

# CS-767 Foundations Network Security

# Public Key Infrastructure Lab

*Chakradhar Reddy Donuri*

E949F496

## Task 1: Becoming a Certificate Authority (CA)

CRS31\_BOX [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

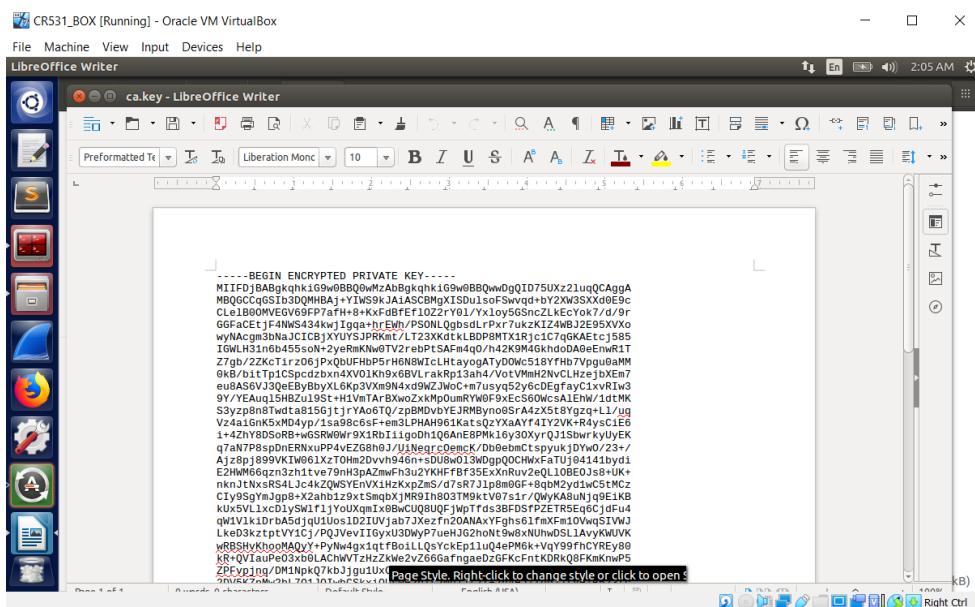
Terminator

/bin/bash

/bin/bash 86x25

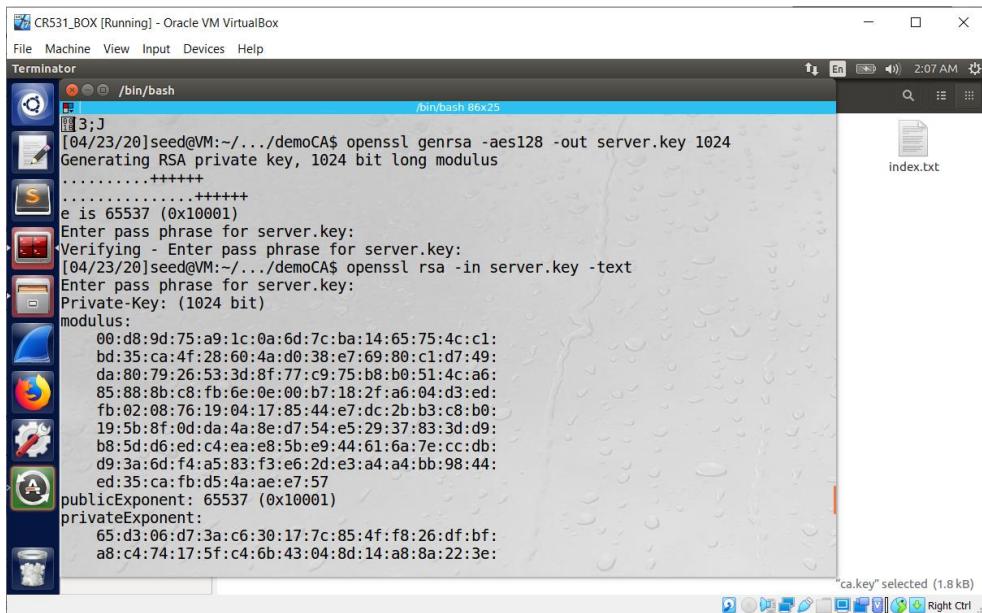
```
[04/23/20]seed@VM:~/.../demoCA$ openssl req -new -x509 -keyout ca.key -out ca.crt -con  
fig openssl.cnf  
Generating a 2048 bit RSA private key  
.....++  
.....++  
writing new private key to 'ca.key'  
Enter PEM pass phrase:  
Verifying - Enter PEM pass phrase:  
-----  
You are about to be asked to enter information that will be incorporated  
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]:US  
State or Province Name (full name) [Some-State]:Kansas  
Locality Name (eg, city) []:Wichita  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:WSU  
Organizational Unit Name (eg, section) []:MS  
Common Name (e.g. server FQDN or YOUR name) []:chakri  
Email Address []:chakradharreddy985@gmail.com  
[04/23/20]seed@VM:~/.../demoCA$
```

index.txt



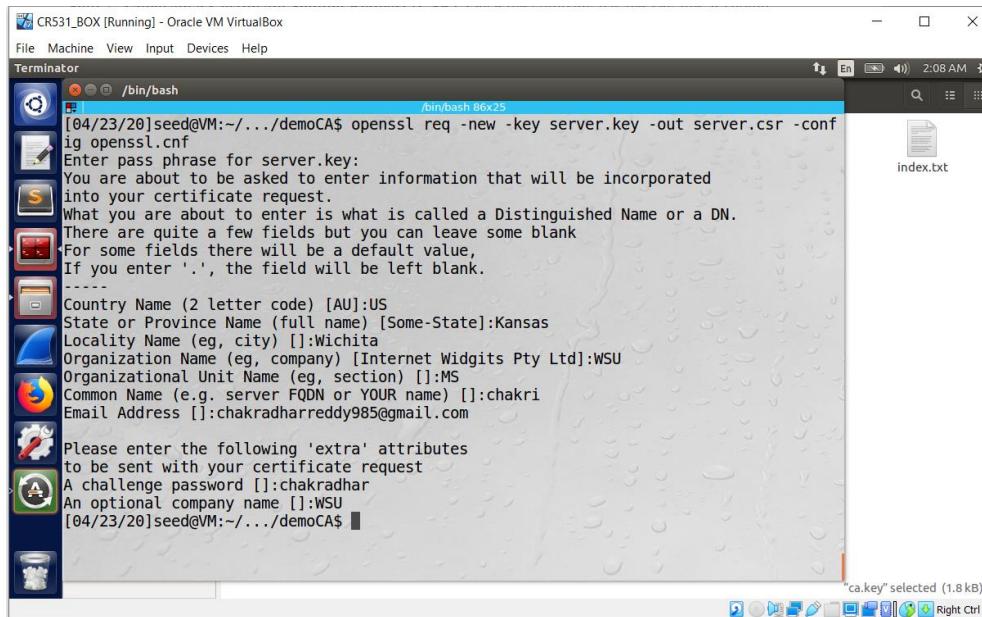
## Task 2: Creating a Certificate for SEEDPKILab2018.com

### Step-1



```
[04/23/20]seed@VM:~/.../demoCA$ openssl genrsa -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:
[04/23/20]seed@VM:~/.../demoCA$ openssl rsa -in server.key -text
Enter pass phrase for server.key:
Private-Key: (1024 bit)
modulus:
 00:d8:9d:75:a9:1c:0a:6d:7c:ba:14:65:75:4c:c1:
  bd:35:ca:4f:28:60:4a:d0:38:e7:69:80:c1:d7:49:
  da:80:79:26:53:3d:8f:77:c9:75:b8:b0:51:4c:a6:
  85:88:8b:c8:fb:6e:0e:00:b7:18:2f:a6:04:d3:ed:
  fb:02:08:76:19:04:17:85:44:e7:dc:2b:b3:c8:b0:
  19:5b:8f:0d:da:4a:8e:d7:54:e5:29:37:83:3d:d9:
  b8:5d:d6:ed:c4:ea:e8:5b:e9:44:61:6a:7e:cc:db:
  d9:3a:6d:f4:a5:83:f3:e6:2d:e3:a4:a4:bb:98:44:
  ed:35:ca:fb:d5:4a:ae:e7:57
publicExponent: 65537 (0x10001)
privateExponent:
  65:d3:06:d7:3a:c6:30:17:7c:85:4f:f8:26:df:bf:
  a8:c4:74:17:5f:c4:6b:43:04:8d:14:a8:8a:22:3e:
```

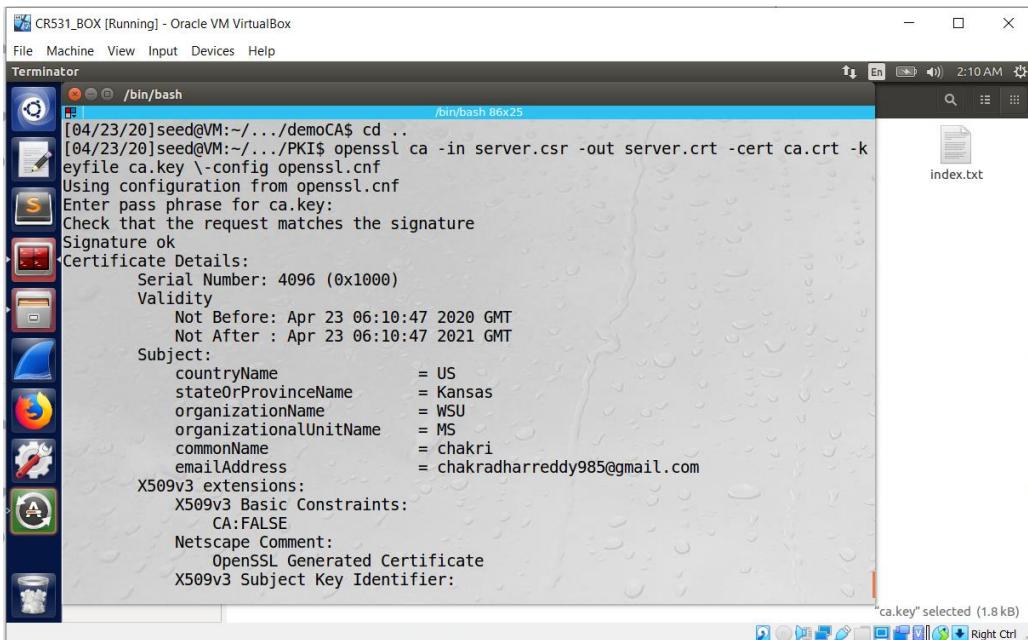
### Step-2



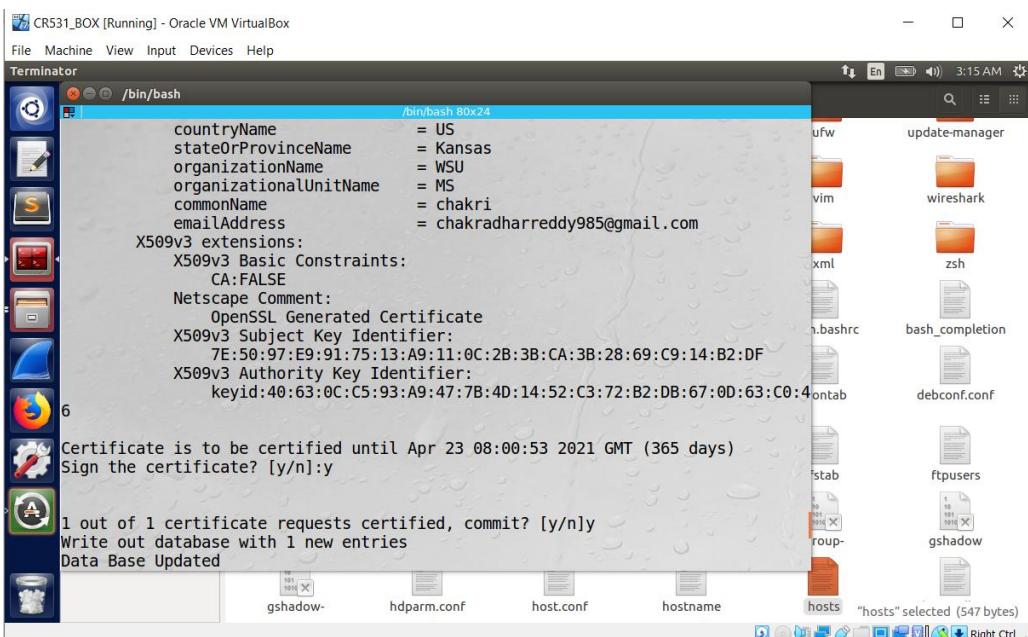
```
[04/23/20]seed@VM:~/.../demoCA$ openssl req -new -key server.key -out server.csr -config openssl.cnf
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished 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]:US
State or Province Name (full name) [Some-State]:Kansas
Locality Name (eg, city) []:Wichita
Organization Name (eg, company) [Internet Widgits Pty Ltd]:WSU
Organizational Unit Name (eg, section) []:MS
Common Name (e.g. server FQDN or YOUR name) []:chakri
Email Address []:chakradharreddy985@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:chakradhar
An optional company name []:WSU
[04/23/20]seed@VM:~/.../demoCA$
```

### Step-3



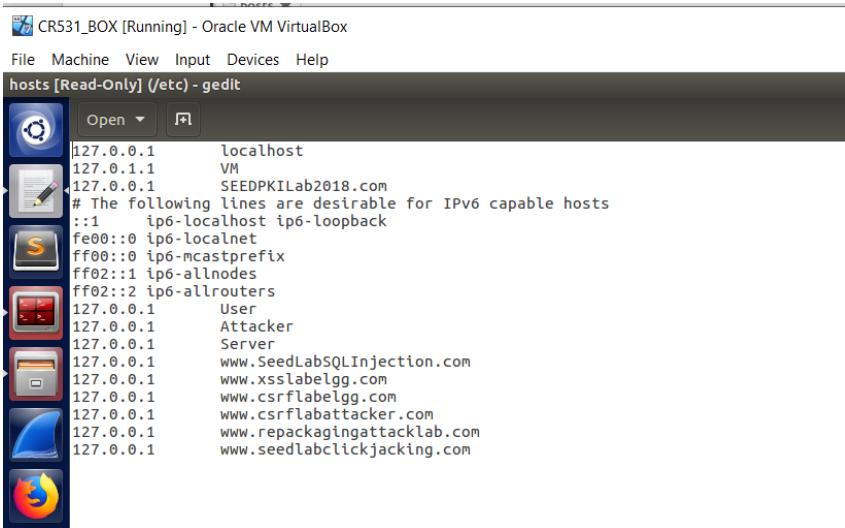
```
[04/23/20]seed@VM:~/.../demoCA$ cd ..
[04/23/20]seed@VM:~/.../PKI$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 4096 (0x1000)
    Validity
        Not Before: Apr 23 06:10:47 2020 GMT
        Not After : Apr 23 06:10:47 2021 GMT
    Subject:
        countryName          = US
        stateOrProvinceName = Kansas
        organizationName   = WSU
        organizationalUnitName = MS
        commonName           = chakri
        emailAddress         = chakradharreddy985@gmail.com
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
```



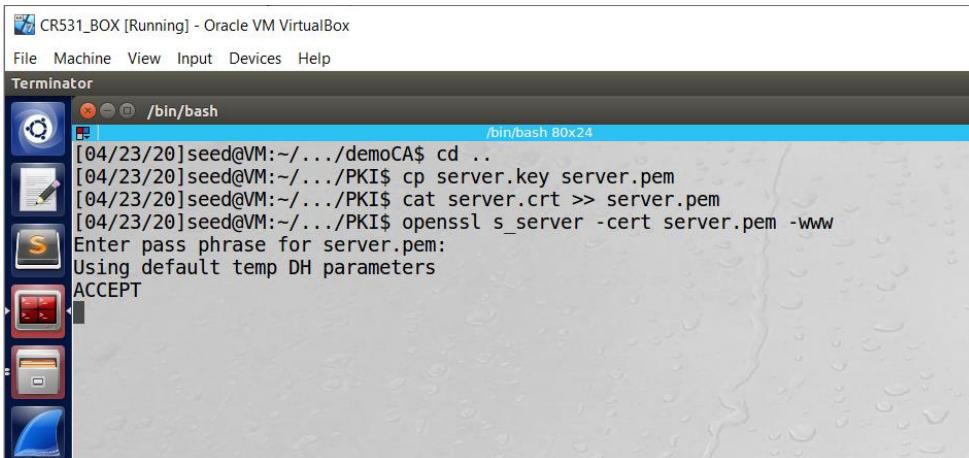
```
countryName          = US
stateOrProvinceName = Kansas
organizationName   = WSU
organizationalUnitName = MS
commonName           = chakri
emailAddress         = chakradharreddy985@gmail.com
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FALSE
    Netscape Comment:
        OpenSSL Generated Certificate
    X509v3 Subject Key Identifier:
        7E:50:97:E9:91:75:13:A9:11:0C:2B:3B:CA:3B:28:69:C9:14:B2:DF
    X509v3 Authority Key Identifier:
        keyid:40:63:0C:C5:93:A9:47:7B:4D:14:52:C3:72:B2:DB:67:0D:63:C0:4
Certificate is to be certified until Apr 23 08:00:53 2021 GMT (365 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]
Write out database with 1 new entries
Data Base Updated
```

### Task 3: Deploying Certificate in an HTTPSWeb Server

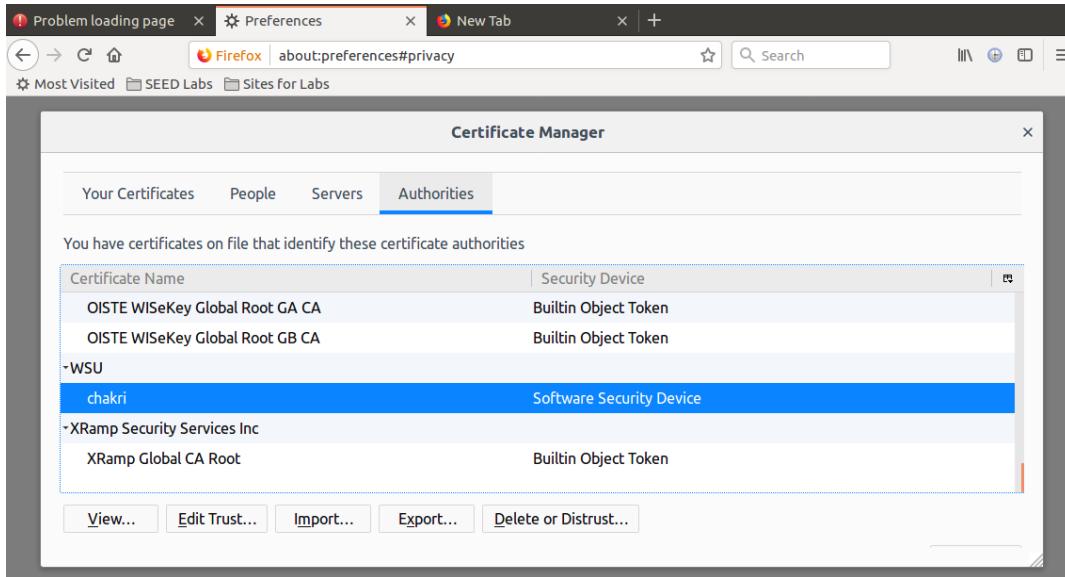
#### Step 1: Configuring DNS.



