East West University

Department of CSE

CSE 487

Cybersecurity, Law and Ethics
FALL 2022

Mini Project-1

Securing a networked system with Public Key Infrastructure
Implementing Transport Layer Security on HTTP for https:// connection

Submitted To:

Dr. Md Hasanul Ferdaus

Lecturer

Department of Computer Science and Engineering

Submitted By

Adri Saha
ID: 2019-1-60-024

Submission Date: 5 January 2023

Project: Securing a networked system with PKI

Project Description: Any website requires SSL (Secure Sockets Layer) certificates to protect user data, confirm the site's ownership, prevent hackers from building a fake version of the site, and inspire trust in users. So, in this project we have to configure SSL certificate and verify a website. Need to generate padlock icon which defines that connection is secure on that specific website. Configured CSR Configuration and Generation for the www.verysecureserver.com. Then transfereed CSR to AcmeCA and AcmeCA to www.verysecureserver.com. Then we installed the certificates and made an simple file uploading html page named index.html which we made secured. Then, we configured DNS to access the secured site from other servers and finally to protect our website from unwanted access we configured firewall. That’s how we verified the security of the connection in ubuntu and finally revoke the certificate.

We did this project on windows server and ubuntu server both. Here, we are explaining the certificate configuration process on Linux ubuntu 20.04 terminal.

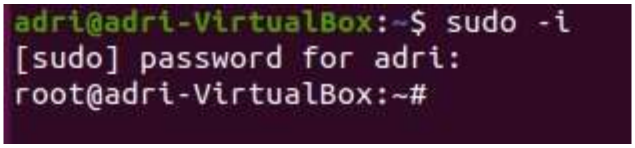
Generating SSL certificate

Websites require SSL (Secure Sockets Layer) certificates to protect user data, confirm the site's ownership, prevent hackers from building a fake version of the site, and inspire trust in users. https means that site has SSLs certificate which is authorized and secured. So, to build https or ssl certificate we have to configure SSL certificate.

Step 1:

- First, we downloaded virtual box. And inside virtual box we installed ubuntu.
- After installing ubuntu we go to the root and to generate Transport Layer Security over HTTP, need to follow some command on ubuntu Terminal which are following.

Preparing the environment moving to the root using and give the ubuntu password - **sudo -i**



```
adri@adri-VirtualBox:~$ sudo -i
[sudo] password for adri:
root@adri-VirtualBox:~#
```

see the tree files inside the root

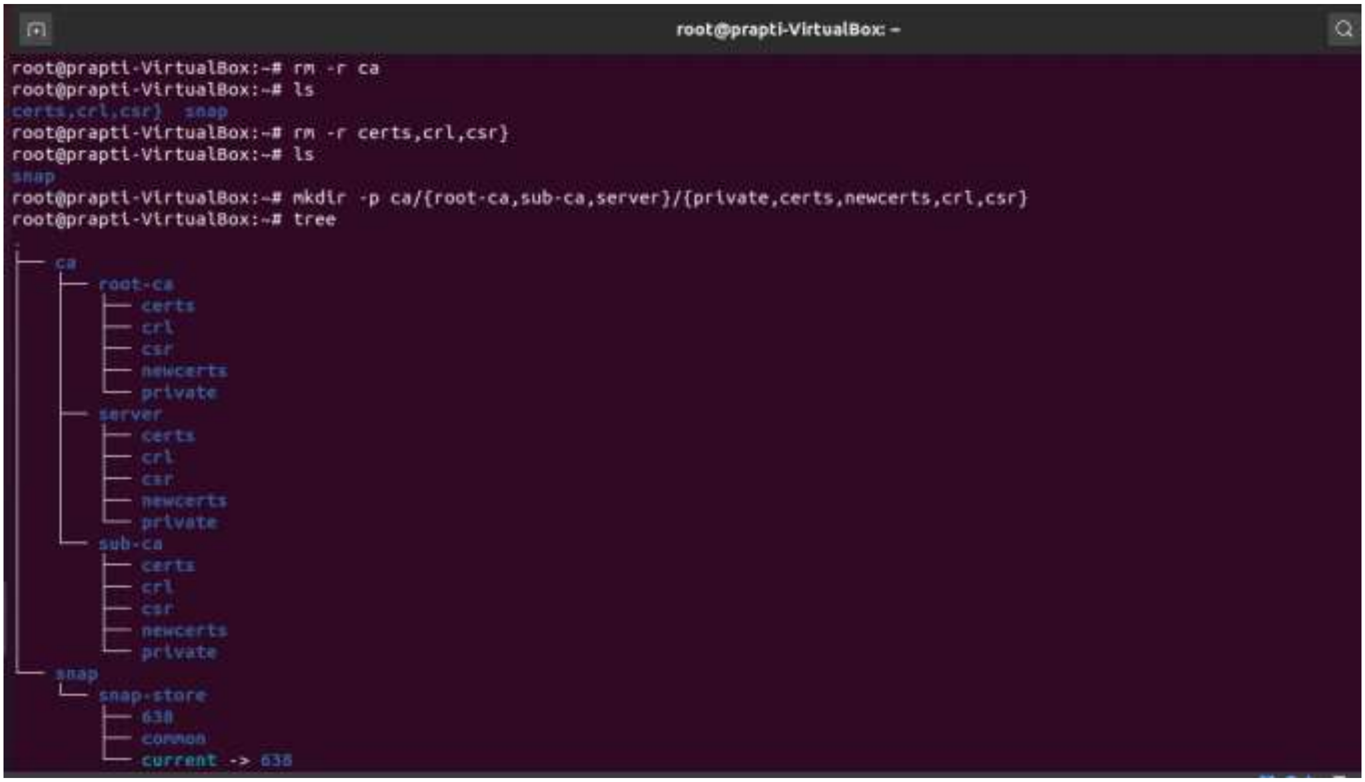
- tree
- rm -r ca (If there is previously other folders on root ca, then remove them) - tree (again check tree if there is any directory inside ca)

Creating directory on ca

- mkdir -p ca/{root-ca,sub-ca,server}/{private,certs,newcerts,crl,csr}

See the folders are created successfully.

