Práctica Ftp – Vsftp

Adjuntos	2020-03 Practica FTP.pdf

Respuestas:

para realizar toda la configuracion elabore un script basico en bash:

```
#!/bin/bash

set -e # Salir en caso de error
set -o pipefail # Captura errores dentro de pipes

VSFTPD_CONF="/etc/vsftpd/vsftpd.conf"
BANNER_MESSAGE="Bienvenido al servidor FTP de la empresa!"
USER_NAME="userftp1"
USER_PASS="password123"
ANON_DIR="/var/anonymous/publico"

is_installed() {
    yum list installed "$@" >/dev/null 2>&1
}

# Función para actualizar o añadir configuración
update_config() {
    local key="$1"
    local value="$2"
    if grep -qE "^\s*#\?\s*$key=" "$VSFTPD_CONF"; then
        sudo sed -i "s|^\(\s*#\?\s*$key=\).*|\1$value|" "$VSFTPD_CONF"
    else
        echo "$key=$value" | sudo tee -a "$VSFTPD_CONF" > /dev/null
    fi
}

if ! is_installed vsftpd; then
    echo "Instalando vsftpd..."
    sudo yum install -y vsftpd
else
    echo "vsftpd ya está instalado."
fi

if [[ -f $VSFTPD_CONF ]]; then
    echo "Creando backup del archivo de configuración..."
    sudo cp "$VSFTPD_CONF" "$VSFTPD_CONF.bak"

    update_config "anonymous_enable" "YES"
    update_config "local_enable" "YES"
    update_config "banner_file" "/etc/ftp_banner"
```

```
    update_config "chroot_local_user" "YES"
else
    echo "Error: Archivo $VSFTPD_CONF no encontrado."
    exit 1
fi

echo "$BANNER_MESSAGE" | sudo tee /etc/ftp_banner > /dev/null

if id "$USER_NAME" &>/dev/null; then
    echo "El usuario $USER_NAME ya existe."
else
    sudo useradd "$USER_NAME"
    echo "$USER_NAME:$USER_PASS" | sudo chpasswd
fi

sudo mkdir -p "$ANON_DIR"
update_config "anon_root" "$ANON_DIR"

sudo systemctl restart vsftpd

echo "Configuración de vsftpd completada con éxito."
```

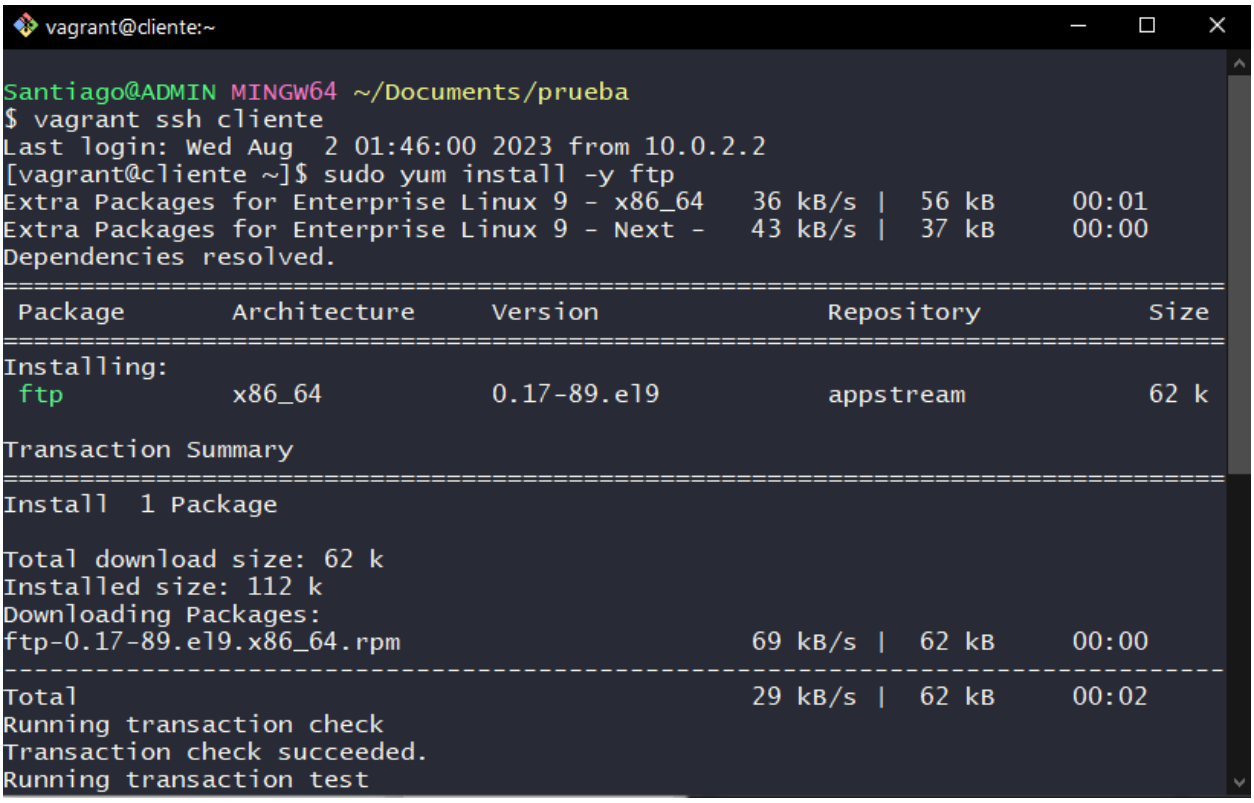
4.1.

- **Usuarios anónimos:** Son aquellos que pueden acceder al servidor FTP sin necesidad de autenticarse con un nombre de usuario y contraseña específicos. Normalmente, tienen acceso a una parte limitada del servidor, principalmente para descargar archivos.
- **Usuarios reales o locales:** Son usuarios que tienen cuentas en el sistema operativo del servidor. Para acceder al servidor FTP, deben autenticarse con su nombre de usuario y contraseña del sistema.
- **Usuarios invitados:** Son usuarios que, aunque requieren autenticación, no tienen una cuenta completa en el sistema operativo. Suelen tener restricciones específicas en su acceso y actividades dentro del servidor.

4.2. Con la configuración por defecto de vsftpd, los usuarios anónimos son ubicados en el directorio `/var/ftp/`, mientras que los usuarios reales son ubicados en su directorio home, generalmente `/home/nombre_usuario`.

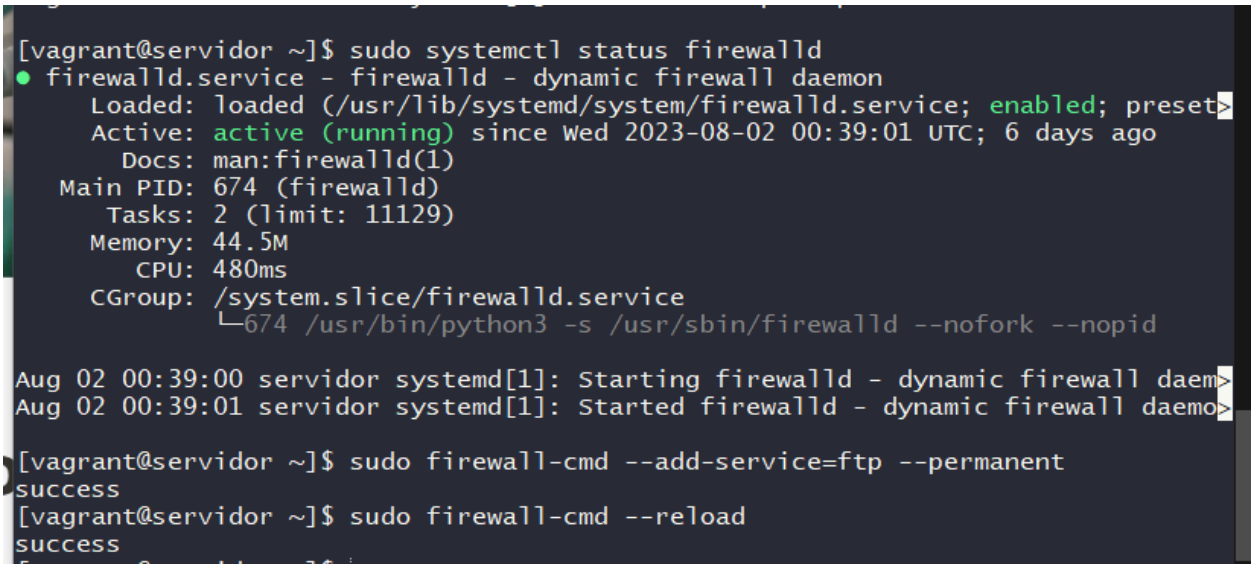
4.3. Para subir y bajar archivos al servidor de FTP, se puede usar un cliente FTP como FileZilla. Una vez conectado al servidor, simplemente se arrastran y sueltan los archivos entre el cliente y el servidor.

desde comandos

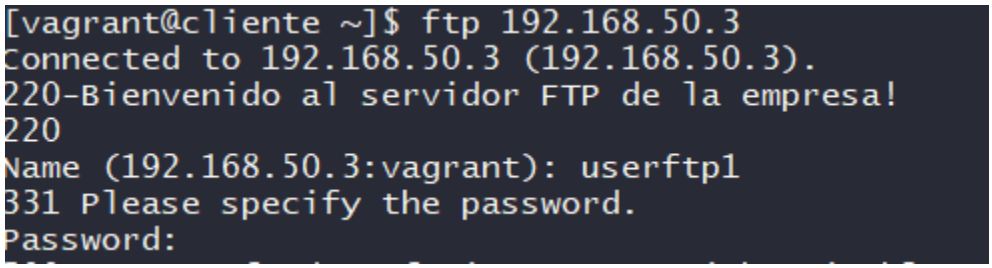


en un inicio no me deja conectarme al servidor ftp, por lo que tengo realizar unos ajustes en el servidor para que permita el trafico con los siguientes comandos:

```
sudo firewall-cmd --add-service=ftp --permanent
sudo firewall-cmd --reload
```



ahora si me conecto desde mi cliente y obtengo lo siguiente:



en un incio me salio el siguiente error: `500 OOPS: vsftpd: refusing to run with writable root inside chroot()` es una medida de seguridad en `vsftpd`. Sucede cuando intentas enjaular (chroot) a un usuario en su directorio principal y ese directorio es escribible por el usuario.

La razón de esta medida es evitar que un usuario enjaulado pueda obtener acceso elevado en el sistema al manipular archivos dentro de su directorio chroot. Entonces realice lo siguiente:

1. que el directorio principal del usuario no sea escribible para el propio usuario:

`sudo chmod a-w /home/userftp1`

Esto hará que el directorio principal no sea escribible. Sin embargo, es posible que necesites crear un subdirectorio dentro de ese directorio principal para que el usuario pueda escribir archivos.

```
sudo mkdir /home/userftp1/upload
sudo chown userftp1:userftp1 /home/userftp1/upload
```

```
[vagrant@servidor ~]$ sudo chmod a-w /home/userftp1
[vagrant@servidor ~]$ sudo mkdir /home/userftp1/upload
[vagrant@servidor ~]$ sudo chown userftp1:userftp1 /home/userftp1/upload
```

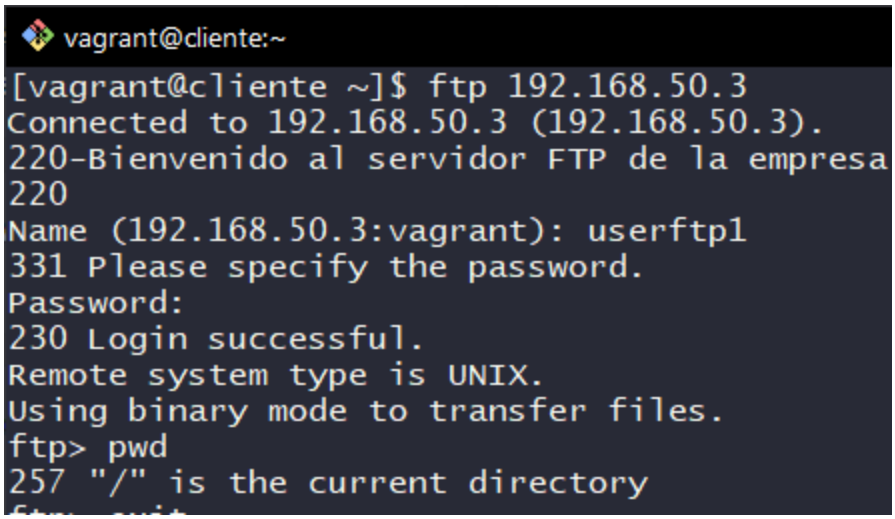
2. otra solucion seria cambiar la configuración de `vsftpd`:

   `chroot_local_user=NO`

por seguridad se realiza la primera opcion, donde proporciono un subdirectorio para las operaciones de lectura/escritura.

4.4. Para cambiar el mensaje de bienvenida, se debe modificar la directiva `banner_file` en `/etc/vsftpd.conf` y apuntarla al archivo que contiene el nuevo mensaje.

4.5. Para enjaular a los usuarios reales, se debe establecer la directiva `chroot_local_user=YES` en `/etc/vsftpd.conf`. Si cambias el valor de `chroot_local_user` a NO, los usuarios podrán navegar por todo el sistema de archivos del servidor.



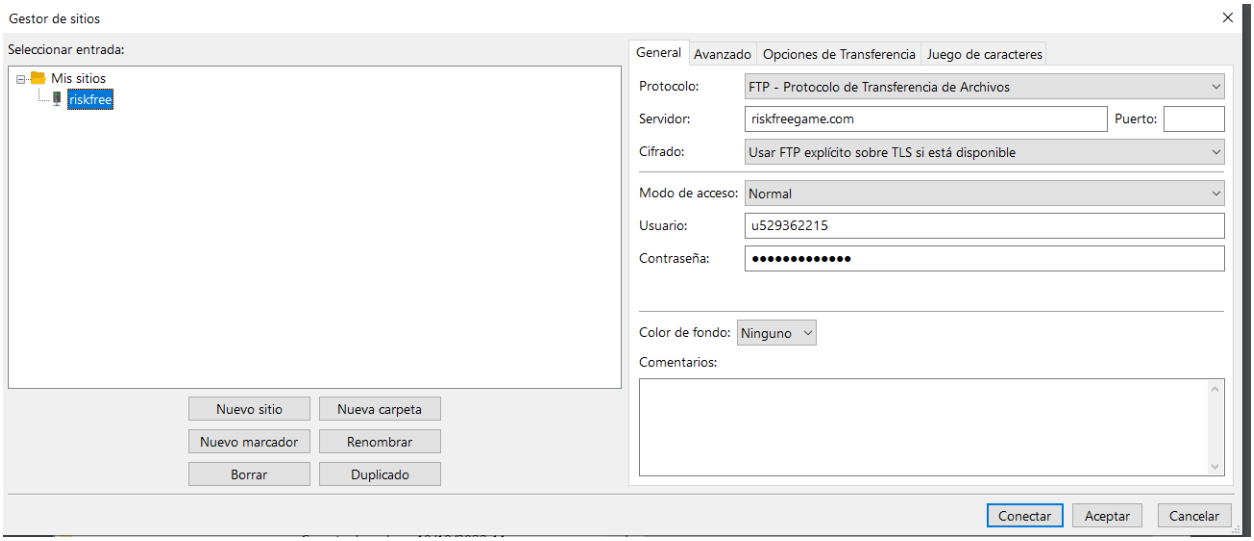
aqui por ejemplo en la imagen los usuarios estan enjaulados.

4.6. Para restringir el acceso de usuarios reales al servidor FTP, se debe establecer la directiva `local_enable=NO` en `/etc/vsftpd.conf`.

4.7. Para cambiar el directorio público de los usuarios anónimos, se debe modificar la directiva `anon_root` en `/etc/vsftpd.conf` y establecerla en `/var/anonymous/publico`.

4.8. Hay múltiples clientes FTP gráficos, como FileZilla, que son fáciles de instalar y usar. Una vez instalado, puedes conectarlo al servidor FTP introduciendo la dirección IP del servidor, el puerto (normalmente 21 para FTP), y las credenciales de usuario.

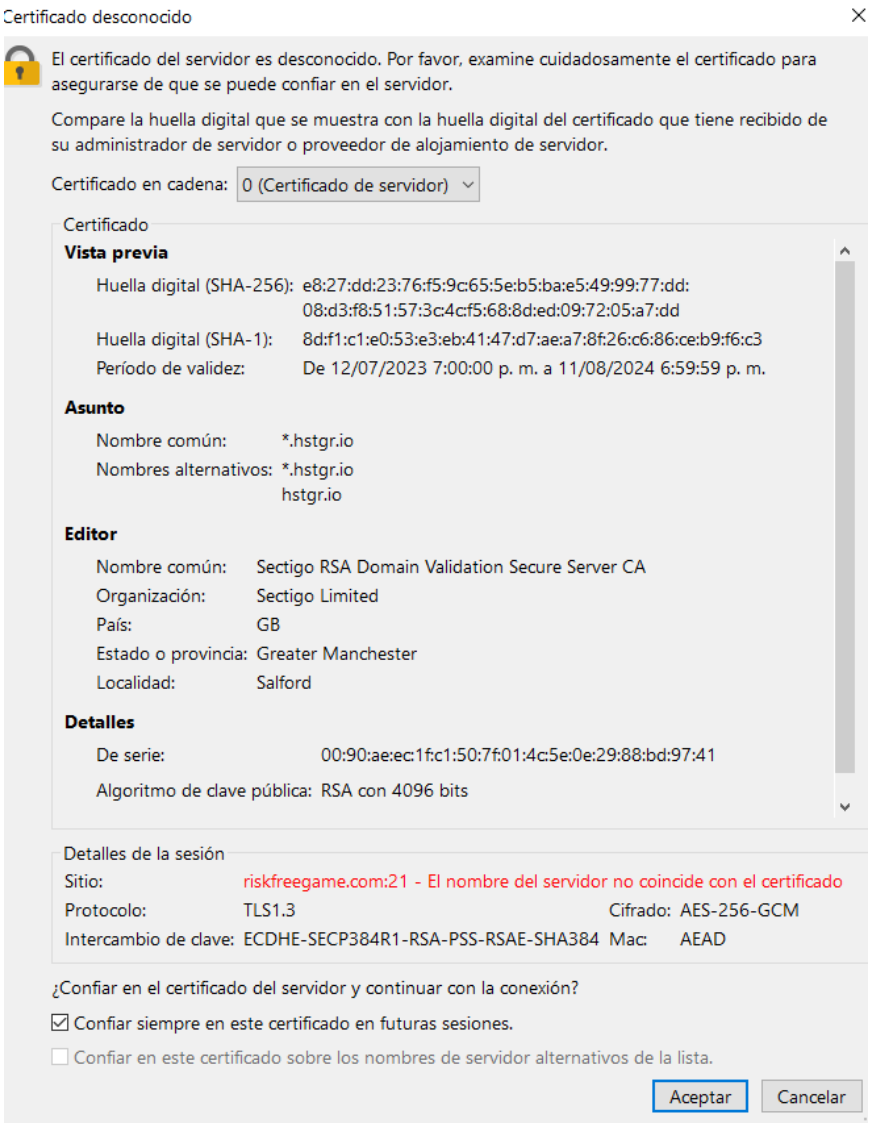
Yo escogi FileZilla, y agregue la siguiente informacion para poder conectarme



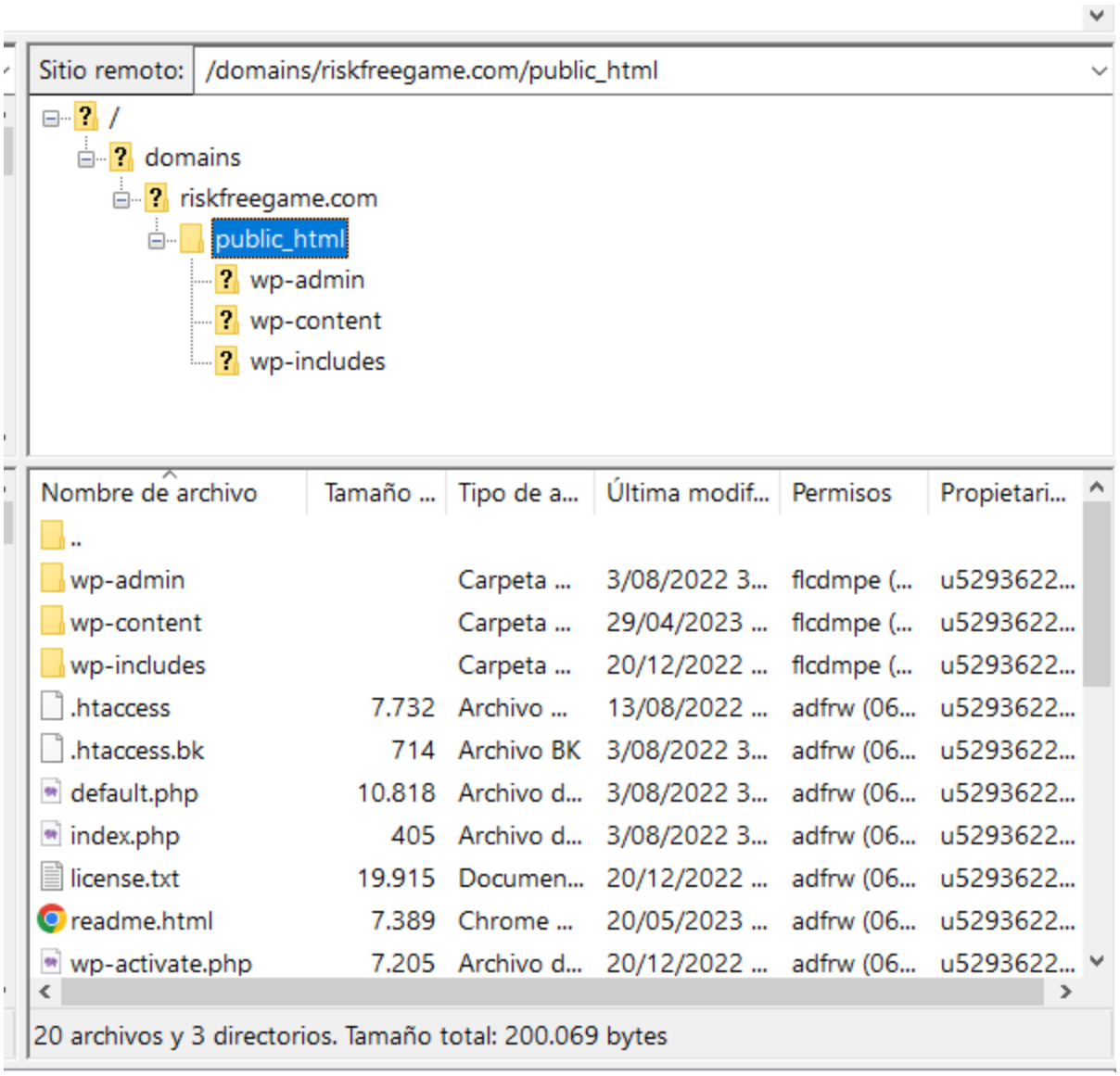
Logs:

```
Estado:  Resolviendo la dirección de riskfreegame.com
Estado:  Conectando a [2a02:4780:13:911:0:1f8d:6d27:1]:21...
Estado:  Falló intento de conexión con "ETIMEDOUT - El intento de conexión superó el tiempo de espera", intentando la siguiente dirección.
Estado:  Conectando a 45.132.157.104:21...
Estado:  Conexión establecida, esperando el mensaje de bienvenida...
Estado:  Inicializando TLS...
Estado:  Conexión TLS establecida.
Estado:  Registrado en
Estado:  Recuperando el listado del directorio...
Estado:  Directorio "/domains/riskfreegame.com/public_html" listado correctamente
```

