

BUSCAR 3 COMANDOS FTP EN EL RFC DEL PROTOCOLO FTP

BUSCAR UN EJEMPLO DE CADA UNO DE ELLOS

USER NAME (USER)

The argument field is a Telnet string identifying the user. The user identification is that which is required by the server for access to its file system. This command will normally be the first command transmitted by the user after the control connections are made (some servers may require this). Additional identification information in the form of a password and/or an account command may also be required by some servers. Servers may allow a new USER command to be entered at any point in order to change the access control and/or accounting information. This has the effect of flushing any user, password, and account information already supplied and beginning the login sequence again. All transfer parameters are unchanged and any file transfer in progress is completed under the old access control parameters.

Este comando está añadido en cualquier servidor FTP que requiera una autentificación. Suele venir precedida por el comando PASS en caso de ser requerida.

PASSIVE (PASV)

This command requests the server-DTP to "listen" on a data port (which is not its default data port) and to wait for a connection rather than initiate one upon receipt of a transfer command. The response to this command includes the host and port address this server is listening on.

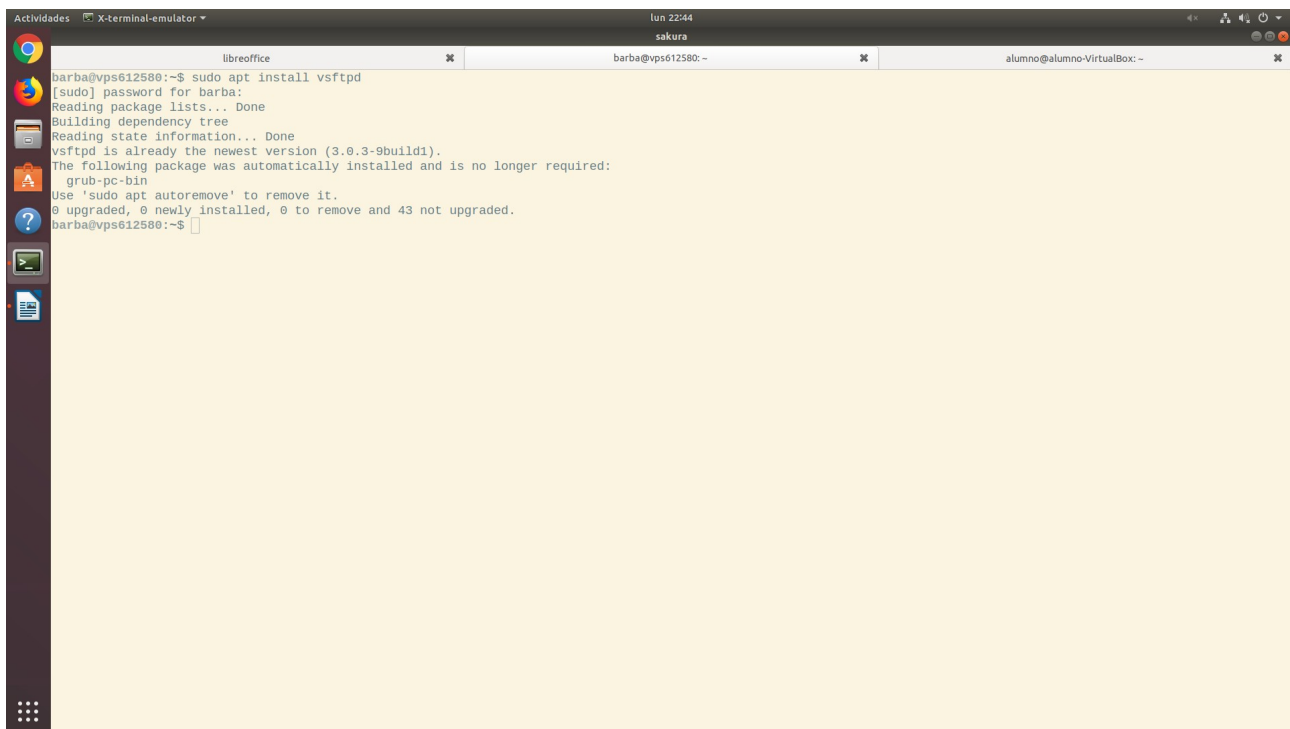
Pide al servidor que se mantenga en escucha por el puerto de datos para realizar transferencias hacia el pasivo.

NOOP (NOOP)

This command does not affect any parameters or previously entered commands. It specifies no action other than that the server send an OK reply.

