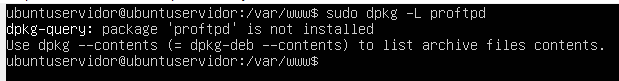
Practica 7 – Servicio FTP

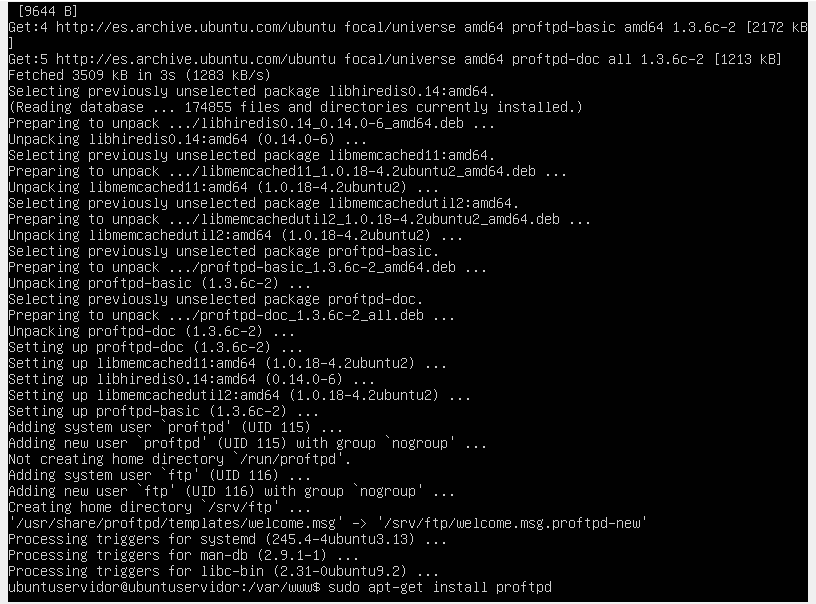
# En el Servidor-1. Preliminares:

## Instala un servicio FTP mediante el paquete proftpd.

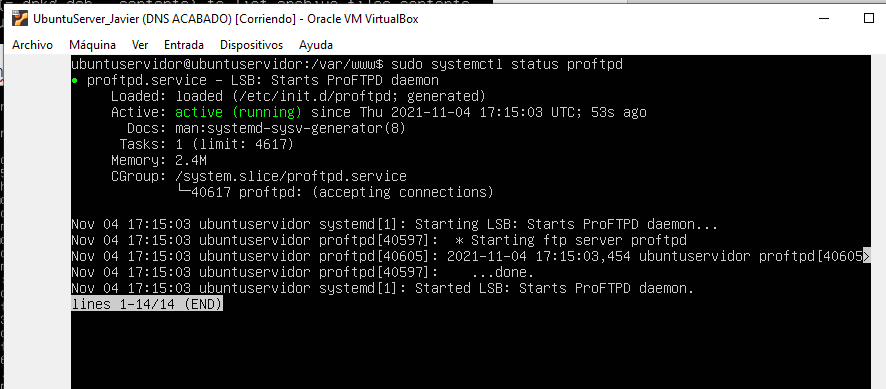
### i. Comprueba que no lo tienes instalado mediante sudo dpkg - L proftpd (si lo tienes instalado demuestra que lo tienes)



