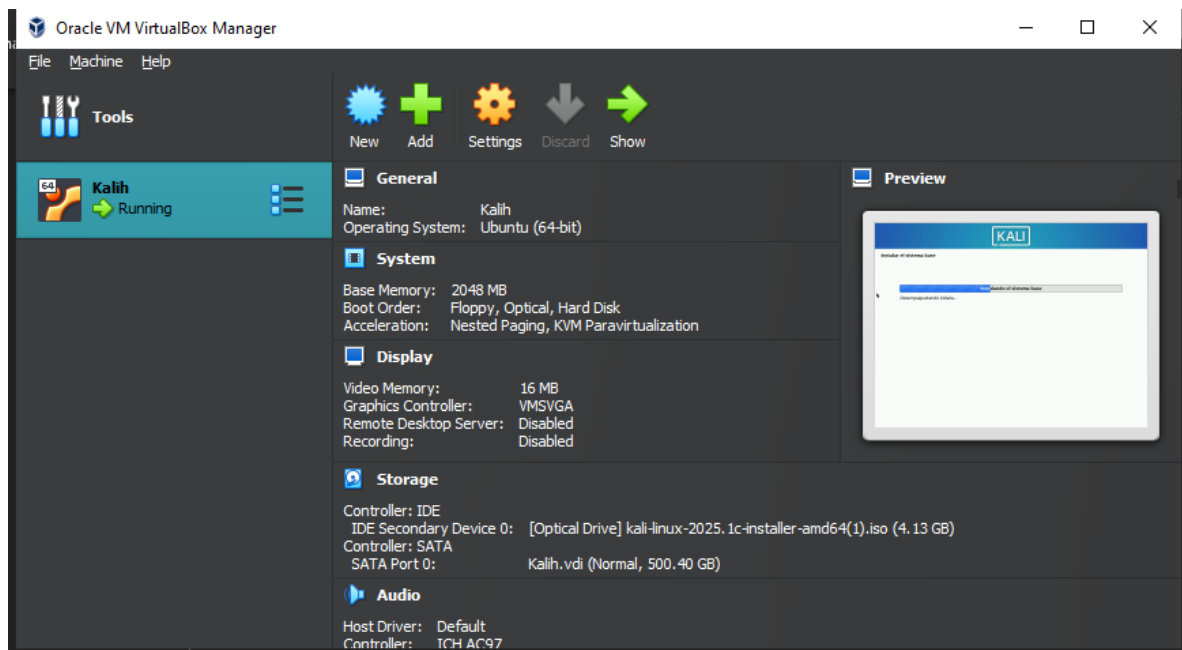


