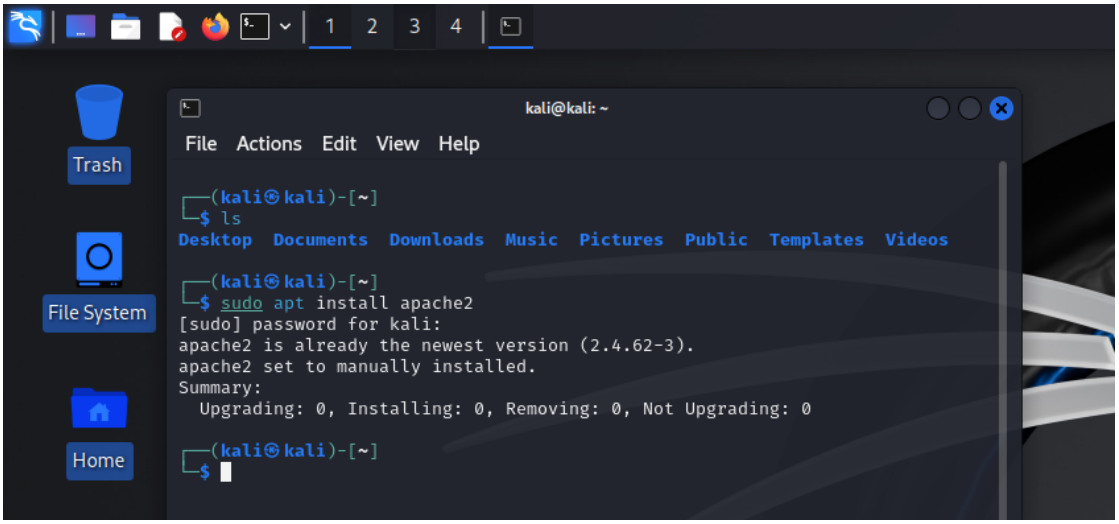
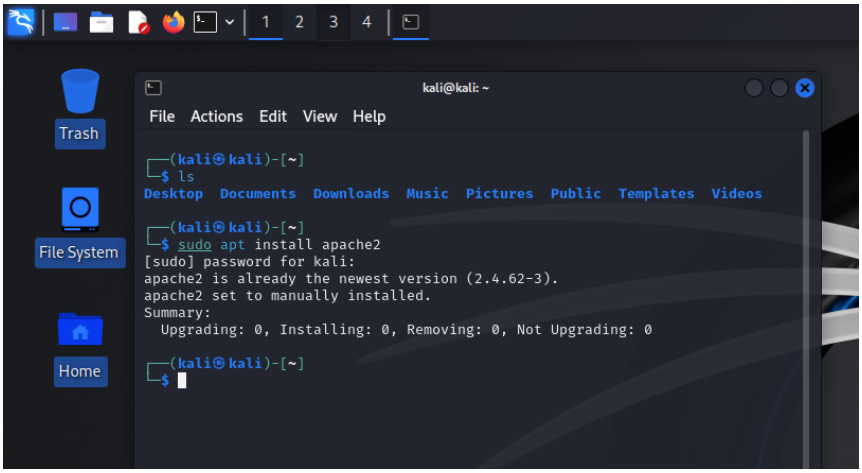
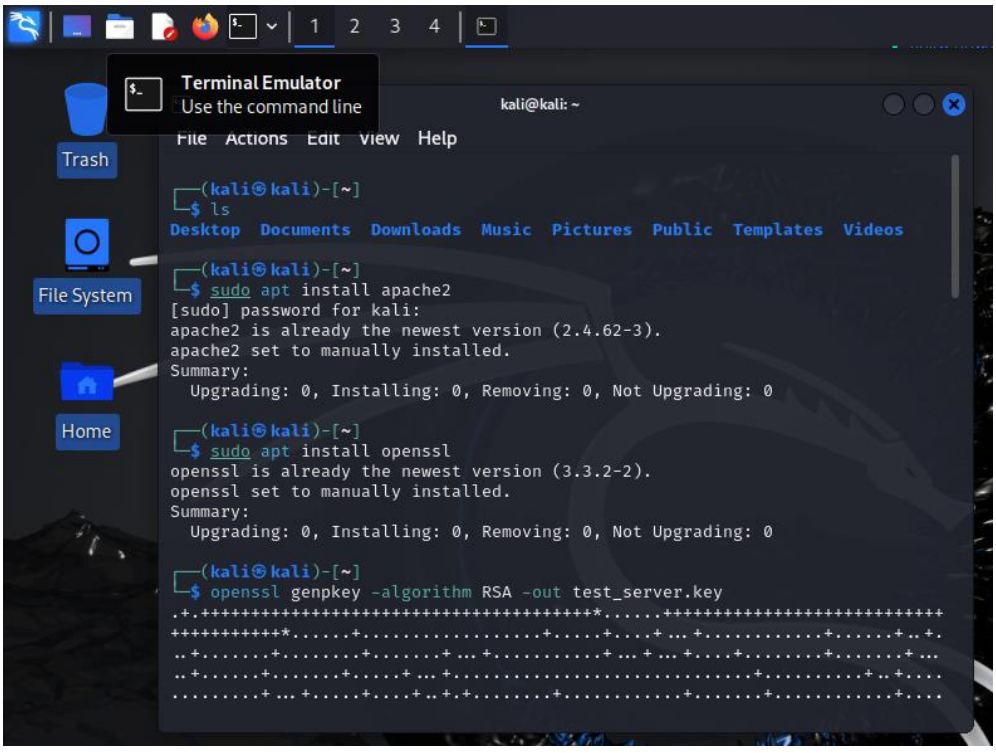
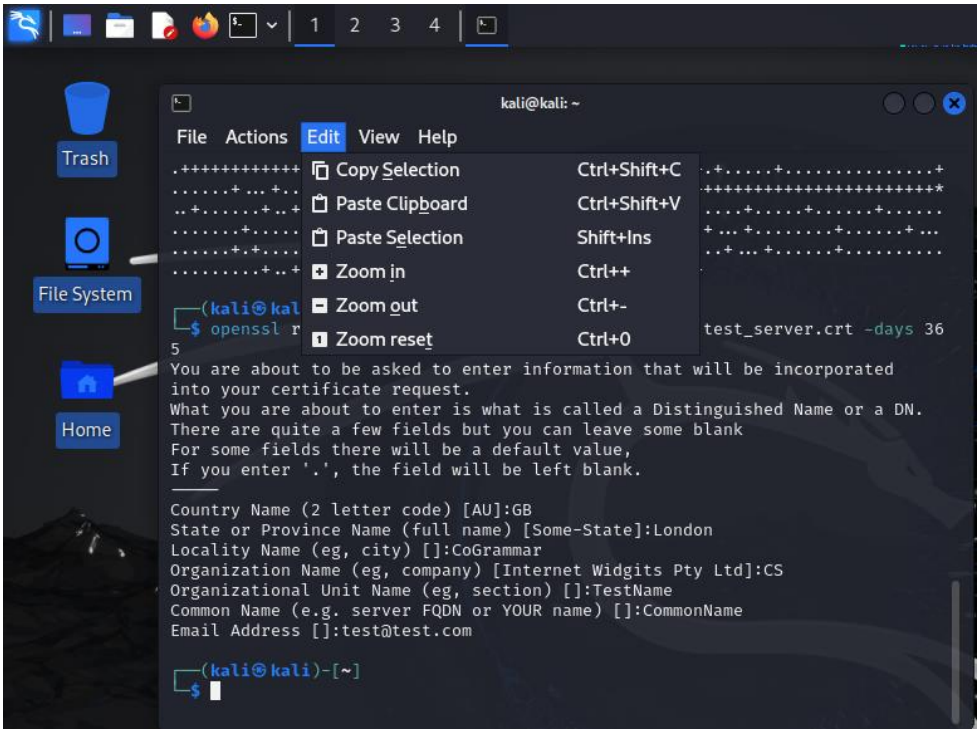
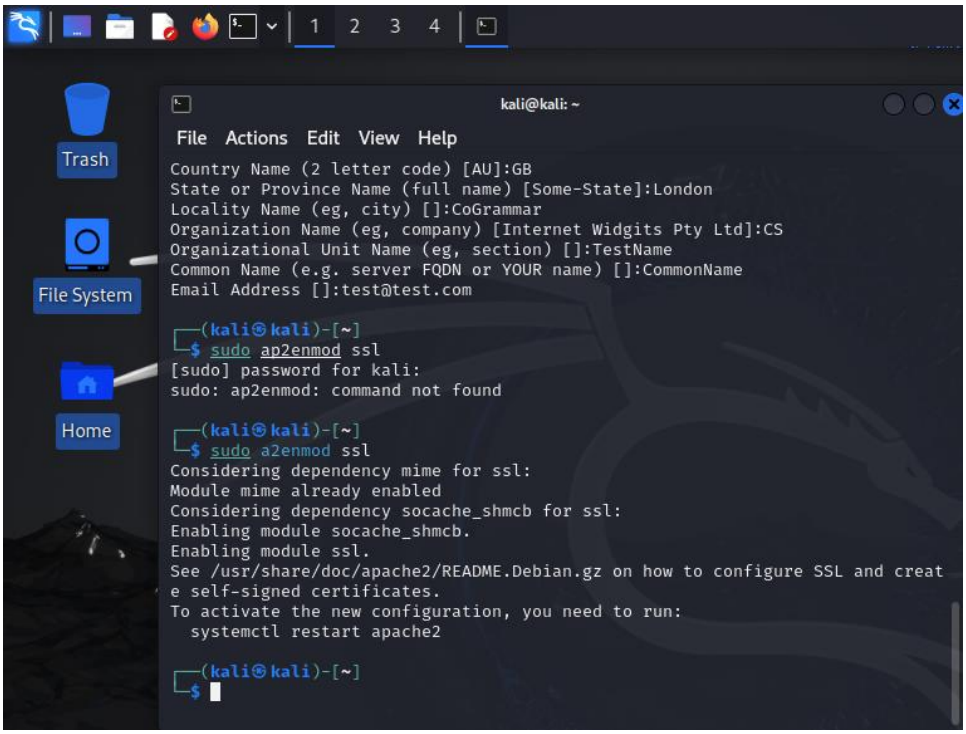
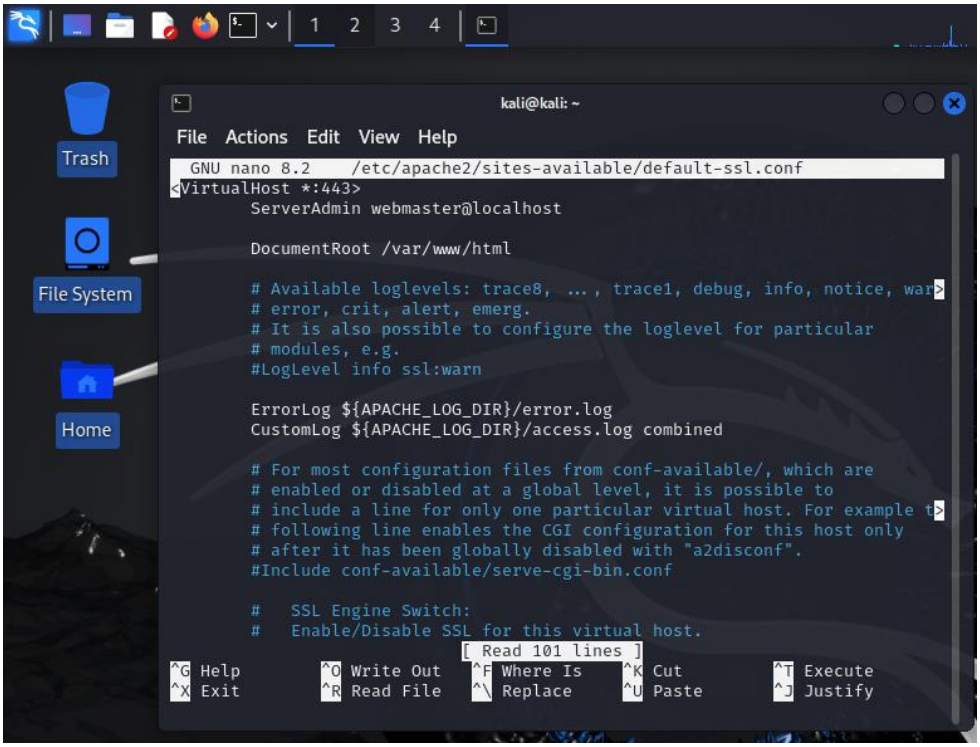