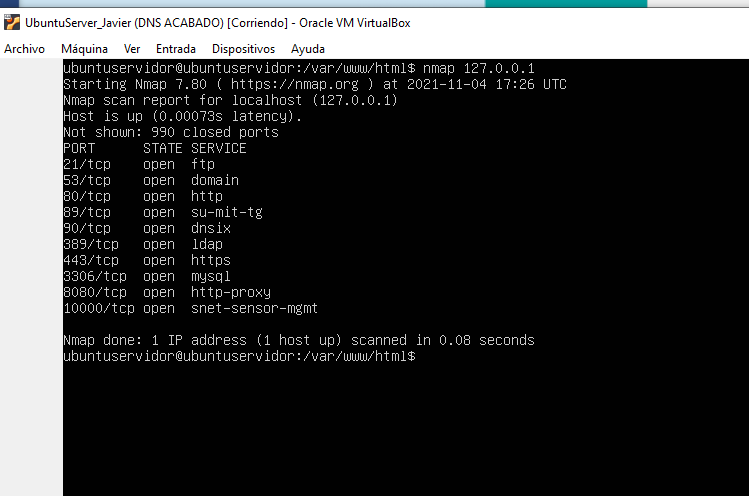
### ii. sudo apt-get install proftpd



### iii. Para, reinicia y verifica el status del servicio con systemctl stop/restart/status proftpd

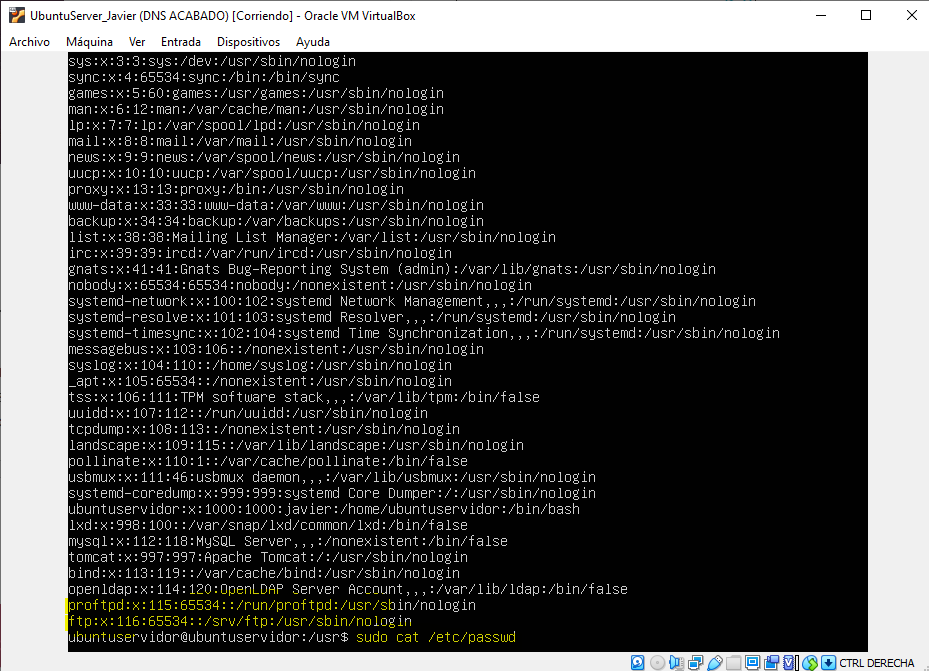


### iv. Verifica que el puerto 21 está abierto con nmap

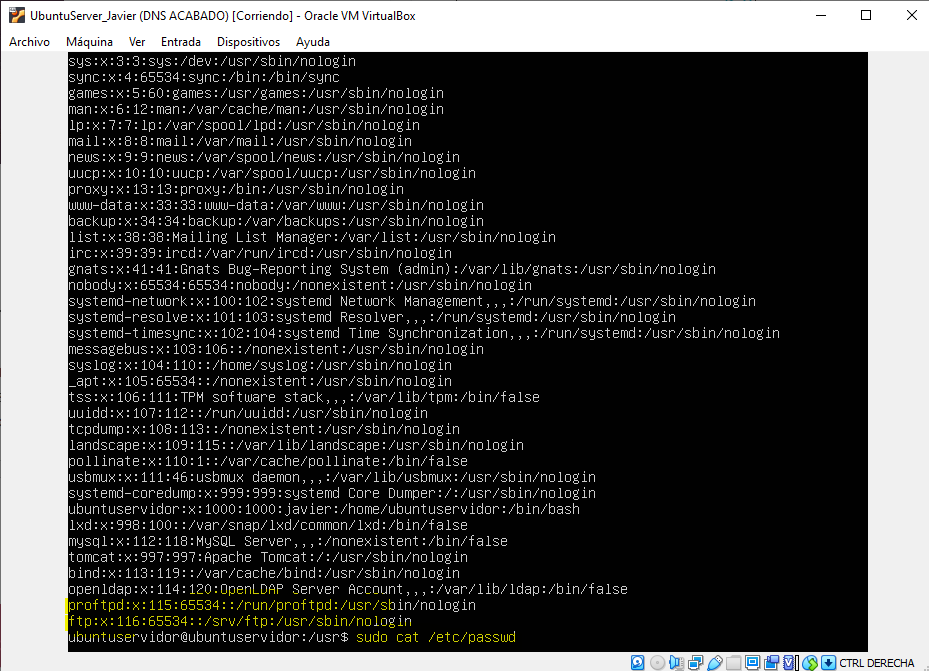


## Verifica que, tras instalar el paquete, se han generado dos nuevos usuarios: proftpd y ftp.

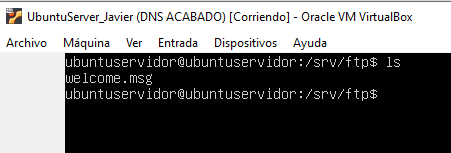
## i. El usuario proftpd es un usuario que utilizará el servicio ftp y el usuario ftp va permitir realizar conexiones anónimas por protocolo ftp pero no son usuarios para ejecutar comandos por shell en el sistema. Demuestra esto último (indaga en /etc/passwd)



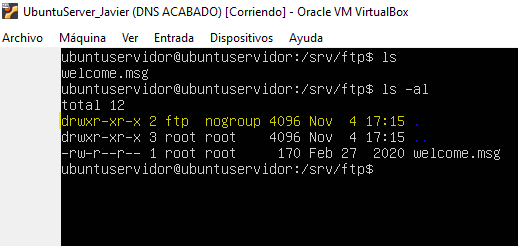
## ii. Demuestra que el directorio asociado al usuario ftp es /srv/ftp



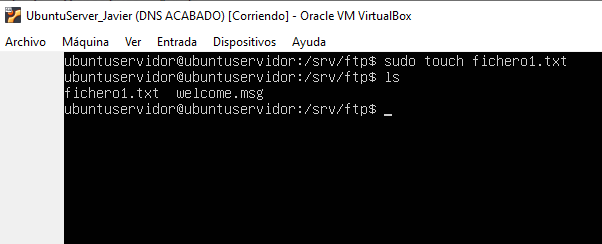
## iii. Verifica que dentro de /srv/ftp está welcome.msg



## iv. Verifica que el directorio /srv/ftp pertenece al usuario ftp y grupo nogroup (ls -al)



## v. Crea fichero1.txt en /srv/ftp

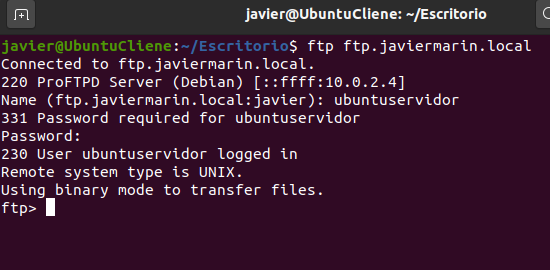


# Autenticación no anónima desde cliente ftp a protftpd:

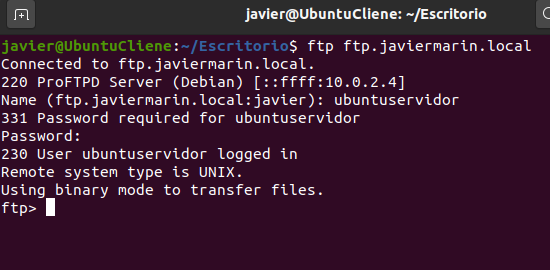
## Desde el cliente Ubuntu conéctate por la terminal al servidor ftp del Ubuntu Server mediante la entrada DNS [ftp.javiermarin.local](ftp://ftp.javiermarin.local)