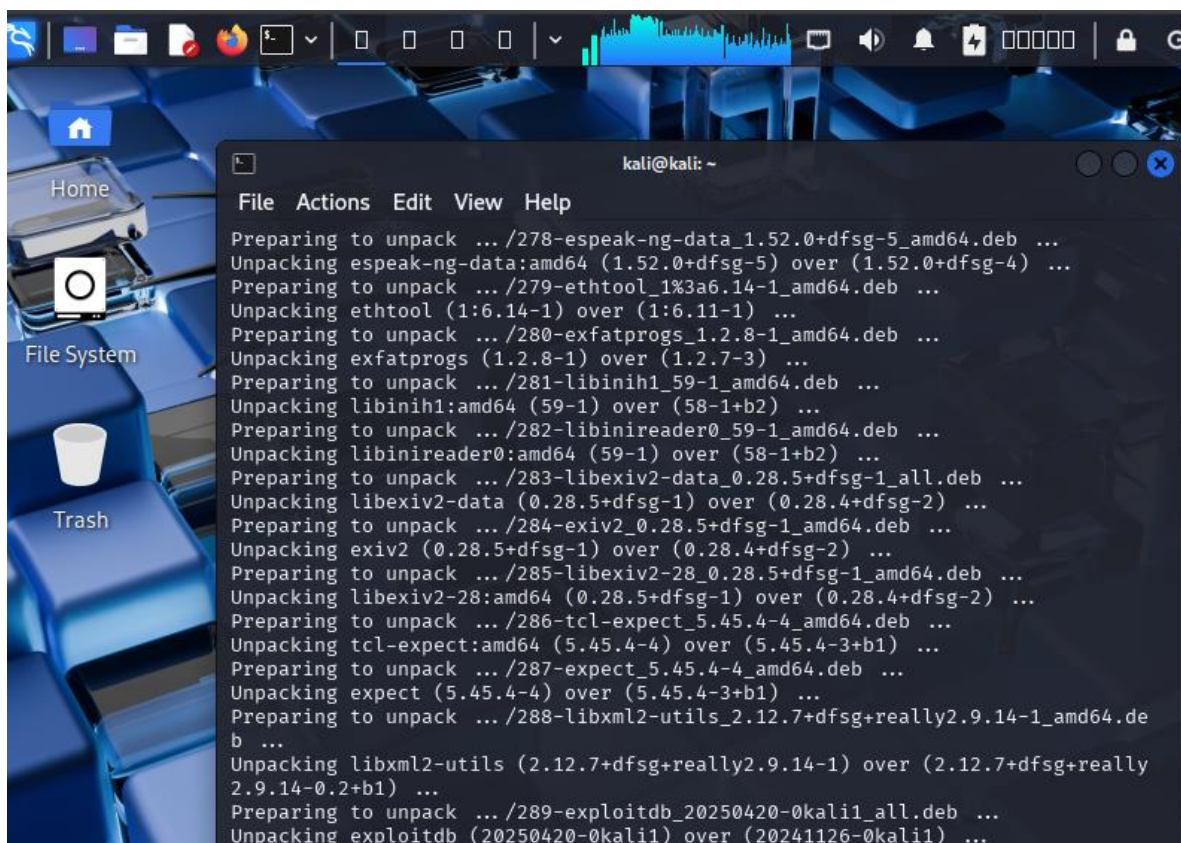
HÉCTOR DIAZ:

PARTE 1: PASO 1:

