

# **CESI**

## **PRÁCTICA 3**

Configuración y utilización básica de  
servicios en S.O de Servidores

DANIEL RANCHAL PARRADO

## INSTALACIÓN DE SERVICIOS Y CONFIGURACIONES

**Cuestión 1: Liste los argumentoss de yum y apt necesarios para instalar, buscar y eliminar paquetes.**

	apt	yum
<b>Instalar</b>	<b>install</b> <nombre_paquete>	<b>install</b> <nombre_paquete>
<b>Buscar</b>	<b>search</b> <paquete_a_buscar>	<b>search</b> <paquete_a_buscar>
<b>Eliminar paquetes</b>	<b>remove</b> <paquete_a_borrar>	<b>erase</b> <paquete_a_borrar>

## GESTIÓN DE LOS CORTAFUEGOS(FIREWALLS)

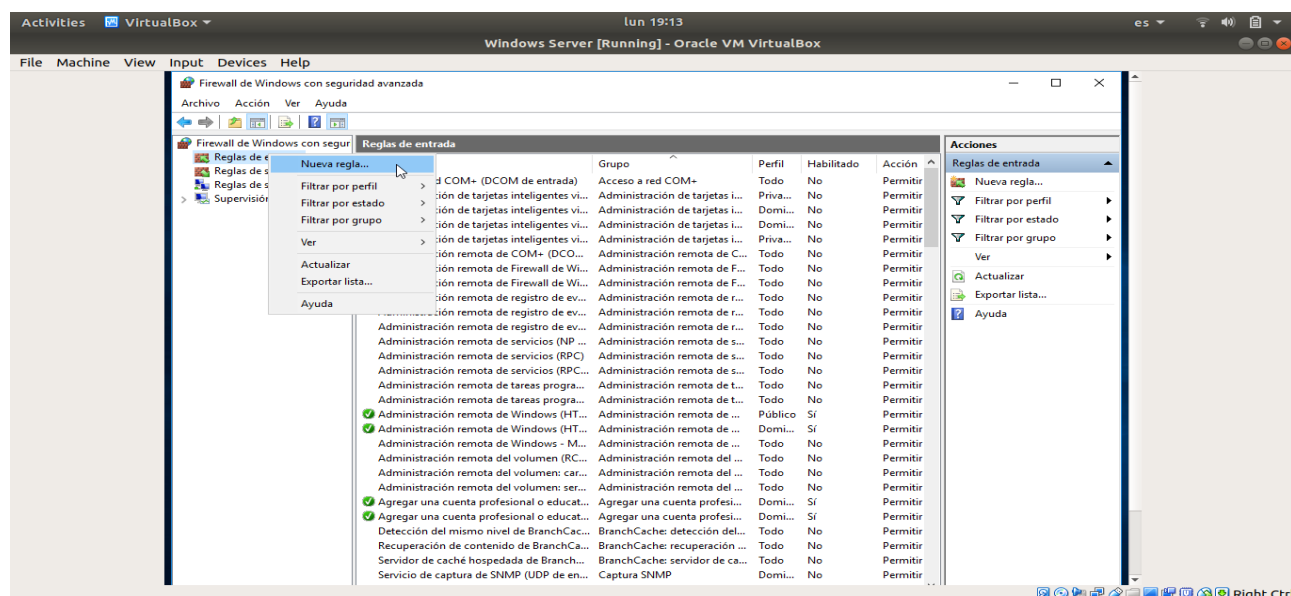
**Cuestión 3: ¿Cómo se denominan y por quien pueden ser usados los puertos comprendidos entre 1024 y 65535?**

Los puertos comprendidos desde el 1024 hasta el puerto 49151 son puertos que están registrados. Están asignados por la organización IANA para servicios específicos, los cuales han sido solicitados por una entidad o empresa.