### i. Auténticate con un usuario y password (administrador, por ejemplo) del servidor.

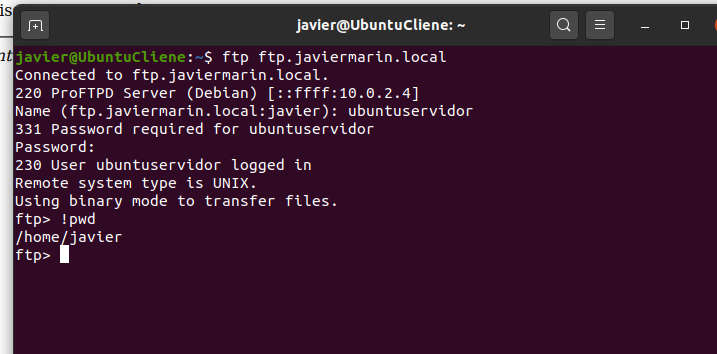
Nombre de usuario y contraseña de la maquina servidor



### ii. Verifica con pwd que ves el directorio del lado servidor

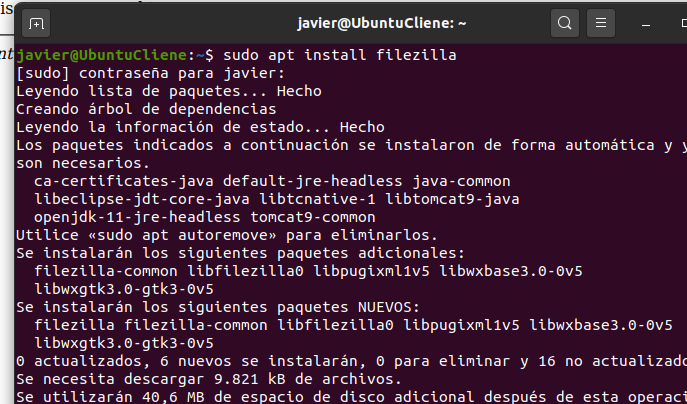


### iii. Verifica con !pwd que ves el directorio local del cliente



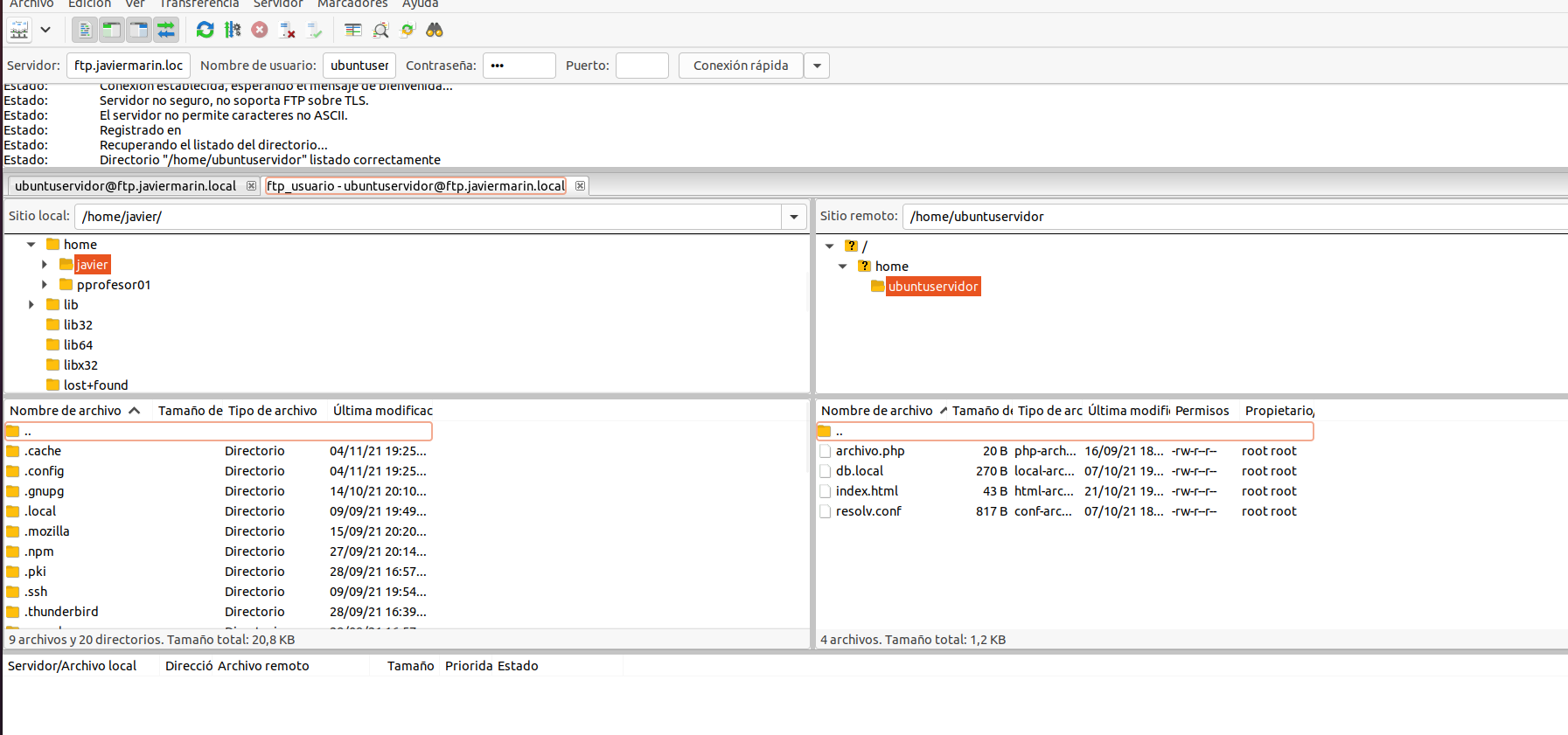
## Instala Filezilla en el cliente Ubuntu desde la terminal:

### i. sudo apt install filezilla

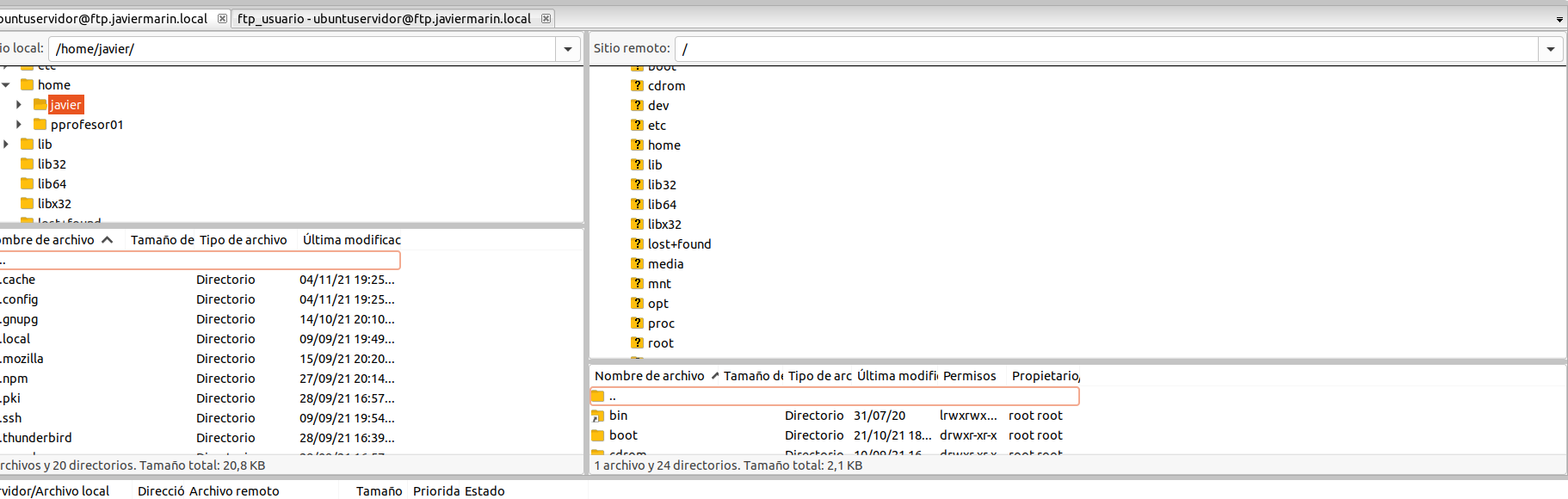


### ii. Conéctate con Filezilla al servicio ftp con el mismo usuario y contraseña de B) a.i generando un Sitio nuevo.





### iii. Verifica que en el panel derecho, sitio remoto, puedes navegar sin control por directorios superiores, con lo que ello conlleva de fallo de seguridad, una vez te has conectado.

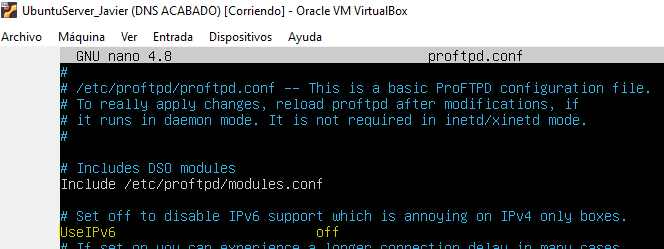


## c. Acude a /etc/proftpd en lado servidor:



### i. Edita proftpd.conf

#### 1. Deshabilita Ipv6

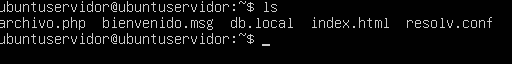


#### 2. Cambia el nombre del servidor por “Servidor FTP de javiermarin.local”

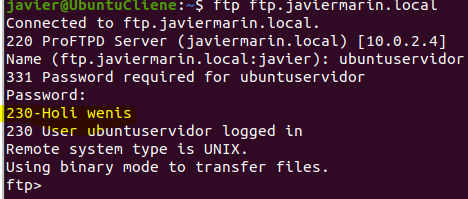


#### 3. Cambia el archivo de bienvenida por otro y dótale de contenido donde proceda. Visualízalo mediante conexión FTP por terminal (Filezilla no lo muestra).





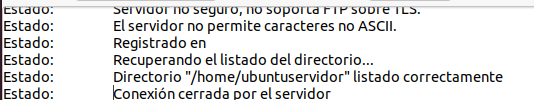
Creamos el fichero en la home del usuario y reiniciamos

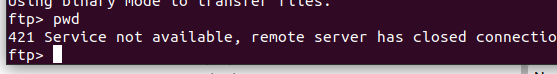


#### 4. Guarda la configuración y reinicia el servicio con restart.



#### 5. Comprueba que las dos conexiones cliente ftp se han quedado desconectadas, bien por terminal, bien por filezilla.