Instalación de VM



- Actualización del sistema



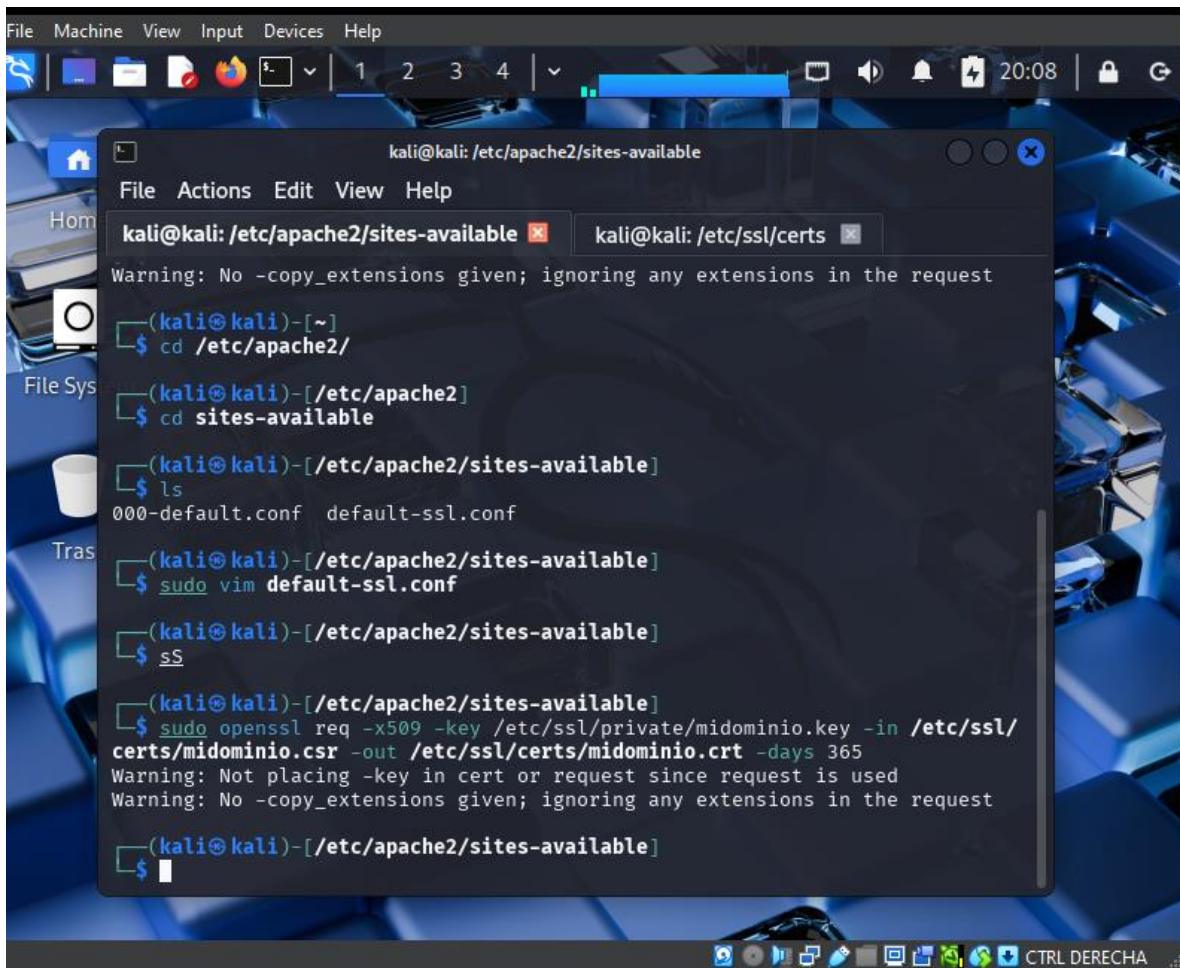
-
- The image shows a Kali Linux desktop environment. A terminal window is open, displaying the following text:
- ```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo apt install apache2
[sudo] password for kali:
Building dependency tree ... 50%
```
- The desktop background is a blue-themed image of a keyboard. The top panel shows various application icons and system status indicators like time (19:51) and battery level. The bottom panel shows a taskbar with application icons and the text "CTRL DERECHA".

### Paso 3:

[illegible]



