

## 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

[illegible]

Aplicar los permisos adecuados:

```
usuario@desaweb:~$ sudo chmod 600 /etc/ssl/certs/proftpd.crt
usuario@desaweb:~$ sudo chmod 644 /etc/ssl/private/proftpd.key
usuario@desaweb:~$
```

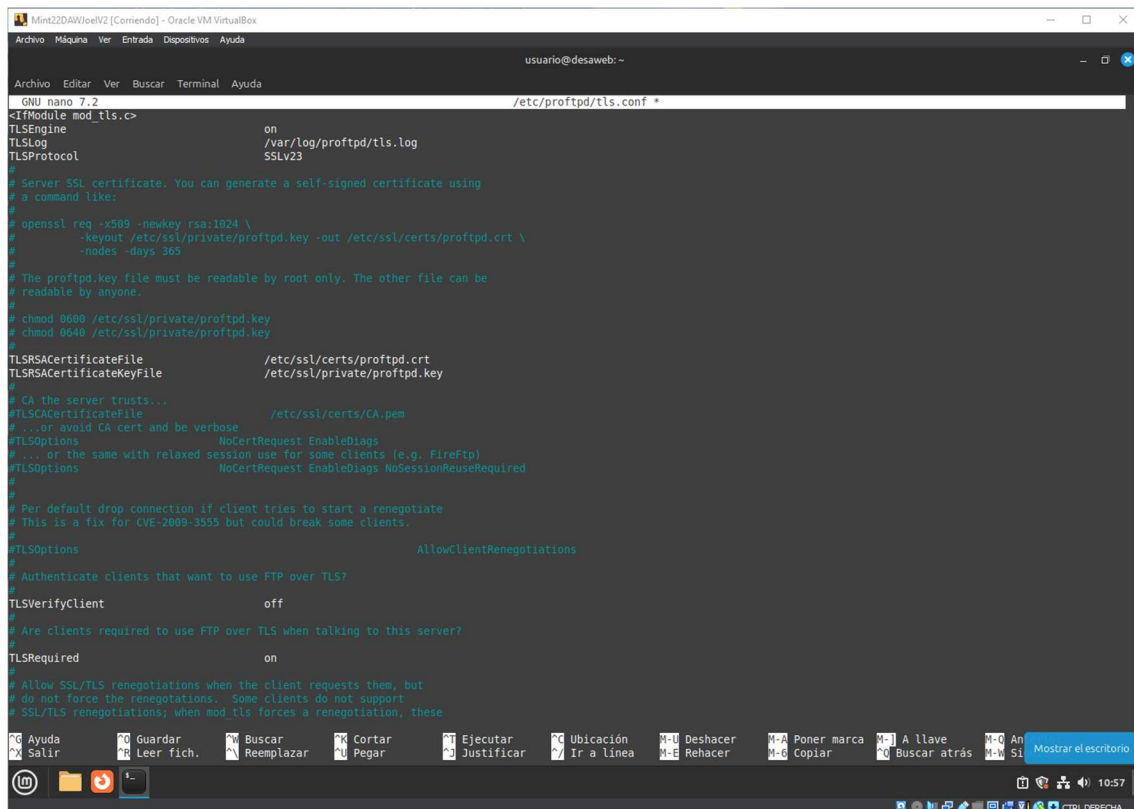
- **600**: Solo el propietario puede leer y escribir el archivo clave privada.
- **644**: Cualquier usuario puede leer el certificado, pero solo el propietario puede modificarlo.

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

```
Include /etc/proftpd/tls.conf
```

