

**Information
Security**

Public Key Infrastructure



**Muhammad Irfan
University of Sahiwal**

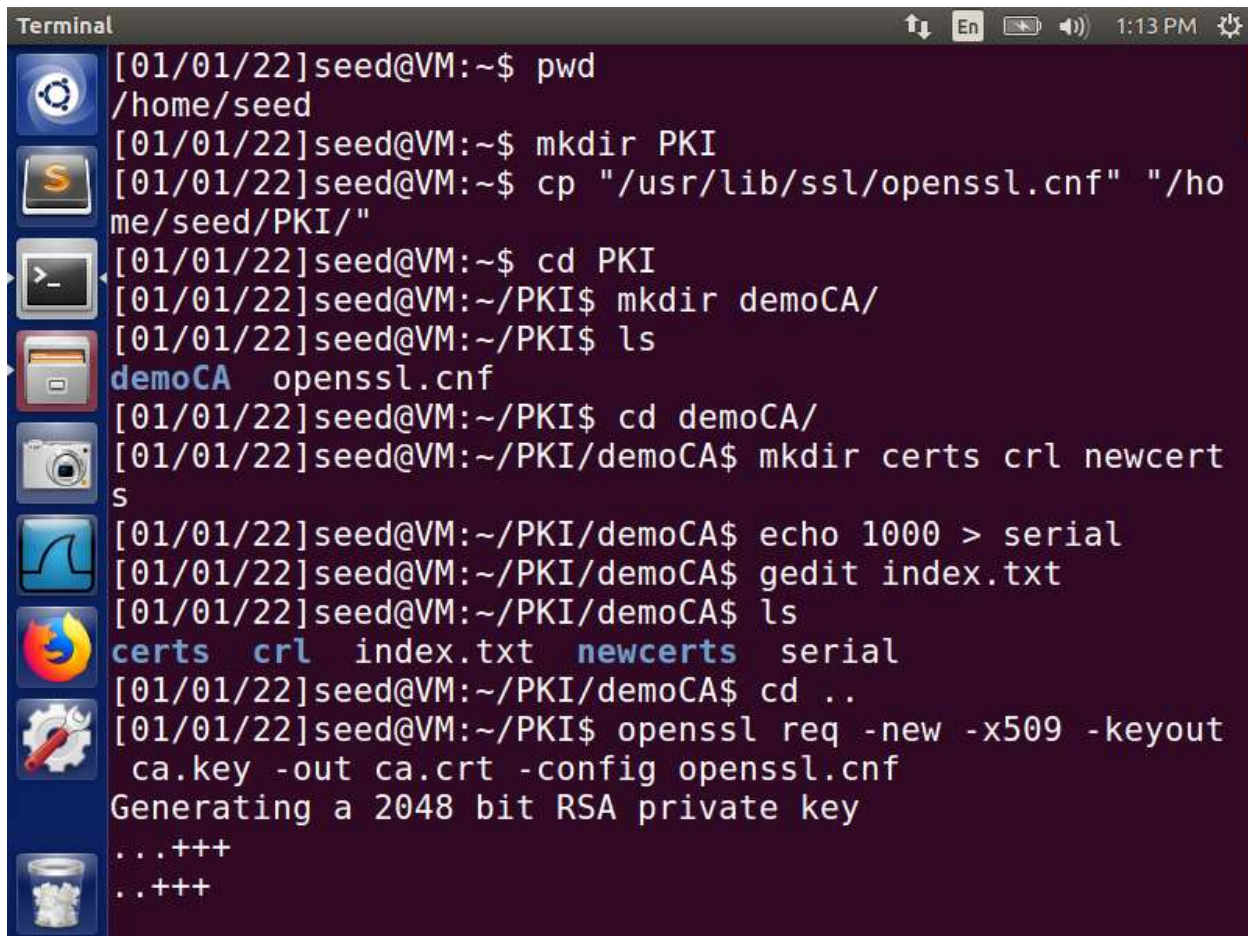
Public Key Infrastructure

Lab Tasks

Task 1: Becoming a Certificate Authority (CA)

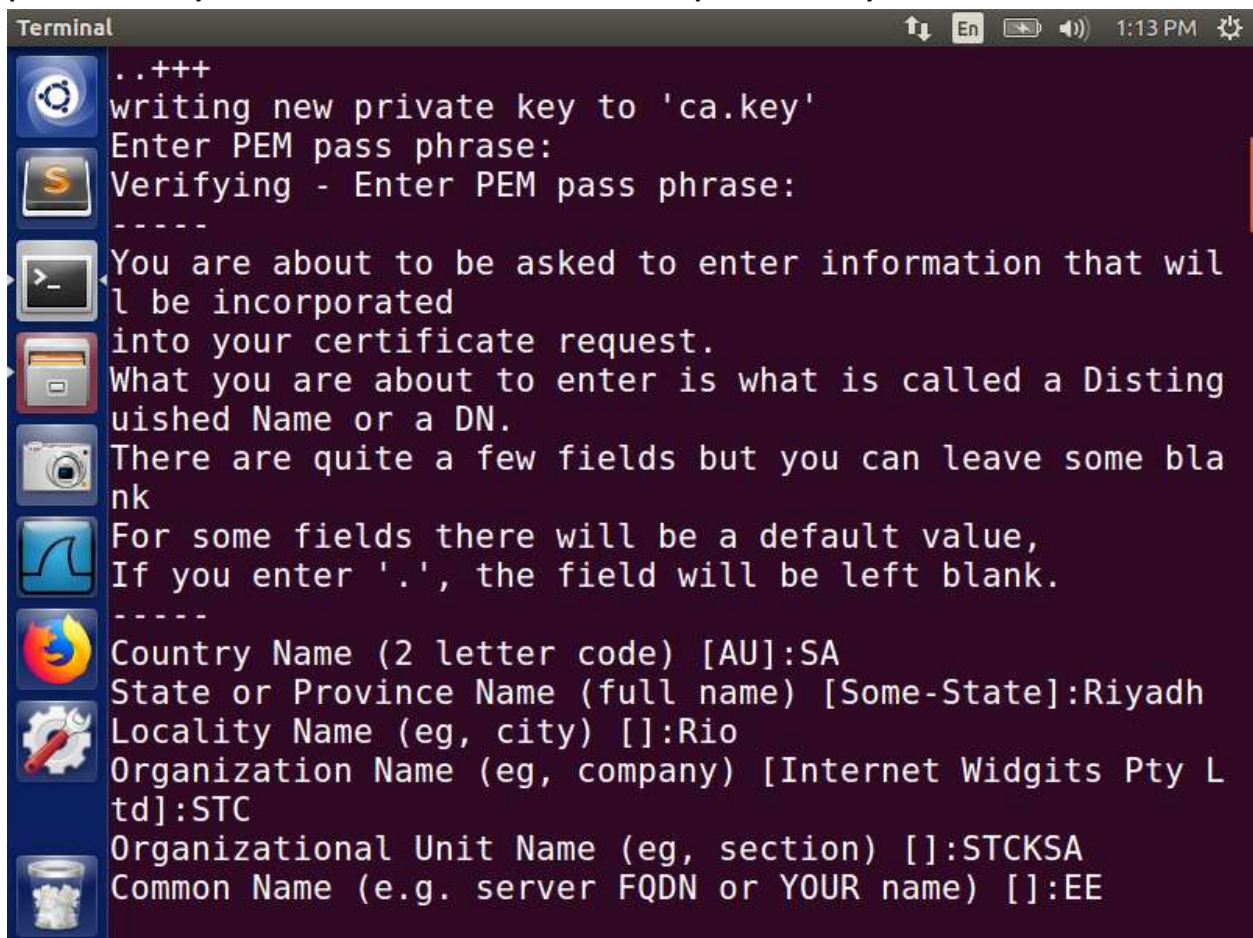
You can run the following command to generate the self-signed certificate for the CA:

```
$ openssl req -new -x509 -keyout ca.key -out ca.crt -config  
openssl.cnf
```



```
Terminal 1:13 PM
[01/01/22]seed@VM:~$ pwd
/home/seed
[01/01/22]seed@VM:~$ mkdir PKI
[01/01/22]seed@VM:~$ cp "/usr/lib/ssl/openssl.cnf" "/home/seed/PKI/"
[01/01/22]seed@VM:~$ cd PKI
[01/01/22]seed@VM:~/PKI$ mkdir demoCA/
[01/01/22]seed@VM:~/PKI$ ls
demoCA  openssl.cnf
[01/01/22]seed@VM:~/PKI$ cd demoCA/
[01/01/22]seed@VM:~/PKI/demoCA$ mkdir certs crl newcerts
[01/01/22]seed@VM:~/PKI/demoCA$ echo 1000 > serial
[01/01/22]seed@VM:~/PKI/demoCA$ gedit index.txt
[01/01/22]seed@VM:~/PKI/demoCA$ ls
certs  crl  index.txt  newcerts  serial
[01/01/22]seed@VM:~/PKI/demoCA$ cd ..
[01/01/22]seed@VM:~/PKI$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
Generating a 2048 bit RSA private key
...+++
..+++
```

You will be prompted for information and a password. Do not lose this password, because you will have to type the passphrase each time you want to use this CA to sign certificates for others. You will also be asked to fill in some information, such as the Country Name, Common Name, etc. The output of the command are stored in two files: ca.key and ca.crt. The file ca.key contains the CA's private key, while ca.crt contains the public-key certificate.



```
Terminal 1:13 PM
...+++
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]:SA
State or Province Name (full name) [Some-State]:Riyadh
Locality Name (eg, city) []:Rio
Organization Name (eg, company) [Internet Widgits Pty Ltd]:STC
Organizational Unit Name (eg, section) []:STCKSA
Common Name (e.g. server FQDN or YOUR name) []:EE
```



```
Terminal Terminal File Edit View Search Terminal Help 1:14 PM
Common Name (e.g. server FQDN or YOUR name) []:EE
Email Address []:elham@elham.com
[01/01/22]seed@VM:~/PKI$ openssl genrsa -aes128 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
[01/01/22]seed@VM:~/PKI$ openssl rsa -in server.key -text
Enter pass phrase for server.key:
Private-Key: (1024 bit)
modulus:
    00:b1:31:bc:62:4b:3c:b9:57:e4:ae:b0:73:c0:ec:
    92:f2:ad:14:a7:cb:7b:f0:fb:42:cb:a8:d5:58:37:
    1a:c4:bb:dd:3c:8d:df:19:6c:b4:d7:5b:4a:14:81:
    c4:69:8c:bd:88:bf:3b:70:25:12:2b:6c:dc:f1:32:
    f4:82:d5:33:88:9f:d7:d3:dc:bb:52:60:64:e6:99:
    e7:38:8c:99:b9:b9:ca:92:c6:9b:92:c2:77:eb:47:
    f4:2c:2f:29:31:5a:4b:a9:41:fd:45:2d:1f:d6:f2:
```

```
Terminal 1:14 PM
    00:b1:31:bc:62:4b:3c:b9:57:e4:ae:b0:73:c0:ec:
    92:f2:ad:14:a7:cb:7b:f0:fb:42:cb:a8:d5:58:37:
    1a:c4:bb:dd:3c:8d:df:19:6c:b4:d7:5b:4a:14:81:
    c4:69:8c:bd:88:bf:3b:70:25:12:2b:6c:dc:f1:32:
    f4:82:d5:33:88:9f:d7:d3:dc:bb:52:60:64:e6:99:
    e7:38:8c:99:b9:b9:ca:92:c6:9b:92:c2:77:eb:47:
    f4:2c:2f:29:31:5a:4b:a9:41:fd:45:2d:1f:d6:f2:
    bd:ed:91:c0:ec:ec:bb:e5:ce:4d:a6:b2:b7:cd:28:
    de:3e:1f:2a:34:31:ce:b5:b1
publicExponent: 65537 (0x10001)
privateExponent:
    1e:9a:7f:75:de:96:bb:50:31:df:f5:fb:d8:0b:44:
    0a:03:d8:b8:6e:4d:96:be:5e:b7:fc:0d:f4:f1:77:
    7f:19:0f:49:e1:1a:f2:32:33:3d:aa:b7:ad:b9:07:
    ea:4e:f3:81:45:be:07:4d:6f:c8:ee:41:6e:ab:25:
    4d:df:72:c9:d1:12:db:f6:cd:b6:79:17:57:6f:d0:
    2b:7b:64:31:c7:ec:5b:df:0c:6d:e1:7c:2d:bd:e2:
    72:6a:59:d4:09:8f:0a:ba:09:15:5b:7a:64:d0:4a:
    84:ed:8e:25:ed:42:cd:63:89:4d:8d:56:7a:76:6c:
    03:1a:4d:7e:73:d2:26:7d
prime1:
    00:ec:2e:52:fe:1d:85:09:54:9b:ee:ee:69:49:51:
```



```
Terminal 1:14 PM
84:ed:8e:25:ed:42:cd:63:89:4d:8d:56:7a:76:6c:
03:1a:4d:7e:73:d2:26:7d
prime1:
00:ec:2e:52:fe:1d:85:09:54:9b:ee:ee:69:49:51:
89:15:a9:2d:73:0a:28:67:bc:a0:e9:62:53:c3:7e:
64:fb:53:2d:ab:3b:0b:4b:e0:e6:79:7a:8d:17:b7:
3d:4c:1f:e5:53:2d:1e:7b:8e:53:4d:be:8d:fb:a8:
ec:d6:fc:84:3f
prime2:
00:c0:10:40:37:36:c0:e7:bf:6c:ae:1a:18:4d:71:
bb:b5:9c:2f:f1:05:08:c9:8d:82:46:dc:ed:2f:f9:
d0:12:46:6f:c2:2f:f4:40:a6:39:4e:99:ad:82:0a:
df:b3:97:4e:35:16:f6:92:37:7a:f7:68:1e:2f:63:
51:24:07:8a:0f
exponent1:
5e:65:bd:82:17:a6:5e:ae:54:8c:d0:f9:7f:f6:78:
c6:11:92:3a:d2:aa:87:9b:da:ec:ad:02:31:b6:c9:
01:b2:a3:24:37:3b:32:9e:b7:3f:82:7d:f6:26:a4:
f7:52:20:44:78:5a:20:a4:28:23:80:b0:1b:0f:cf:
69:b6:0f:dd
exponent2:
0a:d4:1f:ba:bd:34:8d:1c:66:d5:3e:15:66:b0:65:
```

```
Terminal 1:14 PM
0a:d4:1f:ba:bd:34:8d:1c:66:d5:3e:15:66:b0:65:
e3:ec:65:6b:92:5c:17:79:0a:02:52:cc:70:ab:06:
07:31:bf:75:54:5c:d2:14:4d:20:d8:5b:46:fc:b3:
f6:1d:2e:c4:a1:81:cf:66:9f:61:39:96:92:17:68:
68:be:a0:13
coefficient:
00:95:3d:7f:c7:2c:83:f7:3b:f1:2b:a2:ed:5f:82:
26:1e:7e:e4:81:05:17:95:16:d0:4d:db:5f:0d:62:
48:f4:6f:0f:eb:31:08:72:7c:1d:d8:5f:14:ff:68:
3e:cc:96:67:0c:ed:7b:7b:c2:c8:ea:0b:56:06:3a:
7f:42:e0:ed:27
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCxMbxISzy5V+SusHPA7JLyrRSny3vw+0LLqNVYNxr
Eu908jd8Z
bLTxW0oUgcRpjL2IvztwJRIrbNzxMvSC1T0In9fT3LtSYGTmmec4jJm
5ucqSxpuS
wnfrR/QsLykxWkupQf1FLR/W8r3tkcDs7Lvlzk2msrfNKN4+Hyo0Mc6
1sQIDAQAB
AoGAHpp/dd6Wu1Ax3/X72AtECgPYuG5Nlr5et/wN9PF3fxkPSeEa8jI
zPaq3rbkH
6k7zgUW+B01vy05BbqslTd9yydES2/bNtnkXV2/QK3tkMcfsW98MbeF
```



```
Terminal
1sQIDAQAB
AoGAHpp/dd6Wu1Ax3/X72AtECgPYuG5Nlr5et/wN9PF3fxkPSeEa8jI
zPaq3rbkH
6k7zgUW+B01vy05BbqslTd9yydES2/bNtnkXV2/QK3tkMcfsW98MbeF
8Lb3icmpZ
1AmPCroJFVt6ZNBKh020Je1CzW0JTY1WenZsAxpNfnPSJn0CQQDsLlL
+HYUJVJvu
7mLJUYkVqS1zCiHnvKDpYlPDfmT7Uy2r0wtL40Z5eo0Xtz1MH+VTLR5
7jlNNvo37
q0zW/IQ/AkEAwBBANzbA579srhoYTXG7tZwv8QUIyY2CRtztL/nQEkZ
vwi/0QKY5
Tpmtggrfs5d0NRb2kjD692geL2NRJAeKDwJAXmW9ghemXq5UjND5f/Z
4xhGS0tKq
h5va7K0CMbbJAbKjJDc7Mp63P4J99iak91IgRHhaIKQoI4CwGw/PabY
P3QJACTQf
ur00jRxm1T4VZrBl4+xlA5JcF3kKaLLMcKsGBzG/dVRc0hRNINhbRvy
z9h0uxKGB
z2afYTmWkhdoaL6gEwJBAJU9f8csg/c78Sui7V+CJh5+5IEFF5UW0E3
bXwliSPRv
D+sxCHJ8HdhfFP9oPsyWZwzte3vCy0oLVgY6f0Lg7Sc=
-----END RSA PRIVATE KEY-----
[01/01/22]seed@VM:~/PKI$
```

Task 2: Creating a Certificate for SEEDPKILab2021.com

Generate public/private key pair.

```
$ openssl genrsa -aes128 -out server.key 1024
```

```
Terminal
[01/01/22]seed@VM:~/PKI$
[01/01/22]seed@VM:~/PKI$
[01/01/22]seed@VM:~/PKI$ openssl req -new -key server.k
ey -out server.csr -config openssl.cnf
Enter pass phrase for server.key:
You are about to be asked to enter information that wil
l be incorporated
into your certificate request.
What you are about to enter is what is called a Disting
uished Name or a DN.
There are quite a few fields but you can leave some bla
nk
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:SA
State or Province Name (full name) [Some-State]:Riyadh
Locality Name (eg, city) []:Rio
Organization Name (eg, company) [Internet Widgits Pty L
td]:STC
Organizational Unit Name (eg, section) []:STCKSA
Common Name (e.g. server FQDN or YOUR name) []:SEEDPKIL
```

The server.key is an encoded text file (also encrypted), so you will not be able to see the actual content, such as the modulus, private exponents, etc. To see those, you can run the following command:

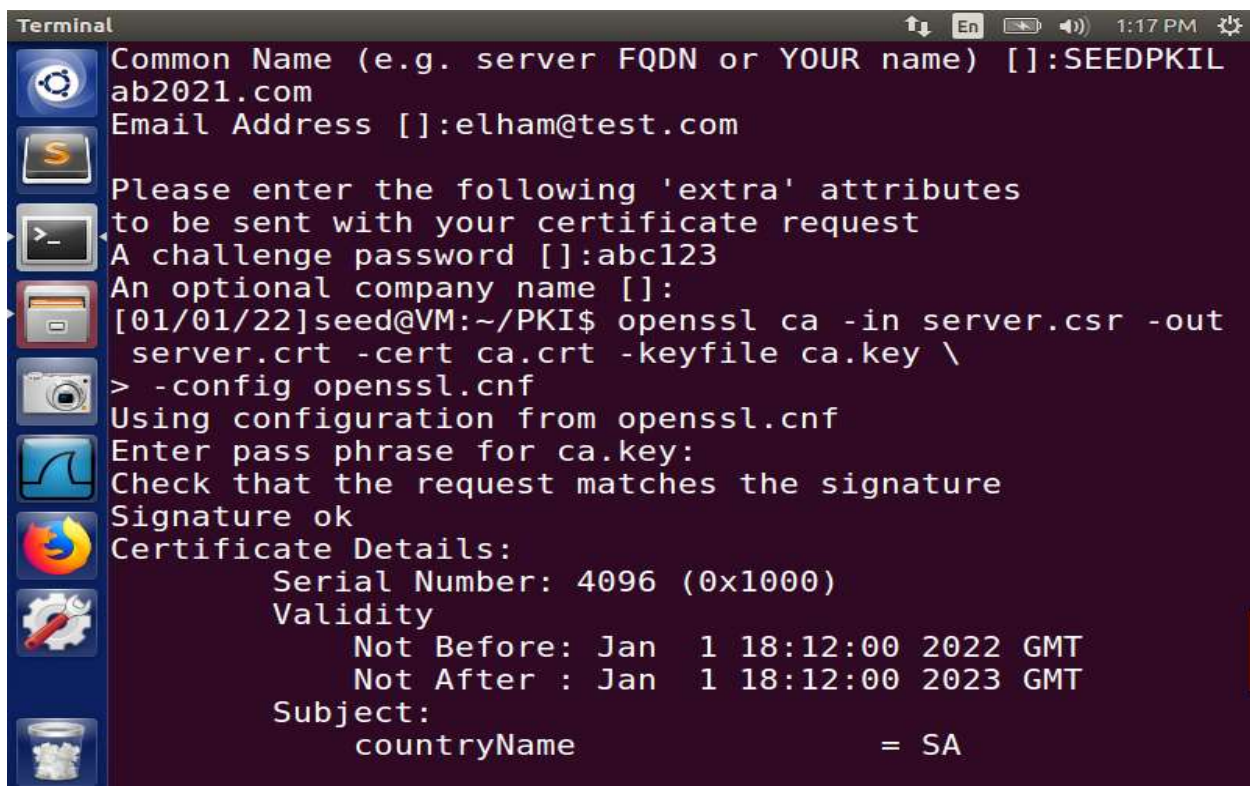
```
$ openssl rsa -in server.key -text
```

please use SEEDPKILab2021.com as the common name of the certificate request.

```
$ openssl req -new -key server.key -out server.csr -config openssl.cnf
```

The following command turns the certificate signing request (server.csr) into an X509 certificate (server.crt), using the CA's ca.crt and ca.key:

```
$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
```



```
Terminal 1:17 PM
Common Name (e.g. server FQDN or YOUR name) []:SEEDPKILab2021.com
Email Address []:elham@test.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:abc123
An optional company name []:
[01/01/22]seed@VM:~/PKI$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key \
> -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 4096 (0x1000)
    Validity
        Not Before: Jan  1 18:12:00 2022 GMT
        Not After : Jan  1 18:12:00 2023 GMT
    Subject:
        countryName = SA
```



```
Terminal 1:17 PM
Not Before: Jan  1 18:12:00 2022 GMT
Not After : Jan  1 18:12:00 2023 GMT
Subject:
countryName           = SA
stateOrProvinceName   = Riyadh
organizationName       = STC
organizationalUnitName = STCKSA
commonName             = SEEDPKILab2021.

com
emailAddress           = elham@test.com
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
DD:3E:89:D8:CF:D8:BF:58:41:6D:B3:9A:EC:
A4:13:59:7A:55:EE:00
X509v3 Authority Key Identifier:
keyid:C0:52:9F:7D:75:5E:18:A8:3F:02:34:
35:14:BA:CF:FF:F3:2E:19:7C
```

```
Terminal 1:18 PM
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
DD:3E:89:D8:CF:D8:BF:58:41:6D:B3:9A:EC:
A4:13:59:7A:55:EE:00
X509v3 Authority Key Identifier:
keyid:C0:52:9F:7D:75:5E:18:A8:3F:02:34:
35:14:BA:CF:FF:F3:2E:19:7C

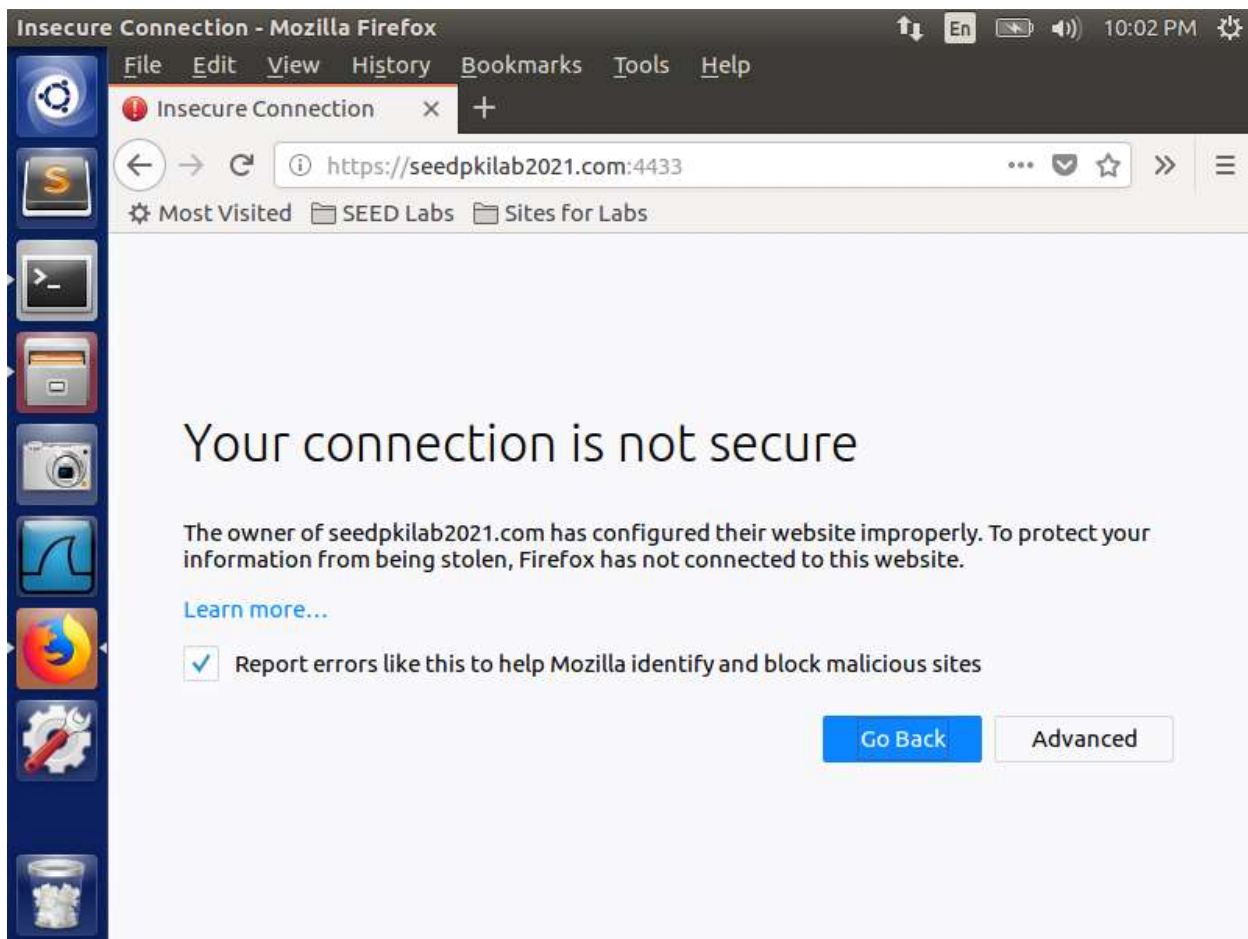
Certificate is to be certified until Jan  1 18:12:00 20
23 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]
y
Write out database with 1 new entries
Data Base Updated
[01/01/22]seed@VM:~/PKI$
```

