Servicios de Red e Internet – ASIR2

**Práctica 6: Servicio FTP**

| Módulo profesional: Servicios de Red e Internet  Ciclo Formativo: C.F.G.S. Administración de Sistemas Informáticos en Red Curso: 2º  Profesor: Anabel Serradilla Fernández |
| --- |

| Esta práctica se realizará en grupos de dos personas.  Todos los pasos deben ser documentados mediante capturas de pantalla y/o explicaciones que se incluirán en la entrega.  Esta práctica se corregirá en clase. La plantilla para la corrección se puede encontrar al final del enunciado. |
| --- |

**Alumno1 : Marco Batista Calado**

**Alumno2 : Enrique González de Anleo Aliaga**

**A. Actividades iniciales**

1. Un sitio FTP tiene la dirección “ftp.anabelclases.es”. En vez de utilizar el puerto 21 como sería habitual, emplea el puerto 1502 en el servidor para el canal de comandos. Uno de los usuarios es “bosco” con clave “asir2asir”. Indica la URL completa que incluya todos los datos para realizar una conexión a este servidor FTP.

**ftp://bosco:asir2asir@fpt.anabelclases.es.1502**

2. Un servidor FTP instalado sobre un servidor Windows:

- Permite conectarse a los clientes con su usuario y contraseña.

- Pero no es posible listar o descargar ningún fichero.

Se sabe que se está utilizando modo pasivo.

¿Cuál es probablemente el problema? ¿Cómo podría solucionarse?

**LA CONEXIÓN BIEN**

**LA TRANSFERENCIA DE DATOS→ CUANDO UN PUERTO EXTERNO SE COMUNICA CON EL SERVIDOR OBVIAMENTE NO SE VA A FIAR (FIREWALL), POR TANTO HAY QUE CREAR UNA REGLA DE ENTRADA.**

[Exacto. Mientras no haya regla de entrada abierta en el firewall, la conexión se establecerá pero no se transmitirá ningún dato, ni siquiera se listará el contenido del directorio en el que se conecta.]

3. Indica brevemente el problema que supondría utilizar siempre FTP en modo activo en Internet.

**Pones fácil que te ataquen ya que siempre va a ser la comunicación a través del puerto 20. En cambio en modo pasivo como cambia no hay problema.**

**[también que habría que abrir puertos en el cliente.]**

4. Indica qué puertos en entrada deben abrirse en un cortafuegos y/o redirigirse en routers NAT para que funcione el servicio FTP en estos casos:

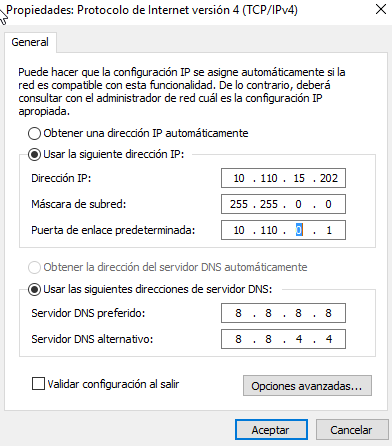
| **FTP ACTIVO** | |
| --- | --- |
| **Puertos Cliente** | **Puertos Servidor** |
| **Puerto específico > 1024** | **21** |
| **Puerto específico > 1024** | **20** |

| **FTP PASIVO** | |
| --- | --- |
| **Puertos Cliente** | **Puertos Servidor** |
| **na** | **21** |
| **na** | **RANGO PUERTOS ESPECÍFICOS** |

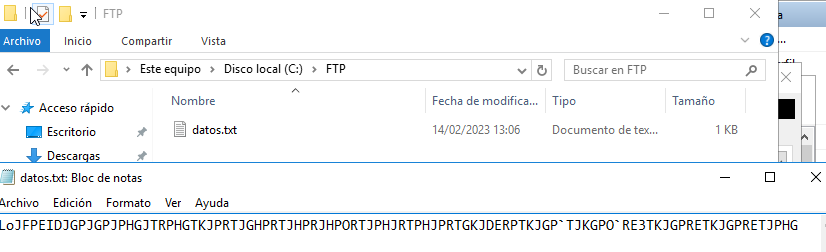
**B. Servidor FTP seguro con Filezilla Server sobre Windows**

**5. Instalación de Filezilla server y creación de un sitio FTP básico**

a) Devuelve tu m. v. Windows 2016 Server a la “Snapshot Base” y asígnale una IP fija de tu rango de direcciones IP. Sobre esa m. v. instala el servidor Filezilla Server.



b) En el servidor, crea una carpeta en C:/ llamada “FTP”. Copia en ella un archivo llamado “datos.txt” que tenga un tamaño de al menos 1 KB.



c) Configura el servidor Filezilla Server de forma que éste permita acceder con

permisos totales a la carpeta C:/FTP a un usuario llamado “ftpwinasir” con

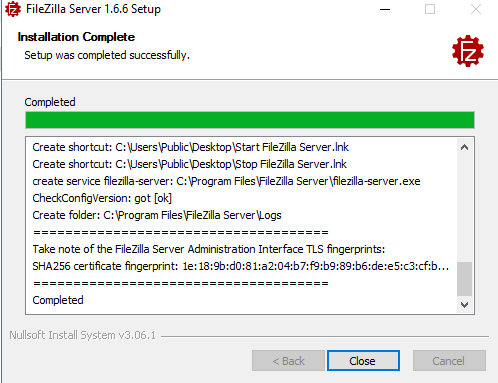
contraseña “2seguro2”. El servidor debe ser seguro (“FTP sobre TLS explícito”).

**WIN+R = iexplore**

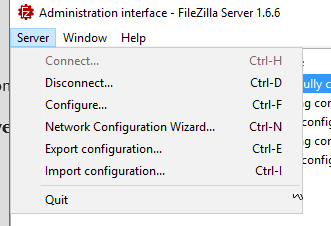
**download filezilla server**

[**https://youtu.be/dPPOrPTGFcw**](https://youtu.be/dPPOrPTGFcw)

