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



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
2. **Generar la clave privada (proftpd.key) y el certificado autofirmado (proftpd.crt)**

****

**Generar el certificado autofirmado (proftpd.crt)**:



Luego, genera el certificado autofirmado con:

Captura de pantalla de un celular

Descripción generada automáticamente

Configuración de ProFTPD para usar TLS/SSL

Texto

Descripción generada automáticamente



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

Los permisos que mencionas son los adecuados para los archivos de clave privada (proftpd.key) y el certificado público (proftpd.crt), ya que aseguran que solo los usuarios autorizados puedan acceder a la clave privada y que el certificado público sea accesible para todos.

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.

Texto

Descripción generada automáticamente

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

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



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

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