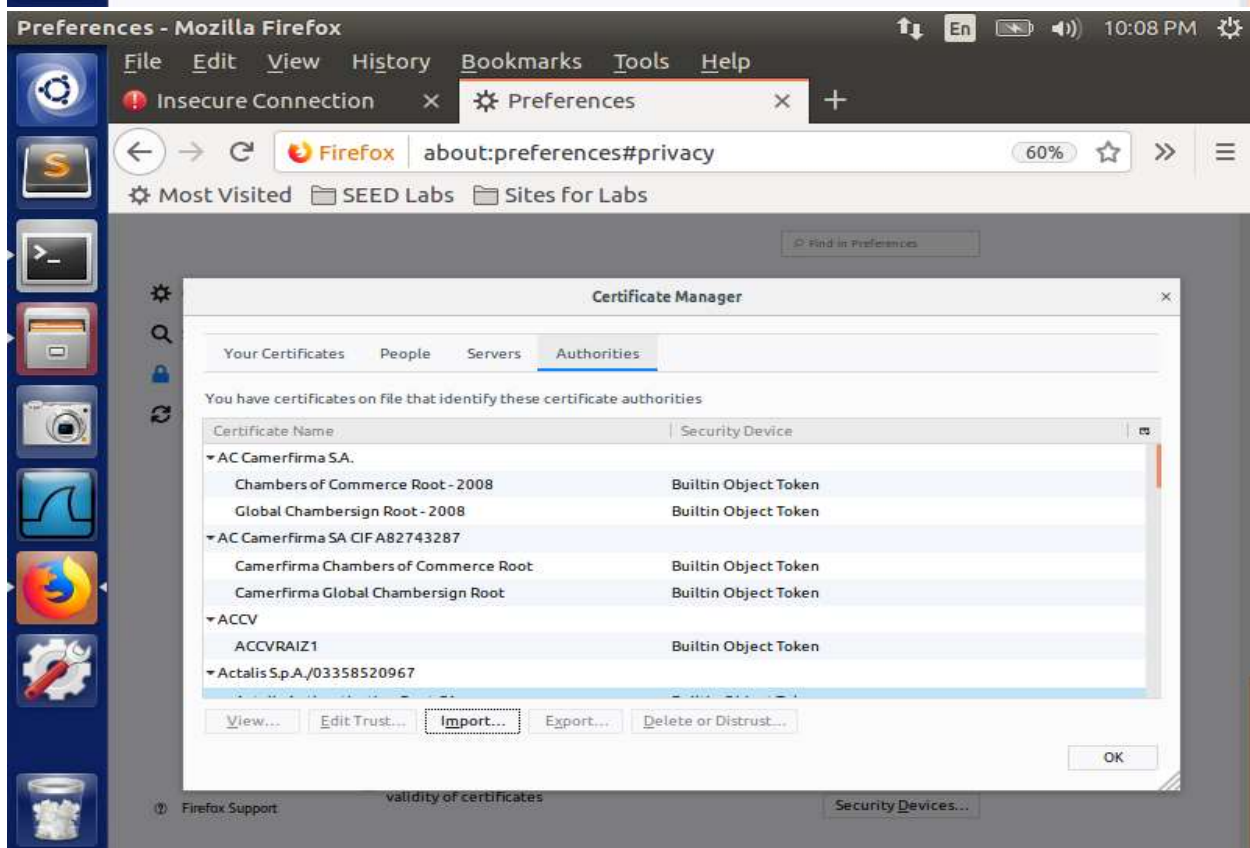
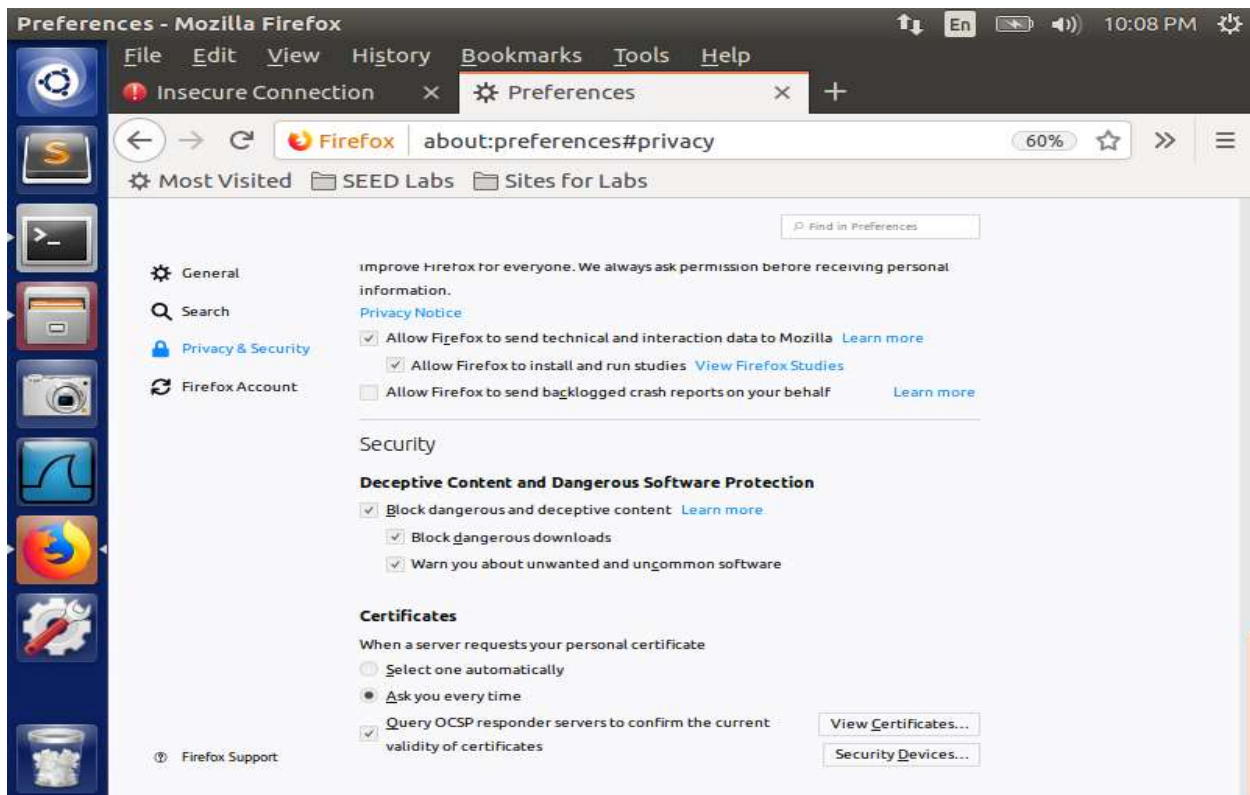

Task 3: Deploying Certificate in an HTTPS Web Server

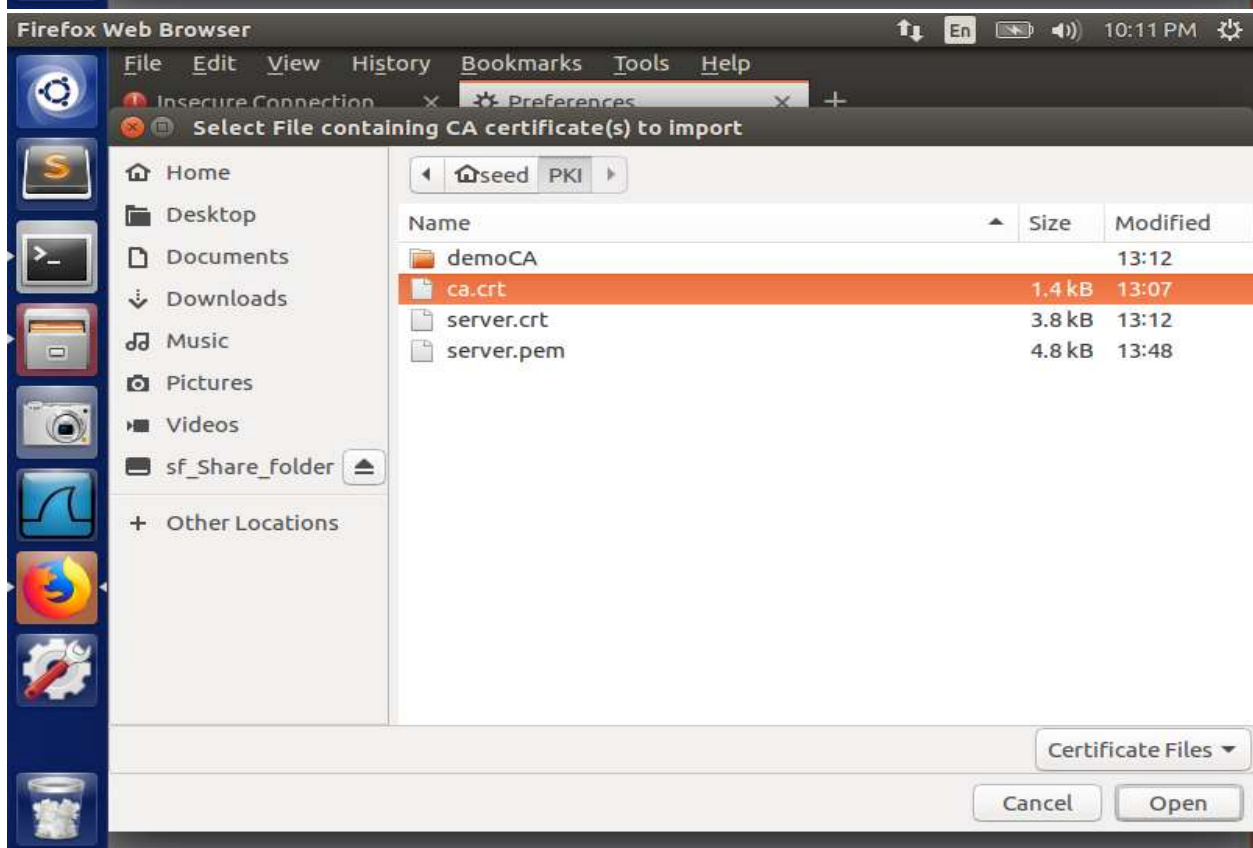
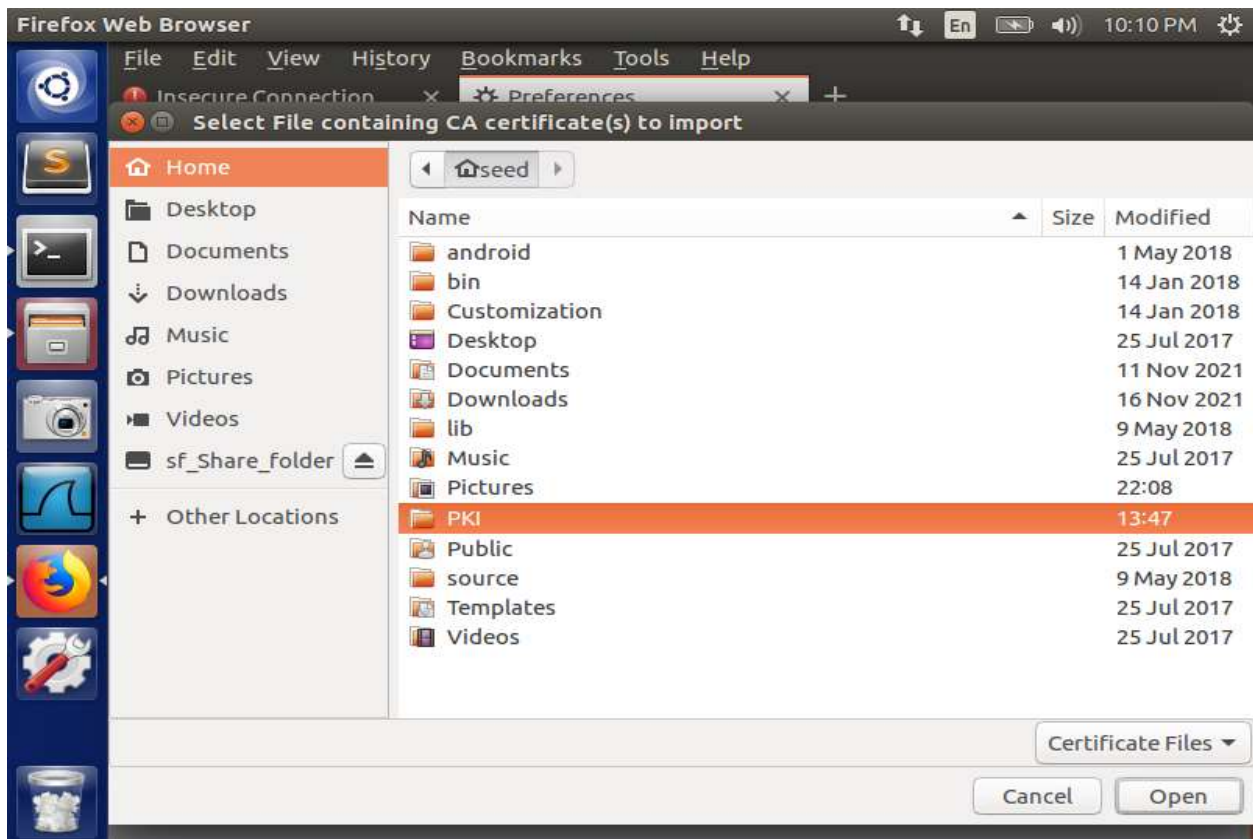
```
Terminal 127.0.0.1 localhost 1:46 PM
127.0.1.1 VM
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1 User
127.0.0.1 Attacker
127.0.0.1 Server
127.0.0.1 www.SeedLabSQLInjection.com
127.0.0.1 www.xsslabelgg.com
127.0.0.1 www.csrflabelgg.com
127.0.0.1 www.csrfabattacker.com
127.0.0.1 www.repackagingattacklab.com
127.0.0.1 www.seedlabclickjacking.com
127.0.0.1 SEEDPKILab2021.com
~
:wq!
```

