# Lab 6

CSE-644 INTERNET SECURITY

DR. SYED SHAZLI

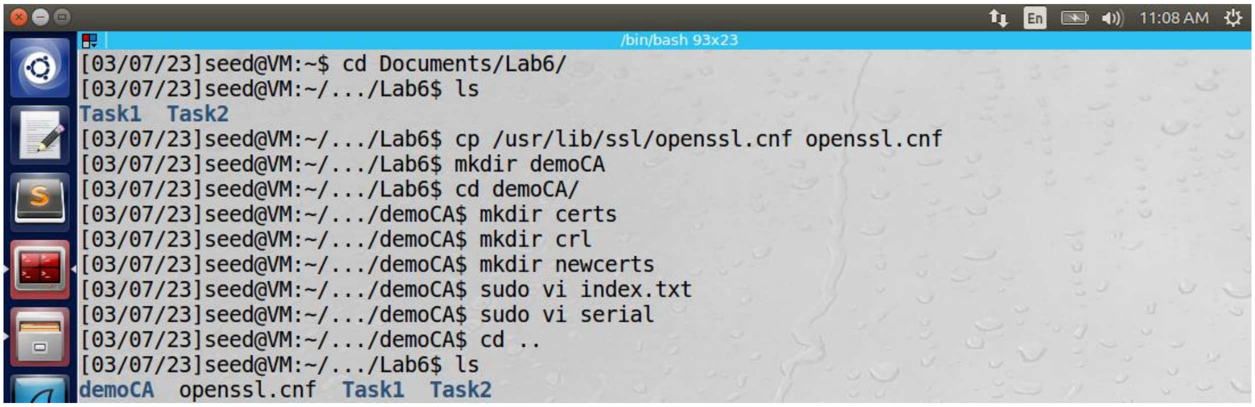
3/8/2023

Anthony Redamonti
SYRACUSE UNIVERSITY

## Task 1: Becoming a Certificate Authority (CA)

### Part 1: The Configuration File

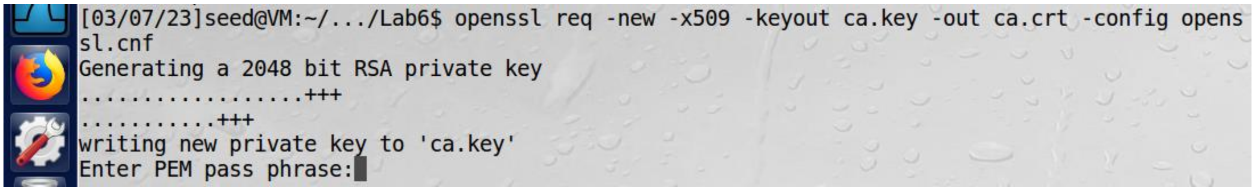
The commands below were used to create a copy of the configuration file “openssl.cnf” along with several sub-directories in the demoCA directory.



```
[03/07/23]seed@VM:~$ cd Documents/Lab6/
[03/07/23]seed@VM:~/.../Lab6$ ls
Task1  Task2
[03/07/23]seed@VM:~/.../Lab6$ cp /usr/lib/ssl/openssl.cnf openssl.cnf
[03/07/23]seed@VM:~/.../Lab6$ mkdir demoCA
[03/07/23]seed@VM:~/.../Lab6$ cd demoCA/
[03/07/23]seed@VM:~/.../demoCA$ mkdir certs
[03/07/23]seed@VM:~/.../demoCA$ mkdir crl
[03/07/23]seed@VM:~/.../demoCA$ mkdir newcerts
[03/07/23]seed@VM:~/.../demoCA$ sudo vi index.txt
[03/07/23]seed@VM:~/.../demoCA$ sudo vi serial
[03/07/23]seed@VM:~/.../demoCA$ cd ..
[03/07/23]seed@VM:~/.../Lab6$ ls
demoCA  openssl.cnf  Task1  Task2
```

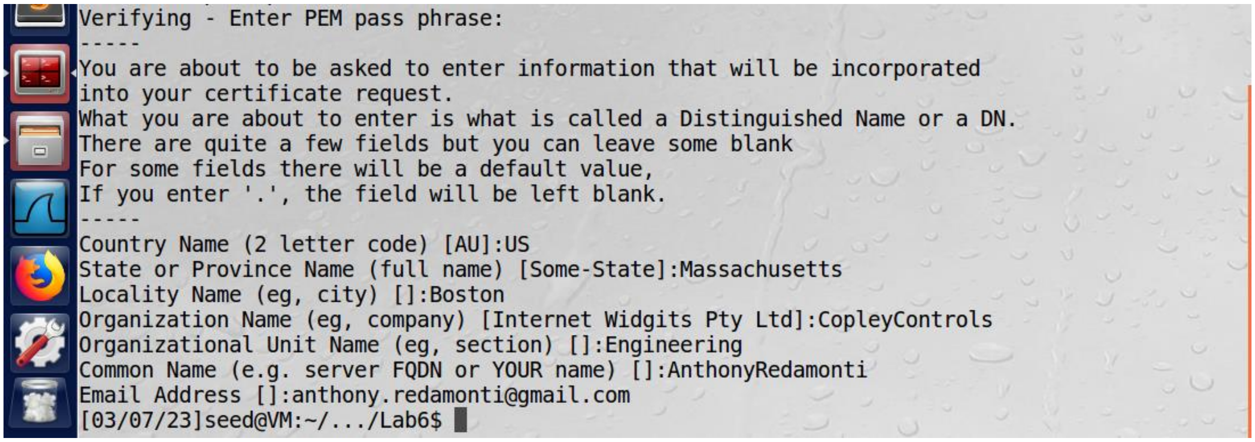
### Part 2: Certificate Authority

The command below was used to generate a self-signed certificate for the certificate authority. After generating this certificate, the CA will act as the root CA.



```
[03/07/23]seed@VM:~/.../Lab6$ openssl req -new -x509 -keyout ca.key -out ca.crt -config opens
sl.cnf
Generating a 2048 bit RSA private key
..................+++
...........+++
writing new private key to 'ca.key'
Enter PEM pass phrase:
```

The information below was entered for the root CA. The common name was “AnthonyRedamonti”.



```
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Massachusetts
Locality Name (eg, city) []:Boston
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CopleyControls
Organizational Unit Name (eg, section) []:Engineering
Common Name (e.g. server FQDN or YOUR name) []:AnthonyRedamonti
Email Address []:anthony.redamonti@gmail.com
[03/07/23]seed@VM:~/.../Lab6$
```

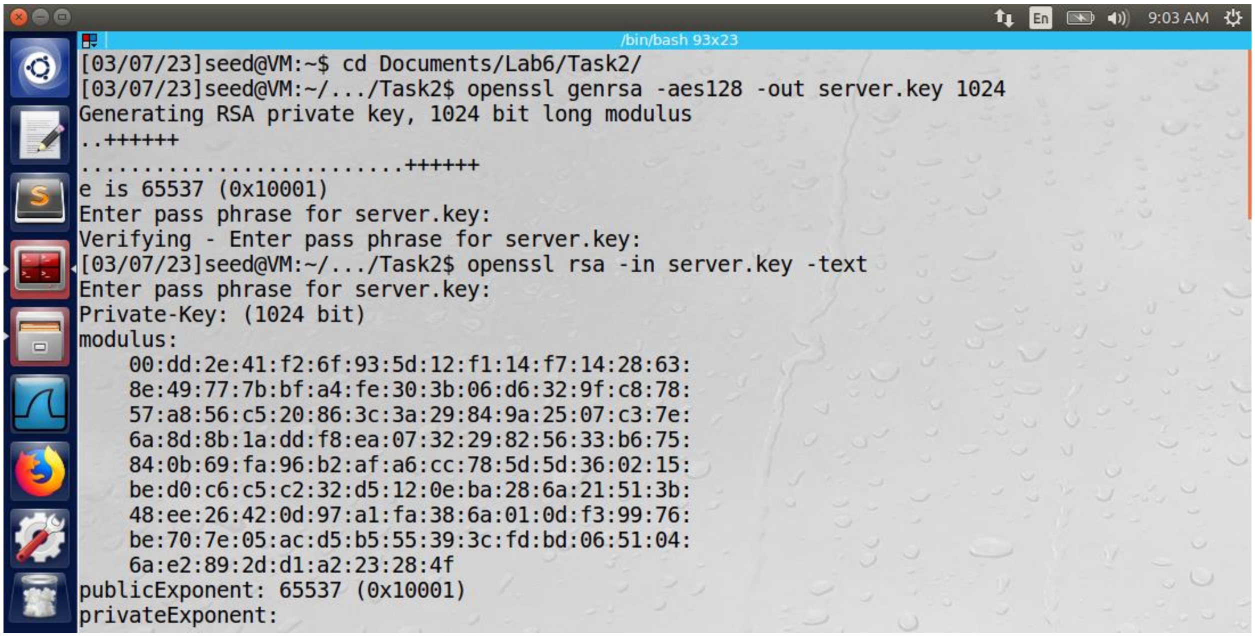
Observation: After executing the commands, the root CA’s private key (ca.key) and certificate (ca.crt) were generated.

Explanation: The root CA will be used in future sections to generate certificates for other servers.

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

### Part 1: Generate public/private key pair

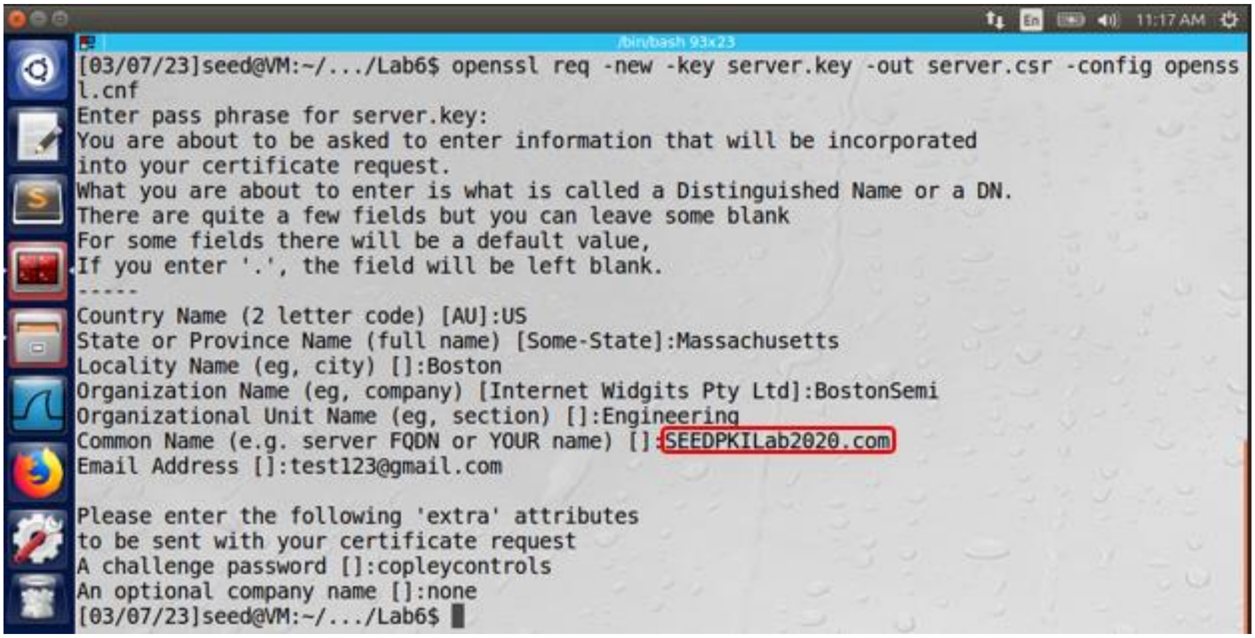
The following command was used to generate the public/private key pair for the SEEDPKILab2020.com server.



```
[03/07/23]seed@VM:~$ cd Documents/Lab6/Task2/
[03/07/23]seed@VM:~/.../Task2$ openssl genrsa -aes128 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
..++++++
..........................++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
[03/07/23]seed@VM:~/.../Task2$ openssl rsa -in server.key -text
Enter pass phrase for server.key:
Private-Key: (1024 bit)
modulus:
    00:dd:2e:41:f2:6f:93:5d:12:f1:14:f7:14:28:63:
    8e:49:77:7b:bf:a4:fe:30:3b:06:d6:32:9f:c8:78:
    57:a8:56:c5:20:86:3c:3a:29:84:9a:25:07:c3:7e:
    6a:8d:8b:1a:dd:f8:ea:07:32:29:82:56:33:b6:75:
    84:0b:69:fa:96:b2:af:a6:cc:78:5d:5d:36:02:15:
    be:d0:c6:c5:c2:32:d5:12:0e:ba:28:6a:21:51:3b:
    48:ee:26:42:0d:97:a1:fa:38:6a:01:0d:f3:99:76:
    be:70:7e:05:ac:d5:b5:55:39:3c:fd:bd:06:51:04:
    6a:e2:89:2d:d1:a2:23:28:4f
publicExponent: 65537 (0x10001)
privateExponent:
```

### Part 2: Generate a Certificate Signing Request (CSR)

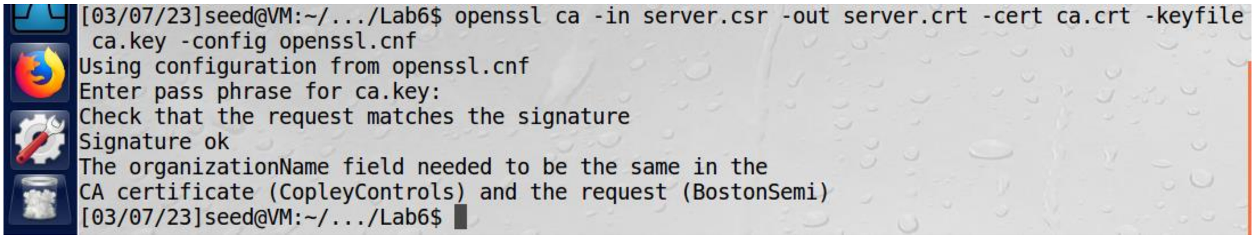
The following command was used to generate a certificate signing request (CSR) for the SEEDPKILab2020.com server. Note the Common Name was “SEEDPKILab2020.com”.



```
[03/07/23]seed@VM:~/.../Lab6$ openssl req -new -key server.key -out server.csr -config openss
l.cnf
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Massachusetts
Locality Name (eg, city) []:Boston
Organization Name (eg, company) [Internet Widgits Pty Ltd]:BostonSemi
Organizational Unit Name (eg, section) []:Engineering
Common Name (e.g. server FQDN or YOUR name) []:SEEDPKILab2020.com
Email Address []:test123@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:copleycontrols
An optional company name []:none
[03/07/23]seed@VM:~/.../Lab6$ 
```

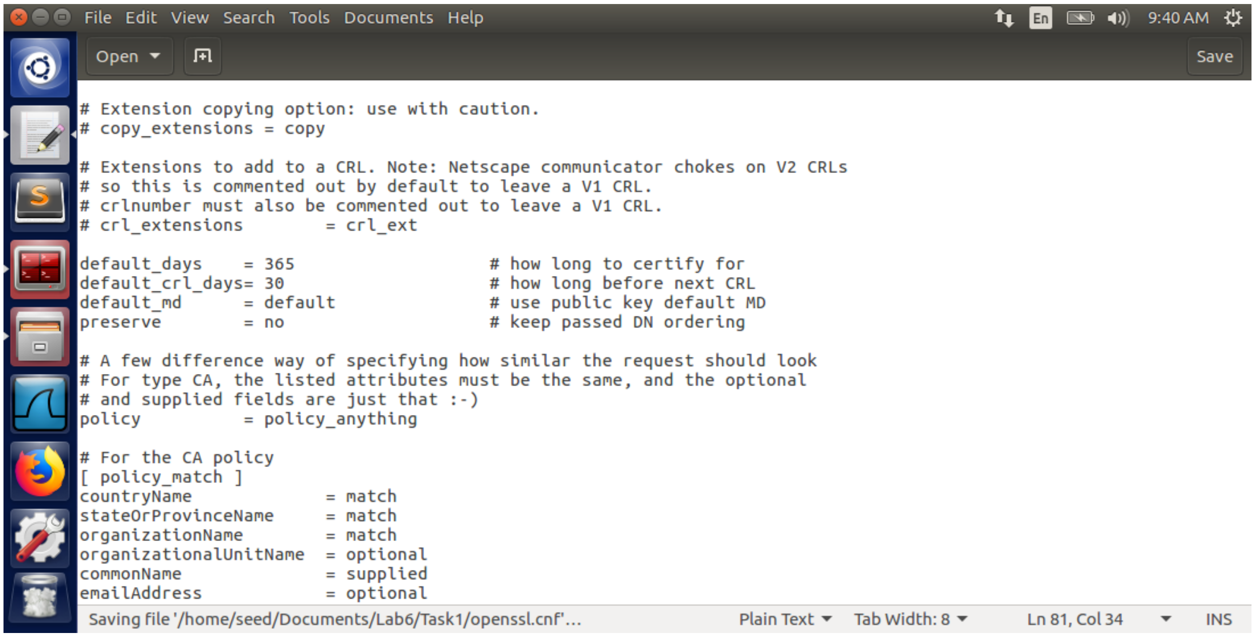
**Part 3: Generating Certificates**

The following command was used to generate a certificate for the SEEDPKILab2020.com server. Note the error returned “The organizationName field needed to be the same in the CA certificate (CopleyControls) and the request (BostonSemi).”



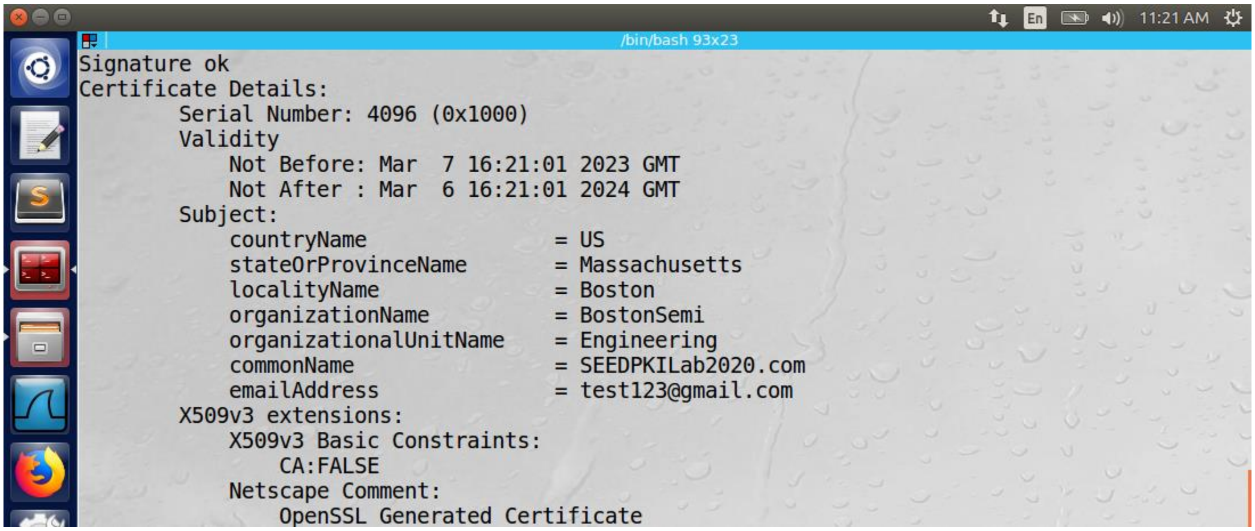
```
[03/07/23]seed@VM:~/.../Lab6$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile
 ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The organizationName field needed to be the same in the
CA certificate (CopleyControls) and the request (BostonSemi)
[03/07/23]seed@VM:~/.../Lab6$
```

To ignore this error, the policy in the configuration file (openssl.cnf) was changed to “policy_anything”.


File Edit View Search Tools Documents Help
En
9:40 AM
Open
Save
Saving file '/home/seed/Documents/Lab6/Task1/openssl.cnf'...
Plain Text
Tab Width: 8
Ln 81, Col 34
INS

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

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

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

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

# For the CA policy
[ policy_match ]
countryName             = match
stateOrProvinceName     = match
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional
```

The previous command to generate the certificate was rerun and successfully completed.



```
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Mar  7 16:21:01 2023 GMT
            Not After : Mar  6 16:21:01 2024 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = Massachusetts
            localityName              = Boston
            organizationName          = BostonSemi
            organizationalUnitName    = Engineering
            commonName                = SEEDPKILab2020.com
            emailAddress              = test123@gmail.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
```

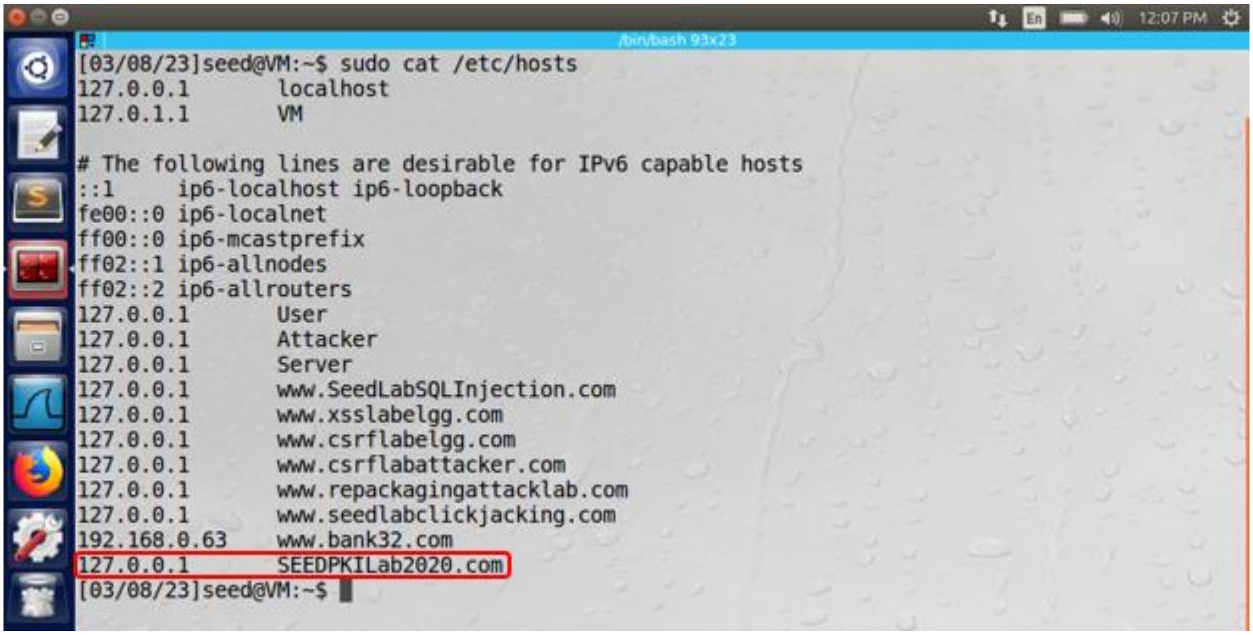
Observation: After executing the commands, the public/private key pair were generated for the SEEDPKILab2020.com server. The certificate signing request was generated and the root CA signed it and generated the certificate for SEEDPKILab2020.com.

Explanation: The SEEDPKILab2020.com server owned a certificate after all these commands were executed. The certificate was then ready for deployment.

## Task 3: Deploying Certificate in an HTTPS Web Server

**Part 1: Configuring DNS**

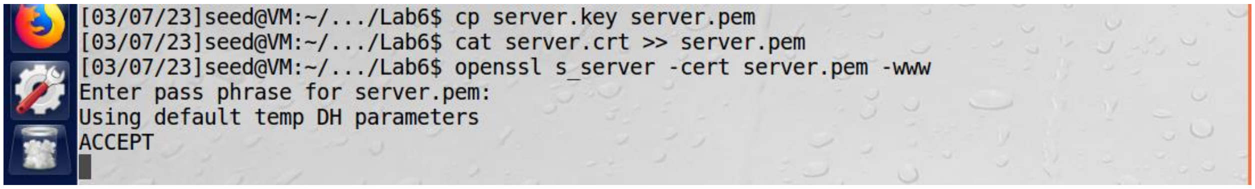
The following entry was added to the IPv6 capable hosts list in the /etc/hosts file. Notice how the IP address is shared between the SEEDPKILab2020.com domain and the localhost domain.



```
[03/08/23]seed@VM:~$ sudo cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       VM

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1       User
127.0.0.1       Attacker
127.0.0.1       Server
127.0.0.1       www.SeedLabSQLInjection.com
127.0.0.1       www.xsslabelgg.com
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
192.168.0.63    www.bank32.com
127.0.0.1       SEEDPKILab2020.com
[03/08/23]seed@VM:~$ 
```

**Part 2: Configuring the web server**

The following commands were used to launch the web server using the previously generated certificate.

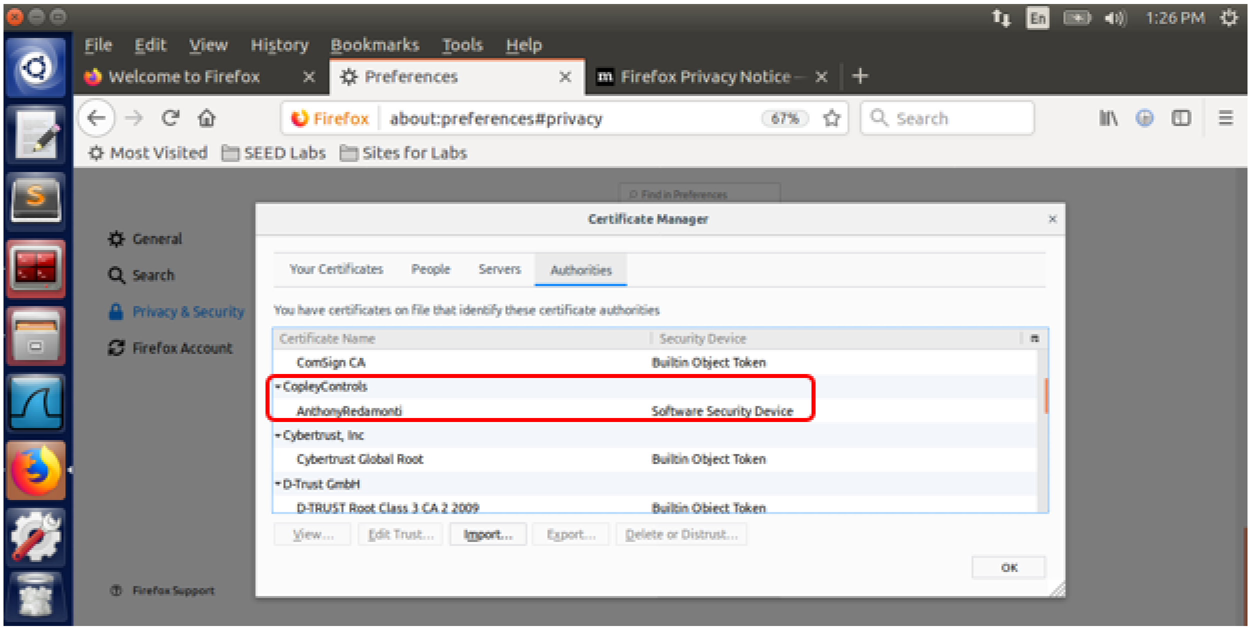


```
[03/07/23]seed@VM:~/.../Lab6$ cp server.key server.pem
[03/07/23]seed@VM:~/.../Lab6$ cat server.crt >> server.pem
[03/07/23]seed@VM:~/.../Lab6$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
```

The openssl tool launched the web server using the s_server command.

**Part 3: Getting the browser to accept our CA certificate**

The ca.crt (self-signed root certificate) was added to the trusted authorities section of the Firefox browser settings shown below.



Certificate Manager

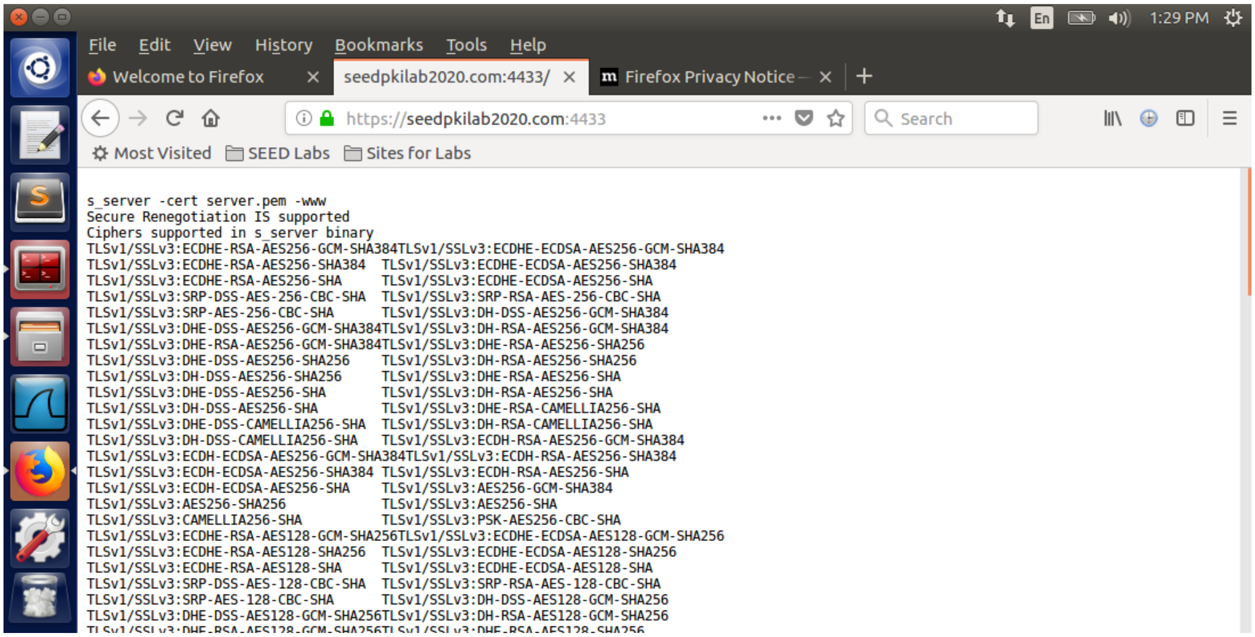
You have certificates on file that identify these certificate authorities

| Certificate Name | Security Device |
|---|---|
| ComSign CA | Builtin Object Token |
| CopleyControls | |
| AnthonyRedamonti | Software Security Device |
| Cybertrust, Inc | |
| Cybertrust Global Root | Builtin Object Token |
| D-Trust GmbH | |
| D-TRUST Root Class 3 CA 2 2009 | Builtin Object Token |

The “Trust this CA to identify web sites” checkbox was checked.

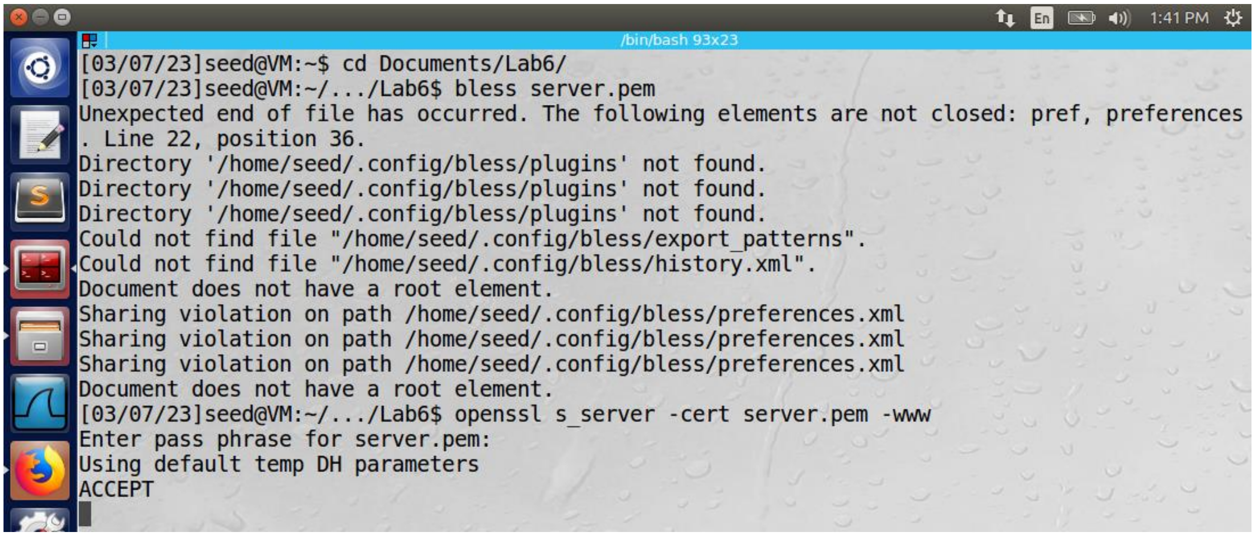
**Part 4: Testing the HTTPS website**

After adding the CA root certificate to the browser’s list of trusted authorities, the SEEDPKILab2020.com server was reachable from the Firefox browser. Note: the openssl tool was still hosting the web server during this test.



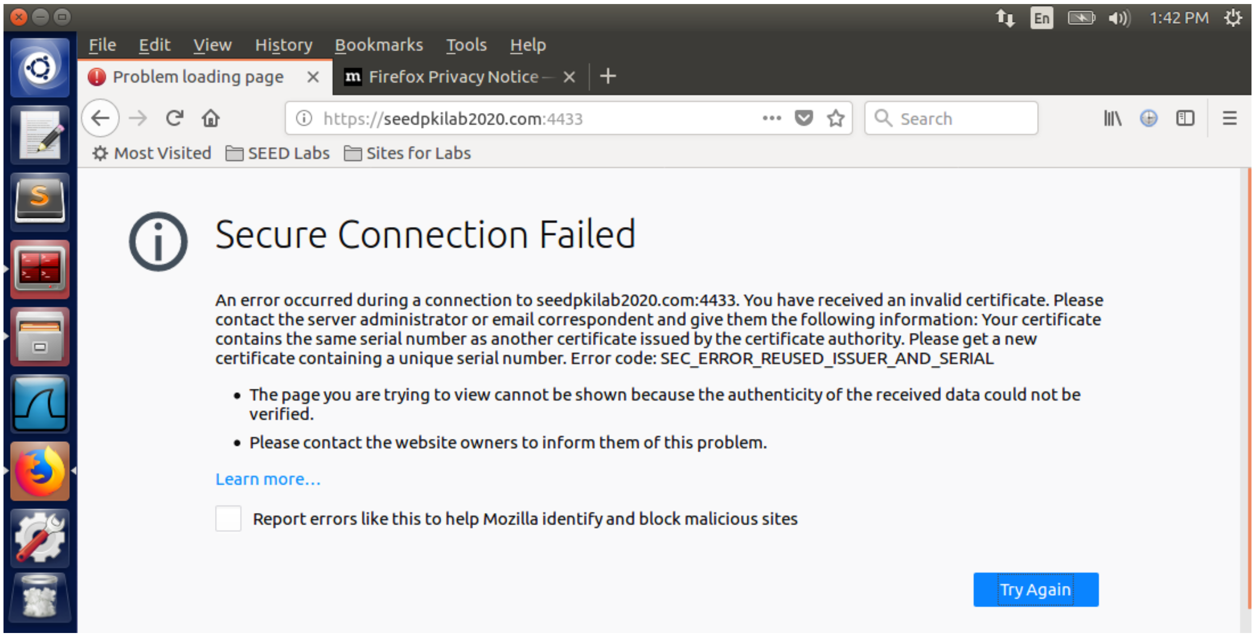
```
s_server -cert server.pem -www
Secure Renegotiation IS supported
Ciphers supported in s_server binary
TLSv1/SSLv3:ECDHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDHE-ECDSA-AES256-GCM-SHA384
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA384  TLSv1/SSLv3:ECDHE-ECDSA-AES256-SHA384
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES256-SHA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

The bless hex editor tool was then used to edit one byte of the server.pem file, and the openssl tool relaunched the web server.



```
[03/07/23]seed@VM:~$ cd Documents/Lab6/
[03/07/23]seed@VM:~/.../Lab6$ bless server.pem
Unexpected end of file has occurred. The following elements are not closed: pref, preferences
. Line 22, position 36.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Directory '/home/seed/.config/bless/plugins' not found.
Could not find file "/home/seed/.config/bless/export_patterns".
Could not find file "/home/seed/.config/bless/history.xml".
Document does not have a root element.
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
Sharing violation on path /home/seed/.config/bless/preferences.xml
Document does not have a root element.
[03/07/23]seed@VM:~/.../Lab6$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
```

The connection to the SEEDPKILab2020.com server failed. The certificate was identified as invalid.



