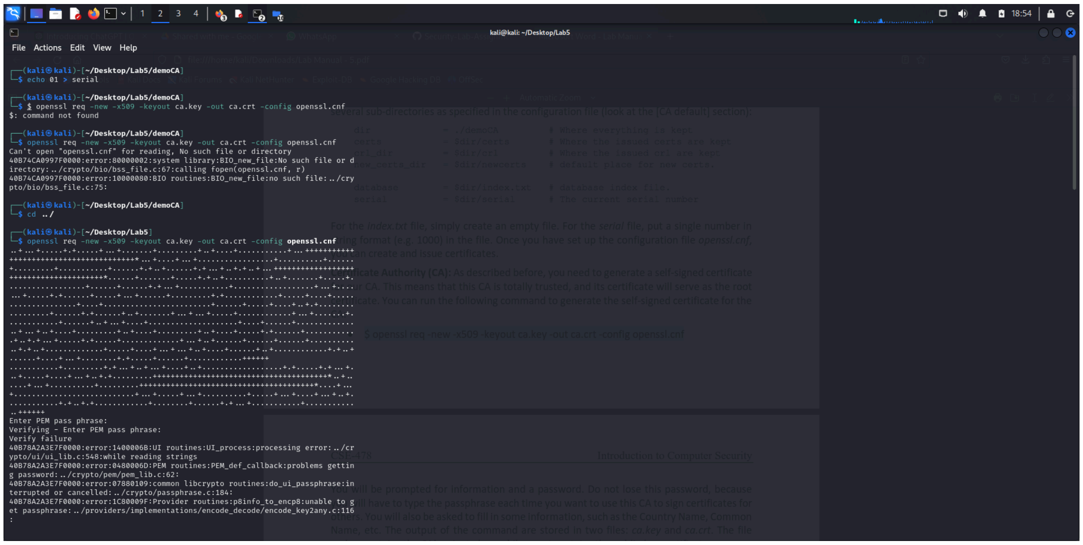
Lab Report 5:

Task-1: Becoming a certificate authority

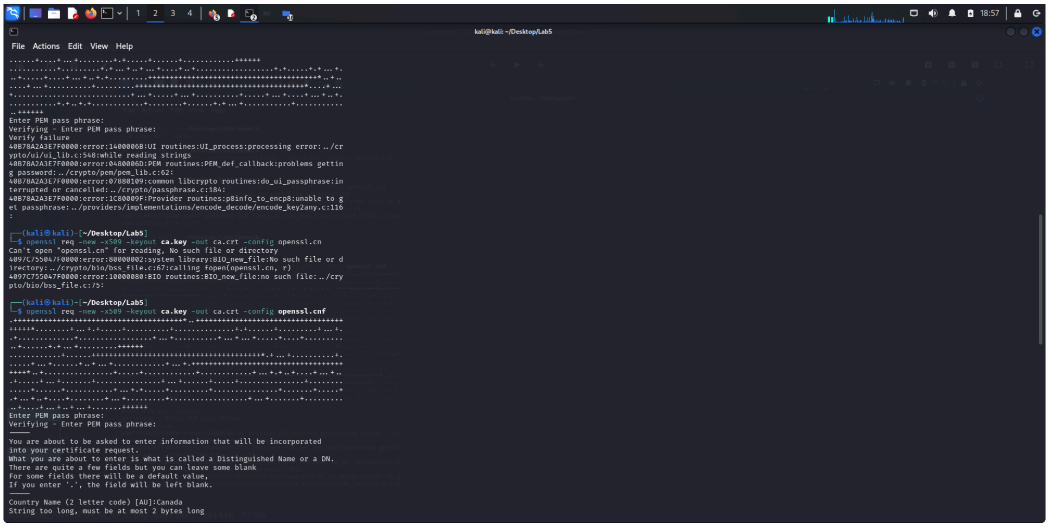
First I've created a configuration file. Then generated a self-signed certificate for our CA.

$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf



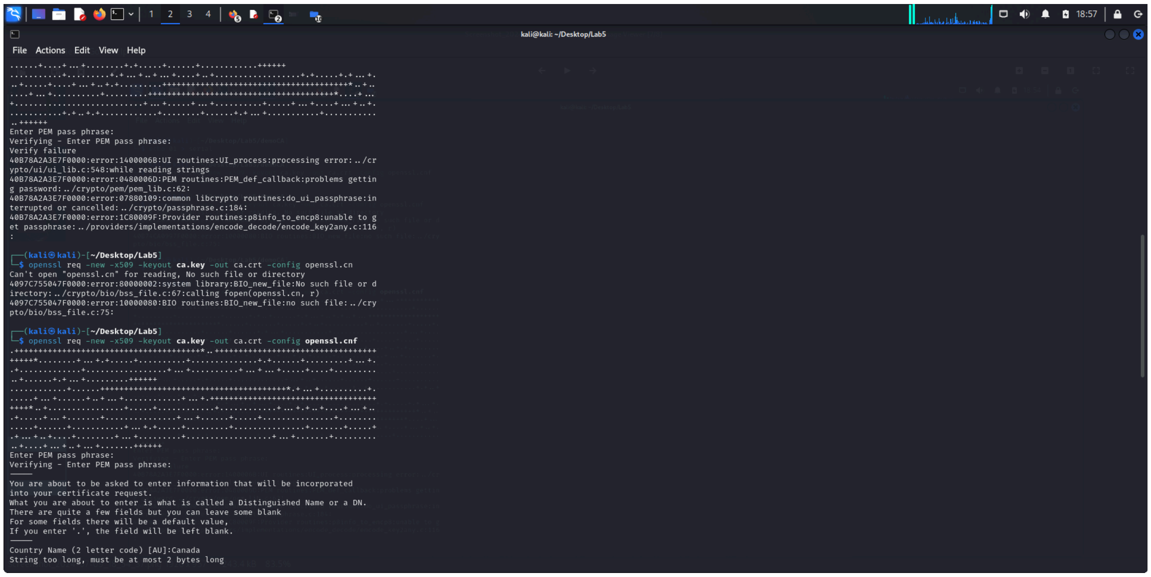
```
┌──(kali㉿kali)-[~/Desktop/Lab5/demoCA]
└─$ echo 01 > serial

┌──(kali㉿kali)-[~/Desktop/Lab5/demoCA]
└─$ $ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
$: command not found

┌──(kali㉿kali)-[~/Desktop/Lab5/demoCA]
└─$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
Can't open "openssl.cnf" for reading, No such file or directory
40B74CA0997F0000:error:80000002:system library:BIO_new_file:No such file or d
irectory:../crypto/bio/bss_file.c:67:calling fopen(openssl.cnf, r)
40B74CA0997F0000:error:10000080:BIO routines:BIO_new_file:no such file:../cry
pto/bio/bss_file.c:75:

┌──(kali㉿kali)-[~/Desktop/Lab5/demoCA]
└─$ cd ../

┌──(kali㉿kali)-[~/Desktop/Lab5]
└─$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
..+...+.....+.+.....+...+.......+.........+..+....+...........+...+++++++++++
+++++++++++++++++++++++++++++*...+....+...+.................+.........+......
+.........+..........+......+.+..+......+.+...+..+.+..+...+++++++++++++++++++
++++++++++++++++++++*......+.......+.....+.+..+..........+..+.......+.....+.
................+......+......+.+...+...........+..................+...+...
...+.....+.+......+.....+...+......+.........+.+.............+.....+....+....
...............+....+.....................+......+.....+....+..+.+........
.........+.....+.+......+..+.......+...+...+.....+............+...+....+.
...........+......+..+...+....+..................+....+......+...........
..+...+..+....+.........+..+....+.........+..+....+......+.+......+.........
.+..+.+...+.....+.+......+.............+...+..+......+......+......+........
..+.+..+............+.....+....+...+...+..+....+......+..+............+.+..+
......+....+...+........+.+.....+......+............++++++
..........+.........+.+...+..+...+.....+..+..................+.+.....+.+...+.
..+.....+....+...+..+.+.........+++++++++++++++++++++++++++++++++++++++*..+..
....+...+..........+.........++++++++++++++++++++++++++++++++++++++++*....+...
+.........................+...+......+...+...........+.....+...+.....+...+..+.
..........+.+..+.+............+........+......+.+...+............+..........
..++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
Verify failure
40B78A2A3E7F0000:error:1400006B:UI routines:UI_process:processing error:../cr
ypto/ui/ui_lib.c:548:while reading strings
40B78A2A3E7F0000:error:0480006D:PEM routines:PEM_def_callback:problems gettin
g password:../crypto/pem/pem_lib.c:62:
40B78A2A3E7F0000:error:07880109:common libcrypto routines:do_ui_passphrase:in
terrupted or cancelled:../crypto/passphrase.c:184:
40B78A2A3E7F0000:error:1C80009F:Provider routines:p8info_to_encp8:unable to g
et passphrase:../providers/implementations/encode_decode/encode_key2any.c:116
:
```

