



**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:**

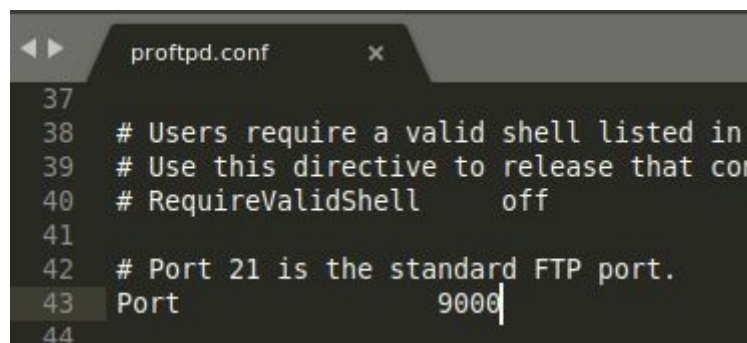
**4CV3**

**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.

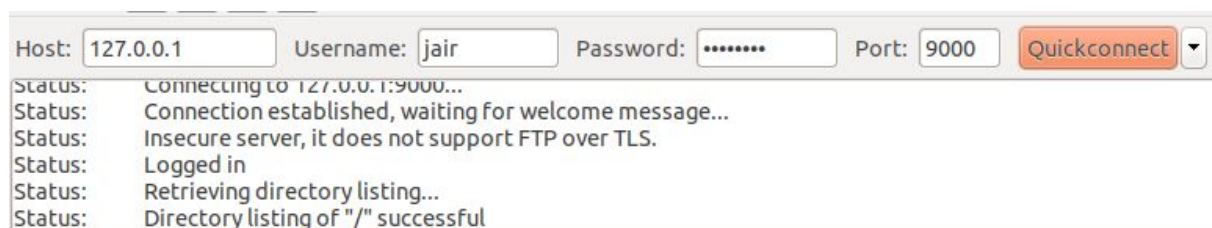


```
37
38 # Users require a valid shell listed in
39 # Use this directive to release that con
40 # RequireValidShell    off
41
42 # Port 21 is the standard FTP port.
43 Port                    9000
44
```

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

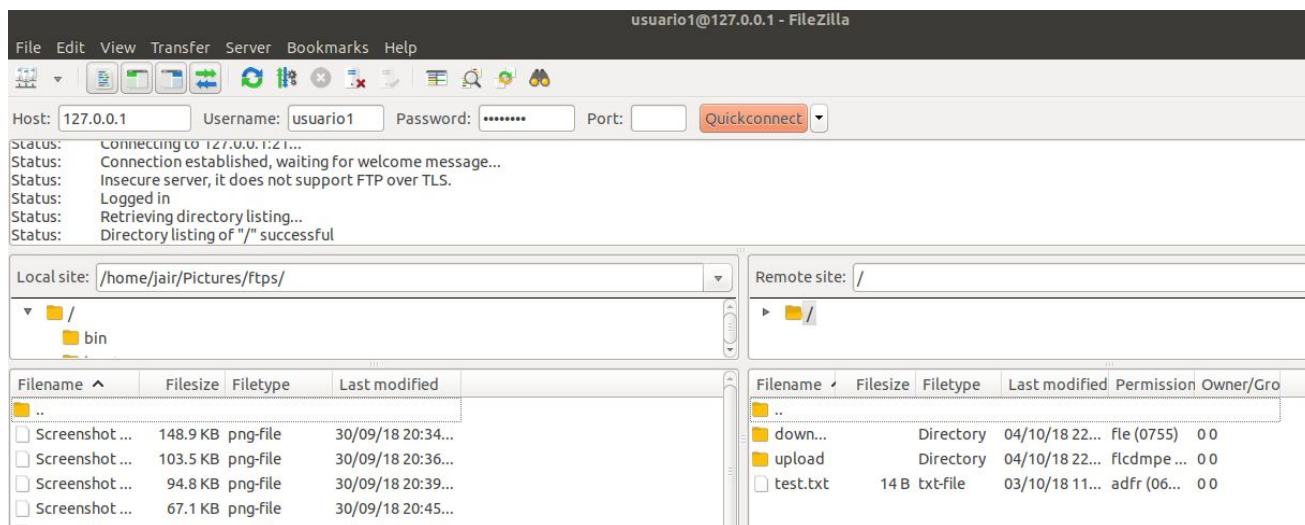
Los usuarios registrados en el servidor son a aquellos a los que se les puede permitir el acceso con sus respectivas contraseñas, para eso, creamos 2 usuarios de pruebas con un shell falso para que no puedan acceder al shell del servidor.

```
shells  x  proftpd.conf
1 # /etc/shells: valid login shells
2 /bin/sh
3 /bin/bash
4 /bin/rbash
5 /bin/dash
6 /bin/false
7
```

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 /bin/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/
```

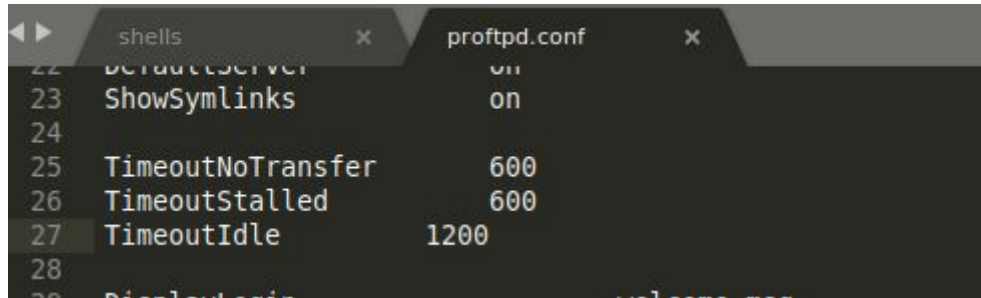
Posteriormente, probamos su funcionalidad utilizando clientes ftp.



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.



```
22 DefaultServer on
23 ShowSymlinks on
24
25 TimeoutNoTransfer 600
26 TimeoutStalled 600
27 TimeoutIdle 1200
28
29 DisallowLocal
```

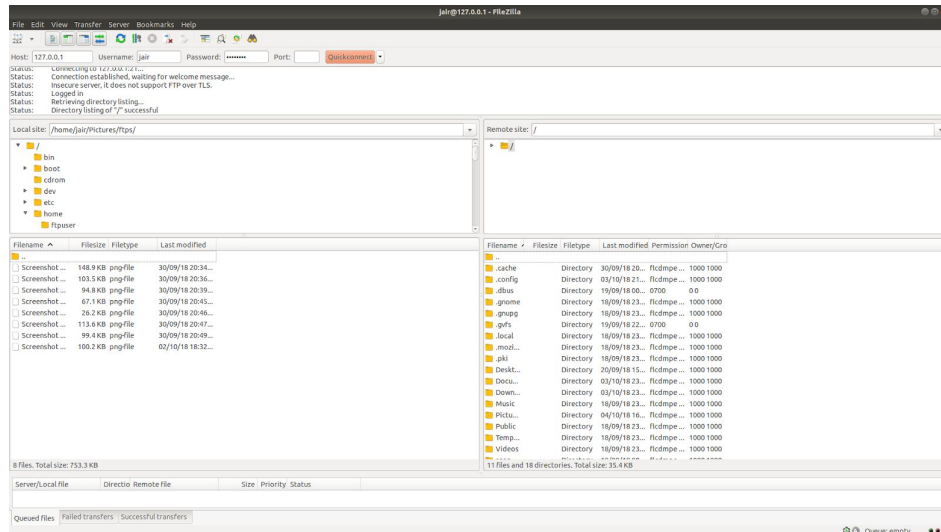
## Conexión desde terminal

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.

```
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
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  4 04:35 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  4 20:40 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
```

## Conexión desde aplicación cliente FTP

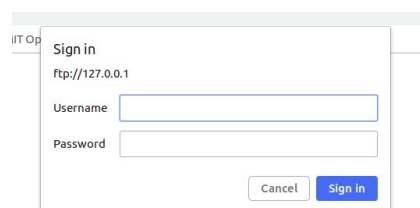
Se utilizó una de las aplicaciones más comunes para utilizar como cliente FTP, Filezilla, el cual facilita el manejo de los archivos tanto locales como del servidor remoto.



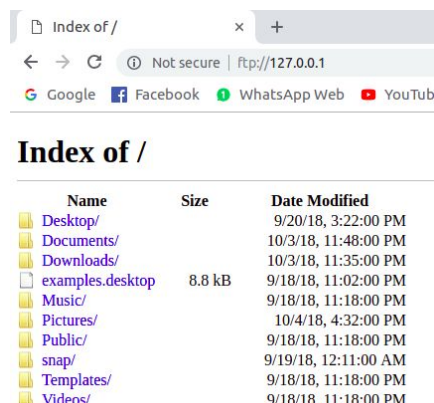
Después de las casillas para ingresar las credenciales y logearse, se encuentra una consola informativa donde da el resultado de cada operación y una interpretación de los mensajes de respuesta del servidor.

## 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.





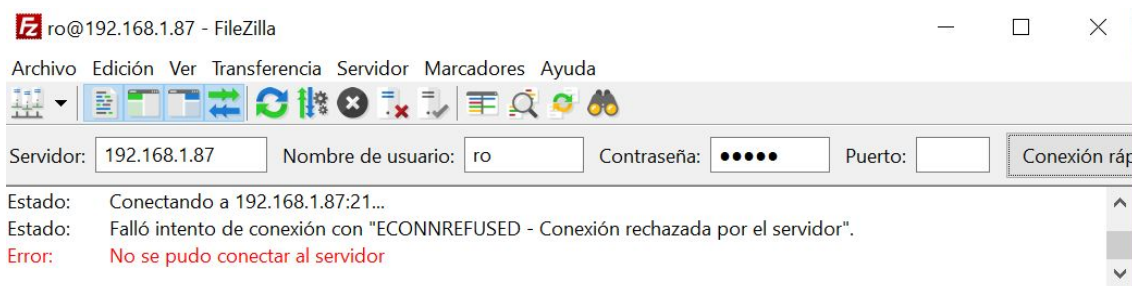
# Restricciones

## 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.

```
ro@ro-VirtualBox: ~  
#  
# # We want 'welcome.msg' displayed at login, and '.message' displayed  
# # in each newly chdir'd directory.  
# DisplayLogin                welcome.msg  
# DisplayChdir                .message  
#  
# # Limit WRITE everywhere in the anonymous chroot  
<Directory *>  
  <Limit LOGIN>  
    Order deny, allow  
    Deny from 192.168.1.81  
    AllowAll  
  </Limit>  
</Directory>  
#  
# # Uncomment this if you're brave.  
# # <Directory incoming>  
# #   # Umask 022 is a good standard umask to prevent new files and dirs  
# #   # (second parm) from being group and world writable.  
# #   Umask                                022 022  
# #  
# #   <Limit READ WRITE>  
# #   DenyAll  
# #   </Limit>
```

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.

```
<Limit LOGIN>  
  AllowUser usuario1  
  AllowUser usuario2  
</Limit>
```

Mientras que el usuario1 si puede acceder

Host:	localhost	Username:	usuario1	Password:	*****	Port:		Quickconnect	▼
Status:	Connecting to 127.0.0.1:21...								
Status:	Connection established, waiting for welcome message...								
Status:	Insecure server, it does not support FTP over TLS.								
Status:	Logged in								
Status:	Retrieving directory listing...								
Status:	Directory listing of "/" successful								

Al usuario2 se le rechaza aún con las credenciales correctas

Host:	localhost	Username:	usuario2	Password:	*****	Port:		Quickconnect	▼
Status:	Insecure server, it does not support FTP over TLS.								
Command:	USER usuario2								
Response:	331 Password required for usuario2								
Command:	PASS *****								
Response:	530 Login incorrect.								
Error:	Critical error: Could not connect to server								

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

```
localhost UNKNOWN - [05/oct/2018:21:27:48 -0500] "USER usuario1" - 331 - R
localhost UNKNOWN usuario1 [06/oct/2018:02:27:48 +0000] "PASS (hidden)" - 230 - R
localhost UNKNOWN usuario1 [06/oct/2018:02:27:48 +0000] "SYST" - 215 - R
localhost UNKNOWN usuario1 [06/oct/2018:02:27:48 +0000] "FEAT" - - - R
localhost UNKNOWN usuario1 [06/oct/2018:02:27:48 +0000] "OPTS UTF8 ON" - 200 - R
localhost UNKNOWN usuario1 [06/oct/2018:02:27:48 +0000] "OPTS UTF8 ON" - - - R
localhost UNKNOWN usuario1 [06/oct/2018:02:27:49 +0000] "PWD" /home/public_FTP/ 257 - R
localhost UNKNOWN usuario1 [06/oct/2018:02:27:49 +0000] "TYPE I" - 200 - R
localhost UNKNOWN usuario1 [06/oct/2018:02:27:49 +0000] "PASV" - 227 - R
localhost UNKNOWN usuario1 [06/oct/2018:02:27:49 +0000] "MLSD" /home/public_FTP/ 226 549 R
localhost UNKNOWN - [05/oct/2018:21:28:11 -0500] "AUTH TLS" - 500 - R
localhost UNKNOWN - [05/oct/2018:21:28:11 -0500] "AUTH SSL" - 500 - R
localhost UNKNOWN - [05/oct/2018:21:28:11 -0500] "USER usuario2" - 331 - R
localhost UNKNOWN - [05/oct/2018:21:28:11 -0500] "PASS (hidden)" - 530 - R
```

## Restringir acceso al recurso por grupo de usuarios

Creamos un grupo

```
jair@lap-jair:~$ sudo adduser usuario1 ftpusers
Adding user `usuario1' to group `ftpusers' ...
Adding user usuario1 to group ftpusers
Done.
jair@lap-jair:~$ sudo adduser usuario2 ftpusers
Adding user `usuario2' to group `ftpusers' ...
Adding user usuario2 to group ftpusers
Done.
jair@lap-jair:~$ id usuario1
uid=1001(usuario1) gid=1001(usuario1) groups=1001(usuario1),1003(ftpusers)
jair@lap-jair:~$ id usuario2
uid=1002(usuario2) gid=1002(usuario2) groups=1002(usuario2),1003(ftpusers)
```

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

Host: localhost Username: usuario2 Password: ..... Port: Quickconnect

Status: Connecting to 127.0.0.1:21...  
Status: Connection established, waiting for welcome message...  
Status: Insecure server, it does not support FTP over TLS.  
Status: Logged in  
Status: Retrieving directory listing...  
Status: Directory listing of "/" successful

Más no el usuario jair

Host: localhost Username: jair Password: ..... Port: Quickconnect

Status: insecure server, it does not support FTP over TLS.  
Command: USER jair  
Response: 331 Password required for jair  
Command: PASS \*\*\*\*\*  
Response: 530 Login incorrect.  
Error: Critical error: Could not connect to server

## 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.