Secure Connection Failed

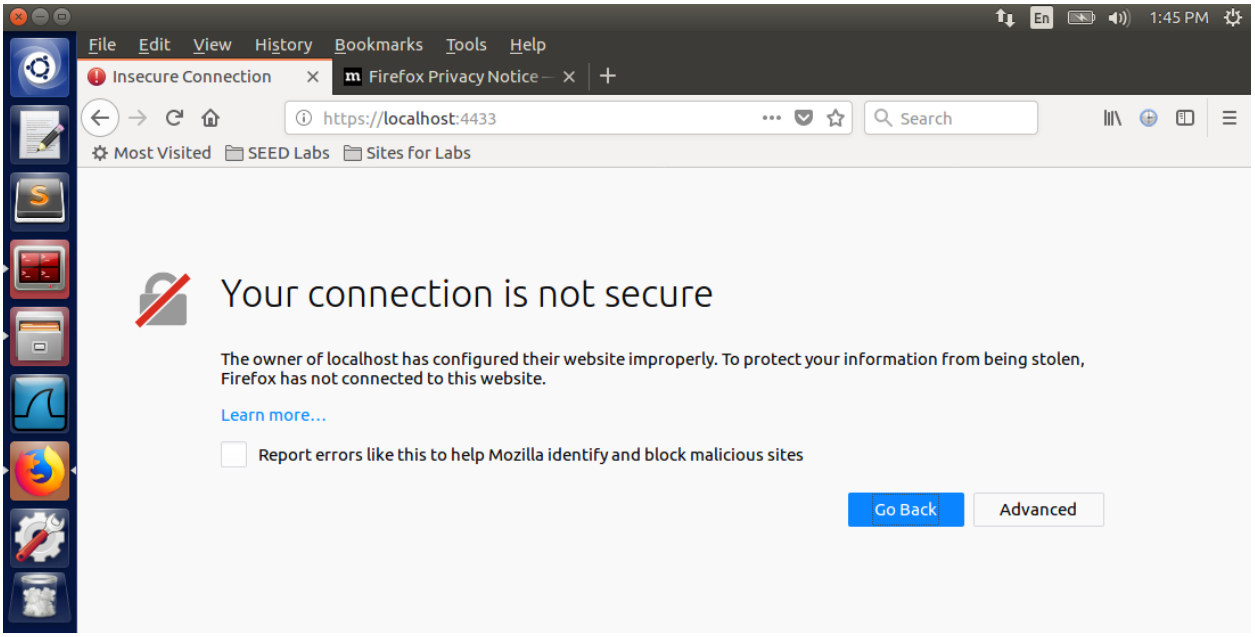
An error occurred during a connection to seedpkilab2020.com:4433. You have received an invalid certificate. Please contact the server administrator or email correspondent and give them the following information: Your certificate contains the same serial number as another certificate issued by the certificate authority. Please get a new certificate containing a unique serial number. Error code: SEC_ERROR_REUSED_ISSUER_AND_SERIAL

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more…

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

Next, the certificate was restored to its original condition and a localhost connection was attempted, since the localhost and SEEDPKILab2020.com server share the same IP address (127.0.0.1).

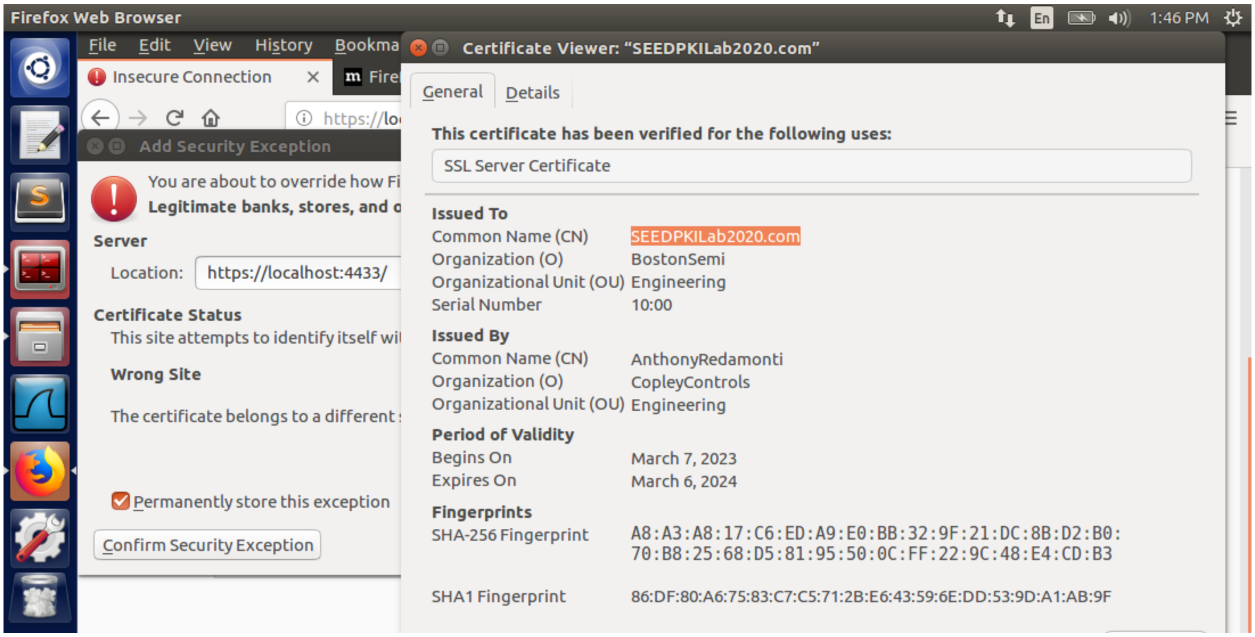


Your connection is not secure

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

Learn more…

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


Firefox Web Browser
1:46 PM
File Edit View History Bookma
Insecure Connection
Fire
https://lo
Add Security Exception
Certificate Viewer: "SEEDPKILab2020.com"
General
Details

You are about to override how Fi

Legitimate banks, stores, and o

**Server**

Location: https://localhost:4433/

**Certificate Status**

This site attempts to identify itself wi

**Wrong Site**

The certificate belongs to a different

☑ Permanently store this exception

Confirm Security Exception

**This certificate has been verified for the following uses:**

SSL Server Certificate

| | |
|---|---|
| **Issued To** | |
| Common Name (CN) | SEEDPKILab2020.com |
| Organization (O) | BostonSemi |
| Organizational Unit (OU) | Engineering |
| Serial Number | 10:00 |
| **Issued By** | |
| Common Name (CN) | AnthonyRedamonti |
| Organization (O) | CopleyControls |
| Organizational Unit (OU) | Engineering |
| **Period of Validity** | |
| Begins On | March 7, 2023 |
| Expires On | March 6, 2024 |
| **Fingerprints** | |
| SHA-256 Fingerprint | A8:A3:A8:17:C6:ED:A9:E0:BB:32:9F:21:DC:8B:D2:B0:<br>70:B8:25:68:D5:81:95:50:0C:FF:22:9C:48:E4:CD:B3 |
| SHA1 Fingerprint | 86:DF:80:A6:75:83:C7:C5:71:2B:E6:43:59:6E:DD:53:9D:A1:AB:9F |

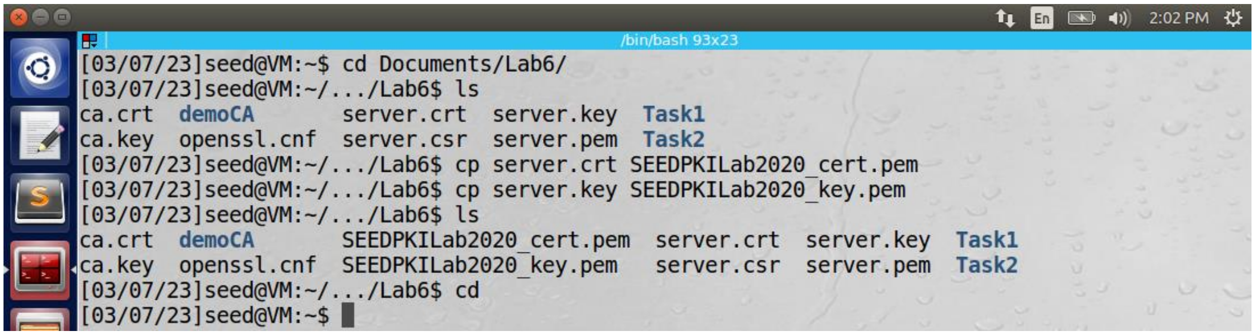
The connection to localhost:4433 failed because the certificate was identified as belonging to a different server (Common Name: SEEDPKILab2020.com). If the "Confirm Security Exception" button is pressed, the security exception is added to the browser, and the localhost::4433 domain can use the certificate and connect to the SEEDPKILab2020.com web server.

Observation: The openssl tool was used to launch the web server SEEDPKILab2020.com. If the certificate has been modified, it will be considered invalid. If the domain name conflicts with the IP address in the local DNS, the connection will not be considered secure.

Explanation: The security measures ensure that an attacker can't modify certificates belonging to other servers and that the domain name/ip address pair is valid.

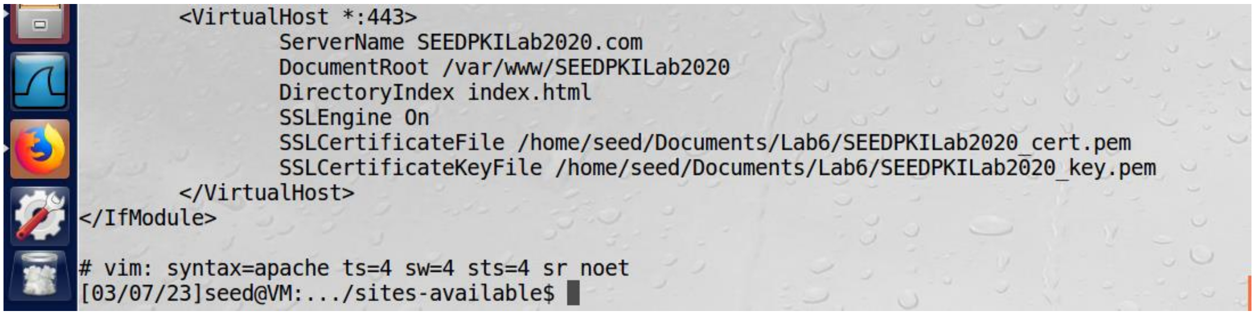
## Task 4: Deploying Certificate in an Apache-Based HTTPS Website

The certificate and key from the previous task were copied and renamed as SEEDPKILab2020_cert.pem and SEEDPKILab2020_key.pem using the commands below.