#### Step 2: Configuring the web server.

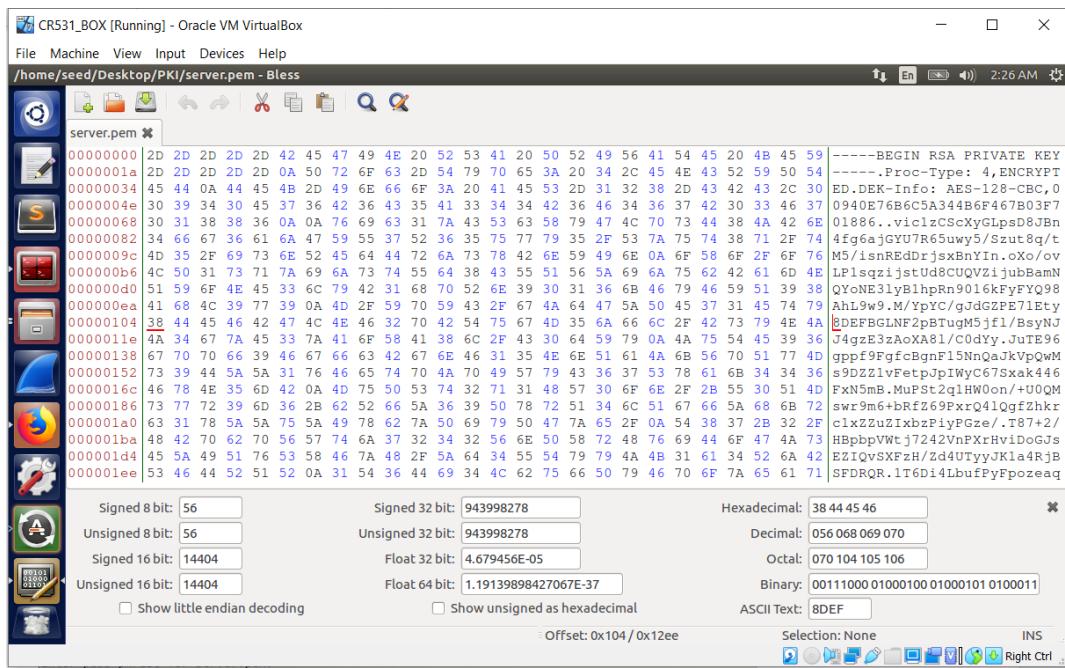


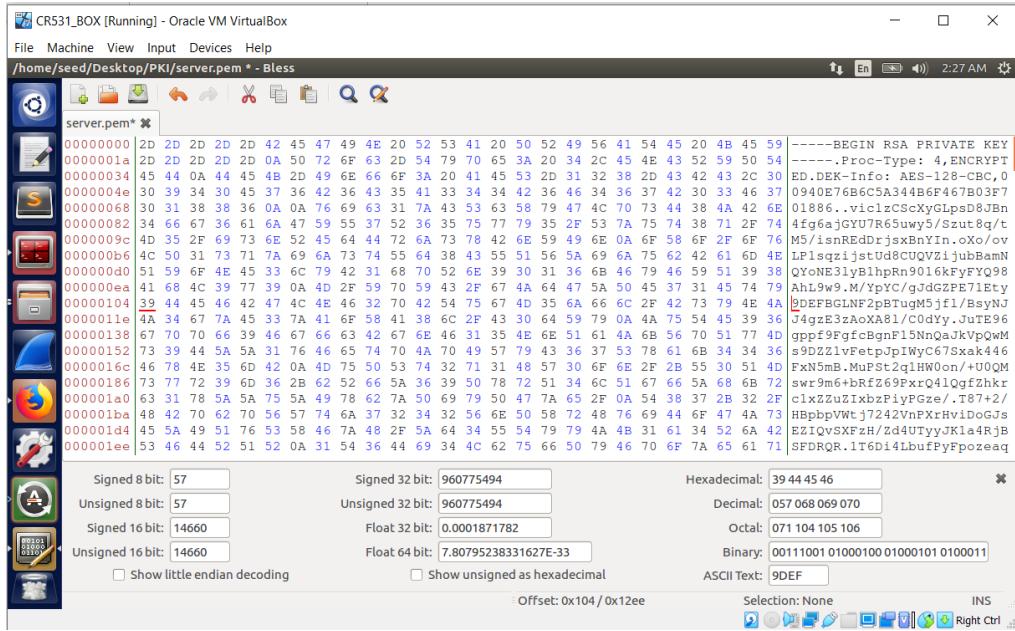
#### Step 3: Getting the browser to accept our CA certificate



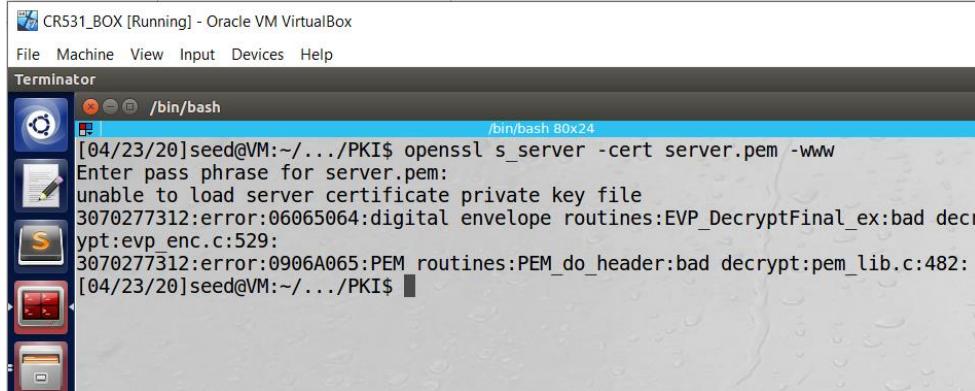
**1. Modify a single byte of server.pem, and restart the server, and reload the URL. What do you observe? Make sure you restore the original server.pem afterward. Note: the server may not be able to restart if certain places of server.pem is corrupted; in that case, choose another place to modify.**

Changing single byte in server.pem from (38 to 39)

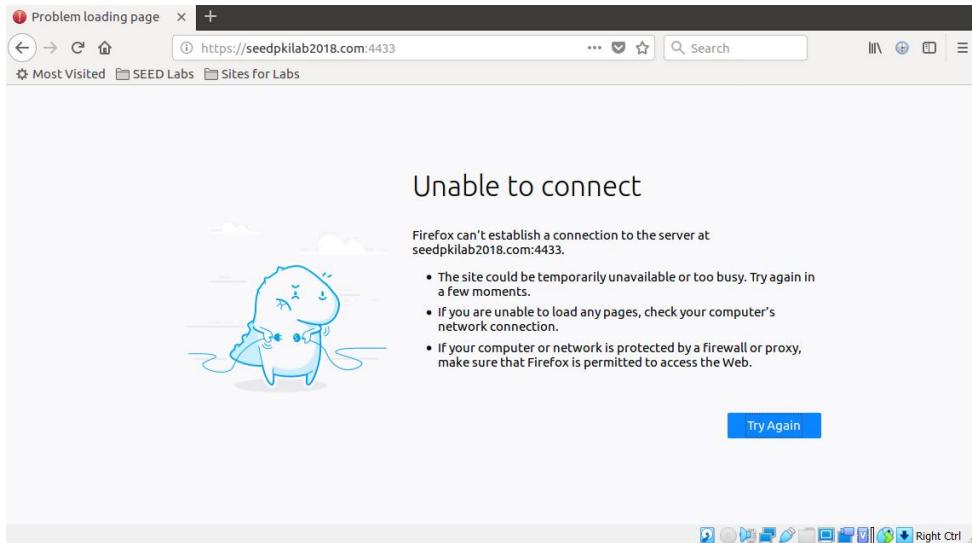




**Now checking this in terminal**



**Observation:** If we change the single byte in server.key part of the server.pem, then the terminal cannot load the server certificate key file.



The connection cannot be established to SEEDPKILab2018.com since the server certificate private key is corrupted.

