Aspectos teóricos previos

- Para la realización de esta práctica hay que partir de la situación de la práctica 4 con configuración SSL explícito, por lo que debes copiar la configuración de dicha práctica sobre el fichero de configuración vsftpd.conf.
- Una de las capacidades que enriquecen los servicios es el poder utilizar un sistema de autenticación externo al propio del servicio. Como hemos visto, la mayoría de los servicios Linux disponen de una autenticación basada en los usuarios locales del sistema. En el caso de FTP hemos tenido que añadir a los usuarios locales de la máquina un usuario "cliente1" que fuera el administrador del sitio "virtual1".
- El objetivo de esta práctica es utilizar MySQL (MariaDB) para la autenticación de usuarios sobre el servicio FTP y que dichos usuarios accedan a un directorio concreto del sistema en el que estarán enjaulados, pudiendo alterar solamente el contenido de dicho directorio. El objetivo final podría será el mismo que en la Práctica 3, es decir, que el usuario "cliente1" tuviera como directorio asignado "/var/www/virtual1". Para no alterar la práctica 3, vamos a usar otro usuario, denominado 'virtual1' pero vamos a mantener el directorio, en este caso "/var/www/virtual1".
- Además de la autenticación que ya conocemos para usuarios locales, los sistemas como Debian proporcionan PAM (módulos de autenticación conectables) que ofrecen mecanismos flexibles de acreditación que son usados por las aplicaciones software como el servicio FTP que nos ocupa. Entre estos sistemas PAM está el necesario para MySQL (libpam-mysql).
- El servidor 'vsftpd' dispone de un archivo en el que se indica el modo de autenticación soportado por cada servicio. El archivo suele encontrarse en el directorio '/etc/pam.d/' y suele llevar el nombre del servicio en cuestión, en nuestro caso 'vsftpd'.
- En definitiva, usaremos MariaDB para almacenar usuarios y contraseñas cifradas y el módulo PAM correspondiente para decirle al servidor 'vsftpd' que será ese el modo de autenticación, así como indicarle qué base de datos, tablas y atributos ha de utilizar.
- Por simplicidad, nosotros vamos a crear usuarios y contraseñas directamente como registros en una tabla, pero se podría utilizar un formulario web para dar de alta al usuario a través de Apache y guardarlo en la base de datos siguiendo las pautas que vimos cuando creamos sitios web y podríamos ampliar los atributos de esta tabla para crear atributos de usuario activo, suspendido, etc.

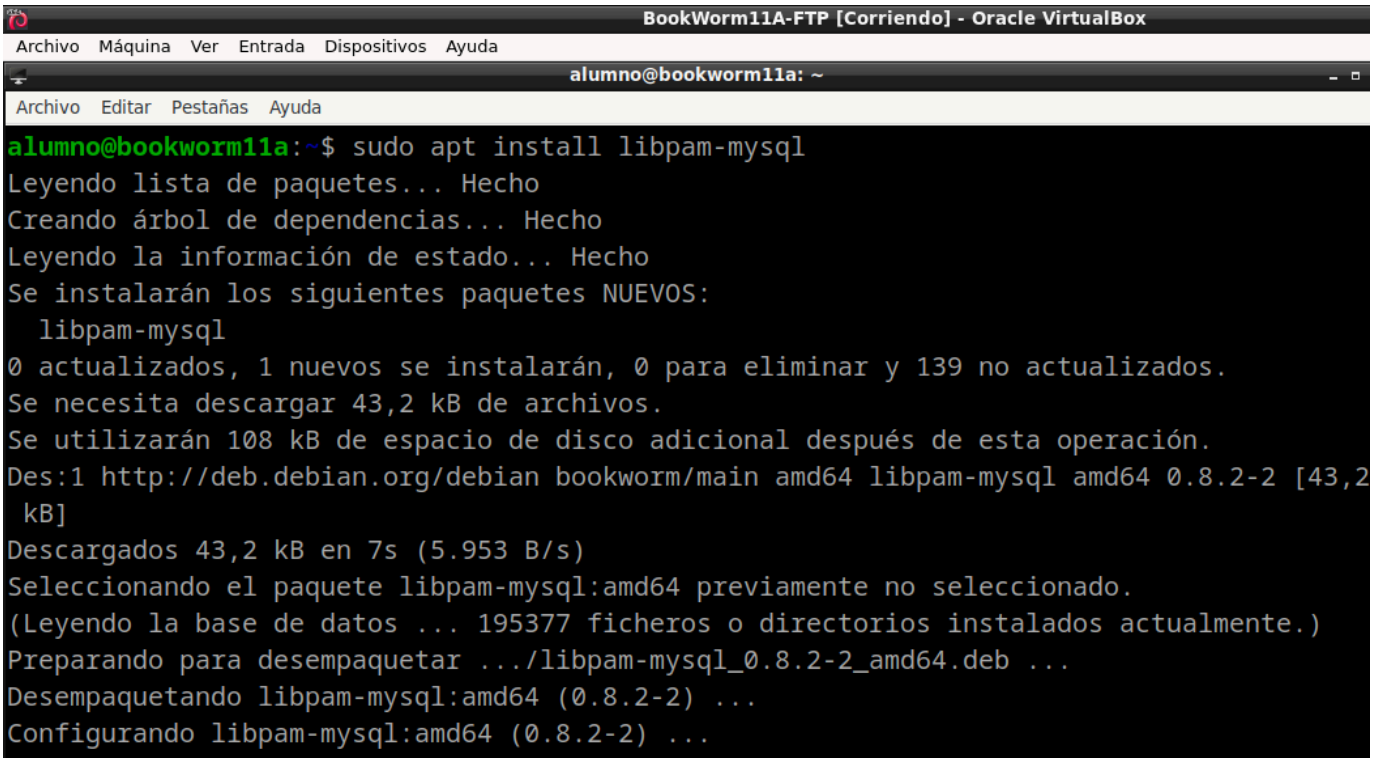
Consideraciones iniciales

- A lo largo de esta práctica se va a utilizar como cliente Filezilla. Si no lo tienes, instálalo en tu cliente LinuxXX

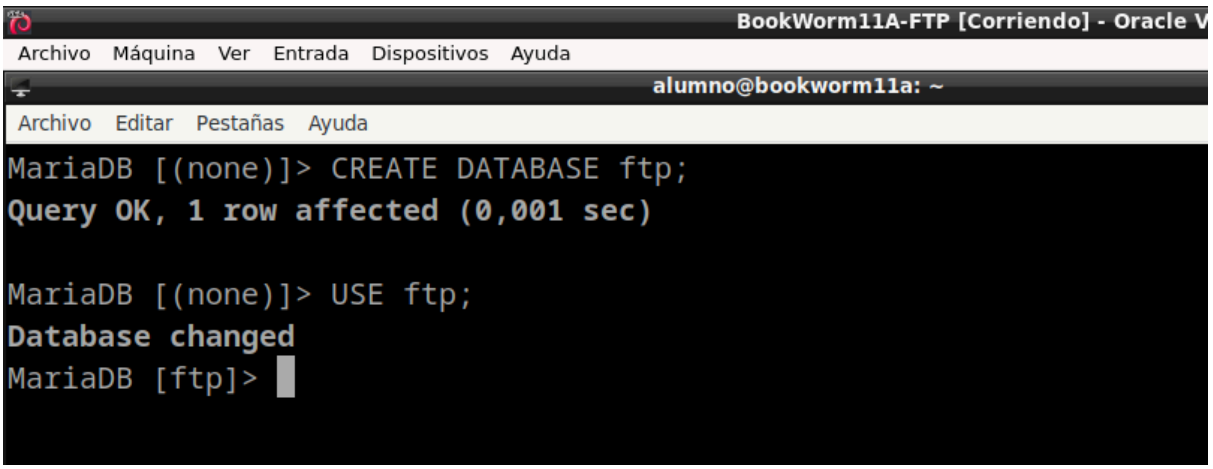
- Crea y almacena en Filezilla una conexión diferente por cada variante que hagas en dicha conexión y nómbralas adecuadamente para poder identificarlas con facilidad y poder volver a usarlas.
- Es importante que por cada intento de conexión solicitado hagas una captura de wireshark para poder observar los diálogos que se producen entre cliente y servidor.
- Utiliza como usuario de prueba 'virtual1'. Recuerda que quizá tengas que añadirlo al archivo de usuarios que se pueden conectar
- Por cada cambio que realices en el servidor haz un reinicio del mismo.
- Ten especial cuidado y utiliza solamente minúsculas en los nombres de las directivas.

Desarrollo de la práctica

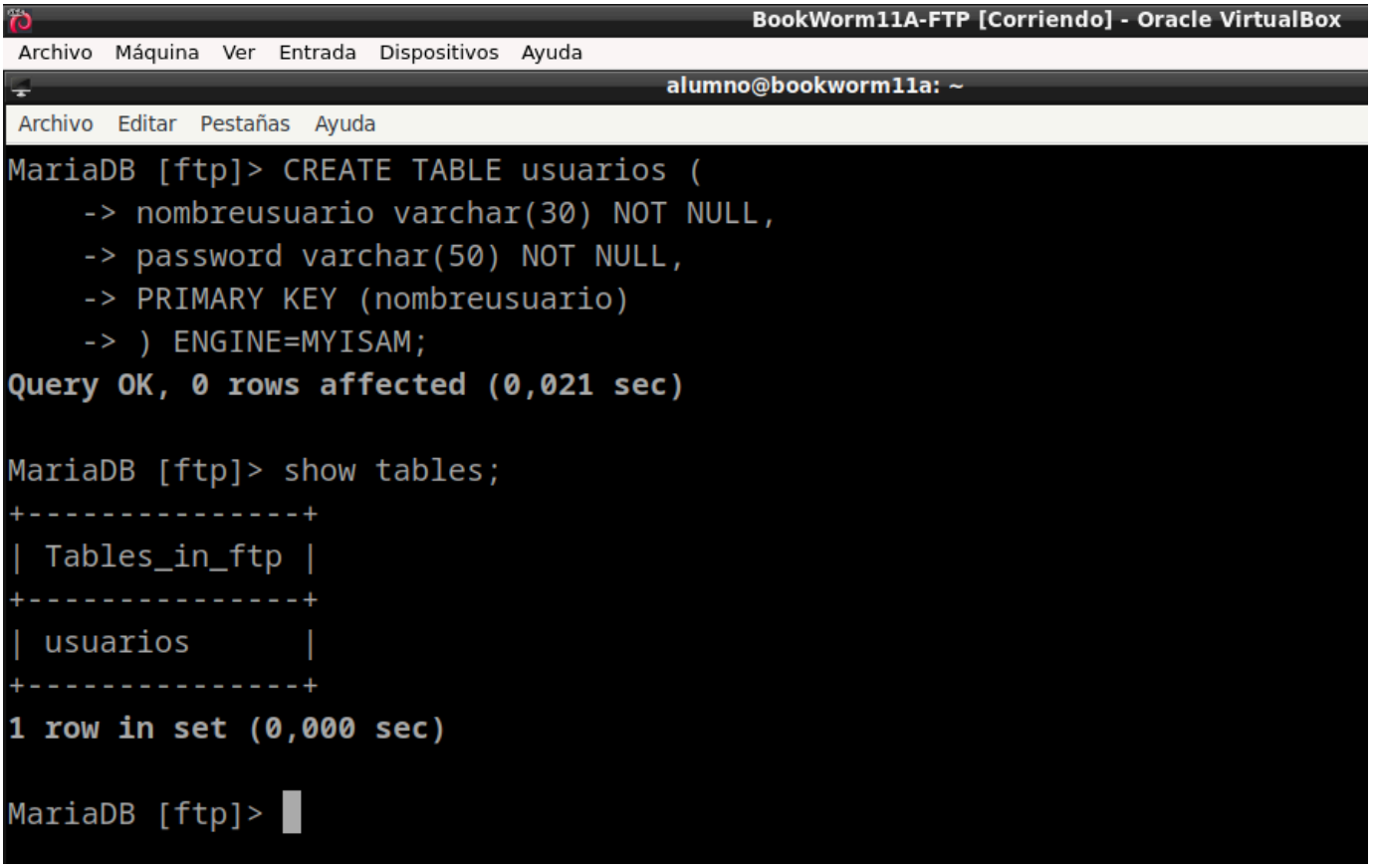
1. Instala en tu servidor BOOKWORMXX la librería 'libpam-mysql' utilizando 'apt'



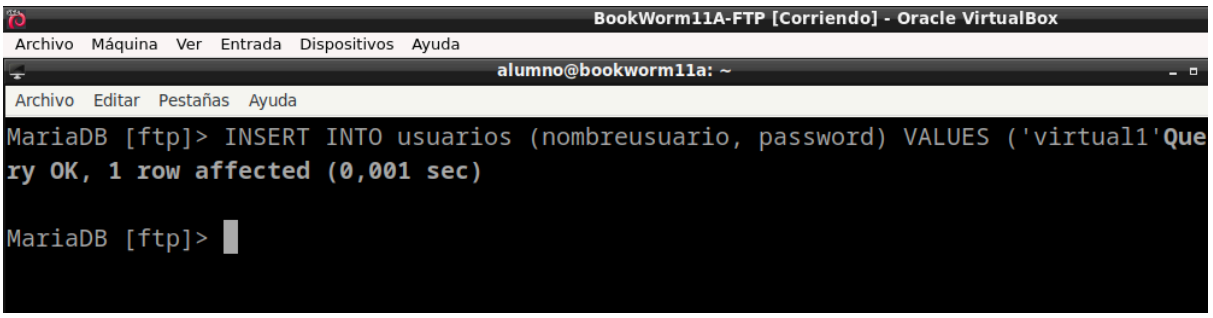
2. En MariaDB:
    1. Crea en MariaDB una base de datos denominada 'ftp'



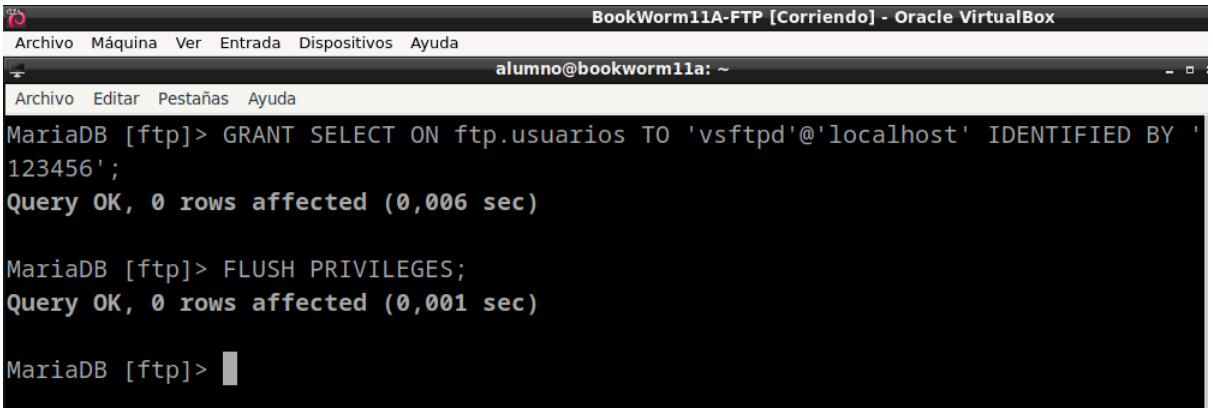
2. Crea una tabla para almacenar usuarios en esta base de datos. Por ejemplo: 'CREATE TABLE usuarios (nombreusuario varchar (30) NOT NULL, password varchar(50) NOT NULL, PRIMARY KEY (nombreusuario)) ENGINE=MYISAM;'



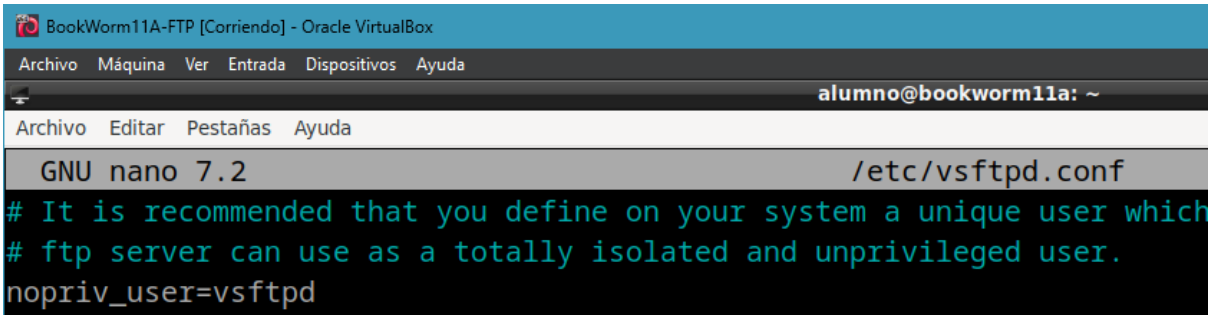
3. Inserta un registro en la tabla anterior con nombre de usuario "virtual1" y password '232425' (recuerda usar PASSWORD('232425') para que la contraseña se inserte en la tabla cifrada).



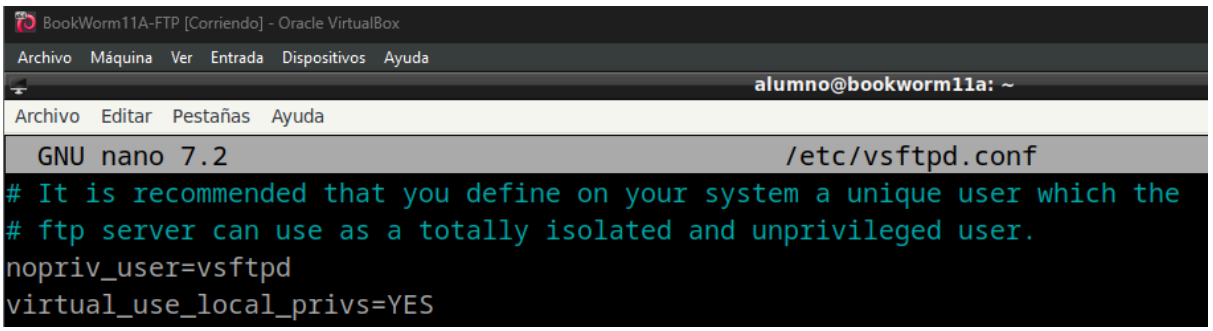
4. Otorga permisos de selección a un usuario de MariaDB denominado 'vsftpd' sobre la tabla 'usuarios' y ponle contraseña '123456'.



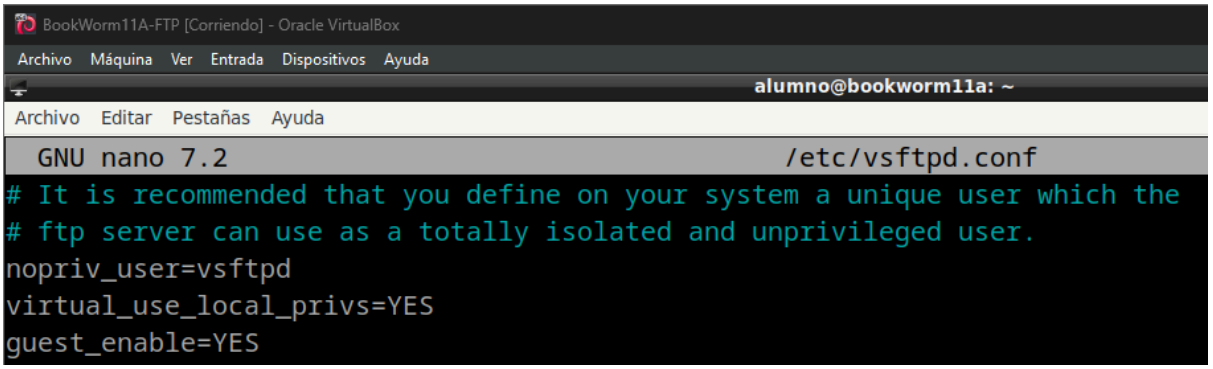
3. En el fichero de configuración hay que habilitar y/o modificar algunas directivas:
    1. La directiva que permite indicar el nombre del usuario sobre el que se mapean los usuarios virtuales de MariaDB: 'nopriv_user=vsftpd'



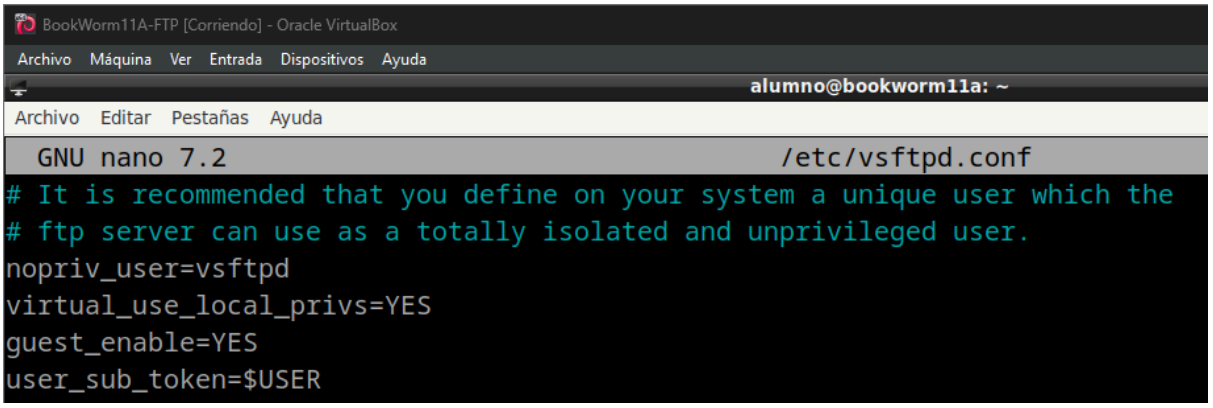
2. En el caso de querer que los usuarios virtuales se coporten con un usuario local en cuanto a permisos/privilegios se refiere: 'virtual_use_local_privs=YES' (hay que tener en cuenta que las directivas sobre las conexiones de los usuarios locales y el archivo con la lista de permitidos/prohibidos tendrá vigencia y habrá que modificarla llegado el caso)



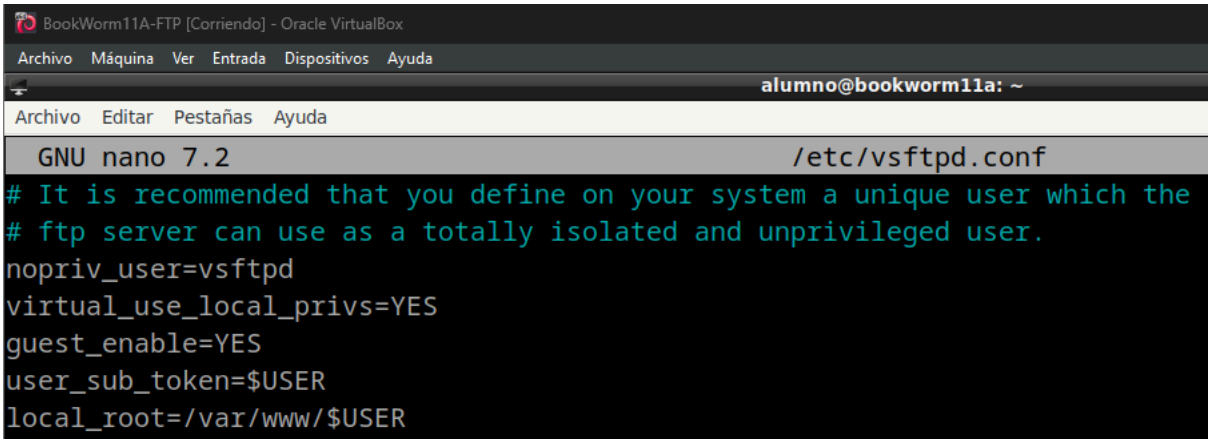
3. Puesto que solo los usuarios de MariaDB van a ser los que permitamos que se conecten: 'guest_enable=YES'



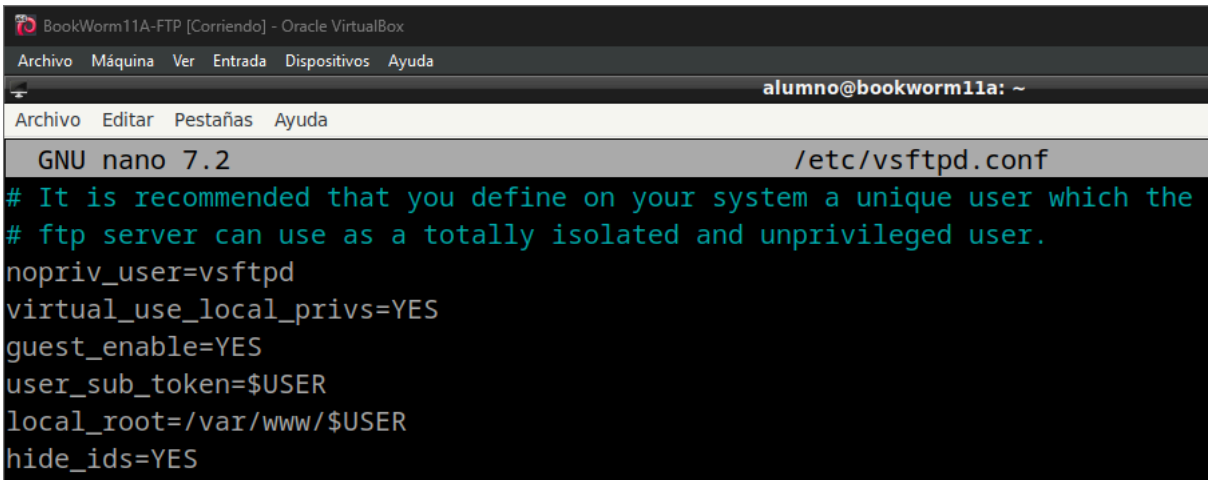
4. Por comodidad vamos a hacer que el nombre del usuario determine también el subdirectorio del sistema de archivos en el que se enjaulará: 'user_sub_token=$USER'



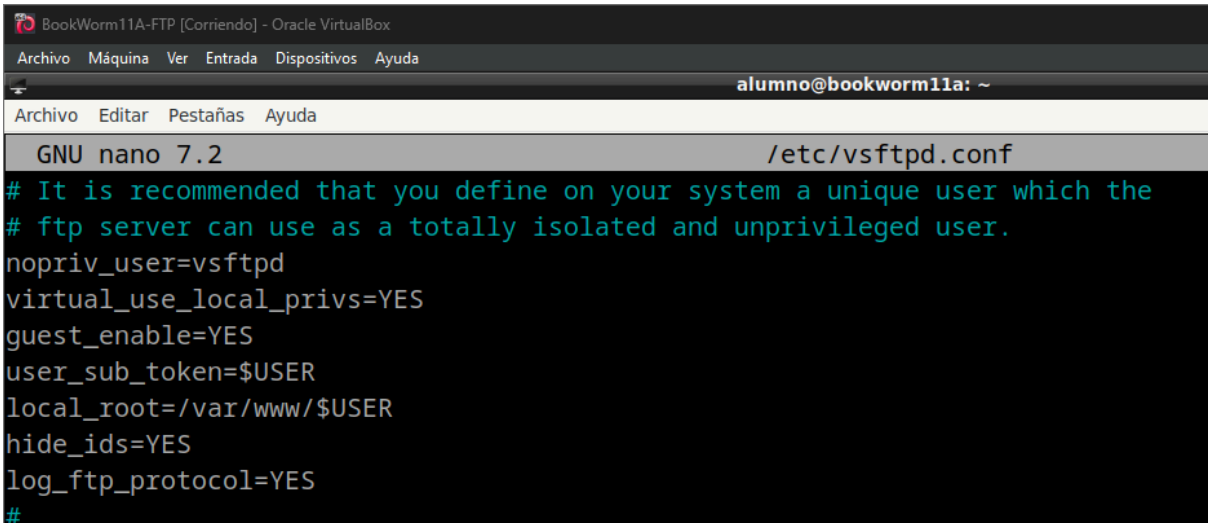
5. Vamos a fijar la raíz de directorios: 'local_root=/var/www/$USER'



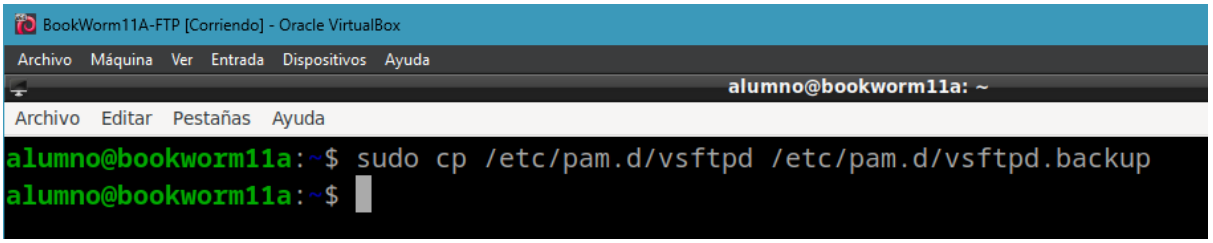
6. Vamos a habilitar la directiva 'hide_ids' para que toda la información de usuarios y grupos en los directorios listados se muestre como 'ftp'



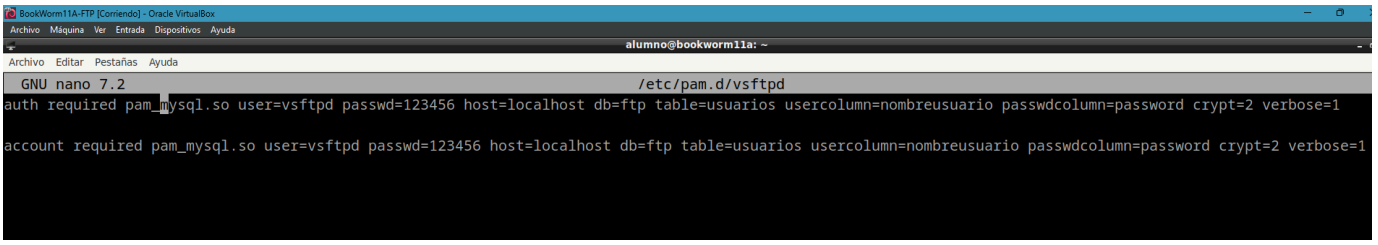
7. Por último vamos a habilitar la directiva 'log_ftp_protocol' para disponer de más detalle en los logs.



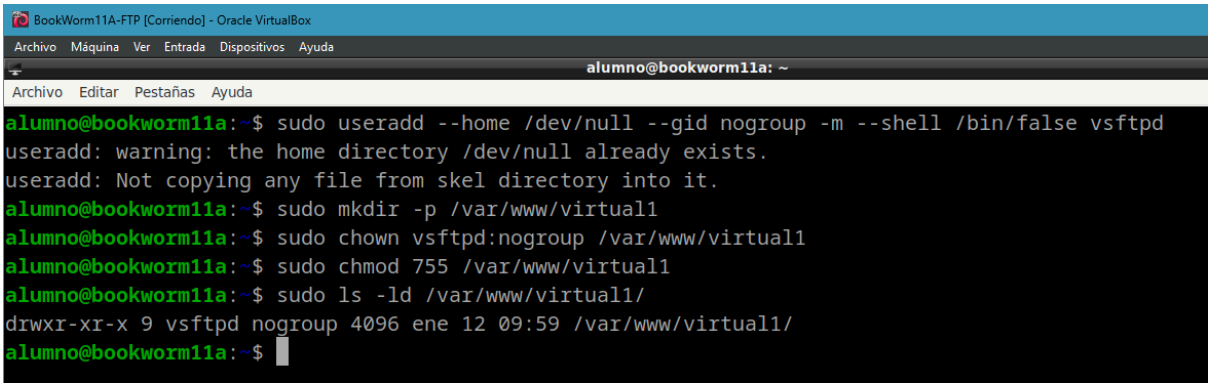
4. Para indicar al servicio dónde se encuentran usuarios y contraseñas así como el modo de autenticación tenemos que modificar el archivo '/etc/pam.d/vsftpd':
    1. Haz copia de seguridad del archivo y llámalo 'vsftpd.backup' y sustituye su contenido por el siguiente:



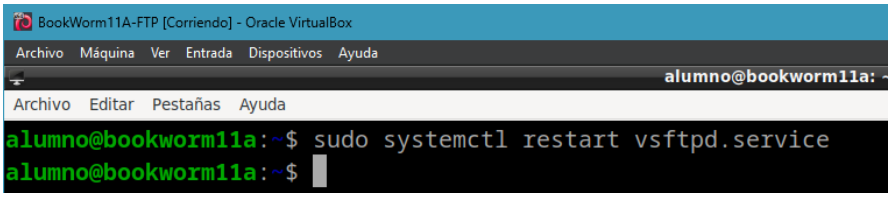
    2. Indicación de que se necesita autenticación sobre mysql, en nuestro caso aportando una contraseña: 'auth required pam_mysql.so user=ftp passwd=123456 host=localhost db=ftp table=usuarios usercolumn=nombreusuario passwdcolumn=password crypt=2 verbose=1'
    3. Indicación sobre qué usuarios están permitidos, si sus contraseñas han podido expirar, etc: 'account required pam_mysql.so user=vsftpd passwd=123456 host=localhost db=ftpd table=users usercolumn=username passwdcolumn=password crypt=2 verbose=1'
    4. Puedes recurrir a información adicional que puedes encontrar en https://github.com/NigelCunningham/pam-MySQL
    5. Observa que si utilizas algún tipo de encriptación de la contraseña diferente deberás modificar el valor del parámetro 'crypt'



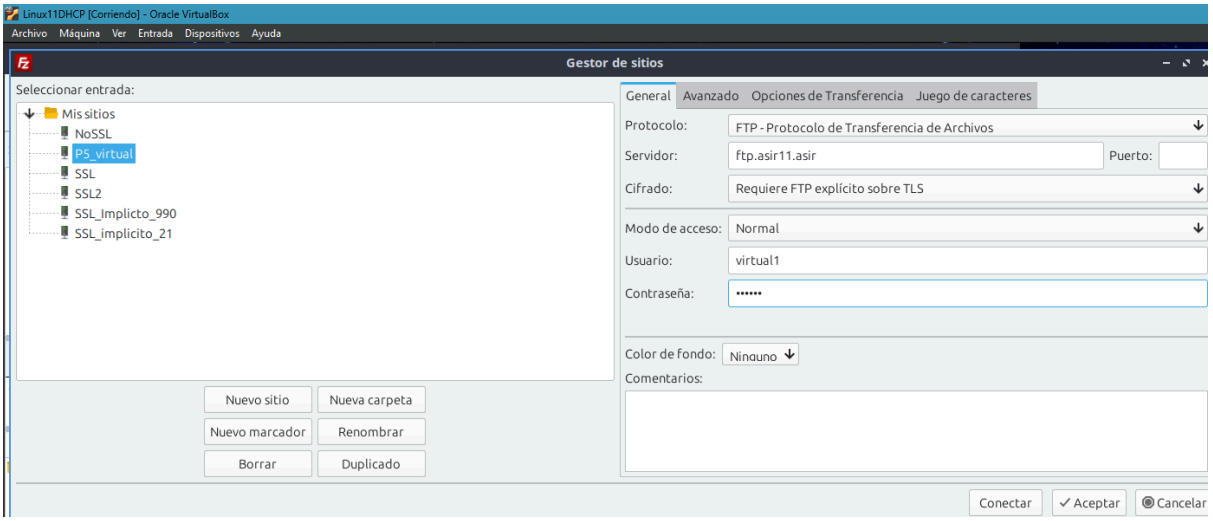
5. Sobre el servidor BOOKWORMXX crea un usuario denominado 'vsftpd' sin grupo ni shell, que será el que se use para mapear la autenticación del resto de usuarios (en nuestro caso el directorio '/var/www/virtual1' ya está creado. En caso de que no fuera así habría que crearlo y hacer propietario al usuario recién creado 'vsftpd').