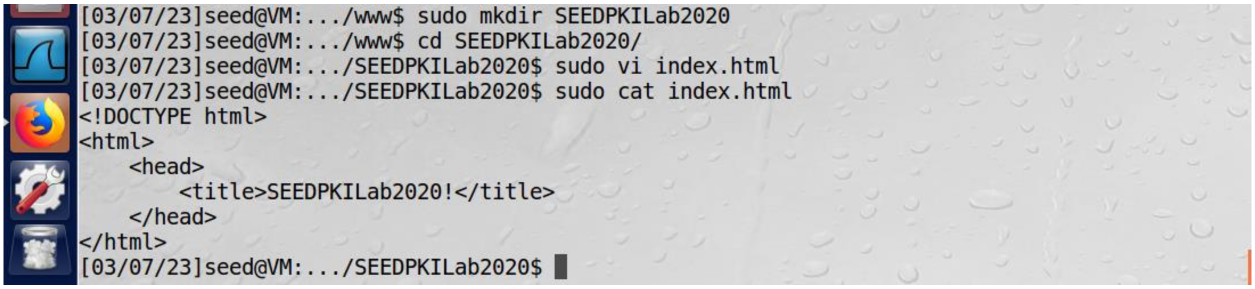
```
[03/07/23]seed@VM:~$ cd Documents/Lab6/
[03/07/23]seed@VM:~/.../Lab6$ ls
ca.crt  demoCA       server.crt  server.key  Task1
ca.key  openssl.cnf  server.csr  server.pem  Task2
[03/07/23]seed@VM:~/.../Lab6$ cp server.crt SEEDPKILab2020_cert.pem
[03/07/23]seed@VM:~/.../Lab6$ cp server.key SEEDPKILab2020_key.pem
[03/07/23]seed@VM:~/.../Lab6$ ls
ca.crt  demoCA       SEEDPKILab2020_cert.pem  server.crt  server.key  Task1
ca.key  openssl.cnf  SEEDPKILab2020_key.pem   server.csr  server.pem  Task2
[03/07/23]seed@VM:~/.../Lab6$ cd
[03/07/23]seed@VM:~$ 
```

The following VirtualHost entry was added to the /etc/apache2/sites-available/default-ssl.conf file. Notice the file paths to the newly created pem files.



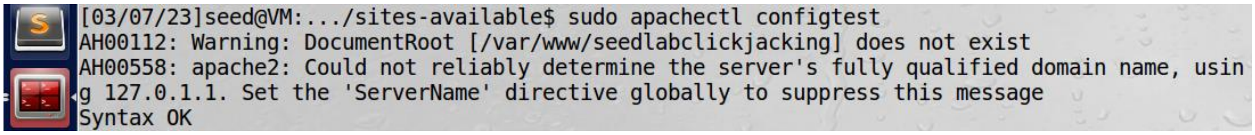
```
        <VirtualHost *:443>
                ServerName SEEDPKILab2020.com
                DocumentRoot /var/www/SEEDPKILab2020
                DirectoryIndex index.html
                SSLEngine On
                SSLCertificateFile /home/seed/Documents/Lab6/SEEDPKILab2020_cert.pem
                SSLCertificateKeyFile /home/seed/Documents/Lab6/SEEDPKILab2020_key.pem
        </VirtualHost>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
[03/07/23]seed@VM:.../sites-available$ 
```

Next, the SEEDPKILab2020 directory was created in /var/www/. Then the index.html file was created using the commands shown below.



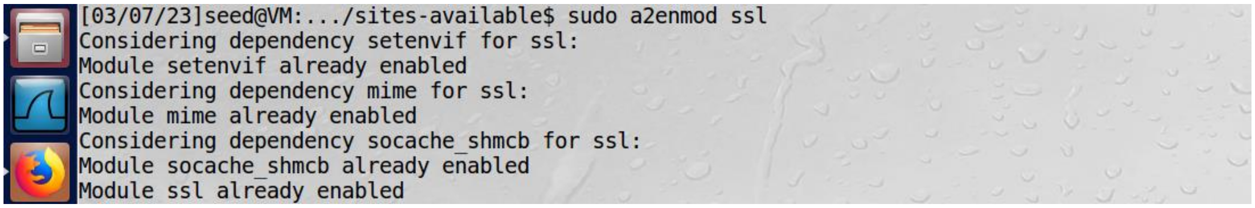
```
[03/07/23]seed@VM:.../www$ sudo mkdir SEEDPKILab2020
[03/07/23]seed@VM:.../www$ cd SEEDPKILab2020/
[03/07/23]seed@VM:.../SEEDPKILab2020$ sudo vi index.html
[03/07/23]seed@VM:.../SEEDPKILab2020$ sudo cat index.html
<!DOCTYPE html>
<html>
    <head>
        <title>SEEDPKILab2020!</title>
    </head>
</html>
[03/07/23]seed@VM:.../SEEDPKILab2020$ 
```

The apache2 configuration file was then tested for errors using the command below.



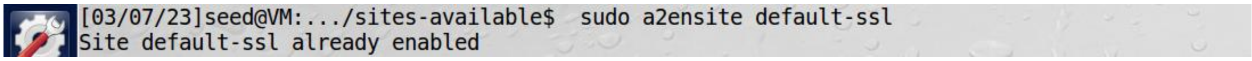
```
[03/07/23]seed@VM:.../sites-available$ sudo apachectl configtest
AH00112: Warning: DocumentRoot [/var/www/seedlabclickjacking] does not exist
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, usin
g 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
```

The SSL module was enabled using the command below.



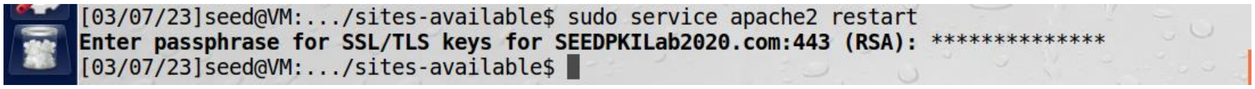
```
[03/07/23]seed@VM:.../sites-available$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
```

The SEEDPKILab2020 web server was enabled using the following command.



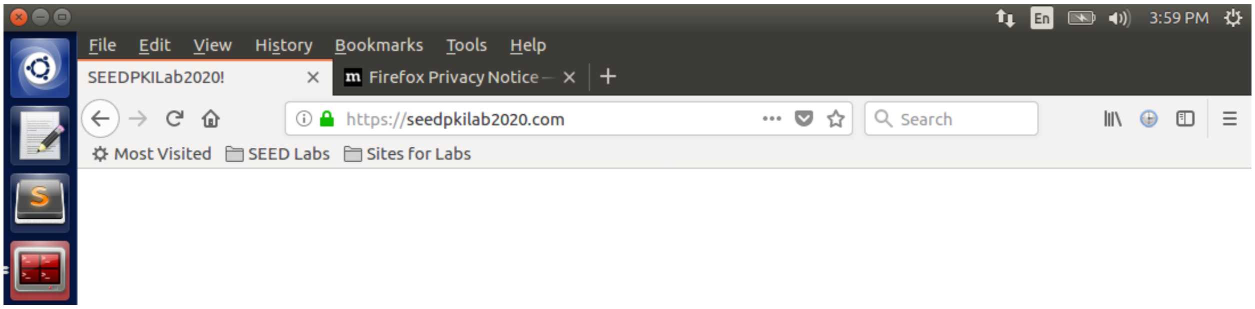
```
[03/07/23]seed@VM:.../sites-available$  sudo a2ensite default-ssl
Site default-ssl already enabled
```

Finally, the apache2 service was restarted using the command below.



```
[03/07/23]seed@VM:.../sites-available$ sudo service apache2 restart
Enter passphrase for SSL/TLS keys for SEEDPKILab2020.com:443 (RSA): **************
[03/07/23]seed@VM:.../sites-available$ 
```

Firefox was able to successfully connect to the SEEDPKILab2020 web server.

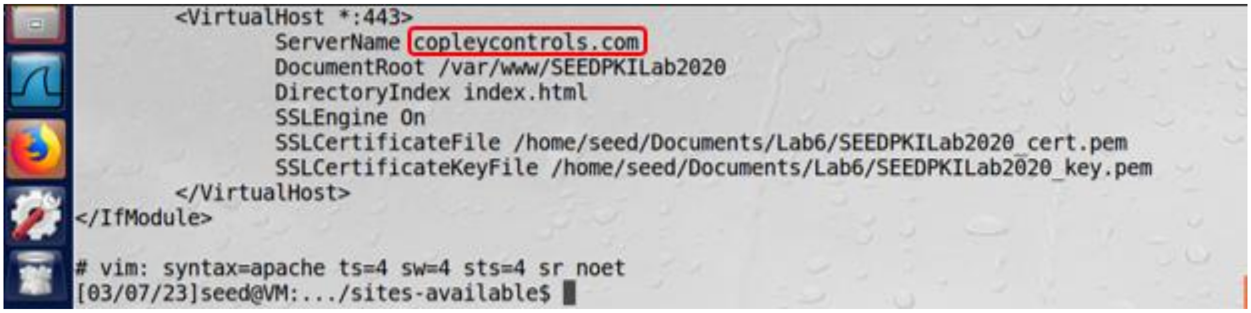


Observation: The apache2 service was used to launch the HTTPS web server. Firefox was able to connect to the SEEDPKILab2020.com server.

Explanation: Apache2 uses the sites-available/default-ssl.conf file to specify virtual hosts. The virtual host contains information relating to the web server, such as the server name, document root (location of HTML file), and the directory index (index.html). Also specified were the location of the PEM files containing the private key and certificate of the virtual host. The index.html file defines the content of the website. After restarting the apache2 service, the website was successfully launched.

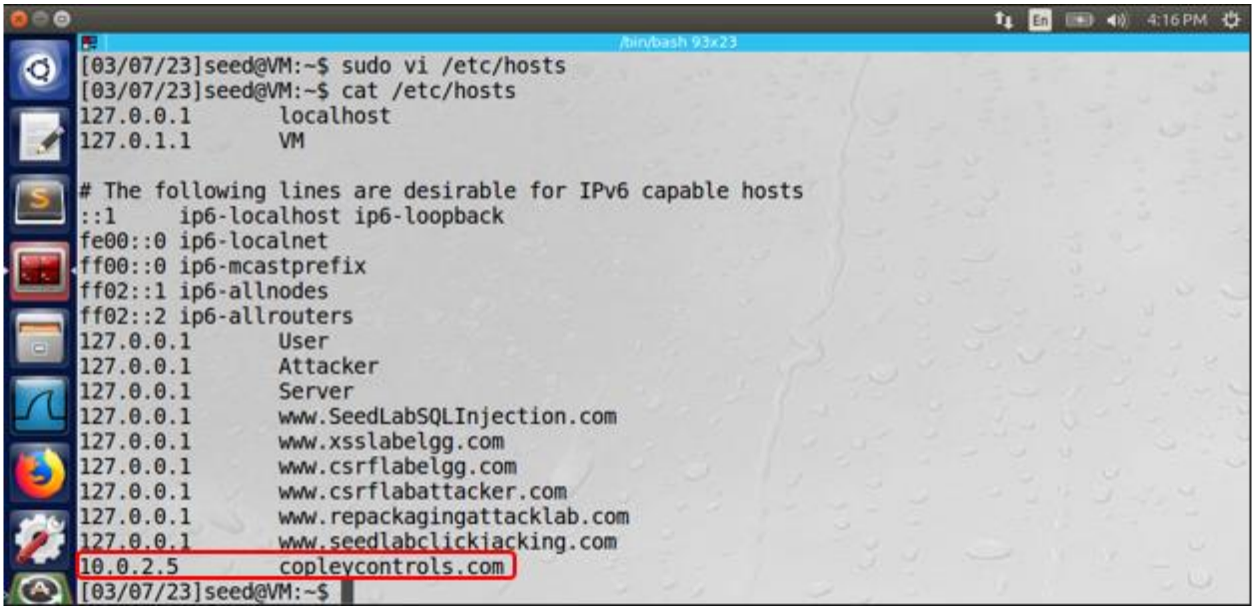
## Task 5: Launching a Man-In-The-Middle Attack

To launch the man-in-the-middle attack, the ServerName was edited in the /etc/apache2/sites-available/default-ssl.conf file.



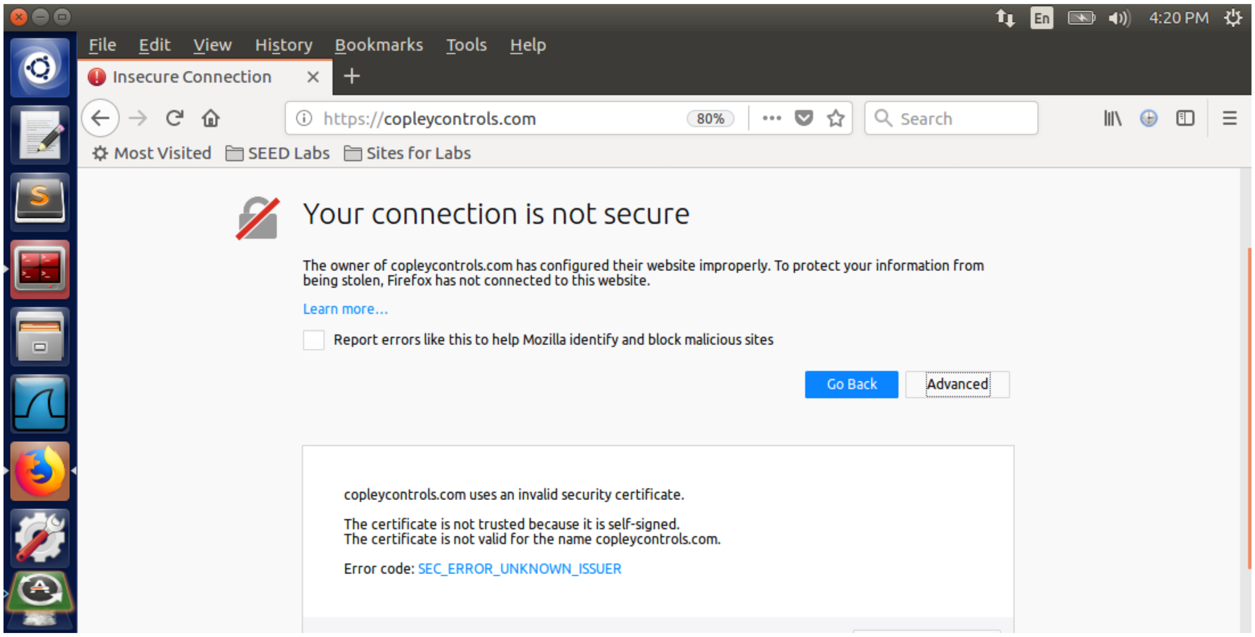
```
        <VirtualHost *:443>
                ServerName copleycontrols.com
                DocumentRoot /var/www/SEEDPKILab2020
                DirectoryIndex index.html
                SSLEngine On
                SSLCertificateFile /home/seed/Documents/Lab6/SEEDPKILab2020_cert.pem
                SSLCertificateKeyFile /home/seed/Documents/Lab6/SEEDPKILab2020_key.pem
        </VirtualHost>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
[03/07/23]seed@VM:.../sites-available$ 
```

The victim's /etc/hosts file was then edited so that the new malicious web server was included in the IPv6 capable hosts section. The IP address matched the IP address of the attacker VM so that any traffic to the copleycontrols.com domain would be redirected to the attacker by the victim's local DNS server.



```
[03/07/23]seed@VM:~$ sudo vi /etc/hosts
[03/07/23]seed@VM:~$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       VM

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1       User
127.0.0.1       Attacker
127.0.0.1       Server
127.0.0.1       www.SeedLabSQLInjection.com
127.0.0.1       www.xsslabelgg.com
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
10.0.2.5        copleycontrols.com
[03/07/23]seed@VM:~$ 
```

The apache2 service was then restarted using the “sudo service apache2 restart” command. The victim then attempted to access https://copleycontrols.com using the Firefox browser. The results are shown below.



Your connection is not secure

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

Learn more…

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

Go Back | Advanced

copleycontrols.com uses an invalid security certificate.

The certificate is not trusted because it is self-signed.
The certificate is not valid for the name copleycontrols.com.

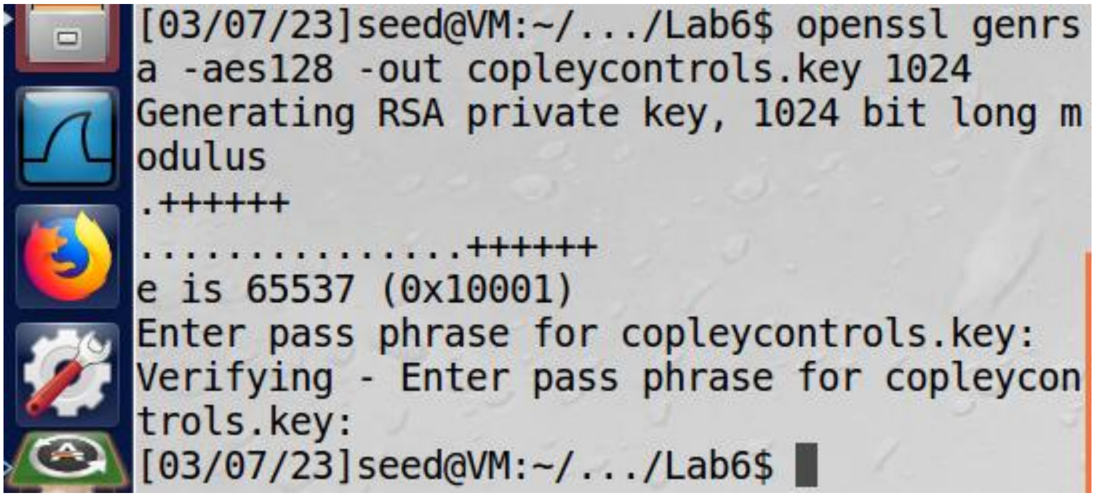
Error code: SEC_ERROR_UNKNOWN_ISSUER

Observation: The Firefox browser would not allow the victim to access the web server because "copleycontrols.com uses an invalid security certificate. The certificate is not trusted because it is self-signed. The certificate is not valid for the name copleycontrols.com."

Explanation: The certificate was not valid for the name copleycontrols.com because the certificate was written for the SEEDPKILab2020.com domain name (Common Domain). The copleycontrols.com domain did not match the common domain in the certificate in SEEDPKILab2020_cert.pem.