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>
```



```
Mint22DAWioeV2 [Corriendo] - Oracle VM VirtualBox
usuario@desaweb: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 7.2 /etc/proftpd/tls.conf *
<IfModule mod_tls.c>
  TLSEngine on
  TLSLog /var/log/proftpd/tls.log
  TLSProtocol SSLv23
  # Server SSL certificate. You can generate a self-signed certificate using
  # a command like:
  # openssl req -x509 -newkey rsa:1024 \
  #   -keyout /etc/ssl/private/proftpd.key -out /etc/ssl/certs/proftpd.crt \
  #   -nodes -days 365
  # The proftpd.key file must be readable by root only. The other file can be
  # readable by anyone.
  # chmod 0600 /etc/ssl/private/proftpd.key
  # chmod 0640 /etc/ssl/private/proftpd.key
  TLSRSACertificateFile /etc/ssl/certs/proftpd.crt
  TLSRSACertificateKeyFile /etc/ssl/private/proftpd.key
  # CA the server trusts...
  # TLSACertificateFile /etc/ssl/certs/CA.pem
  # ... or avoid CA cert and be verbose
  # TLSOptions NoCertRequest EnableDiags
  # ... or the same with relaxed session use for some clients (e.g. FireFTP)
  # TLSOptions NoCertRequest EnableDiags NoSessionReuseRequired
  # Per default drop connection if client tries to start a renegotiate
  # This is a fix for CVE-2009-3555 but could break some clients.
  # TLSOptions AllowClientRenegotiations
  # Authenticate clients that want to use FTP over TLS?
  TLSVerifyClient off
  # Are clients required to use FTP over TLS when talking to this server?
  TLSRequired on
  # Allow SSL/TLS renegotiations when the client requests them, but
  # do not force the renegotiations. Some clients do not support
  # SSL/TLS renegotiations; when mod_tls forces a renegotiation, these
```

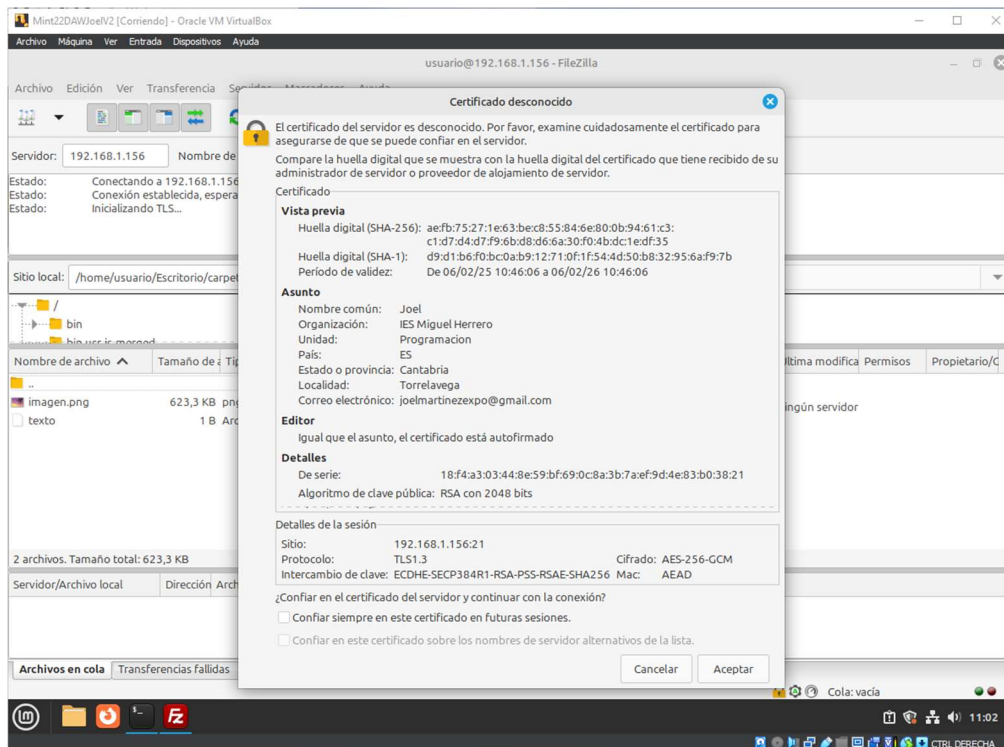
Editar el archivo `/etc/proftpd/modules.conf` y descomentar la línea:

```
LoadModule mod_tls.c
```

Instalar modulo para funcionamiento de TLS:

```
apt-get install proftpd-mod-crypto
```

Reiniciar el servicio y conectar desde filezilla.



Estado: Inicializando TLS...  
Estado: Conexión TLS establecida.