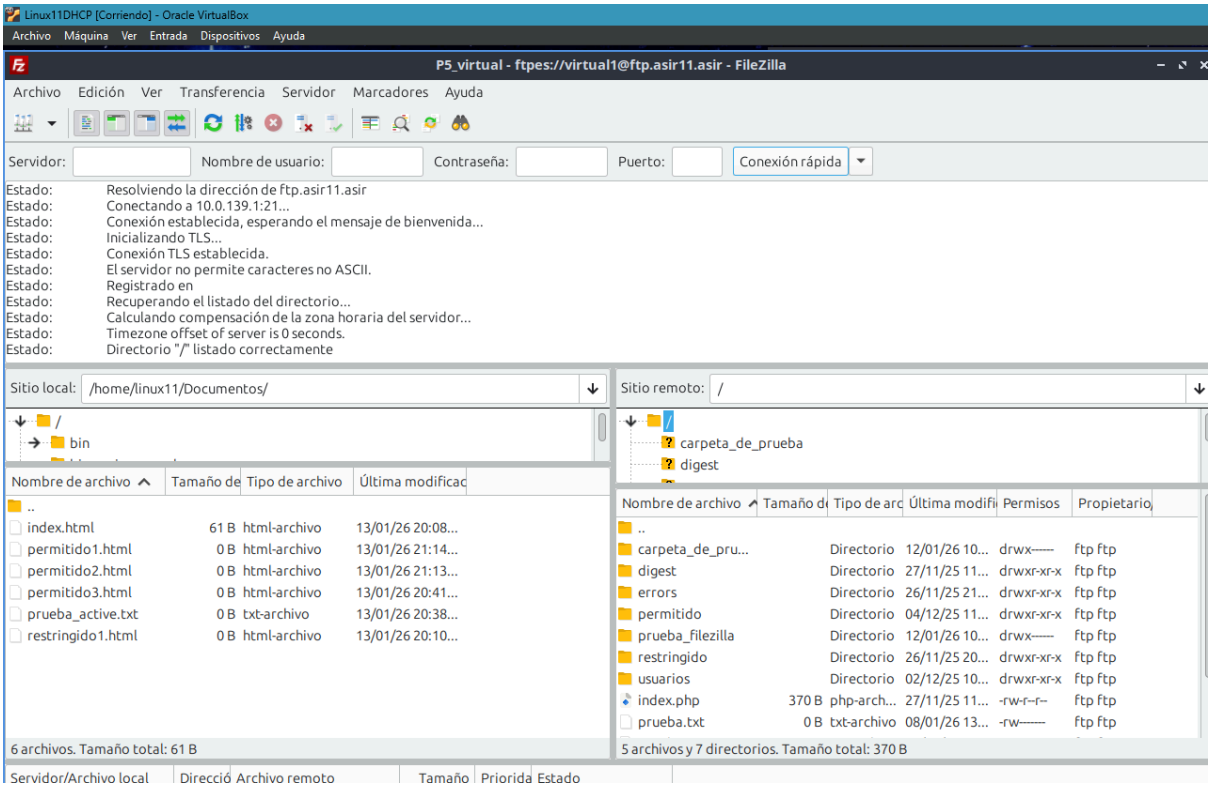


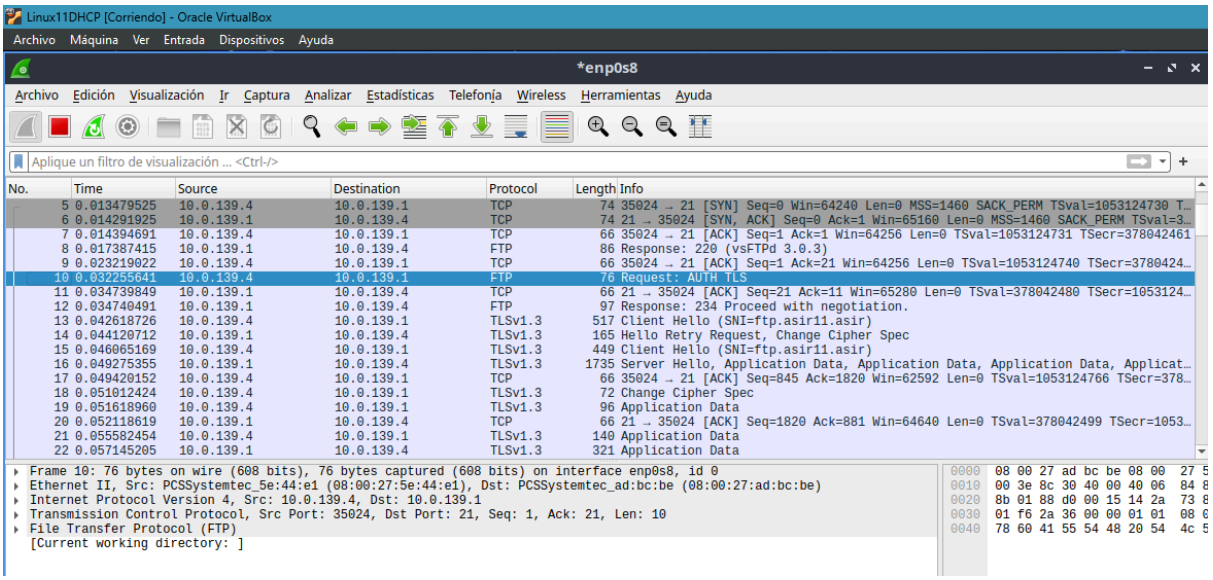
6. Es necesario reiniciar el servidor 'vsftpd' para que los cambios tengan efecto



7. Prueba una conexión con SSL explícito sobre el sitio ftp del usuario 'virtual1' y prueba que el funcionamiento sobre el directorio '/var/www/virtual1' es el esperado. En caso de no ser el esperado revisa los logs de vsftpd (vsftpd.log) y del servicio de autenticación (auth.log o ahora, en su defecto, journalctl) para ver posibles fallos o el funcionamiento correcto de la práctica.



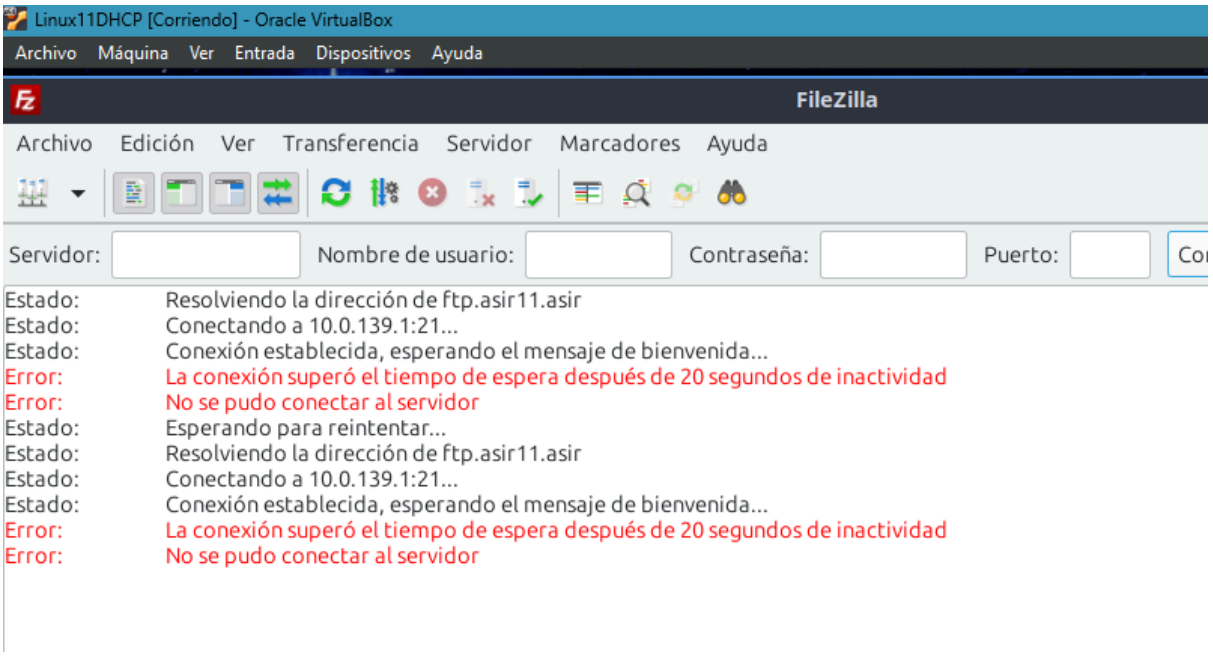

Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
P5_virtual - ftpes://virtual1@ftp.asir11.asir - FileZilla
Archivo Edición Ver Transferencia Servidor Marcadores Ayuda
Servidor: Nombre de usuario: Contraseña: Puerto: Conexión rápida
Estado: Resolviendo la dirección de ftp.asir11.asir
Estado: Conectando a 10.0.139.1:21...
Estado: Conexión establecida, esperando el mensaje de bienvenida...
Estado: Inicializando TLS...
Estado: Conexión TLS establecida.
Estado: El servidor no permite caracteres no ASCII.
Estado: Registrado en
Estado: Recuperando el listado del directorio...
Estado: Calculando compensación de la zona horaria del servidor...
Estado: Timezone offset of server is 0 seconds.
Estado: Directorio "/" listado correctamente
Sitio local: /home/linux11/Documentos/
Nombre de archivo Tamaño de Tipo de archivo Última modificac
index.html 61 B html-archivo 13/01/26 20:08...
permitido1.html 0 B html-archivo 13/01/26 21:14...
permitido2.html 0 B html-archivo 13/01/26 21:13...
permitido3.html 0 B html-archivo 13/01/26 20:41...
prueba_active.txt 0 B txt-archivo 13/01/26 20:38...
restringido1.html 0 B html-archivo 13/01/26 20:10...
6 archivos. Tamaño total: 61 B
Sitio remoto: /
carpeta_de_prueba
digest
Nombre de archivo Tamaño d Tipo de arc Última modifi Permisos Propietario
carpeta_de_pru... Directorio 12/01/26 10... drwx------ ftp ftp
digest Directorio 27/11/25 11... drwxr-xr-x ftp ftp
errors Directorio 26/11/25 21... drwxr-xr-x ftp ftp
permitido Directorio 04/12/25 11... drwxr-xr-x ftp ftp
prueba_filezilla Directorio 12/01/26 10... drwx------ ftp ftp
restringido Directorio 26/11/25 20... drwxr-xr-x ftp ftp
usuarios Directorio 02/12/25 10... drwxr-xr-x ftp ftp
index.php 370 B php-arch... 27/11/25 11... -rw-r--r-- ftp ftp
prueba.txt 0 B txt-archivo 08/01/26 13... -rw------- ftp ftp
5 archivos y 7 directorios. Tamaño total: 370 B
Servidor/Archivo local Direcció Archivo remoto Tamaño Priorida Estado


Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
*enp0s8
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
5 0.013479525 10.0.139.4 10.0.139.1 TCP 74 35024 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1053124730 T…
6 0.014291925 10.0.139.1 10.0.139.4 TCP 74 21 → 35024 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3…
7 0.014394691 10.0.139.4 10.0.139.1 TCP 66 35024 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1053124731 TSecr=378042461
8 0.017387415 10.0.139.1 10.0.139.4 FTP 86 Response: 220 (vsFTPd 3.0.3)
9 0.023219022 10.0.139.4 10.0.139.1 TCP 66 35024 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=1053124740 TSecr=3780424…
10 0.032255641 10.0.139.4 10.0.139.1 FTP 76 Request: AUTH TLS
11 0.034739849 10.0.139.1 10.0.139.4 TCP 66 21 → 35024 [ACK] Seq=21 Ack=11 Win=65280 Len=0 TSval=378042480 TSecr=1053124…
12 0.034740491 10.0.139.1 10.0.139.4 FTP 97 Response: 234 Proceed with negotiation.
13 0.042618726 10.0.139.4 10.0.139.1 TLSv1.3 517 Client Hello (SNI=ftp.asir11.asir)
14 0.044120712 10.0.139.1 10.0.139.4 TLSv1.3 165 Hello Retry Request, Change Cipher Spec
15 0.046065169 10.0.139.4 10.0.139.1 TLSv1.3 449 Client Hello (SNI=ftp.asir11.asir)
16 0.049275355 10.0.139.1 10.0.139.4 TLSv1.3 1735 Server Hello, Application Data, Application Data, Application Data, Applicat…
17 0.049420152 10.0.139.4 10.0.139.1 TCP 66 35024 → 21 [ACK] Seq=845 Ack=1820 Win=62592 Len=0 TSval=1053124766 TSecr=378…
18 0.051012424 10.0.139.4 10.0.139.1 TLSv1.3 72 Change Cipher Spec
19 0.051618960 10.0.139.4 10.0.139.1 TLSv1.3 96 Application Data
20 0.052118619 10.0.139.1 10.0.139.4 TCP 66 21 → 35024 [ACK] Seq=1820 Ack=881 Win=64640 Len=0 TSval=378042499 TSecr=1053…
21 0.055582454 10.0.139.4 10.0.139.1 TLSv1.3 140 Application Data
22 0.057145205 10.0.139.1 10.0.139.4 TLSv1.3 321 Application Data
Frame 10: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface enp0s8, id 0
Ethernet II, Src: PCSSystemtec_5e:44:e1 (08:00:27:5e:44:e1), Dst: PCSSystemtec_ad:bc:be (08:00:27:ad:bc:be)
Internet Protocol Version 4, Src: 10.0.139.4, Dst: 10.0.139.1
Transmission Control Protocol, Src Port: 35024, Dst Port: 21, Seq: 1, Ack: 21, Len: 10
File Transfer Protocol (FTP)
[Current working directory:]
0000 08 00 27 ad bc be 08 00 27 5
0010 00 3e 8c 30 40 00 40 06 84 8
0020 8b 01 88 d0 00 15 14 2a 73 8
0030 01 f6 2a 36 00 00 01 01 08 0
0040 78 60 41 55 54 48 20 54 4c 5

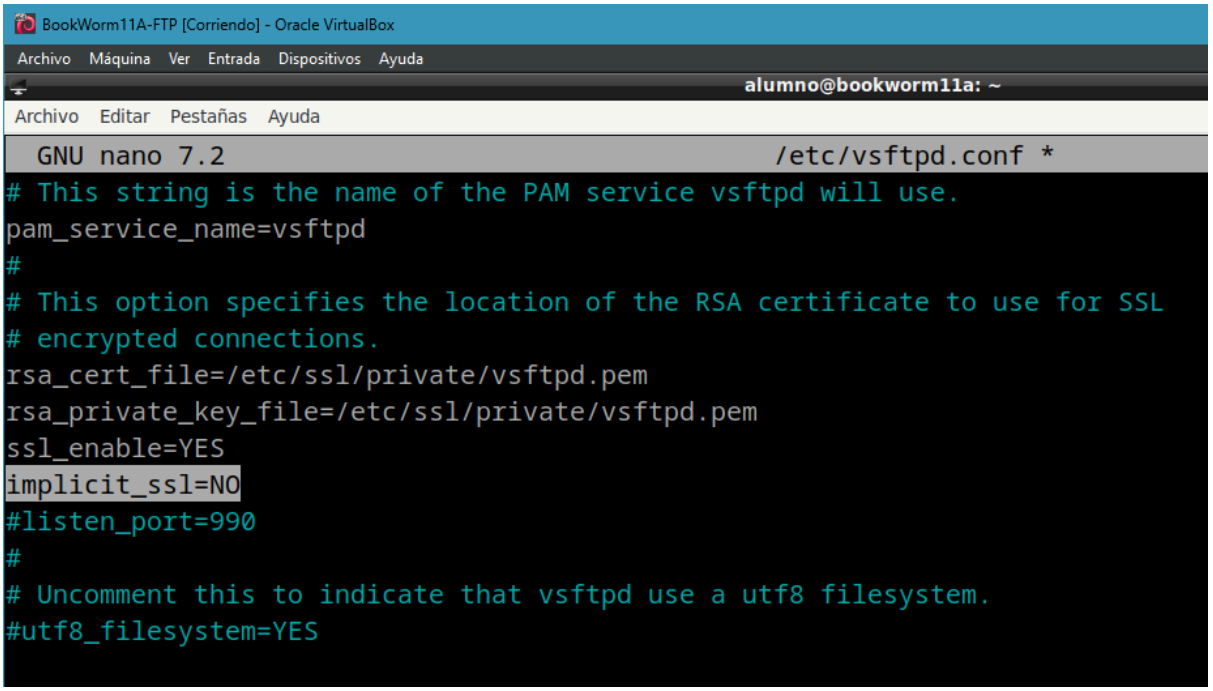
ERROR DE QUE NO SE CONECTA Y SOLUCIÓN:

¿Qué pasaba?

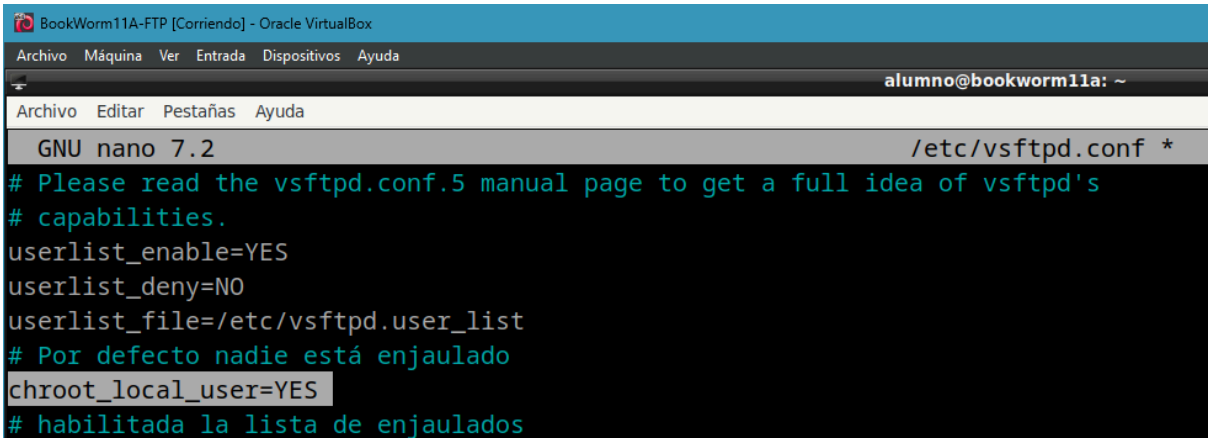
Había un conflicto con las configuraciones anteriores, las mas importantes era que el servidor solo funcionaba en ssl de forma implícita y el usuario virtual1 que era nuevo no estaba dentro de la lista de usuarios que se podían conectar al servicio



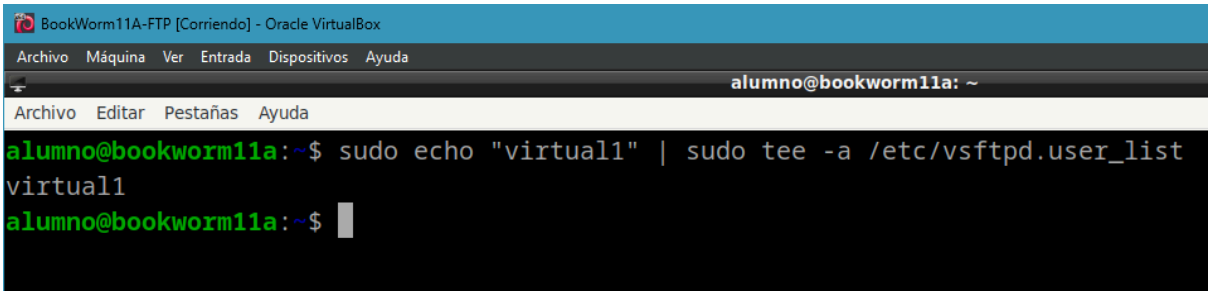
1. Desactivé el modo implícito para permitir que el servidor funcione en modo **Explícito (FTPES)** sobre el puerto 21. Esto permite que la conexión se inicie de forma estándar y luego se eleve a una capa segura mediante el comando AUTH TLS, evitando bloqueos en la negociación inicial



2. Activé esta directiva para obligar a que todos los usuarios locales (incluidos los usuarios virtuales mapeados) queden enjaulados en su directorio raíz al conectarse. Con esto, la carpeta /var/www/virtual1 se convierte en la raíz virtual (/) para el usuario, impidiéndole el acceso a directorios sensibles del sistema operativo

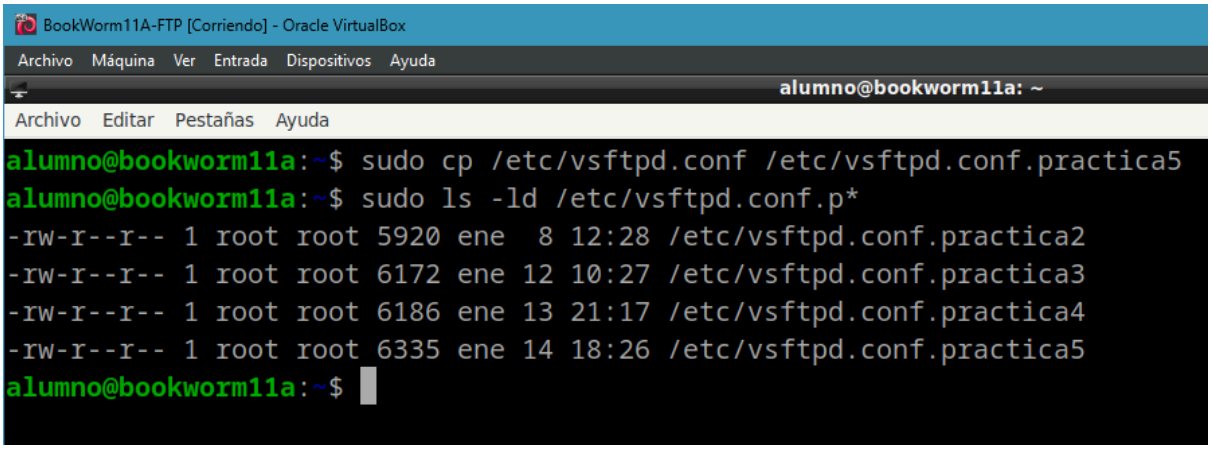


3. Añadí a el usuario de virtual1 a el archivo vsftpd.user_list para que pueda entrar



Recoge toda la información relevante así como las evidencias necesarias como capturas

Haz copia de seguridad de la configuración actual en vsftpd.conf.practica5



COMO VER LOS LOGS EN VSFTPD:

1. El Log de Transferencias (Quién sube/baja qué)

Como tienes activado `xferlog_enable=YES`, este archivo registra cada vez que alguien sube o baja un fichero.

Comando para verlo en tiempo real:

sudo tail -f /var/log/vsftpd.log

2. El Log de Protocolo (Lo que "hablan" cliente y servidor)

Como en tu Práctica 5 activaste log_ftp_protocol=YES, ahora tienes un registro detallado de cada comando (USER, PASS, CWD, STOR...) que envía FileZilla y qué responde el servidor.

Dónde está: Generalmente va al mismo archivo /var/log/vsftpd.log.

Para buscar algo específico (ej. fallos de login):

```
sudo grep "FAIL" /var/log/vsftpd.log
```

3. El Log del Sistema y Errores de Servicio (Cuando no arranca)

Si el servicio vsftpd ni siquiera arranca o si hay problemas con PAM (base de datos), esos errores no van al log de FTP, sino al log del sistema (systemd o auth).

Para ver errores de arranque o estado:

```
sudo journalctl -xeu vsftpd
```

Para ver problemas de autenticación (PAM/MySQL):

```
sudo tail -f /var/log/auth.log
```

(Aquí es donde viste antes las líneas rojas de pam_mysql conectando con la base de datos).

Escenario: Crear el usuario `virtual2` con contraseña `examen`

Paso 1: Insertarlo en la Base de Datos

El usuario no existe para Linux, así que hay que darlo de alta en el "libro de registro" (MariaDB).

Entra en la base de datos:
Bash
sudo mariadb

1. Selecciona la base de datos que creaste (probablemente se llama `ftp`):

   ```
   USE ftp;
   ```

2. Inserta el nuevo usuario. **¡OJO CRÍTICO!** Recuerda que en tu configuración de PAM pusiste `crypt=2`. Eso significa que la contraseña **TIENE** que ir cifrada con la función `PASSWORD()`. Si la pones "a pelo", no entrará.
   SQL

```
INSERT INTO usuarios (nombreusuario, password) VALUES ('virtual2', PASSWORD('examen'));
```

3. Sal de la base de datos:

```
EXIT;
```

Paso 2: Preparar su "Habitación" (La Jaula)

Aunque el usuario esté en la base de datos, si intenta entrar y no tiene "casa", el servidor le dará un error (normalmente *500 OOPS: cannot change directory*). Tienes que crearla manualmente.

Crea el directorio usando el nombre exacto del usuario:

```
sudo mkdir -p /var/www/virtual2
```

1. **El paso que suspende a la gente:** Asignar los permisos. Recuerda: El dueño de la carpeta **NO** es `virtual2` (porque no existe en Linux), ni `root`. El dueño tiene que ser el "usuario puente" (`vsftpd` o `ftp`, según como lo llamaras en `guest_username`). En tu caso es `vsftpd`.

   ```
   sudo chown vsftpd:nogroup /var/www/virtual2
   ```

2. Dale permisos correctos (Lectura/Escritura para el dueño, Lectura para el resto):

   ```
   sudo chmod 755 /var/www/virtual2
   ```

Paso 3: La Trampa de la "Lista Blanca" (¡IMPORTANTE!)

¿Recuerdas el error `530 Permission denied` que te dio hace un rato? Si en tu examen tienes activada la directiva `userlist_enable=YES` (la lista VIP), el usuario `virtual2` **NO** entrará hasta que lo escribas en la lista.

Añádelo a la lista de permitidos:

echo "virtual2" | sudo tee -a /etc/vsftpd.user_list

1. *(Si en el examen el profesor te hace desactivar la lista con `userlist_enable=NO`, te saltas este paso, pero mejor hazlo por si acaso).*

Paso 4: Prueba de Fuego (FileZilla)

No necesitas reiniciar el servicio `vsftpd` (porque la base de datos se lee en tiempo real), pero si quieres ir a lo seguro por si tocaste la lista de usuarios: `sudo systemctl restart vsftpd`.

1. Abre FileZilla.
2. **Nuevo Sitio:**
    - **Host:** `ftp.asir11.asir` (o la IP).
    - **Protocolo:** FTP - Explícito sobre TLS.
    - **Usuario:** `virtual2`
    - **Contraseña:** `examen`
3. **Conectar.**

Si entra y ves la carpeta vacía `/`, es que has triunfado.