```
jair@lap-jair:~$ sudo openssl req -x509 -nodes -newkey rsa:2048 -keyout /etc/ssl/private/proftpdserverkey.pem -out /etc/ssl/certs/proftpdcertificate.pem -days 365
Generating a 2048 bit RSA private key
...+++
.....+++
writing new private key to '/etc/ssl/private/proftpdserverkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:MX
State or Province Name (full name) [Some-State]:Mexico City
Locality Name (eg, city) []:Gustavo A Madero
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ESCOM IPN
Organizational Unit Name (eg, section) []:Equipo 9 Redes 3
Common Name (e.g. server FQDN or YOUR name) []:FTP server
Email Address []:
jair@lap-jair:~$
```

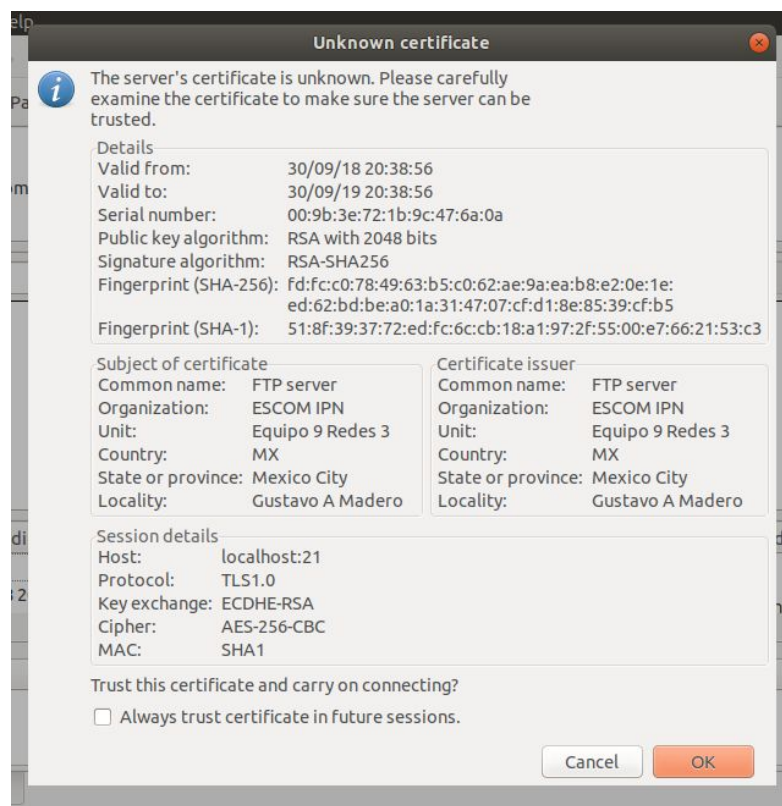


Y para SSH

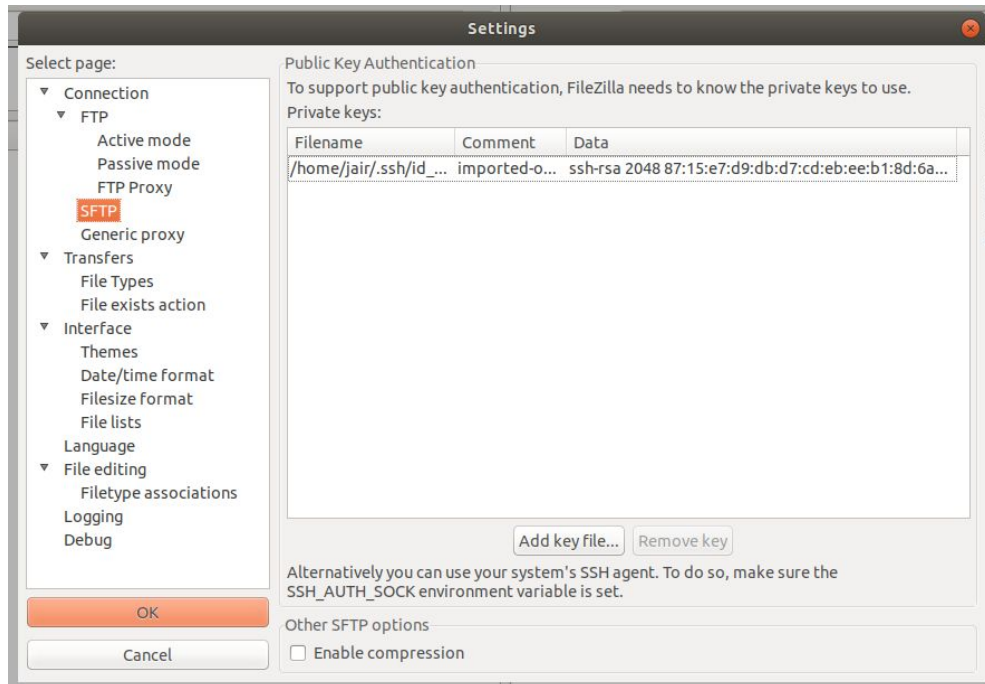
```
jair@lap-jair:~$ cd ~/.ssh/
jair@lap-jair:~/.ssh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/jair/.ssh/id_rsa): id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
The key fingerprint is:
SHA256:SaeVavhvZvoUkkgecxBL/4aH+pzhNJB7cwqfmITKE 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