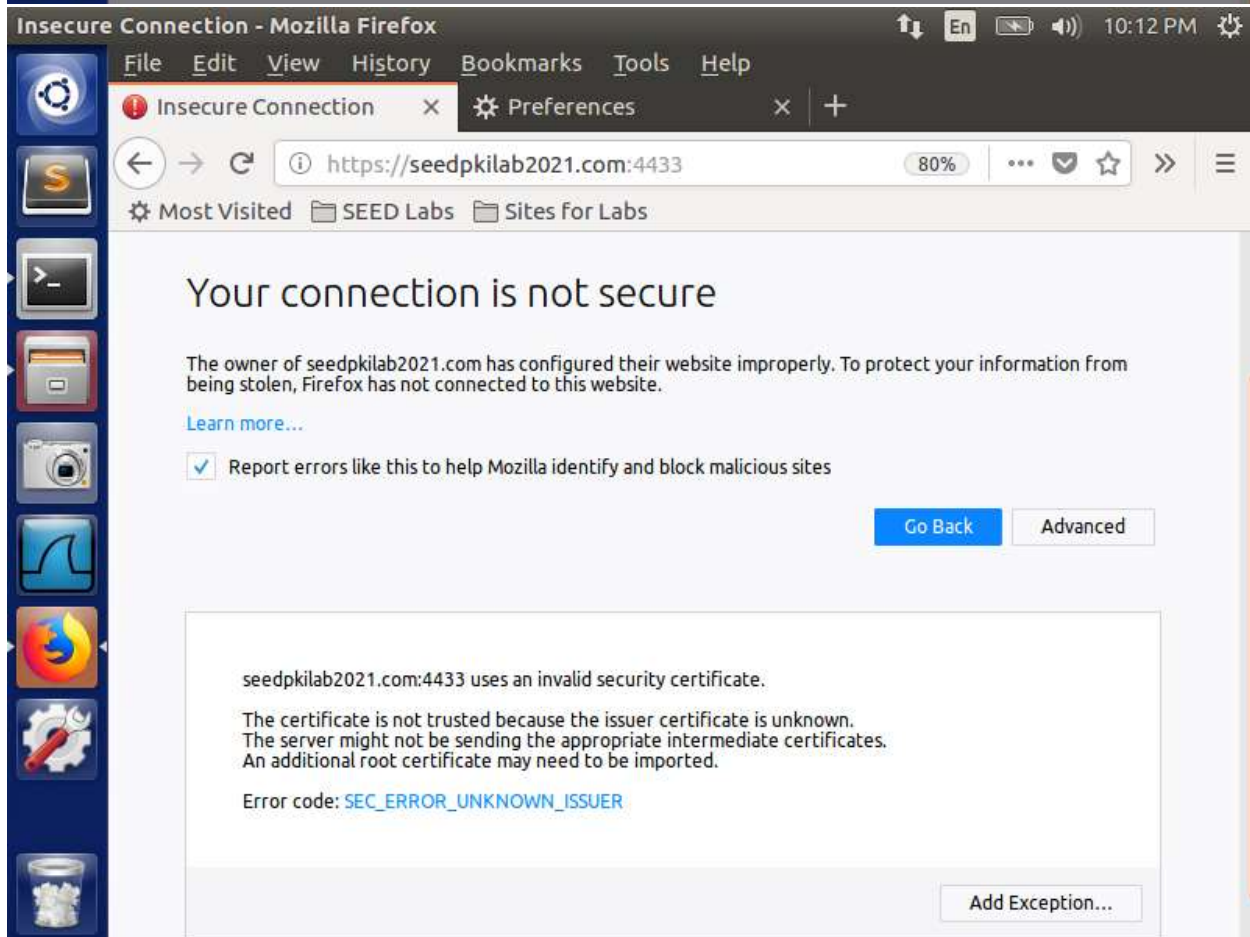
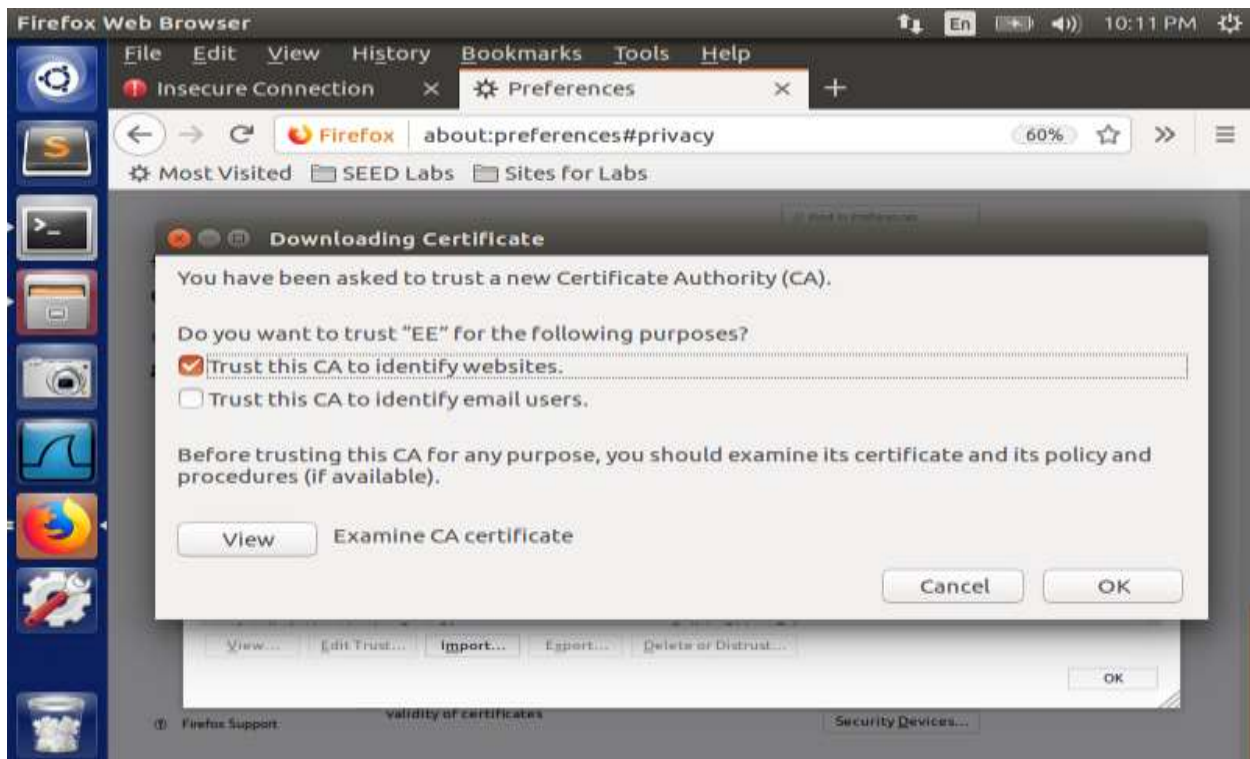
```
Terminal 1:50 PM
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]
y
Write out database with 1 new entries
Data Base Updated
[01/01/22]seed@VM:~/PKI$ sudo vi /etc/hosts
[1]+  Stopped sudo vi /etc/hosts
[01/01/22]seed@VM:~/PKI$ sudo vi /etc/hosts
[01/01/22]seed@VM:~/PKI$ sudo vi /etc/hosts
[01/01/22]seed@VM:~/PKI$ sudo vi /etc/hosts
[01/01/22]seed@VM:~/PKI$ cp server.key server.pem
[01/01/22]seed@VM:~/PKI$ cat server.crt >> server.pem
[01/01/22]seed@VM:~/PKI$ openssl s_server -cert server.
pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
```



```
[01/01/22]seed@VM:~/PKI$ sudo vi /etc/hosts
[01/01/22]seed@VM:~/PKI$ sudo vi /etc/hosts
[01/01/22]seed@VM:~/PKI$ sudo vi /etc/hosts
[01/01/22]seed@VM:~/PKI$ cp server.key server.pem
[01/01/22]seed@VM:~/PKI$ cat server.crt >> server.pem
[01/01/22]seed@VM:~/PKI$ openssl s_server -cert server.
pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
ACCEPT
ACCEPT
ACCEPT
█
```





Mozilla Firefox

File Edit View History Bookmarks Tools Help

seedpkilab2021.com:4433/ x Preferences x +

https://seedpkilab2021.com:4433 70% ... ☆ >> ≡

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-SHA384 TLSv1/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-RSA-AES256-GCM-SHA384 TLSv1/SSLv3: DH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3: DHE-RSA-AES256-SHA256 TLSv1/SSLv3: DH-RSA-AES256-SHA256
TLSv1/SSLv3: DH-DSS-AES256-SHA256 TLSv1/SSLv3: DHE-RSA-AES256-SHA
TLSv1/SSLv3: DH-DSS-AES256-SHA TLSv1/SSLv3: DH-RSA-AES256-SHA
TLSv1/SSLv3: DH-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-SHA384 TLSv1/SSLv3: ECDH-RSA-AES256-SHA384
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-SHA256 TLSv1/SSLv3: ECDHE-ECDSA-AES128-GCM-SHA256
TLSv1/SSLv3: ECDHE-RSA-AES128-SHA256 TLSv1/SSLv3: ECDHE-ECDSA-AES128-SHA256
TLSv1/SSLv3: ECDHE-RSA-AES128-SHA TLSv1/SSLv3: ECDHE-ECDSA-AES128-SHA
TLSv1/SSLv3: SRP-DSS-AES-128-CBC-SHA TLSv1/SSLv3: SRP-RSA-AES-128-CBC-SHA
TLSv1/SSLv3: SRP-AES-128-CBC-SHA TLSv1/SSLv3: DH-DSS-AES128-GCM-SHA256
TLSv1/SSLv3: DHE-RSA-AES128-GCM-SHA256 TLSv1/SSLv3: DH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3: DHE-RSA-AES128-SHA256 TLSv1/SSLv3: DH-RSA-AES128-SHA256
TLSv1/SSLv3: DHE-DSS-AES128-SHA256 TLSv1/SSLv3: DH-RSA-AES128-SHA
TLSv1/SSLv3: DH-DSS-AES128-SHA TLSv1/SSLv3: DH-RSA-SEED-SHA
TLSv1/SSLv3: DHE-DSS-SEED-SHA TLSv1/SSLv3: DH-RSA-SEED-SHA
TLSv1/SSLv3: DH-DSS-SEED-SHA TLSv1/SSLv3: DHE-RSA-CAMELLIA128-SHA
TLSv1/SSLv3: DH-DSS-CAMELLIA128-SHA TLSv1/SSLv3: DH-RSA-CAMELLIA128-SHA
TLSv1/SSLv3: DH-DSS-CAMELLIA128-SHA TLSv1/SSLv3: ECDH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3: ECDH-ECDSA-AES128-GCM-SHA256 TLSv1/SSLv3: ECDH-RSA-AES128-SHA256
TLSv1/SSLv3: ECDH-ECDSA-AES128-SHA TLSv1/SSLv3: AES128-GCM-SHA256
TLSv1/SSLv3: AES128-SHA256 TLSv1/SSLv3: AES128-SHA
TLSv1/SSLv3: SEED-SHA TLSv1/SSLv3: CAMELLIA128-SHA
TLSv1/SSLv3: PSK-AES128-CBC-SHA TLSv1/SSLv3: ECDHE-RSA-RC4-SHA
TLSv1/SSLv3: ECDHE-ECDSA-RC4-SHA TLSv1/SSLv3: ECDH-RSA-RC4-SHA
TLSv1/SSLv3: ECDH-ECDSA-RC4-SHA TLSv1/SSLv3: RC4-SHA
```

Mozilla Firefox

File Edit View History Bookmarks Tools Help

seedpkilab2021.com:4433/ x Preferences x +

https://seedpkilab2021.com:4433 70% ... ☆ >> ≡

Most Visited SEED Labs Sites for Labs

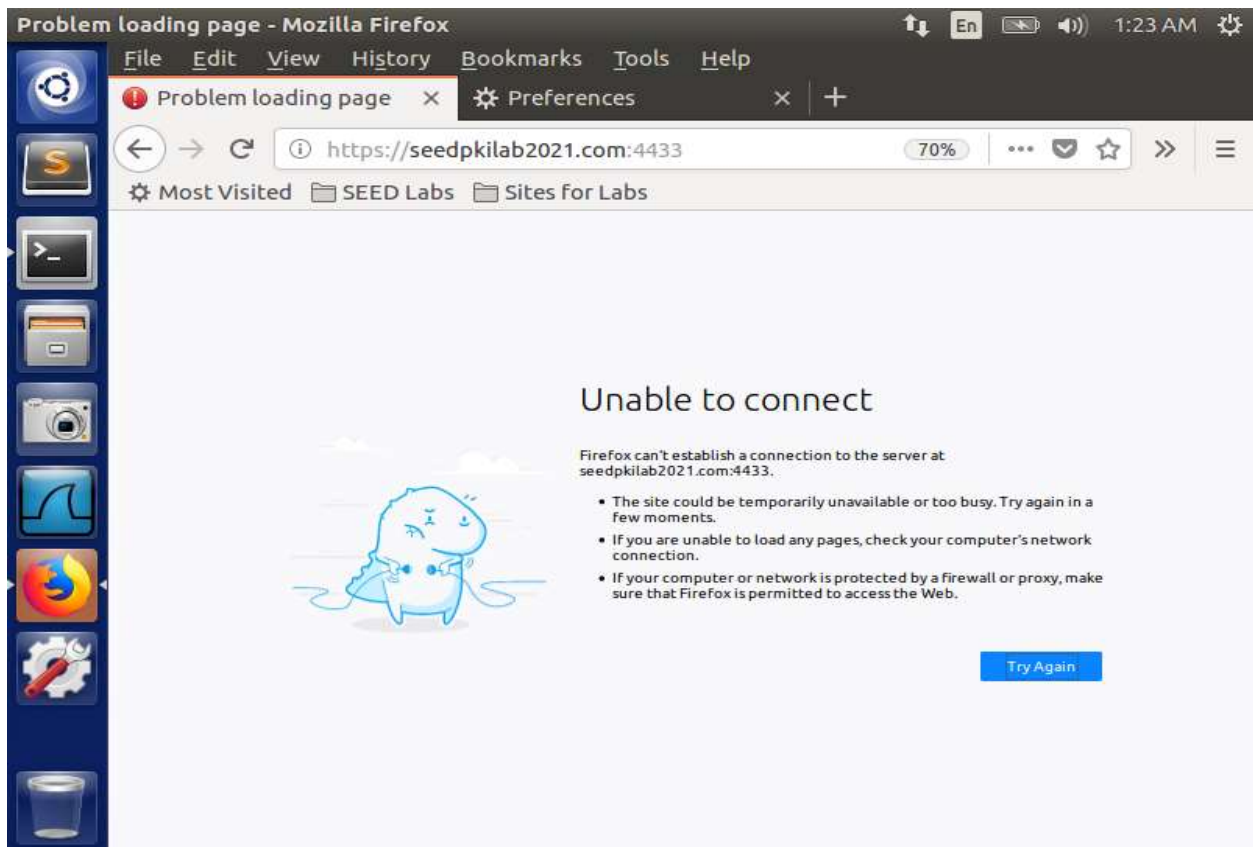
```