Step 1: Generate public/private key pair
$ openssl genrsa -des3 -out server.key 1024



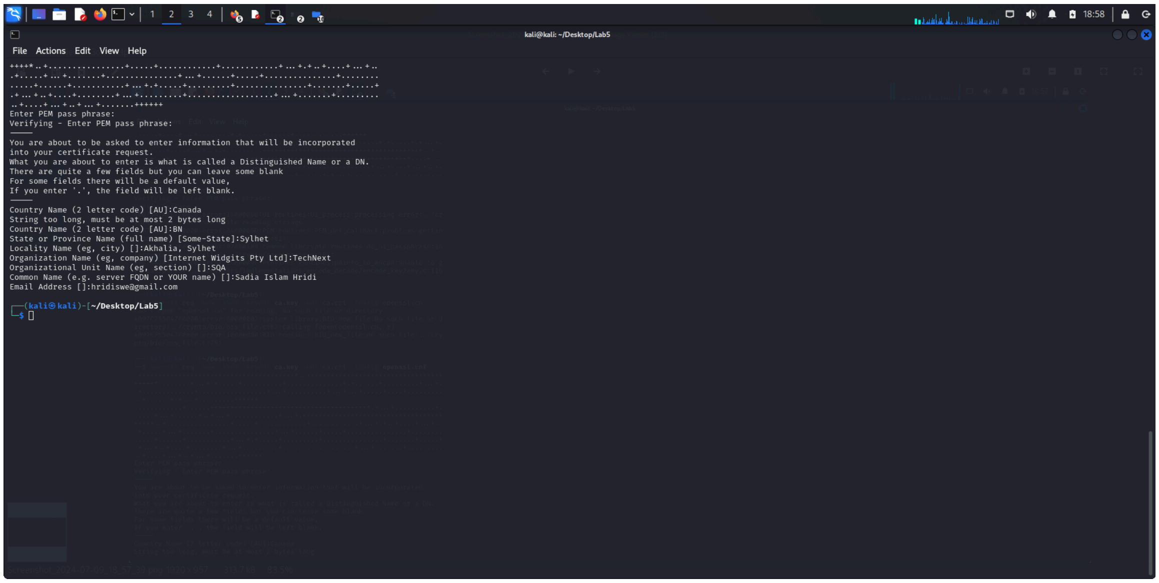
```
......+....+...+........+.+.....+......+............++++++
..........+.........+.+...+..+...+.....+..+..................+.+.....+.+...+.
..+.....+....+...+..+.+.........+++++++++++++++++++++++++++++++++++++++*..+..
....+...+..........+.........++++++++++++++++++++++++++++++++++++++++*....+...
+.........................+...+......+...+...........+.....+...+.....+...+..+.
..........+.+..+.+............+........+......+.+...+............+..........
..++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
Verify failure
40B78A2A3E7F0000:error:1400006B:UI routines:UI_process:processing error:../cr
ypto/ui/ui_lib.c:548:while reading strings
40B78A2A3E7F0000:error:0480006D:PEM routines:PEM_def_callback:problems gettin
g password:../crypto/pem/pem_lib.c:62:
40B78A2A3E7F0000:error:07880109:common libcrypto routines:do_ui_passphrase:in
terrupted or cancelled:../crypto/passphrase.c:184:
40B78A2A3E7F0000:error:1C80009F:Provider routines:p8info_to_encp8:unable to g
et passphrase:../providers/implementations/encode_decode/encode_key2any.c:116
:

┌──(kali㉿kali)-[~/Desktop/Lab5]
└─$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cn
Can't open "openssl.cn" for reading, No such file or directory
4097C755047F0000:error:80000002:system library:BIO_new_file:No such file or d
irectory:../crypto/bio/bss_file.c:67:calling fopen(openssl.cn, r)
4097C755047F0000:error:10000080:BIO routines:BIO_new_file:no such file:../cry
pto/bio/bss_file.c:75:

┌──(kali㉿kali)-[~/Desktop/Lab5]
└─$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
.++++++++++++++++++++++++++++++++++++++++*..++++++++++++++++++++++++++++++++++
+++++*........+...+.+.....+..........+..............+.+......+.........+...+.
.+.............+................+...+..........+...+...+.....+....+.........
..+......+.+...+.........++++++
............+......++++++++++++++++++++++++++++++++++++++++*.+...+..........+.
.....+...+......+..+...+...........+...+.+++++++++++++++++++++++++++++++++++
++++*..+...............+.....+............+...........+...+.+..+....+...+..
.+.....+...+.......+..............+...+......+.....+..............+........
.....+......+..........+...+.+.....+.........+..............+.......+.....+
.+...+..+....+.......+...+.........+.................+...+.......+.........
..+....+...+..+...+.......++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:Canada
String too long, must be at most 2 bytes long
```

Step 2: Generate a Certificate Signing Request (CSR)
$ openssl req -new -key server.key -out server.csr -config openssl.cnf



```
......+....+...+........+.+.....+......+............++++++
..........+..........+.+...+..+...+....+..+...................+.+.....+.+...+.
..+.....+....+...+..+.+.........+++++++++++++++++++++++++++++++++++++++*..+..
....+...+..........+.........+++++++++++++++++++++++++++++++++++++++*....+...
+..........................+...+.....+...+..........+.....+...+....+...+..+.
...........+.+..+.+............+........+......+.+...+...........+...........
..++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
Verify failure
40B78A2A3E7F0000:error:1400006B:UI routines:UI_process:processing error:../cr
ypto/ui/ui_lib.c:548:while reading strings
40B78A2A3E7F0000:error:0480006D:PEM routines:PEM_def_callback:problems gettin
g password:../crypto/pem/pem_lib.c:62:
40B78A2A3E7F0000:error:07880109:common libcrypto routines:do_ui_passphrase:in
terrupted or cancelled:../crypto/passphrase.c:184:
40B78A2A3E7F0000:error:1C80009F:Provider routines:p8info_to_encp8:unable to g
et passphrase:../providers/implementations/encode_decode/encode_key2any.c:116
:

┌──(kali㉿kali)-[~/Desktop/Lab5]
└─$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cn
Can't open "openssl.cn" for reading, No such file or directory
4097C755047F0000:error:80000002:system library:BIO_new_file:No such file or d
irectory:../crypto/bio/bss_file.c:67:calling fopen(openssl.cn, r)
4097C755047F0000:error:10000080:BIO routines:BIO_new_file:no such file:../cry
pto/bio/bss_file.c:75:

┌──(kali㉿kali)-[~/Desktop/Lab5]
└─$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
.+++++++++++++++++++++++++++++++++++++++*..++++++++++++++++++++++++++++++++++
+++++*........+...+.+.....+..........+..............+.+......+.........+...+.
.+............+................+...+..........+...+...+.....+....+.........
..+......+.+...+.........++++++
...........+......+++++++++++++++++++++++++++++++++++++++*.+...+..........+.
.....+...+......+..+...+............+...+.++++++++++++++++++++++++++++++++++
++++*..+................+.....+............+............+...+.+..+....+...+..
.+.....+...+.......+...............+...+......+.....+...............+.......
.....+......+...........+...+.+.....+.........+...............+.......+.....+
.+...+..+....+........+...+.........+.................+...+.......+.........
..+....+...+..+...+.......++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:Canada
String too long, must be at most 2 bytes long
```