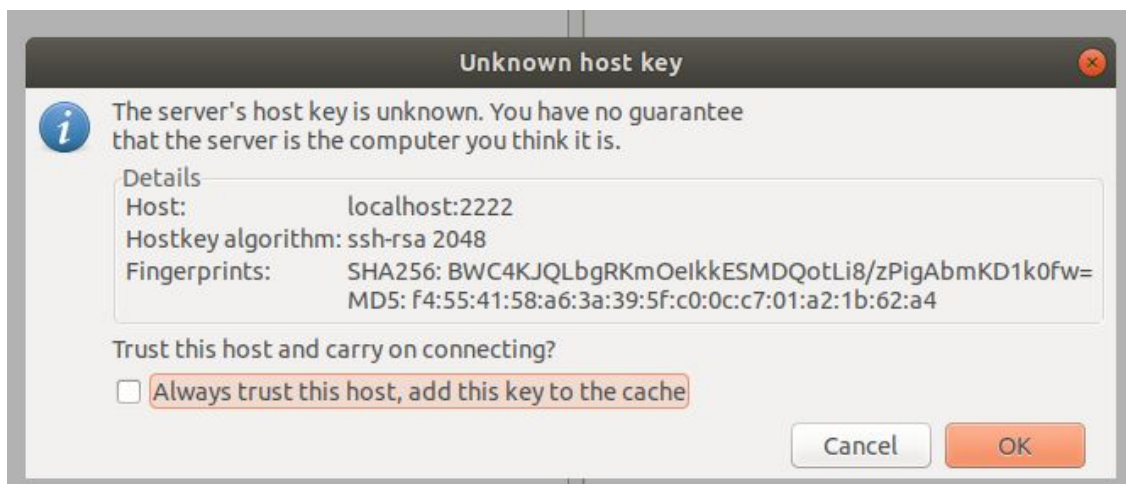
Para FTPS se configura el archivo `tls.conf`, el cual se habilita desde el `proftpd` como muestra el manual de configuración, al final el cliente Filezilla mostrará la siguiente pantalla:



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.

23	0.066168182	127.0.0.1	127.0.0.1	FTP	114 Request: STOR Screenshot from 2018-09-30 20-34-44.png
24	0.066544413	127.0.0.1	127.0.0.1	FTP	153 Response: 150 Opening BINARY mode data connection for S
25	0.092973384	127.0.0.1	127.0.0.1	FTP	91 Response: 226 Transfer complete
26	0.093018469	127.0.0.1	127.0.0.1	TCP	68 34786 -> 21 [ACK] Seq=134 Ack=386 Win=43776 Len=0 TSval=
27	0.119074054	127.0.0.1	127.0.0.1	FTP	74 Request: PASV
28	0.119479314	127.0.0.1	127.0.0.1	FTP	115 Response: 227 Entering Passive Mode (127,0,0,1,172,11)
29	0.122212600	127.0.0.1	127.0.0.1	FTP	74 Request: MLSD
30	0.123063708	127.0.0.1	127.0.0.1	FTP	118 Response: 150 Opening BINARY mode data connection for M
31	0.127396660	127.0.0.1	127.0.0.1	FTP	91 Response: 226 Transfer complete
32	0.128766991	127.0.0.1	127.0.0.1	TCP	68 34786 -> 21 [ACK] Seq=146 Ack=506 Win=43776 Len=0 TSval=

▶ Frame 23: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0

▶ Linux cooked capture

▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

▶ Transmission Control Protocol, Src Port: 34786, Dst Port: 21, Seq: 88, Ack: 278, Len: 46

▶ File Transfer Protocol (FTP)

0000	00 00 03 04 00 06 00 00	00 00 00 00 00 00 00 00	.....
0010	45 00 00 62 23 5f 40 00	40 06 19 35 7f 00 00 01	E..b#_@.0.5....
0020	7f 00 00 01 87 e2 00 15	0d 2c 25 35 1d 50 ce 0b	.....,%,P..
0030	80 18 01 56 fe 56 00 00	01 01 08 0a 25 93 59 5f	...V.V...%Y.
0040	25 93 59 5e 53 54 4f 52	20 53 63 72 65 65 6e 73	%Y^STOR Screens
0050	68 6f 74 20 66 72 6f 6d	20 32 30 31 38 2d 30 39	hot from 2018-09
0060	2d 33 30 20 32 30 2d 33	34 2d 34 34 2e 70 6e 67	-30 20-3 4-44.png
0070	0d 0a		..

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 para SFTP, el resultado es el siguiente.

133	20.176018049	127.0.0.1	127.0.0.1	TCP	146 2222 -> 35435 [PSH, ACK] Seq=104475 Ack=4105 Win=144680 Len=80 TSval=630902121 TSecr=630902127
134	20.176018049	127.0.0.1	127.0.0.1	TCP	146 2222 -> 35435 [PSH, ACK] Seq=104475 Ack=4105 Win=144680 Len=80 TSval=630902121 TSecr=630902127
135	20.182592116	127.0.0.1	127.0.0.1	TCP	146 2222 -> 35435 [PSH, ACK] Seq=104475 Ack=4105 Win=144680 Len=80 TSval=630902121 TSecr=630902127
136	20.182592116	127.0.0.1	127.0.0.1	TCP	146 2222 -> 35435 [PSH, ACK] Seq=104475 Ack=4105 Win=144680 Len=80 TSval=630902121 TSecr=630902127
137	20.182592116	127.0.0.1	127.0.0.1	TCP	146 2222 -> 35435 [PSH, ACK] Seq=104475 Ack=4105 Win=144680 Len=80 TSval=630902121 TSecr=630902127
138	20.182592116	127.0.0.1	127.0.0.1	TCP	146 2222 -> 35435 [PSH, ACK] Seq=104475 Ack=4105 Win=144680 Len=80 TSval=630902121 TSecr=630902127
139	20.183197576	127.0.0.1	127.0.0.1	TCP	146 2222 -> 35435 [PSH, ACK] Seq=104475 Ack=4105 Win=144680 Len=80 TSval=630902121 TSecr=630902127
140	20.226257147	127.0.0.1	127.0.0.1	TCP	66 35435 -> 2222 [ACK] Seq=104715 Ack=5417 Win=146960 Len=0 TSval=630902170 TSecr=630902127

