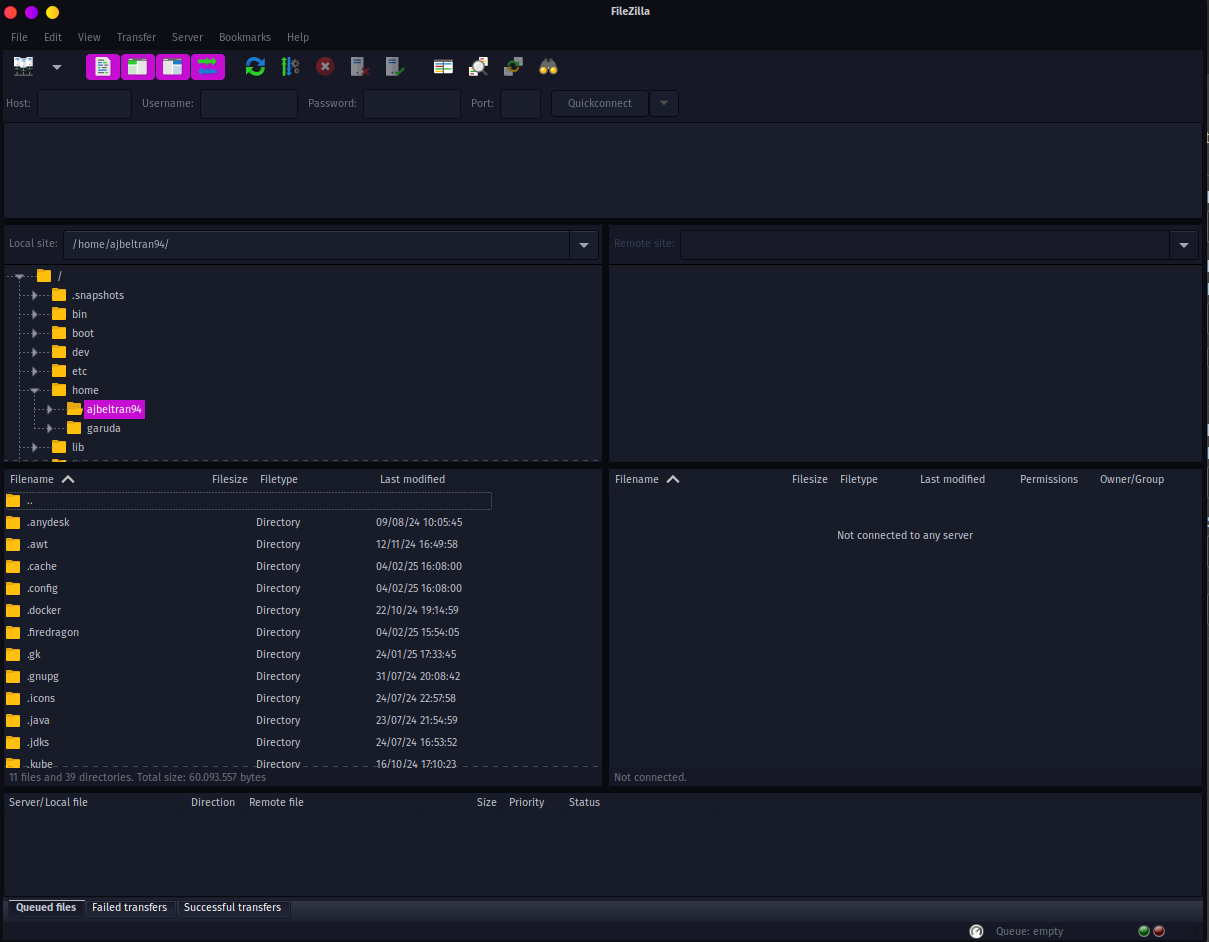
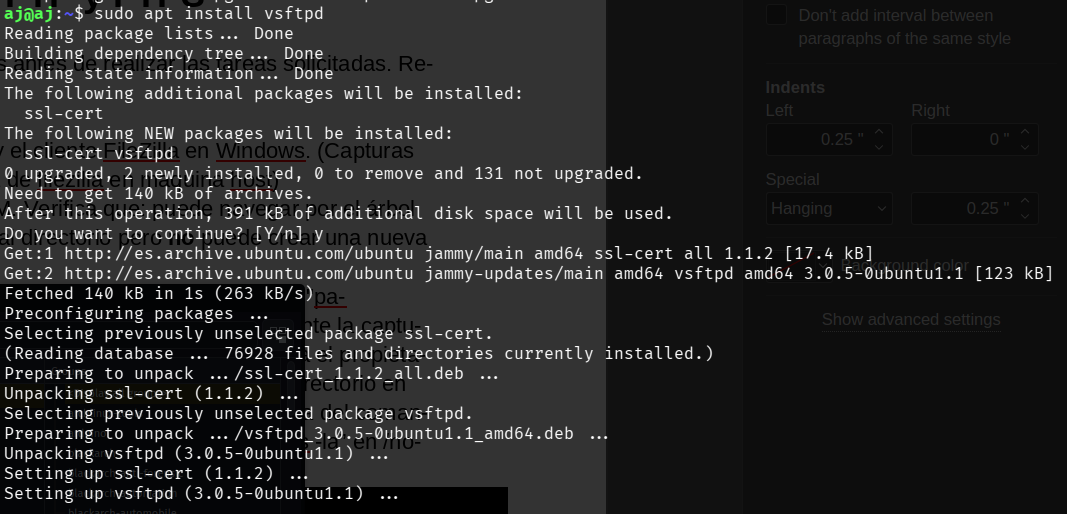
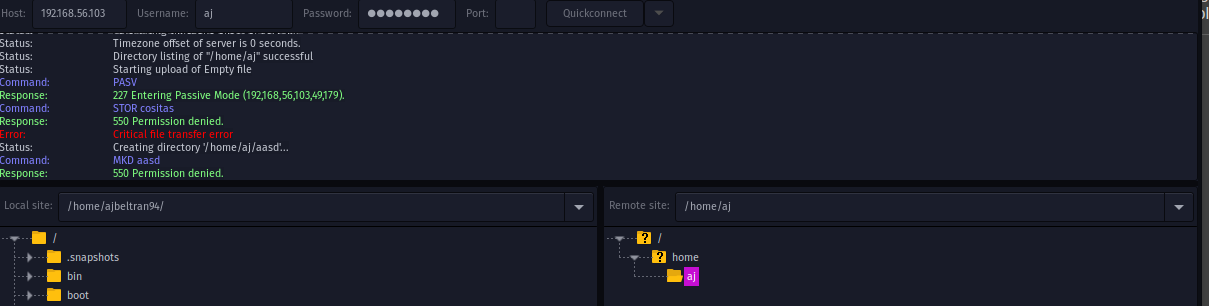
