         600
TimeoutStalled            600
TimeoutIdle               1200

DisplayLogin              welcome.msg
DisplayFirstChdir         .message
ListOptions               "-l"

DenyFilter                \*.*/

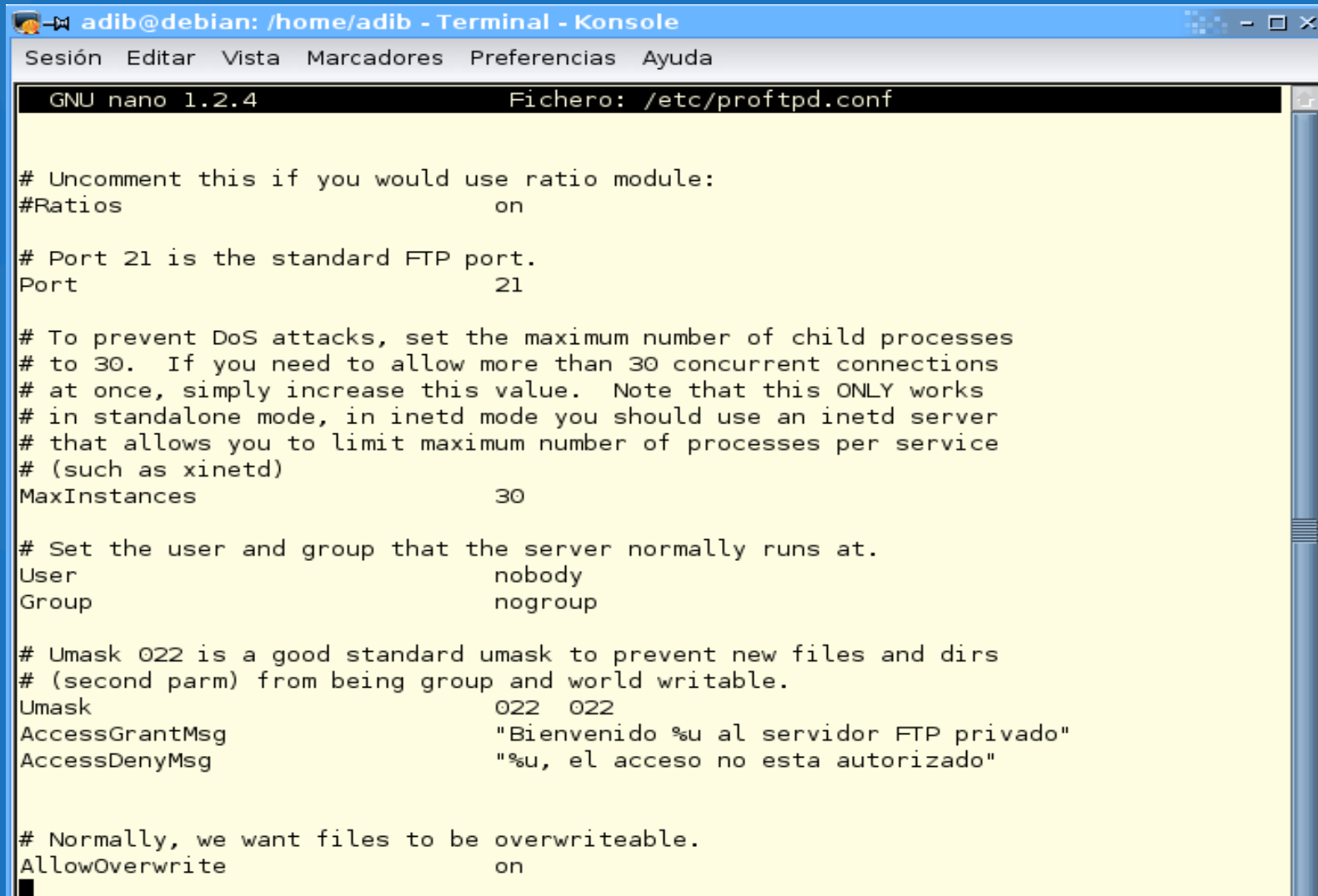
# Uncomment this if you are using NIS or LDAP to retrieve passwords:
#PersistentPasswd         off

# Uncomment this if you would use TLS module:
#TLSEngine                on

# Uncomment this if you would use quota module:
```

Editando el archivo

/etc/proftpd.conf 2a parte



The screenshot shows a terminal window titled "adib@debian: /home/adib - Terminal - Konsole". The window contains the GNU nano 1.2.4 text editor editing the file /etc/proftpd.conf. The editor's menu bar includes "Sesión", "Editar", "Vista", "Marcadores", "Preferencias", and "Ayuda". The file content is as follows:

```
GNU nano 1.2.4 Fichero: /etc/proftpd.conf

# Uncomment this if you would use ratio module:
#Ratios                                on

# Port 21 is the standard FTP port.
Port                                    21

# To prevent DoS attacks, set the maximum number of child processes
# to 30. If you need to allow more than 30 concurrent connections
# at once, simply increase this value. Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd)
MaxInstances                            30