▶ Frame 135: 1202 bytes on wire (9616 bits), 1202 bytes captured (9616 bits) on interface 0

▶ Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)

▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

▶ Transmission Control Protocol, Src Port: 2222, Dst Port: 35435, Seq: 4105, Ack: 104555, Len: 1136

▶ Data (1136 bytes)

0000	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....E.
0010	04 a4 d4 81 40 00 00 06	63 d0 7f 00 00 01 7f 00	...@.0. c.....
0020	00 01 08 ae 8a 6b 28 1b	40 46 9b 46 3f 99 00 18	....k(.0F.F?...
0030	0e 35 02 99 00 00 01 01	08 0a 25 9a cd 6c 25 9a	.S.....%.1%.
0040	cd 69 13 b2 03 76 e0 c3	c4 46 27 f8 ec 24 8e 2f	.i...v...F'.S./
0050	01 01 ae 41 c3 37 12 b4	ad 06 65 bd b7 87 0a a1	.a.A.7...e.....
0060	04 9f 00 c7 72 20 7f b0	02 95 af ac 24 13 77 ac	....f...S.w.
0070	da 2e 1d 51 60 95 11 03	3f c3 df 37 48 d4 45 03	...Q...?..7H.E.
0080	e9 ec b0 2a 78 64 60 77	0d 9f d8 68 2c dc c7 ef	...x'd'w...h,...
0090	b1 65 4d 27 c4 7d 35 91	25 92 16 79 14 34 9f 4e	.eM'.)5.%.y.4.N
00a0	50 7f 19 82 2b c3 8b c5	15 ef a2 5b 19 07 a5 5b	P...+... ...[...]

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 específica, 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:



```
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
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
```

## 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.

```
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
-rw-r--r--  1 1000    1000      0 Oct  6 03:19 prueba.txt
226 Transfer complete
ftp> cd ..
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r--  1 1000    1000      0 Oct  6 03:19 prueba.txt
226 Transfer complete
```

## 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.

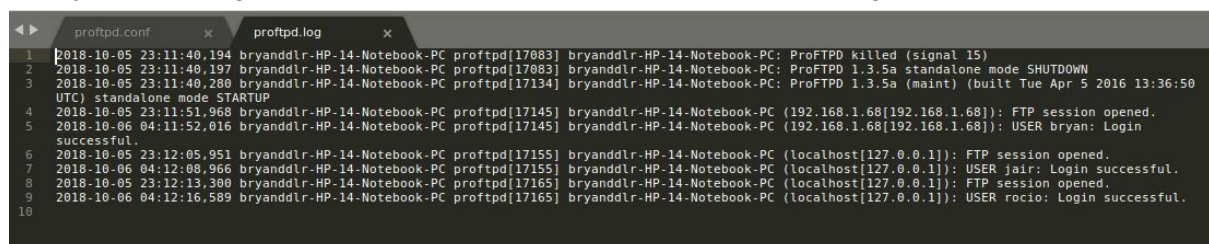
## Configuración de los sistemas de registro de acceso al sistema

### 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:



```
1 2018-10-05 23:11:40,194 bryanddlr-HP-14-Notebook-PC proftpd[17083] bryanddlr-HP-14-Notebook-PC: ProFTPD killed (signal 15)
2 2018-10-05 23:11:40,197 bryanddlr-HP-14-Notebook-PC proftpd[17083] bryanddlr-HP-14-Notebook-PC: ProFTPD 1.3.5a standalone mode SHUTDOWN
3 2018-10-05 23:11:40,280 bryanddlr-HP-14-Notebook-PC proftpd[17134] bryanddlr-HP-14-Notebook-PC: ProFTPD 1.3.5a (maint) (built Tue Apr 5 2016 13:36:50
  UTC) standalone mode STARTUP
4 2018-10-05 23:11:51,968 bryanddlr-HP-14-Notebook-PC proftpd[17145] bryanddlr-HP-14-Notebook-PC (192.168.1.68[192.168.1.68]): FTP session opened.
5 2018-10-06 04:11:52,016 bryanddlr-HP-14-Notebook-PC proftpd[17145] bryanddlr-HP-14-Notebook-PC (192.168.1.68[192.168.1.68]): USER bryan: Login
  successful.
6 2018-10-05 23:12:05,951 bryanddlr-HP-14-Notebook-PC proftpd[17155] bryanddlr-HP-14-Notebook-PC (localhost[127.0.0.1]): FTP session opened.
7 2018-10-06 04:12:08,966 bryanddlr-HP-14-Notebook-PC proftpd[17155] bryanddlr-HP-14-Notebook-PC (localhost[127.0.0.1]): USER jair: Login successful.
8 2018-10-05 23:12:13,300 bryanddlr-HP-14-Notebook-PC proftpd[17165] bryanddlr-HP-14-Notebook-PC (localhost[127.0.0.1]): FTP session opened.
9 2018-10-06 04:12:16,589 bryanddlr-HP-14-Notebook-PC proftpd[17165] bryanddlr-HP-14-Notebook-PC (localhost[127.0.0.1]): USER rocio: Login successful.
10
```