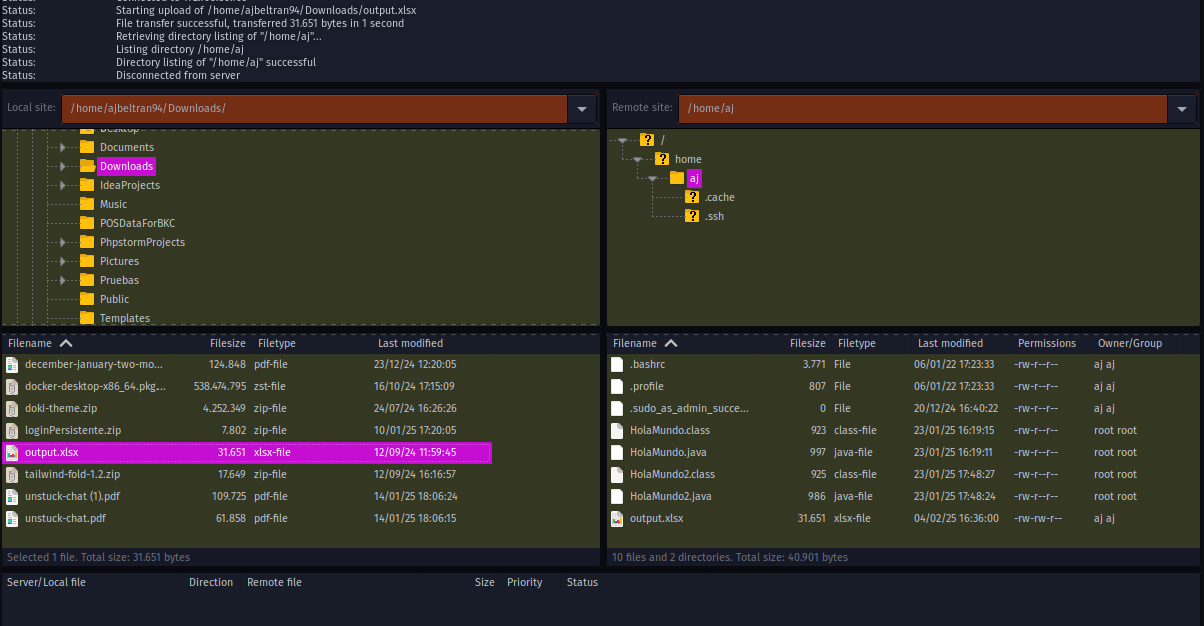
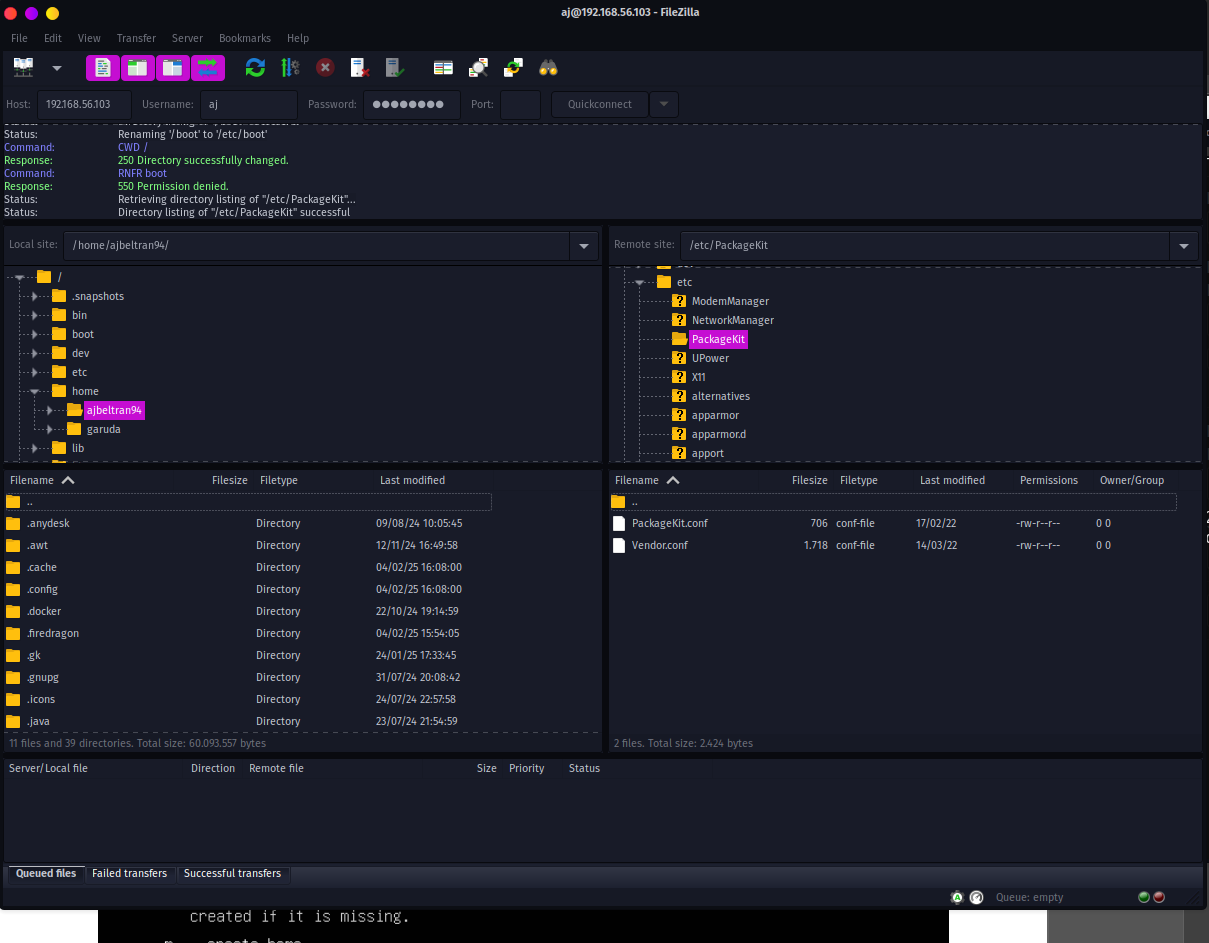
**Práctica 9. FTP y FTPS**