- tree ca



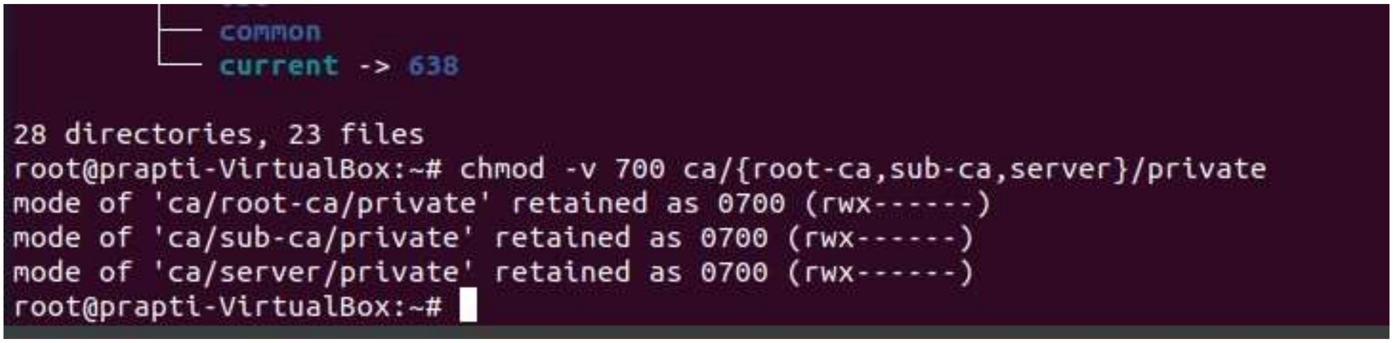
root@prapti-VirtualBox: ~

```
root@prapti-VirtualBox:~# rm -r ca
root@prapti-VirtualBox:~# ls
certs,crl,csr}  snap
root@prapti-VirtualBox:~# rm -r certs,crl,csr}
root@prapti-VirtualBox:~# ls
snap
root@prapti-VirtualBox:~# mkdir -p ca/{root-ca,sub-ca,server}/{private,certs,newcerts,crl,csr}
root@prapti-VirtualBox:~# tree
.
├── ca
│   ├── root-ca
│   │   ├── certs
│   │   ├── crl
│   │   ├── csr
│   │   ├── newcerts
│   │   └── private
│   ├── server
│   │   ├── certs
│   │   ├── crl
│   │   ├── csr
│   │   ├── newcerts
│   │   └── private
│   └── sub-ca
│       ├── certs
│       ├── crl
│       ├── csr
│       ├── newcerts
│       └── private
└── snap
    └── snap-store
        ├── 638
        ├── common
        └── current -> 638
```

Changing the root of ca and sub ca permission to private folder:

- chmod -v 700 ca/{root-ca,sub-ca, server}/private

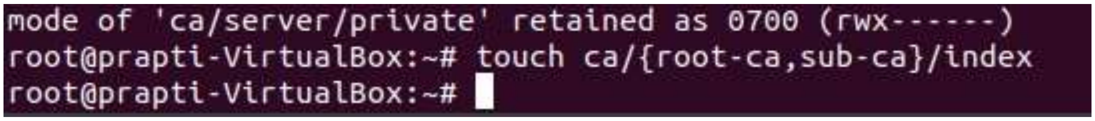
//700 used for make private



```
        ├── common
        └── current -> 638

28 directories, 23 files
root@prapti-VirtualBox:~# chmod -v 700 ca/{root-ca,sub-ca,server}/private
mode of 'ca/root-ca/private' retained as 0700 (rwx------)
mode of 'ca/sub-ca/private' retained as 0700 (rwx------)
mode of 'ca/server/private' retained as 0700 (rwx------)
root@prapti-VirtualBox:~# 
```

Creating file index in both root ca and sub ca

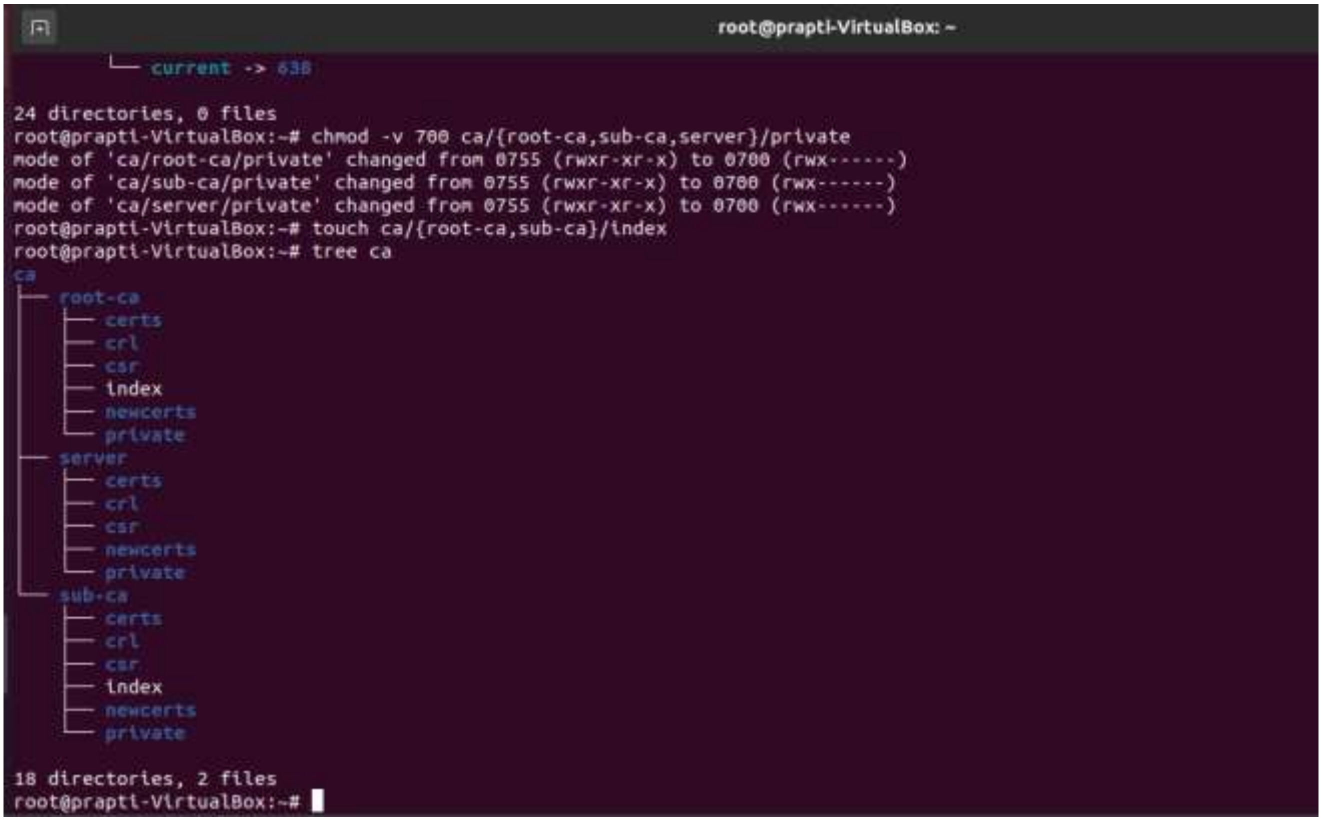
- touch ca/{root-ca,sub-ca}/index



```
mode of 'ca/server/private' retained as 0700 (rwx------)
root@prapti-VirtualBox:~# touch ca/{root-ca,sub-ca}/index
root@prapti-VirtualBox:~# 
```

Seeing ca tree again

- tree ca



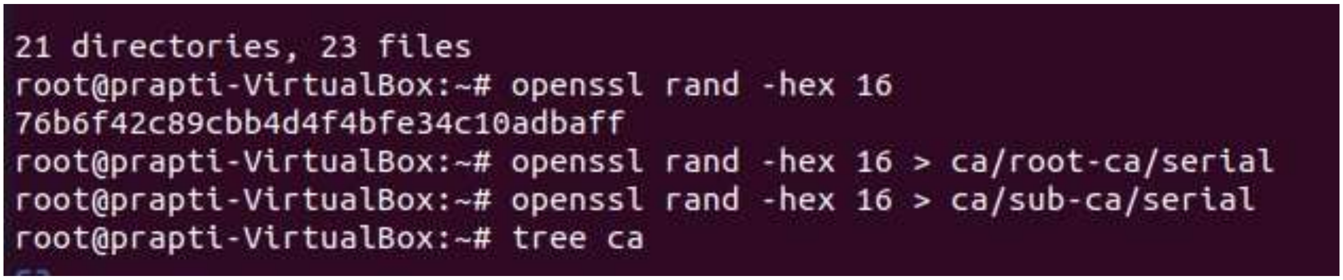
root@prapti-VirtualBox: ~

```
    └── current -> 638

24 directories, 0 files
root@prapti-VirtualBox:~# chmod -v 700 ca/{root-ca,sub-ca,server}/private
mode of 'ca/root-ca/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
mode of 'ca/sub-ca/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
mode of 'ca/server/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
root@prapti-VirtualBox:~# touch ca/{root-ca,sub-ca}/index
root@prapti-VirtualBox:~# tree ca
ca
├── root-ca
│   ├── certs
│   ├── crl
│   ├── csr
│   ├── index
│   ├── newcerts
│   └── private
├── server
│   ├── certs
│   ├── crl
│   ├── csr
│   ├── newcerts
│   └── private
└── sub-ca
    ├── certs
    ├── crl
    ├── csr
    ├── index
    ├── newcerts
    └── private

18 directories, 2 files
root@prapti-VirtualBox:~# 
```

