Computer Cyber Security

Project 2

Secure a Website with HTTPS

11/06/2018

By: **Pranati Trivedi**

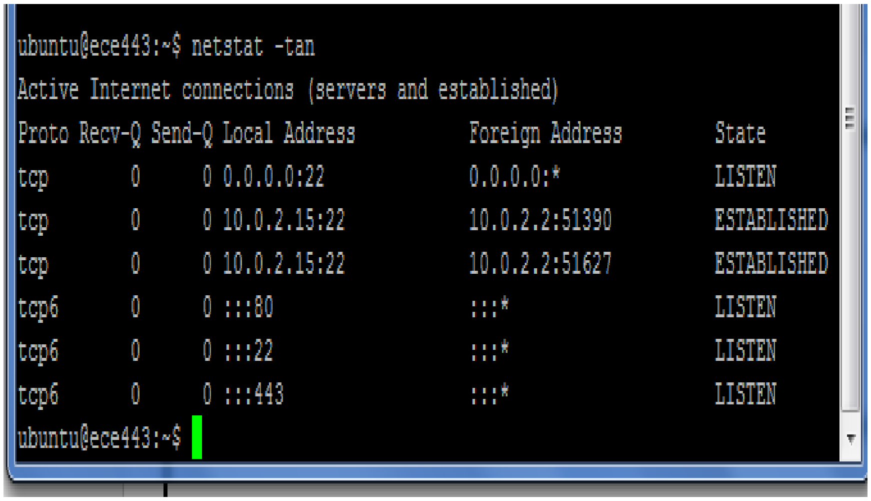
Acknowledgment: I acknowledge that all of the work including figures and codes belong to me and/or persons who are referenced.

Signature: PRANATI TRIVEDI

INDEX

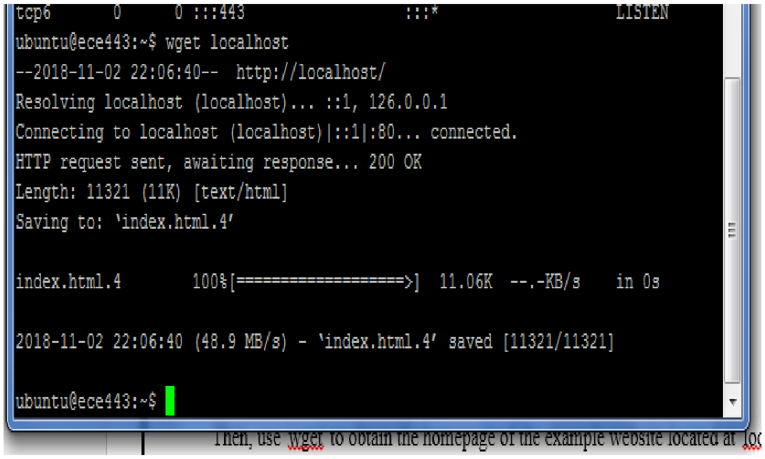
Summary of experimental setup

First I have opened the Putty and use ‘netstat-tan ‘ to verify Apache web server .



```
ubuntu@ece443:~$ netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.15:22            10.0.2.2:51390          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:51627          ESTABLISHED
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
ubuntu@ece443:~$
```

Then, use 'wget' to obtain the homepage of the example website located at 'localhost', which confirms that Apache works properly.



```
tcp6       0      0 :::443                  :::*                    LISTEN
ubuntu@ece443:~$ wget localhost
--2018-11-02 22:06:40--  http://localhost/
Resolving localhost (localhost)... ::1, 126.0.0.1
Connecting to localhost (localhost)|::1|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11321 (11K) [text/html]
Saving to: ‘index.html.4’

index.html.4        100%[===================>]  11.06K  --.-KB/s    in 0s

2018-11-02 22:06:40 (48.9 MB/s) - ‘index.html.4’ saved [11321/11321]

ubuntu@ece443:~$
```

Then, use wget to obtain the homepage of the example website located at loc

wget simply stores the content of the homepage into the file 'index.html'.

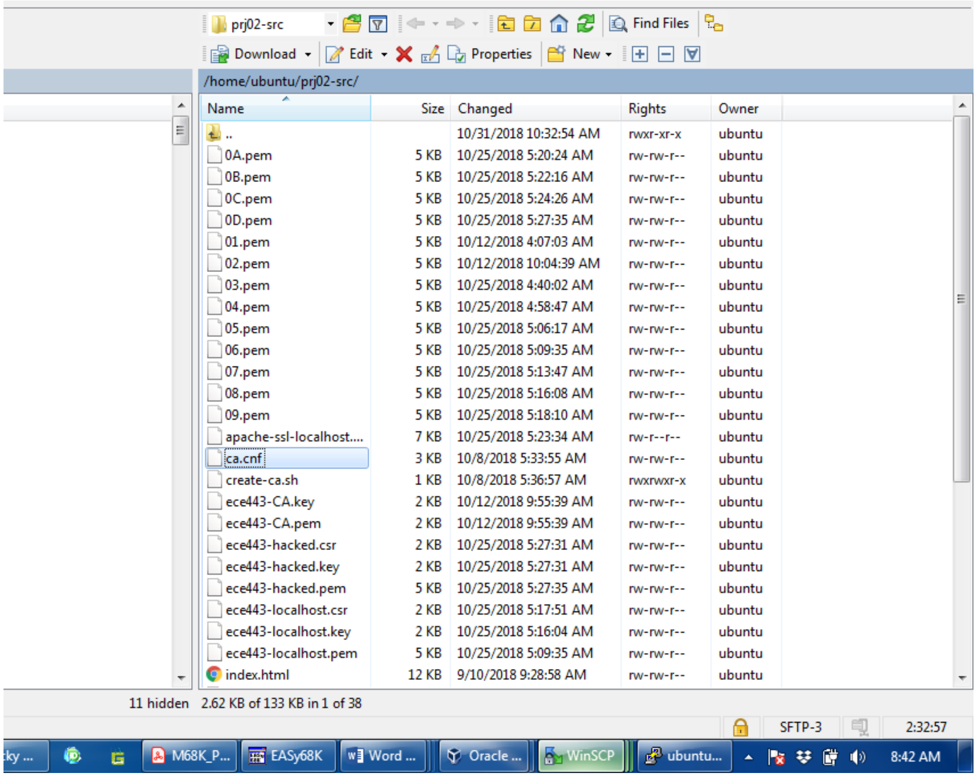
Then I downloaded the source file of Project2 using command:

```
wget http://www.ece.iit.edu/~jwang/ece443-2018f/prj02-src.tgz
```

Extract the file using command:

```
tar -zxf prj02-src.tgz
```

See the files using WinSCP :



Name	Size	Changed	Rights	Owner
..		10/31/2018 10:32:54 AM	rwxr-xr-x	ubuntu
0A.pem	5 KB	10/25/2018 5:20:24 AM	rw-rw-r--	ubuntu
0B.pem	5 KB	10/25/2018 5:22:16 AM	rw-rw-r--	ubuntu
0C.pem	5 KB	10/25/2018 5:24:26 AM	rw-rw-r--	ubuntu
0D.pem	5 KB	10/25/2018 5:27:35 AM	rw-rw-r--	ubuntu
01.pem	5 KB	10/12/2018 4:07:03 AM	rw-rw-r--	ubuntu
02.pem	5 KB	10/12/2018 10:04:39 AM	rw-rw-r--	ubuntu
03.pem	5 KB	10/25/2018 4:40:02 AM	rw-rw-r--	ubuntu
04.pem	5 KB	10/25/2018 4:58:47 AM	rw-rw-r--	ubuntu
05.pem	5 KB	10/25/2018 5:06:17 AM	rw-rw-r--	ubuntu
06.pem	5 KB	10/25/2018 5:09:35 AM	rw-rw-r--	ubuntu
07.pem	5 KB	10/25/2018 5:13:47 AM	rw-rw-r--	ubuntu
08.pem	5 KB	10/25/2018 5:16:08 AM	rw-rw-r--	ubuntu
09.pem	5 KB	10/25/2018 5:18:10 AM	rw-rw-r--	ubuntu
apache-ssl-localhost....	7 KB	10/25/2018 5:23:34 AM	rw-r--r--	ubuntu
ca.cnf	3 KB	10/8/2018 5:33:55 AM	rw-rw-r--	ubuntu
create-ca.sh	1 KB	10/8/2018 5:36:57 AM	rwxrwxr-x	ubuntu
ece443-CA.key	2 KB	10/12/2018 9:55:39 AM	rw-rw-r--	ubuntu
ece443-CA.pem	2 KB	10/12/2018 9:55:39 AM	rw-rw-r--	ubuntu
ece443-hacked.csr	2 KB	10/25/2018 5:27:31 AM	rw-rw-r--	ubuntu
ece443-hacked.key	2 KB	10/25/2018 5:27:31 AM	rw-rw-r--	ubuntu
ece443-hacked.pem	5 KB	10/25/2018 5:27:35 AM	rw-rw-r--	ubuntu
ece443-localhost.csr	2 KB	10/25/2018 5:17:51 AM	rw-rw-r--	ubuntu
ece443-localhost.key	2 KB	10/25/2018 5:16:04 AM	rw-rw-r--	ubuntu
ece443-localhost.pem	5 KB	10/25/2018 5:09:35 AM	rw-rw-r--	ubuntu
index.html	12 KB	9/10/2018 9:28:58 AM	rw-rw-r--	ubuntu

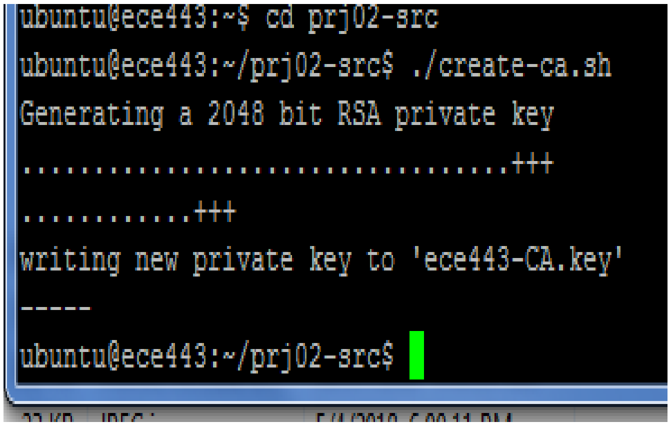
Created CA via 'create-ca.sh' that uses 'openssl'.

```
./create-ca.sh
```

After completion two files are generated:

ece443-CA.key: this is the private key of our CA.

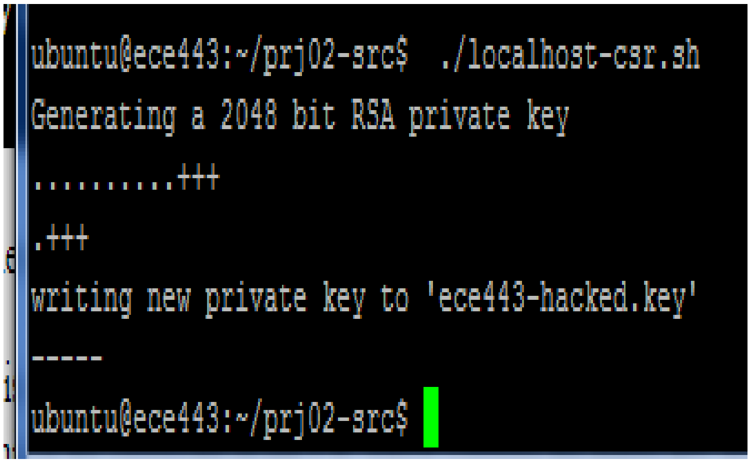
ece443-CA.pem: this is the certificate of our CA, which contains the public key and other information of our CA signed by our CA.



```
ubuntu@ece443:~$ cd prj02-src
ubuntu@ece443:~/prj02-src$ ./create-ca.sh
Generating a 2048 bit RSA private key
..................................+++
...........+++
writing new private key to 'ece443-CA.key'
-----
ubuntu@ece443:~/prj02-src$
```

The identity of our server at 'localhost' can be created via 'localhost-csr.sh' that also uses 'openssl':

```
./localhost-csr.sh
```



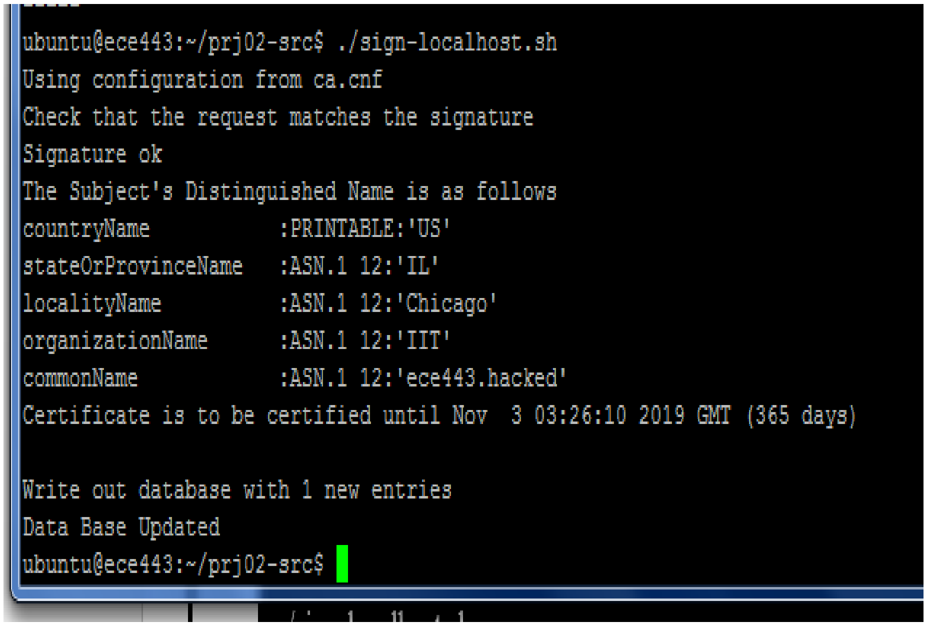
```
ubuntu@ece443:~/prj02-src$  ./localhost-csr.sh
Generating a 2048 bit RSA private key
.........+++
.+++
writing new private key to 'ece443-hacked.key'
-----
ubuntu@ece443:~/prj02-src$ 
```

These two files are generated:

- ece443-localhost.key: this is the private key of our server.
- ece443-localhost.csr: this is a certificate signing request (CSR) that we need to send to a CA to sign a certificate for our website. Note that a CSR should contain the public key and the domain name of the server. You may find the domain name of our server at the last line of 'localhost.cnf', which is used by 'localhost-csr.sh'.

The CA then signs the CSR to issue the server certificate 'ece443-localhost.pem'.

```
./sign-localhost.sh
```



```
-----
ubuntu@ece443:~/prj02-src$ ./sign-localhost.sh
Using configuration from ca.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :ASN.1 12:'IL'
localityName          :ASN.1 12:'Chicago'
organizationName      :ASN.1 12:'IIT'
commonName            :ASN.1 12:'ece443.hacked'
Certificate is to be certified until Nov  3 03:26:10 2019 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
ubuntu@ece443:~/prj02-src$
```

Then I enabled HTTP connections.

enable SSL/TLS support in Apache.

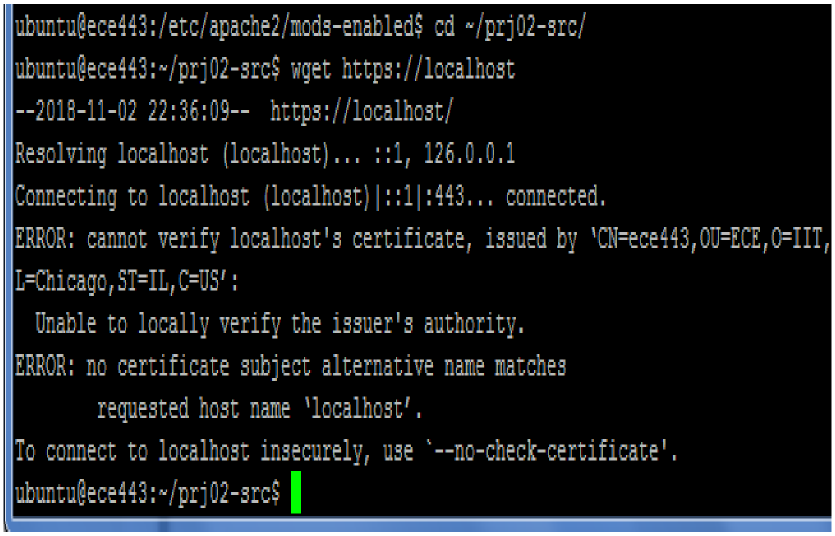
```
cd /etc/apache2/mods-enabled/
sudo ln -s ../mods-available/ssl.* .
sudo ln -s ../mods-available/socache_shmcb.load .
```

Then, Apache needs to know our intent to enable HTTPS connections. An Apache configuration file 'apache-ssl-localhost.conf' is provided for your convenience. The private key and the (signed) certificate of our server are both referred to in this file. We will need to copy it to Apache's configuration directory and to restart Apache so it will see the changes.

```
sudo cp apache-ssl-localhost.conf /etc/apache2/sites-enabled/
sudo service apache2 restart
```

Now, verify that the HTTPS port 443 is in use and then fire 'wget https://localhost'.

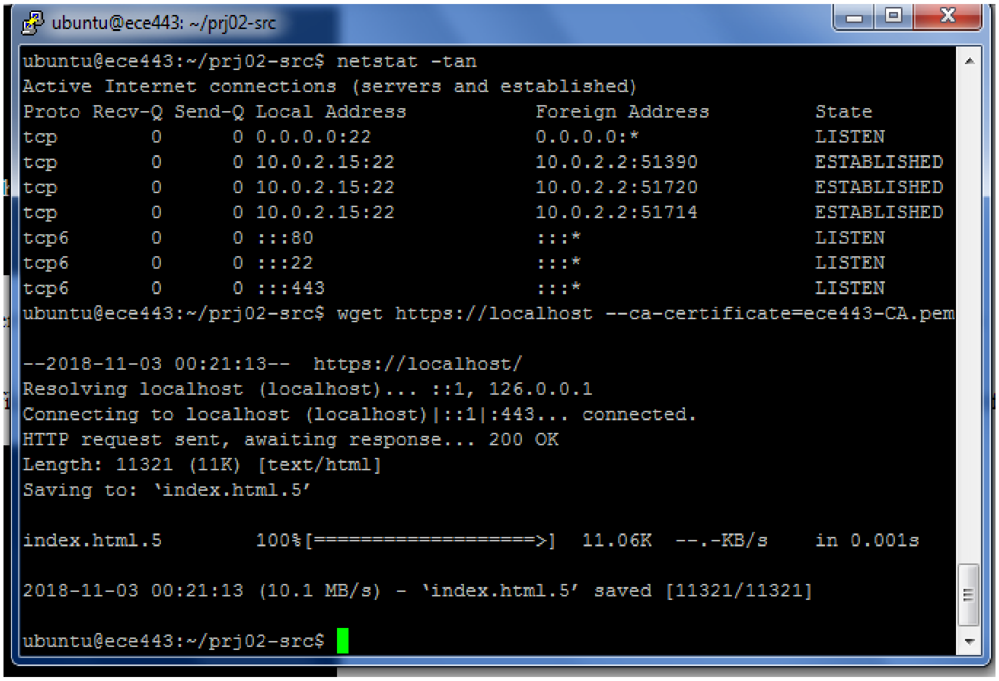
```
wget https://localhost
```



```
ubuntu@ece443:/etc/apache2/mods-enabled$ cd ~/prj02-src/
ubuntu@ece443:~/prj02-src$ wget https://localhost
--2018-11-02 22:36:09--  https://localhost/
Resolving localhost (localhost)... ::1, 126.0.0.1
Connecting to localhost (localhost)|::1|:443... connected.
ERROR: cannot verify localhost's certificate, issued by 'CN=ece443,OU=ECE,O=IIT,
L=Chicago,ST=IL,C=US':
  Unable to locally verify the issuer's authority.
ERROR: no certificate subject alternative name matches
        requested host name 'localhost'.
To connect to localhost insecurely, use `--no-check-certificate'.
ubuntu@ece443:~/prj02-src$
```

Clearly, the HTTPS port 443 is in use and Apache presents wget with the certificate of our server. However, wget complains that it cannot verify the certificate. This is as expected since wget has no knowledge of our CA.

Obviously we do not want to connect to localhost insecurely via the option '--no-check-certificate'. Instead, we tell wget to trust our CA by providing the certificate of our CA via the option '--ca-certificate'.



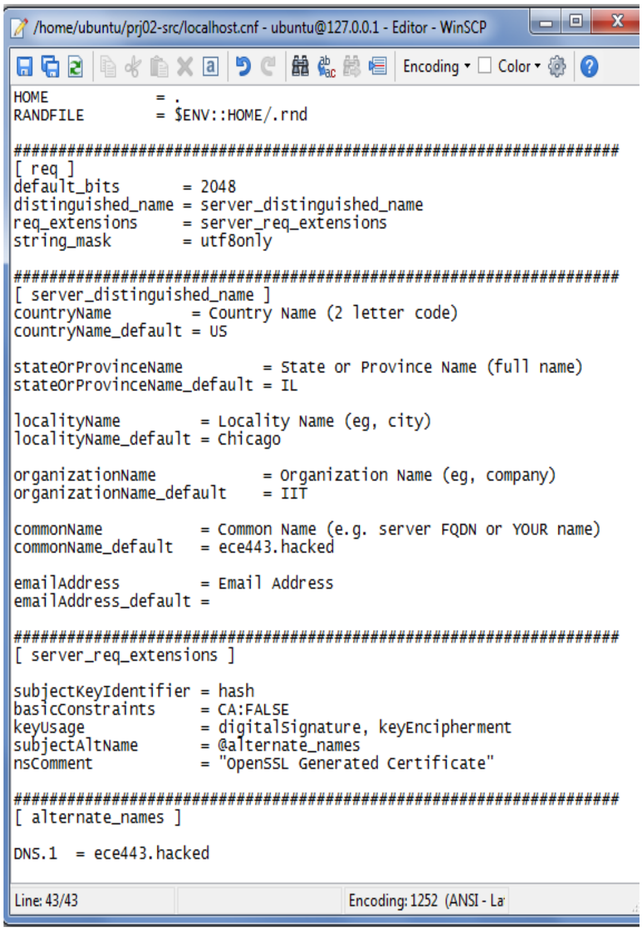
```
ubuntu@ece443:~/prj02-src$ netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.15:22            10.0.2.2:51390          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:51720          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:51714          ESTABLISHED
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
ubuntu@ece443:~/prj02-src$ wget https://localhost --ca-certificate=ece443-CA.pem

--2018-11-03 00:21:13--  https://localhost/
Resolving localhost (localhost)... ::1, 126.0.0.1
Connecting to localhost (localhost)|::1|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11321 (11K) [text/html]
Saving to: 'index.html.5'

index.html.5        100%[===================>]  11.06K  --.-KB/s    in 0.001s

2018-11-03 00:21:13 (10.1 MB/s) - 'index.html.5' saved [11321/11321]

ubuntu@ece443:~/prj02-src$
```

wget believes that our server is secure.

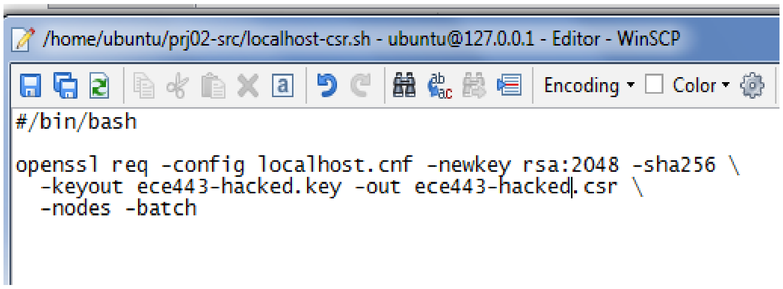
The Attack:

We will now study the vulnerabilities in HTTPS connections by crafting an attack in our virtual machine. The objective is to fool wget to believe a HTTPS website at the domain name 'ece443.hacked' to be secure.