#### PASO 4: OBTENCIÓN DE CERTIFICADO SSL CON OPENSSL



```
kali@kali: /etc/apache2/sites-available
File Actions Edit View Help

kali@kali: /etc/apache2/sites-available x kali@kali: /etc/ssl/certs x
Warning: No -copy_extensions given; ignoring any extensions in the request

(kali@kali)-[~]
$ cd /etc/apache2/

(kali@kali)-[/etc/apache2]
$ cd sites-available

(kali@kali)-[/etc/apache2/sites-available]
$ ls
000-default.conf default-ssl.conf

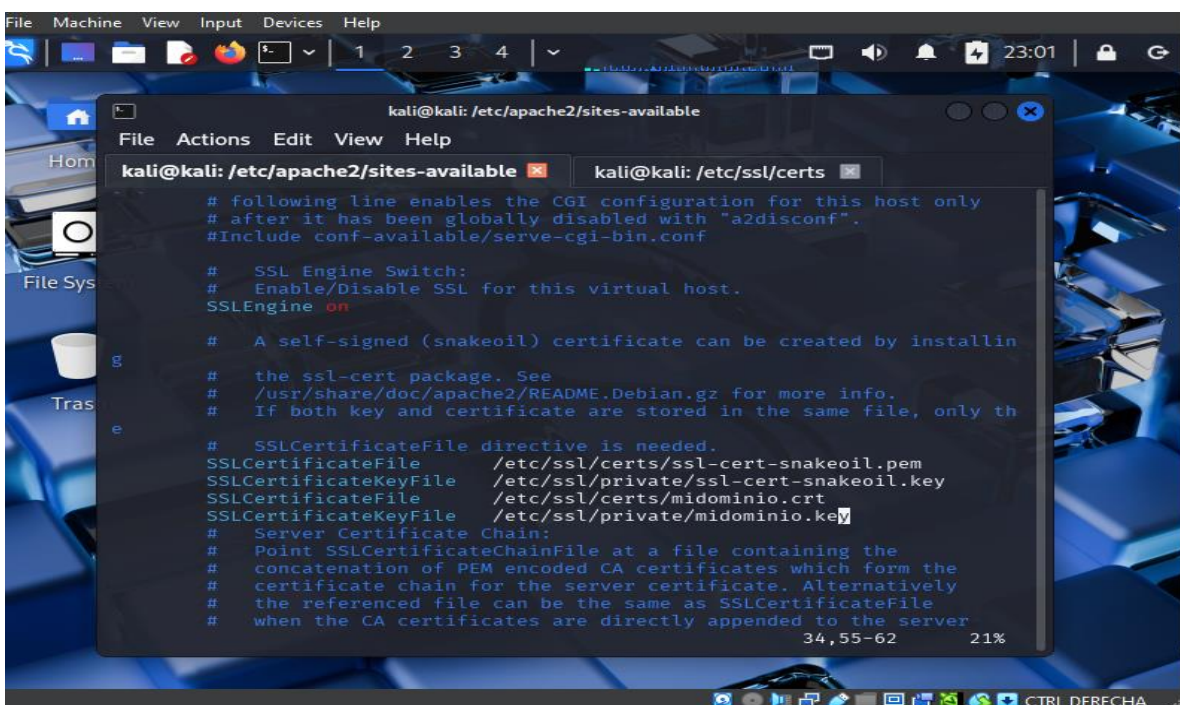
(kali@kali)-[/etc/apache2/sites-available]
$ sudo vim default-ssl.conf

(kali@kali)-[/etc/apache2/sites-available]
$ ss

(kali@kali)-[/etc/apache2/sites-available]
$ sudo openssl req -x509 -key /etc/ssl/private/midominio.key -in /etc/ssl/
certs/midominio.csr -out /etc/ssl/certs/midominio.crt -days 365
Warning: Not placing -key in cert or request since request is used
Warning: No -copy_extensions given; ignoring any extensions in the request

(kali@kali)-[/etc/apache2/sites-available]
$
```