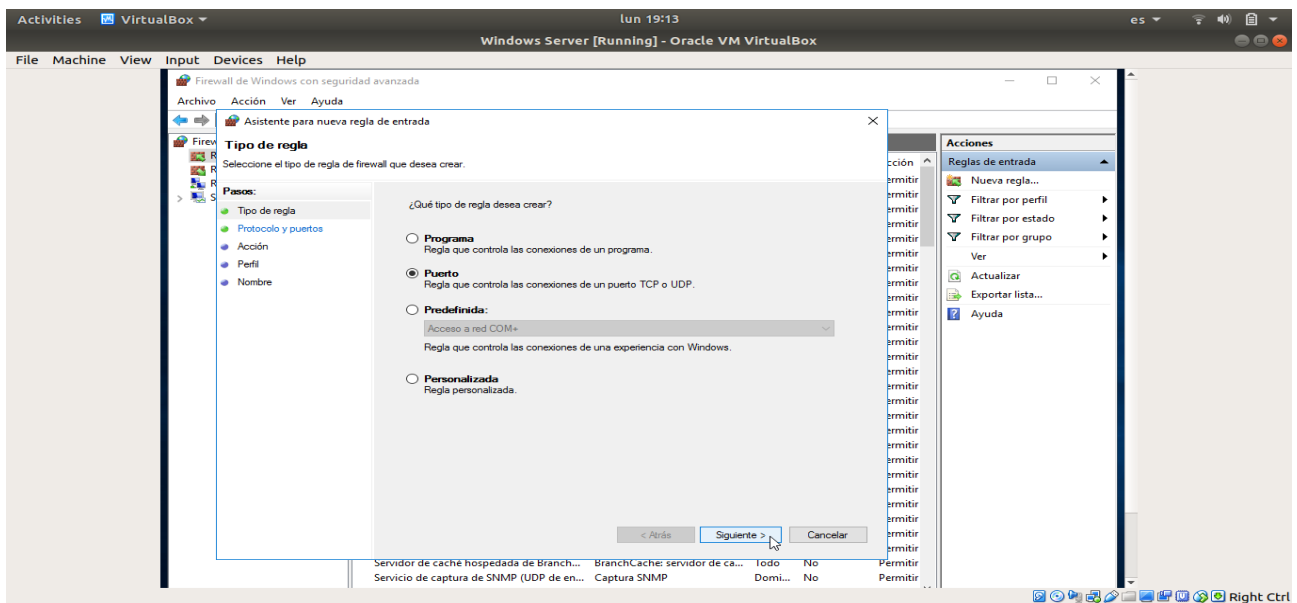
Los puertos comprendidos desde 49152 hasta el puerto 65535 son puertos dinámicos o privados, los cuales no pueden ser registrados por la organización IANA.

**Cuestión 4: Pruebe a abrir y cerrar varios puertos en CentOS y Windows Server. Asegúrese de abrir el puerto 21, 22 y 80 a los servicios asociados por defecto.**

