



Imam Mohammad Ibn Saud Islamic University
College of Computer and Information Sciences Computer
Science Department



Course Project

First Semester 1445 -2023

**PKI using SSL
Network security CS337**

**Student:
Mohammed Wahaq Alsahli 440015334**

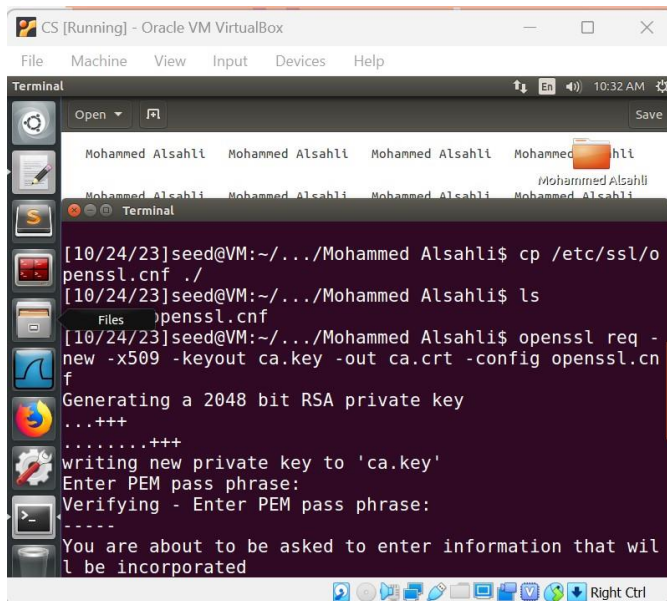
Task 1: Becoming a Certificate Authority (CA)

After creating the directories, wrote this command `cp /etc/ssl/openssl.cnf ./`

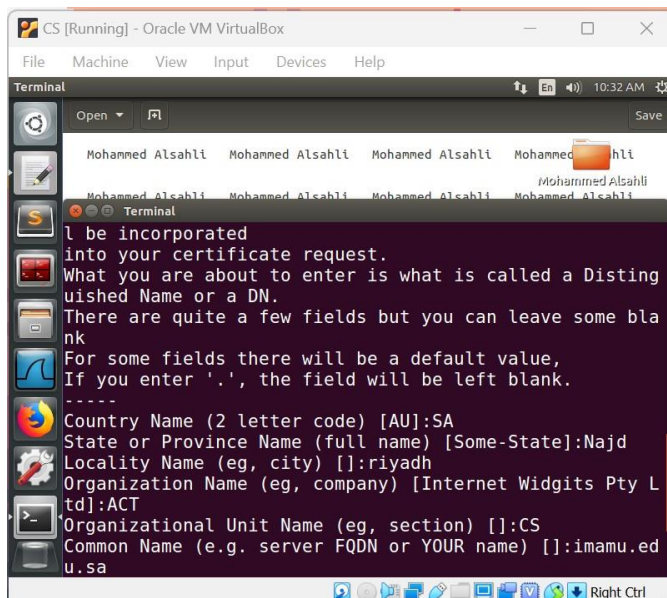
To copy the selected directory and place it where I am in the terminal

And wrote this command :

`openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf`
Wrote the password and the information needed.



```
CS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Open Save
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
[10/24/23]seed@VM:~/.../Mohammed Alsahli$ cp /etc/ssl/openssl.cnf ./
[10/24/23]seed@VM:~/.../Mohammed Alsahli$ ls
Files
openssl.cnf
[10/24/23]seed@VM:~/.../Mohammed Alsahli$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
Generating a 2048 bit RSA private key
...+++
.....+++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
```



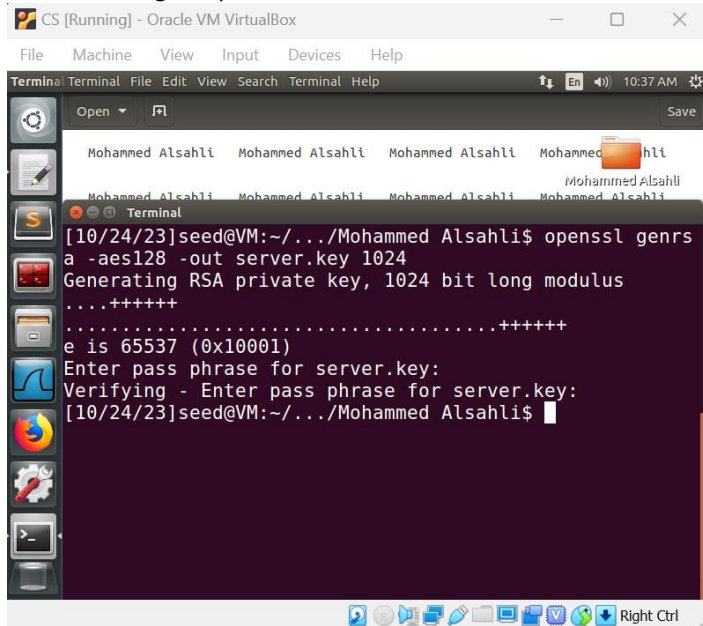
```
l be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:SA
State or Province Name (full name) [Some-State]:Najd
Locality Name (eg, city) []:riyadh
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ACT
Organizational Unit Name (eg, section) []:CS
Common Name (e.g. server FQDN or YOUR name) []:imamu.edu.sa
```

Task 2: Creating a Certificate for SEEDPKILab2018.com

Using this command to create a password.

`openssl genrsa -aes128 -out server.key 1024`

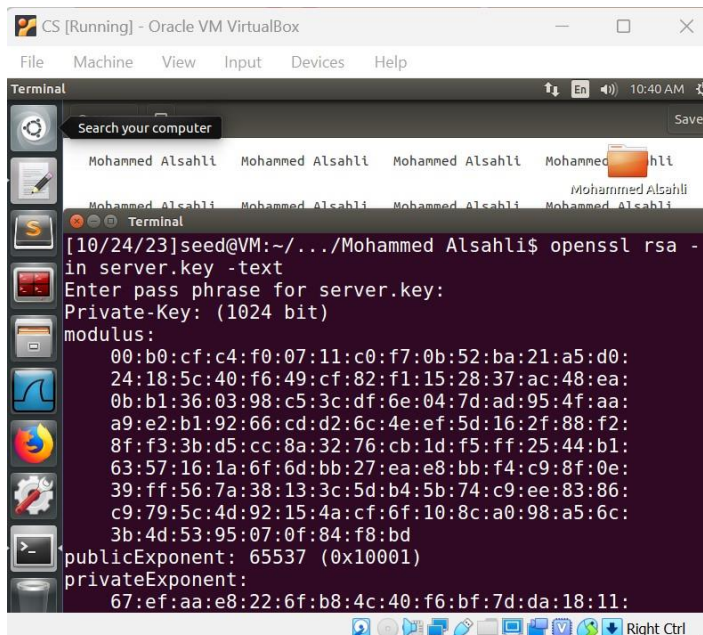
After entering the password it will create a certificate



```
CS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal Terminal File Edit View Search Terminal Help
Open Save
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
Terminal
[10/24/23]seed@VM:~/.../Mohammed Alsahli$ openssl genrsa
a -aes128 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
[10/24/23]seed@VM:~/.../Mohammed Alsahli$
```

This is the command to see the certificate

`openssl rsa -in server.key -text.`



```
CS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal Terminal File Edit View Search Terminal Help
Search your computer Save
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
Terminal
[10/24/23]seed@VM:~/.../Mohammed Alsahli$ openssl rsa -
in server.key -text
Enter pass phrase for server.key:
Private-Key: (1024 bit)
modulus:
00:b0:cf:c4:f0:07:11:c0:f7:0b:52:ba:21:a5:d0:
24:18:5c:40:f6:49:cf:82:f1:15:28:37:ac:48:ea:
0b:b1:36:03:98:c5:3c:df:6e:04:7d:ad:95:4f:aa:
a9:e2:b1:92:66:cd:d2:6c:4e:ef:5d:16:2f:88:f2:
8f:f3:3b:d5:cc:8a:32:76:cb:1d:f5:ff:25:44:b1:
63:57:16:1a:6f:6d:bb:27:ea:e8:bb:f4:c9:8f:0e:
39:ff:56:7a:38:13:3c:5d:b4:5b:74:c9:ee:83:86:
c9:79:5c:4d:92:15:4a:cf:6f:10:8c:a0:98:a5:6c:
3b:4d:53:95:07:0f:84:f8:bd
publicExponent: 65537 (0x10001)
privateExponent:
67:ef:aa:e8:22:6f:b8:4c:40:f6:bf:7d:da:18:11:
```

