Anexando Seguridad a un Servidor Proftpd & modulo mod_sql_mysql.c

Adib Saavedra Bocanegra

http://adib.mx.vg

ENLI 2006

Puebla, Pueb.

Indice general

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 autentificar 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 caracteristicas 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 quotas (de usuario)
* Otros sistemas de authenticación como LDAP, Mysql, Postgresql, ...
* Gestión de ratios
* Gestión de ancho de banda

En un sistema debian o similares, se instala con:

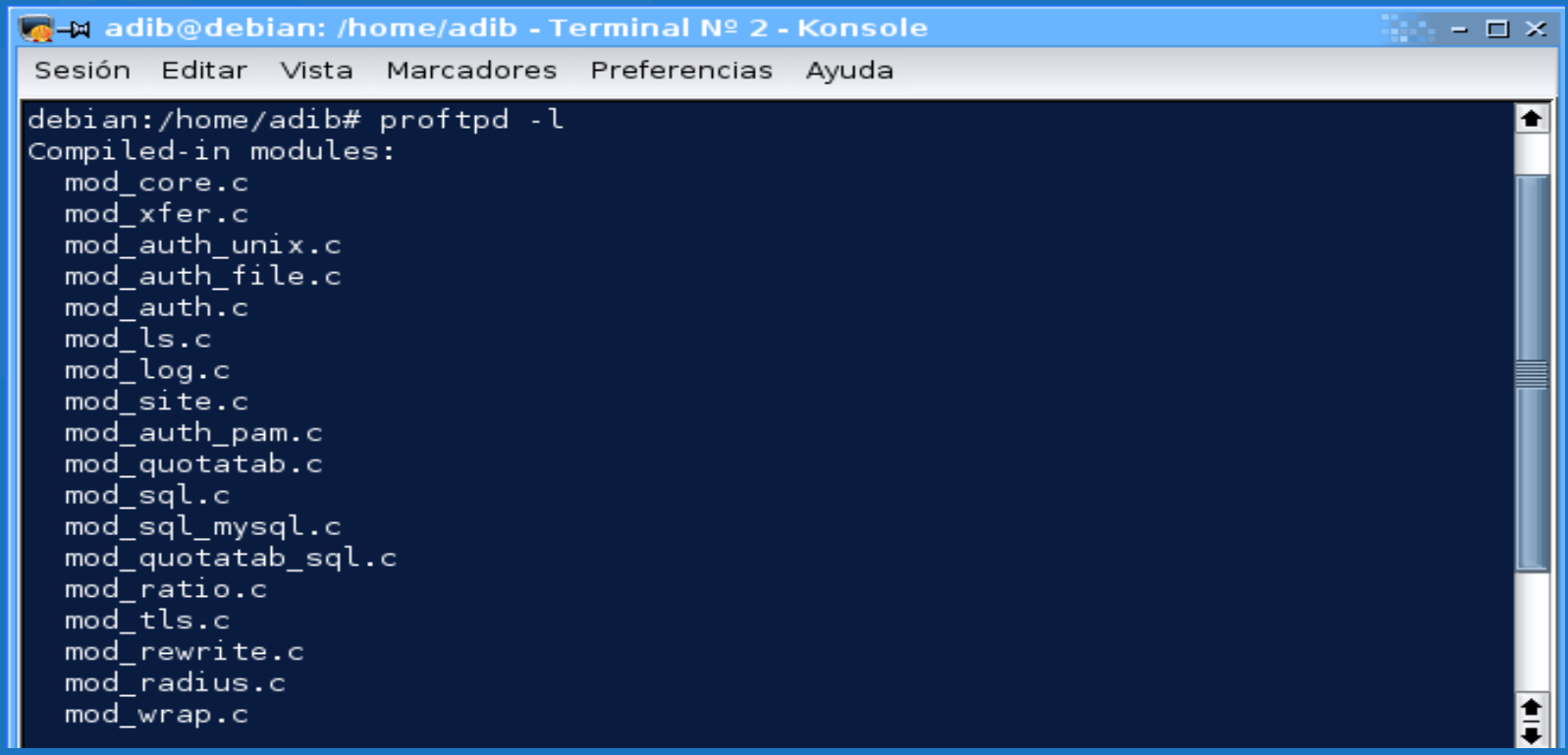
apt-get install proftpd-mysql

Instrucciones basicas

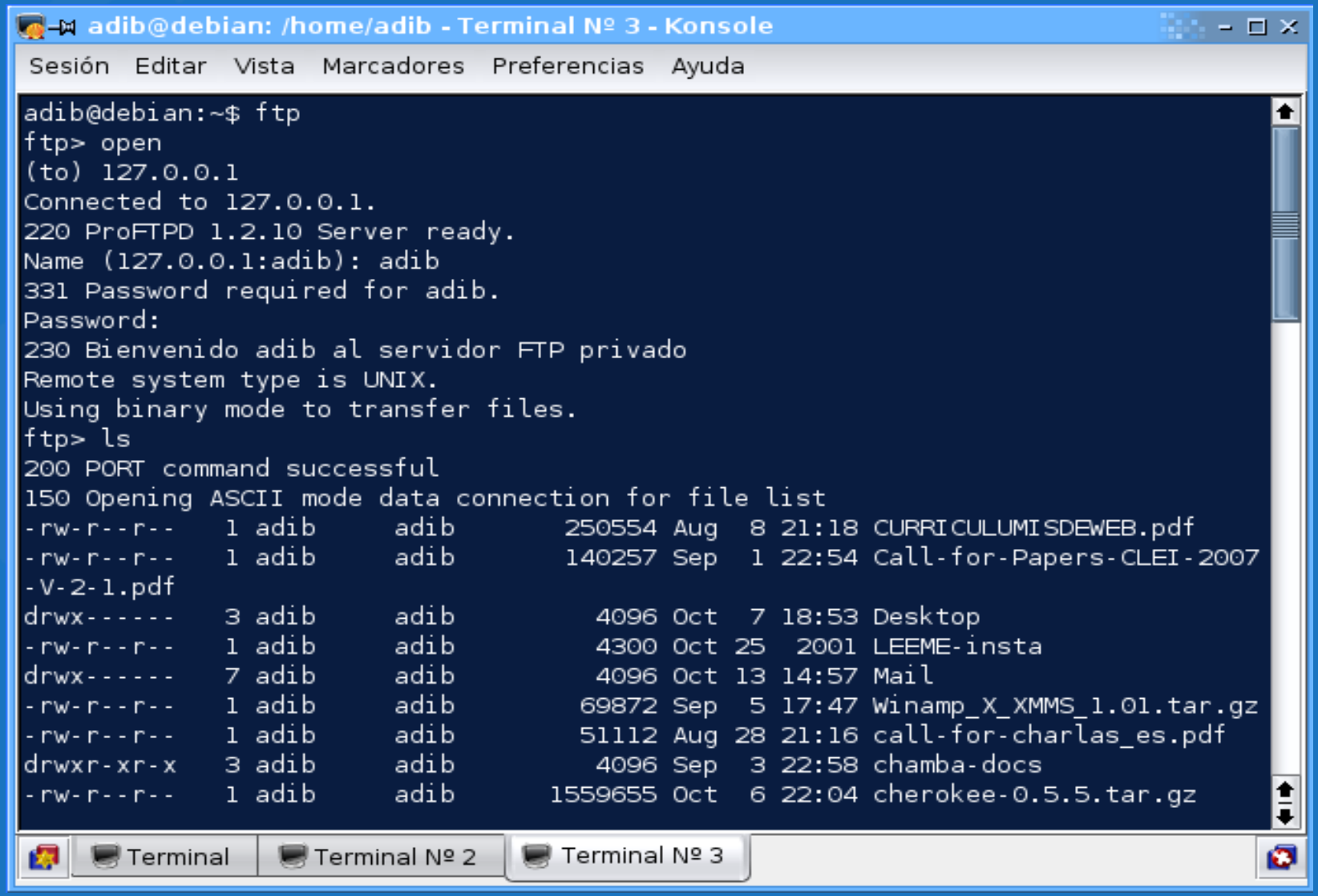
levantar el servicio: proftpd start

detener el servicio: proftpd stop

reiniciar el servicio: proftpd restart



Iniciando el servicio

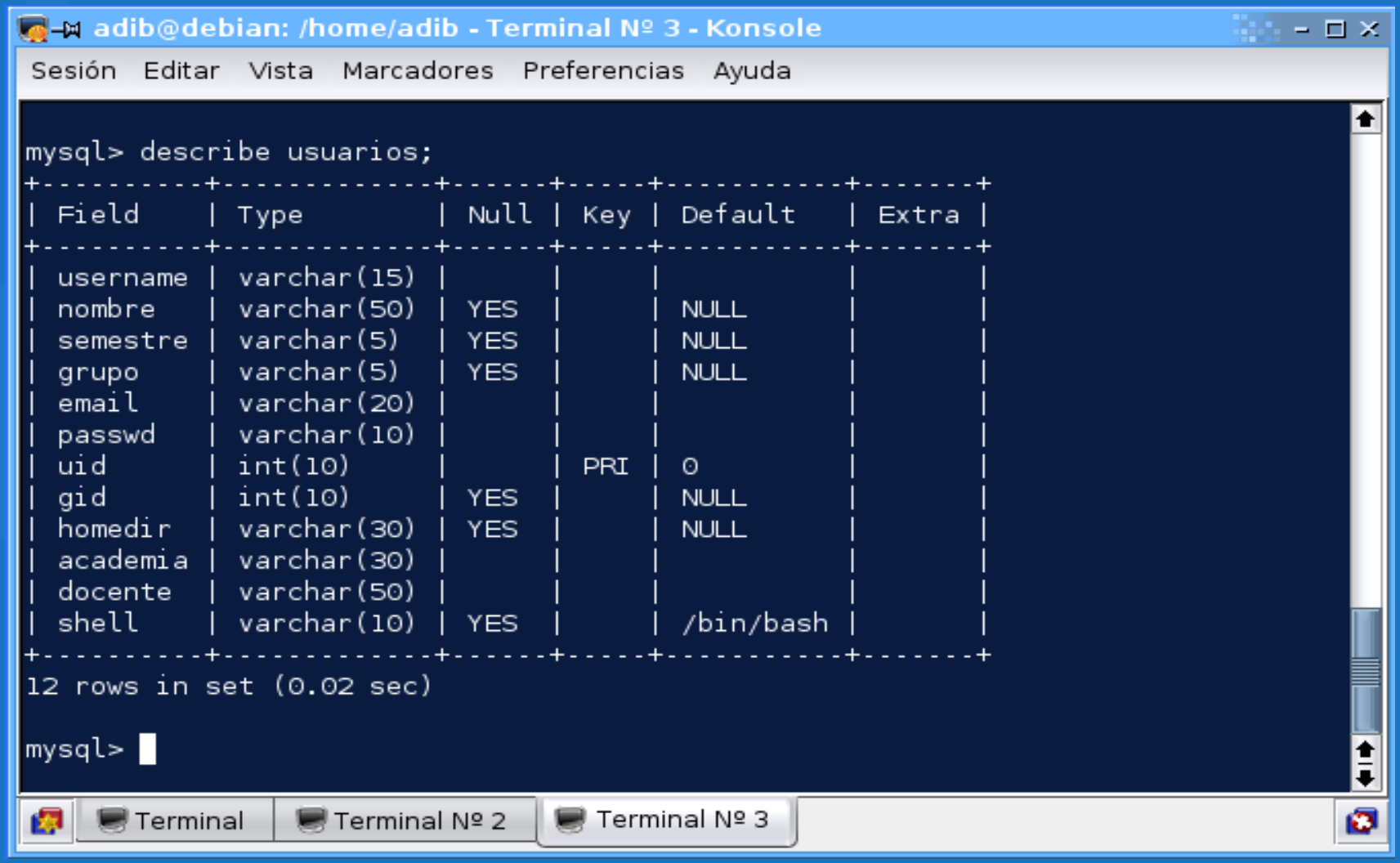


Creando la BD

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



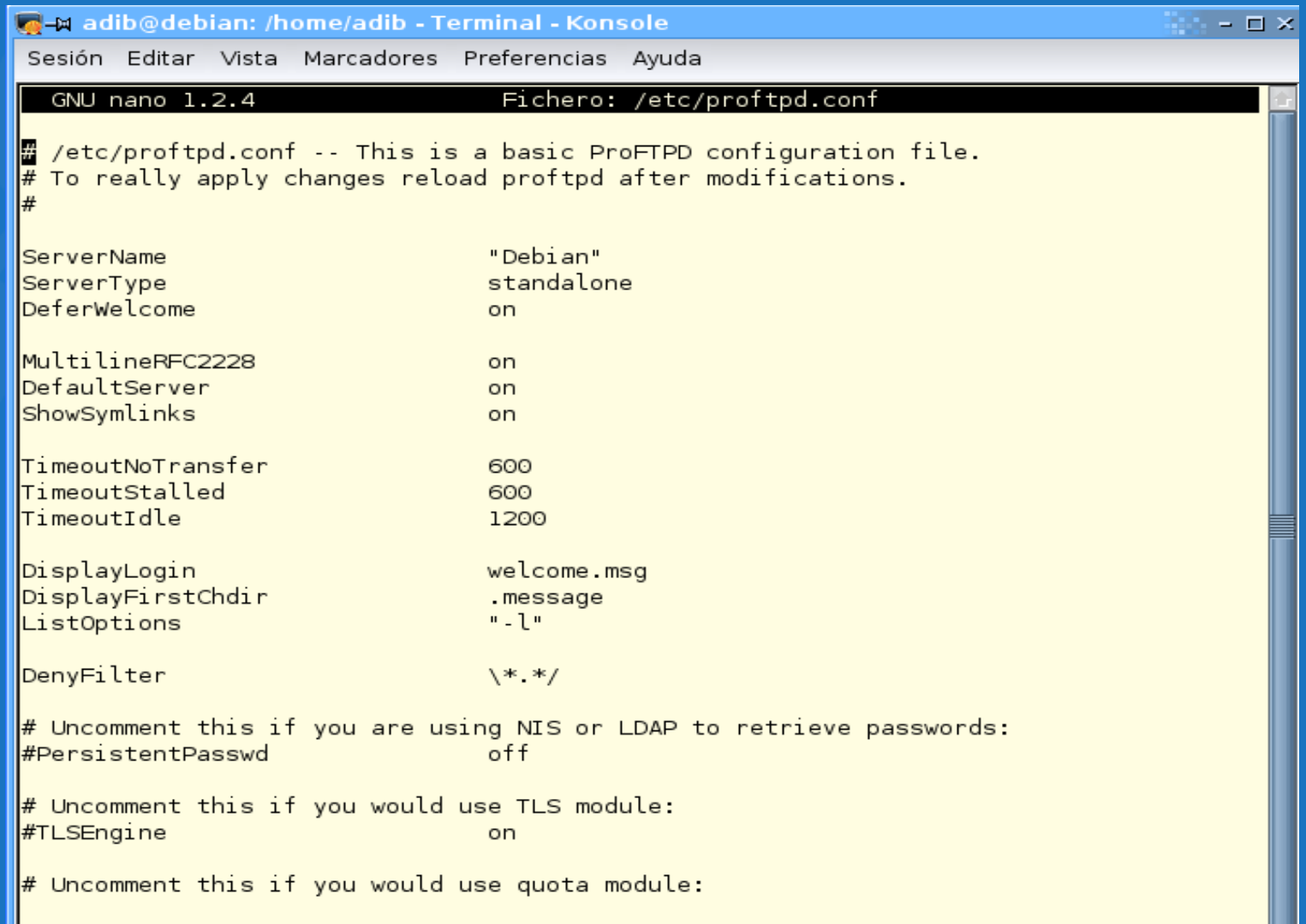
Creando privilegios

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

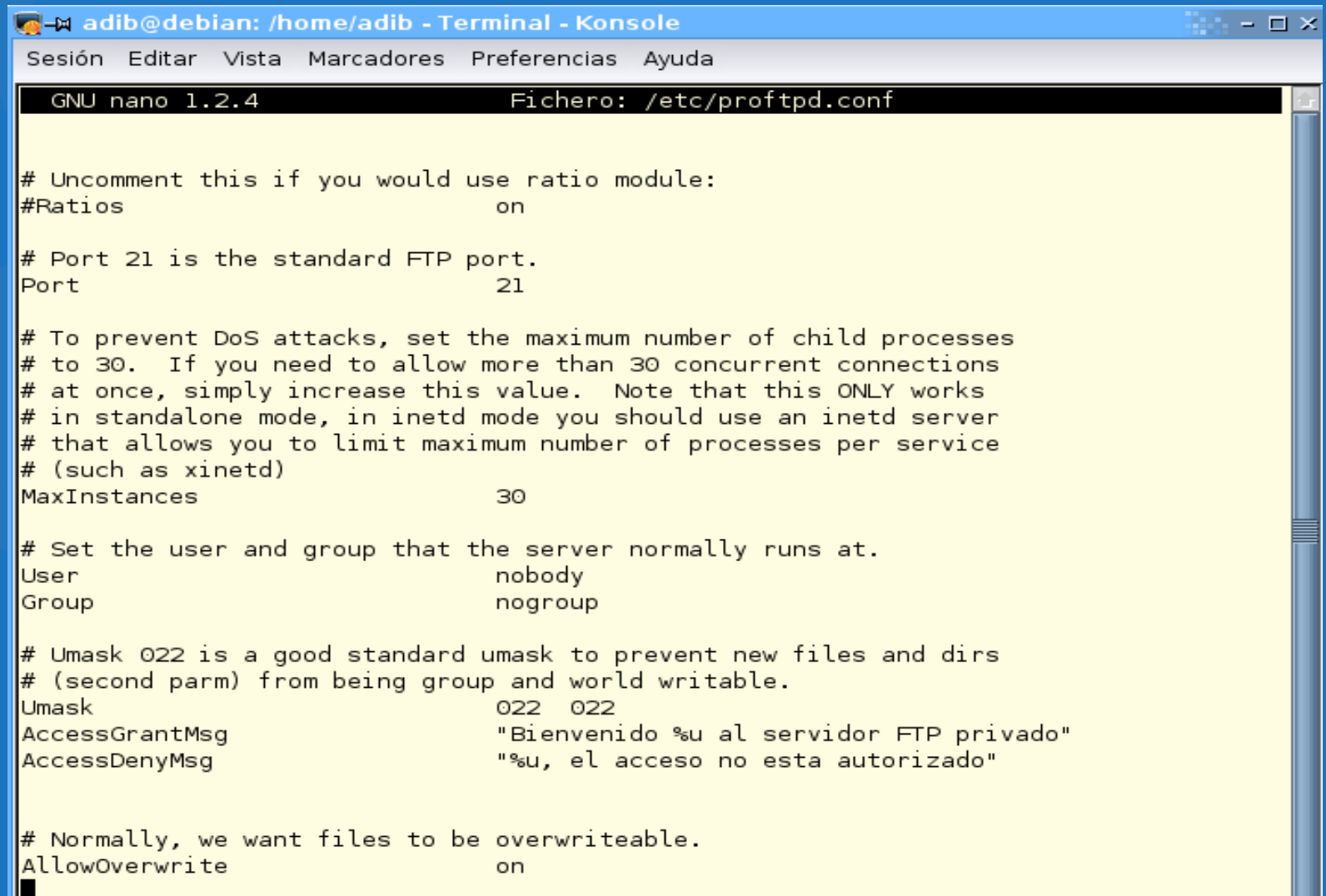
```
mysql -p
Enter password:
mysql> GRANT insert, selec, delete ON proftpd.*
TO ftpadmin@localhost IDENTIFIED BY '123admin';
```