Now, again modifying the byte at another place

CR531\_BOX [Running] - Oracle VM VirtualBox

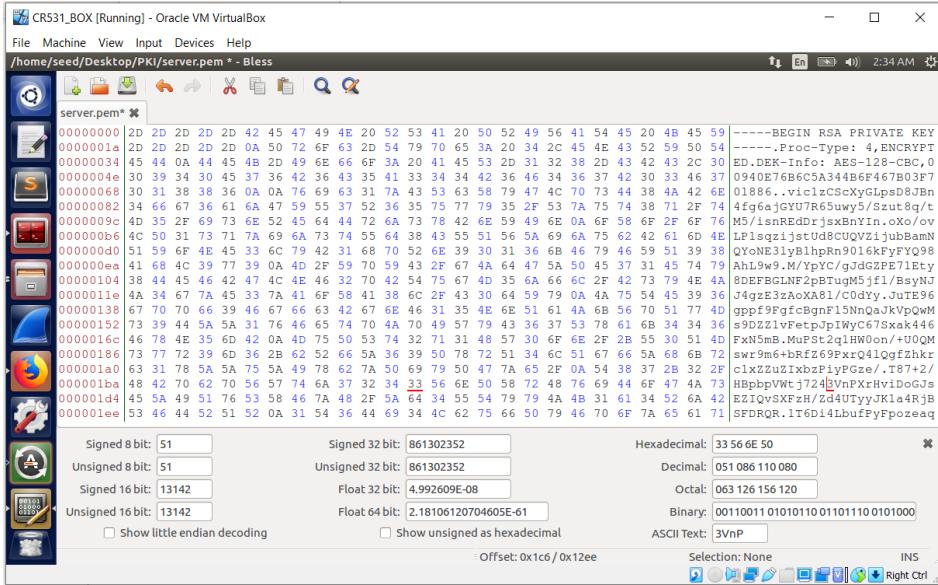
File Machine View Input Devices Help

/home/seed/Desktop/PKI/server.pem \* - Bless

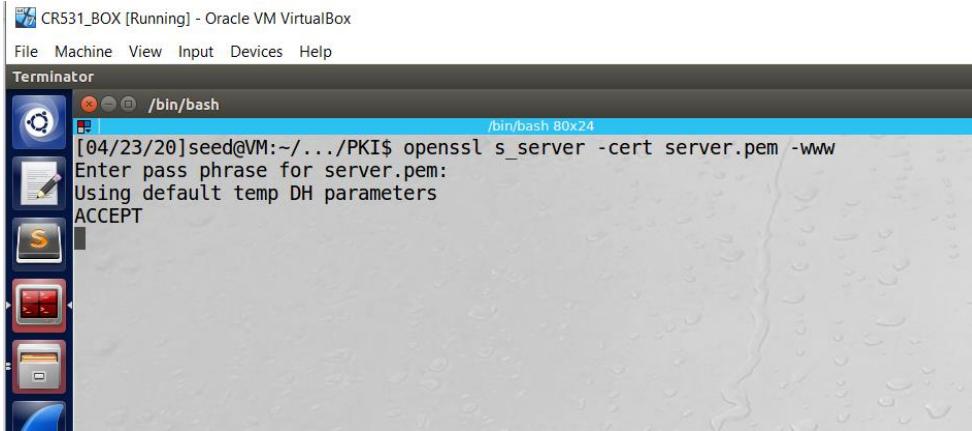
server.pem \*

```
00000000 | 2D 2D 2D 2D 2D 42 45 47 49 4E 20 52 53 41 20 50 52 49 56 41 54 45 20 4B 45 59 -----BEGIN RSA PRIVATE KEY-----  
00000014 | 2D 2D 2D 2D 0A 50 72 6F 63 2D 54 79 70 65 3A 20 34 2C 45 4E 43 52 59 50 54 .Proc-Type: 4,ENCRYPTED  
00000034 | 45 44 0A 44 45 4B 2D 49 62 66 6F 3A 20 41 45 53 2D 31 32 38 2D 43 42 43 2C 30 ED.DEK-Info: AES-128-CBC,0  
0000004e | 30 39 34 30 45 37 36 42 36 43 35 41 33 34 34 42 36 46 34 36 37 42 30 33 46 37 0940E76B6C5A344B6F467B03F7  
00000060 | 30 31 38 38 36 0A 0A 76 69 63 31 7A 43 53 63 58 79 47 4C 70 73 44 38 42 42 6E 01886..Vic1zCScxYGlpsu8JBn  
00000082 | 34 66 67 36 61 6A 47 59 55 37 52 36 35 75 77 79 35 2F 53 7A 75 74 38 73 2F 74 4fg6ajGYUTR6suwy5Szut8q/t  
0000009c | 4D 35 2F 69 73 6E 52 45 64 44 72 6A 73 78 42 6B 59 49 6E 0A 6F 58 6F 2F 6F 76 M5/insREdRdrjsxBnYIn.oKo/ov  
000000b6 | 4C 50 31 73 71 7A 69 6A 73 74 55 6A 38 43 55 51 56 5A 69 6A 75 62 42 61 6D 4E LPlsgzqijstUd8CUQVZijubBamN  
000000d0 | 51 59 6F 4B 45 33 6C 79 42 31 68 70 52 6E 39 30 31 36 6B 46 79 46 59 51 39 38 QYoNE3lyBlhpRn9016KfYFYQ98  
000000ea | 41 68 4C 39 77 39 0A 4B 2F 59 70 59 43 2F 67 4A 64 47 5A 50 45 37 31 45 74 79 AhL9w9.M/WpYC/gJdgZE7lEtY  
00000104 | 38 44 45 46 42 47 4C 4E 46 32 70 42 54 75 67 4D 35 6A 66 6C 2F 42 73 79 4B 4A 8DEFBGLNF2pBTugM5jfl/BsyNj  
0000011e | 4B 34 67 7A 45 33 7A 41 6F 58 41 38 6C 2F 43 30 64 59 79 0A 4B 75 45 39 36 J4gzB3zaoxA8l/C0dyJ.JuTE96  
00000138 | 67 70 70 66 39 46 67 66 63 42 67 6E 46 31 35 4E 6E 51 61 4A 6B 56 70 51 77 4D gppf9FgfcBgnf15NhQa3kVpQWM  
00000152 | 73 39 44 5A 5A 31 76 46 65 74 70 4A 70 49 57 79 43 36 37 53 78 61 6B 34 34 36 s9DZZ1vFetpOpIWyC67sxak446  
0000016c | 46 78 4E 35 6D 42 0A 4B 75 50 53 74 32 71 31 4B 57 30 6F 6B 2F 2B 55 30 51 4D FXN5mB..MuFST2q1HW0on/+U0QM  
00000180 | 73 77 72 39 6D 36 2B 62 52 66 5A 3E 39 50 78 72 51 34 6E 51 67 66 5A 6B 72 swr9m6+BrF269PxrxQ41gfzf2hkr  
000001a0 | 63 31 78 5A 5A 75 5A 49 78 62 7A 50 69 79 50 47 7A 65 2F 0A 54 38 37 2B 32 2F c1xZ2uZ1xbzFiyPGze/.T87+2/  
000001b4 | 48 42 70 62 70 56 57 74 6A 37 32 34 32 56 6E 50 58 72 48 76 69 44 6F 47 4A 73 HBpbpVWtJ724VnPxrHvidoGJs  
000001d4 | 45 5A 49 51 76 53 58 46 7A 48 2F 5A 64 34 55 54 79 79 4A 4B 31 61 34 52 6A 42 EZIQVSXZh/Zd4UTvvJK1a4RjB  
000001ee | 53 46 44 52 51 52 0A 31 54 36 44 69 34 4C 62 75 66 50 79 46 70 6F 7A 65 61 71 SFDRQR.1T6Di4LbufPyFpozeaq
```

Signed 8 bit: 50      Signed 32 bit: 844525136      Hexadecimal: 32 56 6E 50  
 Unsigned 8 bit: 50      Unsigned 32 bit: 844525136      Decimal: 050 086 110 080  
 Signed 16 bit: 12886      Float 32 bit: 1.248152E-08      Octal: 062 126 156 120  
 Unsigned 16 bit: 12886      Float 64 bit: 3.32803528907174E-66      Binary: 00110010 01010110 01101110 01010000  
 Show little endian decoding       Show unsigned as hexadecimal      ASCII Text: 2VnP  
 Offset: 0x1c6 / 0x12ee      Selection: None      INS  
 Right Ctrl



Above screenshots depict that change of byte i.e.(32 to 33) and checking in the terminal



**Observation:** Now, from the above screenshot we can see that the server is launched since there is no corruption in the server's private key part.