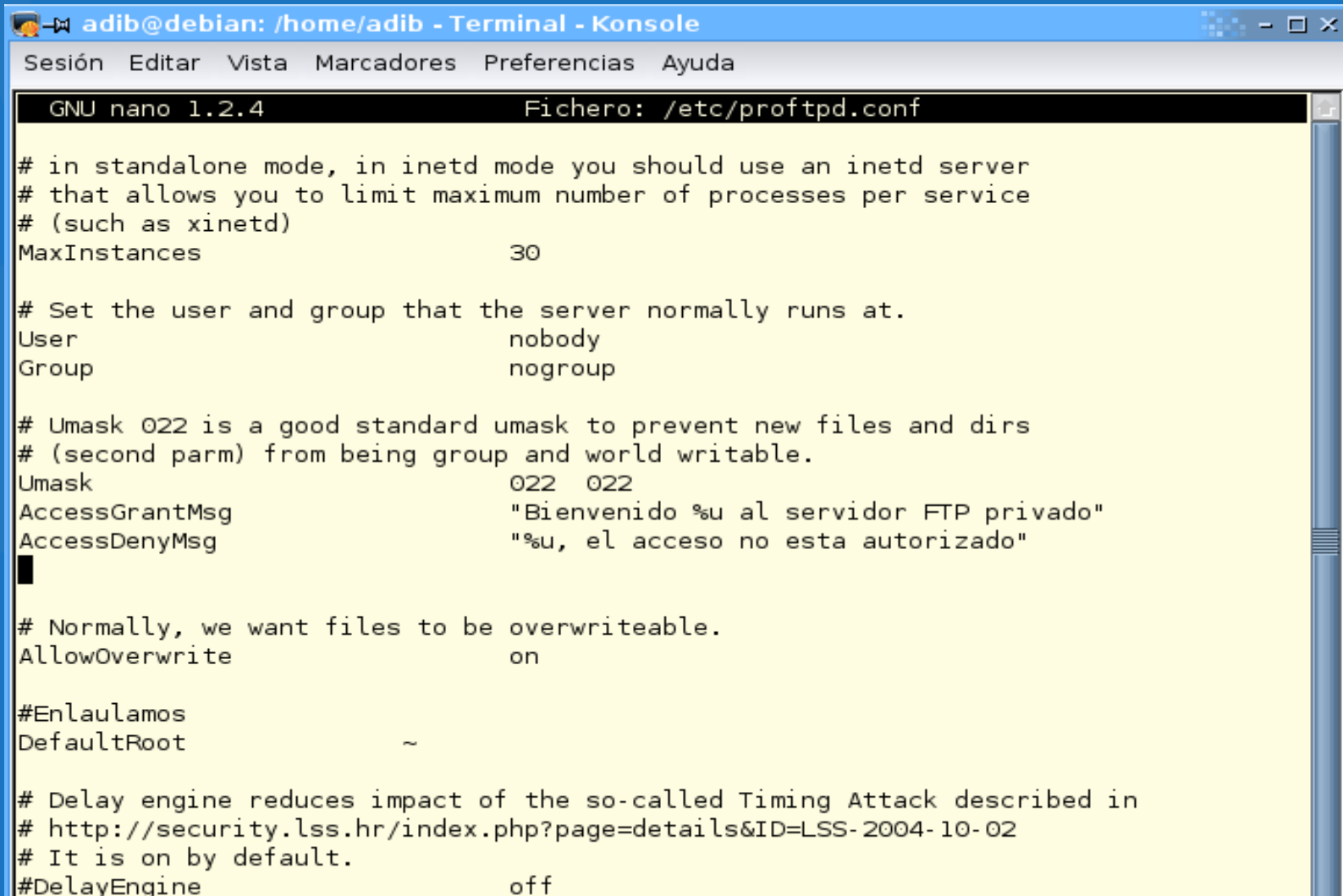
# Set the user and group that the server normally runs at.
User                                    nobody
Group                                    nogroup

# Umask 022 is a good standard umask to prevent new files and dirs
# (second parm) from being group and world writable.
Umask                                    022 022
AccessGrantMsg                           "Bienvenido %u al servidor FTP privado"
AccessDenyMsg                            "%u, el acceso no esta autorizado"

# Normally, we want files to be overwriteable.
AllowOverwrite                           on
```

Editando el archivo

/etc/proftpd.conf 3a parte



The screenshot shows a terminal window titled "adib@debian: /home/adib - Terminal - Konsole". The window contains the GNU nano 1.2.4 text editor editing the file /etc/proftpd.conf. The editor's status bar at the top shows "GNU nano 1.2.4" and "Fichero: /etc/proftpd.conf". The menu bar includes "Sesión", "Editar", "Vista", "Marcadores", "Preferencias", and "Ayuda". The main text area displays the configuration file's content, which includes comments and settings for the ProFTPD server. The settings shown are: MaxInstances set to 30; User and Group set to nobody and nogroup; Umask set to 022 022; AccessGrantMsg set to "Bienvenido %u al servidor FTP privado"; AccessDenyMsg set to "%u, el acceso no esta autorizado"; AllowOverwrite set to on; DefaultRoot set to ~; and DelayEngine set to off.

```
adib@debian: /home/adib - Terminal - Konsole
Sesión  Editar  Vista  Marcadores  Preferencias  Ayuda
GNU nano 1.2.4                                Fichero: /etc/proftpd.conf
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd)
MaxInstances                                30

# Set the user and group that the server normally runs at.
User                                         nobody
Group                                       nogroup

# Umask 022 is a good standard umask to prevent new files and dirs
# (second parm) from being group and world writable.
Umask                                       022 022
AccessGrantMsg                             "Bienvenido %u al servidor FTP privado"
AccessDenyMsg                             "%u, el acceso no esta autorizado"

# Normally, we want files to be overwriteable.
AllowOverwrite                             on

#Enlaulamos
DefaultRoot                                ~

# Delay engine reduces impact of the so-called Timing Attack described in
# http://security.lss.hr/index.php?page=details&ID=LSS-2004-10-02
# It is on by default.
DelayEngine                                off
```

Editando el archivo

/etc/proftpd.conf 4a parte



The screenshot shows a terminal window titled "adib@debian: /home/adib - Terminal - Konsole". The window contains the GNU nano 1.2.4 text editor editing the file /etc/proftpd.conf. The editor's menu bar includes "Sesión", "Editar", "Vista", "Marcadores", "Preferencias", and "Ayuda". The file content shows the end of a configuration block with comments and the start of a new MySQL authentication section.