en un inicio me pide aceptar el siguiente certificado del servidor:

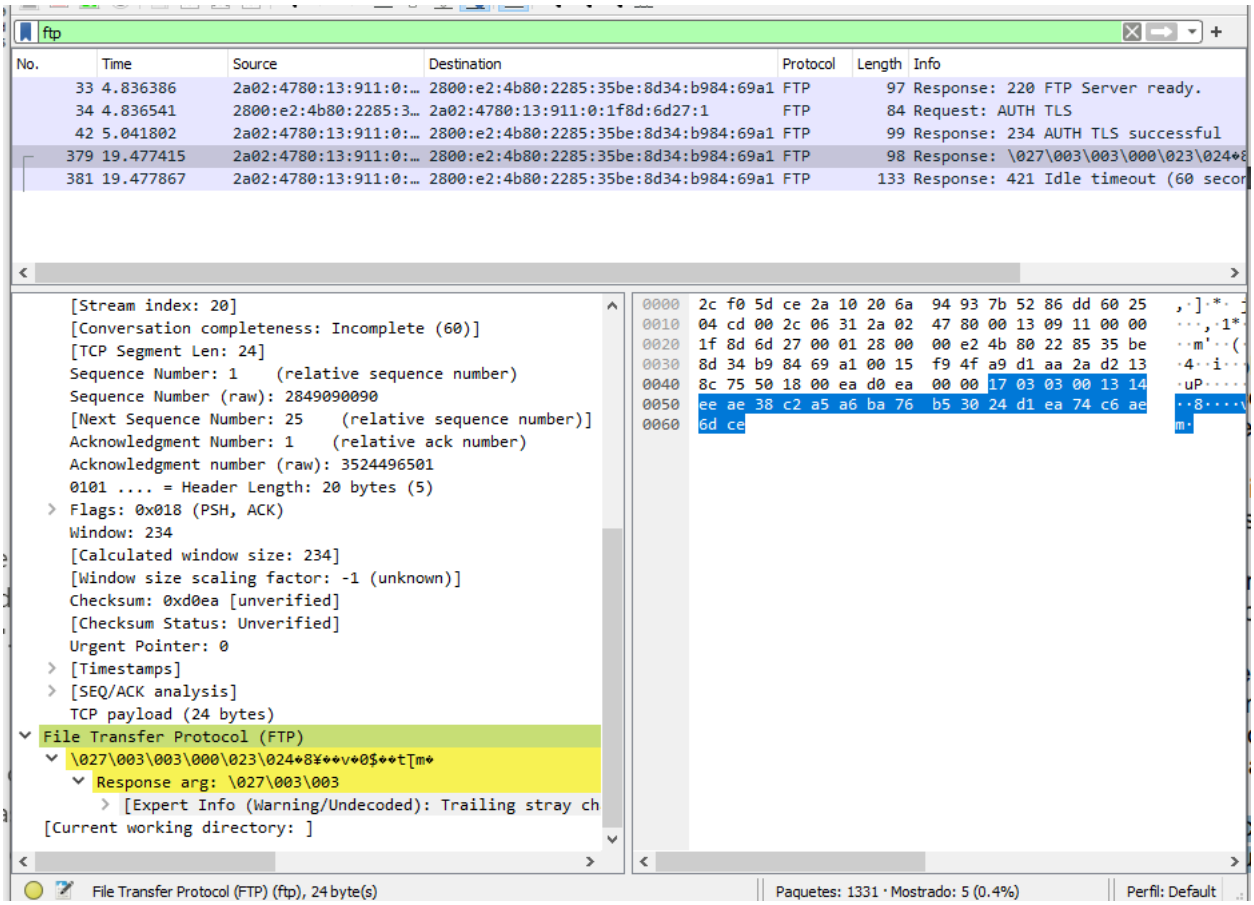


entonces ya una vez conectado puedo navegar por los archivos que tengo en mi sitio remoto:



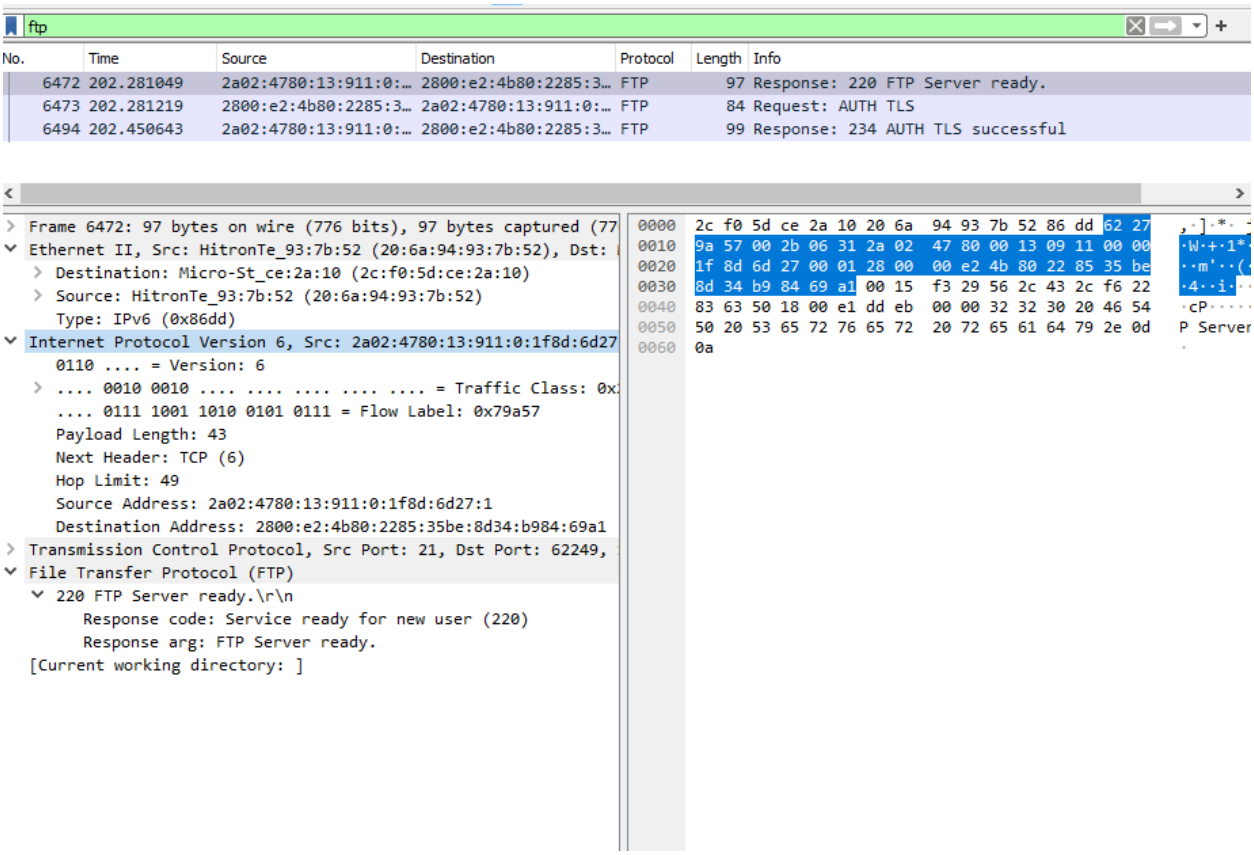
4.9.

Cuando subo archivos (FTPS):



. Las secuencias como `\027\003\003\000\023\024` no son legibles porque están cifradas. Si estuvieras usando FTP plano (sin TLS), aquí verías comandos FTP en texto claro como `STOR` (para almacenar un archivo), pero debido al cifrado, esos detalles están ocultos. Otros comandos (comandos como `USER` y `PASS`), transferencia de archivos (comandos como `STOR` para almacenar y `RETR` para recuperar) y desconexión (`QUIT`) son los que veriamos si la conexion no estuviera cifrada.

Cuando descargo/bajo archivos:



1. `220 FTP Server ready.`

Este es un mensaje de respuesta estándar que indica que el servidor FTP está listo para aceptar una conexión. El código `220` es un código de respuesta estándar de FTP que indica un mensaje de "servicio listo".

2. `AUTH TLS`

Este comando indica que el cliente desea establecer una conexión segura utilizando TLS (Transport Layer Security). En otras palabras, el cliente está solicitando que la sesión se cifre para proteger cualquier dato que se transmita, incluidas las credenciales.

3. `234 AUTH TLS successful`

Este es el mensaje de respuesta del servidor FTP indicando que ha aceptado la solicitud del cliente para usar TLS y que la encriptación ha sido establecida con éxito. La sesión ahora es segura, y cualquier dato transmitido entre el cliente y el servidor será cifrado.

Explicación:

La secuencia de comandos y respuestas que has observado es parte del proceso de "negociación" para establecer una conexión FTP segura utilizando TLS, comúnmente conocida como FTPS (no confundir con SFTP, que es FTP sobre SSH).

El proceso básico es el siguiente:

1. El cliente se conecta al servidor FTP.
2. El servidor indica que está listo con `220 FTP Server ready`.
3. El cliente solicita una sesión segura con `AUTH TLS`.
4. El servidor acepta y establece una sesión segura, luego responde con `234 AUTH TLS successful`.

A partir de este punto, la conexión es segura y tanto el cliente como el servidor pueden intercambiar comandos y datos de manera cifrada.

Modo de conexión FTP: FTP opera en dos modos distintos: activo y pasivo. En el modo activo, el servidor inicia una conexión con el cliente. En el modo pasivo, es el cliente el que inicia la conexión con el servidor. En Wireshark, si ves que el cliente es el que inicia la conexión de datos (en lugar del servidor), entonces están utilizando el modo pasivo. La mayoría de los clientes modernos, incluido FileZilla, usan el modo pasivo por defecto debido a problemas de compatibilidad con firewalls y NAT en el modo activo.

En lo paquetes podriamos oberserva si se está utilizando el modo activo o pasivo. Para eso, deberías buscar comandos FTP adicionales en la captura, como `PORT` (que indica modo activo) o `PASV` (que indica modo pasivo).

#!/bin/bash

set -e
set -o pipefail

VSFTPD_CONF="/etc/vsftpd/vsftpd.conf"
BANNER_MESSAGE="Bienvenido al servidor FTP de la empresa!"
USER_NAME="userftp1"

USER_PASS="password123"
ANON_DIR="/var/anonymous/publico"

is_installed() {
yum list installed "$@" >/dev/null 2>&1
}

Función para actualizar o añadir configuración

update_config() {
local key="$1"
local value="$2"
if grep -qE "^\s*#\?\s*$key=" "$VSFTPD_CONF"; then
sudo sed -i "s|^\(\s*#\?\s*$key=\).*|\1$value|" "$VSFTPD_CONF"
else
echo "$key=$value" | sudo tee -a "$VSFTPD_CONF" > /dev/null
fi
}

if ! is_installed vsftpd; then
echo "Instalando vsftpd..."
sudo yum install -y vsftpd
else
echo "vsftpd ya está instalado."
fi

if [[-f $VSFTPD_CONF]]; then
echo "Creando backup del archivo de configuración..."
sudo cp "$VSFTPD_CONF" "$VSFTPD_CONF.bak"

```
update_config "anonymous_enable" "YES"
update_config "local_enable" "YES"
update_config "banner_file" "/etc/ftp_banner"
update_config "chroot_local_user" "YES"
```

```
else
echo "Error: Archivo $VSFTPD_CONF no encontrado."
exit 1
fi

echo "$BANNER_MESSAGE" | sudo tee /etc/ftp_banner > /dev/null

if id "$USER_NAME" &>/dev/null; then
echo "El usuario $USER_NAME ya existe."
else
sudo useradd "$USER_NAME"
echo "$USER_NAME:$USER_PASS" | sudo chpasswd
fi

sudo mkdir -p "$ANON_DIR"
update_config "anon_root" "$ANON_DIR"

sudo systemctl restart vsftpd

echo "Configuración de vsftpd completada con éxito."
```