TLSv1/SSLv3: ECDH-RSA-AES128-SHA
TLSv1/SSLv3: DH-DSS-DES-CBC3-SHA
TLSv1/SSLv3: ECDH-ECDSA-DES-CBC3-SHA
TLSv1/SSLv3: PSK-3DES-EDE-CBC-SHA
...
Ciphers common between both SSL end points:
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-SHA ECDHE-RSA-AES256-SHA
AES128-SHA AES256-SHA DES-CBC3-SHA
Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:0x04:0x08:0x05:0x08:0x06:0x08:RSA+SHA256:RSA+SHA384:RSA+SHA512:ECDSA+SHA1:RSA+SHA1
Shared Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:RSA+SHA256:RSA+SHA384:RSA+SHA512:ECDSA+SHA1:RSA+SHA1
Supported Elliptic Curves: 0x0010:P-256:P-384:P-521:0x0100:0x0101
Shared Elliptic curves: P-256:P-384:P-521
...
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
SSL-Session:
  Protocol : TLSv1.2
  Cipher : ECDHE-RSA-AES128-GCM-SHA256
  Session-ID:
  Session-ID-ctx: 01000000
  Master-Key: E0E8E0C2514B6F37526B698B75C1C018382A17A11A7B4F4E7479E87FE79C0032465322E339F314F3141183C2FF710C
  Key-Arg : None
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  Start Time: 1641093150
  Timeout : 300 (sec)
  Verify return code: 0 (ok)
...
0 items in the session cache
0 client connects (SSL_connect())
0 client renegotiates (SSL_connect())
0 client connects that finished
4 server accepts (SSL_accept())
0 server renegotiates (SSL_accept())
4 server accepts that finished
0 session cache hits
4 session cache misses
0 session cache timeouts
0 callback cache hits
0 cache full overflows (128 allowed)
...
no client certificate available
```



```
Terminal 1:17 AM
23 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
[01/02/22]seed@VM:~/PKI$ sudo vi /etc/hosts
[01/02/22]seed@VM:~/PKI$ sudo vi /etc/hosts
[01/02/22]seed@VM:~/PKI$ cp server.key server.pem
[01/02/22]seed@VM:~/PKI$ cat server.crt >> server.pem
[01/02/22]seed@VM:~/PKI$ openssl s_server -cert server.
pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
```

```
Terminal 1:23 AM
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,A1E9F441B87453FF0E1BF4AC6B2BA667
hMkApDquPYVpXoKpi6U3QA5Y9xc710/HQA1VzdC9q5rq05+qZzKsZeQ
4mAW18ehP
CRWYTp0RQjldaz9t1F6KRGkxwe7AupRmoFY3v0foavx4VFAGiBpCg7V
cxNSXKYoc
0z4xVac10MGM69MsVoZj54E3q+d5L0w/f4q4Let56L94KbQYQ0ZLcUR
8UixJ4r60
Sl0JNpaZcjwZ24t6eldmljK7dt+TaB44Ldk5BWa1FVVDrhZv4y6bED5
/xG3RKwiS
Gck8MRXEG0/yfLQVGQnvstfNV04NaA5pN5PaiiNm7aMZJ2uUG1x9n+j
+u1sG9mLK
/+gscSD83r8Z0U0eE3XRbWX7suIiXwzto1gt1VxCn3I6b0b0ydbj1gb
+WubMFZoi
LunsjcAbtFKTs2A+PCfeFikYkEKKoID8ghs06jE4gkKzfps3hS2181F
yf0LTiKpw
2r6xMMhrLcChe7KkiukxkY3SyLApVHfZigGbgksiV6ZX0U11mBYshGU
Q6axGXPav
@
-- INSERT -- 5,2 Top
```



```
[01/02/22]seed@VM:~/PKI$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
unable to load server certificate private key file
3070461632:error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag:tasn_dec.c:1197:
3070461632:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error:tasn_dec.c:374:Type=RSA
3070461632:error:04093004:rsa routines:OLD_RSA_PRIV_DECODE:RSA lib:rsa_ameth.c:119:
3070461632:error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag:tasn_dec.c:1197:
3070461632:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error:tasn_dec.c:374:Type=PKCS8_PRIV_KEY_INFO
3070461632:error:0907B00D:PEM routines:PEM_READ_BIO_PRIVATEKEY:ASN1 lib:pem_pkey.c:141:
[01/02/22]seed@VM:~/PKI$
```



```
[01/02/22]seed@VM:~/PKI$ sudo vi server.pem
[01/02/22]seed@VM:~/PKI$ openssl s_server -cert server.
pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
ACCEPT
```

Terminal ↑ En 🔊 1:35 AM ⚙️

```
unable to load server certificate private key file
3070461632:error:0D0680A8:asn1 encoding routines:ASN1_C
HECK_TLEN:wrong tag:tasn_dec.c:1197:
3070461632:error:0D07803A:asn1 encoding routines:ASN1_I
TEM_EX_D2I:nested asn1 error:tasn_dec.c:374:Type=RSA
3070461632:error:04093004:rsa routines:OLD_RSA_PRIV_DEC
ODE:RSA lib:rsa_ameth.c:119:
3070461632:error:0D0680A8:asn1 encoding routines:ASN1_C
HECK_TLEN:wrong tag:tasn_dec.c:1197:
3070461632:error:0D07803A:asn1 encoding routines:ASN1_I
TEM_EX_D2I:nested asn1 error:tasn_dec.c:374:Type=PKCS8_
PRIV_KEY_INFO
3070461632:error:0907B00D:PEM routines:PEM_READ_BIO_PRI
VATEKEY:ASN1 lib:pem_pkey.c:141:
[01/02/22]seed@VM:~/PKI$ sudo vi server.pem
[01/02/22]seed@VM:~/PKI$ openssl s_server -cert server.
pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
ACCEPT
```

Mozilla Firefox

File Edit View History Bookmarks Tools Help

seedpkilab2021.com:4433/ x Preferences x +

https://seedpkilab2021.com:4433 70% ...

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-SHA384
TLSv1/SSLv3: ECDHE-RSA-AES256-SHA
TLSv1/SSLv3: SRP-DSS-AES-256-CBC-SHA
TLSv1/SSLv3: SRP-AES-256-CBC-SHA
TLSv1/SSLv3: DHE-DSS-AES256-GCM-SHA384
TLSv1/SSLv3: DHE-RSA-AES256-GCM-SHA384
TLSv1/SSLv3: DHE-RSA-AES256-SHA
TLSv1/SSLv3: DHE-DSS-AES256-SHA256
TLSv1/SSLv3: DH-DSS-AES256-SHA
TLSv1/SSLv3: DH-DSS-CAMELLIA256-SHA
TLSv1/SSLv3: DH-DSS-CAMELLIA256-SHA
TLSv1/SSLv3: ECDH-ECDSA-AES256-GCM-SHA384
TLSv1/SSLv3: ECDH-ECDSA-AES256-SHA
TLSv1/SSLv3: AES256-GCM-SHA384
TLSv1/SSLv3: AES256-SHA
TLSv1/SSLv3: CAMELLIA256-SHA
TLSv1/SSLv3: ECDHE-RSA-AES128-GCM-SHA256
TLSv1/SSLv3: ECDHE-RSA-AES128-SHA
TLSv1/SSLv3: SRP-DSS-AES-128-CBC-SHA
TLSv1/SSLv3: SRP-AES-128-CBC-SHA
TLSv1/SSLv3: DHE-DSS-AES128-GCM-SHA256
TLSv1/SSLv3: DHE-RSA-AES128-GCM-SHA256
TLSv1/SSLv3: DHE-DSS-AES128-SHA
TLSv1/SSLv3: DH-DSS-AES128-SHA
TLSv1/SSLv3: DH-DSS-SEED-SHA
TLSv1/SSLv3: DH-DSS-SEED-SHA
TLSv1/SSLv3: DHE-DSS-CAMELLIA128-SHA
TLSv1/SSLv3: DH-DSS-CAMELLIA128-SHA
TLSv1/SSLv3: ECDH-ECDSA-AES128-GCM-SHA256
TLSv1/SSLv3: ECDH-ECDSA-AES128-SHA
TLSv1/SSLv3: ECDH-ECDSA-AES128-SHA
TLSv1/SSLv3: AES128-GCM-SHA256
TLSv1/SSLv3: AES128-SHA
TLSv1/SSLv3: SEED-SHA
TLSv1/SSLv3: PSK-AES128-CBC-SHA
TLSv1/SSLv3: ECDHE-ECDSA-RC4-SHA
TLSv1/SSLv3: ECDH-ECDSA-RC4-SHA
TLSv1/SSLv3: ECDHE-ECDSA-AES256-GCM-SHA384
TLSv1/SSLv3: ECDHE-ECDSA-AES256-SHA
TLSv1/SSLv3: SRP-RSA-AES-256-CBC-SHA
TLSv1/SSLv3: DH-DSS-AES256-GCM-SHA384
TLSv1/SSLv3: DH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3: DH-RSA-AES256-SHA
TLSv1/SSLv3: DHE-RSA-AES256-SHA
TLSv1/SSLv3: DHE-RSA-CAMELLIA256-SHA
TLSv1/SSLv3: DH-RSA-CAMELLIA256-SHA
TLSv1/SSLv3: ECDH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3: ECDH-RSA-AES256-SHA
TLSv1/SSLv3: AES256-GCM-SHA384
TLSv1/SSLv3: AES256-SHA
TLSv1/SSLv3: PSK-AES256-CBC-SHA
TLSv1/SSLv3: ECDHE-ECDSA-AES128-GCM-SHA256
TLSv1/SSLv3: ECDHE-ECDSA-AES128-SHA
TLSv1/SSLv3: ECDH-ECDSA-AES128-SHA
TLSv1/SSLv3: SRP-RSA-AES-128-CBC-SHA
TLSv1/SSLv3: DH-DSS-AES128-GCM-SHA256
TLSv1/SSLv3: DH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3: DHE-RSA-AES128-SHA
TLSv1/SSLv3: DH-RSA-AES128-SHA
TLSv1/SSLv3: DHE-RSA-AES128-SHA
TLSv1/SSLv3: DH-RSA-SEED-SHA
TLSv1/SSLv3: DH-RSA-SEED-SHA
TLSv1/SSLv3: DHE-RSA-CAMELLIA128-SHA
TLSv1/SSLv3: DH-RSA-CAMELLIA128-SHA
TLSv1/SSLv3: ECDH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3: ECDH-RSA-AES128-SHA
TLSv1/SSLv3: AES128-GCM-SHA256
TLSv1/SSLv3: AES128-SHA
TLSv1/SSLv3: CAMELLIA128-SHA
TLSv1/SSLv3: ECDHE-RSA-RC4-SHA
TLSv1/SSLv3: ECDH-RSA-RC4-SHA
TLSv1/SSLv3: RC4-SHA
```

Mozilla Firefox

File Edit View History Bookmarks Tools Help

seedpkilab2021.com:4433/ x Preferences x +

https://seedpkilab2021.com:4433 70% ...