Generating hexadecimal random number of 16 character
- openssl rand -hex 16
//openssl: open secure sockets layer

writing serial number of root ca openssl
- rand -hex 16 > ca/root-ca/serial

writing serial number of sub ca
- openssl rand -hex 16 > ca/sub-ca/serial



```
21 directories, 23 files
root@prapti-VirtualBox:~# openssl rand -hex 16
76b6f42c89cbb4d4f4bfe34c10adbaff
root@prapti-VirtualBox:~# openssl rand -hex 16 > ca/root-ca/serial
root@prapti-VirtualBox:~# openssl rand -hex 16 > ca/sub-ca/serial
root@prapti-VirtualBox:~# tree ca
```

- tree ca

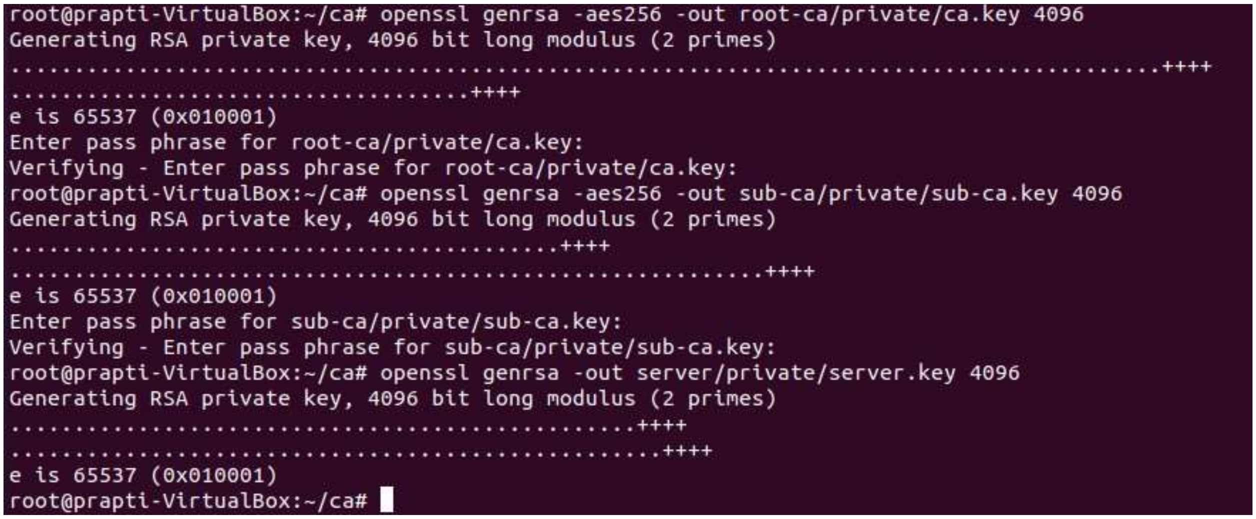
moving to ca directory
- cd ca

Step 2: Generating private key for root ca, sub ca, and server

a) Public key for rootCA
   - openssl genrsa -aes256 -out root-ca/private/ca.key 4096
   //Give the password which has to be remembered

b) Public key for subCA
   - openssl genrsa -aes256 -out sub-ca/private/sub-ca.key 4096
   //Give the password which has to be remembered

c) Public key for server
   - openssl genrsa -out server/private/server.key 2048



```
root@prapti-VirtualBox:~/ca# openssl genrsa -aes256 -out root-ca/private/ca.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
..........................................................................................++++
....................................++++
e is 65537 (0x010001)
Enter pass phrase for root-ca/private/ca.key:
Verifying - Enter pass phrase for root-ca/private/ca.key:
root@prapti-VirtualBox:~/ca# openssl genrsa -aes256 -out sub-ca/private/sub-ca.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
...........................................++++
...........................................................++++
e is 65537 (0x010001)
Enter pass phrase for sub-ca/private/sub-ca.key:
Verifying - Enter pass phrase for sub-ca/private/sub-ca.key:
root@prapti-VirtualBox:~/ca# openssl genrsa -out server/private/server.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.................................................++++
...................................................++++
e is 65537 (0x010001)
root@prapti-VirtualBox:~/ca# █
```

1. **Generating certificates**
   a) Root-CA
   # Creating root ca.config
   - gedit root-ca/root-ca.conf //also can use vim root-ca/root-ca.conf