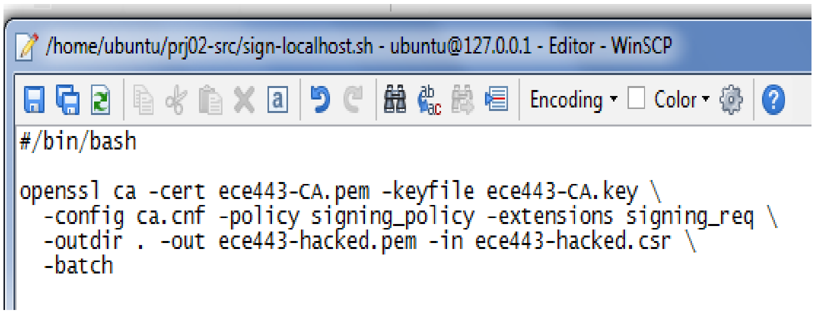
First I have modify 'localhost.cnf', 'localhost-csr.sh', and 'sign-localhost.sh'.


/home/ubuntu/prj02-src/localhost.cnf - ubuntu@127.0.0.1 - Editor - WinSCP
Encoding
Color
Line: 43/43
Encoding: 1252 (ANSI - La

```
HOME            = .
RANDFILE        = $ENV::HOME/.rnd

####################################################################
[ req ]
default_bits       = 2048
distinguished_name = server_distinguished_name
req_extensions     = server_req_extensions
string_mask        = utf8only

####################################################################
[ server_distinguished_name ]
countryName         = Country Name (2 letter code)
countryName_default = US

stateOrProvinceName         = State or Province Name (full name)
stateOrProvinceName_default = IL

localityName         = Locality Name (eg, city)
localityName_default = Chicago

organizationName            = Organization Name (eg, company)
organizationName_default    = IIT

commonName           = Common Name (e.g. server FQDN or YOUR name)
commonName_default   = ece443.hacked

emailAddress         = Email Address
emailAddress_default =

####################################################################
[ server_req_extensions ]

subjectKeyIdentifier = hash
basicConstraints     = CA:FALSE
keyUsage             = digitalSignature, keyEncipherment
subjectAltName       = @alternate_names
nsComment            = "OpenSSL Generated Certificate"

####################################################################
[ alternate_names ]

DNS.1  = ece443.hacked
```

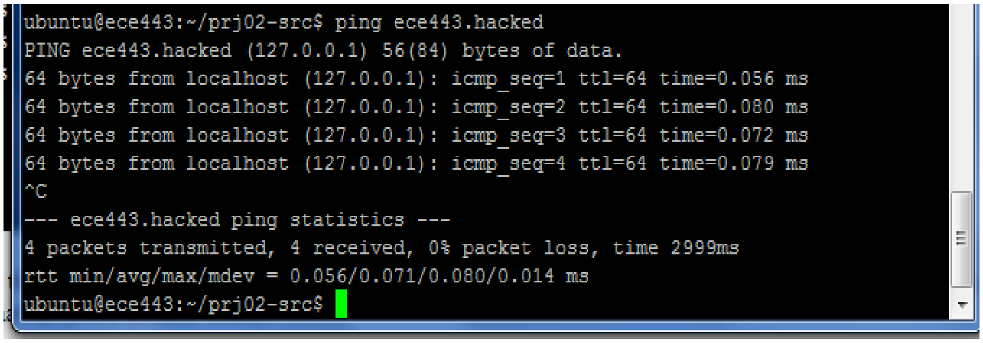

/home/ubuntu/prj02-src/localhost-csr.sh - ubuntu@127.0.0.1 - Editor - WinSCP
Encoding
Color

```
#/bin/bash

openssl req -config localhost.cnf -newkey rsa:2048 -sha256 \
  -keyout ece443-hacked.key -out ece443-hacked.csr \
  -nodes -batch
```


/home/ubuntu/prj02-src/sign-localhost.sh - ubuntu@127.0.0.1 - Editor - WinSCP
Encoding
Color

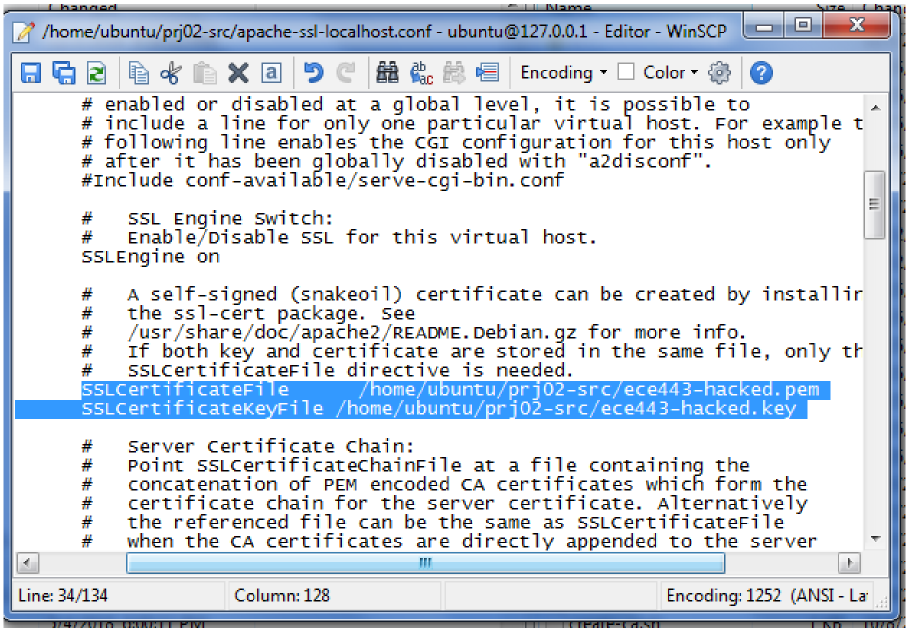
```
#/bin/bash

openssl ca -cert ece443-CA.pem -keyfile ece443-CA.key \
  -config ca.cnf -policy signing_policy -extensions signing_req \
  -outdir . -out ece443-hacked.pem -in ece443-hacked.csr \
  -batch
```

Second, you will need to point the domain name 'ece443.hacked' to 'localhost' via DNS spoofing. Since we don't want to setup or modify any DNS server, we will achieve this by modifying the file '/etc/hosts' that all DNS queries will consult first. You will need to add one line '127.0.0.1 ece443.hacked' to the end of the file. Note that since this file is a system file, you will also need to use 'sudo' to access it, e.g. 'sudo vim /etc/hosts'.

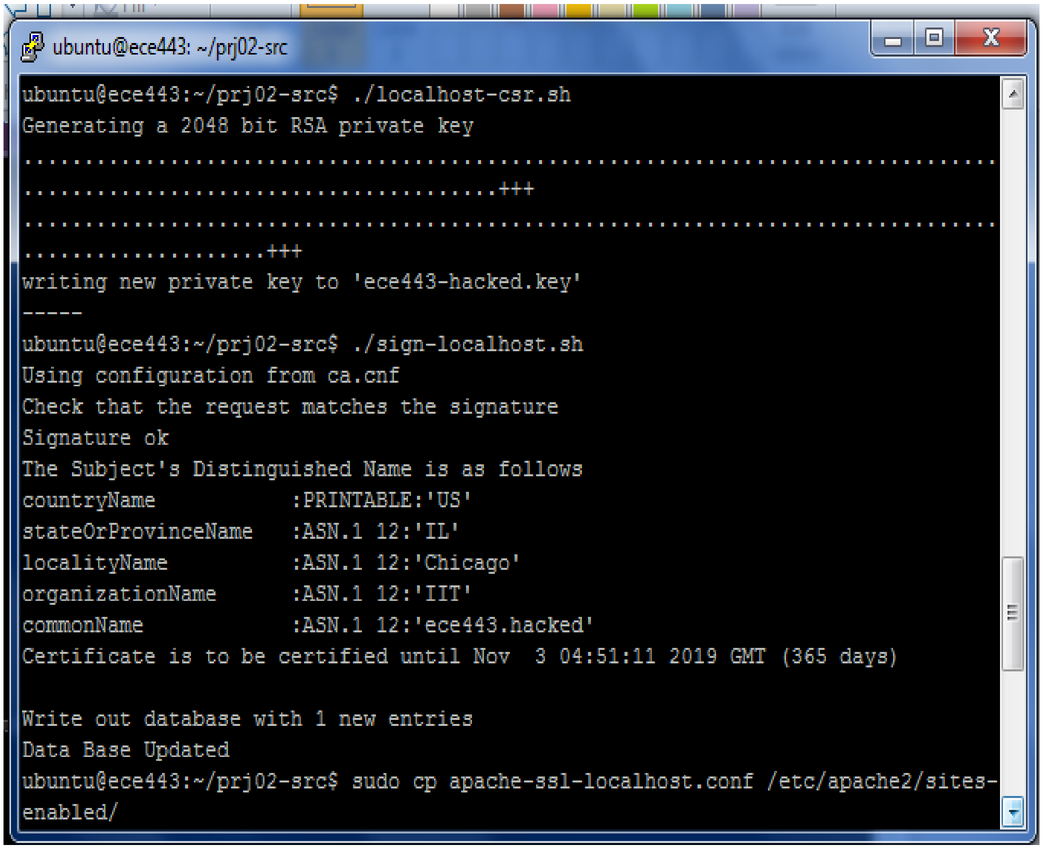


```
ubuntu@ece443:~/prj02-src$ ping ece443.hacked
PING ece443.hacked (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.056 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.080 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.072 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.079 ms
^C
--- ece443.hacked ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.056/0.071/0.080/0.014 ms
ubuntu@ece443:~/prj02-src$
```

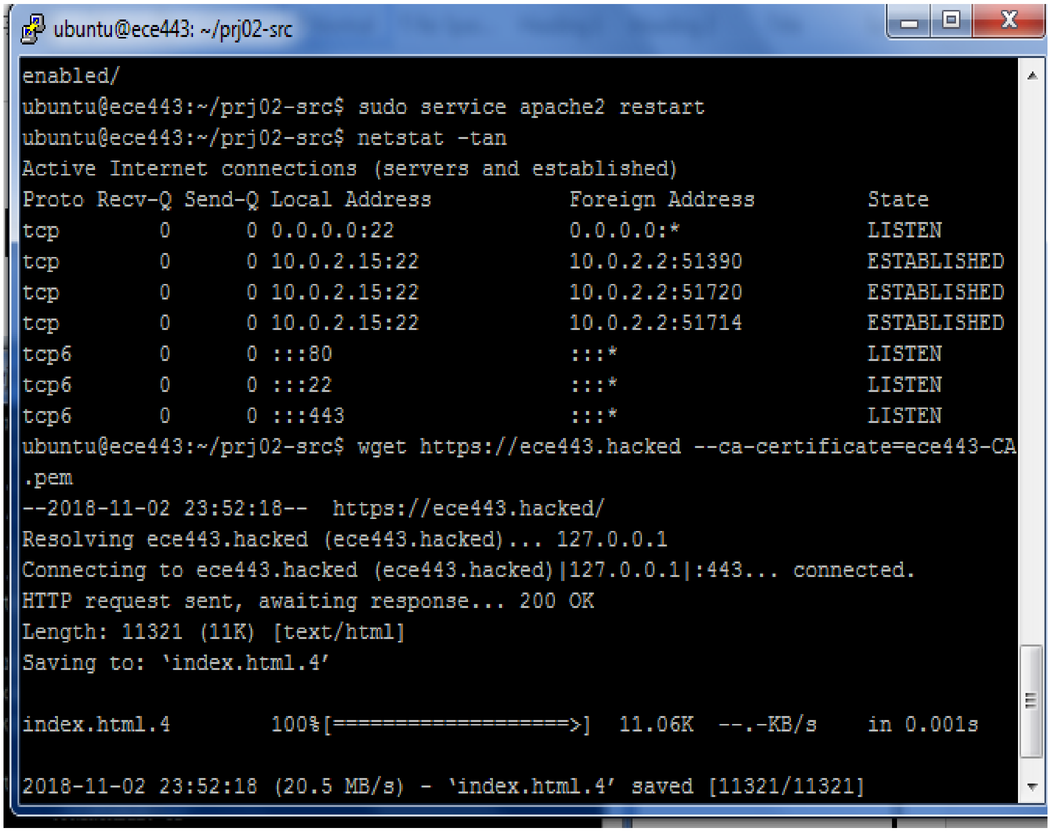
Then I have modified 'apache-ssl-localhost.conf' to refer to the private key and the (signed) certificate of the server at 'ece443.hacked', copy it to Apache's configuration directory again, and restart Apache.


