

## 1) BUSCAR 3 COMANDOS FTP EN EL RFC DEL PROTOCOLO FTP

### 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.

### MAKE DIRECTORY [MKD]

This command causes the directory specified in the pathname to be created as a directory (if the pathname is absolute) or as a subdirectory of the current working directory (if the pathname is relative).

### STATUS [STAT]

This command shall cause a status response to be sent over the control connection in the form of a reply. The command may be sent during a file transfer (along with the Telnet IP and Synch signals--see the Section on FTP Commands) in which case the server will respond with the status of the operation in progress, or it may be sent between file transfers. In the latter case, the command may have an argument field. If the argument is a pathname, the command is analogous to the "list" command except that data shall be transferred over the control connection. If a partial pathname is given, the server may respond with a list of file names or attributes associated with that specification. If no argument is given, the server should return general status information about the server FTP process. This should include current values of all transfer parameters and the status of connections.

## 2) BUSCAR UN EJEMPLO DE CADA UNO DE ELLOS

NOOP: Saber si el servidor está activo o reiniciar el temporizador de desconexión automática

MKD: Crear una carpeta y comprobar si tenemos permiso de creación

STAT: Saber cómo está™ la conexión

## 3) INSTALAR EN EL VPS DEL ALUMNO EL SERVIDOR FTP VSFTPD

```

saborido@vps612590: ~
# 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, this
# 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.
pam_service_name=vsftpd
# This option specifies the location of the RSA certificate to use for
# 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
saborido@vps612590:~$ nano /etc/vsftpd.conf

saborido@p7pc08: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
saborido@p7pc08:~$ telnet 51.75.248.163 20
Trying 51.75.248.163...
telnet: Unable to connect to remote host: Connection refused
saborido@p7pc08:~$ telnet 51.75.248.163 2
Trying 51.75.248.163...
telnet: Unable to connect to remote host: Connection refused
saborido@p7pc08:~$ telnet 51.75.248.163 21
Trying 51.75.248.163...
Connected to 51.75.248.163.
Escape character is '^]'.
220 (vsFTPd 3.0.3)

```

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

telnet 51.75.248.163 21  
STOU, STOR, APPE, RETR

5) 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.

```

saborido@p7pc08:~$ telnet 51.75.248.163 21
Trying 51.75.248.163...
Connected to 51.75.248.163.
Escape character is '^]'.
220 eclipse es lo mejor

```

```

C:\Users\wasd3>ftp 51.75.248.163
Conectado a 51.75.248.163.
220-      888d8b
220-      888Y8P
220-      888
220- .d88b. .d8888b888888888888b. .d8888b .d88b.
220-d8P  Y8bd88P" 8888888888 "88b88K d8P Y8b
220-888888888888 8888888888 888"Y8888b.88888888
220-Y8b. Y88b. 8888888888 d88P X88Y8b.
220- "Y8888 "Y8888P888888888888P" 88888P' "Y8888
220-      888
220-      888
220-      888
220
200 Always in UTF8 mode.

```

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

```
ftp> put SALUDOS.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp: 4 bytes enviados en 0.04segundos 0.11a KB/s.
ftp> appe SALUDOS.txt hola
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp: 4 bytes enviados en 0.04segundos 0.10a KB/s.
```

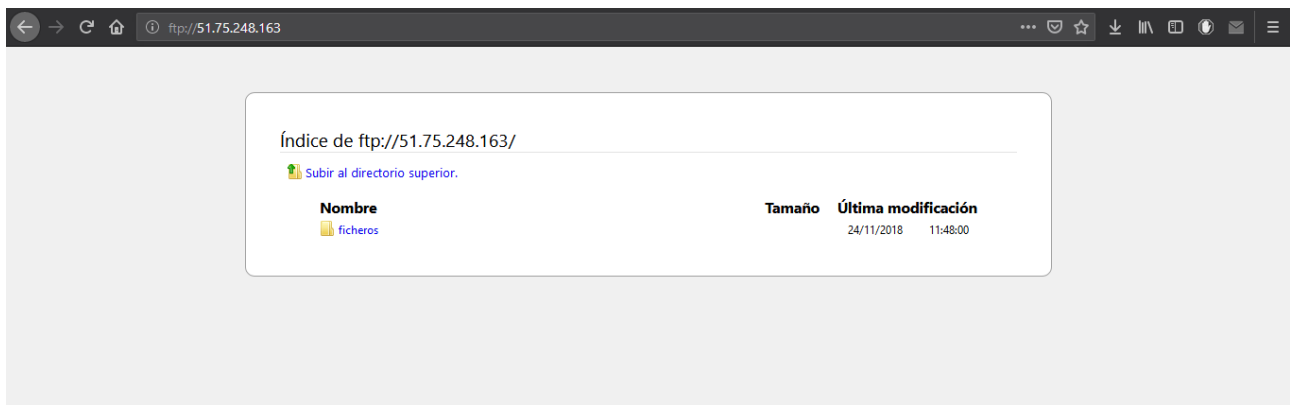
0 68 6f 6c 61																hola											
SALUDOS.txt																											
00000000	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f											
00000000	68	6f	6c	61	..	..	..	..	..	..	..	..	..	..	..	..	hola										

