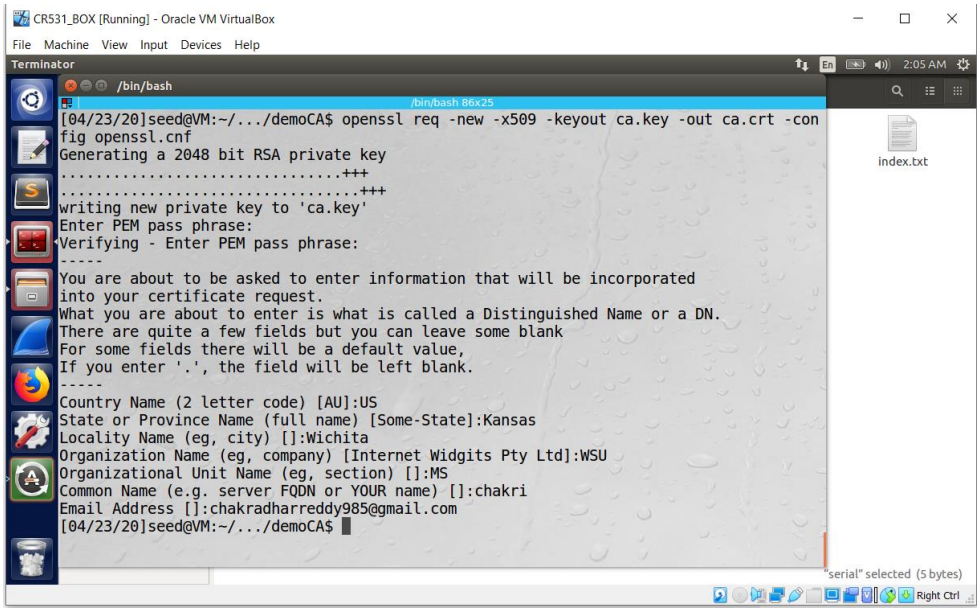
CS-767 Foundations Network Security

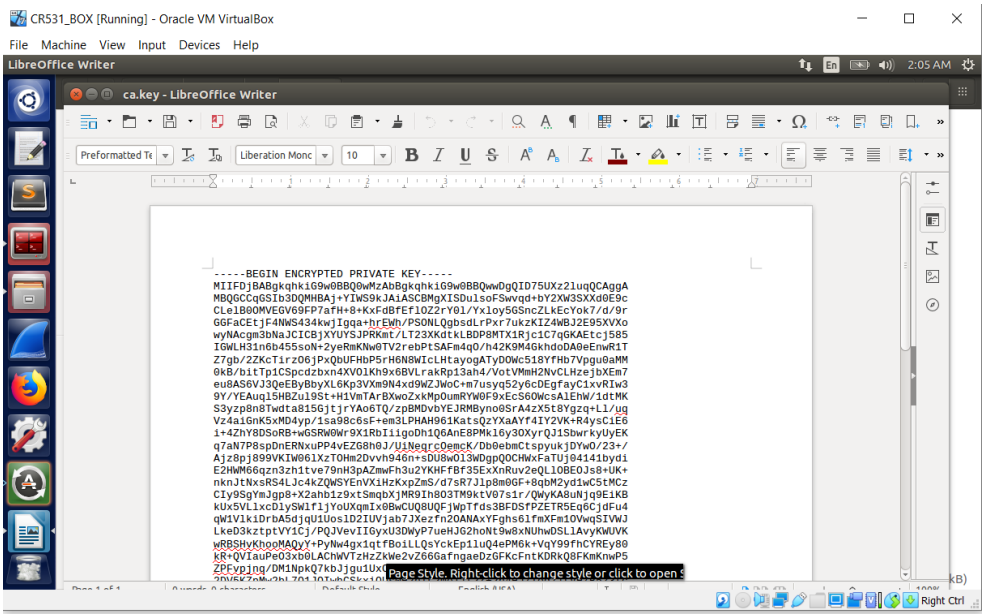
Public Key Infrastructure Lab

Chakradhar Reddy Donuri

E949F496

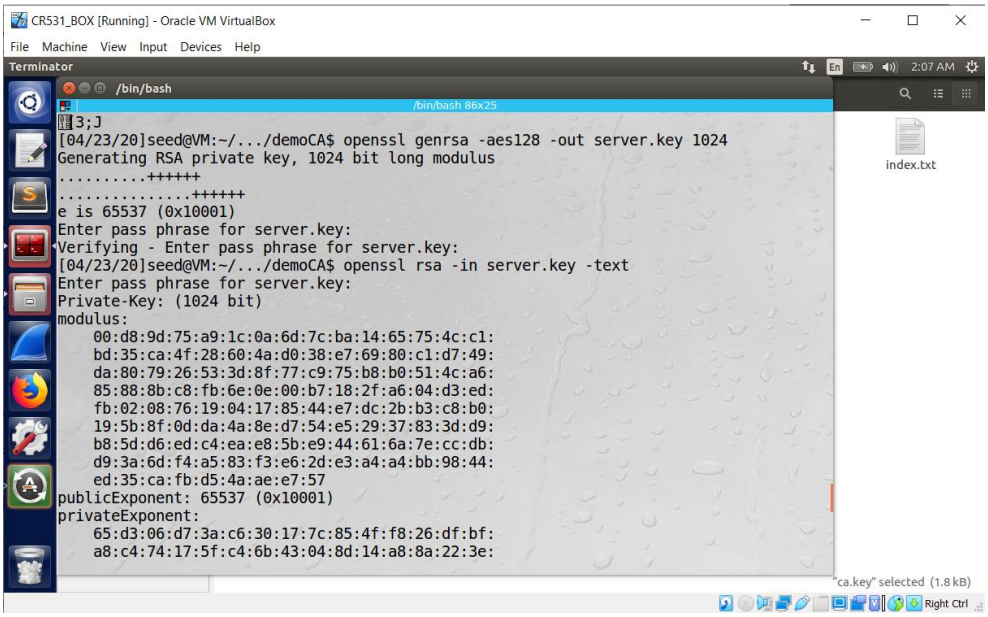
Task 1: Becoming a Certificate Authority (CA)