CS [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal 10:41 AM

Open Save

Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli

Terminal

```
40:5f:ed:1b:58:0e:a1:94:ed:c4:e7:4e:57:47:8e:
98:39:24:43:94:88:36:ac:ec:1e:7f:55:30:1e:ce:
aa:00:29:7c:19:5e:ea:26:0a:a8:0d:8e:26:40:e5:
46:88:e5:1d:b5:aa:43:b8:9e:bc:fd:ac:28:9c:1d:
e2:41:9d:a1:b1:4e:8c:e7:43:33:8c:1d:9c:43:d4:
b3:8f:ff:9f:2c:ba:c1:dd:81:e1:44:c8:70:ca:f0:
71:c6:3d:19:2e:c3:b2:c1
prime1:
00:e7:27:28:5d:a1:64:5b:79:87:16:4d:d8:75:0b:
4e:69:80:46:e9:29:19:8b:94:6f:91:37:0d:b6:35:
8b:ed:68:b8:e0:96:0d:02:c3:65:93:83:d4:2c:b0:
75:af:37:eb:2f:b7:a7:82:70:db:34:ab:1c:
f1:ce:f4:7f:51
prime2:
00:c3:d1:40:7a:e4:13:f7:8e:73:5a:97:22:ed:2f:
db:c0:08:3c:0b:69:fe:eb:a0:ee:20:8e:4b:5e:de:
59:a3:02:cd:62:14:9b:dc:14:4d:53:92:77:45:52:
```

System Settings

Right Ctrl

CS [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal 10:41 AM

Open Save

Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli

Terminal

```
85:98:16:3f:ad
exponent1:
5a:17:79:f5:1c:3d:28:25:f2:8f:af:e1:88:a4:d2:
77:ee:26:35:23:ee:af:e7:37:a0:aa:8b:6e:93:ea:
28:aa:e3:3b:ad:5f:fe:ce:b7:5d:4a:49:3c:ed:9f:
ca:47:84:16:50:54:f5:c8:94:df:75:a0:4e:7c:e6:
86:19:e7:31
exponent2:
00:a1:f1:94:9a:0d:b6:55:ae:01:c8:91:e5:d8:b3:
13:d2:24:fd:43:93:4d:b8:21:47:ce:b4:df:b0:7d:
c3:34:05:45:46:30:35:16:35:d4:1d:a1:ab:f2:31:
08:1f:30:59:7c:e4:76:2b:62:3e:48:4d:d6:b1:8d:
88:1e:d7:87:a1
coefficient:
23:03:f9:22:dd:80:3d:ca:c6:d3:38:40:f3:12:55:
45:85:39:1c:a2:40:04:c3:85:27:85:4b:c0:6d:73:
22:bd:7e:5f:1f:11:fe:c4:f0:4c:fb:d6:59:dc:4c:
```

System Settings

Right Ctrl

CS [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal 10:41 AM

Open Save

Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli

Terminal

```
b2:ac:26:3a:5d:6b:37:f8:64:51:19:54:8d:aa:7b:
ed:e6:dd:12
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCwz8TwBxHA9wtSuiGl0CQYXED2Sc+C8RUoN6xI6gu
xNg0YxTzf
bgR9rZVPqgnisZJmzdJsTu9dFi+I8o/z09XMijJ2yx31/yVEsWNXFhp
vbbsn6ui7
9MmPDjn/Vno4EzxdTf0ye6DhsL5XE2SFurPbxCMoJilbDtnU5UHD4T
4vQIDAQAB
AoGAZ++q6CJvuExA9r992hgRr9RDR8Q53NJVSo/3keErQF/tG1g0oZT
tx0d0V0e0
mDkkQ5SINqzsHn9VMB70qgApfBle6iYKqA20JKdLRojlHbWqQ7ievP2
sKJwd4kGd
obF0j0dDM4wdnEPUs4//nyy6wd2B4UTicMrwccY9GS7DssECQQDnJyh
doWRbeYcW
TdhlC05pgEbpKRmLlG+RNw22NYvtaLjglg0Cw2WTg9QssCjPVa836y+
```

Right Ctrl

CS [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal 10:42 AM

Open Save

Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli

Terminal

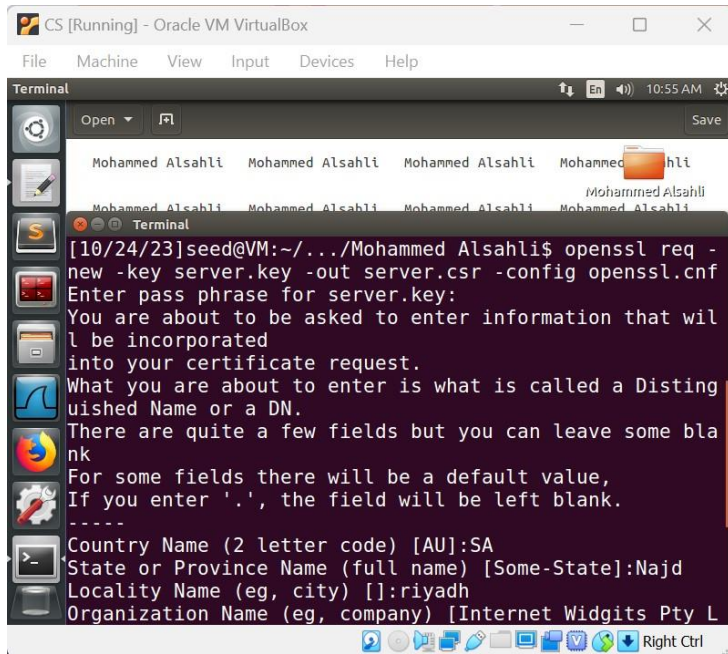
```
obF0j0dDM4wdnEPUs4//nyy6wd2B4UTicMrwccY9GS7DssECQQDnJyh
doWRbeYcW
TdhlC05pgEbpKRmLlG+RNw22NYvtaLjglg0Cw2WTg9QssCjPVa836y+
3p4Jw2zSr
HPH09H9RAkEAw9FAeuQT945zWpci7S/bwAg8C2n+66DuII5Lxt5ZowL
NYhSb3BRN
U5J3RVKvyAqLpNm8vX+mHoNDhUqFmBY/rQJAWhd59Rw9KCXyj6/hlKT
Sd+4mNSPu
r+c3oKqLbpPqKKrj061f/s63XUpJP02fykeEF1BU9ciU33WgTnmhhn
nMQJBAXHx
lJoNtlWuAcir5dizE9Ik/U0TTbghR86037B9wzQFRUYwNRY11B2hq/I
xCB8wWXzk
ditiPkhN1rGNiB7Xh6ECQCMD+SLdgD3KxtM4QPMsVUWF0RyiQATDhSe
FS8BtcyK9
f18fEf7E8Ez71lncTLKsJjpdazf4ZFEZVI2qe+3m3RI=
-----END RSA PRIVATE KEY-----
[10/24/23]seed@VM:~/.../Mohammed Alsahli$
```

Right Ctrl

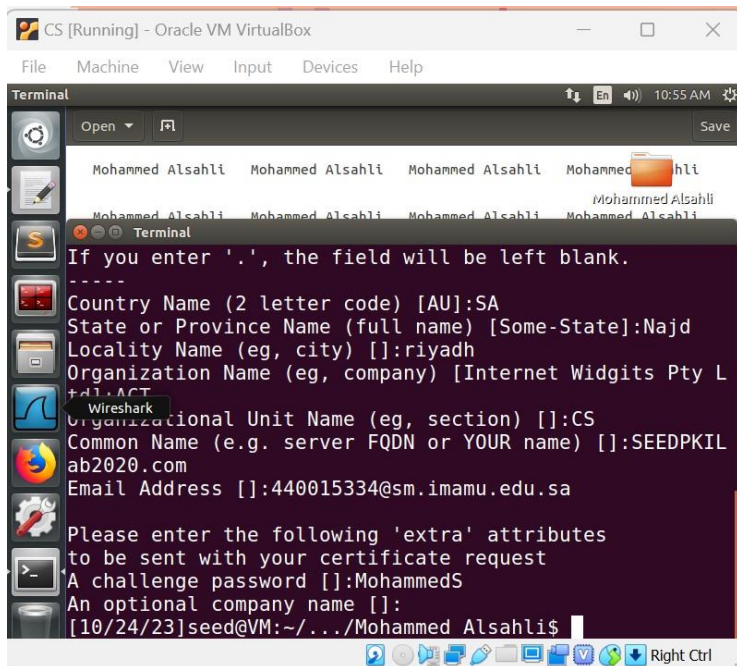

```
openssl req -new -key server.key -out server.csr -config openssl.cnf
```

By this command suppose that the client is asking for certificate and I authorize it

After entering the password you have to fill in the blanks

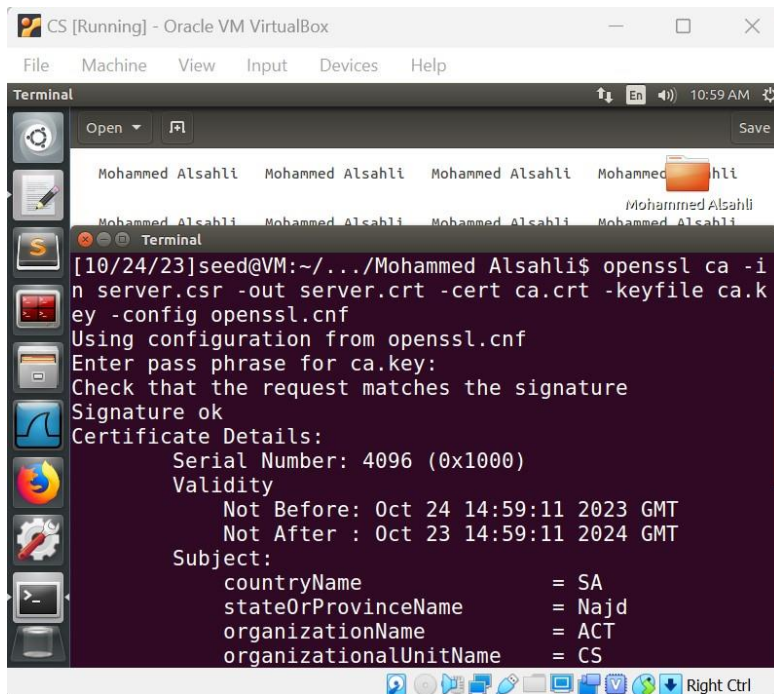


```
CS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
[10/24/23]seed@VM:~/../Mohammed Alsahli$ openssl req -
new -key server.key -out server.csr -config openssl.cnf
Enter pass phrase for server.key:
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 Disting
uished Name or a DN.
There are quite a few fields but you can leave some bla
nk
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:SA
State or Province Name (full name) [Some-State]:Najd
Locality Name (eg, city) []:riyadh
Organization Name (eg, company) [Internet Widgits Pty L
```

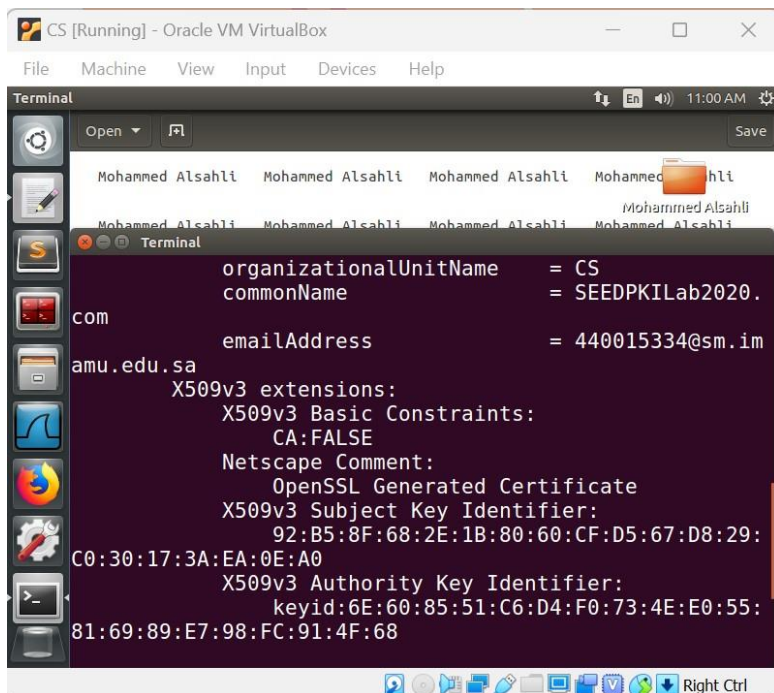


```
CS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:SA
State or Province Name (full name) [Some-State]:Najd
Locality Name (eg, city) []:riyadh
Organization Name (eg, company) [Internet Widgits Pty L
Additional Name (eg, section) []:CS
Common Name (e.g. server FQDN or YOUR name) []:SEEDPKIL
ab2020.com
Email Address []:440015334@sm.imamu.edu.sa
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:MohammedS
An optional company name []:
[10/24/23]seed@VM:~/../Mohammed Alsahli$
```

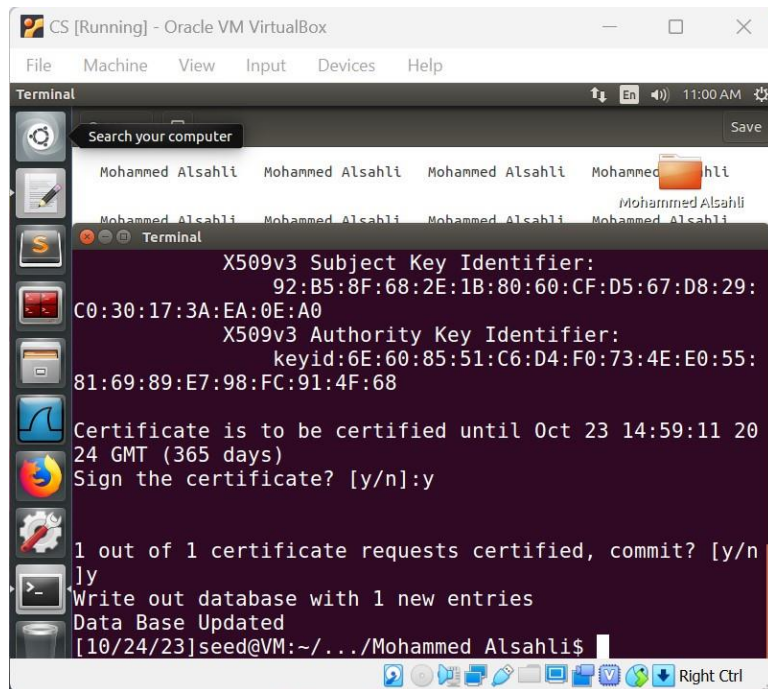
openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
We put this command to sign the certificate And answer the request to certify



```
CS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
[10/24/23]seed@VM:~/.../Mohammed Alsahli$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 4096 (0x1000)
  Validity
    Not Before: Oct 24 14:59:11 2023 GMT
    Not After : Oct 23 14:59:11 2024 GMT
  Subject:
    countryName           = SA
    stateOrProvinceName   = Najd
    organizationName      = ACT
    organizationalUnitName = CS
```



```
CS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
    organizationalUnitName = CS
    commonName             = SEEDPKILab2020.
com
    emailAddress           = 440015334@sm.im
amu.edu.sa
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
  Netscape Comment:
    OpenSSL Generated Certificate
  X509v3 Subject Key Identifier:
    92:B5:8F:68:2E:1B:80:60:CF:D5:67:D8:29:
C0:30:17:3A:EA:0E:A0
  X509v3 Authority Key Identifier:
    keyid:6E:60:85:51:C6:D4:F0:73:4E:E0:55:
81:69:89:E7:98:FC:91:4F:68
```



