EAST WEST UNIVERSITY

Mini Project

Department of Computer Science & Engineering

Course Name: **Computer & Cybersecurity**

Course Code: **CSE487**

Section No: **01**

Submitted To

Rashedul Amin Tuhin

Senior Lecturer, Assistant Proctor

Department of Computer Science & Engineering

Submitted by

Student's Name	**Student's ID**
Nabila Naz Ameen	2019-1-60-038
Ishrat Jahan	2019-1-60-039
Talha Rahman	2019-1-60-044

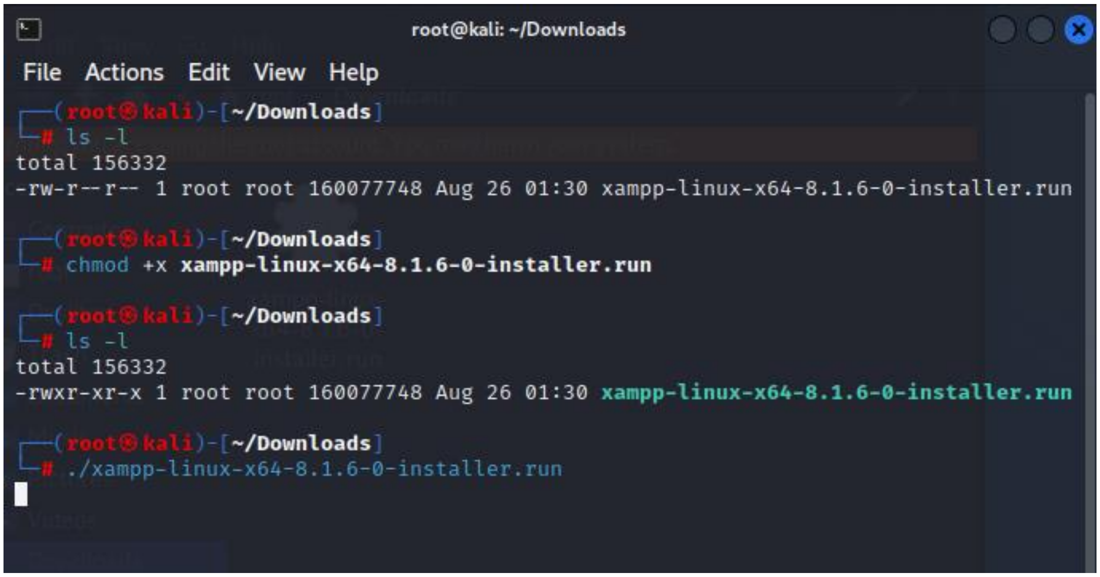
Date of Submission: **25th August, 2022**

<u>Installation of XAMPP:</u>

- If Apache2 sever is already installed then it needs to be uninstalled by using the **Command Line:** "sudo apt purge apache2".If Apache2 is not in the machine then no need to execute the command line.
- Download XAMPP from https://www.apachefriends.org/download.html.
- To install XAMPP go to the downloads and open terminal there and execute some necessary commands. After that the installation process will start.
- **Command Lines:** "ls -l"

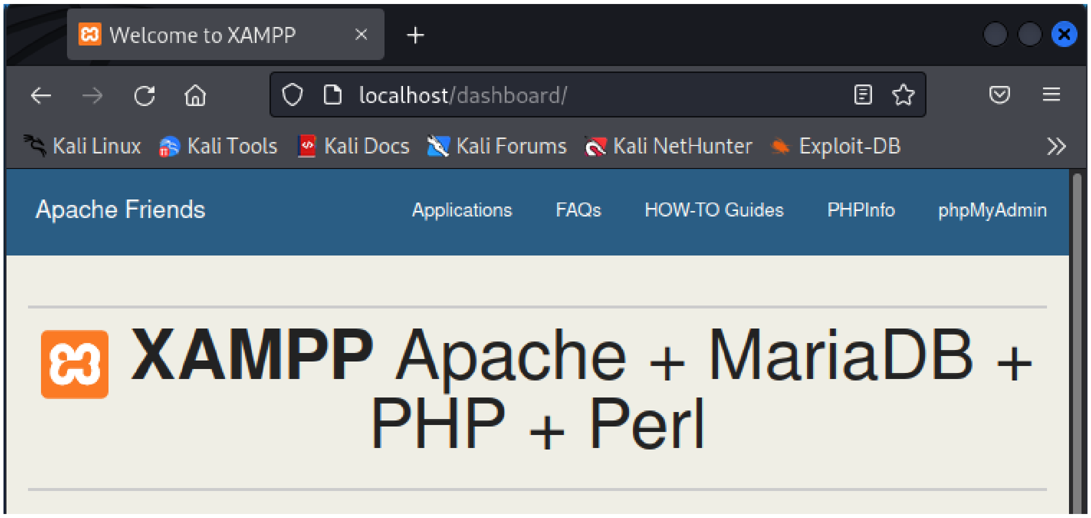
  "chmod +x xampp-linux-x64-8.1.6-0-installer.run"

  "./xampp-linux-x64-8.1.6-0-installer.run"



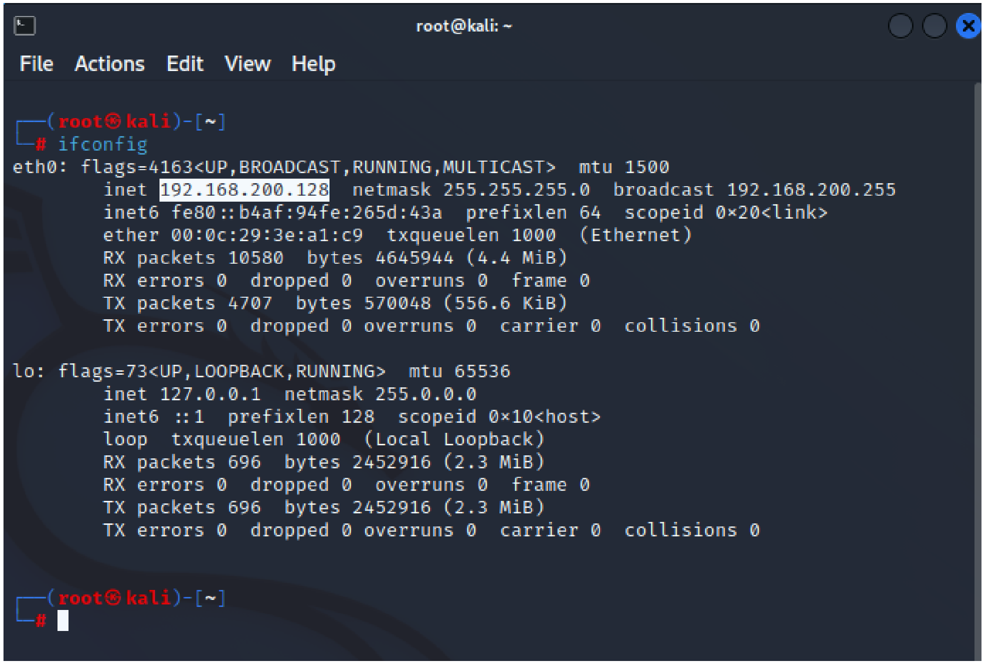
```
┌──(root㉿kali)-[~/Downloads]
└─# ls -l
total 156332
-rw-r--r-- 1 root root 160077748 Aug 26 01:30 xampp-linux-x64-8.1.6-0-installer.run

┌──(root㉿kali)-[~/Downloads]
└─# chmod +x xampp-linux-x64-8.1.6-0-installer.run

┌──(root㉿kali)-[~/Downloads]
└─# ls -l
total 156332
-rwxr-xr-x 1 root root 160077748 Aug 26 01:30 xampp-linux-x64-8.1.6-0-installer.run

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

- To check the Apache2 sever is running go to the browser and type "localhost".



XAMPP Apache + MariaDB + PHP + Perl

- To view the web server from windows, it is necessary to know the IP or default getway of the webserver.
  Command Lines: “sudo apt-get install net-tools”
  “ifconfig”

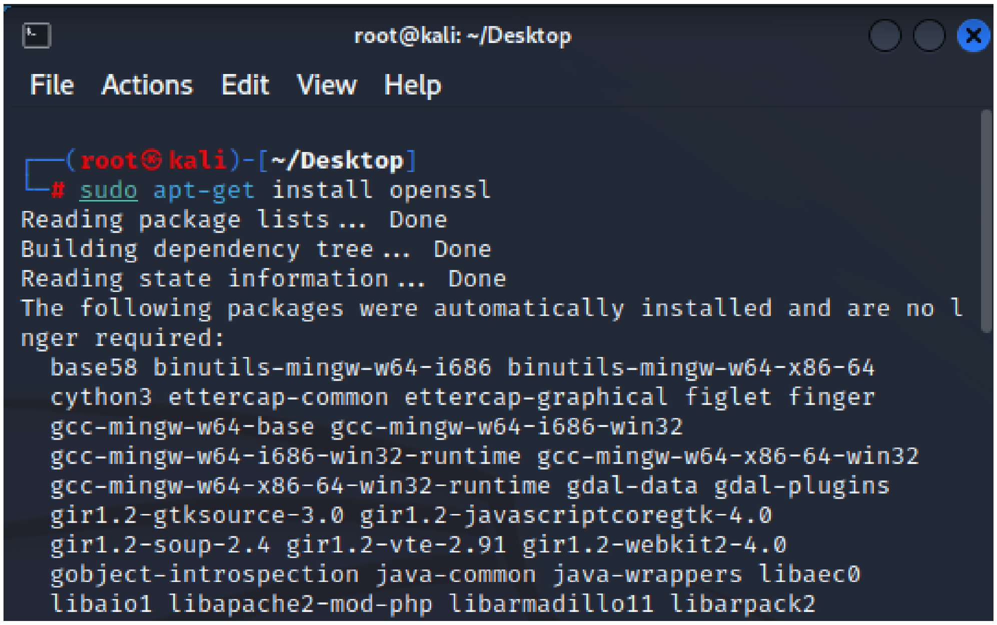


