EAST WEST UNIVERSITY

Department of Computer Science and Engineering

CSE- 487

MP-1(Cybersecurity) project report

Mini Project-1: Securing a networked system with Public Key Infrastructure
(Implementing Transport Layer Security on HTTP for https:// connection)

Submitted by

Name	Id
Minhazul Amin Tomal	2019-1-60-145
Md. Abir Hasan	2019-1-60-201

Submitted to

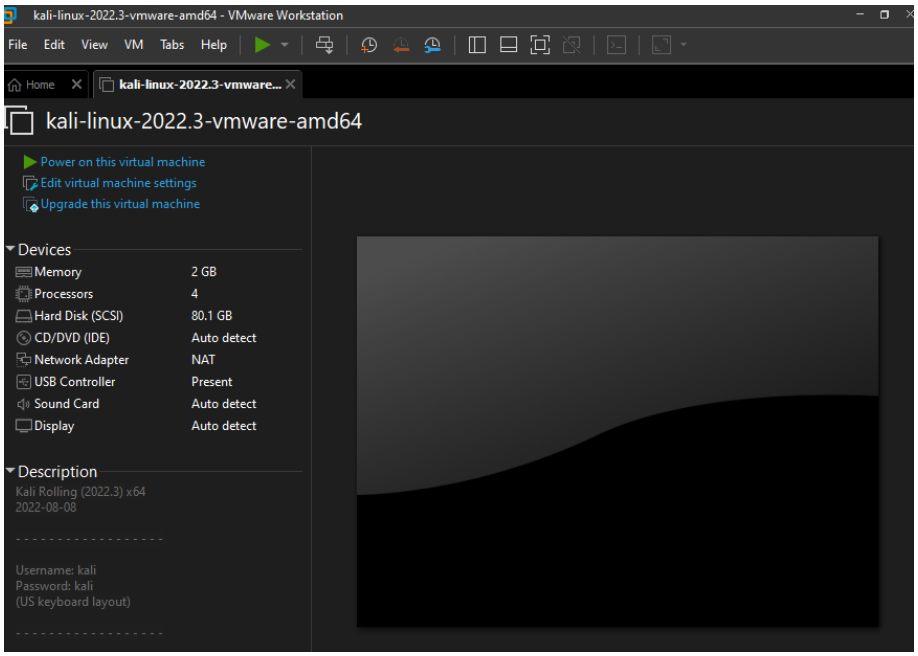
Rashedul Amin Tuhin

Senior Lecturer
Department of Computer Science and Engineering
East West University

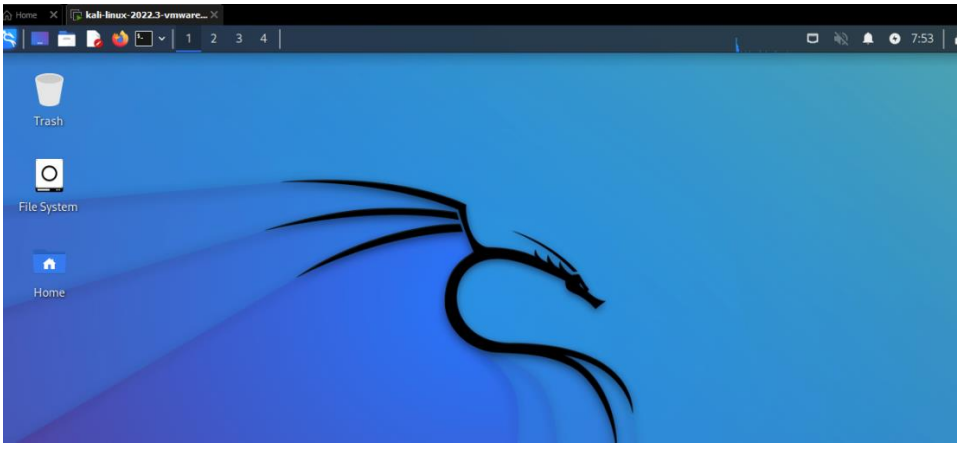
1. **Configuration of Certification Authority AcmeCA with AcmeRootCA as the RootCA.**

Step 1: Download and install vmware software on your device.

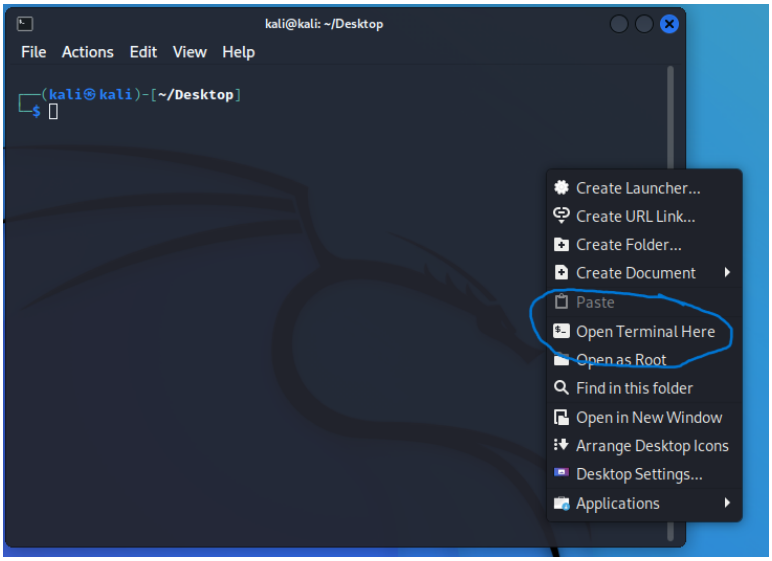
Step 2: Now download kali linux from any web browser and open it with the vmware software. You have to click on "open a new project " then you must open up the vmx file which is in the kali linux file.



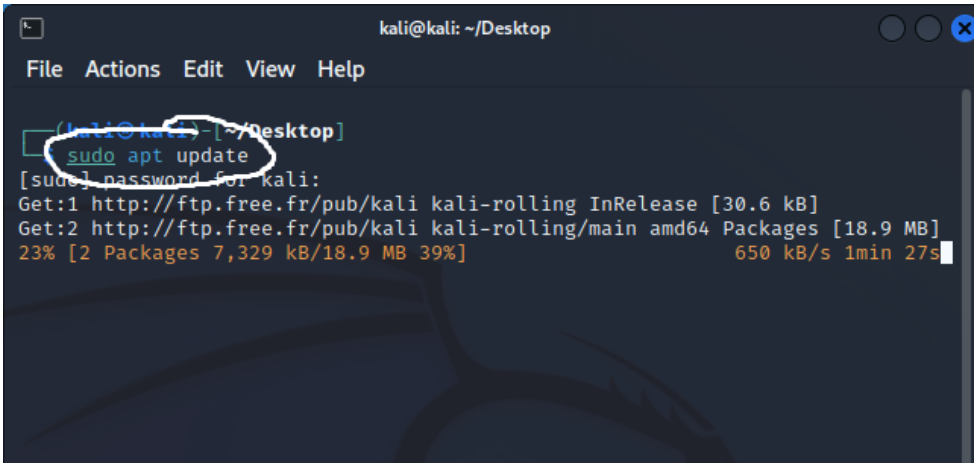
Step 3: Then click on "power on virtual machine" and kali will be open in the vmware. After that you to give username and password both "kali" to use the kali linux. The home page will be look like this.



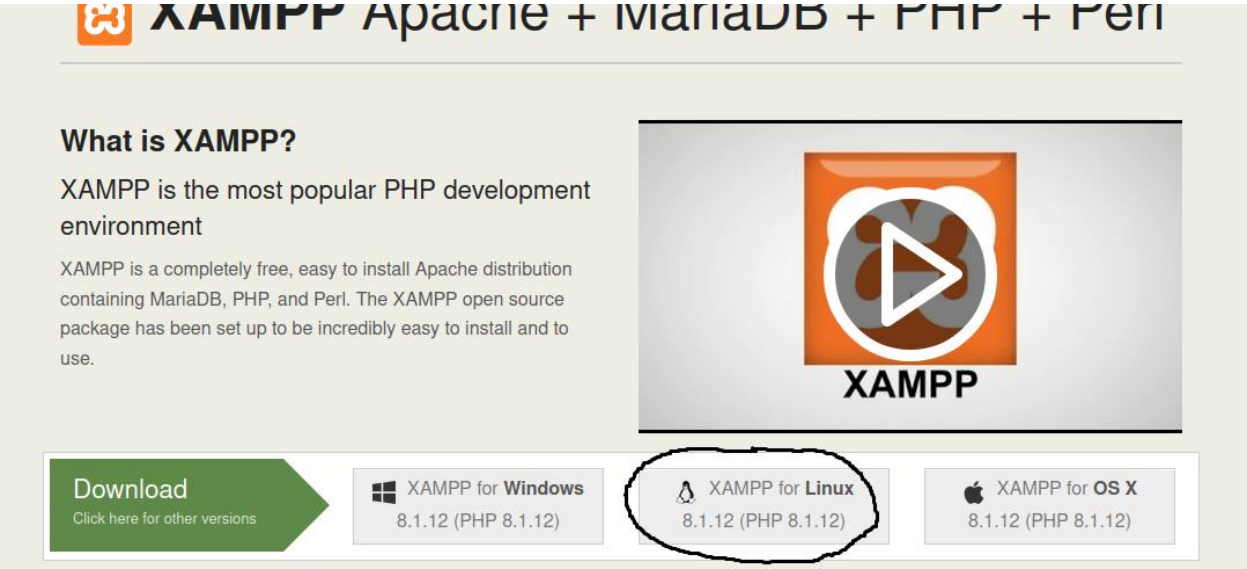
Step 4: To open the terminal you have to right click on the home page and open terminal here.



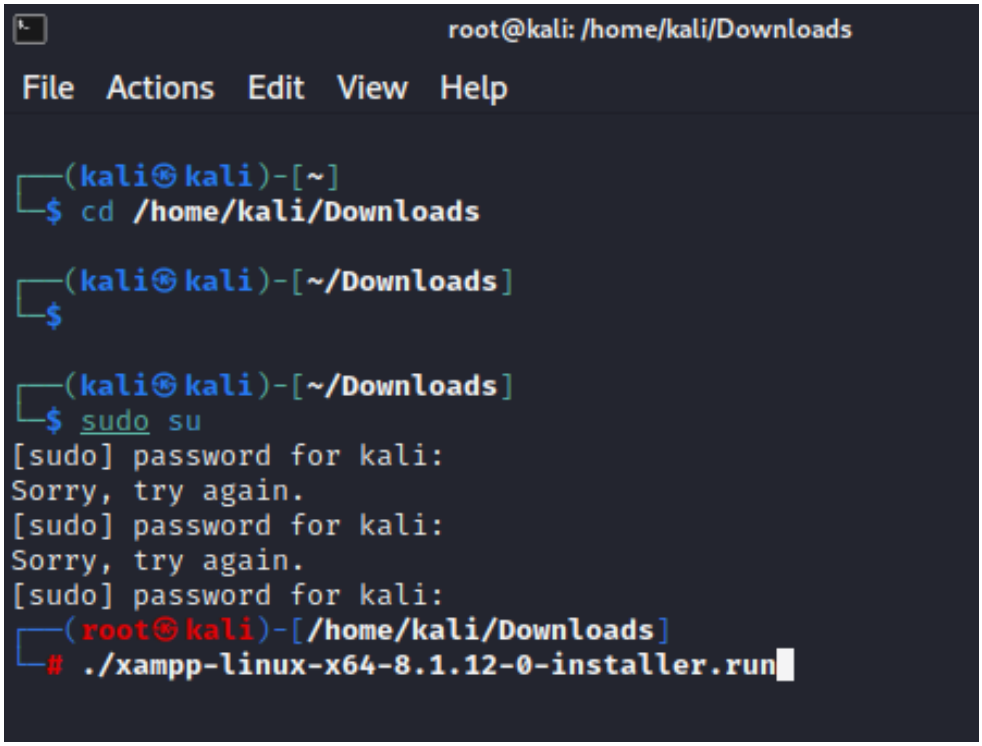
Step 5: Now write “sudo apt update” for necessary update for the machine and you have to give password in the terminal. The password does not show up you just have to type it and press enter.



Step 6: Now open the firefox browser of the kali and search for “xampp”. Then click on the first link and download it for linux.



Step 7: After download we must install the xampp. For that we must have to be root user. So, follow the picture given below.



Step 8: Now open terminal and write down the following to generate root certificate

openssl req -config root-ca/root-ca.conf -key root-ca/private/ca.key -new -x509 -days 7305 -sha256 -extensions v3_ca -out root-ca/certs/ca.crt

```
Country Name (2 letter code) [BD]:
State or Province Name [DHK]:
Locality Name [RAMPURA]:
Organization Name [EWUBD]:
Organizational Unit Name [ADMIN]:
Common Name [rootCA]:
Email Address []:
```

Step 9: Then create subrootCA

openssl ca -config root-ca/root-ca.conf -extensions v3_intermediate_ca -days 3652 -notext -in sub-ca/csr/sub-ca.csr -out sub-ca/certs/sub-ca.crt

Step 10: After that create a server.

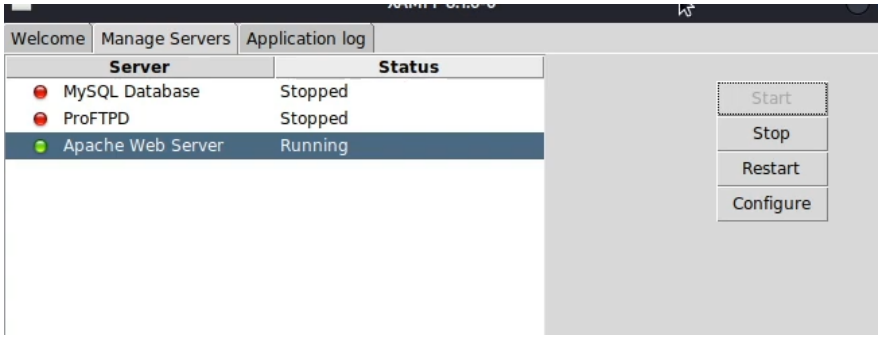
openssl ca -config sub-ca/sub-ca.conf -extensions server_cert -days 365 -notext -in server/csr/server.csr -out server/certs/server.crt
openssl pkcs12 -inkey server/private/server.key -in server/certs/server.crt -export -out server/certs/server.pfx

The server's name will be – www.verysecureserver.com

Step 11: Open terminal and follow the command to open xampp and run it

```
┌──(root㉿kali)-[/opt/lampp]
└─# cd /opt/lampp

┌──(root㉿kali)-[/opt/lampp]
└─# ./manager-linux-x64.run
```



Step 11: Open any file then go to file system. Then opt>>lamp>>etc>>extra then open this file.

Step 12: Now go to line number 106 then edit this to

```
105 #   parallel.
106 SSLCertificateFile "/opt/lampp/etc/ssl.crt/server.crt"
107 #SSLCertificateFile "/opt/lampp/etc/server-dsa.crt"
108 #SSLCertificateFile "/opt/lampp/etc/server-ecc.crt"
109
```

This line

```
05 #   parallel.
06 SSLCertificateFile "/root/Desktop/ssl/generated/server.crt"
07 #SSLCertificateFile "/opt/lampp/etc/server-dsa.crt"
08 #SSLCertificateFile "/opt/lampp/etc/server-ecc.crt"
09
```

Step 13: Now go to line number 116 then edit this to

```
115 #   ECC keys, when in use, can also be configured in parallel
116 SSLCertificateKeyFile "/opt/lampp/etc/ssl.key/server.key"
117 #SSLCertificateKeyFile "/opt/lampp/etc/server-dsa.key"
118 #SSLCertificateKeyFile "/opt/lampp/etc/server-ecc.key"
119
```

This line

```
115 #   ECC keys, when in use, can also be configured in parallel
116 SSLCertificateKeyFile "/root/Desktop/ssl/generated/server.key"
117 #SSLCertificateKeyFile "/opt/lampp/etc/server-dsa.key"
118 #SSLCertificateKeyFile "/opt/lampp/etc/server-ecc.key"
119
```

Step 14: Now go to line number 136 then edit this to

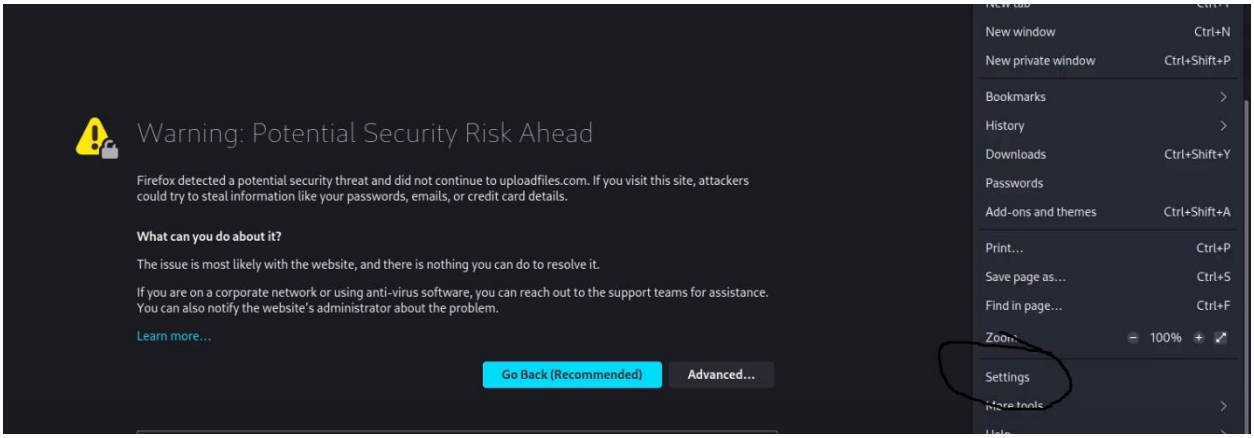
```
135 #         Makefile to update the hash symlinks after changes.
136 SSLCACertificatePath "/opt/lampp/etc/ssl.crt"
137 #SSLCACertificateFile "/opt/lampp/etc/ssl.crt/ca-bundle.crt"
```

This line

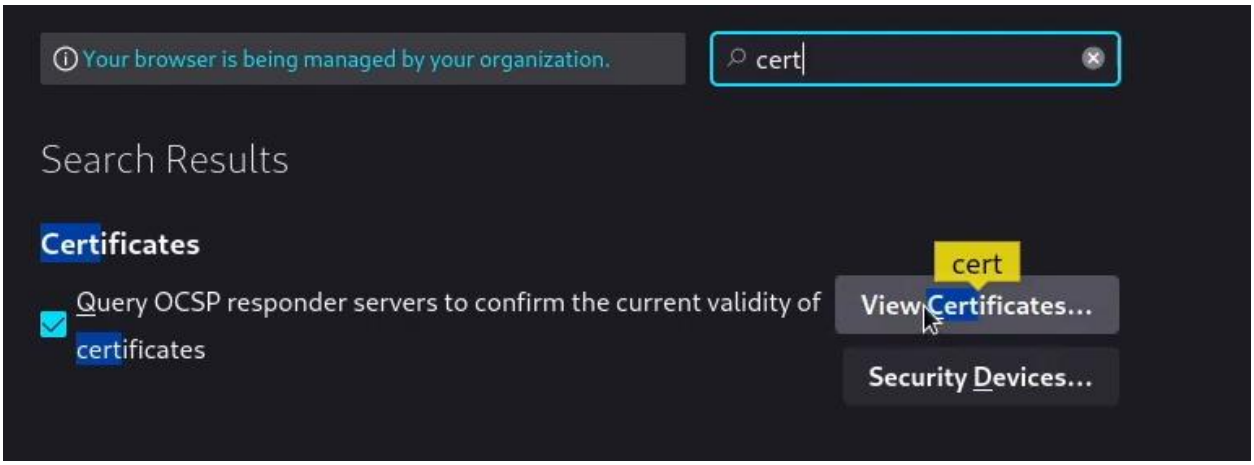
```
134 #         to point to the certificate files. Use the provided
135 #         Makefile to update the hash symlinks after changes.
136 SSLCACertificatePath "/root/Desktop/ssl/generated"
137 #SSLCACertificateFile "/opt/lampp/etc/ssl.crt/ca-bundle.crt"
138
```

After that do the step 11 again to open xampp.

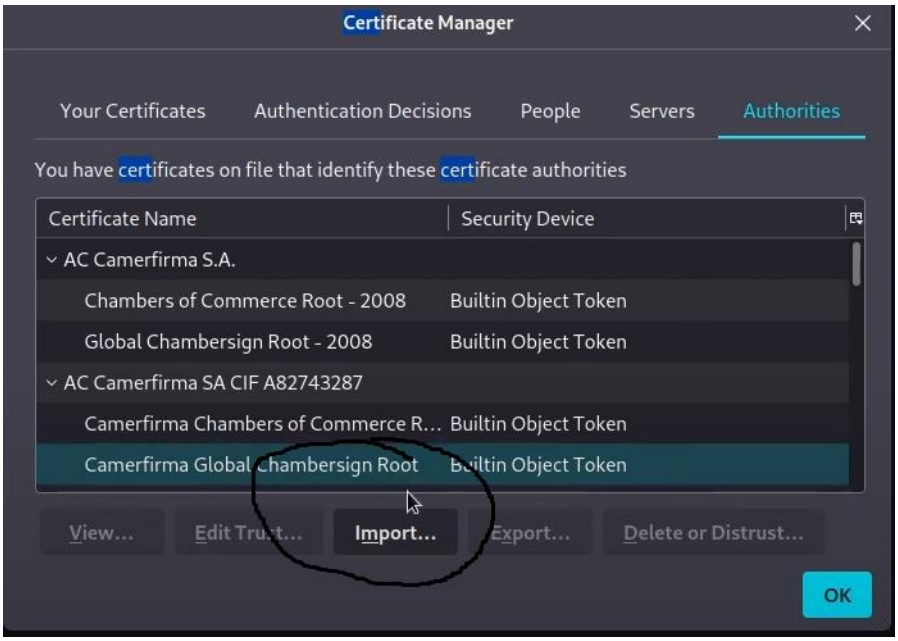
Step 15: Now if you search it on firefox https://www.verysecureserver.com then it will not work cause you have to import the certificate. So go to settings.