1 2 3 4
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali㉿kali)-[~]
$ sudo apt install apache2
[sudo] password for kali:
apache2 is already the newest version (2.4.62-3).
apache2 set to manually installed.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
(kali㉿kali)-[~]
$

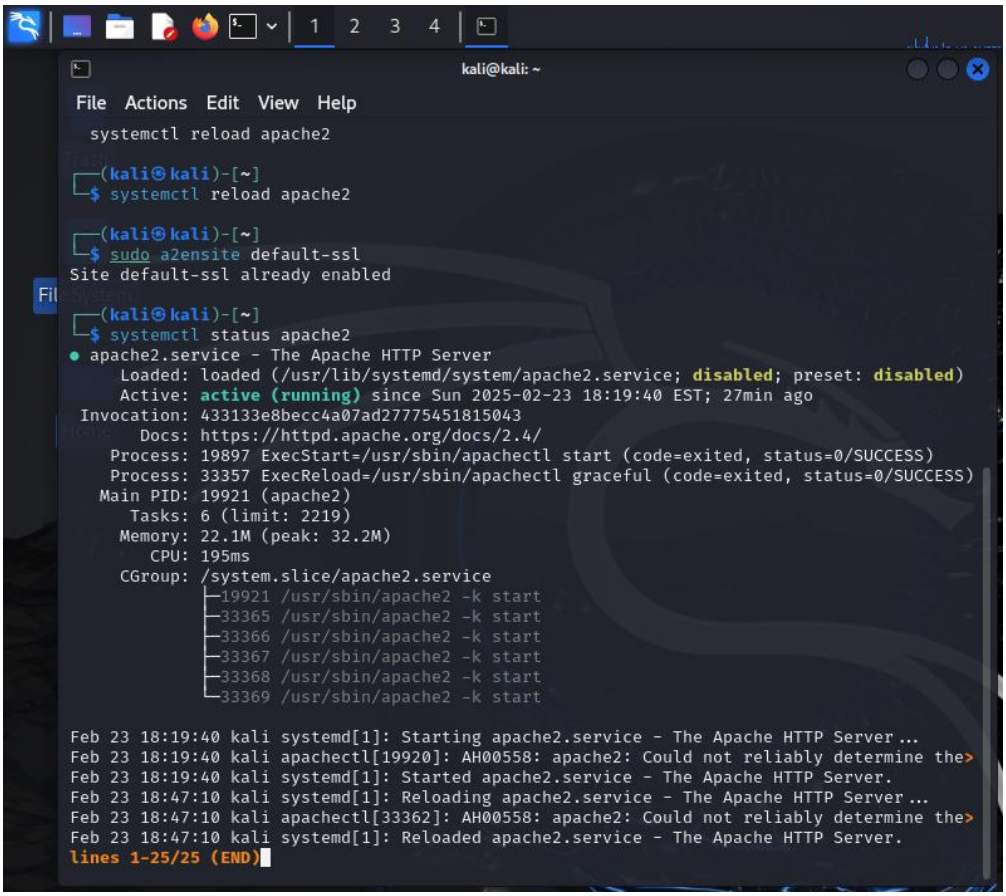

1 2 3 4
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali㉿kali)-[~]
$ sudo apt install apache2
[sudo] password for kali:
apache2 is already the newest version (2.4.62-3).
apache2 set to manually installed.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
(kali㉿kali)-[~]
$

