#### Lab Manual 5

# **Checkpoint-1:**

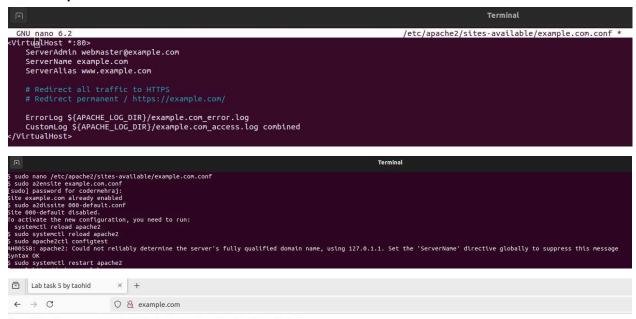
```
GNU nano 6.2

127.0.0.1 localhost
127.0.0.1 example.com
127.0.0.1 webserverlab.com
127.0.1.1 me0r

# 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
```

```
$ cd
$ sudo mkdir -p /var/www/example.com/html
$ sudo chown -R $USER:$USER /var/www/example.com/html
$ sudo chmod -R 755 /var/www/example.com
$ cd /var/www/example.com
$ pwd
/var/www/example.com
$ sudo nano html/index.html
$ sudo nano html/index.html
$ cd
```

### Checkpoint-2:



hello I am taohid, This is Lab task 5



```
[ ca ]
default ca
             = CA default
                                  # The default ca section
[ CA_default ]
dir
             = ./demoCA
                                  # Where everything is kept
             = $dir/certs
                                  # Where the issued certs are kept
certs
                                  # Where the issued crl are kept
crl dir
             = $dir/crl
                                  # database index file.
database
             = $dir/index.txt
                                  # Set to 'no' to allow creation of
#unique subject = no
                                  # several certs with same subject.
new_certs_dir = $dir/newcerts
                                  # default place for new certs.
certificate
             = $dir/cacert.pem
                                  # The CA certificate
serial
             = $dir/serial
                                  # The current serial number
crlnumber
             = $dir/crlnumber
                                  # the current crl number
                                  # must be commented out to leave a V1 CRL
                                  # The current CRL
crl
             = $dir/crl.pem
private key
             = $dir/private/cakey.pem# The private key
                                  # The extensions to add to the cert
x509 extensions = usr cert
# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name opt
             = ca default
                                  # Subject Name options
cert opt
             = ca_default
                                  # Certificate field options
```

```
Terminal
$ cd /usr/lib/ssl/
certs misc openssl.cnf private
$ mkdir taohid_lab5/
.
Desktop Documents Downloads Music Pictures Public snap taohid lab5 Templates Videos
$ cd taohid_lab5
$ ls
$ cp /usr/lib/ssl/openssl.cnf .
$ ls
openssl.cnf
 nano openssl.cnf
 nano openssl.cnf
 nano openssl.cnf
 mkdir demoCA
 cd demoCA
 mkdir certs
mkdir crl
$ mkdir newcerts
$ touch index.txt
  touch serial
```

```
$ ls
demoCA openssl.cnf
$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
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]:BD
State or Province Name (full name) [Some-State]:Barisal
Locality Name (eg, city) []:Barisal
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Taohid
Organizational Unit Name (eg, section) []:SUST
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:
$ openssl genrsa -des3 -out server.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
$ openssl req -new -key server.key -out server.csr -config openssl.cnf
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:BD
State or Province Name (full name) [Some-State]:Barisal
Locality Name (eg, city) []:Barisal
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Taohid
Organizational Unit Name (eg, section) []:SUST
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:hello
An optional company name []:
$
```

```
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]:BD
State or Province Name (full name) [Some-State]:Barisal
Locality Name (eg, city) []:Barisal
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Taohid
Organizational Unit Name (eg, section) []:SUST
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:hello
An optional company name []:
$ 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: Jul 7 15:26:34 2024 GMT
Not After: Jul 7 15:26:34 2025 GMT
         Subject:
             countryName
                                         = BD
             stateOrProvinceName
                                         = Barisal
             organizationName
                                         = Taohid
             organizationalUnitName
                                        = SUST
             commonName
                                         = example.com
         X509v3 extensions:
             X509v3 Basic Constraints:
                 CA: FALSE
             X509v3 Subject Key Identifier:
                 C5:5B:0B:D7:EB:01:E7:20:AF:F9:41:E5:CE:B0:35:F3:EB:9C:1C:80
             X509v3 Authority Key Identifier:
                 51:15:6D:FE:C0:0C:25:F7:85:A8:6B:EF:53:F8:75:F4:EB:41:C8:A4
Certificate is to be certified until Jul 7 15:26:34 2025 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
$ cp server.key server.pem
$ cat server.crt >> server.pem
```

```
S pwd
//home/codermehraj/certs
$ ls
$ openssl genrsa -des3 -out myCA.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
$ openssl genrsa -des3 -out myCA.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
$ openssl genrsa -des3 -out myCA.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
$ openssl req -x509 -new -nodes -key myCA.key -sha256 -days 1825 -out myCA.pem
Enter pass phrase for myCA.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]:BD
State or Province Name (full name) [Some-State]:Barisal
Locality Name (eg, city) []:Barisal
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Taohid
Organizational Unit Name (eg, section) []:SUST
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:
```

```
$ sudo apt-get install -y ca-certificates
[sudo] password for codermehraj:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ca-certificates is already the newest version (20230311ubuntu0.22.04.1).
ca-certificates set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
$ sudo cp ~/certs/mycA.pem /usr/local/share/ca-certificates/mycA.crt
$ sudo update-ca-certificates
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
Adding debian:mycA.pem
done.
$
```

```
$ sudo apt-get install -y ca-certificates
[sudo] password for codermehraj:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ca-certificates is already the newest version (20230311ubuntu0.22.04.1).
ca-certificates set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
$ sudo cp ~/certs/myCA.pem /usr/local/share/ca-certificates/myCA.crt
$ sudo update-ca-certificates
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
Adding debian:myCA.pem
done.
$ $
```

```
Tor some fields there will be a default value,

for some fields the will be left black.

Coparty Name (2 letter code) [AD] [10]

State of Province Name (61] in all the left black.

Coparty Name (2 letter code) [AD] [10]

State of Province Name (61] in Signature (1) [130]

State of Province Name (61] in Signature (1) [130]

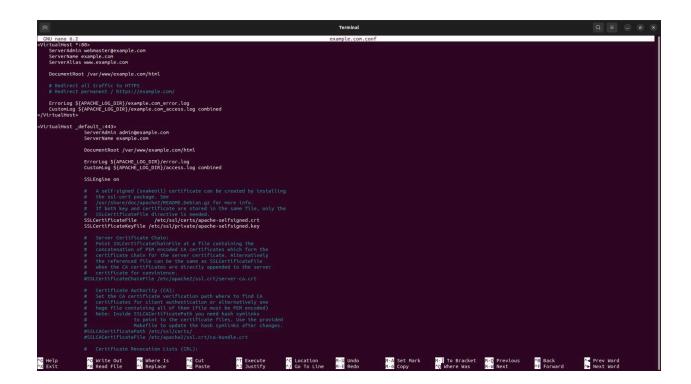
Some (60, City) [130]

Some (60, City) [130]

Some (60, City) [130]

Some (60, City) [130]

Some (61, City) [13
```



## Checkpoint-3:



hello I am taohid, This is Lab task 5

### **Checkpoint-4:**