Lee detenidamente cada uno de los puntos antes de realizar las tareas solicitadas. Revisa los recursos incluidos.

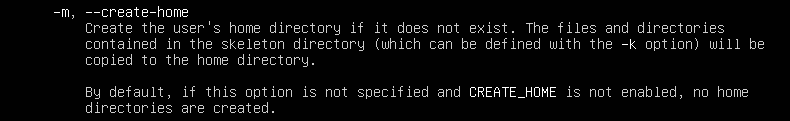
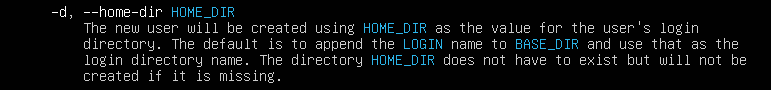
1. Instala el servidor vsftpd en la VM y el cliente FileZilla en Windows. (Capturas de sudo apt install vsftpd y ventana de filezilla en maquina host)



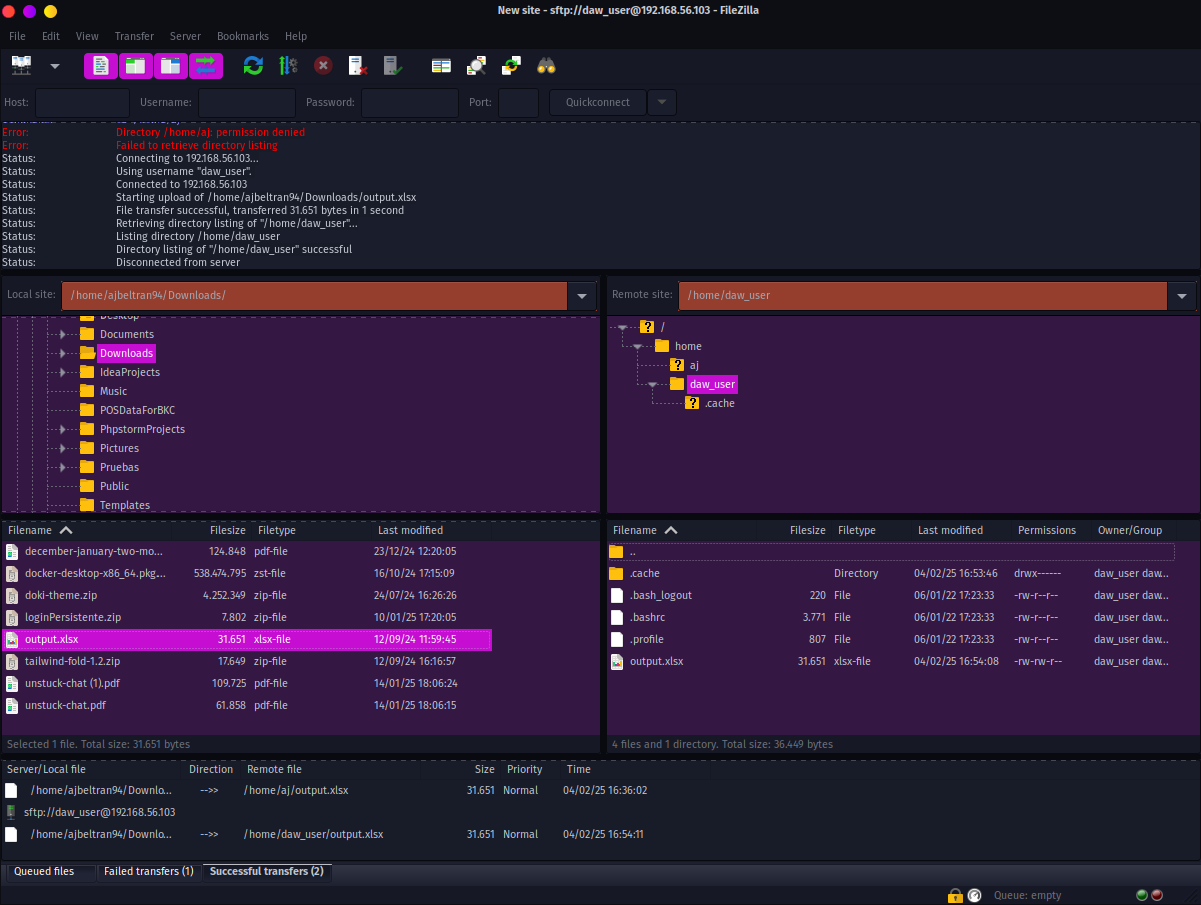
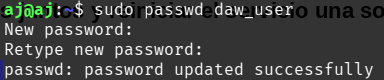
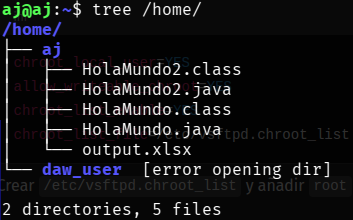
1. Accede con tu usuario root de la VM. Verifica que: puede navegar por el árbol de directorios, arrastrar un archivo al directorio pero **no** puede crear una nueva carpeta (3 capturas de FileZilla).



1. En la maquina virtual, crea un usuario "daw\_user" con contraseña "password"(no pongas una contraseña que utilices porque más adelante la capturaremos). Asígnale un directorio en /home/daw\_user para que sea el propietario y que esa carpeta sea su home. Verifica que se ha creado el directorio en /home. Utiliza el comando useradd y las opciones -d y -m. (Captura del comando “sudo useradd -d /home/daw\_user -m daw\_user”, captura de “ls -la” en /home, y captura de “sudo passwd daw\_user”)

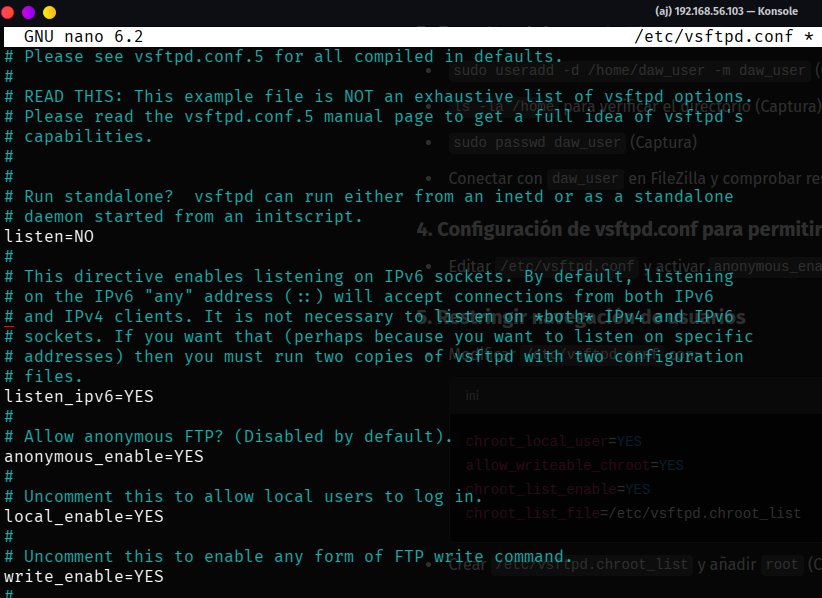


Conéctate con el usuario user\_daw al servidor mediante FileZilla. Verifica que este usuario puede navegar por el árbol de directorios pero que **no** puede arrastrar un archivo al directorio ni crear un una nueva carpeta (Capturas de FileZilla, mostrando el uso del nuevo usuario y navegación).