   *****Code to be used- [ca]

```
#/root/ca/root-ca/root-ca.conf
#see man ca
default_ca    = CA_default
[CA_default]
```

```
dir     = /root/ca/root-ca certs
=  $dir/certs crl_dir    =
$dir/crl new_certs_dir   =
$dir/newcerts database   =
$dir/index serial    =
$dir/serial
RANDFILE   = $dir/private/.rand private_key
= $dir/private/ca.key
certificate   = $dir/certs/ca.crt


crlnumber   = $dir/crlnumber
crl            =      $dir/crl/ca.crl
crl_extensions        =   crl_ext
default_crl_days    = 30
default_md   = sha256


name_opt   = ca_default
cert_opt     =  ca_default
default_days       =   365
preserve     =  no  policy
= policy_strict
[ policy_strict ]

countryName   = supplied

stateOrProvinceName    =    supplied
organizationName           =     match
organizationalUnitName  =  optional
commonName   =  supplied
emailAddress   =  optional


[  policy_loose  ]  countryName      =
optional   stateOrProvinceName     =
optional  localityName     =  optional
organizationName        =    optional
organizationalUnitName   = optional
commonName   = supplied
emailAddress   = optional

[ req ]

# Options for the req tool, man req.
```

```
default_bits      =  2048  distinguished_name    =
req_distinguished_name    string_mask            =
utf8only

default_md   =  sha256

# Extension to add when the -x509 option is used.

x509_extensions   = v3_ca



[ req_distinguished_name ]

countryName                     = Country Name (2 letter code)

stateOrProvinceName             = State or Province Name

localityName                    = Locality Name

0.organizationName              = Organization Name

organizationalUnitName          = Organizational Unit Name

commonName                      = Common Name

emailAddress                    = Email Address

countryName_default  = BD

stateOrProvinceName_default = Dhaka

localityName_default = Sutrapur

0.organizationName_default = EWU

organizationalUnitName_default = Cyber_Security

commonName_default = AcmeRootCA

emailAddress_default = adri@acmeroot_ca.com
```

```
[ v3_ca ]
# Extensions to apply when createing root ca
# Extensions for a typical CA, man x509v3_config
subjectKeyIdentifier  = hash
authorityKeyIdentifier  = keyid:always,issuer
basicConstraints  = critical, CA:true
keyUsage   =  critical, digitalSignature, cRLSign, keyCertSign

[ v3_intermediate_ca ]
# Extensions to apply when creating intermediate or sub-ca
# Extensions for a typical intermediate CA, same man as above
subjectKeyIdentifier  = hash
authorityKeyIdentifier  = keyid:always,issuer
#pathlen:0 ensures no more sub-ca can be created below an intermediate
basicConstraints  = critical, CA:true, pathlen:0
keyUsage   = critical, digitalSignature, cRLSign, keyCertSign


[ server_cert ]
# Extensions for server certificates
basicConstraints  = CA:FALSE
nsCertType   = server
nsComment   =  "OpenSSL Generated Server Certificate"
```

subjectKeyIdentifier = hash

authorityKeyIdentifier = keyid,issuer:always

keyUsage   = critical, digitalSignature, keyEncipherment

extendedKeyUsage = serverAuth

[save and exit] (:wq then ctrl+c)

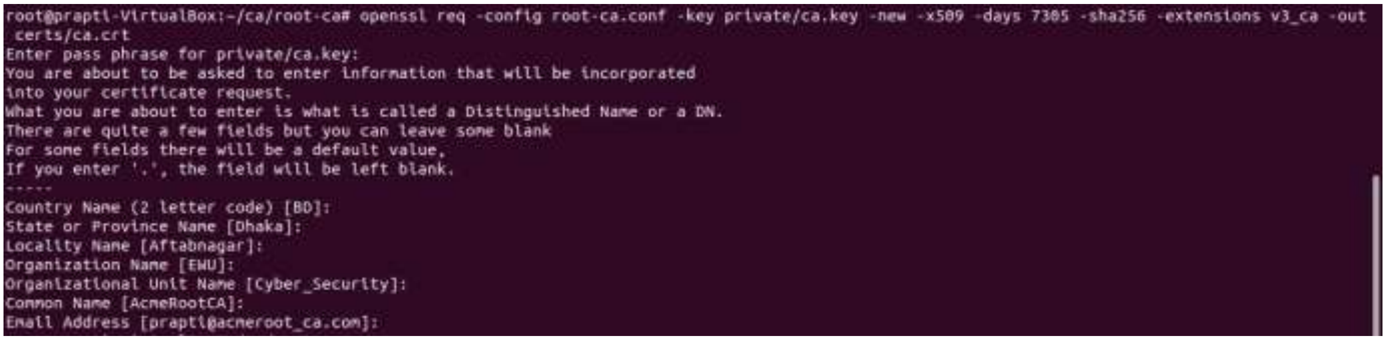
Moving inside root-ca

- cd root-ca

Generating root ca certificate: validation for 7305 days

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

Give the password
Press enter to by default fill up

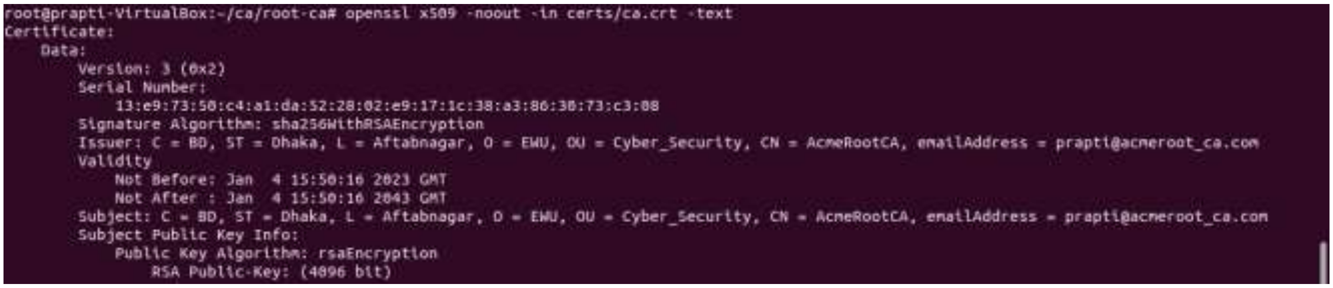


```
root@prapti-VirtualBox:~/ca/root-ca# openssl req -config root-ca.conf -key private/ca.key -new -x509 -days 7305 -sha256 -extensions v3_ca -out
 certs/ca.crt
Enter pass phrase for private/ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
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]:
State or Province Name [Dhaka]:
Locality Name [Aftabnagar]:
Organization Name [EWU]:
Organizational Unit Name [Cyber_Security]:
Common Name [AcmeRootCA]:
Email Address [prapti@acmeroot_ca.com]:
```