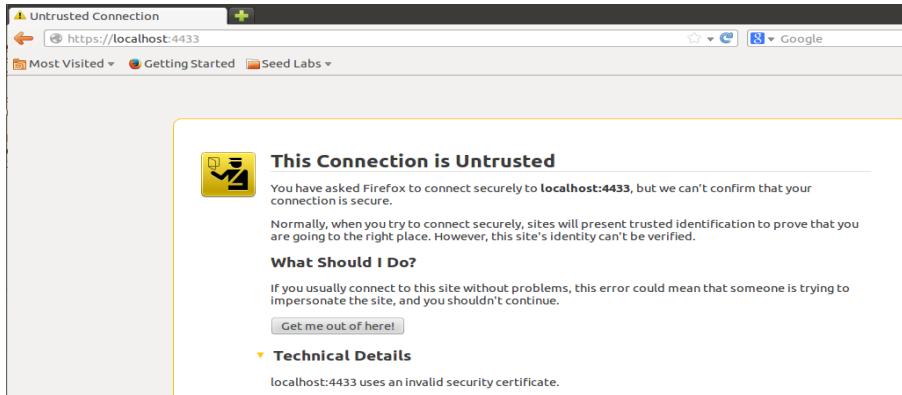
**2. Since SEEDPKILab2018.com points to the localhost, if we use https://localhost:4433 instead, we will be connecting to the same web server. Please do so, describe and explain your observation.**

Now, we replace SEEDPKILab2018.com to localhost in the url and accessed the server again. But, we can see that connection is untrusted because even though localhost and SEEDPKILab2018.com points to 127.0.0.1 from below screenshot, it fails to accept initially.

```

File Machine View Input Devices Help
hosts [Read-Only] (/etc) - gedit
Open ▾
127.0.0.1      localhost
127.0.1.1      VM
127.0.0.1      SEEDPKILab2018.com
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
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

```

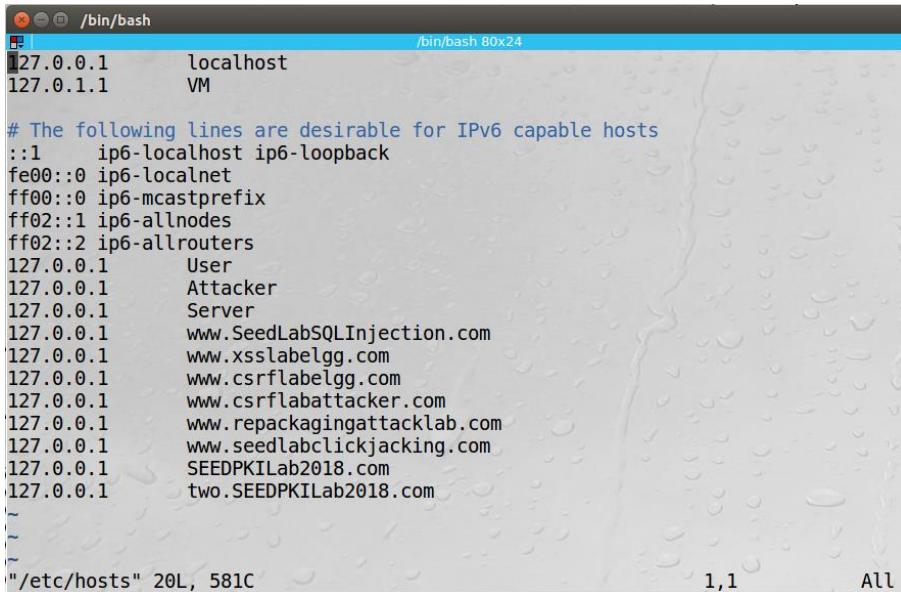


Now, after adding the exception to localhost name we can see the data in web browser as shown in the below screenshot



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

Adding 127.0.0.1 two.SEEDPKILab2018.com to /etc/hosts

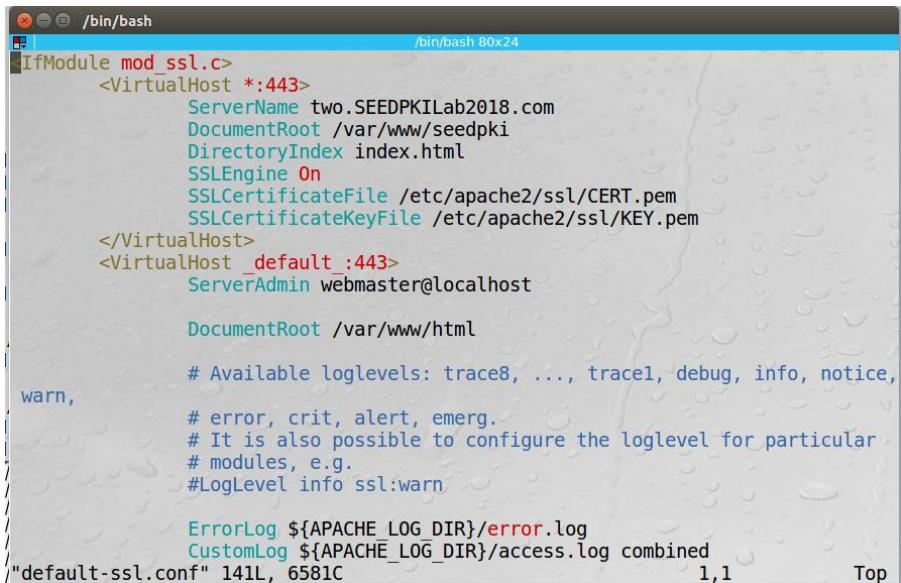


```
/bin/bash
127.0.0.1      localhost
127.0.1.1      VM

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
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.csrfattacker.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      two.SEEDPKILab2018.com
~
~
~

"/etc/hosts" 20L, 581C          1,1          All
```

Adding VirtualHost code snippet to etc/apache2/sites-available/default-ssl.conf



```
IfModule mod_ssl.c>
<VirtualHost *:443>
    ServerName two.SEEDPKILab2018.com
    DocumentRoot /var/www/seedpki
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /etc/apache2/ssl/CERT.pem
    SSLCertificateKeyFile /etc/apache2/ssl/KEY.pem
</VirtualHost>
<VirtualHost _default_:443>
    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
    CustomLog ${APACHE_LOG_DIR}/access.log combined
"/default-ssl.conf" 141L, 6581C          1,1          Top
```