Sirve para mantener viva una conexión FTP

INSTALAR EN EL VPS DEL ALUMNO EL SERVIDOR FTP VSFTPD



The screenshot shows a terminal window titled 'X-terminal-emulator' with a dark theme. The user 'barba' is logged in on a VPS with IP 'vps612580'. The terminal output shows the command 'sudo apt install vsftpd' being executed. The system prompts for the password, then reads package lists and builds a dependency tree. It reports that 'vsftpd' is already the newest version (3.0.3-9build1) and that 'grub-pc-bin' was automatically installed and is no longer required. The terminal ends with the prompt 'barba@vps612580:~\$'.

```
barba@vps612580:~$ sudo apt install vsftpd
[sudo] password for barba:
Reading package lists... Done
Building dependency tree
Reading state information... Done
vsftpd is already the newest version (3.0.3-9build1).
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 43 not upgraded.
barba@vps612580:~$
```

USAR EL CLIENTE TELNET REALIZANDO UNA CONEXION AL SERVIDOR FTP Y DETERMINAR QUE COMANDOS NECESITAN LA CONEXION DE DATOS Y CUALES NO

telnet vps612580.ovh.net 21
STOU, STOR, APPE, RETR

CAMBIAR EL MENSAJE DE BIENVENIDA (GREETING) Y COMPROBAR QUE SE MUESTRA EL NUEVO MENSAJE AL CONECTARSE UN CLIENTE. USAR UNA SOLA LINEA DE MENSAJE Y TAMBIEN UN FICHERO CON VARIAS LINEAS. VER:

https://www.centos.org/docs/5/html/5.2/Deployment_Guide/s2-server-ftp-gbanner.html

nano /etc/vsftpd.conf
nano /etc/banners/fpt.msg

REALIZAR UNA CONEXION A UN SERVIDOR FTP USANDO EL CLIENTE FTP EN LINEA DE COMANDOS.

USAR COMANDO DIR. CREAR UN FICHERO LLAMADO SALUDO.TXT QUE CONTENGA hola EN UN SUBDIRECTORIO LLAMADO ficheros DEL DIRECTORIO DE INICIO DEL USUARIO LOCAL;

```
ftp -- !dir -- !mkdir ficheros -- lcd ficheros -- !nano SALUDO.TXT // LOCAL
```

```
ftp vps612580.ovh.net -- mkdir ficheros -- cd ficheros -- put saludo.txt -- appe saludo.txt hola
```


SIN SALIR DEL CLIENTE USANDO LOS COMANDOS INTERNOS lcd y !. MOSTRAR EL DIRECTORIO DE TRABAJO LOCAL Y REMOTO.

lcd te permite moverte entre carpetas, !cd no hace nada

MOSTRAR EL CONTENIDO DEL FICHERO saludos.txt EN HEXADECIMAL Y RAW, EN EL SERVIDOR Y EN EL CLIENTE. OBSERVAR CONEXIONES AL PUERTO 21 USANDO EL COMANDO NETSTAT



```
mar 01:10
fleeza libreoffice sakura barba@vps612580 - alumno@alumno-VirtualBox -
ftp> !hexdump SALUDO.TXT
00000000 6f68 616c 000a
00000005
ftp> !cat SALUDO.TXT
hola
ftp>
```



```
mar 01:20
fleeza libreoffice sakura ftp vps612580.ovh.net barba@vps612580 -
barba@vps612580:~$ netstat -ano | grep :21
tcp6      0      0  ::::21                :::*                LISTEN     off (0.00/0/0)
tcp6      0  0  51.75.248.153:21       62.117.181.224:44310 ESTABLISHED keepalive (6798.33/0/0)
barba@vps612580:~$
```