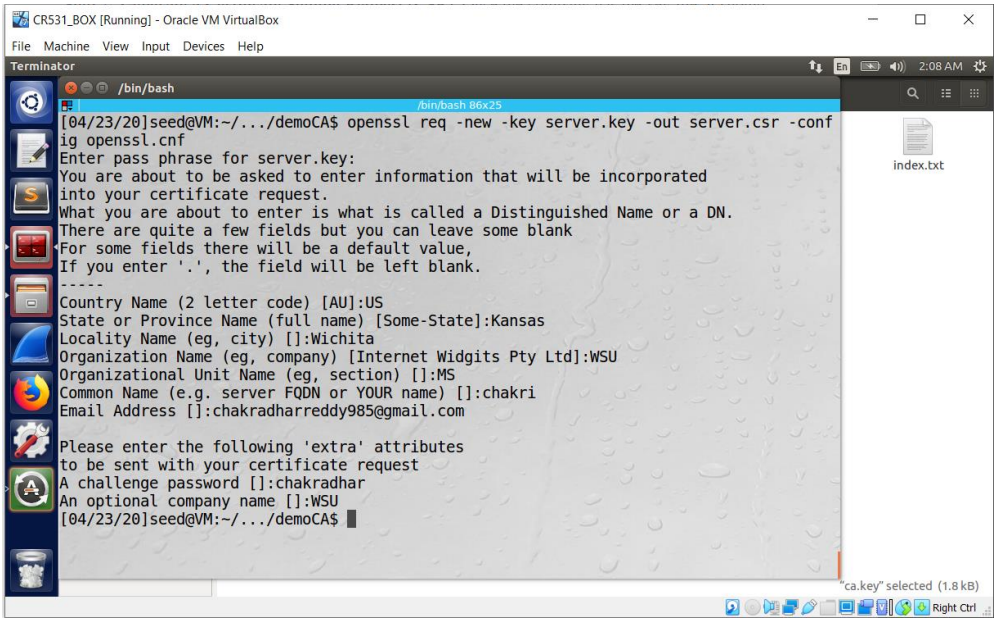


Task 2: Creating a Certificate for SEEDPKILab2018.com

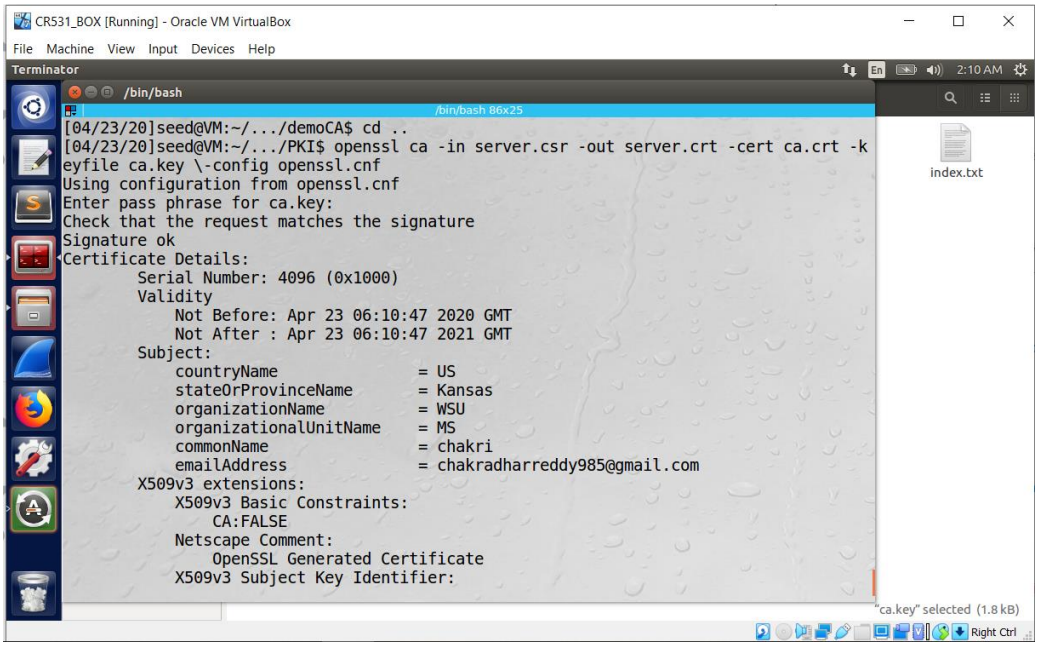
Step-1

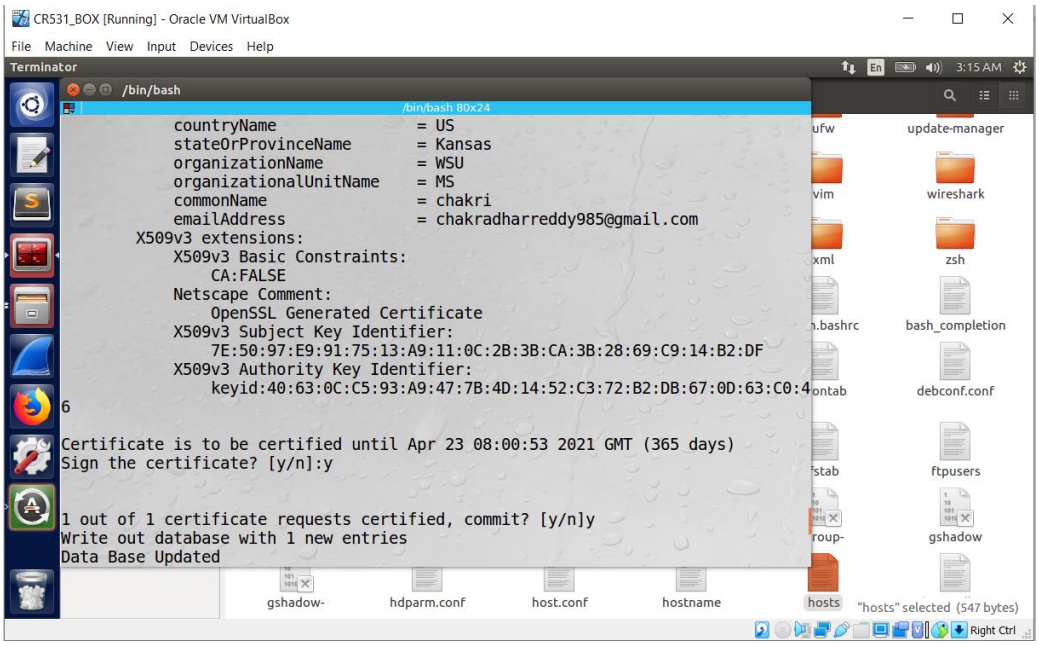


Step-2



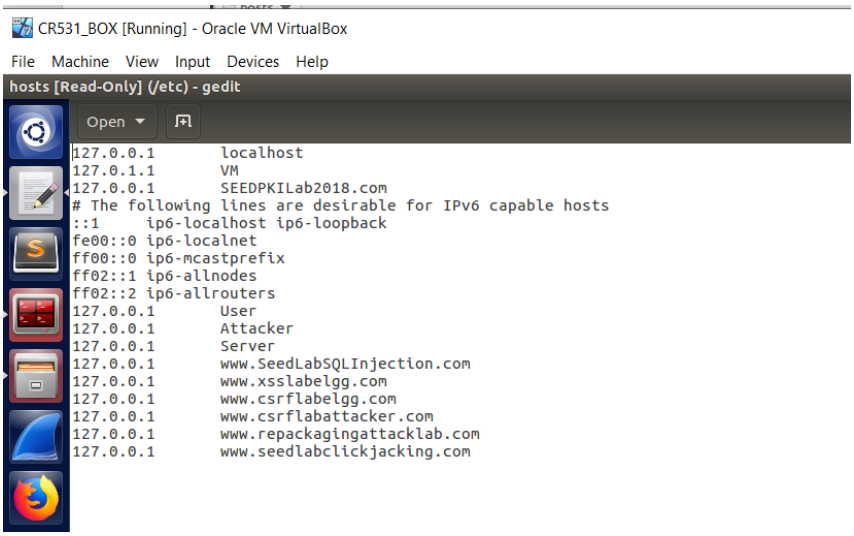
Step-3


CR531_BOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 86x25
[04/23/20]seed@VM:~/.../demoCA$ cd ..
[04/23/20]seed@VM:~/.../PKI$ openssl ca -in server.csr -out server.crt -cert ca.crt -k
eyfile 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:
index.txt
"ca.key" selected (1.8 kB)
Right Ctrl

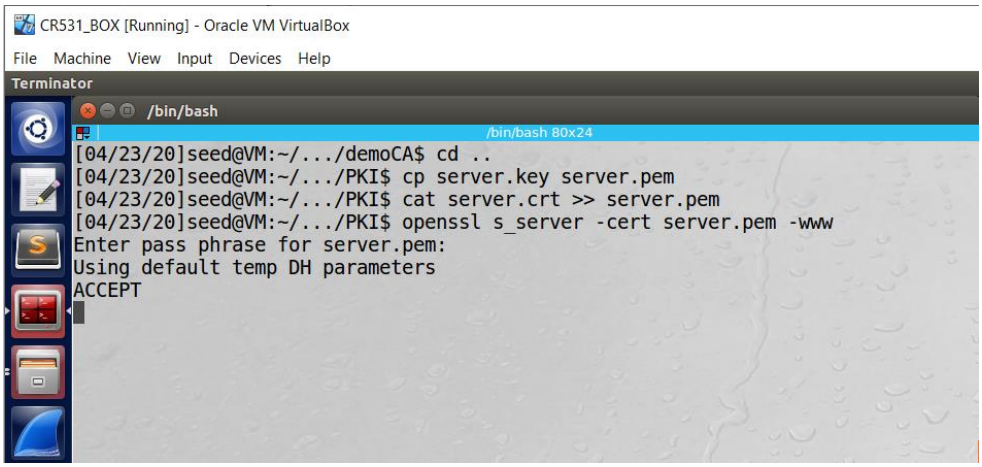

CR531_BOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 80x24
countryName = US
stateOrProvinceName = Kansas
organizationName = WSU
organizationalUnitName = MS
commonName = chakri
emailAddress = chakradharreddy985@gmail.com
X509v3 extensions:
X509v3 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
6
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]y
Write out database with 1 new entries
Data Base Updated
update-manager
wireshark
zsh
bash_completion
debconf.conf
ftpusers
gshadow
gshadow-
hdparm.conf
host.conf
hostname
hosts
"hosts" selected (547 bytes)
Right Ctrl