```
GNU nano 1.2.4                                Fichero: /etc/proftpd.conf
# #                                     </Limit>
# # </Directory>
#
# </Anonymous>
# Autentificacion por MySQL
#
SQLAuthTypes                                Plaintext
SQLAuthenticate                            users*
SQLConnectInfo                            proftpd@localhost adib ladib
SQLDefaultGID                             65534
SQLDefaultUID                             65534
SQLMinUserGID                             100
SQLMinUserUID                             500
SQLUserInfo                               usuarios  username passwd uid gid homedir shell
```


Agregando usuarios

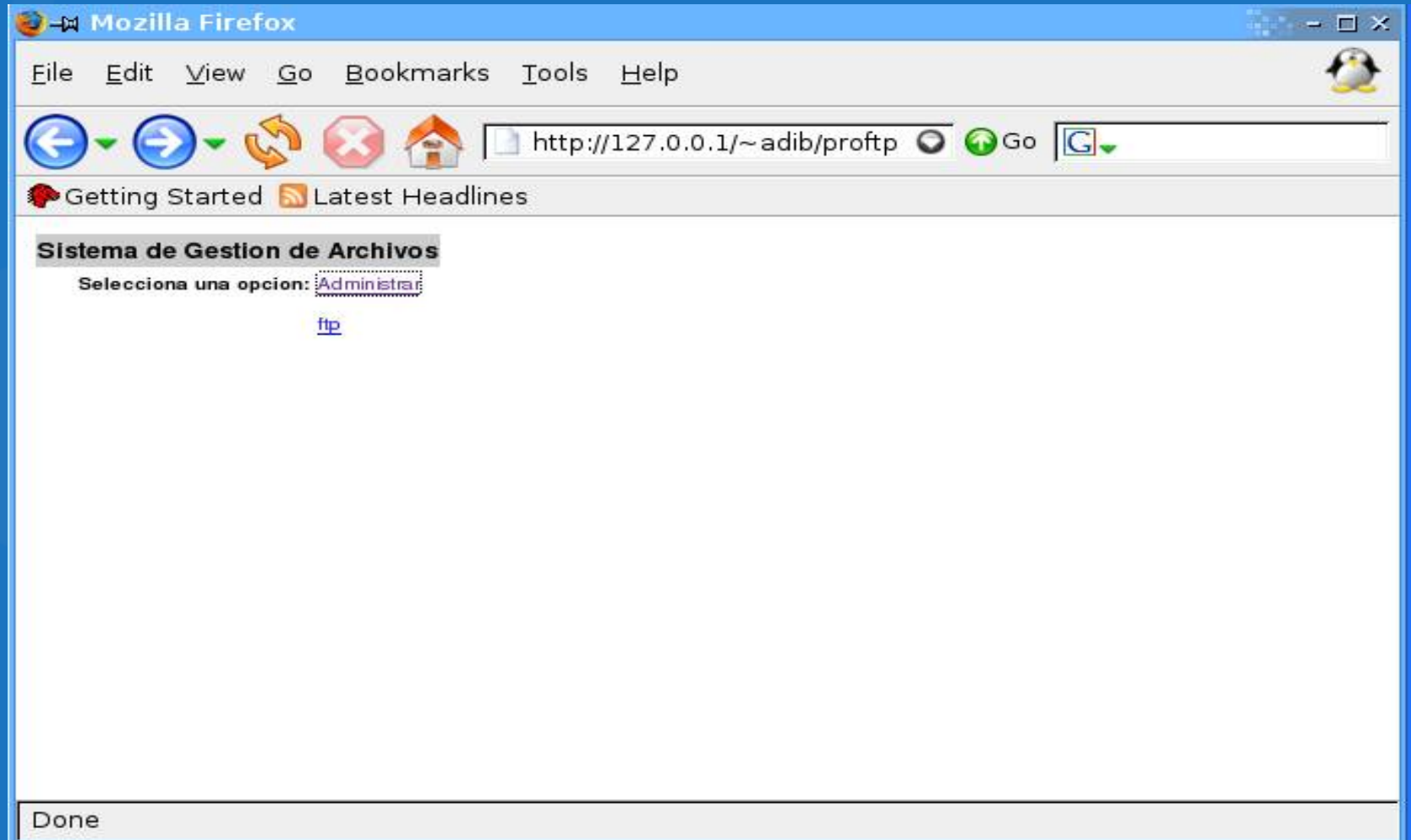
Solo se necesita reiniciar el servicio, si el archivo de configuracion esta mal editado, el demonio no podra arrancar.