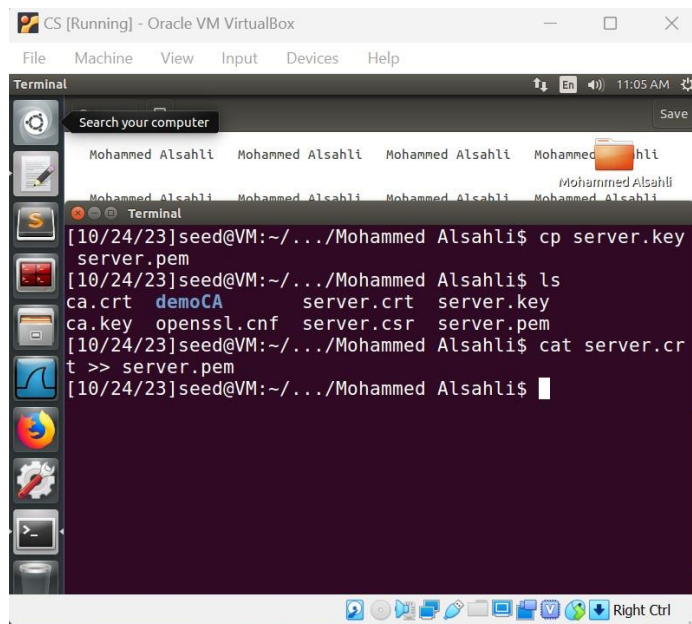
```
CS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Search your computer
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
Terminal
X509v3 Subject Key Identifier:
    92:B5:8F:68:2E:1B:80:60:CF:D5:67:D8:29:
C0:30:17:3A:EA:0E:A0
X509v3 Authority Key Identifier:
    keyid:6E:60:85:51:C6:D4:F0:73:4E:E0:55:
81:69:89:E7:98:FC:91:4F:68
Certificate is to be certified until Oct 23 14:59:11 20
24 GMT (365 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]
y
Write out database with 1 new entries
Data Base Updated
[10/24/23]seed@VM:~/../Mohammed Alsahli$
```

cp server.key server.pem

By this command we created server.pem Directory

cat server.crt >> server.pem

The content of server.crt will be added to server.pem

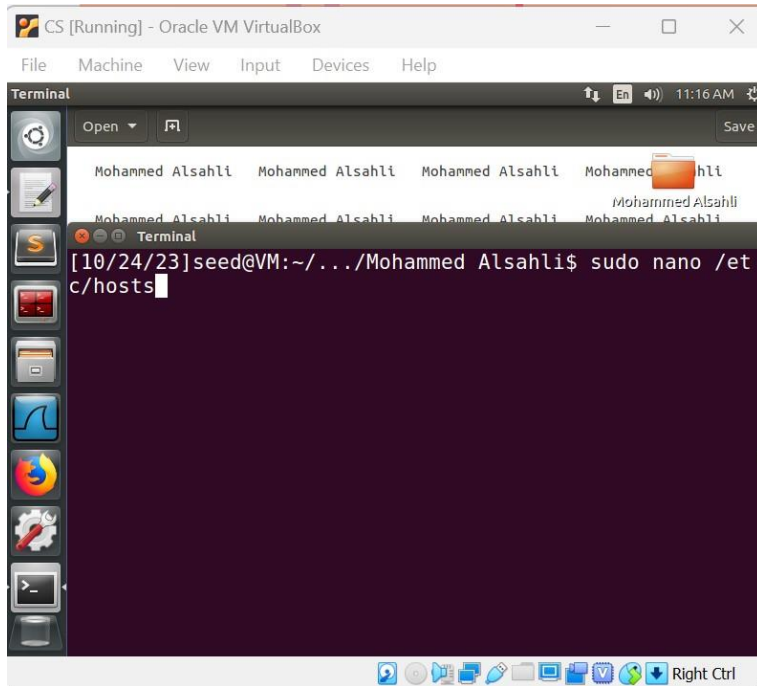


```
CS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Search your computer
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
Terminal
[10/24/23]seed@VM:~/../Mohammed Alsahli$ cp server.key
server.pem
[10/24/23]seed@VM:~/../Mohammed Alsahli$ ls
ca.crt demoCA server.crt server.key
ca.key openssl.cnf server.csr server.pem
[10/24/23]seed@VM:~/../Mohammed Alsahli$ cat server.cr
t >> server.pem
[10/24/23]seed@VM:~/../Mohammed Alsahli$
```