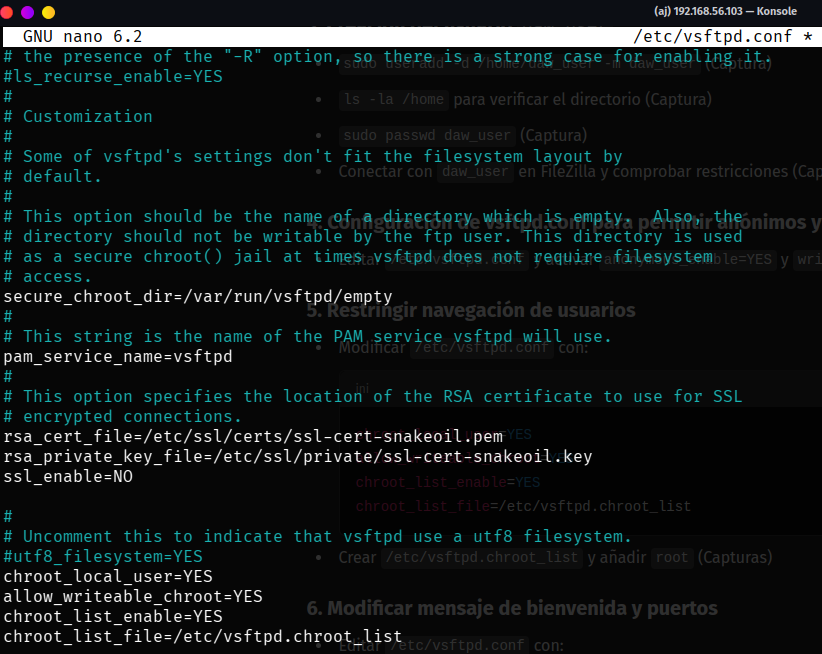


**Los pasos 4, 5, 6 puedes hacerlos juntos y reiniciar el servicio una sola vez en el paso 7.**

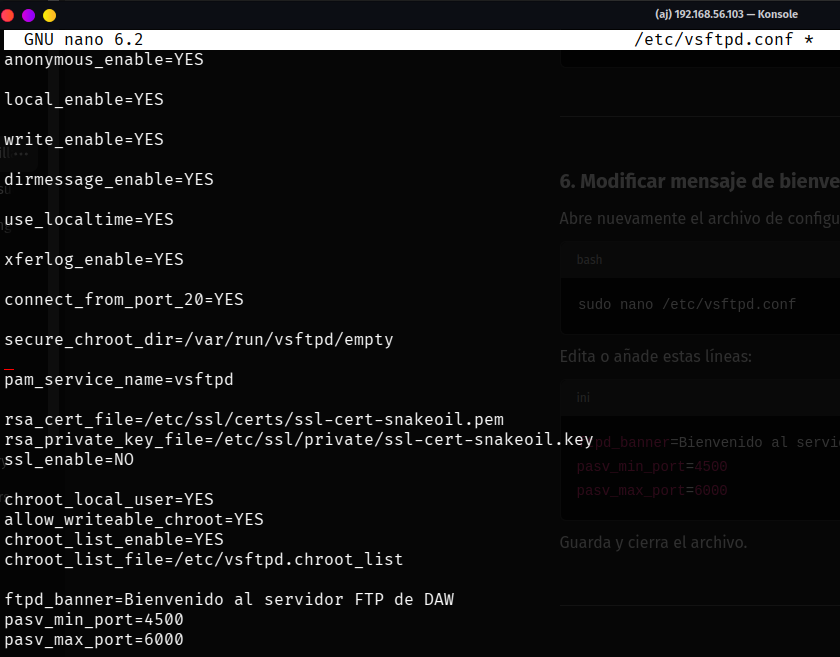
1. Modifica el archivo vsftpd.com para que puedan conectarse usuarios anónimos y los usuarios locales puedan subir ficheros. (Capturas de “sudo nano /etc/vsftpd.conf con anonymous\_enable=YES y write\_enable=YES habilitado).