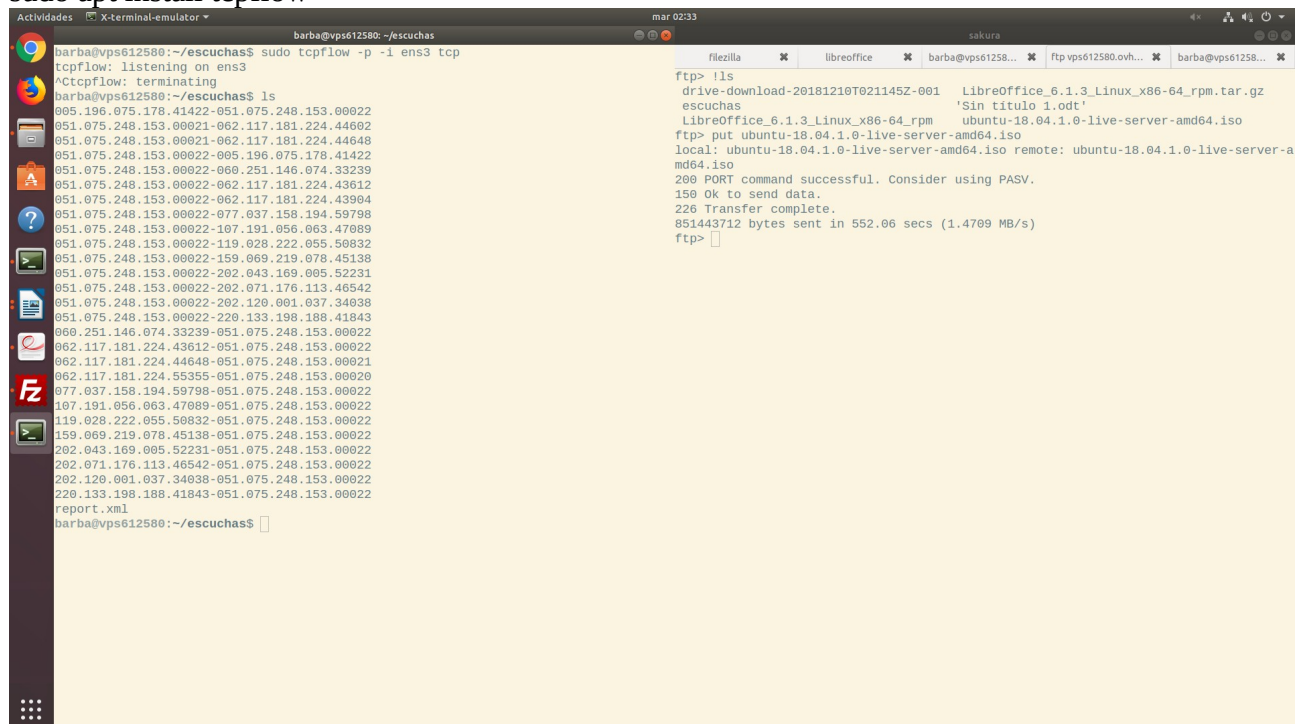
REALIZAR UNA CONEXION FTP DESDE FIREFOX Y USAR LAS HERRAMIENTAS DEL DESARROLLADOR PARA VER PETICIONES Y RESPUESTAS. ¿QUE COMANDOS USA EL CLIENTE? ¿EL MODO USADO POR DEFECTO EN ESTE CASO ES EL ACTIVO O EL PASIVO?

<ftp://vps612580.ovh.net/>

Modo pasivo.

MONITORIZAR UNA SESION FTP USANDO TCPFLOW, VSFTPD COMO SERVIDOR FTP, CLIENTE FTP EN MODO TEXTO REALIZANDO TRANSFERENCIAS DE FICHEROS EN AMBOS SENTIDOS (SERVIDOR<-->CLIENTE)