/home/ubuntu/prj02-src/apache-ssl-localhost.conf - ubuntu@127.0.0.1 - Editor - WinSCP
Encoding
Color
Line: 34/134
Column: 128
Encoding: 1252 (ANSI - La

```
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example t
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf

        #   SSL Engine Switch:
        #   Enable/Disable SSL for this virtual host.
        SSLEngine on

        #   A self-signed (snakeoil) certificate can be created by installir
        #   the ssl-cert package. See
        #   /usr/share/doc/apache2/README.Debian.gz for more info.
        #   If both key and certificate are stored in the same file, only th
        #   SSLCertificateFile directive is needed.
        SSLCertificateFile      /home/ubuntu/prj02-src/ece443-hacked.pem
        SSLCertificateKeyFile /home/ubuntu/prj02-src/ece443-hacked.key

        #   Server Certificate Chain:
        #   Point SSLCertificateChainFile at a file containing the
        #   concatenation of PEM encoded CA certificates which form the
        #   certificate chain for the server certificate. Alternatively
        #   the referenced file can be the same as SSLCertificateFile
        #   when the CA certificates are directly appended to the server
```

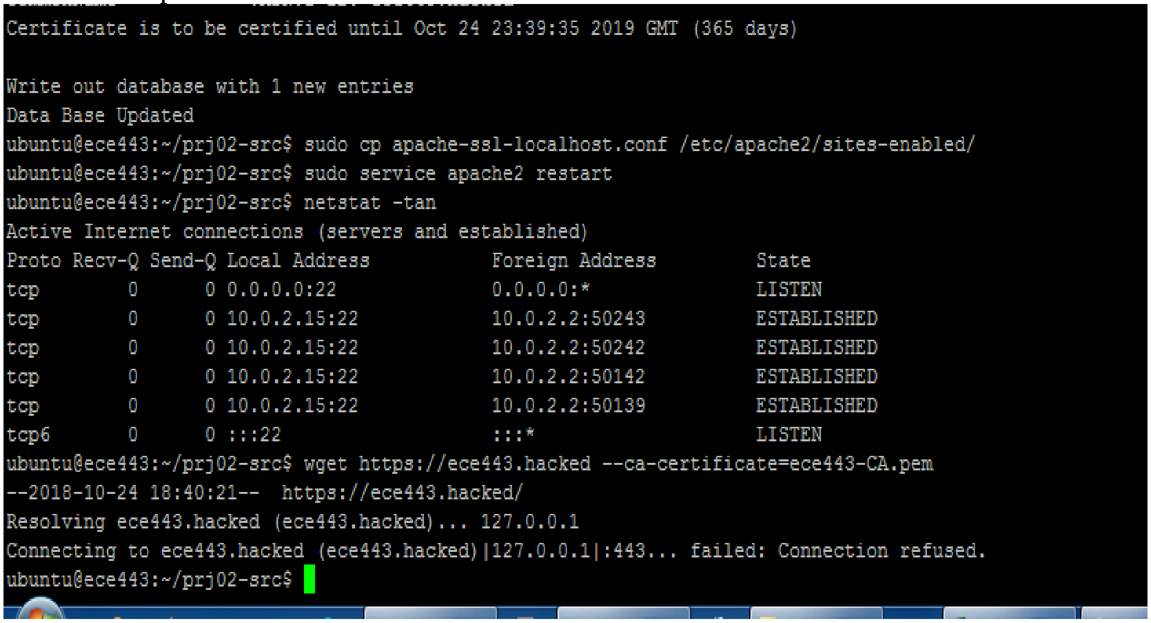


```
ubuntu@ece443:~/prj02-src$ ./localhost-csr.sh
Generating a 2048 bit RSA private key
...............................................................................
.....................................+++
...............................................................................
...................+++
writing new private key to 'ece443-hacked.key'
-----
ubuntu@ece443:~/prj02-src$ ./sign-localhost.sh
Using configuration from ca.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :ASN.1 12:'IL'
localityName          :ASN.1 12:'Chicago'
organizationName      :ASN.1 12:'IIT'
commonName            :ASN.1 12:'ece443.hacked'
Certificate is to be certified until Nov  3 04:51:11 2019 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
ubuntu@ece443:~/prj02-src$ sudo cp apache-ssl-localhost.conf /etc/apache2/sites-
enabled/
```



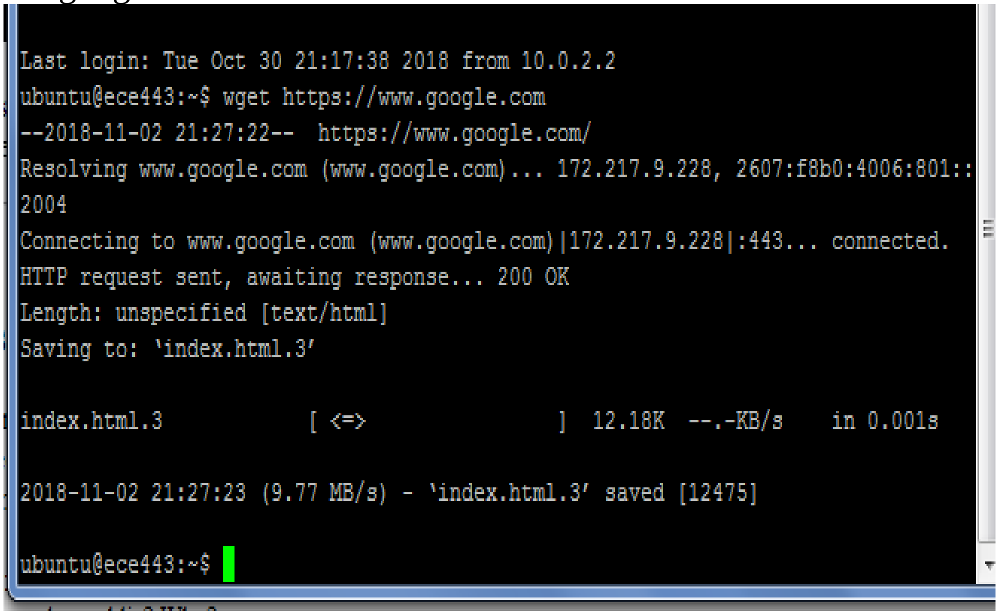
```
enabled/
ubuntu@ece443:~/prj02-src$ sudo service apache2 restart
ubuntu@ece443:~/prj02-src$ netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.15:22            10.0.2.2:51390          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:51720          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:51714          ESTABLISHED
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
ubuntu@ece443:~/prj02-src$ wget https://ece443.hacked --ca-certificate=ece443-CA
.pem
--2018-11-02 23:52:18--  https://ece443.hacked/
Resolving ece443.hacked (ece443.hacked)... 127.0.0.1
Connecting to ece443.hacked (ece443.hacked)|127.0.0.1|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11321 (11K) [text/html]
Saving to: ‘index.html.4’

index.html.4        100%[===================>]  11.06K  --.-KB/s    in 0.001s

2018-11-02 23:52:18 (20.5 MB/s) - ‘index.html.4’ saved [11321/11321]
```

But I also got some error before this due to .pem file, which is for connection. So if there is no connection .pem file is not matched to the ece443-hacked.



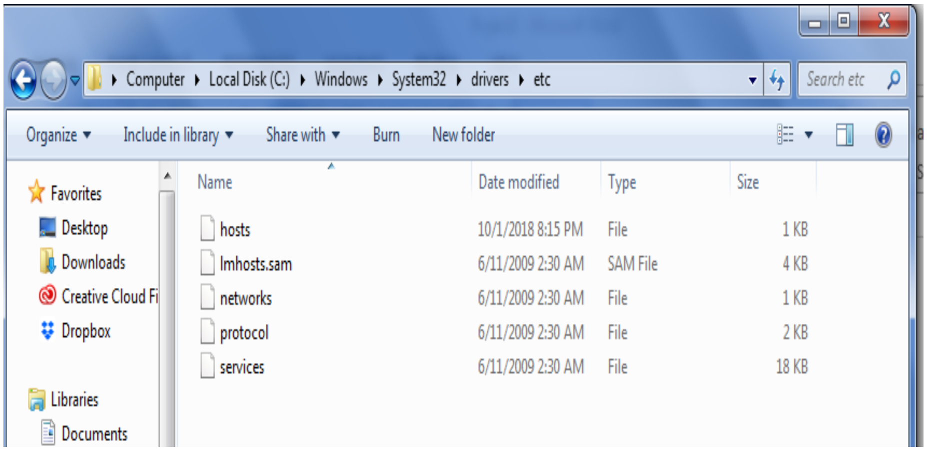
```
Certificate is to be certified until Oct 24 23:39:35 2019 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
ubuntu@ece443:~/prj02-src$ sudo cp apache-ssl-localhost.conf /etc/apache2/sites-enabled/
ubuntu@ece443:~/prj02-src$ sudo service apache2 restart
ubuntu@ece443:~/prj02-src$ netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.15:22            10.0.2.2:50243          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:50242          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:50142          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:50139          ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
ubuntu@ece443:~/prj02-src$ wget https://ece443.hacked --ca-certificate=ece443-CA.pem
--2018-10-24 18:40:21--  https://ece443.hacked/
Resolving ece443.hacked (ece443.hacked)... 127.0.0.1
Connecting to ece443.hacked (ece443.hacked)|127.0.0.1|:443... failed: Connection refused.
ubuntu@ece443:~/prj02-src$
```

Discussion of Findings

- Consider the four files: 'ece443-CA.key', 'ece443-CA.pem', 'ece443-localhost.key', 'ece443-localhost.pem'. Which one is the secret of the CA? Which one is the secret of the server? Which one(s) should be released to public? Why?
  - Secret of the CA is ece443-CA.key.
  - Secret of the server is ece443-localhost.key.
  - ‘ece443-localhost.pem’ should be released to public because it is generated certificate.
- Run 'wget https://www.google.com' in the VM. Does wget complain? Where is the CA of google's server certificate located in the VM?
  - 

```
Last login: Tue Oct 30 21:17:38 2018 from 10.0.2.2
ubuntu@ece443:~$ wget https://www.google.com
--2018-11-02 21:27:22--  https://www.google.com/
Resolving www.google.com (www.google.com)... 172.217.9.228, 2607:f8b0:4006:801::
2004
Connecting to www.google.com (www.google.com)|172.217.9.228|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html.3’

index.html.3            [ <=>               ]  12.18K  --.-KB/s    in 0.001s

2018-11-02 21:27:23 (9.77 MB/s) - ‘index.html.3’ saved [12475]

ubuntu@ece443:~$ 
```

  - No. Wget does not complain.
  - The CA of google’s server certificate located at “/etc/ssl/certs” in the VM.
- What is the purpose of the file '/etc/hosts'? Where is '/etc/hosts' located in your own computer? (Yes, Windows and MacOS both use that file too.) Check that file and see if there is anything unusual there.
  - The hosts file is used to map hostnames (in other words domains) to IP addresses. With the hosts file you can change the IP address that you resolve a given domain name to.
  - ‘etc/hosts’ located in my computer : C:\Windows\System32\drivers\etc



Name	Date modified	Type	Size
hosts	10/1/2018 8:15 PM	File	1 KB
lmhosts.sam	6/11/2009 2:30 AM	SAM File	4 KB
networks	6/11/2009 2:30 AM	File	1 KB
protocol	6/11/2009 2:30 AM	File	2 KB
services	6/11/2009 2:30 AM	File	18 KB

- There is not anything unusual in file.

