Instituto Politécnico Nacional
Escuela Superior de Cómputo

Administración de Servicios en Red

Profesor:
Soto Ramos Manuel Alejandro

Alumnos:
Dominguez de la Rosa Bryan
Pacheco Díaz Fernando Jair
Vivia Delgadillo Rocío

Grupo:
4CV3

Pruebas del Servidor PROFTPD

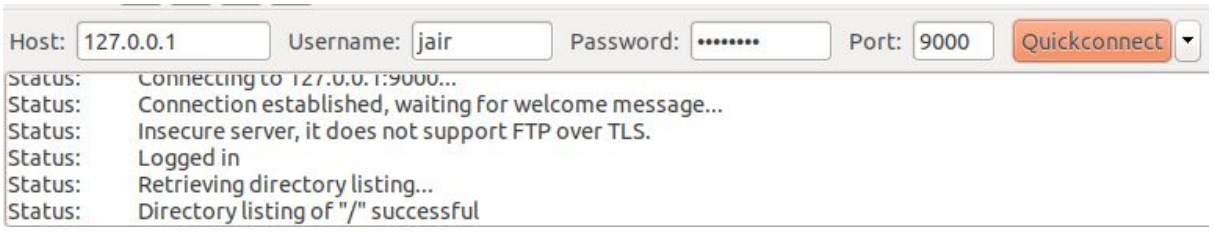
Acceso al recurso

Configuración de puerto

Como se especificó en el manual de instalación y configuración, en el archivo de proftpd.conf se especifica el puerto sobre el cual va a correr el servidor, por lo que vamos a dicha línea y la modificamos, por defecto FTP corre en el puerto 21, al cambiarlo por el puerto 9000, se tiene que especificar que se va a entrar por ese puerto.

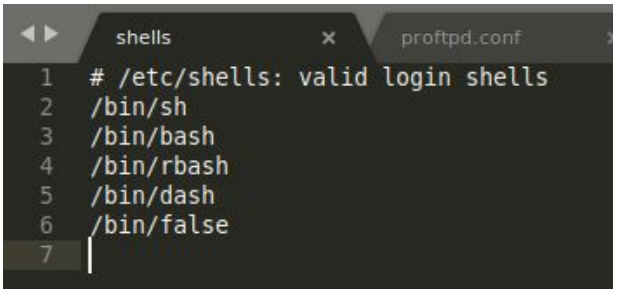
Al reiniciar el servidor y probarlo con un cliente sin especificar el puerto, no conecta con el servidor.

Por lo que se tiene que colocar el puerto correspondiente



Configuración de usuarios y tiempos de conexión

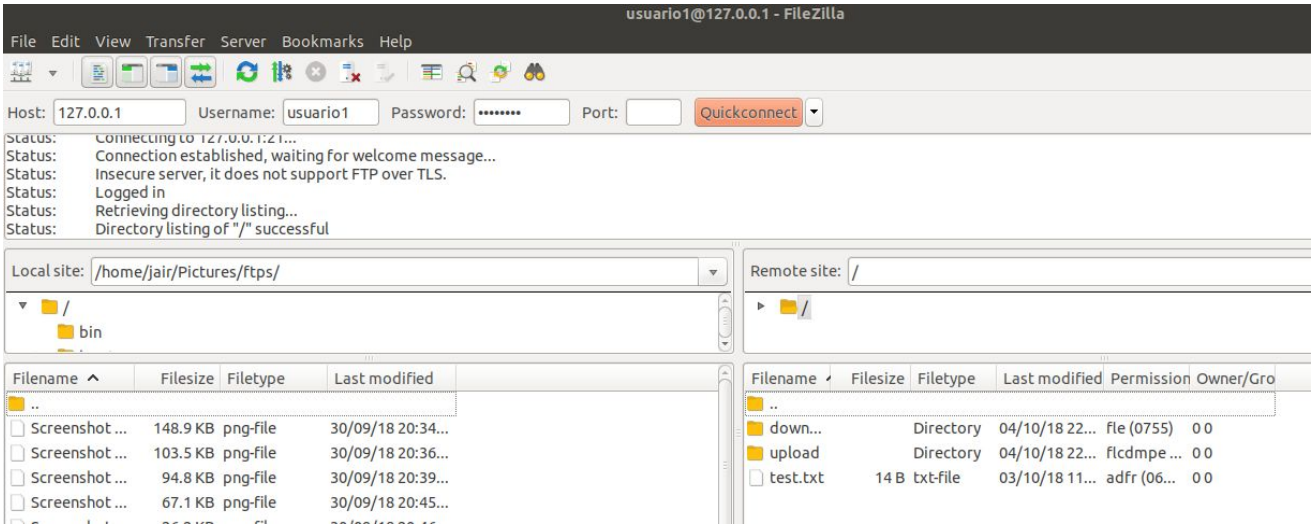
Los usuarios registrados en el servidor son a aquellos a los que se les puede permitir el acceso con sus respectivas contraseñas, para eso, creamos 2 usuarios de pruebas con un shell falso para que no puedan acceder al shell del servidor.



Y creamos las carpetas para subir y bajar archivos, cada una con sus respectivos permisos.

```
jair@lap-jair:/home$ sudo useradd usuario2 -p usuario2 -d /home/public_FTP -s /b
in/false
jair@lap-jair:/home$ sudo mkdir /home/public_FTP/download
jair@lap-jair:/home$ sudo mkdir /home/public_FTP/upload
jair@lap-jair:/home$ sudo chmod 755 /home/public_FTP/
jair@lap-jair:/home$ sudo chmod 755 /home/public_FTP/download/
jair@lap-jair:/home$ sudo chmod 777 /home/public_FTP/upload/
```

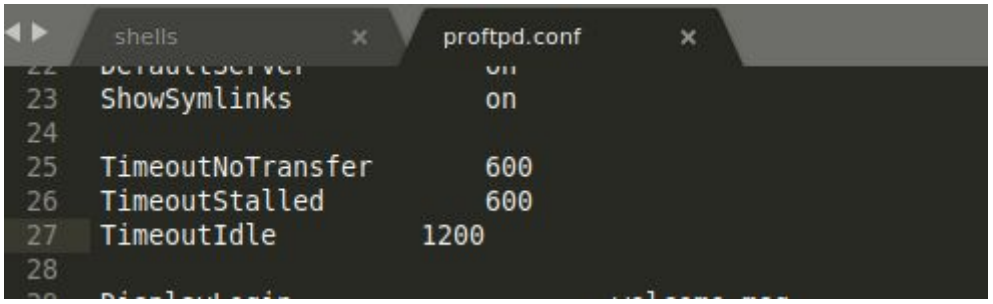
Posteriormente, probamos su funcionalidad utilizando clientes ftp.



Además se puede visualizar los usuarios que están conectados en este momento.