En nuestra BD agregamos un usuario,...

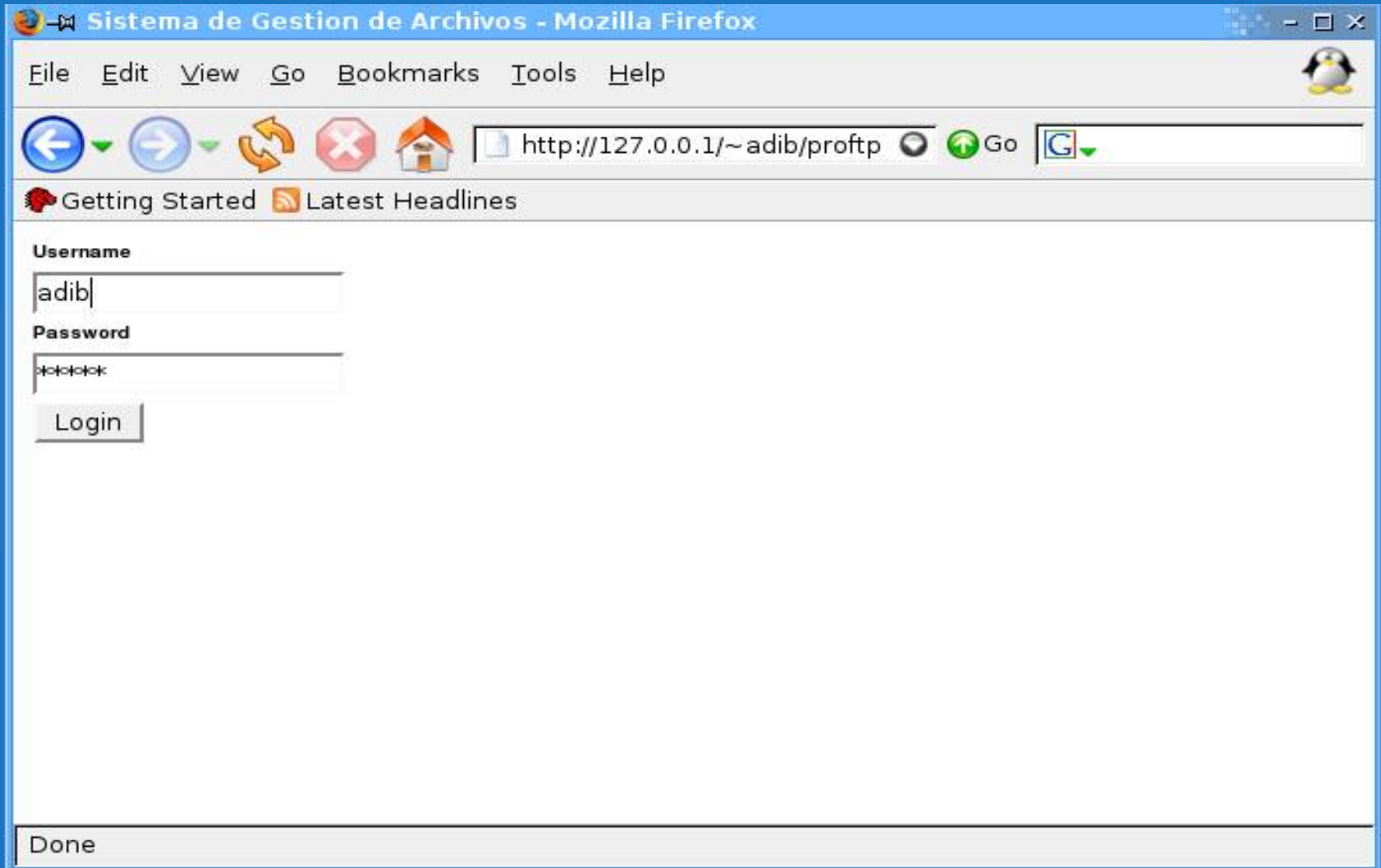
```
INSERT INTO usuarios (username, passwd,uid, gid,  
homedir, shell) VALUES  
("pepe","123pepe","501","101","/home/ftp", "/bin/sh");
```

y eso es todo, asi podremos administrar todos nuestros usuarios que necesitemos.

Administrando los usuarios



Login

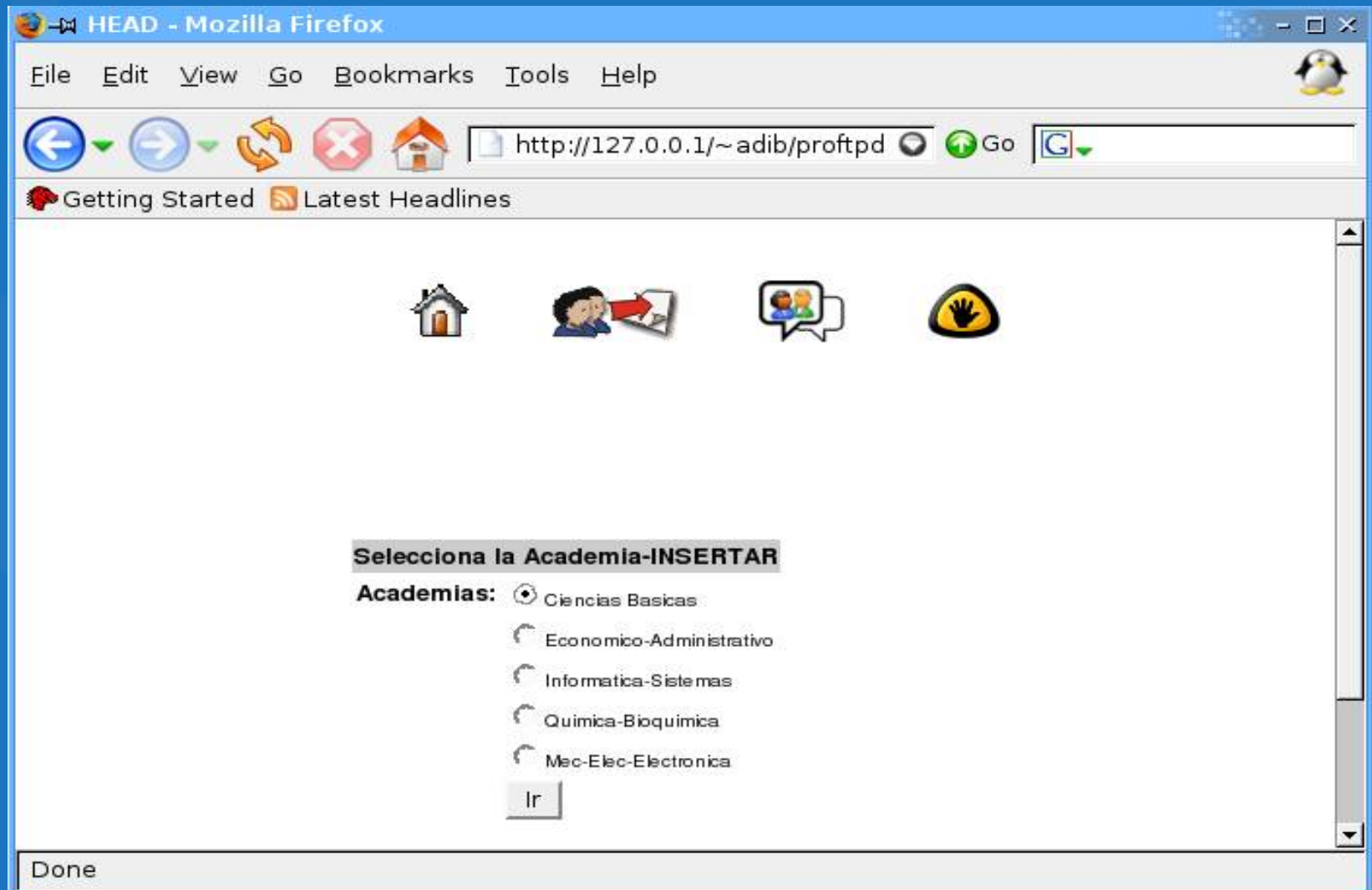


The screenshot shows a Mozilla Firefox browser window with the title "Sistema de Gestion de Archivos - Mozilla Firefox". The address bar displays the URL "http://127.0.0.1/~adib/proftp". The page content includes a login form with the following elements:

- Username**: A text input field containing the text "adib".
- Password**: A password input field with masked characters "*****".
- Login**: A button labeled "Login".