```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.200.128  netmask 255.255.255.0  broadcast 192.168.200.255
        inet6 fe80::b4af:94fe:265d:43a  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:3e:a1:c9  txqueuelen 1000  (Ethernet)
        RX packets 10580  bytes 4645944 (4.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4707  bytes 570048 (556.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 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 696  bytes 2452916 (2.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 696  bytes 2452916 (2.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
└─# 
```

Installation of Openssl:

To get Openssl we need to type a command on terminal:

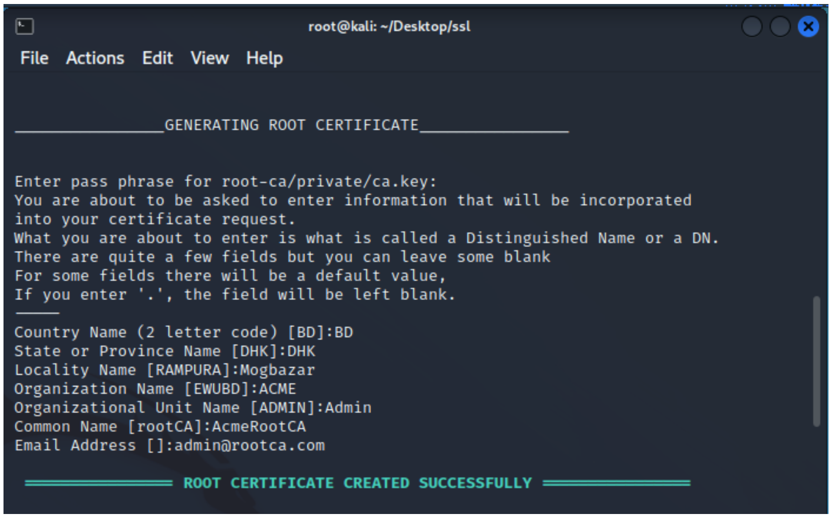
Command Line: “sudo apt-get install openssl”



```
┌──(root㉿kali)-[~/Desktop]
└─# sudo apt-get install openssl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no l
nger required:
  base58 binutils-mingw-w64-i686 binutils-mingw-w64-x86-64
  cython3 ettercap-common ettercap-graphical figlet finger
  gcc-mingw-w64-base gcc-mingw-w64-i686-win32
  gcc-mingw-w64-i686-win32-runtime gcc-mingw-w64-x86-64-win32
  gcc-mingw-w64-x86-64-win32-runtime gdal-data gdal-plugins
  gir1.2-gtksource-3.0 gir1.2-javascriptcoregtk-4.0
  gir1.2-soup-2.4 gir1.2-vte-2.91 gir1.2-webkit2-4.0
  gobject-introspection java-common java-wrappers libaec0
  libaio1 libapache2-mod-php libarmadillo11 libarpack2
```

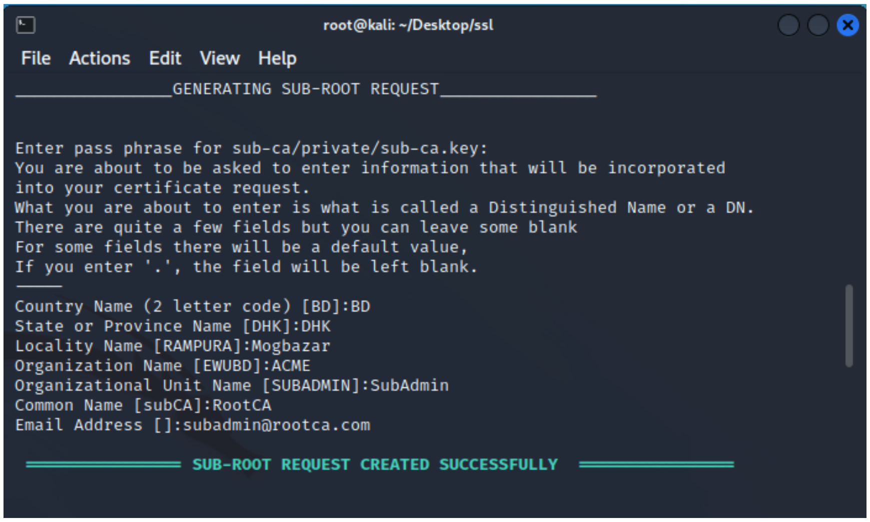
Generating the Certificates:

- Creating a file named “ssl” to keep the newly generated certificates. Open the terminal on Desktop>ssl.
- Generating **RootCA Certificate** named as “AcmeRootCA” using the command line below.
  Command Line: “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”

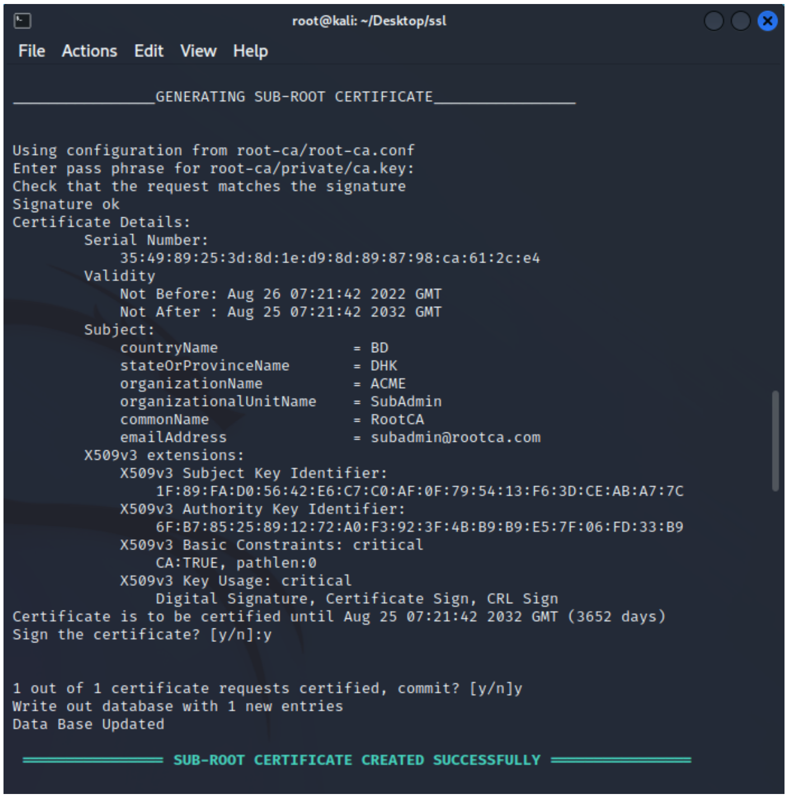


```
_______________GENERATING ROOT CERTIFICATE_______________

Enter pass phrase for root-ca/private/ca.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) [BD]:BD
State or Province Name [DHK]:DHK
Locality Name [RAMPURA]:Mogbazar
Organization Name [EWUBD]:ACME
Organizational Unit Name [ADMIN]:Admin
Common Name [rootCA]:AcmeRootCA
Email Address []:admin@rootca.com