Appendix A

Private Key for CA

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDZsHs2ZICxBYXf
Paulk1+TGQTNU7RLxjYouAcXqiwqv/HRBgCKeoZMd+3np2K/nz9nwMHhXmpECnJ+
dV1qiwoMUxKP8oJ2zqbFNFuwXirG0+GeBJM8v4tNgNtqBpT3iyFxdFXSxIne4VJo
NnRdbgPc8wWawi1W5n83ZzTnSC0LnTzlg+7xSuuTw4Acyf3hxE32dgwXkgXYDmZE
fgUl5w0bzhfFkXqmsWJSJyIkMBOHR/8+4dgdxCLSI2HaqfO7o5H/hoLMxN2zkY9m
8cFbphUP4gou1JmHIJ0FmfowXWzULKRPFYP8bNJZ7YhyZb3eHgs9alEwZhsRyez0
oqIxlIRlAgMBAAECggEBANYTUMfnxArR1Jn6Ks+UgzvEMc2+ECMoVGBswUTLa83K
nwKgdW25GlMe6Y2TNXAeKhtdGw0HbVdmMrwbrPc2rnX6R9nZceVmSejLGZPytvx6
p3hfJXBrKZHZM2Or9dkOMKBC+JdiAfd1/DVRv9OVeiURtKRBapb364lPbF45w1qT
wFGfruIZH+asRdxzKG6NrDk+r9Ygih8LIehqAt/i+Mm+E92mNGeCpC/dW5EVlZ/9
ZuAI+AgnIeGQoQlgpTesi6/S9F62BXmMWvDJRWjWsvYT+EdYthXo6xzxzTA3aanh
gEllUTZ0gBCibLqp5lMXrWgRUwMwYXlPwT2BDAMuA4ECgYEA/HcNxSNLPz1impxC
/NySe28ZyWyjILD5Ku/YoYdohfVEWadyBkPsVZJn2ypzNBdACq8z2CvznYUD1IuO
vQbBUHcllSquR8TUmgYQZdL/R1G1fKHEvGzV+NsnlL4hm9EOE6DvpSzgu2qN/5ws
R6J2JJeYKgm/HUuf4a78HOxCuOECgYEA3LzGsTtAkOD9Rvmvbs2hyzFK5d0QYRS1
9+G0ayWPLi8QEuRbGZeJDUuPZDd0yKGee9q1vb+eN6zRXrO2sB8agwooVymCM7IL
awlTYX3WyKvc3tr4rz/5pToW5tGK5/QXN6pI3MgpArdjU5L6TAqDO3MnSIrsW6YS
jPcUnj0b6AUCgYAZ6AmUsiN1kNH+dYx2MBgj7Gmj/q7amu5mlogPQzrZjCqAXKtZ
szycJ1La7Yc2OC/1KLdUNmZgQpb7B377aqcJn8BOhzutB6idSYQDPtyNL/hEmsD6
aNyoFa0BGWWPfK8wWHJe67T/5lY95YOxsh0XcireHXPsCKeWXANo4GGUYQKBgFSN
uO6Ic+MLS/m0Cw9WlXNQHnCOjYeid1HMk1+3s3DtdirGbl8PPOBq4TJyS7nOrvai
gJt+mwyYllrD//7W6ODm0yOQKV/EA7ushtQBcBTOQHzdRAVdbDNuXPdtrNfNGFeq
Ut6/jXYM6W9KDbazEDHlmlafYIp6wwBcZPl4TwhBAoGBAKfKEIU3G0gcZe6KUPeh
fUlurpeTSy8L6CY7CtCR6v166XAtqOVQHUkZlH2bdudOCtkSfxhtCzKfJtgfJL/+
ZBwTBb8K3gh7r1pPVoz5aONXO0AktwwqE2UCyCTCw1tZ8npU5XhQRoe4o891e9At
FI3fmvLpMgO+/q11xh34pg6f
-----END PRIVATE KEY-----
```

Certificate for CA

```
-----BEGIN CERTIFICATE-----
MIIDlTCCAn2gAwIBAgIJAPtP5kpkGyU+MA0GCSqGSIb3DQEBCwUAMFkxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJJTDEQMA4GA1UEBwwHQ2hpY2FnbzEMMAoGA1UECgwD
SUlUMQwwCgYDVQQLDANFQ0UxDzANBgNVBAMMBmVjZTQ0MzAeFw0xODExMDMwMzU2
MzBaFw0xOTExMDMwMzU2MzBaMFkxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJJTDEQ
MA4GA1UEBwwHQ2hpY2FnbzEMMAoGA1UECgwDSUlUMQwwCgYDVQQLDANFQ0UxDzAN
BgNVBAMMBmVjZTQ0MzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANmw
ezZkgLEFhd89q6WTX5MZBM1TtEvGNii4BxeqLCq/8dEGAIp6hkx37eenYr+fP2fA
weFeakQKcn51XWqLCgxTEo/ygnbOpsU0W7BeKsbT4Z4Ekzy/i02A22oGlPeLIXF0
VdLEid7hUmg2dF1uA9zzBZrCLVbmfzdnNOdILQudPOWD7vFK65PDgBzJ/eHETfZ2
DBeSBdgOZkR+BSXnDRvOF8WReqaxYlInIiQwE4dH/z7h2B3EItIjYdqp87ujkf+G
gszE3bORj2bxwVumFQ/iCi7UmYcgnQWZ+jBdbNQspE8Vg/xs0lntiHJlvd4eCz1q
UTBmGxHJ7PSiojGUhGUCAwEAAaNgMF4wHQYDVR0OBBYEFKW54FgphjPT7w/ZA1vm
NtNAt31aMB8GA1UdIwQYMBaAFKW54FgphjPT7w/ZA1vmNtNAt31aMA8GA1UdEwEB
/wQFMAMBAf8wCwYDVR0PBAQDAgEGMA0GCSqGSIb3DQEBCwUAA4IBAQBSC8krh6YS
J2vdozIJ9HAA8yV59yF26yUa77q3zfbW/Iq/xXrYTZPYWv2dsiGJFnSxOa9u7pLr
wnb1hRp5/bPG/v6f6qm1iplSqLA67my0nf74gVDHQSk5twtGxuyJLb3tL3Syp9FF
bPJD2GEBIfFnGVDPpyhYfRFsny7XxX96hEHYrhk9cRLM4qoA6dhg3ivu72UMzQ1O
Fplr2BEyoca1rut/2j5qRH7XRSpgeghEnbWXiSGa2eGSBcLYzG3yBCFdU/6b9oYP
BfokcogLtSaG0YOblaDvD5bwnPkdeKf5snWBgaz+zO68fAliXRraksMu+xI4KhWz
MBjM1kBUrWIb
-----END CERTIFICATE-----
```

Private Key for the localhost server:

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCxWvikx1Jn0May
Jypqxe08sGX005SEKeGx+iE/JPhuG0QmLek1RmeiShPeOV6uAzOLi0pMBidBLNDt
YRdVjZJ3Ayv8ATvH1porO41+4MCbl0dtrSauNNHMVu0x520pFyl8Drdcg7b4x29d
y8keaunnhZB1xEZ6vnWVMQZ9cP2wdl0b4BMhG2j29yVRI1e1lbAy5qE+2V0R4SpM
HPCDsZizJmv+zcfbdEKW/iYt40+W+u9xXe7tj3QyC397plSMBoeuQKza7m/AvdUY
e+Ey0ALu7rovmO9Oxob/U7LQk27LyHifi7fujDBhrJGpmM2ZHEGQmeJl54GSnaAd
2+jEi/I9AgMBAAECggEBAJlKC4ZAUNUx+cqZV2wZzkaaIEVPahohKNVvX7T3+1EP
eAOXwu0tAP2gETQNWewFEFQX/AthdiQ63AmP1V84kdMThry1RDohHfcn7dAv6cmR
I0eEVN5VANAggbqUUCEnx89V2N25ajf0CCmFrTsBJVHae1WOY2xLmc1tJjLdqicN
dl+aQmCIEB8YGewI4j2Sharlv3pOrfccXPc8HQ/BmDFGN2P2dA72JBx4KbZJatzh
Up511j/13G90ERZ4ePAfil/wLkfpFoM1k9aFyPjkMjag+h+TooI9xxyP4H37GSG1
uAdRbRL/5etHXg9qa2m2P/62KXfR544QhISB+kJ62XECgYEA2NJy7qbXRh6t2pdV
8L95ySxwTDKzKVy1bv8mTq3eije7VihGVTR6s4wOhkLQL8b7Gdd0l2uno9qmtWyP
f8tNucvaEST5C2RVOEtQKhq8sYYKWQb0MyYX7mHrxQ5SYNBA83jMnD7FwyIpPAoz
wDCCzyQLprWqnNumQ7wMGwI1BYcCgYEA0WbojQJPDVqpmx4DWqzokJtaknCB7Xef
l5AG+SI1lLcLz+vVomOt46KW8XAq5DMVQkSZps6E0WJK2F13sdeED1i1ZkEWm62B
XYdULPeoGj3Vm0bFckjStaMkJnXlL+k0Iyo1/HI72yo6yDky2wZt6GnjbuA4H6qn
qYP3sGFv+xsCgYAMqUVi4EVD5/i5AgtXsqa286xfFrrVmH9Tyvx+rbKIGbcL0fBB
e34KzAvxFSe5EoKJQMajLPsuG0+O2pcKnGGejuPeCm2sl6BOWD+HJeaM60nhZwGN
lxTgq8Er0alH1AFm9k/kc9nyiiUkR2g8Odj5pZ40jvk2jbEI1YtTbG6SMwKBgQC0
ytvHOxITno5G/d+5fwYALBFDO91psFla2yAaIz4NmwiYyK4XWWZ93hfidoyhn7Ug
FOhwS2gC+5FRQ0mfg0pikZ10noete1zw6nFzrZM2rOJrAOxiIpvB9Qu2JR3ugrLg
FYas4dfp/ojn6/KLhf6IpjuVtALg3E+LnQPSBh5PtwKBgADzGtLjAvWc24YpIGlL
HXqK80xxfdUwwOb5zn/0UdIZdW/DtxVni8tnlTvqAqUhtE5iTiejHr80dDiyb3dy
vsKxR8YAD8wguiiukGythJ5Idi7uz1OSDDP0/R2jVh6ns7OGlRbP/6h2IJLyoMy3
Q2DcRfmw7LYm3r/7BBezTBaS
-----END PRIVATE KEY-----
```

Certificate for the localhost :

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 16 (0x10)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=IL, L=Chicago, O=IIT, OU=ECE, CN=ece443
        Validity
            Not Before: Nov  3 03:56:55 2018 GMT
            Not After : Nov  3 03:56:55 2019 GMT
        Subject: C=US, ST=IL, L=Chicago, O=IIT, CN=ece443.localhost
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b1:5a:f8:a4:c7:52:67:d0:c6:b2:27:2a:6a:c5:
                    ed:3c:b0:65:f4:d3:94:84:29:e1:b1:fa:21:3f:24:
                    f8:6e:1b:44:26:2d:e9:35:46:67:a2:4a:13:de:39:
                    5e:ae:03:33:8b:8b:4a:4c:06:27:41:2c:d0:ed:61:
                    17:55:8d:92:77:03:2b:fc:01:3b:c7:d6:9a:2b:3b:
                    8d:7e:e0:c0:9b:97:47:6d:ad:26:ae:34:d1:cc:56:
                    ed:31:e7:6d:29:17:29:7c:0e:b7:5c:83:b6:f8:c7:
                    6f:5d:cb:c9:1e:6a:e9:e7:85:90:75:c4:46:7a:be:
                    75:95:31:06:7d:70:fd:b0:76:5d:1b:e0:13:21:1b:
                    68:f6:f7:25:51:23:57:b5:95:b0:32:e6:a1:3e:d9:
                    5d:11:e1:2a:4c:1c:f0:83:b1:98:b3:26:6b:fe:cd:
                    c7:db:74:42:96:fe:26:2d:e3:4f:96:fa:ef:71:5d:
                    ee:ed:8f:74:32:0b:7f:7b:a6:54:8c:06:87:ae:40:
                    ac:da:ee:6f:c0:bd:d5:18:7b:e1:32:d0:02:ee:ee:
                    ba:2f:98:ef:4e:c6:86:ff:53:b2:d0:93:6e:cb:c8:
```