Most Visited SEED Labs Sites for Labs

```

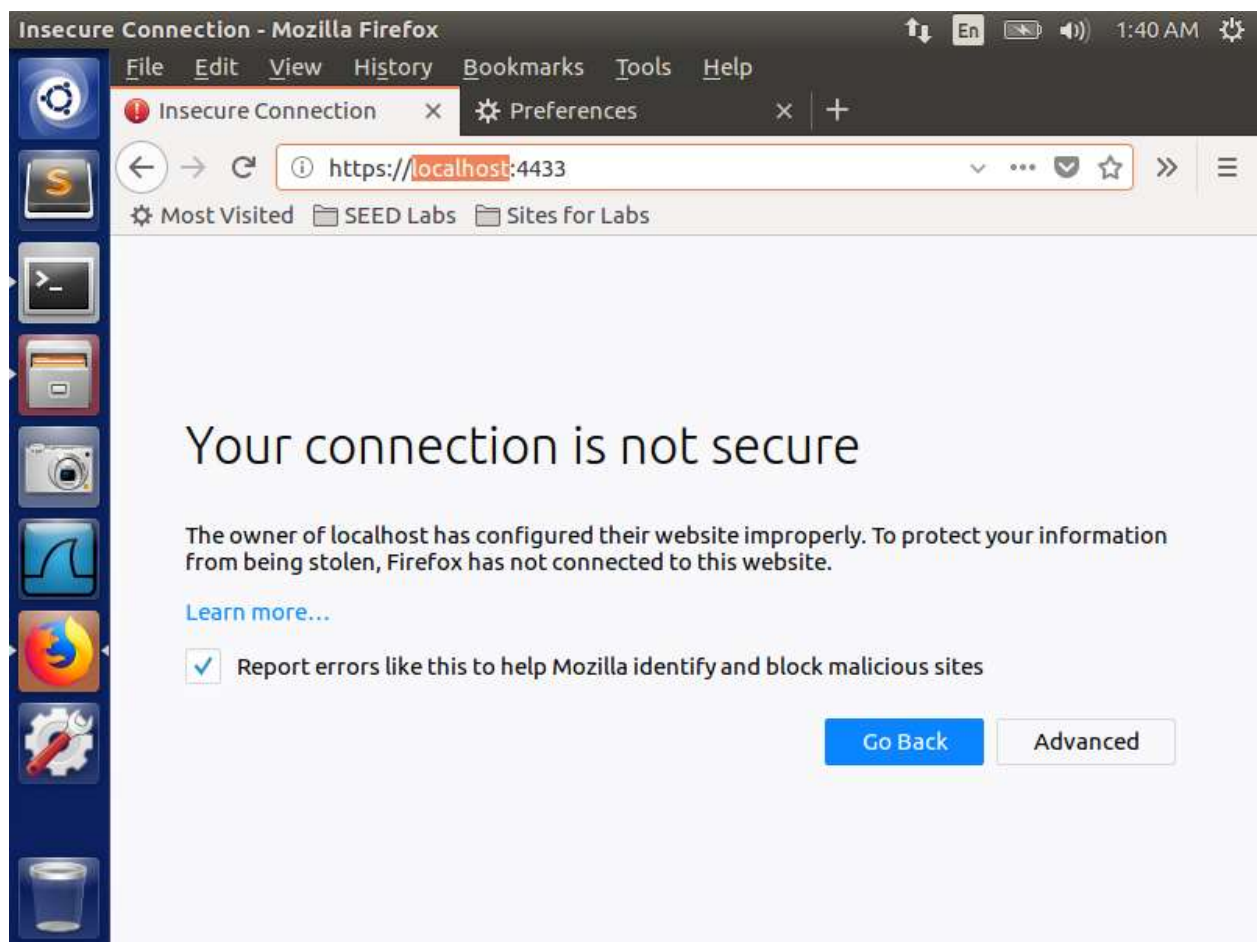
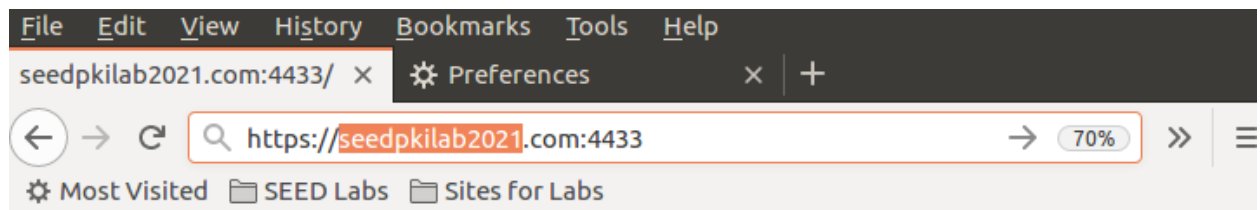
TLSv1/SSLv3: ECDH-ECDSA-AES128-GCM-SHA256
TLSv1/SSLv3: ECDH-ECDSA-AES128-SHA
TLSv1/SSLv3: SRP-DSS-AES-128-CBC-SHA
TLSv1/SSLv3: SRP-AES-128-CBC-SHA
TLSv1/SSLv3: DHE-DSS-AES128-GCM-SHA256
TLSv1/SSLv3: DHE-RSA-AES128-GCM-SHA256
TLSv1/SSLv3: DHE-DSS-AES128-SHA
TLSv1/SSLv3: DH-DSS-AES128-SHA
TLSv1/SSLv3: DH-DSS-SEED-SHA
TLSv1/SSLv3: DH-DSS-SEED-SHA
TLSv1/SSLv3: DHE-DSS-CAMELLIA128-SHA
TLSv1/SSLv3: DH-DSS-CAMELLIA128-SHA
TLSv1/SSLv3: ECDH-ECDSA-AES128-GCM-SHA256
TLSv1/SSLv3: ECDH-ECDSA-AES128-SHA
TLSv1/SSLv3: ECDH-ECDSA-AES128-SHA
TLSv1/SSLv3: AES128-GCM-SHA256
TLSv1/SSLv3: AES128-SHA
TLSv1/SSLv3: SEED-SHA
TLSv1/SSLv3: PSK-AES128-CBC-SHA
TLSv1/SSLv3: ECDHE-ECDSA-RC4-SHA
TLSv1/SSLv3: ECDH-ECDSA-RC4-SHA
TLSv1/SSLv3: RC4-SHA

Ciphers common between both SSL end points:
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-SHA
AES128-SHA AES256-SHA DES-CBC3-SHA
Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:0x04:0x08:0x05:0x08:0x06:0x08:RSA+SHA256:RSA+SHA384:RSA+SHA512:ECDSA+SHA1:RSA+SHA1
Shared Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:RSA+SHA256:RSA+SHA384:RSA+SHA512:ECDSA+SHA1:RSA+SHA1
Supported Elliptic Curves: 0x001D:P-256:P-384:P-521:0x0100:0x0101
Shared Elliptic curves: P-256:P-384:P-521

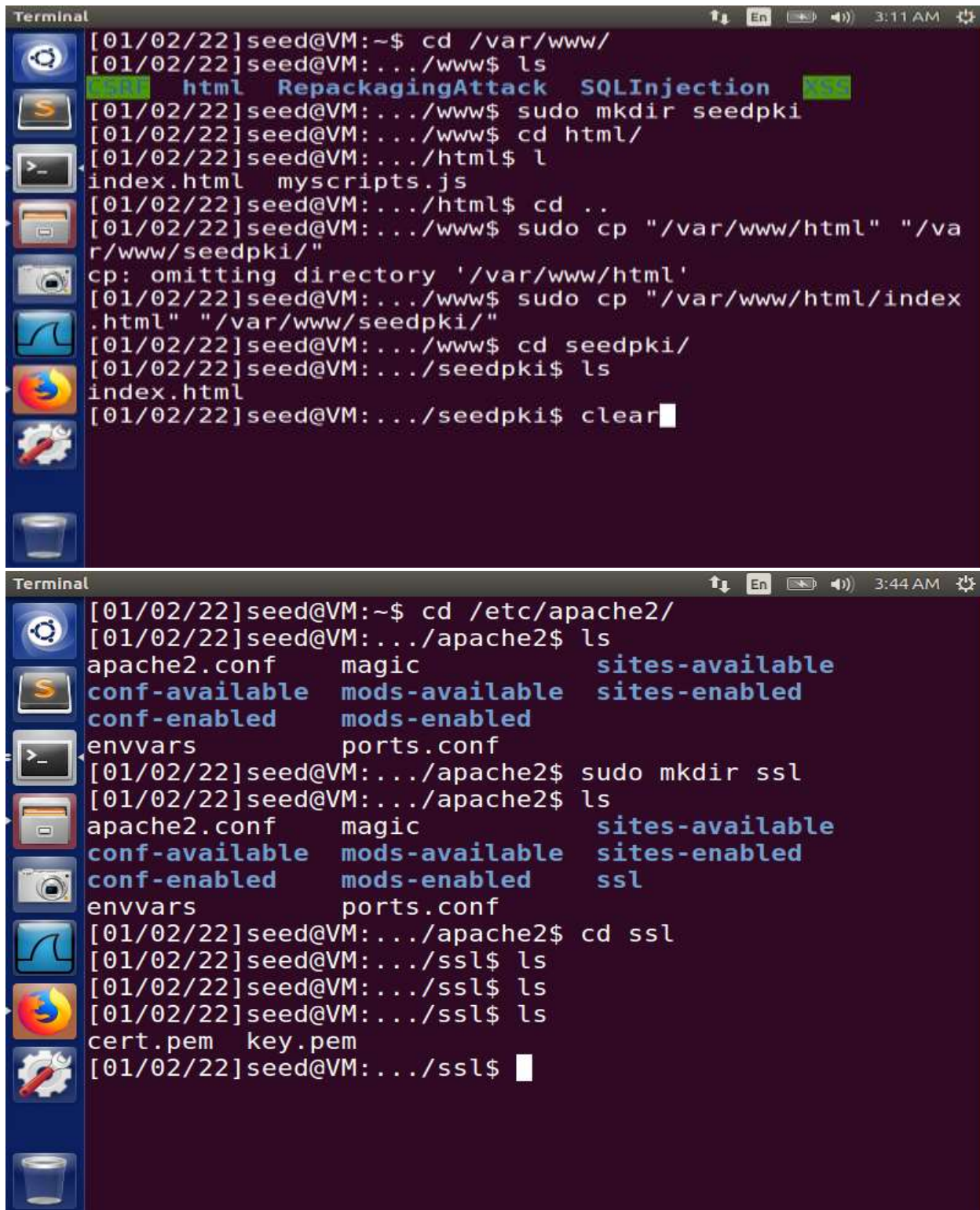
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
SSL Session:
Protocol : TLSv1.2
Cipher : ECDHE-RSA-AES128-GCM-SHA256
Session-ID:
Session-ID-ctx: 01000000
Master-Key: 9A6FB1063906A49EA69B34A659ECBC031A6FDEE109AE8B03582939982AFE42B390003FC2E58ED94D012290D89495EBA6
Key-Arg : None
PSK identity: None
PSK identity hint: None
SRP username: None
Start Time: 1641105259
Timeout : 300 (sec)
Verify return code: 0 (ok)

0 items in the session cache
0 client connects (SSL_connect())
0 client renegotiates (SSL_connect())
0 client connects that finished
1 server accepts (SSL_accept())
0 server renegotiates (SSL_accept())
1 server accepts that finished
0 session cache hits
1 session cache misses
0 session cache timeouts
0 callback cache hits
0 cache full overflows (128 allowed)

no client certificate available
```

