EAST WEST UNIVERSITY

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

Group - 315

CSE487: Cybersecurity, Law and Ethics

Sec-03

Submitted to:

Rashedul Amin Tuhin

Senior Lecturer, Assistant Proctor

Department of Computer Science & Engineering

East West University

Submitted by:

Malyha Bintha Mabud-------2019-1-60-128

Humaira Anan Neela-------2019-1-60-218

Submission Date: 25/08/2022

Installation of XAMPP in Kali Linux:

First, we need to install apache server to Kali. For that we need to install XAMPP.

• Download XAMPP, then launch the terminal, navigate to the installation folder, and run. A procedure of installation will begin.

• After creating a web page, we'll try to host it within the same local area network (LAN). Verify if you have access to it..

•Go to the browser and type "Localhost" to see if the Apache server is operating.

•We require the IP address or default gateway in order to visit the web server. To do so, enter the command "sudo apt get installed net-tools" in the terminal. Get the IP by typing "ifconfig" right away.

•After browsing the IP address in the window, we can observe that the web server is also being run by Windows.

•We may use the ip address to visit the web server within the LAN as long as Linux is turned on..

Configuring Certificates with OpenSSL:

- For generating openssl certificate we need to login as root user to our Kali operating system and write the below command on the terminal:

```
echo "\n\n_____GENERATING ALL DIRECTORIES_____\n\n"

gr='\033[1;32m'

nc='\033[0m' # No Color


mkdir -p {root-ca,sub-ca,server}/{private,certs,index,serial,pem,crl,csr}

mkdir generated

touch root-ca/index/index

touch sub-ca/index/index

openssl rand -hex 16 > root-ca/serial/serial

openssl rand -hex 16 > sub-ca/serial/serial

cp root-ca.conf root-ca

cp sub-ca.conf sub-ca

echo "${gr}\n ================ FOLDERS CREATED SUCCESSFULLY ================ \n${nc}"
```

```
echo "\n\n_____GENERATING ALL THE KEYS_____\n\n"

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

echo "${gr}\n ================ KEYS CREATED SUCCESSFULLY ================ \n${nc}"

echo "\n\n_____GENERATING ROOT CERTIFICATE_____\n\n"

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

echo "${gr}\n ================ ROOT CERTIFICATE CREATED SUCCESSFULLY ================ \n${nc}"

echo "\n\n_____GENERATING SUB-ROOT REQUEST_____\n\n"

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

echo "${gr}\n ================ SUB-ROOT REQUEST CREATED SUCCESSFULLY ================ \n${nc}"

echo "\n\n_____GENERATING SUB-ROOT CERTIFICATE_____\n\n"

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

echo "${gr}\n ================ SUB-ROOT CERTIFICATE CREATED SUCCESSFULLY ================ \n${nc}"

echo "\n\n_____GENERATING SERVER REQUEST_____\n\n"

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

echo "${gr}\n ================ SERVER REQUEST CREATED SUCCESSFULLY ================ \n${nc}"

echo "\n\n_____GENERATING SERVER CERTIFICATE_____\n\n"

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

echo "${gr}\n ================ SERVER CERTIFICATE CREATED SUCCESSFULLY ================ \n${nc}"

echo "\n\n_____GATHERING NECESSARY FILES_____\n\n"

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

echo "${gr}\n ================ SUCCESSFULLY GATHERED ================ \n${nc}"

echo "\n\n_____CREATING HOST ENTRY_____\n\n"

echo -n "Server CommonName: "

read commonName

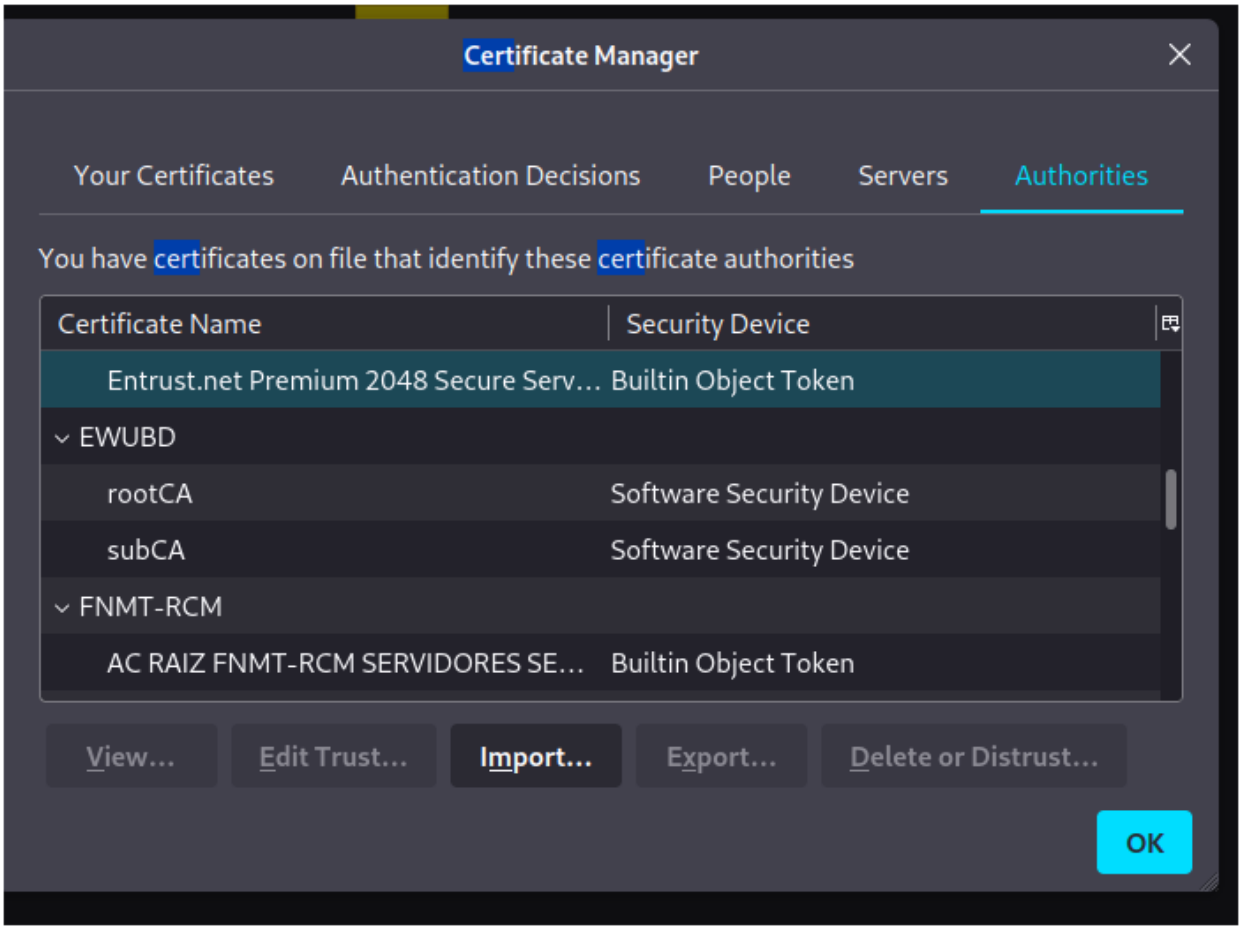
echo "127.0.0.1 "$commonName >> /etc/hosts

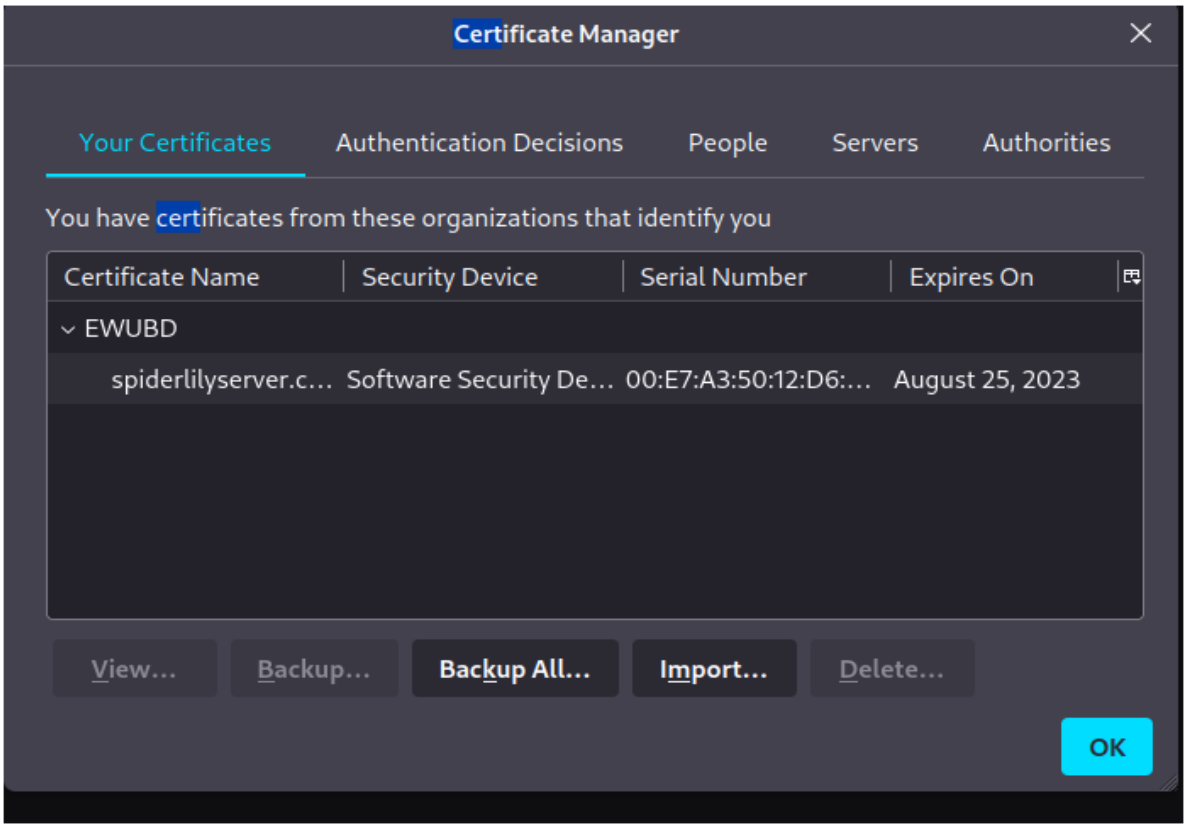
echo "${gr}\n ================ SUCCESSFULLY APPENDED HOST ================ \n${nc}"

- After generating this command, we can see the certs files on our generated folder. We generated our server name as https://spiderlilyserver.com.

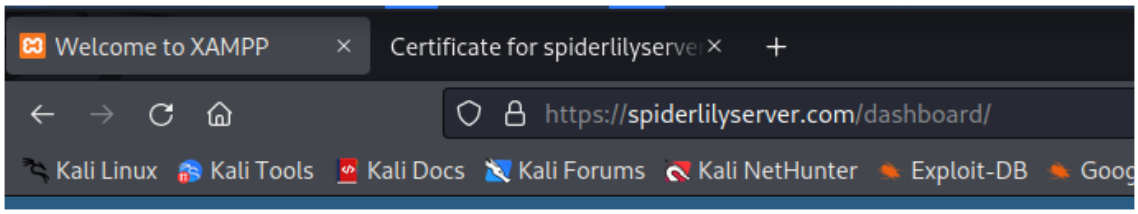
- Then we have to install our certificates in our XAMPP. For this first we have to start our XAMPP:
  cd opt /lamp
  ./manager-linux-x64.run
- The go to this file and edits the httpd-ssl.conf file:
  File system ->opt -> lamp -> etc-> extra-> http-ssl.conf

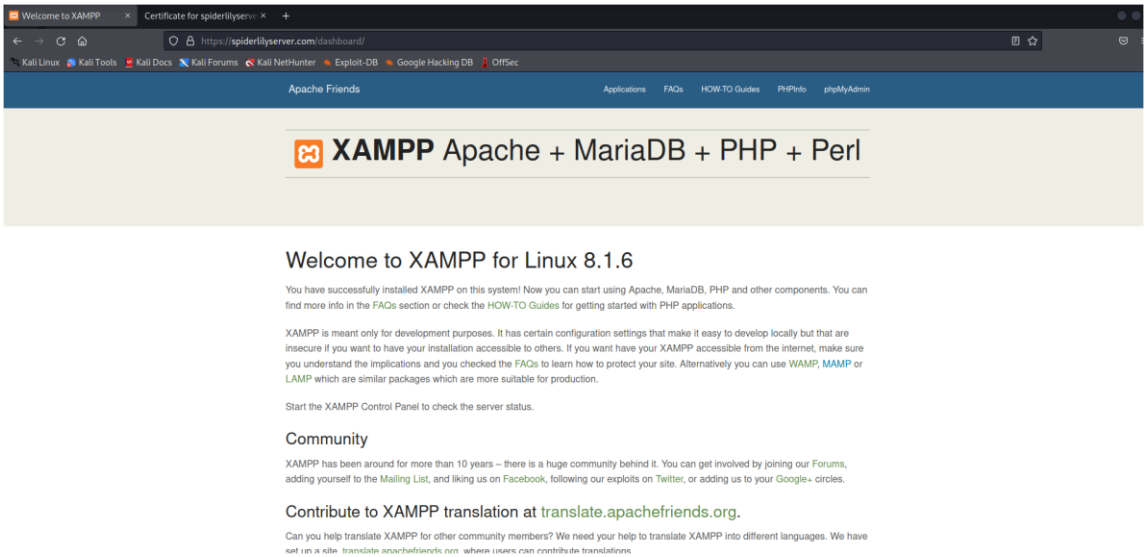
- Then copy the location of spiderlilyserver.com.pem then go to the word editor and edit the SSLCertificateFile location.
- Then copy the path of server.cert file SSLCACertificate "/home/neela/desktop/certs" and save the file.
- Then restart the xampp.
- Then type https://locathost in the browser then in the settings import the rootCA, subCA and server(spiderlilyserver.com) certificates.