```
                    78:9f:8b:b7:ee:8c:30:61:ac:91:a9:98:cd:99:1c:
                    41:90:99:e2:65:e7:81:92:9d:a0:1d:db:e8:c4:8b:
                    f2:3d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                ED:23:9E:B1:13:1E:B3:C4:4D:03:34:99:51:CE:DA:ED:69:1F:90:AB
            X509v3 Authority Key Identifier:

keyid:A5:B9:E0:58:29:86:33:D3:EF:0F:D9:03:5B:E6:36:D3:40:B7:7D:5A

            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            X509v3 Subject Alternative Name:
                DNS:localhost
            Netscape Comment:
                OpenSSL Generated Certificate
    Signature Algorithm: sha256WithRSAEncryption
         6a:8a:fd:0e:42:28:bc:0c:1f:b4:6a:08:ca:d4:cd:e2:f7:d0:
         d5:05:01:fc:3c:56:1c:5b:58:b3:70:13:d9:a7:56:57:fe:b4:
         b3:3d:b0:8b:aa:6f:e9:4c:7c:88:aa:06:e1:0a:da:3a:74:b5:
         11:7a:e4:2d:95:57:39:d2:be:2c:d7:db:b8:4f:85:20:80:6f:
         bb:c6:e3:73:73:c6:cf:37:2c:b2:16:3a:25:76:75:fb:2e:74:
         c5:68:d0:b9:66:a6:36:c8:c3:87:bd:d4:27:76:61:67:b3:58:
         3a:5f:cb:f9:f5:31:70:11:50:36:35:4f:5b:ab:fc:e6:fe:c5:
         0b:bd:9f:e9:02:99:f0:be:6b:ba:b8:a9:c0:52:5b:27:dd:db:
         ff:ae:ae:41:e9:f4:9e:34:41:f0:1f:db:38:4d:f4:b2:4f:eb:
         a1:c2:03:96:88:d7:ce:d1:68:f2:b5:4c:b0:a7:bd:ff:dd:71:
         4a:8f:19:d7:48:ad:eb:fd:e5:0e:a4:38:62:9c:5d:b2:c6:55:
         47:5f:f9:3f:29:7c:08:dc:9c:d6:5c:80:2c:67:6b:6c:d5:fe:
         97:22:36:94:74:41:59:a4:2e:7d:a3:75:67:0b:19:fd:c0:bc:
         bd:01:7e:7d:91:6c:2a:f5:73:f2:87:c4:5f:bc:d0:ad:cb:5a:
         f7:8f:2e:f7
```

```
-----BEGIN CERTIFICATE-----
MIIDyTCCArGgAwIBAgIBEDANBgkqhkiG9w0BAQsFADBZMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCSUwxEDAOBgNVBAcMB0NoaWNhZ28xDDAKBgNVBAoMA0lJVDEMMAoG
A1UECwwDRUNFMQ8wDQYDVQQDDAZlY2U0NDMwHhcNMTgxMTAzMDM1NjU1WhcNMTkx
MTAzMDM1NjU1WjBVMQswCQYDVQQGEwJVUzELMAkGA1UECAwCSUwxEDAOBgNVBAcM
B0NoaWNhZ28xDDAKBgNVBAoMA0lJVDEZMBcGA1UEAwwQZWNlNDQzLmxvY2FsaG9z
dDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALFa+KTHUmfQxrInKmrF
7TywZfTTlIQp4bH6IT8k+G4bRCYt6TVGZ6JKE945Xq4DM4uLSkwGJ0Es0O1hF1WN
kncDK/wBO8fWmis7jX7gwJuXR22tJq400cxW7THnbSkXKXwOt1yDtvjHb13LyR5q
6eeFkHXERnq+dZUxBn1w/bB2XRvgEyEbaPb3JVEjV7WVsDLmoT7ZXRHhKkwc8IOx
mLMma/7Nx9t0Qpb+Ji3jT5b673Fd7u2PdDILf3umVIwGh65ArNrub8C91Rh74TLQ
Au7uui+Y707Ghv9TstCTbsvIeJ+Lt+6MMGGskamYzZkcQZCZ4mXngZKdoB3b6MSL
8j0CAwEAAaOBnzCBnDAdBgNVHQ4EFgQU7SOesRMes8RNAzSZUc7a7WkfkKswHwYD
VR0jBBgwFoAUpbngWCmGM9PvD9kDW+Y200C3fVowCQYDVR0TBAIwADALBgNVHQ8E
BAMCBaAwFAYDVR0RBA0wC4IJbG9jYWxob3N0MCwGCWCGSAGG+EIBDQQfFh1PcGVu
U1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTANBgkqhkiG9w0BAQsFAAOCAQEAaor9
DkIovAwftGoIytTN4vfQ1QUB/DxWHFtYs3AT2adWV/60sz2wi6pv6Ux8iKoG4Qra
OnS1EXrkLZVXOdK+LNfbuE+FIIBvu8bjc3PGzzcsshY6JXZ1+y50xWjQuWamNsjD
h73UJ3ZhZ7NYOl/L+fUxcBFQNjVPW6v85v7FC72f6QKZ8L5ruripwFJbJ93b/66u
Qen0njRB8B/bOE30sk/rocIDlojXztFo8rVMsKe9/91xSo8Z10it6/3lDqQ4Ypxd
ssZVR1/5Pyl8CNyc1lyALGdrbNX+lyI2lHRBWaQufaN1ZwsZ/cC8vQF+fZFsKvVz
8ofEX7zQrcta948u9w==
-----END CERTIFICATE-----
```

Private Key for the ece443.hacked server.

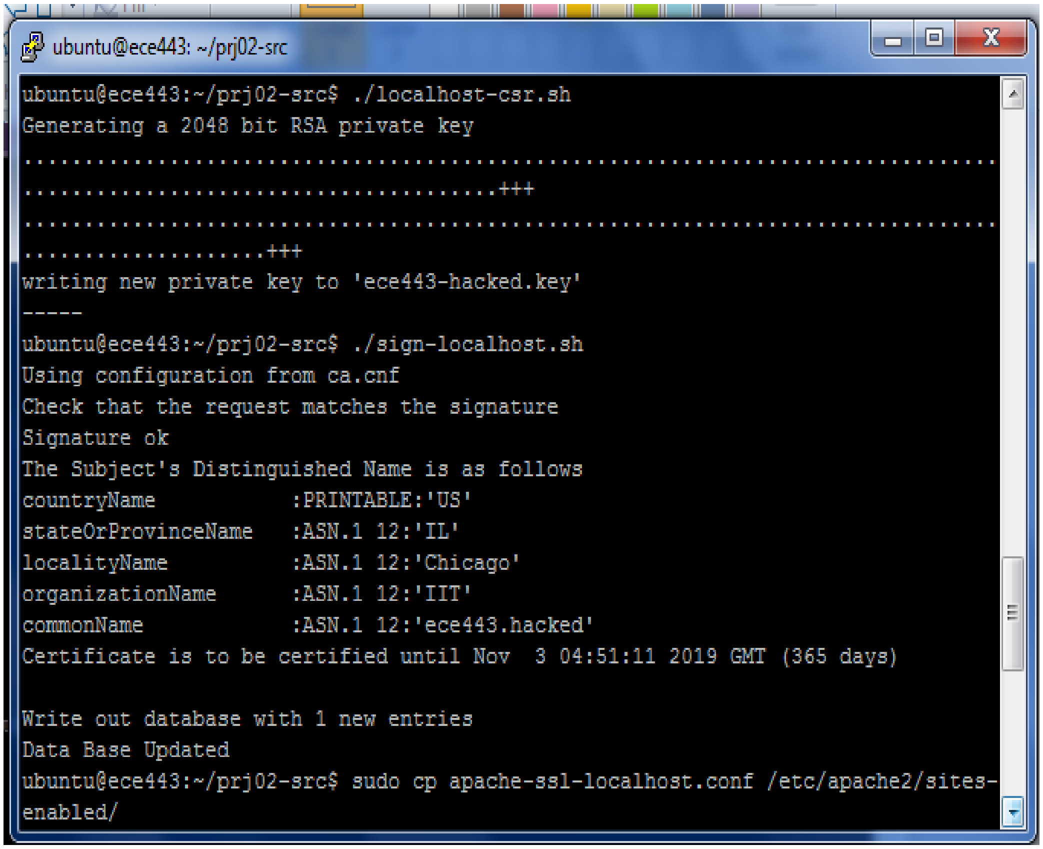
```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQDvhjM9Bi4IEXuq
RYM0L2jSJE54GFD1hMQSWxYYQXmWqtPjgPdguiJxy3Hl/0h5bh/22kYFMInj12n9
JExsM7xqA06WmsaAtYsoGKsjOnHmk8EluKRwNjvtc6HsyjeUAwvDqzTiHxfW9D26
3DBkdodjmxufR+HRsCNyBp7+IKyXH/b7oaEF9Dqs7qSvc8+KnRY2C2rhuU7HuCq6
Mj61bh0eZzI1qwznAhIlEI47QSrKCmhauKDJgjZ8xR4CAxLpZVXifB0Q6zXnsAKU
CJAbqsqSlrD+5ExIWXj3glty7J1pD66XQWC+ff/4BuZ3sfFe6jE9mp6yxKlYVU0l
5eMOpyMXAgMBAAECggEAMbSHrYI6yzHVl+AU+h9cgT9HiWSCaHDEv4pna2Eq+jk4
/10j+M6nlzXAzRnM0GYp+/AP18Pa2Y06UW3W7h1OXDGTfW1hBBSobAmyef0G5fKD
gnBur1qR1RTJ5XmRTwXSyygcMVCCgfjtVnmbET4HmoP1l3gzRHBo6qC1HcdqCXIR
52hOfPvLOTx2B6c6HmGgdq7GvZZcHn6eDA4ibJeTHvIN85kieFEE+Hu+ZIyi3uNI
C/d4HUu1K3GgEhULo/9GIt07+gmqoGKowUEG/kCU/sWKo8uq2zcTIxryIcRn/kJx
bZdYyUbnS1qob0JTlk81k56vWfu8/EqLVIcgZP3zAQKBgQD6HrXt6nDClBILK8aX
Rha3pc6vITZp0zuV0OuMQtGJpJHFsGsPstugVCdrwtHB+P1sl8k/XRobTaWO4Lg5
1wlMM1dV+QJt4KFmuY+XZ35axJ515hF95NawXgFDsd5T5EJ3zYoou4zYgKD6m0sy
xlXflLtbr+6+ZZ8clLW8Z5H98wKBgQD1J7iwmTY2parrW17hbFw59vPlrxj/qxlC
MB/fuTMrcoIOcnGRqAmVLQ6m+4pgKq98+vaIL39AGBsgOjGXi9RRUuuTdJDAAfz3
8JNR3ZflRosHHm1Vyd/gzaTVjqLid1p4vrVKrDWCriztezhPTKFY1arNFoEn747k
sCm7zt57TQKBgAnbogIBhnY0zc1A6W/W5FhSoaXHYlSjbarG9DGwBIAvS0uGW4Hf
48Ya6v7VS90gSiS4iscDjV7cHZVXCAvHjOdC8sNBsDXSb6oT0DQAcTt0mmY9Lh1P
IqMK4XPgk8msqm38XOCkG7YAw9d8vWb/6CyKuSOw+HDqom3G8q69SkS/AoGAac5b
8rQdZtZ3fx6vQ4FeCJJhz2aT1nyE6UEV8JvgzsacBRo1k9S/VgfdRApaPYkOtlUm
I77EH+iHhJA5KRvrZbHxBHIRqxzwjh3hpzqJPSYGCOuD6ru3CTIYCyeFe1Jh1K0S
V4kdiyobL9+3fNoo5MtK7TriQVcuB9tUF79/3B0CgYBW0DKKNktkrSHQr0aai8Vm
qAJPGjmTyllcFNz0kG0vWIuiUOYLZdddsTrtwzYvupfsDvRGmKmZVbheD5g5NF9U
ed6cJffa/zWCAU9WEdPdD/HJ87BM5ouTsDFltCQr20z8Ls6TTy0B9hj9R7C6/jZe
aEGLz9H9KoWBtfaKdOUoiA==
-----END PRIVATE KEY-----
```

Certificate for the ece443.hacked server:

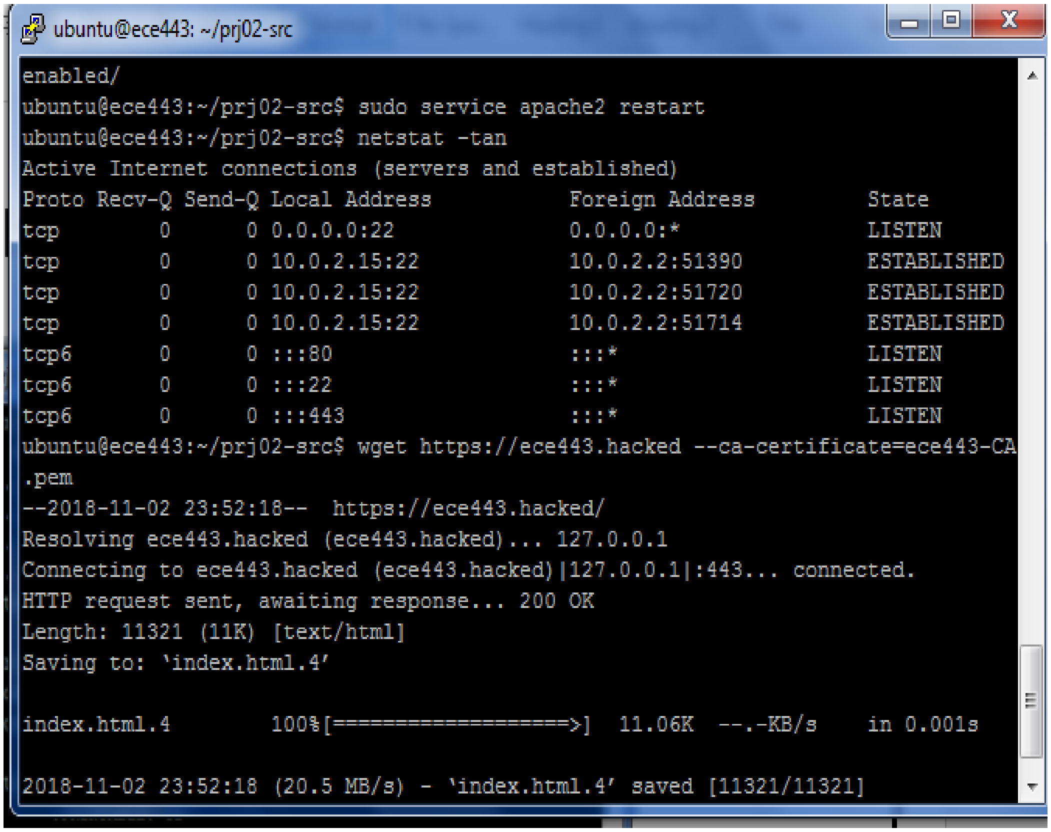
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 15 (0xf)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=IL, L=Chicago, O=IIT, OU=ECE, CN=ece443
        Validity
            Not Before: Nov  3 03:30:13 2018 GMT
            Not After : Nov  3 03:30:13 2019 GMT
        Subject: C=US, ST=IL, L=Chicago, O=IIT, CN=ece443.hacked
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ef:86:33:3d:06:2e:08:11:7b:aa:45:83:34:2f:
                    68:d2:24:4e:78:18:50:f5:84:c4:12:5b:16:18:41:
                    79:96:aa:d3:e3:80:f7:60:ba:22:71:cb:71:e5:ff:
                    48:79:6e:1f:f6:da:46:05:30:89:e3:d7:69:fd:24:
                    4c:6c:33:bc:6a:03:4e:96:9a:c6:80:b5:8b:28:18:
                    ab:23:3a:71:e6:93:c1:25:b8:a4:70:36:3b:ed:73:
                    a1:ec:ca:37:94:03:0b:c3:ab:34:e2:1f:17:d6:f4:
                    3d:ba:dc:30:64:76:87:63:9b:1b:9f:47:e1:d1:b0:
                    23:72:06:9e:fe:20:ac:97:1f:f6:fb:a1:a1:05:f4:
                    3a:ac:ee:a4:af:73:cf:8a:9d:16:36:0b:6a:e1:b9:
                    4e:c7:b8:2a:ba:32:3e:b5:6e:1d:1e:67:32:35:ab:
                    0c:e7:02:12:25:10:8e:3b:41:2a:ca:0a:68:5a:b8:
                    a0:c9:82:36:7c:c5:1e:02:03:12:e9:65:55:e2:7c:
                    1d:10:eb:35:e7:b0:02:94:08:90:1b:aa:ca:92:96:
                    b0:fe:e4:4c:48:59:78:f7:82:5b:72:ec:9d:69:0f:
                    ae:97:41:60:be:7d:ff:f8:06:e6:77:b1:f1:5e:ea:
```

```
                    31:3d:9a:9e:b2:c4:a9:58:55:4d:25:e5:e3:0e:a7:
                    23:17
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier: 
                C2:97:A5:37:19:9A:C2:05:A4:7B:04:A9:F2:17:69:FC:E7:65:1C:9E
            X509v3 Authority Key Identifier: 

keyid:9A:5B:7D:C9:C3:3B:23:04:B8:44:50:D6:96:8E:54:20:02:3A:72:14

            X509v3 Basic Constraints: 
                CA:FALSE
            X509v3 Key Usage: 
                Digital Signature, Key Encipherment
            X509v3 Subject Alternative Name: 
                DNS:ece443.hacked
            Netscape Comment: 
                OpenSSL Generated Certificate
    Signature Algorithm: sha256WithRSAEncryption
         2c:9e:1f:16:96:04:dc:9b:1d:51:b9:a9:79:f5:14:9e:41:c7:
         7b:31:23:84:a9:c3:1e:94:24:59:c3:c2:ac:87:d1:0b:ba:4c:
         ad:79:66:cb:a7:c0:d0:5b:73:1b:a2:d9:6d:d7:18:a2:f8:6e:
         68:39:cf:b3:43:16:46:f4:51:25:fc:e7:dc:80:4a:77:fc:c1:
         55:c5:eb:71:c7:49:94:25:90:e2:90:65:57:65:5d:4f:e0:94:
         cc:6d:7b:d1:b2:ee:1a:67:a0:5f:61:3e:10:74:30:d6:6e:7e:
         e2:83:82:52:82:b6:21:d1:7b:69:dc:92:7b:99:71:7b:c0:0c:
         bd:f8:80:f8:62:b8:e8:21:0d:bf:e0:26:2e:fd:49:48:76:48:
         35:b8:66:ef:19:b6:a9:0c:e1:c1:22:be:ed:d9:af:6f:69:dd:
         61:1b:71:01:d0:af:65:e0:2d:65:6c:3a:6c:76:bf:02:35:9b:
         60:f8:e3:ca:d4:22:49:24:ea:30:d3:20:5c:69:65:85:14:a2:
         f4:c1:9b:b9:46:11:53:f2:f1:09:c0:ac:37:1e:4d:6f:0a:89:
         ad:c7:20:6c:4d:22:34:ff:f1:1f:02:e3:2c:87:8d:08:92:c0:
         6b:49:b7:ee:d1:fb:b1:f7:24:8d:d7:07:4a:8d:bf:25:32:1f:
         92:f4:5b:f4
-----BEGIN CERTIFICATE-----
MIIDyjCCArKgAwIBAgIBDzANBgkqhkiG9w0BAQsFADBZMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCSUwxEDAOBgNVBAcMB0NoaWNhZ28xDDAKBgNVBAoMA0lJVDEMMAoG
A1UECwwDRUNFMQ8wDQYDVQQDDAZlY2U0NDMwHhcNMTgxMTAzMDMzMDEzWhcNMTkx
MTAzMDMzMDEzWjBSMQswCQYDVQQGEwJVUzELMAkGA1UECAwCSUwxEDAOBgNVBAcM
B0NoaWNhZ28xDDAKBgNVBAoMA0lJVDEWMBQGA1UEAwwNZWNlNDQzLmhhY2tlZDCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAO+GMz0GLggRe6pFgzQvaNIk
TngYUPWExBJbFhhBeZaq0+OA92C6InHLceX/SHluH/baRgUwiePXaf0kTGwzvGoD
TpaaxoC1iygYqyM6ceaTwSW4pHA2O+1zoezKN5QDC8OrNOIfF9b0PbrcMGR2h2Ob
G59H4dGwI3IGnv4grJcf9vuhoQX0OqzupK9zz4qdFjYLauG5Tse4KroyPrVuHR5n
MjWrDOcCEiUQjjtBKsoKaFq4oMmCNnzFHgIDEullVeJ8HRDrNeewApQIkBuqypKW
sP7kTEhZePeCW3LsnWkPrpdBYL59//gG5nex8V7qMT2anrLEqVhVTSXl4w6nIxcC
AwEAAaOBozCBoDAdBgNVHQ4EFgQUwpelNxmawgWkewSp8hdp/OdlHJ4wHwYDVR0j
BBgwFoAUmlt9ycM7IwS4RFDWlo5UIAI6chQwCQYDVR0TBAIwADALBgNVHQ8EBAMC
BaAwGAYDVR0RBBEwD4INZWNlNDQzLmhhY2tlZDAsBglghkgBhvhCAQ0EHxYdT3Bl
blNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwDQYJKoZIhvcNAQELBQADggEBACye
HxaWBNybHVG5qXn1FJ5Bx3sxI4Spwx6UJFnDwqyH0Qu6TK15ZsunwNBbcxui2W3X
GKL4bmg5z7NDFkb0USX859yASnf8wVXF63HHSZQlkOKQZVdlXU/glMxte9Gy7hpn
oF9hPhB0MNZufuKDglKCtiHRe2ncknuZcXvADL34gPhiuOghDb/gJi79SUh2SDW4
Zu8ZtqkM4cEivu3Zr29p3WEbcQHQr2XgLWVsOmx2vwI1m2D448rUIkkk6jDTIFxp
ZYUUovTBm7lGEVPy8QnArDceTW8Kia3HIGxNIjT/8R8C4yyHjQiSwGtJt+7R+7H3
JI3XB0qNvyUyH5L0W/Q=
-----END CERTIFICATE-----
```