Adding index.html to "seedpki" folder just by changing the title of the page

CR531\_BOX [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Index.html (/var/www/seedpk) - gedit

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<!--
    Modified from the Debian original for Ubuntu
    Last updated: 2014-03-19
    See: https://launchpad.net/bugs/1288690
-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>PKI is working!!</title>
<style type="text/css" media="screen">
* {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
}

body, html {
    padding: 3px 3px 3px 3px;
    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
}

div.main_page {
    position: relative;
    display: table;
    width: 800px;

    margin-bottom: 3px;
    margin-left: auto;
    margin-right: auto;
    padding: 0px 0px 0px 0px;
}

```

Now performing below actions

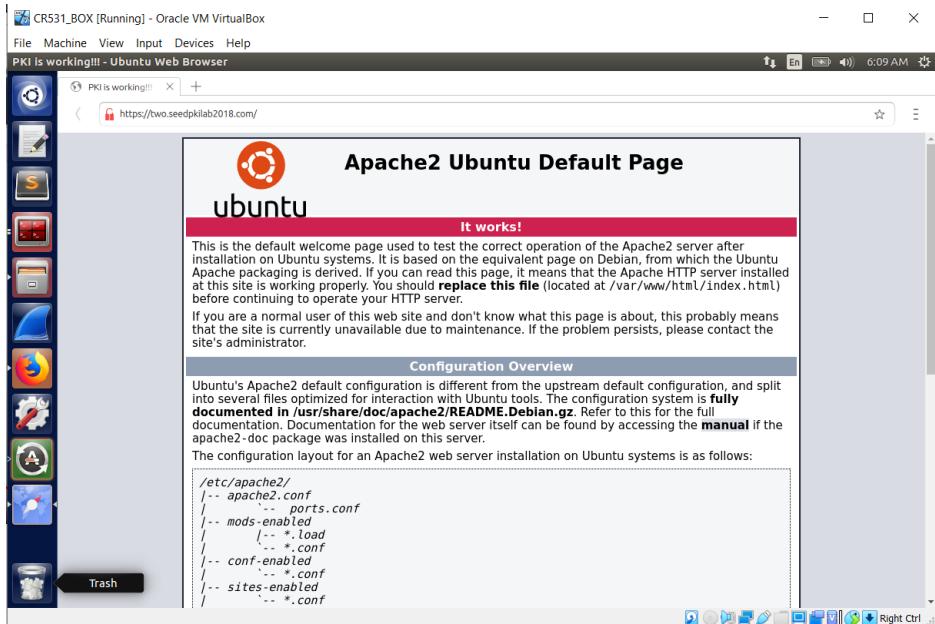
CR531\_BOX [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminator

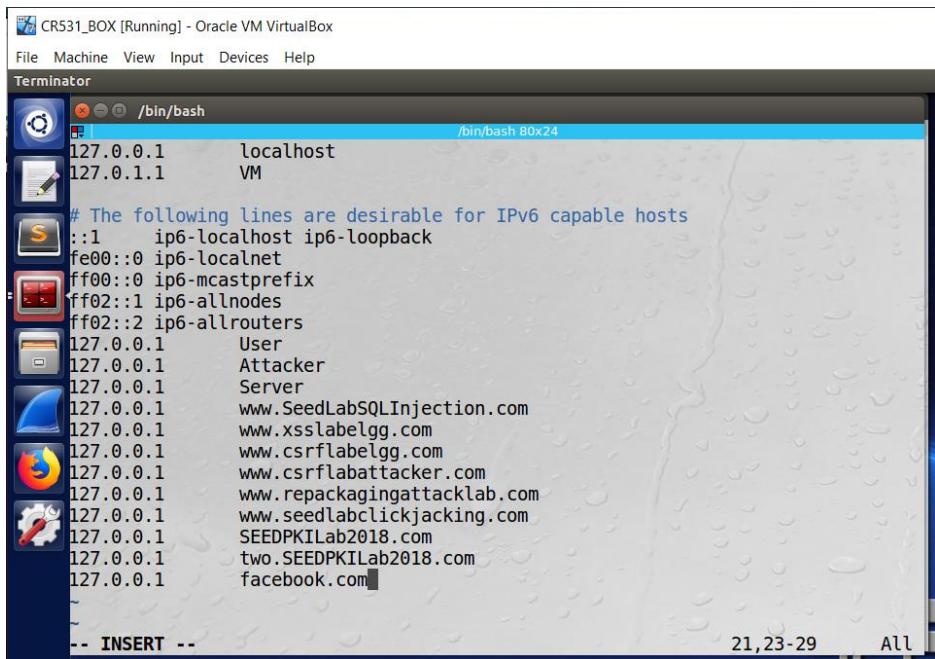
```
/bin/bash
[04/23/20]seed@VM:~/.../PKI2$ sudo apachectl configtest
AH00112: Warning: DocumentRoot [/var/www/seedlabclickjacking] does not exist
AH00112: Warning: DocumentRoot [/var/www/Example_One] does not exist
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
[04/23/20]seed@VM:~/.../PKI2$ 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
[04/23/20]seed@VM:~/.../PKI2$ sudo a2ensite default-ssl
Site default-ssl already enabled
[04/23/20]seed@VM:~/.../PKI2$ sudo service apache2 restart
Enter passphrase for SSL/TLS keys for two.SEEDPKILab2018.com:443 (RSA): ****
*
[04/23/20]seed@VM:~/.../PKI2$
```

Output: From the below screenshot we can see the title of the page is “PKI is working!!!”



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

Adding 127.0.0.1 facebook.com to /etc/hosts



Now, adding the VirtualHost code snippet to /etc/apache2/sites-available/default-ssl.conf

CR531\_BOX [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

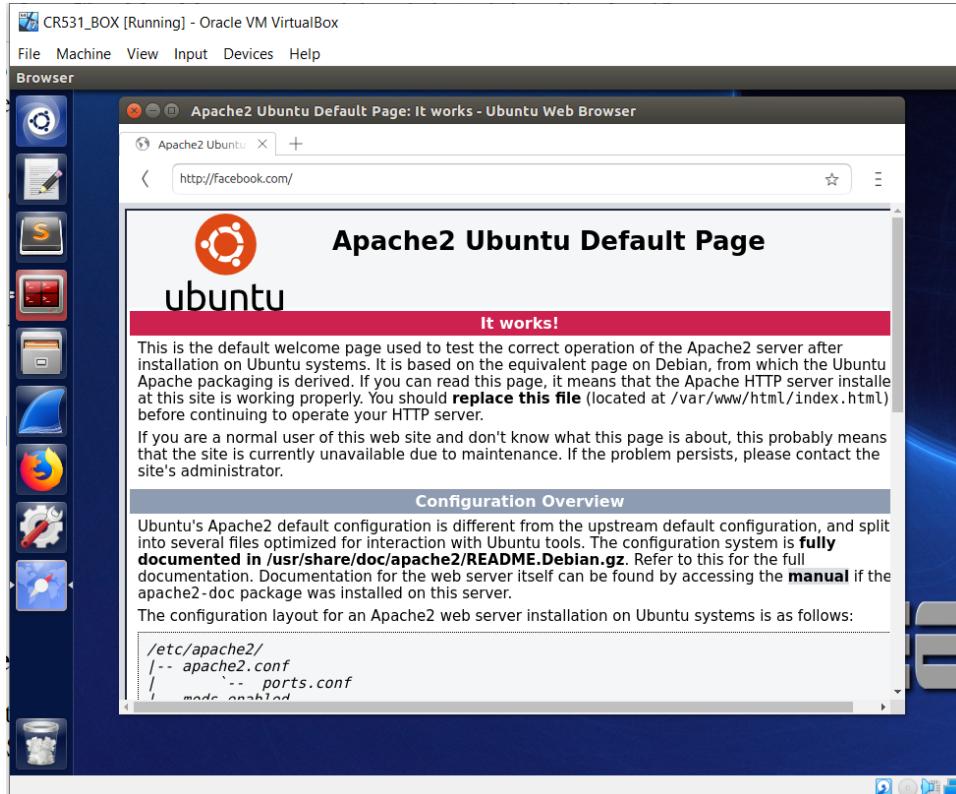
Terminator