Step 3: Generating Certificates
$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf



```
++++*..+................+.....+............+............+...+.+..+....+...+..
.+.....+...+.......+...............+...+......+.....+...............+.......
.....+......+...........+...+.+.....+.........+...............+.......+.....+
.+...+..+....+........+...+.........+.................+...+.......+.........
..+....+...+..+...+.......++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:Canada
String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]:BN
State or Province Name (full name) [Some-State]:Sylhet
Locality Name (eg, city) []:Akhalia, Sylhet
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TechNext
Organizational Unit Name (eg, section) []:SQA
Common Name (e.g. server FQDN or YOUR name) []:Sadia Islam Hridi
Email Address []:hridiswe@gmail.com

┌──(kali㉿kali)-[~/Desktop/Lab5]
└─$ 
```

Apache Web Server Installation & Maintenance:

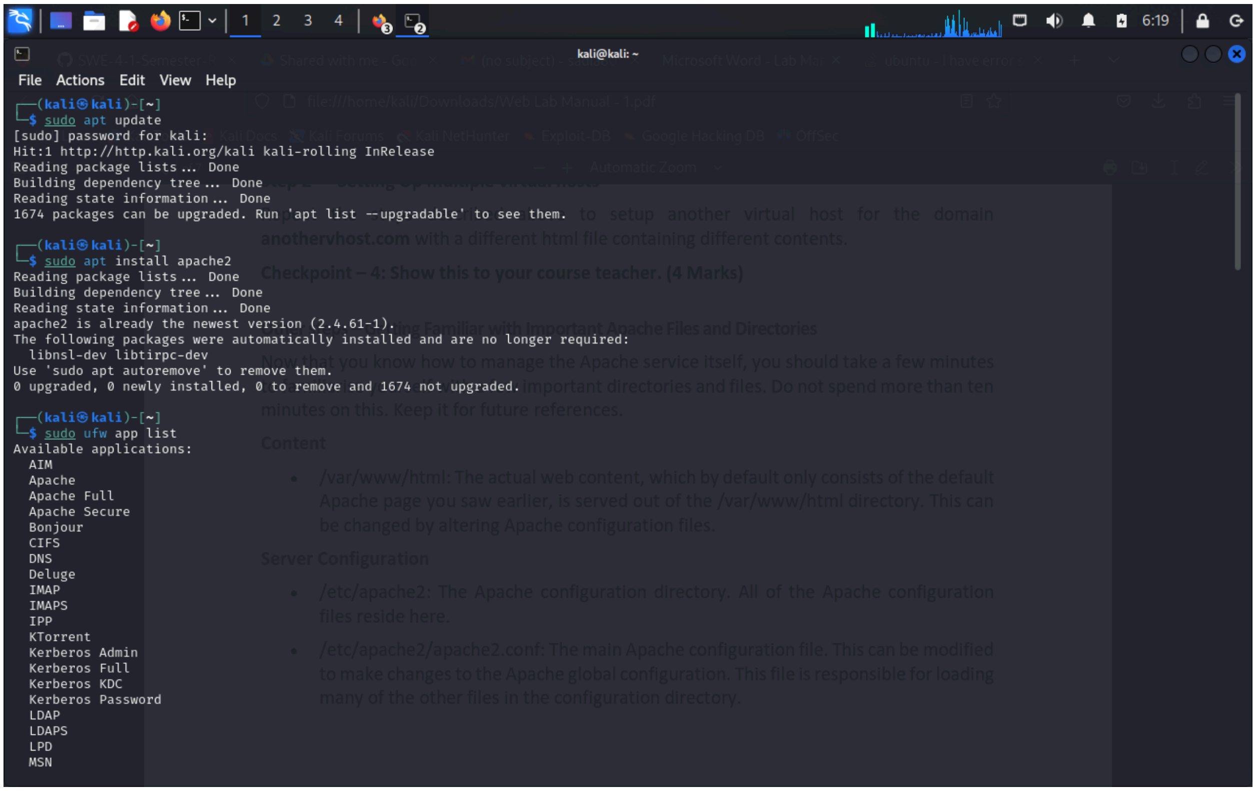
Task-1: Setting up an Apache web server

Step 1 — Installing Apache

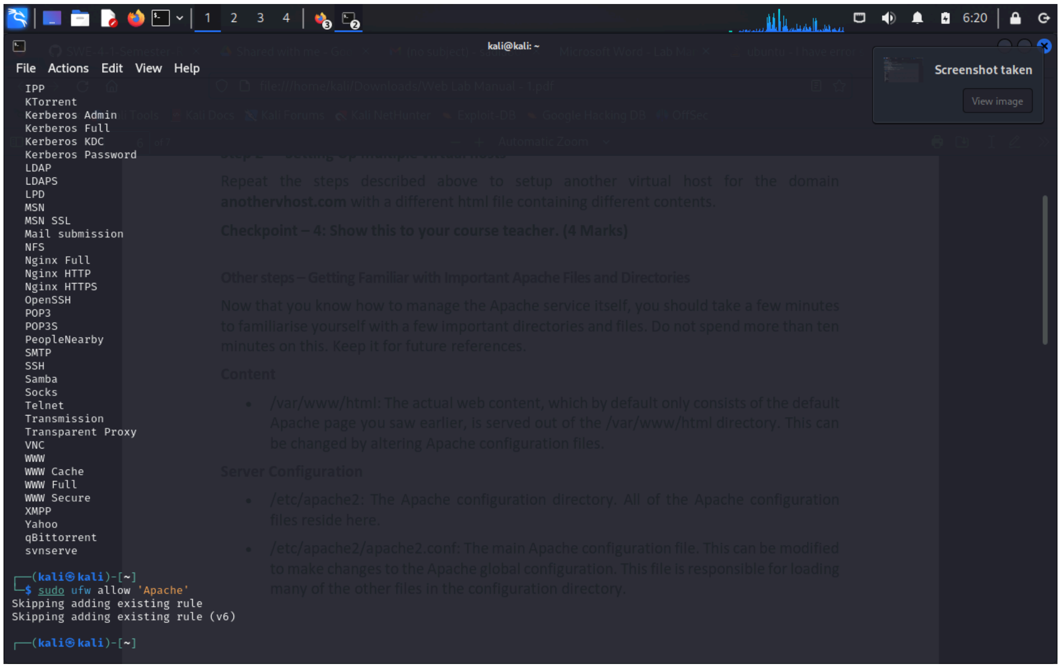
sudo apt update
sudo apt install apache2