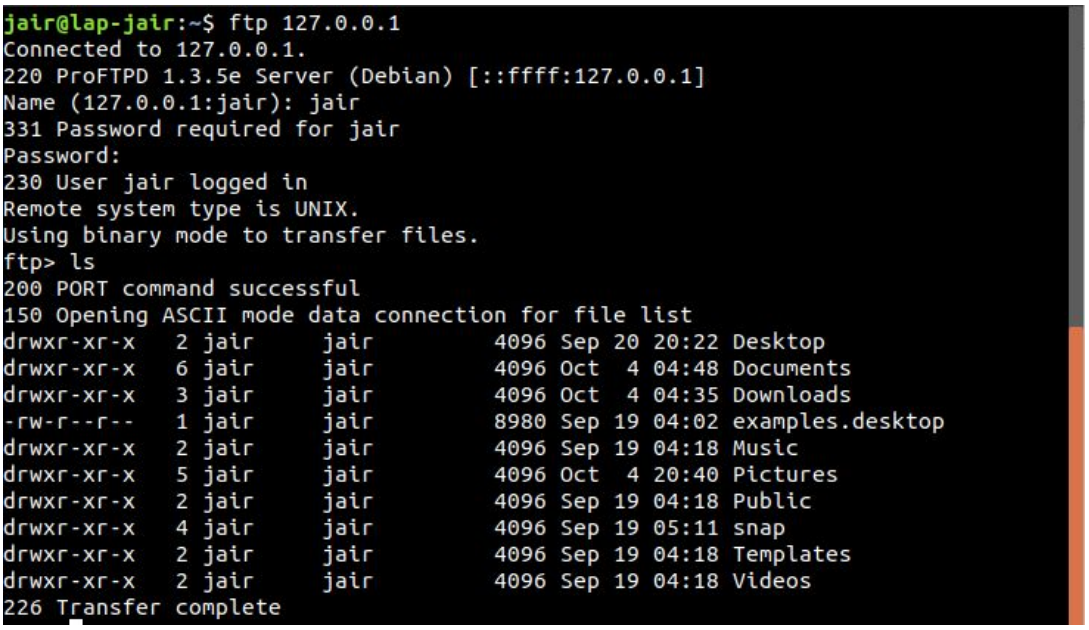
```
jair@lap-jair:/home$ sudo ftpwho
[sudo] password for jair:
standalone FTP daemon [14732], up for 4 min
14920 usuario1 [ 0m52s]  0m26s idle
14925 usuario1 [ 0m15s]  0m15s idle
Service class                   -   2 users
jair@lap-jair:/home$
```

Para modificar el tiempo de conexión, en el mismo archivo de configuración se modifican los valores (En segundos) de los tiempos.



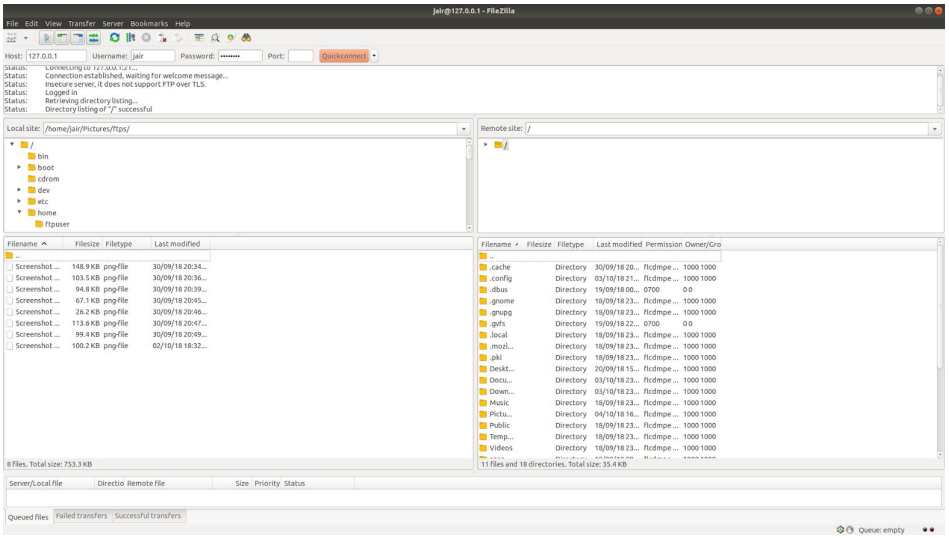
Conexión desde terminal

Utilizando el comando ftp se puede conectar a un servidor ftp, la cual, al ingresar las credenciales adecuadas y logearnos, nos cambiará a una shell de ftp, donde se pueden usar varios comandos muy parecidos a los de linux.



Conexión desde aplicación cliente FTP

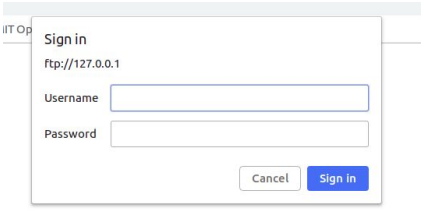
Se utilizó una de las aplicaciones más comunes para utilizar como cliente FTP, Filezilla, el cual facilita el manejo de los archivos tanto locales como del servidor remoto.



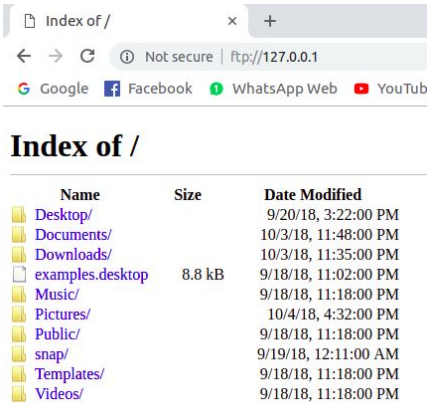
Después de las casillas para ingresar las credenciales y logearse, se encuentra una consola informativa donde da el resultado de cada operación y una interpretación de los mensajes de respuesta del servidor.

Conexión desde navegador

Desde el navegador Google Chrome basta con poner en la barra de direcciones *ftp://dominio.com* para poder acceder al servidor ftp.



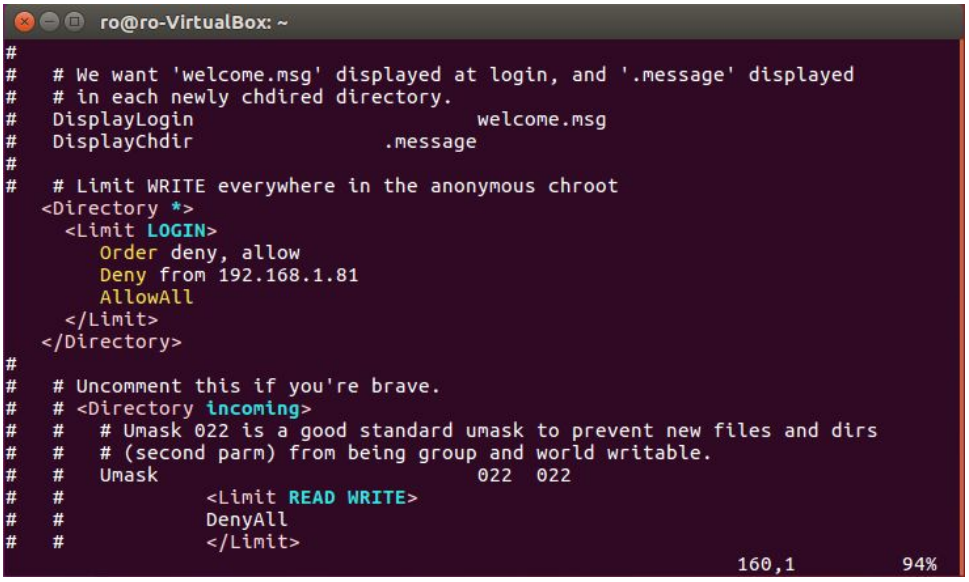
Evidentemente solicitará las credenciales para acceder y posteriormente visualizar los archivos y directorios de la carpeta raíz del usuario.



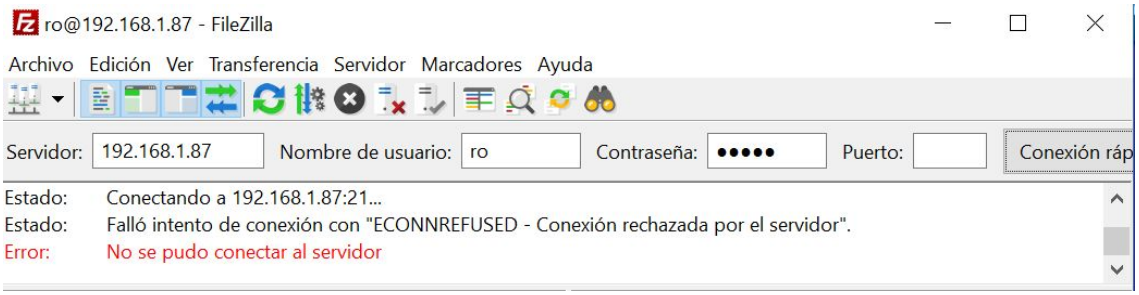
Restricciones

Restringir acceso al recurso por dirección IP del cliente

Si a todos los directorios se les coloca un limit específico de una dirección se puede bloquear el acceso de esta.

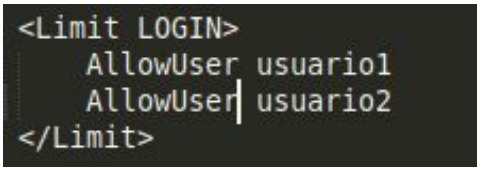


Ya modificado el archivo de configuración se reinicia el servidor y se prueba.

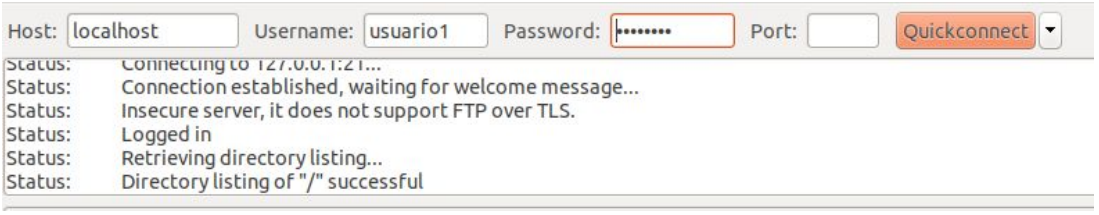


Restringir acceso al recurso por usuario

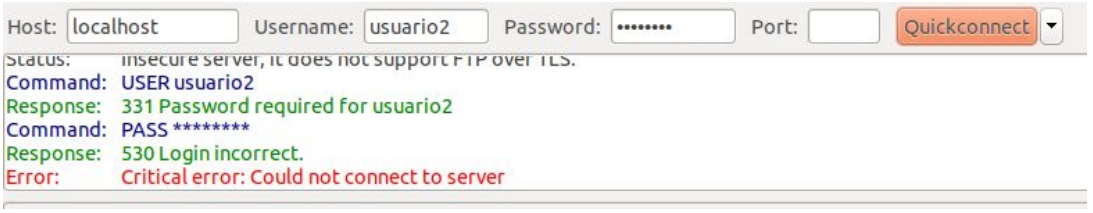
Usando limit, en el LOGIN o en un recurso en específico, negamos la entrada a un usuario en especial.



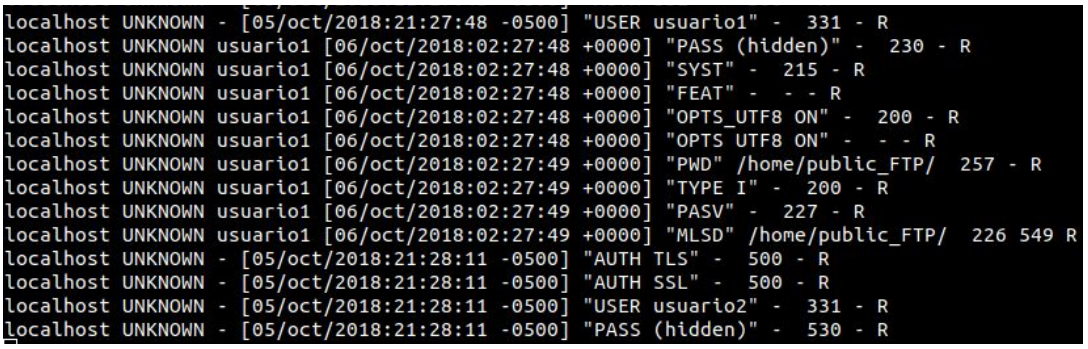
Mientras que el usuario1 si puede acceder



Al usuario2 se le rechaza aún con las credenciales correctas

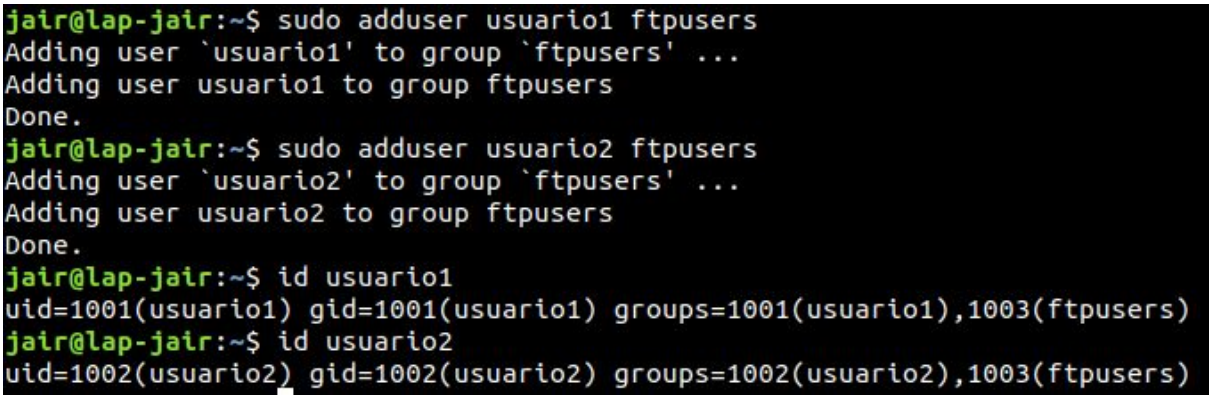


Y el custom log se puede ver que reconoce al usuario pero le impide su autentificación