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:

```
11 2018-10-06 04:14:36,231 bryanddlr-HP-14-Notebook-PC proftpd[17267] bryanddlr-HP-14-Notebook-PC (localhost[127.0.0.1]): USER jair: Login successful.
12 2018-10-06 04:15:11,584 bryanddlr-HP-14-Notebook-PC proftpd[17267] bryanddlr-HP-14-Notebook-PC (localhost[127.0.0.1]): FTP session closed.
13 2018-10-05 23:15:16,141 bryanddlr-HP-14-Notebook-PC proftpd[17289] bryanddlr-HP-14-Notebook-PC (localhost[127.0.0.1]): FTP session opened.
14 2018-10-05 23:15:17,559 bryanddlr-HP-14-Notebook-PC proftpd[17289] bryanddlr-HP-14-Notebook-PC (localhost[127.0.0.1]): FTP session closed.
15 2018-10-05 23:15:33,859 bryanddlr-HP-14-Notebook-PC proftpd[17300] bryanddlr-HP-14-Notebook-PC (localhost[127.0.0.1]): FTP session opened.
16 2018-10-06 04:15:45,990 bryanddlr-HP-14-Notebook-PC proftpd[17300] bryanddlr-HP-14-Notebook-PC (localhost[127.0.0.1]): USER jair: Login successful.
17 2018-10-06 04:15:48,226 bryanddlr-HP-14-Notebook-PC proftpd[17300] bryanddlr-HP-14-Notebook-PC (localhost[127.0.0.1]): FTP session closed.
18 2018-10-06 04:15:56,182 bryanddlr-HP-14-Notebook-PC proftpd[17145] bryanddlr-HP-14-Notebook-PC (192.168.1.68[192.168.1.68]): FTP session closed.
19 2018-10-05 23:16:32,038 bryanddlr-HP-14-Notebook-PC proftpd[17134] bryanddlr-HP-14-Notebook-PC: ProFTPD killed (signal 15)
20 2018-10-05 23:16:32,039 bryanddlr-HP-14-Notebook-PC proftpd[17134] bryanddlr-HP-14-Notebook-PC: ProFTPD 1.3.5a standalone mode SHUTDOWN
21 2018-10-05 23:16:32,099 bryanddlr-HP-14-Notebook-PC proftpd[17376] bryanddlr-HP-14-Notebook-PC: ProFTPD 1.3.5a (maint) (built Tue Apr 5 2016 13:36:50 UTC) standalone mode STARTUP
22 2018-10-06 04:16:32,242 bryanddlr-HP-14-Notebook-PC proftpd[17155] bryanddlr-HP-14-Notebook-PC (localhost[127.0.0.1]): FTP session closed.
23 2018-10-06 04:16:32,242 bryanddlr-HP-14-Notebook-PC proftpd[17165] bryanddlr-HP-14-Notebook-PC (localhost[127.0.0.1]): FTP session closed.
24
```

```
bryanddlr@bryanddlr-HP-14-Notebook-PC: /etc/proftpd
bryanddlr@bryanddlr-HP-14-Notebook-PC: /etc/proftpd$ ftp localhost
Connected to localhost.
220 ProFTPD 1.3.5a Server (FTPService) (127.0.0.1)
Name (localhost:bryanddlr): jair
331 Password required for jair
Password:
230 User jair logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bye
221 Goodbye.
bryanddlr@bryanddlr-HP-14-Notebook-PC: /etc/proftpd$
```

## 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:



```
proftpd.conf x proftpd.log x custom.log x
192.168.1.68 - [05/oct/2018:22:50:48 -0500] USER - 331 -
192.168.1.68 jair [06/oct/2018:03:50:49 +0000] PASS - 230 -
192.168.1.68 jair [06/oct/2018:03:50:49 +0000] TYPE - 200 -
192.168.1.68 jair [06/oct/2018:03:50:49 +0000] SYST - 215 -
192.168.1.68 jair [06/oct/2018:03:50:49 +0000] FEAT - - -
192.168.1.68 jair [06/oct/2018:03:50:49 +0000] OPTS UTF8 - 200 -
192.168.1.68 jair [06/oct/2018:03:50:49 +0000] OPTS - - -
192.168.1.68 jair [06/oct/2018:03:50:49 +0000] MODE - 501 -
192.168.1.68 jair [06/oct/2018:03:50:49 +0000] PWD /home/FTP-public/ 257 -
192.168.1.68 jair [06/oct/2018:03:50:49 +0000] NOOP - 200 -
192.168.1.68 jair [06/oct/2018:03:50:49 +0000] NOOP - 200 -
192.168.1.68 jair [06/oct/2018:03:50:49 +0000] PASV - 227 -
192.168.1.68 jair [06/oct/2018:03:50:49 +0000] MLSD /home/FTP-public/ 226 427
192.168.1.68 jair [06/oct/2018:03:50:58 +0000] CWD /home/FTP-public/download 250 -
192.168.1.68 jair [06/oct/2018:03:50:58 +0000] PWD /home/FTP-public/download 257 -
192.168.1.68 jair [06/oct/2018:03:50:59 +0000] PASV - 227 -
192.168.1.68 jair [06/oct/2018:03:50:59 +0000] MLSD /home/FTP-public/download/ 226 207
192.168.1.68 jair [06/oct/2018:03:51:02 +0000] CWD /home/FTP-public 250 -
192.168.1.68 jair [06/oct/2018:03:51:02 +0000] PWD /home/FTP-public/ 257 -
192.168.1.68 jair [06/oct/2018:03:51:02 +0000] PASV - 227 -
192.168.1.68 jair [06/oct/2018:03:51:02 +0000] MLSD /home/FTP-public/ 226 427
192.168.1.68 jair [06/oct/2018:03:51:03 +0000] CWD /home/FTP-public/upload 250 -
192.168.1.68 jair [06/oct/2018:03:51:03 +0000] PWD /home/FTP-public/upload 257 -
192.168.1.68 jair [06/oct/2018:03:51:03 +0000] PASV - 227 -
192.168.1.68 jair [06/oct/2018:03:51:03 +0000] MLSD /home/FTP-public/upload/ 226 211
192.168.1.68 jair [06/oct/2018:03:51:05 +0000] CWD /home/FTP-public 250 -
192.168.1.68 jair [06/oct/2018:03:51:05 +0000] PWD /home/FTP-public/ 257 -
192.168.1.68 jair [06/oct/2018:03:51:05 +0000] PASV - 227 -
192.168.1.68 jair [06/oct/2018:03:51:05 +0000] MLSD /home/FTP-public/ 226 427
192.168.1.68 - [05/oct/2018:22:53:23 -0500] USER - 331 -
192.168.1.68 jair [06/oct/2018:03:53:23 +0000] PASS - 230 -
192.168.1.68 jair [06/oct/2018:03:53:23 +0000] TYPE - 200 -
192.168.1.68 jair [06/oct/2018:03:53:23 +0000] SYST - 215 -
192.168.1.68 jair [06/oct/2018:03:53:23 +0000] FEAT - - -
192.168.1.68 jair [06/oct/2018:03:53:23 +0000] OPTS UTF8 - 200 -
192.168.1.68 jair [06/oct/2018:03:53:23 +0000] OPTS - - -
192.168.1.68 jair [06/oct/2018:03:53:23 +0000] MODE - 501 -
192.168.1.68 jair [06/oct/2018:03:53:23 +0000] PWD /home/FTP-public/ 257 -
```