Screenshot of OUTPUT

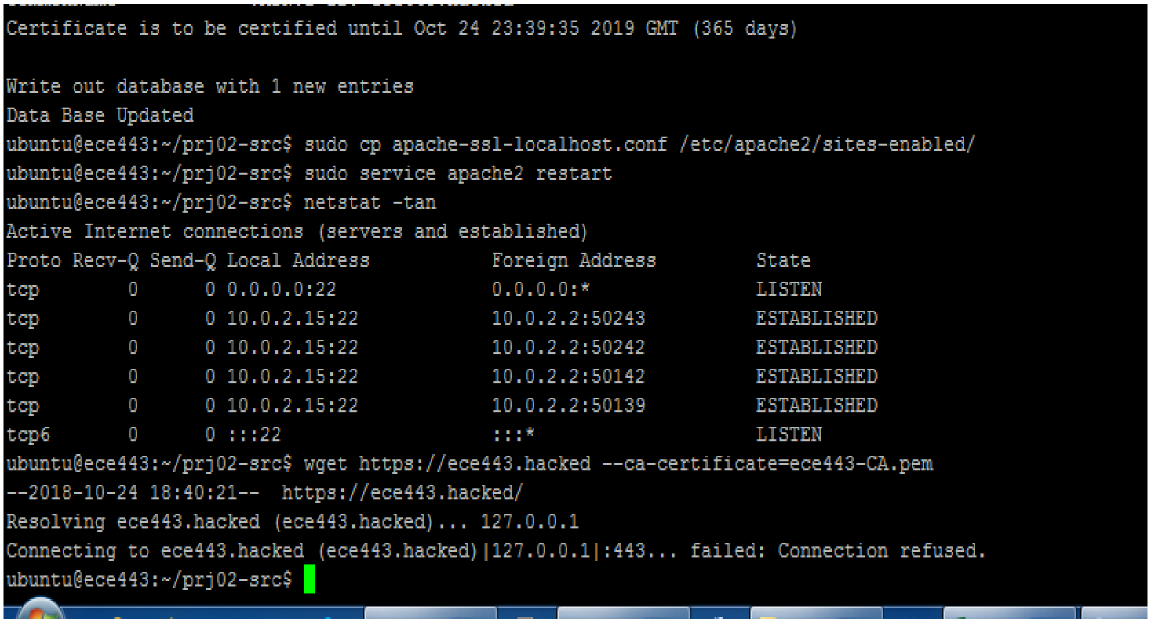


```
ubuntu@ece443:~/prj02-src$ ./localhost-csr.sh
Generating a 2048 bit RSA private key
................................................................................
.......................................+++
................................................................................
....................+++
writing new private key to 'ece443-hacked.key'
-----
ubuntu@ece443:~/prj02-src$ ./sign-localhost.sh
Using configuration from ca.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :ASN.1 12:'IL'
localityName          :ASN.1 12:'Chicago'
organizationName      :ASN.1 12:'IIT'
commonName            :ASN.1 12:'ece443.hacked'
Certificate is to be certified until Nov  3 04:51:11 2019 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
ubuntu@ece443:~/prj02-src$ sudo cp apache-ssl-localhost.conf /etc/apache2/sites-
enabled/
```