At the bottom of the browser window, the status bar shows the word "Done".

Agregando usuarios 1







Agregando usuarios 2

HEAD - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://127.0.0.1/~adib/proftpd-admin2/in Go

Getting Started Latest Headlines

username	Docente	e-mail	home
fernando	Cancino Nolasco Carlos Fernando	fernando@itesco.edu.mx	/home/fermandocl
adib	Saavedra Bocanegra Adib	adib.saavedra@itesco.edu.mx	/home/adib

Done





Agregando usuarios 3

HEAD - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://127.0.0.1/~adib/proftpd-admin2/in Go

Getting Started Latest Headlines

Datos de docente

Academia: Ciencias-Basicas

Docente: Saavedra Bocanegra Adib

Directorio: /home/adib

GID: 1000

Agregar usuarios

* Username:

Nombre usuario:

Semestre:

Grupo:

* e-mail:

El directorio debe existir y ser de tipo /usuario

Directorio usuario:

* denotes required field

Done





Agregando usuarios 4

HEAD - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://127.0.0.1/~adib/proftpd-admin2/in Go

Getting Started Latest Headlines

Datos de docente

Academia: Ciencias-Basicas

Docente: Saavedra Bocanegra Adib

Directorio: /home/adib

GID: 1000

Agregar usuarios

* Username: monica

Nombre usuario: Monica Garcia Kin

Semestre: 4

Grupo: D

* e-mail: jaz@itesco.edu.mx

El directorio debe existir y ser de tipo /usuario

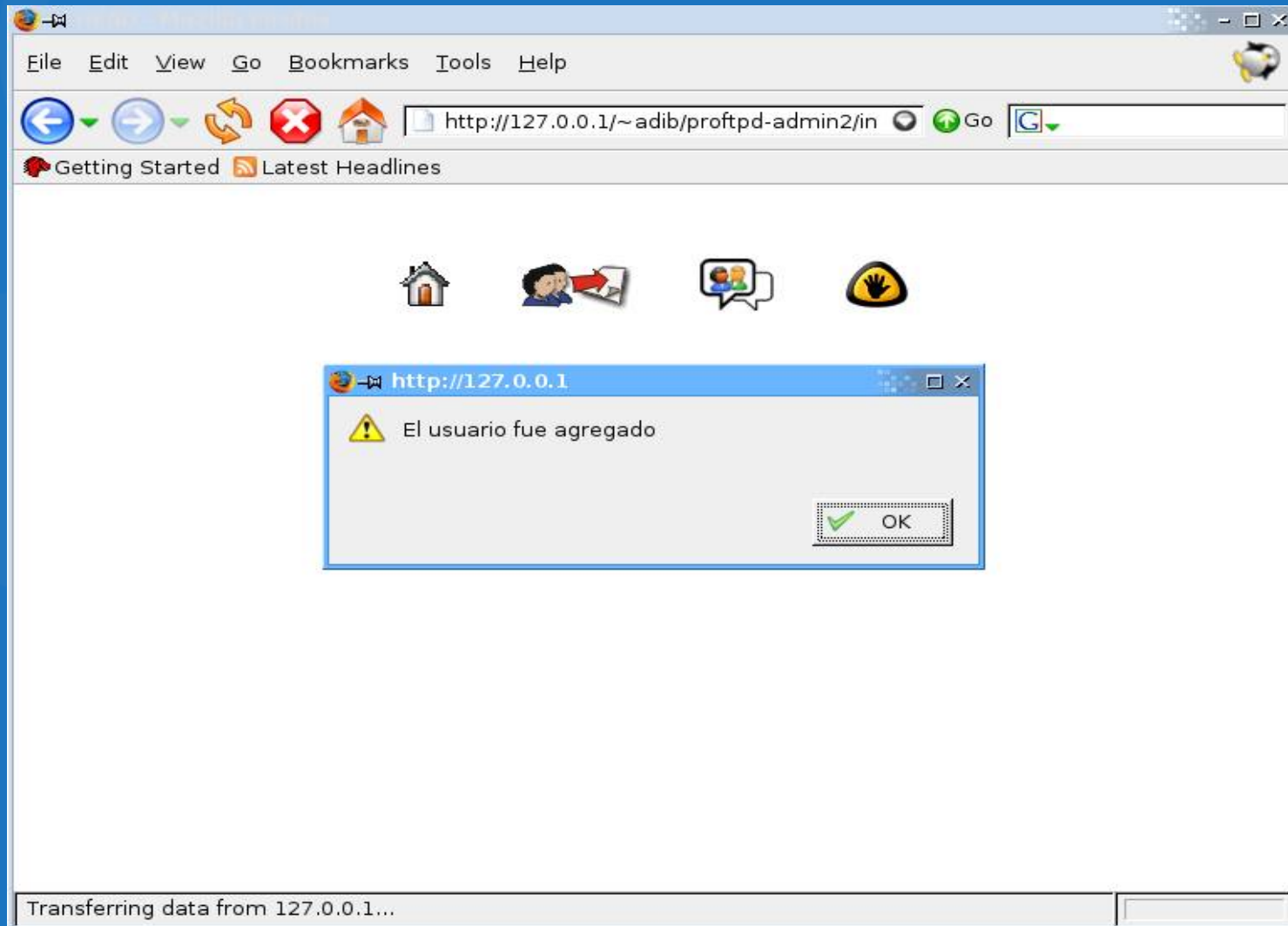
Directorio usuario: /monica

Borrar Agregar

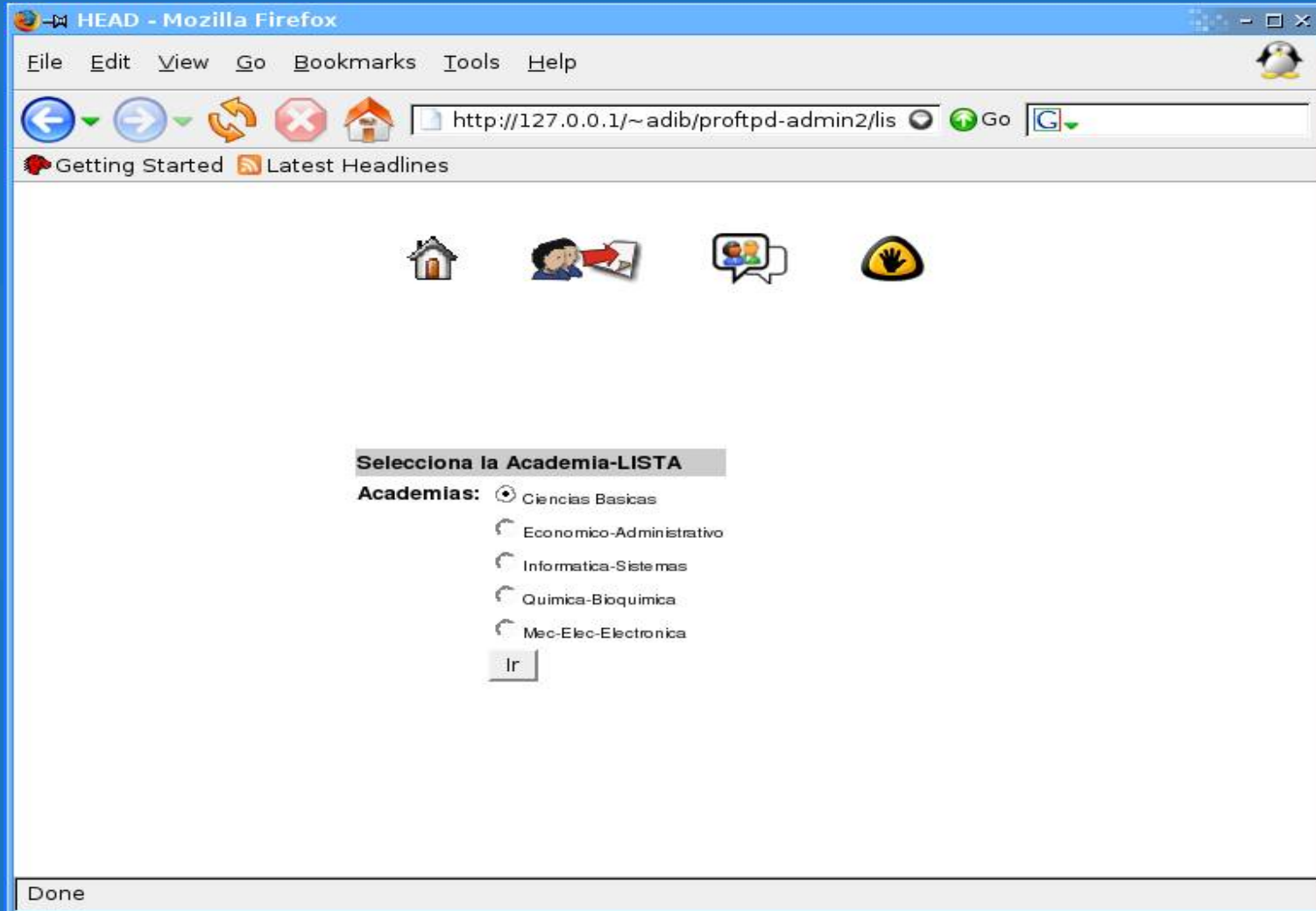
* denotes required field

Done

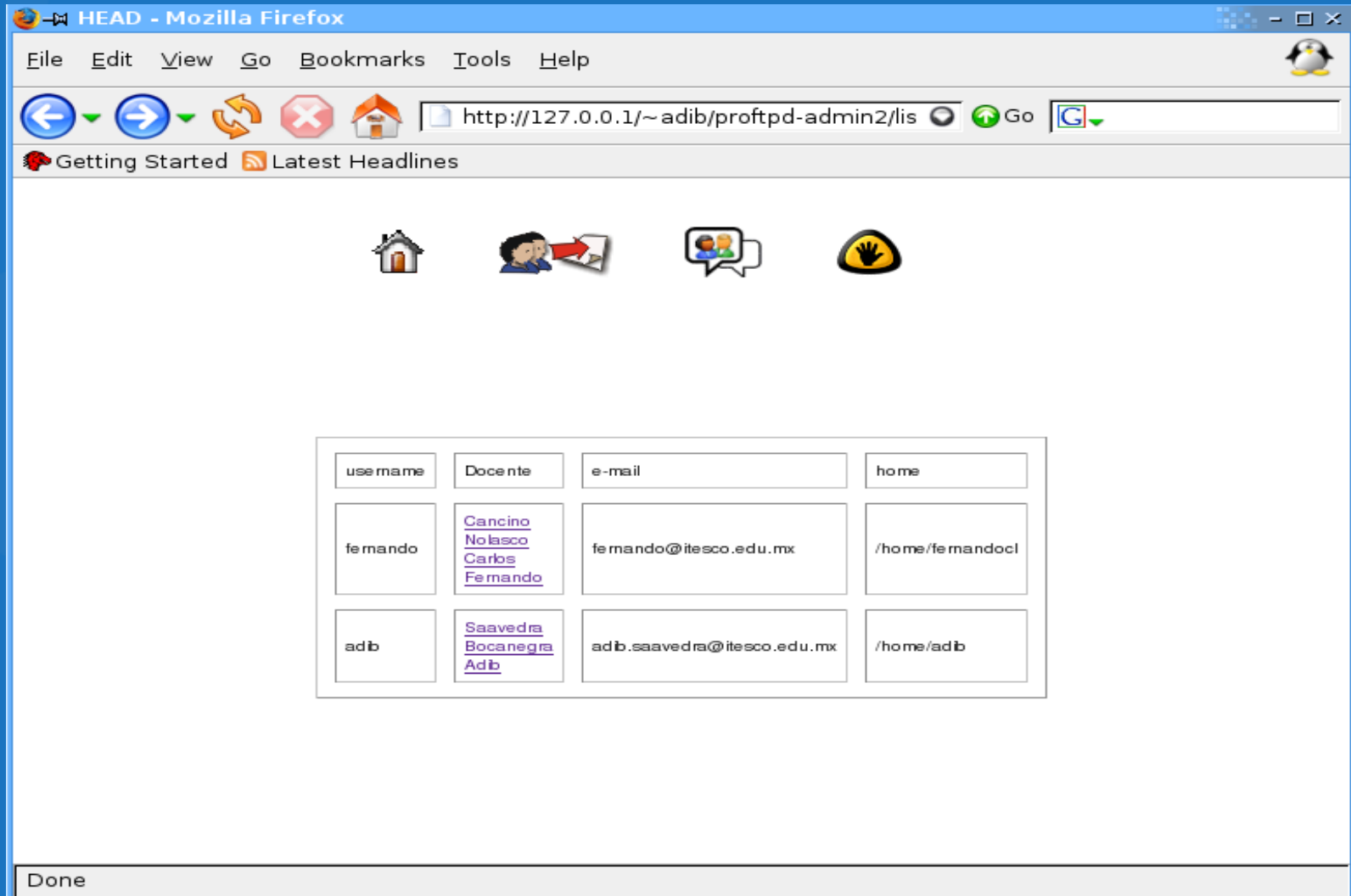
Agregando usuarios 5



Ver lista de usuarios 2



Ver lista de usuarios 3