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

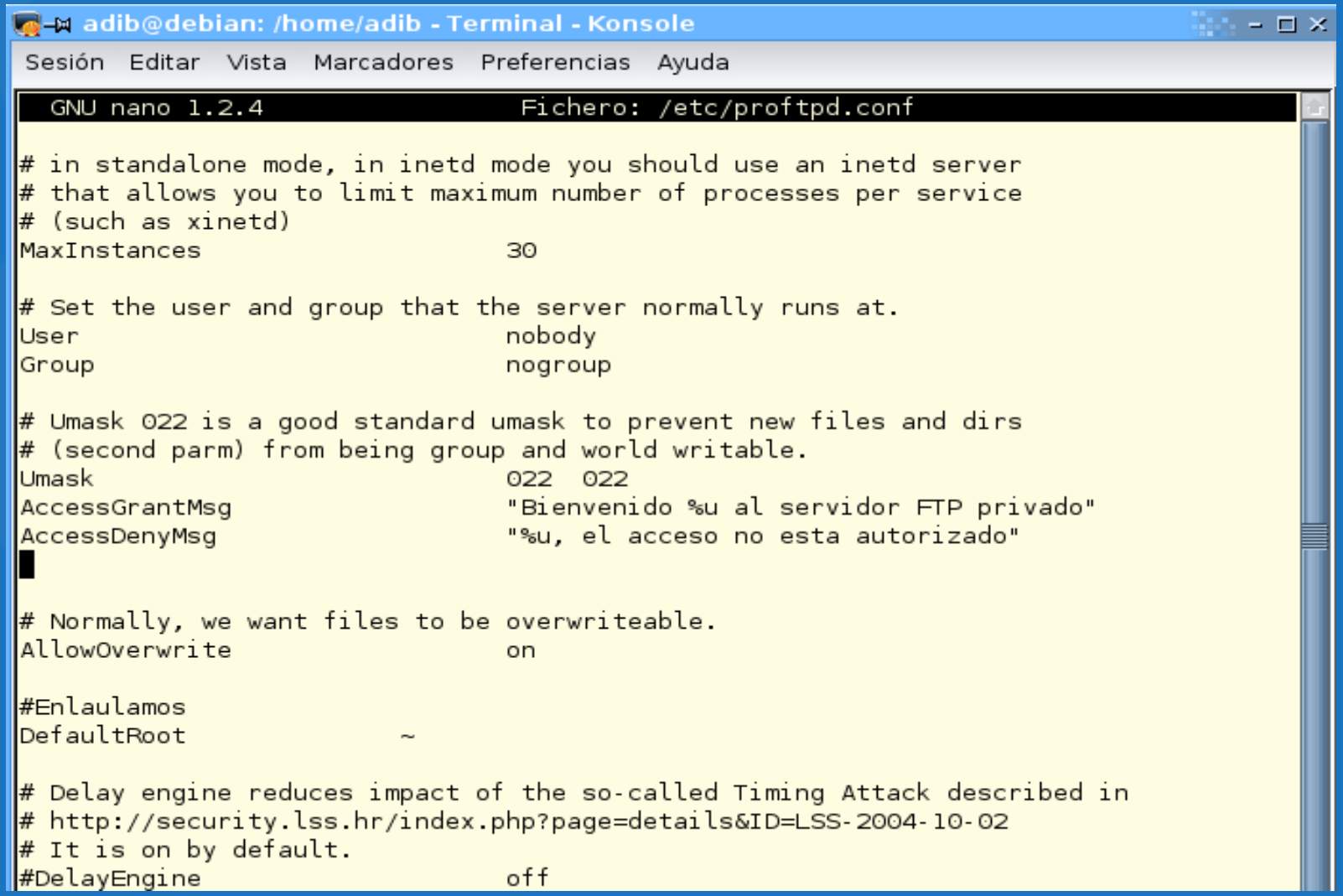
Editando el archivo /etc/proftpd.conf 1a parte



Editando el archivo /etc/proftpd.conf 2a parte



Editando el archivo /etc/proftpd.conf 3a parte



Editando el archivo /etc/proftpd.conf 4a parte

Agregando usuarios

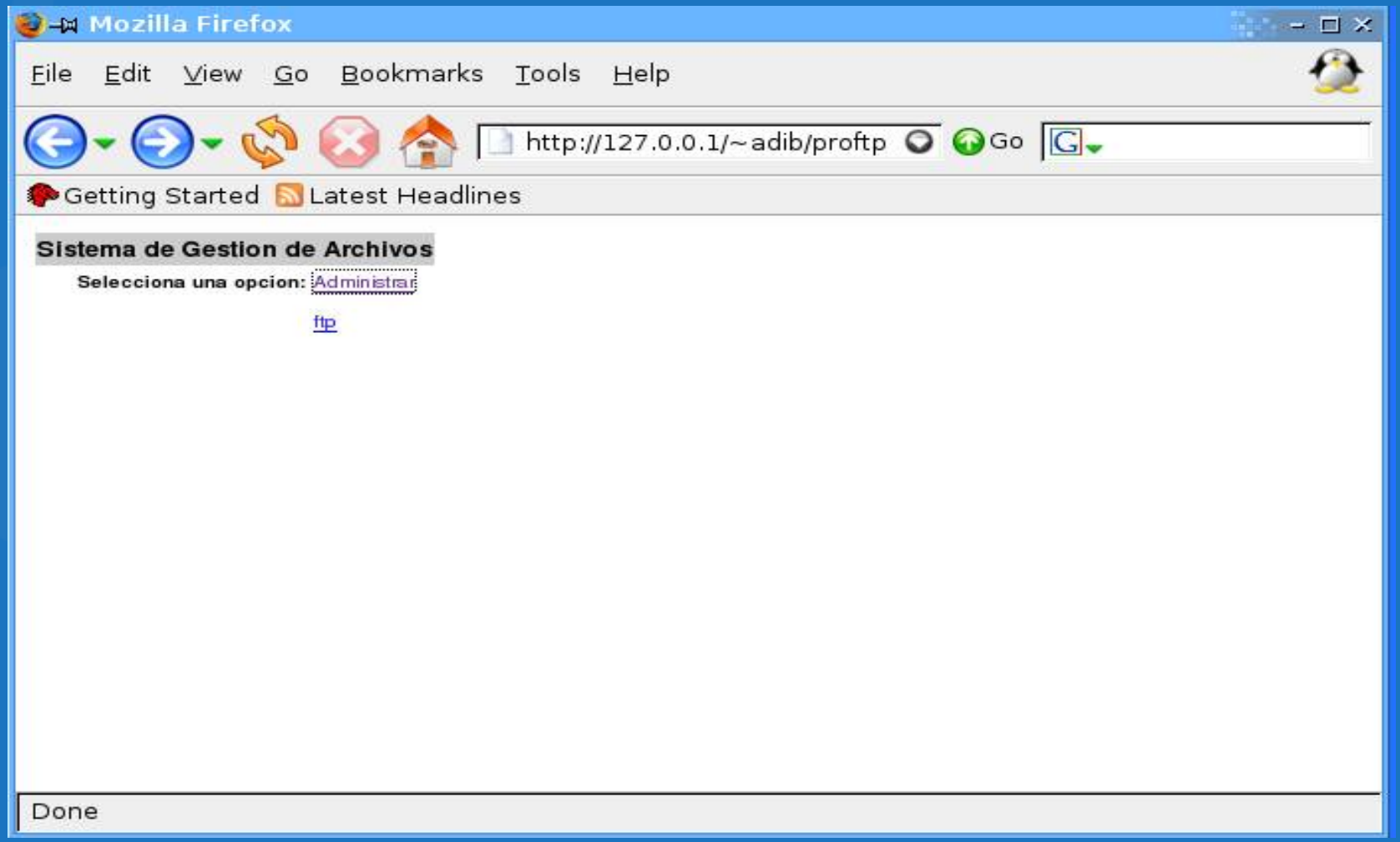
Solo se necesita reiniciar el servicio, si el archivo de configuracion esta mal editado, el demonio no podra arrancar.

En nuestra BD agregamos un usuario,..

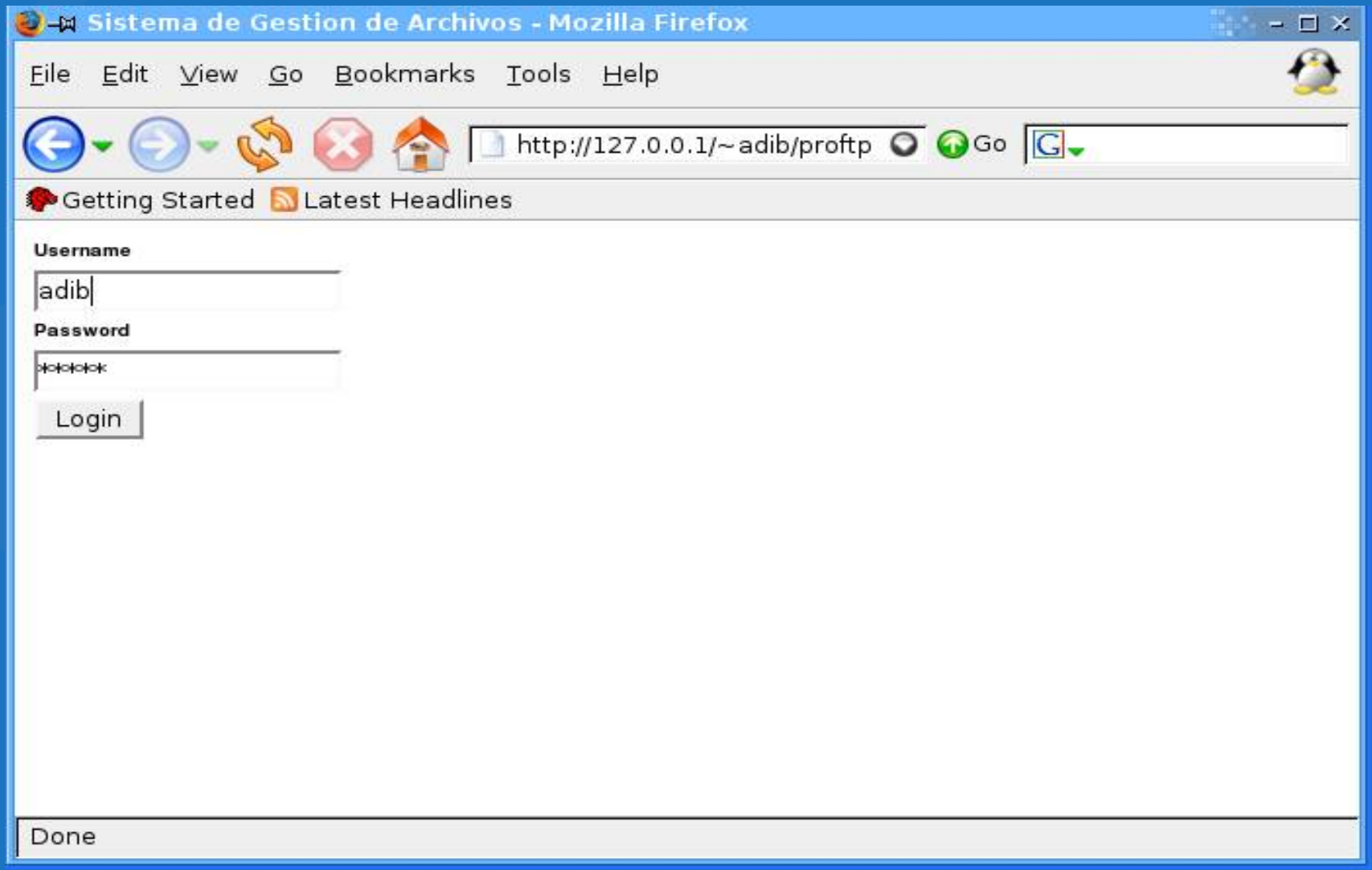
INSERT INTO usuarios (username, passwd,uid, gid, homedir, shell) VALUES ("pepe","123pepe","501","101","/home/ftp", "/bin/sh");

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

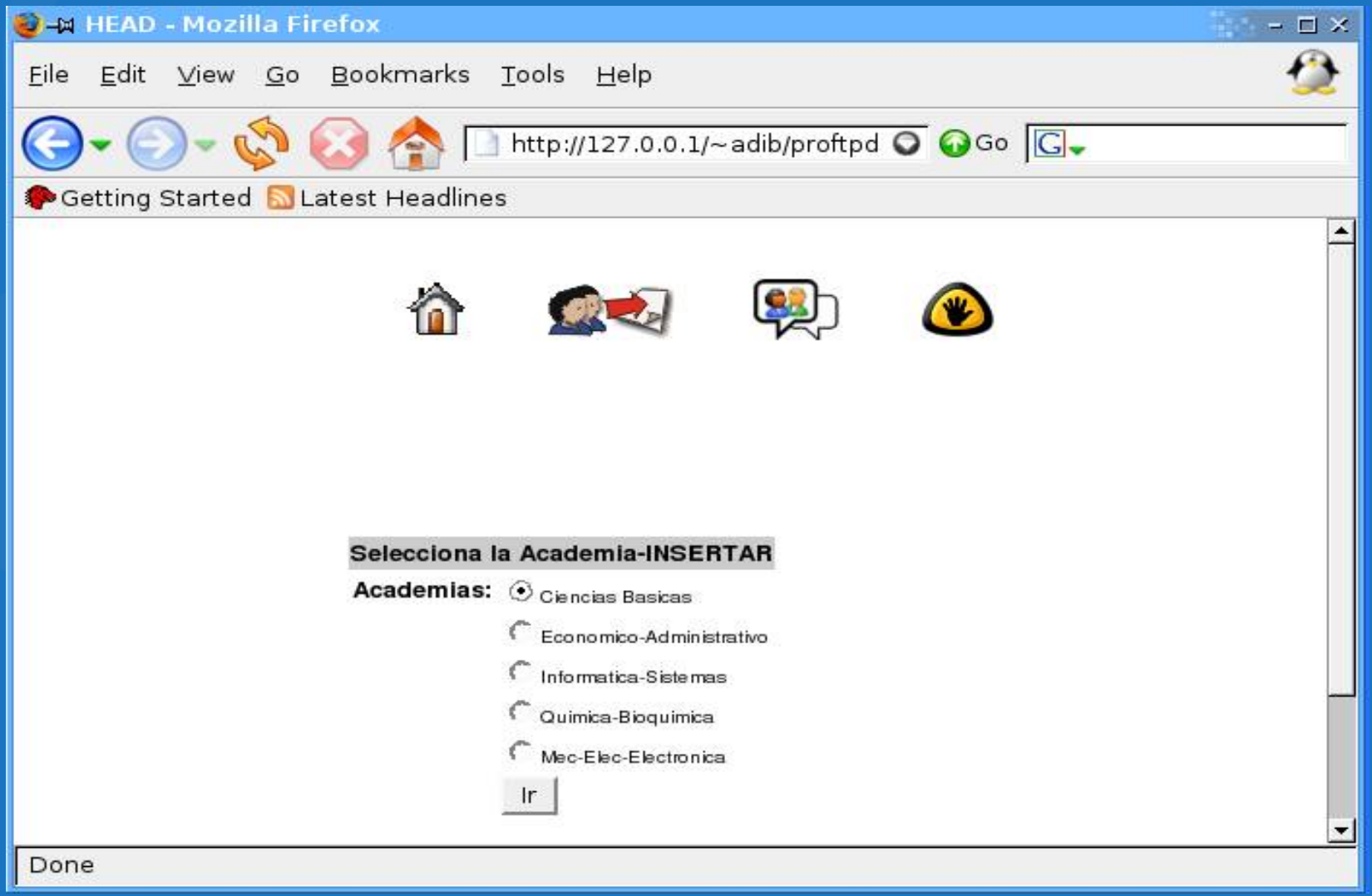
Administrando los usuarios



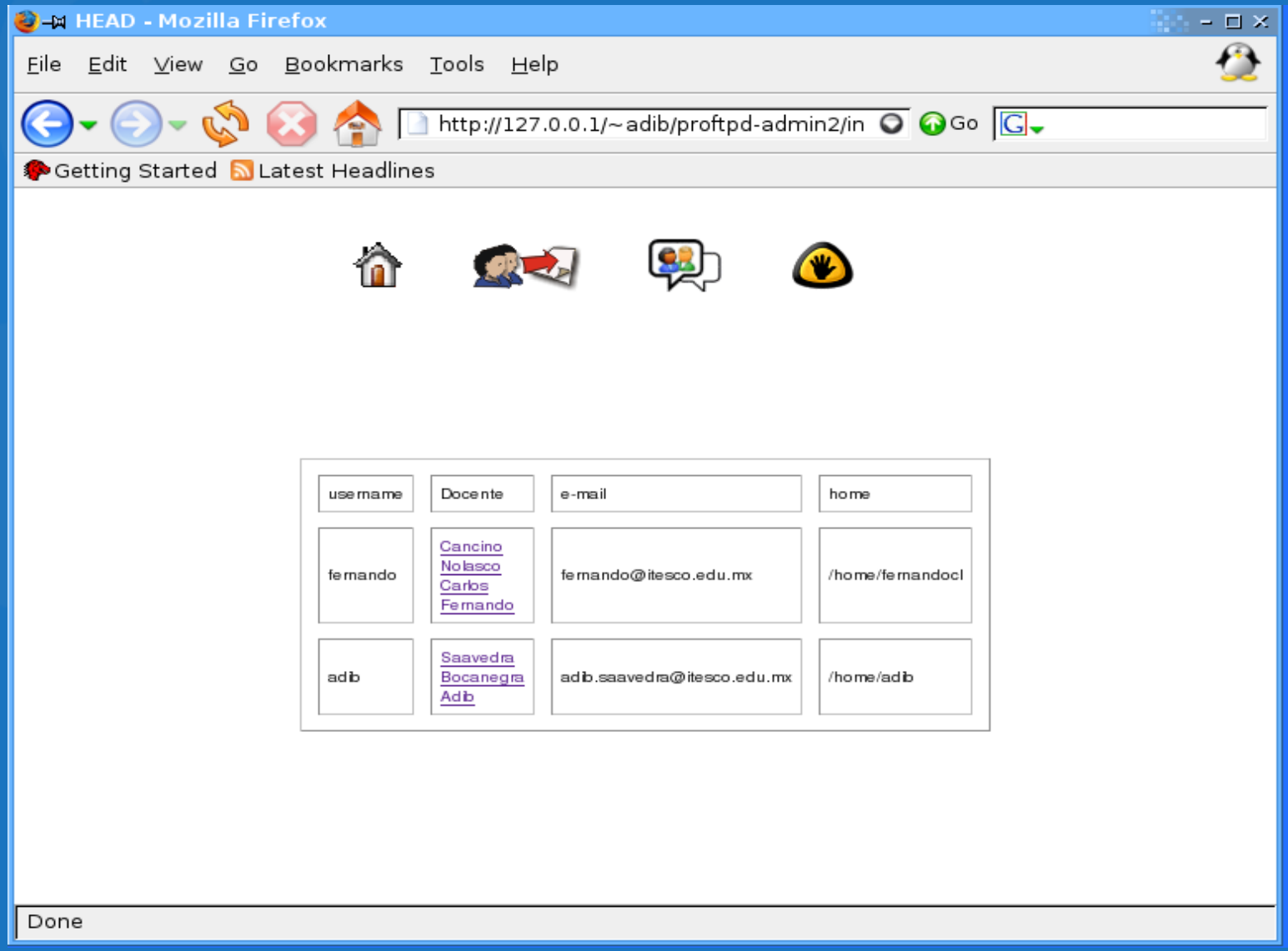
Login


Sistema de Gestion de Archivos - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://127.0.0.1/~adib/proftp
Go
Getting Started
Latest Headlines
Username
adib
Password
Login
Done