Ensuring that the certificate has been created properly

- openssl x509 -noout -in certs/ca.crt -text

Find the signature which is created by using RSA algorithm



```
root@prapti-VirtualBox:~/ca/root-ca# openssl x509 -noout -in certs/ca.crt -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            13:e9:73:50:c4:a1:da:52:28:02:e9:17:1c:38:a3:86:30:73:c3:08
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = BD, ST = Dhaka, L = Aftabnagar, O = EWU, OU = Cyber_Security, CN = AcmeRootCA, emailAddress = prapti@acmeroot_ca.com
        Validity
            Not Before: Jan  4 15:50:16 2023 GMT
            Not After : Jan  4 15:50:16 2043 GMT
        Subject: C = BD, ST = Dhaka, L = Aftabnagar, O = EWU, OU = Cyber_Security, CN = AcmeRootCA, emailAddress = prapti@acmeroot_ca.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
```

Moving a step back and then to sub-ca

- cd ../sub-ca

Sub-CA

- Creating sub-ca.config
- gedit sub-ca.conf

*****Code to be used- [ca]

```
#/root/ca/sub-ca/sub-ca.conf
#see man ca default_ca
= CA_default



[CA_default]    dir                  =
/root/ca/sub-ca   certs              =
$dir/certs  crl_dir        =  $dir/crl
new_certs_dir   = $dir/newcerts
database   = $dir/index serial   =
$dir/serial
RANDFILE   = $dir/private/.rand

private_key   = $dir/private/sub-ca.key
certificate   = $dir/certs/sub-ca.crt

crlnumber   = $dir/crlnumber
crl             =       $dir/crl/ca.crl
crl_extensions   = crl_ext
default_crl_days    = 30

default_md   = sha256 name_opt
= ca_default cert_opt   =
ca_default default_days   = 365
preserve   = no

policy    = policy_loose



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

[ policy_loose ]
```

```
countryName   = optional

stateOrProvinceName  = optional

localityName   = optional organizationName  = optional

organizationalUnitName   = optional

commonName   = supplied

emailAddress   = optional

[ req ]

# Options for the req tool, man req.

default_bits   = 2048

distinguished_name  = req_distinguished_name

string_mask   = utf8only

default_md   =  sha256

# Extension to add when the -x509 option is used.

x509_extensions   = v3_ca

[ req_distinguished_name ]

countryName                     = Country Name (2 letter code)

stateOrProvinceName             = State or Province Name

localityName                    = Locality Name

0.organizationName              = Organization Name

organizationalUnitName          = Organizational Unit Name

commonName                      = Common Name
```

```
emailAddress                    = Email Address

countryName_default  = BD

stateOrProvinceName_default = Dhaka

localityName_default = Sutrapur
0.organizationName_default = EWU

organizationalUnitName_default = Cyber_Security

commonName_default  = AcmeCA

emailAddress_default = adri@acmesub_ca.com

[ v3_ca ]

# Extensions to apply when createing root ca

# Extensions for a typical CA, man x509v3_config

subjectKeyIdentifier  = hash

authorityKeyIdentifier  = keyid:always,issuer

basicConstraints  = critical, CA:true

keyUsage   =  critical, digitalSignature, cRLSign, keyCertSign



[ v3_intermediate_ca ]

# Extensions to apply when creating intermediate or sub-ca

# Extensions for a typical intermediate CA, same man as above

subjectKeyIdentifier  = hash

authorityKeyIdentifier  = keyid:always,issuer

#pathlen:0 ensures no more sub-ca can be created below an intermediate
```

basicConstraints = critical, CA:true, pathlen:0

keyUsage   = critical, digitalSignature, cRLSign, keyCertSign

[server_cert]

# Extensions for server certificates
basicConstraints = CA:FALSE

nsCertType   = server

nsComment   = "OpenSSL Generated Server Certificate"

subjectKeyIdentifier = hash

authorityKeyIdentifier = keyid,issuer:always

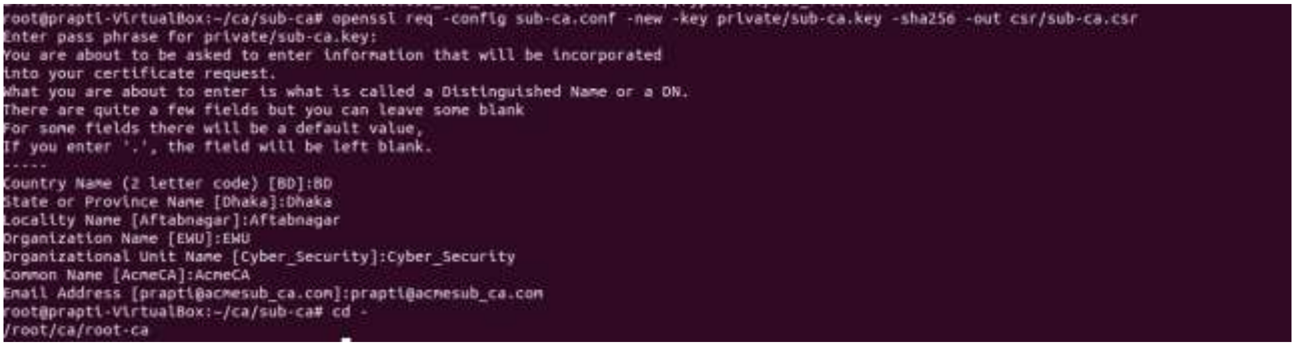
keyUsage   = critical, digitalSignature, keyEncipherment

extendedKeyUsage = serverAuth

[save and exit] (:wq then ctrl+c)