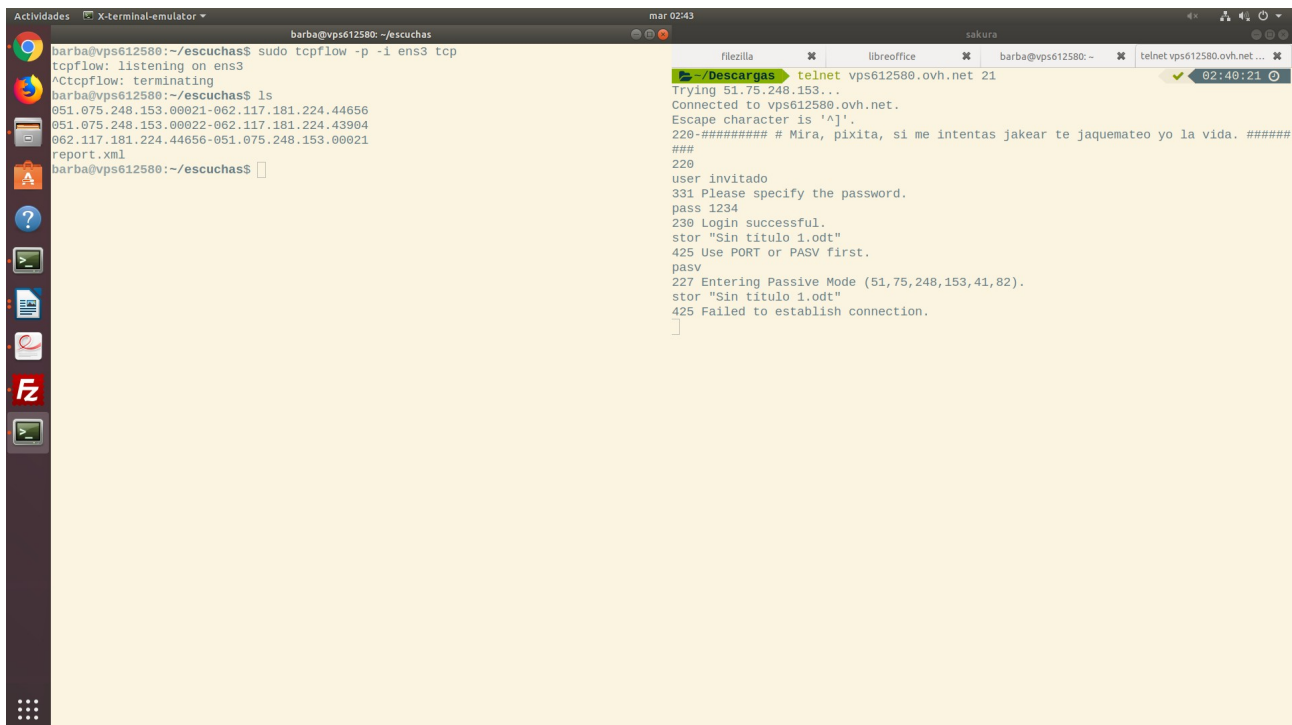
sudo apt install tcpflow



```
barba@vps612580:~/escuchas$ sudo tcpflow -p -i ens3 tcp
tcpflow: listening on ens3
^Ctcpflow: terminating
barba@vps612580:~/escuchas$ ls
005.196.075.178.41422-051.075.248.153.00022
051.075.248.153.00021-062.117.181.224.44602
051.075.248.153.00021-062.117.181.224.44648
051.075.248.153.00022-005.196.075.178.41422
051.075.248.153.00022-060.251.146.074.33239
051.075.248.153.00022-062.117.181.224.43612
051.075.248.153.00022-062.117.181.224.43904
051.075.248.153.00022-077.037.158.194.59798
051.075.248.153.00022-107.191.056.063.47089
051.075.248.153.00022-119.028.222.055.50832
051.075.248.153.00022-159.069.219.078.45138
051.075.248.153.00022-202.043.169.005.52231
051.075.248.153.00022-202.071.176.113.46542
051.075.248.153.00022-202.120.001.037.34038
051.075.248.153.00022-220.133.198.188.41843
060.251.146.074.33239-051.075.248.153.00022
062.117.181.224.43612-051.075.248.153.00022
062.117.181.224.44648-051.075.248.153.00021
062.117.181.224.55355-051.075.248.153.00020
077.037.158.194.59798-051.075.248.153.00022
107.191.056.063.47089-051.075.248.153.00022
119.028.222.055.50832-051.075.248.153.00022
159.069.219.078.45138-051.075.248.153.00022
202.043.169.005.52231-051.075.248.153.00022
202.071.176.113.46542-051.075.248.153.00022
202.120.001.037.34038-051.075.248.153.00022
220.133.198.188.41843-051.075.248.153.00022
report.xml
barba@vps612580:~/escuchas$
```

```
ftp> ll
drive-download-20181210T021145Z-001  LibreOffice_6.1.3_Linux_x86-64_rpm.tar.gz
escuchas                               'Sin titulo 1.odt'
LibreOffice_6.1.3_Linux_x86-64_rpm    ubuntu-18.04.1.0-live-server-amd64.iso
ftp> put ubuntu-18.04.1.0-live-server-amd64.iso
local: ubuntu-18.04.1.0-live-server-amd64.iso remote: ubuntu-18.04.1.0-live-server-a
md64.iso
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
851443712 bytes sent in 552.06 secs (1.4709 MB/s)
ftp>
```

IDEM USANDO COMO CLIENTE TELNET



```
barba@vps612580:~/escuchas$ sudo tcpflow -p -i ens3 tcp
tcpflow: listening on ens3
^Ctcpflow: terminating
barba@vps612580:~/escuchas$ ls
051.075.248.153.00021-062.117.181.224.44656
051.075.248.153.00022-062.117.181.224.43904
062.117.181.224.44656-051.075.248.153.00021
report.xml
barba@vps612580:~/escuchas$
```

```
telnet vps612580.ovh.net 21
Trying 51.75.248.153...
Connected to vps612580.ovh.net.
Escape character is '^['.
220-##### # Mira, pixita, si me intentas jakear te jaquemateo yo la vida. #####
###
220
user invitado
331 Please specify the password.
pass 1234
230 Login successful.
stor "Sin titulo 1.odt"
425 Use PORT or PASV first.
pasv
227 Entering Passive Mode (51,75,248,153,41,82).
stor "Sin titulo 1.odt"
425 Failed to establish connection.
]
```

Telnet no está pensado para conexiones ftp debido a que solo mantiene una conexión simultaneamente, por lo cual falla al intentar conectarse por el puerto de datos.