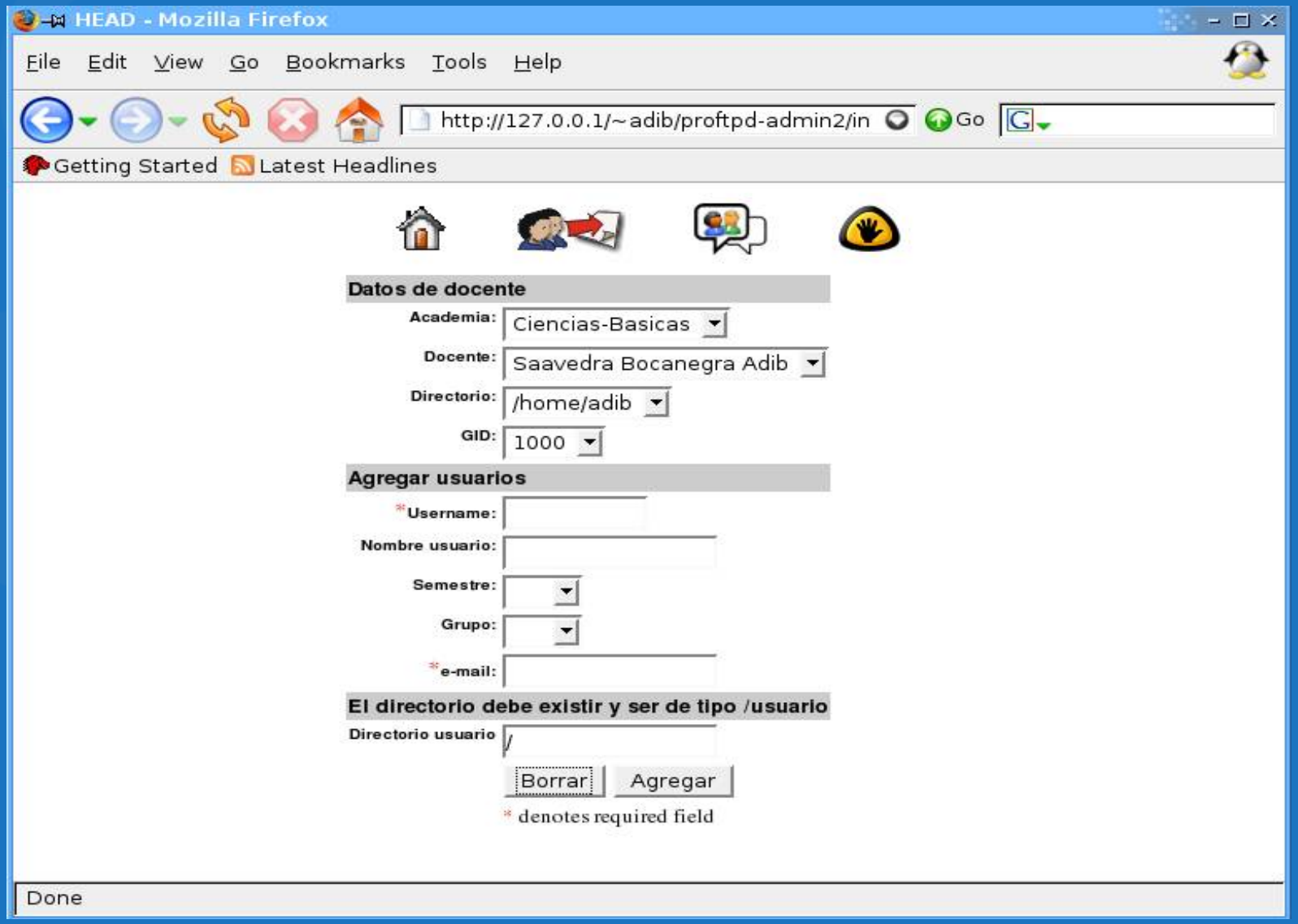
Agregando usuarios 1



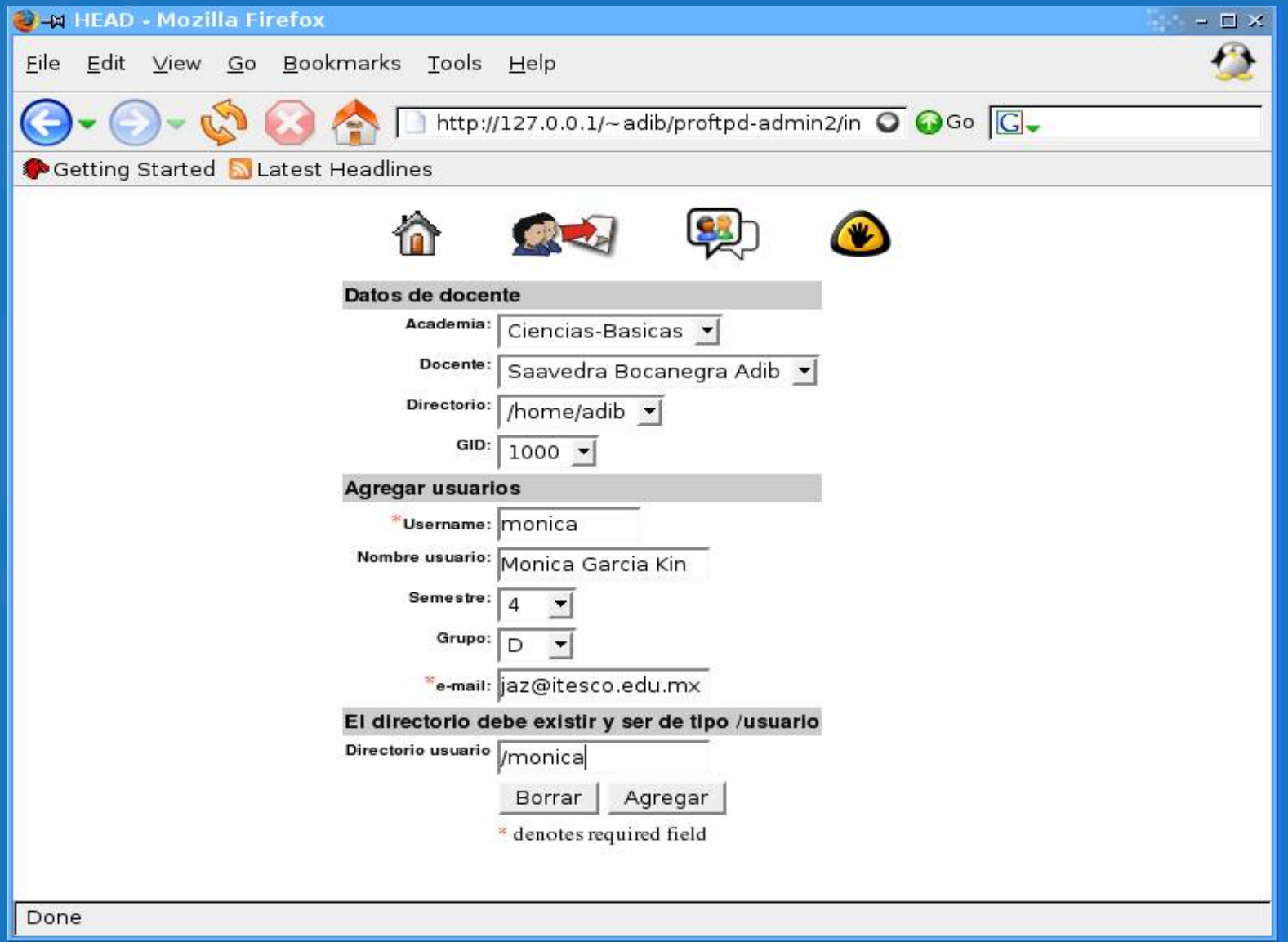
Agregando usuarios 2



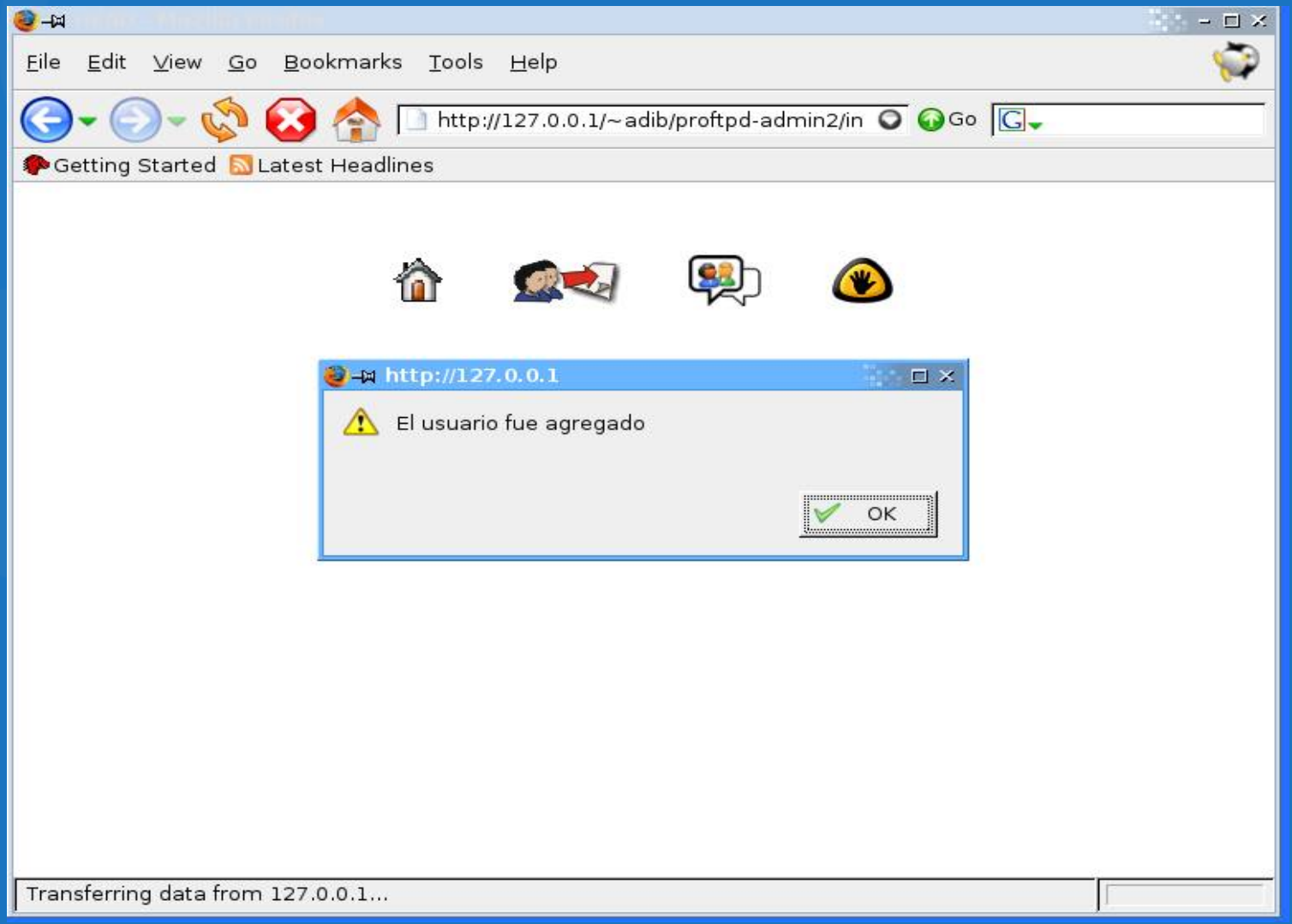
Agregando usuarios 3