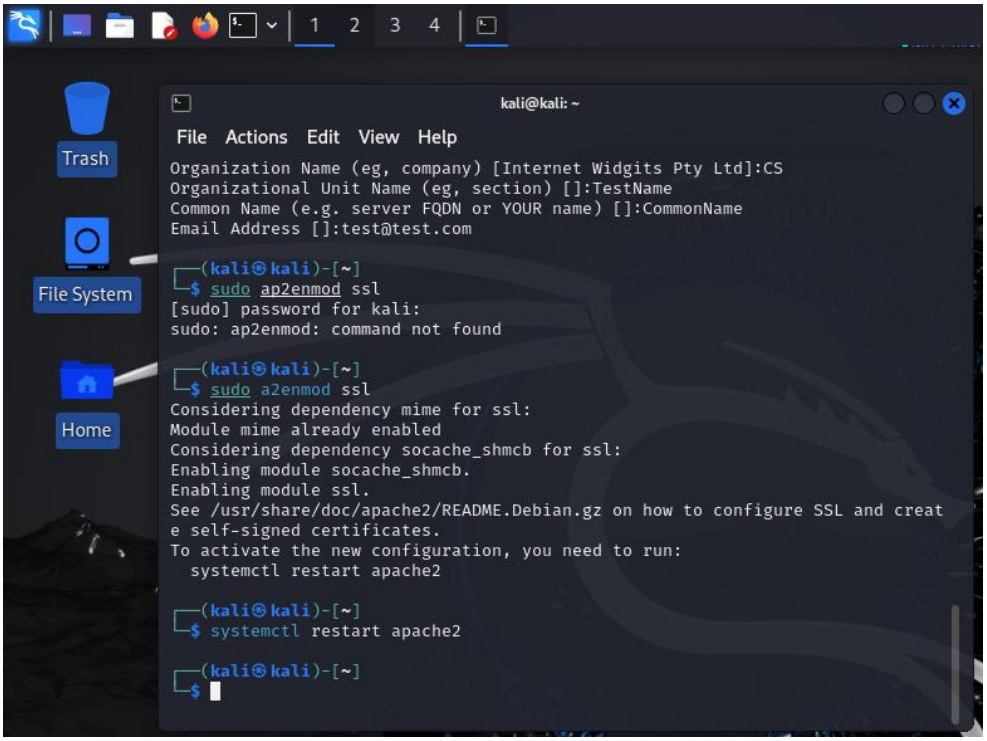

1 2 3 4
Terminal Emulator
Use the command line
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali㉿kali)-[~]
$ sudo apt install apache2
[sudo] password for kali:
apache2 is already the newest version (2.4.62-3).
apache2 set to manually installed.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
(kali㉿kali)-[~]
$ sudo apt install openssl
openssl is already the newest version (3.3.2-2).
openssl set to manually installed.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
(kali㉿kali)-[~]
$ openssl genpkey -algorithm RSA -out test_server.key

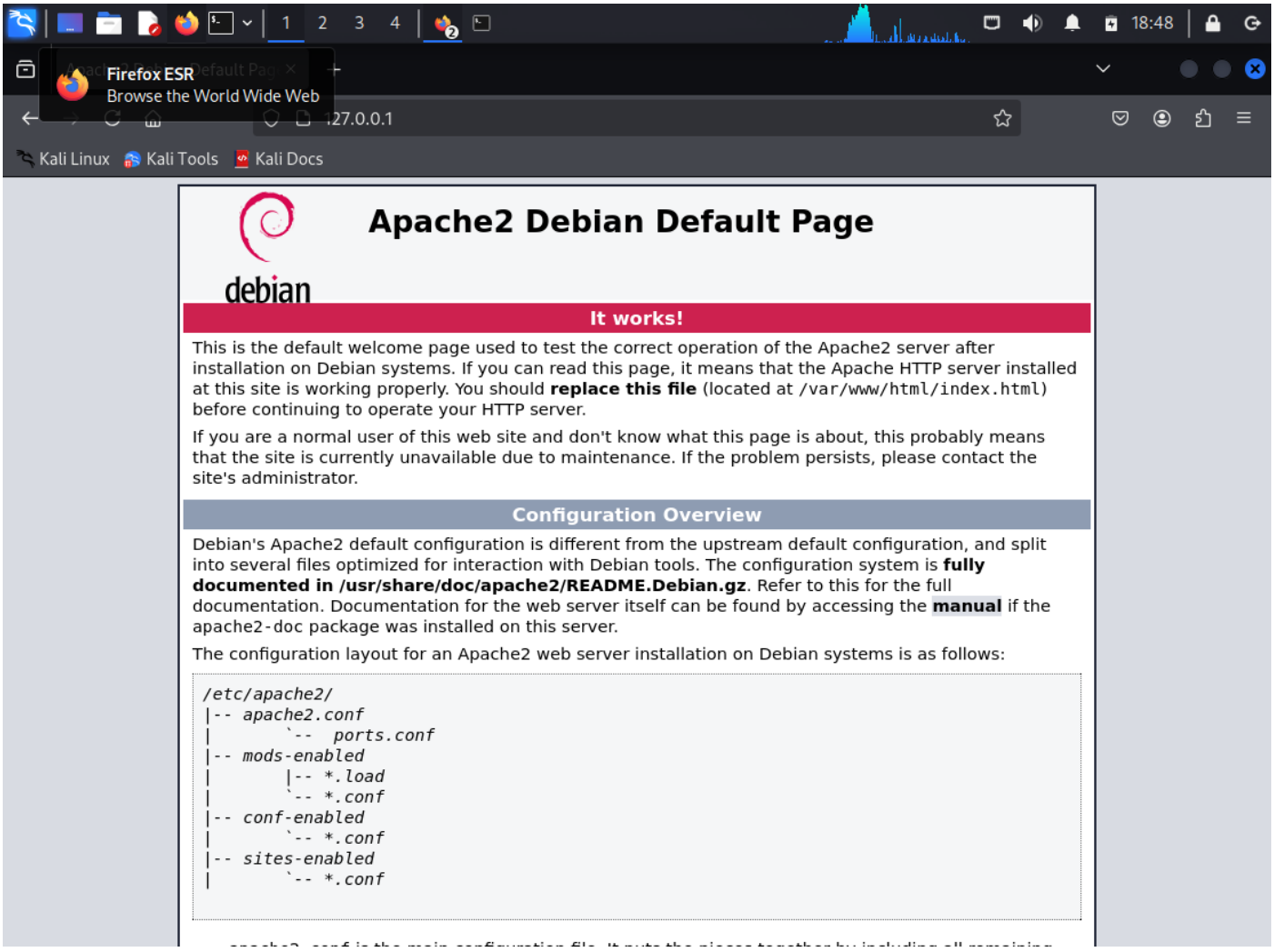

1 2 3 4
kali@kali: ~
File Actions Edit View Help
Copy Selection Ctrl+Shift+C
Paste Clipboard Ctrl+Shift+V
Paste Selection Shift+Ins
Zoom in Ctrl++
Zoom out Ctrl+-
Zoom reset Ctrl+0
Trash
File System
Home
test_server.crt -days 36
5
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:GB
State or Province Name (full name) [Some-State]:London
Locality Name (eg, city) []:CoGrammar
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CS
Organizational Unit Name (eg, section) []:TestName
Common Name (e.g. server FQDN or YOUR name) []:CommonName
Email Address []:test@test.com
(kali㉿kali)-[~]
$