```
/bin/bash
/bn/bash 80x24

<IfModule mod_ssl.c>
    <VirtualHost *:443>
        ServerName two.SEEDPKILab2018.com
        DocumentRoot /var/www/seedpki
        DirectoryIndex index.html
        SSLEngine On
        SSLCertificateFile /etc/apache2/ssl/CERT.pem
        SSLCertificateKeyFile /etc/apache2/ssl/KEY.pem
    </VirtualHost>
    <VirtualHost *:443>
        ServerName facebook.com
        DocumentRoot /var/www/seedpki
        DirectoryIndex index.html
        SSLEngine On
        SSLCertificateFile /etc/apache2/ssl/CERT.pem
        SSLCertificateKeyFile /etc/apache2/ssl/KEY.pem
    </VirtualHost>
    <VirtualHost _default_:443>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
    
```

-- INSERT -- 18,1 Top

Now, open browser and type facebook.com and see the output.



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

```
CR531_BOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash 80x24
[04/24/20]seed@VM:~$ cd Desktop/PKI2
[04/24/20]seed@VM:~/.../PKI2$ openssl req -new -key server.key -out facebook.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 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]:US
State or Province Name (full name) [Some-State]:Kansas
Locality Name (eg, city) []:Wichita
Organization Name (eg, company) [Internet Widgits Pty Ltd]:WSU
Organizational Unit Name (eg, section) []:MS
Common Name (e.g. server FQDN or YOUR name) []:facebook.com
Email Address []:chakradharreddy985@gmail.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:chakradhar
An optional company name []:WSU
[04/24/20]seed@VM:~/.../PKI2$
```

```
CR531_BOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash 80x24
A challenge password []:chakradhar
An optional company name []:WSU
[04/24/20]seed@VM:~/.../PKI2$ openssl ca -in facebook.csr -out facebook.crt -cer
t 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: 4097 (0x1001)
    Validity
        Not Before: Apr 24 16:21:53 2020 GMT
        Not After : Apr 24 16:21:53 2021 GMT
    Subject:
        countryName          = US
        stateOrProvinceName = Kansas
        organizationName    = WSU
        organizationalUnitName= MS
        commonName           = facebook.com
        emailAddress         = chakradharreddy985@gmail.com
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
```

CR531\_BOX [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminator

```
/bin/bash 80x24
    OpenSSL Generated Certificate
    X509v3 Subject Key Identifier:
        B6:78:41:9D:9E:CA:7C:FB:84:7B:B0:65:D4:D3:86:27:E5:A3:34:F8
    X509v3 Authority Key Identifier:
        keyid:AF:57:4F:C6:46:40:E2:F9:93:83:96:DC:24:77:35:39:E9:41:1D:E
7
Certificate is to be certified until Apr 24 16:21:53 2021 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
[04/24/20]seed@VM:~/.../PKI2$ cp server.key facebook.pem
[04/24/20]seed@VM:~/.../PKI2$ cat facebook.crt >> facebook.pem
[04/24/20]seed@VM:~/.../PKI2$
[04/24/20]seed@VM:~/.../PKI2$ ls
ca.crt demoCA facebook.csr openssl.cnf server.csr server.pem
ca.key facebook.crt facebook.pem server.crt server.key
[04/24/20]seed@VM:~/.../PKI2$ cp facebook.crt CERT2.pem
[04/24/20]seed@VM:~/.../PKI2$ sudo mv "/home/seed/Desktop/PKI2/CERT2.pem" "/etc/
apache2/ssl"
[04/24/20]seed@VM:~/.../PKI2$
```

Now, change the Virtual host code snippet of facebook.com with new CERT2.pem

CR531\_BOX [Running] - Oracle VM VirtualBox

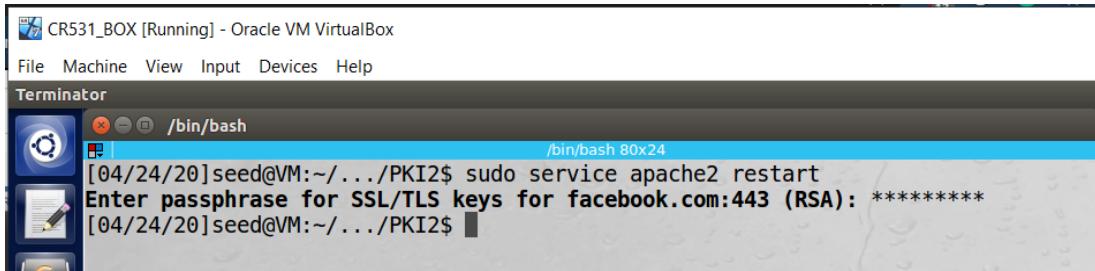
File Machine View Input Devices Help

Terminator

```
/bin/bash 80x23
<VirtualHost *:443>
    ServerName two.SEEDPKILab2018.com
    DocumentRoot /var/www/seedpki
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /etc/apache2/ssl/CERT.pem
    SSLCertificateKeyFile /etc/apache2/ssl/KEY.pem
</VirtualHost>
<VirtualHost *:443>
    ServerName facebook.com
    DocumentRoot /var/www/seedpki
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /etc/apache2/ssl/CERT2.pem
    SSLCertificateKeyFile /etc/apache2/ssl/KEY.pem
</VirtualHost>

<VirtualHost _default_:443>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
-- INSERT --
```

Now, restart the apache service



```
[04/24/20]seed@VM:~/.../PKI2$ sudo service apache2 restart
Enter passphrase for SSL/TLS keys for facebook.com:443 (RSA): *****
[04/24/20]seed@VM:~/.../PKI2$
```

From the below screenshot we can see that the title of the page is “**PKI is working**” which we have written in index.html file. Hence, Victim landed on our site.