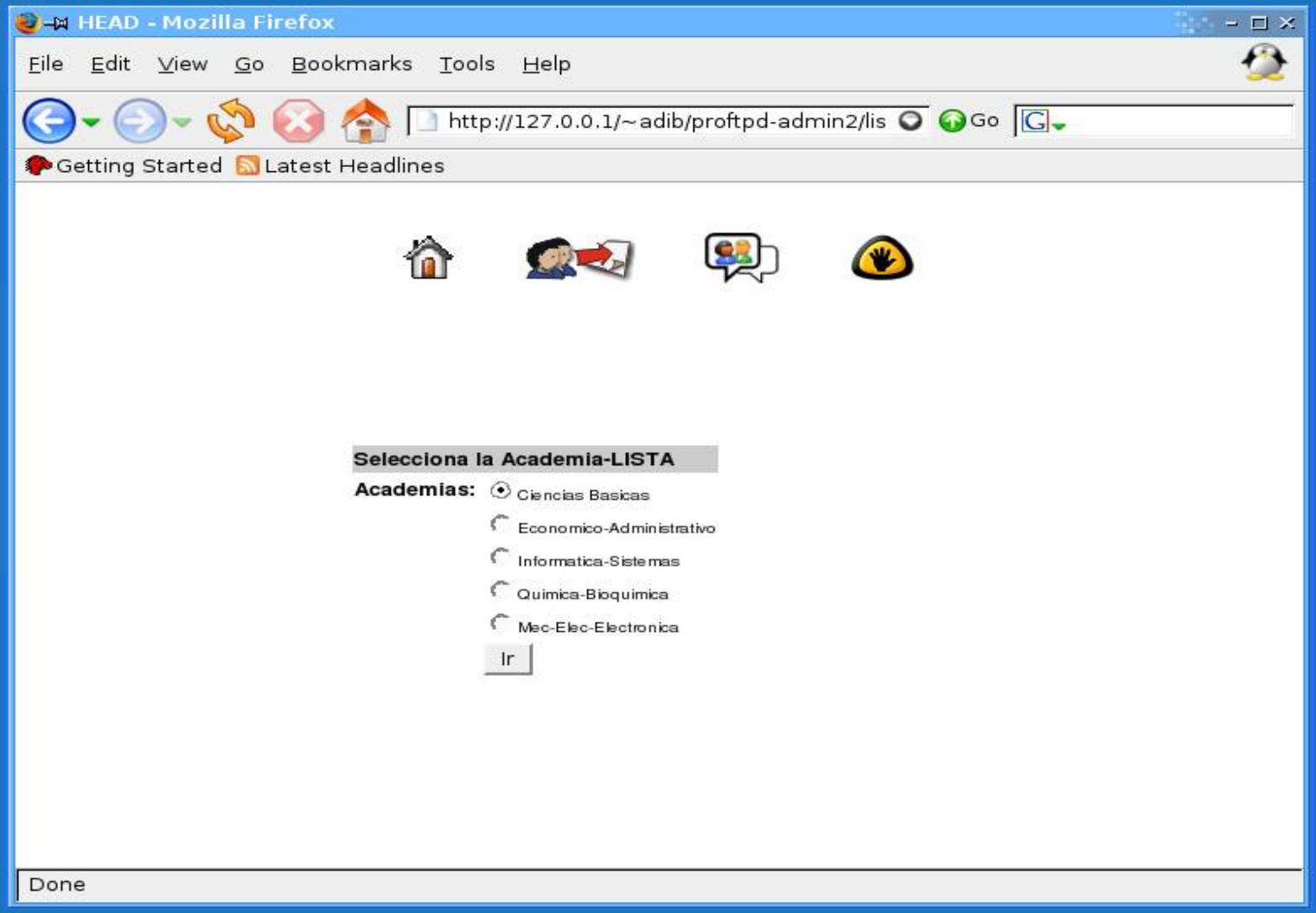
Agregando usuarios 4



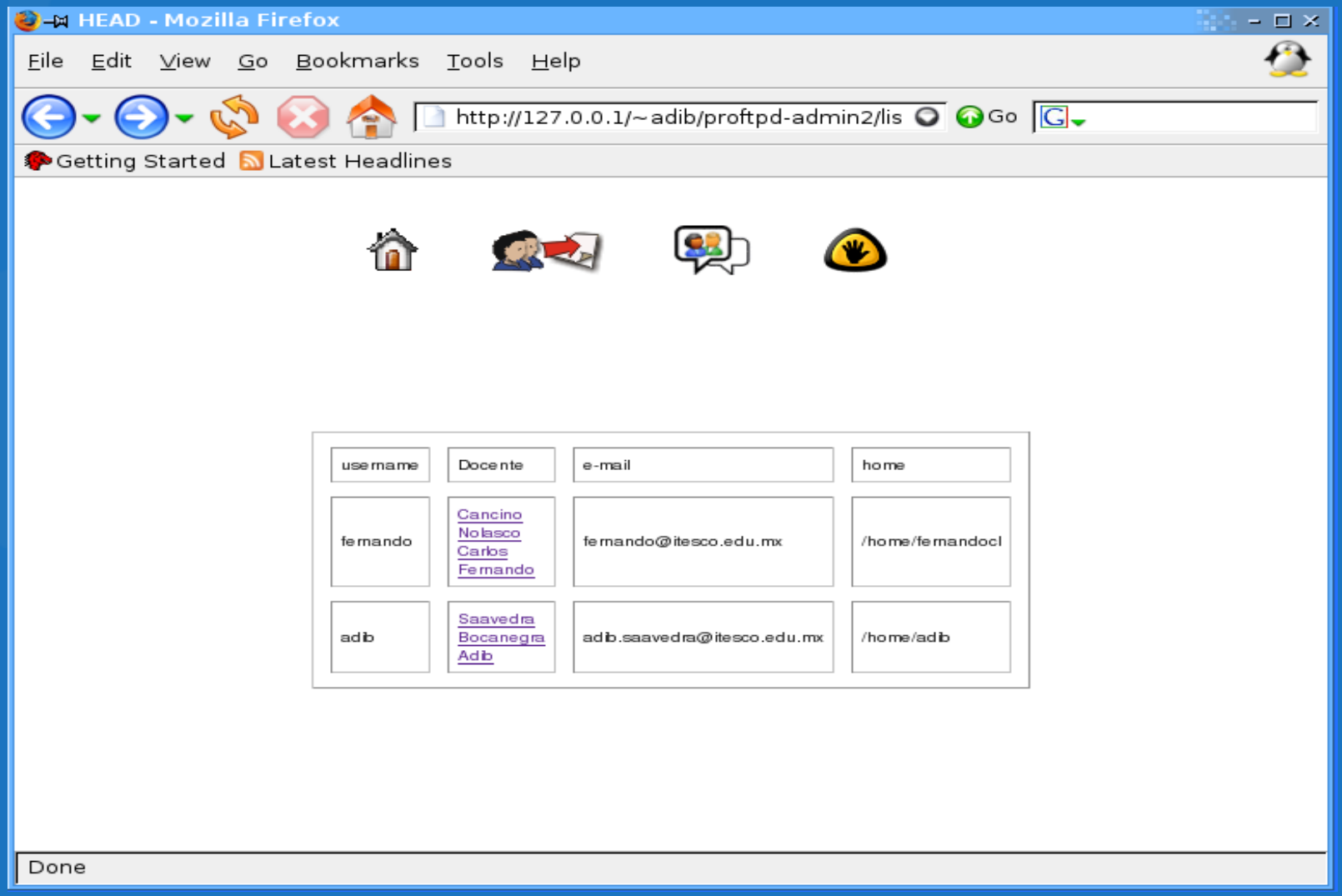
Agregando usuarios 5



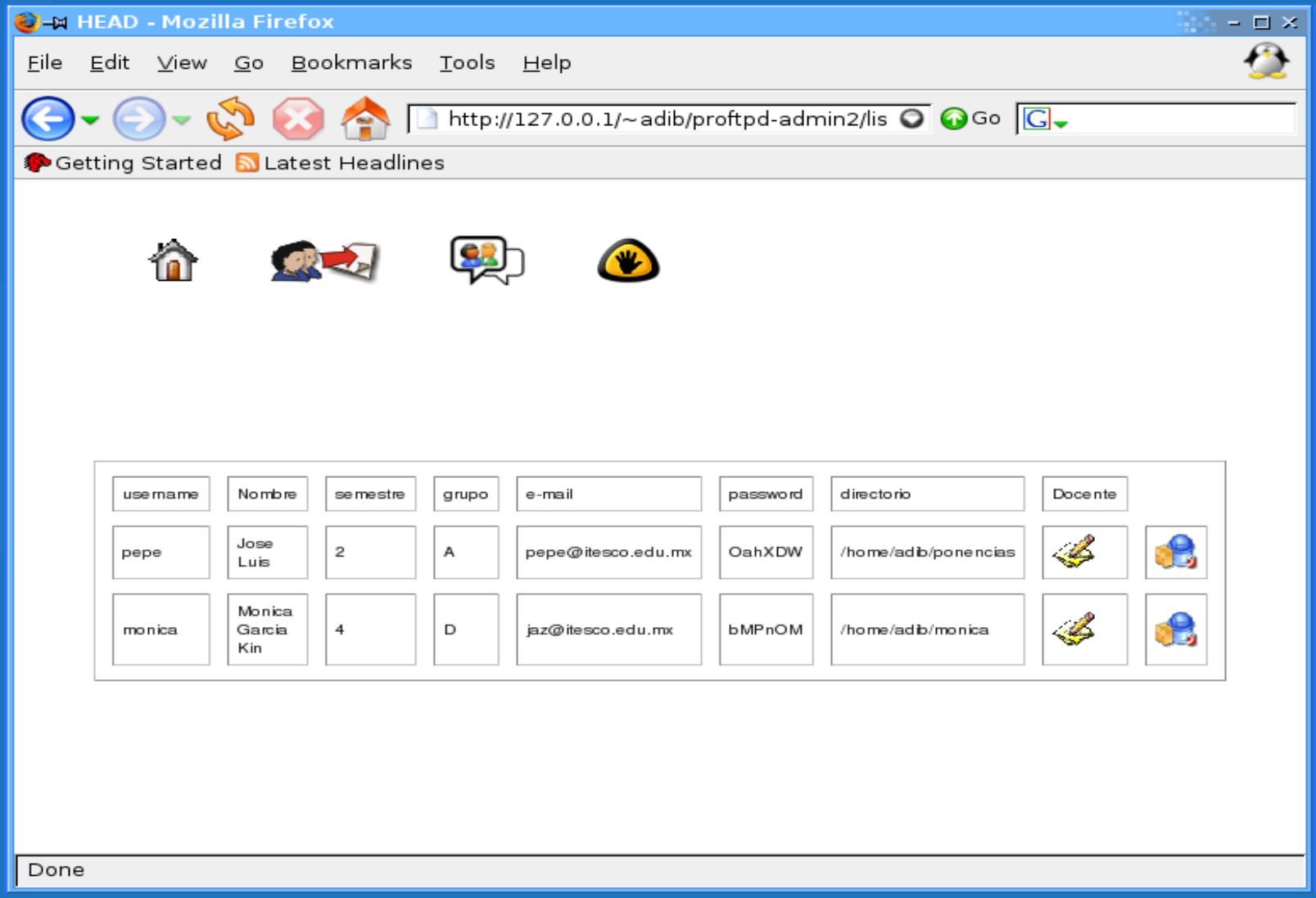
