EAST WEST UNIVERSITY

Summer 2022

Department: Computer Science and Engineering

Course Title : Cyber Security Law and Ethics

Course Code: CSE 487

Section No: 02

Project-01

Project Title: Securing a networked system with Public Key Infrastructure

Submitted By:

Mridul Ranjan

Submitted To:

Rashedul Amin Tuhin (RDA)
Senior Lecturer
Department of Computer Science and Engineering

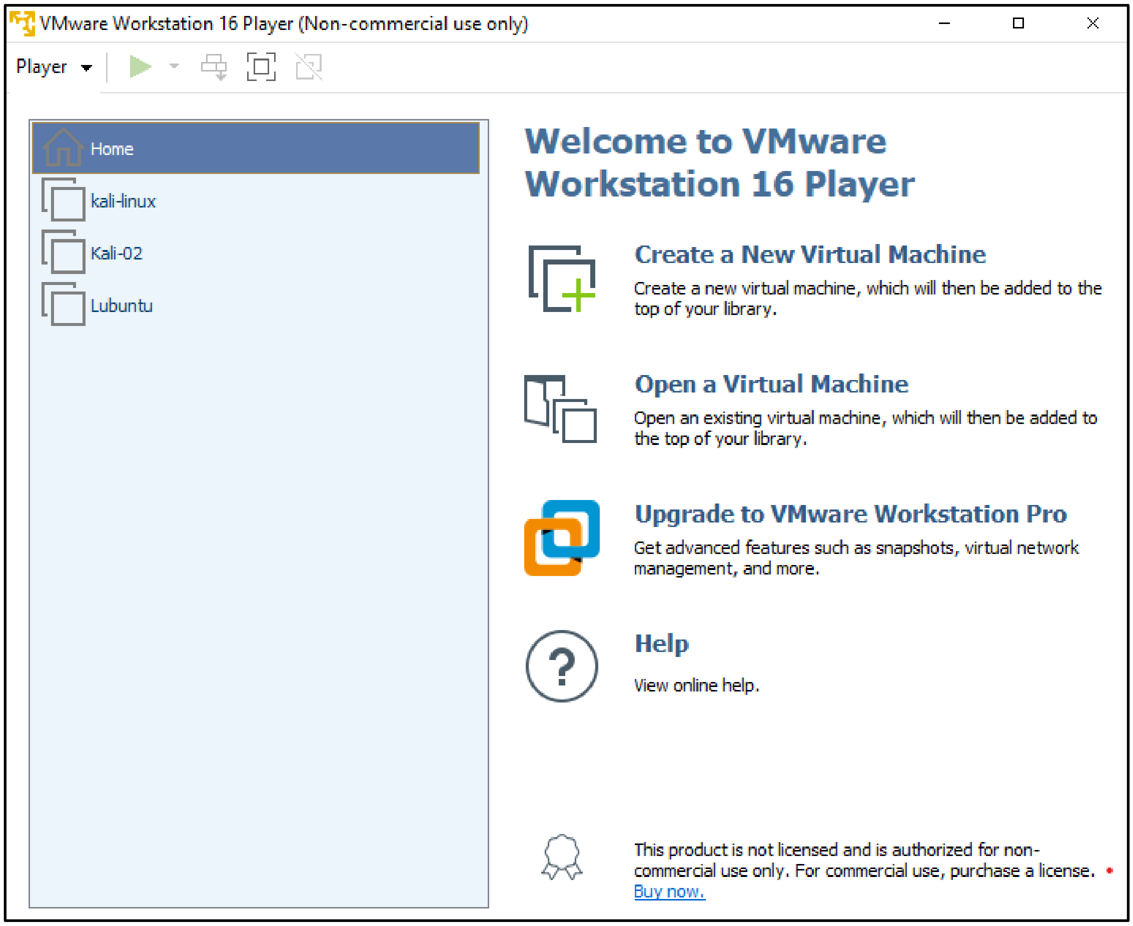
Title: **Securing a networked system with Public Key Infrastructure (Implementing Transport Layer Security on HTTP for https://mrkbprojectcs.com)**

In this project we use the "VMware workstation 16 player" as our virtual machine.

For installation of VMware we go to the official website of VMware and download the

"VMware Workstation 16.2.4 Player for Windows 64-bit Operating Systems" and then install the VMware manually.

This is the our installed VMware interface in our windows machine:



Welcome to VMware Workstation 16 Player

Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine

Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation Pro

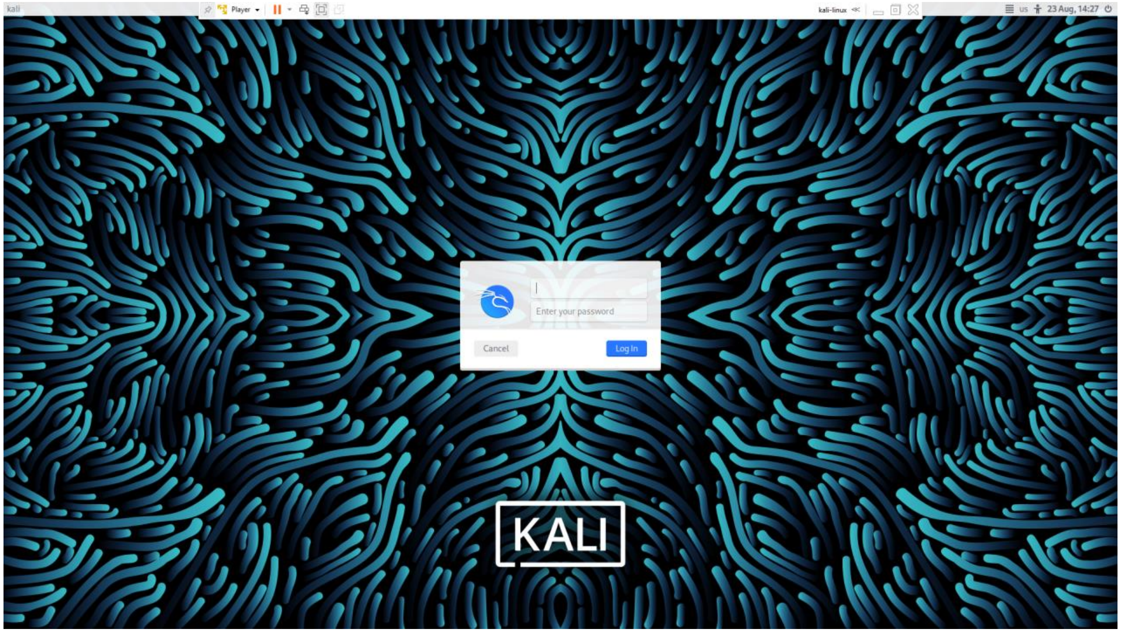
Get advanced features such as snapshots, virtual network management, and more.

Help

View online help.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

Then we use The “Kali Linux” for this project on the VMware workstation. As “Kali-Linux is built in VMware so we just open the iso file to on the VMware. This is the interface of the kali on the VMware.



For accessing KaLi:

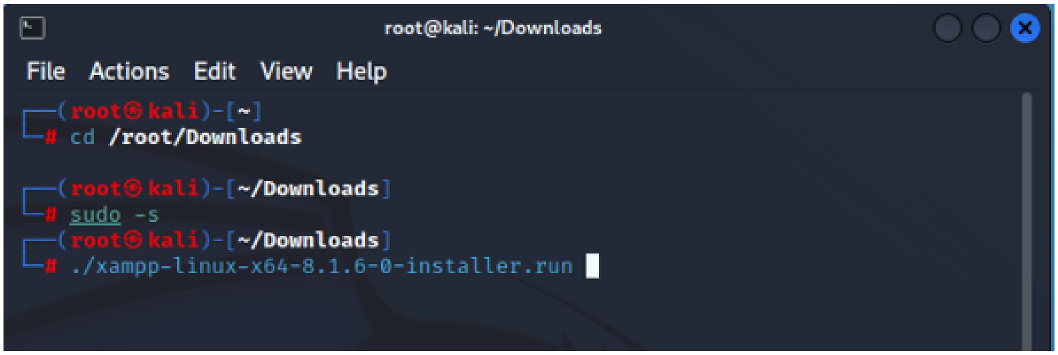
User Name: **root**

Password: **MRIDUL**

Then we use “xampp” for generating Apache web server.

We download “xampp-linux-x64-8.1.6.0-installer.run” from www.apachefriends.org.

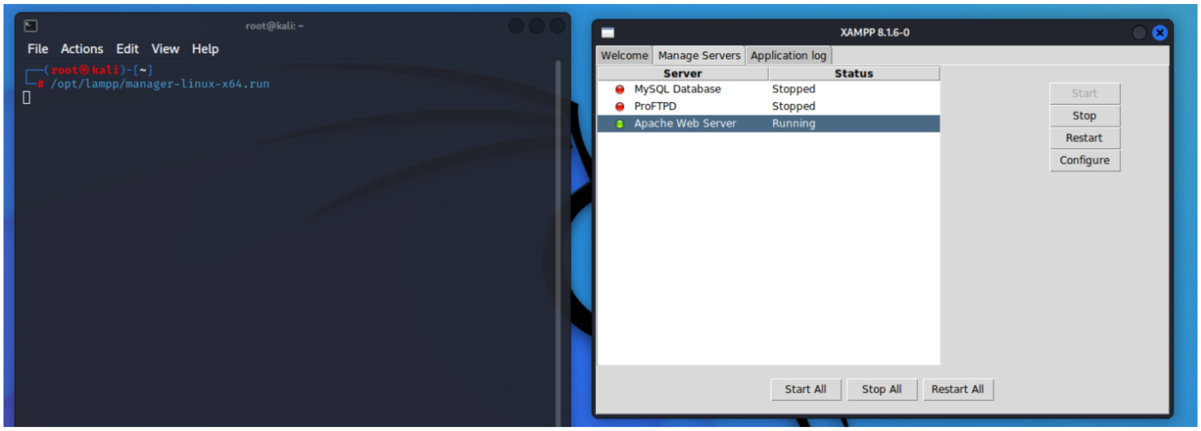
We open terminal and go to the xampp downloaded folder and entry command for install xampp:



```
┌──(root㉿kali)-[~]
└─# cd /root/Downloads

┌──(root㉿kali)-[~/Downloads]
└─# sudo -s
┌──(root㉿kali)-[~/Downloads]
└─# ./xampp-linux-x64-8.1.6-0-installer.run
```

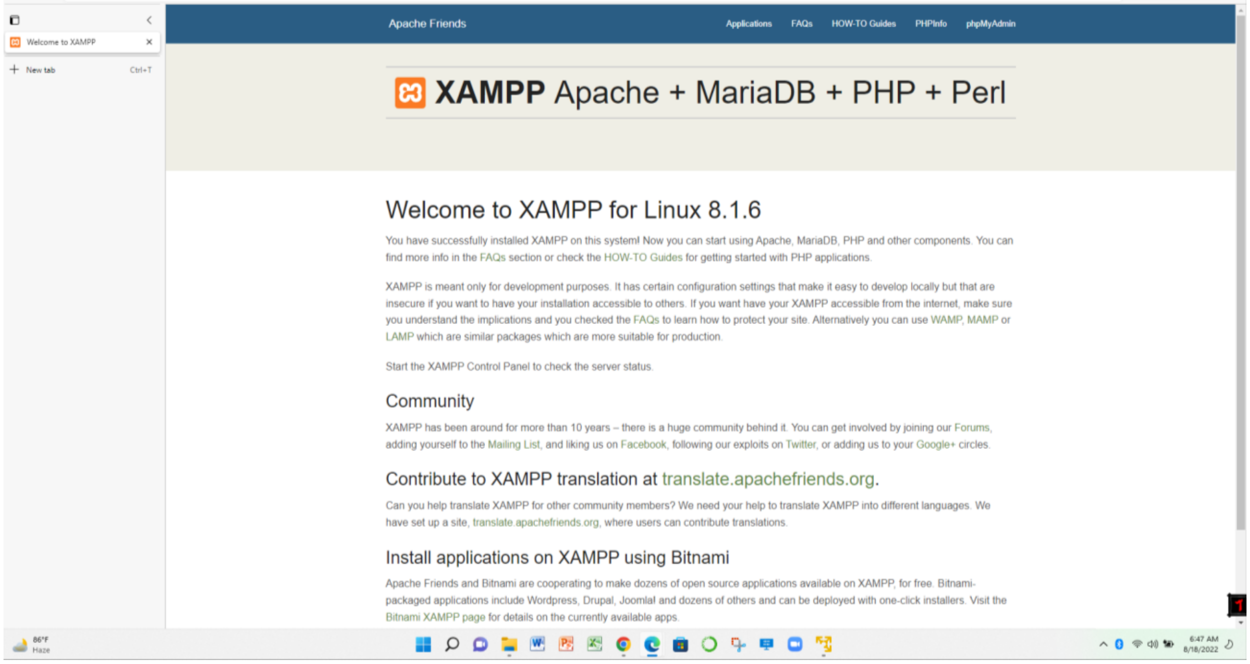
After installation we do ”/opt/lamp/manager-linux-x64.run” command to open xampp > Manage server> and select the apache and press the start button. The apache is successfully running.



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

Server	Status
● MySQL Database	Stopped
● ProFTPD	Stopped
● Apache Web Server	Running

After that open the Mozila Firefox and search the ip “192.168.171.129” then we can see our apache server on browser:



XAMPP Apache + MariaDB + PHP + Perl

Welcome to XAMPP for Linux 8.1.6

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others. If you want have your XAMPP accessible from the internet, make sure you understand the implications and you checked the FAQs to learn how to protect your site. Alternatively you can use WAMP, MAMP or LAMP which are similar packages which are more suitable for production.

Start the XAMPP Control Panel to check the server status.

Community

XAMPP has been around for more than 10 years – there is a huge community behind it. You can get involved by joining our Forums, adding yourself to the Mailing List, and liking us on Facebook, following our exploits on Twitter, or adding us to your Google+ circles.

Contribute to XAMPP translation at translate.apachefriends.org.

Can you help translate XAMPP for other community members? We need your help to translate XAMPP into different languages. We have set up a site, translate.apachefriends.org, where users can contribute translations.

Install applications on XAMPP using Bitnami

Apache Friends and Bitnami are cooperating to make dozens of open source applications available on XAMPP, for free. Bitnami-packaged applications include Wordpress, Drupal, Joomla! and dozens of others and can be deployed with one-click installers. Visit the Bitnami XAMPP page for details on the currently available apps.

Now we Generate all the certificates for secure our Server:

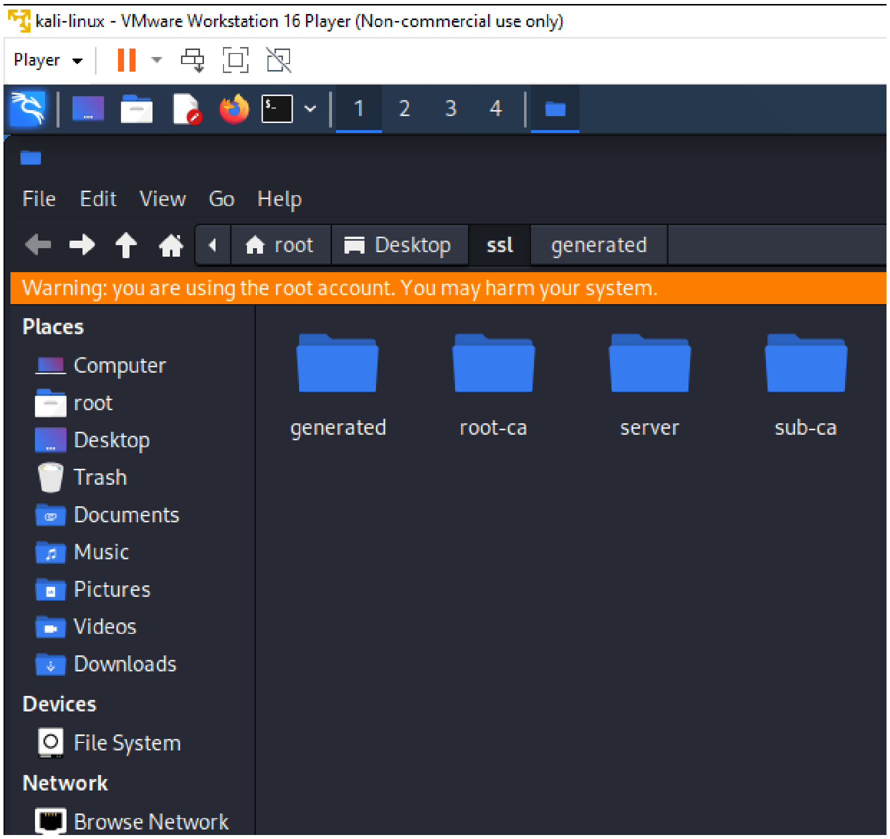
At first we created a folder ssl in which there will store our openssl certificates folder by do command

“mkdir root-ca

“mkdir sub-ca”

“mkdir Server”

“mkdir generated” in kali-Linux terminal.



Now Generating All the keys by below commands in those folder:

openssl genrsa -aes256 -out root-ca/private/ca.key 4096

openssl genrsa -aes256 -out sub-ca/private/sub-ca.key 4096

openssl genrsa -out server/private/server.key 2048

Then we do below command for thr root CA 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”
```

Then we generating certificate signing request for sub-ca by below command:

```
“openssl req -config sub-ca/sub-ca.conf -new -key sub-ca/private/sub-ca.key -sha256 -out sub-ca/csr/sub-ca.csr”
```

Then we do below command for the sub root CA certificate:

```
“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”
```

Genarating server certificate signing request by below command:

```
“openssl req -key server/private/server.key -new -sha256 -out server/csr/server.csr”
```

Generate Server certificate and server pfx file:

```
“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”
```

We enter certificate information credential for **root-CA**:

Country:BD

State/Province: DHK

Locality: RAMPURA

Organization: EWUBD

Organizational Unit: ADMIN

Common Name: rootCA

We enter certificate information credential for **sub-CA**:

Country:BD

State/Province: DHK

Organization: EWUBD

Organizational Unit: SUBADMIN

Common Name: subtCA

We enter certificate information credential for **server-CA**:

Country: BD

State/Province: DHK

Locality: RAMPURA

Organization: mrkbprojectcs

Organizational Unit: ADMIN

Common Name: mrkbprojectcs.com

Email Address: admin@mrkb.com

Copy All the certificate and pfx file to the generated folder by below command:

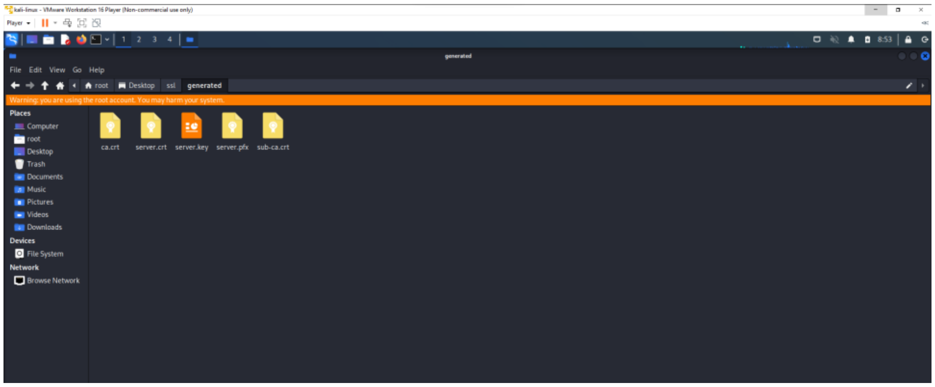
cp root-ca/certs/ca.crt generated

cp sub-ca/certs/sub-ca.crt generated

cp server/certs/server.crt generated

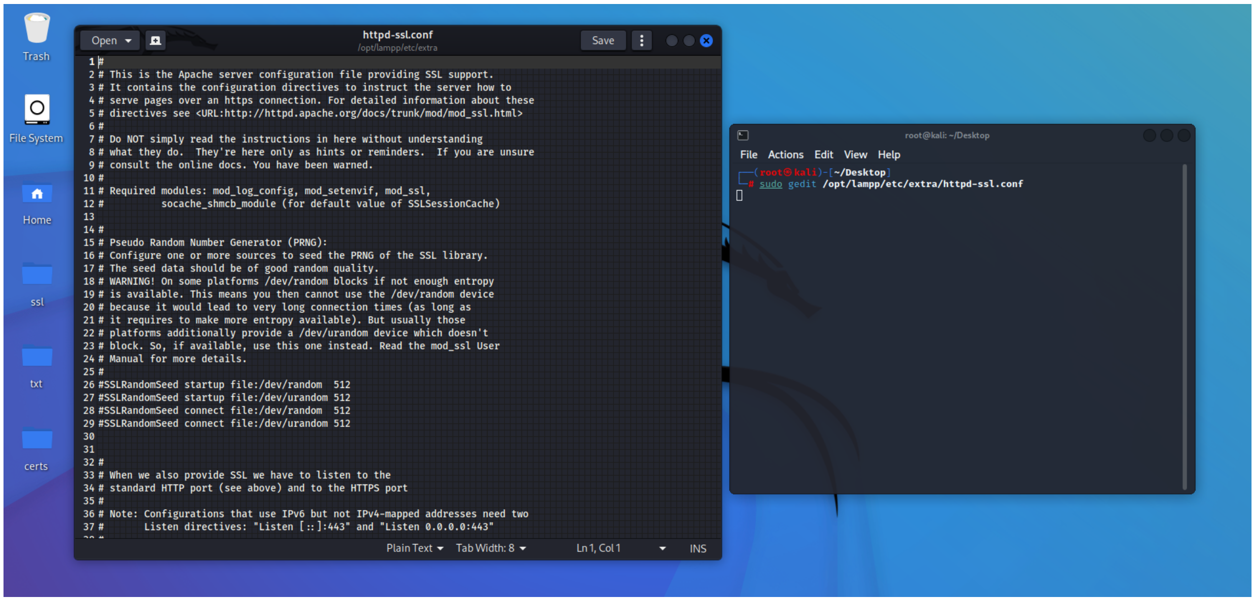
cp server/private/server.key generated

cp server/certs/server.pfx generated



Warning: you are using the root account. You may harm your system.

Now we open the terminal in the desktop and do command “sudo gedit /opt/lamp/etc/extra/httpd-ssl.conf “ and open-up the http configuration file.



```
#
# This is the Apache server configuration file providing SSL support.
# It contains the configuration directives to instruct the server how to
# serve pages over an https connection. For detailed information about these
# directives see <URL:http://httpd.apache.org/docs/trunk/mod/mod_ssl.html>
#
# Do NOT simply read the instructions in here without understanding
# what they do.  They're here only as hints or reminders.  If you are unsure
# consult the online docs. You have been warned.
#
# Required modules: mod_log_config, mod_setenvif, mod_ssl,
#          socache_shmcb_module (for default value of SSLSessionCache)

#
# Pseudo Random Number Generator (PRNG):
# Configure one or more sources to seed the PRNG of the SSL library.
# The seed data should be of good random quality.
# WARNING! On some platforms /dev/random blocks if not enough entropy
# is available. This means you then cannot use the /dev/random device
# because it would lead to very long connection times (as long as
# it requires to make more entropy available). But usually those
# platforms additionally provide a /dev/urandom device which doesn't
# block. So, if available, use this one instead. Read the mod_ssl User
# Manual for more details.
#
#SSLRandomSeed startup file:/dev/random  512
#SSLRandomSeed startup file:/dev/urandom 512
#SSLRandomSeed connect file:/dev/random  512
#SSLRandomSeed connect file:/dev/urandom 512


#
# When we also provide SSL we have to listen to the
# standard HTTP port (see above) and to the HTTPS port
#
# Note: Configurations that use IPv6 but not IPv4-mapped addresses need two
#       Listen directives: "Listen [::]:443" and "Listen 0.0.0.0:443"
```

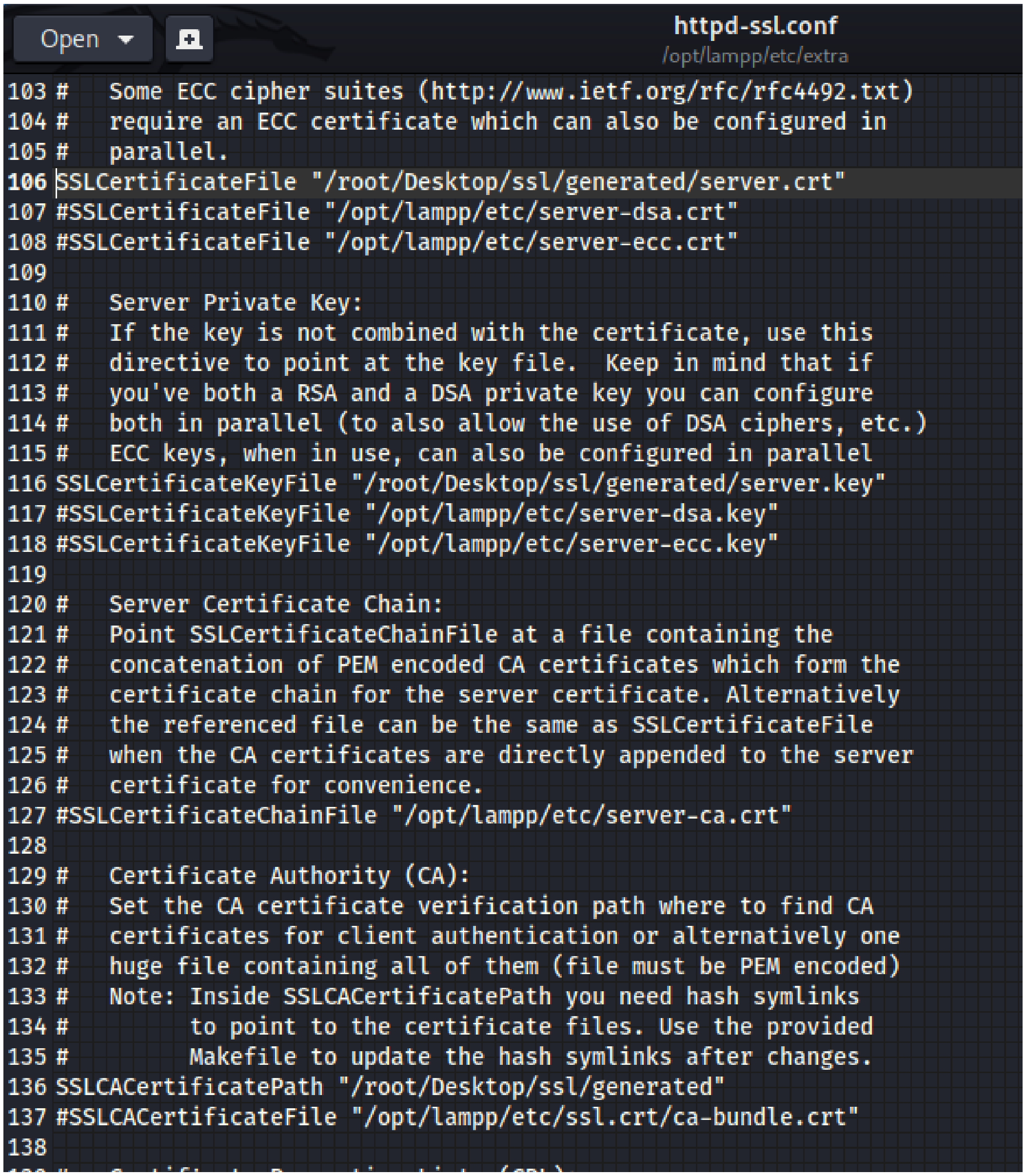
```
┌──(root㉿kali)-[~/Desktop]
└─# sudo gedit /opt/lampp/etc/extra/httpd-ssl.conf
```

Then we change the .conf file on Line 106,116,136 the line to replace the certificate path as followings:

106> SSLCertificateFile "/root/Desktop/ssl/generated/server.crt"

116> SSLCertificateKeyFile "/root/Desktop/ssl/generated/server.key"

136> SSLCACertificatePath "/root/Desktop/ssl/generated"

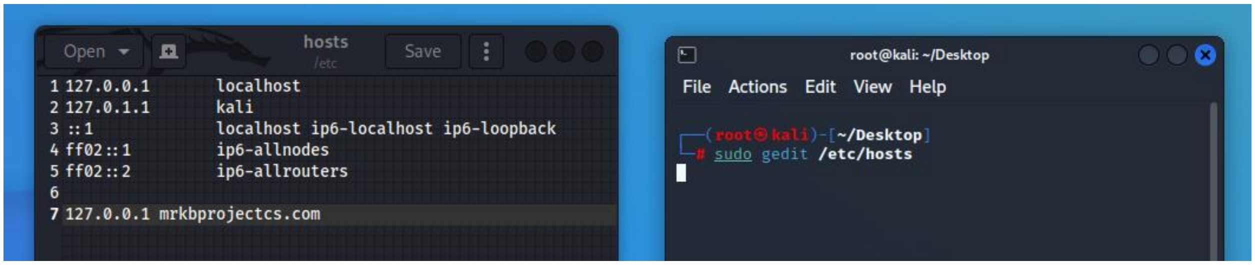


```
103 #   Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
104 #   require an ECC certificate which can also be configured in
105 #   parallel.
106 SSLCertificateFile "/root/Desktop/ssl/generated/server.crt"
107 #SSLCertificateFile "/opt/lampp/etc/server-dsa.crt"
108 #SSLCertificateFile "/opt/lampp/etc/server-ecc.crt"
109
110 #   Server Private Key:
111 #   If the key is not combined with the certificate, use this
112 #   directive to point at the key file.  Keep in mind that if
113 #   you've both a RSA and a DSA private key you can configure
114 #   both in parallel (to also allow the use of DSA ciphers, etc.)
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
120 #   Server Certificate Chain:
121 #   Point SSLCertificateChainFile at a file containing the
122 #   concatenation of PEM encoded CA certificates which form the
123 #   certificate chain for the server certificate. Alternatively
124 #   the referenced file can be the same as SSLCertificateFile
125 #   when the CA certificates are directly appended to the server
126 #   certificate for convenience.
127 #SSLCertificateChainFile "/opt/lampp/etc/server-ca.crt"
128
129 #   Certificate Authority (CA):
130 #   Set the CA certificate verification path where to find CA
131 #   certificates for client authentication or alternatively one
132 #   huge file containing all of them (file must be PEM encoded)
133 #   Note: Inside SSLCACertificatePath you need hash symlinks
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
```

Then save the configuration File.

Then we open terminal in the desktop and do command " sudo gedit /etc/hosts" and open the etc host file for assigning xampp server to the host file.

When xampp server is opened then we write "127.0.0.1 mrkbprojectcs.com" to the host file and save it.



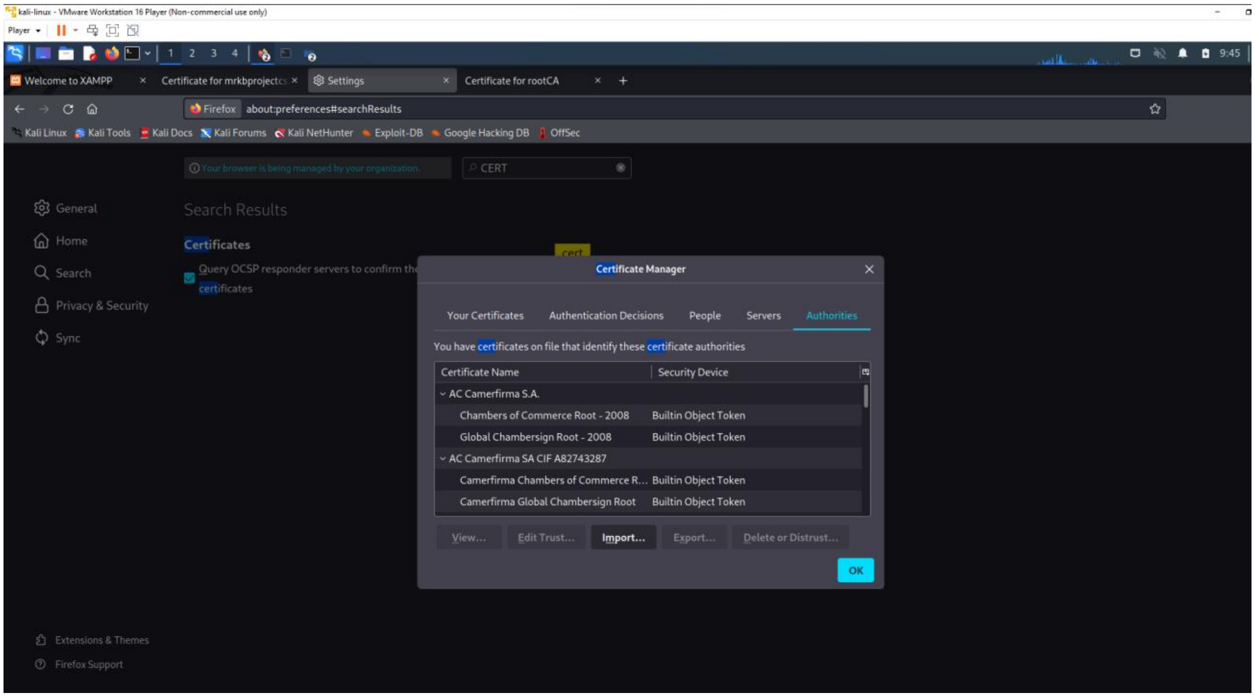
```
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

127.0.0.1 mrkbprojectcs.com
```

```
┌──(root㉿kali)-[~/Desktop]
└─# sudo gedit /etc/hosts
```

Now we import the certificates to the Browser that it can trust our SSL certificates for the https connection.

We went : >Mozila Fire-fox > New tabs > settings > Certificate Manager > Authorities >

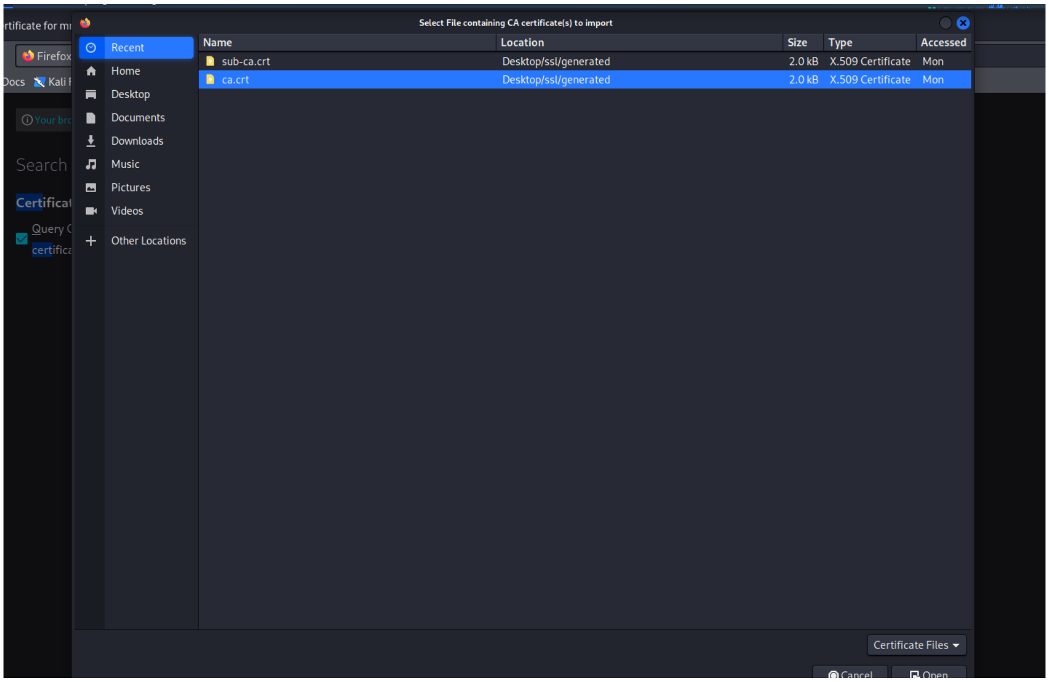


☑ Query OCSP responder servers to confirm the current validity of certificates

You have certificates on file that identify these certificate authorities

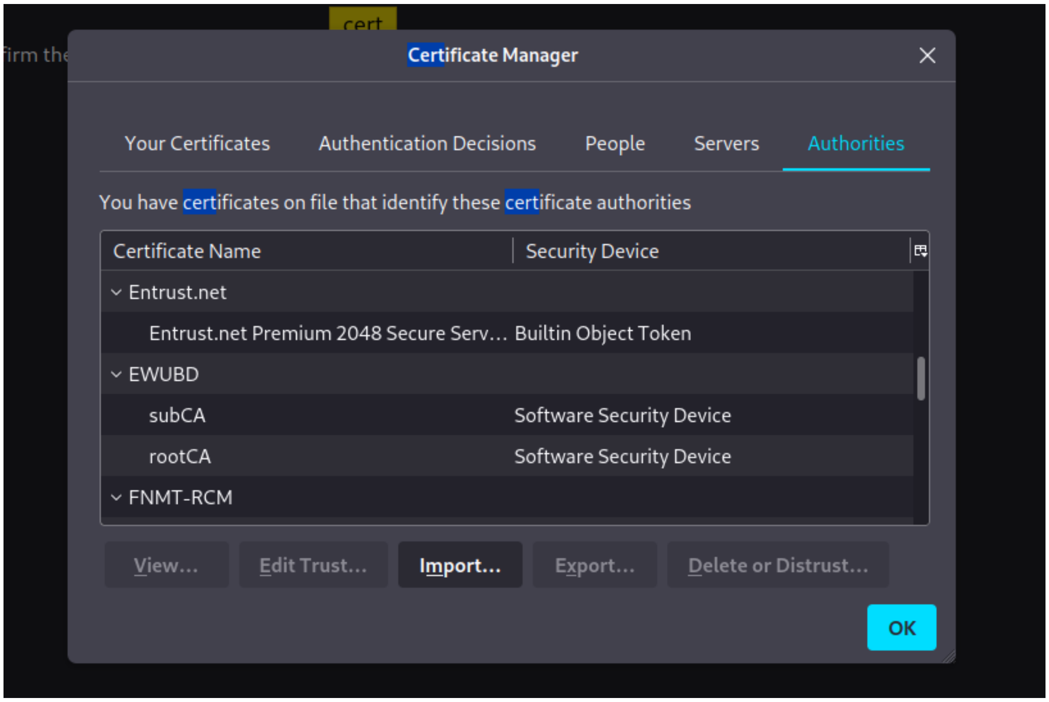
Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce R...	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token

Now click import and select the root-ca certificate and open then click the trust buttons then press ok. The same procedure will be followed for sub-ca and our sever-certificate.



Select File containing CA certificate(s) to import

Name	Location	Size	Type	Accessed
sub-ca.crt	Desktop/ssl/generated	2.0 kB	X.509 Certificate	Mon
ca.crt	Desktop/ssl/generated	2.0 kB	X.509 Certificate	Mon

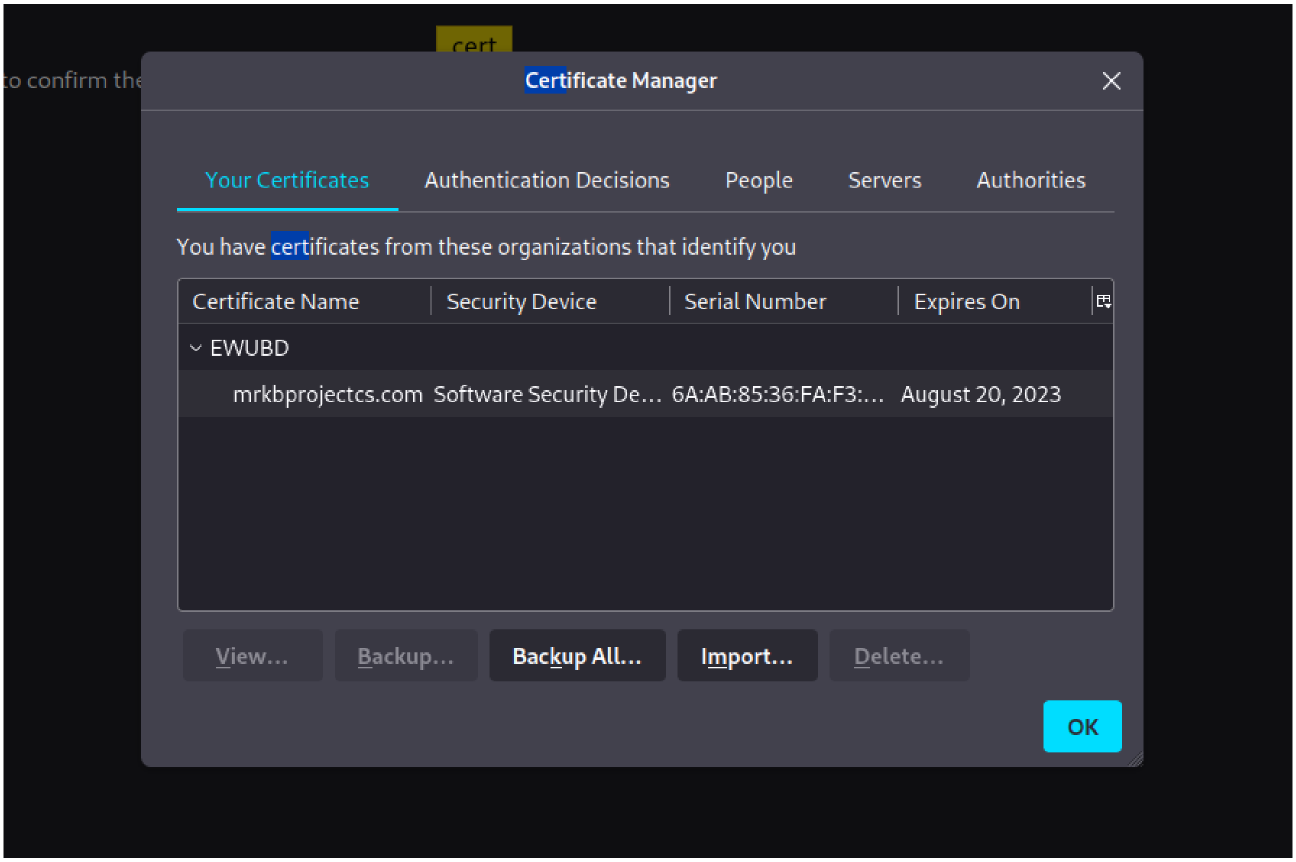


Certificate Manager

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
Entrust.net	
Entrust.net Premium 2048 Secure Serv…	Builtin Object Token
EWUBD	
subCA	Software Security Device
rootCA	Software Security Device
FNMT-RCM	

Our root-CA and sub-CA is successfully imported under the EWUBD.



You have certificates from these organizations that identify you

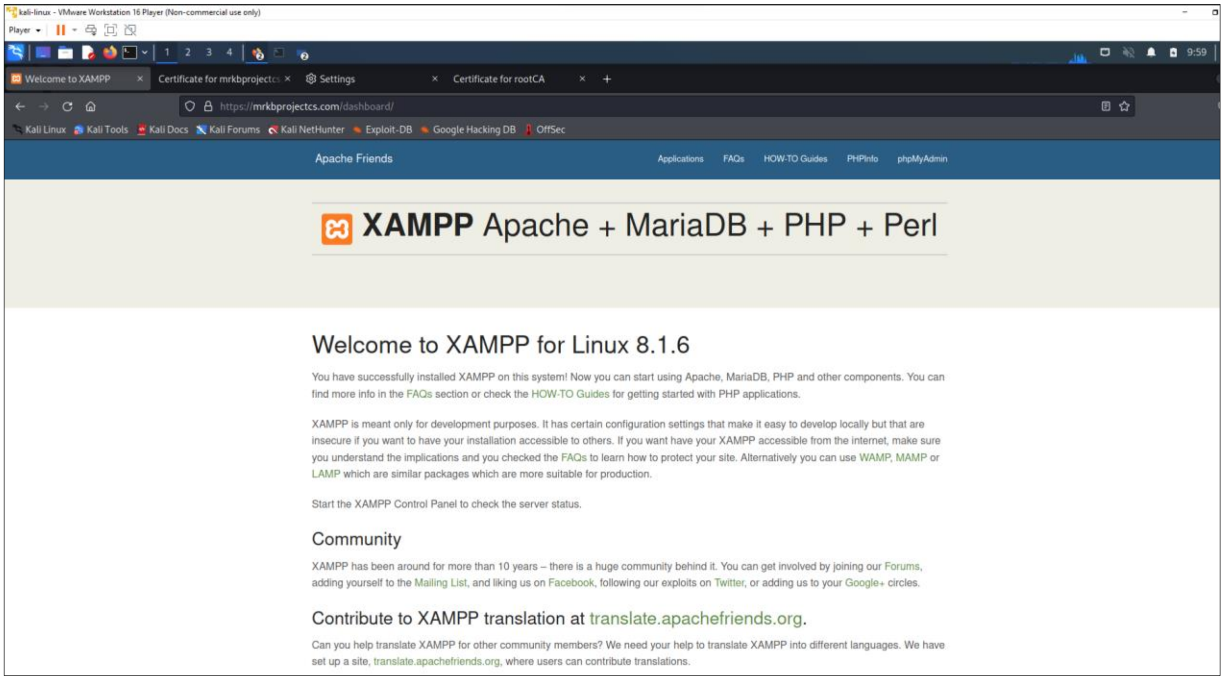
Certificate Name	Security Device	Serial Number	Expires On
EWUBD			
mrkbprojectcs.com	Software Security De…	6A:AB:85:36:FA:F3:…	August 20, 2023

Our server certificate is successfully imported under the EWUBD.

[P.T.O]

Now we refresh the Browser and search the “https://mrkbprojectcs.com”

Then finally we can see the server is on https connection with the padlock.



XAMPP Apache + MariaDB + PHP + Perl

Welcome to XAMPP for Linux 8.1.6

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others. If you want have your XAMPP accessible from the internet, make sure you understand the implications and you checked the FAQs to learn how to protect your site. Alternatively you can use WAMP, MAMP or LAMP which are similar packages which are more suitable for production.

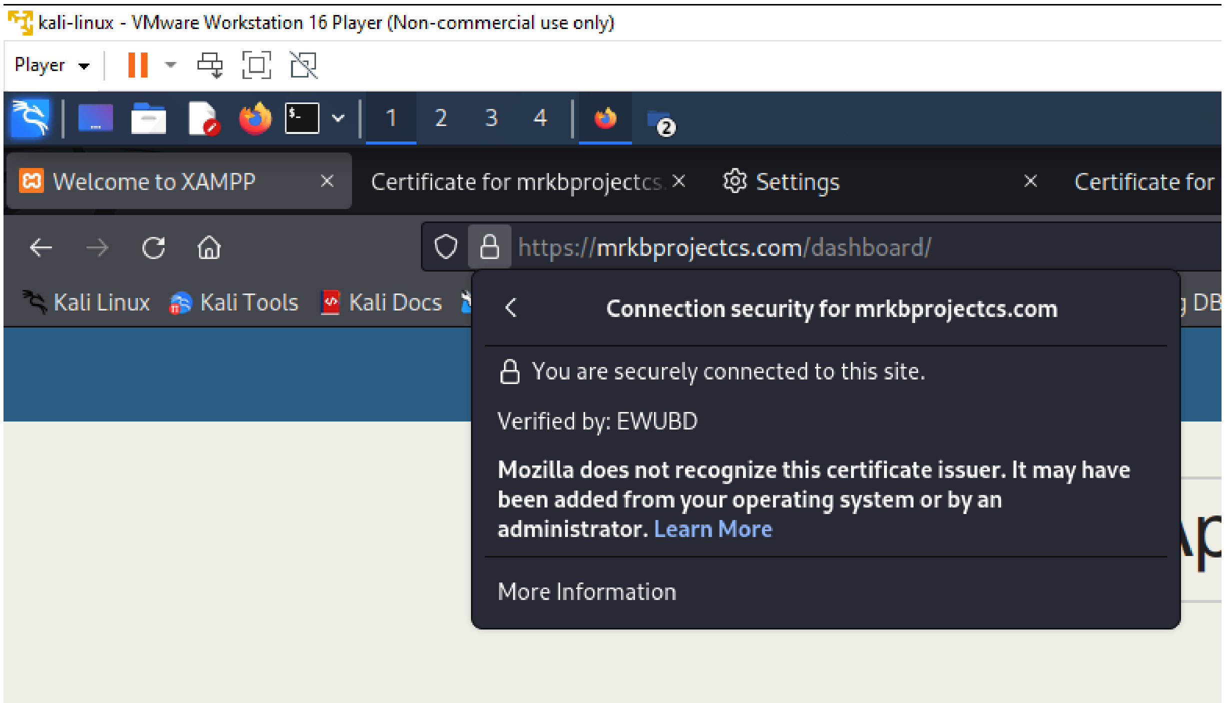
Start the XAMPP Control Panel to check the server status.

Community

XAMPP has been around for more than 10 years – there is a huge community behind it. You can get involved by joining our Forums, adding yourself to the Mailing List, and liking us on Facebook, following our exploits on Twitter, or adding us to your Google+ circles.

Contribute to XAMPP translation at translate.apachefriends.org.

Can you help translate XAMPP for other community members? We need your help to translate XAMPP into different languages. We have set up a site, translate.apachefriends.org, where users can contribute translations.


kali-linux - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
Welcome to XAMPP
Certificate for mrkbprojectcs
Settings
Certificate for
https://mrkbprojectcs.com/dashboard/
Kali Linux
Kali Tools
Kali Docs
DB

Connection security for mrkbprojectcs.com

You are securely connected to this site.

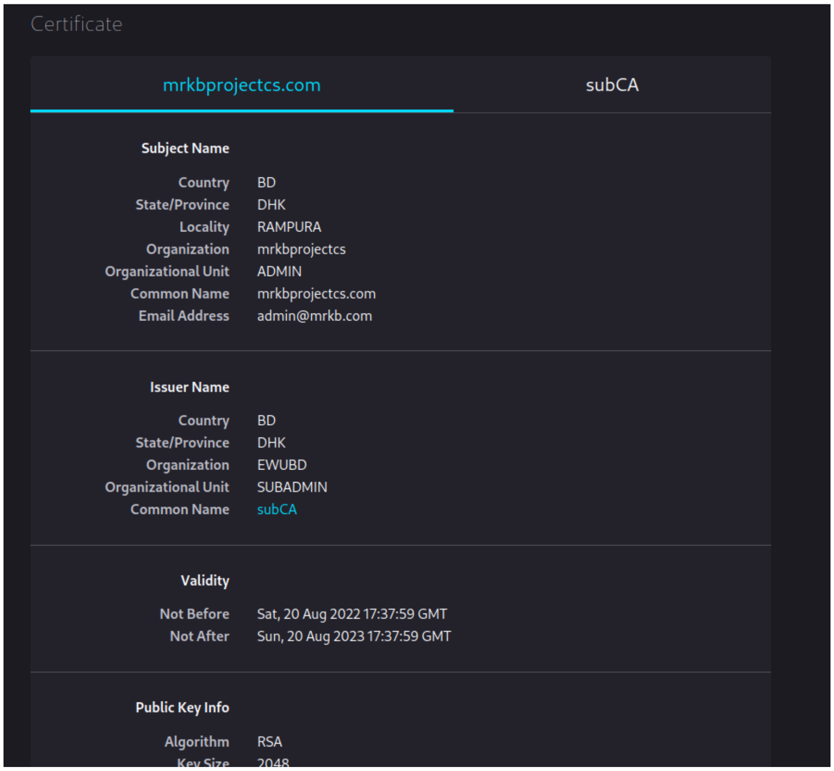
Verified by: EWUBD

Mozilla does not recognize this certificate issuer. It may have been added from your operating system or by an administrator. Learn More

More Information

The Connection is Secure.

We can see the certificate on the web server:



Subject Name

Country	BD
State/Province	DHK
Locality	RAMPURA
Organization	mrkbprojectcs
Organizational Unit	ADMIN
Common Name	mrkbprojectcs.com
Email Address	admin@mrkb.com

Issuer Name

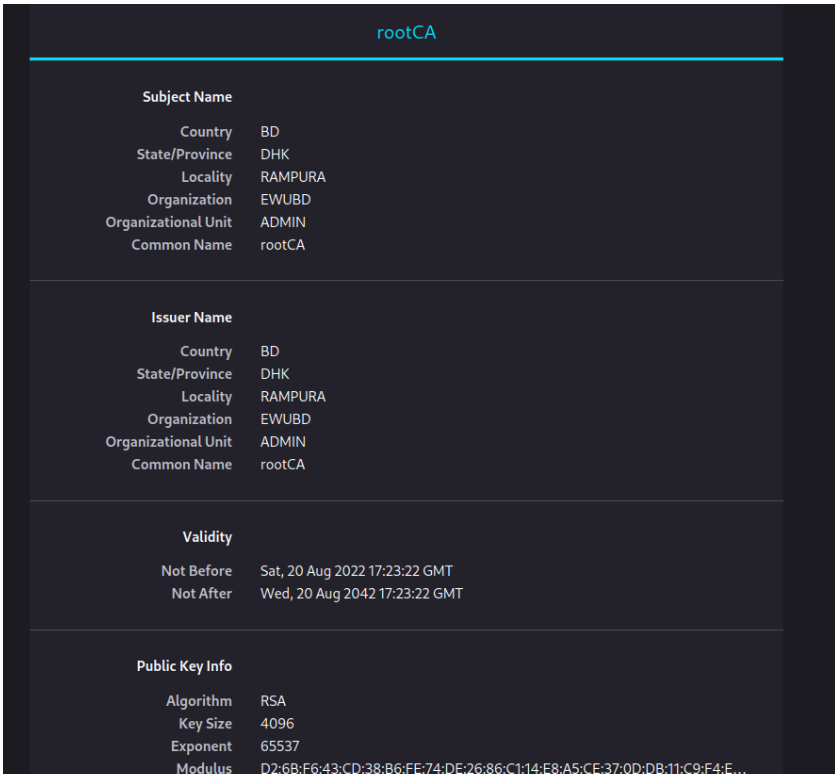
Country	BD
State/Province	DHK
Organization	EWUBD
Organizational Unit	SUBADMIN
Common Name	subCA

Validity

Not Before	Sat, 20 Aug 2022 17:37:59 GMT
Not After	Sun, 20 Aug 2023 17:37:59 GMT

Public Key Info

Algorithm	RSA
Key Size	2048



Subject Name

Country	BD
State/Province	DHK
Locality	RAMPURA
Organization	EWUBD
Organizational Unit	ADMIN
Common Name	rootCA

Issuer Name

Country	BD
State/Province	DHK
Locality	RAMPURA
Organization	EWUBD
Organizational Unit	ADMIN
Common Name	rootCA

Validity

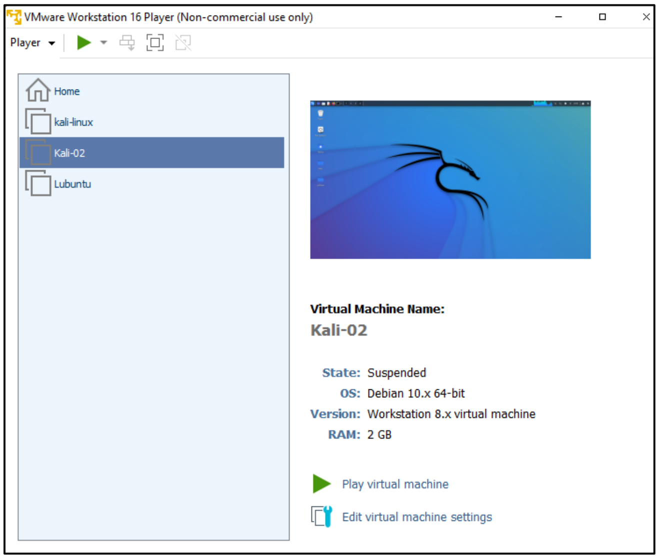
Not Before	Sat, 20 Aug 2022 17:23:22 GMT
Not After	Wed, 20 Aug 2042 17:23:22 GMT

Public Key Info

Algorithm	RSA
Key Size	4096
Exponent	65537
Modulus	D2:6B:F6:43:CD:38:B6:FE:74:DE:26:86:C1:14:E8:A5:CE:37:0D:DB:11:C9:F4:E...

Now we work for the client pc/os on the same virtual machine(VMware workstation):

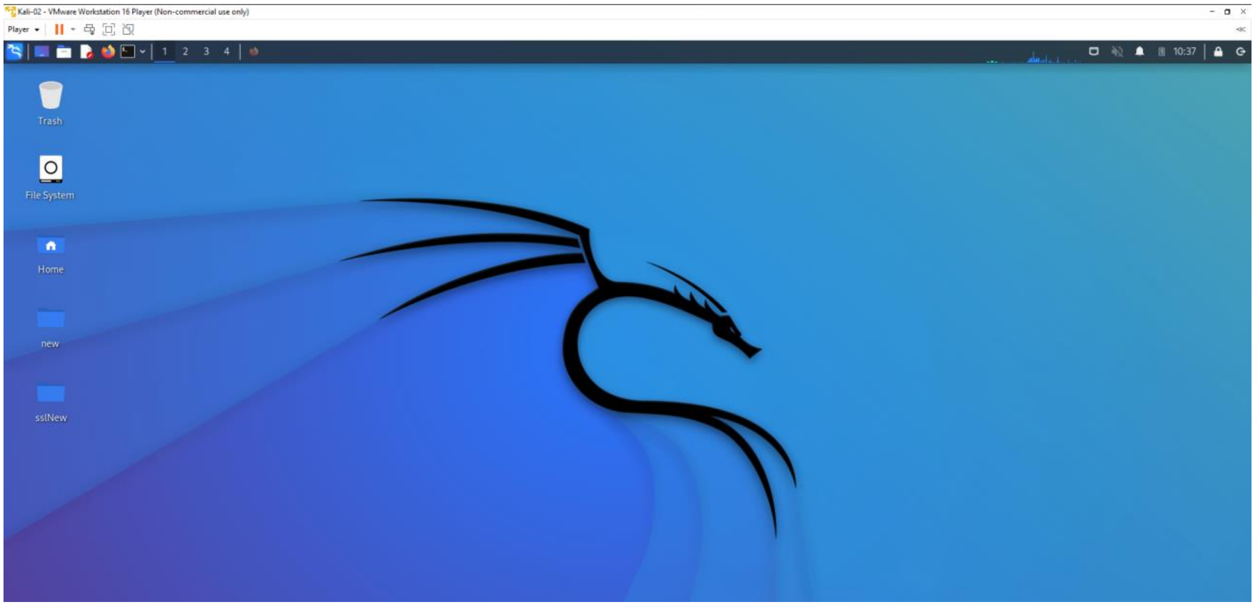
We install a Linux operating system for clienting named “Kali-02”


VMware Workstation 16 Player (Non-commercial use only)
Player
Home
kali-linux
Kali-02
Lubuntu
Play virtual machine
Edit virtual machine settings

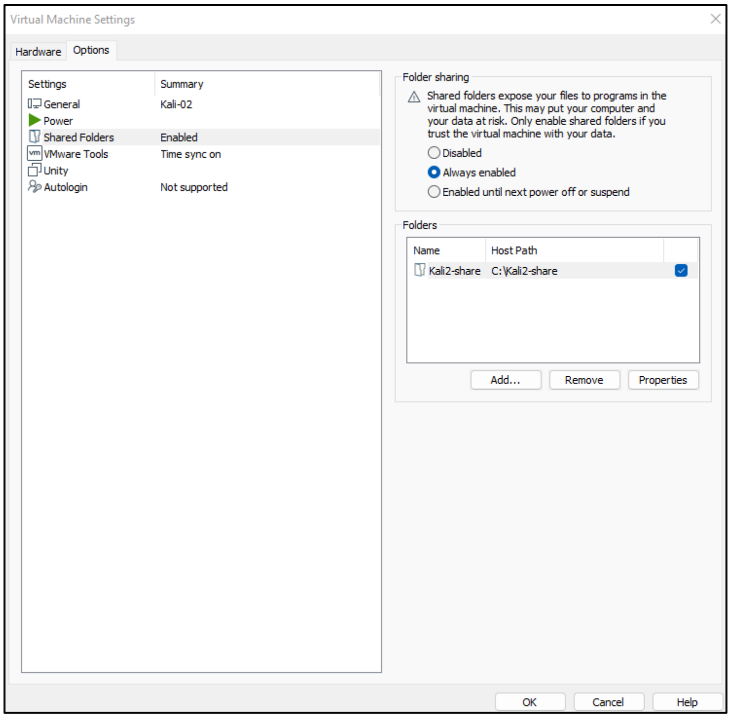
Virtual Machine Name:
Kali-02

State: Suspended
OS: Debian 10.x 64-bit
Version: Workstation 8.x virtual machine
RAM: 2 GB

This is our “Kali-02” Desktop view:


Kali-02 - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
10:37
Trash
File System
Home
new
sslNew

Then we create a shared folder so that we can have the SSL certificates from the host operating system “kali-Linux” to the “client operating system “Kali-02”.



Settings	Summary
General	Kali-02
Power	
Shared Folders	Enabled
VMware Tools	Time sync on
Unity	
Autologin	Not supported

Folder sharing

⚠ Shared folders expose your files to programs in the virtual machine. This may put your computer and your data at risk. Only enable shared folders if you trust the virtual machine with your data.

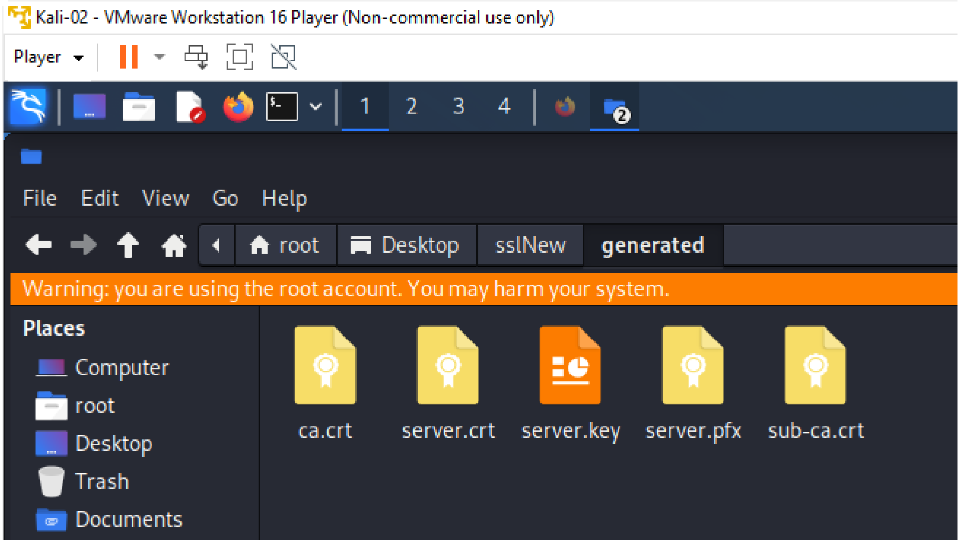
○ Disabled
● Always enabled