Como son los mismos valores, en raw serían los mismos, solo que en binario, es decir:

```
68 = 0110 1000
6f = 0110 1111
6c = 0110 1100
61 = 0110 0001
```

```
saborido@vps612590:~/ficheros$ netstat --numeric-ports | grep ":21"
tcp6          0          0 vps612590.ovh.net:21    221.26.220.87.dyn:58537 ESTABLISHED
```

7) 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?



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

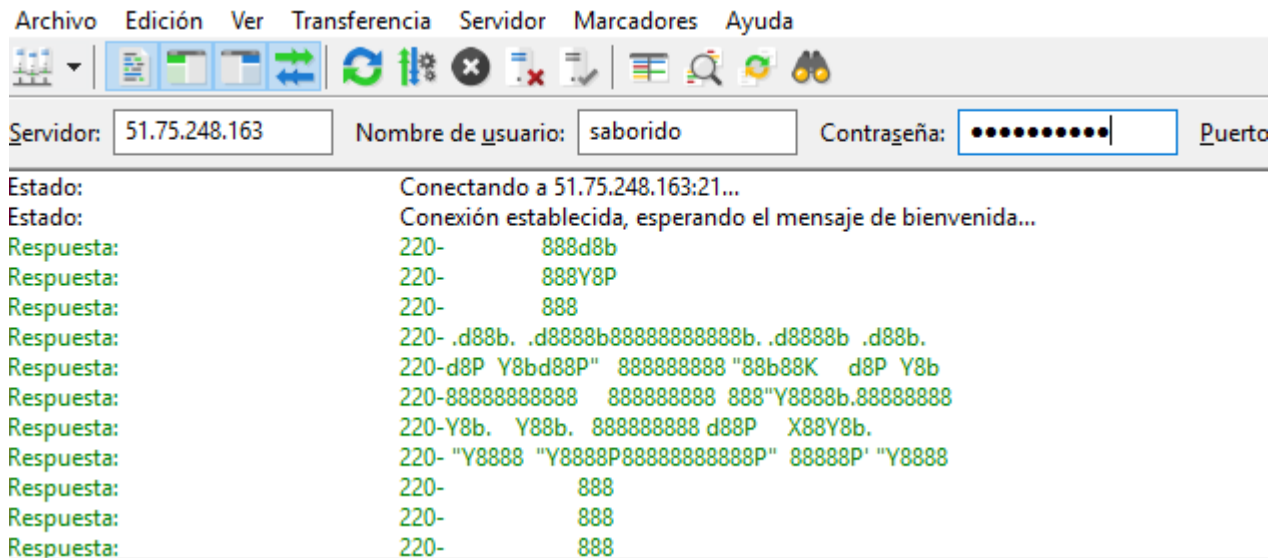
```
188.076.040.032.03344-051.075.248.163.00021: STOR Atlanta 2x01 - El hombre del c
aiman [WEB-DL AMZN 1080p H264 Dual AC3 2.0-5.1 Subs][GrupoHDS].mkv
051.075.248.163.00021-188.076.040.032.03344: 150 Ok to send data.
188.076.040.032.02046-051.075.248.163.00021: PWD
051.075.248.163.00021-188.076.040.032.02046: 257 "/home/saborido/ficheros" is th
e current directory
```

```
tcpflow: listening on ens3
188.076.040.032.03966-051.075.248.163.00021: NOOP
051.075.248.163.00021-188.076.040.032.03966: 200 NOOP ok.
188.076.040.032.03966-051.075.248.163.00021: CWD /home/saborido
051.075.248.163.00021-188.076.040.032.03966: 250 Directory successfully changed.
188.076.040.032.03966-051.075.248.163.00021: CWD DAW 18-19
051.075.248.163.00021-188.076.040.032.03966: 550 Failed to change directory.
188.076.040.032.03966-051.075.248.163.00021: CWD /home/saborido
051.075.248.163.00021-188.076.040.032.03966: 250 Directory successfully changed.
188.076.040.032.03966-051.075.248.163.00021: CWD DAW 18-19
051.075.248.163.00021-188.076.040.032.03966: 550 Failed to change directory.
188.076.040.032.03966-051.075.248.163.00021: CWD /home/saborido
051.075.248.163.00021-188.076.040.032.03966: 250 Directory successfully changed.
188.076.040.032.03966-051.075.248.163.00021: TYPE I
051.075.248.163.00021-188.076.040.032.03966: 200 Switching to Binary mode.
188.076.040.032.03966-051.075.248.163.00021: PASV
051.075.248.163.00021-188.076.040.032.03966: 227 Entering Passive Mode [51,75,248,163,120,16].
188.076.040.032.03966-051.075.248.163.00021: LIST
051.075.248.163.00021-188.076.040.032.03966: 150 Here comes the directory listing.
051.075.248.163.00021-188.076.040.032.03966: 226 Directory send OK.
```