Step 2 — Adjusting the Firewall

sudo ufw app list

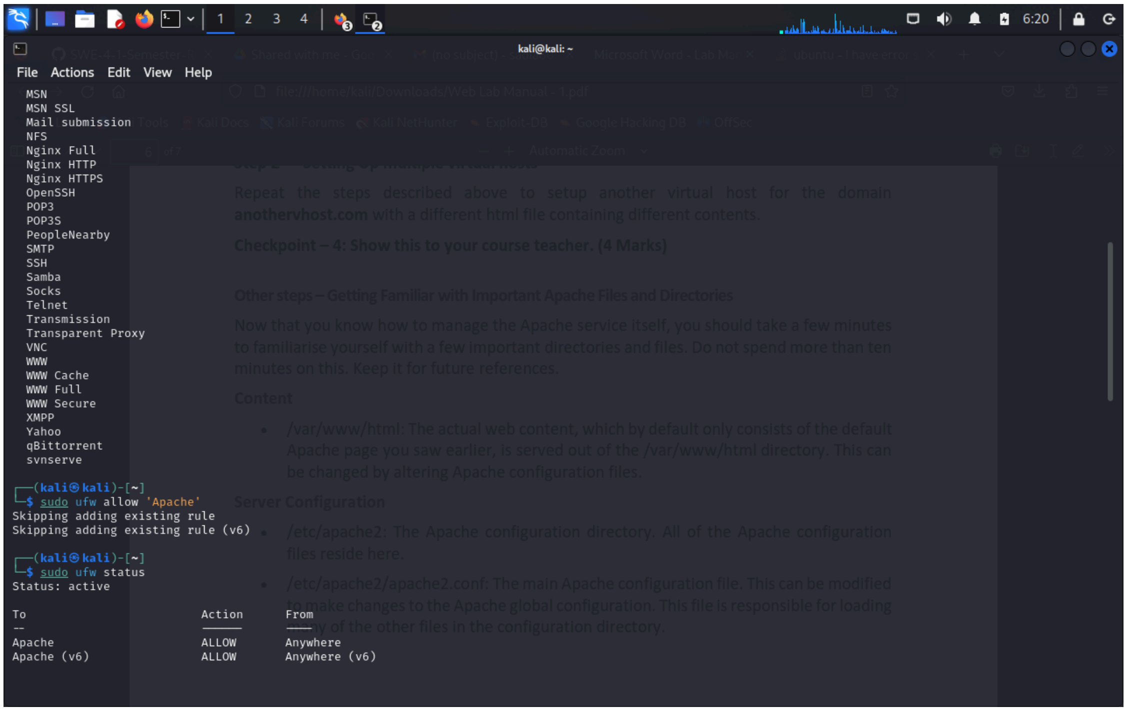


```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1674 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(kali㉿kali)-[~]
└─$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.61-1).
The following packages were automatically installed and are no longer required:
  libnsl-dev libtirpc-dev
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1674 not upgraded.

┌──(kali㉿kali)-[~]
└─$ sudo ufw app list
Available applications:
  AIM
  Apache
  Apache Full
  Apache Secure
  Bonjour
  CIFS
  DNS
  Deluge
  IMAP
  IMAPS
  IPP
  KTorrent
  Kerberos Admin
  Kerberos Full
  Kerberos KDC
  Kerberos Password
  LDAP
  LDAPS
  LPD
  MSN
```



```
IPP
KTorrent
Kerberos Admin
Kerberos Full
Kerberos KDC
Kerberos Password
LDAP
LDAPS
LPD
MSN
MSN SSL
Mail submission
NFS
Nginx Full
Nginx HTTP
Nginx HTTPS
OpenSSH
POP3
POP3S
PeopleNearby
SMTP
SSH
Samba
Socks
Telnet
Transmission
Transparent Proxy
VNC
WWW
WWW Cache
WWW Full
WWW Secure
XMPP
Yahoo
qBittorrent
svnserve

┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 'Apache'
Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(kali㉿kali)-[~]
```

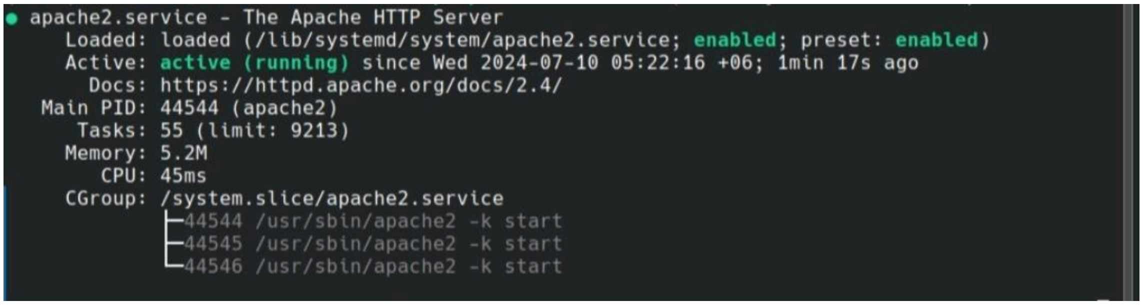
sudo ufw allow 'Apache'
sudo ufw status



```
MSN
MSN SSL
Mail submission
NFS
Nginx Full
Nginx HTTP
Nginx HTTPS
OpenSSH
POP3
POP3S
PeopleNearby
SMTP
SSH
Samba
Socks
Telnet
Transmission
Transparent Proxy
VNC
WWW
WWW Cache
WWW Full
WWW Secure
XMPP
Yahoo
qBittorrent
svnserve

┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 'Apache'
Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(kali㉿kali)-[~]
└─$ sudo ufw status
Status: active

To                          Action      From
--                          ------      ----
Apache                      ALLOW       Anywhere
Apache (v6)                 ALLOW       Anywhere (v6)
```

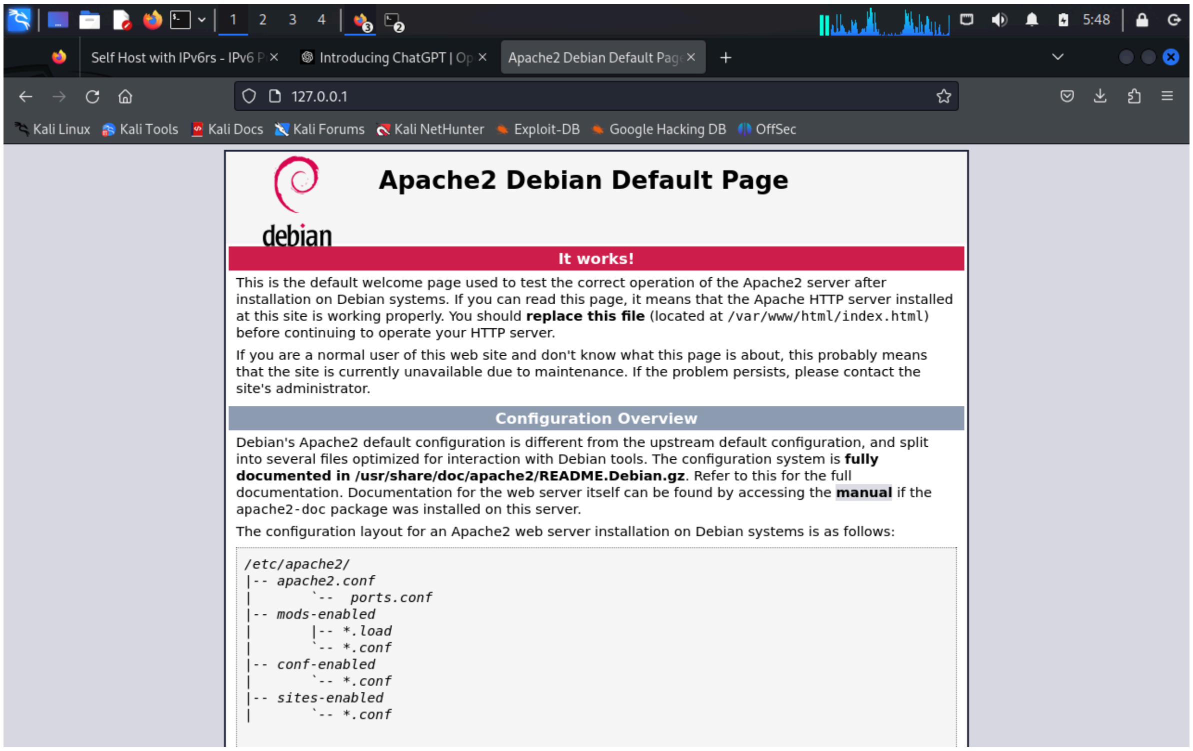
Step 3 — Checking your Web Server

sudo systemctl status apache2



```
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Wed 2024-07-10 05:22:16 +06; 1min 17s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 44544 (apache2)
      Tasks: 55 (limit: 9213)
     Memory: 5.2M
        CPU: 45ms
     CGroup: /system.slice/apache2.service
             ├─44544 /usr/sbin/apache2 -k start
             ├─44545 /usr/sbin/apache2 -k start
             └─44546 /usr/sbin/apache2 -k start
```

Now, to check the installation of Apache, enter this domain or its IP address into your browser's address bar:
http://webserverlab.com or http://localhost or http://127.0.0.1 or http://ip_address



Apache2 Debian Default Page

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.