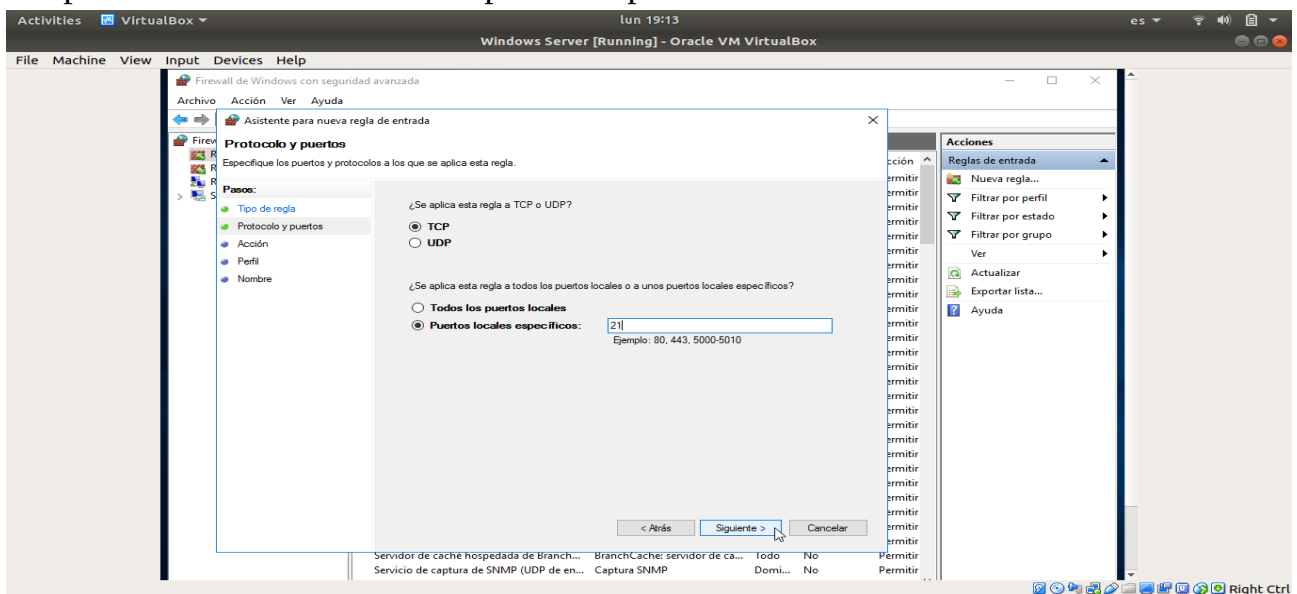
Para abrir un puerto o varios en Windows Server, hay que añadir una nueva regla en el Firewall de Windows. Para ello, nos movemos a reglas de entrada y añadimos una.



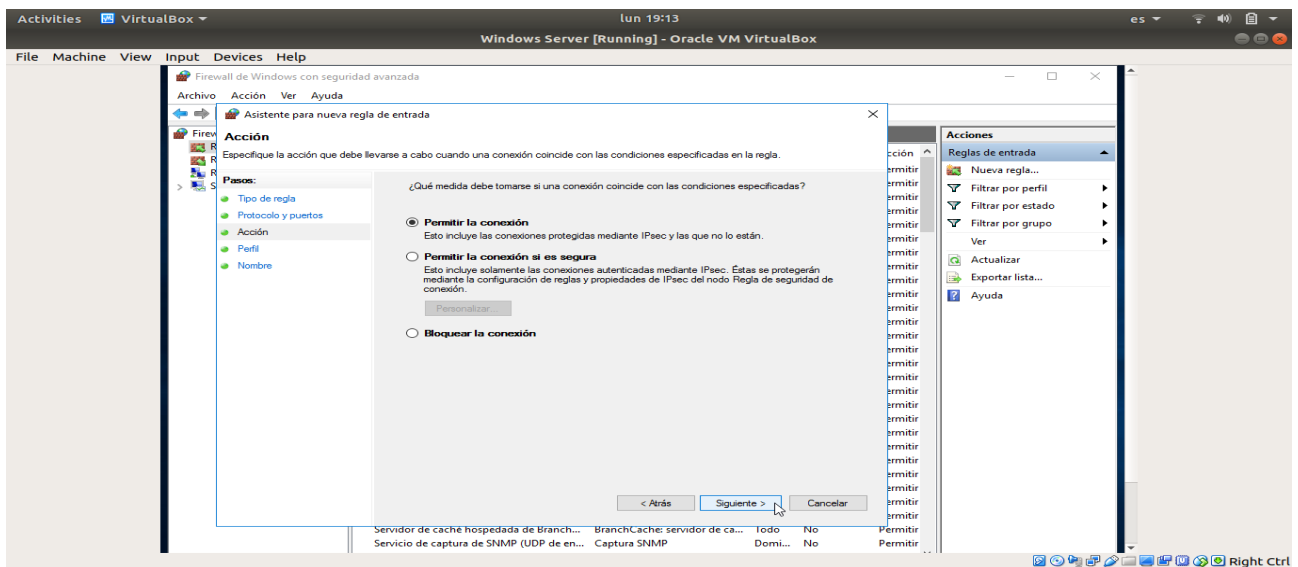
Una vez aquí, seleccionamos la opción de Puerto, ya que queremos crear una regla asociada a eso.