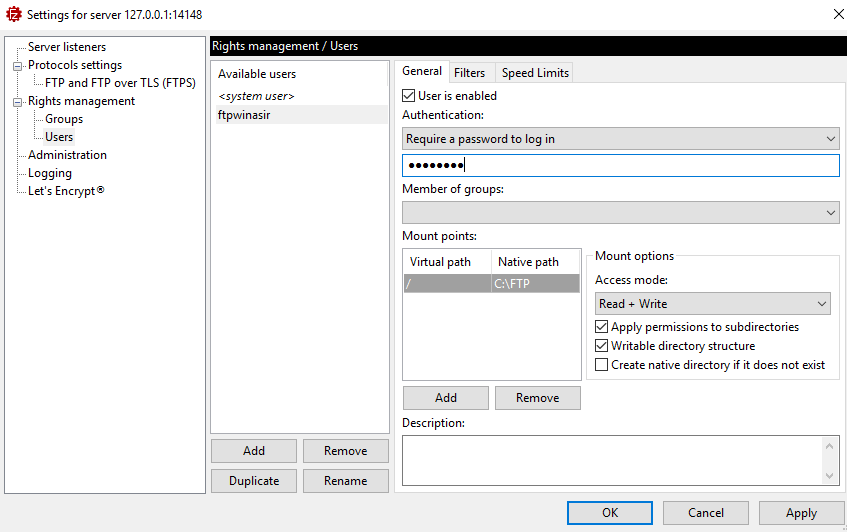
**Toda la instalación: aceptar.**

****

**Abrimos, connect server, aceptar el por defecto.**

** Configure**

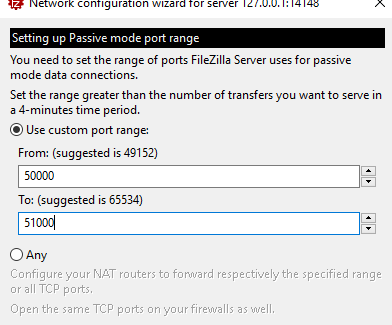
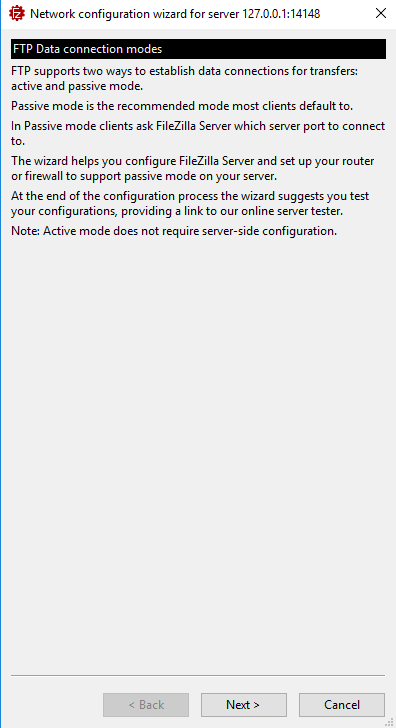
**Add, nombre y en authentication la contraseña.**

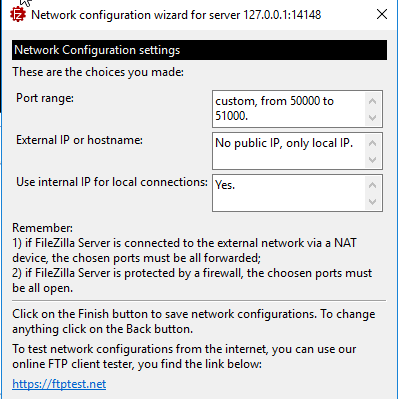
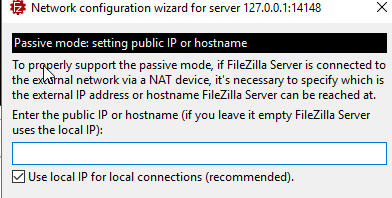
****

****

d) Configura el servidor FTP de forma que los puertos para utilizar en el canal de datos en modo pasivo sean del 50.000 al 51.000.







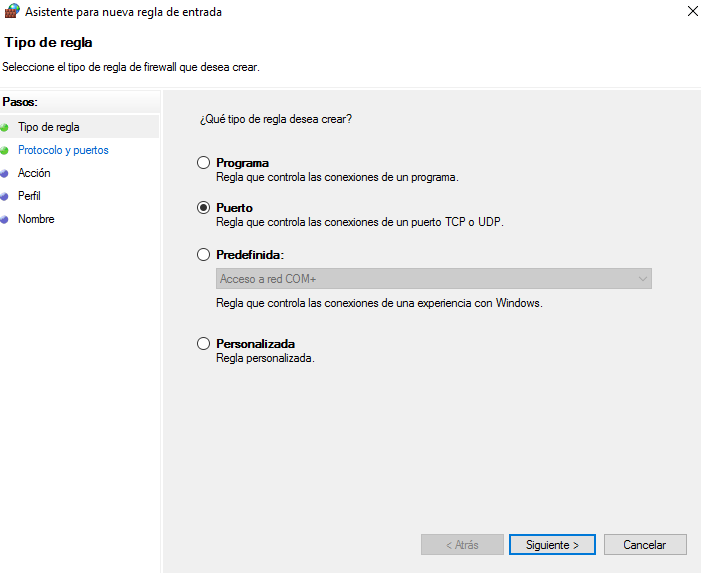
e) Configura el cortafuegos del servidor para que permita el acceso al sitio FTP. Debes utilizar la **máxima restricción** posible, pero que garantice que el servicio FTP

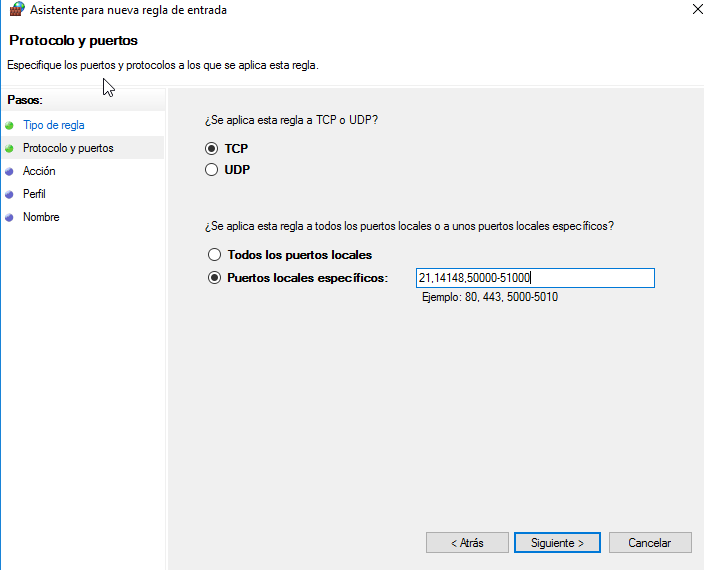
funcionará correctamente.

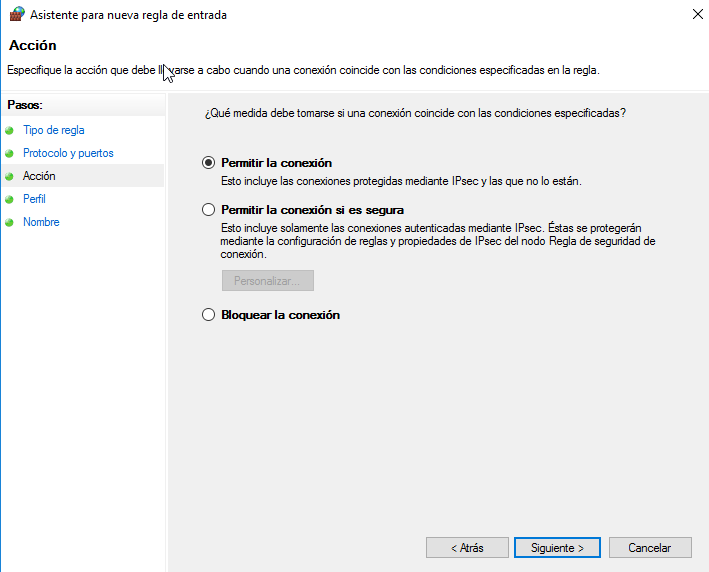


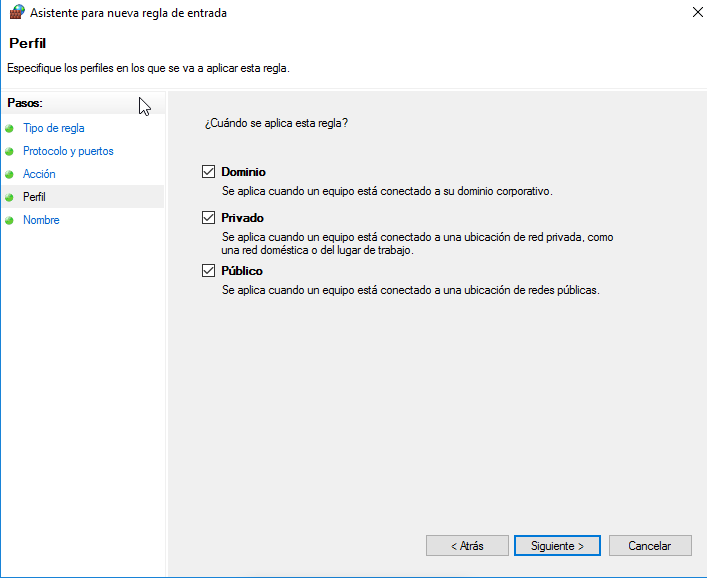


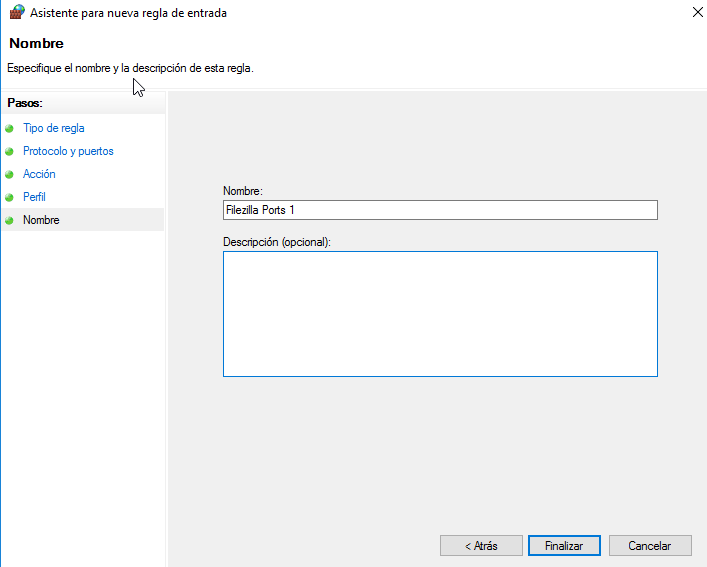




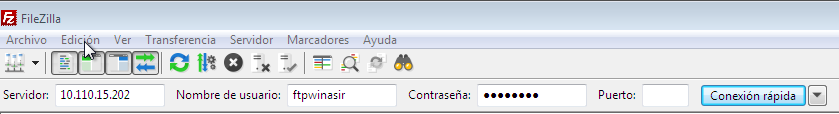


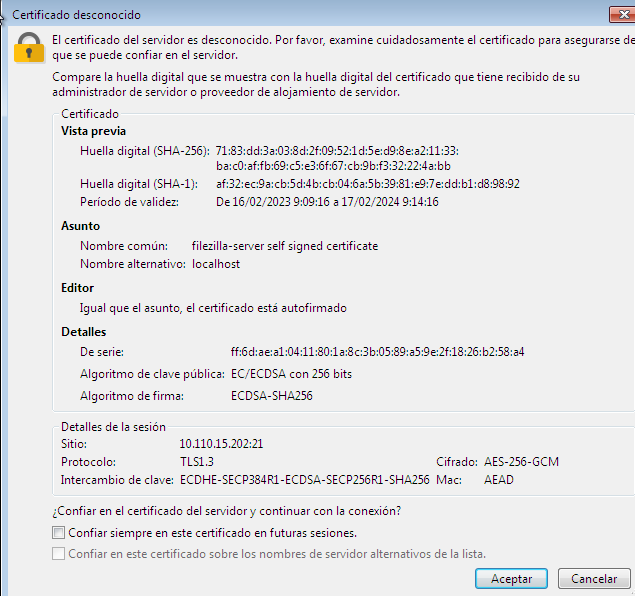




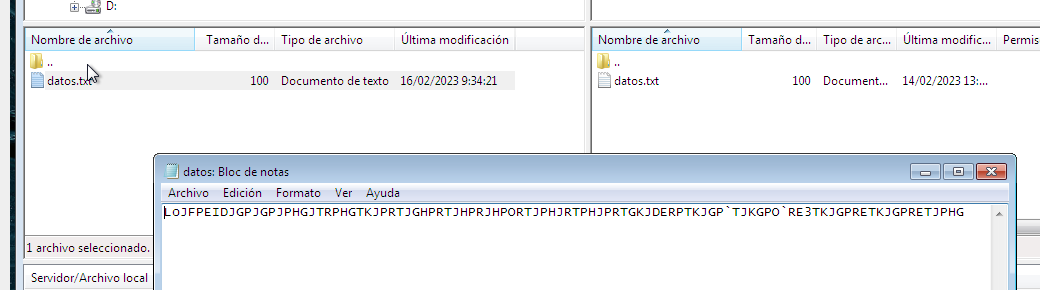


f) Desde otra máquina (física o virtual a libre elección) que llamaremos "Cliente", accede mediante el cliente FTP "Filezilla client" al FTP que acabas de configurar y descarga el fichero "datos.txt". Comprueba que el contenido del fichero es correcto en el cliente.





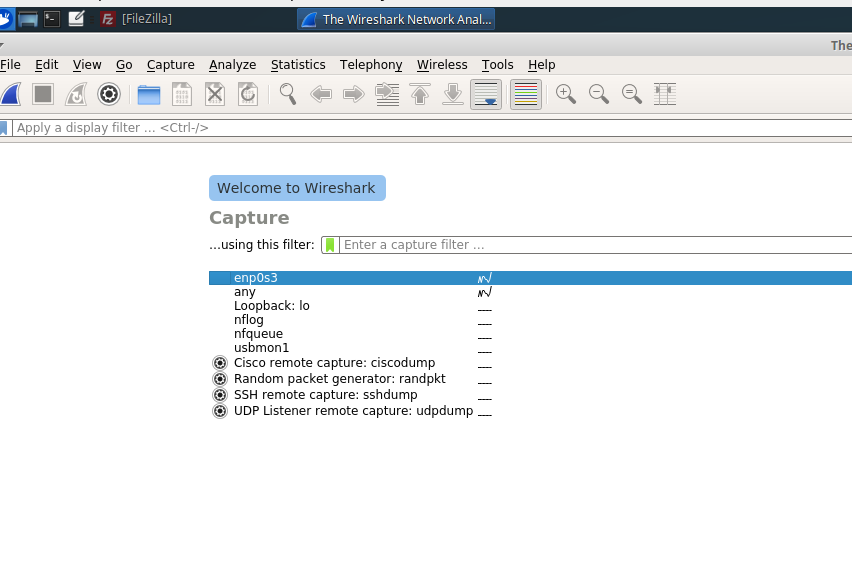


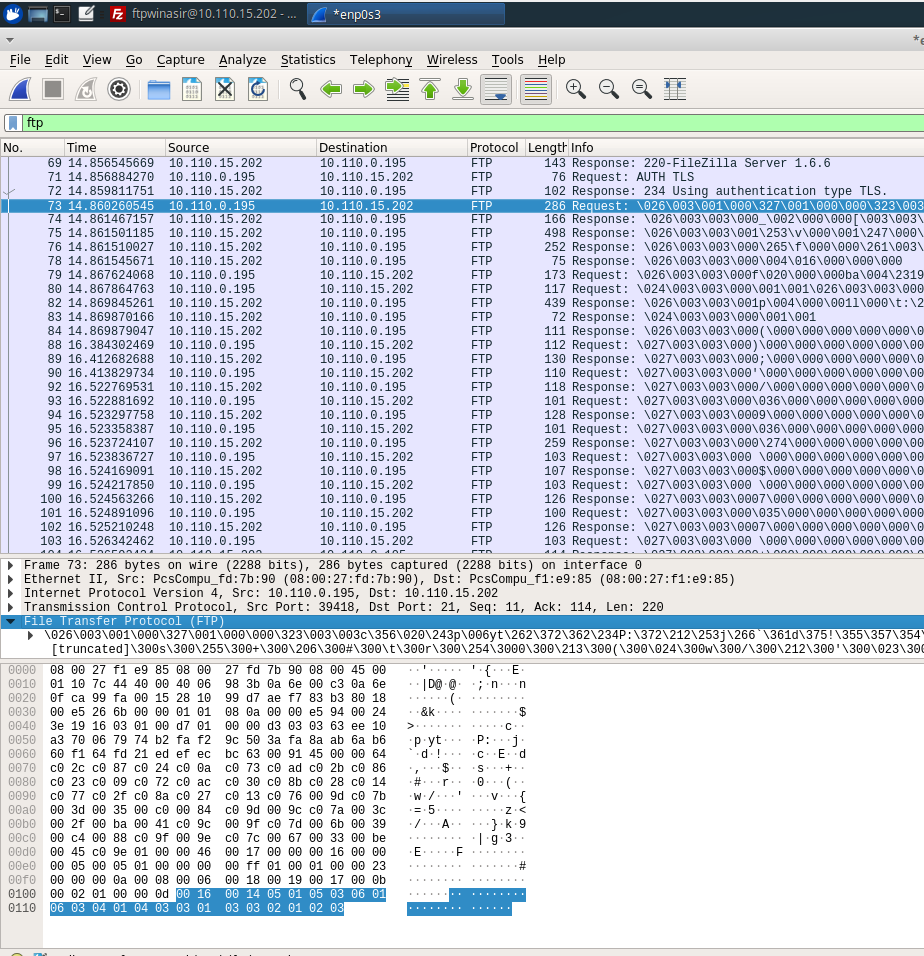


**6. Análisis de la comunicación FTP entre cliente y servidor**

a) En el cliente o en el servidor, instala el packet sniffer "Wireshark" y configúralo para capturar el tráfico FTP (filtro "FTP"). Vuelve a acceder a tu sitio FTP desde Filezilla client y comprueba si Wireshark captura el nombre de usuario y la contraseña ¿Qué sucede? ¿La transmisión es segura?

**sudo apt-get install wireshark**



****

**La transmisión hyper-segura porque está cifrada por SSL (certificado).**

b) A la vista de lo que ves en Wireshark, para la transmisión del fichero de datos, ¿Se ha usado el modo **activo** o **pasivo**? (aporta capturas y justifica la respuesta).

Nota para realizar este ejercicio:

• El filtro "FTP" en Wireshark hace que se muestren únicamente los paquetes del canal de comandos, que usan el puerto 21 en el servidor.

• Al estar la conexión encriptada, no podrás obtener en estos paquetes (del canal de comandos) si se está usando modo activo o pasivo.

• Para averiguarlo, debes capturar todos los paquetes entre cliente y servidor, usando por ejemplo el filtro "ip.src==IP\_serv" || ip.dst==IP\_serv".

• Cuando se muestren esos paquetes, se debe buscar uno que no sea de comandos (es decir, que el servidor no use el puerto 21). Si ese paquete usa en el servidor el puerto 20, es modo activo. En caso contrario, es pasivo). Debes aportar una

captura de ese paquete.

src= cliente

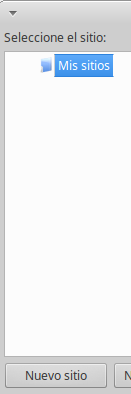
dest= servidor

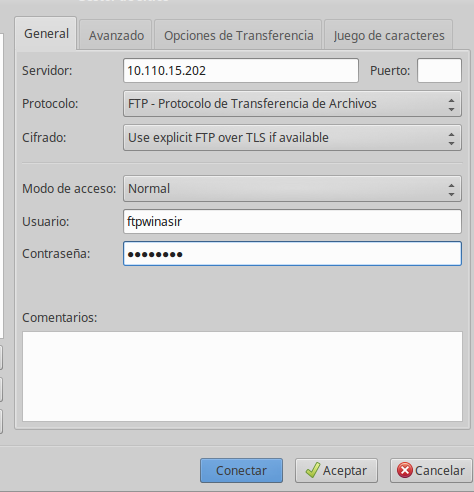


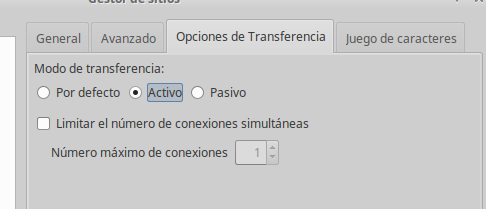


**Modo pasivo comprobado, ya que usa el rango de puertos que hemos asignado. Y primero se sincronizan por el 21. En nuestro caso el cliente ha cogido también un puerto del rango pero no tiene porque.**

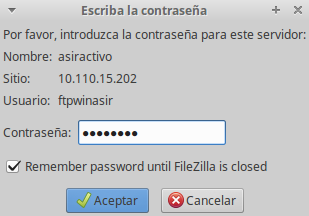
c) Fuerza que el cliente FTP utilice el **modo activo** y vuelve a capturar el tráfico. Haciendo un análisis similar a lo indicado en el apartado



**IMPORTANTE USUARIO NORMAL.**



**CONECTAR**

****

h) indica qué puerto de escucha se utiliza en el cliente para el canal de datos. Aporta la captura de un paquete del canal de datos en el que se muestre ese puerto. **Puerto 20 (la versión del server reciente no nos permite, aunque activemos el modo activo en el cliente). → por tanto si se pide algo en el examen tendremos que tener la versión antigua.**

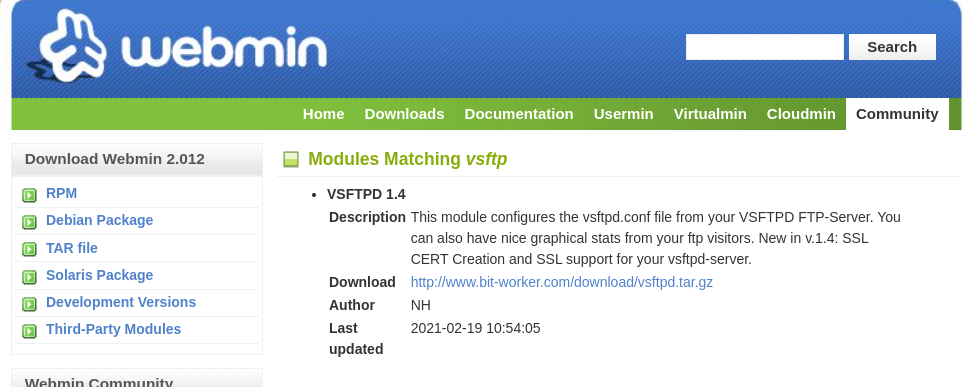
**poner mejor IP dst y src NOOO FTP**

****

**C. Servidor FTP con vsFTPd sobre Ubuntu**

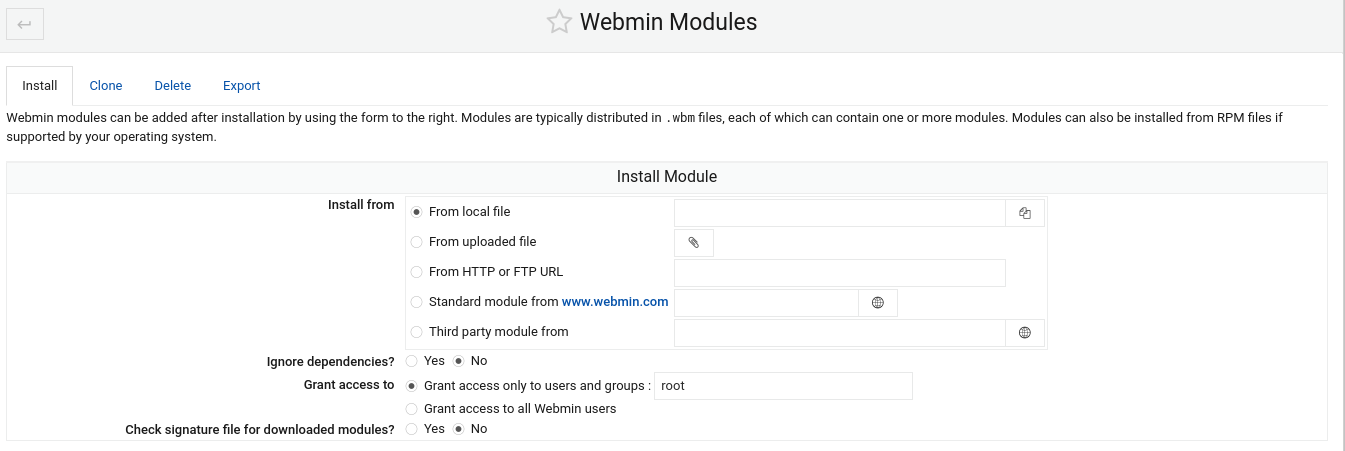
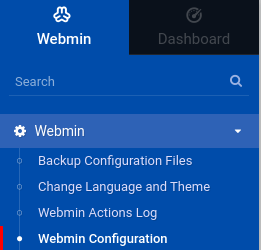
**7. Instalación de VSFTPD (Very Secure FTP Daemon) y creación de un sitio FTP básico** a) Devuelve tu M.V. Ubuntu 22.04 Server a la "Snapshot Base", con solo Webmin y Open SSH instalado

b) Sobre esa M.V. Ubuntu 22.04, instala el servidor FTP "vsFTPd".



<https://www.webmin.com/cgi-bin/search_third.cgi?search=vsftp>

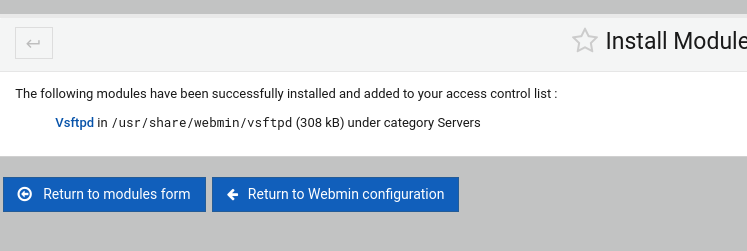
**Descargar para luego subir**



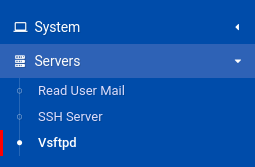




sudo



 **En el servidor**



c) A través de Webmin o del fichero de configuración, realiza las siguientes tareas en el servidor (realiza capturas):

• Fuerza que los ficheros subidos al servidor a través del FTP por cada usuario tengan:

i. Permiso de lectura, escritura (y ejecución si fueran ejecutables) para el “propietario”

***0***

ii. Solo lectura (y ejecución si fueran ejecutables) para el “grupo”

***2***

iii. Solo lectura (y ejecución si fueran ejecutables) para el resto de usuarios del sistema

**Aclaración: un fichero ejecutable deberá guardarse con permisos 755 y uno no ejecutable con permisos 644.**

***2***

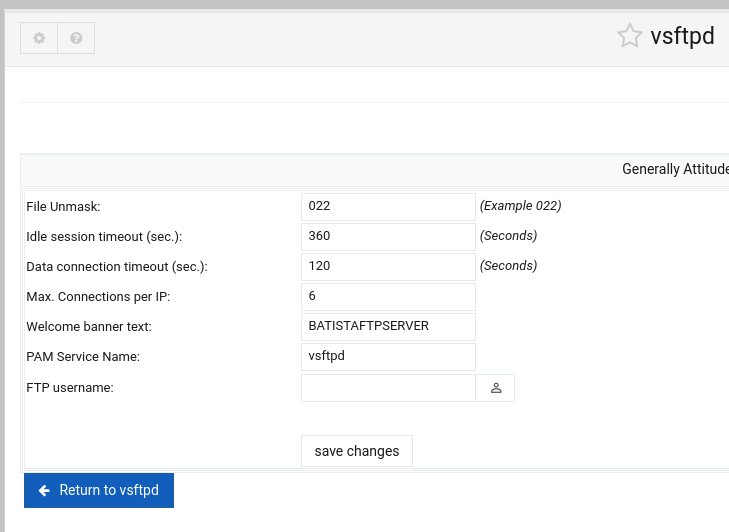
**Permiso 644 (permisos normales: lectura escritura ejecución 4,2,1)**

• Fuerza que cualquier conexión de un cliente se desconecte a los 6 minutos si no tiene actividad (es decir, si está conectado al FTP pero no envía órdenes para listar archivos, subir o descargar ficheros, etc, …)

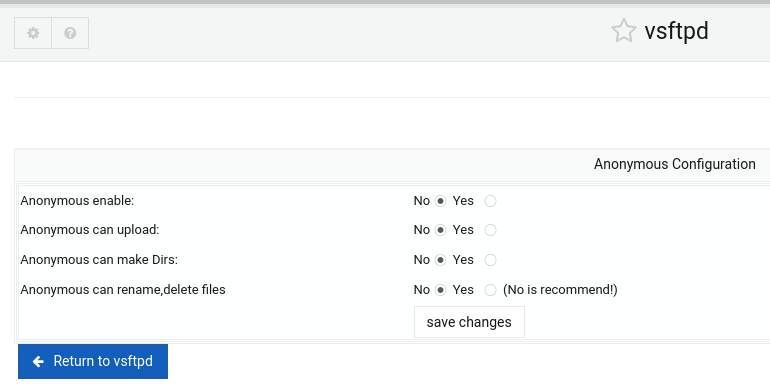
• Limita a 6 el número máximo de conexiones por IP

• Haz que el mensaje de bienvenida sea "APELLIDO FTP Server" (con APELLIDO= el apellido de uno de los miembros del grupo)

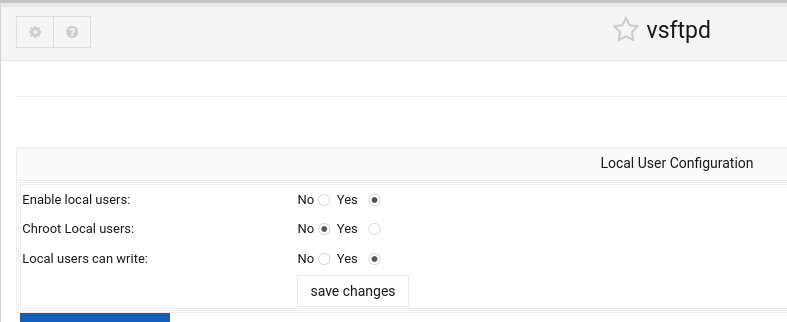
****

****

• Desactiva completamente el acceso anónimo al servidor.

****

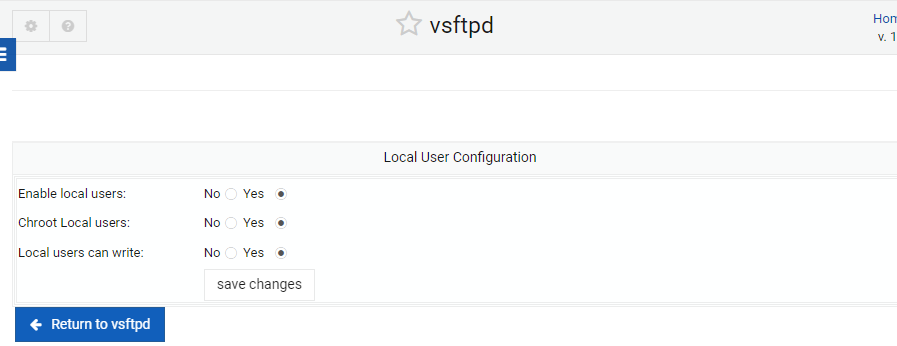
• Permite el acceso de los usuarios locales con permiso de escritura y lectura.



**La lectura ya es por defecto**

• Limita el acceso de los usuarios locales sólo a su "home" (es decir, que no se puedan mover por todo el sistema)

**CHROOT →YES**

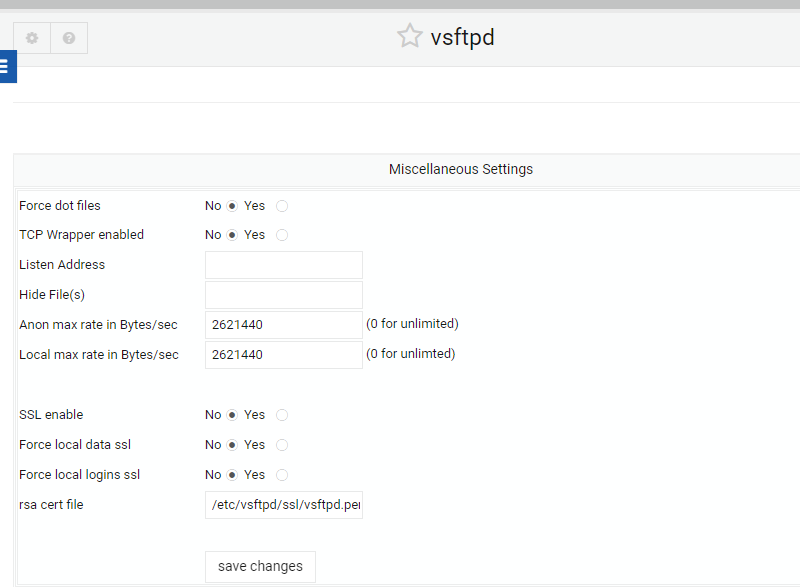


• Haz que los archivos ocultos NO sean accesibles a través del servidor FTP. ¿A través de qué opción se controla esta limitación?

**MISCELLANEOUS → force dot files —> NOO.**

**Si queremos que sean accesibles: YEES**

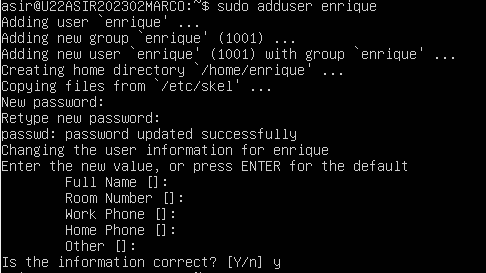
En la captura de abajo sale la opción

• Limita la velocidad de acceso al FTP para todos los usuarios a 20 Mbps. 

d) Crea el usuario "nombre" (nombre de uno de los miembros del grupo) con

contraseña "2asir2" para acceder al servidor FTP. Crea una carpeta en el home de este usuario llamada "EscrituraFTP". En ella copia o crea un archivo llamado

"archivoprueba.txt" que tenga un tamaño de al menos 1 KB.

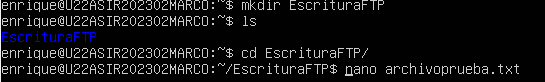


**PARA ACCEDER A TU USUARIO**





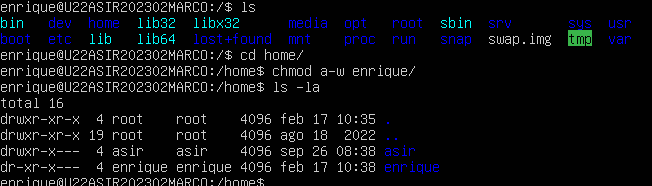
**OBLIGATORIO INICIAR SESION CON EL USUARIO PARA ACCEDER A TU HOME**

****

****

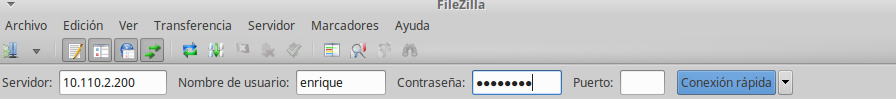
****

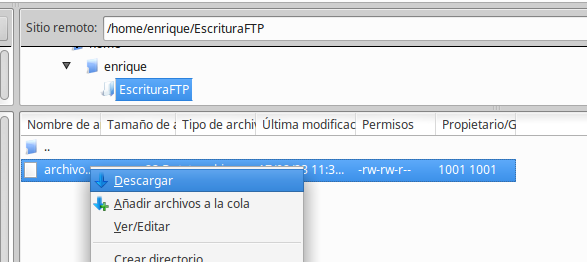
e) Realiza los ajustes necesarios en los permisos para que sea posible acceder a esta carpeta mediante FTP.

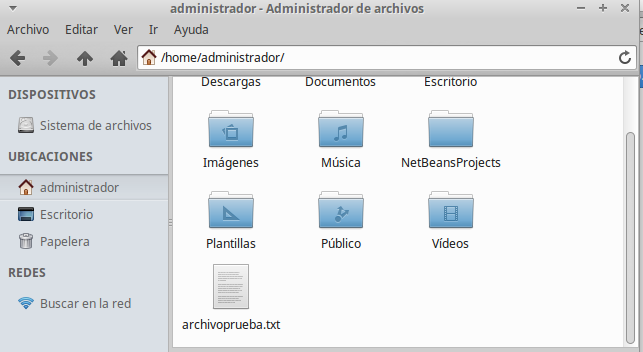
**QUITAR PERMISOS DE ESCRITURA: chmod a-w enrique/**

f) Desde otra máquina (física o virtual Linux o Windows), que llamaremos "Cliente", accede mediante el cliente FTP "Filezilla client" u otro cliente gráfico al FTP que

acabas de configurar (usuario "nombre") y descarga el fichero del servidor.







**EN EL CLIENTE SE HA DESCARGADO**

g) Sube un fichero al servidor y comprueba que los permisos del fichero en el servidor son los que has configurado.



**CREAR FICHERO EN EL CLIENTE Y TRANSFERIRLO AL SERVIDOR**

**COMPROBAMOS QUE LOS PERMISOS 022 SE HAN APLICADO CORRECTAMENTE**



**DESDE EL SERVIDOR, se puede ver en el mismo filezilla.**

**8. Análisis de la comunicación FTP entre cliente y servidor**

a) En el cliente o en el servidor (si usas el servidor tendrás que acceder por SSH) instala el packet sniffer "Wireshark" y configúralo para capturar el tráfico FTP (filtro "FTP"). Vuelve a acceder a tu sitio FTP desde el cliente y comprueba que Wireshark captura el nombre de usuario y la contraseña.

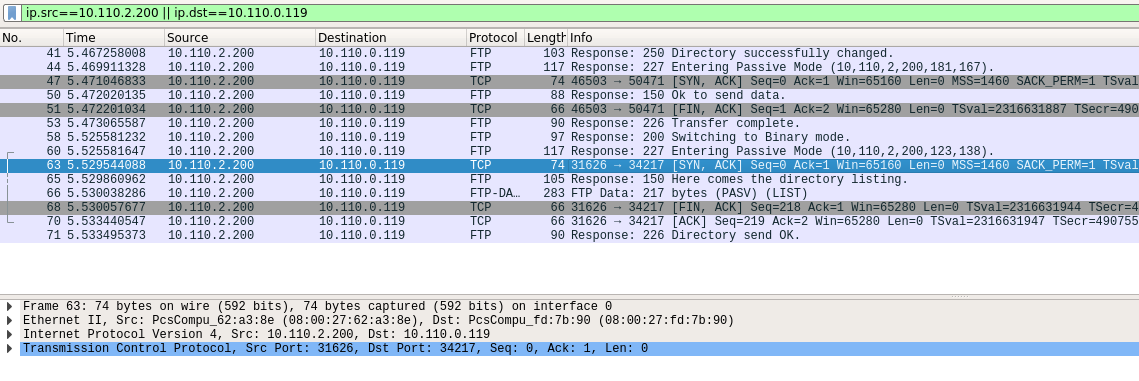
**CAPTURAMOS CON WIRESHARK Y CONECTAMOS FILEZILLA:**