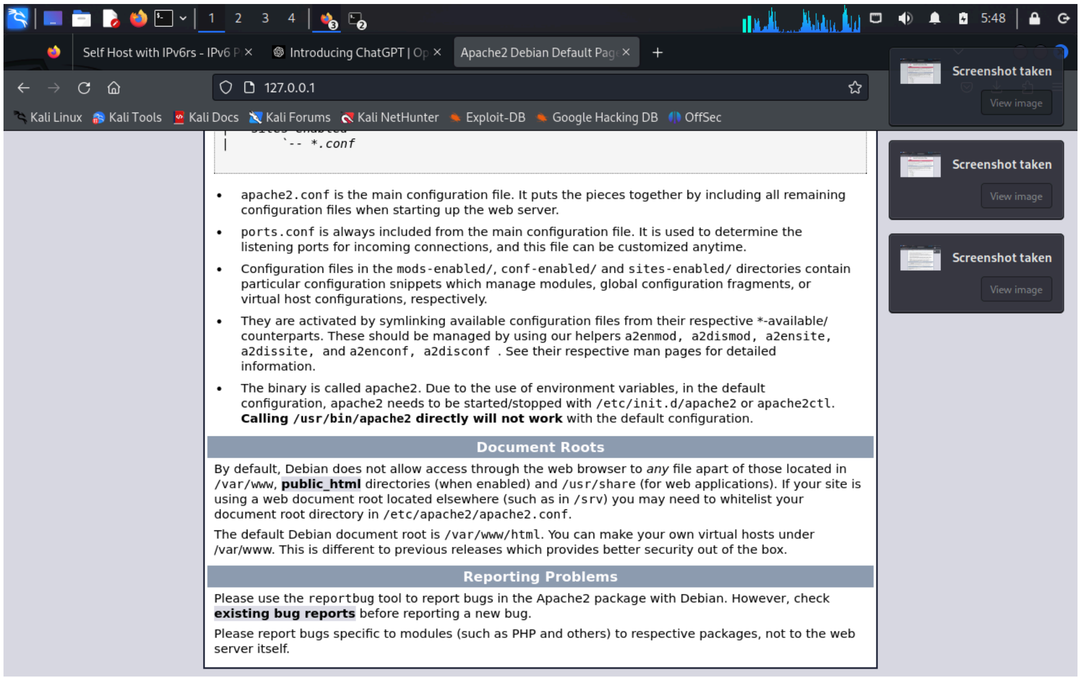
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

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
```



```
|       `-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. **Calling /usr/bin/apache2 directly will not work** with the default configuration.

Document Roots

By default, Debian does not allow access through the web browser to *any* file apart of those located in /var/www, **public_html** directories (when enabled) and /usr/share (for web applications). If your site is using a web document root located elsewhere (such as in /srv) you may need to whitelist your document root directory in /etc/apache2/apache2.conf.

The default Debian document root is /var/www/html. You can make your own virtual hosts under /var/www. This is different to previous releases which provides better security out of the box.

Reporting Problems

Please use the reportbug tool to report bugs in the Apache2 package with Debian. However, check **existing bug reports** before reporting a new bug.

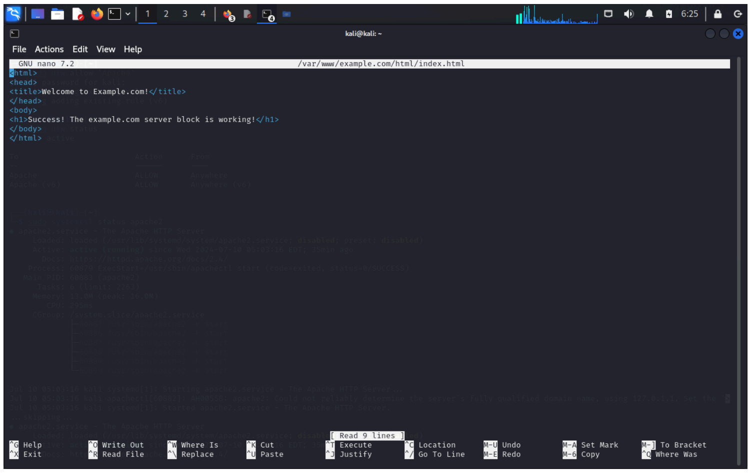
Please report bugs specific to modules (such as PHP and others) to respective packages, not to the web server itself.

Task-2: Setting up virtual hosts

sudo chown -R $USER:$USER /var/www/example.com/html

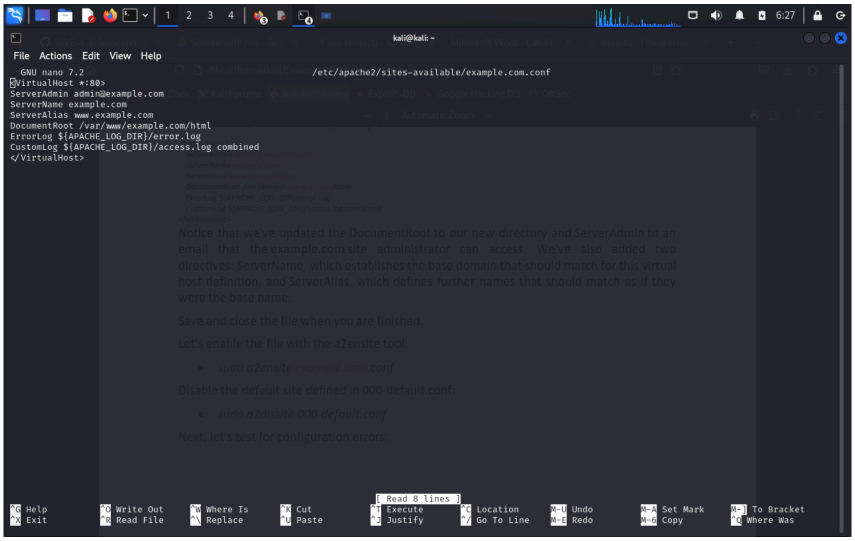
sudo chmod -R 755 /var/www/example.com

nano /var/www/example.com/html/index.html



```
  GNU nano 7.2                    /var/www/example.com/html/index.html
<html>
<head>
<title>Welcome to Example.com!</title>
</head>
<body>
<h1>Success! The example.com server block is working!</h1>
</body>
</html>

                                [ Read 9 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute   ^C Location    M-U Undo    M-A Set Mark  M-] To Bracket
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify   ^/ Go To Line  M-E Redo    M-6 Copy      ^Q Where Was
```

sudo nano /etc/apache2/sites-available/example.com.conf



```
  GNU nano 7.2                       /etc/apache2/sites-available/example.com.conf
<VirtualHost *:80>
ServerAdmin admin@example.com
ServerName example.com
ServerAlias www.example.com
DocumentRoot /var/www/example.com/html
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

                                        [ Read 8 lines ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark   M-] To Bracket
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy       ^Q Where Was
```

Let's enable the file with the a2ensite tool:

->sudo a2ensite example.com.conf
Disable the default site defined in 000-default.conf:

->sudo a2dissite 000-default.conf

Next, let's test for configuration errors:

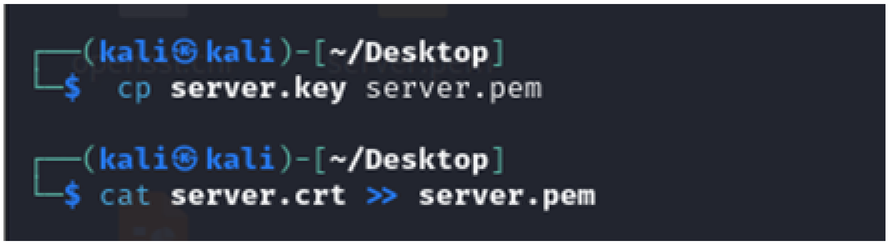
->sudo apache2ctl configtest
I’ve seen a “Syntax OK” output, so it means it is properly configured.

