

SERVICIOS EN RED

2º SMR

IES Ramón del Valle Inclán

Profesor: José Luis Rodríguez Rodríguez

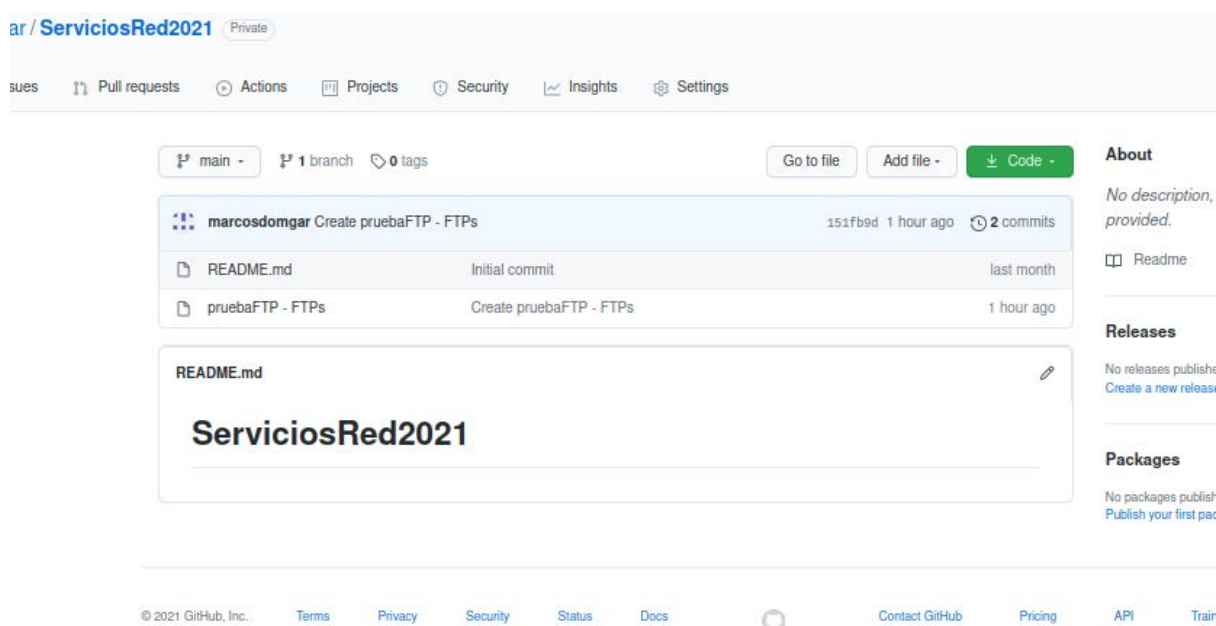
ENUNCIADO

Inicia la instancia AWS que usastes en clase para la unidad de FTP. Responde a los siguientes apartados (*debes responder en cada apartado de la sección “Criterios de evaluación”; no respondas en este enunciado*):

1. FTPs:

- a. Crea otro par de ficheros para el certificado y la clave privada cuyo nombre sean **pruebaftp.cer** y **pruebaftp.key**, respectivamente, los cuales sustituyen a los que tuvieras configurado. Debes indicar la ubicación de ambos ficheros y la configuración del servidor FTP. Usar Webmin para la configuración.
 - i. El certificado debe ser expedido para una empresa de nombre “PruebaFTP.SL” ubicada en Sevilla con nombre DNS pruebaftp.iesvi, con dirección de correo admin@pruebaftp.sl, gestionada por el departamento “estudiantes”.
- b. Realiza una conexión desde Filezilla en **modo activo**:
 - i. Muestra la configuración a realizar en el cliente, dejando de forma clara que se usa el modo activo.
 - ii. Mostrar que el cliente recibe el certificado previamente creado en el servidor.
 - iii. Muestra evidencias de que la sesión está cifrada.
 - iv. Sube y baja algún fichero.
 - v. Renombra ficheros remotos así como alguna carpeta remota.

[antes de seguir debes realizar commit con mensaje “**pruebaftp - FTPs**”]

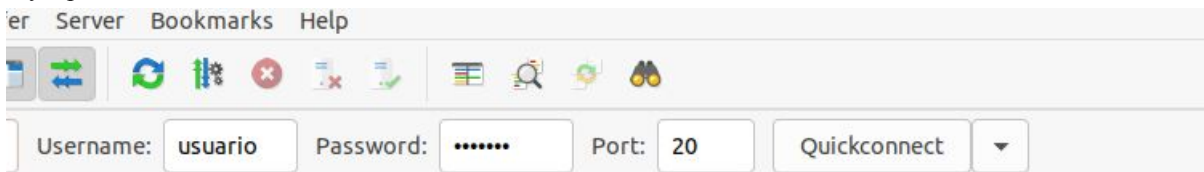


a.: En mi caso, he generado los ficheros en /etc/proftpd;

```
usuario@usuario-OptiPlex-3050:/etc/proftpd$ ls
blacklist.dat  ldap.conf      pruebaftp.cer  tls.conf
conf.d         modules.conf   pruebaftp.key  virtuals.conf
dfoparams.pem  proftpd.conf   sal.conf
```

b.

Antes que nada, para realizar la conexión en modo activo, debemos asegurarnos que en el apartado de “Ports” de Filezilla sea 20, debido a que es este el puerto que el que usa el modo activo, tal y como lo voy a poner a continuación:



Local site			Remote site:		
Filesize	Filetype	Last modified	Filename ^	Filesize	Filetype
	Directory	27/02/20 20:34...			
1,4 MB	dat-file	27/02/20 20:34...			
9,5 KB	pem-file	27/02/20 20:34...			
701 B	conf-file	03/02/21 12:31...			
3,0 KB	conf-file	03/02/21 12:31...			
5,7 KB	conf-file	22/02/21 09:52...			

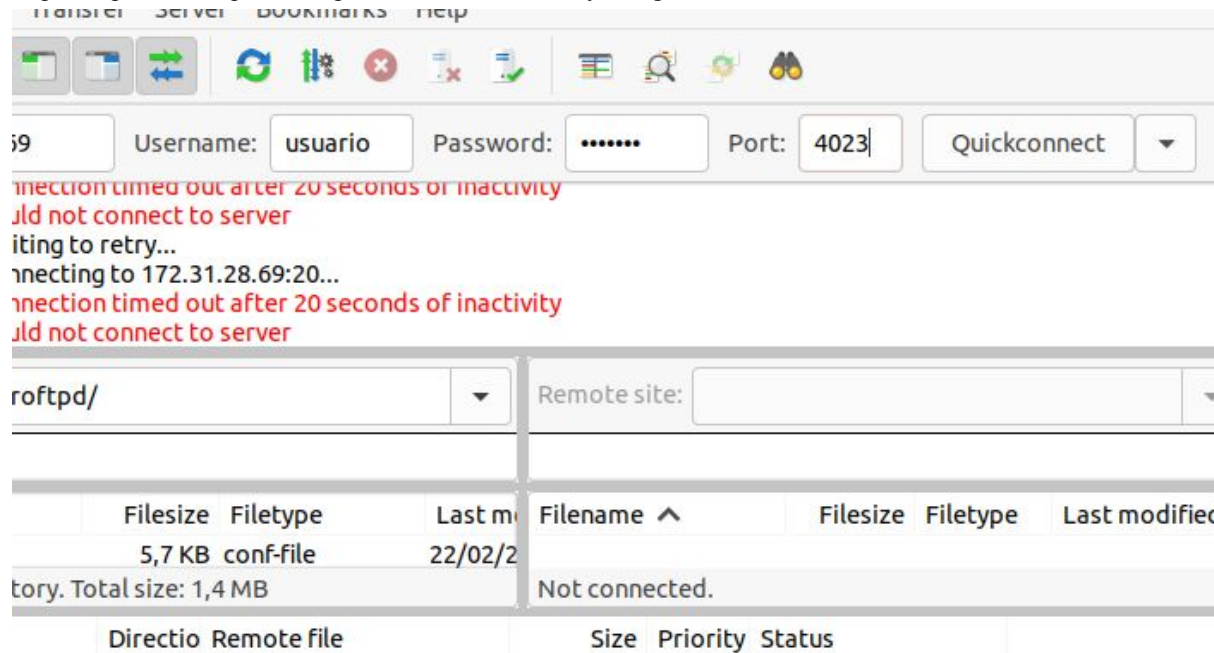
2. Modo pasivo:

- Habilita el modo pasivo en los puertos **4000 a 4500**. Explica todos los parámetros necesarios para disponer el servidor en este modo en una instancia AWS.
- Realiza la configuración usando Webmin.
- Realiza pruebas de conexión en Filezilla.
- Muestra evidencias de que se realiza la conexión en modo pasivo.

[antes de seguir debes realizar commit con mensaje “**pruebaftp - Modo pasivo**”]

- a. Lo mismo, configuramos en filezilla de tal manera que se pueda conectar de forma pasiva, poniendo los puertos de esta manera:

Se puede poner cualquier otro puerto de 4000 a 5000, yo elegí el 4023



3. Acceso anónimo:

- a. Deshabilita el acceso anónimo, realizando pruebas que así lo demuestren.
- b. Vuelve a habilitarlo, mostrando que no es posible subir ficheros al repositorio FTP.
- c. Configura el servicio para permitir que puedan subirse ficheros.

[antes de seguir debes realizar commit con mensaje “pruebaftp - Acceso anónimo”]

4. sFTP:

- a. Muestra la configuración que se pidió en clase, dando una explicación de la misma.
- b. Realiza pruebas de conexión desde Filezilla mostrando los diferentes “accesos” permitidos.
- c. Muestra evidencias de que la sesión está cifrada.
- d. Batería de pruebas] Realiza las siguientes pruebas **desde un terminal sftp**:
 - i. Establece una conexión FTP con la instancia AWS. Inicia la sesión con uno de los usuarios que se crearon en esta práctica en clase.
 - ii. Desconecta la sesión sin salir del prompt FTP. Vuelve a conectar con el mismo usuario (debes estar en el prompt FTP)
 - iii. Desde el prompt FTP sitúate en la carpeta /home/usuario/Documents de tu máquina local. Muestra el directorio local
 - iv. Sin cerrar la sesión FTP, ve a la shell del sistema, crea 3 documentos: prueba1.txt, prueba2.txt e imagen.jpg (no importa que no sea una imagen real pero llámalo así) en la carpeta /home/usuario/Documents.

- v. Vuelve al prompt del sistema.
- vi. Crea un directorio en el servidor FTP de nombre repositorio.
- vii. Sube los ficheros prueba1.txt y prueba2.txt al directorio repositorio. Muestra que se han subido. Debes usar un único comando para la subida de ambos ficheros.
- viii. Sube el fichero imagen.jpg al mismo directorio.
- ix. Baja el fichero imagen.jpg renombrándolo en el mismo comando a imagen2.jpg.
- e. Haciendo uso de la utilidad **scp** realiza la transferencia de un fichero ubicado en la carpeta home del usuario de la instancia de AWS y con destino la carpeta home de tu máquina física.

Debes anotar **comentarios** en los ficheros de configuración, que expliquen cada aspecto que configures. **No se dará por válidas aquellas configuraciones NO comentadas.**

Debes aportar **evidencias** de la configuración pedida, según cada apartado indicado en “Criterios de evaluación”, con **capturas de pantalla**.

a.

Como lo hemos hecho en clase, paso a paso ha sido así:

en una instancia, debemos ver en inbound rules si tenemos las reglas añadidas, con custom ftp con puerto 21, otro con el puerto 20, y otro de 49152 a 85534. Cada una con 0.0.0.0/0.

En el fichero /etc/proftpd/proftpd.conf, debemos asegurarnos de que está configurado de forma correcta.

Ahora ya podemos conectarnos con sFTP a amazon.

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
SSH	TCP	22	Custom <input type="text" value="0.0.0.0/0"/>		Delete
Custom TCP	TCP	21	Custom <input type="text" value="0.0.0.0/0"/>		Delete
Custom TCP	TCP	50123	Custom <input type="text" value="0.0.0.0/0"/>		Delete
Custom TCP	TCP	20	Custom <input type="text" value="0.0.0.0/0"/>		Delete

Criterios de evaluación

REPOSITORIO REMOTO GITHUB: <https://github.com/jlr2/PruebaFTP-Alumnos.git>

Una vez terminada la prueba, debes crear una rama con nombre tu nombre (Ej: José Ruiz Martín es RMJ) y subirla al repositorio github.

b Se ha instalado un servicio de transferencia de ficheros.

Se pide:

1. **[4 puntos] Configuración de FTPs:** generación de certificado y clave privada, configuración del servidor, evidencia de conexión cifrada

Generamos la clave, (privada, la cual nos interesa, y la pública):

```
usuario@usuario-OptiPlex-3050:/etc/proftpd$ gpg --full-generate-key
gpg (GnuPG) 2.2.19; Copyright (C) 2019 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

Please select what kind of key you want:

- (1) RSA and RSA (default)
- (2) DSA and Elgamal
- (3) DSA (sign only)
- (4) RSA (sign only)
- (14) Existing key from card

Your selection? 1

RSA keys may be between 1024 and 4096 bits long.

What keysize do you want? (3072) 2000

Requested keysize is 2000 bits

rounded up to 2048 bits

Please specify how long the key should be valid.

- 0 = key does not expire
- <n> = key expires in n days
- <n>w = key expires in n weeks
- <n>m = key expires in n months
- <n>y = key expires in n years

Key is valid for? (0) 0

Key does not expire at all

Is this correct? (y/N) y

2. **[4 puntos] Control de versiones GIT:** versionado pedido en toda la prueba y subida a repositorio remoto. **NOTA:** este apartado se puntúa en este criterio de evaluación siendo además **REQUISITO IMPRESCINDIBLE PARA PODER EVALUAR TODOS LOS CRITERIOS**, es decir, sin realizar versionado y tener subidos al repositorio remoto los ficheros de configuración usados en la prueba, se dará por prueba no válida.

Muestra los comandos git usados para realizar uno de los commits y la subida al repositorio github.

3. **[2 puntos] sFTP:** mostrar que el servicio está operativo.

c Se han creado usuarios y grupos para acceso remoto al servidor.

Se pide:

1. **[6 puntos]** sFTP: Muestra la configuración que se pidió en clase, dando una explicación de la misma.
2. **[2 puntos]** Realiza pruebas de conexión desde Filezilla mostrando los diferentes “accesos” permitidos.
3. **[2 puntos]** Muestra evidencias de que la sesión está cifrada.

d Se ha configurado el acceso anónimo.

Se pide:

1. **[5 puntos]** Deshabilita el acceso anónimo, realizando pruebas que así lo demuestren.
2. **[5 puntos]** Vuelve a habilitarlo, mostrando que no es posible subir ficheros al repositorio FTP.

e Se han establecido límites en los distintos modos de acceso.

1. **[5 puntos]** Configura el servicio para permitir que puedan subir ficheros en modo anónimo.
2. **[5 puntos]** Cambia la configuración realizada con los usuarios sFTP de forma que sea posible acceder a la carpeta “archivos” de algunos de los 2 usuarios pedidos desde cualquier otro usuario. Realizar prueba desde el otro usuario de la práctica.

f Se ha comprobado el acceso al servidor, tanto en modo activo como en modo pasivo.

Se pide:

1. **[4 puntos]** FTPs: Configuración cliente Filezilla para sesión FTPs y en modo activo, evidencias de funcionamiento.
2. **[6 puntos]** Modo pasivo: configuración del servidor FTPs, pruebas desde Filezilla, evidencias de funcionamiento.

g Se han realizado pruebas con clientes en línea de comandos y en modo gráfico.

Se pide:

1. **[2 puntos]** FTPs (modo gráfico): Sube y baja algún fichero + Renombra ficheros remotos así como alguna carpeta.
2. **[6 puntos]** sFTP (cliente sftp): batería de pruebas pedidas.
3. **[2 puntos]** sFTP (cliente scp): transferencia de fichero pedida.