○ Enabled until next power off or suspend

Folders

Name	Host Path	
Kali2-share	C:\Kali2-share	☑

Creating shared folder with the help of the windows host machine for Bidirectional file sharing.

We copy the SSL certificates to the client OS Desktop > sslNew > generated:

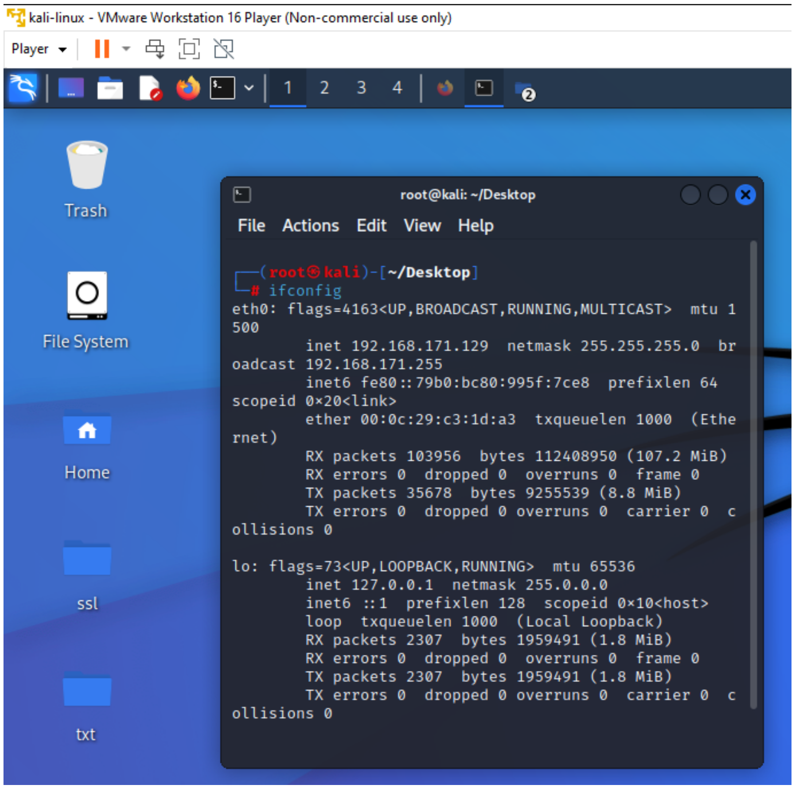


root Desktop sslNew generated

Warning: you are using the root account. You may harm your system.

ca.crt server.crt server.key server.pfx sub-ca.crt

Now we can have the (mrkbprojectcs.com) host server’s network(ip) address by command “ifconfig” on Kali-Linux (host) OS:


kali-linux - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
Trash
File System
Home
ssl
txt
root@kali: ~/Desktop
File Actions Edit View Help

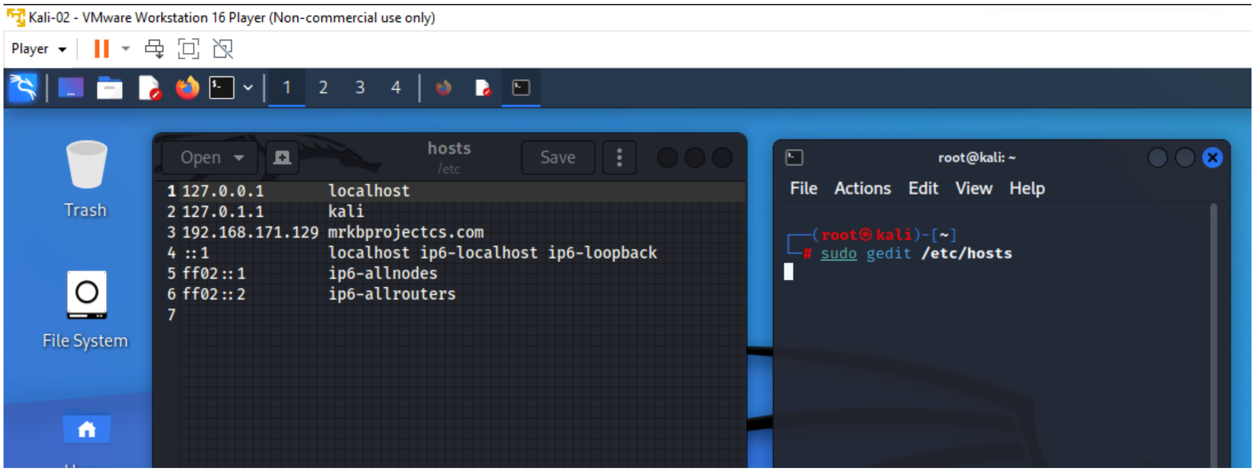
```
┌──(root㉿kali)-[~/Desktop]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1
500
        inet 192.168.171.129  netmask 255.255.255.0  br
oadcast 192.168.171.255
        inet6 fe80::79b0:bc80:995f:7ce8  prefixlen 64
scopeid 0×20<link>
        ether 00:0c:29:c3:1d:a3  txqueuelen 1000  (Ethe
rnet)
        RX packets 103956  bytes 112408950 (107.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35678  bytes 9255539 (8.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  c
ollisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2307  bytes 1959491 (1.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2307  bytes 1959491 (1.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  c
ollisions 0
```

The ip address is : 192.168.171.129

Now we open terminal on client OS (Kali-02) Desktop and do command “sudo gedit /etc/hosts”

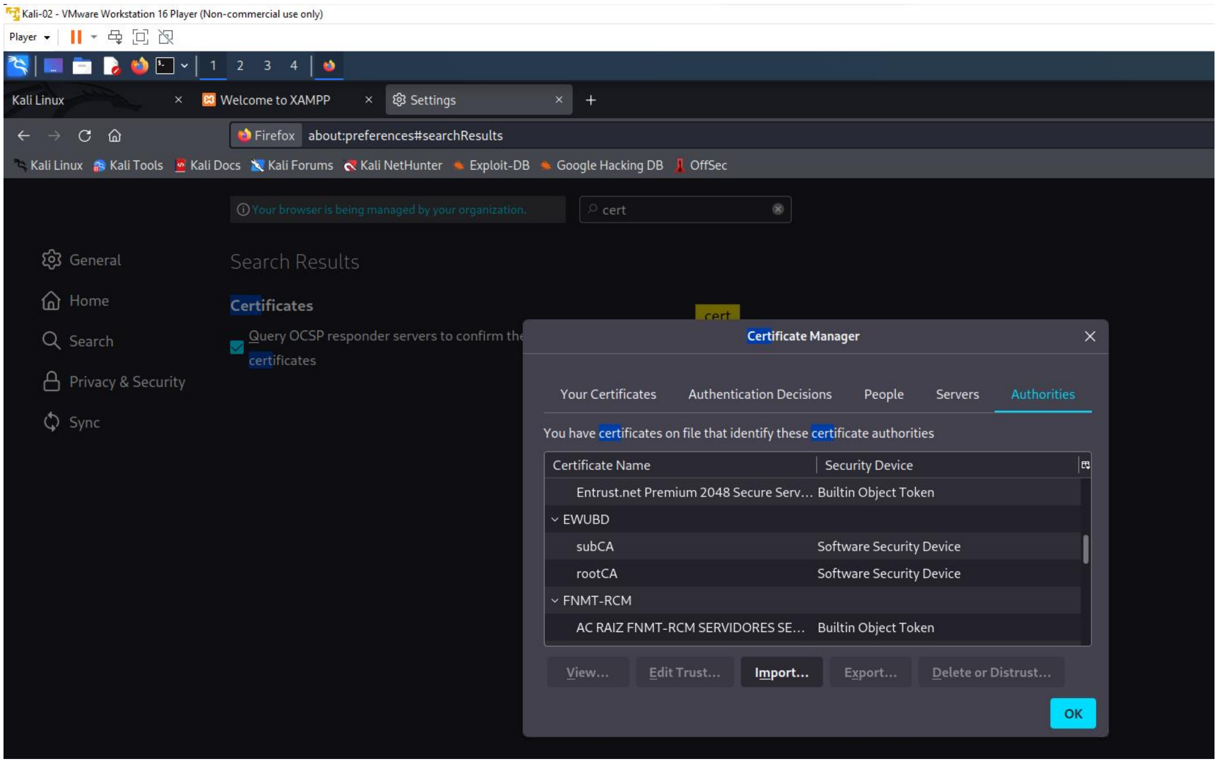
So the host file open-up and we assign the ip and our webserver name and save it.


Kali-02 - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
Trash
File System
Open
hosts
/etc
Save
root@kali: ~
File Actions Edit View Help

```
127.0.0.1       localhost
127.0.1.1       kali
192.168.171.129 mrkbprojectcs.com
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
```

```
┌──(root㉿kali)-[~]
└─# sudo gedit /etc/hosts
```

After that we import the copied SSL certificate to the Browser as same procedure of the host OS browser.



Your browser is being managed by your organization.

Search Results

Certificates

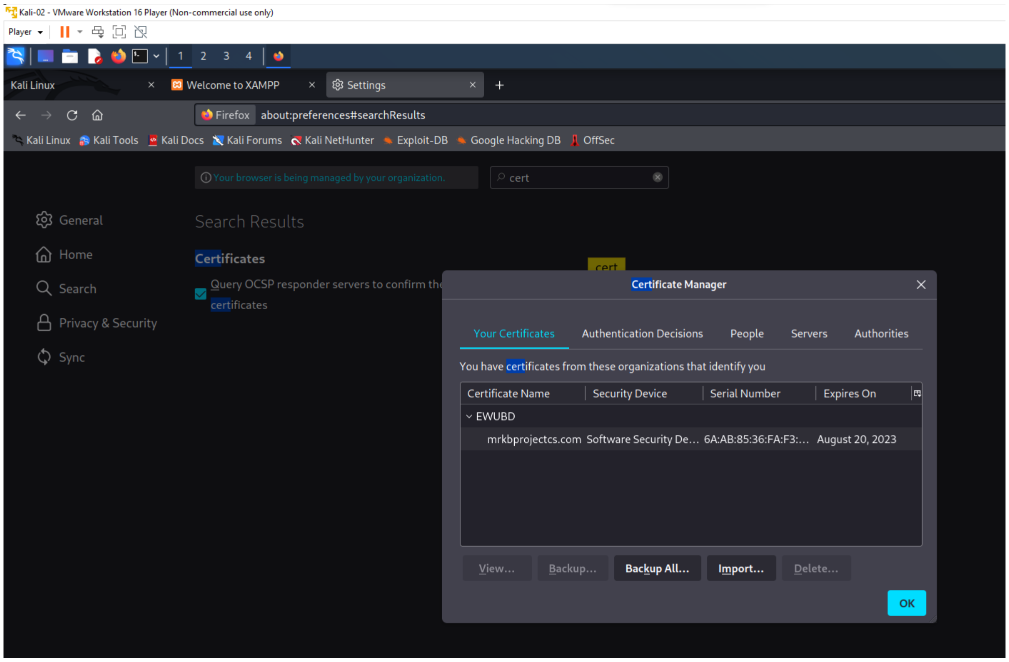
☑ Query OCSP responder servers to confirm the current validity of certificates

Certificate Manager

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
Entrust.net Premium 2048 Secure Serv…	Builtin Object Token
⌄ EWUBD	
subCA	Software Security Device
rootCA	Software Security Device
⌄ FNMT-RCM	
AC RAIZ FNMT-RCM SERVIDORES SE…	Builtin Object Token

Imported Root-CA and sub-CA.



Your browser is being managed by your organization.

Search Results

Certificates

☑ Query OCSP responder servers to confirm the current validity of certificates

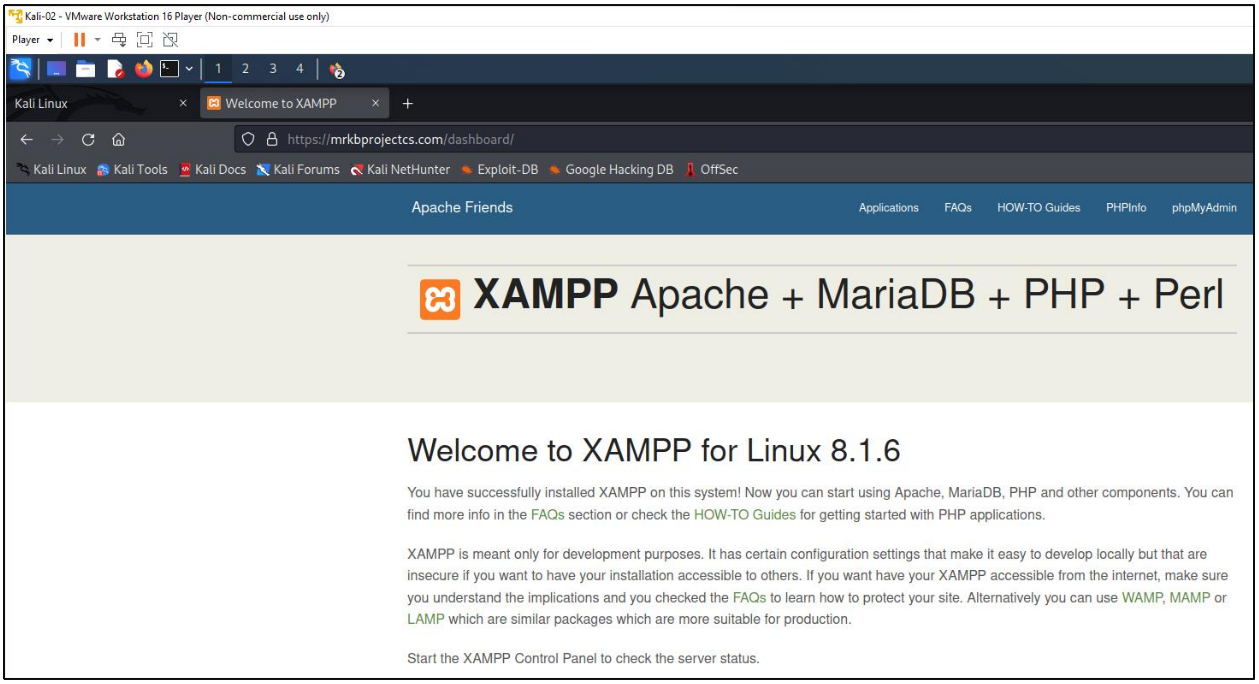
Certificate Manager

You have certificates from these organizations that identify you

Certificate Name	Security Device	Serial Number	Expires On
⌄ EWUBD			
mrkbprojectcs.com	Software Security De…	6A:AB:85:36:FA:F3:…	August 20, 2023

Imported the server-Certificate.

Now we search the webserver name on the browser and see the https connection with the padlock.


Kali-02 - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
Kali Linux
Welcome to XAMPP
https://mrkbprojectcs.com/dashboard/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Apache Friends
Applications FAQs HOW-TO Guides PHPInfo phpMyAdmin

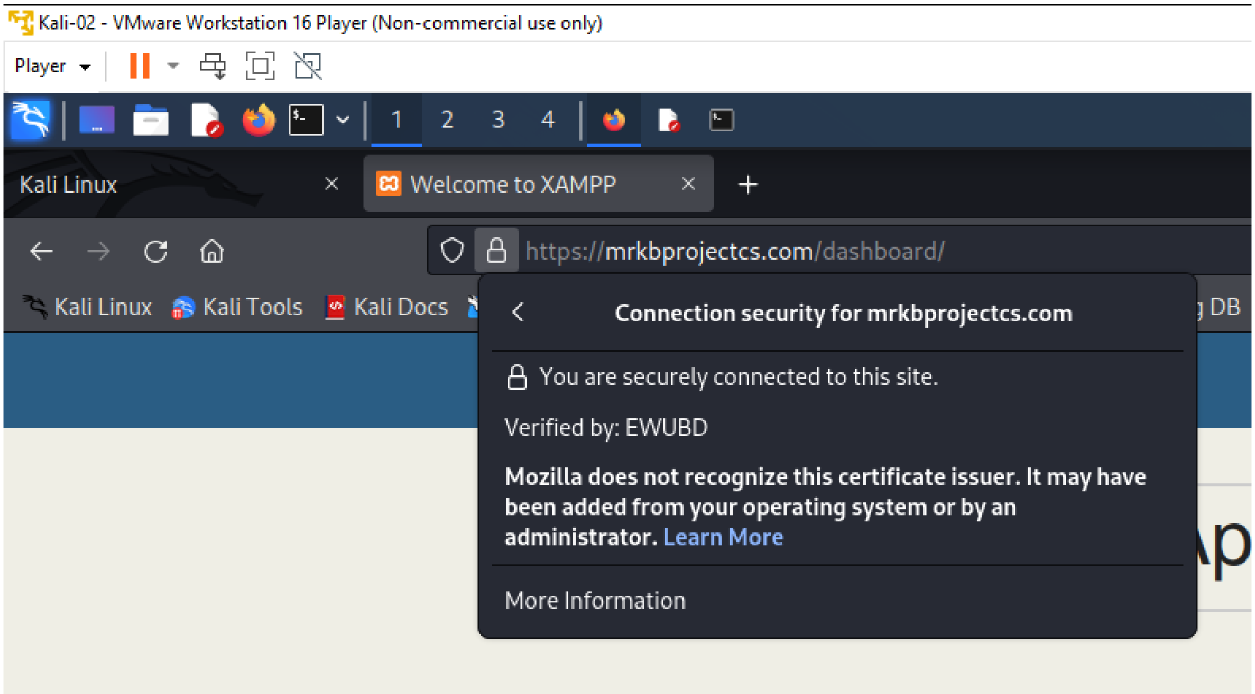
XAMPP Apache + MariaDB + PHP + Perl

Welcome to XAMPP for Linux 8.1.6

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others. If you want have your XAMPP accessible from the internet, make sure you understand the implications and you checked the FAQs to learn how to protect your site. Alternatively you can use WAMP, MAMP or LAMP which are similar packages which are more suitable for production.

Start the XAMPP Control Panel to check the server status.


Kali-02 - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
Kali Linux
Welcome to XAMPP
https://mrkbprojectcs.com/dashboard/
Kali Linux Kali Tools Kali Docs
DB

Connection security for mrkbprojectcs.com

You are securely connected to this site.

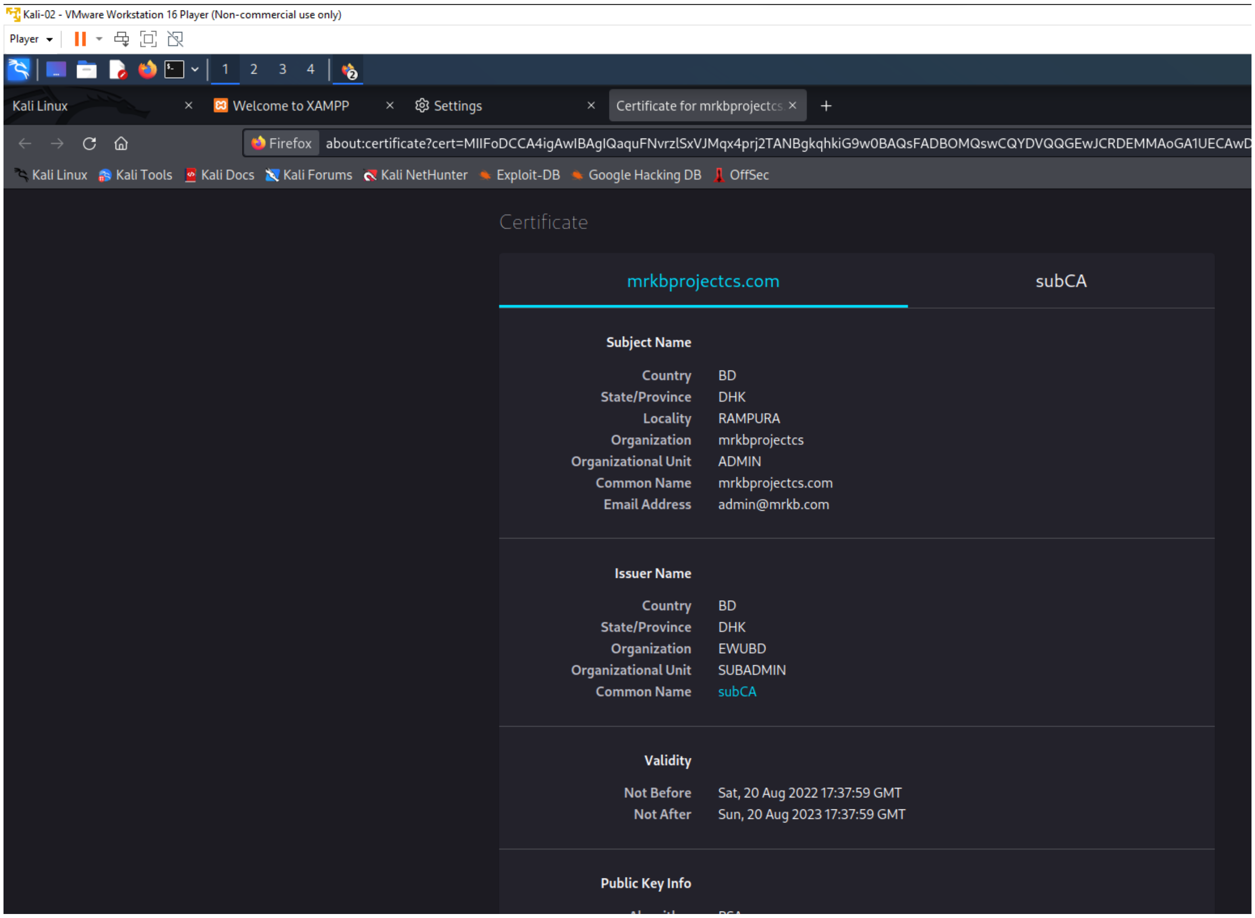
Verified by: EWUBD

Mozilla does not recognize this certificate issuer. It may have been added from your operating system or by an administrator. Learn More

More Information

The connection is secure.

We can see the Certificate also on the client Host server.



about:certificate?cert=MIIFoDCCA4igAwIBAgIQaquFNvrzlSxVJMqx4prj2TANBgkqhkiG9w0BAQsFADBOMQswCQYDVQQGEwJCRDEMMAoGA1UECAwD

Certificate

mrkbprojectcs.com | subCA

Subject Name

Country	BD
State/Province	DHK
Locality	RAMPURA
Organization	mrkbprojectcs
Organizational Unit	ADMIN
Common Name	mrkbprojectcs.com
Email Address	admin@mrkb.com

Issuer Name

Country	BD
State/Province	DHK
Organization	EWUBD
Organizational Unit	SUBADMIN
Common Name	subCA

Validity

Not Before	Sat, 20 Aug 2022 17:37:59 GMT
Not After	Sun, 20 Aug 2023 17:37:59 GMT

Public Key Info

THE END