 ═══════════════ ROOT CERTIFICATE CREATED SUCCESSFULLY ═══════════════
```

- To generate IntermediateCA first request to “AcmeRootCA” then generate the certificate named as “RootCA”. It will be signed by the RootCA.
  Command Lines: “openssl req -config sub-ca/sub-ca.conf -new -key sub-ca/private/sub-ca.key -sha256 -out sub-ca/csr/sub-ca.csr” -**SubRootCA Request**.
  “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” -**SubRootCA certificate**.

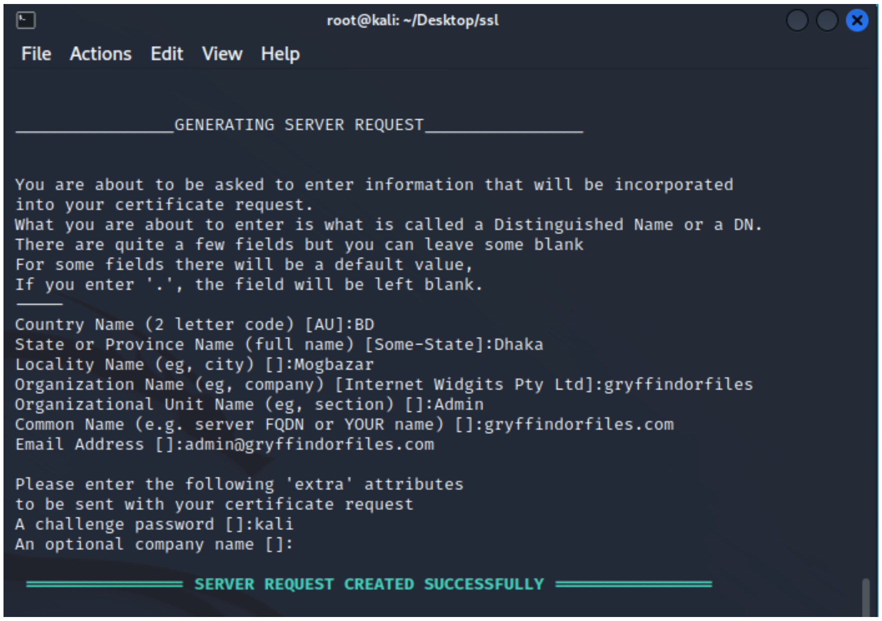


```
________________GENERATING SUB-ROOT REQUEST________________

Enter pass phrase for sub-ca/private/sub-ca.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) [BD]:BD
State or Province Name [DHK]:DHK
Locality Name [RAMPURA]:Mogbazar
Organization Name [EWUBD]:ACME
Organizational Unit Name [SUBADMIN]:SubAdmin
Common Name [subCA]:RootCA
Email Address []:subadmin@rootca.com

 ═══════════════ SUB-ROOT REQUEST CREATED SUCCESSFULLY ═══════════════
```

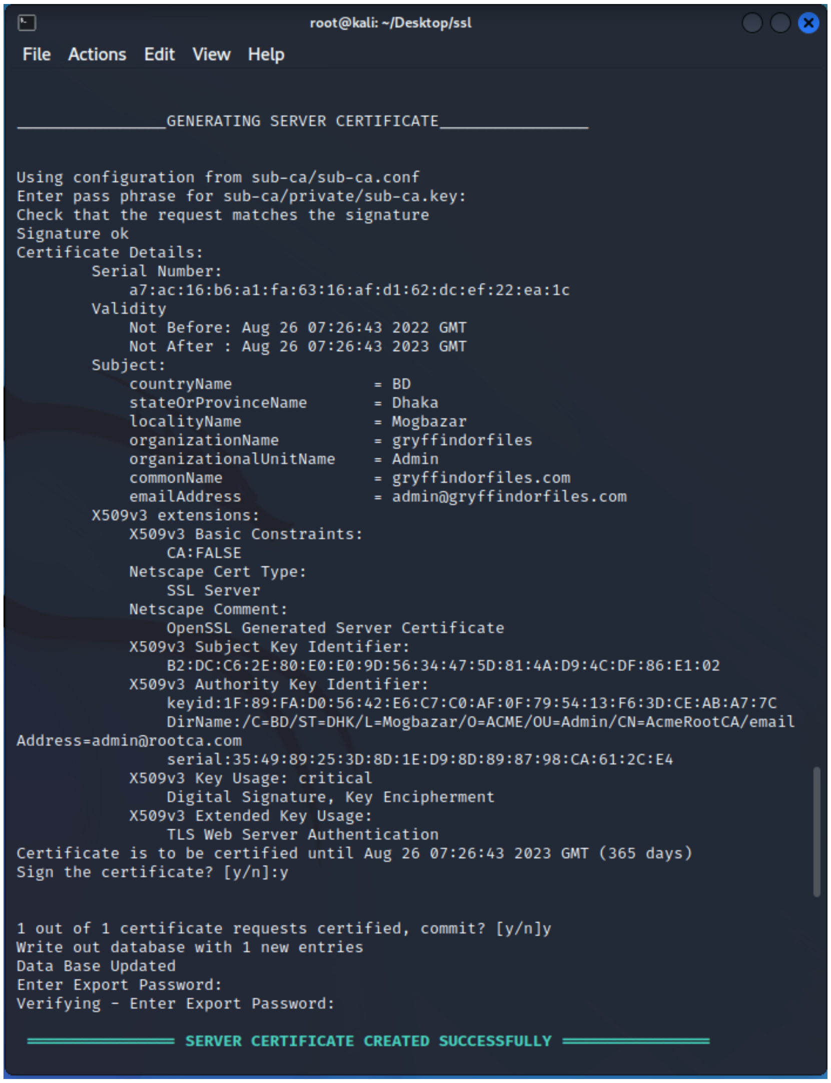


```
_______________GENERATING SUB-ROOT CERTIFICATE_______________

Using configuration from root-ca/root-ca.conf
Enter pass phrase for root-ca/private/ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            35:49:89:25:3d:8d:1e:d9:8d:89:87:98:ca:61:2c:e4
        Validity
            Not Before: Aug 26 07:21:42 2022 GMT
            Not After : Aug 25 07:21:42 2032 GMT
        Subject:
            countryName               = BD
            stateOrProvinceName       = DHK
            organizationName          = ACME
            organizationalUnitName    = SubAdmin
            commonName                = RootCA
            emailAddress              = subadmin@rootca.com
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                1F:89:FA:D0:56:42:E6:C7:C0:AF:0F:79:54:13:F6:3D:CE:AB:A7:7C
            X509v3 Authority Key Identifier:
                6F:B7:85:25:89:12:72:A0:F3:92:3F:4B:B9:B9:E5:7F:06:FD:33:B9
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Aug 25 07:21:42 2032 GMT (3652 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

 ═══════════════ SUB-ROOT CERTIFICATE CREATED SUCCESSFULLY ═══════════════
```

- Generating server certificate which is a TLS client. It will be signed by the IntermediateCA. So, here first need to send a request to IntermediateCA which is “RootCA” then generate the certificate.
  Command Lines: “openssl req -key server/private/server.key -new -sha256 -out server/csr/server.csr” -**Server Request**
  “openssl ca -config sub-ca/sub-ca.conf -extensions server_cert -days 365 -notext -in server/csr/server.csr -out server/certs/server.crt” -**Server Certificate**

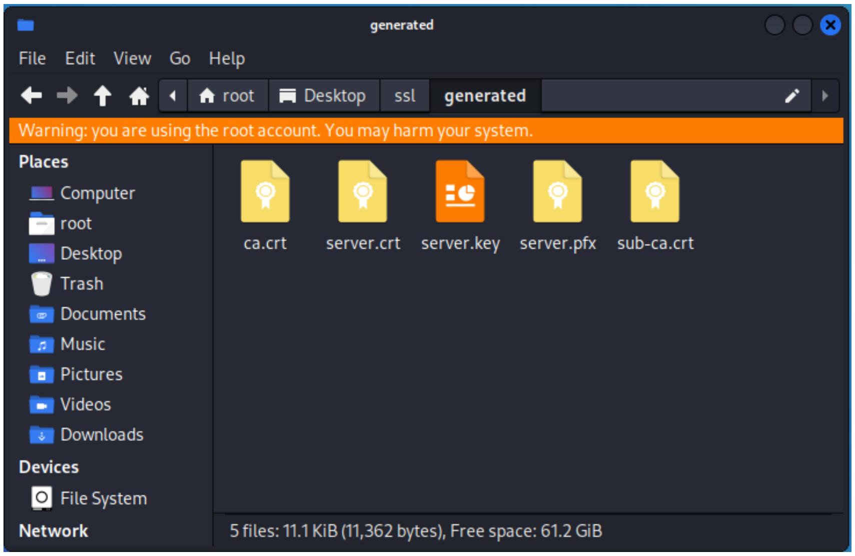


```
________________GENERATING SERVER REQUEST________________

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]:Dhaka
Locality Name (eg, city) []:Mogbazar
Organization Name (eg, company) [Internet Widgits Pty Ltd]:gryffindorfiles
Organizational Unit Name (eg, section) []:Admin
Common Name (e.g. server FQDN or YOUR name) []:gryffindorfiles.com
Email Address []:admin@gryffindorfiles.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:kali
An optional company name []:

 ════════════════ SERVER REQUEST CREATED SUCCESSFULLY ════════════════
```



```
________________GENERATING SERVER CERTIFICATE________________

Using configuration from sub-ca/sub-ca.conf
Enter pass phrase for sub-ca/private/sub-ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            a7:ac:16:b6:a1:fa:63:16:af:d1:62:dc:ef:22:ea:1c
        Validity
            Not Before: Aug 26 07:26:43 2022 GMT
            Not After : Aug 26 07:26:43 2023 GMT
        Subject:
            countryName               = BD
            stateOrProvinceName       = Dhaka
            localityName              = Mogbazar
            organizationName          = gryffindorfiles
            organizationalUnitName    = Admin
            commonName                = gryffindorfiles.com
            emailAddress              = admin@gryffindorfiles.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Server
            Netscape Comment:
                OpenSSL Generated Server Certificate
            X509v3 Subject Key Identifier:
                B2:DC:C6:2E:80:E0:E0:9D:56:34:47:5D:81:4A:D9:4C:DF:86:E1:02
            X509v3 Authority Key Identifier:
                keyid:1F:89:FA:D0:56:42:E6:C7:C0:AF:0F:79:54:13:F6:3D:CE:AB:A7:7C
                DirName:/C=BD/ST=DHK/L=Mogbazar/O=ACME/OU=Admin/CN=AcmeRootCA/email
Address=admin@rootca.com
                serial:35:49:89:25:3D:8D:1E:D9:8D:89:87:98:CA:61:2C:E4
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
Certificate is to be certified until Aug 26 07:26:43 2023 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
Enter Export Password:
Verifying - Enter Export Password:

 ================ SERVER CERTIFICATE CREATED SUCCESSFULLY ================
```

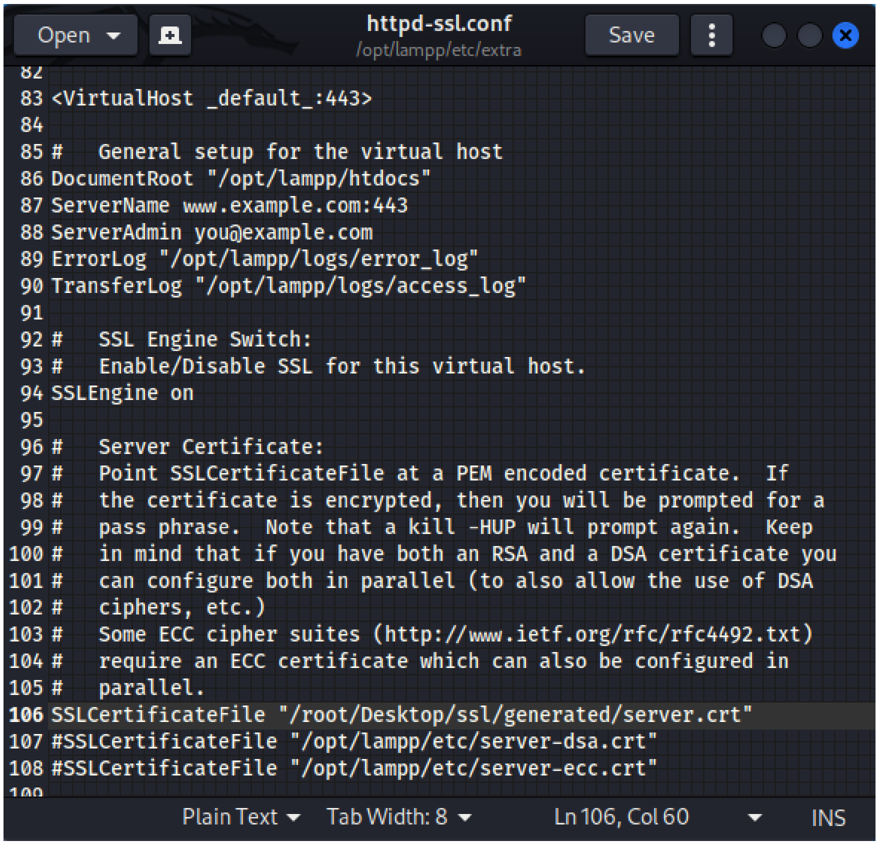
- Keeping all the files in a folder named as generated. Total generated file is 5.



5 files: 11.1 KiB (11,362 bytes), Free space: 61.2 GiB

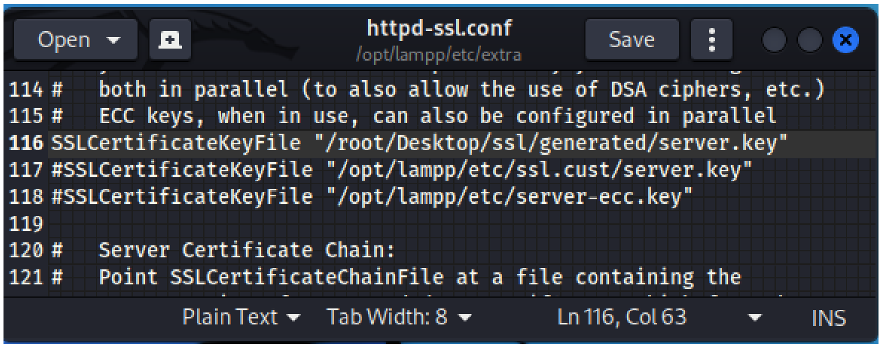
Installing Certificates in XAMPP, Browser & getting the Padlock:

- Go to the location “root>opt>lampp>etc>extra”
- Open the file named “httpd-ssl.conf” in “gedit”. To install “gedit” use the command line below.
  Command Line: “sudo apt-get install gedit”
- Copy the location of generated certificates and paste the location in line: 106, 116, 137
- SSLCertificateFile "/root/Desktop/ssl/generated/server.crt"



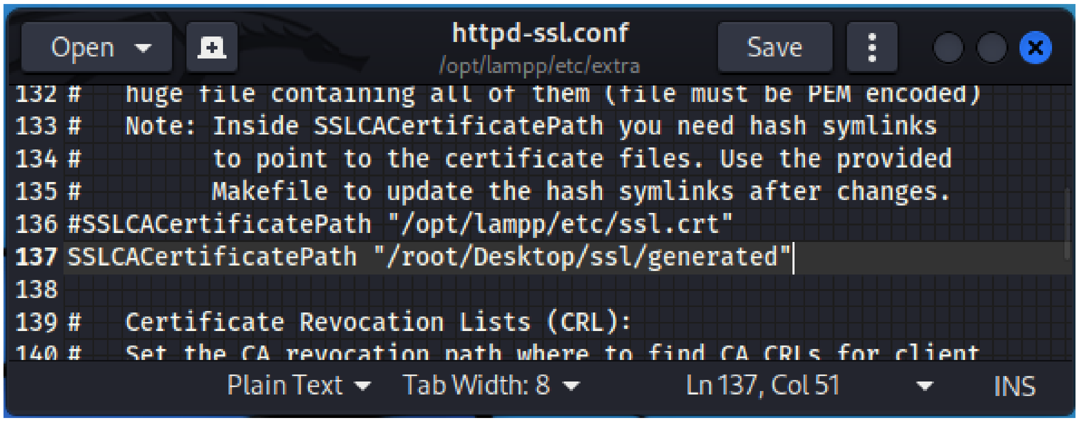
```
 82
 83 <VirtualHost _default_:443>
 84
 85 #   General setup for the virtual host
 86 DocumentRoot "/opt/lampp/htdocs"
 87 ServerName www.example.com:443
 88 ServerAdmin you@example.com
 89 ErrorLog "/opt/lampp/logs/error_log"
 90 TransferLog "/opt/lampp/logs/access_log"
 91
 92 #   SSL Engine Switch:
 93 #   Enable/Disable SSL for this virtual host.
 94 SSLEngine on
 95
 96 #   Server Certificate:
 97 #   Point SSLCertificateFile at a PEM encoded certificate.  If
 98 #   the certificate is encrypted, then you will be prompted for a
 99 #   pass phrase.  Note that a kill -HUP will prompt again.  Keep
100 #   in mind that if you have both an RSA and a DSA certificate you
101 #   can configure both in parallel (to also allow the use of DSA
102 #   ciphers, etc.)
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"
```

- SSLCertificateKeyFile "/root/Desktop/ssl/generated/server.key"



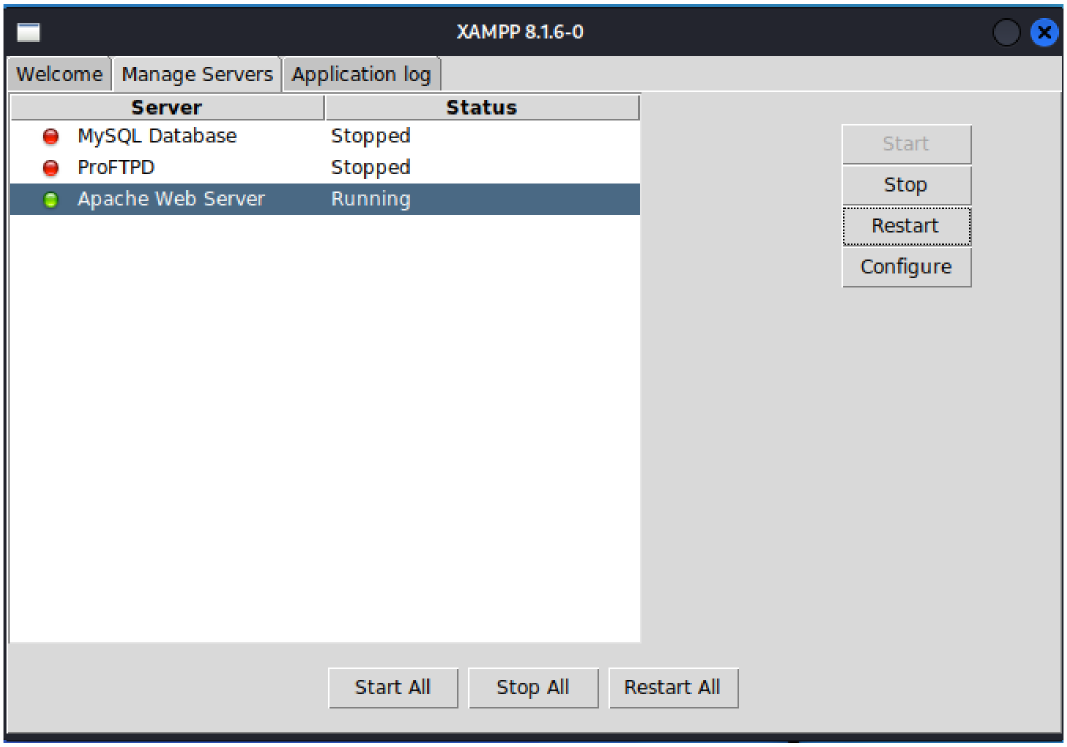
```
114 #   both in parallel (to also allow the use of DSA ciphers, etc.)
115 #   ECC keys, when in use, can also be configured in parallel
116 SSLCertificateKeyFile "/root/Desktop/ssl/generated/server.key"
117 #SSLCertificateKeyFile "/opt/lampp/etc/ssl.cust/server.key"
118 #SSLCertificateKeyFile "/opt/lampp/etc/server-ecc.key"
119
120 #   Server Certificate Chain:
121 #   Point SSLCertificateChainFile at a file containing the
```

- SSLCACertificatePath "/root/Desktop/ssl/generated"



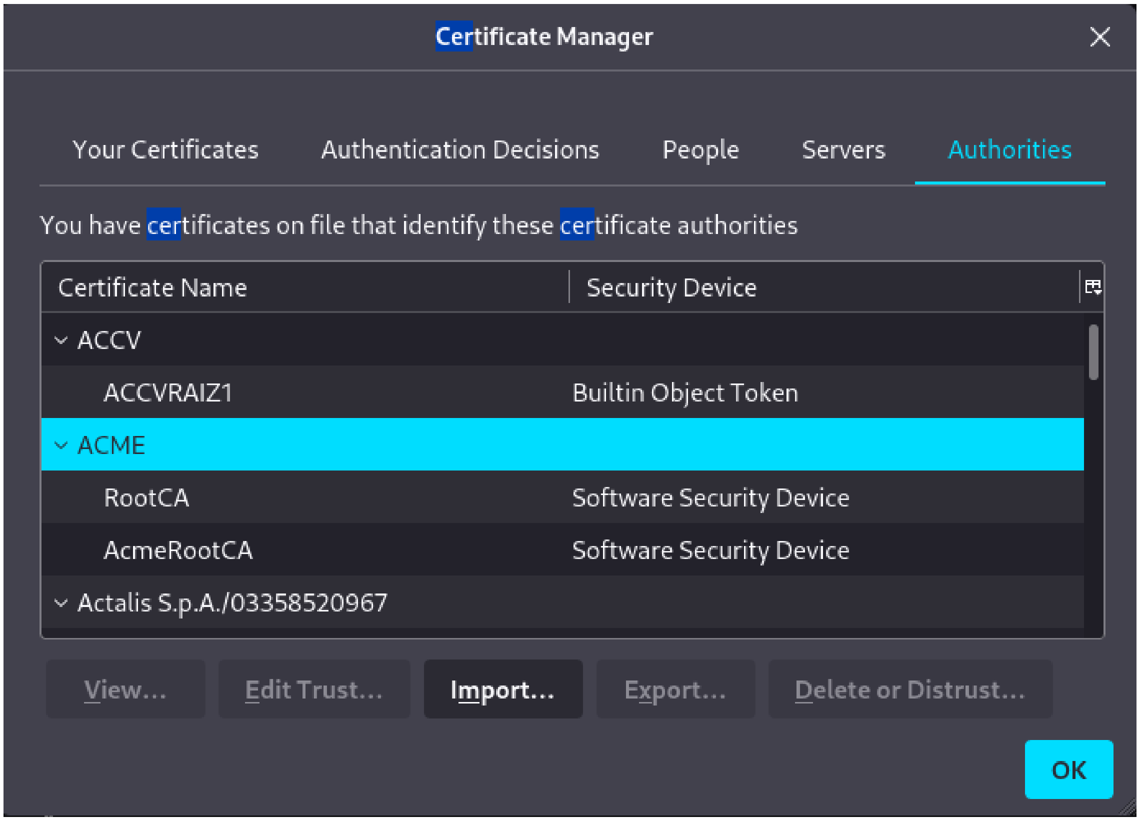
```
#   huge file containing all of them (file must be PEM encoded)
#   Note: Inside SSLCACertificatePath you need hash symlinks
#         to point to the certificate files. Use the provided
#         Makefile to update the hash symlinks after changes.
#SSLCACertificatePath "/opt/lampp/etc/ssl.crt"
SSLCACertificatePath "/root/Desktop/ssl/generated"

#   Certificate Revocation Lists (CRL):
#   Set the CA revocation path where to find CA CRLs for client
```

- Open the XAMPP form the file location “root>opt>lamp” and click on “manager-linux-x64.run” or use the terminal and use the command below. Click on “Manage Servers” and start “Apache Web Server”.
  Command Line: “/opt/lampp/manager-linux-x64.run”



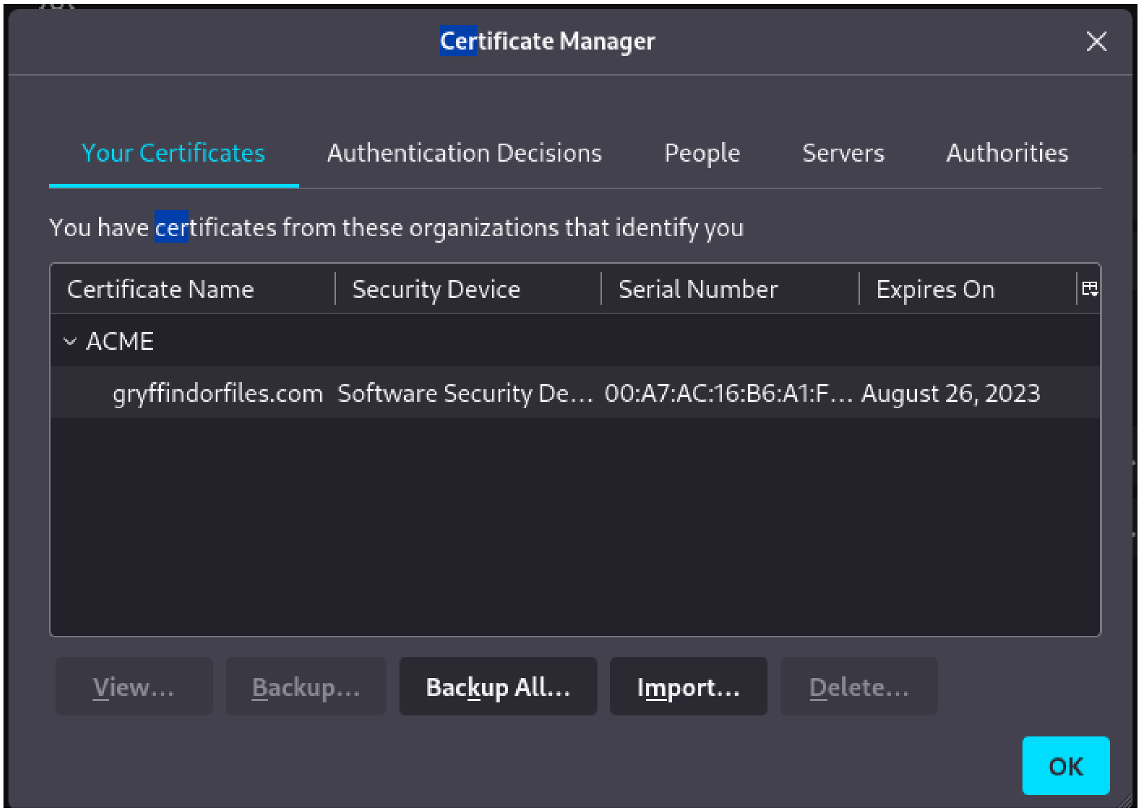
Server	Status
● MySQL Database	Stopped
● ProFTPD	Stopped
● Apache Web Server	Running

- Go to the browser and search https://gryffindor.com. Initially the padlock won’t be appeared. Now, go to browser’s “Settings>Certificate Manager>Authorities”. Import the certificates “ca.crt” & “sub-ca.crt”. then go to “your Certificates” and import “server.pfx”.



You have certificates on file that identify these certificate authorities

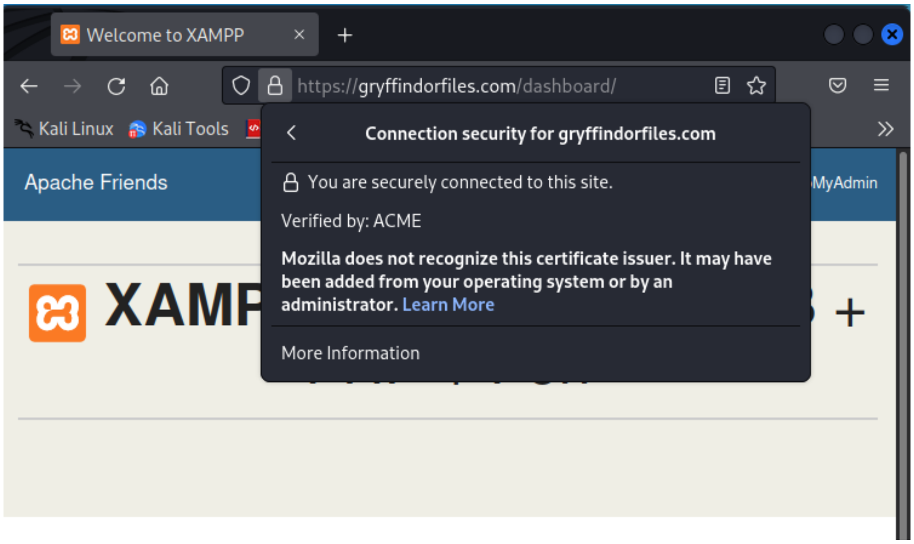
Certificate Name	Security Device
ACCV	
ACCVRAIZ1	Builtin Object Token
ACME	
RootCA	Software Security Device
AcmeRootCA	Software Security Device
Actalis S.p.A./03358520967	



You have certificates from these organizations that identify you

Certificate Name	Security Device	Serial Number	Expires On
ACME			
gryffindorfiles.com	Software Security De…	00:A7:AC:16:B6:A1:F…	August 26, 2023

- Restart the browser and again type https://gryffindorfiles.com and it will show the Padlock sign as a secure website.



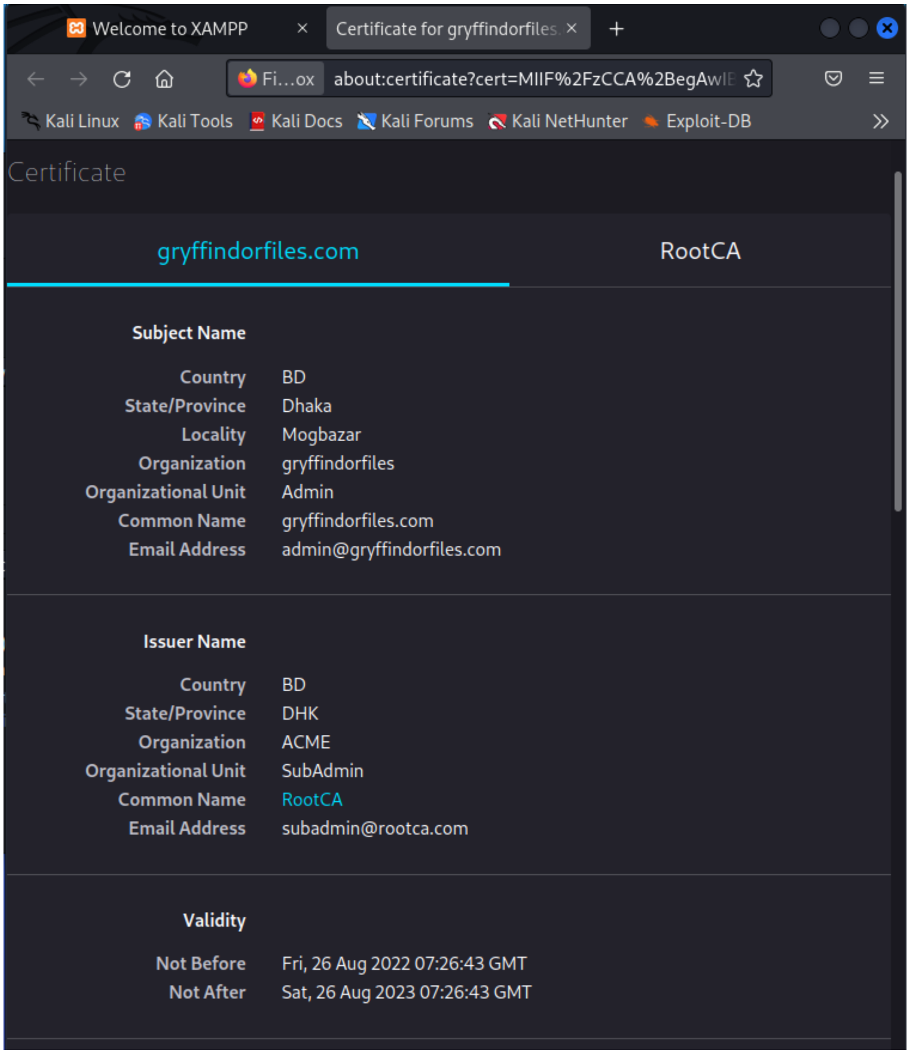
Connection security for gryffindorfiles.com

You are securely connected to this site.

Verified by: ACME

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

More Information



Certificate

Subject Name

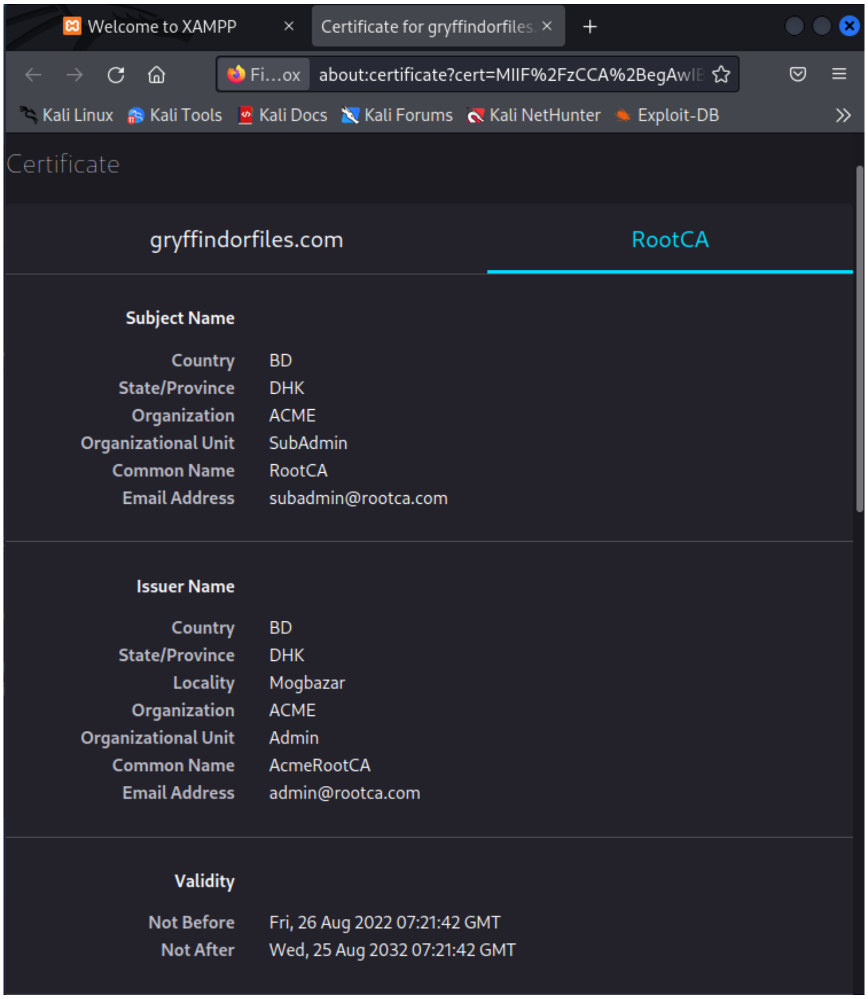
Country	BD
State/Province	Dhaka
Locality	Mogbazar
Organization	gryffindorfiles
Organizational Unit	Admin
Common Name	gryffindorfiles.com
Email Address	admin@gryffindorfiles.com

Issuer Name

Country	BD
State/Province	DHK
Organization	ACME
Organizational Unit	SubAdmin
Common Name	RootCA
Email Address	subadmin@rootca.com

Validity

Not Before	Fri, 26 Aug 2022 07:26:43 GMT
Not After	Sat, 26 Aug 2023 07:26:43 GMT



Subject Name

Country BD
State/Province DHK
Organization ACME
Organizational Unit SubAdmin
Common Name RootCA
Email Address subadmin@rootca.com

Issuer Name

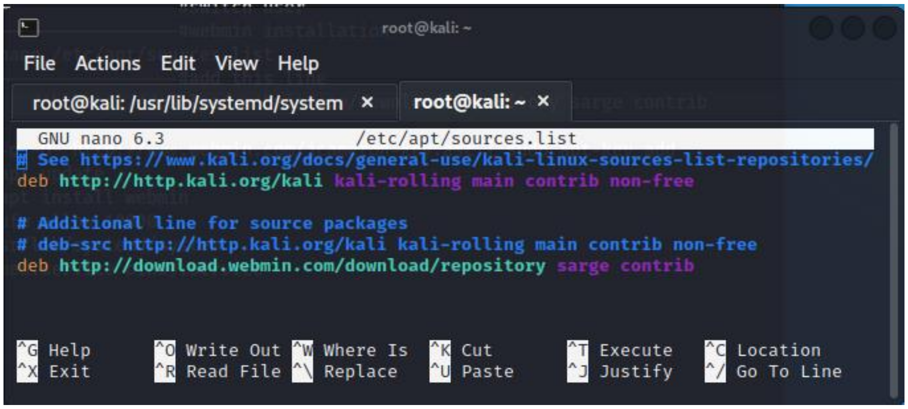
Country BD
State/Province DHK
Locality Mogbazar
Organization ACME
Organizational Unit Admin
Common Name AcmeRootCA
Email Address admin@rootca.com

Validity

Not Before Fri, 26 Aug 2022 07:21:42 GMT
Not After Wed, 25 Aug 2032 07:21:42 GMT

Configuration of DNS Server:

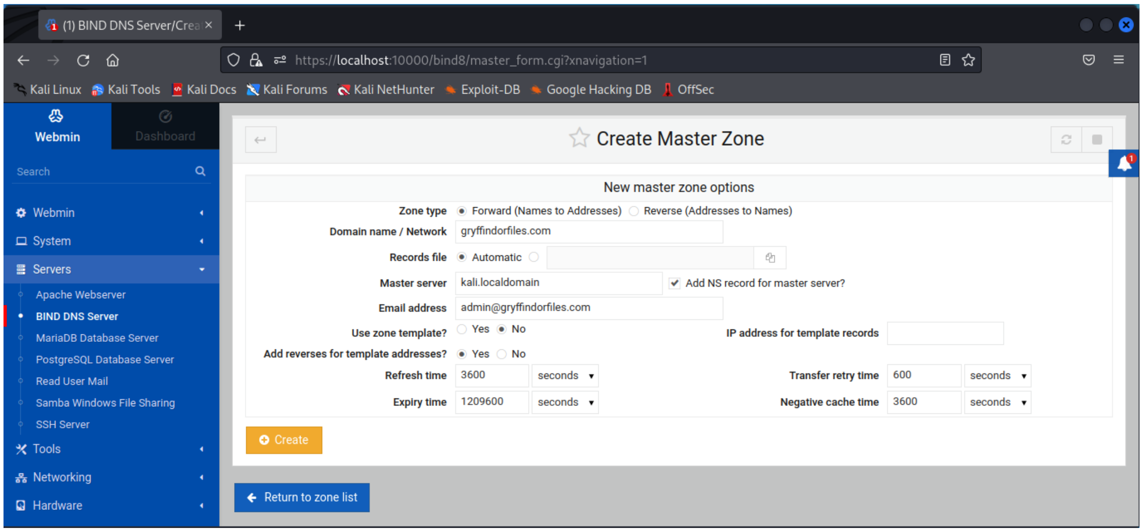
- to configure the DNS server, it will require “Webmin” which is a web interface and “Bind9” which is used to manage the DNs server.
- To install webmin use the command “sudo nano /etc/apt/sources.list” then add the line “deb http://download.webmin.com/download/repository sarge contrib”


root@kali: ~
File Actions Edit View Help
root@kali: /usr/lib/systemd/system
root@kali: ~

```
  GNU nano 6.3                    /etc/apt/sources.list
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
deb http://http.kali.org/kali kali-rolling main contrib non-free

# Additional line for source packages
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free
deb http://download.webmin.com/download/repository sarge contrib



^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

Command Lines: “sudo nano /etc/apt/sources.list”
“wget -q -O- http://www.webmin.com/jcameron-key.asc | sudo apt-key add”
“sudo apt update”
“sudo apt install webmin”
“ufw allow 10000”
“cd /usr/lib/systemd/system”
“cp named.service bind9.service”

- Webmin runs on port:10000 and uses localhost. Here Bind9 will be used. https://localhost:10000/bind8/index.cgi?xnavigation=1
- Creating a Forward Master Zone for Name Server



https://localhost:10000/bind8/master_form.cgi?xnavigation=1

Create Master Zone

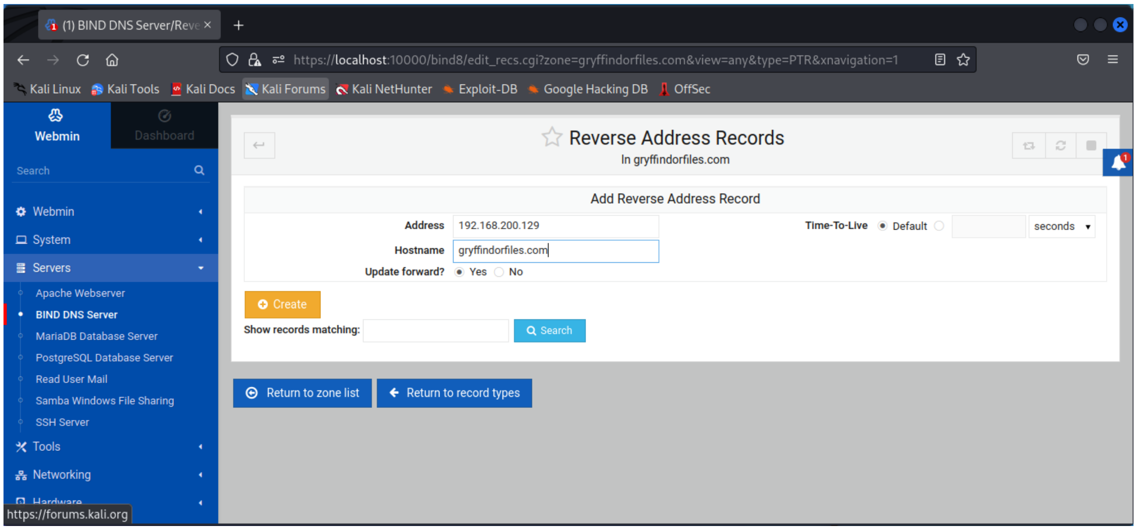
New master zone options

Zone type ● Forward (Names to Addresses) ○ Reverse (Addresses to Names)
Domain name / Network gryffindorfiles.com
Records file ● Automatic ○
Master server kali.localdomain ☑ Add NS record for master server?
Email address admin@gryffindorfiles.com
Use zone template? ○ Yes ● No
IP address for template records
Add reverses for template addresses? ● Yes ○ No
Refresh time 3600 seconds
Transfer retry time 600 seconds
Expiry time 1209600 seconds
Negative cache time 3600 seconds

Create

Return to zone list

- Creating a Reverse address on master zone



https://localhost:10000/bind8/edit_recs.cgi?zone=gryffindorfiles.com&view=any&type=PTR&xnavigation=1

Reverse Address Records
In gryffindorfiles.com

Add Reverse Address Record

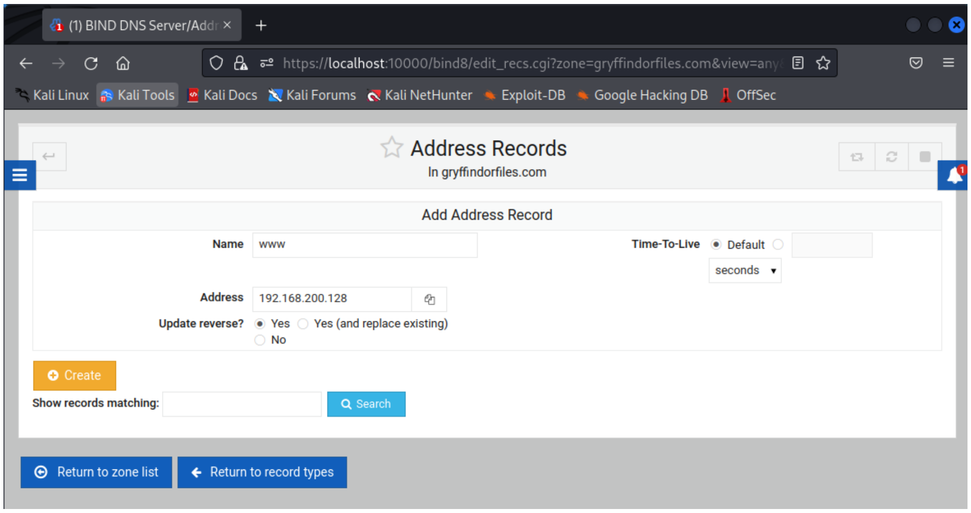
Address 192.168.200.129
Hostname gryffindorfiles.com
Update forward? ● Yes ○ No
Time-To-Live ● Default ○ seconds

Create

Show records matching: Search

Return to zone list
Return to record types

- Creating address



https://localhost:10000/bind8/edit_recs.cgi?zone=gryffindorfiles.com&view=any

Address Records

In gryffindorfiles.com

Add Address Record

Name: www

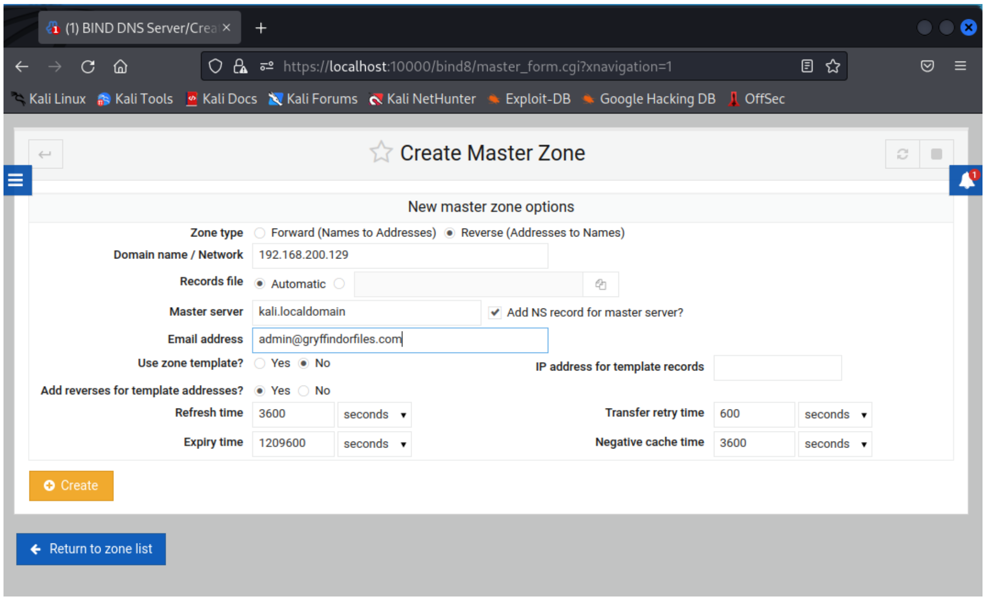
Time-To-Live: ● Default ○ seconds

Address: 192.168.200.128

Update reverse? ● Yes ○ Yes (and replace existing) ○ No

Show records matching:

- Creating Reverse Master Zone and reverse address



https://localhost:10000/bind8/master_form.cgi?xnavigation=1

Create Master Zone

New master zone options

Zone type: ○ Forward (Names to Addresses) ● Reverse (Addresses to Names)

Domain name / Network: 192.168.200.129

Records file: ● Automatic ○

Master server: kali.localdomain ☑ Add NS record for master server?

Email address: admin@gryffindorfiles.com

Use zone template? ○ Yes ● No

IP address for template records:

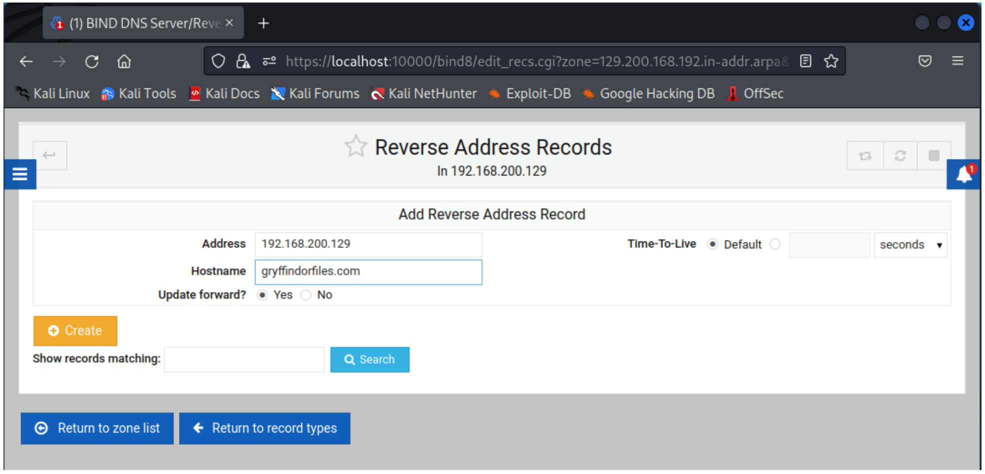
Add reverses for template addresses? ● Yes ○ No

Refresh time: 3600 seconds

Transfer retry time: 600 seconds

Expiry time: 1209600 seconds

Negative cache time: 3600 seconds



https://localhost:10000/bind8/edit_recs.cgi?zone=129.200.168.192.in-addr.arpa&

Reverse Address Records

In 192.168.200.129

Add Reverse Address Record

Address: 192.168.200.129

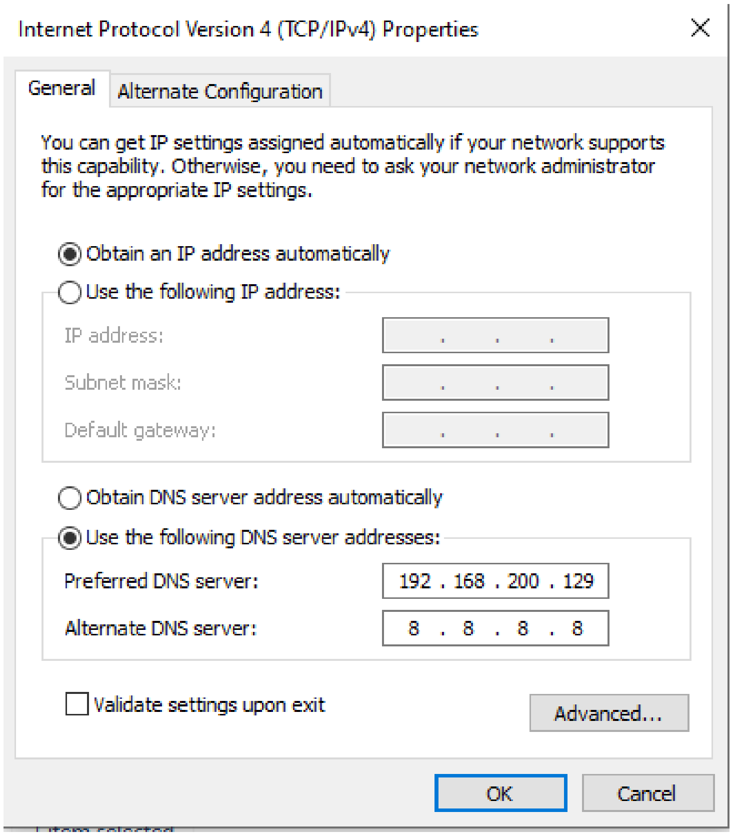
Time-To-Live: ● Default ○ seconds

Hostname: gryffindorfiles.com

Update forward? ● Yes ○ No

Show records matching:

- go to control panel on windows machine. Go to the location “Open Network and Internet settings>Change adapter options” and go to properties of the IPv4 settings.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

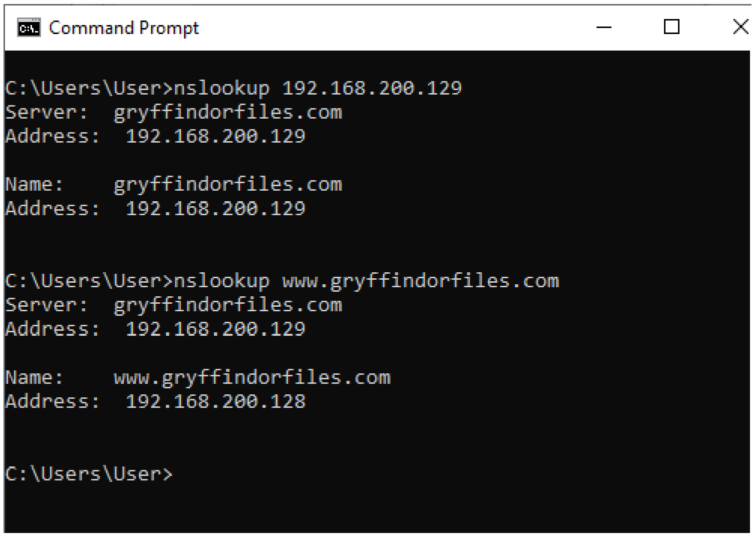
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 200 . 129

Alternate DNS server: 8 . 8 . 8 . 8

□ Validate settings upon exit

- nslookup from windows. The IP of
  DNS Server: 192.168.200.129
  WEB Server: 192.168.200.128



```
C:\Users\User>nslookup 192.168.200.129
Server:  gryffindorfiles.com
Address:  192.168.200.129

Name:    gryffindorfiles.com
Address:  192.168.200.129


C:\Users\User>nslookup www.gryffindorfiles.com
Server:  gryffindorfiles.com
Address:  192.168.200.129

Name:    www.gryffindorfiles.com
Address:  192.168.200.128


C:\Users\User>
```