The screenshot shows a Mozilla Firefox browser window titled "HEAD - Mozilla Firefox". The address bar displays the URL "http://127.0.0.1/~adib/proftpd-admin2/lis". The browser interface includes a menu bar (File, Edit, View, Go, Bookmarks, Tools, Help) and a toolbar with navigation buttons. Below the toolbar, there are links for "Getting Started" and "Latest Headlines". The main content area features four icons: a house, a person with a red arrow, a group of people in a speech bubble, and a yellow warning sign. At the bottom of the page, a table lists user information.

use name	Docente	e-mail	home
fermando	Cancino Nolasco Carlos Fernando	fermando@itesco.edu.mx	/home/fermandocl
adib	Saavedra Bocanegra Adib	adib.saavedra@itesco.edu.mx	/home/adib

Done





Ver lista de usuarios 4





HEAD - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://127.0.0.1/~adib/proftpd-admin2/lis Go

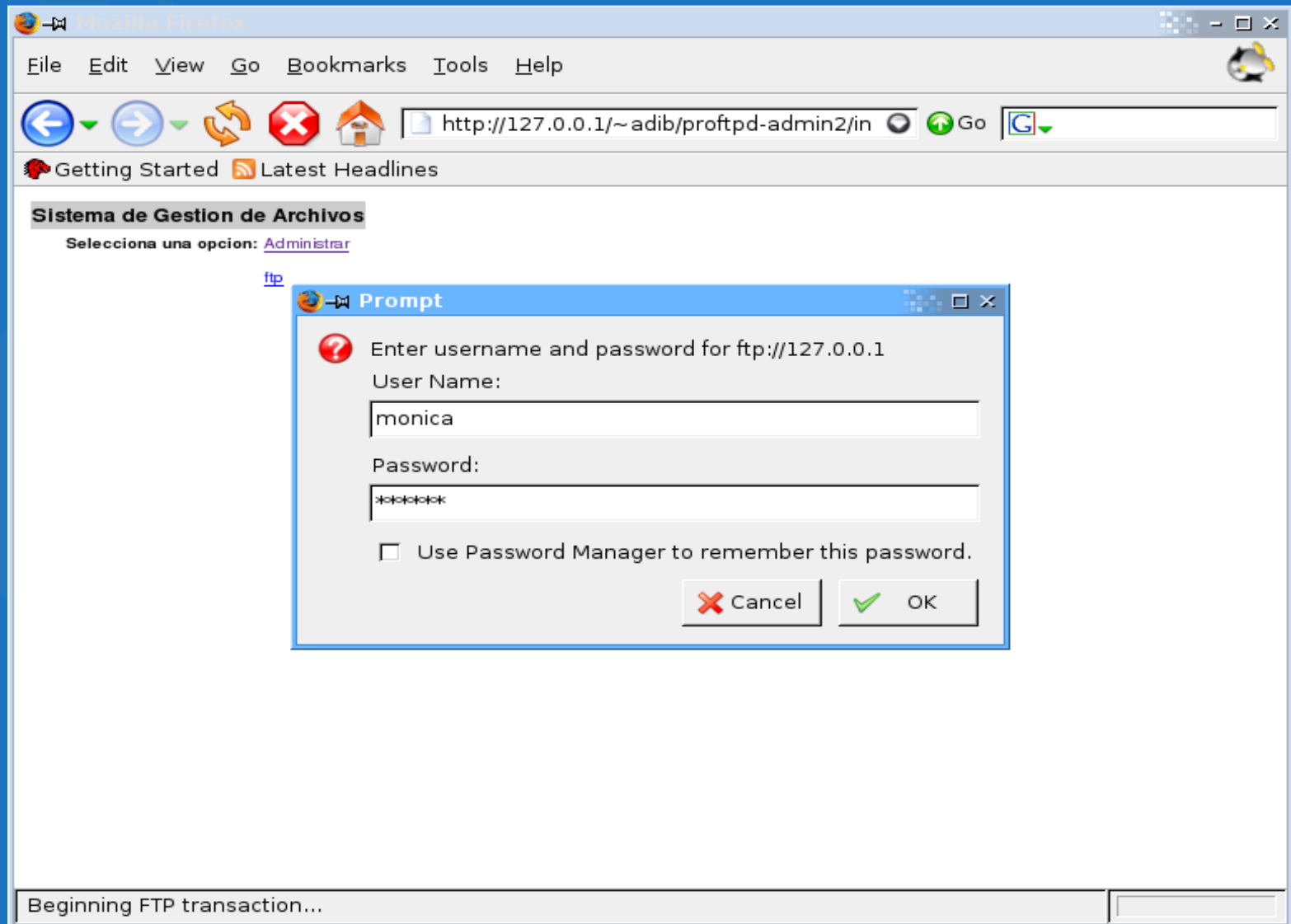
Getting Started Latest Headlines

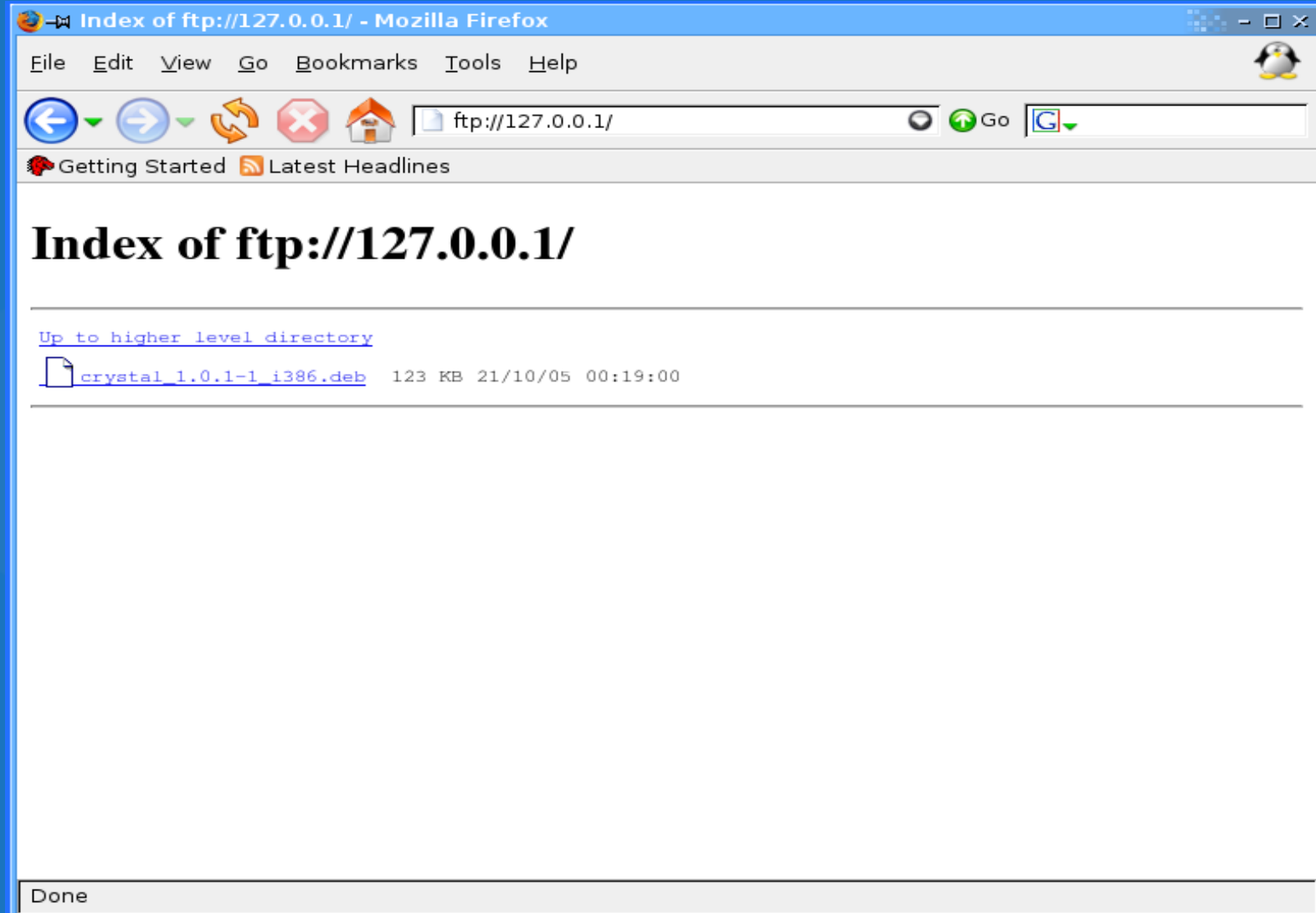
username	Nombre	se mestre	grupo	e-mail	password	directorio	Docente
pepe	Jose Luis	2	A	pepe@itesco.edu.mx	OahXDW	/home/adib/ponencias	 
monica	Monica Garcia Kin	4	D	jaz@itesco.edu.mx	bMPnOM	/home/adib/monica	 

Done

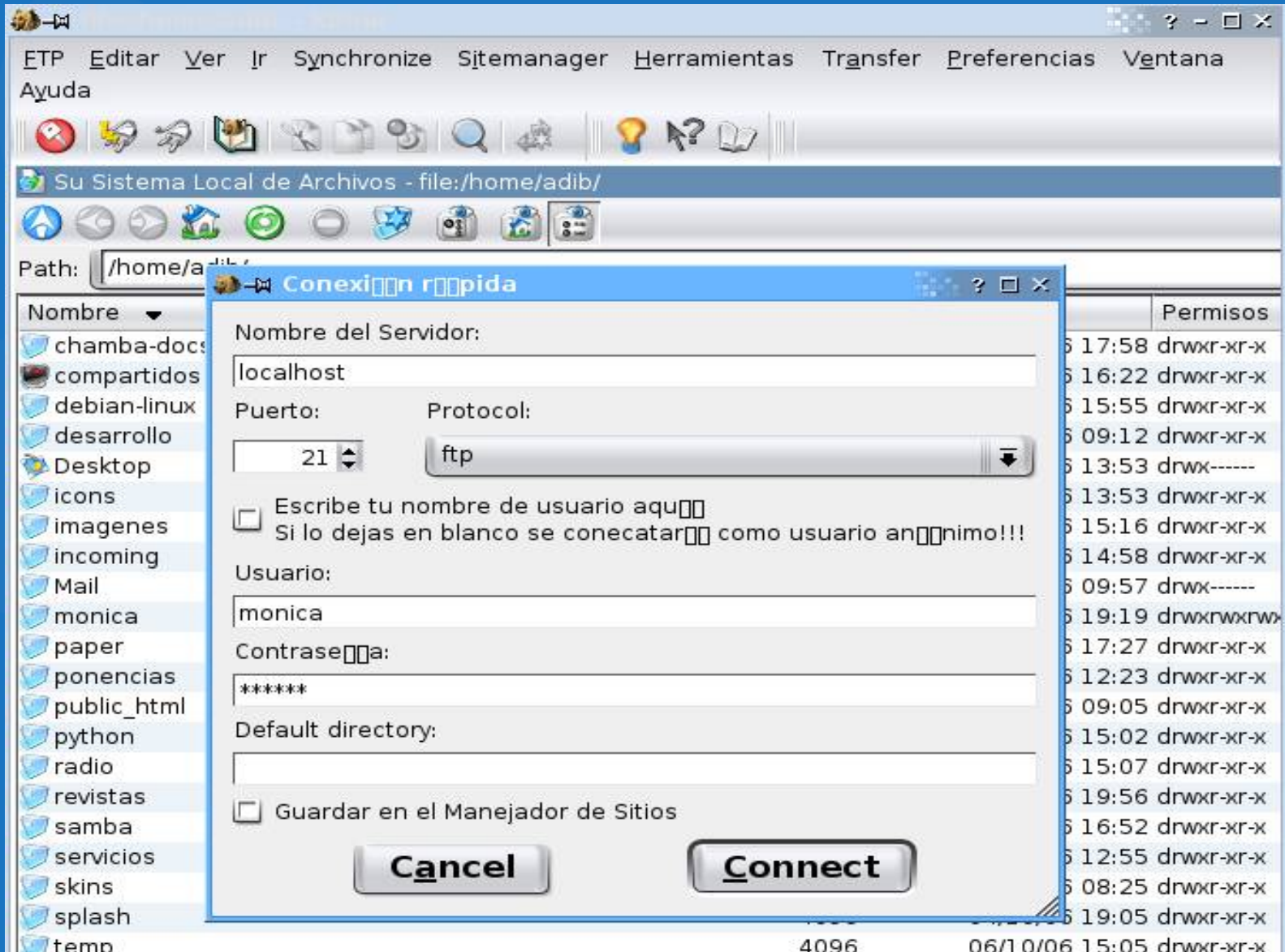
Ingresar al servidor 1



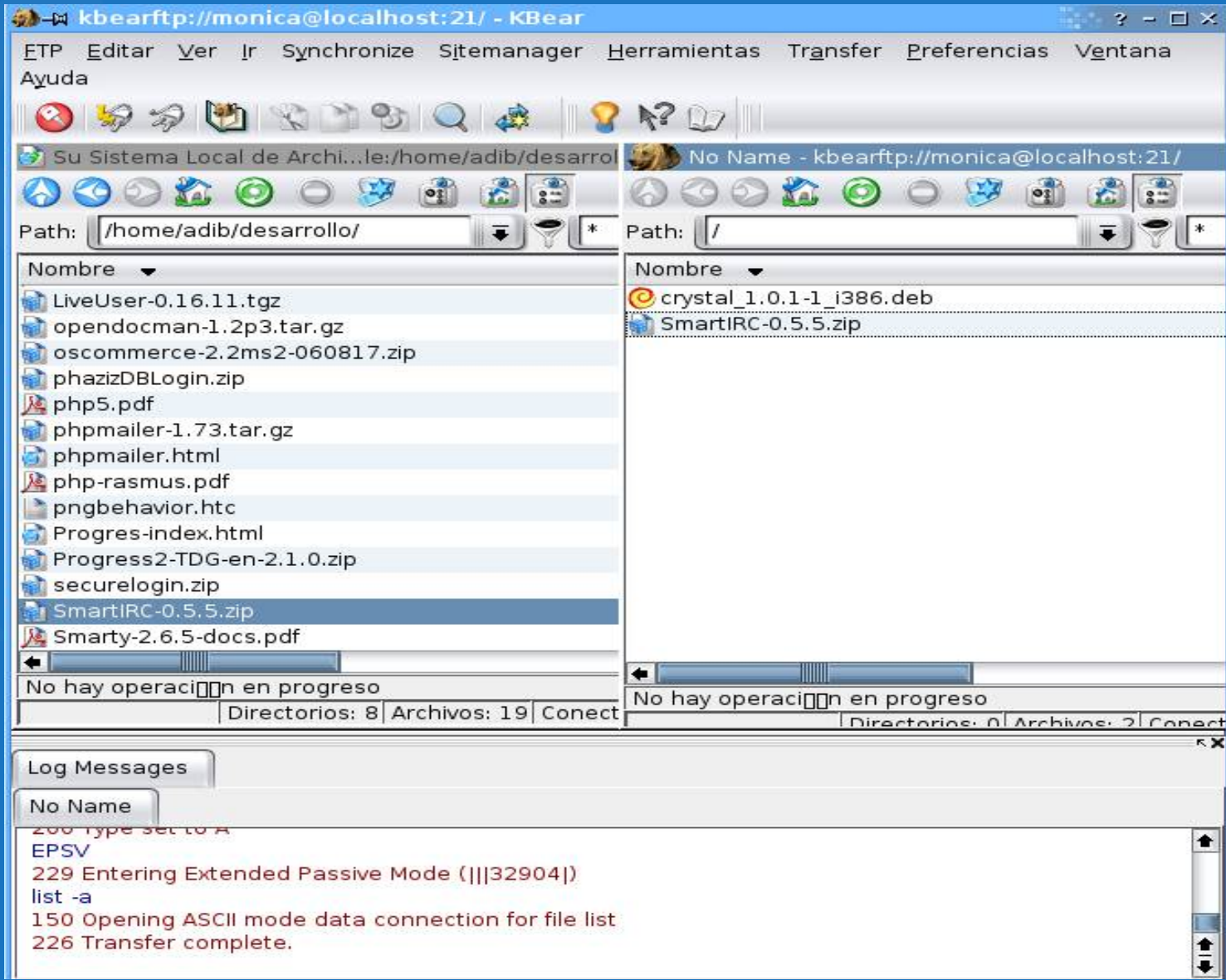
Ingresar al servidor 2



Subir archivos al servidor 1



Subir archivos al servidor 2



Analisar logs

Los logs se pueden analizar en el path, `/var/log/xferlogs`, es un archivo cuyo contenido puede ser extraido a un archivo de texto, o de la mejor manera a una BD, para su administracion.

Preguntas

,.....