Restringir acceso al recurso por grupo de usuarios

Creamos un grupo

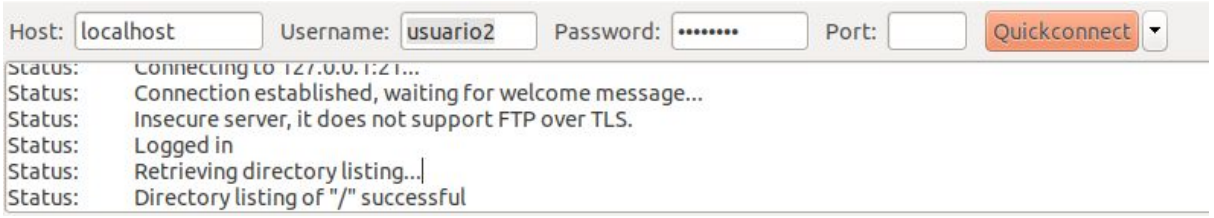


Y verificamos que los usuarios si se hayan agregado al grupo.

En el archivo de configuración se modifican los permisos específicos para el grupo.

```
<Limit LOGIN>
    AllowGroup ftpusers
    DenyAll
</Limit>
```

Y solo pueden entrar los que pertenezcan al grupo como el usuario2



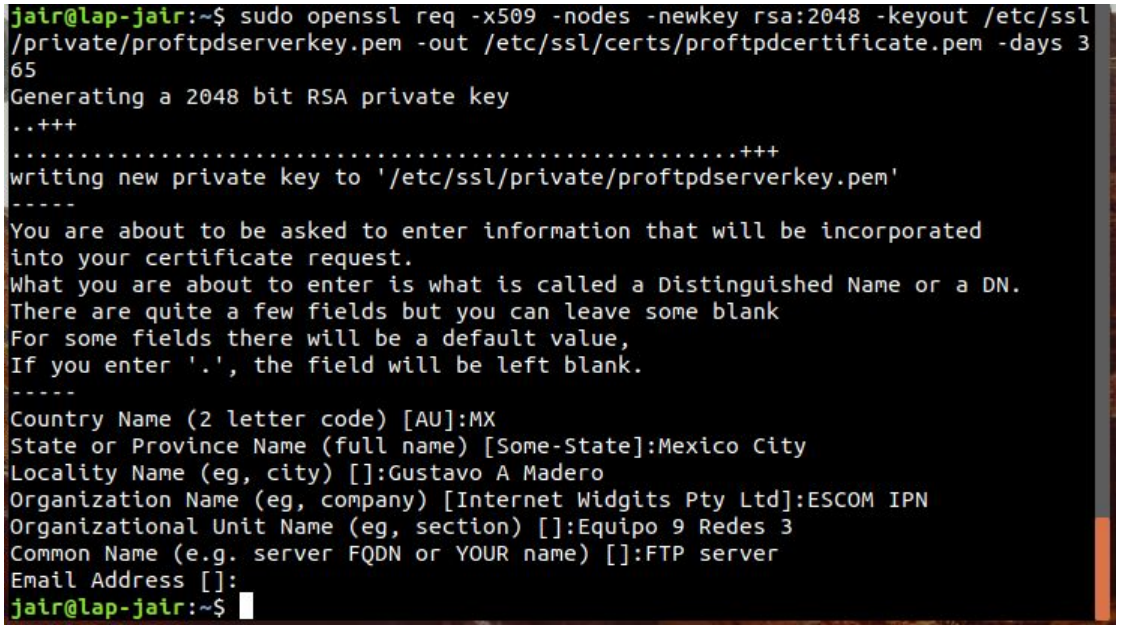
Más no el usuario jair

Protocolo seguro para la transferencia de archivos

Existen 2 maneras, utilizando SSL para FTPS y utilizando SSH para SFTP.

Definición de certificados de operación

Para FTPS utilizamos SSL y básicamente se crea utilizando la herramienta OpenSSL.