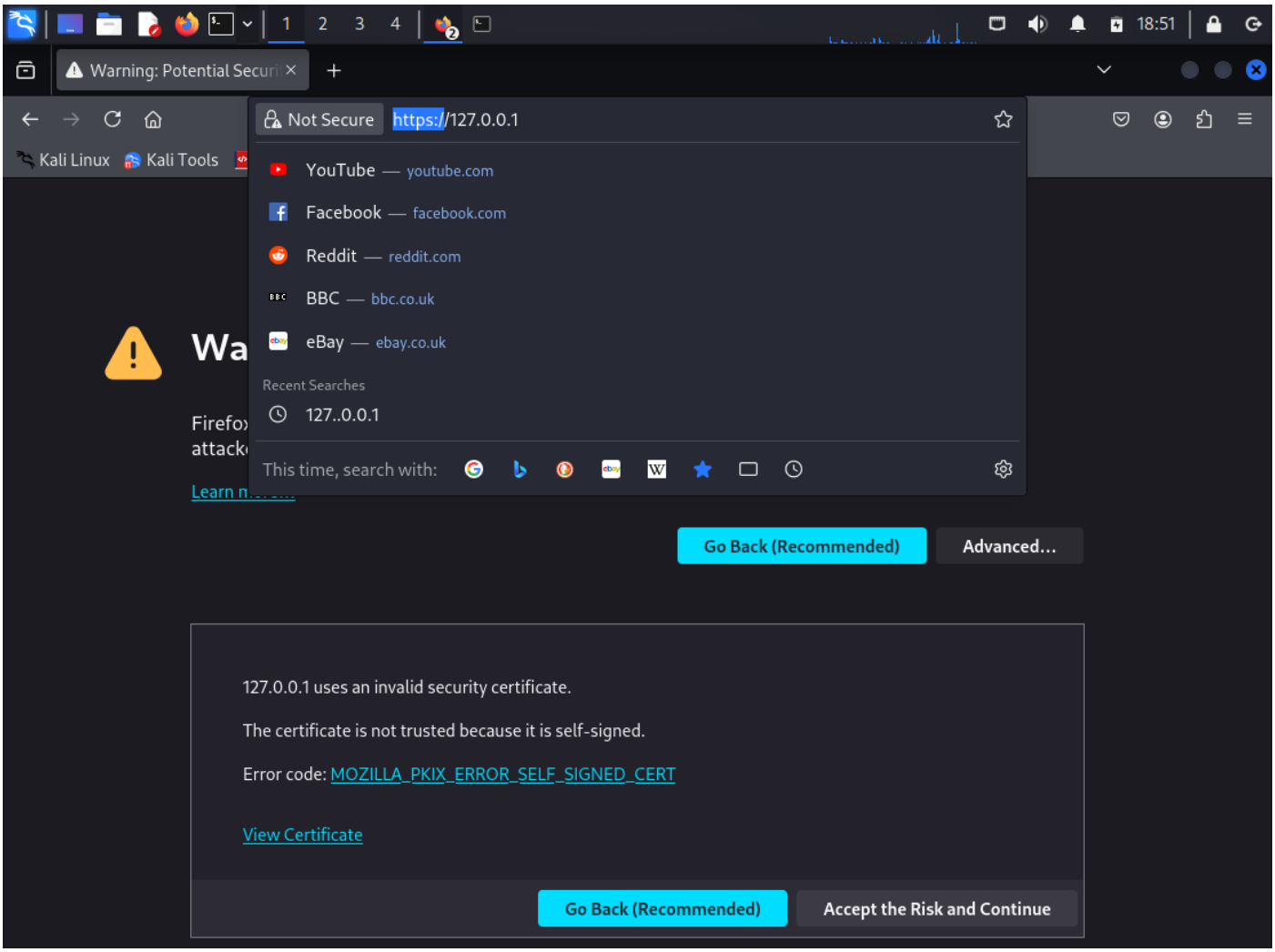

1 2 3 4
kali@kali: ~
File Actions Edit View Help
Country Name (2 letter code) [AU]:GB
State or Province Name (full name) [Some-State]:London
Locality Name (eg, city) []:CoGrammar
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CS
Organizational Unit Name (eg, section) []:TestName
Common Name (e.g. server FQDN or YOUR name) []:CommonName
Email Address []:test@test.com
(kali㉿kali)-[~]
$ sudo ap2enmod ssl
[sudo] password for kali:
sudo: ap2enmod: command not found
(kali㉿kali)-[~]
$ 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 creat
e self-signed certificates.
To activate the new configuration, you need to run:
systemctl restart apache2
(kali㉿kali)-[~]
$
Trash
File System
Home