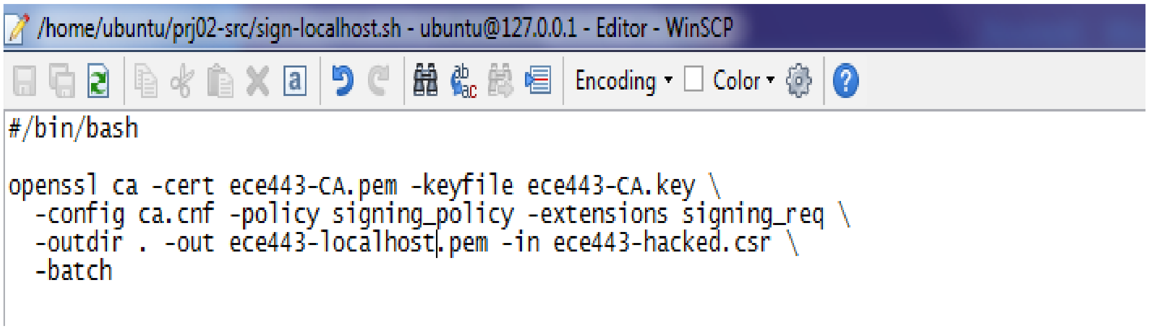
```
enabled/
ubuntu@ece443:~/prj02-src$ sudo service apache2 restart
ubuntu@ece443:~/prj02-src$ netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.15:22            10.0.2.2:51390          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:51720          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:51714          ESTABLISHED
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
ubuntu@ece443:~/prj02-src$ wget https://ece443.hacked --ca-certificate=ece443-CA
.pem
--2018-11-02 23:52:18--  https://ece443.hacked/
Resolving ece443.hacked (ece443.hacked)... 127.0.0.1
Connecting to ece443.hacked (ece443.hacked)|127.0.0.1|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11321 (11K) [text/html]
Saving to: ‘index.html.4’

index.html.4        100%[===================>]  11.06K  --.-KB/s    in 0.001s

2018-11-02 23:52:18 (20.5 MB/s) - ‘index.html.4’ saved [11321/11321]
```

Screenshot of Errors:

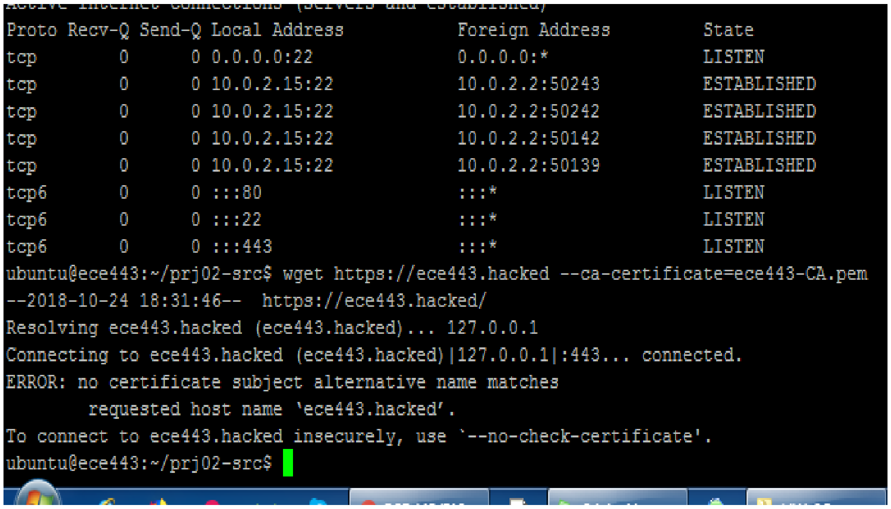


```
Certificate is to be certified until Oct 24 23:39:35 2019 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
ubuntu@ece443:~/prj02-src$ sudo cp apache-ssl-localhost.conf /etc/apache2/sites-enabled/
ubuntu@ece443:~/prj02-src$ sudo service apache2 restart
ubuntu@ece443:~/prj02-src$ netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.15:22            10.0.2.2:50243          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:50242          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:50142          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:50139          ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
ubuntu@ece443:~/prj02-src$ wget https://ece443.hacked --ca-certificate=ece443-CA.pem
--2018-10-24 18:40:21--  https://ece443.hacked/
Resolving ece443.hacked (ece443.hacked)... 127.0.0.1
Connecting to ece443.hacked (ece443.hacked)|127.0.0.1|:443... failed: Connection refused.
ubuntu@ece443:~/prj02-src$
```

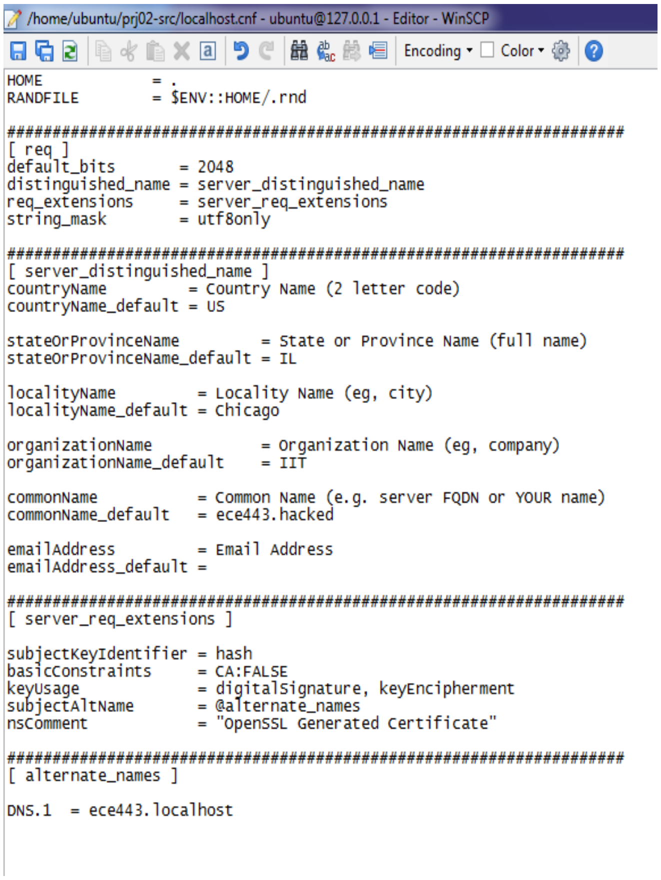
.pem file is for connection. So if there is no connection .pem file is not matched to the ece443-hacked.


/home/ubuntu/prj02-src/sign-localhost.sh - ubuntu@127.0.0.1 - Editor - WinSCP
Encoding
Color

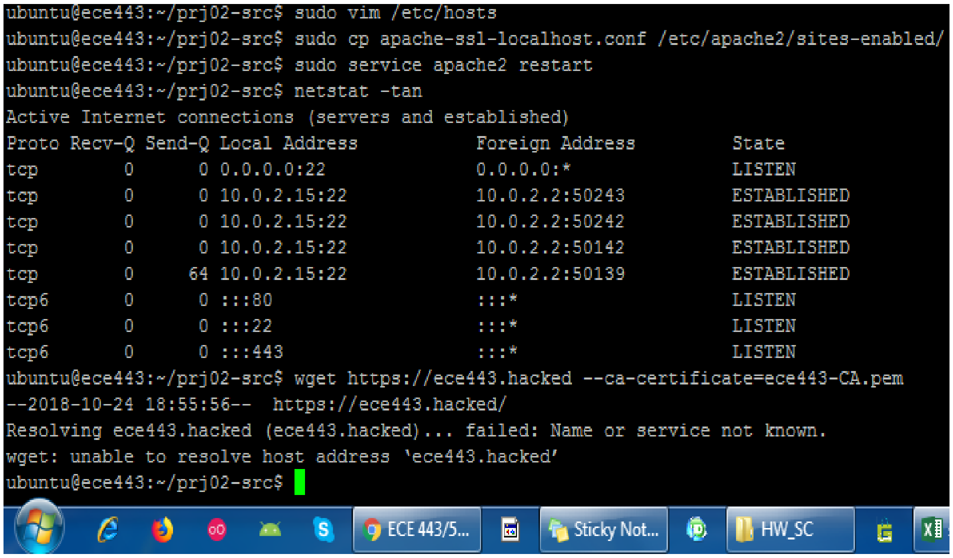
```
#/bin/bash

openssl ca -cert ece443-CA.pem -keyfile ece443-CA.key \
  -config ca.cnf -policy signing_policy -extensions signing_req \
  -outdir . -out ece443-localhost.pem -in ece443-hacked.csr \
  -batch
```



```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.15:22            10.0.2.2:50243          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:50242          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:50142          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:50139          ESTABLISHED
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
ubuntu@ece443:~/prj02-src$ wget https://ece443.hacked --ca-certificate=ece443-CA.pem
--2018-10-24 18:31:46--  https://ece443.hacked/
Resolving ece443.hacked (ece443.hacked)... 127.0.0.1
Connecting to ece443.hacked (ece443.hacked)|127.0.0.1|:443... connected.
ERROR: no certificate subject alternative name matches
        requested host name 'ece443.hacked'.
To connect to ece443.hacked insecurely, use `--no-check-certificate'.
ubuntu@ece443:~/prj02-src$
```


/home/ubuntu/prj02-src/localhost.cnf - ubuntu@127.0.0.1 - Editor - WinSCP
Encoding
Color

```
HOME                = .
RANDFILE            = $ENV::HOME/.rnd

####################################################################
[ req ]
default_bits        = 2048
distinguished_name  = server_distinguished_name
req_extensions      = server_req_extensions
string_mask         = utf8only

####################################################################
[ server_distinguished_name ]
countryName         = Country Name (2 letter code)
countryName_default = US

stateOrProvinceName         = State or Province Name (full name)
stateOrProvinceName_default = IL

localityName         = Locality Name (eg, city)
localityName_default = Chicago

organizationName            = Organization Name (eg, company)
organizationName_default    = IIT

commonName           = Common Name (e.g. server FQDN or YOUR name)
commonName_default   = ece443.hacked

emailAddress         = Email Address
emailAddress_default =

####################################################################
[ server_req_extensions ]

subjectKeyIdentifier = hash
basicConstraints     = CA:FALSE
keyUsage             = digitalSignature, keyEncipherment
subjectAltName       = @alternate_names
nsComment            = "OpenSSL Generated Certificate"

####################################################################
[ alternate_names ]

DNS.1  = ece443.localhost
```



```
ubuntu@ece443:~/prj02-src$ sudo vim /etc/hosts
ubuntu@ece443:~/prj02-src$ sudo cp apache-ssl-localhost.conf /etc/apache2/sites-enabled/
ubuntu@ece443:~/prj02-src$ sudo service apache2 restart
ubuntu@ece443:~/prj02-src$ netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.15:22            10.0.2.2:50243          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:50242          ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.2:50142          ESTABLISHED
tcp        0     64 10.0.2.15:22            10.0.2.2:50139          ESTABLISHED
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
ubuntu@ece443:~/prj02-src$ wget https://ece443.hacked --ca-certificate=ece443-CA.pem
--2018-10-24 18:55:56--  https://ece443.hacked/
Resolving ece443.hacked (ece443.hacked)... failed: Name or service not known.
wget: unable to resolve host address 'ece443.hacked'
ubuntu@ece443:~/prj02-src$
```

When I forgot to put the last line '127.0.0.1 ece443.hacked' in ‘sudo vim /etc/hosts’.