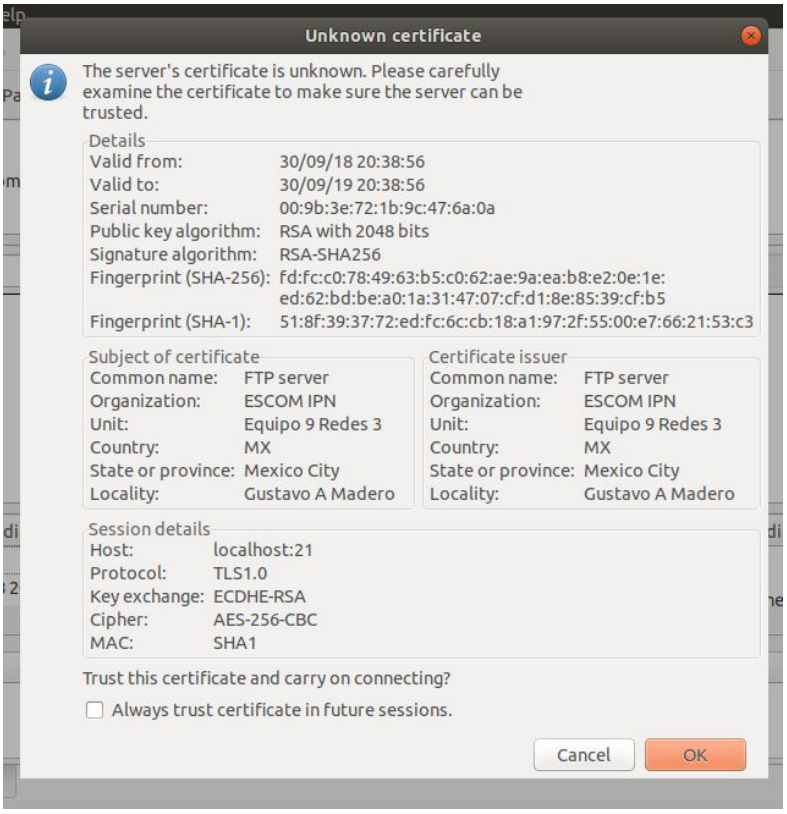


Y para SSH

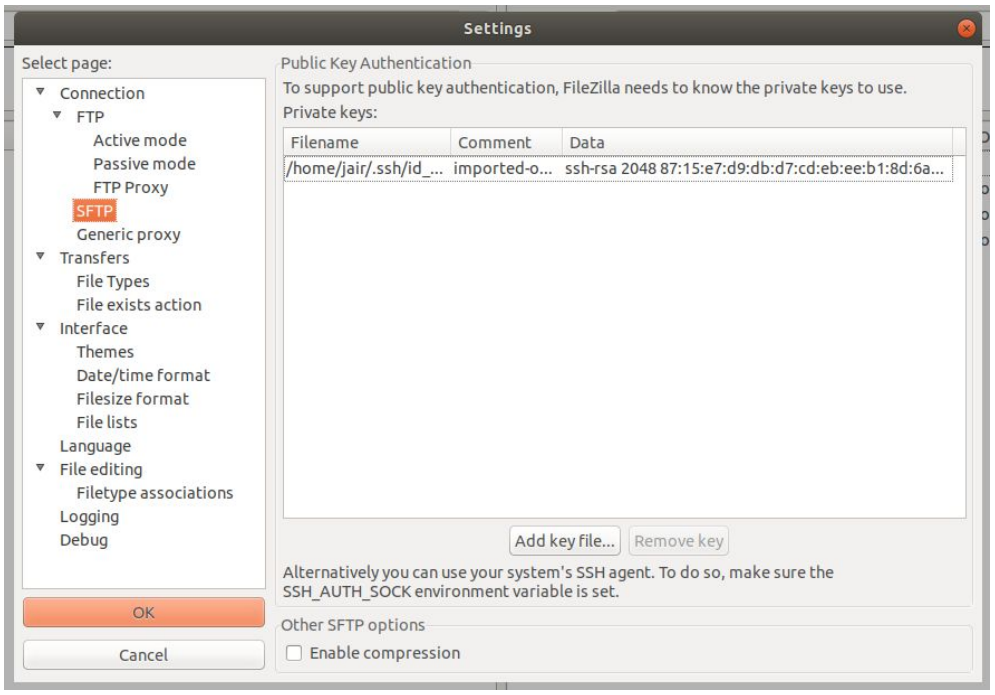
```
jair@lap-jair:~$ cd ~/.ssh/
jair@lap-jair:~/.ssh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/jair/.ssh/id_rsa): id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
The key fingerprint is:
SHA256:SaeVavhvZvoUkkgecxbBL/4aH+pzhNJWB7cwqfmITKE jair@lap-jair
The key's randomart image is:
+---[RSA 2048]----+
|       .o. .     |
|      . ..=..    |
|     .+.+++= .   |
|    Eo.O+Bo o    |
|     o++S*..     |
|      +o*.o.     |
|       oooo      |
|        .**.     |
|       .=X+      |
+----[SHA256]-----+
jair@lap-jair:~/.ssh$ cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
```

Uso de certificados de operación

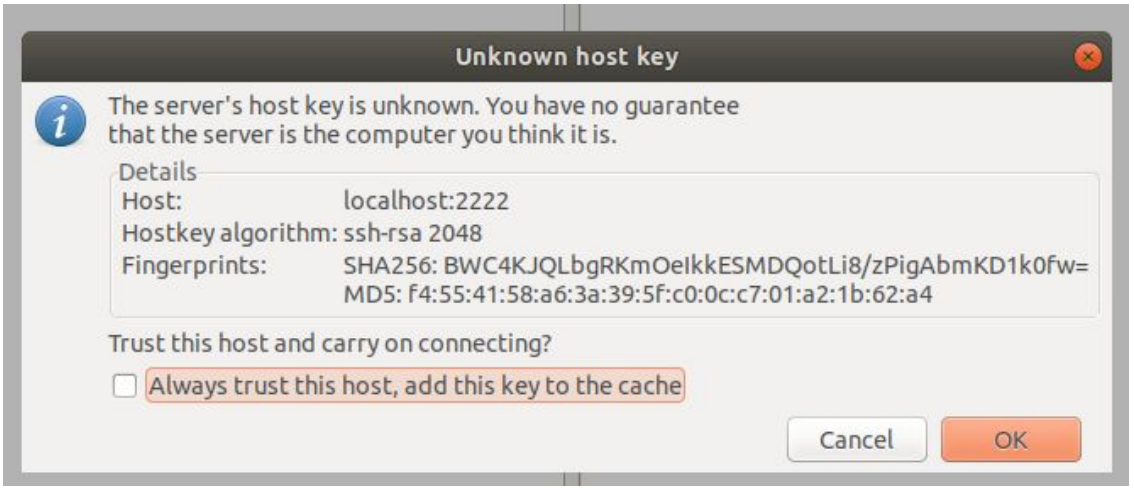
Para FTPS se configura el archivo tls.conf, el cual se ahbilita desde el proftpd como muestra el manual de configuración, al final el cliente Filezilla mostrará la siguiente pantalla:



Para SSH basta con direccionar el cliente con la llave pública del usuario con el queremos acceder, dicha clave ya debe de estar linkeada con la que tiene el servidor por cada usuario.

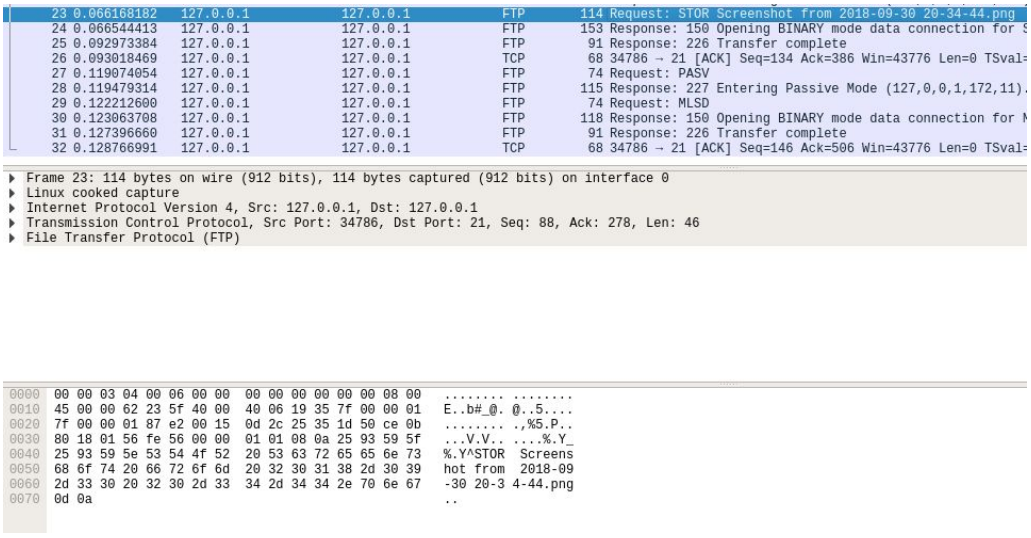


Además de que la primera conexión nos pedirá revisar la llave del servidor remoto.