#### PASO 5: CONFIGURACIÓN DE SERVIDOR WEB PARA HTTPS



```
kali@kali: /etc/apache2/sites-available
File Actions Edit View Help

kali@kali: /etc/apache2/sites-available x kali@kali: /etc/ssl/certs x

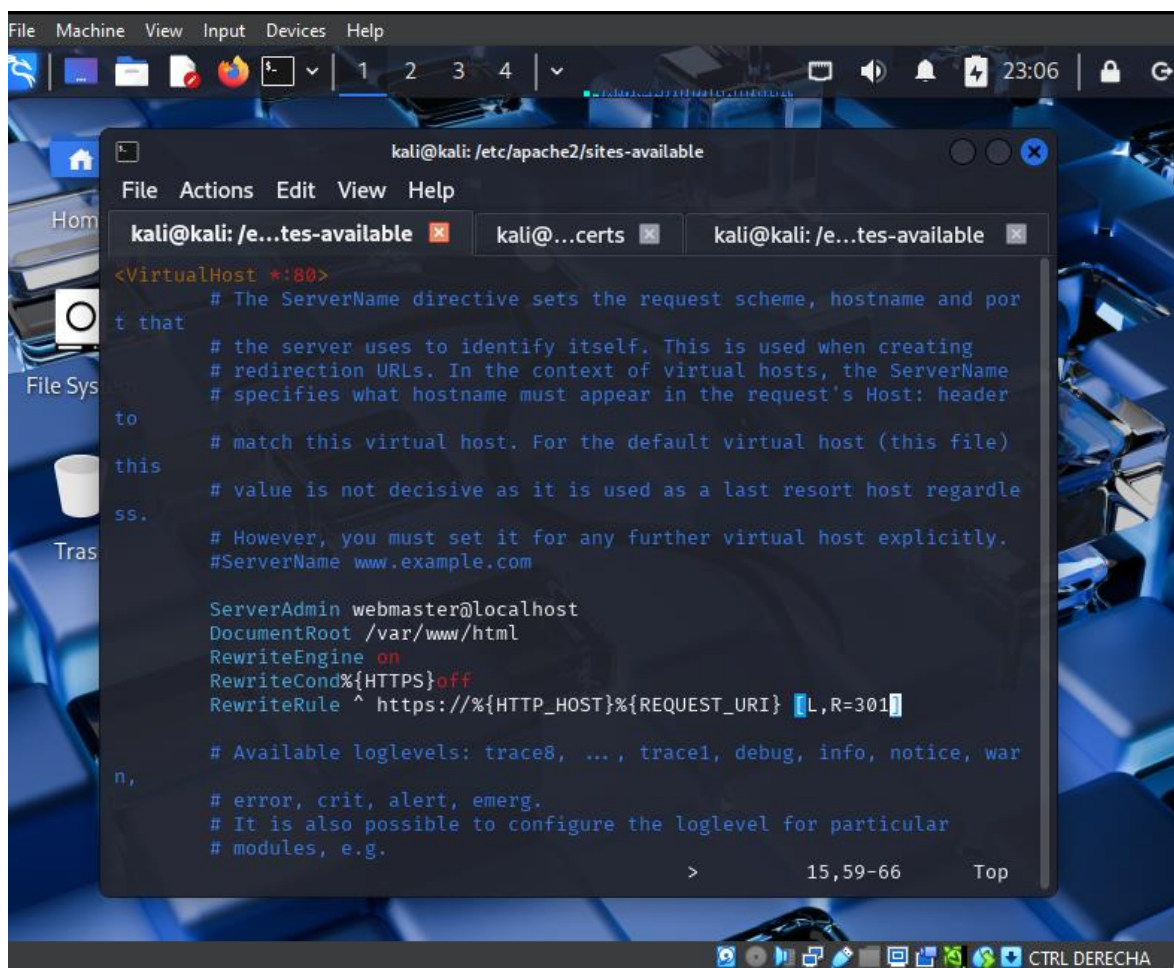
following line enables the CGI configuration for this host only
after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

SSL Engine Switch:
Enable/Disable SSL for this virtual host.
SSLEngine on

A self-signed (snakeoil) certificate can be created by installing
the ssl-cert package. See
/usr/share/doc/apache2/README.Debian.gz for more info.
If both key and certificate are stored in the same file, only the
SSLCertificateFile directive is needed.
SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
SSLCertificateFile /etc/ssl/certs/midominio.crt
SSLCertificateKeyFile /etc/ssl/private/midominio.key

Server Certificate Chain:
Point SSLCertificateChainFile at a file containing the
concatenation of PEM encoded CA certificates which form the
certificate chain for the server certificate. Alternatively
the referenced file can be the same as SSLCertificateFile
when the CA certificates are directly appended to the server
34,55-62 21%
```