9) IDEM USANDO COMO CLIENTE TELNET  
No se puede enviar archivos con telnet

10) IDEM ANTERIOR USANDO COMO CLIENTE EL NAVEGADOR  
Ni Chrome ni Firefox te muestran los comandos FTP que usan.

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



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

Netstat -ano | grep ":21"

14) 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?

Gestor de sitios

Seleccione el sitio:

Mis sitios

Nuevo sitio

Nuevo sitio

Nueva carpeta

Nuevo marcador

Renombrar

Borrar

Duplicado

General

Avanzado

Opciones de Transferencia

Juego de caracteres

Modo de transferencia:

☐ Predeterminado

☐ Activo

☒ Pasivo

☐ Limitar el número de conexiones simultáneas

Número máximo de conexiones

1

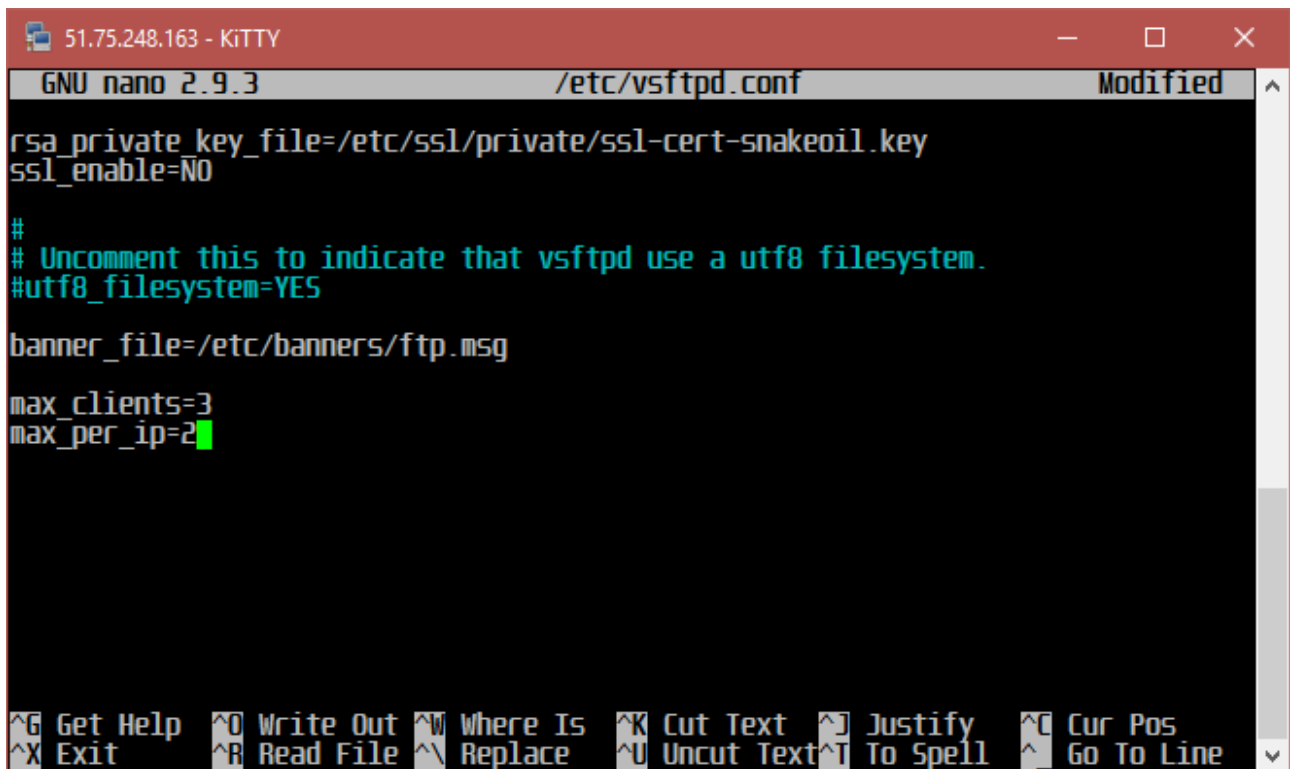
Conectar

Aceptar

Cancelar

```
051.075.248.163.00021-188.076.040.032.02602: 230 Login successful.
188.076.040.032.02602-051.075.248.163.00021: CWD /home/saborido/ficheros
051.075.248.163.00021-188.076.040.032.02602: 250 Directory successfully changed.
188.076.040.032.02602-051.075.248.163.00021: PWD
051.075.248.163.00021-188.076.040.032.02602: 257 "/home/saborido/ficheros" is the current directory
188.076.040.032.02602-051.075.248.163.00021: TYPE I
051.075.248.163.00021-188.076.040.032.02602: 200 Switching to Binary mode.
188.076.040.032.02602-051.075.248.163.00021: PASV
051.075.248.163.00021-188.076.040.032.02602: 227 Entering Passive Mode (51,75,248,163,135,47).
188.076.040.032.02602-051.075.248.163.00021: LIST
051.075.248.163.00021-188.076.040.032.02602: 150 Here comes the directory listing.
051.075.248.163.00021-188.076.040.032.02602: 226 Directory send OK.
188.076.040.032.02602-051.075.248.163.00021: PASV
051.075.248.163.00021-188.076.040.032.02602: 227 Entering Passive Mode (51,75,248,163,142,171).