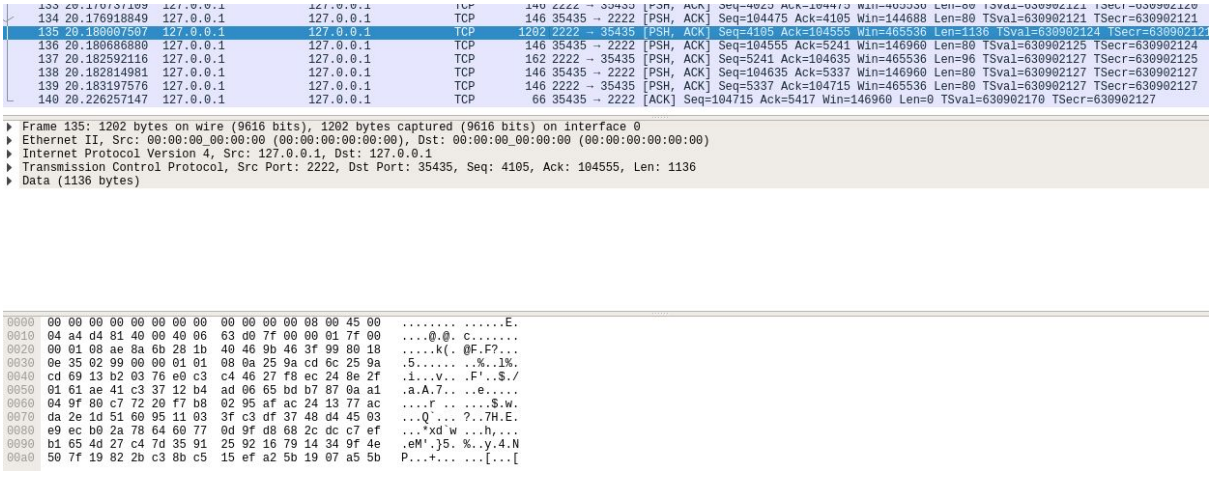


Traza de comunicación cifrada

Podemos utilizar un analizador de paquetes como Wireshark para rastrear la comunicación que hay por el puerto que definimos para el servidor, a continuación una transferencia sin utilizar SFTP.



Donde observamos la información que estamos transfiriendo, siendo vulnerable a espías externos, al utilizar el canal SSH y por lo tanto, cambiando del puerto default 21 al 2222 que usamos pasa SFTP, el resultado es el siguiente.



Donde observamos que los paquetes están cifrados mientras que los archivos llegan a su destino correctamente.

Implementación de jaulas para diferentes usuarios

Para enjaular a los usuarios en distintas carpetas, se utiliza DefaultRoot en el archivo de configuración

```
# Use this to jail all users in their homes
#DefaultRoot            /home/public_FTP
DefaultRoot        ~
```

Mientras la opción comentada mandaría a todos los usuarios a una carpeta especifica, la opción de abajo manda a los usuarios a la carpeta raíz de sus respectivos usuarios.

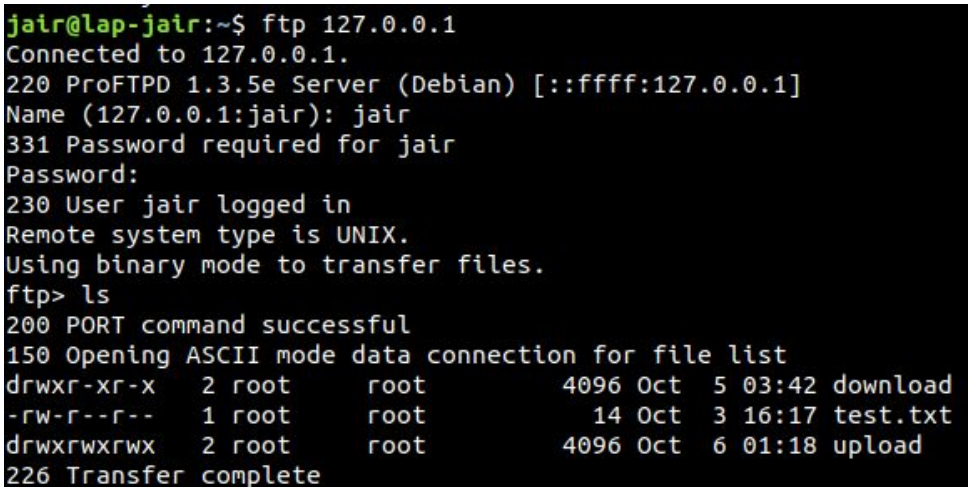
Permisos de usuario 1 en carpeta individual

El usuario jair al logearse verá un home por efecto de ubuntu.

```
jair@lap-jair:~$ ftp 127.0.0.1
Connected to 127.0.0.1.
220 ProFTPD 1.3.5e Server (Debian) [::ffff:127.0.0.1]
Name (127.0.0.1:jair): jair
331 Password required for jair
Password:
230 User jair logged in
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
-rwxrwxrwx   1 root     root        28488 Oct  6 01:13 custom1.log
drwxr-xr-x   2 jair     jair         4096 Sep 20 20:22 Desktop
drwxr-xr-x   6 jair     jair         4096 Oct  4 04:48 Documents
drwxr-xr-x   3 jair     jair         4096 Oct  6 03:00 Downloads
-rw-r--r--   1 jair     jair         8980 Sep 19 04:02 examples.desktop
drwxr-xr-x   2 jair     jair         4096 Sep 19 04:18 Music
drwxr-xr-x   5 jair     jair         4096 Oct  6 03:11 Pictures
drwxr-xr-x   2 jair     jair         4096 Sep 19 04:18 Public
drwxr-xr-x   4 jair     jair         4096 Sep 19 05:11 snap
drwxr-xr-x   2 jair     jair         4096 Sep 19 04:18 Templates
drwxr-xr-x   2 jair     jair         4096 Sep 19 04:18 Videos
226 Transfer complete
ftp>
```