Task 3: Deploying Certificate in an HTTPSWeb Server

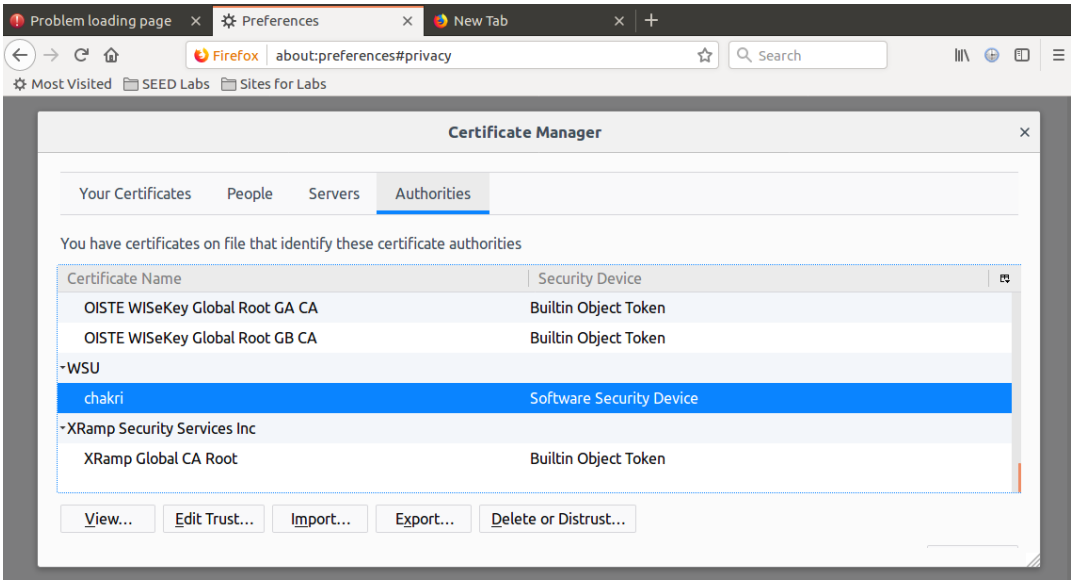
Step 1: Configuring DNS.



Step 2: Configuring the web server.

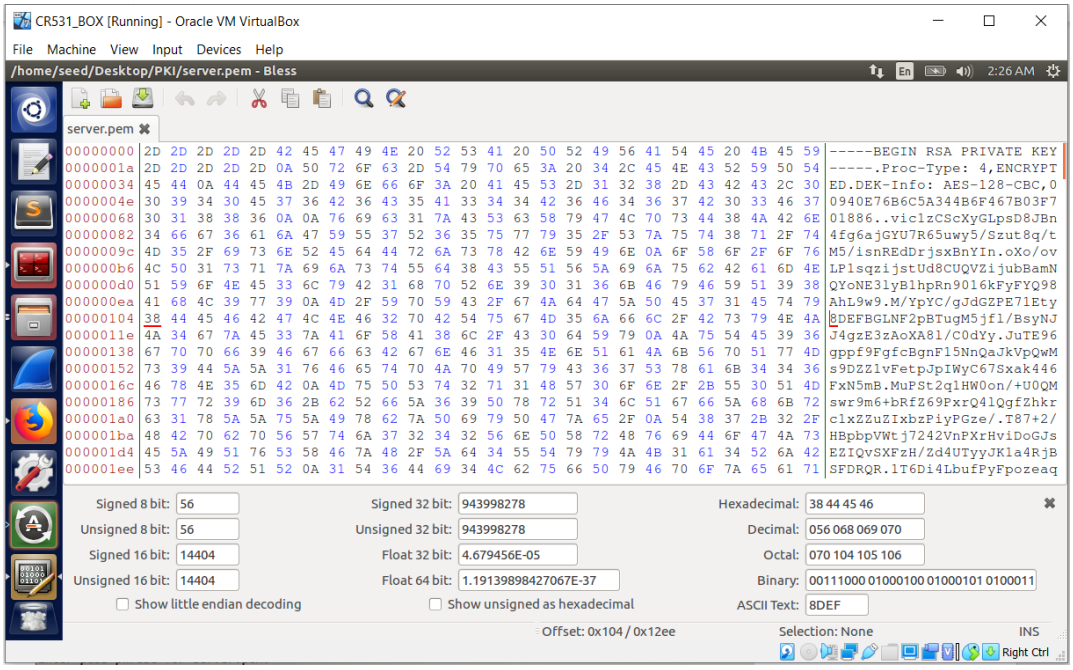


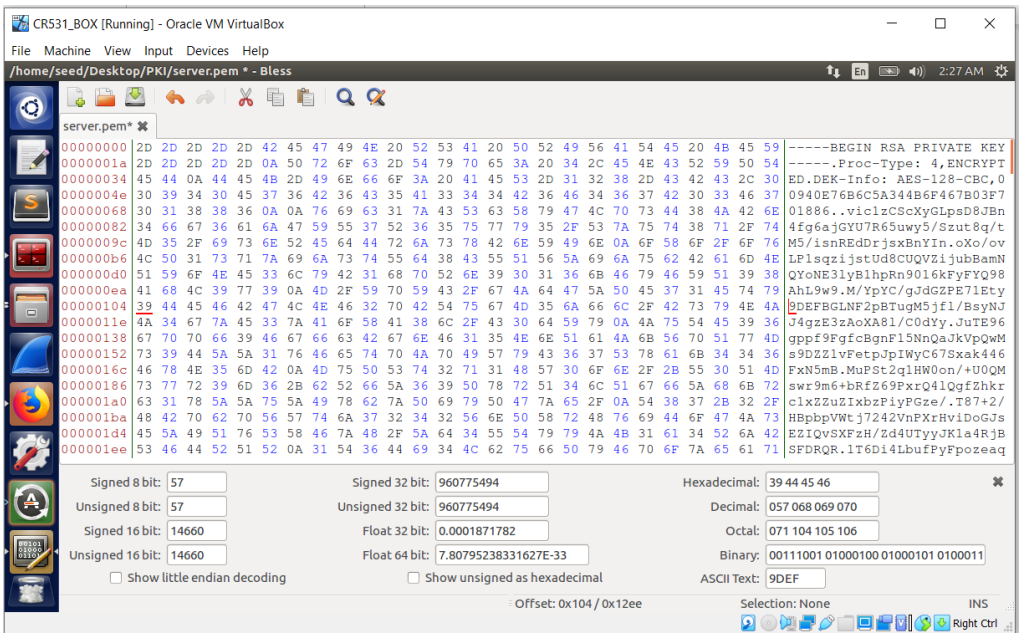
Step 3: Getting the browser to accept our CA certificate



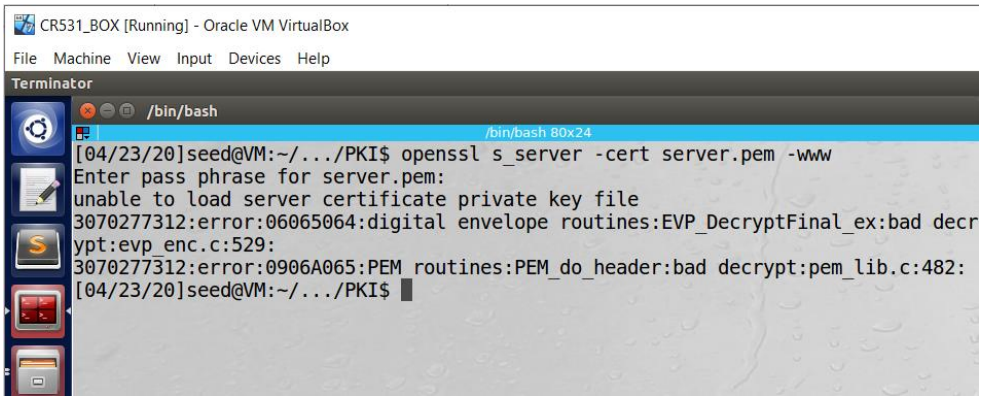
1. Modify a single byte of server.pem, and restart the server, and reload the URL. What do you observe? Make sure you restore the original server.pem afterward. Note: the server may not be able to restart if certain places of server.pem is corrupted; in that case, choose another place to modify.

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

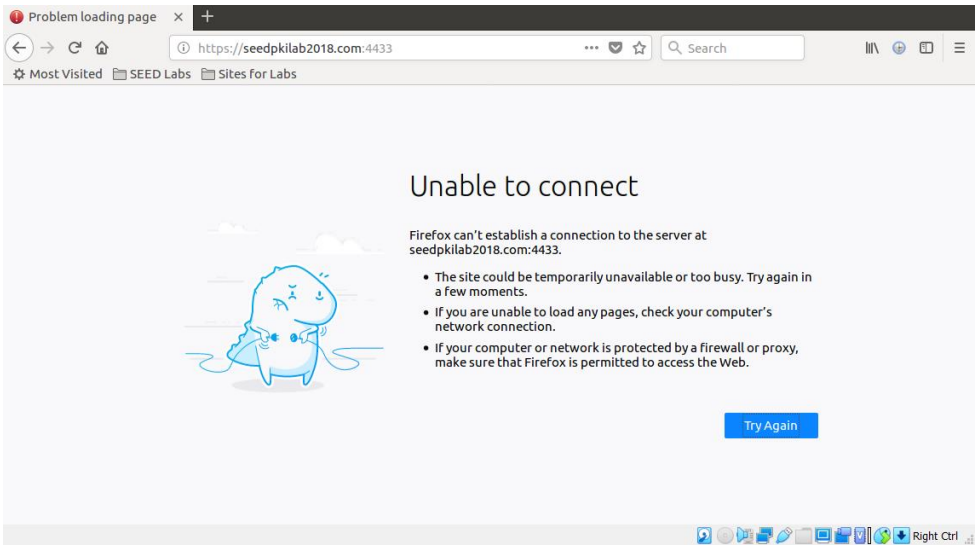




Now checking this in terminal

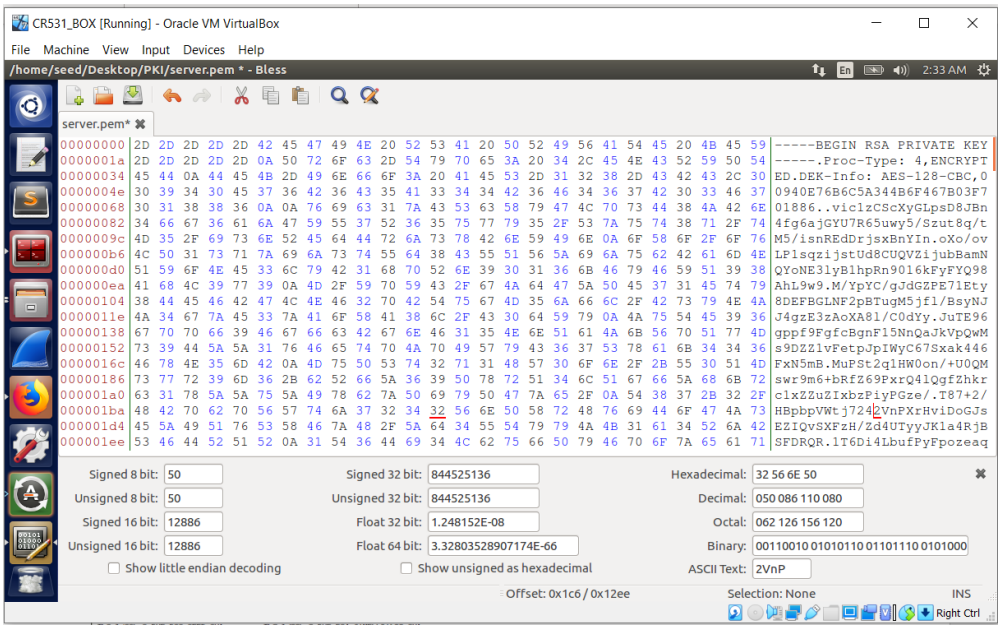


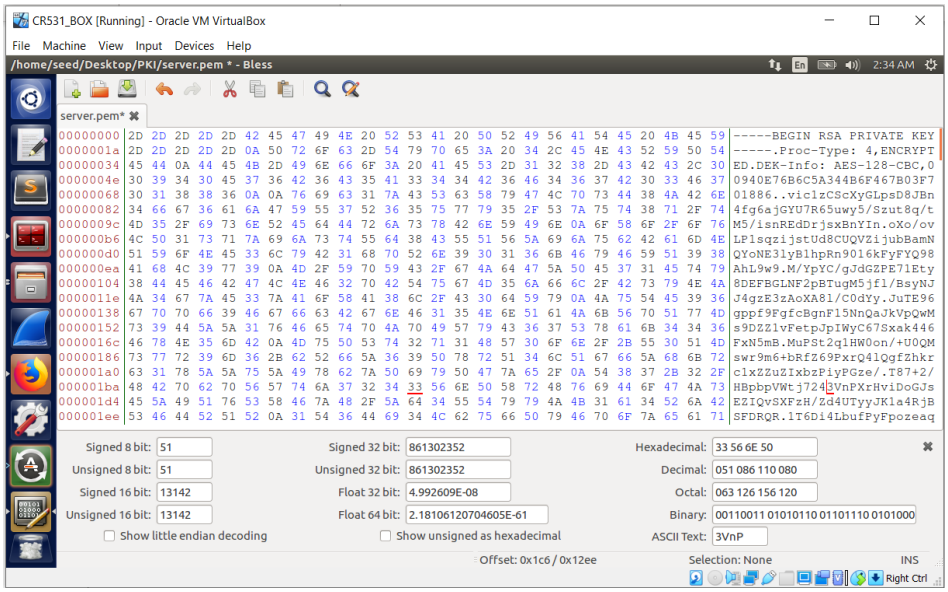
Observation: If we change the single byte in server.key part of the server.pem, then the terminal cannot load the server certificate key file.



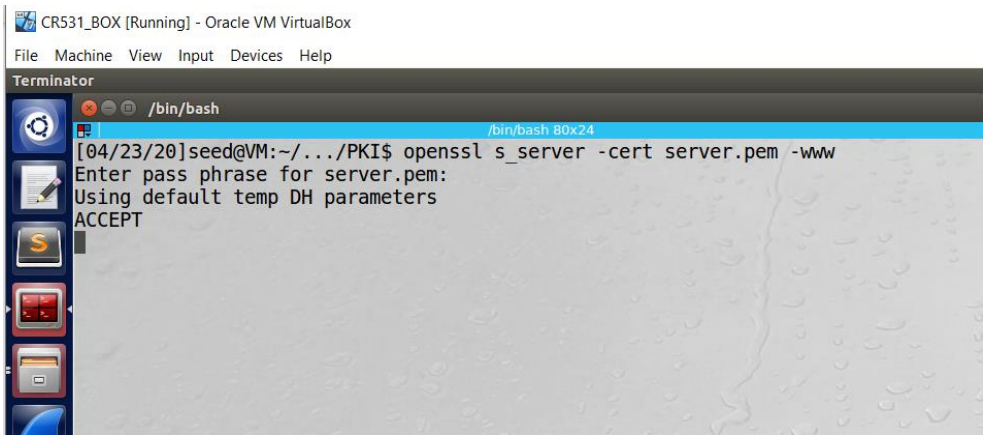
The connection cannot be established to SEEDPKILab2018.com since the server certificate private key is corrupted.

