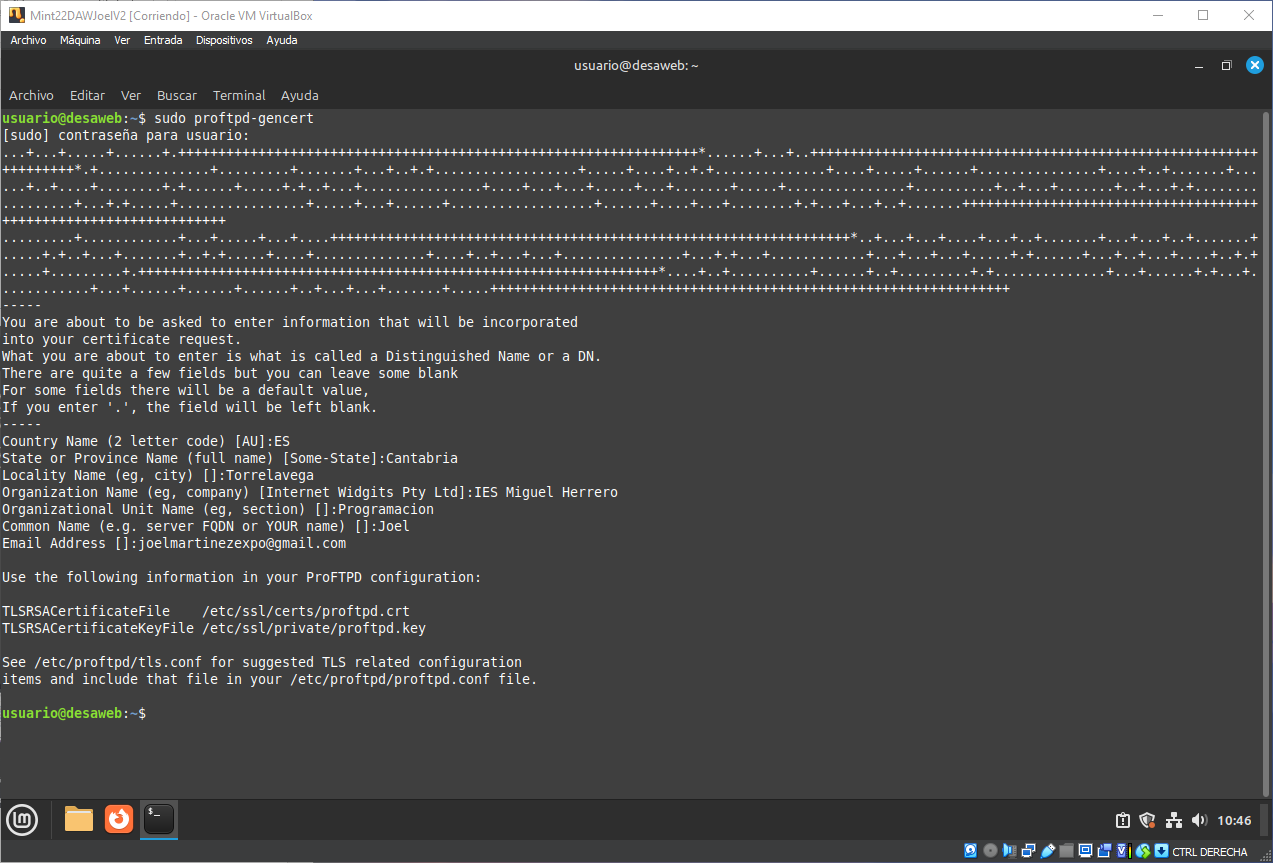
# DAW Práctica 4.4:

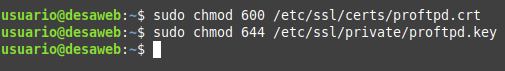
* **¿Qué es SSH?**  
  SSH (*Secure Shell*) es un protocolo de red que permite acceder de forma segura a sistemas remotos mediante cifrado. Se usa para administrar servidores y transferir archivos de manera segura.
* **¿Qué es TLS?**  
  TLS (*Transport Layer Security*) es un protocolo de seguridad que cifra las comunicaciones entre clientes y servidores en la web. Es una evolución de SSL y se usa en HTTPS, FTPS, correos electrónicos seguros, entre otros.
* **¿Para qué vale una función resumen HASH?**  
  Una función *hash* toma una entrada y genera un valor único de longitud fija, lo que permite verificar la integridad de datos sin revelar la información original. Ejemplos: SHA-256, MD5.
* **Explica brevemente cómo funciona el cifrado de clave pública o asimétrica.**  
  Usa un par de claves:
  + **Clave pública**: Se comparte con cualquiera y se usa para cifrar datos.
  + **Clave privada**: Se mantiene secreta y se usa para descifrar datos.  
    Este sistema permite asegurar la confidencialidad y autenticidad de las comunicaciones.

