Actividades

1. Explica qué hace este comando. ¿Dónde se almacena el certificado, la calve pública y la clave privada?

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem

sudo => Ejecuta un comando como administrador.
openssl => Proporciona acceso a una biblioteca de comandos para trabajar con certificados y claves.
req => Inicia el proceso de creación de certificado/clave.
-x509 => Cambia el formato del certificado de PKCS#10 a X509.
-nodes => No cifre la clave de salida.
-days 365 => Número de días de validez del certificado.
-newkey rsa:2048 => Genera una nueva clave de 2048 bits. Alto nivel de seguridad.
-keyout /etc/ssl/private/vsftpd.pem => Crea una clave privada con el nombre y la ubicación especificados.
-out /etc/ssl/private/vsftpd.pem => Crea una clave pública con el nombre y la ubicación especificados.

Durante la ejecución, el programa solicitará al usuario información adicional. Esto es opcional.

De forma predeterminada, SSL almacena las claves privadas en **/etc/ssl/private**, y las claves públicas y los certificados en **/etc/ssl/certs**.

2. Explica que hace cada línea del archivo de configuración de ftp:

rsa_cert_file=/etc/ssl/private/vsftpd.pem => **Especifica la ubicación del certificado/clave pública para una conexión SSL cifrada.**

rsa_private_key_file=/etc/ssl/private/vsftpd.pem => **Especifica la ubicación de la clave privada para una conexión SSL cifrada.**

ssl_enable=YES => **Habilita el soporte SSL para vsftpd.**

allow_anon_ssl=NO => **Evita el inicio de sesión anónimo cifrado con SSL/TLS (ej. el usuario invitado)**

force_local_data_ssl=YES => **Fuerza el cifrado SSL/TLS del nombre de usuario/contraseña para mantenerlo seguro.**

force_local_logins_ssl=YES => **Fuerza el cifrado SSL/TLS de los para mantenerlos seguro.**

ssl_tlsv1=YES => **Habilita el protocolo de "Transport Layer Security" de versión 1.0 para mayor seguridad**

ssl_sslv2=NO => **Desactiva el protocolo de “Secure Sockets Layer” de la versión 2 porque está en desuso**

ssl_sslv3=NO => **Desactiva el protocolo de “Secure Sockets Layer” de la versión 3 porque está en desuso. También es una versión anterior de TLS ver 1.**

require_ssl_reuse=NO => **Si se establece en "YES", todas las conexiones de datos SSL deben exhibir reutilización de sesión SSL, sin embargo algunos clientes FTP pueden no funcionar debido a esta opción.**

ssl_ciphers=HIGH => **Solo permite cifrados SSL fuertes que vsftpd permitirá para conexiones SSL cifradas.**

local_root=/home/nombre_usuario/ftp => **Especifica el directorio al que el servidor cambia después de que un usuario local inicia sesión.**