Now, again modifying the byte at another place





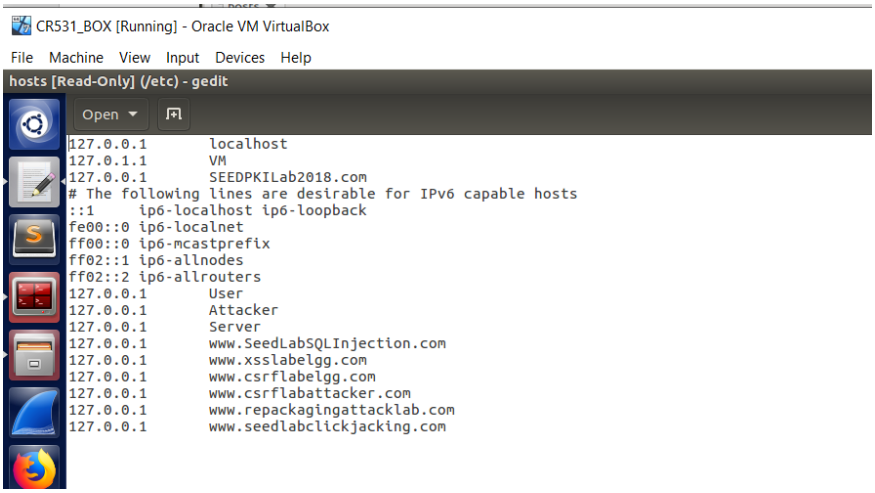
Above screenshots depict that change of byte i.e.(32 to 33) and checking in the terminal

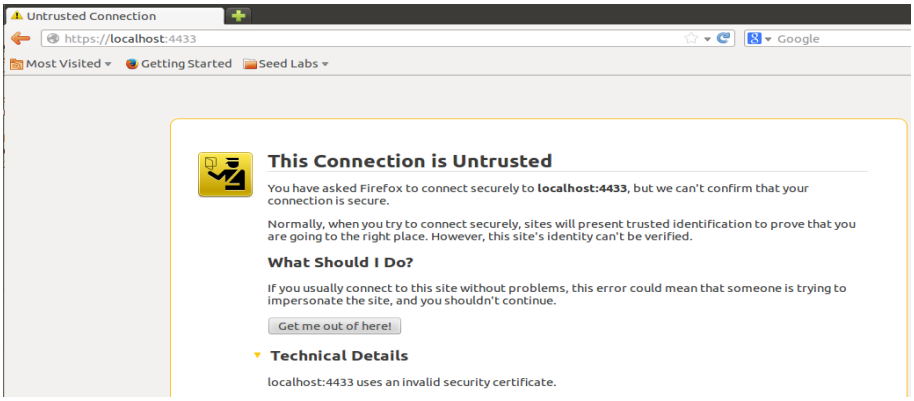


Observation: Now, from the above screenshot we can see that the server is launched since there is no corruption in the server's private key part.

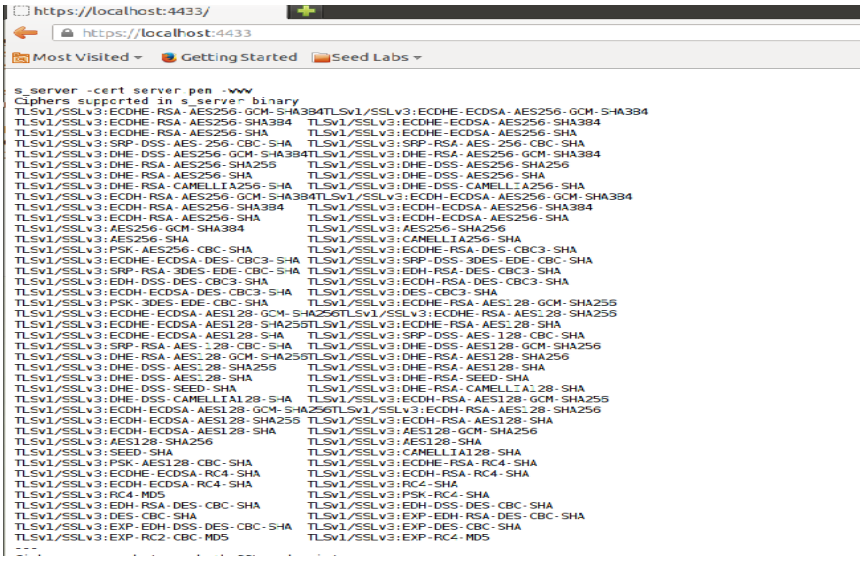
2. Since SEEDPKILab2018.com points to the localhost, if we use https://localhost:4433 instead, we will be connecting to the same web server. Please do so, describe and explain your observation.

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.



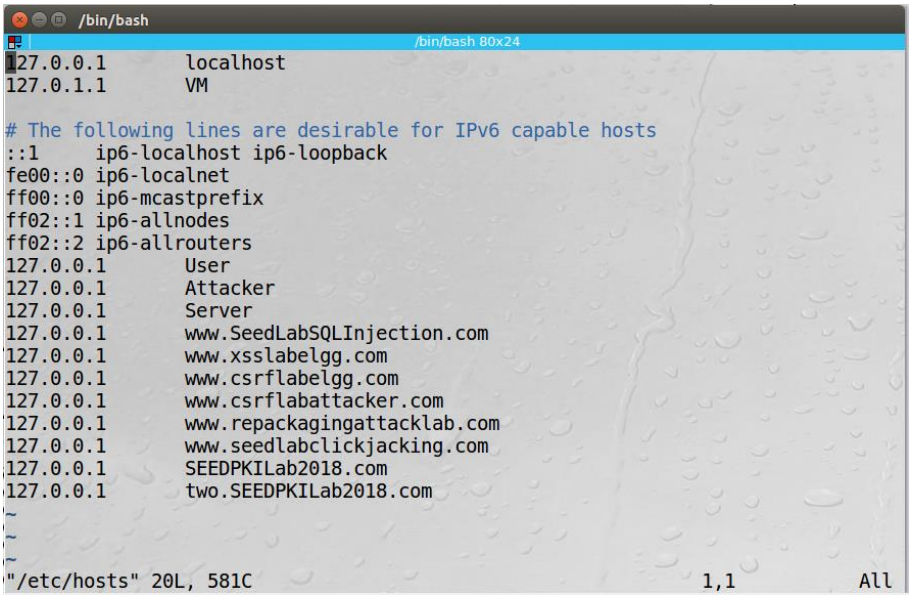


Now, after adding the exception to localhost name we can see the data in web browser as shown in the below screenshot

