1 HTTP Lab

For this task first you have to setup a Web Server in a Linux machine. You have to follow the given instructions to configure the ssl setup. At the end you have to show it to one of the instructors and get marked before leaving the lab.

- Setup the Web Server
- Change the host_name to a some domain name ***eg: example.com***
- Open /etc/hosts and change

```
127.0.0.1   localhost
to
127.0.0.1 example.com example.com
```

- Change openssl CA dir
  1. Open /usr/lib/ssl/openssl.cnf
  2. Change the following configurations according to the given commands.

```
[ CA_default ]
dir = ./demoCA
```

To

```
[ CA_default ]
dir = /root/ca
```

```
[ policy_match ]
countryName   = match
stateOrProvinceName = match
organizationName  = match
organizationalUnitName  = optional
commonName    = supplied
emailAddress    = optional
```

To

```
[ policy_match ]
countryName             = match
stateOrProvinceName     = optional
organizationName        = optional
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional
```

- Create root CA
  1. Switch to root
  2. Make necessary directories for root CA

```
mkdir /root/ca
cd /root/ca
mkdir newcerts certs crl private requests
```

3. To proceed with the next step we need to create two files. The first one is called **"index.txt"**. This is where OpenSSL keeps track of all signed certificates. The second file is called **"serial.txt"**. Each signed certificate will have a serial number. Let's start with number 1234.

```
touch index.txt
echo '1234' > serial
```

4. generate the root private key

```
openssl genrsa -aes256 -out private/cakey.pem 4096
```

5. create the root certificate using root private key. Insert accurate information as much as possible

```
openssl req -new -x509 -key /root/ca/private/cakey.pem -out cacert.
   pem -days 3650 -set_serial 0
```

- Create a certificate

1. Go to requests dir
2. Generate private key

```
openssl genrsa -aes256 -out some_serverkey.pem 2048
```

3. Create CSR

```
openssl req -new -key some_serverkey.pem -out some_server.csr
```

4. Sign the CSR

```
openssl ca -in some_server.csr -out some_server.pem
```

- Install the certificate into your web server. Follow the following tutorial. Instead of self-signed certificate use the certificate you created earlier. Tutorial
- Install the root certificate to the browser.
- Test the https connection using the browser. Check whether the padlock icon is shown in the address bar. Click that and view certificate to see what details it holds.
- Use Wireshark or some kind of packet capturing tool capture the packets transmitting when connecting to the website. Try to understand and reason out what you see.