Generar un certificado TLS autofirmado con el comando:

proftpd-gencert



Aplicar los permisos adecuados:



* **600**: Solo el propietario puede leer y escribir el archivo clave privada.
* **644**: Cualquier usuario puede leer el certificado, pero solo el propietario puede modificarlo.

Editar el archivo de configuración principal de proFTPD (/etc/proftpd/proftpd.conf) y descomentar la línea que referencia la configuración de TLS:



Luego, abrir /etc/proftpd/tls.conf y descomentar/modificar las siguientes líneas para apuntar a los archivos generados:

<IfModule mod\_tls.c>

TLSEngine on

TLSLog /var/log/proftpd/tls.log

TLSProtocol SSLv23

TLSRSACertificateFile /etc/proftpd/ssl/proftpd.crt

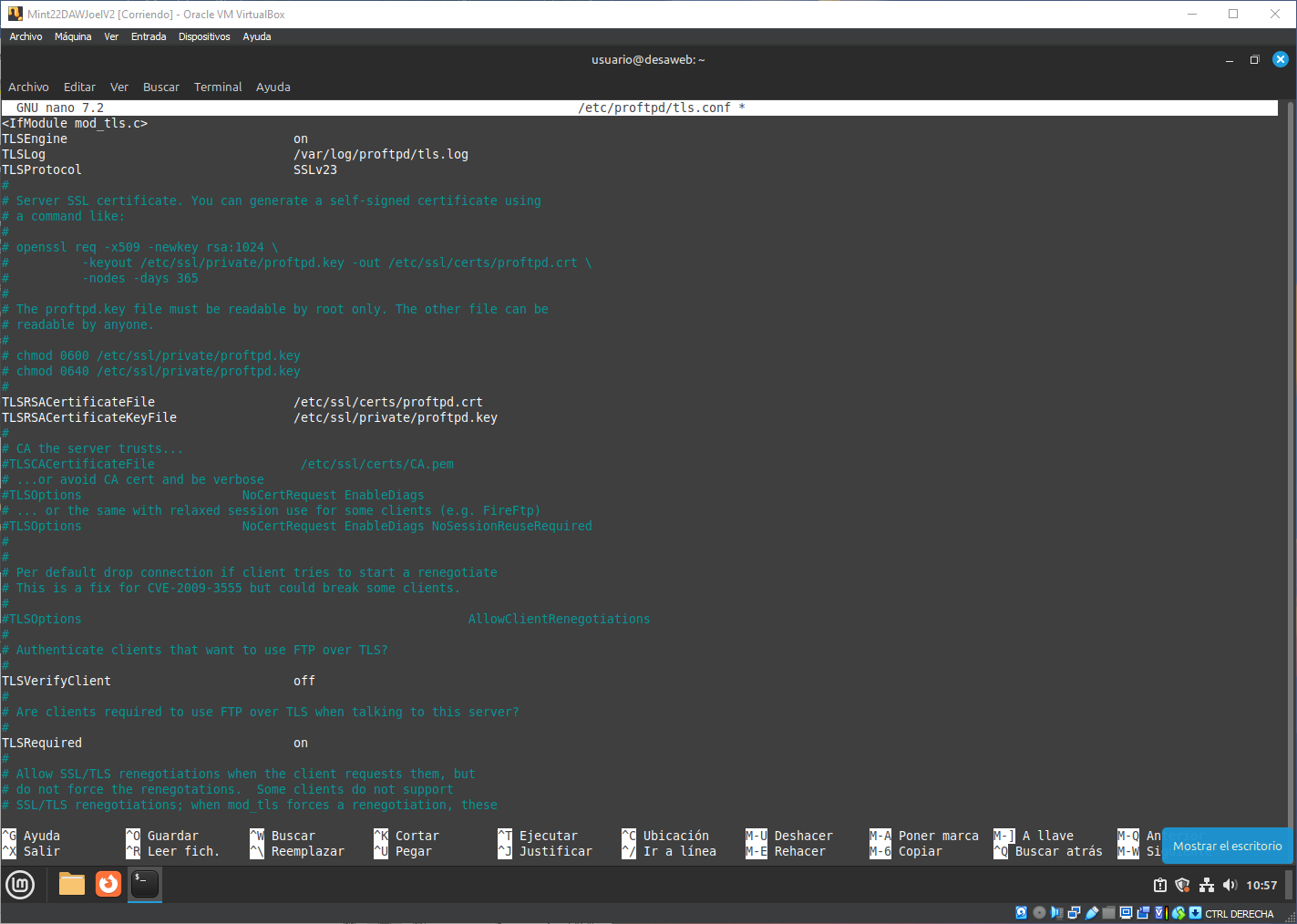
TLSRSACertificateKeyFile /etc/proftpd/ssl/proftpd.key

TLSOptions NoCertRequest

TLSVerifyClient off

TLSRequired on

</IfModule>



Editar el archivo /etc/proftpd/modules.conf y descomentar la línea:



Instalar modulo para funcionamiento de TLS:

apt-get install proftpd-mod-crypto

Reiniciar el servicio y conectar desde filezilla.