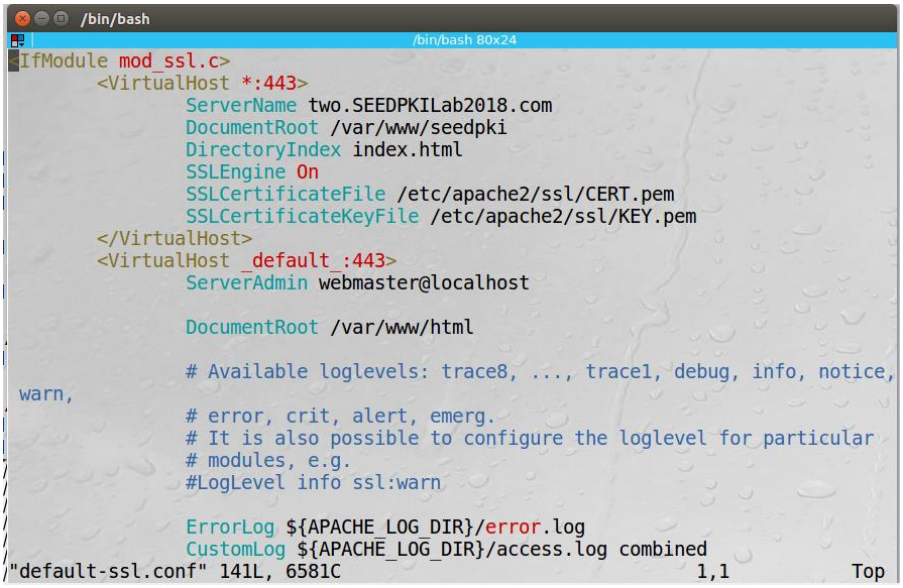


Task 4: Deploying Certificate in an Apache-Based HTTPS Website

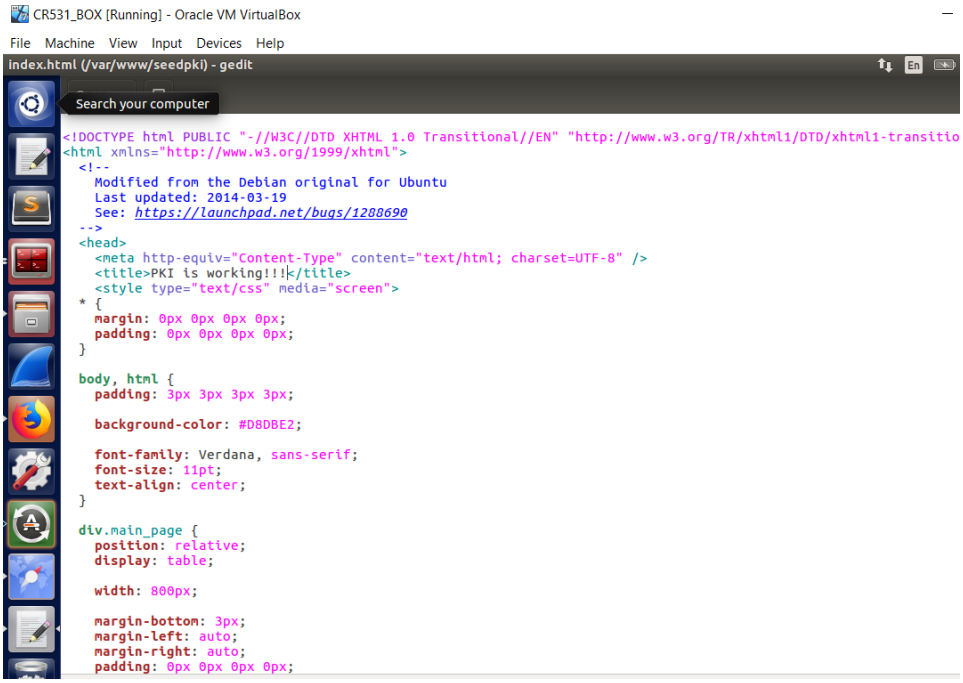
Adding 127.0.0.1 two.SEEDPKILab2018.com to /etc/hosts



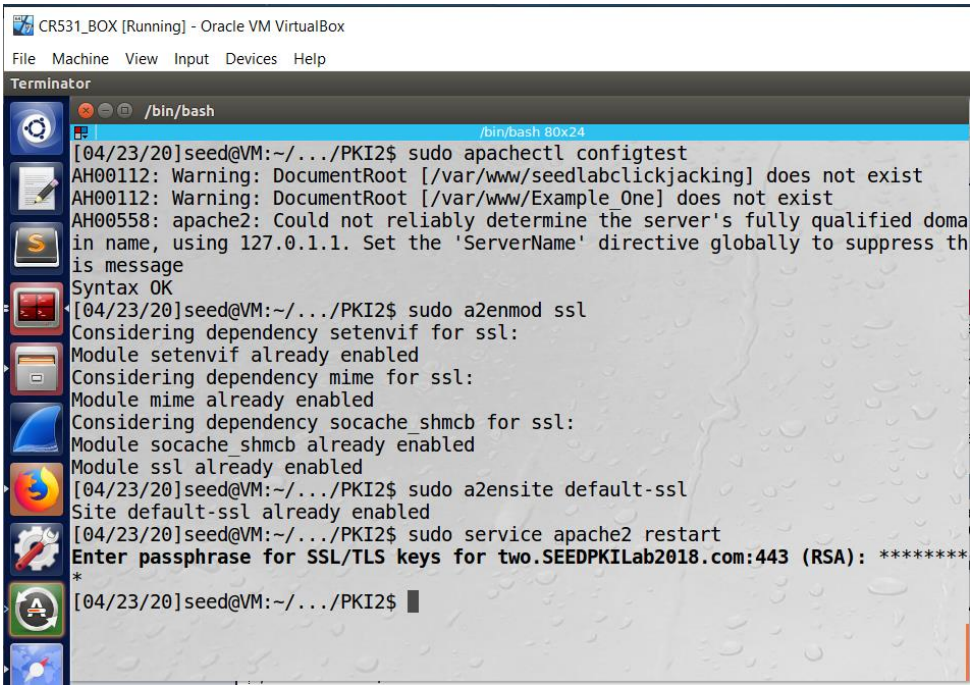
Adding VirtualHost code snippet to etc/apache2/sites-available/default-ssl.conf



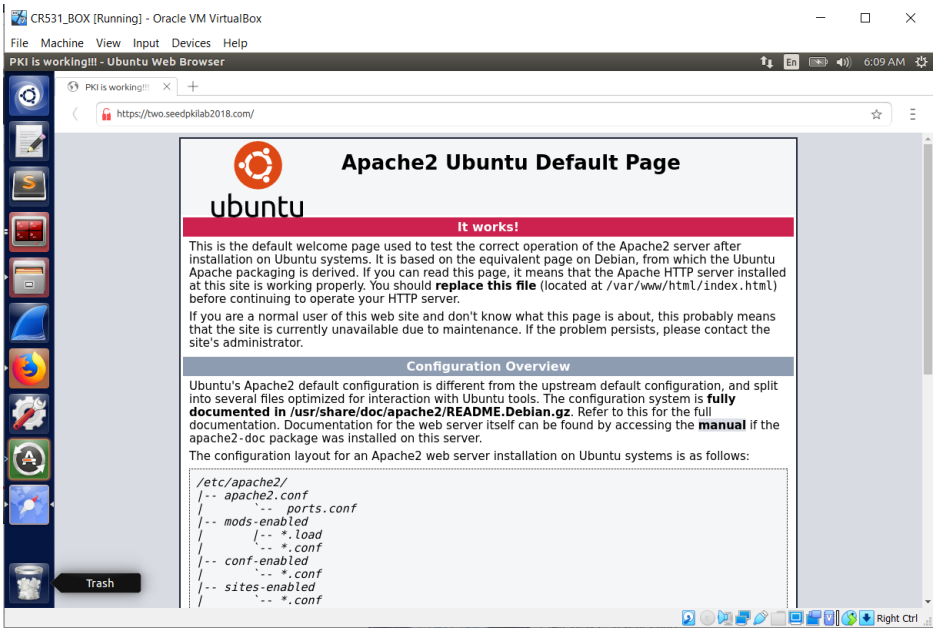
Adding index.html to “seedpki” folder just by changing the title of the page



Now performing below actions

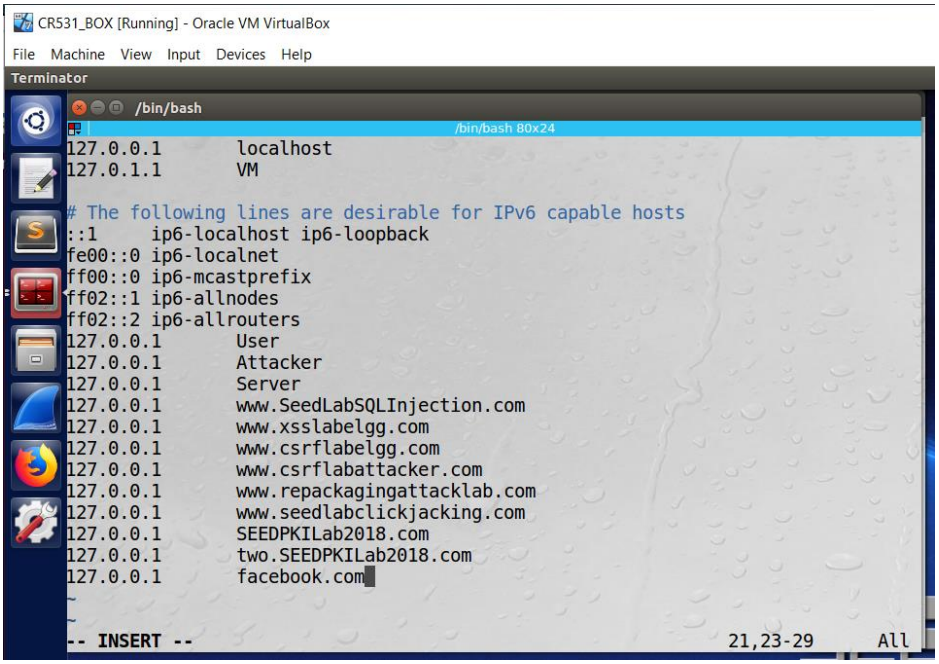


Output: **From the below screenshot we can see the title of the page is “PKI is working!!!”**

