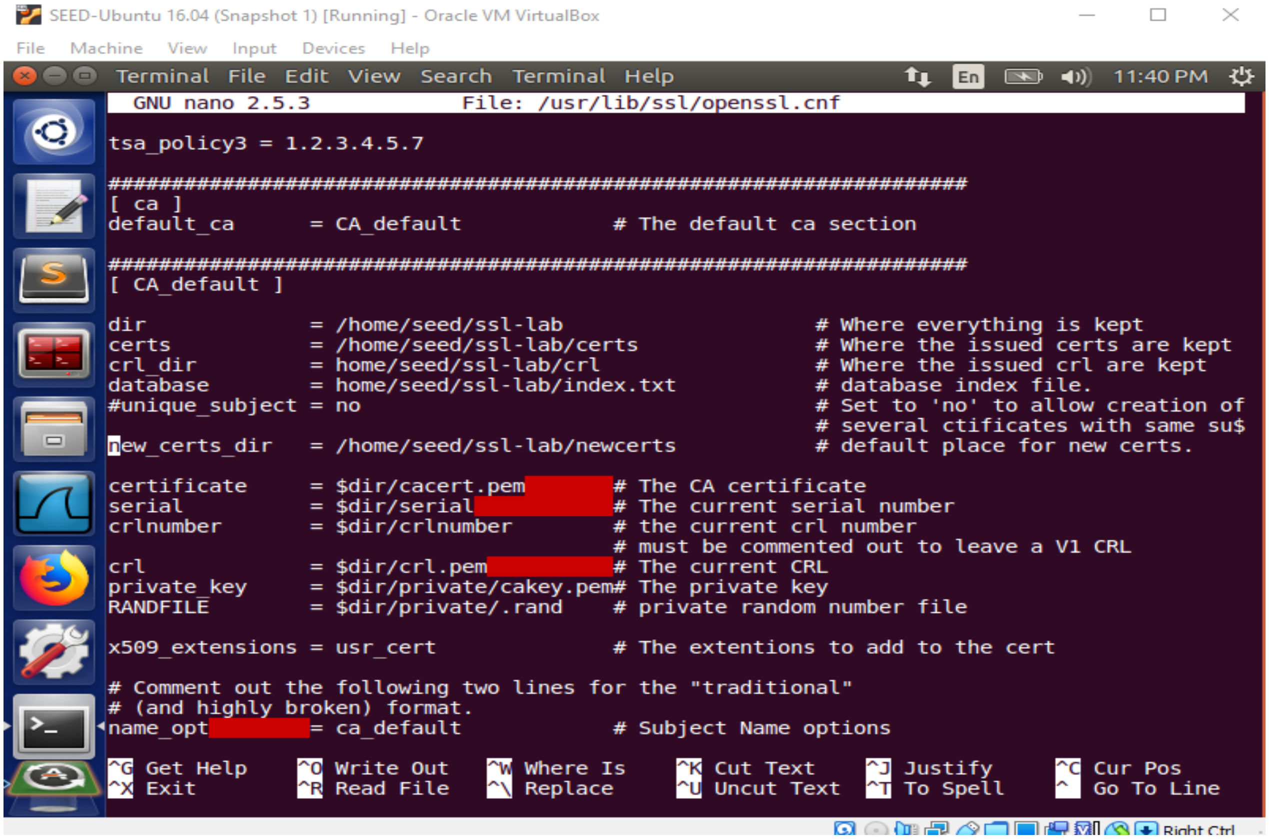
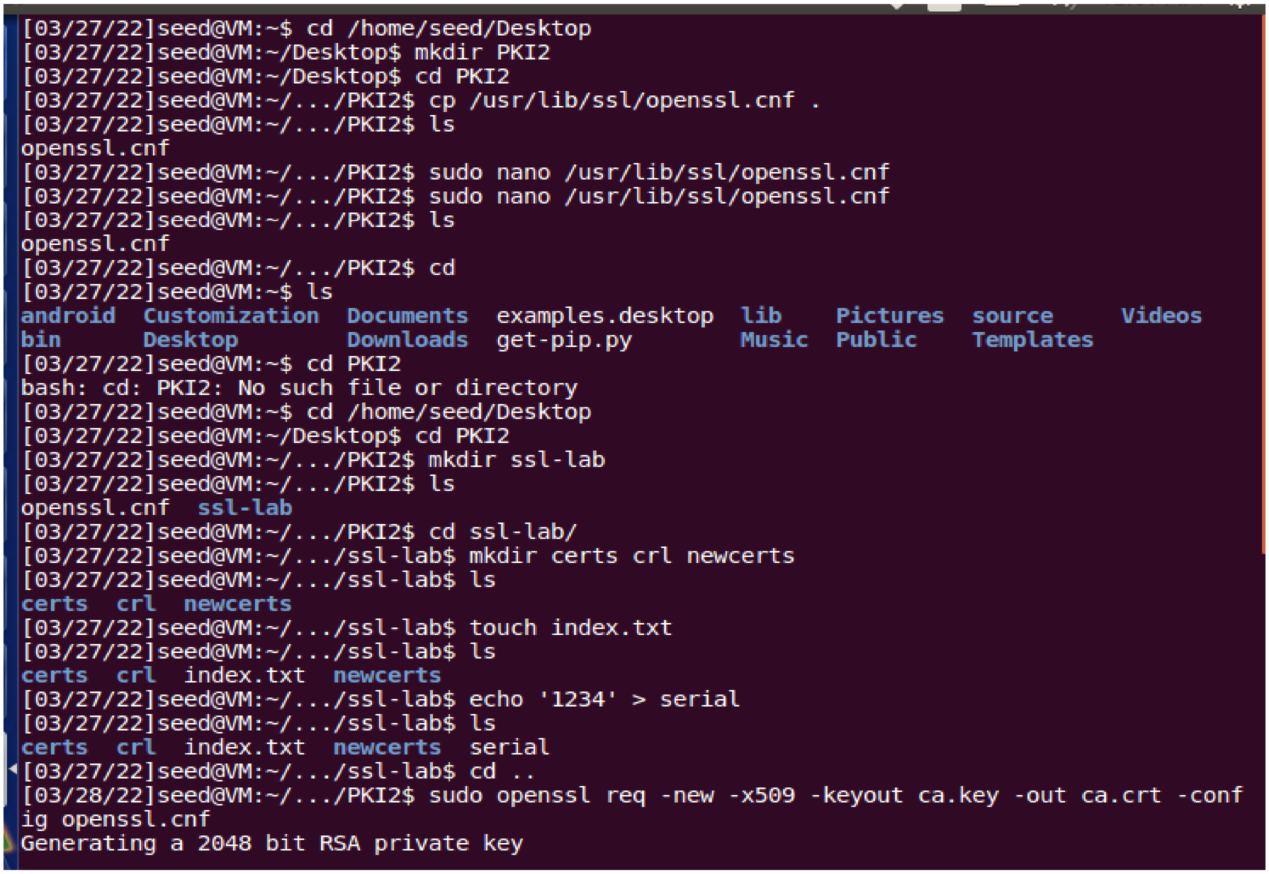
Task 1: Becoming a Certificate Authority (CA)

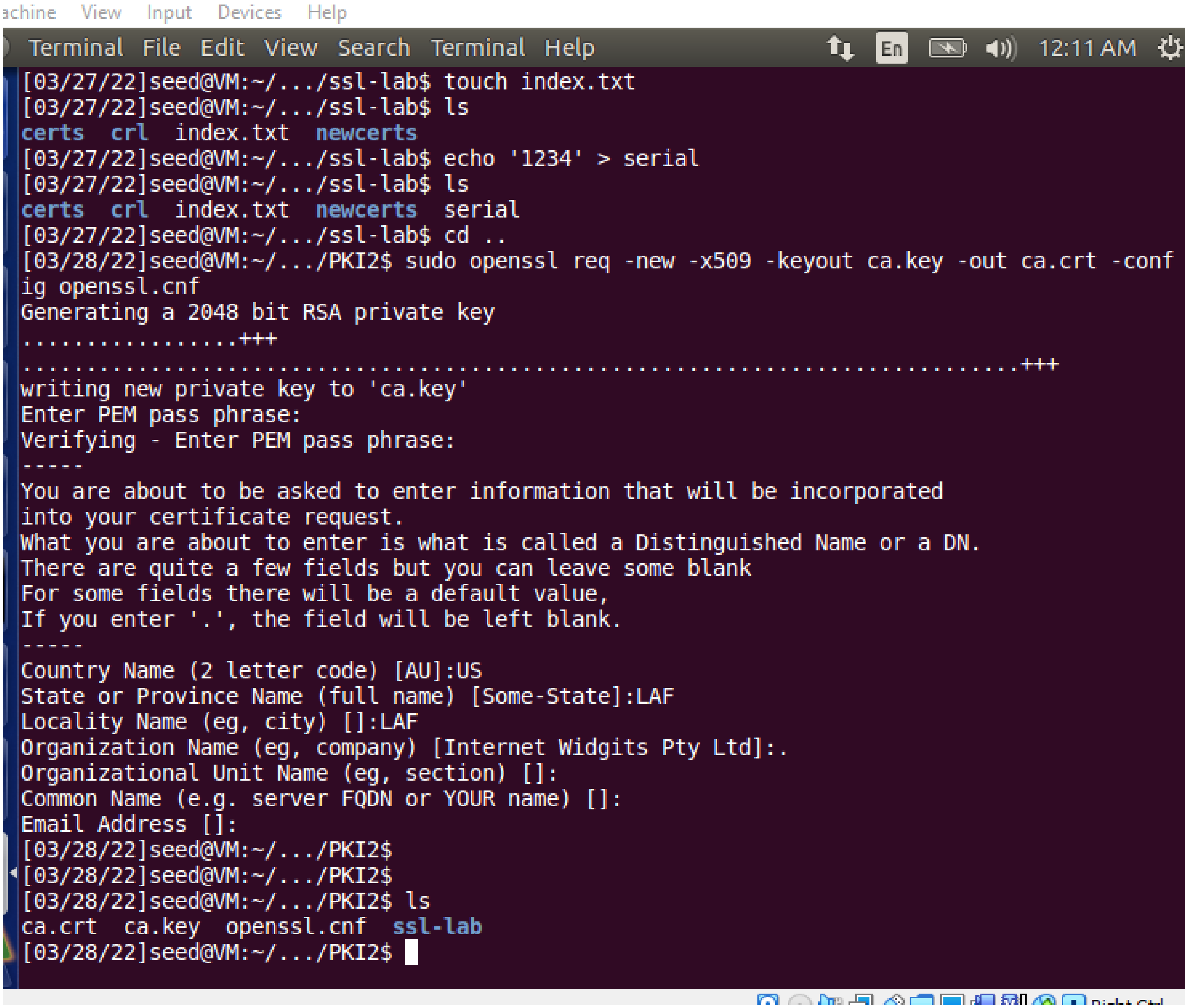


SEED-Ubuntu 16.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
En
11:40 PM
Right Ctrl

```
  GNU nano 2.5.3              File: /usr/lib/ssl/openssl.cnf

tsa_policy3 = 1.2.3.4.5.7

####################################################################
[ ca ]
default_ca      = CA_default            # The default ca section

####################################################################
[ CA_default ]

dir             = /home/seed/ssl-lab                    # Where everything is kept
certs           = /home/seed/ssl-lab/certs              # Where the issued certs are kept
crl_dir         = home/seed/ssl-lab/crl                 # Where the issued crl are kept
database        = home/seed/ssl-lab/index.txt           # database index file.
#unique_subject = no                                    # Set to 'no' to allow creation of
                                                        # several ctificates with same su$
new_certs_dir   = /home/seed/ssl-lab/newcerts           # default place for new certs.

certificate     = $dir/cacert.pem[redacted]# The CA certificate
serial          = $dir/serial[redacted]# The current serial number
crlnumber       = $dir/crlnumber        # the current crl number
                                        # must be commented out to leave a V1 CRL
crl             = $dir/crl.pem[redacted]# The current CRL
private_key     = $dir/private/cakey.pem# The private key
RANDFILE        = $dir/private/.rand    # private random number file

x509_extensions = usr_cert              # The extentions to add to the cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt[redacted]= ca_default          # Subject Name options

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line
```



```
[03/27/22]seed@VM:~$ cd /home/seed/Desktop
[03/27/22]seed@VM:~/Desktop$ mkdir PKI2
[03/27/22]seed@VM:~/Desktop$ cd PKI2
[03/27/22]seed@VM:~/.../PKI2$ cp /usr/lib/ssl/openssl.cnf .
[03/27/22]seed@VM:~/.../PKI2$ ls
openssl.cnf
[03/27/22]seed@VM:~/.../PKI2$ sudo nano /usr/lib/ssl/openssl.cnf
[03/27/22]seed@VM:~/.../PKI2$ sudo nano /usr/lib/ssl/openssl.cnf
[03/27/22]seed@VM:~/.../PKI2$ ls
openssl.cnf
[03/27/22]seed@VM:~/.../PKI2$ cd
[03/27/22]seed@VM:~$ ls
android  Customization  Documents  examples.desktop  lib    Pictures  source     Videos
bin      Desktop        Downloads  get-pip.py        Music  Public    Templates
[03/27/22]seed@VM:~$ cd PKI2
bash: cd: PKI2: No such file or directory
[03/27/22]seed@VM:~$ cd /home/seed/Desktop
[03/27/22]seed@VM:~/Desktop$ cd PKI2
[03/27/22]seed@VM:~/.../PKI2$ mkdir ssl-lab
[03/27/22]seed@VM:~/.../PKI2$ ls
openssl.cnf  ssl-lab
[03/27/22]seed@VM:~/.../PKI2$ cd ssl-lab/
[03/27/22]seed@VM:~/.../ssl-lab$ mkdir certs crl newcerts
[03/27/22]seed@VM:~/.../ssl-lab$ ls
certs  crl  newcerts
[03/27/22]seed@VM:~/.../ssl-lab$ touch index.txt
[03/27/22]seed@VM:~/.../ssl-lab$ ls
certs  crl  index.txt  newcerts
[03/27/22]seed@VM:~/.../ssl-lab$ echo '1234' > serial
[03/27/22]seed@VM:~/.../ssl-lab$ ls
certs  crl  index.txt  newcerts  serial
[03/27/22]seed@VM:~/.../ssl-lab$ cd ..
[03/28/22]seed@VM:~/.../PKI2$ sudo openssl req -new -x509 -keyout ca.key -out ca.crt -conf
ig openssl.cnf
Generating a 2048 bit RSA private key
```



achine View Input Devices Help
Terminal File Edit View Search Terminal Help
En
12:11 AM
Right Ctrl

```
[03/27/22]seed@VM:~/.../ssl-lab$ touch index.txt
[03/27/22]seed@VM:~/.../ssl-lab$ ls
certs  crl  index.txt  newcerts
[03/27/22]seed@VM:~/.../ssl-lab$ echo '1234' > serial
[03/27/22]seed@VM:~/.../ssl-lab$ ls
certs  crl  index.txt  newcerts  serial
[03/27/22]seed@VM:~/.../ssl-lab$ cd ..
[03/28/22]seed@VM:~/.../PKI2$ sudo openssl req -new -x509 -keyout ca.key -out ca.crt -conf
ig 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]:LAF
Locality Name (eg, city) []:LAF
Organization Name (eg, company) [Internet Widgits Pty Ltd]:.
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
[03/28/22]seed@VM:~/.../PKI2$
[03/28/22]seed@VM:~/.../PKI2$
[03/28/22]seed@VM:~/.../PKI2$ ls
ca.crt  ca.key  openssl.cnf  ssl-lab
[03/28/22]seed@VM:~/.../PKI2$
```

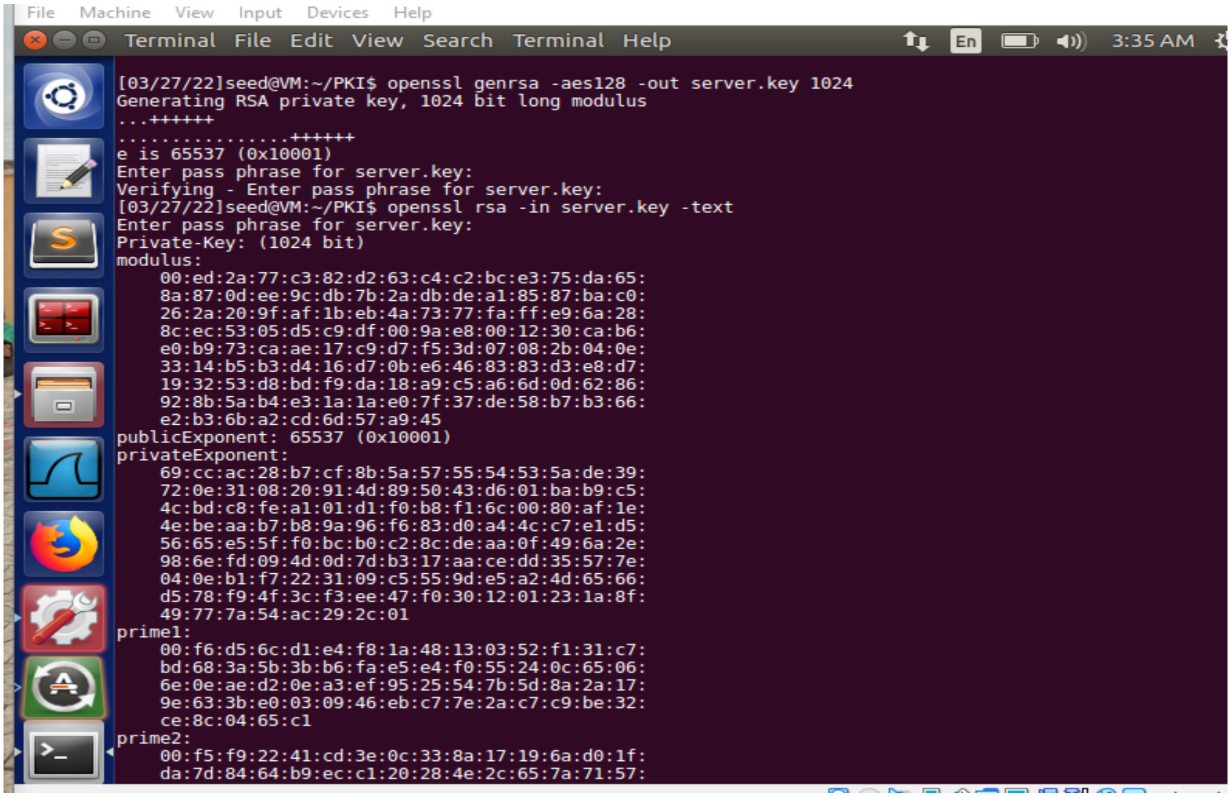
The below command was run:
$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf to generate the self-signed certificate for the CA.

Information and a password were prompted – These were filled, and password

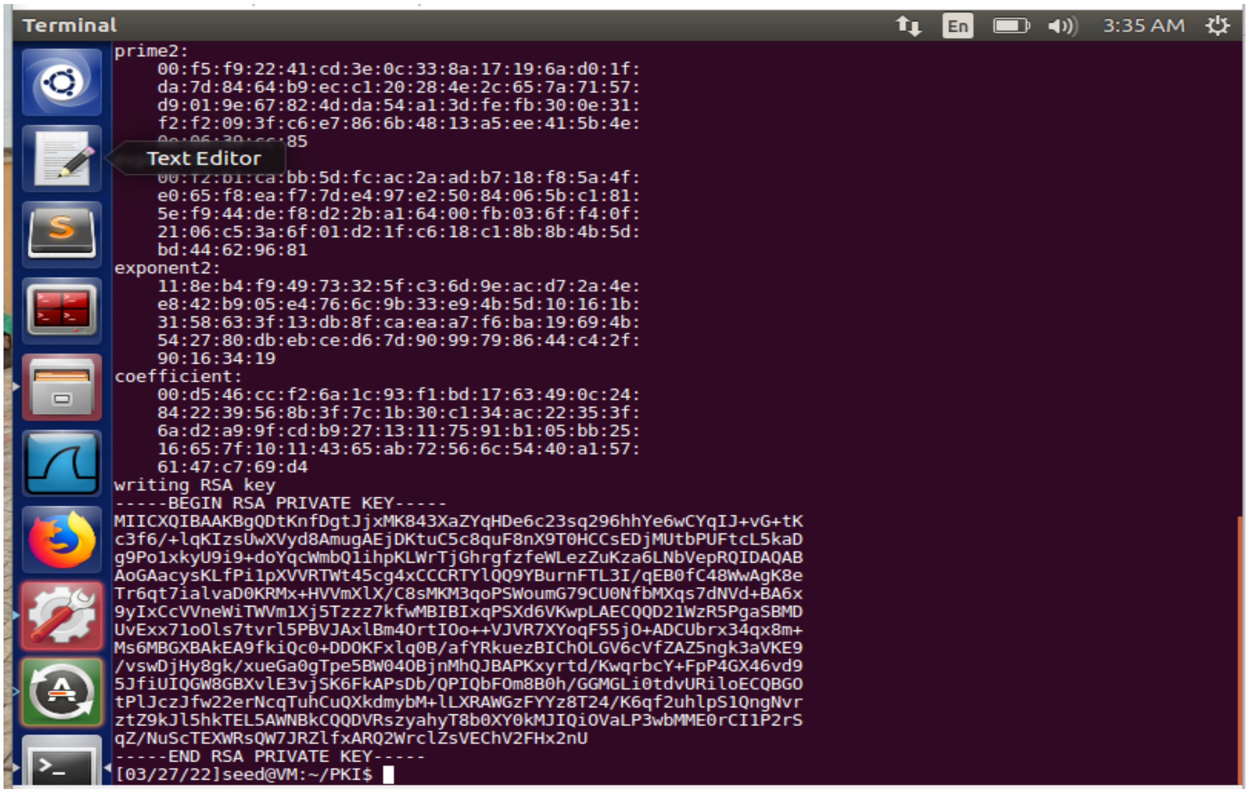
The outputs of the command were stored in two files: ***ca.key*** and ***ca.crt***

The file ca.key contains the CA's private key, while ca.crt contains the public-key certificate.

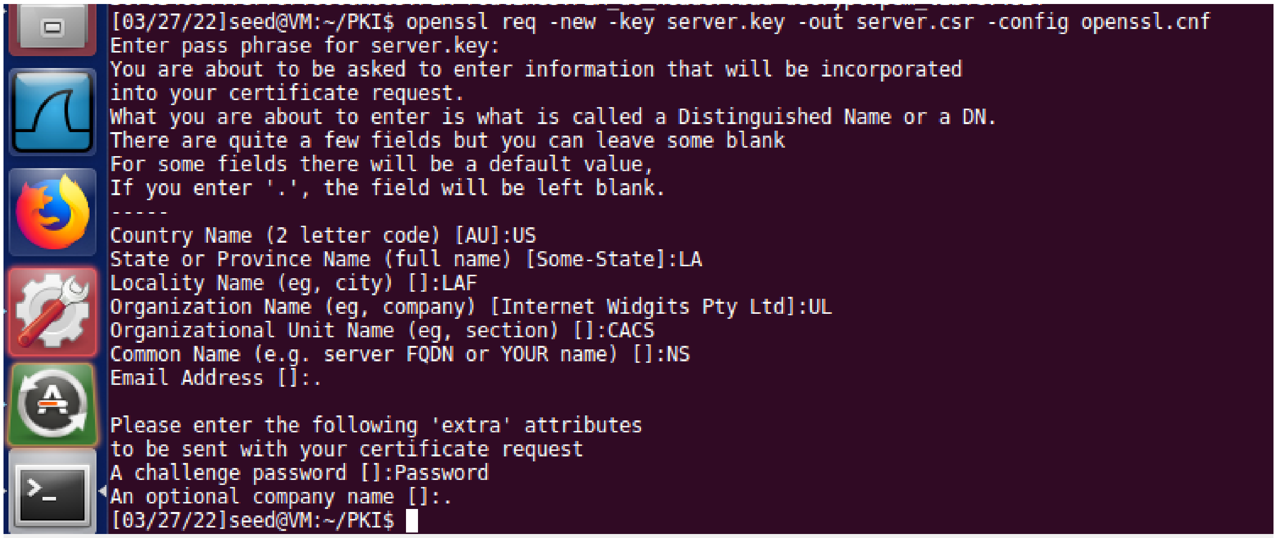
Task 2: Creating a Certificate for *SEEDPKILab2020.com*



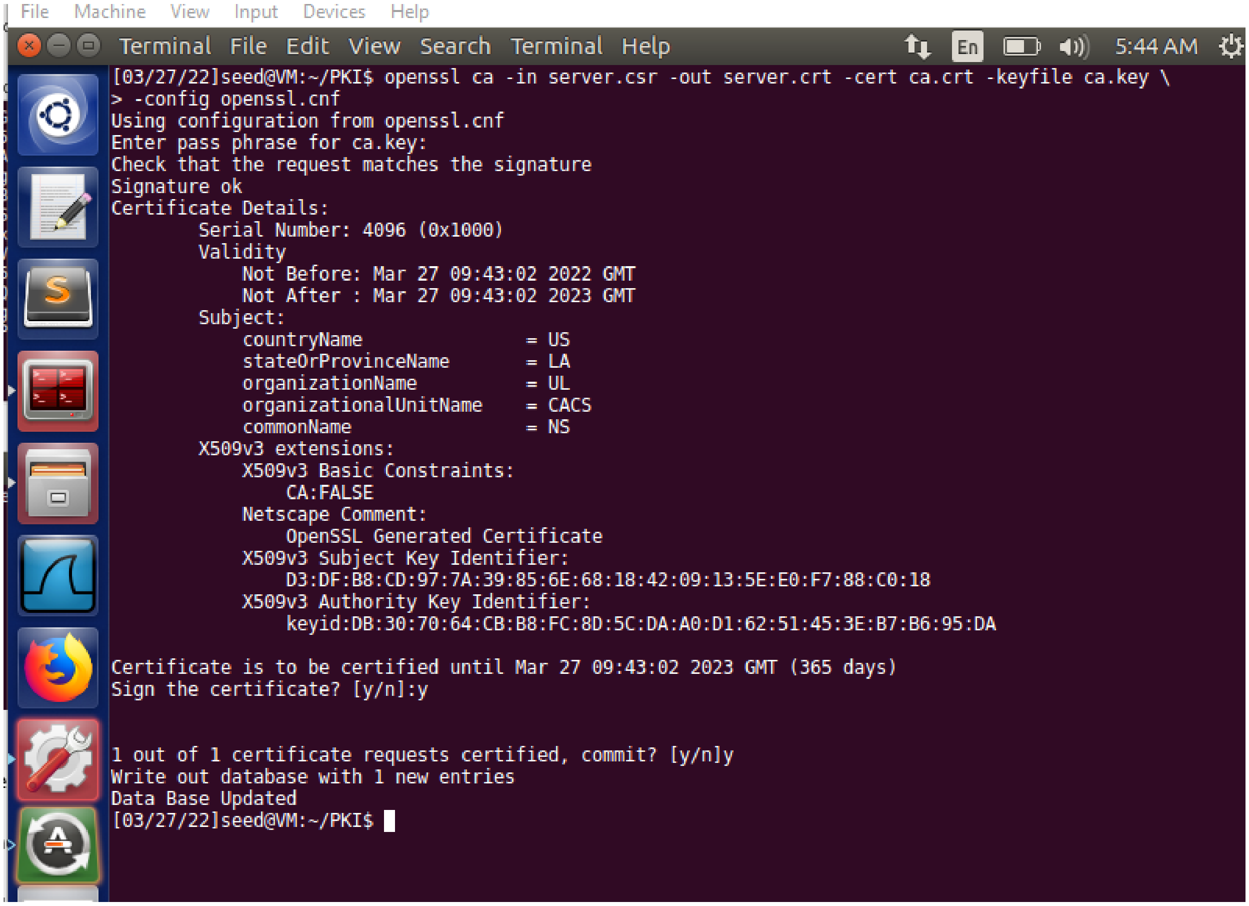
```
[03/27/22]seed@VM:~/PKI$ openssl genrsa -aes128 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
...++++++
................++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
[03/27/22]seed@VM:~/PKI$ openssl rsa -in server.key -text
Enter pass phrase for server.key:
Private-Key: (1024 bit)
modulus:
    00:ed:2a:77:c3:82:d2:63:c4:c2:bc:e3:75:da:65:
    8a:87:0d:ee:9c:db:7b:2a:db:de:a1:85:87:ba:c0:
    26:2a:20:9f:af:1b:eb:4a:73:77:fa:ff:e9:6a:28:
    8c:ec:53:05:d5:c9:df:00:9a:e8:00:12:30:ca:b6:
    e0:b9:73:ca:ae:17:c9:d7:f5:3d:07:08:2b:04:0e:
    33:14:b5:b3:d4:16:d7:0b:e6:46:83:83:d3:e8:d7:
    19:32:53:d8:bd:f9:da:18:a9:c5:a6:6d:0d:62:86:
    92:8b:5a:b4:e3:1a:1a:e0:7f:37:de:58:b7:b3:66:
    e2:b3:6b:a2:cd:6d:57:a9:45
publicExponent: 65537 (0x10001)
privateExponent:
    69:cc:ac:28:b7:cf:8b:5a:57:55:54:53:5a:de:39:
    72:0e:31:08:20:91:4d:89:50:43:d6:01:ba:b9:c5:
    4c:bd:c8:fe:a1:01:d1:f0:b8:f1:6c:00:80:af:1e:
    4e:be:aa:b7:b8:9a:96:f6:83:d0:a4:4c:c7:e1:d5:
    56:65:e5:5f:f0:bc:b0:c2:8c:de:aa:0f:49:6a:2e:
    98:6e:fd:09:4d:0d:7d:b3:17:aa:ce:dd:35:57:7e:
    04:0e:b1:f7:22:31:09:c5:55:9d:e5:a2:4d:65:66:
    d5:78:f9:4f:3c:f3:ee:47:f0:30:12:01:23:1a:8f:
    49:77:7a:54:ac:29:2c:01
prime1:
    00:f6:d5:6c:d1:e4:f8:1a:48:13:03:52:f1:31:c7:
    bd:68:3a:5b:3b:b6:fa:e5:e4:f0:55:24:0c:65:06:
    6e:0e:ae:d2:0e:a3:ef:95:25:54:7b:5d:8a:2a:17:
    9e:63:3b:e0:03:09:46:eb:c7:7e:2a:c7:c9:be:32:
    ce:8c:04:65:c1
prime2:
    00:f5:f9:22:41:cd:3e:0c:33:8a:17:19:6a:d0:1f:
    da:7d:84:64:b9:ec:c1:20:28:4e:2c:65:7a:71:57:
```



```
prime2:
    00:f5:f9:22:41:cd:3e:0c:33:8a:17:19:6a:d0:1f:
    da:7d:84:64:b9:ec:c1:20:28:4e:2c:65:7a:71:57:
    d9:01:9e:67:82:4d:da:54:a1:3d:fe:fb:30:0e:31:
    f2:f2:09:3f:c6:e7:86:6b:48:13:a5:ee:41:5b:4e:
    0e:06:39:cc:85
    00:f2:b1:ca:bb:5d:fc:ac:2a:ad:b7:18:f8:5a:4f:
    e0:65:f8:ea:f7:7d:e4:97:e2:50:84:06:5b:c1:81:
    5e:f9:44:de:f8:d2:2b:a1:64:00:fb:03:6f:f4:0f:
    21:06:c5:3a:6f:01:d2:1f:c6:18:c1:8b:8b:4b:5d:
    bd:44:62:96:81
exponent2:
    11:8e:b4:f9:49:73:32:5f:c3:6d:9e:ac:d7:2a:4e:
    e8:42:b9:05:e4:76:6c:9b:33:e9:4b:5d:10:16:1b:
    31:58:63:3f:13:db:8f:ca:ea:a7:f6:ba:19:69:4b:
    54:27:80:db:eb:ce:d6:7d:90:99:79:86:44:c4:2f:
    90:16:34:19
coefficient:
    00:d5:46:cc:f2:6a:1c:93:f1:bd:17:63:49:0c:24:
    84:22:39:56:8b:3f:7c:1b:30:c1:34:ac:22:35:3f:
    6a:d2:a9:9f:cd:b9:27:13:11:75:91:b1:05:bb:25:
    16:65:7f:10:11:43:65:ab:72:56:6c:54:40:a1:57:
    61:47:c7:69:d4
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDtKnfDgtJjxMK843XaZYqHDe6c23sq296hhYe6wCYqIJ+vG+tK
c3f6/+lqKIzsUwXVyd8AmugAEjDKtuC5c8quF8nX9T0HCCsEDjMUtbPUFtcL5kaD
g9Po1xkyU9i9+doYqcWmbQ1ihpKLWrTjGhrgfzfeWLezZuKza6LNbVepRQIDAQAB
AoGAacysKLfPi1pXVVRTWt45cg4xCCCRTYlQQ9YBurnFTL3I/qEB0fC48WwAgK8e
Tr6qt7ialvaD0KRMx+HVVmXlX/C8sMKM3qoPSWoumG79CU0NfbMXqs7dNVd+BA6x
9yIxCcVVneWiTWVm1Xj5Tzzz7kfwMBIBIxqPSXd6VKwpLAECQQD21WzR5PgaSBMD
UvExx71oOls7tvrl5PBVJAxlBm4OrtIOo++VJVR7XYoqF55jO+ADCUbrx34qx8m+
Ms6MBGXBAkEA9fkiQc0+DDOKFxlq0B/afYRkuezBIChOLGV6cVfZAZ5ngk3aVKE9
/vswDjHy8gk/xueGa0gTpe5BW04OBjnMhQJBAPKxyrtd/KwqrbcY+FpP4GX46vd9
5JfiUIQGW8GBXvlE3vjSK6FkAPsDb/QPIQbFOm8B0h/GGMGLi0tdvURiloECQBGO
tPlJczJfw22erNcqTuhCuQXkdmybM+lLXRAWGzFYYz8T24/K6qf2uhlpS1QngNvr
ztZ9kJl5hkTEL5AWNBkCQQDVRszyahyT8b0XY0kMJIQiOVaLP3wbMME0rCI1P2rS
qZ/NuScTEXWRsQW7JRZlfxARQ2WrclZsVEChV2FHx2nU
-----END RSA PRIVATE KEY-----
[03/27/22]seed@VM:~/PKI$
```



```
[03/27/22]seed@VM:~/PKI$ 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]:LA
Locality Name (eg, city) []:LAF
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UL
Organizational Unit Name (eg, section) []:CACS
Common Name (e.g. server FQDN or YOUR name) []:NS
Email Address []:.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Password
An optional company name []:.
[03/27/22]seed@VM:~/PKI$ 
```

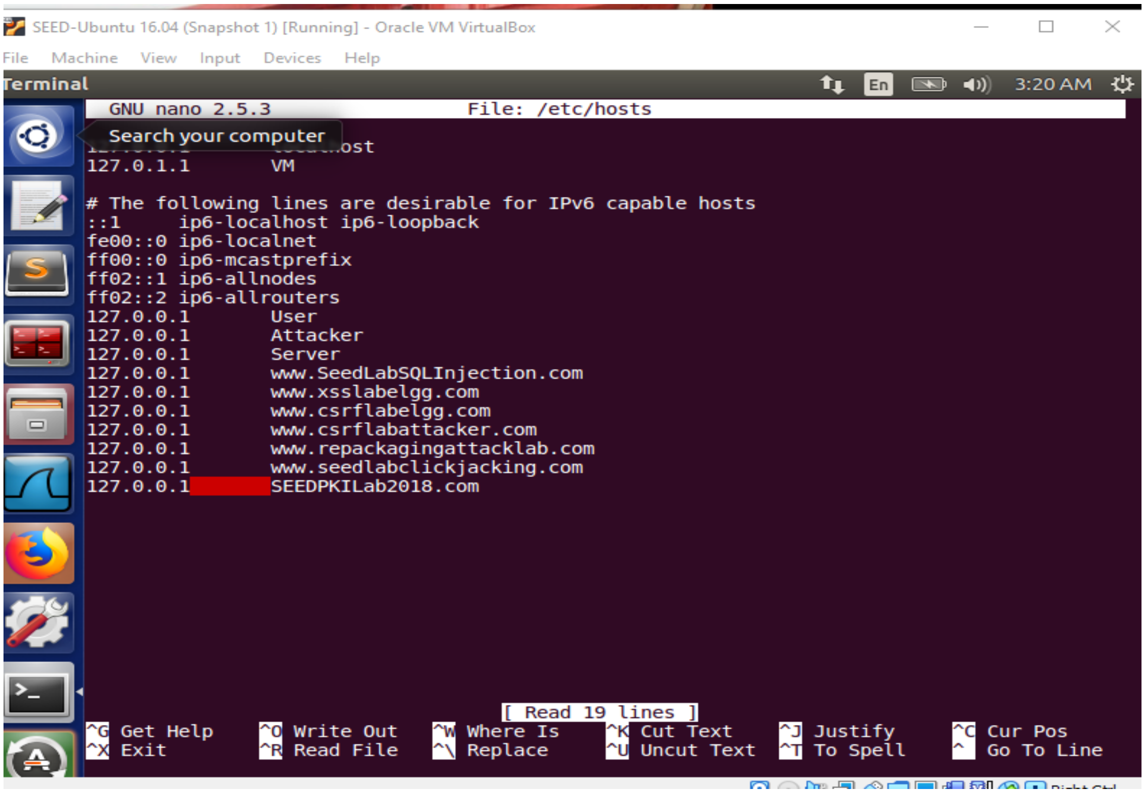

File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
En
5:44 AM

```
[03/27/22]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: Mar 27 09:43:02 2022 GMT
            Not After : Mar 27 09:43:02 2023 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = LA
            organizationName          = UL
            organizationalUnitName    = CACS
            commonName                = NS
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                D3:DF:B8:CD:97:7A:39:85:6E:68:18:42:09:13:5E:E0:F7:88:C0:18
            X509v3 Authority Key Identifier:
                keyid:DB:30:70:64:CB:B8:FC:8D:5C:DA:A0:D1:62:51:45:3E:B7:B6:95:DA

Certificate is to be certified until Mar 27 09:43:02 2023 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
[03/27/22]seed@VM:~/PKI$ 
```

The following command was run to generate an RSA key pair (both private and public keys):
$ openssl genrsa -aes128 -out server.key 1024.
A password was provided to encrypt the private key ***which was*** stored in the file server.key

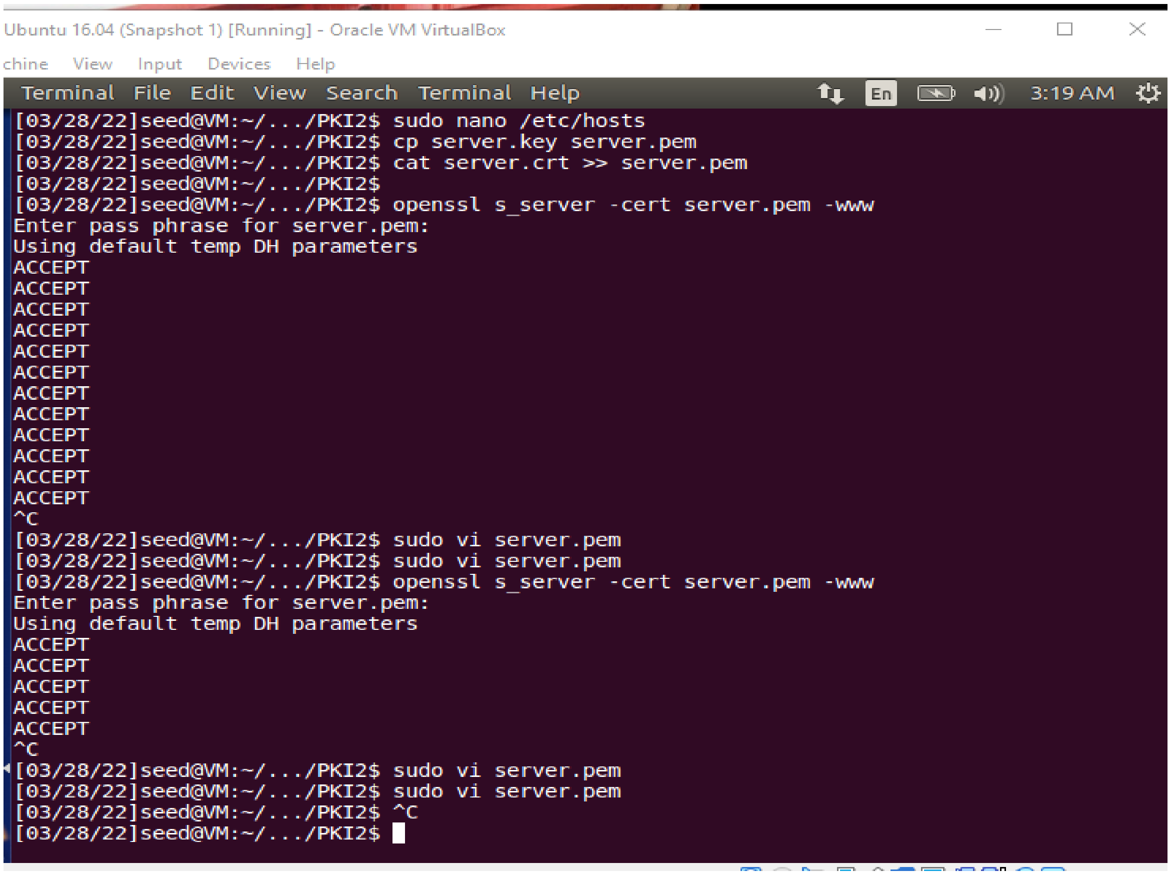
The company generated a Certificate Signing Request (CSR), which basically includes the company's public key. The CSR was sent to the CA, who generated a certificate for the key.
The trusted CA created in Task 1 was used generate certificate using its signature.

Task 3: Deploying Certificate in an HTTPSWeb Server

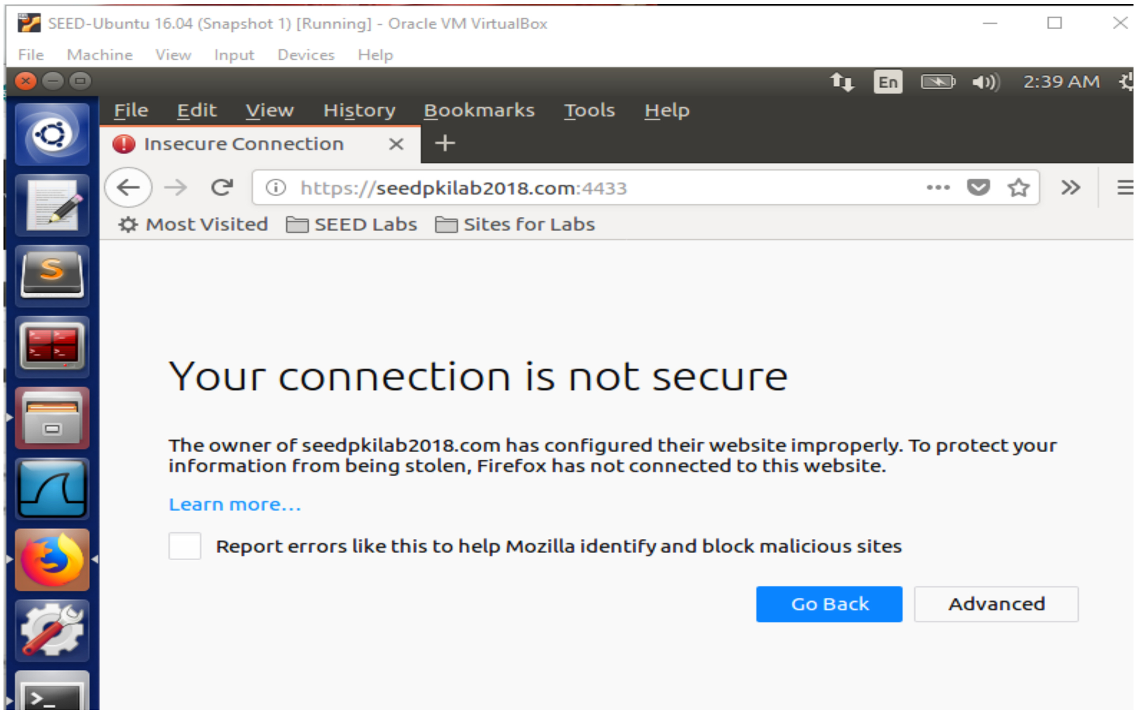

SEED-Ubuntu 16.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
En
3:20 AM
Search your computer

```
  GNU nano 2.5.3                 File: /etc/hosts

                ost
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.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
127.0.0.1[redacted]SEEDPKILab2018.com

                                   [ Read 19 lines ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line
```

Adding the entry: SEEDPKILab2018.com to /etc/hosts, in other to map the hostname SEEDPKILab2020.com to our localhost (i.e., 127.0.0.1):


Ubuntu 16.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
chine View Input Devices Help
Terminal File Edit View Search Terminal Help
En
3:19 AM

```
[03/28/22]seed@VM:~/.../PKI2$ sudo nano /etc/hosts
[03/28/22]seed@VM:~/.../PKI2$ cp server.key server.pem
[03/28/22]seed@VM:~/.../PKI2$ cat server.crt >> server.pem
[03/28/22]seed@VM:~/.../PKI2$
[03/28/22]seed@VM:~/.../PKI2$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
^C
[03/28/22]seed@VM:~/.../PKI2$ sudo vi server.pem
[03/28/22]seed@VM:~/.../PKI2$ sudo vi server.pem
[03/28/22]seed@VM:~/.../PKI2$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
^C
[03/28/22]seed@VM:~/.../PKI2$ sudo vi server.pem
[03/28/22]seed@VM:~/.../PKI2$ sudo vi server.pem
[03/28/22]seed@VM:~/.../PKI2$ ^C
[03/28/22]seed@VM:~/.../PKI2$ 
```



SEED-Ubuntu 16.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
En
2:39 AM
File Edit View History Bookmarks Tools Help
Insecure Connection
https://seedpkilab2018.com:4433
Most Visited
SEED Labs
Sites for Labs
Go Back
Advanced

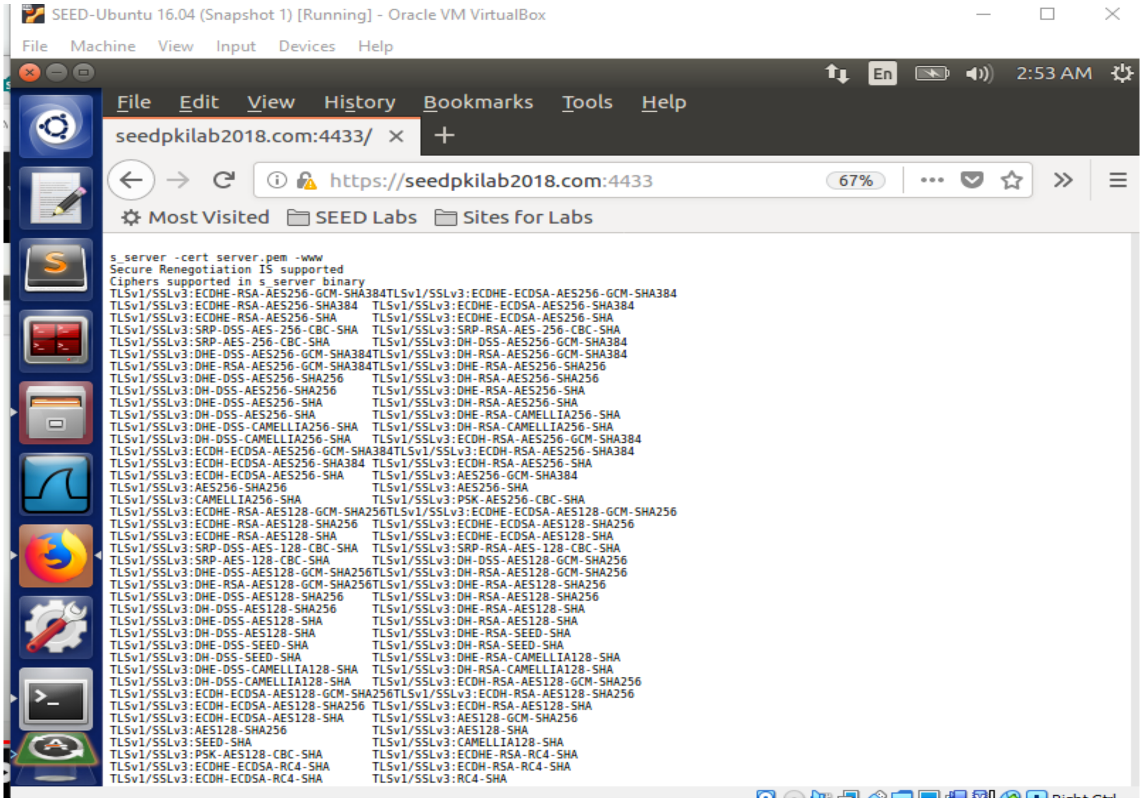
Your connection is not secure

The owner of seedpkilab2018.com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more…

□ Report errors like this to help Mozilla identify and block malicious sites

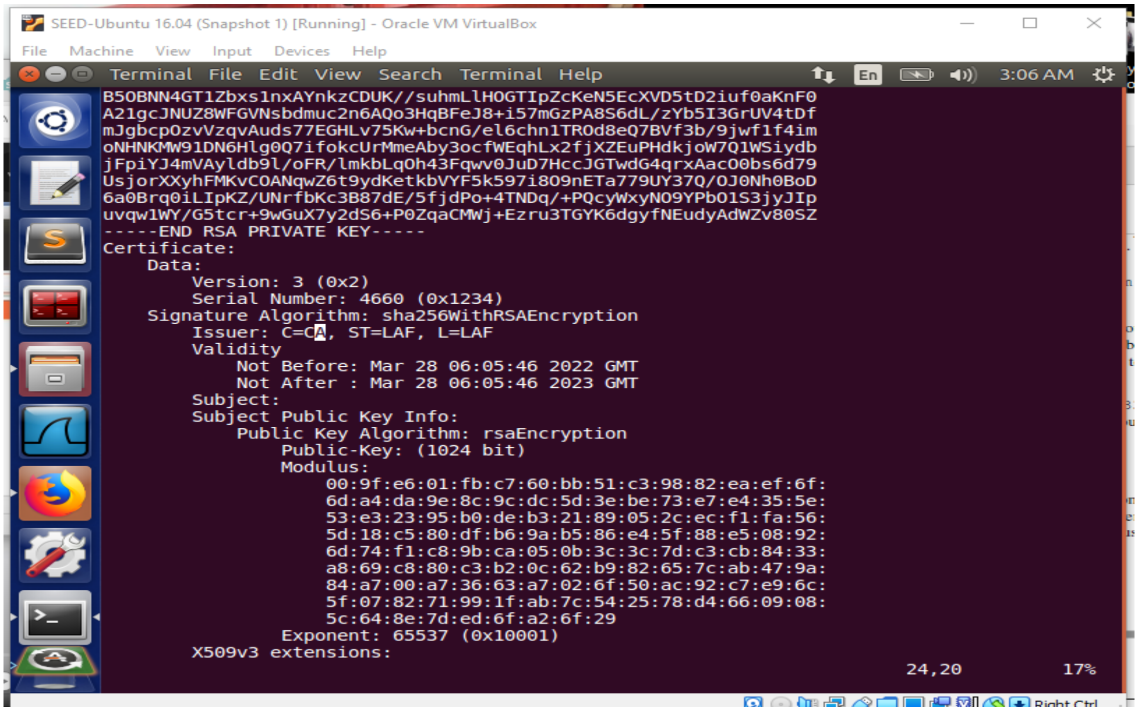
“Your connection is not secure” was displayed.



SEED-Ubuntu 16.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
En
2:53 AM
File Edit View History Bookmarks Tools Help
seedpkilab2018.com:4433/
https://seedpkilab2018.com:4433
67%
Most Visited
SEED Labs
Sites for Labs

```
s_server -cert server.pem -www
Secure Renegotiation IS supported
Ciphers supported in s_server binary
TLSv1/SSLv3:ECDHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDHE-ECDSA-AES256-GCM-SHA384
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA384  TLSv1/SSLv3:ECDHE-ECDSA-AES256-SHA384
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES256-SHA
TLSv1/SSLv3:SRP-DSS-AES-256-CBC-SHA  TLSv1/SSLv3:SRP-RSA-AES-256-CBC-SHA
TLSv1/SSLv3:SRP-AES-256-CBC-SHA      TLSv1/SSLv3:DH-DSS-AES256-GCM-SHA384
TLSv1/SSLv3:DHE-DSS-AES256-GCM-SHA384TLSv1/SSLv3:DH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3:DHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:DHE-RSA-AES256-SHA256
TLSv1/SSLv3:DHE-DSS-AES256-SHA256    TLSv1/SSLv3:DH-RSA-AES256-SHA256
TLSv1/SSLv3:DH-DSS-AES256-SHA256     TLSv1/SSLv3:DHE-RSA-AES256-SHA
TLSv1/SSLv3:DHE-DSS-AES256-SHA       TLSv1/SSLv3:DH-RSA-AES256-SHA
TLSv1/SSLv3:DH-DSS-AES256-SHA        TLSv1/SSLv3:DHE-RSA-CAMELLIA256-SHA
TLSv1/SSLv3:DHE-DSS-CAMELLIA256-SHA  TLSv1/SSLv3:DH-RSA-CAMELLIA256-SHA
TLSv1/SSLv3:DH-DSS-CAMELLIA256-SHA   TLSv1/SSLv3:ECDH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3:ECDH-ECDSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDH-RSA-AES256-SHA384
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA384 TLSv1/SSLv3:ECDH-RSA-AES256-SHA
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA    TLSv1/SSLv3:AES256-GCM-SHA384
TLSv1/SSLv3:AES256-SHA256            TLSv1/SSLv3:AES256-SHA
TLSv1/SSLv3:CAMELLIA256-SHA          TLSv1/SSLv3:PSK-AES256-CBC-SHA
TLSv1/SSLv3:ECDHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:ECDHE-ECDSA-AES128-GCM-SHA256
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA256  TLSv1/SSLv3:ECDHE-ECDSA-AES128-SHA256
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES128-SHA
TLSv1/SSLv3:SRP-DSS-AES-128-CBC-SHA  TLSv1/SSLv3:SRP-RSA-AES-128-CBC-SHA
TLSv1/SSLv3:SRP-AES-128-CBC-SHA      TLSv1/SSLv3:DH-DSS-AES128-GCM-SHA256
TLSv1/SSLv3:DHE-DSS-AES128-GCM-SHA256TLSv1/SSLv3:DH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3:DHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:DHE-RSA-AES128-SHA256
TLSv1/SSLv3:DHE-DSS-AES128-SHA256    TLSv1/SSLv3:DH-RSA-AES128-SHA256
TLSv1/SSLv3:DH-DSS-AES128-SHA256     TLSv1/SSLv3:DHE-RSA-AES128-SHA
TLSv1/SSLv3:DHE-DSS-AES128-SHA       TLSv1/SSLv3:DH-RSA-AES128-SHA
TLSv1/SSLv3:DH-DSS-AES128-SHA        TLSv1/SSLv3:DHE-RSA-SEED-SHA
TLSv1/SSLv3:DHE-DSS-SEED-SHA         TLSv1/SSLv3:DH-RSA-SEED-SHA
TLSv1/SSLv3:DH-DSS-SEED-SHA          TLSv1/SSLv3:DHE-RSA-CAMELLIA128-SHA
TLSv1/SSLv3:DHE-DSS-CAMELLIA128-SHA  TLSv1/SSLv3:DH-RSA-CAMELLIA128-SHA
TLSv1/SSLv3:DH-DSS-CAMELLIA128-SHA   TLSv1/SSLv3:ECDH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3:ECDH-ECDSA-AES128-GCM-SHA256TLSv1/SSLv3:ECDH-RSA-AES128-SHA256
TLSv1/SSLv3:ECDH-ECDSA-AES128-SHA256 TLSv1/SSLv3:ECDH-RSA-AES128-SHA
TLSv1/SSLv3:ECDH-ECDSA-AES128-SHA    TLSv1/SSLv3:AES128-GCM-SHA256
TLSv1/SSLv3:AES128-SHA256            TLSv1/SSLv3:AES128-SHA
TLSv1/SSLv3:SEED-SHA                 TLSv1/SSLv3:CAMELLIA128-SHA
TLSv1/SSLv3:PSK-AES128-CBC-SHA       TLSv1/SSLv3:ECDHE-RSA-RC4-SHA
TLSv1/SSLv3:ECDHE-ECDSA-RC4-SHA      TLSv1/SSLv3:ECDH-RSA-RC4-SHA
TLSv1/SSLv3:ECDH-ECDSA-RC4-SHA       TLSv1/SSLv3:RC4-SHA
```

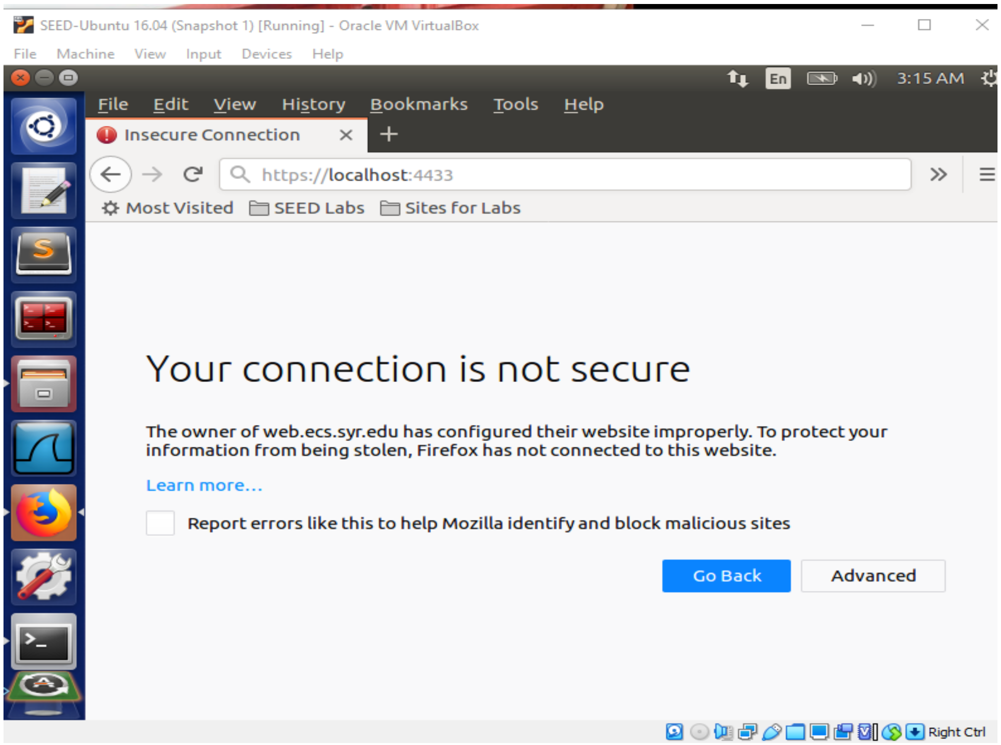
After importing the certificate (ca.crt), and reloading, the site returned information.



SEED-Ubuntu 16.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
En
3:06 AM
Right Ctrl

```
B5OBNN4GT1Zbxs1nxAYnkzCDUK//suhmLlHOGTIpZcKeN5EcXVD5tD2iuf0aKnF0
A21gcJNUZ8WFGVNsbdmuc2n6AQo3HqBFeJ8+i57mGzPA8S6dL/zYb5I3GrUV4tDf
mJgbcpOzvVzqvAuds77EGHLv75Kw+bcnG/el6chn1TROd8eQ7BVf3b/9jwf1f4im
oNHNKMW91DN6Hlg0Q7ifokcUrMmeAby3ocfWEqhLx2fjXZEuPHdkjoW7Q1WSiydb
jFpiYJ4mVAyldb9l/oFR/lmkbLqOh43Fqwv0JuD7HccJGTwdG4qrxAacO0bs6d79
UsjorXXyhFMKvCOANqwZ6t9ydKetkbVYF5k597i8O9nETa779UY37Q/OJ0Nh0BoD
6a0Brq0iLIpKZ/UNrfbKc3B87dE/5fjdPo+4TNDq/+PQcyWxyNO9YPbO1S3jyJIp
uvqw1WY/G5tcr+9wGuX7y2dS6+P0ZqaCMWj+Ezru3TGYK6dgyfNEudyAdWZv80SZ
-----END RSA PRIVATE KEY-----
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4660 (0x1234)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CA, ST=LAF, L=LAF
        Validity
            Not Before: Mar 28 06:05:46 2022 GMT
            Not After : Mar 28 06:05:46 2023 GMT
        Subject:
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:9f:e6:01:fb:c7:60:bb:51:c3:98:82:ea:ef:6f:
                    6d:a4:da:9e:8c:9c:dc:5d:3e:be:73:e7:e4:35:5e:
                    53:e3:23:95:b0:de:b3:21:89:05:2c:ec:f1:fa:56:
                    5d:18:c5:80:df:b6:9a:b5:86:e4:5f:88:e5:08:92:
                    6d:74:f1:c8:9b:ca:05:0b:3c:3c:7d:c3:cb:84:33:
                    a8:69:c8:80:c3:b2:0c:62:b9:82:65:7c:ab:47:9a:
                    84:a7:00:a7:36:63:a7:02:6f:50:ac:92:c7:e9:6c:
                    5f:07:82:71:99:1f:ab:7c:54:25:78:d4:66:09:08:
                    5c:64:8e:7d:ed:6f:a2:6f:29
                Exponent: 65537 (0x10001)
        X509v3 extensions:
                                                          24,20          17%
```

After modifying the Issuer country from US to CA, no difference, it still returned information when reloaded.



SEED-Ubuntu 16.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
En
3:15 AM
File Edit View History Bookmarks Tools Help
Insecure Connection
https://localhost:4433
Most Visited
SEED Labs
Sites for Labs
Right Ctrl

Your connection is not secure

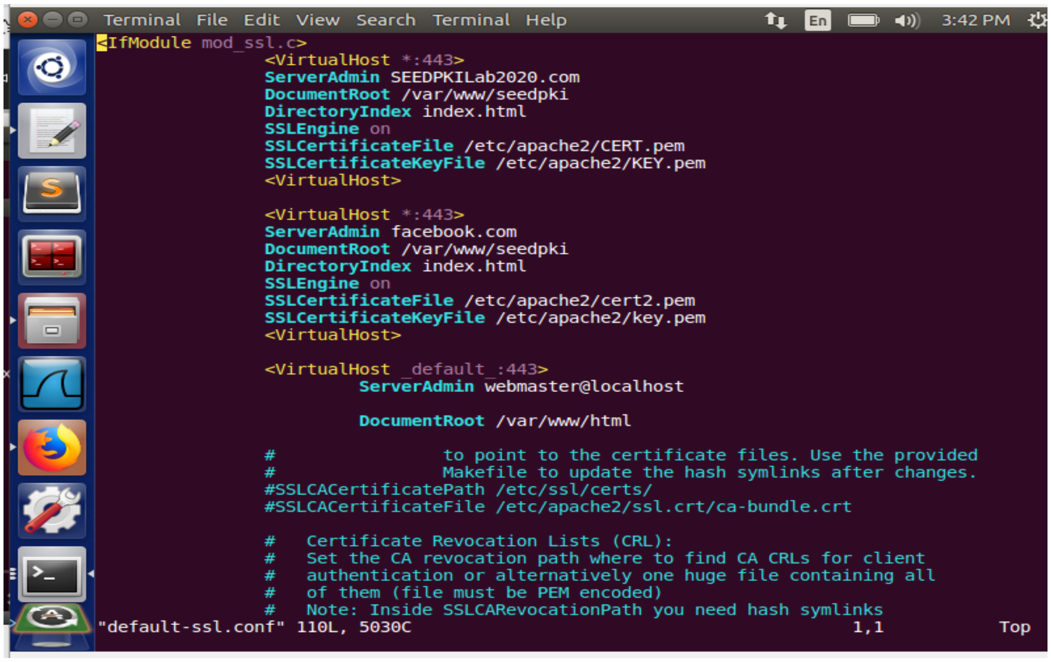
The owner of web.ecs.syr.edu has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more…

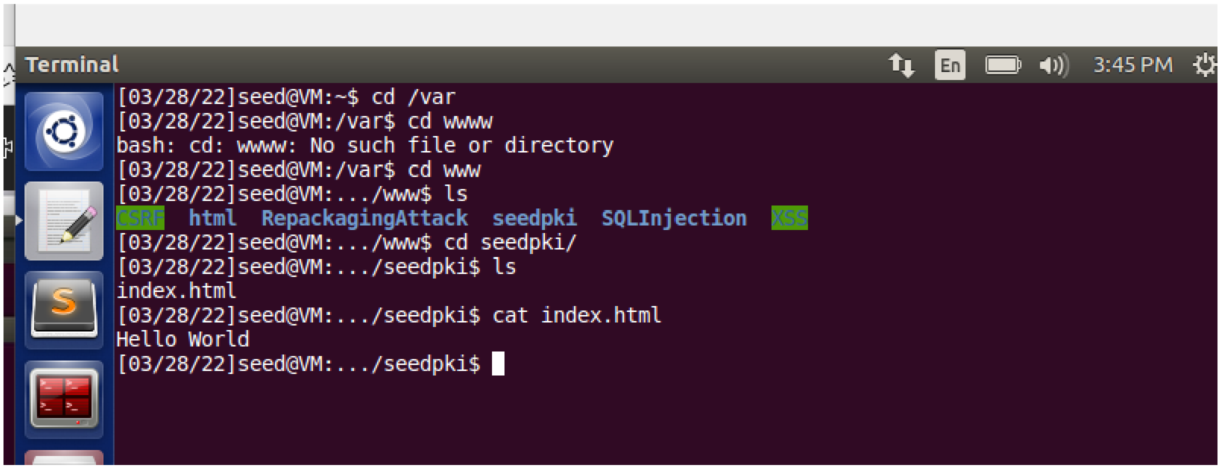
□ Report errors like this to help Mozilla identify and block malicious sites

When https://localhost:4433 was used as the address, it returned “an insecure connection”.

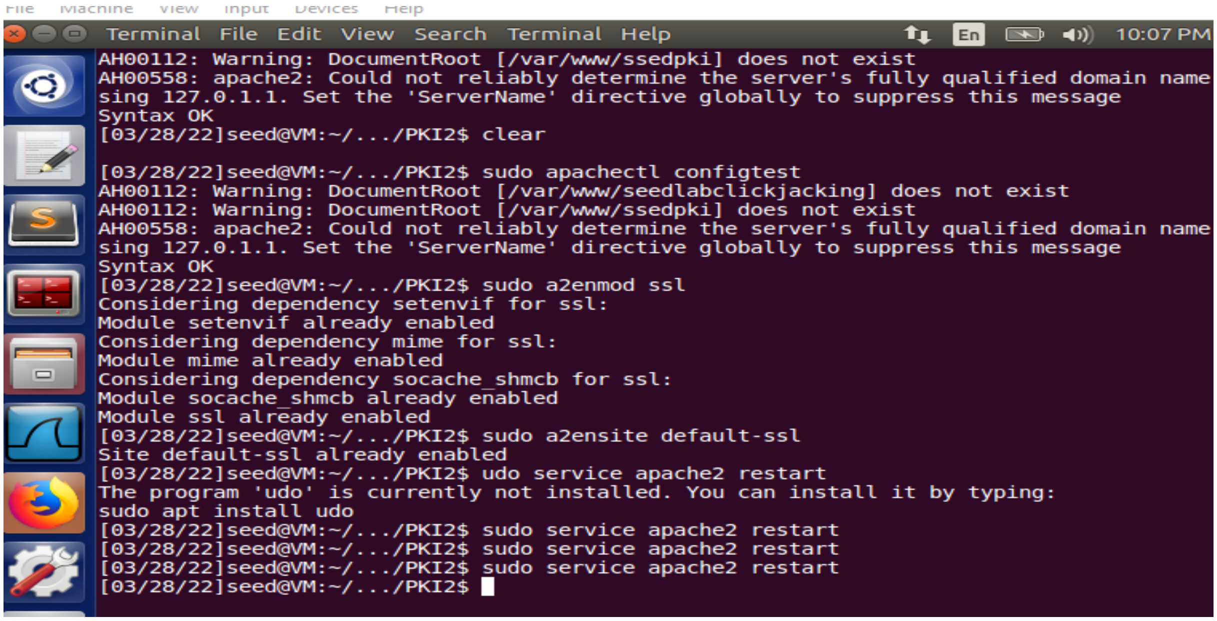
Task 4: Deploying Certificate in an Apache-Based HTTPSWebsite



```
<IfModule mod_ssl.c>
                <VirtualHost *:443>
                ServerAdmin SEEDPKILab2020.com
                DocumentRoot /var/www/seedpki
                DirectoryIndex index.html
                SSLEngine on
                SSLCertificateFile /etc/apache2/CERT.pem
                SSLCertificateKeyFile /etc/apache2/KEY.pem
                <VirtualHost>

                <VirtualHost *:443>
                ServerAdmin facebook.com
                DocumentRoot /var/www/seedpki
                DirectoryIndex index.html
                SSLEngine on
                SSLCertificateFile /etc/apache2/cert2.pem
                SSLCertificateKeyFile /etc/apache2/key.pem
                <VirtualHost>

                <VirtualHost _default_:443>
                        ServerAdmin webmaster@localhost

                        DocumentRoot /var/www/html

                #               to point to the certificate files. Use the provided
                #               Makefile to update the hash symlinks after changes.
                #SSLCACertificatePath /etc/ssl/certs/
                #SSLCACertificateFile /etc/apache2/ssl.crt/ca-bundle.crt

                #   Certificate Revocation Lists (CRL):
                #   Set the CA revocation path where to find CA CRLs for client
                #   authentication or alternatively one huge file containing all
                #   of them (file must be PEM encoded)
                #   Note: Inside SSLCARevocationPath you need hash symlinks
"default-ssl.conf" 110L, 5030C                                    1,1           Top
```

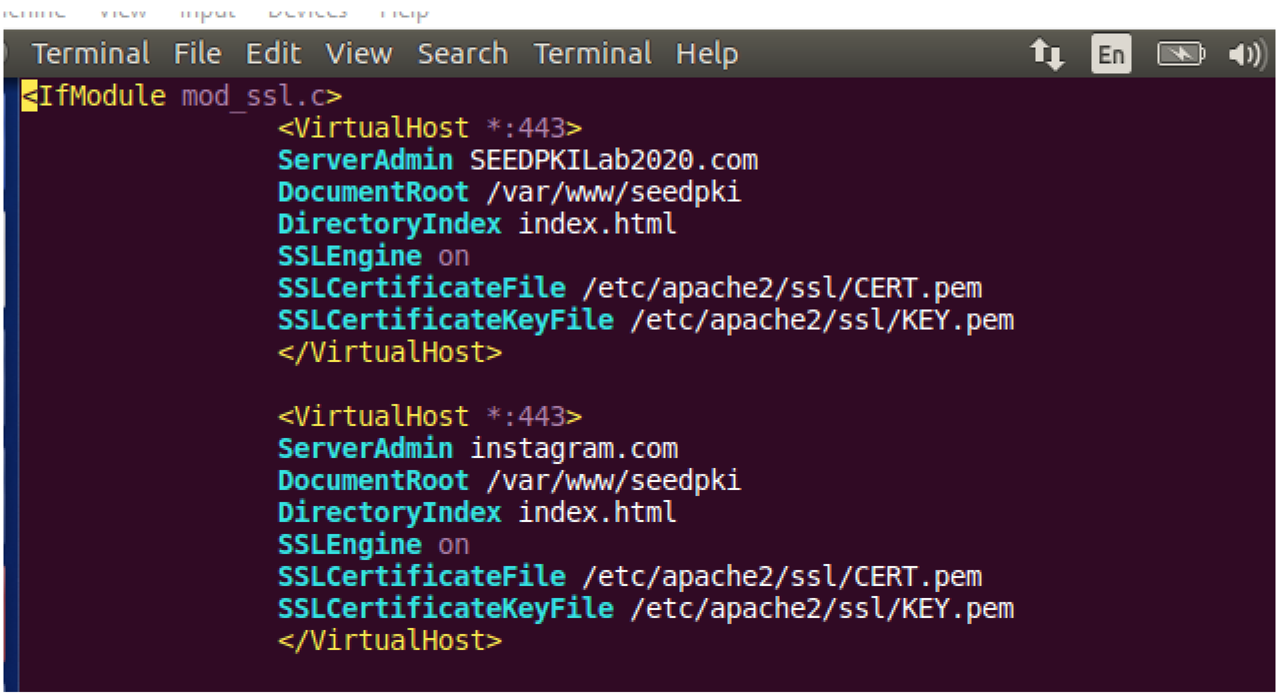


```
[03/28/22]seed@VM:~$ cd /var
[03/28/22]seed@VM:/var$ cd wwww
bash: cd: wwww: No such file or directory
[03/28/22]seed@VM:/var$ cd www
[03/28/22]seed@VM:.../www$ ls
CSRF  html  RepackagingAttack  seedpki  SQLInjection  XSS
[03/28/22]seed@VM:.../www$ cd seedpki/
[03/28/22]seed@VM:.../seedpki$ ls
index.html
[03/28/22]seed@VM:.../seedpki$ cat index.html
Hello World
[03/28/22]seed@VM:.../seedpki$ 
```

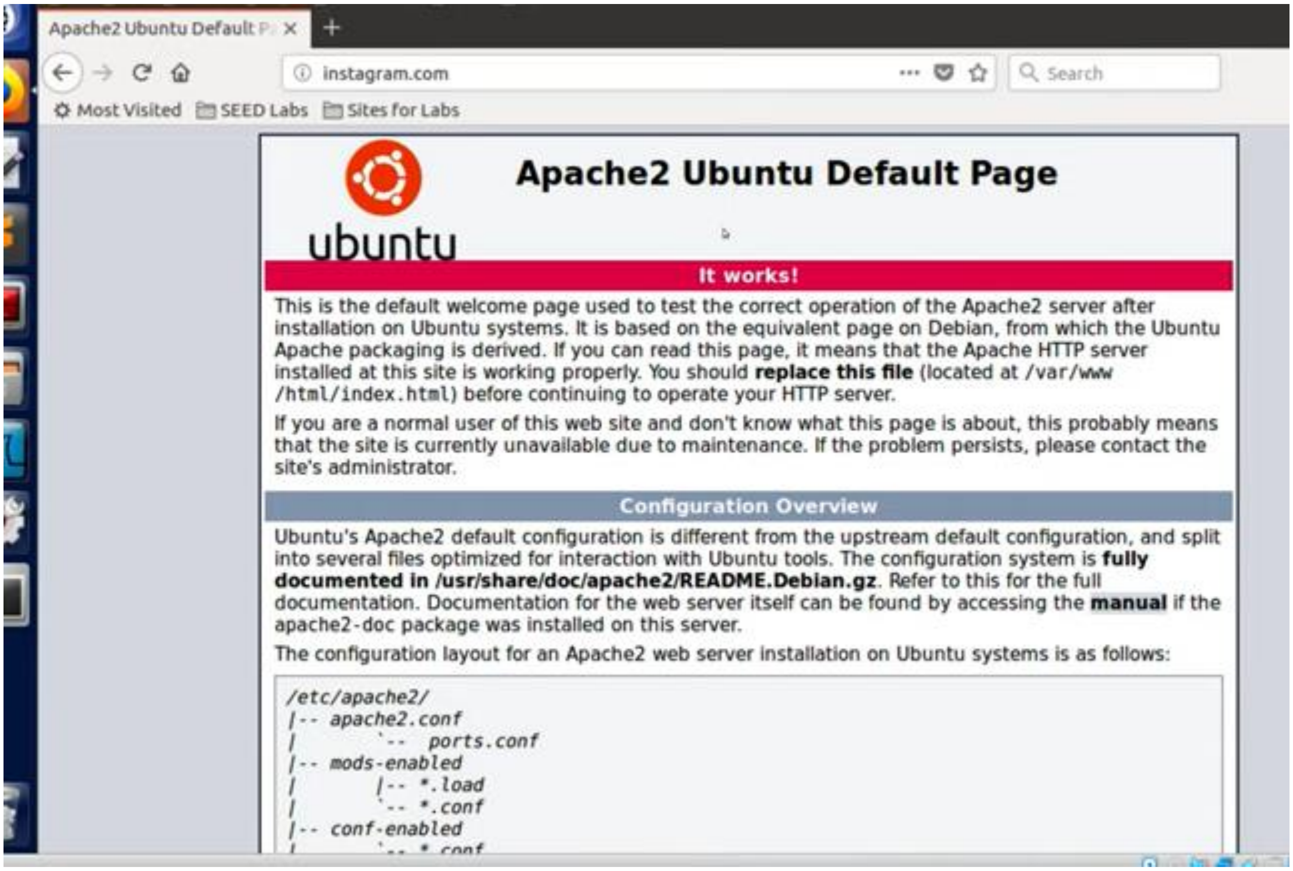

File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
En
10:07 PM

```
AH00112: Warning: DocumentRoot [/var/www/ssedpki] does not exist
AH00558: apache2: Could not reliably determine the server's fully qualified domain name
sing 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
[03/28/22]seed@VM:~/.../PKI2$ clear

[03/28/22]seed@VM:~/.../PKI2$ sudo apachectl configtest
AH00112: Warning: DocumentRoot [/var/www/seedlabclickjacking] does not exist
AH00112: Warning: DocumentRoot [/var/www/ssedpki] does not exist
AH00558: apache2: Could not reliably determine the server's fully qualified domain name
sing 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
[03/28/22]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
[03/28/22]seed@VM:~/.../PKI2$ sudo a2ensite default-ssl
Site default-ssl already enabled
[03/28/22]seed@VM:~/.../PKI2$ udo service apache2 restart
The program 'udo' is currently not installed. You can install it by typing:
sudo apt install udo
[03/28/22]seed@VM:~/.../PKI2$ sudo service apache2 restart
[03/28/22]seed@VM:~/.../PKI2$ sudo service apache2 restart
[03/28/22]seed@VM:~/.../PKI2$ sudo service apache2 restart
[03/28/22]seed@VM:~/.../PKI2$ 
```

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


Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
En

```
<IfModule mod_ssl.c>
                <VirtualHost *:443>
                ServerAdmin SEEDPKILab2020.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>
                ServerAdmin instagram.com
                DocumentRoot /var/www/seedpki
                DirectoryIndex index.html
                SSLEngine on
                SSLCertificateFile /etc/apache2/ssl/CERT.pem
                SSLCertificateKeyFile /etc/apache2/ssl/KEY.pem
                </VirtualHost>
```



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. 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.

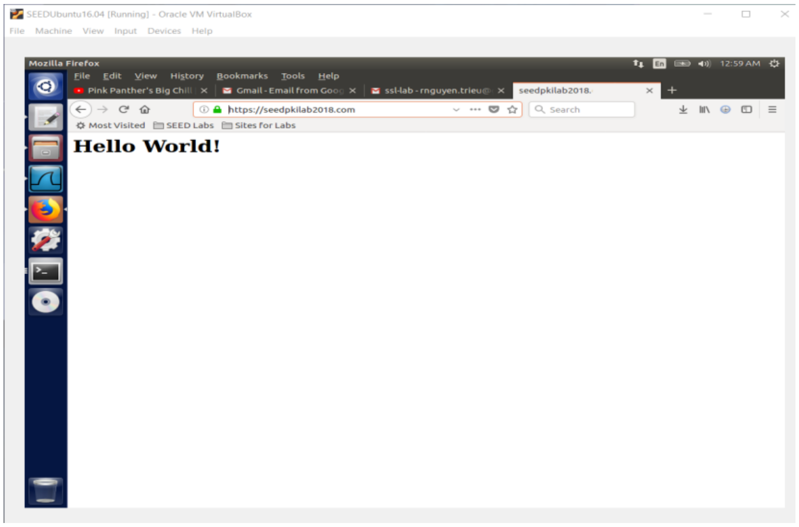
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu 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 Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
```

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


SEEDUbuntu16.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Mozilla Firefox
12:59 AM
File Edit View History Bookmarks Tools Help
Pink Panther's Big Chili
Gmail - Email from Goo
ssl-lab - rnguyen.trieu@
seedpkilab2018.
https://seedpkilab2018.com
Search
Most Visited
SEED Labs
Sites for Labs

Hello World!

This task shows that the attacker can generate any arbitrary certificate using the CA’s key as it is already compromised.