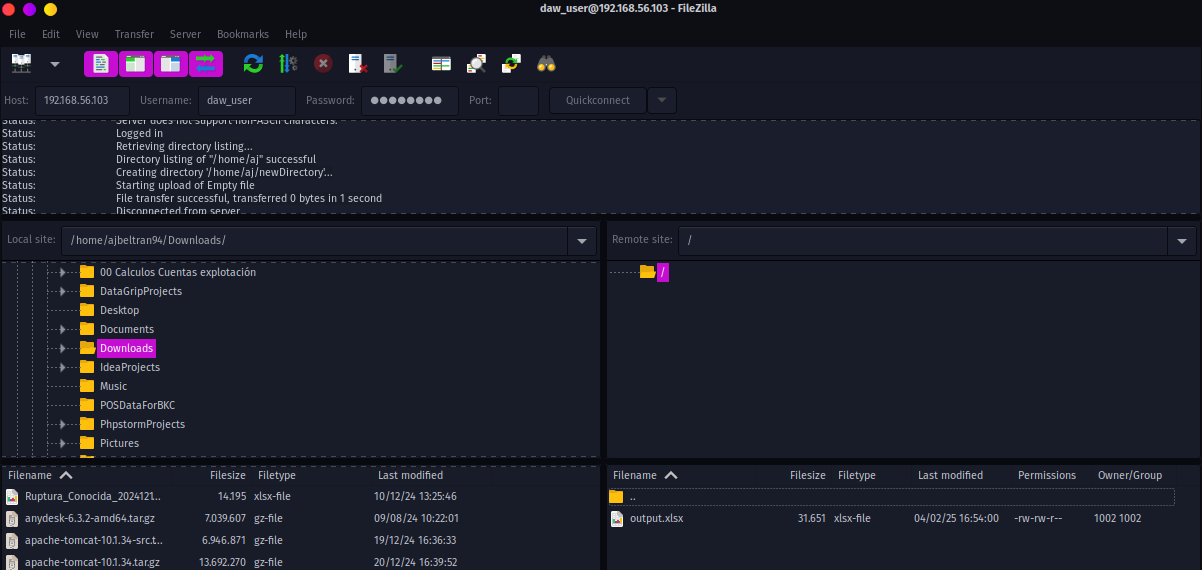
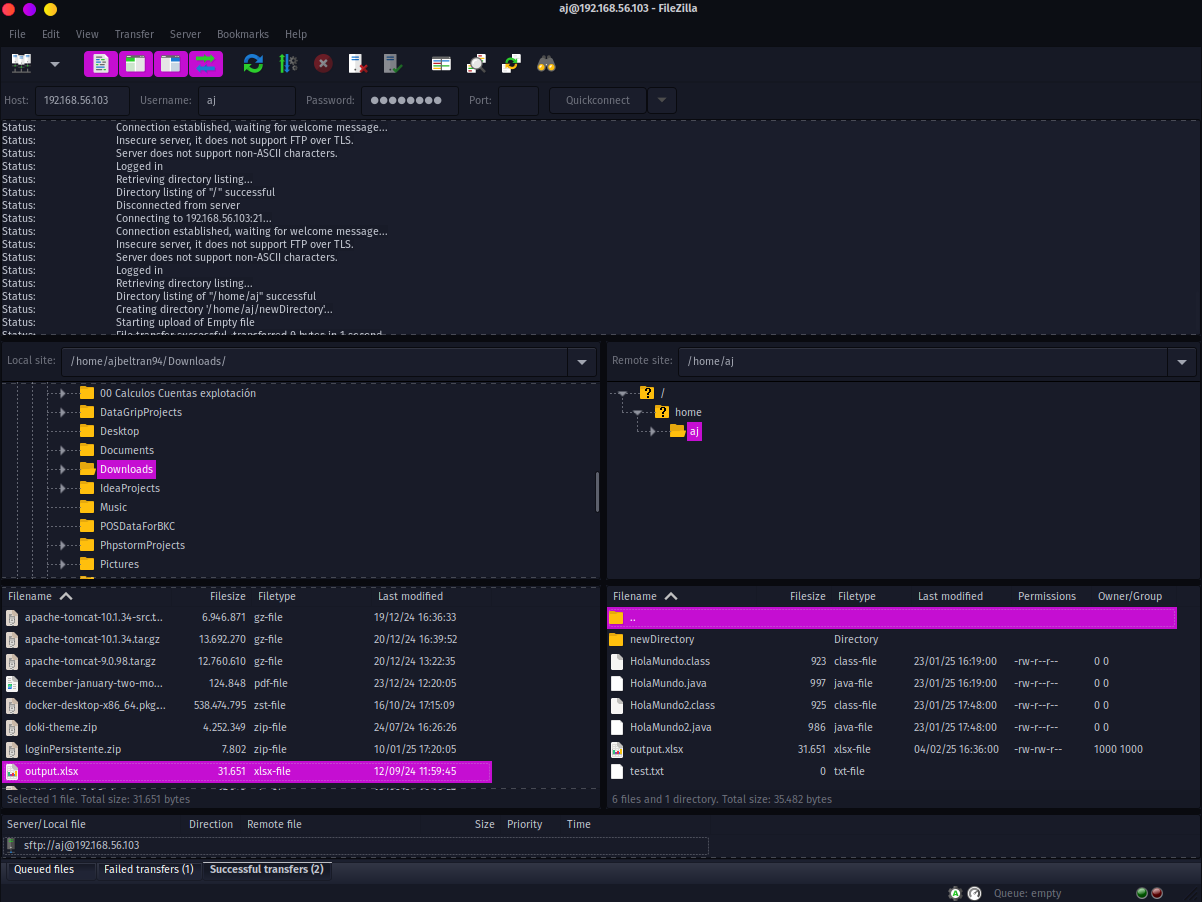
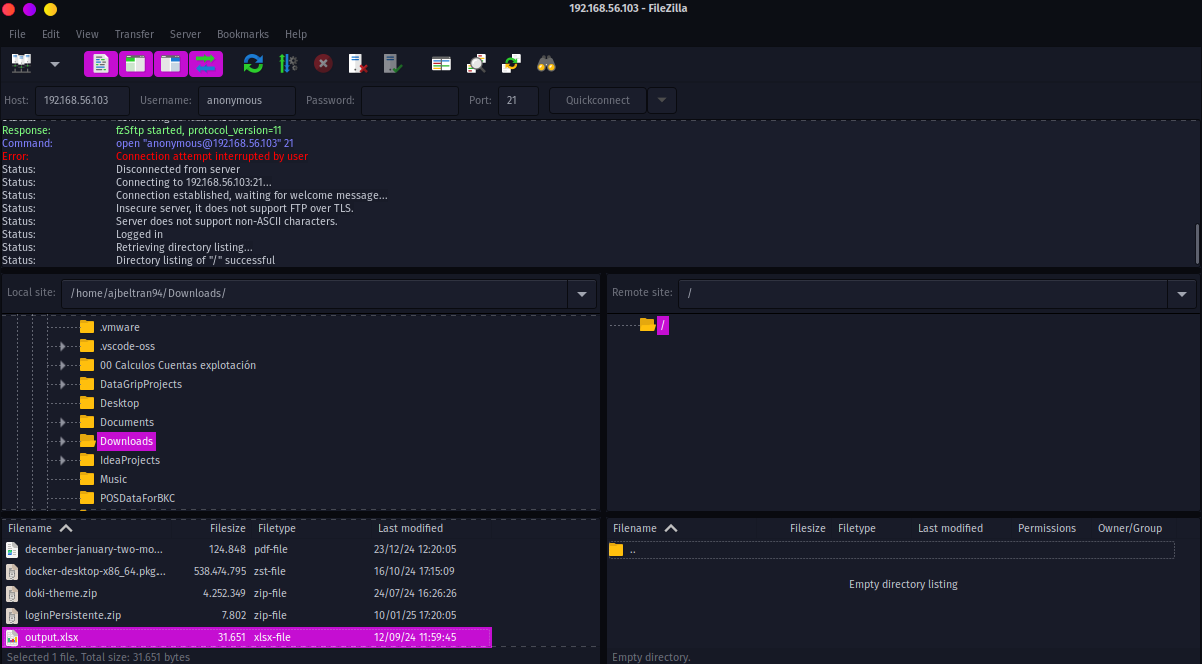
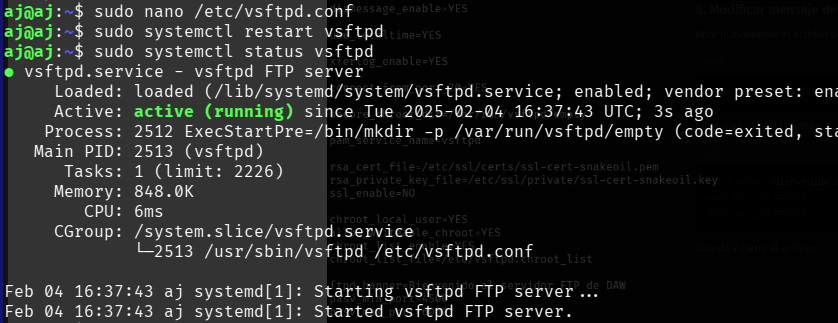
1. Modifica el archivo vsftpd.com para que los usuarios no puedan navegar por el árbol de directorios, excepto el usuario root. (Capturas de “sudo nano /etc/vsftpd.conf con chroot\_local\_user=YES, allow\_writeable\_chroot=YES, chroot\_list\_enable=YES y chroot\_list\_file=/etc/vsftpd.chroot\_list activados. Captura de sudo nano /etc/vsftpd.chroot\_list donde se ha introducido el usuario root de la maquina virtual).