## 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:

```
bryanddlr@bryanddlr-HP-14-Notebook-PC: ~/Documentos/Redes/Redes/FTP/script
bryanddlr@bryanddlr-HP-14-Notebook-PC:~/Documentos/Redes/Redes/FTP/script$ python filter.py custom.log bryan 1
IP          User      Access      Operation    File                                     Response Code
-----
192.168.1.75 bryan    06/oct/2018:00:59:57 MKD          /home/FTP-public/upload/test          257
192.168.1.75 bryan    06/oct/2018:01:00:05 STOR         /home/FTP-public/upload/file.txt      226
bryanddlr@bryanddlr-HP-14-Notebook-PC:~/Documentos/Redes/Redes/FTP/script$
```

Archivos que el usuario ha descargado:



```
bryanddlr@bryanddlr-HP-14-Notebook-PC: ~/Documentos/Redes/Redes/FTP/script
bryanddlr@bryanddlr-HP-14-Notebook-PC:~/Documentos/Redes/Redes/FTP/script$ python filter.py custom.log jair 2
```

IP	User	Access	Operation	File	Response Code
192.168.1.68	jair	06/oct/2018:01:00:41	RETR	/home/FTP-public/upload/file.txt	226
192.168.1.68	jair	06/oct/2018:01:00:50	RETR	/home/FTP-public/upload/file2.txt	226
192.168.1.68	jair	06/oct/2018:01:00:58	RETR	/home/FTP-public/upload/file3.txt	226

```
bryanddlr@bryanddlr-HP-14-Notebook-PC:~/Documentos/Redes/Redes/FTP/script$
```

Archivos o carpetas que el usuario ha borrado:

```
bryanddlr@bryanddlr-HP-14-Notebook-PC: ~/Documentos/Redes/Redes/FTP/script
bryanddlr@bryanddlr-HP-14-Notebook-PC:~/Documentos/Redes/Redes/FTP/script$ python filter.py custom.log jair 3
```

IP	User	Access	Operation	File	Response Code
192.168.1.68	jair	06/oct/2018:01:01:55	RMD	/home/FTP-public/upload/test	250
192.168.1.68	jair	06/oct/2018:01:02:01	RMD	/home/FTP-public/upload/test2	250
192.168.1.68	jair	06/oct/2018:01:02:06	DELE	/home/FTP-public/upload/fileRenamed.txt	250
192.168.1.68	jair	06/oct/2018:01:02:14	DELE	/home/FTP-public/upload/fileRenamed.txt	250

```
bryanddlr@bryanddlr-HP-14-Notebook-PC:~/Documentos/Redes/Redes/FTP/script$
```

Archivos o carpetas que el usuario ha renombrado:

```
bryanddlr@bryanddlr-HP-14-Notebook-PC: ~/Documentos/Redes/Redes/FTP/script
bryanddlr@bryanddlr-HP-14-Notebook-PC:~/Documentos/Redes/Redes/FTP/script$ python filter.py custom.log jair 4
```

IP	User	Access	Operation	File	Response Code
192.168.1.68	jair	06/oct/2018:01:01:19	RNFR	/home/FTP-public/upload/file.txt	350
192.168.1.68	jair	06/oct/2018:01:01:19	RNTO	/home/FTP-public/upload/fileRenamed.txt	250

```
bryanddlr@bryanddlr-HP-14-Notebook-PC:~/Documentos/Redes/Redes/FTP/script$
```