Task 3: Deploying Certificate in an HTTPS Web Server

Step 1: Configuring DNS. we add

127.0.0.1 SEEDPKILab2018.com to our localhost



CS [Running] - Oracle VM VirtualBox

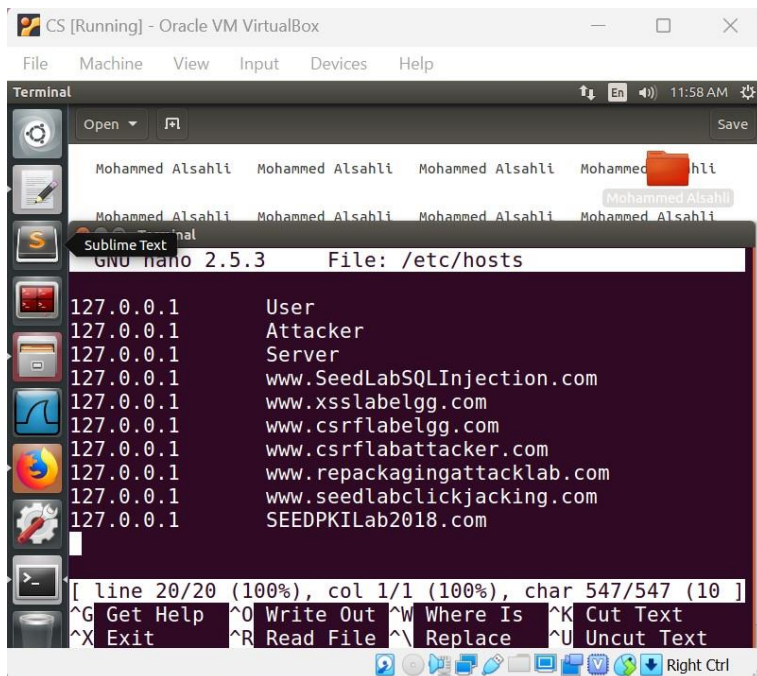
File Machine View Input Devices Help

Terminal

Open Save

Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli

[10/24/23]seed@VM:~/../Mohammed Alsahli\$ sudo nano /etc/hosts



CS [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

Open Save

Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli

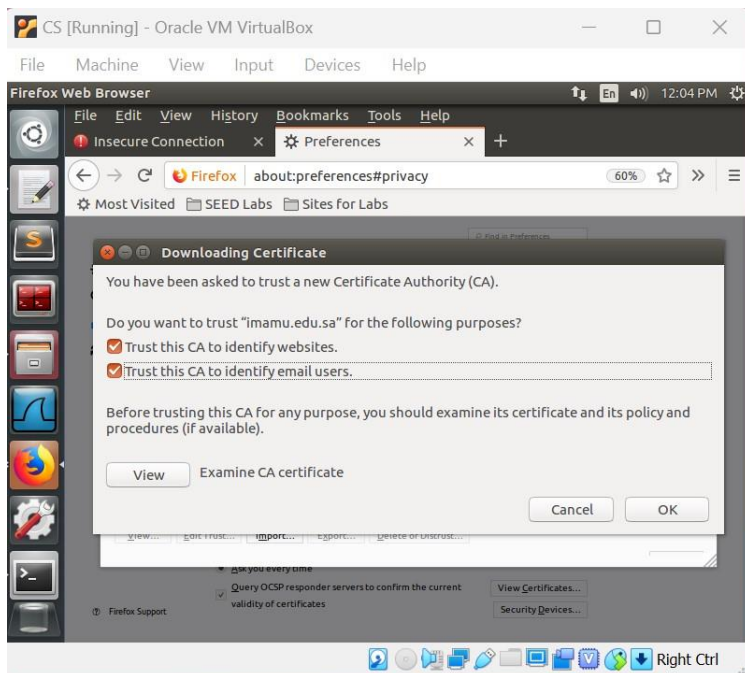
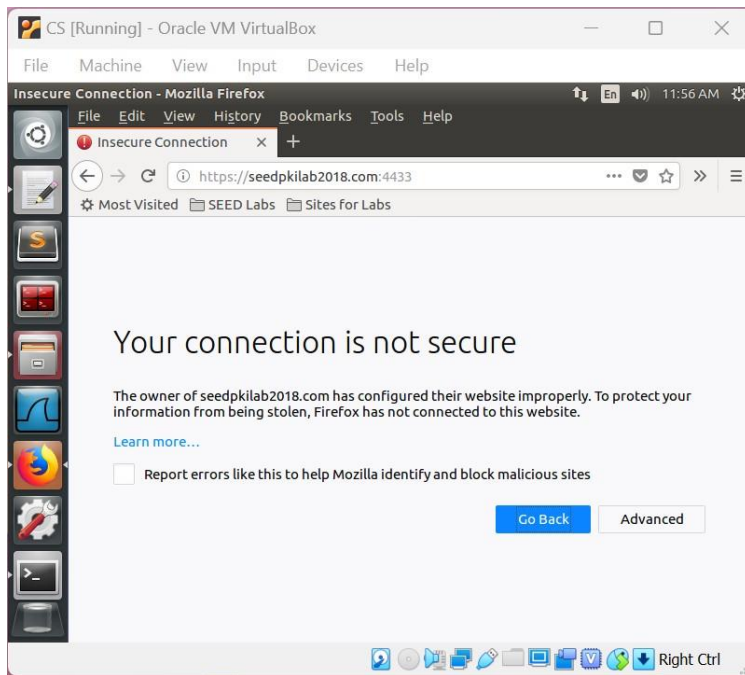
Sublime Text GNU nano 2.5.3 File: /etc/hosts

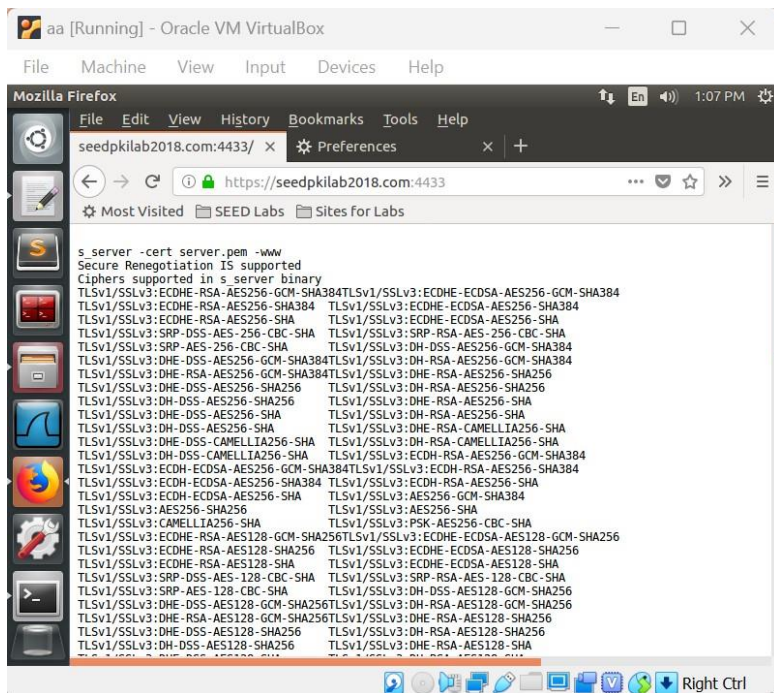
```
127.0.0.1 User
127.0.0.1 Attacker
127.0.0.1 Server
127.0.0.1 www.SeedLabSQLInjection.com
127.0.0.1 www.xsslabelgg.com
127.0.0.1 www.csrflabelgg.com
127.0.0.1 www.csrfLabAttacker.com
127.0.0.1 www.repackagingattacklab.com
127.0.0.1 www.seedlabclickjacking.com
127.0.0.1 SEEDPKILab2018.com
```

[line 20/20 (100%), col 1/1 (100%), char 547/547 (100%)]

^G Get Help ^O Write Out ^W Where Is ^K Cut Text
^X Exit ^R Read File ^\ Replace ^U Uncut Text

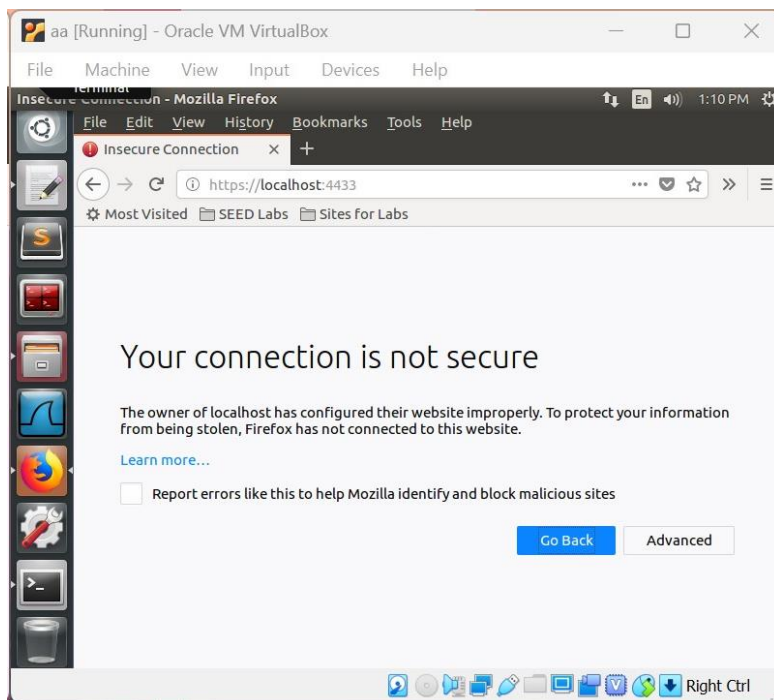
This message appeared because the the certificate is not verified





When we changed it from seedpkilab2018.com to localhost

This is what happened:

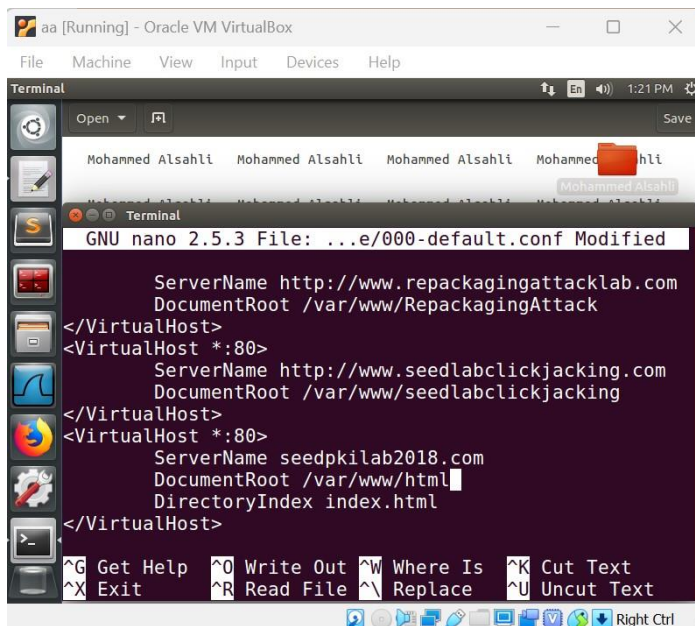


Task 4: Deploying Certificate in an Apache-Based HTTPS Website

we run this command `sudo nano /etc/apache2/sites-available/000-default.conf`

And insert this code:

```
<VirtualHost *:80>
    ServerName seedpkilab2018.com
    DocumentRoot /var/www/html
    DirectoryIndex index.html
</VirtualHost>
```