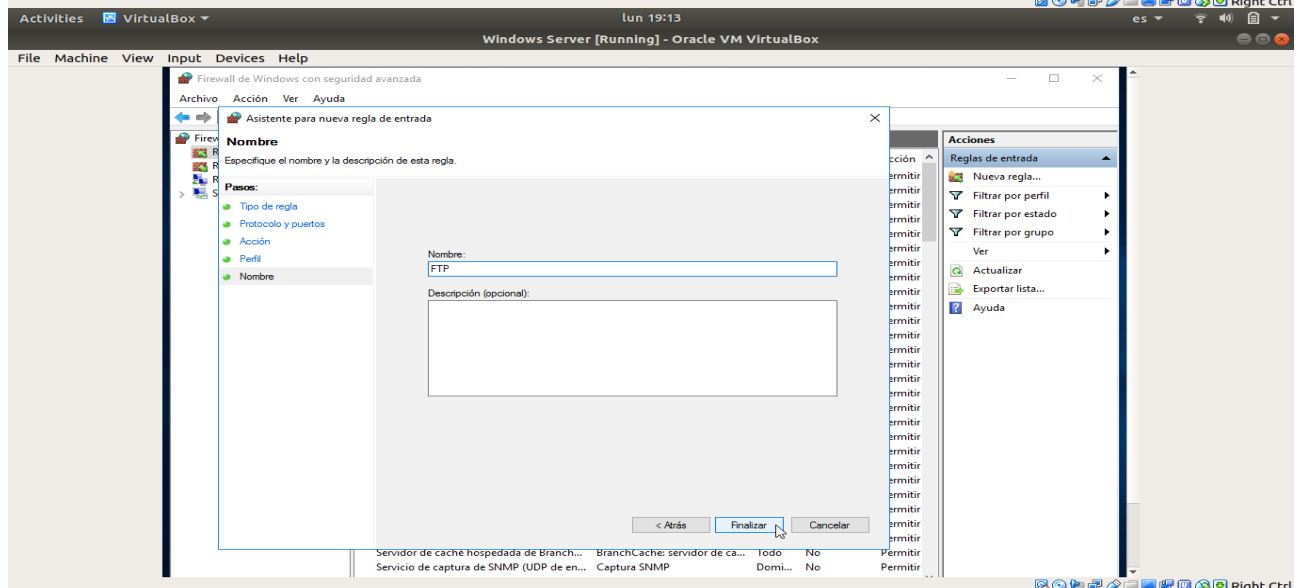
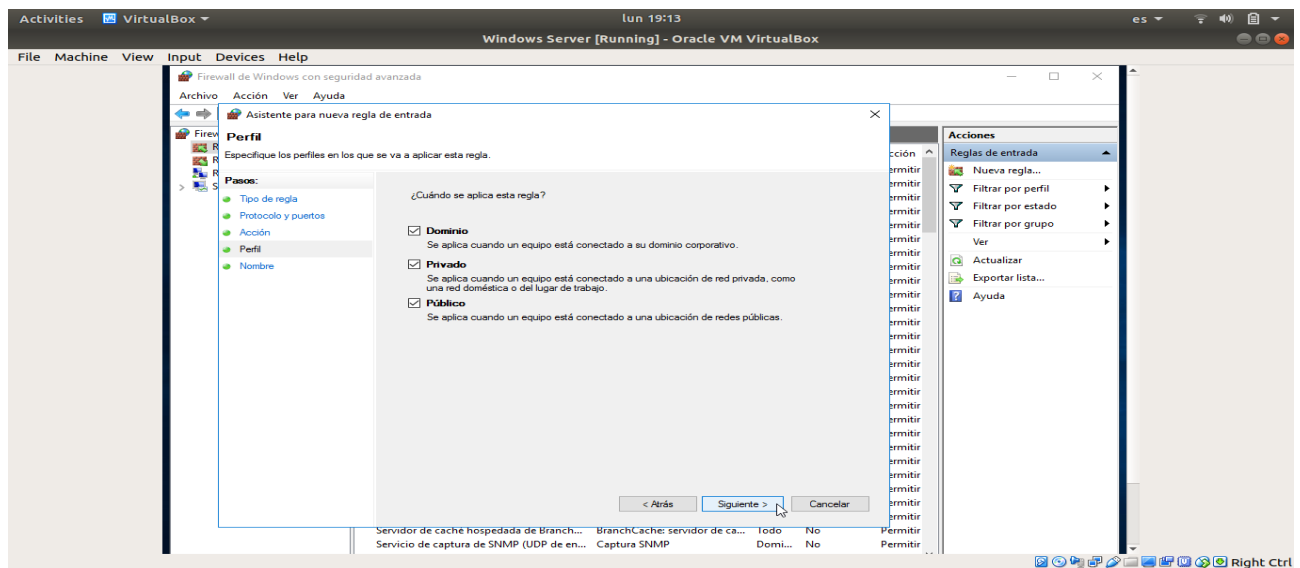
Seleccionamos que esta regla se aplica a TCP, y el número específico de puerto al que se aplicará. En este caso hemos puesto el puerto 21.