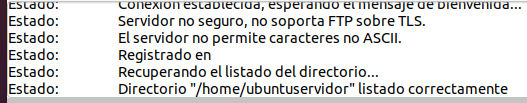




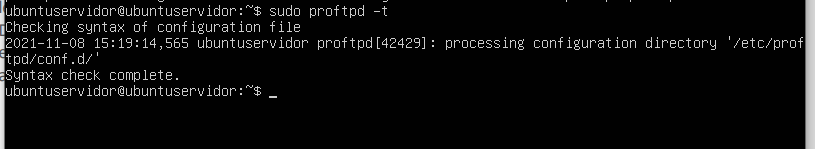
#### 6. Verifica que 5 no sucede si utilizas reload en vez de restart



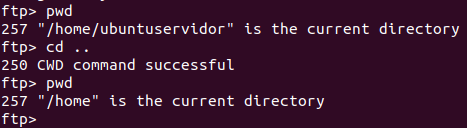




### ii. El comando proftpd -t indica si la sintaxis del archivo de configuración es correcta



## d. Verifica también desde el cliente ftp terminal que, al igual que en Filezilla, el usuario puede navegar por encima del directorio del usuario autenticado, con lo que ello supone de riesgo de seguridad.

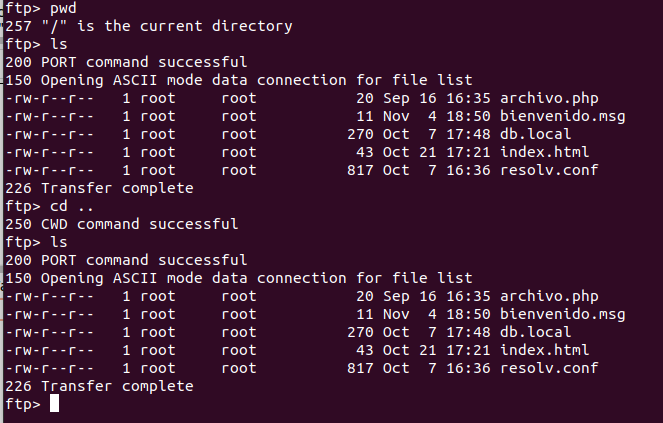


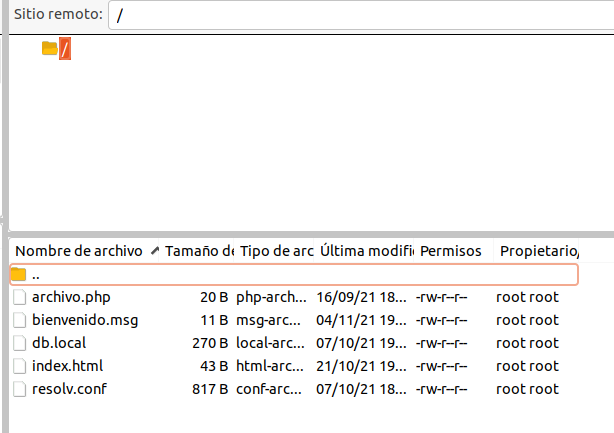
### i. Modifica ese comportamiento desconmentando la línea adecuada en proftpd.conf (investiga cuál debe ser, basta que leas los comentarios, referido a “jaula” en inglés.)



### ii. Demuestra que las conexiones ftp ya quedan encapsuladas/enjauladas en el directorio del usuario autenticado y no pueden navegar por encima.

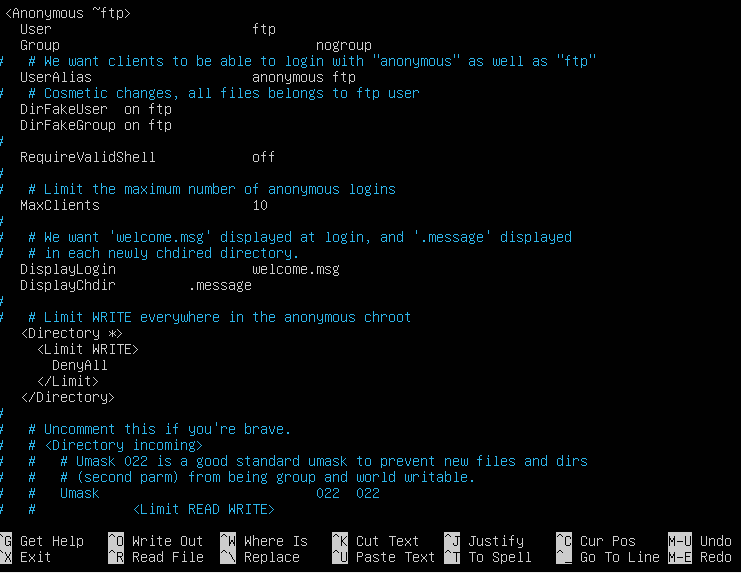


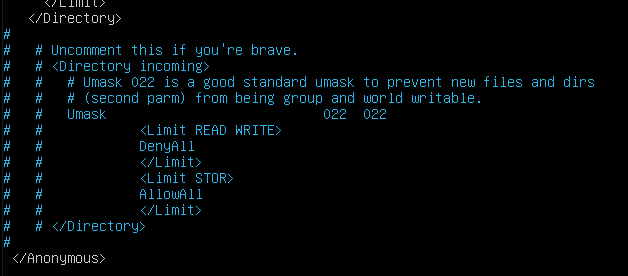




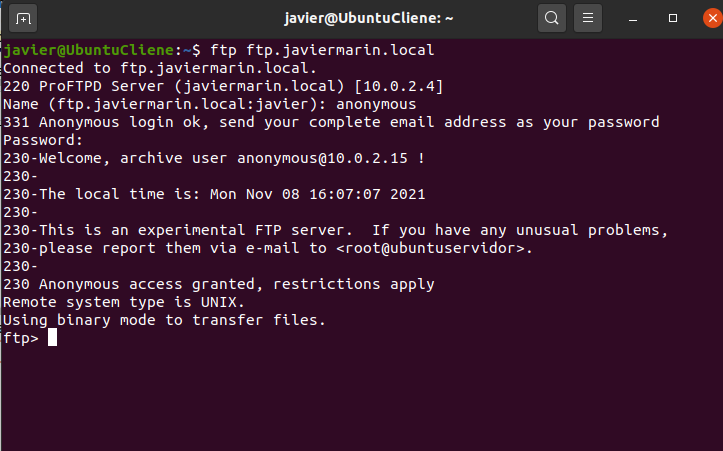
## C) Autenticación anónima:

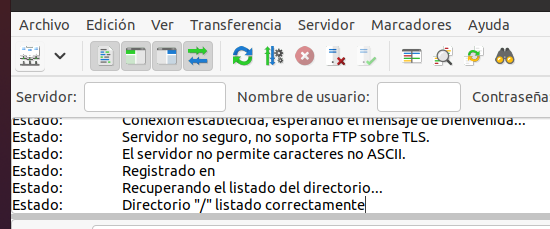
### a. Para poder acceder de forma anónima, analiza qué directivas debes habilitar en proftp.conf. No elimines los comentarios ni habilites más de lo necesario.



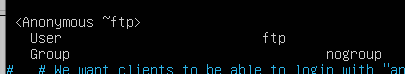




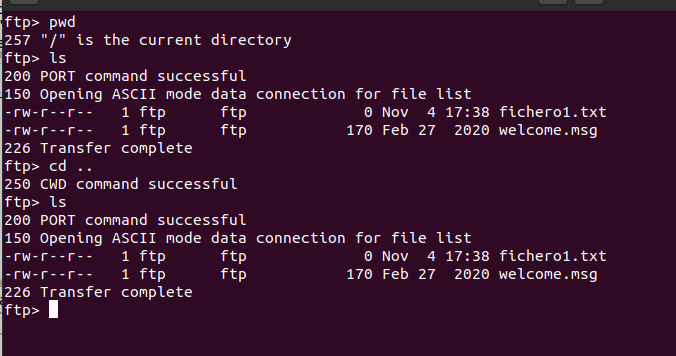




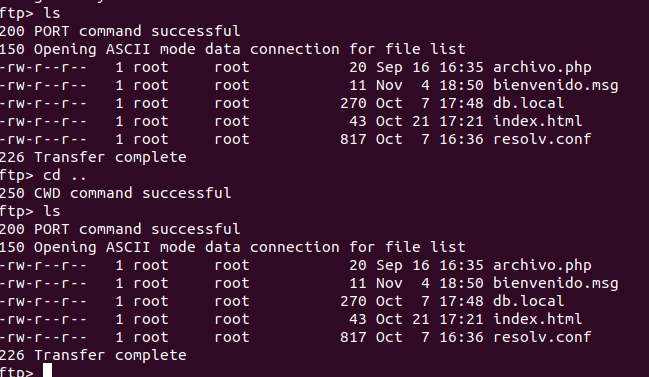
#### i. Observa que el usuario anónimo se referencia al usuario ftp del grupo nogroup.



#### ii. El usuario ftp queda encapsulado en /srv/ftp. Verifícalo accediendo con los clientes de consola y filezilla y verificando que no pueden salir de dicho directorio. (usuario anonymous ó ftp y password vacío).

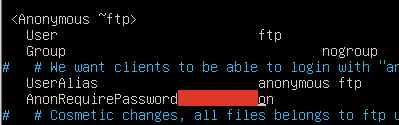


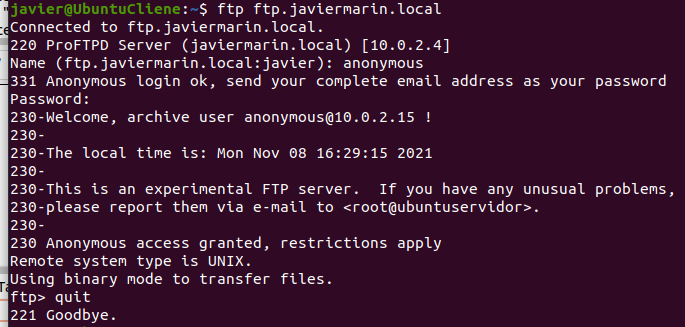
Usuario anonimo



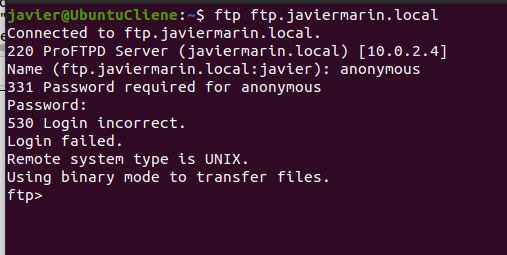
Usuario admin

#### iii. Agrega la directiva "AnonRequirePassword on" debajo de la directiva UserAlias y verifica que ahora al usuario anónimo se le solicita password. Ese password habría que aplicarlo en el archivo passwd para el usuario ftp (verifica en shadow que en efecto el usuario ftp no tiene password asociado). No le asignes password en la práctica, sólo juega con “AnonRequirePassword on” y con “AnonRequirePassword off”