Restart Apache to implement the changes:

->sudo systemctl restart apache2

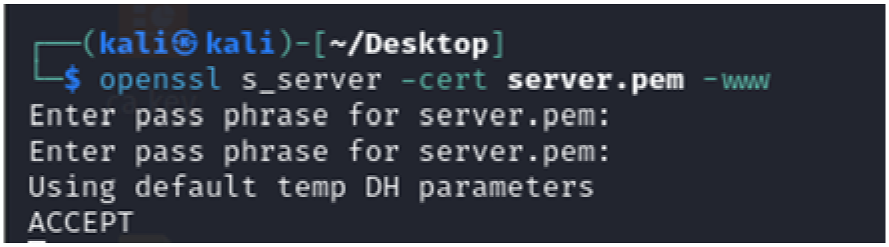
Tasks - 3 : Launching a simple web server with the certificate generated(Lab manual-5)

2. Combining the secret key and certificate into one file:

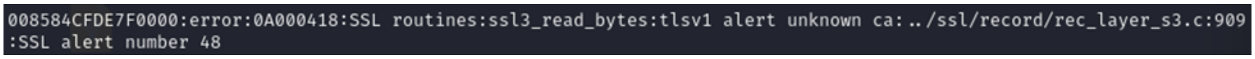


```
┌──(kali㉿kali)-[~/Desktop]
└─$ cp server.key server.pem

┌──(kali㉿kali)-[~/Desktop]
└─$ cat server.crt >> server.pem
```

2. **Launch the web server using server.pem:**

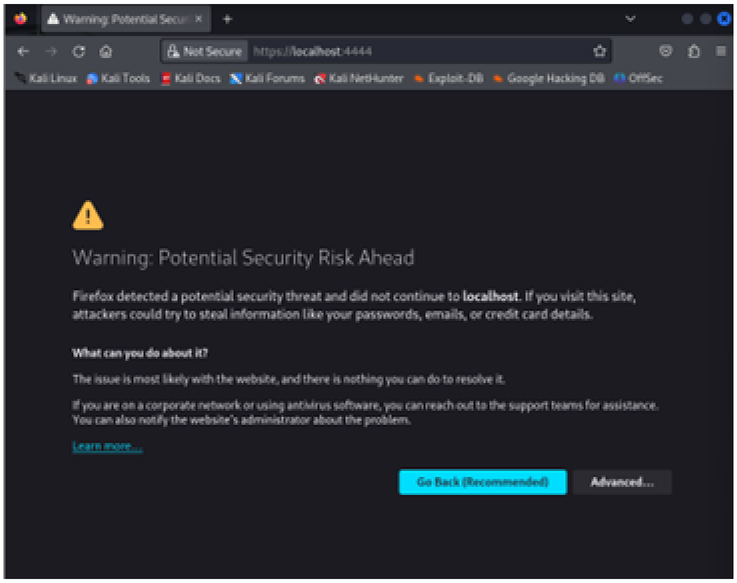


```
┌──(kali㉿kali)-[~/Desktop]
└─$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
```



```
008584CFDE7F0000:error:0A000418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca:../ssl/record/rec_layer_s3.c:909
:SSL alert number 48
```

3.Error message from the browser:



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **localhost**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

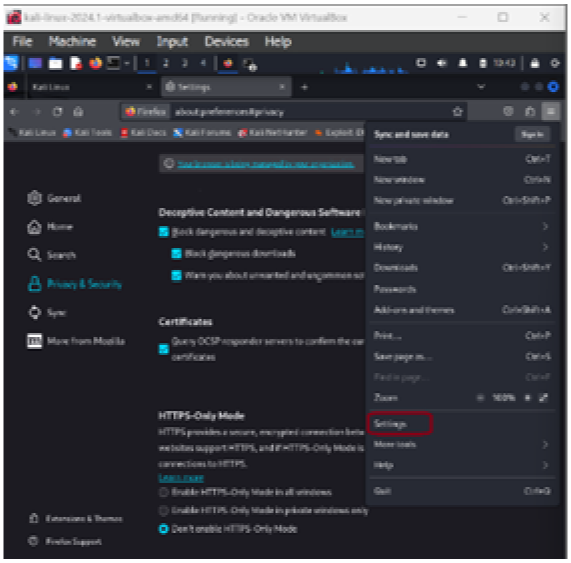
What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more...

4.Manually adding our CA’s certificate to the Firefox browser:



Deceptive Content and Dangerous Software

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

Certificates

☑ Query OCSP responder servers to confirm the current validity of certificates

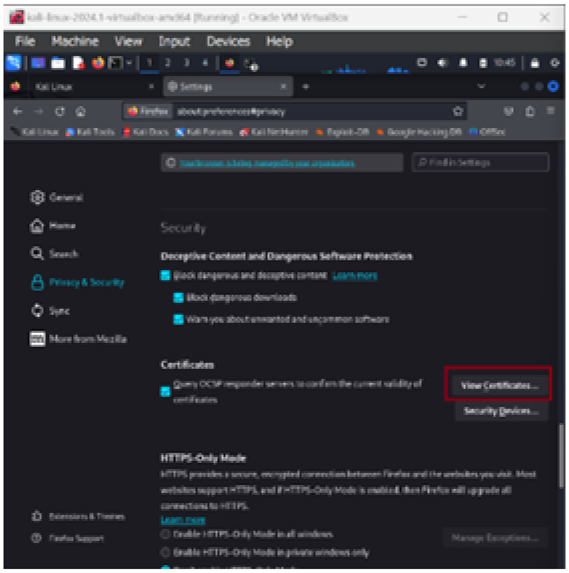
HTTPS-Only Mode

HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS.

○ Enable HTTPS-Only Mode in all windows

○ Enable HTTPS-Only Mode in private windows only

● Don't enable HTTPS-Only Mode


kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Firefox about:preferences#privacy
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Find in Settings
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Extensions & Themes
Firefox Support
View Certificates…
Security Devices…
Manage Exceptions…

Security

Deceptive Content and Dangerous Software Protection

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

Certificates

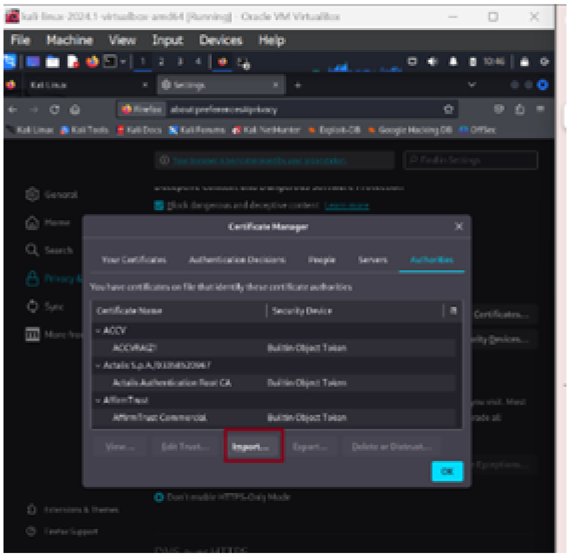
☑ Query OCSP responder servers to confirm the current validity of certificates

HTTPS-Only Mode

HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS.

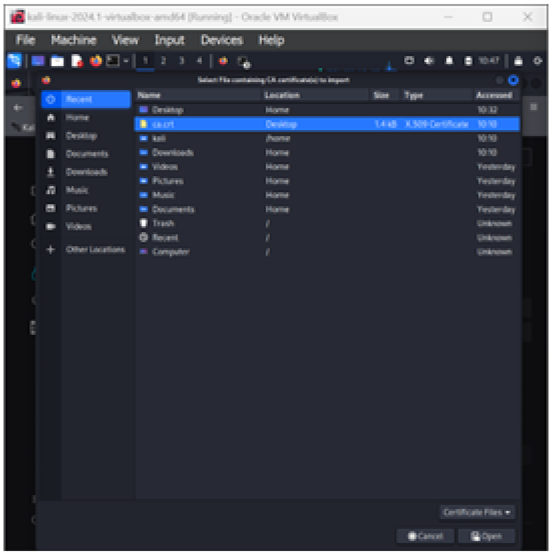
○ Enable HTTPS-Only Mode in all windows

○ Enable HTTPS-Only Mode in private windows only

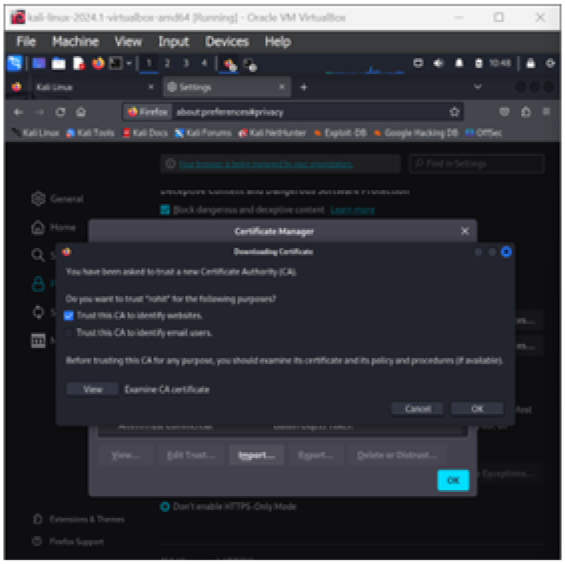

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Firefox about:preferences#privacy
Certificate Manager
Your Certificates
Authentication Decisions
People
Servers
Authorities
View…
Edit Trust…
Import…
Export…
Delete or Distrust…
OK