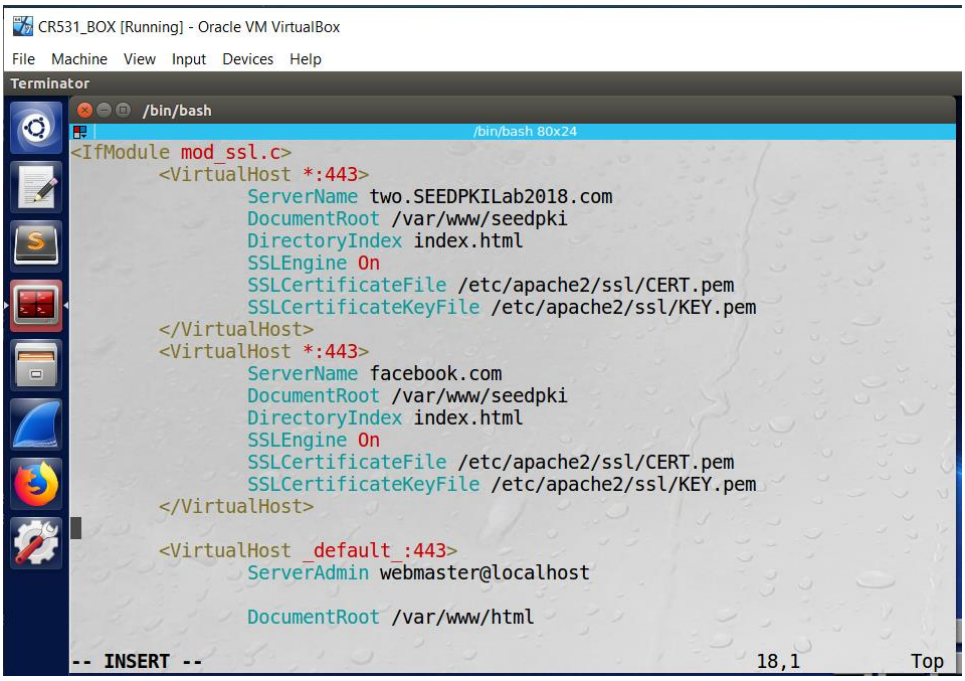


Task 5: Launching a Man-In-The-Middle Attack

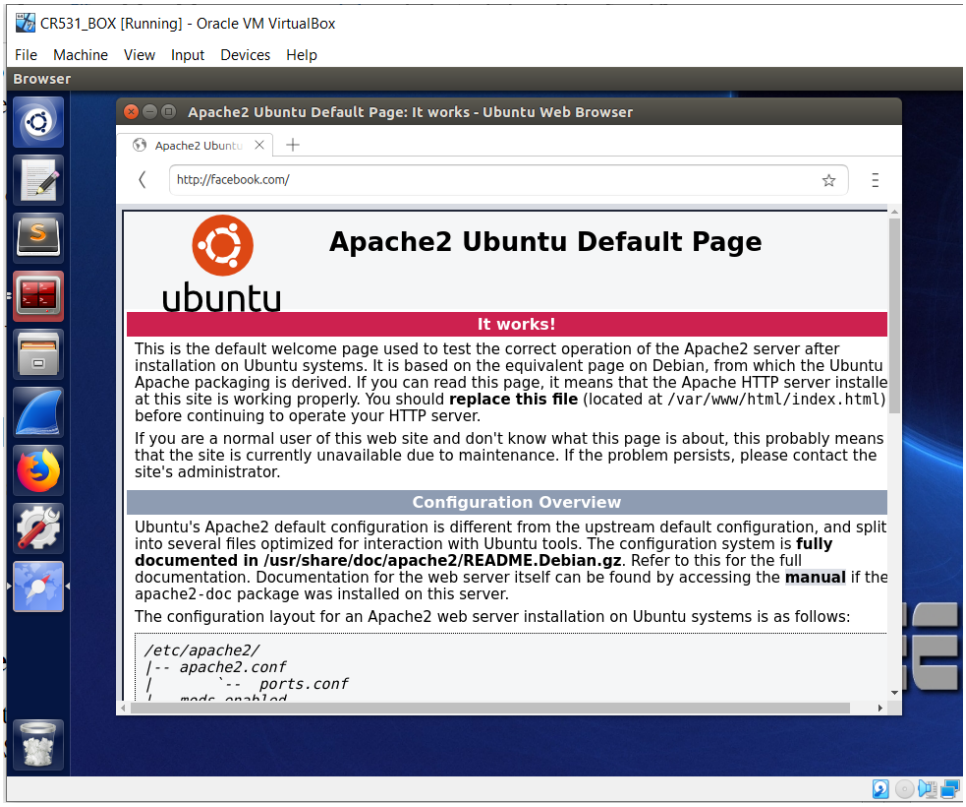
Adding 127.0.0.1 facebook.com to /etc/hosts



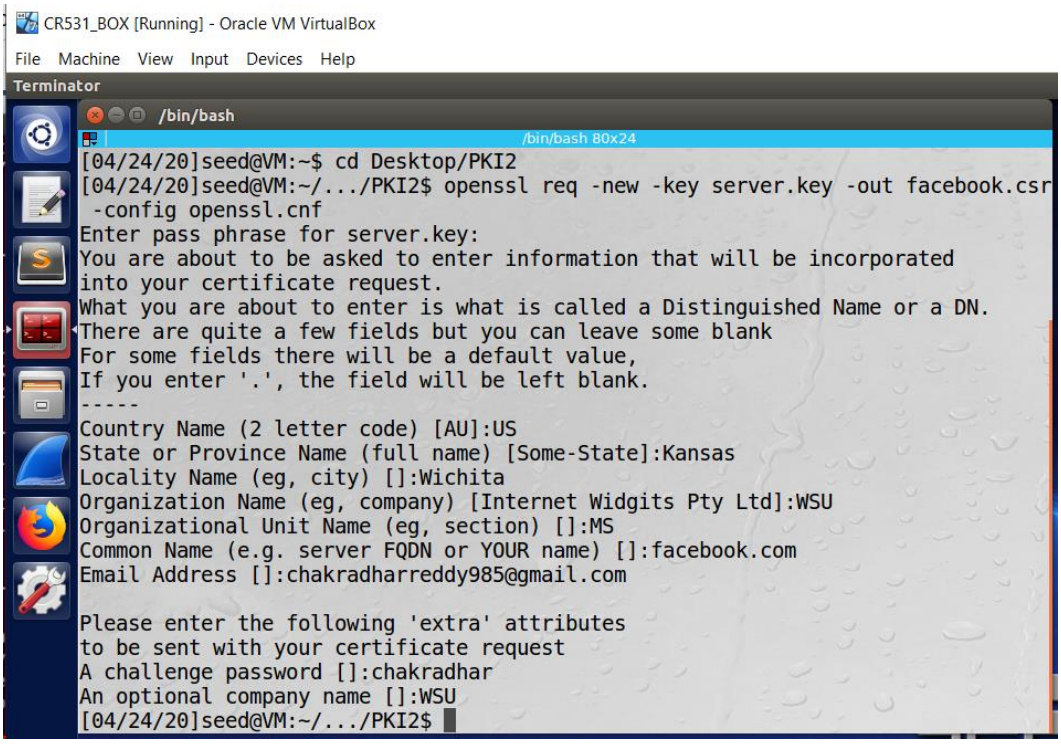
Now, adding the VirtualHost code snippet to /etc/apache2/sites-available/default-ssl.conf