Cuando se cumpla las condiciones que hemos puesto anteriormente, queremos que se permita la conexión.



A continuación, se elige que se aplique la aplicación de la regla obviando desde que sitio se está realizando la conexión al servicio que opera en ese puerto. Como último paso, se le pone un nombre a la regla.



Para abrir puertos en CentOS, se ha utilizado el CLI firewall-cmd. Para abrir un puerto hay que hacer lo siguiente con permisos de administrador:

**firewall-cmd --zone=<zone> --add-port=<port>/<udp|tcp> --permanent**

donde <port> es el número de puerto que se quiere abrir, <udp|tcp> el protocolo y <zone> determina la zona que estamos utilizando. El significado de zona es un firewall define el nivel de confianza que se va a tener con los dispositivos que se conecten por este puerto. Como se va a acceder por redes públicas, no se debe confiar en ningún dispositivo. Cada zona define sus propias características y como debe funcionar el firewall. Al comando se le añade la bandera --permanent para que la regla del firewall persista después de un reboot del sistema. Para abrir los puertos indicados y que se queden registrados en el sistema, hay que poner los siguientes comandos:

```
firewall-cmd --zone=public --add-port=21/tcp --permanent
firewall-cmd --zone=public --add-port=22/tcp --permanent
firewall-cmd --zone=public --add-port=80/tcp --permanent
firewall-cmd --reload
```

## **CONFIGURACIÓN DEL SERVICIO DE ACCESO REMOTO A LA CONSOLA(SECURE SHELL)**

**Cuestión 5: ¿Para que sirve la opción -X? ¿Qué ocurre si ejecutamos el comando gedit?**

La opción -X nos permite establecer una conexión ssh con el servicio X11, que se encarga del sistema de ventanas en Linux. Si ejecutamos gedit, el servidor nos mandará, por así decirlo, la información de como se tiene que mostrar la ventana que representa gedit en nuestra máquina local.

**Cuestión 6: Muestre la secuencia de comandos y las modificaciones a los archivos correspondientes para permitir acceder a la consola sin introducir la contraseña.**

Para poder entrar a nuestro servidor sin introducir la contraseña disponemos de un comando, el cuál es ssh-copy-id. Si queremos acceder desde nuestra máquina local con una clave pública y privada establecida (ssh-keygen), introducimos el siguiente comando:

**ssh-copy-id <user>@<hostname>**

Al introducir ese comando, nos pedirá la contraseña para ese usuario y esa máquina. Si se ha introducido bien, se ha añadido al servidor las claves públicas autorizadas que pueden entrar al sistema sin poner la contraseña. Para probarlo, se introduce el siguiente comando y ya no pide contraseña:

```
ssh <user>@<hostname>
```

**Cuestión 7:** ¿Qué archivo es el que contiene la configuración de sshd? Compruebe que modificando el archivo correspondiente permite acceder con o sin contraseña al servidor.

El archivo que contiene la configuración de sshd es `/etc/ssh/sshd_config`. Para que no pida la contraseña hay que modificar la directiva por defecto (`PasswordAuthentication yes`) a (`PasswordAuthentication no`).

**Cuestión 8:** Indique si es necesario reiniciar el servicio. ¿Cómo se reinicia un servicio en Ubuntu? ¿y en CentOS? Muestre la secuencia de comandos para hacerlo.

Cada vez que se modifica el archivo de configuración, es necesario reiniciar el servicio. Para en ello, en Ubuntu al igual que en CentOS se reinicia de la siguiente manera:

```
sudo systemctl restart sshd
```

## CONFIGURACIÓN DEL SERVICIO FTP

**Cuestión 9:** Existen dos modos de conexión FTP, detalle el funcionamiento de cada uno y sus diferencias.

Existe la conexión de manera activa y de manera pasiva. En modo activo, el servidor siempre crea el canal de datos en su puerto 20, mientras que en el lado del cliente el canal de datos se asocia a un puerto aleatorio mayor que el 1024. Para ello, el cliente manda un comando `PORT` al servidor por el canal de control indicándole ese número de puerto, de manera que el servidor pueda abrirle una conexión de datos por donde se transferirán los archivos y los listados, en el puerto especificado. Mientras que en el modo pasivo, el cliente envía el comando `PASV` al servidor y este le responde a que puerto debe de conectarse para recibir datos.

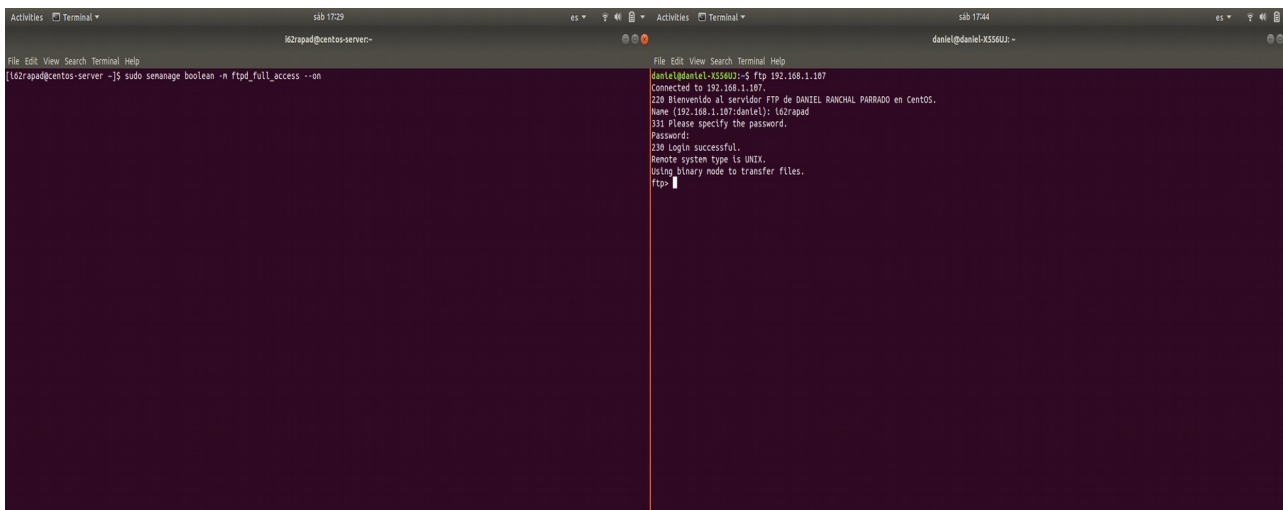
## Cuestión 10: Configure el servicio vsftpd con los siguientes cambios e ilústrelo con capturas de pantalla.