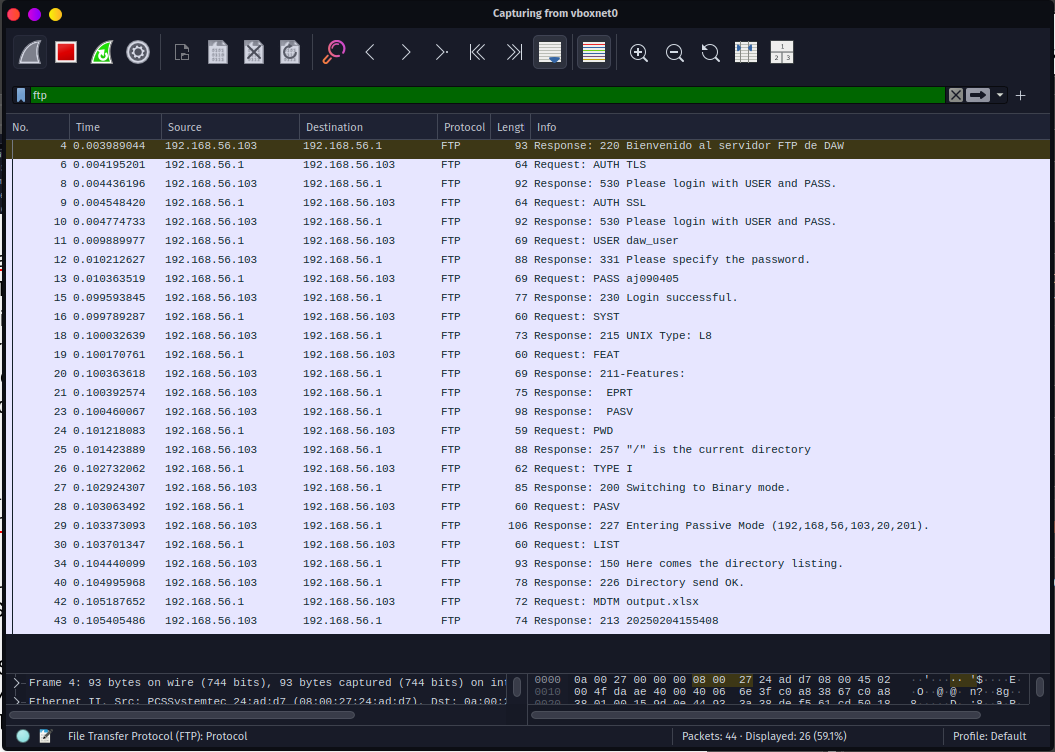
1. Modifica el mensaje de bienvenida cuando te conectas al servidor a "Bienvenido al servidor FTP de DAW" y para que use los puertos del 4500 al 6000. Guarda los cambios y reinicia el servicio. (Captura de “sudo nano /etc/vsftpd.conf con ftpd\_banner modificado y pasv\_min\_port=4500 y pasv\_max\_port=6000).



1. Reinicia el servicio del servidor (sudo service vsftpd restart) y comprueba:
   1. Se pueden conectar usuarios anónimos. (Captura de FileZilla conectado sin usuario)
   2. Los usuarios con credenciales pueden subir ficheros y crear carpetas. (Captura de FileZilla tras crear directorio con usuario root o user\_daw)
   3. Comprueba que los usuarios no pueden navegar por el árbol de directorios a excepción del usuario root (Captura FileZilla).



1. Abre Wireshark y FileZilla. Empieza a capturar datos y conéctate con el usuario “daw\_user” al servidor FTP. En el Wireshark identifica: el banner de bienvenida, las credenciales, el directorio home (current directory) y el puerto de control como la solicitud de puerto pasivo (request: PASV, response: 227 Entering Passive Mode) y verifica que está en el rango 4500-6000 (aparece en el apartado de FTP en los paquetes del protocolo FTP capturados). (Capturas de WireShark)

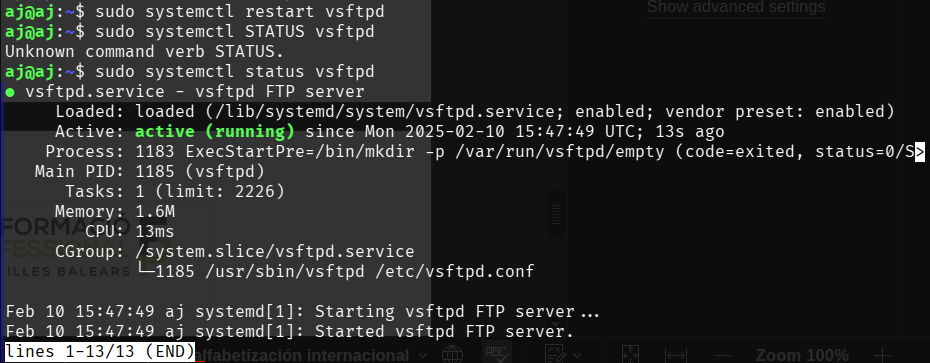
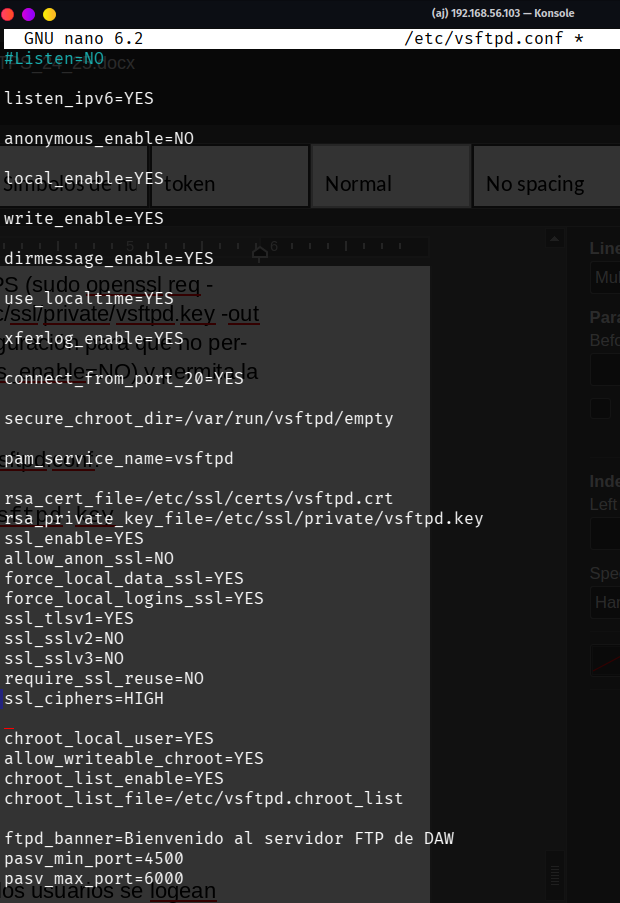


1. Crea el certificado mediante openssl para utilizar FTPS (sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.key -out /etc/ssl/certs/vsftpd.crt) y modifica el archivo de configuración para que no permita conectarse a los usuarios anónimos (anonymous\_enable=NO) y permita la conexión mediante FTPS (FTP sobre SSL).