Ver lista de usuarios 2



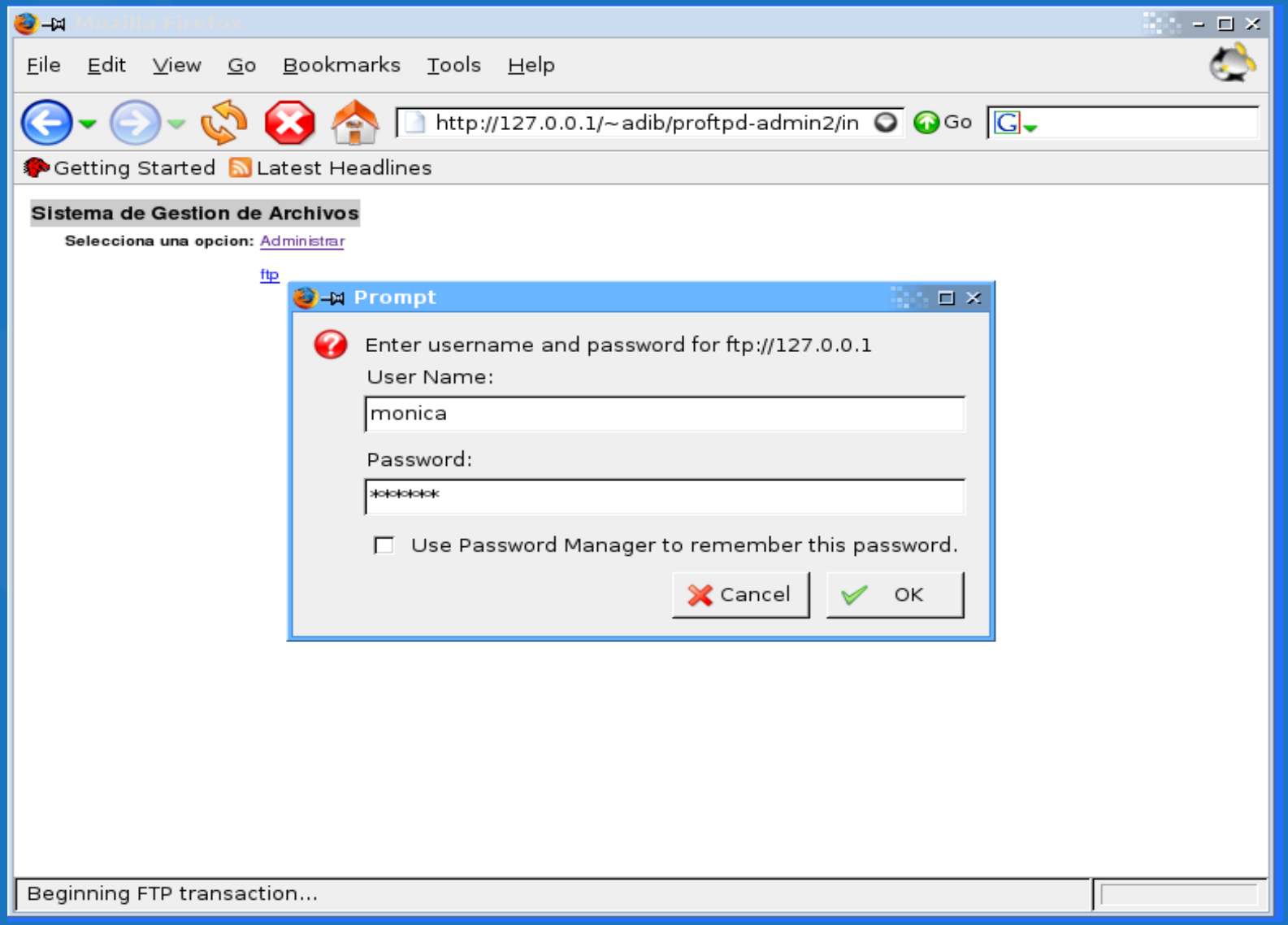
Ver lista de usuarios 3



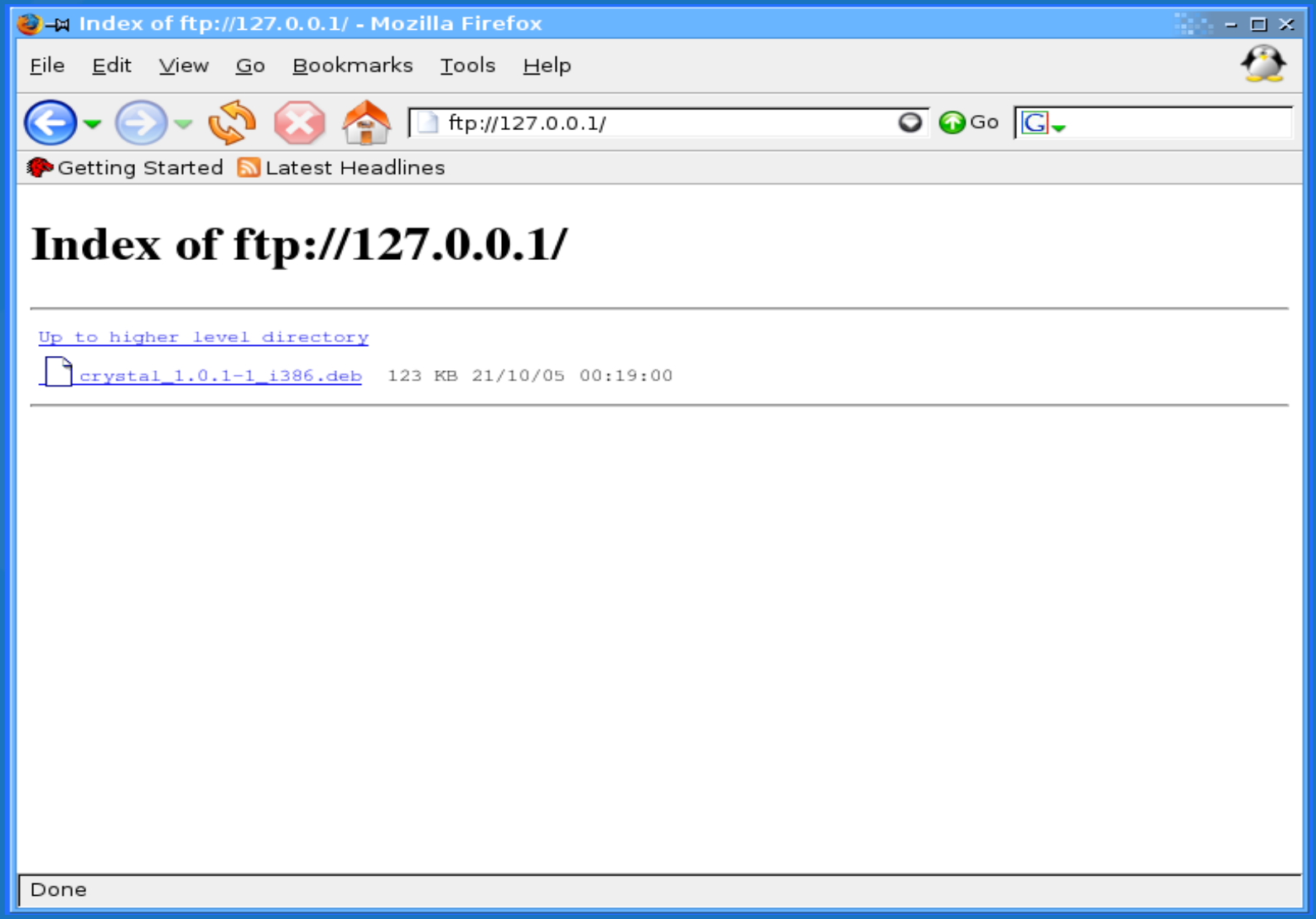
Ver lista de usuarios 4



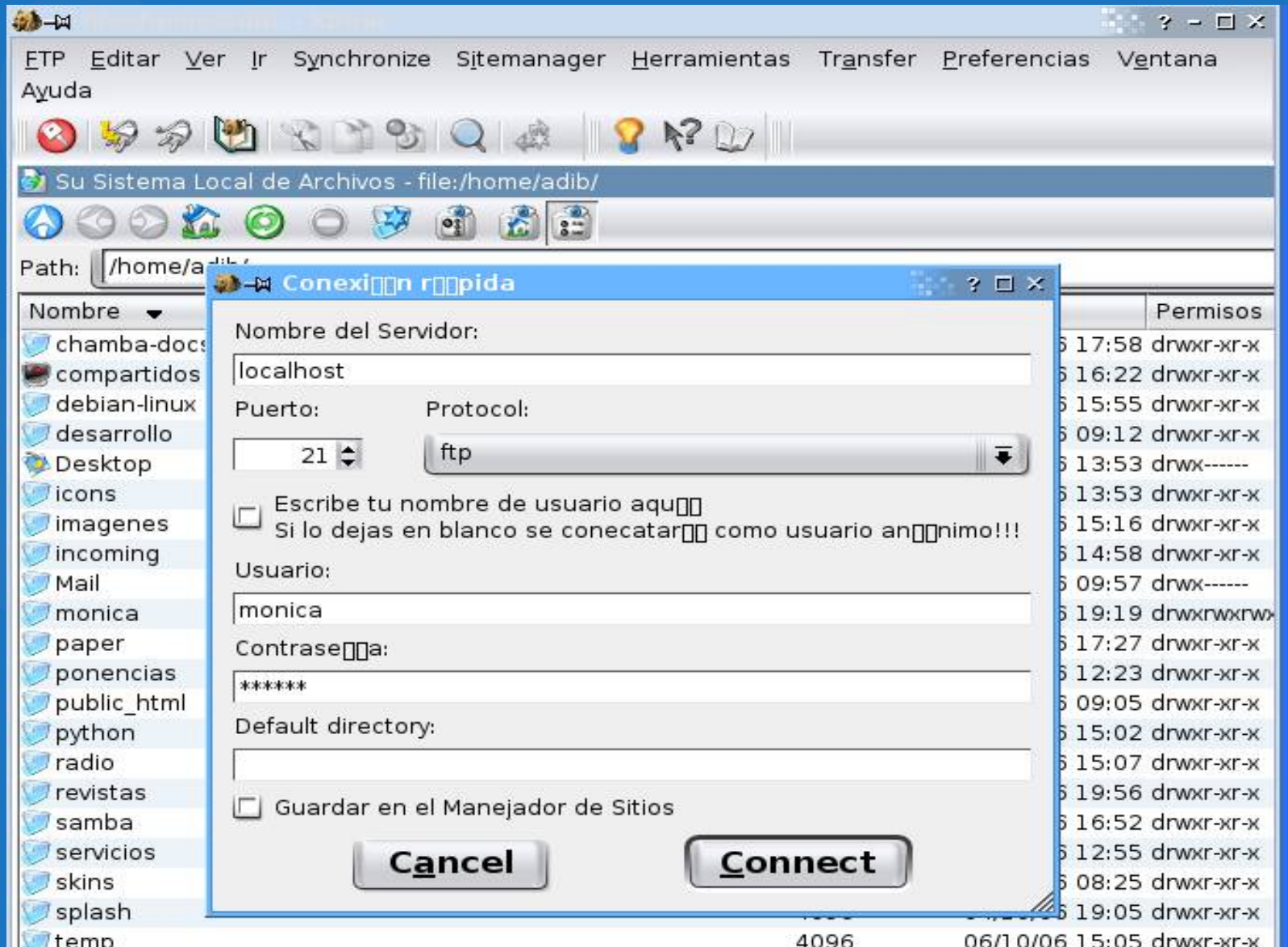