- No permitir la conexión a usuarios anónimos
- Permitir el acceso utilizando las cuentas de usuarios del anfitrión local.
- Activar los registros, tanto para conexiones como para transferencias.
- Establecer el mensaje “Bienvenido al servidor FTP de NOMBRE-APELLIDOS en CentOS” como mensaje de bienvenida del servicio.

```
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
# When SELinux is enforcing check for SE bool ftp_home_dir
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the ftp user.
# When SELinux is enforcing check for SE bool allow_ftp_anon_write, allow_ftp_full_access
anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
#message_enable=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
chown_uploads=YES
chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
xferlog_file=/var/log/xferlog
#
# If you want, you can have your log file in standard xferlog format.
# Note that the default log file location is /var/log/xferlog in this case.
xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
idle_session_timeout=600
#
# You may change the default value for timing out a data connection.
data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
passive_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that on some FTP servers, ASCII support allows a denial of service
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
ascii_upload_enable=YES
ascii_download_enable=YES
#
# You may fully customise the login banner string:
ftpd_banner=Bienvenido al servidor FTP de DANIEL RANCHOAL PARRADO en CentOS.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combating certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
#
# 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'log 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)
```

Como se muestran en las capturas, para no permitir la conexión de usuarios anónimos, se ha puesto la directiva `anonymous_enable` a `NO`. Para que ftp utilice las cuentas de la máquina local para logearse en este mismo servicio, se ha puesto la directiva `local_enable` a `YES`. Luego habrá que comunicarle esta decisión a SELinux poniendo a `true` una variable llamada `ftpd_full_access`. Luego ponemos a `YES` la directiva `xferlog_enable` para guardar un log de lo que se envía y recibe, además de los inicios de sesión. También se pone a `YES` `dual_log_enable`, hace que se escriban dos logs simultáneamente, uno que es compatible con `wu-ftp` y el otro no.

La directiva `ftpd_banner` contiene el mensaje de bienvenida.

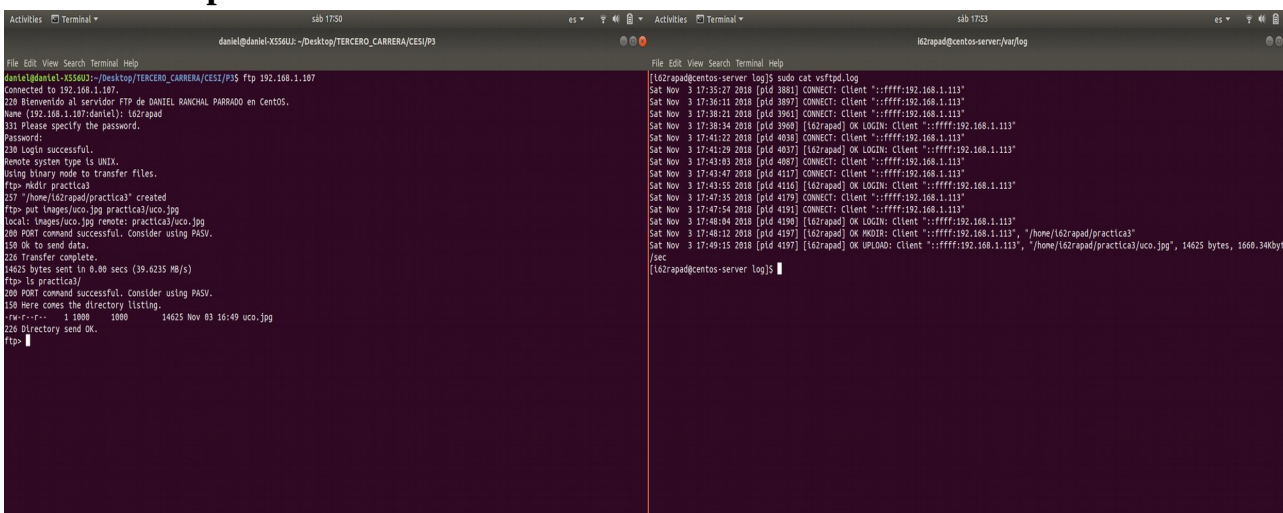


Como se ha comentado anteriormente, hay que definir la variable `ftpd_full_access` a `true` con la herramienta `semanage`, la cual se encarga de la gestión de SELinux. Una vez hecho todos estos cambios en la configuración de `vsftpd`, hay que reiniciar el servidor con el comando **`sudo systemctl restart vsftpd`**. Par