Se puede entrar sin poner contraseña



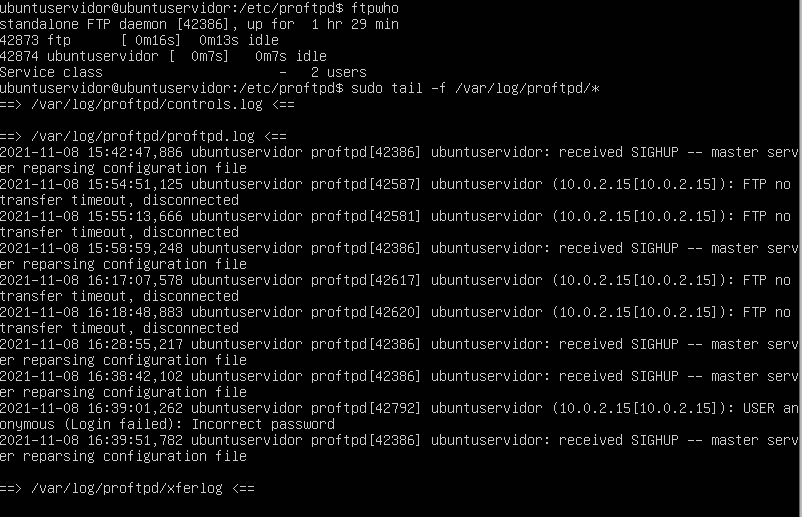
Poniéndolo en on nos pide contraseña

### b. Verifica con ftpwho en el servidor los clientes conectados que hay en cada momento y con qué usuario (con filezilla auténtica sin ser anónimo y con la consola anónimamente).



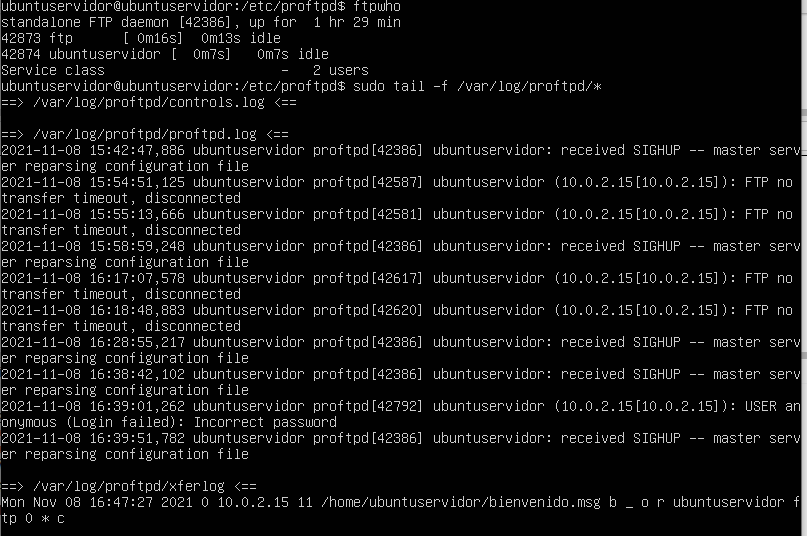
El primero es el anonimo y el otro no

### c. Para monitorizar el servicio ftp utiliza tail -f /var/log/proftpd/\*

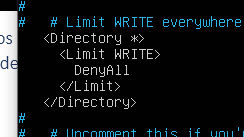


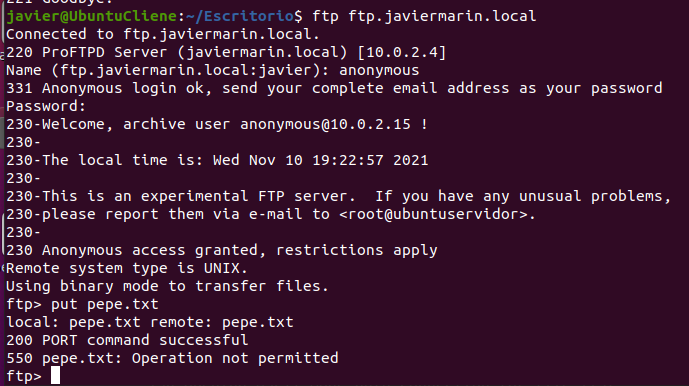
#### i. Deja abierta la monitorización

#### ii. Ejecuta acciones desde los clientes ftp y observa el registro de dichas acciones

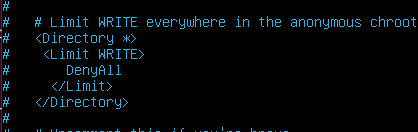


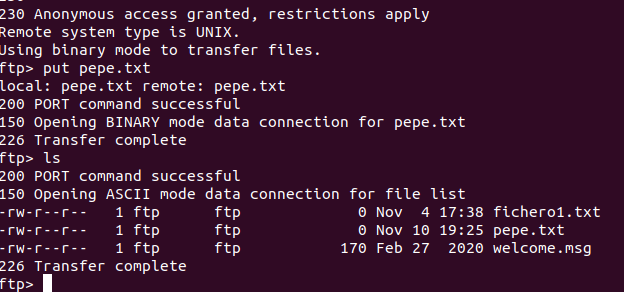
### d. En la directiva del usuario anónimo tenemos un DENYALL para escritura. Verifica que es así intentando subir un archivo al servidor desde el cliente ftp.

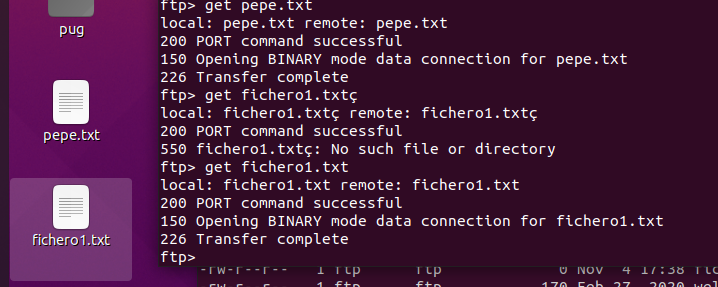




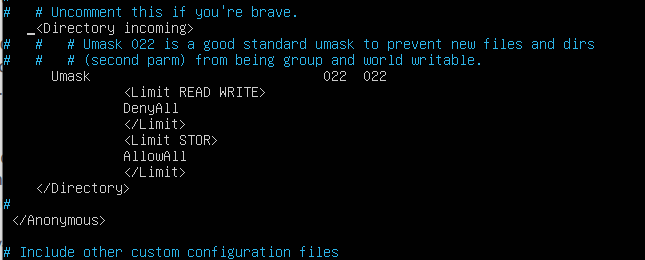
e. Si comentas toda la directiva que engloba a DENYALL verifica que ahora sí puedes subir archivos y descargarlos. Vuelve a dejarlo descomentado tras verificarlo.