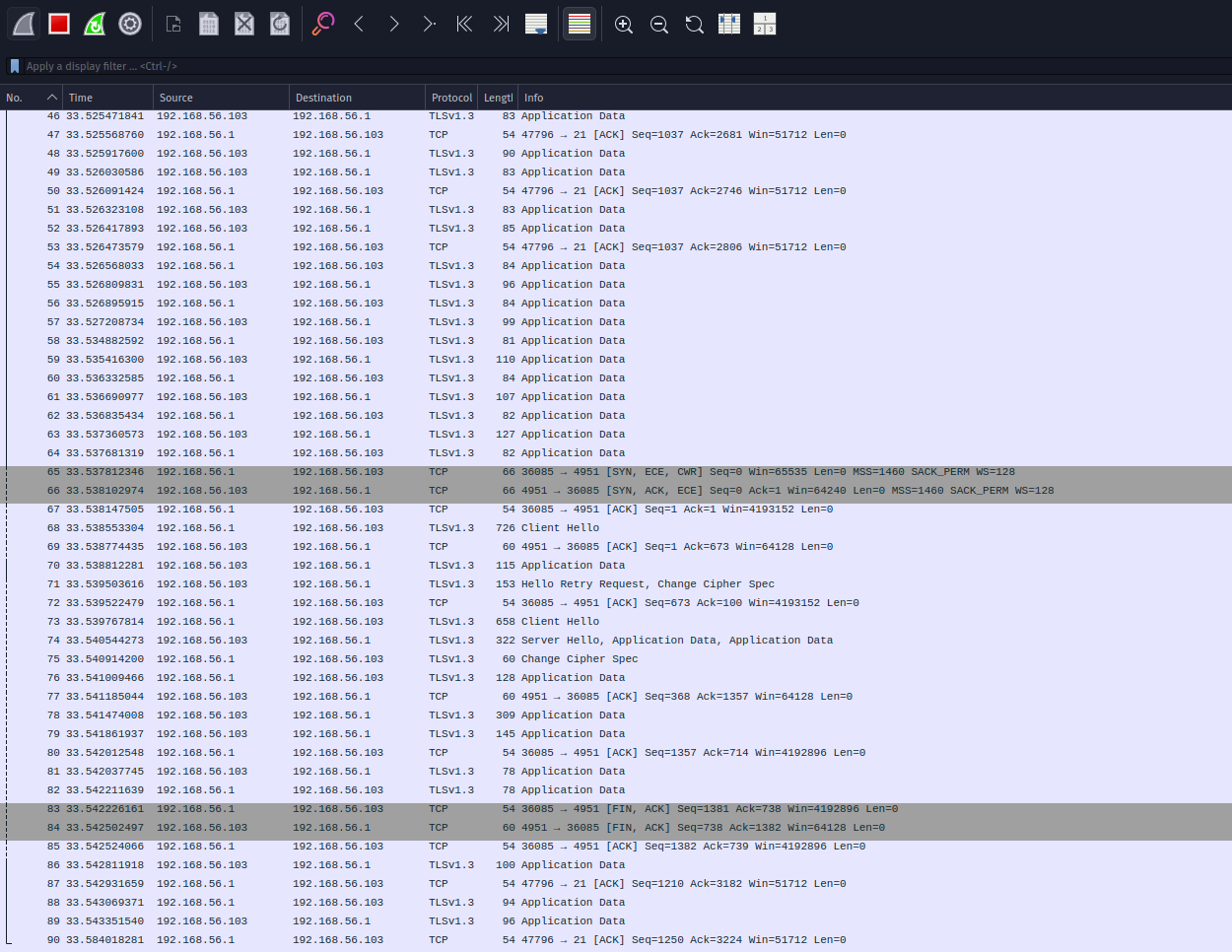
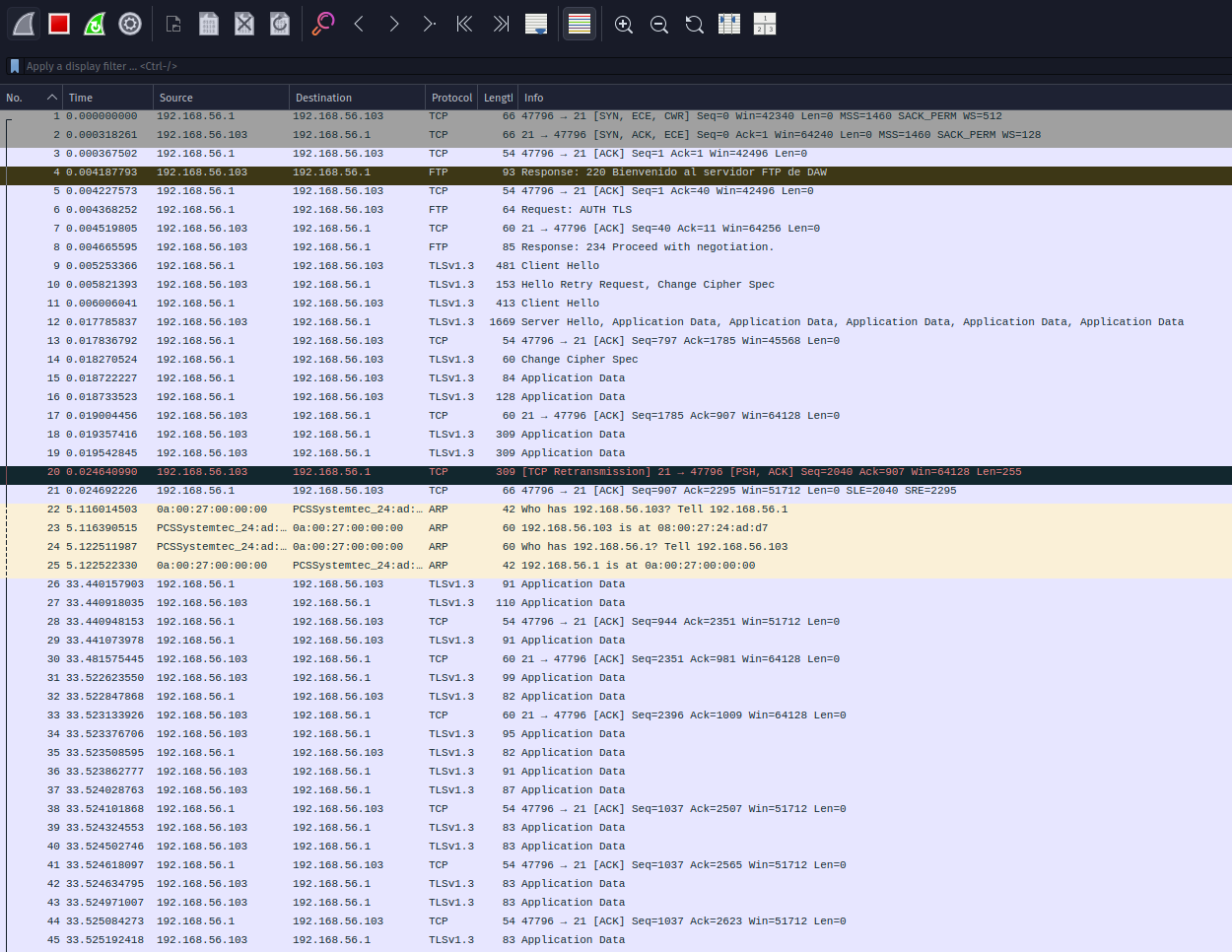
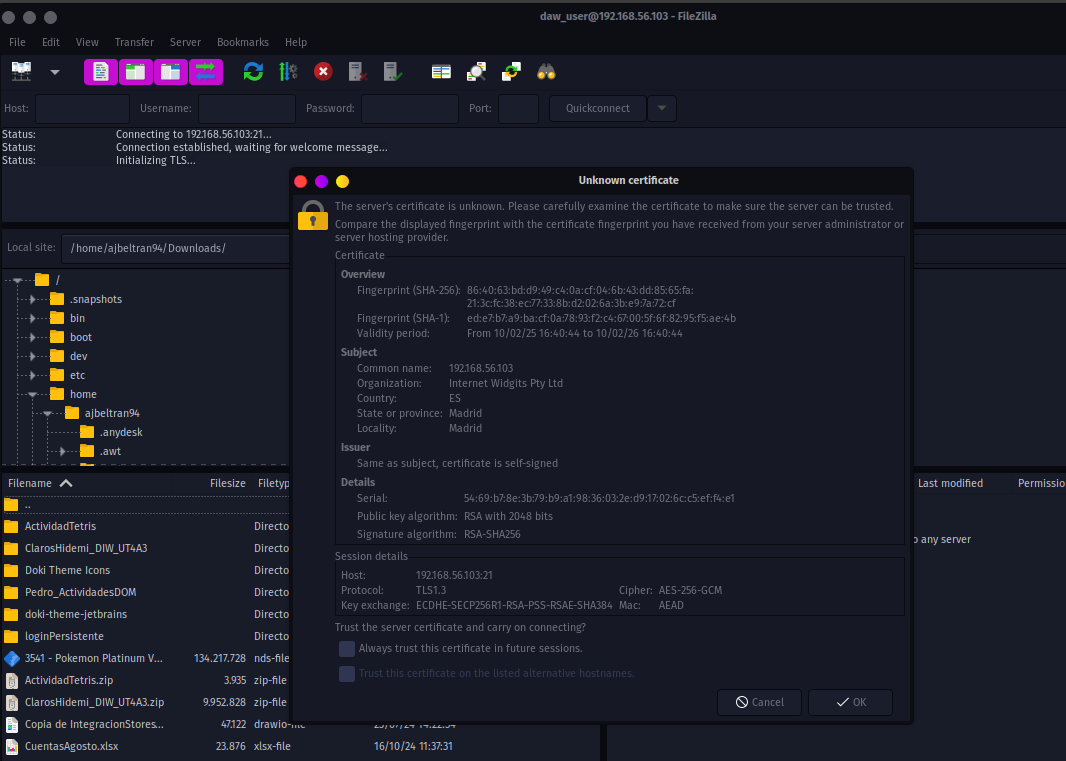
Para conectar vía TLS/SSL, se debe indicar en /etc/vsftpd.conf:

rsa\_cert\_file=/etc/ssl/certs/vsftpd.crt  
rsa\_private\_key\_file=/etc/ssl/private/vsftpd.key

ssl\_enable=YES  
allow\_anon\_ssl=NO  
force\_local\_data\_ssl=YES  
force\_local\_logins\_ssl=YES  
#ssl\_tlsv1\_1=YES  
#ssl\_tlsv1\_2=YES  
ssl\_tlsv1=YES  
ssl\_sslv2=NO  
ssl\_sslv3=NO  
require\_ssl\_reuse=NO  
ssl\_ciphers=HIGH



1. Vuelve a capturar tráfico en Wireshark y verifica que los usuarios se logean mediante FTPS (Captura de Request: AUTH TLS y Response: 234 Proceed with negotiation por parte de protocolo FTP, Captura de FileZilla estableciendo conexión con TLS), muestra el tráfico en Wireshark con las credenciales encriptadas.



**Recursos:**

* <https://www.liquidweb.com/kb/configure-vsftpd-ssl/>
* <https://docs.rockylinux.org/guides/file_sharing/secure_ftp_server_vsftpd/>
* (ampliada) [https://docs.redhat.com/en/documentation/red\_hat\_enterprise\_linux/6/html/deployment\_guide/s2-ftp-servers-vsftpd#s2-ftp-servers-vsftpd](https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/6/html/deployment_guide/s2-ftp-servers-vsftpd" \l "s2-ftp-servers-vsftpd)
* <https://wiki.filezilla-project.org/Documentation>

**Recordatorio:**

* FTP = File Transfer Protocol.
* FTPS = FTP con cifrado SSL/TLS.
* SFTP = Transferencia de archivos sobre SSH.

FTPS y SFTP son seguros, pero son diferentes en implementación y uso.

**Condiciones de entrega:**

* La práctica se **debe** entregar de forma **individual**, cada uno debe presentar sus propias respuestas. Sin embargo, se puede trabajar en equipo.
* Se debe entregar un documento de texto (.pdf, .docx, .odt, etc.) con los ejercicios correctamente ordenados, identificados y **numerados**.
* En cada página del documento debe aparecer el nombre completo del alumno.
* La nota comprenderá un valor numérico entre 0 y 10.
* **La fecha límite de entrega es la indicada en Google Classroom.**
* **Se podrá entregar hasta 72 horas más tarde de la fecha límite pero con una penalización sobre su puntuación (no será posible aspirar al 10).**