

✓ Parte 1: Preparación del Entorno

Paso 1: Actualización del Sistema

Abre la terminal de tu máquina virtual y ejecuta:

```
sudo apt update && sudo apt upgrade -y
```

```
(root@kali)-[~]
# sudo apt update && sudo apt upgrade -y
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Err:1 http://kali.download/kali kali-rolling InRelease
  Sub-process /usr/bin/sqv returned an error code (1), error message is: Missing key 827C8569F2518CC677FECA1AE
  D65462EC8D5E4C5, which is needed to verify signature.
Hit:2 https://ngrok-agent.s3.amazonaws.com buster InRelease
6 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: An error occurred during the signature verification. The repository is not updated and the previous i
ndex files will be used. OpenPGP signature verification failed: http://kali.download/kali kali-rolling InRelea
se: Sub-process /usr/bin/sqv returned an error code (1), error message is: Missing key 827C8569F2518CC677FECA1
AED65462EC8D5E4C5, which is needed to verify signature.
Warning: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease Sub-process /usr/bin/sqv retu
rned an error code (1), error message is: Missing key 827C8569F2518CC677FECA1AED65462EC8D5E4C5, which is neede
d to verify signature.
Warning: Some index files failed to download. They have been ignored, or old ones used instead.
Not upgrading:
  bulk-extractor          libgstreamer-plugins-bad1.0-0  libre2-11
  gstreamer1.0-plugins-bad libjavascriptcoregtk-4.1-0  libwebkit2gtk-4.1-0
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 6
```

Paso 2: Instalación del Servidor Web

Instala Apache o Nginx (usa uno de los dos; aquí va Apache como ejemplo):

```
sudo apt install apache2 -y
```

```
(root@kali)-[~]
# sudo apt install apache2 -y
apache2 is already the newest version (2.4.63-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 6
```

✓ Parte 2: Configuración de HTTPS en el Servidor Web

Paso 3: Generación de una Solicitud de Firma de Certificado (CSR)

Crea un directorio para los certificados y genera la clave privada y el CSR:

```
mkdir ~/ssl
cd ~/ssl
openssl req -newkey rsa:2048 -nodes -keyout mi_sitio.key -out
mi_sitio.csr
```

```
(root@kali)-[~]
# mkdir ~/ssl
cd ~/ssl
openssl req -newkey rsa:2048 -nodes -keyout mi_sitio.key -out mi_sitio.csr
```

Paso 4: Obtención del Certificado SSL

Para propósitos de laboratorio, puedes generar un **certificado autofirmado**:

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

```
(root@kali)-[~/ssl]  
# openssl x509 -req -days 365 -in mi_sitio.csr -signkey mi_sitio.key -out mi_sitio.crt  
Certificate request self-signature ok  
subject=C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
```

Paso 5: Configuración del Servidor Web para HTTPS

Activa el módulo SSL y configura Apache:

```
sudo a2enmod ssl
```

```
sudo nano /etc/apache2/sites-available/default-ssl.conf
```

```
(root@kali)-[~/ssl]  
# sudo a2enmod ssl  
sudo nano /etc/apache2/sites-available/default-ssl.conf  
Considering dependencies for ssl:
```

Luego activa el sitio y reinicia Apache:

```
sudo a2ensite default-ssl.conf  
sudo systemctl restart apache2
```

```
(root@kali)-[~/ssl]  
# sudo a2ensite default-ssl.conf  
sudo systemctl restart apache2  
Enabling site default-ssl.
```

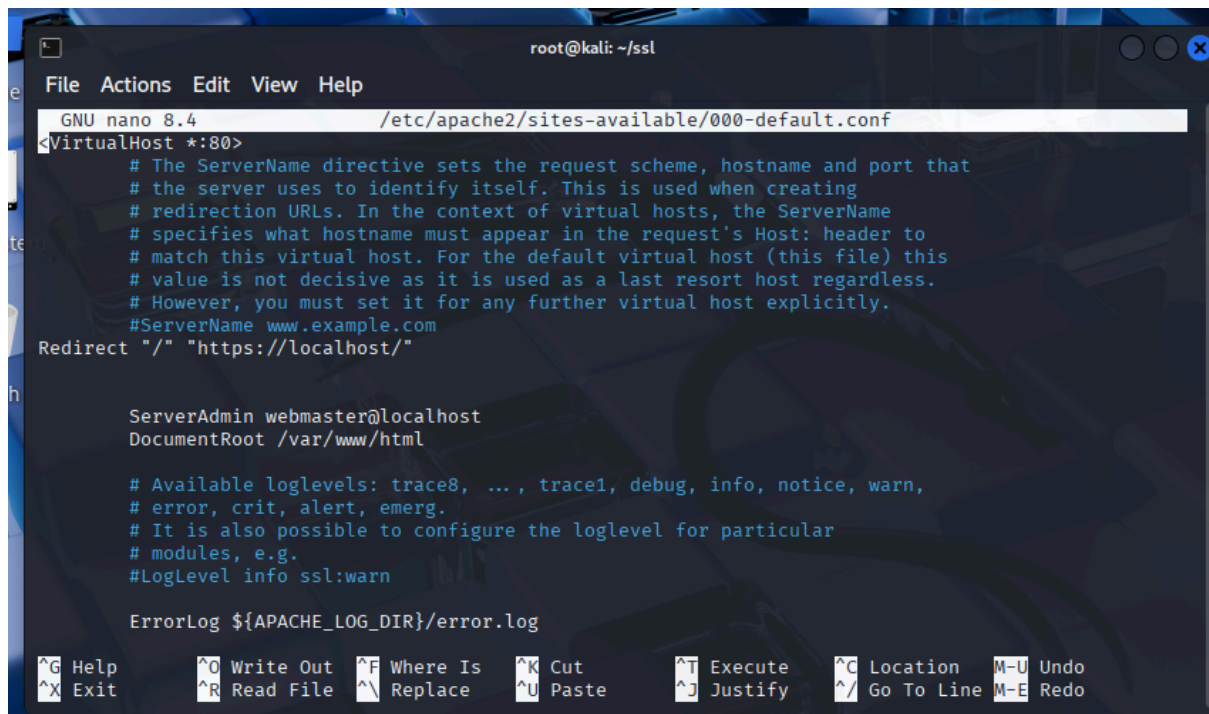
✓ Parte 3: Redirección de HTTP a HTTPS

Paso 6: Configuración de la Redirección

Edita el archivo de configuración del sitio por defecto:

```
sudo nano /etc/apache2/sites-available/000-default.conf
```

Redirect "/" "<https://localhost/>"



```
root@kali: ~/ssl
File Actions Edit View Help
GNU nano 8.4 /etc/apache2/sites-available/000-default.conf
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com
Redirect "/" "https://localhost/"

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html

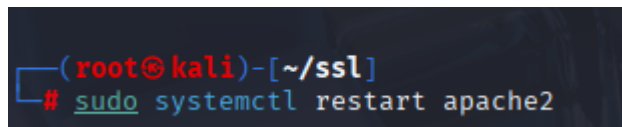
# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log

^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line  M-E Redo
```

Reinicia Apache:

`sudo systemctl restart apache2`



```
(root@kali)-[~/ssl]
# sudo systemctl restart apache2
```

✓ Parte 4: Verificación

Paso 7: Verificación de la Conexión Segura

Abre tu navegador en la VM o desde el host y accede a:

arduino

CopiarEditar

<https://localhost>