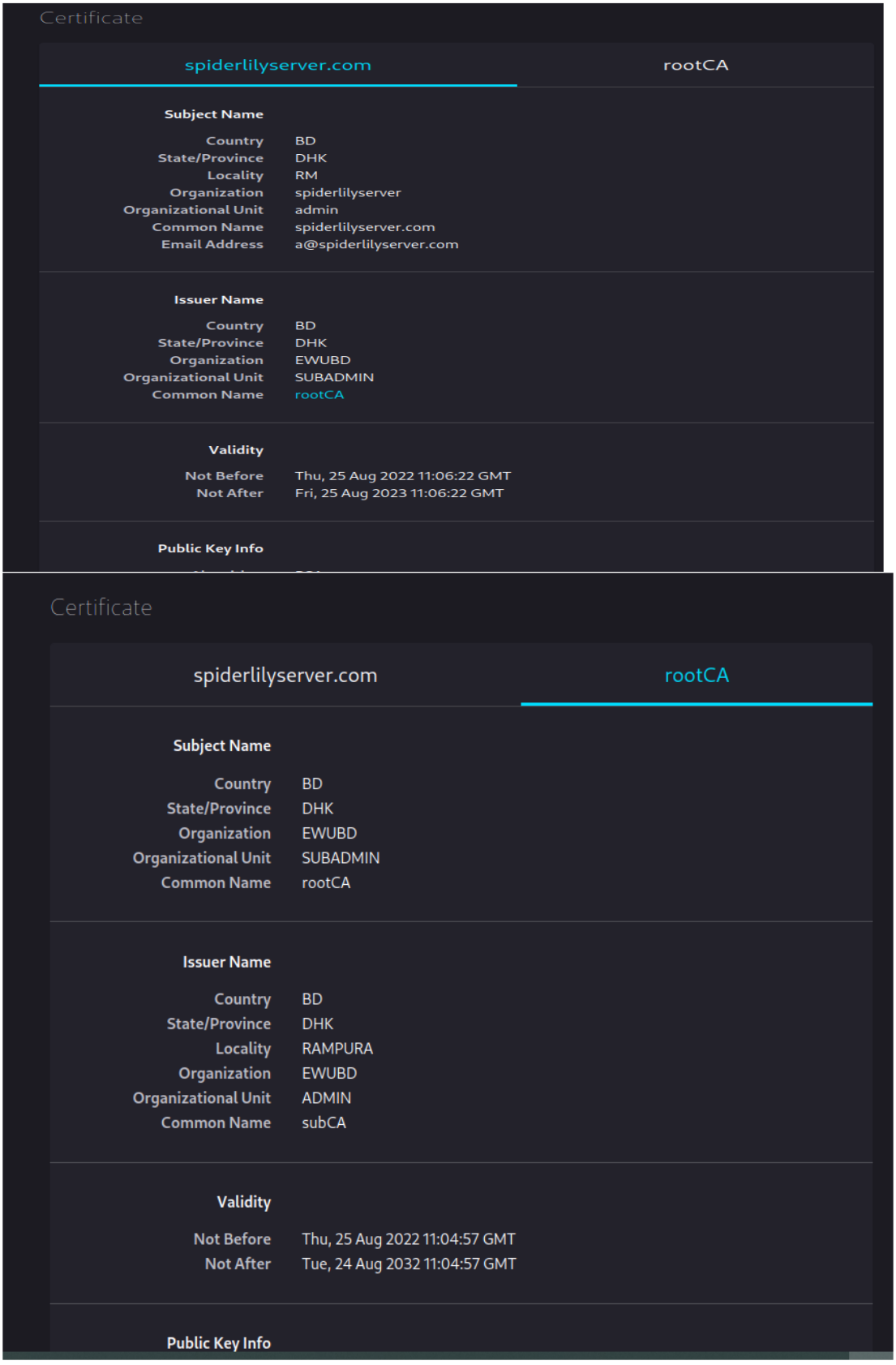


- Restart the browser and type https://spiderlily.com and we have the secured website with the padlock as we wanted.



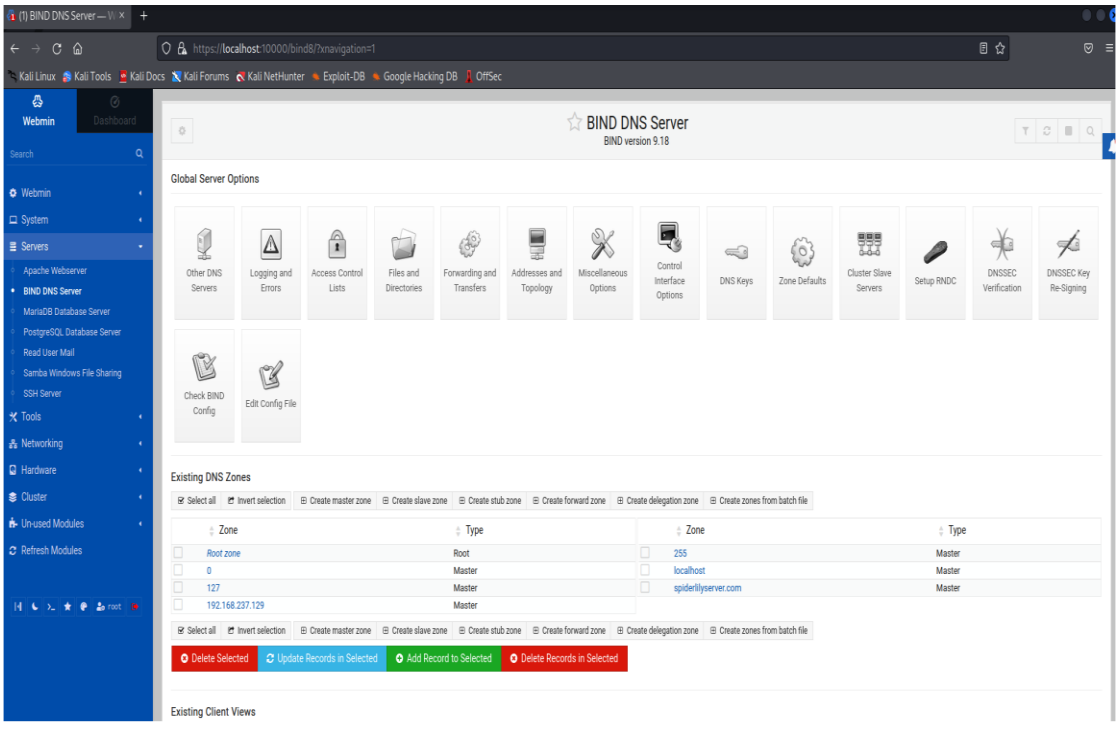


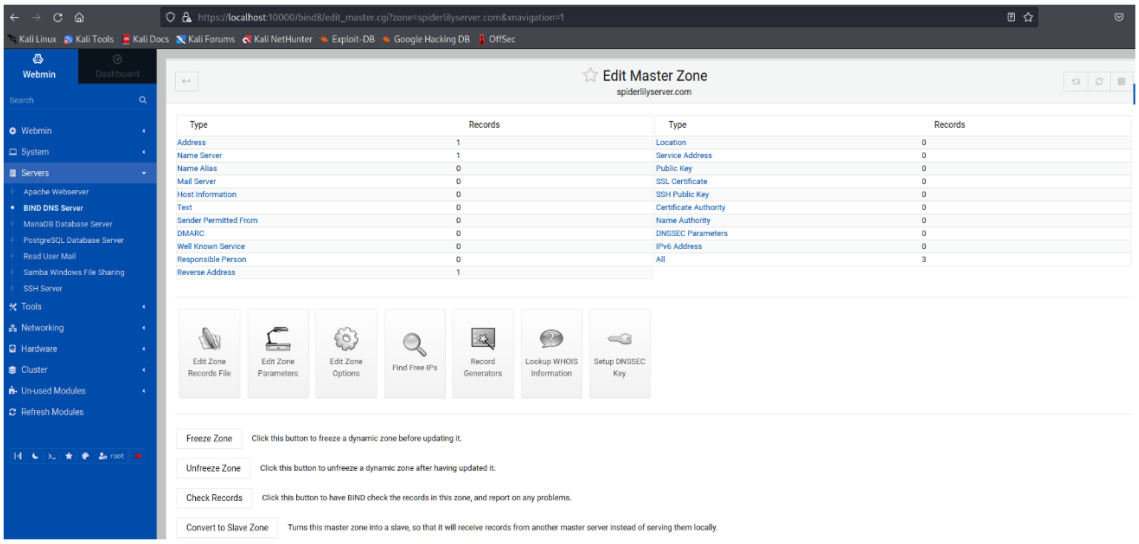
- And the certificate of our secured server.



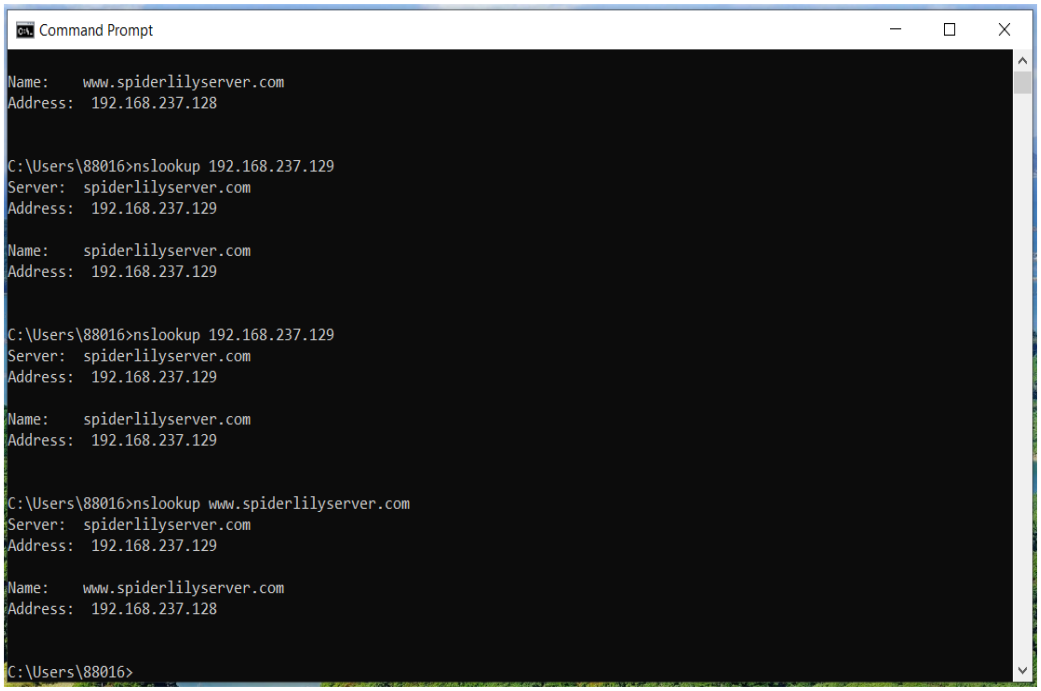
Installing DNS server in Kali using webmin(GUI of bind9):

- We have to open another Kali on VMware.
- sudo apt update
- sudo apt-get install open-vm-tools-desktop
- reboot
- sudo apt install kali-root-login
- sudo passwd
- ----------#switch user
- ----------#webmin installation
- sudo nano /etc/apt/sources.list
- ----------#add this line
- deb http://download.webmin.com/download/repository sarge contrib
-
- wget -q -O- http://www.webmin.com/jcameron-key.asc | sudo apt-key add
- sudo apt update
- sudo apt install webmin
- sudo ufw allow 10000
- sudo cd /usr/lib/systemd/system
- sudo cp named.service bind9.service
- Then configure the ip addresses with the command “ipconfig” of our Xampp, DNS and Windows.





- Then we can check the forward and reverse addresses from the windows with the “nslookup”.We will get the same ip address.


Command Prompt
Name: www.spiderlilyserver.com
Address: 192.168.237.128
C:\Users\88016>nslookup 192.168.237.129
Server: spiderlilyserver.com
Address: 192.168.237.129
Name: spiderlilyserver.com
Address: 192.168.237.129
C:\Users\88016>nslookup 192.168.237.129
Server: spiderlilyserver.com
Address: 192.168.237.129
Name: spiderlilyserver.com
Address: 192.168.237.129
C:\Users\88016>nslookup www.spiderlilyserver.com
Server: spiderlilyserver.com
Address: 192.168.237.129
Name: www.spiderlilyserver.com
Address: 192.168.237.128
C:\Users\88016>