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



The image shows two terminal windows from a VM named 'seed'. The top window shows the process of creating a directory structure for the website and copying files. The bottom window shows the process of creating an SSL directory and generating certificates.

```
Terminal
[01/02/22]seed@VM:~$ cd /var/www/
[01/02/22]seed@VM:.../www$ ls
html  RepackagingAttack  SQLInjection  XSS
[01/02/22]seed@VM:.../www$ sudo mkdir seedpki
[01/02/22]seed@VM:.../www$ cd html/
[01/02/22]seed@VM:.../html$ ls
index.html  myscripts.js
[01/02/22]seed@VM:.../html$ cd ..
[01/02/22]seed@VM:.../www$ sudo cp "/var/www/html" "/va
r/www/seedpki/"
cp: omitting directory '/var/www/html'
[01/02/22]seed@VM:.../www$ sudo cp "/var/www/html/index
.html" "/var/www/seedpki/"
[01/02/22]seed@VM:.../www$ cd seedpki/
[01/02/22]seed@VM:.../seedpki$ ls
index.html
[01/02/22]seed@VM:.../seedpki$ clear

Terminal
[01/02/22]seed@VM:~$ cd /etc/apache2/
[01/02/22]seed@VM:.../apache2$ ls
apache2.conf  magic  sites-available
conf-available  mods-available  sites-enabled
conf-enabled  mods-enabled
envvars  ports.conf
[01/02/22]seed@VM:.../apache2$ sudo mkdir ssl
[01/02/22]seed@VM:.../apache2$ ls
apache2.conf  magic  sites-available
conf-available  mods-available  sites-enabled
conf-enabled  mods-enabled  ssl
envvars  ports.conf
[01/02/22]seed@VM:.../apache2$ cd ssl
[01/02/22]seed@VM:.../ssl$ ls
[01/02/22]seed@VM:.../ssl$ ls
[01/02/22]seed@VM:.../ssl$ ls
cert.pem  key.pem
[01/02/22]seed@VM:.../ssl$
```



```
Terminal
[01/02/22]seed@VM:~$ cd PKI/
[01/02/22]seed@VM:~/PKI$ cp server.crt cert.pem
[01/02/22]seed@VM:~/PKI$ cp server.key key.pem
[01/02/22]seed@VM:~/PKI$ sudo mv "/home/seed/PKI/cert.p
em" "/etc/apache2/ssl/"
[01/02/22]seed@VM:~/PKI$ sudo mv "/home/seed/PKI/key.pe
m" "/etc/apache2/ssl/"
[01/02/22]seed@VM:~/PKI$
```

```
Terminal
<VirtualHost *:80>
    ServerName SEEDPKILab2021.com
    DocumentRoot /var/www/seedpki
    DirectoryIndex index.html
</VirtualHost>

<VirtualHost *:80>
    # The ServerName directive sets the request sch
eme, hostname and port that
    # the server uses to identify itself. This is u
sed when creating
    # redirection URLs. In the context of virtual h
osts, the ServerName
    # specifies what hostname must appear in the re
quest's Host: header to
    # match this virtual host. For the default virt
ual host (this file) this
    # value is not decisive as it is used as a last
resort host regardless.
-- INSERT --                    5,15                    Top
```

```
Terminal 3:56 AM
<IfModule mod_ssl.c>
<VirtualHost *:80>
    ServerName SEEDPKILab2021.com
    DocumentRoot /var/www/seedpki
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /etc/apache2/ssl/cert.pem
    SSLCertificateKeyFile /etc/apache2/ssl/key.pem
</VirtualHost>

    <VirtualHost _default_:443>
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www/html

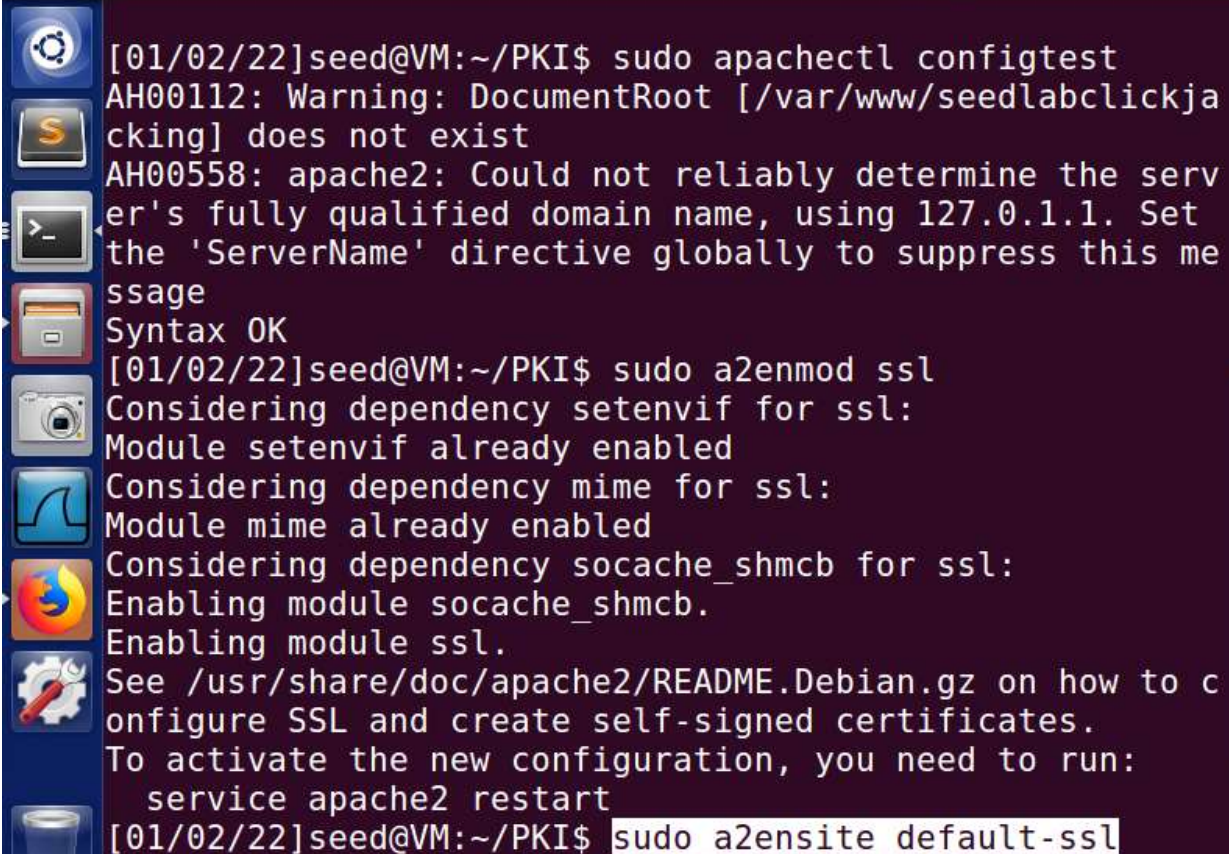
        # Available loglevels: trace8, ..., tra
cel, debug, info, notice, warn,
        # error, crit, alert, emerg.
-- INSERT --                                     9,48-55      Top
```

```
Terminal 3:59 AM
[01/02/22]seed@VM:~/ssl$ ls
[01/02/22]seed@VM:~/ssl$ ls
cert.pem  key.pem
[01/02/22]seed@VM:~/ssl$ clear
[01/02/22]seed@VM:~/ssl$ cd ..
[01/02/22]seed@VM:~/apache2$ ls
apache2.conf  magic  sites-available
conf-available  mods-available  sites-enabled
conf-enabled  mods-enabled  ssl
envvars  ports.conf
[01/02/22]seed@VM:~/apache2$ cd sites-available
[01/02/22]seed@VM:~/sites-available$ ls
000-default.conf  default-ssl.conf
[01/02/22]seed@VM:~/sites-available$ sudo vi 000-defa
ult.conf
[01/02/22]seed@VM:~/sites-available$ sudo vi default-
ssl.conf
[01/02/22]seed@VM:~/sites-available$
```



```
Terminal
[01/02/22]seed@VM:~/PKI$ sudo apachectl configtest
AH00112: Warning: DocumentRoot [/var/www/seedlabclickja
cking] does not exist
AH00558: apache2: Could not reliably determine the serv
er's fully qualified domain name, using 127.0.1.1. Set
the 'ServerName' directive globally to suppress this me
ssage
Syntax OK
[01/02/22]seed@VM:~/PKI$ 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 c
onfigure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    service apache2 restart
[01/02/22]seed@VM:~/PKI$ sudo a2ensite default-ssl
```

```
Terminal
[01/02/22]seed@VM:~/PKI$ sudo apachectl configtest
AH00112: Warning: DocumentRoot [/var/www/seedlabclickja
cking] does not exist
AH00558: apache2: Could not reliably determine the serv
er's fully qualified domain name, using 127.0.1.1. Set
the 'ServerName' directive globally to suppress this me
ssage
Syntax OK
[01/02/22]seed@VM:~/PKI$ 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 c
onfigure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    service apache2 restart
[01/02/22]seed@VM:~/PKI$ sudo a2ensite default-ssl
```

```
[01/02/22]seed@VM:~/PKI$ sudo apachectl configtest
AH00112: Warning: DocumentRoot [/var/www/seedlabclickja
cking] does not exist
AH00558: apache2: Could not reliably determine the serv
er's fully qualified domain name, using 127.0.1.1. Set
the 'ServerName' directive globally to suppress this me
ssage
Syntax OK
[01/02/22]seed@VM:~/PKI$ 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 c
onfigure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    service apache2 restart
[01/02/22]seed@VM:~/PKI$ sudo a2ensite default-ssl
```

To activate the new configuration, you need to run:

```
service apache2 restart
```

```
[01/02/22]seed@VM:~/PKI$ sudo a2ensite default-ssl
```

Enabling site default-ssl.

To activate the new configuration, you need to run:

```
service apache2 reload
```

```
[01/02/22]seed@VM:~/PKI$ sudo service apache2 restart
```

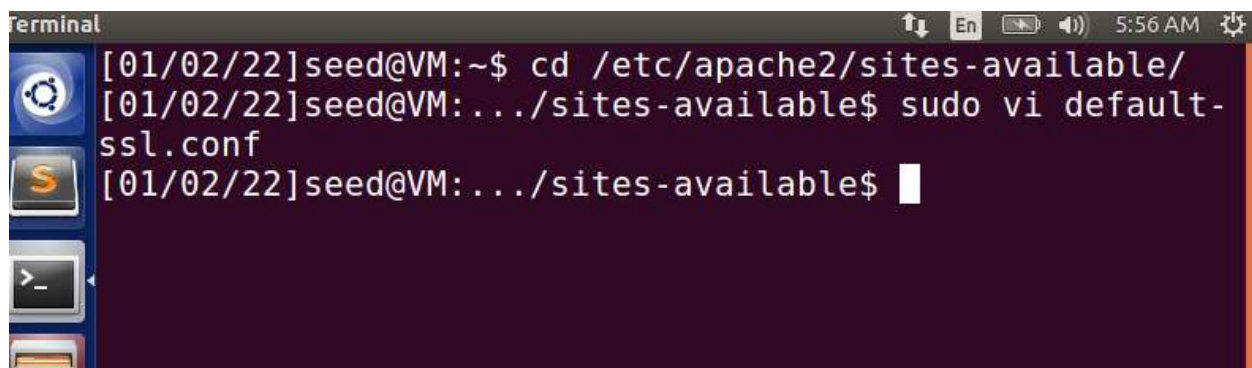
Enter passphrase for SSL/TLS keys for SEEDPKILab2021.co

m:443 (RSA): ****

```
[01/02/22]seed@VM:~/PKI$
```




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



Terminal 5:54 AM

```
<IfModule mod_ssl.c>

<VirtualHost *:443>
    ServerName SEEDPKILab2021.com
    DocumentRoot /var/www/seedpki
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /etc/apache2/ssl/cert.pem
    SSLCertificateKeyFile /etc/apache2/ssl/key.pem
</VirtualHost>

<VirtualHost *:443>
    ServerName instagram.com
    DocumentRoot /var/www/seedpki
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /etc/apache2/ssl/cert.pem
    SSLCertificateKeyFile /etc/apache2/ssl/key.pem
</VirtualHost>

:wq!
```