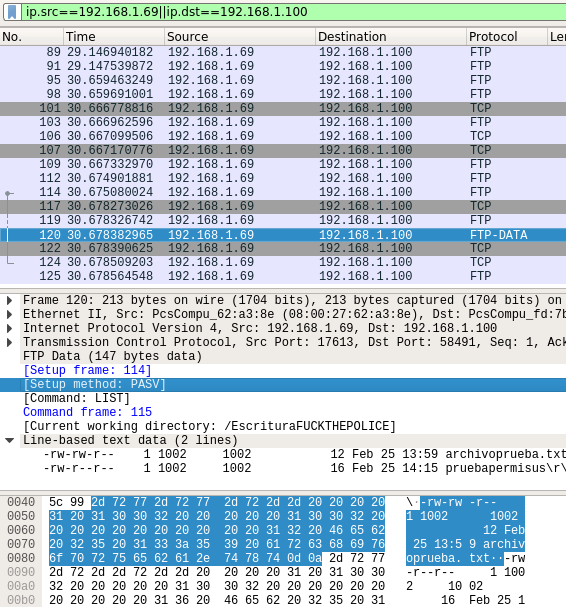
****

b) A la vista de lo que ves en Wireshark, para la transmisión del fichero de datos, ¿Se ha usado el modo **activo** o **pasivo**? (aporta capturas y justifica la respuesta)

**Se transfieren datos a través del puerto del servidor: 31626. Por ello sabemos que es Pasivo, este puerto ha sido indicado anteriormente en la conexión por el servidor. Si fuese Activo se comunican a través del puerto 20.**

**mirar en columna protocol: FTP-DATA (x si acaso)**

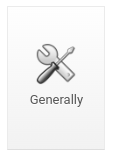
****

****

**9. Reconfiguración del servidor**

a) Reconfigura el servidor de forma que los archivos que suban los clientes tengan permisos de lectura, escritura y ejecución (si es ejecutable) tanto para el

"propietario", para el "grupo" y para el resto de usuarios.





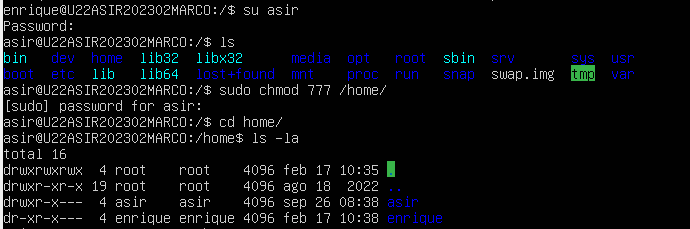
Aclaración: Un fichero ejecutable deberá guardarse con permisos 777 y uno no ejecutable con permisos 666.

Transfiere un archivo desde el cliente y comprueba que la nueva configuración funciona correctamente.



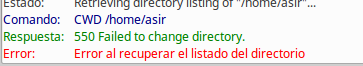
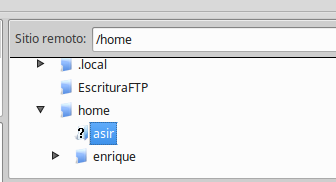
rw-rw-rw

b) Reconfigura el servidor de forma que los usuarios locales no tengan limitado el acceso a su HOME. Accede desde el cliente con el usuario "nombre" y comprueba si puedes acceder y descargar los archivos de "asir". ¿Puedes borrar a través del FTP, conectado como "nombre" los archivos del usuario "asir"? ¿Por qué?



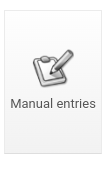


**Enjaular**



**No se puede borrar archivos de asir porque los permisos dados para /home no se heredan ya que pertenece a otro usuario.**

c) Reconfigura el servidor de forma que el puerto de escucha del canal de control sea el 1206 en vez del 21. Indica claramente cómo lo has configurado (puedes acceder al fichero de configuración desde Webmin o directamente desde un terminal con vi, nano, etc.).





**Añadir está línea en el archivo de configuración**

**IMPORTANTE REINICIAR SERVIDOR EN CADA APARTADO!!!**

****

Para encontrar cuál es el parámetro a cambiar busca ayuda en el manual de vsftpd, accesible desde Webmin en la opción "vsftpd.conf Doc".

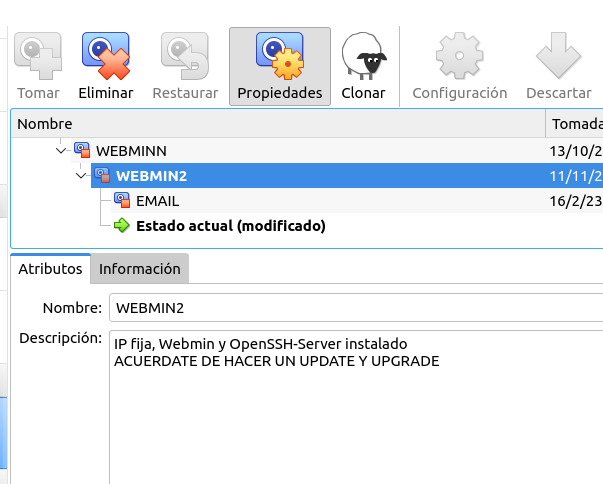
Conecta el cliente al servidor utilizando el nuevo puerto (1206)



**D. Transferencia de ficheros en Linux mediante SSH**

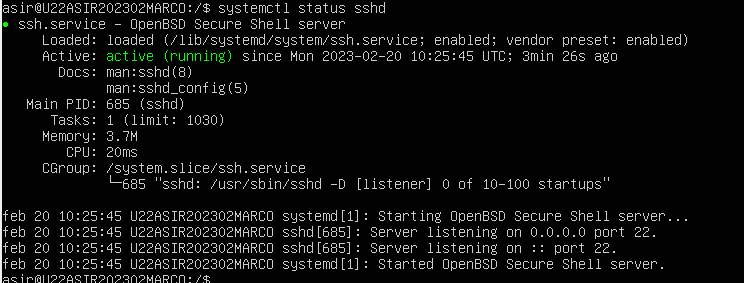
**10. Instalación de servidor SSH**

a) Devuelve tu m. v. Ubuntu 22.04 Server a la "Snapshot base".

****

b) Sobre esa M.V. Ubuntu 22.04, comprueba que tienes instalado el servidor SSH

"OpenSSH-server".



c) Crea una carpeta llamada "SFTP" en la raíz del sistema de archivos (/SFTP) y asigna como asigna como usuario y grupo propietario a "asir". usuario y grupo propietario a "asir".





d) Desde otra máquina (física o virtual Linux o Windows), que llamaremos "Cliente", accede mediante el cliente FTP "Filezilla client" al servidor que acabas de configurar utilizando SFTP (usuario "asir") y envía un fichero de al menos 1 KB al servidor.