## PASO 6: CONFIGURACIÓN DE REDIRECCIONAMIENTO



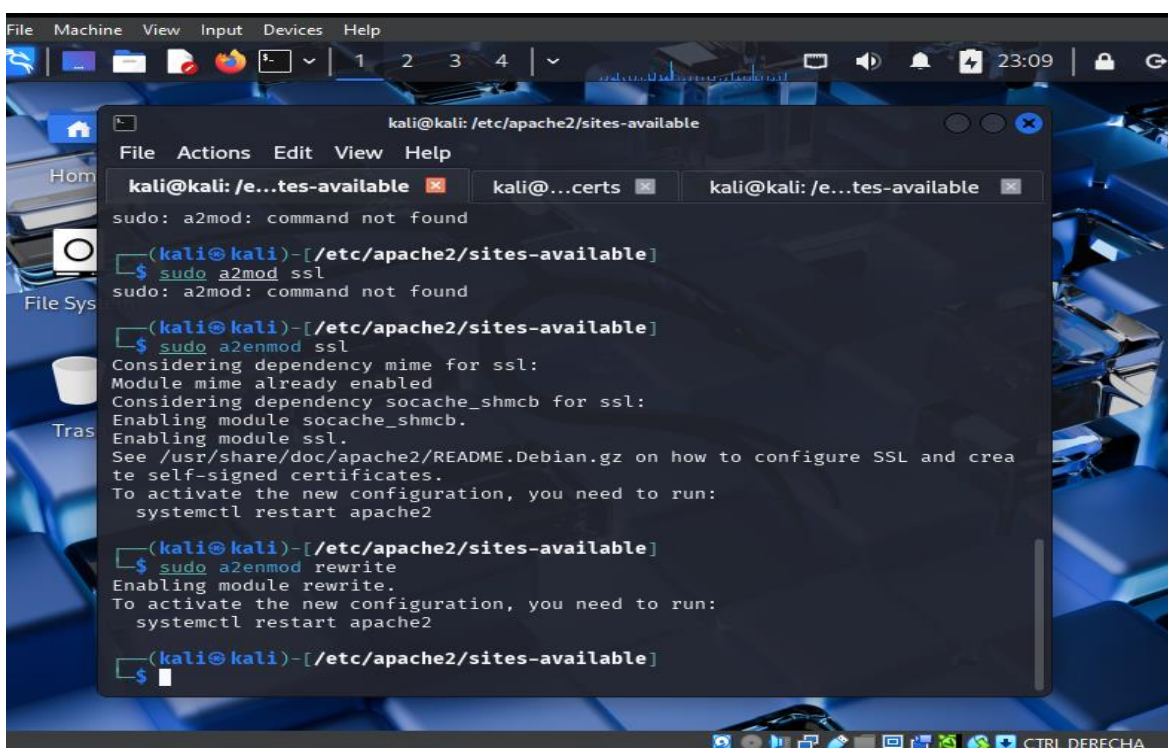
```
kali@kali: /etc/apache2/sites-available
File Actions Edit View Help
kali@kali: /e...tes-available x kali@...certs x kali@kali: /e...tes-available x
<VirtualHost *:80>
 # The ServerName directive sets the request scheme, hostname and port
 # that
 # the server uses to identify itself. This is used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

 ServerAdmin webmaster@localhost
 DocumentRoot /var/www/html
 RewriteEngine on
 RewriteCond %{HTTPS}off
 RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]

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

 > 15,59-66 Top
```

## COMANDO PARA QUE LA MODIFICACIÓN RESULTE



```
kali@kali: /etc/apache2/sites-available
File Actions Edit View Help
kali@kali: /e...tes-available x kali@...certs x kali@kali: /e...tes-available x
sudo: a2mod: command not found
(kali@kali)-[/etc/apache2/sites-available]
$ sudo a2mod ssl
sudo: a2mod: command not found
(kali@kali)-[/etc/apache2/sites-available]
$ sudo a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and crea
te self-signed certificates.
To activate the new configuration, you need to run:
systemctl restart apache2
(kali@kali)-[/etc/apache2/sites-available]
$ sudo a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
systemctl restart apache2
(kali@kali)-[/etc/apache2/sites-available]
$
```



## PART 7: VERIFICAMOS QUE SI HACE EL REDIRECCIONAMIENTO AL HTTPS