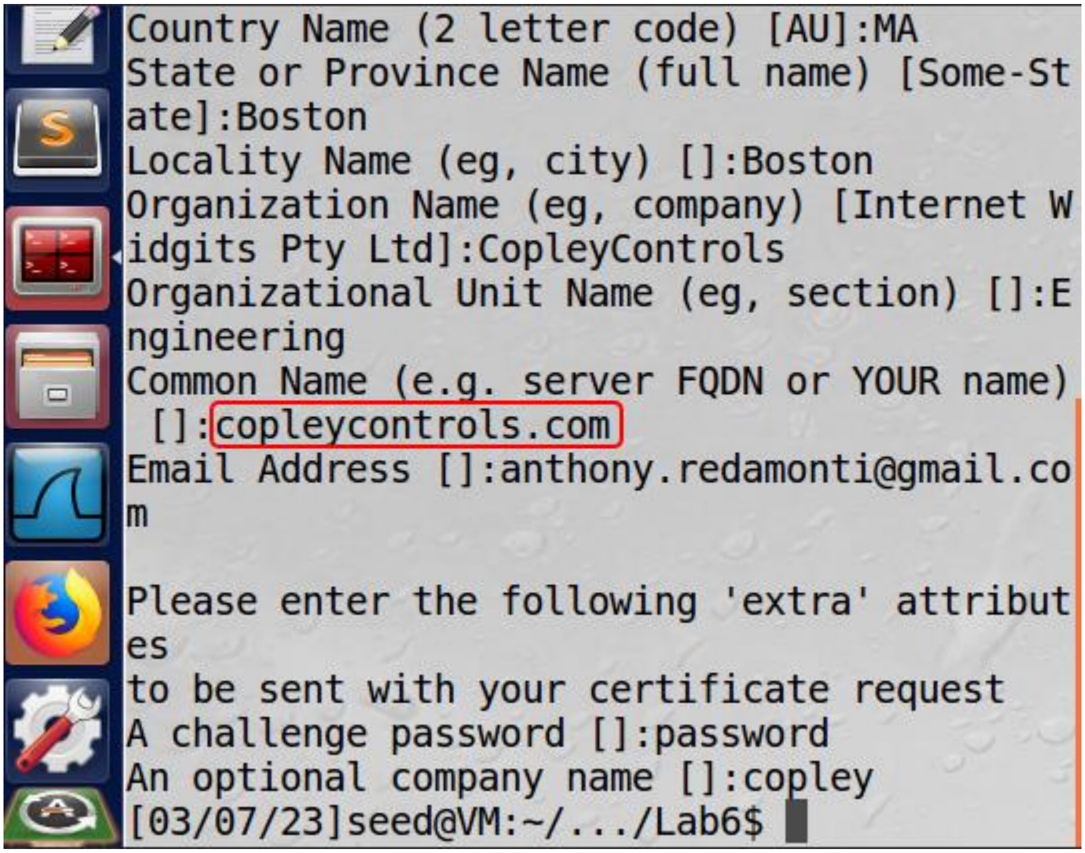
## Task 6: Launching a Man-In-The-Middle Attack with a Compromised CA

The private key of the root CA was compromised, so the attacker generated a new public/private key pair for the malicious webserver "copleycontrols.com" using the following command.



```
[03/07/23]seed@VM:~/.../Lab6$ openssl genrs
a -aes128 -out copleycontrols.key 1024
Generating RSA private key, 1024 bit long m
odulus
.++++++
...............++++++
e is 65537 (0x10001)
Enter pass phrase for copleycontrols.key:
Verifying - Enter pass phrase for copleycon
trols.key:
[03/07/23]seed@VM:~/.../Lab6$ 
```

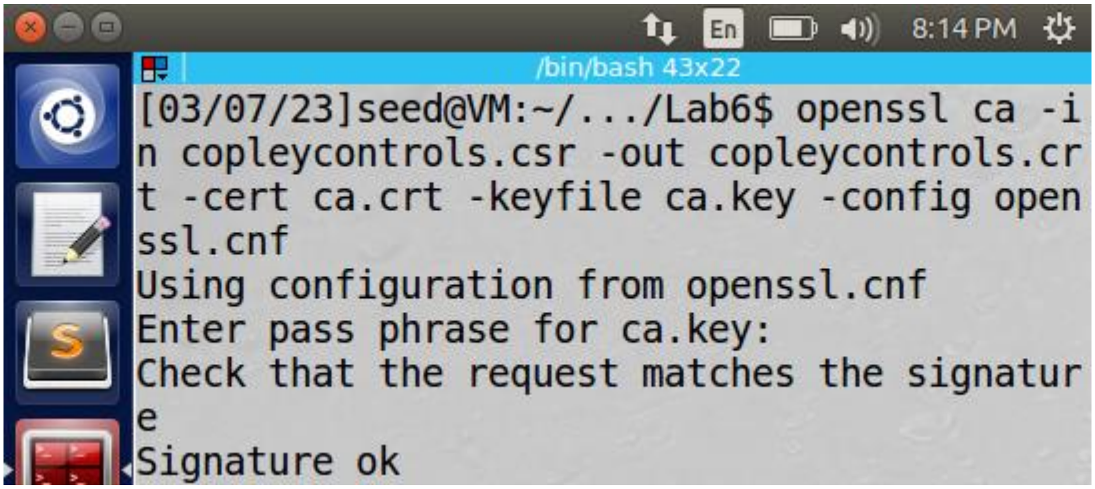
The new certificate signing request was created using "openssl req -new -key copleycontrols.key -out copleycontrols.csr -config openssl.cnf". The information for the request is below.



```
Country Name (2 letter code) [AU]:MA
State or Province Name (full name) [Some-St
ate]:Boston
Locality Name (eg, city) []:Boston
Organization Name (eg, company) [Internet W
idgits Pty Ltd]:CopleyControls
Organizational Unit Name (eg, section) []:E
ngineering
Common Name (e.g. server FQDN or YOUR name)
 []:copleycontrols.com
Email Address []:anthony.redamonti@gmail.co
m

Please enter the following 'extra' attribut
es
to be sent with your certificate request
A challenge password []:password
An optional company name []:copley
[03/07/23]seed@VM:~/.../Lab6$ 
```

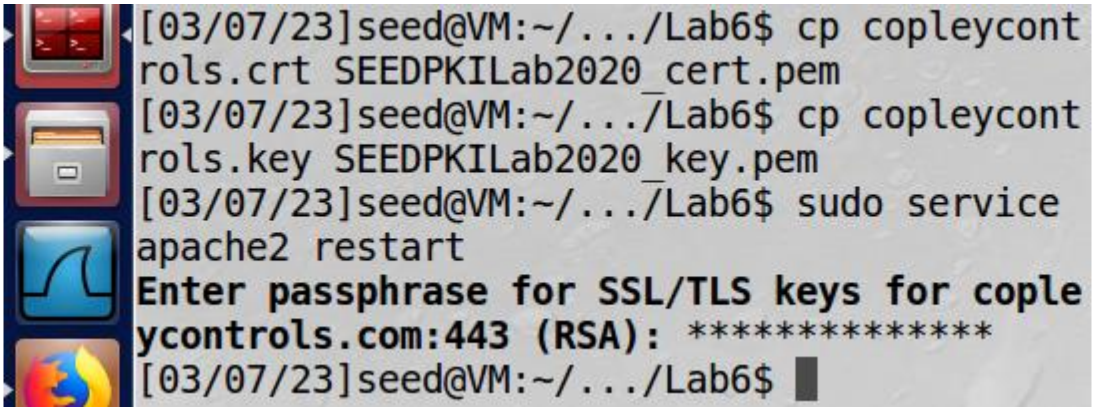
Note that the Common Name is copleycontrols.com.

The following command was then used to generate the new certificate for copleycontrols.com using the compromised private key of the certificate authority.



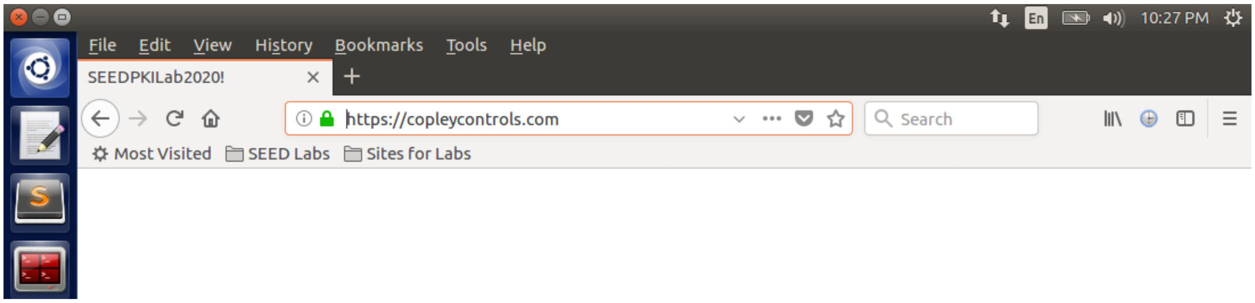
```
[03/07/23]seed@VM:~/.../Lab6$ openssl ca -i
n copleycontrols.csr -out copleycontrols.cr
t -cert ca.crt -keyfile ca.key -config open
ssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signatur
e
Signature ok
```

The original SEEDPKILab2020_cert.pem and SEEDPKILab2020_key.pem files were overwritten with the newly created copleycontrols.crt and copleycontrols.key files, and the apache2 service was restarted.



```
[03/07/23]seed@VM:~/.../Lab6$ cp copleycont
rols.crt SEEDPKILab2020_cert.pem
[03/07/23]seed@VM:~/.../Lab6$ cp copleycont
rols.key SEEDPKILab2020_key.pem
[03/07/23]seed@VM:~/.../Lab6$ sudo service
apache2 restart
Enter passphrase for SSL/TLS keys for cople
ycontrols.com:443 (RSA): **************
[03/07/23]seed@VM:~/.../Lab6$ 
```

The victim then attempted to access the https://copleycontrols.com website and was successfully redirected to the attacker's malicious web server.


10:27 PM
File Edit View History Bookmarks Tools Help
SEEDPKILab2020!
https://copleycontrols.com
Search
Most Visited
SEED Labs
Sites for Labs

Observation: The Firefox browser allowed the victim to access the web server because copleycontrols.com used a valid security certificate. The certificate was generated using the compromised private key of the root CA.

Explanation: The following error was no longer present: "*The certificate is not valid for the name copleycontrols.com.*" The certificate was valid because the certificate was written for the copleycontrols.com domain name (Common Domain). The copleycontrols.com domain matched the common domain in the certificate in SEEDPKILab2020_cert.pem. Note: in order to overcome the error, "*The certificate is not trusted because it is self-signed*," the victim's Firefox had to add the certificate of the root CA as a trusted authority (similar to task 3 part 3).