188.076.040.032.02602-051.075.248.163.00021: STOR Captura.PNG
051.075.248.163.00021-188.076.040.032.02602: 150 Ok to send data.
051.075.248.163.00021-188.076.040.032.02602: 226 Transfer complete.
188.076.040.032.02545-051.075.248.163.00021: NOOP
051.075.248.163.00021-188.076.040.032.02545: 200 NOOP ok.
```

15) y 16) [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



```
51.75.248.163 - KITTY
GNU nano 2.9.3 /etc/vsftpd.conf Modified
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

banner_file=/etc/banners/ftp.msg

max_clients=3
max_per_ip=2

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^I To Spell   ^_ Go To Line
```

17) [EN PAREJA] DESCUBRIR LA IP, EL USUARIO Y CONTRASEÑA QUE USA TU COMPAÑERO PARA CONECTARSE A TU SERVIDOR FTP

Para ver la IP tendrías que hacer un tcpflow -c port 21

18) [EN PAREJA] ENJAULAR AL COMPAÑERO (CHROOT\_LIST). COMPROBAR COMO TU NO ESTAS ENJAULADO Y TU COMPAÑERO SI

Tendríamos que saber el usuario local que usa el compañero y habilitar la opción "chroot\_list\_enable" en vsftpd.conf. Una vez habilitada decidimos el archivo donde vamos a guardar con la opción "chroot\_list\_file=archivo". Si esta hecho todo bien estaría el usuario del compañero enjaulado y tu usuario no.

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

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

Pondríamos en vsftpd.conf el comando "userlist\_enable=yes" y no entraría ningún usuario cuyo nombre este en el archivo.txt del comando "userlist\_file=archivo.txt"

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

Pondríamos en vsftpd.conf el comando "userlist\_deny" y "userlist\_enable=no" y no entraría ningún usuario a no ser que su nombre este en el archivo.txt del comando "userlist\_file=archivo.txt"