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
ACCV	
ACCVRAIZ1	Builtin Object Token
Actalis S.p.A./03358520967	
Actalis Authentication Root CA	Builtin Object Token
AffirmTrust	
AffirmTrust Commercial	Builtin Object Token


kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Select File containing CA certificate(s) to import
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Other Locations
Certificate Files
Cancel
Open

Name	Location	Size	Type	Accessed
Desktop	Home			10:32
ca.crt	Desktop	1.4 kB	X.509 Certificate	10:10
kali	/home			10:10
Downloads	Home			10:10
Videos	Home			Yesterday
Pictures	Home			Yesterday
Music	Home			Yesterday
Documents	Home			Yesterday
Trash	/			Unknown
Recent	/			Unknown
Computer	/			Unknown



kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
about:preferences#privacy
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
General
Home
Extensions & Themes
Firefox Support
Certificate Manager
View... Edit Trust... Import... Export... Delete or Distrust...
OK

Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "rohit" for the following purposes?

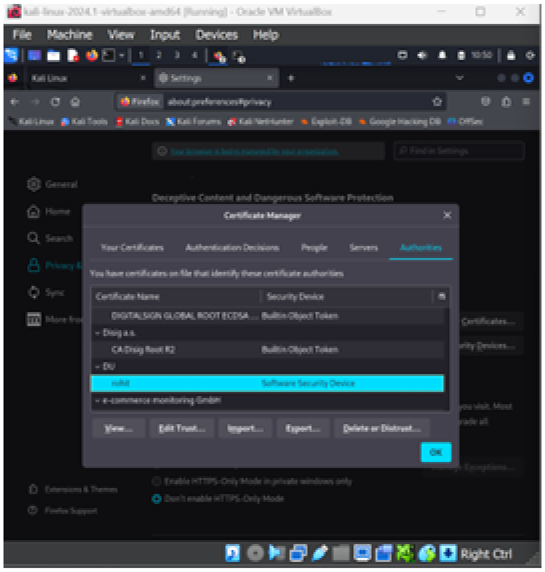
☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

Cancel OK

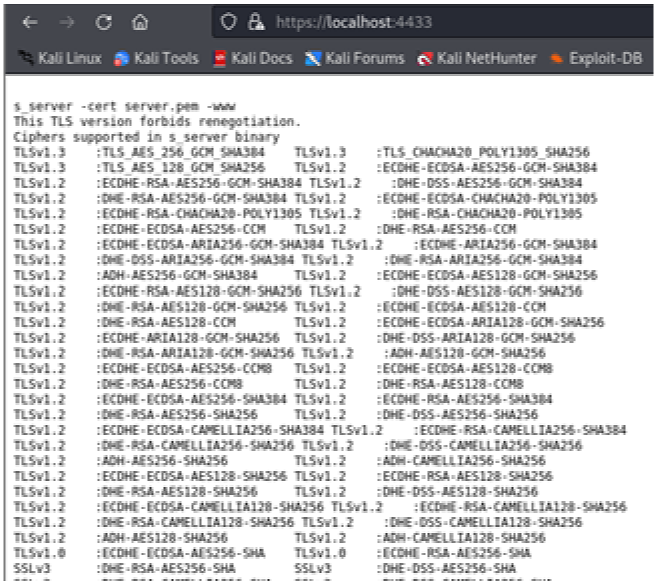


kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
about:preferences#privacy
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Deceptive Content and Dangerous Software Protection
Certificate Manager
Your Certificates
Authentication Decisions
People
Servers
Authorities
View... Edit Trust... Import... Export... Delete or Distrust...
OK
Enable HTTPS-Only Mode in private windows only
Don't enable HTTPS-Only Mode
Right Ctrl

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
DIGITALSIGN GLOBAL ROOT ECDSA ...	Builtin Object Token
⌄ Disig a.s.	
CA Disig Root R2	Builtin Object Token
⌄ DU	
rohit	Software Security Device
⌄ e-commerce monitoring GmbH	

5.In webpage, showing certificaticates’ details:

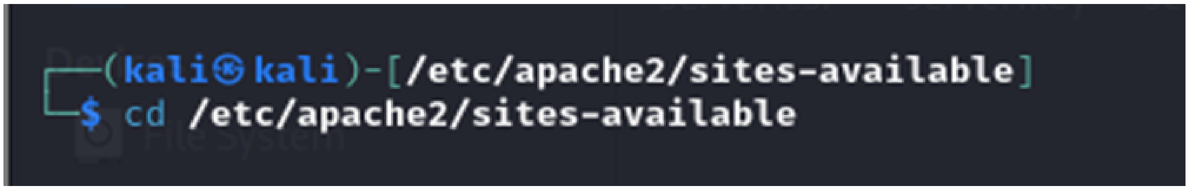


https://localhost:4433
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

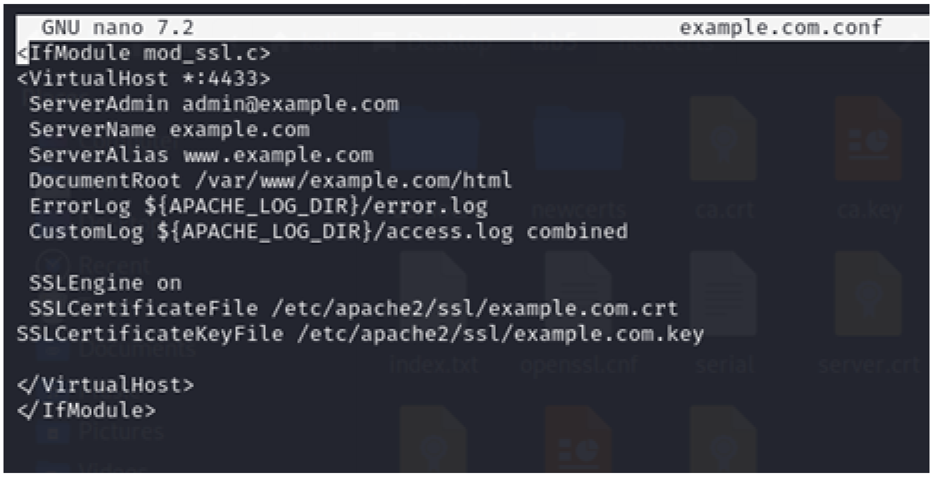
```
s_server -cert server.pem -www
This TLS version forbids renegotiation.
Ciphers supported in s_server binary
TLSv1.3    :TLS_AES_256_GCM_SHA384    TLSv1.3    :TLS_CHACHA20_POLY1305_SHA256
TLSv1.3    :TLS_AES_128_GCM_SHA256    TLSv1.2    :ECDHE-ECDSA-AES256-GCM-SHA384
TLSv1.2    :ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2    :DHE-DSS-AES256-GCM-SHA384
TLSv1.2    :DHE-RSA-AES256-GCM-SHA384 TLSv1.2    :ECDHE-ECDSA-CHACHA20-POLY1305
TLSv1.2    :ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2    :DHE-RSA-CHACHA20-POLY1305
TLSv1.2    :ECDHE-ECDSA-AES256-CCM    TLSv1.2    :DHE-RSA-AES256-CCM
TLSv1.2    :ECDHE-ECDSA-ARIA256-GCM-SHA384 TLSv1.2    :ECDHE-ARIA256-GCM-SHA384
TLSv1.2    :DHE-DSS-ARIA256-GCM-SHA384 TLSv1.2    :DHE-RSA-ARIA256-GCM-SHA384
TLSv1.2    :ADH-AES256-GCM-SHA384     TLSv1.2    :ECDHE-ECDSA-AES128-GCM-SHA256
TLSv1.2    :ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2    :DHE-DSS-AES128-GCM-SHA256
TLSv1.2    :DHE-RSA-AES128-GCM-SHA256 TLSv1.2    :ECDHE-ECDSA-AES128-CCM
TLSv1.2    :DHE-RSA-AES128-CCM        TLSv1.2    :ECDHE-ECDSA-ARIA128-GCM-SHA256
TLSv1.2    :ECDHE-ARIA128-GCM-SHA256  TLSv1.2    :DHE-DSS-ARIA128-GCM-SHA256
TLSv1.2    :DHE-RSA-ARIA128-GCM-SHA256 TLSv1.2    :ADH-AES128-GCM-SHA256
TLSv1.2    :ECDHE-ECDSA-AES256-CCM8   TLSv1.2    :ECDHE-ECDSA-AES128-CCM8
TLSv1.2    :DHE-RSA-AES256-CCM8       TLSv1.2    :DHE-RSA-AES128-CCM8
TLSv1.2    :ECDHE-ECDSA-AES256-SHA384 TLSv1.2    :ECDHE-RSA-AES256-SHA384
TLSv1.2    :DHE-RSA-AES256-SHA256     TLSv1.2    :DHE-DSS-AES256-SHA256
TLSv1.2    :ECDHE-ECDSA-CAMELLIA256-SHA384 TLSv1.2    :ECDHE-RSA-CAMELLIA256-SHA384
TLSv1.2    :DHE-RSA-CAMELLIA256-SHA256 TLSv1.2    :DHE-DSS-CAMELLIA256-SHA256
TLSv1.2    :ADH-AES256-SHA256         TLSv1.2    :ADH-CAMELLIA256-SHA256
TLSv1.2    :ECDHE-ECDSA-AES128-SHA256 TLSv1.2    :ECDHE-RSA-AES128-SHA256
TLSv1.2    :DHE-RSA-AES128-SHA256     TLSv1.2    :DHE-DSS-AES128-SHA256
TLSv1.2    :ECDHE-ECDSA-CAMELLIA128-SHA256 TLSv1.2    :ECDHE-RSA-CAMELLIA128-SHA256
TLSv1.2    :DHE-RSA-CAMELLIA128-SHA256 TLSv1.2    :DHE-DSS-CAMELLIA128-SHA256
TLSv1.2    :ADH-AES128-SHA256         TLSv1.2    :ADH-CAMELLIA128-SHA256
TLSv1.0    :ECDHE-ECDSA-AES256-SHA    TLSv1.0    :ECDHE-RSA-AES256-SHA
SSLv3      :DHE-RSA-AES256-SHA        SSLv3      :DHE-DSS-AES256-SHA
```