Requesting for sub ca certificate signing request

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



```
root@prapti-VirtualBox:~/ca/sub-ca# openssl req -config sub-ca.conf -new -key private/sub-ca.key -sha256 -out csr/sub-ca.csr
Enter pass phrase for 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 [Dhaka]:Dhaka
Locality Name [Aftabnagar]:Aftabnagar
Organization Name [EWU]:EWU
Organizational Unit Name [Cyber_Security]:Cyber_Security
Common Name [AcmeCA]:AcmeCA
Email Address [prapti@acmesub_ca.com]:prapti@acmesub_ca.com
root@prapti-VirtualBox:~/ca/sub-ca# cd -
/root/ca/root-ca
```

Now root ca signed sub-ca done

moving to the previous folder

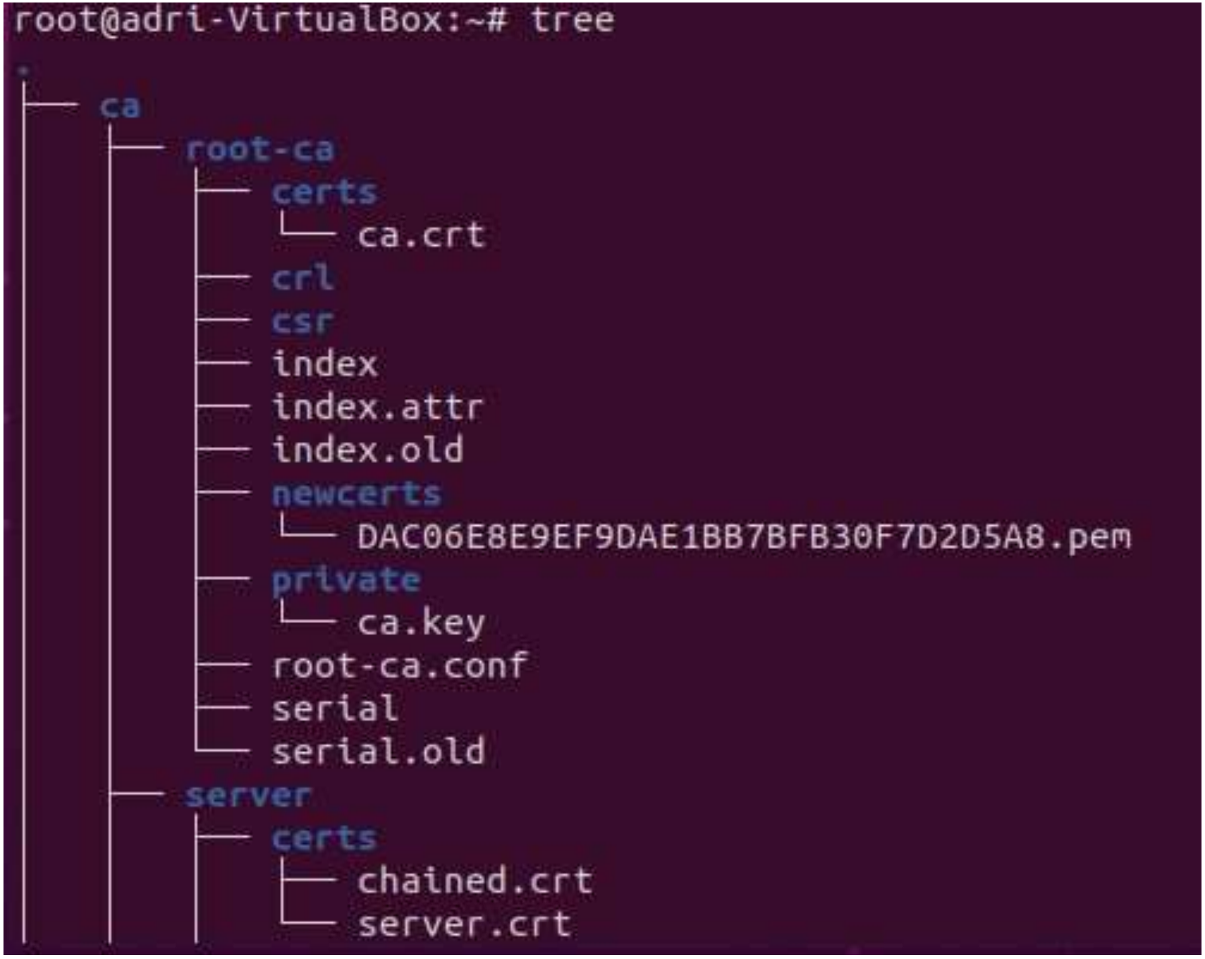
- cd –

Signing the request of sub ca by root ca

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

Now if we see directory Tree

→we can see a .pem file has been generated



```
root@adri-VirtualBox:~# tree
.
├── ca
│   ├── root-ca
│   │   ├── certs
│   │   │   └── ca.crt
│   │   ├── crl
│   │   ├── csr
│   │   ├── index
│   │   ├── index.attr
│   │   ├── index.old
│   │   ├── newcerts
│   │   │   └── DAC06E8E9EF9DAE1BB7BFB30F7D2D5A8.pem
│   │   ├── private
│   │   │   └── ca.key
│   │   ├── root-ca.conf
│   │   ├── serial
│   │   └── serial.old
│   ├── server
│   │   ├── certs
│   │   │   ├── chained.crt
│   │   │   └── server.crt
```

Root ca and sub-ca created a pem file.