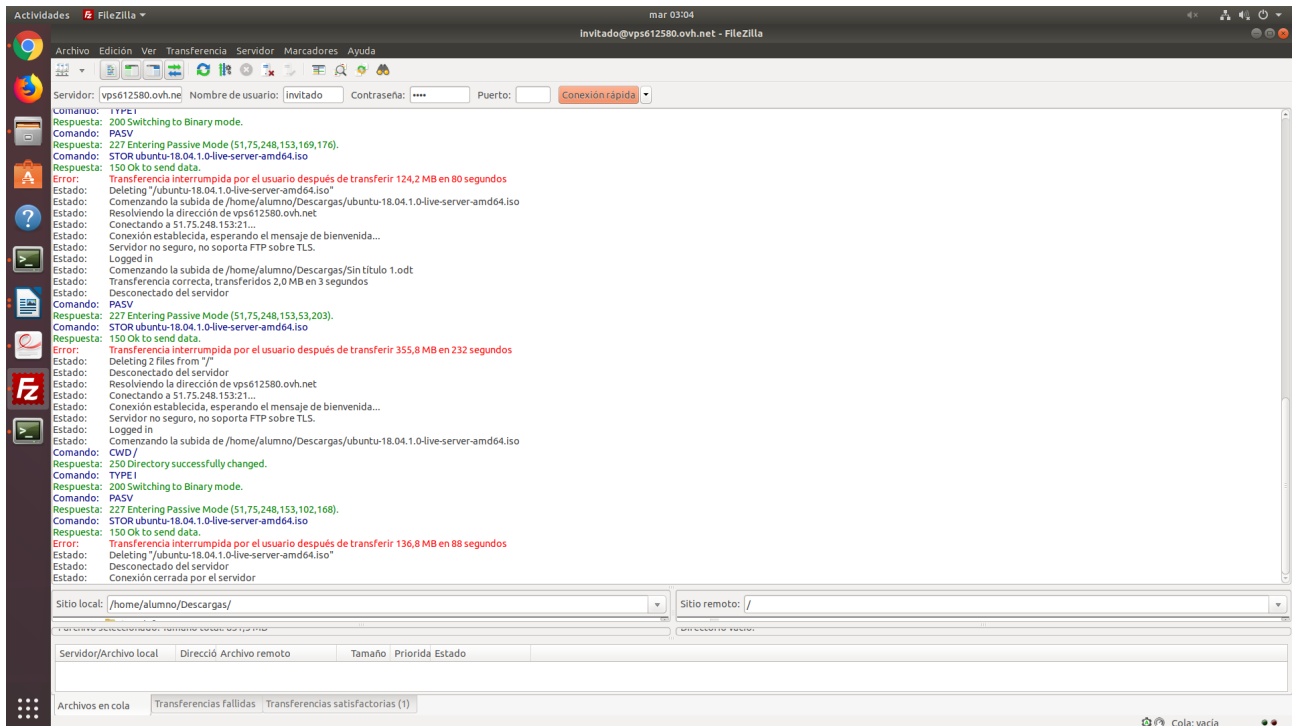
IDEM ANTERIOR USANDO COMO CLIENTE EL NAVEGADOR



```
barba@vps612580:~/escuchas$ sudo tcpflow -p -i ens3 tcp
tcpflow: listening on ens3
```

Nombre	Tamaño	Fecha de modificación
051.075.248.153.00021-062.117.181.224.44800	133 B	11/12/18 3:53:00
051.075.248.153.00021-062.117.181.224.44802	482 B	11/12/18 3:53:00
051.075.248.153.00021-062.117.181.224.44806	133 B	11/12/18 3:53:00
051.075.248.153.00021-062.117.181.224.44808	441 B	11/12/18 3:53:00
051.075.248.153.00021-062.117.181.224.44812	133 B	11/12/18 3:53:00
051.075.248.153.00021-062.117.181.224.44814	276 B	11/12/18 3:53:00
051.075.248.153.00022-062.117.181.224.43904	132 B	11/12/18 3:53:00
051.075.248.153.45330-062.117.181.224.36852	162 B	11/12/18 3:53:00
062.117.181.224.44800-051.075.248.153.00021	22 B	11/12/18 3:53:00
062.117.181.224.44802-051.075.248.153.00021	234 B	11/12/18 3:53:00
062.117.181.224.44806-051.075.248.153.00021	22 B	11/12/18 3:53:00
062.117.181.224.44808-051.075.248.153.00021	109 B	11/12/18 3:53:00
062.117.181.224.44812-051.075.248.153.00021	22 B	11/12/18 3:53:00
062.117.181.224.44814-051.075.248.153.00021	79 B	11/12/18 3:53:00
report.xml	7.9 kB	11/12/18 3:53:00