Tasks - 4 : Deploy HTTPS into Apache

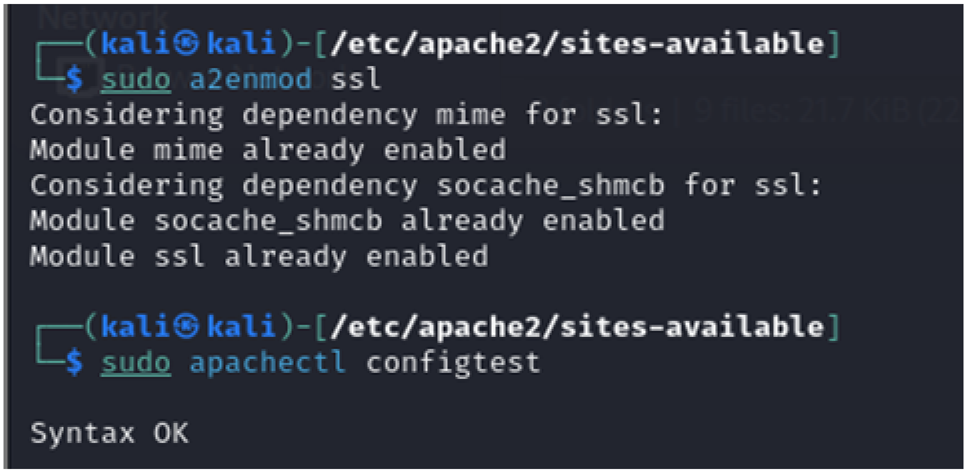
1.Writing contents in /etc/apache2/sites-available/example.com.conf file:



```
┌──(kali㉿kali)-[/etc/apache2/sites-available]
└─$ cd /etc/apache2/sites-available
```



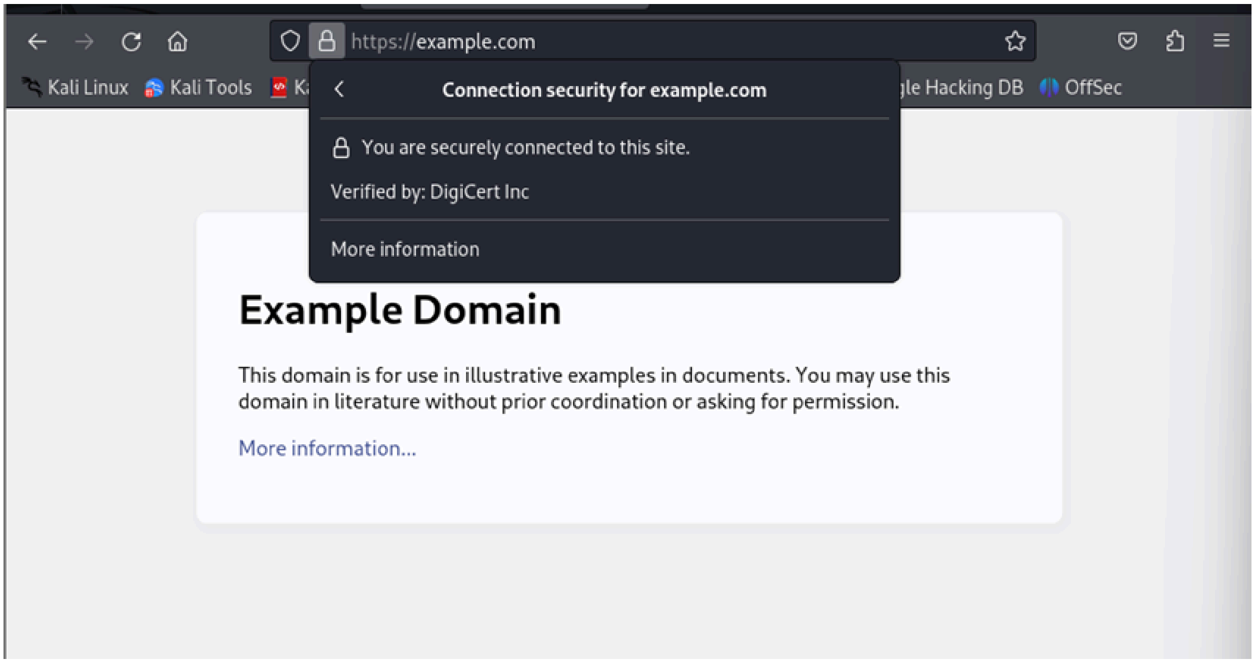
```
  GNU nano 7.2                                                    example.com.conf
<IfModule mod_ssl.c>
<VirtualHost *:4433>
 ServerAdmin admin@example.com
 ServerName example.com
 ServerAlias www.example.com
 DocumentRoot /var/www/example.com/html
 ErrorLog ${APACHE_LOG_DIR}/error.log
 CustomLog ${APACHE_LOG_DIR}/access.log combined

 SSLEngine on
 SSLCertificateFile /etc/apache2/ssl/example.com.crt
SSLCertificateKeyFile /etc/apache2/ssl/example.com.key

</VirtualHost>
</IfModule>
```



```
┌──(kali㉿kali)-[/etc/apache2/sites-available]
└─$ sudo a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled

┌──(kali㉿kali)-[/etc/apache2/sites-available]
└─$ sudo apachectl configtest

Syntax OK
```

2.Restarting the apache server:

3.Now, try to access the http://example.com. It'll view the webpage in HTTPS:



Connection security for example.com

You are securely connected to this site.

Verified by: DigiCert Inc

Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...