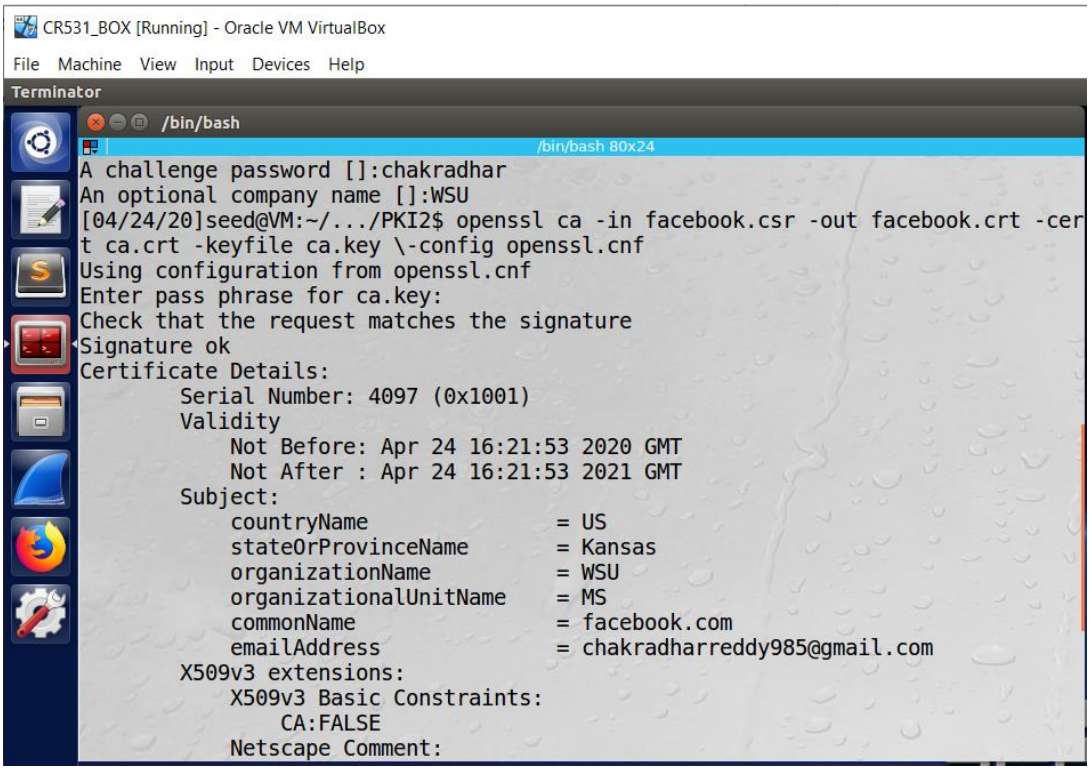


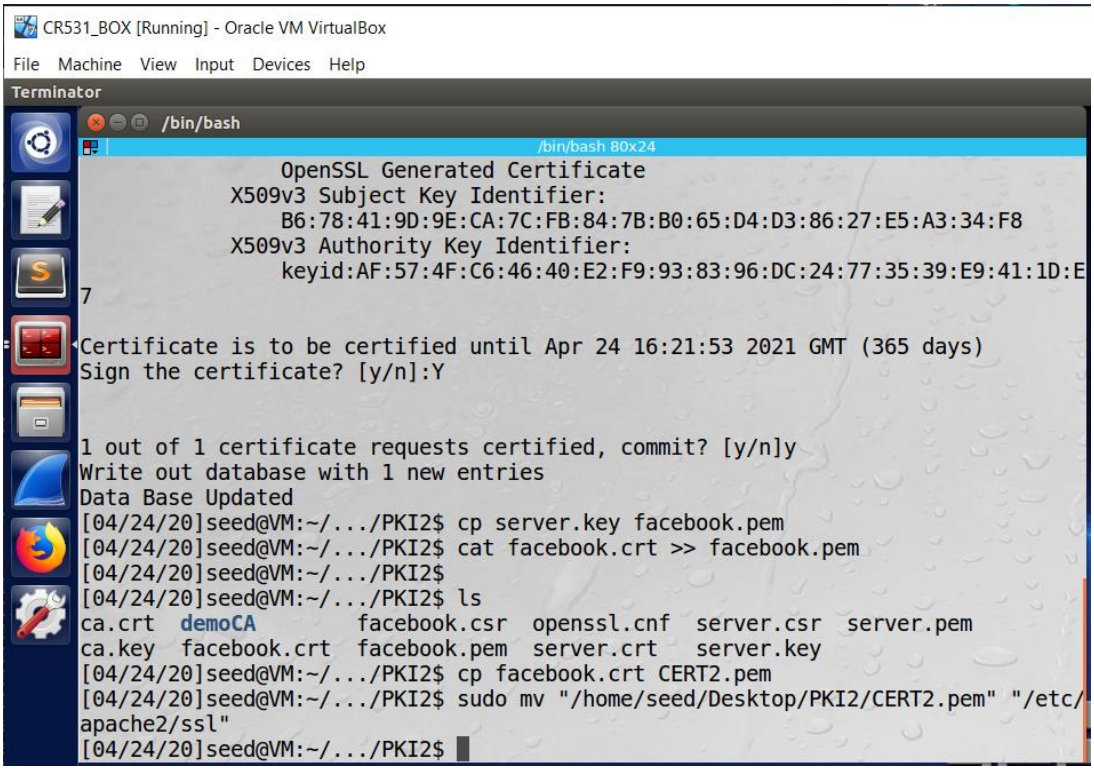
Now, open browser and type facebook.com and see the output.



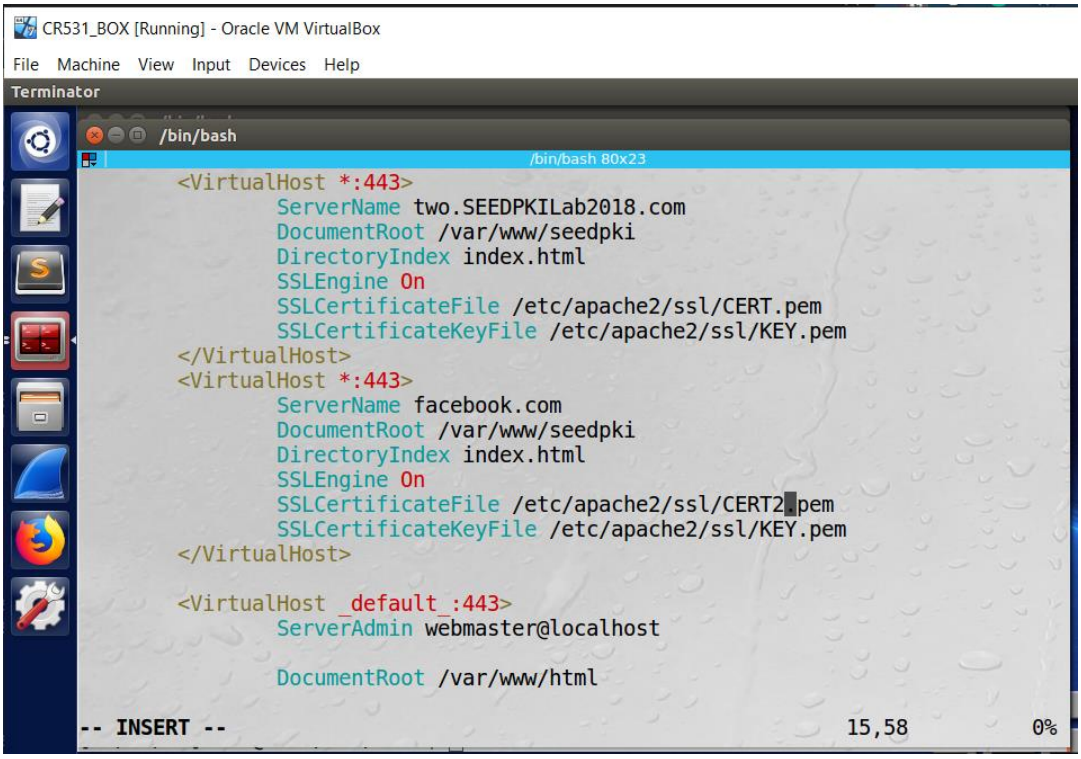
Task 6: Launching a Man-In-The-Middle Attack with a Compromised CA







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



Now, restart the apache service

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.