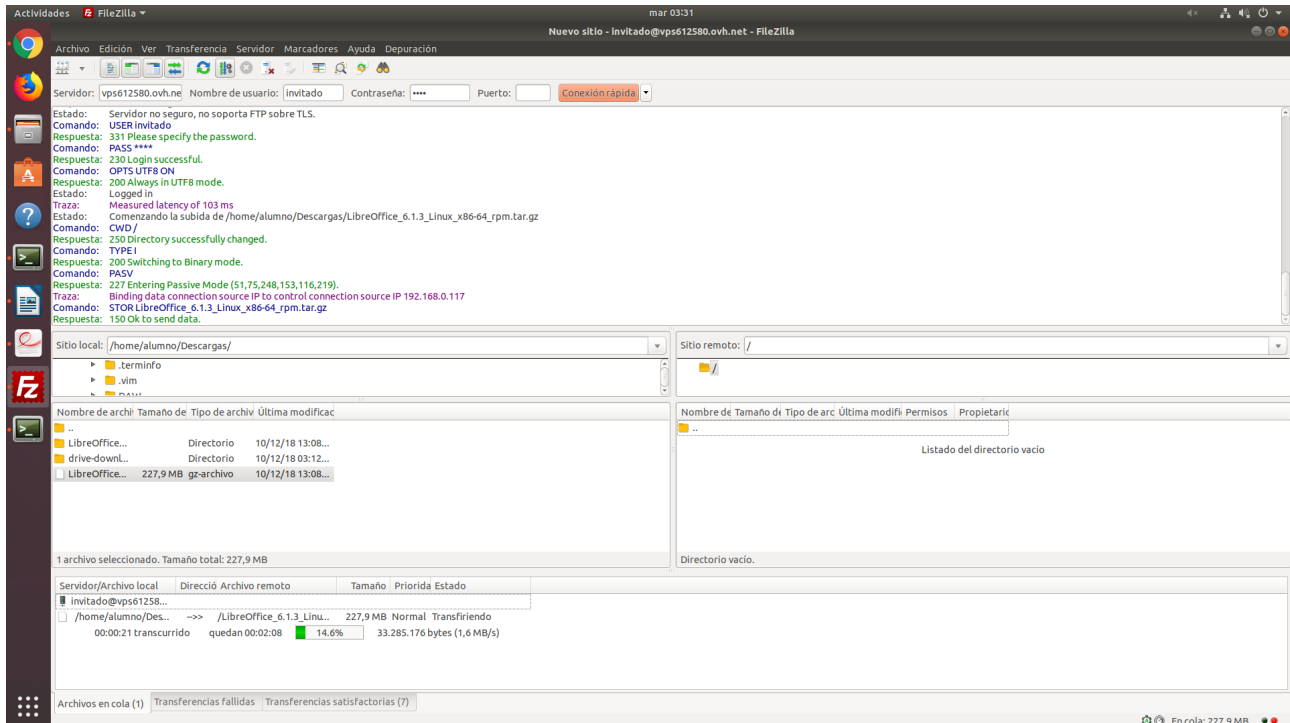
REALIZAR UNA CONEXION A UN SERVIDOR FTP USANDO EL CLIENTE FTP FILEZILLA. OBSERVAR LOS COMANDOS QUE ENVIA EL CLIENTE Y LAS RESPUESTAS DEL SERVIDOR.



USAR UN COMANDO EN LINUX PARA VER LOS PROCESOS QUE TIENEN ESTABLECIDA CONEXION A UN SERVIDOR FTP POR EL PUERTO 21

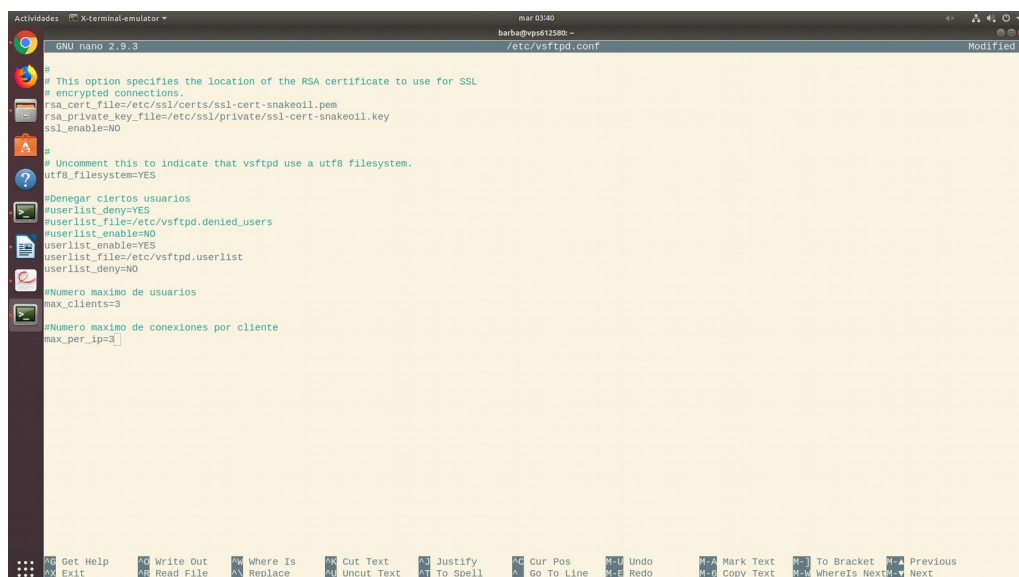
netstat -tano | grep ":21"