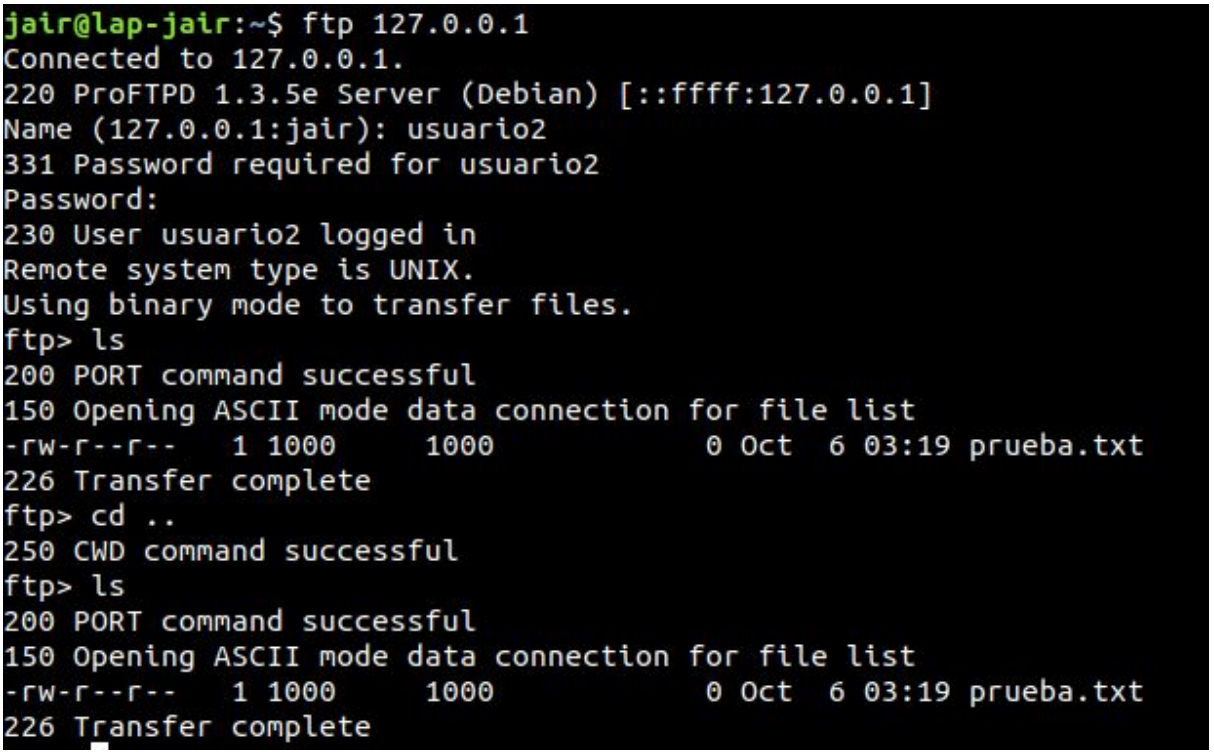
Permisos de usuario 1 en carpeta compartida

Descomentando la ruta de public_FTP y comentando la de home, ahora al logearse el usuario jair obtiene lo siguiente:



Permisos de usuario 2 en carpeta individual

Para el usuario 2 se hizo un home de prueba, para mostrar que se enjaula en ese home definido y no puede subir escalones e este.



Permisos de usuario 2 en carpeta compartida

Si se vuelve a activar la opción de la carpeta compartida. vuelve a la carpeta de public_FTP

```
jair@lap-jair:~$ ftp 127.0.0.1
Connected to 127.0.0.1.
220 ProFTPD 1.3.5e Server (Debian) [::ffff:127.0.0.1]
Name (127.0.0.1:jair): usuario2
331 Password required for usuario2
Password:
230 User usuario2 logged in
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
drwxr-xr-x   2 root     root         4096 Oct  5 03:42 download
-rw-r--r--   1 root     root           14 Oct  3 16:17 test.txt
drwxrwxrwx   2 root     root         4096 Oct  6 01:18 upload
226 Transfer complete
ftp>
```

Y vuelve a estar en la carpeta compartida de public_FTP.

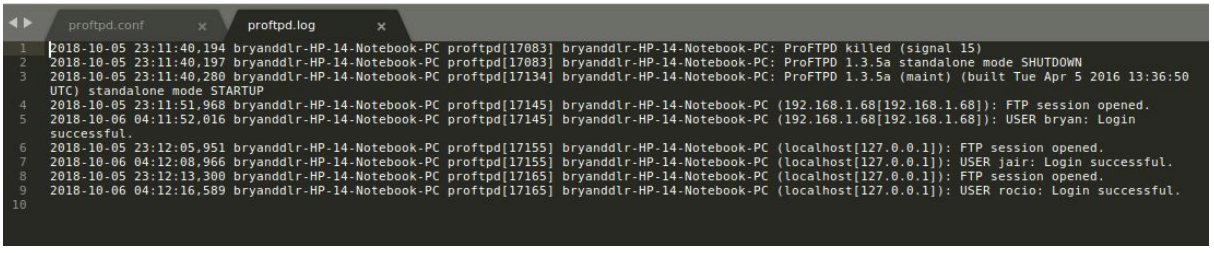
Configuración de los sistemas de registro de acceso al sistema

Diferentes niveles de operación de las bitácoras

BItácoras

Los mensajes que llegan al sistema se clasifican en diferentes niveles de logeo. Por default el servidor guarda todos los niveles, sin embargo mediante la directiva **SyslogLevel** podemos elegir que mensajes queremos resguardar. Los niveles tienen una prioridad, así que dependiendo el nivel que elijamos serán los niveles que se guardarán.

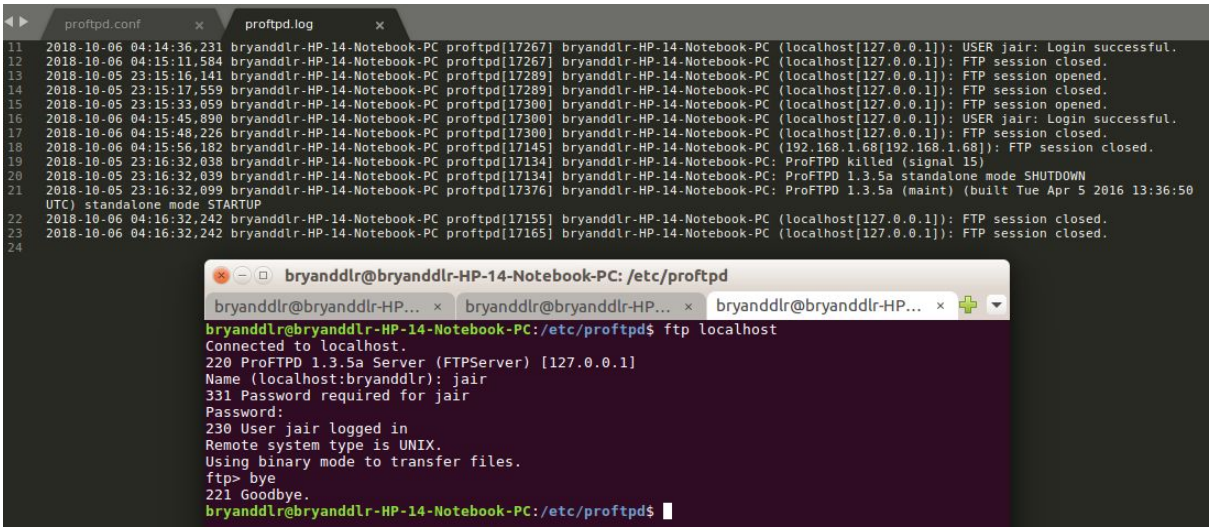
Por ejemplo, el login de usuarios es de nivel INFO, por lo tanto se guarda por default:



Si queremos ignorar los mensajes de nivel INFO, tenemos darle como parámetro a la directiva **SyslogLevel** un nivel mayor a INFO, por ejemplo:

```
LogFormat custom "%a %u %t %m %f %s %b"
TransferLog /var/log/proftpd/xferlog
SystemLog   /var/log/proftpd/proftpd.log
ExtendedLog /var/log/proftpd/custom.log ALL custom
SyslogLevel notice
```

Reiniciando el servidor, e intentando loggear de nuevo, nos damos cuenta de que ya no se registró el login de los usuarios:



Especificación de los parámetros de bitácora solicitados

Parámetros

Se puede personalizar un archivo de bitácora, de tal manera que nosotros seleccionemos los parámetros que deseamos que sean guardados.