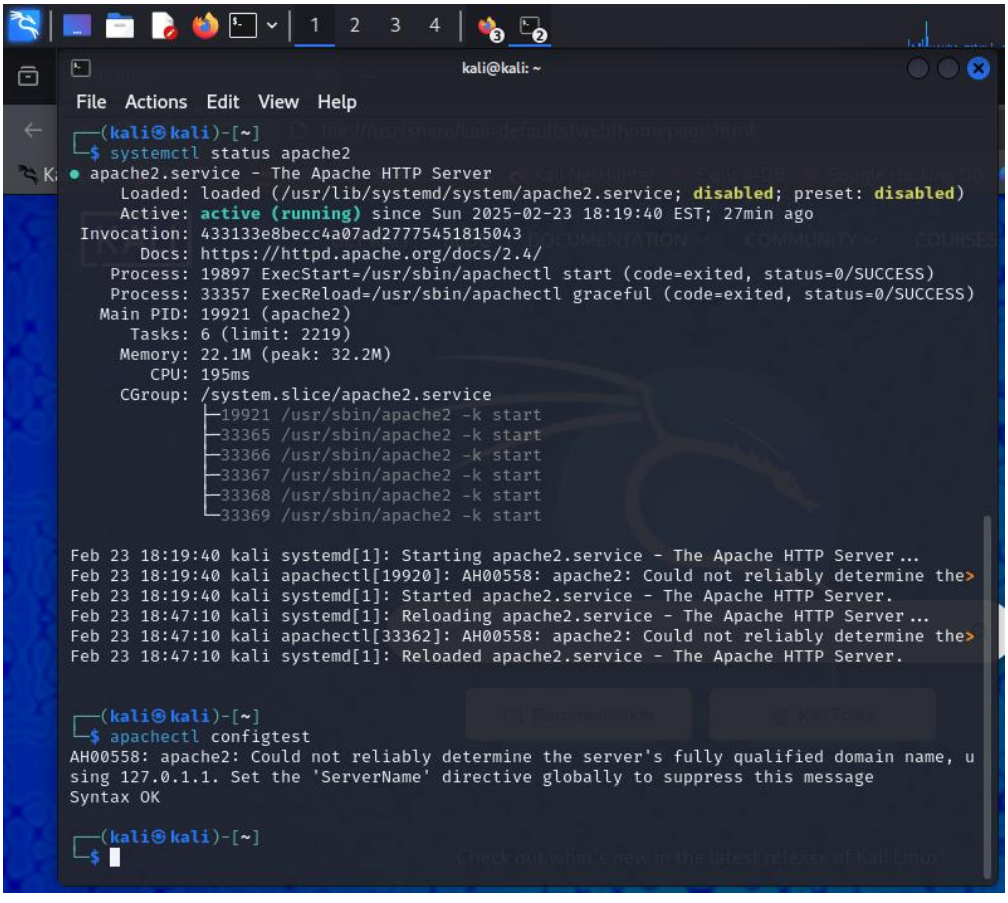

1 2 3 4
kali@kali: ~
File Actions Edit View Help
GNU nano 8.2 /etc/apache2/sites-available/default-ssl.conf
<VirtualHost *:443>
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html
Available loglevels: trace8, ... , trace1, debug, info, notice, war>
error, crit, alert, emerg.
It is also possible to configure the loglevel for particular
modules, e.g.
#LogLevel info ssl:warn
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
For most configuration files from conf-available/, which are
enabled or disabled at a global level, it is possible to
include a line for only one particular virtual host. For example t>
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.
[Read 101 lines]
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
Trash
File System
Home