CONFIGURAR EL CLIENTE FTP FILEZILLA PARA QUE USE EL MODO DE TRANSFERENCIA PASIVO. IDENTIFICAR Y MOSTRAR QUE COMANDOS Y RESPUESTAS SE INTERCAMBIAN ENTRE EL SERVIDOR Y EL CLIENTE EN ESTE CASO. ¿QUE IP Y QUE NUMERO DE PUERTO HA INDICADO EL SERVIDOR AL CLIENTE PARA EL USO DEL MODO PASIVO?



21 para el de comandos y uno aleatorio para el de datos.

[EN PAREJA] LIMITAR EL NUMERO MAXIMO DE USUARIOS GLOBAL QUE PUEDEN ESTAR SIMULTANEAMENTE CONECTADOS AL SERVIDOR A 3



[EN PAREJA] LIMITAR EL NUMERO MAXIMO DE USUARIOS POR IP QUE PUEDEN ESTAR CONECTADOS A LA VEZ AL SERVIDOR FTP



```
GNU nano 2.9.3 /etc/vsftpd.conf
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO

#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
utf8_filesystem=YES

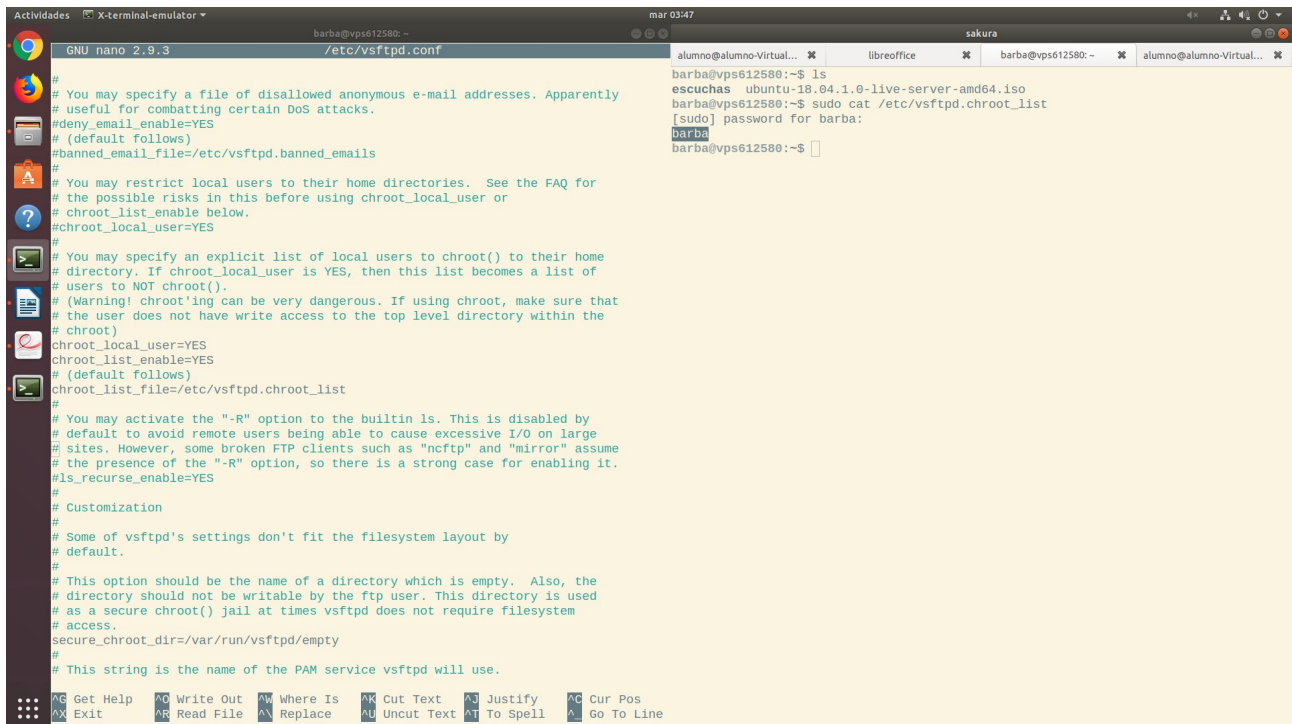
#Denegar ciertos usuarios
userlist_deny=YES
userlist_file=/etc/vsftpd.denied_users
userlist_enable=NO
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO

#Numero maximo de usuarios
max_clients=3

#Numero maximo de conexiones por cliente
max_per_ip=3
```