The screenshot shows a terminal window titled "aa [Running] - Oracle VM VirtualBox". The terminal is running the nano text editor, editing the file `...e/000-default.conf`. The current content of the file is as follows:

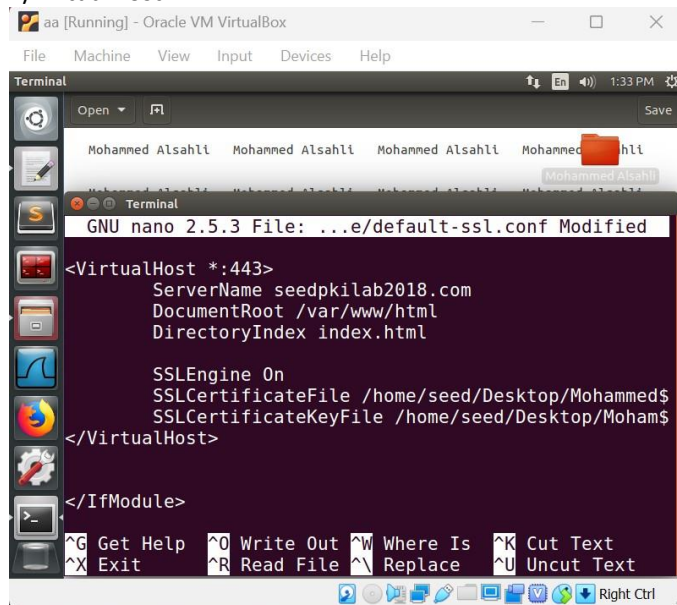
```
ServerName http://www.repackagingattacklab.com
DocumentRoot /var/www/RepackagingAttack
</VirtualHost>
<VirtualHost *:80>
    ServerName http://www.seedlabclickjacking.com
    DocumentRoot /var/www/seedlabclickjacking
</VirtualHost>
<VirtualHost *:80>
    ServerName seedpkilab2018.com
    DocumentRoot /var/www/html
    DirectoryIndex index.html
</VirtualHost>
```

The terminal window also displays a sidebar with icons for various applications and a bottom status bar with keyboard shortcuts like `^G Get Help`, `^X Exit`, `^O Write Out`, `^R Read File`, `^W Where Is`, `^L Replace`, `^K Cut Text`, and `^U Uncut Text`.

we run this command too `sudo nano /etc/apache2/sites-available/default-ssl.conf`

And insert this code:

```
<VirtualHost *:443>
    ServerName seedpkilab2018.com
    DocumentRoot /var/www/html
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /home/seed/Desktop/MohammedAlsahli/server.pem
    SSLCertificateKeyFile /home/seed/Desktop/MohammedAlsahli/server.pem
</VirtualHost>
```



And then we have to run four of these commands:

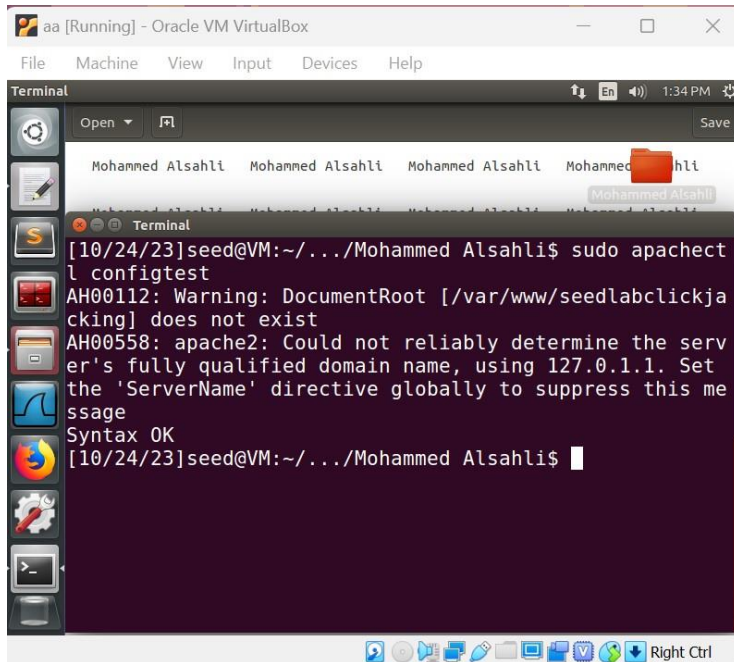
1-`sudo apachectl configtest`

2-`sudo a2enmod ssl`

3-`sudo a2ensite default-ssl`

4-`sudo service apache2 restart`

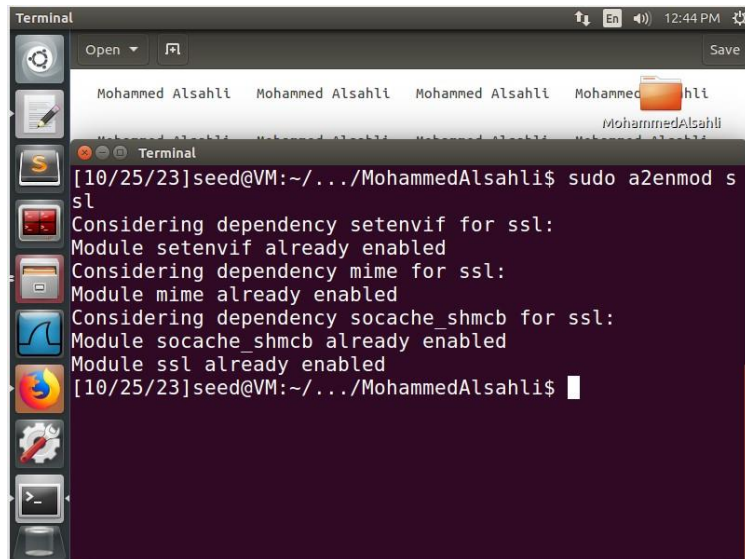
1-sudo apachectl configtest



The screenshot shows a terminal window titled "aa [Running] - Oracle VM VirtualBox". The terminal output is as follows:

```
[10/24/23]seed@VM:~/../Mohammed Alsahli$ sudo apachectl configtest
AH00112: Warning: DocumentRoot [/var/www/seedlabclickjacking] does not exist
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
[10/24/23]seed@VM:~/../Mohammed Alsahli$
```

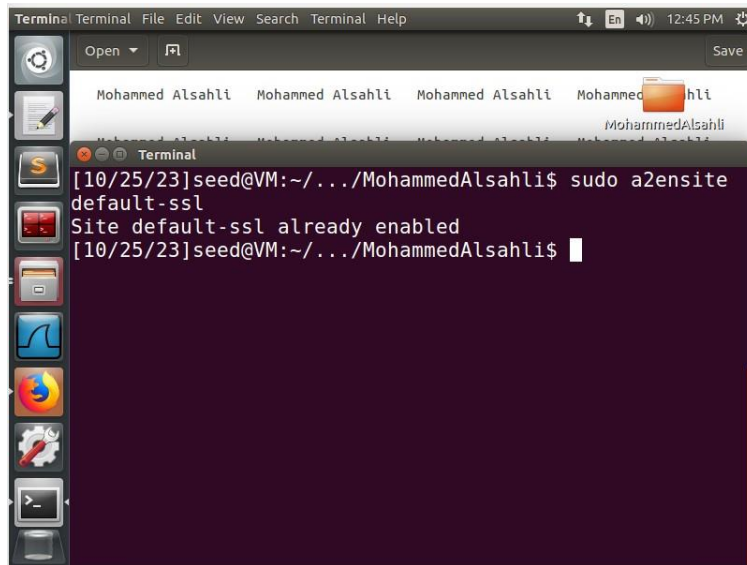
2-sudo a2enmod ssl



The screenshot shows a terminal window titled "Terminal". The terminal output is as follows:

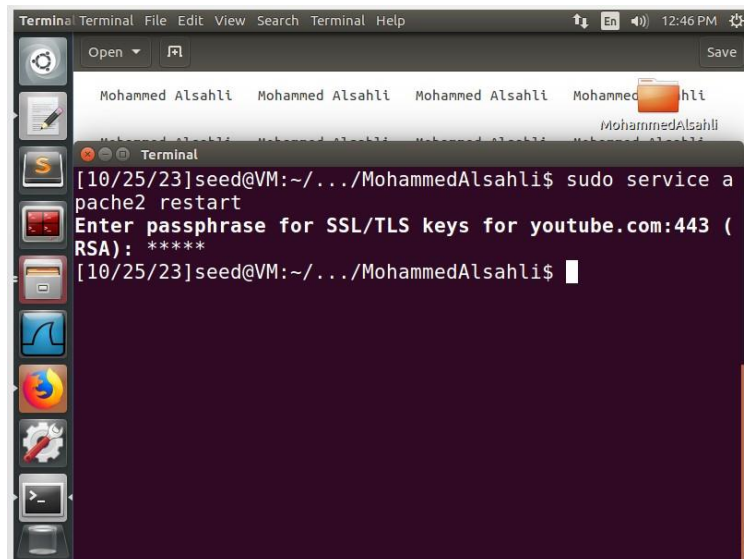
```
[10/25/23]seed@VM:~/../MohammedAlsahli$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
[10/25/23]seed@VM:~/../MohammedAlsahli$
```

3-sudo a2ensite default-ssl



```
Terminal Terminal File Edit View Search Terminal Help 12:45 PM
Open Save
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
Mohammed Alsahli
Terminal
[10/25/23]seed@VM:~/../MohammedAlsahli$ sudo a2ensite default-ssl
Site default-ssl already enabled
[10/25/23]seed@VM:~/../MohammedAlsahli$
```

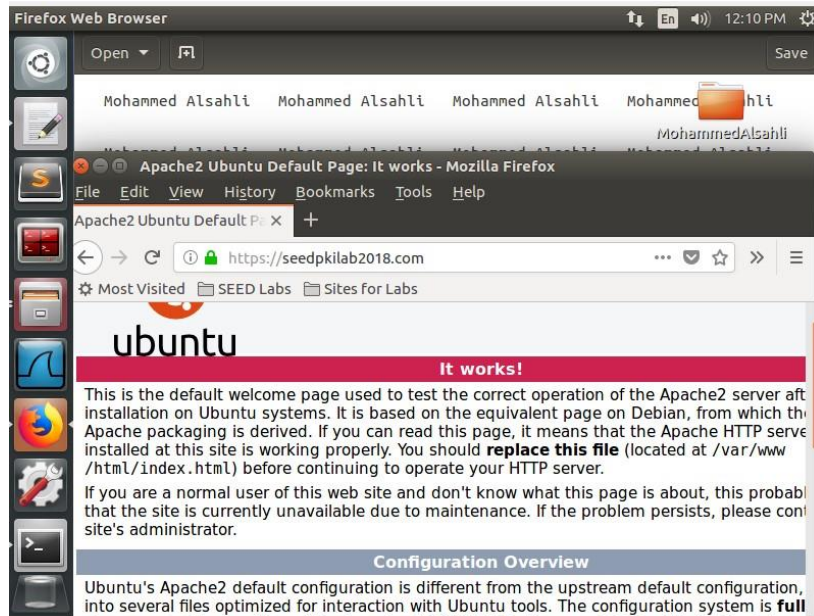
4-sudo service apache2 restart



```
Terminal Terminal File Edit View Search Terminal Help 12:46 PM
Open Save
Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli Mohammed Alsahli
Mohammed Alsahli
Terminal
[10/25/23]seed@VM:~/../MohammedAlsahli$ sudo service apache2 restart
Enter passphrase for SSL/TLS keys for youtube.com:443 (RSA): *****
[10/25/23]seed@VM:~/../MohammedAlsahli$
```

And now when you go to <https://seedpkilab2018.com>

You will see this

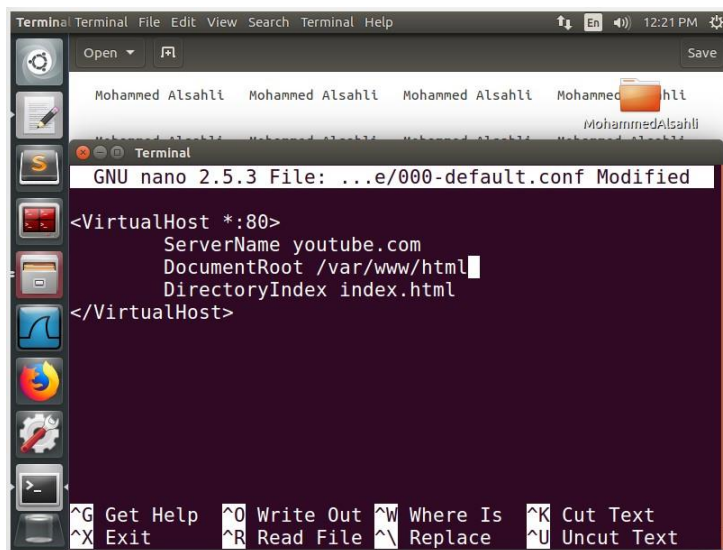


Task 5: Launching a Man-In-The-Middle Attack

we run this command `sudo nano /etc/apache2/sites-available/000-default.conf`

And insert this code:

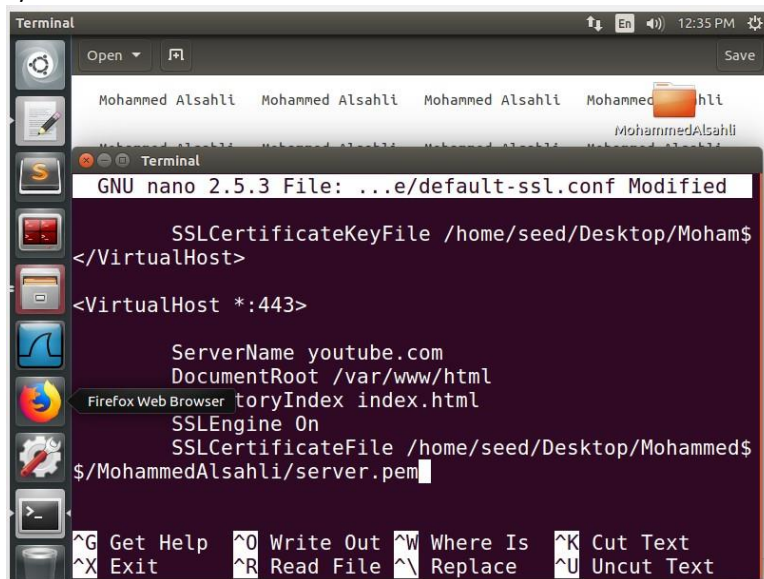
```
<VirtualHost *:80>
    ServerName youtube.com
    DocumentRoot /var/www/html
    DirectoryIndex index.html
</VirtualHost>
```



we run this command too `sudo nano /etc/apache2/sites-available/default-ssl.conf`

And insert this code:

```
<VirtualHost *:443>
    ServerName youtube.com
    DocumentRoot /var/www/html
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /home/seed/Desktop/MohammedAlsahli/server.pem
    SSLCertificateKeyFile /home/seed/Desktop/MohammedAlsahli/server.pem
</VirtualHost>
```



The screenshot shows a terminal window with the nano 2.5.3 text editor open. The file being edited is `...e/default-ssl.conf`. The cursor is at the end of the `SSLCertificateKeyFile` line. The configuration code being entered is as follows:

```
SSLCertificateKeyFile /home/seed/Desktop/Moham$
</VirtualHost>
<VirtualHost *:443>
    ServerName youtube.com
    DocumentRoot /var/www/html
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /home/seed/Desktop/Mohammed$
    SSLCertificateKeyFile /home/seed/Desktop/Mohammed$
$ /MohammedAlsahli/server.pem
```

At the bottom of the terminal, there is a legend for nano editor shortcuts:

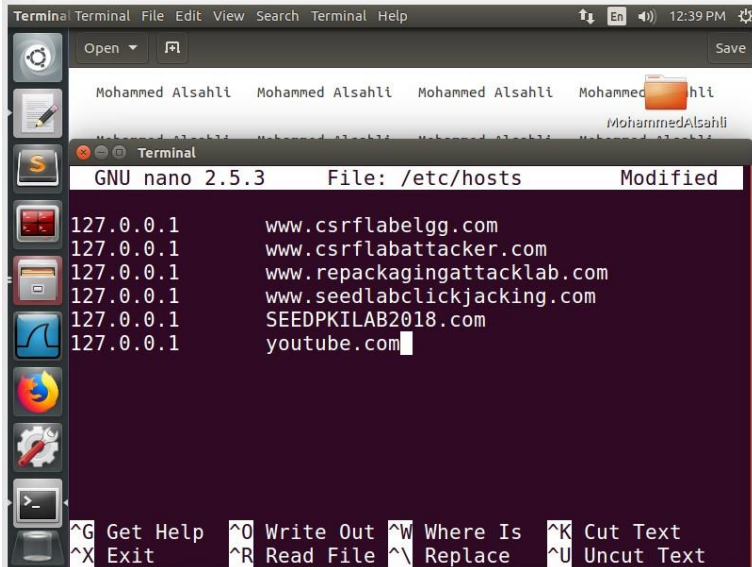
<code>^G</code> Get Help	<code>^O</code> Write Out	<code>^W</code> Where Is	<code>^K</code> Cut Text
<code>^X</code> Exit	<code>^R</code> Read File	<code>^_</code> Replace	<code>^U</code> Uncut Text

And now we add it to the host file

Sudo nano /etc/hosts

And add

127.0.0.1 youtube.com



```
GNU nano 2.5.3 File: /etc/hosts Modified
127.0.0.1 www.csrflabelgg.com
127.0.0.1 www.csrfbattacker.com
127.0.0.1 www.repackagingattacklab.com
127.0.0.1 www.seedlabclickjacking.com
127.0.0.1 SEEDPKILAB2018.com
127.0.0.1 youtube.com
```

And when I ran these commands

1-sudo apachectl configtest

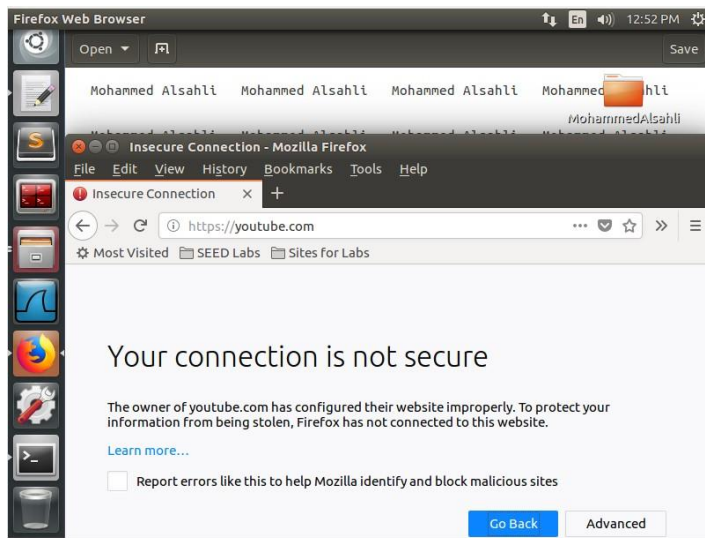
2-sudo a2enmod ssl

3-sudo a2ensite default-ssl

4-sudo service apache2 restart

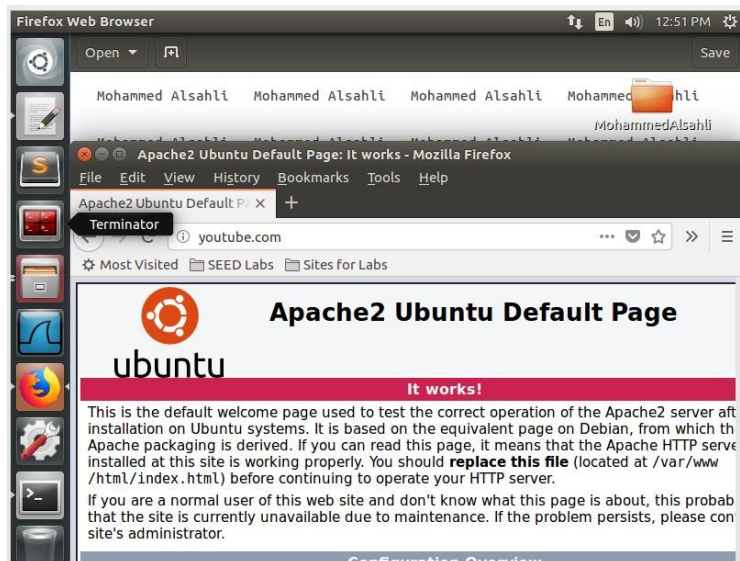
I got the same result as before meaning there is no mistake.

When opening the browser and searching <https://youtube.com> we will see this



Because there is no certificate for it

When opening the browser and searching youtube.com



Task 6: Launching a Man-In-The-Middle Attack with a Compromised CA

```
openssl req -new -key server.key -out server.csr -config openssl.cnf
```

the attacker will request a new certificate to put the YouTube link in it

Then he will authenticate the certificate because he has the password

Where are you going to repeat the process that happened in task 2

after creating the certificate we are on these commands

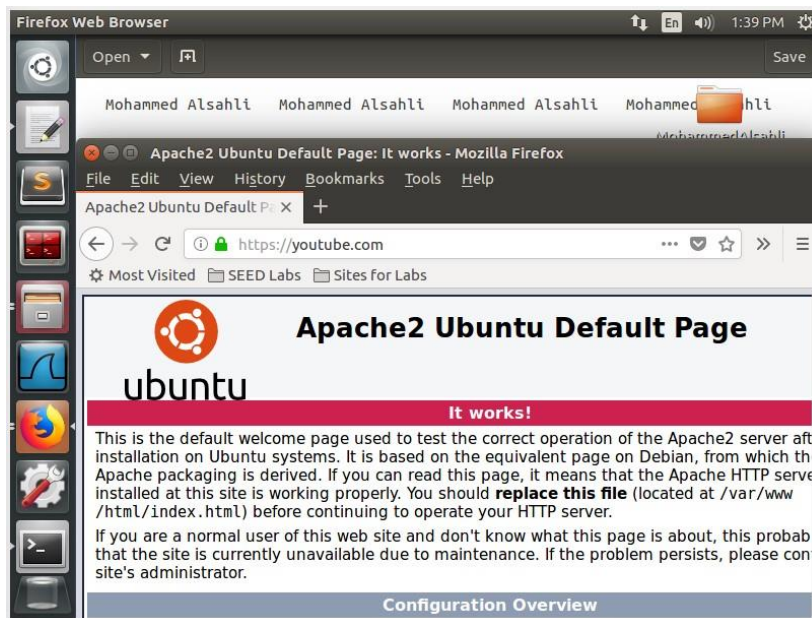
```
1-sudo apachectl configtest
```

```
2-sudo a2enmod ssl
```

```
3-sudo a2ensite default-ssl
```

```
4-sudo service apache2 restart
```

Then we go to the browser to see



References:

https://seedsecuritylabs.org/Labs_16.04/PDF/Crypto_PKI.pdf

https://www.youtube.com/watch?v=iloLMYNS4J0&t=1653s&ab_channel=ElhamAli

https://www.youtube.com/watch?v=6878gk8HK2M&t=1458s&ab_channel=%D9%85%D8%AD%D8%A7%D8%B6%D8%B1%D8%A7%D8%AA%D8%A7%D9%84%D9%83%D9%84%D9%8A%D8%A9%D8%A7%D9%84%D8%AA%D9%82%D9%86%D9%8A%D8%A9%D8%A8%D8%A7%D9%84%D8%A3%D8%AD%D8%B3%D8%A7%D8%A1

<https://hackmd.io/@ephemeral-instance/B1yPH7Qf>