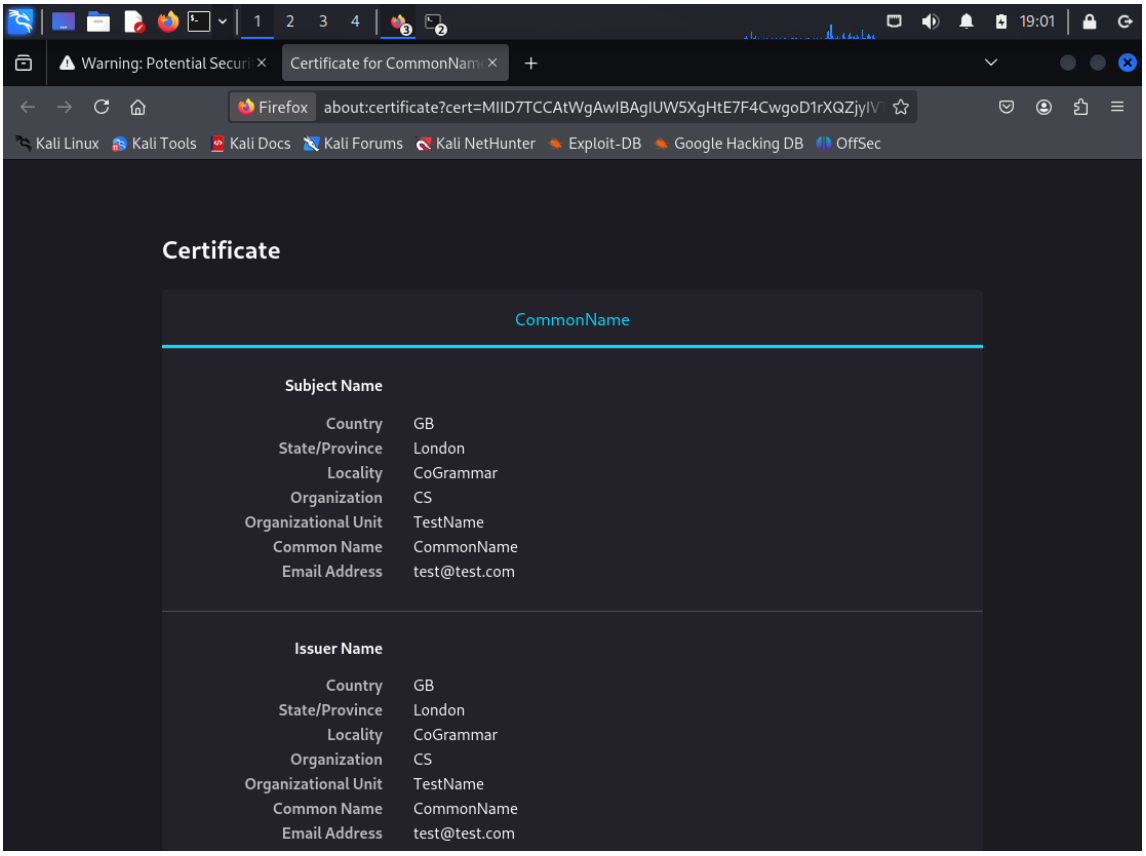

1 2 3 4
kali@kali: ~
File Actions Edit View Help
systemctl reload apache2
(kali㉿kali)-[~]
$ systemctl reload apache2
(kali㉿kali)-[~]
$ sudo a2ensite default-ssl
Site default-ssl already enabled
(kali㉿kali)-[~]
$ systemctl status apache2
● apache2.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
Active: active (running) since Sun 2025-02-23 18:19:40 EST; 27min ago
Invocation: 433133e8becc4a07ad27775451815043
Docs: https://httpd.apache.org/docs/2.4/
Process: 19897 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Process: 33357 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
Main PID: 19921 (apache2)
Tasks: 6 (limit: 2219)
Memory: 22.1M (peak: 32.2M)
CPU: 195ms
CGroup: /system.slice/apache2.service
├─19921 /usr/sbin/apache2 -k start
├─33365 /usr/sbin/apache2 -k start
├─33366 /usr/sbin/apache2 -k start
├─33367 /usr/sbin/apache2 -k start
├─33368 /usr/sbin/apache2 -k start
└─33369 /usr/sbin/apache2 -k start
Feb 23 18:19:40 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Feb 23 18:19:40 kali apachectl[19920]: AH00558: apache2: Could not reliably determine the>
Feb 23 18:19:40 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
Feb 23 18:47:10 kali systemd[1]: Reloading apache2.service - The Apache HTTP Server ...
Feb 23 18:47:10 kali apachectl[33362]: AH00558: apache2: Could not reliably determine the>
Feb 23 18:47:10 kali systemd[1]: Reloaded apache2.service - The Apache HTTP Server.
lines 1-25/25 (END)

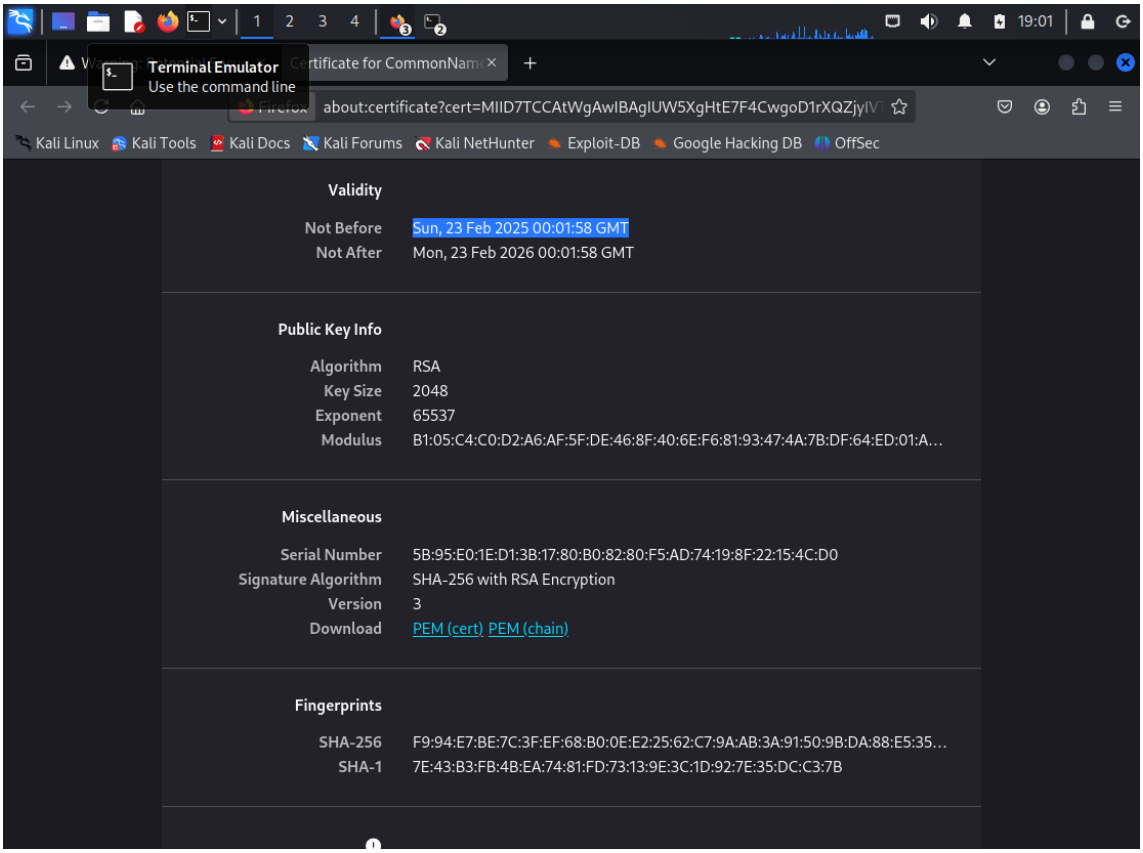

1 2 3 4
kali@kali: ~
File Actions Edit View Help
Trash
File System
Home
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CS
Organizational Unit Name (eg, section) []:TestName
Common Name (e.g. server FQDN or YOUR name) []:CommonName
Email Address []:test@test.com
(kali㉿kali)-[~]
$ sudo ap2enmod ssl
[sudo] password for kali:
sudo: ap2enmod: command not found
(kali㉿kali)-[~]
$ 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 creat
e self-signed certificates.
To activate the new configuration, you need to run:
systemctl restart apache2
(kali㉿kali)-[~]
$ systemctl restart apache2
(kali㉿kali)-[~]
$


1 2 3 4
18:48
Firefox ESR
Browse the World Wide Web
127.0.0.1
Kali Linux
Kali Tools
Kali Docs
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf


Warning: Potential Securi
Not Secure
https://127.0.0.1
YouTube — youtube.com
Facebook — facebook.com
Reddit — reddit.com
BBC — bbc.co.uk
eBay — ebay.co.uk
Recent Searches
127..0.0.1
This time, search with:
Go Back (Recommended)
Advanced...
127.0.0.1 uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT
View Certificate
Go Back (Recommended)
Accept the Risk and Continue


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ systemctl status apache2
● apache2.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
Active: active (running) since Sun 2025-02-23 18:19:40 EST; 27min ago
Invocation: 433133e8becc4a07ad27775451815043
Docs: https://httpd.apache.org/docs/2.4/
Process: 19897 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Process: 33357 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
Main PID: 19921 (apache2)
Tasks: 6 (limit: 2219)
Memory: 22.1M (peak: 32.2M)
CPU: 195ms
CGroup: /system.slice/apache2.service
├─19921 /usr/sbin/apache2 -k start
├─33365 /usr/sbin/apache2 -k start
├─33366 /usr/sbin/apache2 -k start
├─33367 /usr/sbin/apache2 -k start
├─33368 /usr/sbin/apache2 -k start
└─33369 /usr/sbin/apache2 -k start
Feb 23 18:19:40 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Feb 23 18:19:40 kali apachectl[19920]: AH00558: apache2: Could not reliably determine the>
Feb 23 18:19:40 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
Feb 23 18:47:10 kali systemd[1]: Reloading apache2.service - The Apache HTTP Server ...
Feb 23 18:47:10 kali apachectl[33362]: AH00558: apache2: Could not reliably determine the>
Feb 23 18:47:10 kali systemd[1]: Reloaded apache2.service - The Apache HTTP Server.
(kali㉿kali)-[~]
$ apachectl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, u
sing 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
(kali㉿kali)-[~]
$


Warning: Potential Securi
Certificate for CommonNam
Firefox
about:certificate?cert=MIID7TCCAtWgAwIBAgIUW5XgHtE7F4CwgoD1rXQZjyIV
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Certificate
CommonName
Subject Name
Country GB
State/Province London
Locality CoGrammar
Organization CS
Organizational Unit TestName
Common Name CommonName
Email Address test@test.com
Issuer Name
Country GB
State/Province London
Locality CoGrammar
Organization CS
Organizational Unit TestName
Common Name CommonName
Email Address test@test.com


Terminal Emulator
Use the command line
about:certificate?cert=MIID7TCCAtWgAwIBAgIUW5XgHtE7F4CwgoD1rXQZjyIV
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Validity
Not Before Sun, 23 Feb 2025 00:01:58 GMT
Not After Mon, 23 Feb 2026 00:01:58 GMT
Public Key Info
Algorithm RSA
Key Size 2048
Exponent 65537
Modulus B1:05:C4:C0:D2:A6:AF:5F:DE:46:8F:40:6E:F6:81:93:47:4A:7B:DF:64:ED:01:A…
Miscellaneous
Serial Number 5B:95:E0:1E:D1:3B:17:80:B0:82:80:F5:AD:74:19:8F:22:15:4C:D0
Signature Algorithm SHA-256 with RSA Encryption
Version 3
Download PEM (cert) PEM (chain)
Fingerprints
SHA-256 F9:94:E7:BE:7C:3F:EF:68:B0:0E:E2:25:62:C7:9A:AB:3A:91:50:9B:DA:88:E5:35…
SHA-1 7E:43:B3:FB:4B:EA:74:81:FD:73:13:9E:3C:1D:92:7E:35:DC:C3:7B

1
2
File Actions Edit View Help
GNU nano 8.2
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 /home/kali/test_server.crt
SSLCertificateKeyFile /home/kali/test_server.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
certificate for convinience.
#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt
Certificate Authority (CA):
Set the CA certificate verification path where to find CA
certificates for client authentication or alternatively one
huge file containing all of them (file must be PEM encoded)
Note: Inside SSLCACertificatePath you need hash symlinks
to point to the certificate files. Use the provided
Makefile to update the hash symlinks after changes.
#SSLCACertificatePath /etc/ssl/certs/
#SSLCACertificateFile /etc/apache2/ssl.crt/ca-bundle.crt
Certificate Revocation Lists (CRL):
Set the CA revocation path where to find CA CRLs for client
authentication or alternatively one huge file containing all
of them (file must be PEM encoded)
Note: Inside SSLCARevocationPath you need hash symlinks
to point to the certificate files. Use the provided
Makefile to update the hash symlinks after changes.
#SSLCARevocationPath /etc/apache2/ssl.crl/
#SSLCARevocationFile /etc/apache2/ssl.crl/ca-bundle.crl
Client Authentication (Type):
Client certificate verification type and depth. Types are
none, optional, require and optional_no_ca. Depth is a
number which specifies how deeply to verify the certificate
issuer chain before deciding the certificate is not valid.
#SSLVerifyClient require
#SSLVerifyDepth 10
SSL Engine Options:
Set various options for the SSL engine.
o FakeBasicAuth:
Translate the client X.509 into a Basic Authorisation. This means that
the standard Auth/DBMAuth methods can be used for access control. The
user name is the 'one line' version of the client's X.509 certificate.
Note that no password is obtained from the user. Every entry in the user
file needs this password: 'xxj31ZMTZzkVA'.
o ExportCertData:
This exports two additional environment variables: SSL_CLIENT_CERT and
SSL_SERVER_CERT. These contain the PEM-encoded certificates of the
server (always existing) and the client (only existing when client
authentication is used). This can be used to import the certificates
into CGI scripts.
o StdEnvVars:
This exports the standard SSL/TLS related 'SSL_*' environment variables.
Per default this exportation is switched off for performance reasons,
because the extraction step is an expensive operation and is usually
useless for serving static content. So one usually enables the
exportation for CGI and SSI requests only.
o OptRenegotiate:
This enables optimized SSL connection renegotiation handling when SSL
directives are used in per-directory context.
#SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
<FilesMatch "\.(?:cgi|shtml|phtml|php)$">
SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
SSLOptions +StdEnvVars
</Directory>
<Directory /var/www/html>
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
<IfModule mod_headers.c>
Header always set X-Content-Type-Options "nosniff"
</IfModule>
</VirtualHost>
Warning: Potential Sec
Kali Tools
Kali Docs

6.

I am issued the certificate. And the certificate will be expire in 365 days.