[EN PAREJA] DESCUBRIR LA IP, EL USUARIO Y CONTRASEÑA QUE USA TU COMPAÑERO PARA CONECTARSE A TU SERVIDOR FTP (SIN QUE TE LO DIGA EL EVIDENTEMENTE!!!)

[EN PAREJA] ENJAULAR AL COMPAÑERO (CHROOT_LIST). COMPROBAR COMO TU NO ESTAS ENJAULADO Y TU COMPAÑERO SI



```
GNU nano 2.9.3 /etc/vsftpd.conf
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may restrict local users to their home directories. See the FAQ for
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
#chroot_local_user=YES
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# Customization
#
# Some of vsftpd's settings don't fit the filesystem layout by
# default.
#
# This option should be the name of a directory which is empty. Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.

AC Get Help  AC Write Out  AW Where Is  AK Cut Text  AJ Justify  AC Cur Pos
AX Exit      AR Read File  AL Replace  AU Uncut Text AT To Spell  A Go To Line
```

Todos estan enjaulados menos el usuario barba

CREAR UNA CUENTA EN UN SERVIDOR FTP GRATUITO Y MONITORIZAR DE NUEVO USANDO EL CLIENTE FTP DE UBUNTU DESDE EL VPS DEL ALUMNO

[EN PAREJA] RESTRINGIR EL ACCESO AL SERVIDOR AL USUARIO DE TU COMPAÑERO EN TU SERVIDOR FTP

The screenshot shows a terminal window with the title 'barba@vps612580: ~'. The user is editing the file `/etc/vsftpd.conf` using the `nano` editor. The configuration file contains the following settings:

```
# This option specifies the location of the RSA certificate to use for SSL  
# encrypted connections.  
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem  
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key  
ssl_enable=NO  
  
# Uncomment this to indicate that vsftpd use a utf8 filesystem.  
utf8_filesystem=YES  
  
#Denegar ciertos usuarios  
userlist_enable=YES  
userlist_deny=YES  
userlist_file=/etc/vsftpd.denied_users  
#userlist_enable=YES  
#userlist_file=/etc/vsftpd.userlist  
#userlist_deny=NO  
  
#Numero maximo de usuarios  
max_clients=3  
  
#Numero maximo de conexiones por cliente  
max_per_ip=3
```

The terminal also shows the following commands and output:

```
barba@vps612580:~$ sudo nano /etc/vsftpd.denied_users  
barba@vps612580:~$ sudo cat /etc/vsftpd.denied_users  
intruso  
invitado  
barba@vps612580:~$
```

[EN GRUPO] PERMITIR EL ACCESO A TU SERVIDOR SOLO A TU COMPAÑERO Y A TI

The screenshot shows a terminal window with the title 'barba@vps612580: ~'. The user is editing the file `/etc/vsftpd.conf` using the `nano` editor. The configuration file contains the following settings:

```
# This option specifies the location of the RSA certificate to use for SSL  
# encrypted connections.  
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem  
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key  
ssl_enable=NO  
  
# Uncomment this to indicate that vsftpd use a utf8 filesystem.  
utf8_filesystem=YES  
  
#Denegar ciertos usuarios  
#userlist_enable=YES  
#userlist_deny=YES  
userlist_enable=YES  
userlist_file=/etc/vsftpd.denied_users  
#userlist_enable=YES  
userlist_file=/etc/vsftpd.userlist  
#userlist_deny=NO  
  
#Numero maximo de usuarios  
max_clients=3  
  
#Numero maximo de conexiones por cliente  
max_per_ip=3
```

The terminal also shows the following commands and output:

```
barba@vps612580:~$ sudo nano /etc/vsftpd.denied_users  
barba@vps612580:~$ sudo cat /etc/vsftpd.denied_users  
intruso  
invitado  
barba@vps612580:~$ sudo nano /etc/vsftpd.userlist  
barba@vps612580:~$ sudo cat /etc/vsftpd.userlist  
barba  
invitado  
barba@vps612580:~$
```