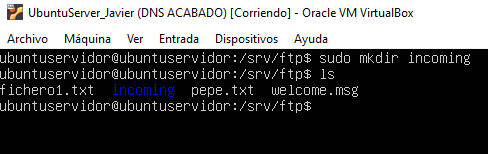




## D) En el archivo de configuración descomenta la parte “brava”. Hacerlo implica que, para el usuario anónimo, se puede permitir subir archivos (STORE) para el directorio incoming aunque no se va poder leer ni escribir pero sí almacenar archivos.



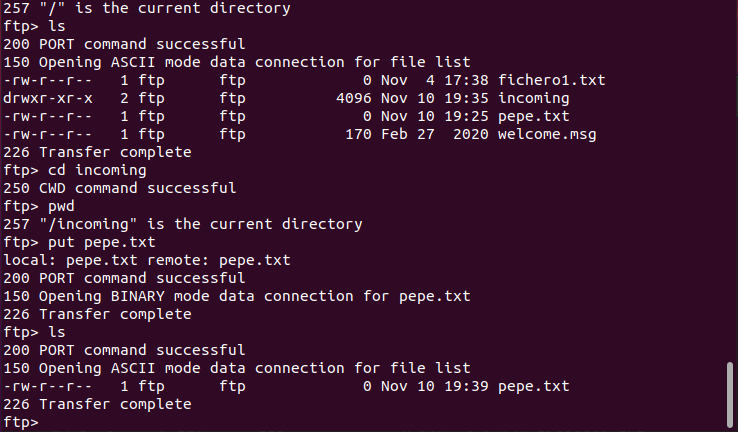
### a. En lado servidor crear en /srv/ftp el directorio incoming



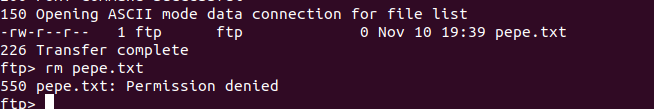
### b. chown -R ftp:nogroup incoming/ -> haremos que pase a ser parte del usuario ftp

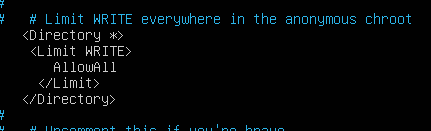


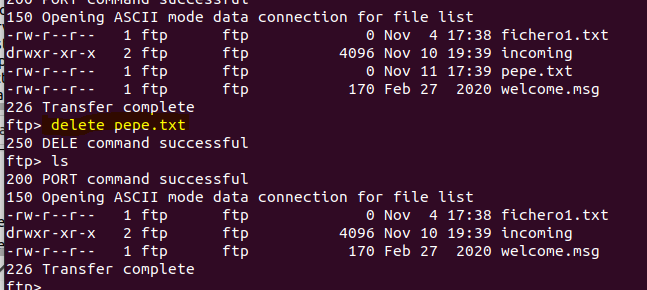
### c. Verifica que puedes usar el comando PUT con un archivo desde el cliente ftp y la operación termina con éxito. Para ello, desde lado cliente, debes estar posicionado dentro de incoming (con pwd aparecerá /incoming tras ejecutar cd incoming)



### d. Verifica que no puedes eliminar el archivo desde el cliente FTP. Después, modifica la directiva para que puedas eliminar un archivo.

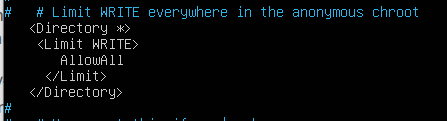






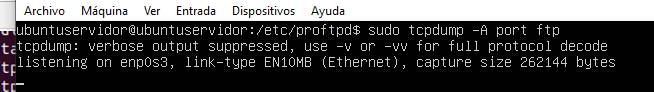
### e. Si intentas subir un archivo encima del directorio incoming, en la raíz del usuario ftp ¿qué sucede?

Me deja subir cosas debido a esta directiva descomentdada

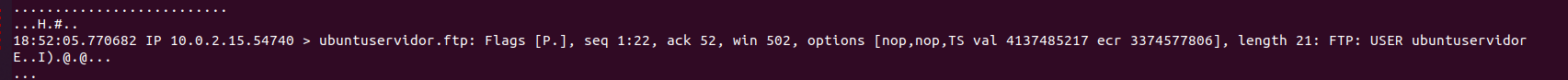


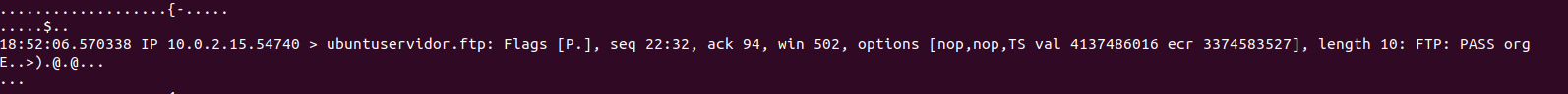
## E) Comprueba que mediante un sniffer podemos ver el usuario y contraseña del servicio ftp como datos planos:

### a. Ejecuta en lado servidor tcpdump -A port ftp



### b. Desde el cliente ftp autenticarse con usuario y contraseña y observar cómo en los paquetes se ve como texto plano el usuario y contraseña.

usuario



Contraseña

## F) Hemos visto hasta ahora que hay usuarios del sistema y usuarios anónimos. Los primeros coinciden con un usuario del sistema operativo y los segundos con un usuario. Creemos usuarios virtuales.