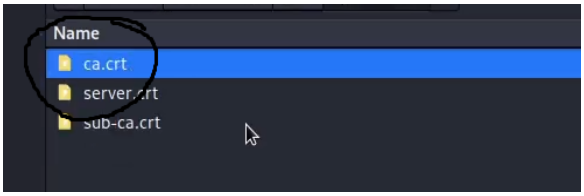


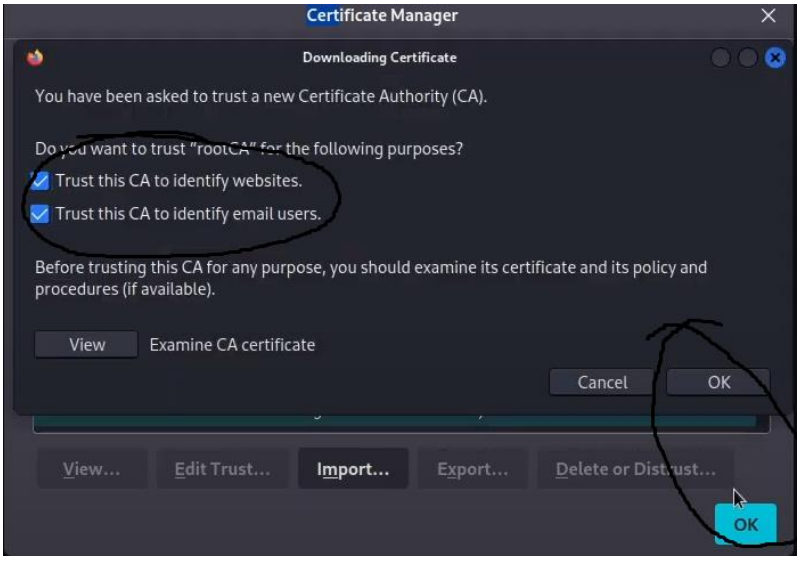
Step 16: Now search for certificate and click on view certificate.



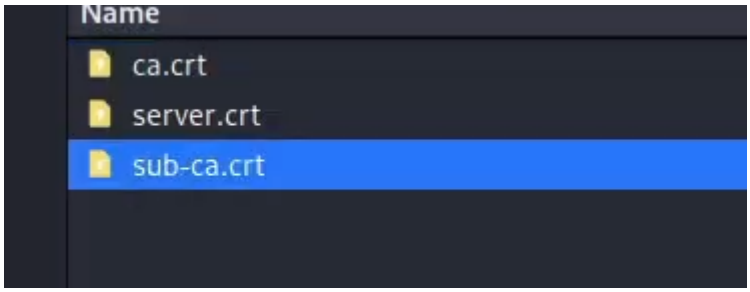
Step 17: Click on import then import the ca.crt file.



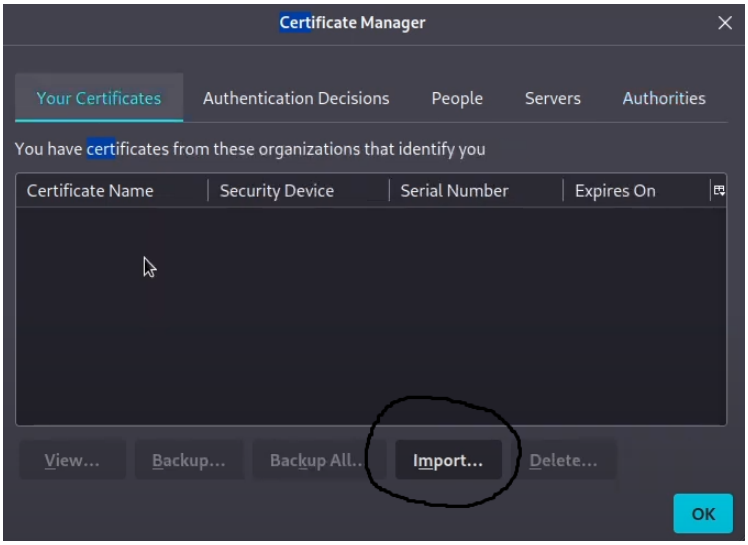


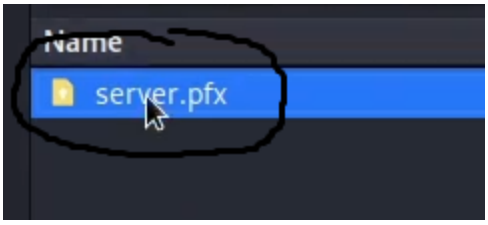


Step 18: Now again click on import and import the sub-ca.crt

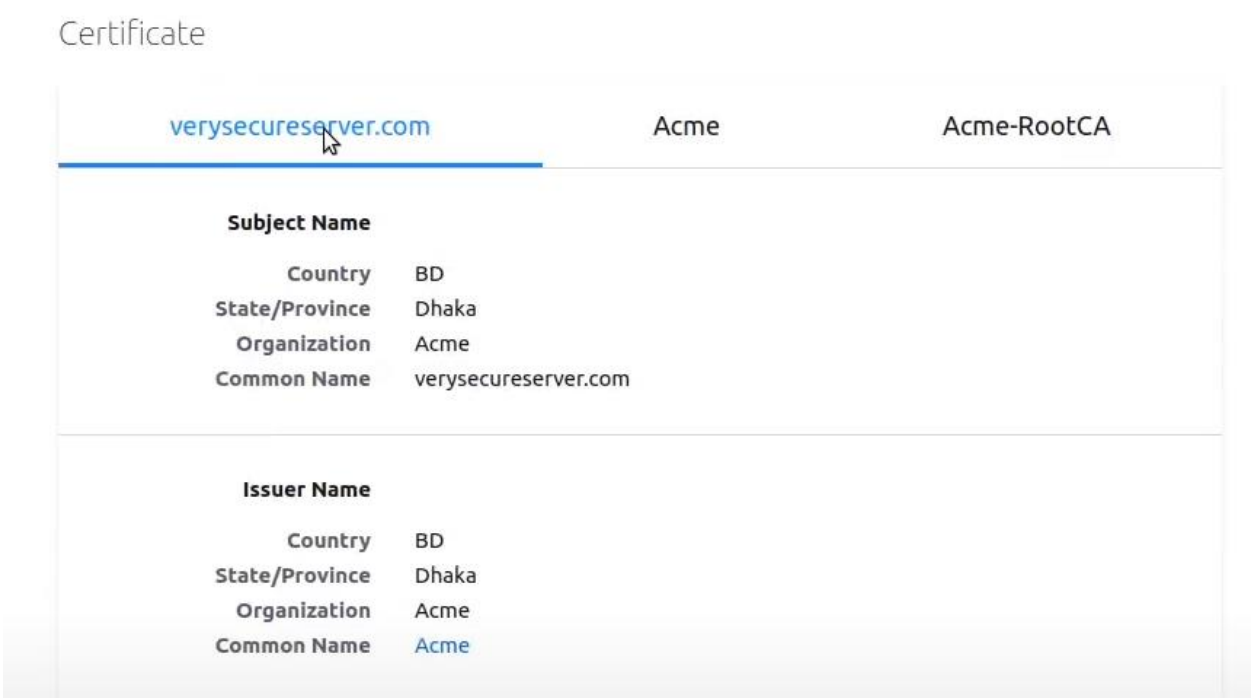


Step 19: Go on your certificates click on import and import the server pfx file.





Step 20: Clear browser history then search for https://www.verysecureserver.com you can see the padlock sign and if you go to certificates of the server, you can see the certificates.


Certificate
verysecureserver.com
Acme
Acme-RootCA
Subject Name
Country BD
State/Province Dhaka
Organization Acme
Common Name verysecureserver.com
Issuer Name
Country BD
State/Province Dhaka
Organization Acme
Common Name Acme