### **Cuestión 11: ¿Qué es SELinux y qué funcionalidad tiene?**

SELinux (Security Enhanced Linux) es un sistema de control obligatorio de acceso basado en la interfaz LSM (Linux Security Modules). SELinux utiliza una serie de reglas para autorizar o denegar operaciones. Por lo que antes de cada llamada al sistema, el kernel pregunta si el proceso que se está ejecutando puede ejecutar una operación específica según las reglas.

**Cuestión 12: Muestre la secuencia de comandos que utilizaría para subir una imagen al directorio `/home/usuario/practica3` del servidor ftp de CentOS desde la máquina anfitriona. Muestre también el log que ha registrado el servicio al realizar las operaciones anteriores.**



Las tres últimas líneas del log representan las operaciones realizadas.



**Cuestión 12:** Muestre la secuencia de comandos que utilizaría para subir una imagen al directorio /usuario/practica3 del servidor ftp de Windows desde la máquina anfitriona.

```
Activities Terminal
sáb 19:56
daniel@daniel-X556UJ: ~/Desktop/TERCERO_CARRERA/CESI/P3
File Edit View Search Terminal Help
daniel@daniel-X556UJ:~/Desktop/TERCERO_CARRERA/CESI/P3$ ftp 192.168.1.112
Connected to 192.168.1.112.
220 Microsoft FTP Service
Name (192.168.1.112:daniel): i62rapad
331 Password required
Password:
230-Bienvenido al servidor FTP de DANIEL RANCHAL PARRADO en Windows Server
230 User logged in.
Remote system type is Windows_NT.
ftp> mkdir practica3
257 "practica3" directory created.
ftp> put images/uco.jpg practica3/uco.jpg
local: images/uco.jpg remote: practica3/uco.jpg
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
14923 bytes sent in 0.00 secs (14.0352 MB/s)
ftp> ls practica3/
200 PORT command successful.
125 Data connection already open; Transfer starting.
-rwxrwxrwx 1 owner group 14923 Nov 3 19:56 uco.jpg
226 Transfer complete.
ftp>
```

## CONFIGURACIÓN DE UN SERVIDOR WEB BÁSICO

**Cuestión 14:** Enumere otros servidores web.

Otros servidores web son httpd, TomCat y Google Web Server.



**DANIEL, RANCHAL PARRADO**

PRÁCTICA 3, CESI. Directorio Virtual. WINDOWS SERVER



UNIVERSIDAD DE CÓRDOBA



## **DANIEL, RANCHAL PARRADO**

PRÁCTICA 3, CESI. Directorio Virtual. CENTOS



UNIVERSIDAD DE CÓRDOBA



## **DANIEL, RANCHAL PARRADO**

PRÁCTICA 3, CESI. Directorio Virtual. UBUNTU SERVER



UNIVERSIDAD DE CÓRDOBA

### **Pregunta 1: ¿Cómo se puede ver el estado de un demonio (sshd, vsftpd)?**

`sudo systemctl status <demonio>`

### **Pregunta 2: ¿Qué son las zonas de un firewall?**

Las zonas definen un conjunto de reglas dependiendo del nivel de confianza con los equipos a los que nos conectamos.

## **REFERENCIAS**

- **Port Numbers Wikipedia**
- **IANA Port Registry**
- **How to open a port**
- **Firewall Zones**
- **Passive FTP**
- **Vsftpd and SELinux**
- **ftp\_home\_dir removed**
- **SELinux**