Ingresar al servidor 1



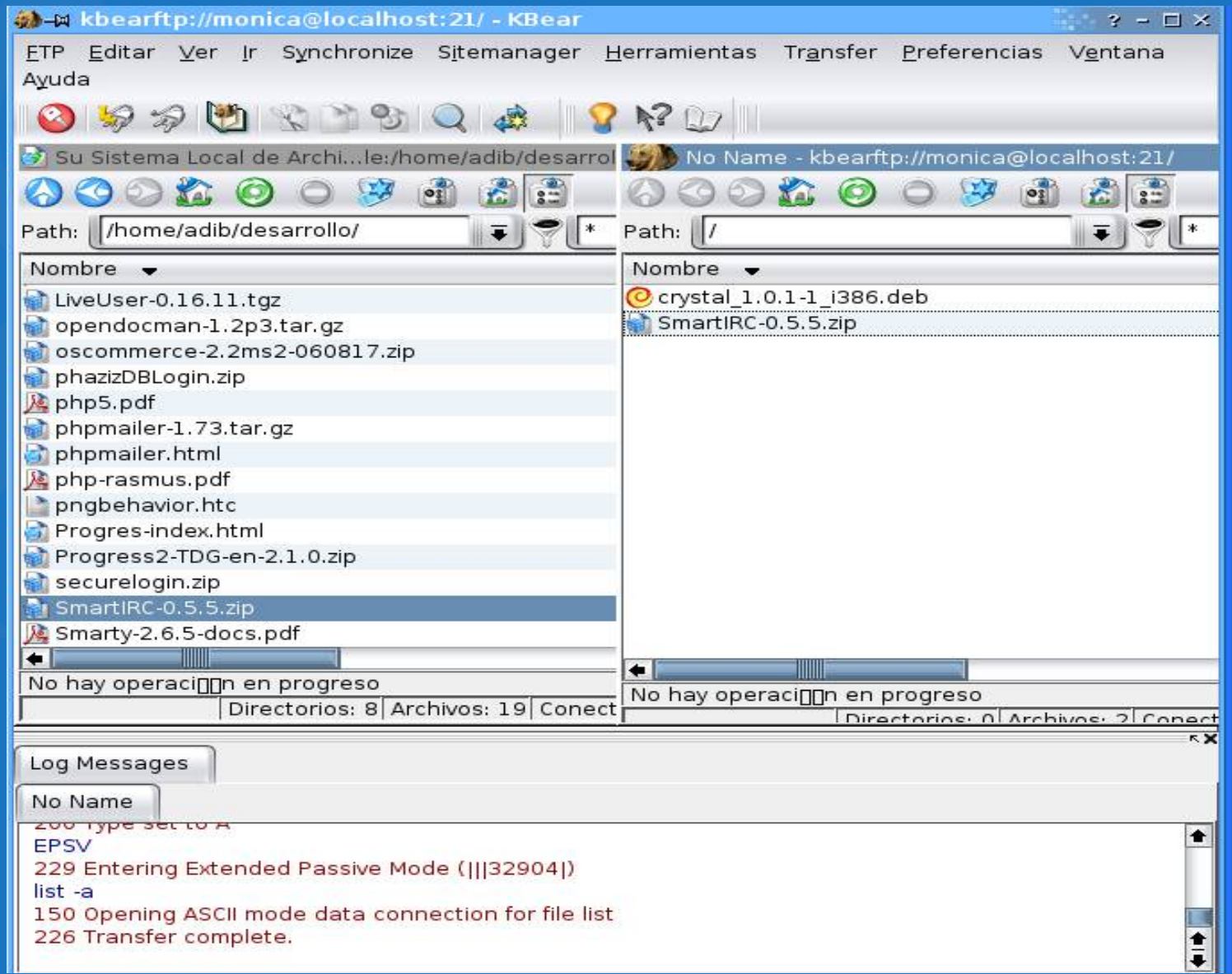
Ingresar al servidor 2



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 administraccion.

Preguntas

,.....