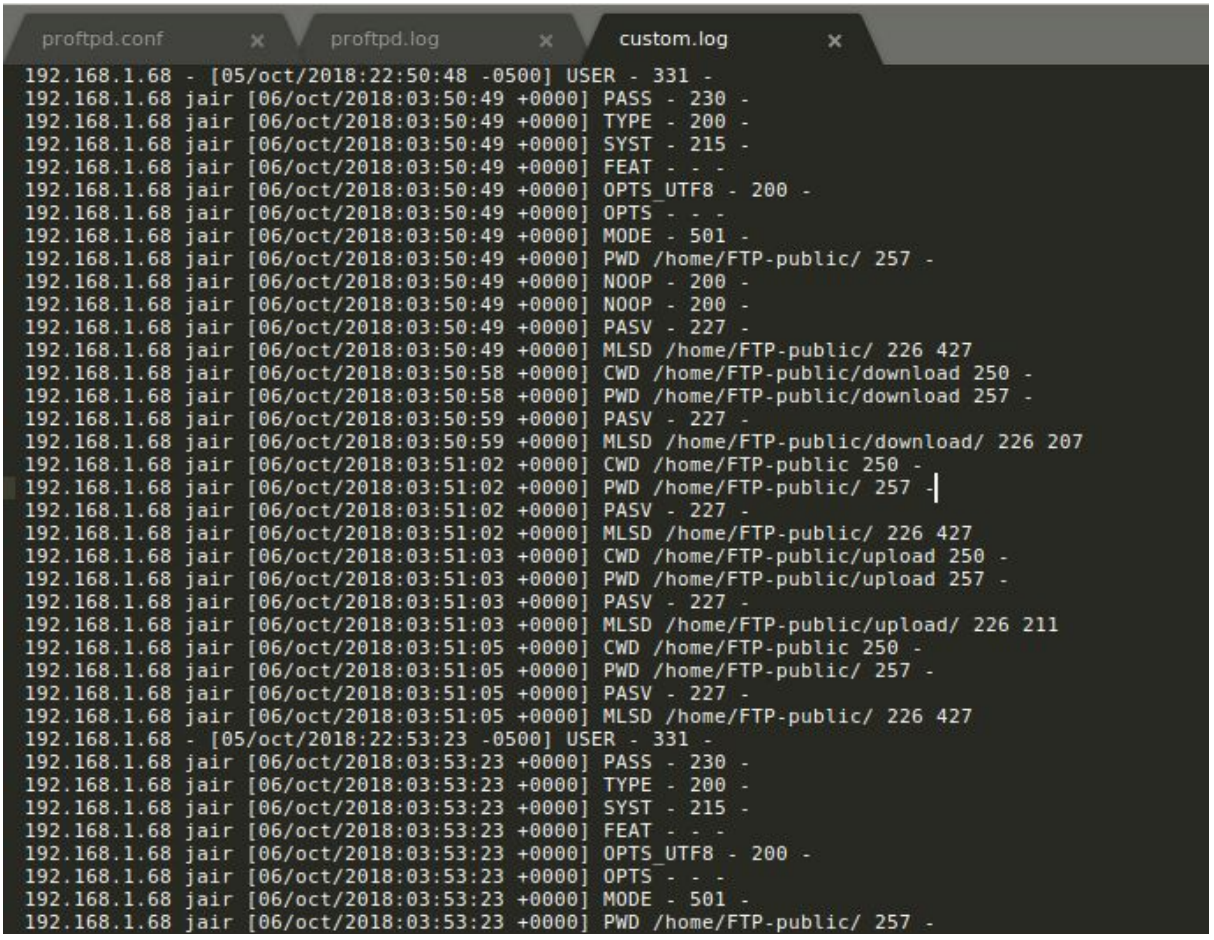
La directiva **LogFormat** permite dar un nombre al formato que estamos creando, y seleccionar los parámetros que deseamos guardar.

La directiva **ExtendedLog** permite crear el archivo en donde guardaremos la bitácora personalizada.

Se realizó una configuración que permitiera crear un archivo de log personalizado, para facilitar el análisis del mismo. Se agregaron las siguientes directivas al archivo proftpd.conf:

```
LogFormat custom "%a %u %t %m %f %s %b"
TransferLog /var/log/proftpd/xferlog
SystemLog   /var/log/proftpd/proftpd.log
ExtendedLog /var/log/proftpd/custom.log ALL custom
```

Y la bitácora generada es la siguiente:



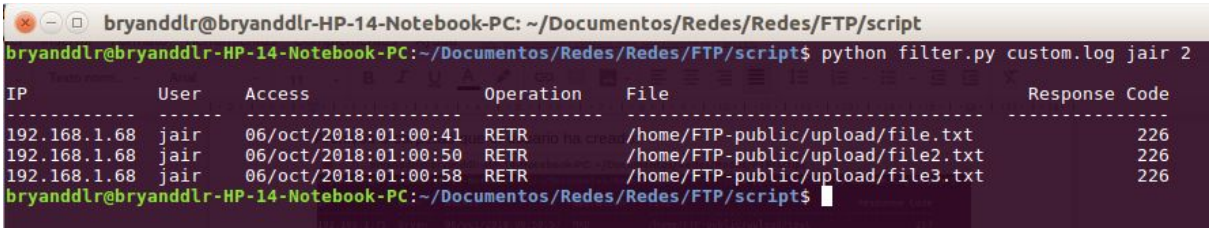
Resumen de operación del servidor

Resumen de usuarios

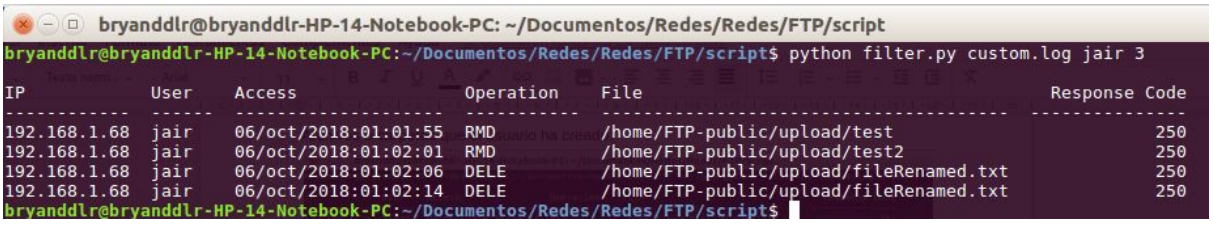
Se implementó un analizador que filtra el archivo de logs por usuario y por operación realizada.

Archivos o carpetas que el usuario ha creado:

Archivos que el usuario ha descargado:



Archivos o carpetas que el usuario ha borrado:



Archivos o carpetas que el usuario ha renombrado: