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?

SSH (Secure Shell) es un protocolo de red seguro que permite la comunicación cifrada entre un cliente y un servidor, normalmente para la administración remota de sistemas y la transferencia segura de archivos.

* ¿Qué es TLS?

TLS (Transport Layer Security) es un protocolo criptográfico que garantiza la seguridad de las comunicaciones en la web. Se utiliza para proteger datos sensibles en la transferencia entre dos partes, como en HTTPS, correos electrónicos, VPNs y VoIP.

* ¿Para qué vale una función resumen HASH?

Una función resumen HASH es un algoritmo que toma una entrada (mensaje o archivo) y genera un valor único de longitud fija. Se usa para verificar la integridad de datos y autenticación.

* Explica brevemente cómo funciona el cifrado de clave pública o asimétrica.

El cifrado asimétrico usa dos claves diferentes:

Clave pública: Se comparte libremente y se usa para cifrar datos.

Clave privada: Se mantiene en secreto y se usa para descifrar los datos.

# 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

Texto

Descripción generada automáticamente

1. 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





Texto

Descripción generada automáticamente

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

Los permisos asignados a los archivos son:

proftpd.key (chmod 600):

Propietario: Lectura (r) y Escritura (w)

Grupo: Sin permisos

Otros: Sin permisos

Esto asegura que solo el propietario puede leer y modificar el archivo, lo cual es adecuado para archivos sensibles como claves privadas.

proftpd.crt (chmod 644):

Propietario: Lectura (r) y Escritura (w)

Grupo: Lectura (r)

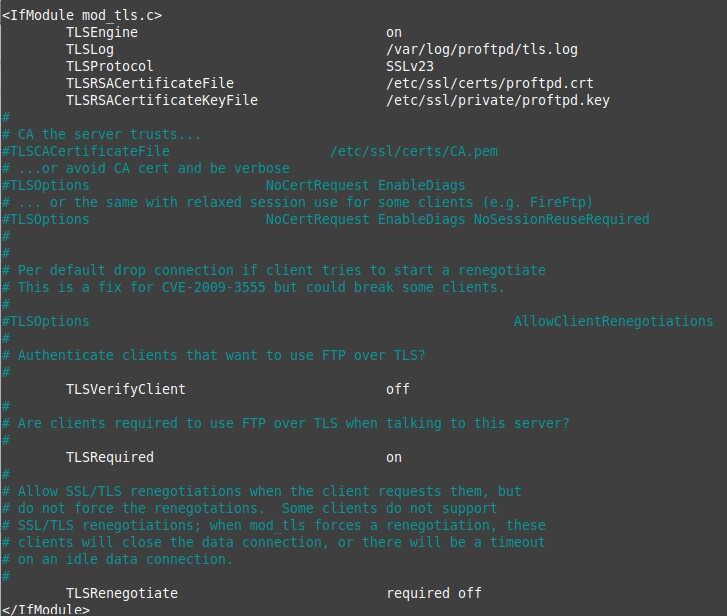
Otros: Lectura (r)

Estos permisos permiten que el propietario lea y modifique el archivo, mientras que el grupo y otros usuarios solo pueden leerlo. Esto es común para certificados públicos, ya que deben ser accesibles para leer por los servicios que los utilizan.

1. 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.



1. 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**):



Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

1. 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.



1. 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

Texto

Descripción generada automáticamente con confianza media

1. Reinicia el servicio.



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



Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

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

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente 