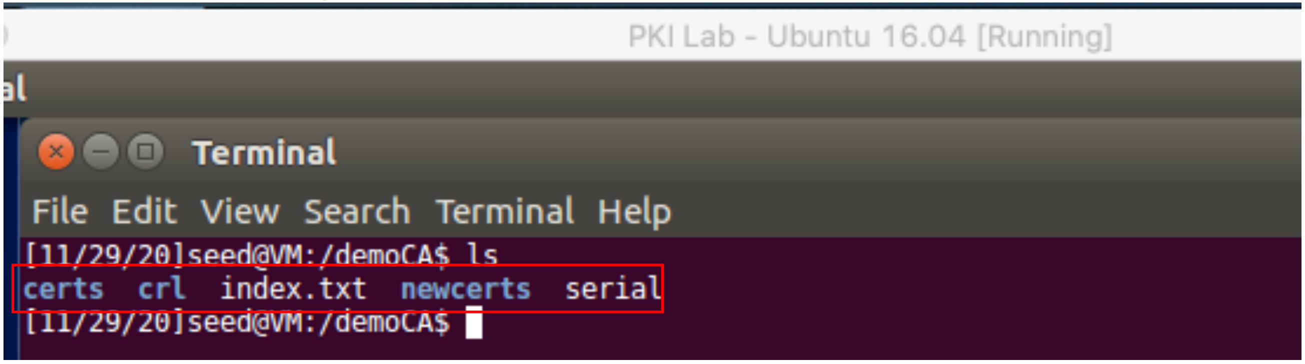
Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

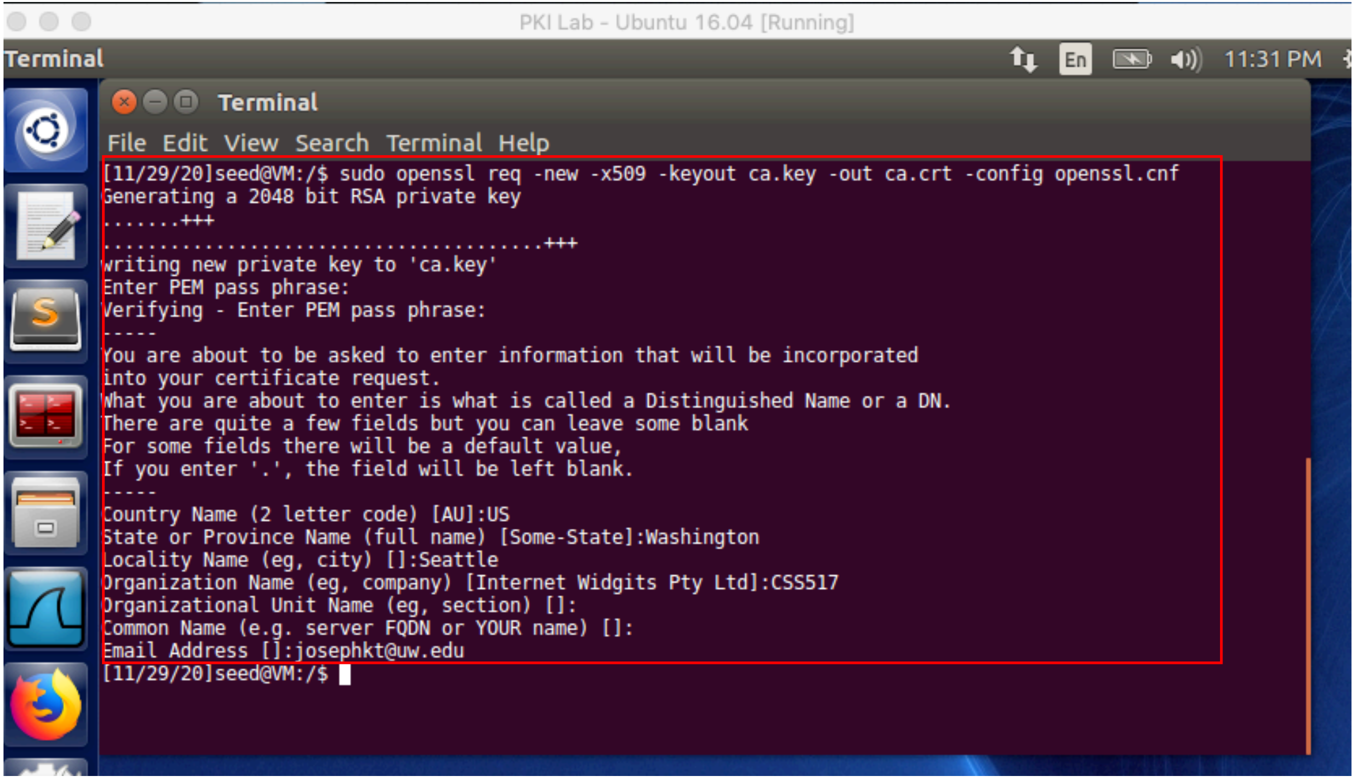
Task 1: Becoming a Certificate Authority (CA)

Screenshot 1: Creating the necessary files within the /demoCA directory in order to later run the commands that will generate the certificates.


PKI Lab - Ubuntu 16.04 [Running]
Terminal
File Edit View Search Terminal Help

```
[11/29/20]seed@VM:/demoCA$ ls
certs  crl  index.txt  newcerts  serial
[11/29/20]seed@VM:/demoCA$
```

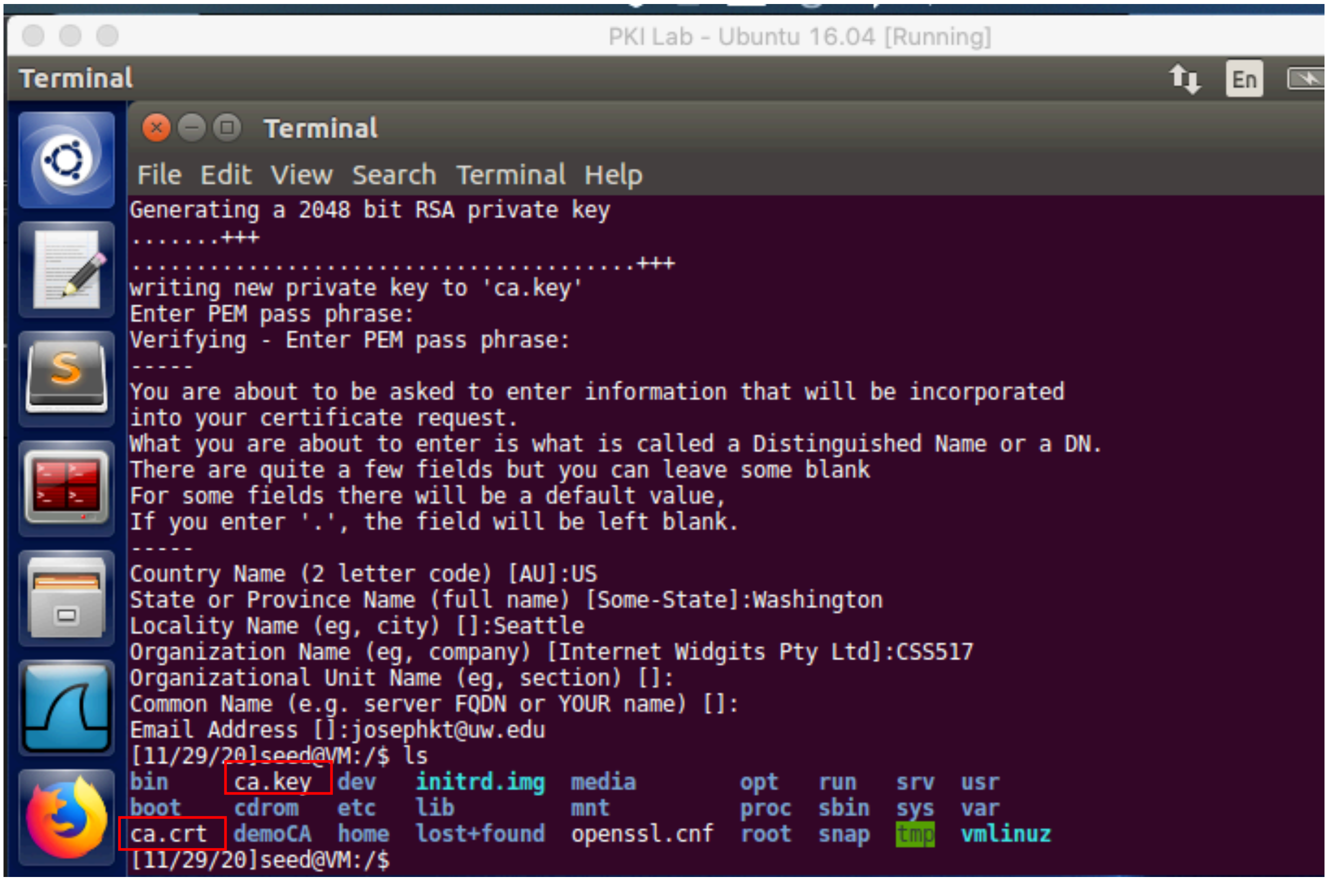
Screenshot 2: Generating the self-signed root certificate for the Certificate Authority (CA).


PKI Lab - Ubuntu 16.04 [Running]
Terminal
En
11:31 PM
Terminal
File Edit View Search Terminal Help

```
[11/29/20]seed@VM:/$ sudo 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
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]:Washington
Locality Name (eg, city) []:Seattle
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CSS517
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:josephkt@uw.edu
[11/29/20]seed@VM:/$
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

Screenshot 3: Verifying that the private key (ca.key) and public key (ca.crt) for the CA have been created.

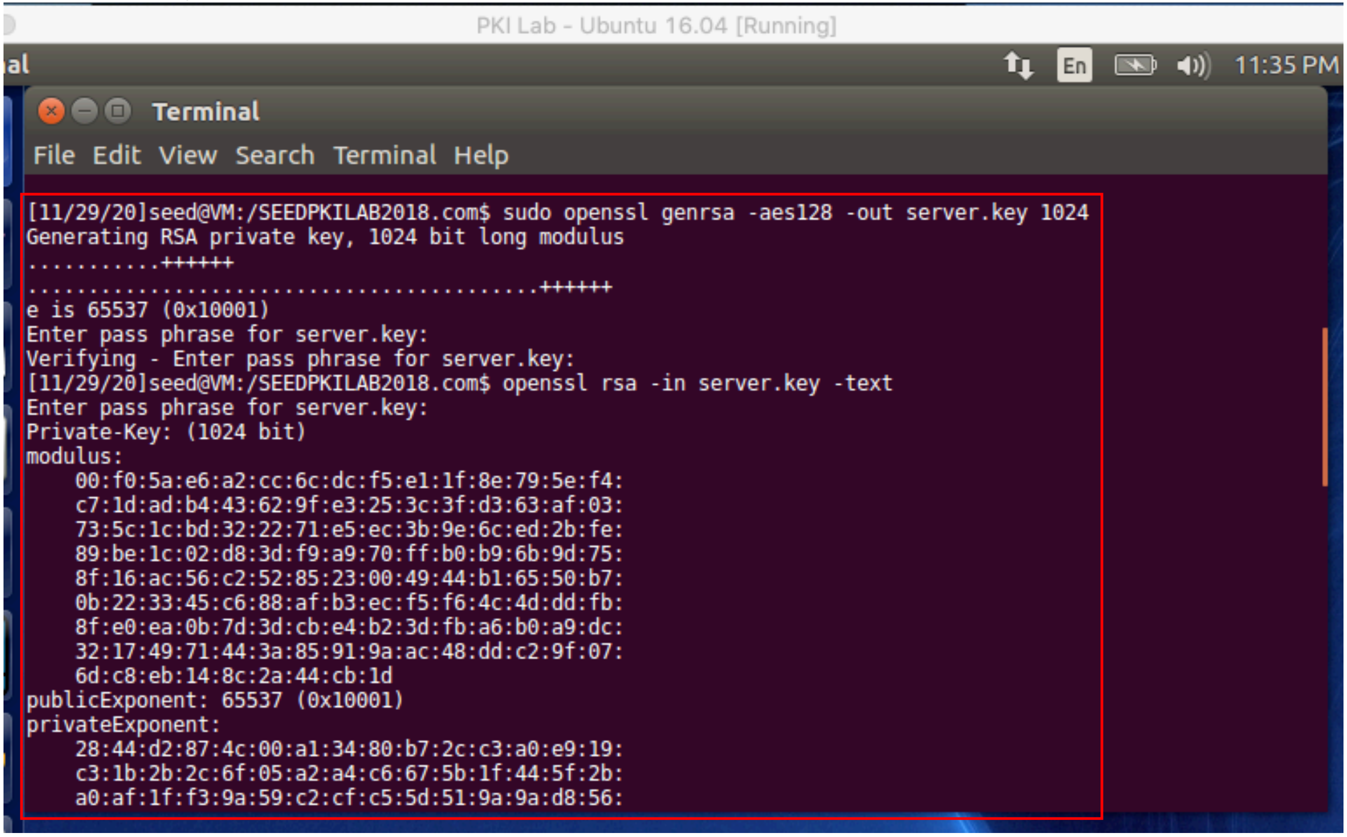

PKI Lab - Ubuntu 16.04 [Running]
Terminal
En
Terminal
File Edit View Search Terminal Help

```
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]:Washington
Locality Name (eg, city) []:Seattle
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CSS517
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:josephkt@uw.edu
[11/29/20]seed@VM:/$ ls
bin      ca.key  dev   initrd.img  media        opt   run   srv  usr
boot     cdrom   etc   lib         mnt          proc  sbin  sys  var
ca.crt   demoCA  home  lost+found  openssl.cnf  root  snap  tmp  vmlinuz
[11/29/20]seed@VM:/$
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

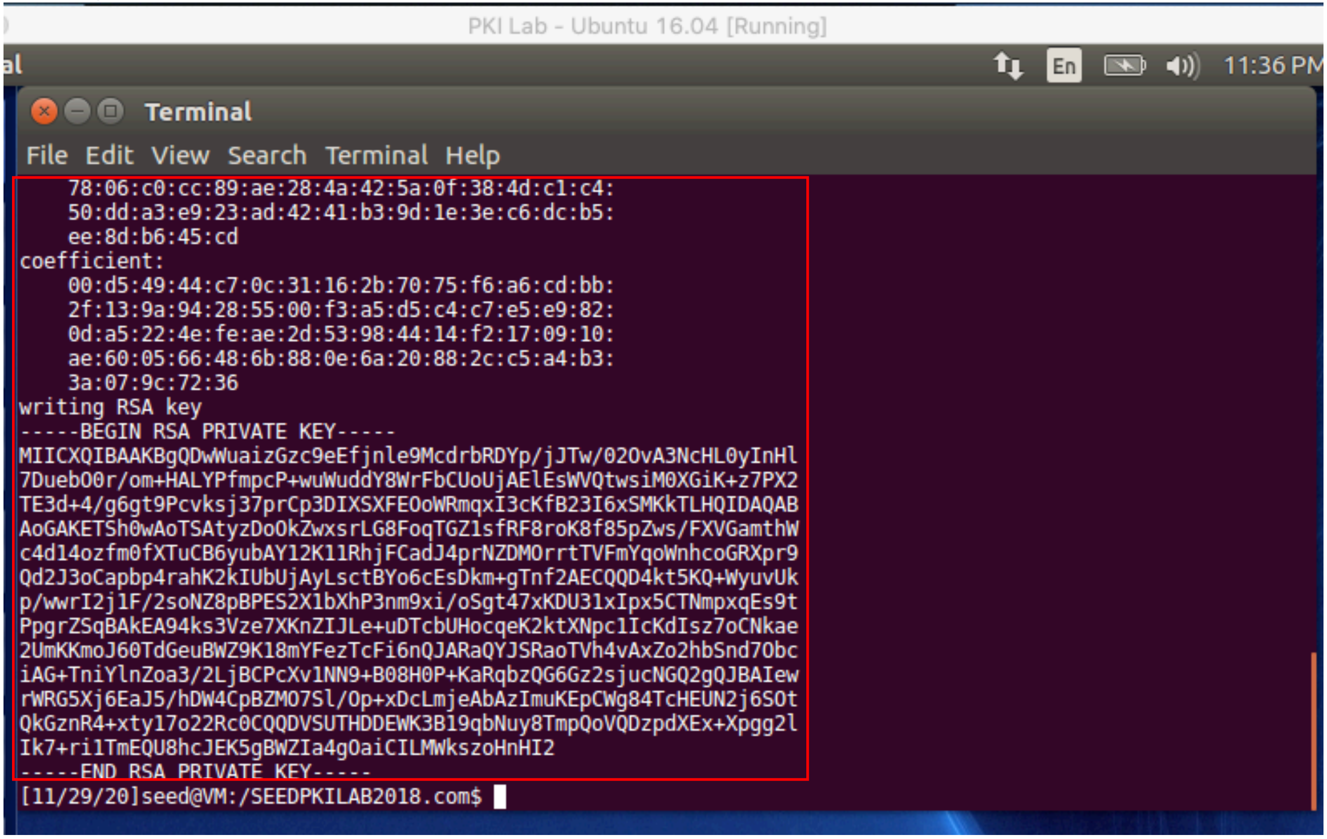
Task 2: Creating a Certificate for SEEDPKILAB2018.com

Screenshot 4: Generating the public/private key pair and looking at the contents of the key within the .key file


PKI Lab - Ubuntu 16.04 [Running]
al
En
11:35 PM
Terminal
File Edit View Search Terminal Help

```
[11/29/20]seed@VM:/SEEDPKILAB2018.com$ sudo 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:
[11/29/20]seed@VM:/SEEDPKILAB2018.com$ openssl rsa -in server.key -text
Enter pass phrase for server.key:
Private-Key: (1024 bit)
modulus:
    00:f0:5a:e6:a2:cc:6c:dc:f5:e1:1f:8e:79:5e:f4:
    c7:1d:ad:b4:43:62:9f:e3:25:3c:3f:d3:63:af:03:
    73:5c:1c:bd:32:22:71:e5:ec:3b:9e:6c:ed:2b:fe:
    89:be:1c:02:d8:3d:f9:a9:70:ff:b0:b9:6b:9d:75:
    8f:16:ac:56:c2:52:85:23:00:49:44:b1:65:50:b7:
    0b:22:33:45:c6:88:af:b3:ec:f5:f6:4c:4d:dd:fb:
    8f:e0:ea:0b:7d:3d:cb:e4:b2:3d:fb:a6:b0:a9:dc:
    32:17:49:71:44:3a:85:91:9a:ac:48:dd:c2:9f:07:
    6d:c8:eb:14:8c:2a:44:cb:1d
publicExponent: 65537 (0x10001)
privateExponent:
    28:44:d2:87:4c:00:a1:34:80:b7:2c:c3:a0:e9:19:
    c3:1b:2b:2c:6f:05:a2:a4:c6:67:5b:1f:44:5f:2b:
    a0:af:1f:f3:9a:59:c2:cf:c5:5d:51:9a:9a:d8:56:
```

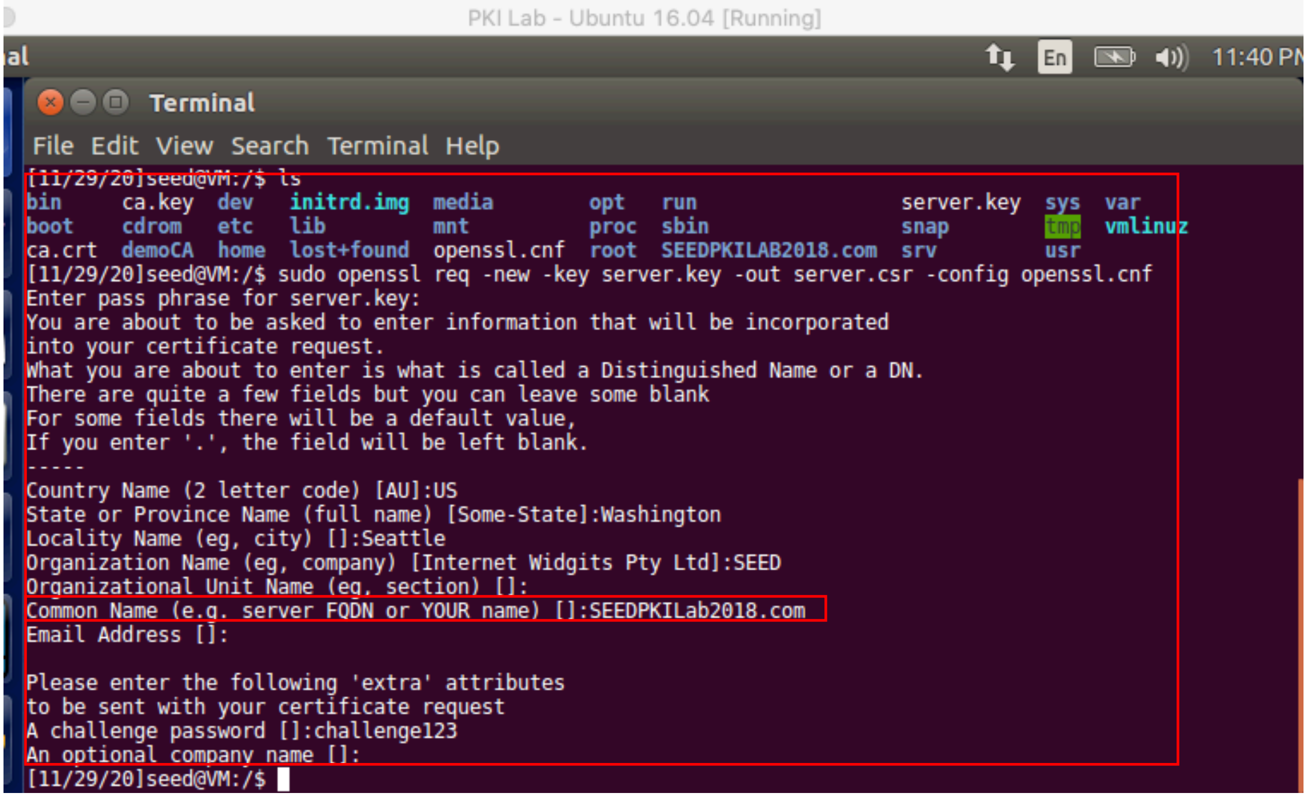
Screenshot 5: Contents of the server.key file, continued, which displays the private key within the .key file.


PKI Lab - Ubuntu 16.04 [Running]
En
11:36 PM
Terminal
File Edit View Search Terminal Help

```
    78:06:c0:cc:89:ae:28:4a:42:5a:0f:38:4d:c1:c4:
    50:dd:a3:e9:23:ad:42:41:b3:9d:1e:3e:c6:dc:b5:
    ee:8d:b6:45:cd
coefficient:
    00:d5:49:44:c7:0c:31:16:2b:70:75:f6:a6:cd:bb:
    2f:13:9a:94:28:55:00:f3:a5:d5:c4:c7:e5:e9:82:
    0d:a5:22:4e:fe:ae:2d:53:98:44:14:f2:17:09:10:
    ae:60:05:66:48:6b:88:0e:6a:20:88:2c:c5:a4:b3:
    3a:07:9c:72:36
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDwWuaizGzc9eEfjnle9McdrbRDYp/jJTw/02OvA3NcHL0yInHl
7DuebO0r/om+HALYPfmpcP+wuWuddY8WrFbCUoUjAElEsWVQtwsiM0XGiK+z7PX2
TE3d+4/g6gt9Pcvksj37prCp3DIXSXFEOoWRmqxI3cKfB23I6xSMKkTLHQIDAQAB
AoGAKETSh0wAoTSAtyzDoOkZwxsrLG8FoqTGZ1sfRF8roK8f85pZws/FXVGamthW
c4d14ozfm0fXTuCB6yubAY12K11RhjFCadJ4prNZDMOrrtTVFmYqoWnhcoGRXpr9
Qd2J3oCapbp4rahK2kIUbUjAyLsctBYo6cEsDkm+gTnf2AECQQD4kt5KQ+WyuvUk
p/wwrI2j1F/2soNZ8pBPES2X1bXhP3nm9xi/oSgt47xKDU31xIpx5CTNmpxqEs9t
PpgrZSqBAkEA94ks3Vze7XKnZIJLe+uDTcbUHocqeK2ktXNpc1IcKdIsz7oCNkae
2UmKKmoJ60TdGeuBWZ9K18mYFezTcFi6nQJARaQYJSRaoTVh4vAxZo2hbSnd7Obc
iAG+TniYlnZoa3/2LjBCPcXv1NN9+B08H0P+KaRqbzQG6Gz2sjucNGQ2gQJBAIew
rWRG5Xj6EaJ5/hDW4CpBZMO7Sl/Op+xDcLmjeAbAzImuKEpCWg84TcHEUN2j6SOt
QkGznR4+xty17o22Rc0CQQDVSUTHDDEWK3B19qbNuy8TmpQoVQDzpdXEx+Xpgg2l
Ik7+ri1TmEQU8hcJEK5gBWZIa4gOaiCILMWkszoHnHI2
-----END RSA PRIVATE KEY-----
[11/29/20]seed@VM:/SEEDPKILAB2018.com$
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

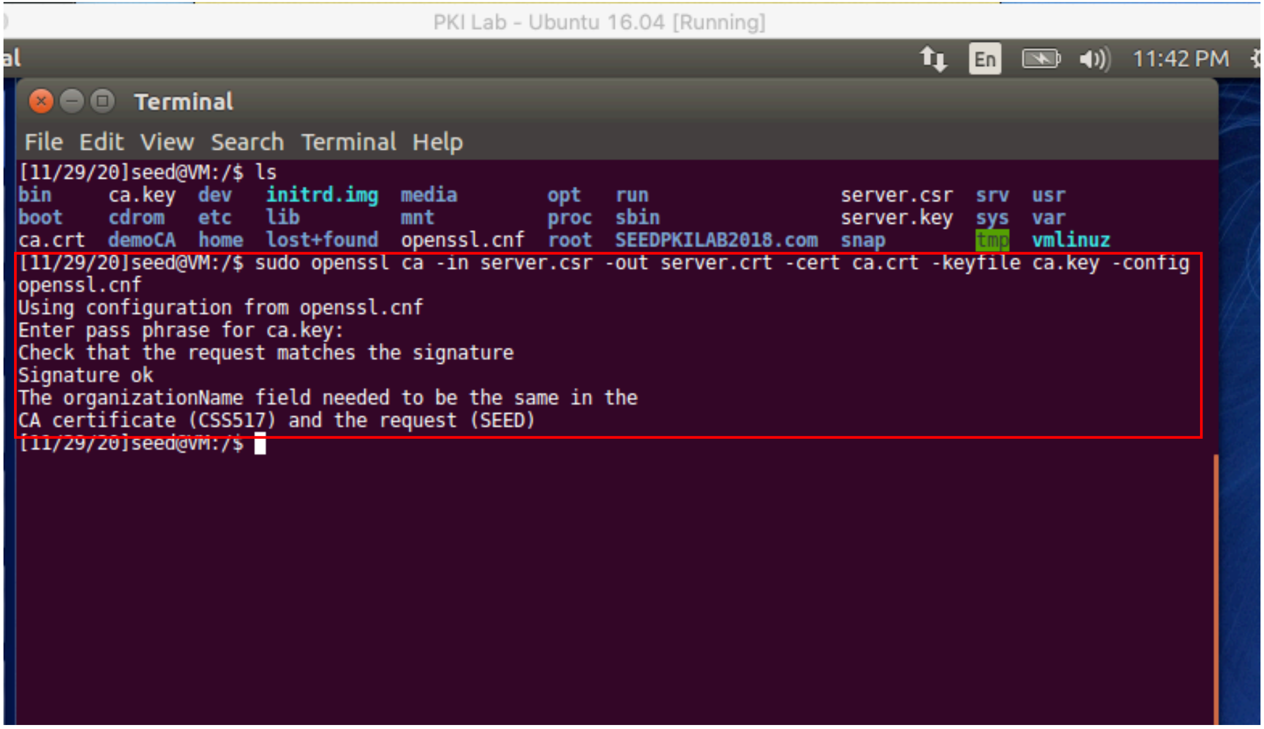
Screenshot 6: Generating the certificate signing request for SEEDPKILab2018.com, as indicated by the usage of the server.key file generated in Screenshot 4, as well as the usage of the common name, "SEEDPKILab2018.com"


PKI Lab - Ubuntu 16.04 [Running]
al
En
11:40 PM
Terminal
File Edit View Search Terminal Help

```
[11/29/20]seed@VM:/$ ls
bin      ca.key  dev   initrd.img  media        opt   run                 server.key  sys   var
boot     cdrom   etc   lib         mnt          proc  sbin                snap        tmp   vmlinuz
ca.crt   demoCA  home  lost+found  openssl.cnf  root  SEEDPKILAB2018.com  srv         usr
[11/29/20]seed@VM:/$ sudo 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]:Washington
Locality Name (eg, city) []:Seattle
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SEED
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:SEEDPKILab2018.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:challenge123
An optional company name []:
[11/29/20]seed@VM:/$
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

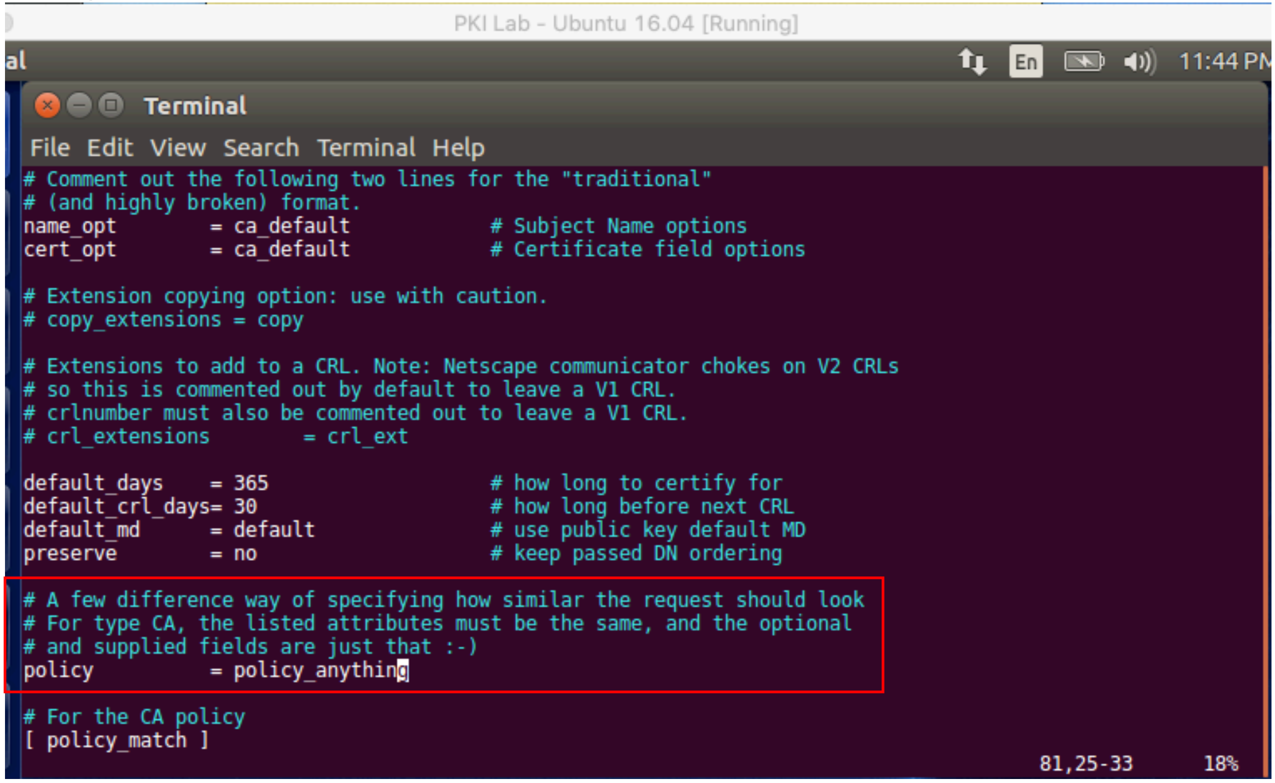
Screenshot 7: Attempting to generate the certificate using the CA key, but being initially denied the generation of the certificates because I had used different organization names. This makes sense, as the initial policy for signing certificates is set such that only certificates within the same organization of the CA can be signed.


PKI Lab - Ubuntu 16.04 [Running]
En
11:42 PM
Terminal
File Edit View Search Terminal Help

```
[11/29/20]seed@VM:/$ ls
bin      ca.key  dev    initrd.img  media       opt   run                server.csr  srv  usr
boot     cdrom   etc    lib         mnt         proc  sbin               server.key  sys  var
ca.crt   demoCA  home   lost+found  openssl.cnf root  SEEDPKILAB2018.com snap        tmp  vmlinuz
[11/29/20]seed@VM:/$ sudo 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
The organizationName field needed to be the same in the
CA certificate (CSS517) and the request (SEED)
[11/29/20]seed@VM:/$ 
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

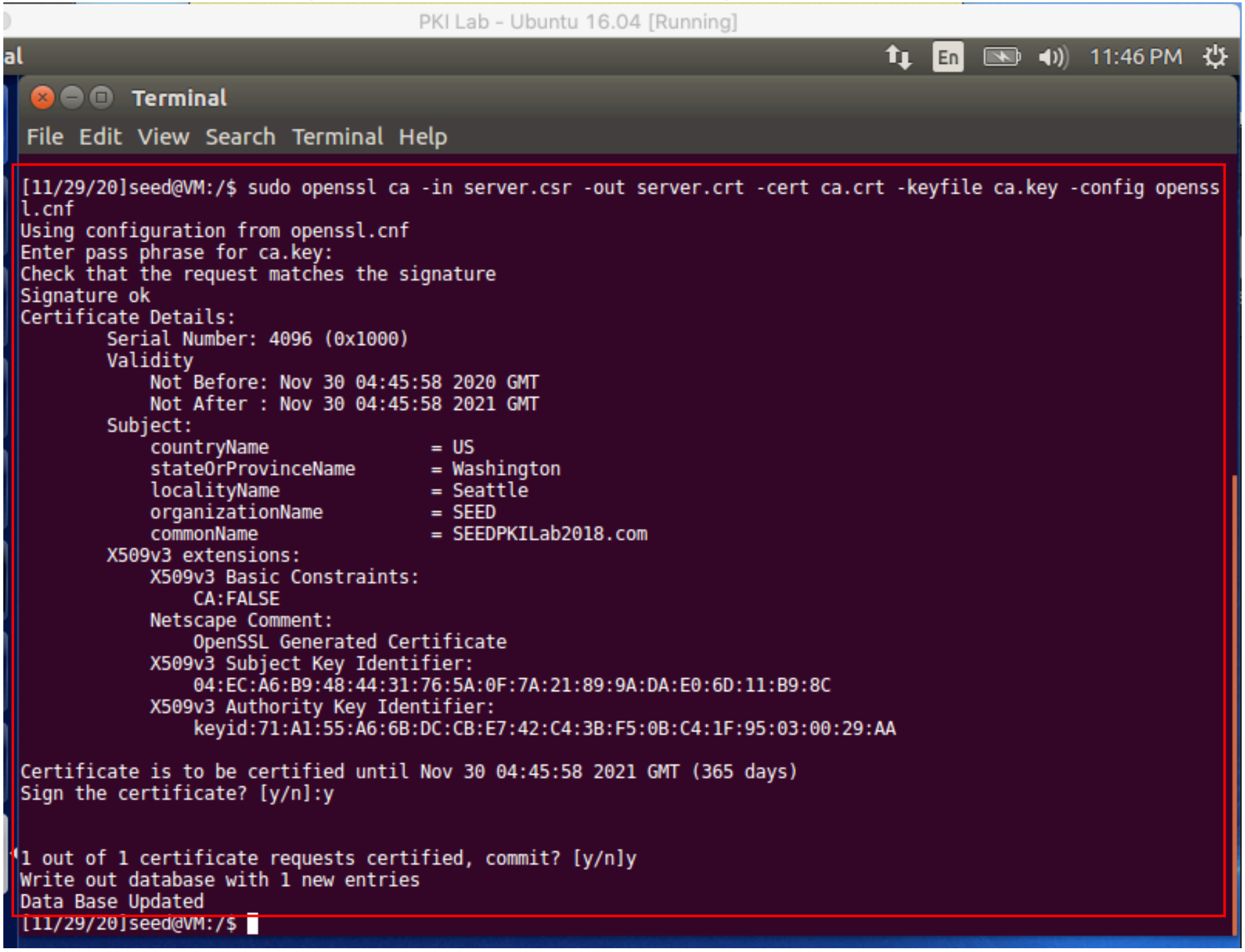
Screenshot 8: Adjusting the configuration file to have a policy match of policy_anything so that the organization names do not need to match.


PKI Lab - Ubuntu 16.04 [Running]
al
En
11:44 PM
Terminal
File Edit View Search Terminal Help

```
# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt        = ca_default            # Subject Name options
cert_opt        = ca_default            # Certificate field options

# Extension copying option: use with caution.
# copy_extensions = copy

# Extensions to add to a CRL. Note: Netscape communicator chokes on V2 CRLs
# so this is commented out by default to leave a V1 CRL.
# crlnumber must also be commented out to leave a V1 CRL.
# crl_extensions        = crl_ext

default_days    = 365                   # how long to certify for
default_crl_days= 30                    # how long before next CRL
default_md      = default               # use public key default MD
preserve        = no                    # keep passed DN ordering

# A few difference way of specifying how similar the request should look
# For type CA, the listed attributes must be the same, and the optional
# and supplied fields are just that :-)
policy          = policy_anything

# For the CA policy
[ policy_match ]
                                                              81,25-33      18%
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

Screenshot 9: Signing the SEEDPKILab2018.com certificate and verifying that changing the policies allowed me to sign a certificate with a different organization.

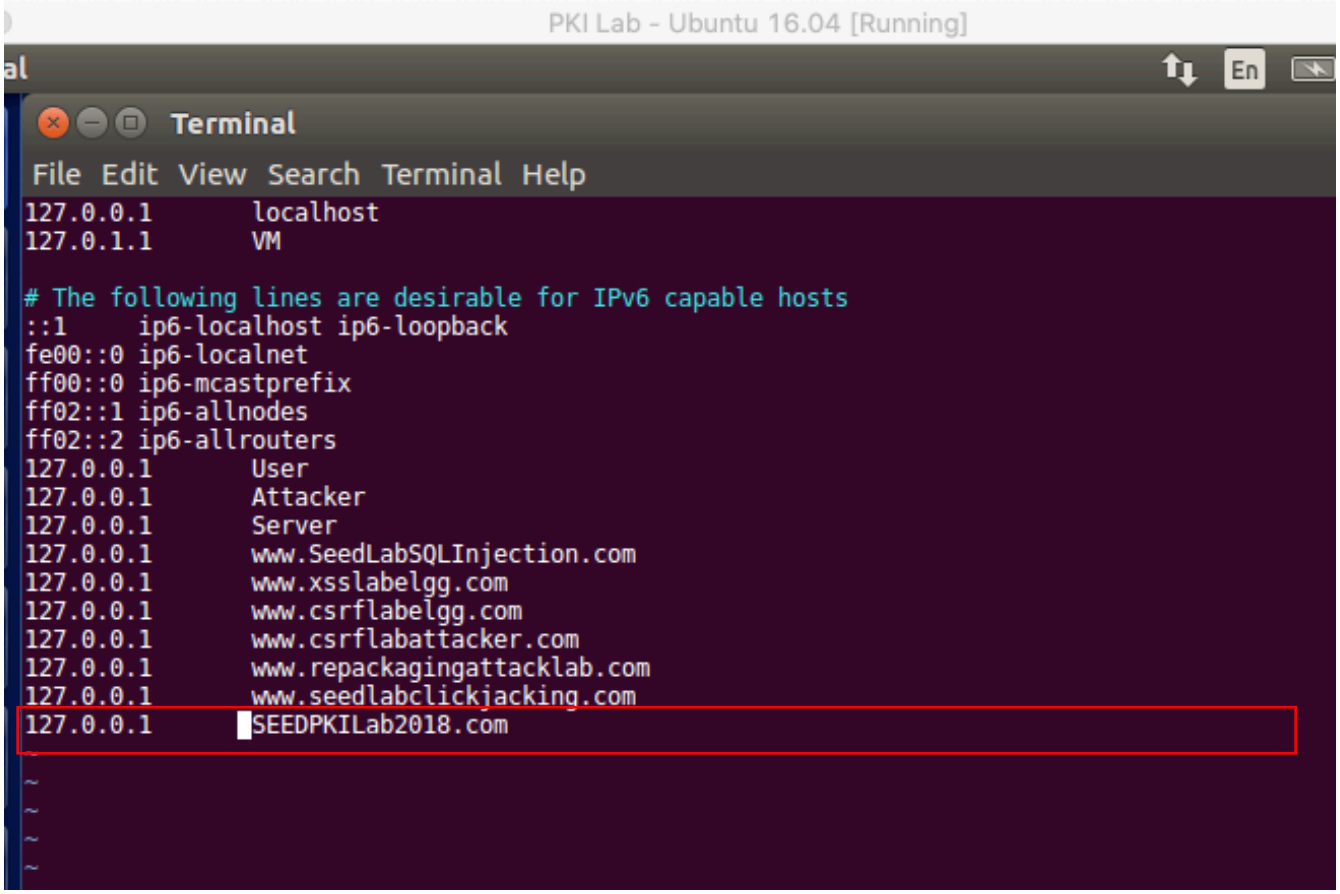

PKI Lab - Ubuntu 16.04 [Running]
al
En
11:46 PM
Terminal
File Edit View Search Terminal Help

```
[11/29/20]seed@VM:/$ sudo openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openss
l.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: Nov 30 04:45:58 2020 GMT
            Not After : Nov 30 04:45:58 2021 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = Washington
            localityName              = Seattle
            organizationName          = SEED
            commonName                = SEEDPKILab2018.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                04:EC:A6:B9:48:44:31:76:5A:0F:7A:21:89:9A:DA:E0:6D:11:B9:8C
            X509v3 Authority Key Identifier:
                keyid:71:A1:55:A6:6B:DC:CB:E7:42:C4:3B:F5:0B:C4:1F:95:03:00:29:AA

Certificate is to be certified until Nov 30 04:45:58 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
[11/29/20]seed@VM:/$ 
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

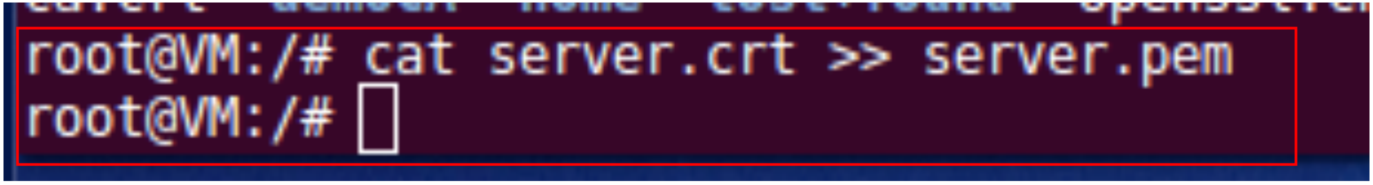
Task 3: Deploying Certificate in an HTTPS Web Server

Screenshot 10: Configuring DNS so that SEEDPKILab2018.com will map to localhost.


PKI Lab - Ubuntu 16.04 [Running]
Terminal
File Edit View Search Terminal Help

```
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.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
127.0.0.1       SEEDPKILab2018.com
~
~
~
~
~
```

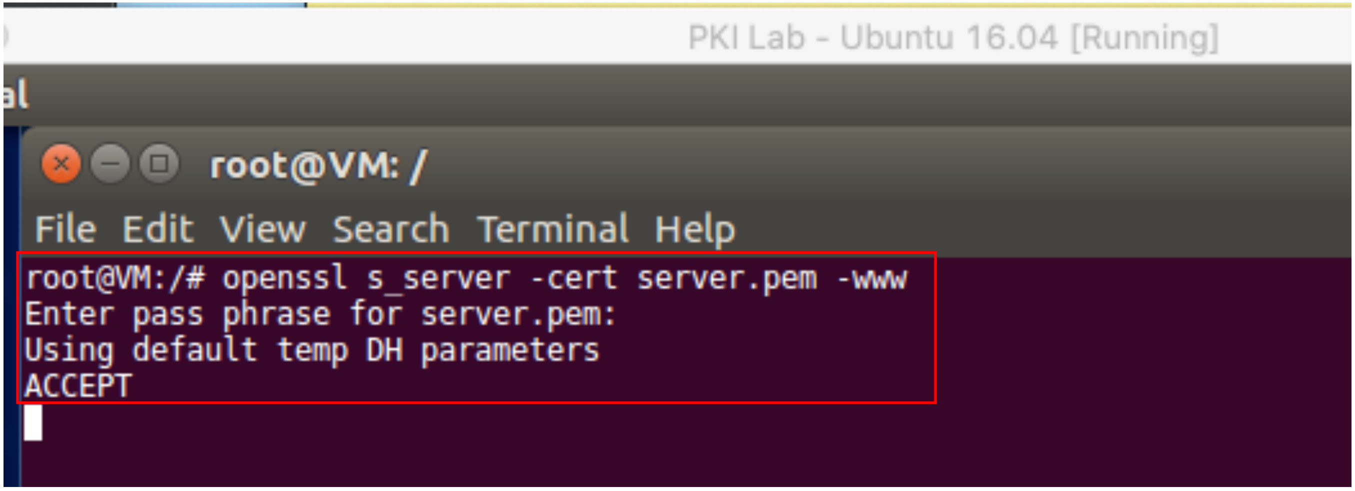
Screenshot 11: Combining the secret key and certificate into one file. “server.pem” is a copy of the file server.key which I made, as indicated within step 2 for task 3 of the lab.



```
root@VM:/# cat server.crt >> server.pem
root@VM:/# 
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

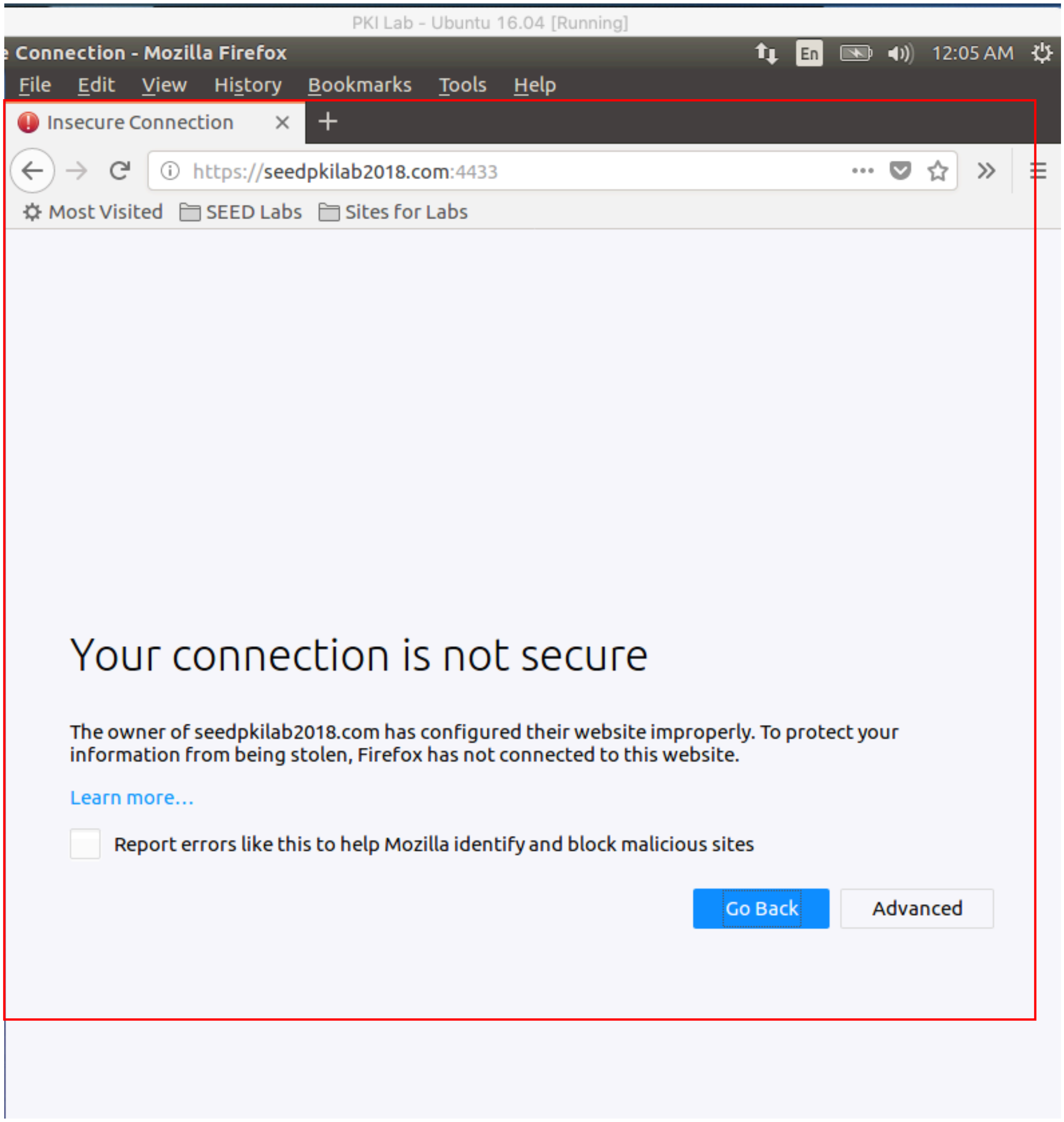
Screenshot 12: Starting the web server.


PKI Lab - Ubuntu 16.04 [Running]
root@VM: /
File Edit View Search Terminal Help

```
root@VM:/# openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

Screenshot 13: Attempting to connect to the website, but being informed that the connection is not secure.


PKI Lab - Ubuntu 16.04 [Running]
Connection - Mozilla Firefox
En
12:05 AM
File Edit View History Bookmarks Tools Help
Insecure Connection
https://seedpkilab2018.com:4433
Most Visited
SEED Labs
Sites for Labs

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.

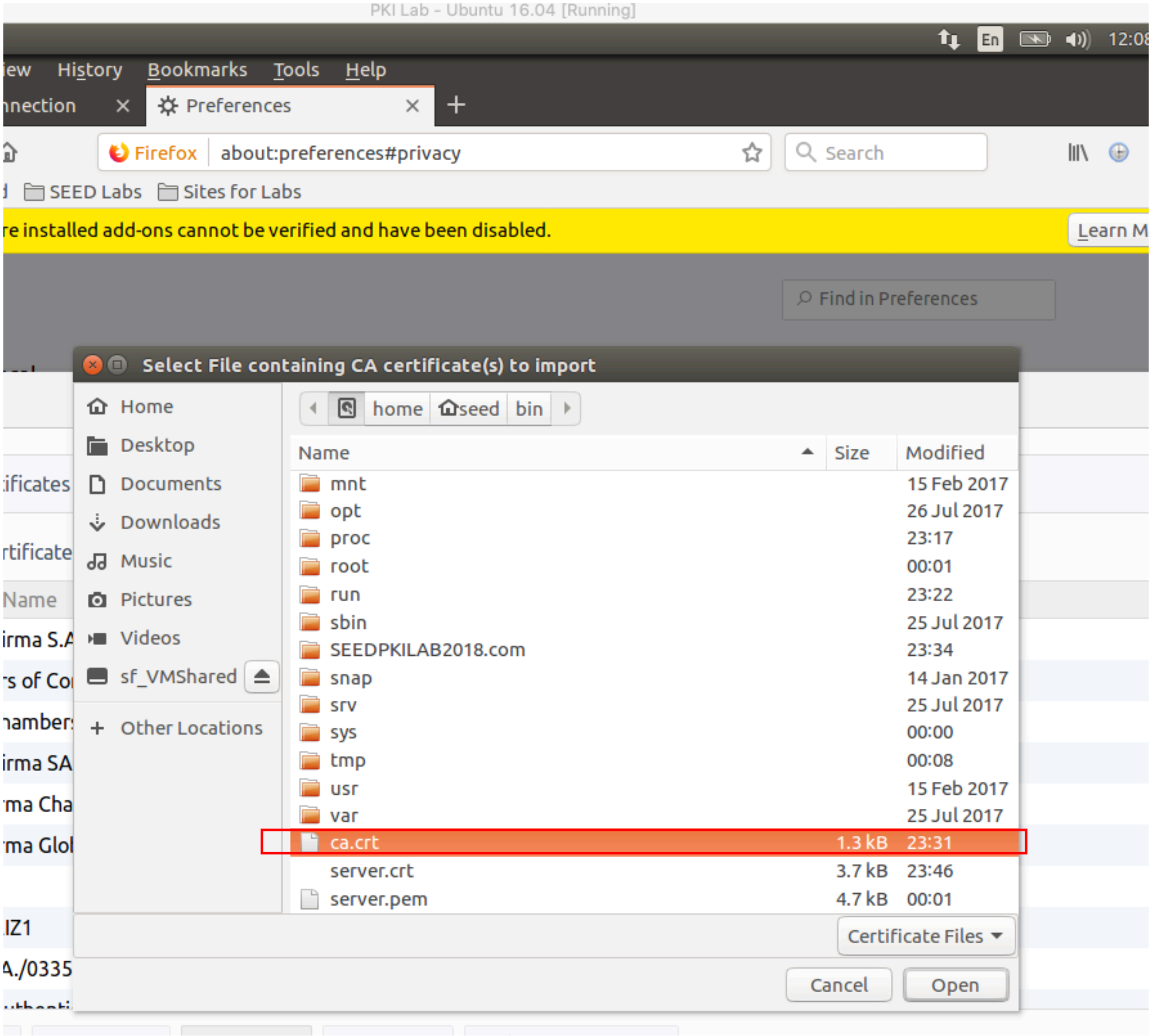
Learn more…

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

Go Back Advanced

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

Screenshot 14: Navigating to the security and privacy settings within Firefox, and importing the CA certificate file.



PKI Lab - Ubuntu 16.04 [Running]

about:preferences#privacy

re installed add-ons cannot be verified and have been disabled.

Select File containing CA certificate(s) to import

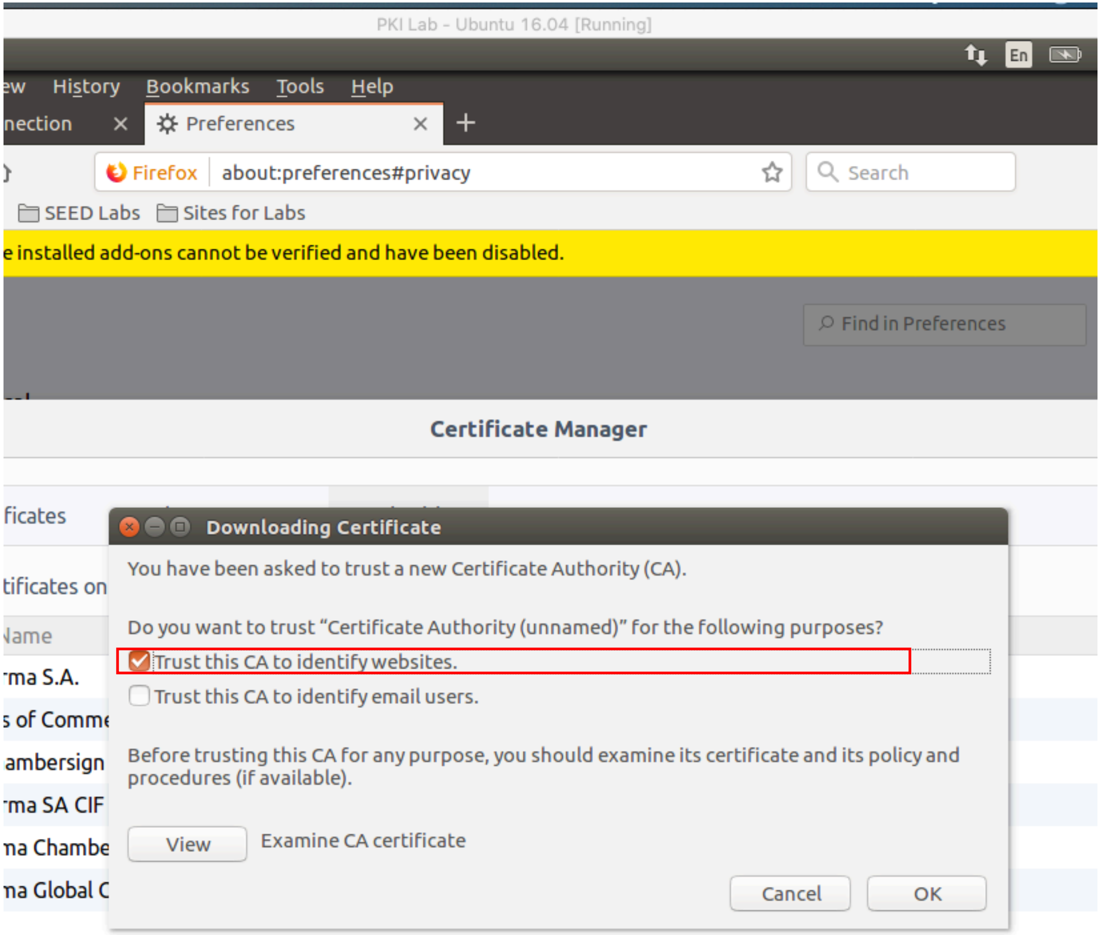
home / seed / bin

Name	Size	Modified
mnt		15 Feb 2017
opt		26 Jul 2017
proc		23:17
root		00:01
run		23:22
sbin		25 Jul 2017
SEEDPKILAB2018.com		23:34
snap		14 Jan 2017
srv		25 Jul 2017
sys		00:00
tmp		00:08
usr		15 Feb 2017
var		25 Jul 2017
ca.crt	1.3 kB	23:31
server.crt	3.7 kB	23:46
server.pem	4.7 kB	00:01

Certificate Files

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

Screenshot 15: Allowing the CA which we created to identify websites.



about:preferences#privacy

e installed add-ons cannot be verified and have been disabled.

Downloading Certificate

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

Do you want to trust “Certificate Authority (unnamed)” for the following purposes?

☑ Trust this CA to identify websites.

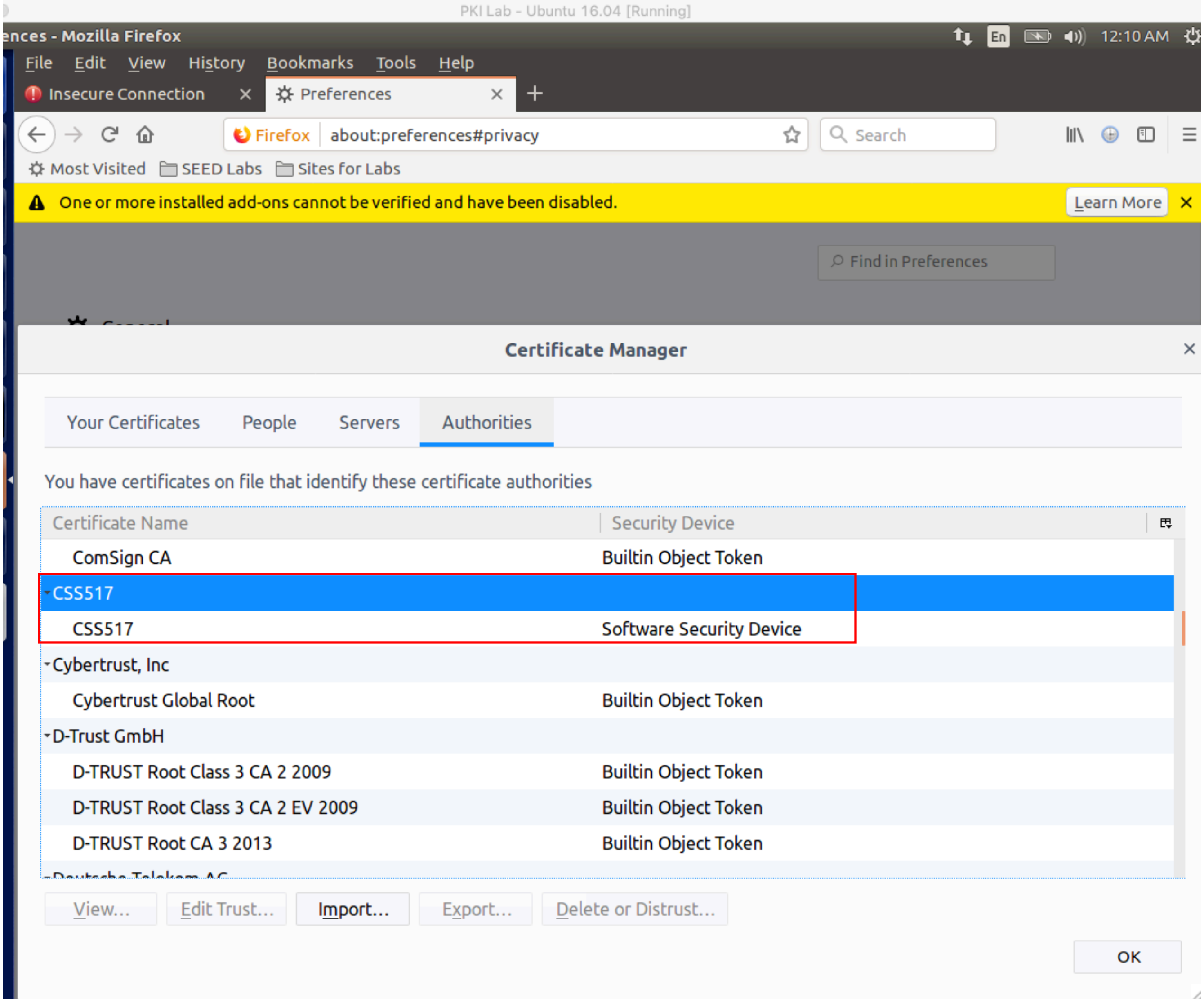
☐ Trust this CA to identify email users.

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

Examine CA certificate

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

Screenshot 16: Seeing the certificate within the Firefox certificate manager.



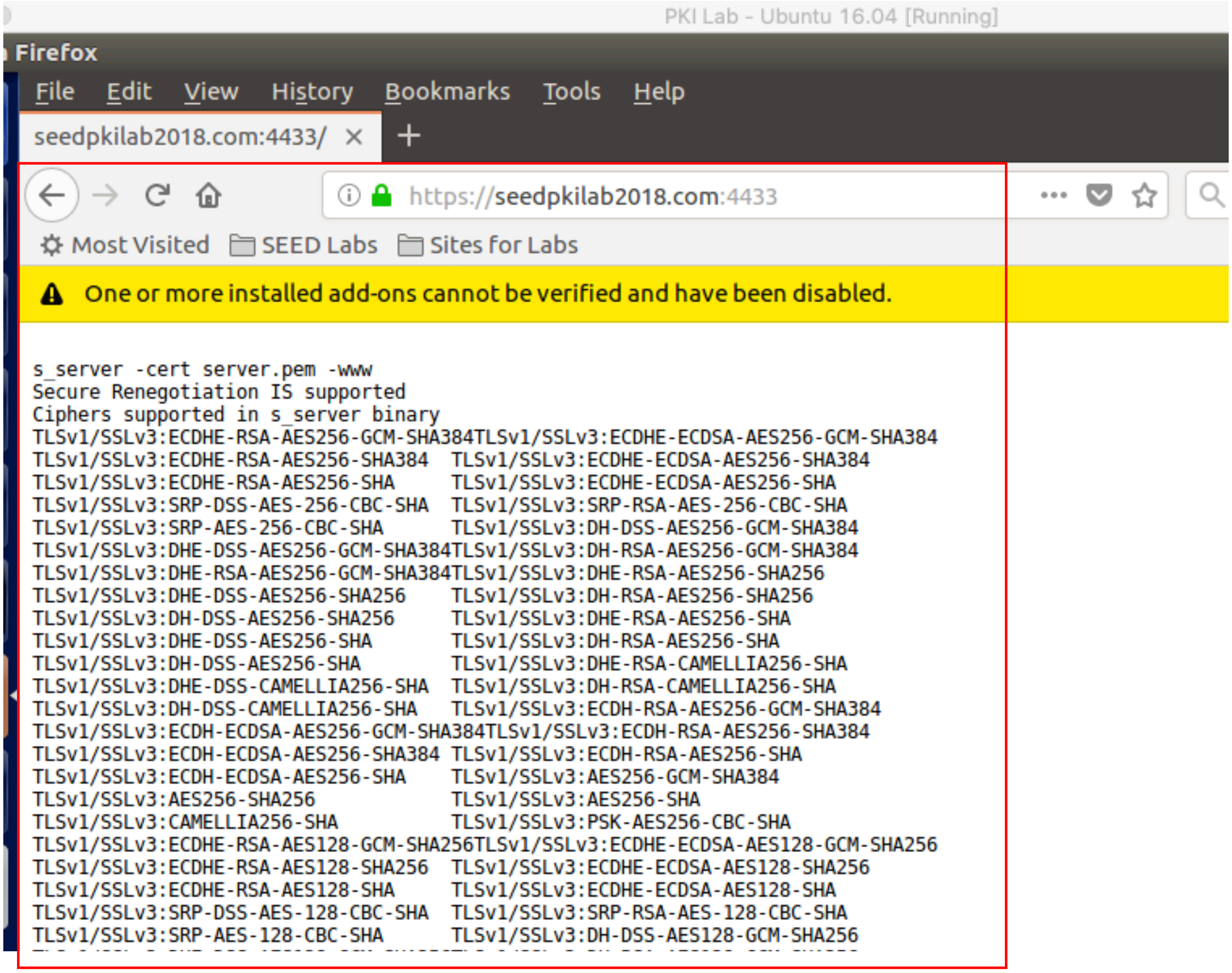
One or more installed add-ons cannot be verified and have been disabled.

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
ComSign CA	Builtin Object Token
CSS517	
CSS517	Software Security Device
Cybertrust, Inc	
Cybertrust Global Root	Builtin Object Token
D-Trust GmbH	
D-TRUST Root Class 3 CA 2 2009	Builtin Object Token
D-TRUST Root Class 3 CA 2 EV 2009	Builtin Object Token
D-TRUST Root CA 3 2013	Builtin Object Token
Deutsche Telekom AG	

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

Screenshot 17: Going to the website and noticing that HTTPS is now enabled, and that the website does not present an error. I am also now able to load the website without any warnings.

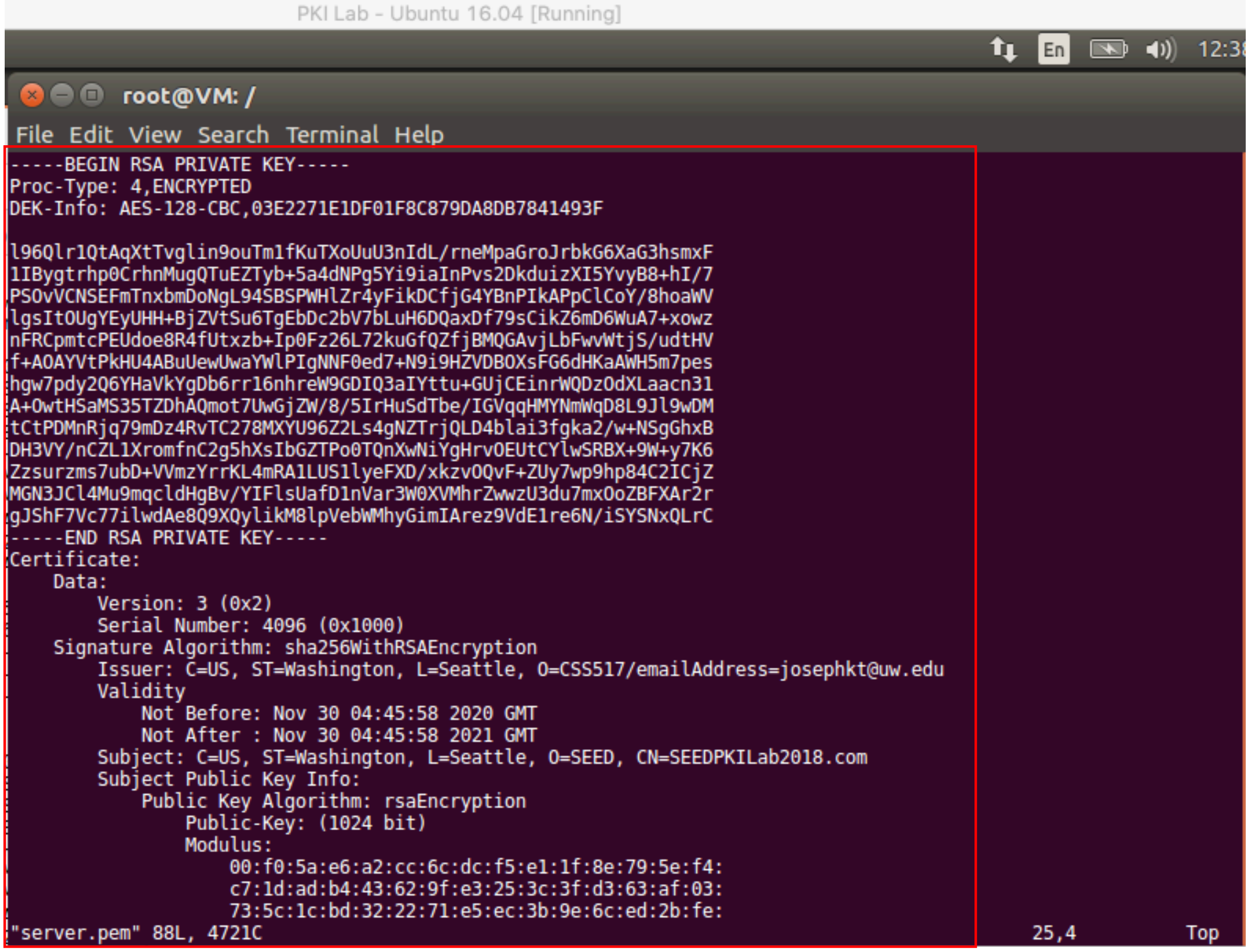


One or more installed add-ons cannot be verified and have been disabled.

```
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
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

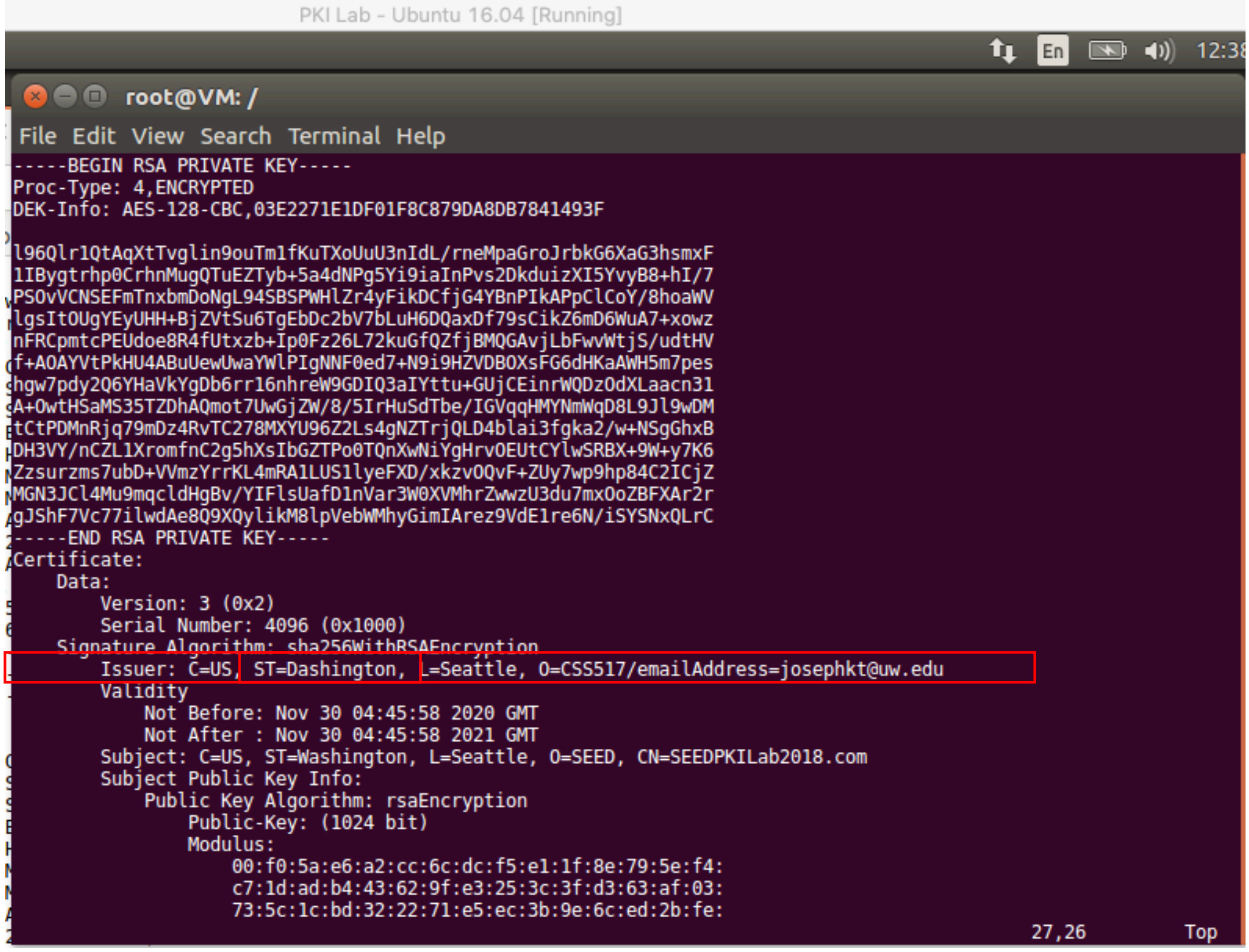
Screenshot 18: Task 3 Step 4 - server.pem File before modification.


PKI Lab - Ubuntu 16.04 [Running]
En
12:3
root@VM: /
File Edit View Search Terminal Help

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,03E2271E1DF01F8C879DA8DB7841493F

l96Qlr1QtAqXtTvglin9ouTm1fKuTXoUuU3nIdL/rneMpaGroJrbkG6XaG3hsmxF
1IBygtrhp0CrhnMugQTuEZTyb+5a4dNPg5Yi9iaInPvs2DkduizXI5YvyB8+hI/7
PSOvVCNSEFmTnxbmDoNgL94SBSPWHlZr4yFikDCfjG4YBnPIkAPpClCoY/8hoaWV
lgsItOUgYEyUHH+BjZVtSu6TgEbDc2bV7bLuH6DQaxDf79sCikZ6mD6WuA7+xowz
nFRCpmtcPEUdoe8R4fUtxzb+Ip0Fz26L72kuGfQZfjBMQGAvjLbFwvWtjS/udtHV
f+AOAYVtPkHU4ABuUewUwaYWlPIgNNF0ed7+N9i9HZVDBOXsFG6dHKaAWH5m7pes
hgw7pdy2Q6YHaVkYgDb6rr16nhreW9GDIQ3aIYttu+GUjCEinrWQDzOdXLaacn31
A+OwtHSaMS35TZDhAQmot7UwGjZW/8/5IrHuSdTbe/IGVqqHMYNmWqD8L9Jl9wDM
tCtPDMnRjq79mDz4RvTC278MXYU96Z2Ls4gNZTrjQLD4blai3fgka2/w+NSgGhxB
DH3VY/nCZL1XromfnC2g5hXsIbGZTPo0TQnXwNiYgHrvOEUtCYlwSRBX+9W+y7K6
Zzsurzms7ubD+VVmzYrrKL4mRA1LUS1lyeFXD/xkzvOQvF+ZUy7wp9hp84C2ICjZ
MGN3JCl4Mu9mqcldHgBv/YIFlsUafD1nVar3W0XVMhrZwwzU3du7mxOoZBFXAr2r
gJShF7Vc77ilwdAe8Q9XQylikM8lpVebWMhyGimIArez9VdE1re6N/iSYSNxQLrC
-----END RSA PRIVATE KEY-----
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Seattle, O=CSS517/emailAddress=josephkt@uw.edu
        Validity
            Not Before: Nov 30 04:45:58 2020 GMT
            Not After : Nov 30 04:45:58 2021 GMT
        Subject: C=US, ST=Washington, L=Seattle, O=SEED, CN=SEEDPKILab2018.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:f0:5a:e6:a2:cc:6c:dc:f5:e1:1f:8e:79:5e:f4:
                    c7:1d:ad:b4:43:62:9f:e3:25:3c:3f:d3:63:af:03:
                    73:5c:1c:bd:32:22:71:e5:ec:3b:9e:6c:ed:2b:fe:
"server.pem" 88L, 4721C                                               25,4          Top
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

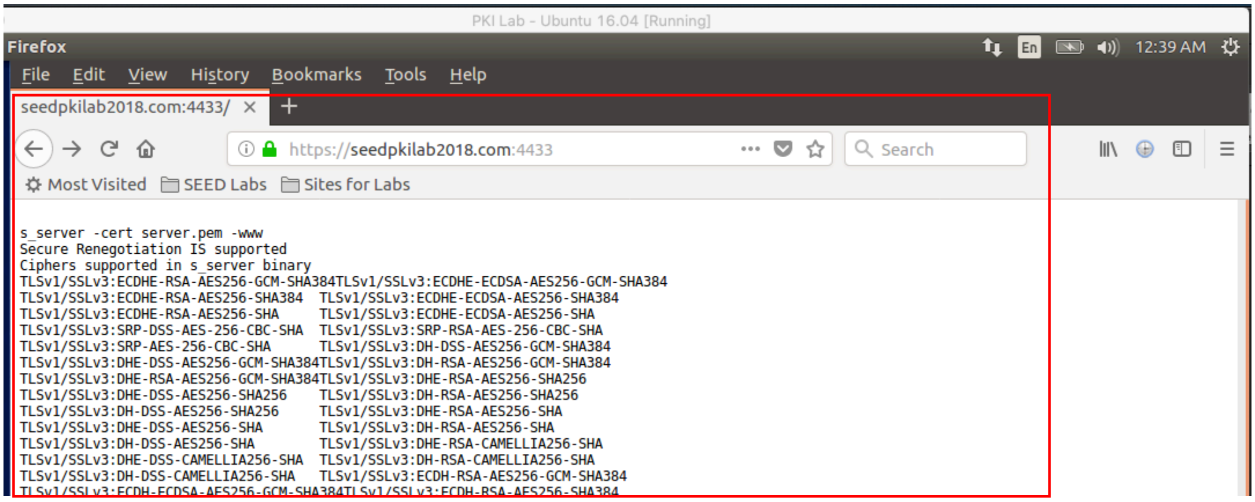
Screenshot 19: File after modification (I changed the “W” in “Washington” to a “D”).



PKI Lab - Ubuntu 16.04 [Running]
En
12:38
root@VM: /
File Edit View Search Terminal Help

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,03E2271E1DF01F8C879DA8DB7841493F

l96Qlr1QtAqXtTvglin9ouTm1fKuTXoUuU3nIdL/rneMpaGroJrbkG6XaG3hsmxF
1IBygtrhp0CrhnMugQTuEZTyb+5a4dNPg5Yi9iaInPvs2DkduizXI5YvyB8+hI/7
PSOvVCNSEFmTnxbmDoNgL94SBSPWHlZr4yFikDCfjG4YBnPIkAPpClCoY/8hoaWV
lgsItOUgYEyUHH+BjZVtSu6TgEbDc2bV7bLuH6DQaxDf79sCikZ6mD6WuA7+xowz
nFRCpmtcPEUdoe8R4fUtxzb+Ip0Fz26L72kuGfQZfjBMQGAvjLbFwvWtjS/udtHV
f+AOAYVtPkHU4ABuUewUwaYWlPIgNNF0ed7+N9i9HZVDBOXsFG6dHKaAWH5m7pes
hgw7pdy2Q6YHaVkYgDb6rr16nhreW9GDIQ3aIYttu+GUjCEinrWQDzOdXLaacn31
A+OwtHSaMS35TZDhAQmot7UwGjZW/8/5IrHuSdTbe/IGVqqHMYNmWqD8L9Jl9wDM
tCtPDMnRjq79mDz4RvTC278MXYU96Z2Ls4gNZTrjQLD4blai3fgka2/w+NSgGhxB
DH3VY/nCZL1XromfnC2g5hXsIbGZTPo0TQnXwNiYgHrvOEUtCYlwSRBX+9W+y7K6
Zzsurzms7ubD+VVmzYrrKL4mRA1LUS1lyeFXD/xkzvOQvF+ZUy7wp9hp84C2ICjZ
MGN3JCl4Mu9mqcldHgBv/YIFlsUafD1nVar3W0XVMhrZwwzU3du7mxOoZBFXAr2r
gJShF7Vc77ilwdAe8Q9XQylikM8lpVebWMhyGimIArez9VdE1re6N/iSYSNxQLrC
-----END RSA PRIVATE KEY-----
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Dashington, L=Seattle, O=CSS517/emailAddress=josephkt@uw.edu
        Validity
            Not Before: Nov 30 04:45:58 2020 GMT
            Not After : Nov 30 04:45:58 2021 GMT
        Subject: C=US, ST=Washington, L=Seattle, O=SEED, CN=SEEDPKILab2018.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:f0:5a:e6:a2:cc:6c:dc:f5:e1:1f:8e:79:5e:f4:
                    c7:1d:ad:b4:43:62:9f:e3:25:3c:3f:d3:63:af:03:
                    73:5c:1c:bd:32:22:71:e5:ec:3b:9e:6c:ed:2b:fe:
                                                       27,26         Top
```

Screenshot 20: Task 3, Step 4, Question 1 – After changing a byte within server.pem, I was still able to load the website without any evident issues. Prior to changing the “W” in “Washington” to a “D”, I had changed a different byte that corrupted the file and made the website unloadable.

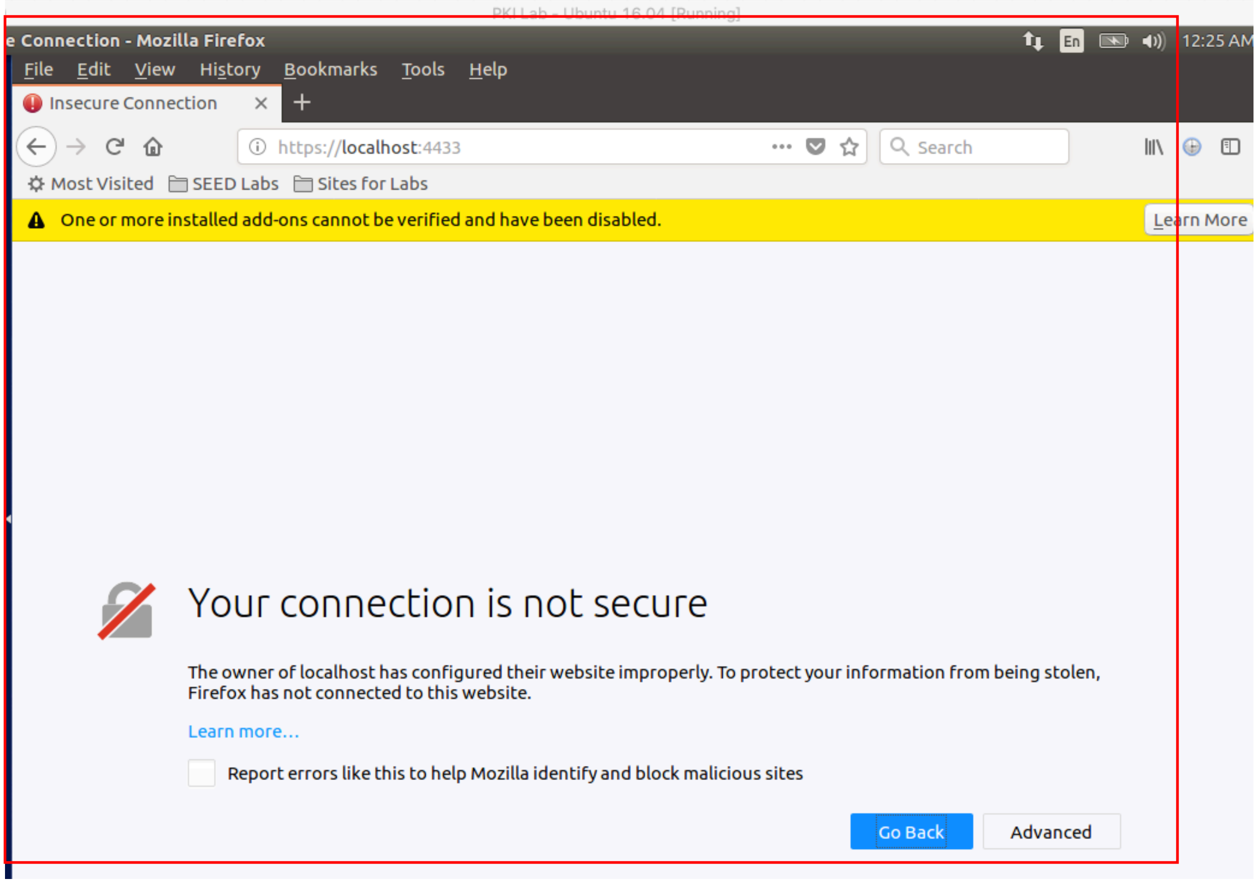


PKI Lab - Ubuntu 16.04 [Running]
Firefox
En
12:39 AM
File Edit View History Bookmarks Tools Help
seedpkilab2018.com:4433/
https://seedpkilab2018.com:4433
Search
Most Visited
SEED Labs
Sites for Labs

```
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
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

Screenshot 21: Task 3, Step 4, Question 2 – Upon attempting to connect to localhost, Firefox indicated that is unsecured. This makes sense, because only the common name of SEEDPKILab2018.com was registered with the CA, not “localhost”.



One or more installed add-ons cannot be verified and have been disabled.

Your connection is not secure

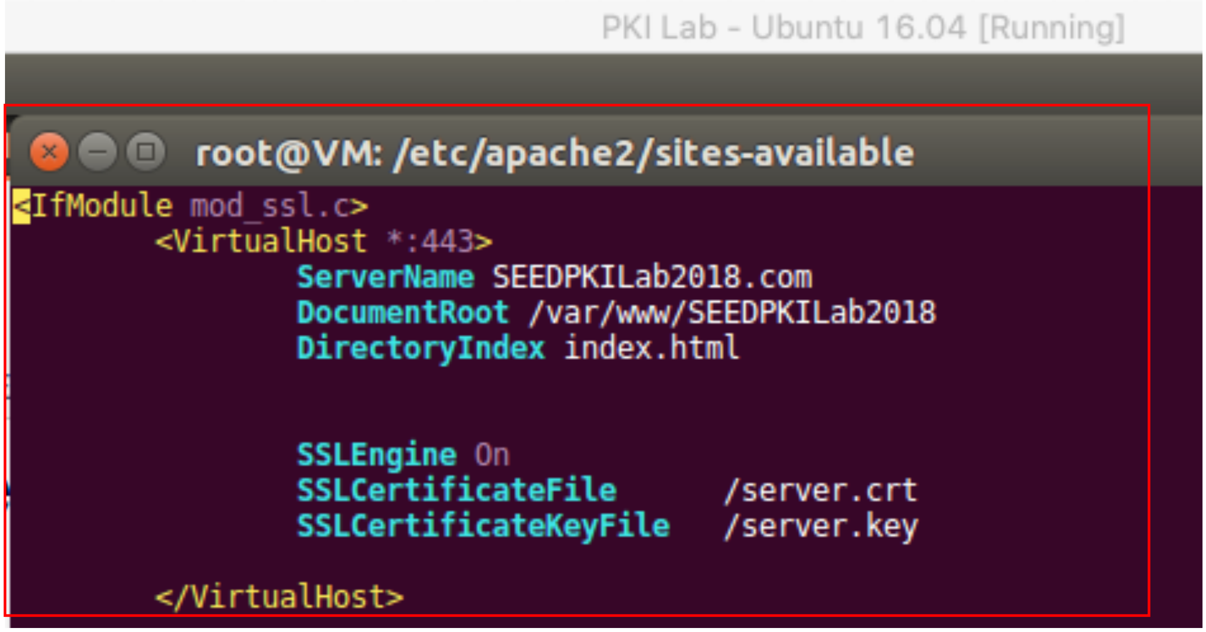
The owner of localhost has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

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

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

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

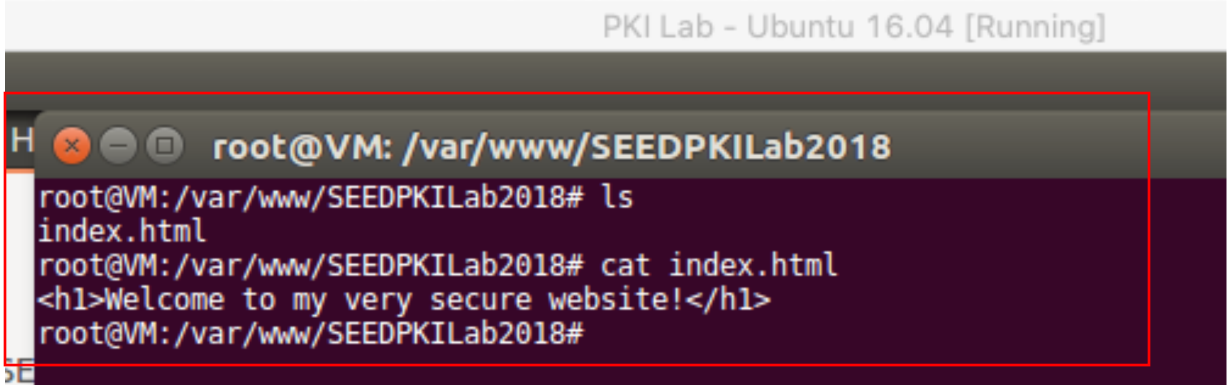
Screenshot 22: Setting up SSL and adjusting the code to point to the relevant key and certificate.



PKI Lab - Ubuntu 16.04 [Running]
root@VM: /etc/apache2/sites-available

```
<IfModule mod_ssl.c>
        <VirtualHost *:443>
                ServerName SEEDPKILab2018.com
                DocumentRoot /var/www/SEEDPKILab2018
                DirectoryIndex index.html


                SSLEngine On
                SSLCertificateFile      /server.crt
                SSLCertificateKeyFile   /server.key

        </VirtualHost>
```

Screenshot 23: I also created a basic HTML website in the relevant directory which would load upon a successful https connection to the website.

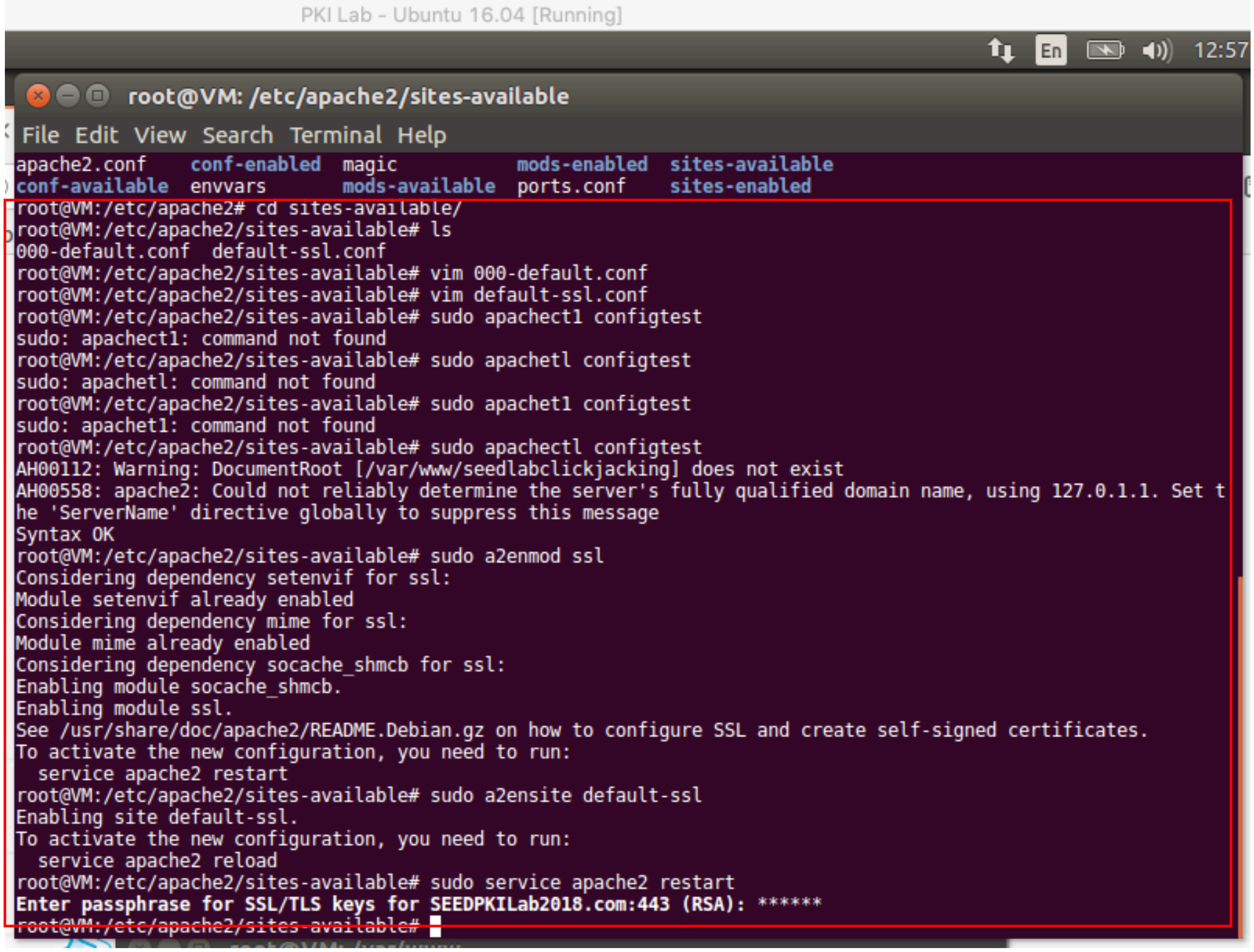


PKI Lab - Ubuntu 16.04 [Running]
root@VM: /var/www/SEEDPKILab2018

```
root@VM:/var/www/SEEDPKILab2018# ls
index.html
root@VM:/var/www/SEEDPKILab2018# cat index.html
<h1>Welcome to my very secure website!</h1>
root@VM:/var/www/SEEDPKILab2018#
```

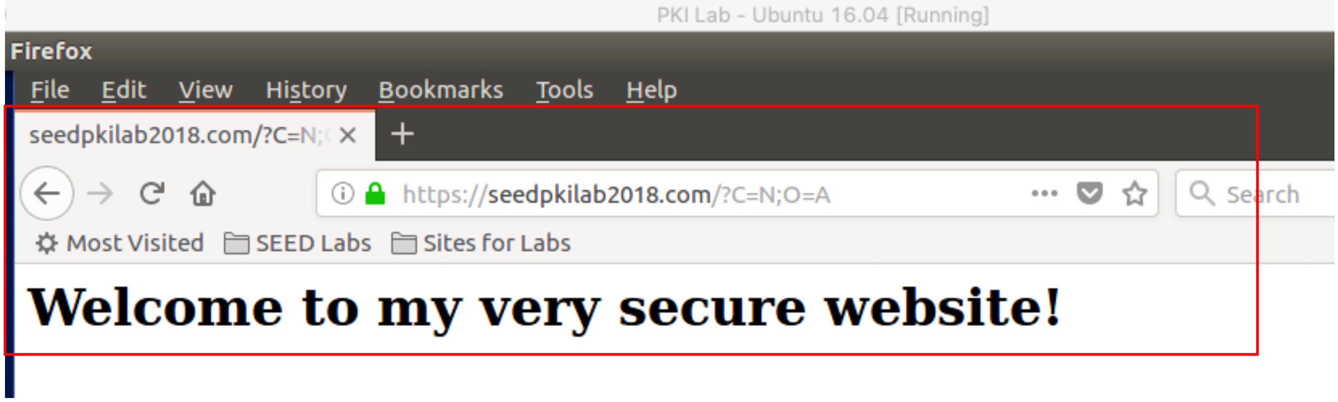
Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

Screenshot 24: Running the apache commands to set up and enable SSL.


PKI Lab - Ubuntu 16.04 [Running]
En
12:57
root@VM: /etc/apache2/sites-available
File Edit View Search Terminal Help

```
apache2.conf    conf-enabled  magic          mods-enabled  sites-available
conf-available  envvars       mods-available ports.conf    sites-enabled
root@VM:/etc/apache2# cd sites-available/
root@VM:/etc/apache2/sites-available# ls
000-default.conf  default-ssl.conf
root@VM:/etc/apache2/sites-available# vim 000-default.conf
root@VM:/etc/apache2/sites-available# vim default-ssl.conf
root@VM:/etc/apache2/sites-available# sudo apachect1 configtest
sudo: apachect1: command not found
root@VM:/etc/apache2/sites-available# sudo apachetl configtest
sudo: apachetl: command not found
root@VM:/etc/apache2/sites-available# sudo apachet1 configtest
sudo: apachet1: command not found
root@VM:/etc/apache2/sites-available# 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 t
he 'ServerName' directive globally to suppress this message
Syntax OK
root@VM:/etc/apache2/sites-available# 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:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart
root@VM:/etc/apache2/sites-available# sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  service apache2 reload
root@VM:/etc/apache2/sites-available# sudo service apache2 restart
Enter passphrase for SSL/TLS keys for SEEDPKILab2018.com:443 (RSA): ******
root@VM:/etc/apache2/sites-available# 
```

Screenshot 25: Loading seedpkilab2018.com via an https connection, and noting that my custom html page had loaded.

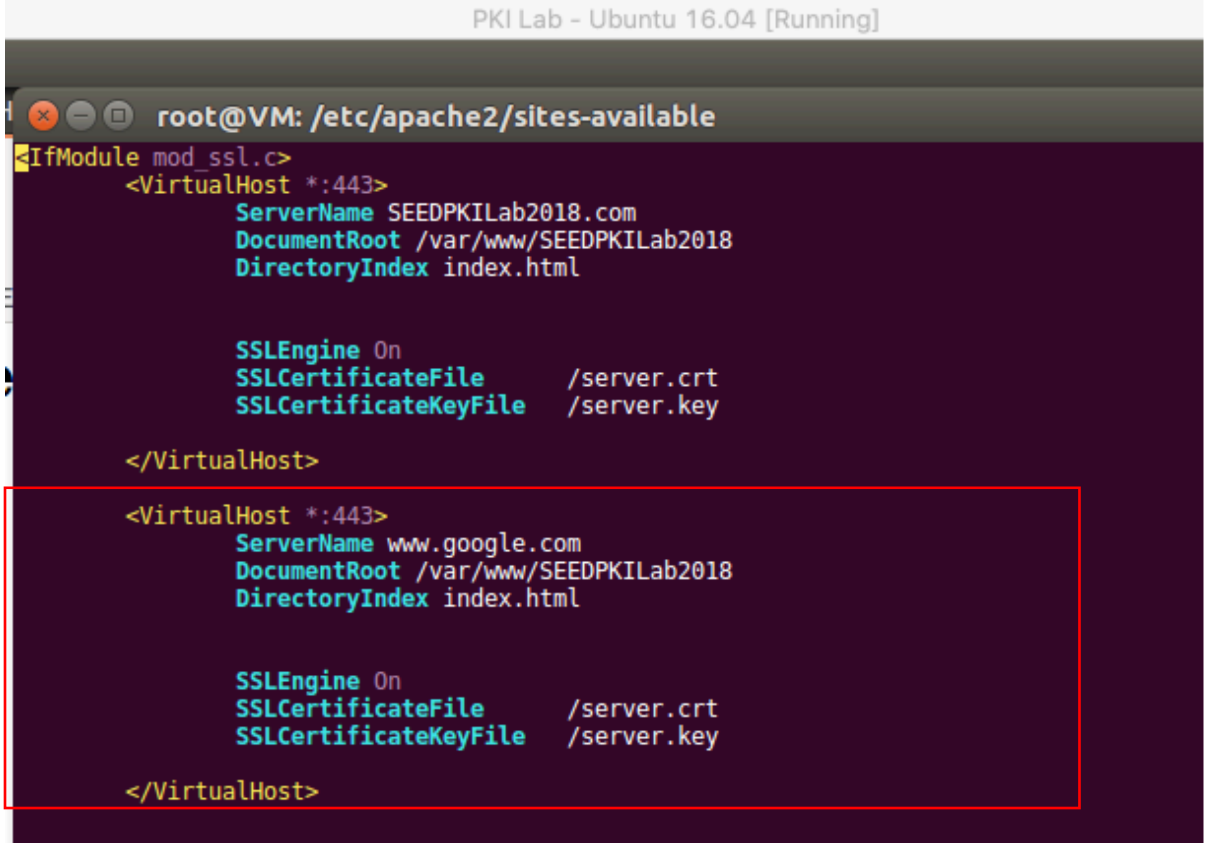

PKI Lab - Ubuntu 16.04 [Running]
Firefox
File Edit View History Bookmarks Tools Help
seedpkilab2018.com/?C=N;
https://seedpkilab2018.com/?C=N;O=A
Search
Most Visited
SEED Labs
Sites for Labs

Welcome to my very secure website!

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

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

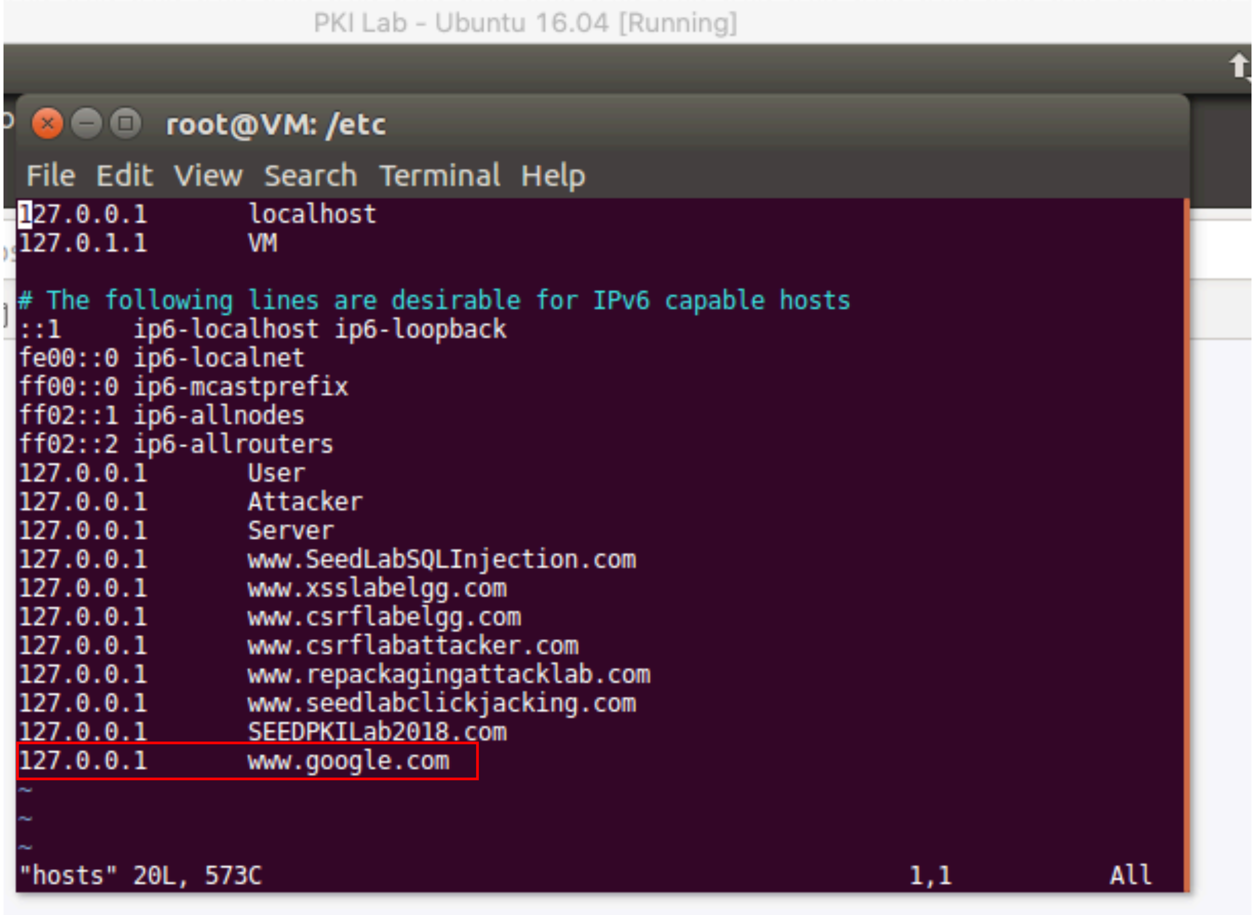
Screenshot 26: Creating an entry for Google.com which points back to the website I had created in Task 4.


PKI Lab - Ubuntu 16.04 [Running]
root@VM: /etc/apache2/sites-available

```
<IfModule mod_ssl.c>
        <VirtualHost *:443>
                ServerName SEEDPKILab2018.com
                DocumentRoot /var/www/SEEDPKILab2018
                DirectoryIndex index.html


                SSLEngine On
                SSLCertificateFile      /server.crt
                SSLCertificateKeyFile   /server.key

        </VirtualHost>

        <VirtualHost *:443>
                ServerName www.google.com
                DocumentRoot /var/www/SEEDPKILab2018
                DirectoryIndex index.html


                SSLEngine On
                SSLCertificateFile      /server.crt
                SSLCertificateKeyFile   /server.key

        </VirtualHost>
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

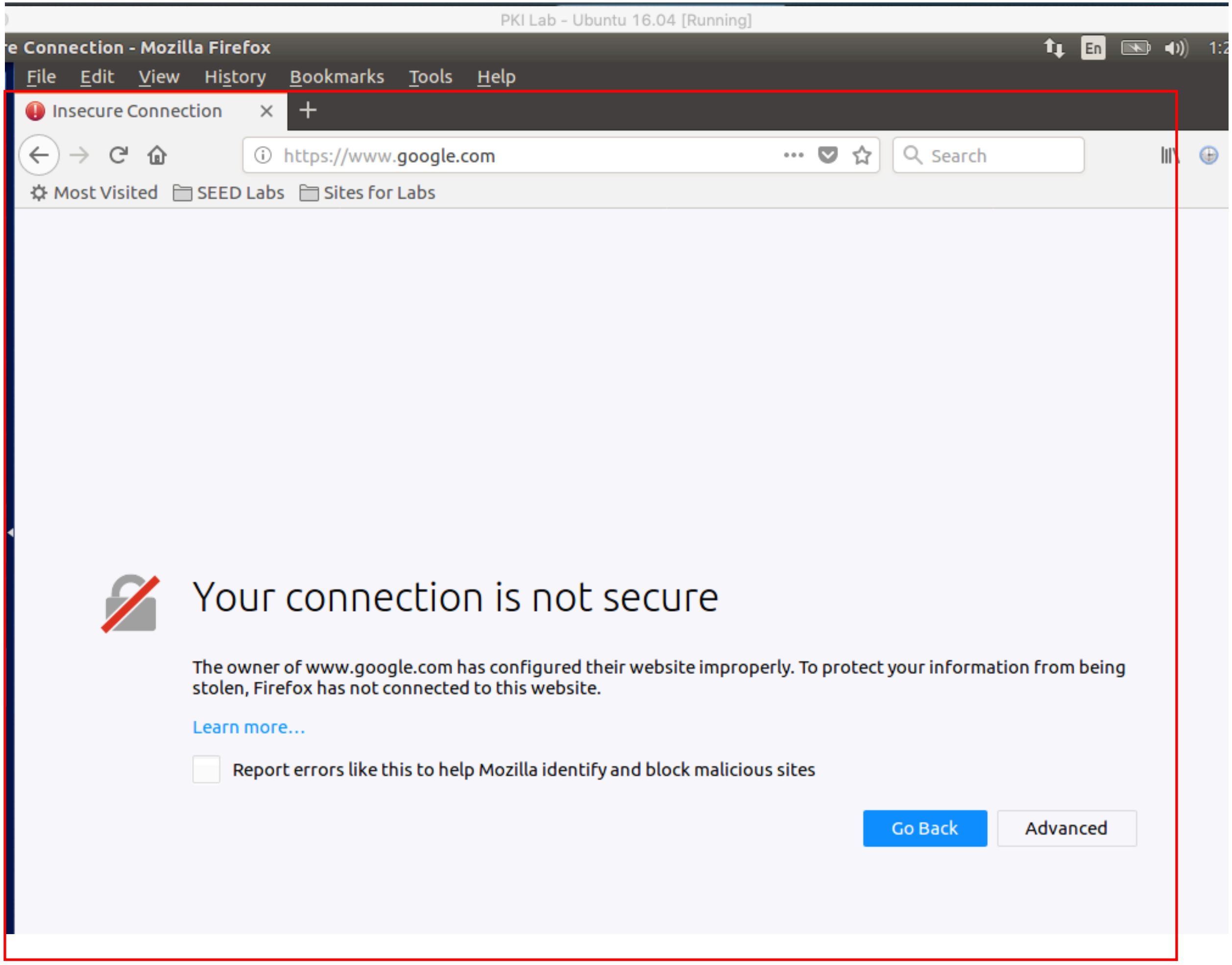
Screenshot 27: “Attacking” the DNS by editing the ip address for google.com to point to 127.0.0.1.


PKI Lab - Ubuntu 16.04 [Running]
root@VM: /etc
File Edit View Search Terminal Help

```
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.csrflabattacker.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       www.google.com
~
~
~
"hosts" 20L, 573C                                             1,1           All
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

Screenshot 28: Task 5 Step 3 – Attempting to visit google.com via an https connection. The URL does not match the common name of what was signed within the certificate and thus, Firefox does not trust going to the website. An attempted https connection cannot be established with the given website. I found this to be a key learning point of the lab in that it taught me how browsers, when combined with the usage of PKI, can prevent users from accessing malicious websites. Hence, I gained a better understanding of PKI in this task through learning how PKI allows the browser to "trust" a given website and ultimately, permit the user to access it without any warnings like the one seen below.


PKI Lab - Ubuntu 16.04 [Running]
e Connection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Insecure Connection
https://www.google.com
Search
Most Visited
SEED Labs
Sites for Labs

Your connection is not secure

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

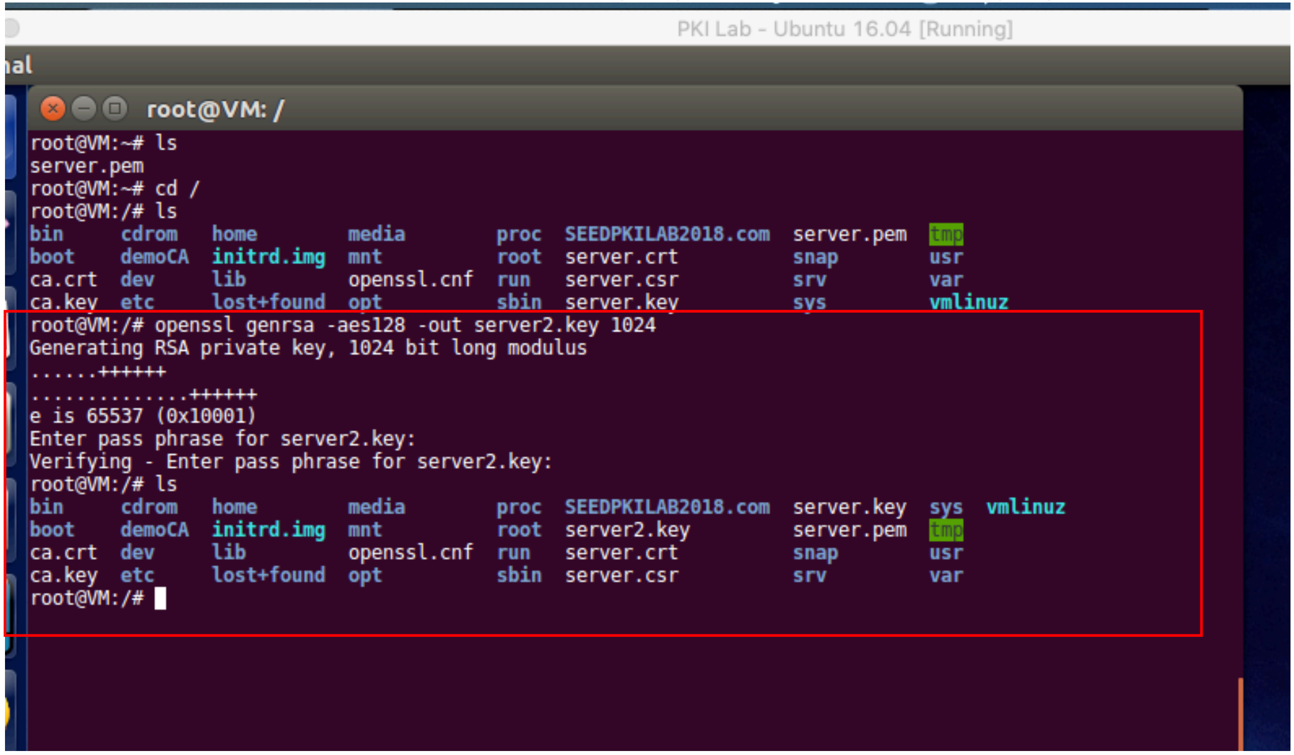
Learn more…

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

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

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

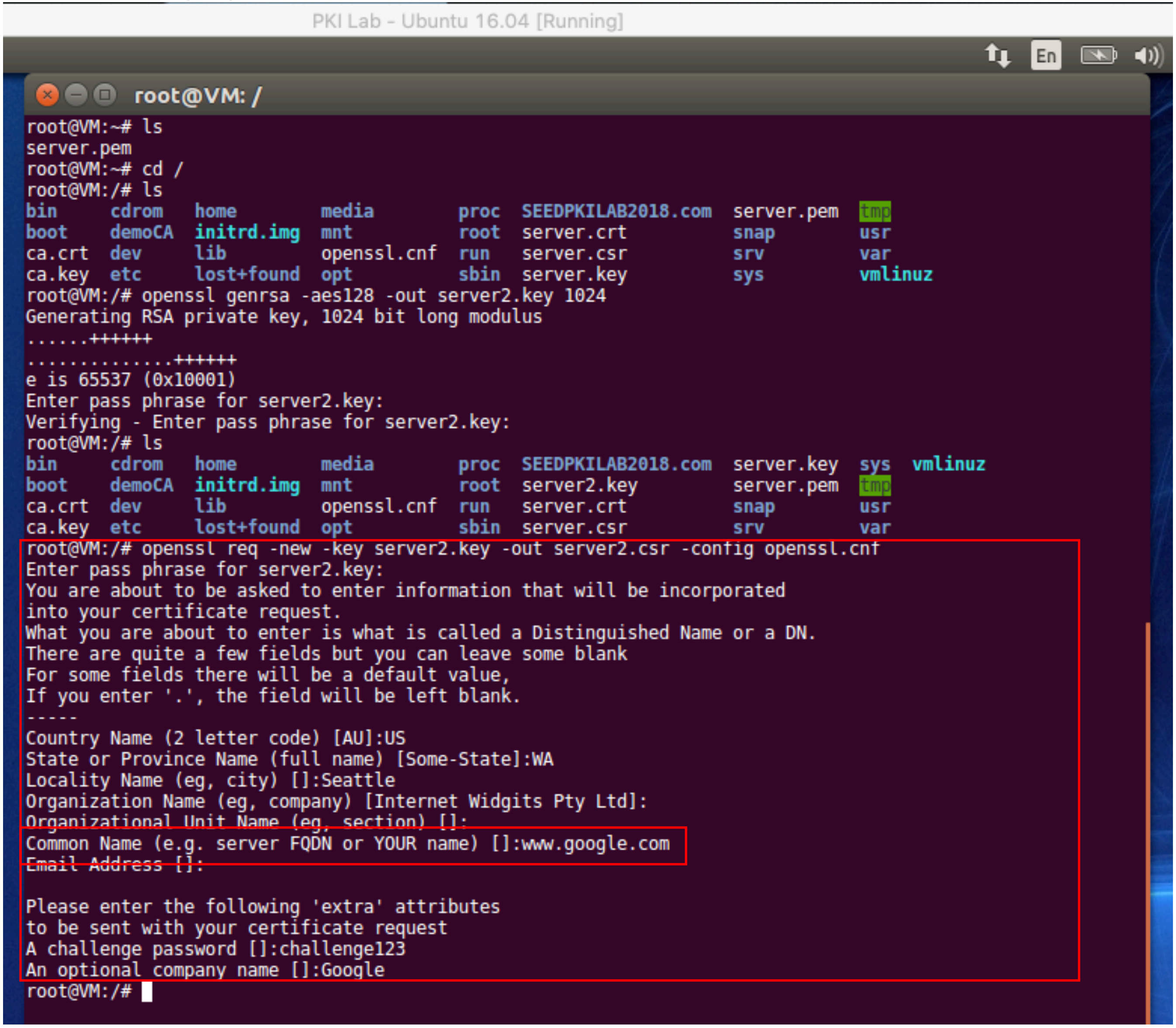
Screenshot 29: Creating a fake key to use for signing the certificate of www.google.com.



```
root@VM:~# ls
server.pem
root@VM:~# cd /
root@VM:/# ls
bin     cdrom   home        media        proc  SEEDPKILAB2018.com  server.pem  tmp
boot    demoCA  initrd.img  mnt          root  server.crt          snap        usr
ca.crt  dev     lib         openssl.cnf  run   server.csr          srv         var
ca.key  etc     lost+found  opt          sbin  server.key          sys         vmlinuz
root@VM:/# openssl genrsa -aes128 -out server2.key 1024
Generating RSA private key, 1024 bit long modulus
......++++++
..............++++++
e is 65537 (0x10001)
Enter pass phrase for server2.key:
Verifying - Enter pass phrase for server2.key:
root@VM:/# ls
bin     cdrom   home        media        proc  SEEDPKILAB2018.com  server.key  sys  vmlinuz
boot    demoCA  initrd.img  mnt          root  server2.key         server.pem  tmp
ca.crt  dev     lib         openssl.cnf  run   server.crt          snap        usr
ca.key  etc     lost+found  opt          sbin  server.csr          srv         var
root@VM:/# 
```