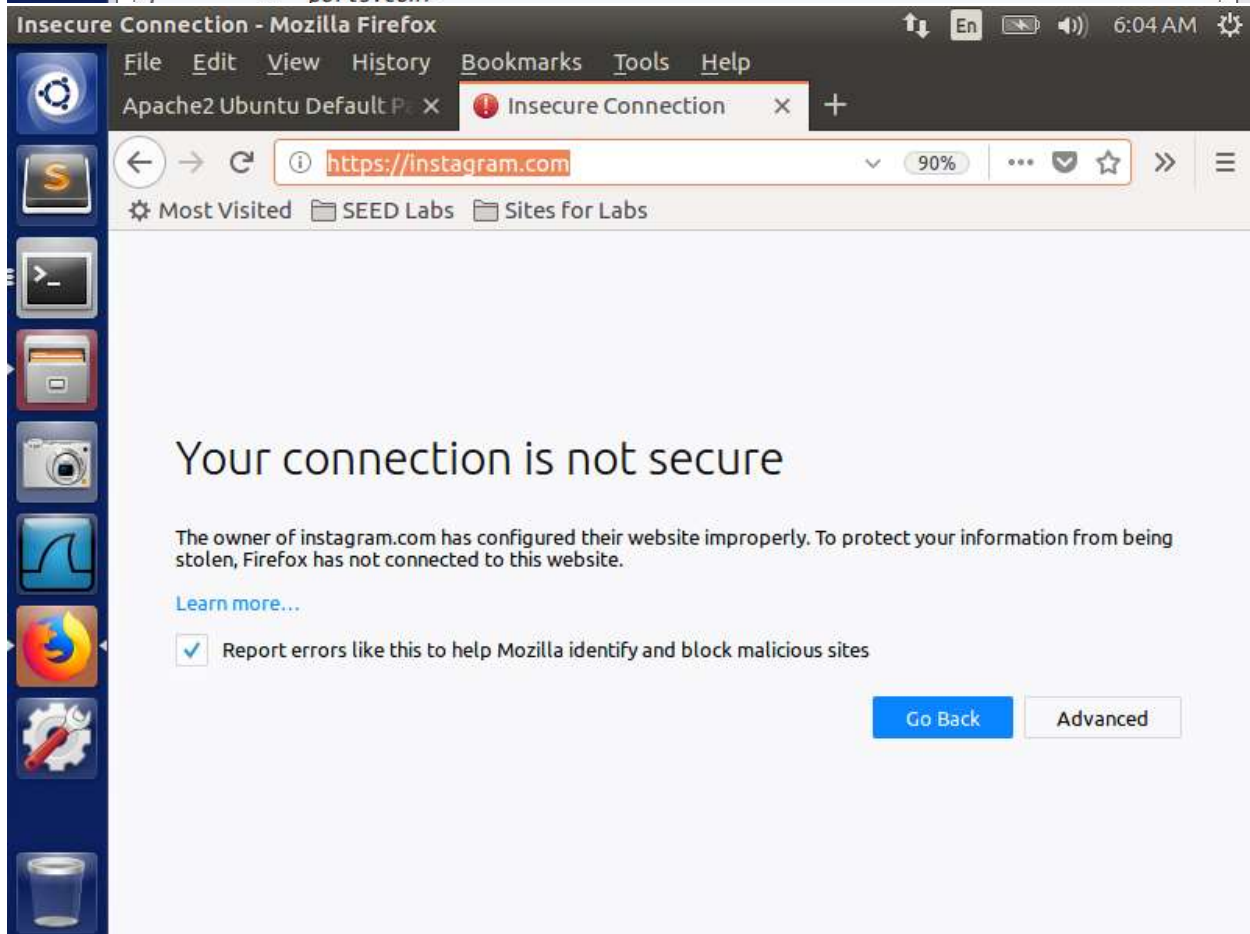
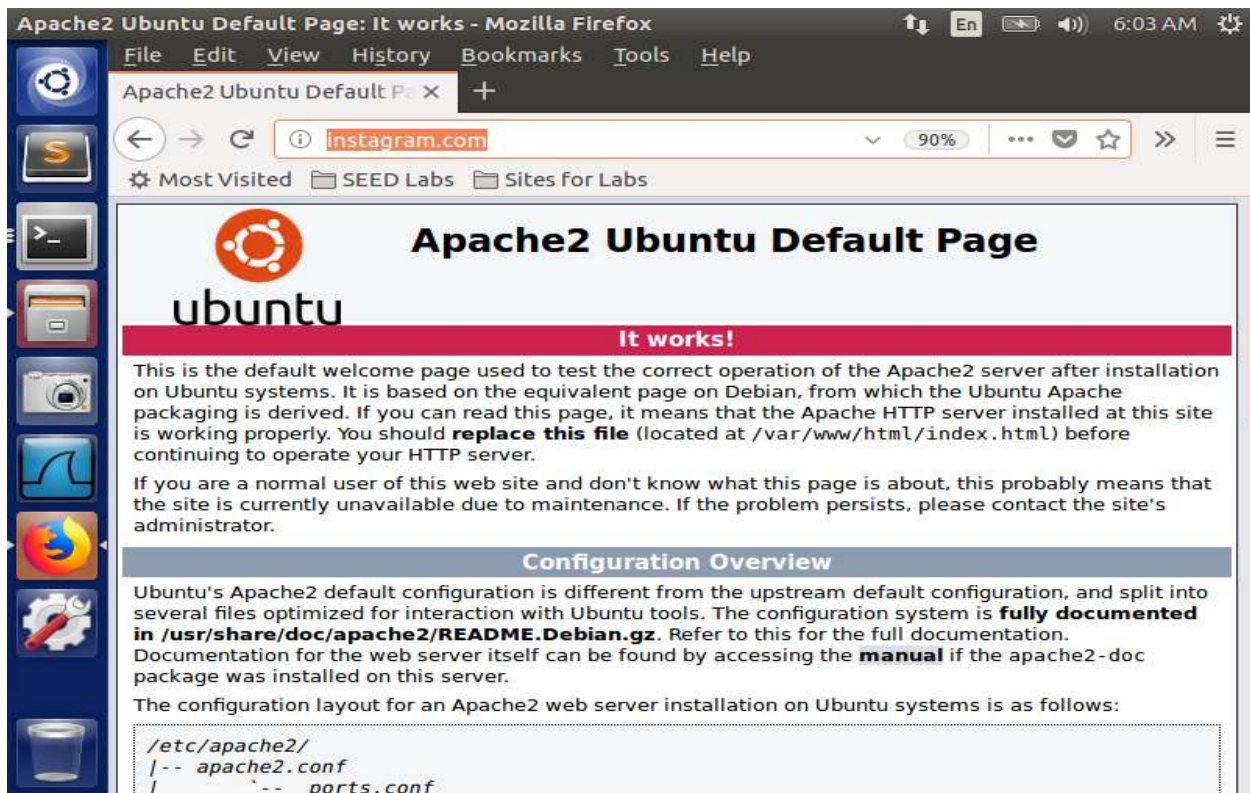


```
Terminal
127.0.0.1      localhost
127.0.1.1      VM

# The following lines are desirable for IPv6 capable ho
sts
::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.csrfattacklab.com
127.0.0.1     www.repackagingattacklab.com
127.0.0.1     www.seedlabclickjacking.com
127.0.0.1     SEEDPKILab2021.com
127.0.0.1     instagram.com
-- INSERT --
```

```
Terminal
[01/02/22]seed@VM:~$ sudo vi /etc/hosts
[01/02/22]seed@VM:~$ sudo vi /etc/hosts
[01/02/22]seed@VM:~$
```

```
Terminal
[01/02/22]seed@VM:~$ cd PKI/
[01/02/22]seed@VM:~/PKI$ sudo service apache2 restart
Enter passphrase for SSL/TLS keys for instagram.com:443
(RSA): ****
[01/02/22]seed@VM:~/PKI$
```



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

```
Terminal
[01/02/22]seed@VM:~/PKI$ openssl req -new -key server.key -out youtube.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]:SA
State or Province Name (full name) [Some-State]:Riyadh
Locality Name (eg, city) []:Rio
Organization Name (eg, company) [Internet Widgits Pty Ltd]:STC
Organizational Unit Name (eg, section) []:STCKSA
Common Name (e.g. server FQDN or YOUR name) []:youtube.com
Email Address []:elham@gmail.com

Terminal
Email Address []:elham@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:abc123
An optional company name []:
[01/02/22]seed@VM:~/PKI$
[01/02/22]seed@VM:~/PKI$
[01/02/22]seed@VM:~/PKI$
[01/02/22]seed@VM:~/PKI$
[01/02/22]seed@VM:~/PKI$
[01/02/22]seed@VM:~/PKI$
[01/02/22]seed@VM:~/PKI$
[01/02/22]seed@VM:~/PKI$ openssl ca -in youtube.csr -out youtube.crt -cert ca.crt -config openssl.cnf
Using configuration from openssl.cnf
Error opening CA private key ./demoCA/private/cakey.pem
3071043264:error:02001002:system library:fopen:No such file or directory:bss_file.c:398:fopen('./demoCA/private/cakey.pem','r')
3071043264:error:20074002:BIOS routines:FILE_CTRL:system lib:bss_file.c:400:
unable to load CA private key
```

```
Terminal
unable to load CA private key
[01/02/22]seed@VM:~/PKI$ openssl ca -in youtube.csr -out youtube.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: Jan  2 11:36:49 2022 GMT
        Not After : Jan  2 11:36:49 2023 GMT
    Subject:
        countryName               = SA
        stateOrProvinceName       = Riyadh
        organizationName          = STC
        organizationalUnitName    = STCKSA
        commonName                 = youtube.com
        emailAddress               = elham@gmail.com
    X509v3 extensions:
        X509v3 Basic Constraints:
```

```
Terminal
X509v3 Basic Constraints:
    CA:FALSE
Netscape Comment:
    OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
    63:75:19:6D:FF:8C:EA:DC:EF:21:6B:D2:27:
03:6A:CB:C1:B9:95:0C
X509v3 Authority Key Identifier:
    keyid:0C:83:EF:F7:91:DC:3A:21:2D:E1:0B:
15:04:39:44:E6:17:A5:E3:03
Certificate is to be certified until Jan  2 11:36:49 20
23 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
[01/02/22]seed@VM:~/PKI$ cp server.key youtube.pem
[01/02/22]seed@VM:~/PKI$ cat youtube.crt >> youtube.pem
```



```
Certificate is to be certified until Jan  2 11:36:49 20
23 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
```

```
[01/02/22]seed@VM:~/PKI$ cp server.key youtube.pem
```

```
[01/02/22]seed@VM:~/PKI$ cat youtube.crt >> youtube.pem
```

```
[01/02/22]seed@VM:~/PKI$ cp youtube.crt cert2.pem
```

```
[01/02/22]seed@VM:~/PKI$ sudo mv "/home/seed/PKI/cert2.
pem" "/etc/apache2/ssl/"
```

```
[01/02/22]seed@VM:~/PKI$
```

Terminal

↑↓ En 🔊 6:44 AM ⚙

```
<IfModule mod_ssl.c>

<VirtualHost *:443>
    ServerName SEEDPKILab2021.com
    DocumentRoot /var/www/seedpki
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /etc/apache2/ssl/cert.pem
    SSLCertificateKeyFile /etc/apache2/ssl/key.pem
</VirtualHost>

<VirtualHost *:443>
    ServerName youtube.com
    DocumentRoot /var/www/seedpki
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /etc/apache2/ssl/cert2.pem
    SSLCertificateKeyFile /etc/apache2/ssl/key.pem
</VirtualHost>

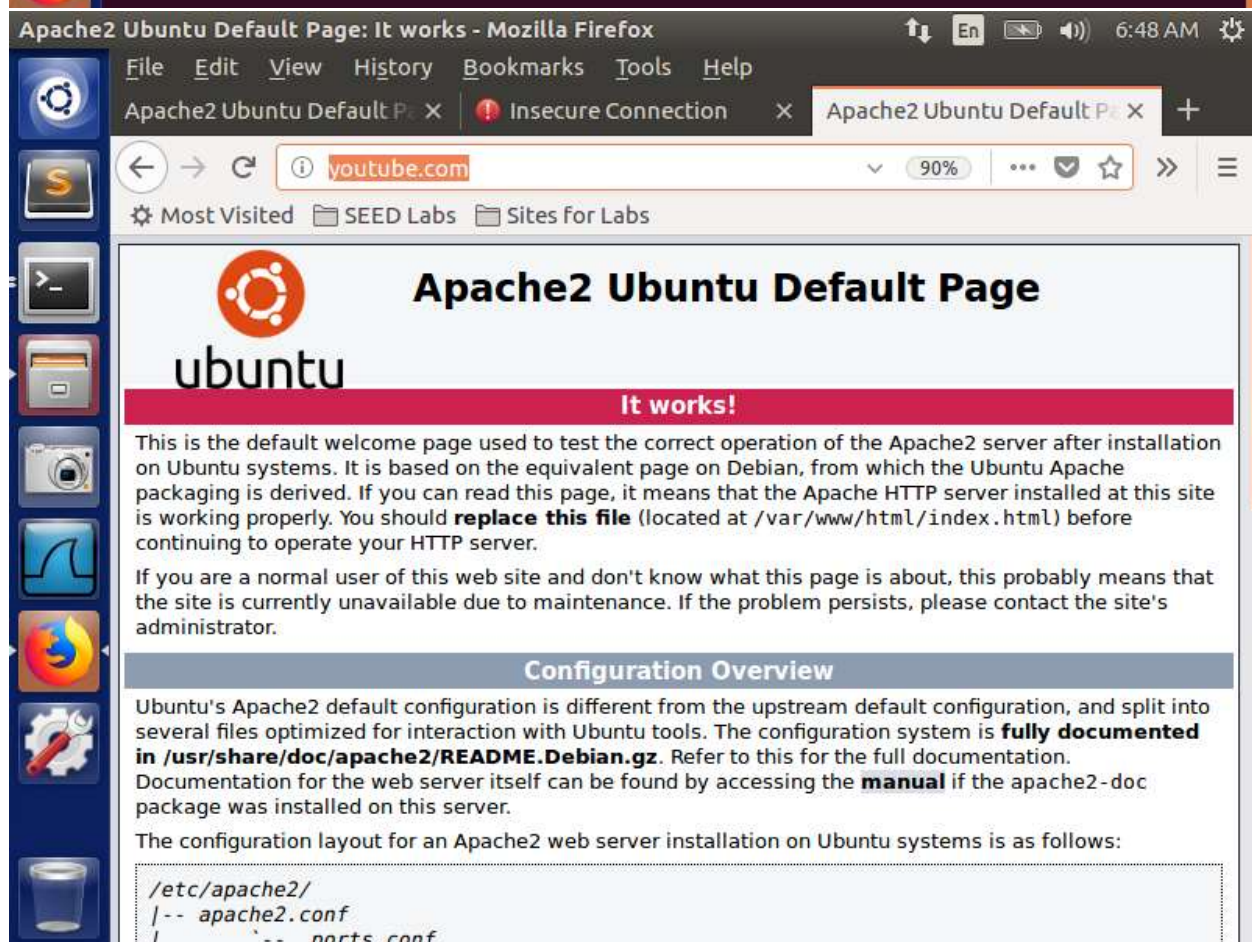
:wq!
```

```
Terminal
[01/02/22]seed@VM:~$ cd /etc/apache2/ssl/
[01/02/22]seed@VM:.../ssl$ ls
cert2.pem  cert.pem  key.pem
[01/02/22]seed@VM:.../ssl$ sd ..
The program 'sd' is currently not installed. You can in
stall it by typing:
sudo apt install sd
[01/02/22]seed@VM:.../ssl$ cd ..
[01/02/22]seed@VM:.../apache2$ cd sites-available/
[01/02/22]seed@VM:.../sites-available$ ls
000-default.conf  default-ssl.conf
[01/02/22]seed@VM:.../sites-available$ sudo vi default-
ssl.conf
[01/02/22]seed@VM:.../sites-available$
```

```
Terminal
# The following lines are desirable for IPv6 capable ho
sts
::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.csrfattacklab.com
127.0.0.1    www.repackagingattacklab.com
127.0.0.1    www.seedlabclickjacking.com
127.0.0.1    SEEDPKILab2021.com
127.0.0.1    instagram.com
127.0.0.1    youtube.com
:wq!
```



```
Terminal
[01/02/22]seed@VM:~$ sudo vi /etc/hosts
[01/02/22]seed@VM:~$ cd PKI/
[01/02/22]seed@VM:~/PKI$ sudo service apache2 restart
Enter passphrase for SSL/TLS keys for youtube.com:443 (
RSA): ****
[01/02/22]seed@VM:~/PKI$
```




Apache2 Ubuntu Default Page: It works - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Apache2 Ubuntu De X Insecure Connec X Apache2 Ubuntu De X Apache2 Ubuntu De X

← → ↻ <https://youtube.com> 90% ... ☆ >> ≡

⚙ Most Visited 📁 SEED Labs 📁 Sites for Labs



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|  
|-- ports.conf
```