Ejercicio 2

Habilitar ssl en el servidor proftpd usando el módulo TLS

Pasos a seguir:

1. Instalar **OpenSSL**
2. Crear una **llave privada**
3. Crear un **CSR** (Certificate Signing Request)
4. Generar el **certificado SSL**
5. Habilitar el módulo **tls** en proftpd
6. Configurar **tls.conf**
7. Verificar la conexión segura a través de un cliente **ftp**. (filezilla)

Realizamos paso a paso cada uno de los puntos:

1. Instalar OpenSSL

OpenSSL es una api que proporciona un entorno adecuado para encriptar los datos enviados a otra computadora dentro de una red y a su vez desencriptarlos adecuadamente por el receptor, evitando así, el acceso a la información por intrusos con la utilización de sniffer.

Para instalar OpenSSL debes ejecutar el siguiente comando en tu terminal:

- sudo apt-get update
- sudo apt-get install openssl

Una vez instalado vamos a usar esta herramienta para crear la llave privada de nuestro certificado y

2. Crear una **llave privada**

La llave privada nos será útil para la generación del certificado. Una vez creado, nuestro certificado SSL dependerá de esta llave para la implementación del mismo en cualquier servicio que requiera una conexión segura.

En este ejemplo vamos a crear una llave de 1024 bits.

En un terminal escribimos:

- openssl genrsa -out server.key 1024

https://www.certsuperior.com/Blog/llave-publica-y-llave-privada-que-son-y-como-funcionan

3. Crear un **CSR** (Certificate Signing Request)

Un CSR es la base para un certificado SSL, en el se definen datos como el dominio, organización, ubicación, información de contacto, entre otros.

Es importante destacar que estos pasos también son necesarios cuando vas a adquirir un certificado SSL de un proveedor autorizado, durante la gestión del mismo, el proveedor va a solicitar este archivo para crear tu certificado. Por lo tanto, debemos tener mucho cuidado en que la información que ingresamos sea correcta.

Si te equivocas no te preocupes, puedes generarlo las veces que quieras.

Para generar el CSR debes ejecutar el siguiente comando, si te fijas uno de los parámetros es la llave privada que acabamos de crear:

- openssl req -new -key server.key -out server.csr

Al ejecutar este comando vendrán una serie de preguntas que rellenaremos para generar nuestra petición de certificado

4. Generar el **certificado SSL**

Para generar el certificado SSL vamos a necesitar tanto la llave privada como el CSR que acabamos de crear.

Para generar el certificado SSL debemos ejecutar el siguiente comando:

- openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

5. **Almacenar** el certificado SSL en la ruta correcta

Primero vamos a copiar los archivos a la carpeta **/etc/ssl/certs.**

- sudo cp server.crt /etc/ssl/certs/server.crt
- sudo cp server.key /etc/ssl/private/server.key

6. Habilitamos el módulo **tls** en proftpd

Editamos proftpd.conf y descomentamos **Include /etc/proftpd/tls.conf**

7. Configuramos el módulo **tls** en proftpd

Asegurate que tienes descomentado en proftpd.conf:
Include /etc/proftpd/tls.conf

Editamos **tls.conf** e incluimos al menos las directivas:

```
TLSEngine                   on
TLSLog                      /var/log/proftpd/tls.log
TLSProtocol                 SSLv23
TLSRSACertificateFile       /etc/ssl/certs/server.crt
TLSRSACertificateKeyFile    /etc/ssl/private/server.key
TLSOptions                  NoCertRequest
TLSVerifyClient             off
TLSRequired                 on
```

Reiniciamos el servidor para que los cambios surgan efecto

8. Accedemos a través de un cliente ftp (s) para comprobar que podemos conectarnos usando tls

De forma más simple podemos crear el certificado usando el comando proftpd-gencert