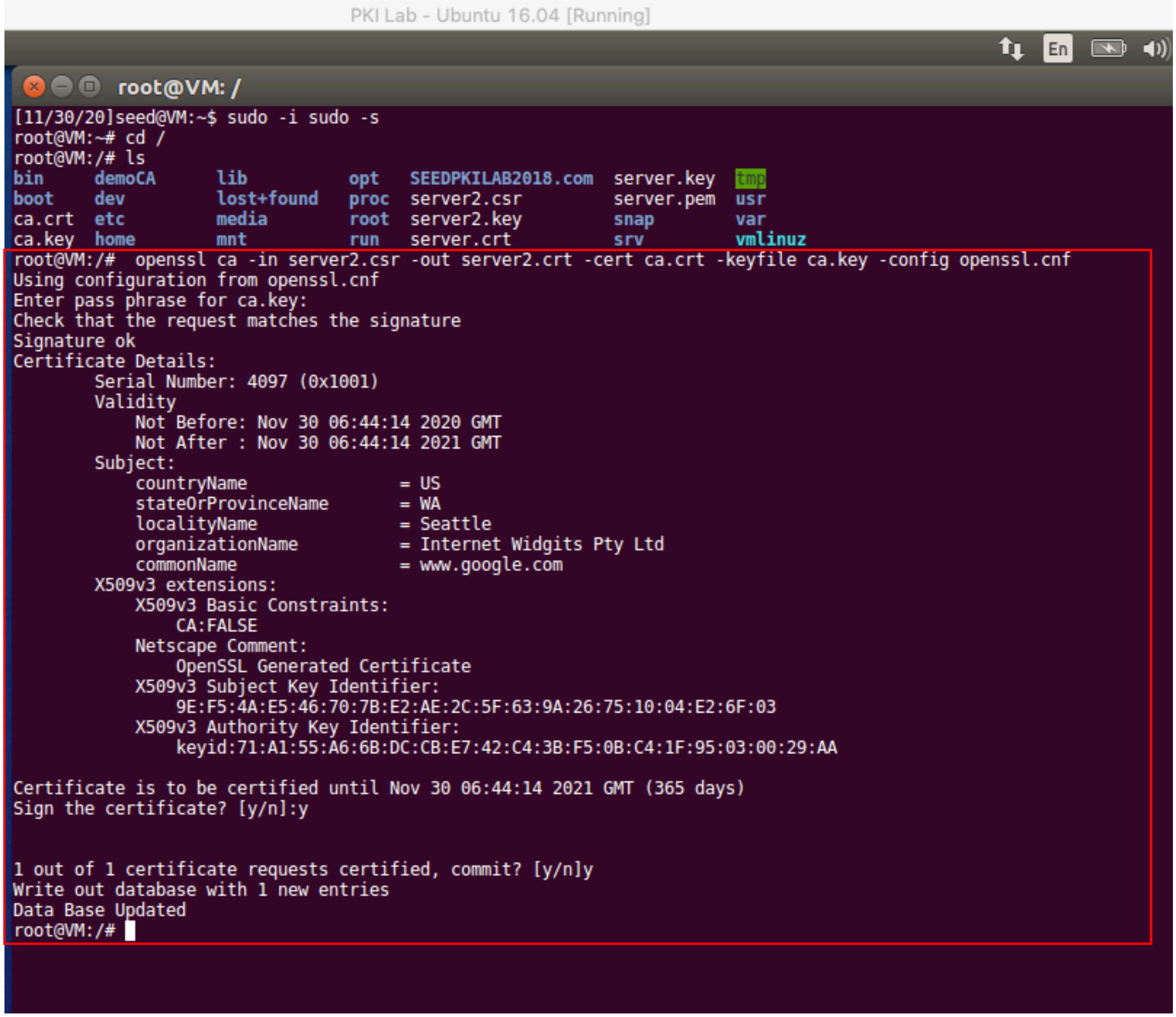
Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

Screenshot 30: Creating a fake certificate signing request from Google, and using the common name of "www.google.com".



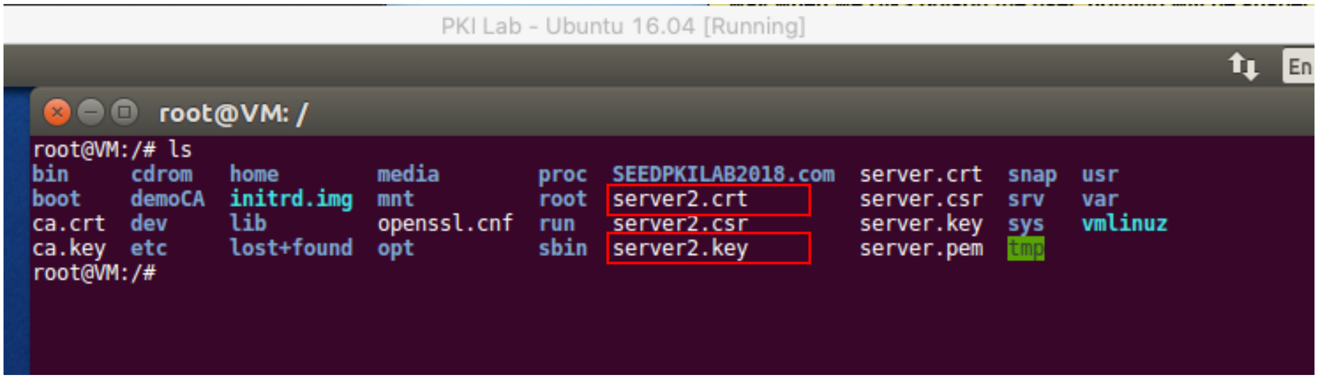
```
root@VM:~# ls
server.pem
root@VM:~# cd /
root@VM:/# ls
bin      cdrom    home        media        proc  SEEDPKILAB2018.com  server.pem  tmp
boot     demoCA   initrd.img  mnt          root  server.crt          snap        usr
ca.crt   dev      lib         openssl.cnf  run   server.csr          srv         var
ca.key   etc      lost+found  opt          sbin  server.key          sys         vmlinuz
root@VM:/# openssl genrsa -aes128 -out server2.key 1024
Generating RSA private key, 1024 bit long modulus
......++++++
..............++++++
e is 65537 (0x10001)
Enter pass phrase for server2.key:
Verifying - Enter pass phrase for server2.key:
root@VM:/# ls
bin      cdrom    home        media        proc  SEEDPKILAB2018.com  server.key  sys  vmlinuz
boot     demoCA   initrd.img  mnt          root  server2.key         server.pem  tmp
ca.crt   dev      lib         openssl.cnf  run   server.crt          snap        usr
ca.key   etc      lost+found  opt          sbin  server.csr          srv         var
root@VM:/# openssl req -new -key server2.key -out server2.csr -config openssl.cnf
Enter pass phrase for server2.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]:WA
Locality Name (eg, city) []:Seattle
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:www.google.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:challenge123
An optional company name []:Google
root@VM:/# 
```

Screenshot 31: Signing the fake key as the certificate authority.



```
[11/30/20]seed@VM:~$ sudo -i sudo -s
root@VM:~# cd /
root@VM:/# ls
bin      demoCA      lib          opt   SEEDPKILAB2018.com  server.key  tmp
boot     dev         lost+found   proc  server2.csr         server.pem  usr
ca.crt   etc         media        root  server2.key         snap        var
ca.key   home        mnt          run   server.crt          srv         vmlinuz
root@VM:/#  openssl ca -in server2.csr -out server2.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: 4097 (0x1001)
        Validity
            Not Before: Nov 30 06:44:14 2020 GMT
            Not After : Nov 30 06:44:14 2021 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = WA
            localityName              = Seattle
            organizationName          = Internet Widgits Pty Ltd
            commonName                = www.google.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                9E:F5:4A:E5:46:70:7B:E2:AE:2C:5F:63:9A:26:75:10:04:E2:6F:03
            X509v3 Authority Key Identifier:
                keyid:71:A1:55:A6:6B:DC:CB:E7:42:C4:3B:F5:0B:C4:1F:95:03:00:29:AA

Certificate is to be certified until Nov 30 06:44:14 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
root@VM:/# 
```

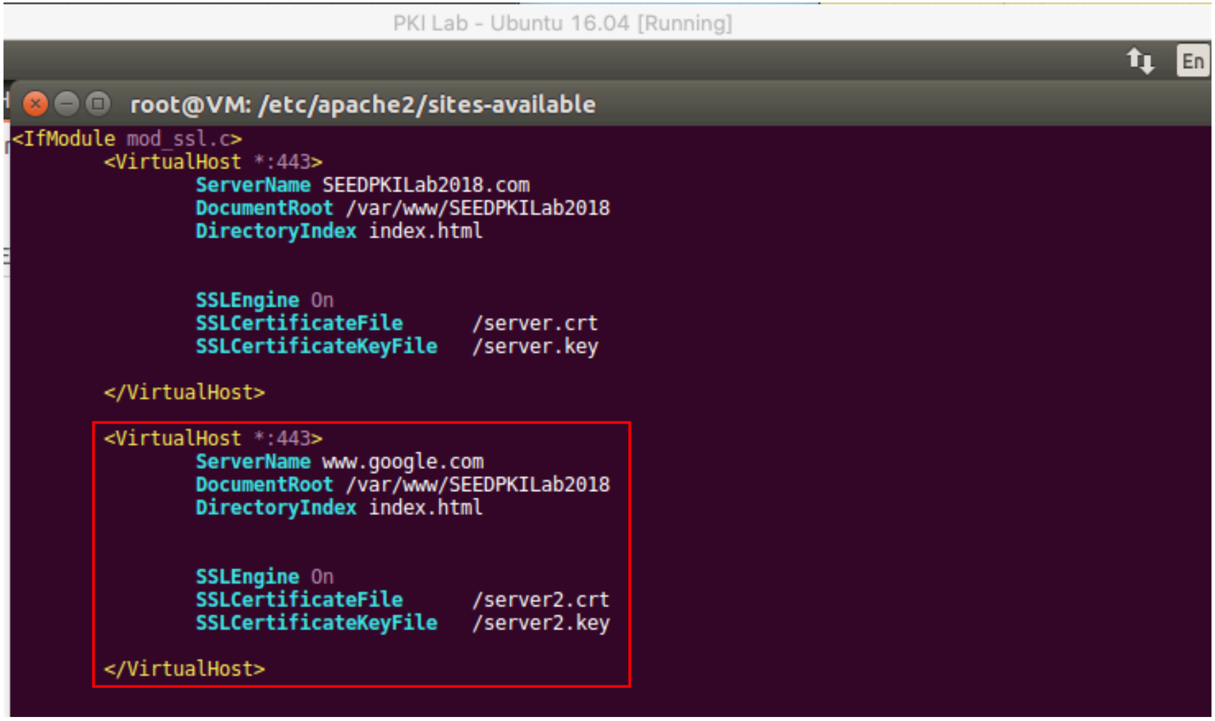
Screenshot 32: Verifying that the key (server2.key) and certificate (server2.crt) had been made



```
root@VM:/# ls
bin     cdrom   home        media        proc  SEEDPKILAB2018.com  server.crt  snap  usr
boot    demoCA  initrd.img  mnt          root  server2.crt         server.csr  srv   var
ca.crt  dev     lib         openssl.cnf  run   server2.csr         server.key  sys   vmlinuz
ca.key  etc     lost+found  opt          sbin  server2.key         server.pem  tmp
root@VM:/#
```

Joseph Tsai
CSS 517 – Assignment 3: PKI Lab
November 29th, 2020

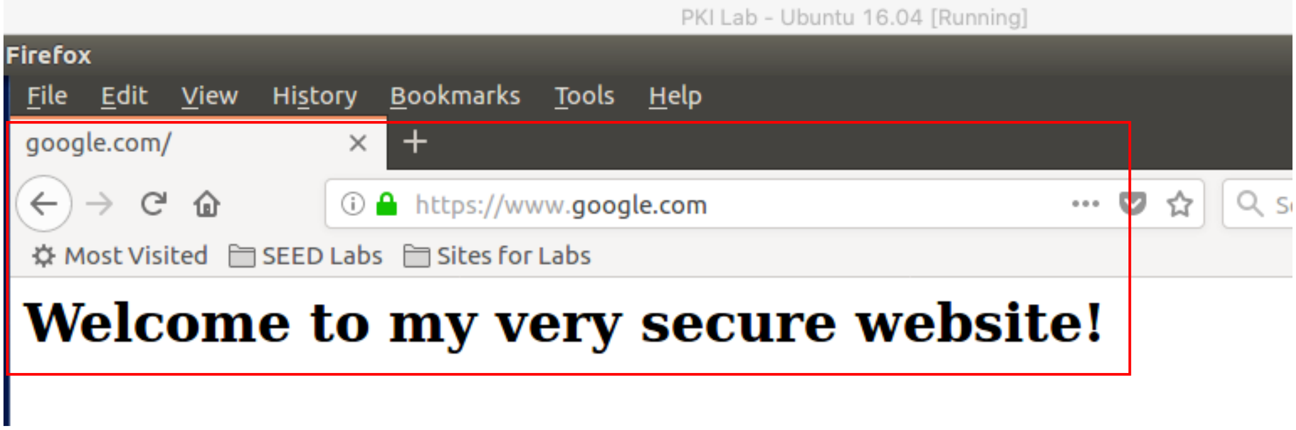
Screenshot 33: Editing the apache file to point to the fake certificate for www.google.com.



PKI Lab - Ubuntu 16.04 [Running]
En
root@VM: /etc/apache2/sites-available

```
<IfModule mod_ssl.c>
        <VirtualHost *:443>
                ServerName SEEDPKILab2018.com
                DocumentRoot /var/www/SEEDPKILab2018
                DirectoryIndex index.html


                SSLEngine On
                SSLCertificateFile      /server.crt
                SSLCertificateKeyFile   /server.key

        </VirtualHost>

        <VirtualHost *:443>
                ServerName www.google.com
                DocumentRoot /var/www/SEEDPKILab2018
                DirectoryIndex index.html


                SSLEngine On
                SSLCertificateFile      /server2.crt
                SSLCertificateKeyFile   /server2.key

        </VirtualHost>
```

Screenshot 34: Reloading https://www.google.com with the fake certificate, which sent the browser to my website instead of www.google.com. Hence, a successful man-in-the-middle attack was completed. In this task, I learned how important it is for CA's to maintain their integrity, as a compromised CA can lead to many users being directed to malicious websites that seem trustworthy to the browser. I also found it quite interesting that just because a website has https enabled, it does not mean that the website can be trusted. This is true not only in the case of a compromised CA, but even in the case where an attacker is able to obtain a legitimate certificate for their malicious website.



Welcome to my very secure website!