DAW Práctica 4.4:

En esta actividad se establecerá una conexión TLS para establecer comunicaciones seguras y cifradas entre dos sistemas.

Actividad previa:

Responde a las siguientes preguntas:

- ¿Qué es SSH?
- ¿Qué es TLS?
- ¿Para qué vale una función resumen HASH?
- Explica brevemente cómo funciona el cifrado de clave pública o asimétrica.

Requisitos:

Servidor proFTPD y FileZilla instalado junto al conocimiento de su funcionamiento.

Procedimiento:

1. Como venimos viendo a lo largo del curso para los protocolos seguros es necesaria la creación de un certificado. En nuestro caso realizaremos uno autofirmado. Podemos usar diferentes comandos vistos anteriormente o utilizar una herramienta que nos proporciona proftpd:

   ```
   proftpd-gencert
   ```

2. Podemos mover tanto el certificado como la clave a una carpeta nueva. Deberemos asegurarnos de que tengan los permisos necesarios:

   ```
   chmod 600 proftpd.key
   chmod 644 proftpd.crt
   ```

3. ¿Qué permisos le hemos otorgado a los archivos?

4. En el fichero de configuración de proftpd aparece una referencia a un archivo de configuración para configurar el protocolo FTPS, pero por defecto está comentada. Descomenta la referencia y accede a dicho fichero de configuración.

5. En dicho fichero descomenta las siguientes líneas modificando la configuración si es necesario (**la ruta de la clave y del certificado debe indicar donde se encuentran esos ficheros**):

```
<IfModule mod_tls.c>
        TLSEngine                               on
        TLSLog                                  /var/log/proftpd/tls.log
        TLSProtocol                             SSLv23
        TLSRSACertificateFile                   /etc/ssl/certs/proftpd.crt
        TLSRSACertificateKeyFile                /etc/ssl/private/proftpd.key
#
# CA the server trusts...
#TLSCACertificateFile                    /etc/ssl/certs/CA.pem
# ...or avoid CA cert and be verbose
#TLSOptions                         NoCertRequest EnableDiags
# ... or the same with relaxed session use for some clients (e.g. FireFtp)
#TLSOptions                         NoCertRequest EnableDiags NoSessionReuseRequired
#
#
# Per default drop connection if client tries to start a renegotiate
# This is a fix for CVE-2009-3555 but could break some clients.
#
#TLSOptions                                                      AllowClientRenegotiations
#
# Authenticate clients that want to use FTP over TLS?
#
        TLSVerifyClient                         off
#
# Are clients required to use FTP over TLS when talking to this server?
#
        TLSRequired                             on
#
# Allow SSL/TLS renegotiations when the client requests them, but
# do not force the renegotations.  Some clients do not support
# SSL/TLS renegotiations; when mod_tls forces a renegotiation, these
# clients will close the data connection, or there will be a timeout
# on an idle data connection.
#
        TLSRenegotiate                          required off
</IfModule>
```

6. En el punto anterior hemos estado configurando una directiva que modifica un módulo. Accede al archivo /etc/proftpd/modules.conf y descomenta la instrucción que carga ese módulo.

7. En el fichero de configuración del punto anterior, justo encima de la instrucción que hemos descomentado nos indica la necesidad de instalar un módulo para el funcionamiento de TLS. **Recuerda actualizar los repositorios antes de cualquier descarga.**

```
apt-get install proftpd-mod-crypto
```

8. Reinicia el servicio.

9. Prueba el acceso desde Filezilla y nos mostrará el certificado creado anteriormente.

10. Una vez aceptado el certificado podemos observar como se ha establecido el protocolo seguro.