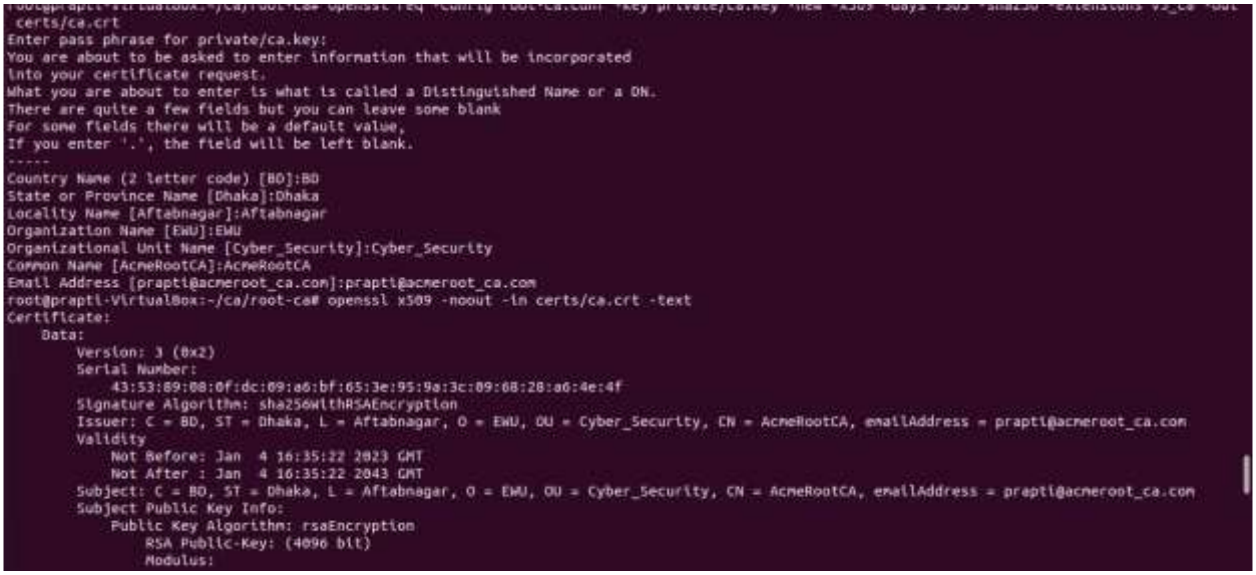
We can see the signing -

cat index

→Root ca signed sub ca

We can see the detail by

- openssl x509 -noout -in .certs/ca.crt text
- openssl x509 -noout -text -in ../sub-ca/certs/sub-ca.crt



```
root@prapti-VirtualBox:~/ca/root-ca# openssl req -config root-ca.conf -key private/ca.key -new -x509 -days 7305 -sha256 -extensions v3_ca -out
 certs/ca.crt
Enter pass phrase for 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 [Dhaka]:Dhaka
Locality Name [Aftabnagar]:Aftabnagar
Organization Name [EWU]:EWU
Organizational Unit Name [Cyber_Security]:Cyber_Security
Common Name [AcmeRootCA]:AcmeRootCA
Email Address [prapti@acmeroot_ca.com]:prapti@acmeroot_ca.com
root@prapti-VirtualBox:~/ca/root-ca# openssl x509 -noout -in certs/ca.crt -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            43:53:89:08:0f:dc:09:a6:bf:65:3e:95:9a:3c:09:68:28:a6:4e:4f
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = BD, ST = Dhaka, L = Aftabnagar, O = EWU, OU = Cyber_Security, CN = AcmeRootCA, emailAddress = prapti@acmeroot_ca.com
        Validity
            Not Before: Jan  4 16:35:22 2023 GMT
            Not After : Jan  4 16:35:22 2043 GMT
        Subject: C = BD, ST = Dhaka, L = Aftabnagar, O = EWU, OU = Cyber_Security, CN = AcmeRootCA, emailAddress = prapti@acmeroot_ca.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
```

Step 4: Configuring server

Moving to server

- cd ../server

Generating certificate signing request from server

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

Fill up the blanks carefully:

Common name: www.verysecureserver.com (domain name)

moving to sub ca to sign the server's certificate -
cd ../sub-ca

As root ca signed sub-ca, now sub-ca can also sign other servers.

Sub ca signing certificate request of server

- openssl ca -config sub-ca.conf -extensions server_cert -days 365 -notext - in ../server/csr/server.csr -out ../server/certs/server.crt

moving to certs folder to see certificate of server

- cd ../server/certs/

We can see the directory by using the command:

- ls → **We can see that the server.crt file has been generated**

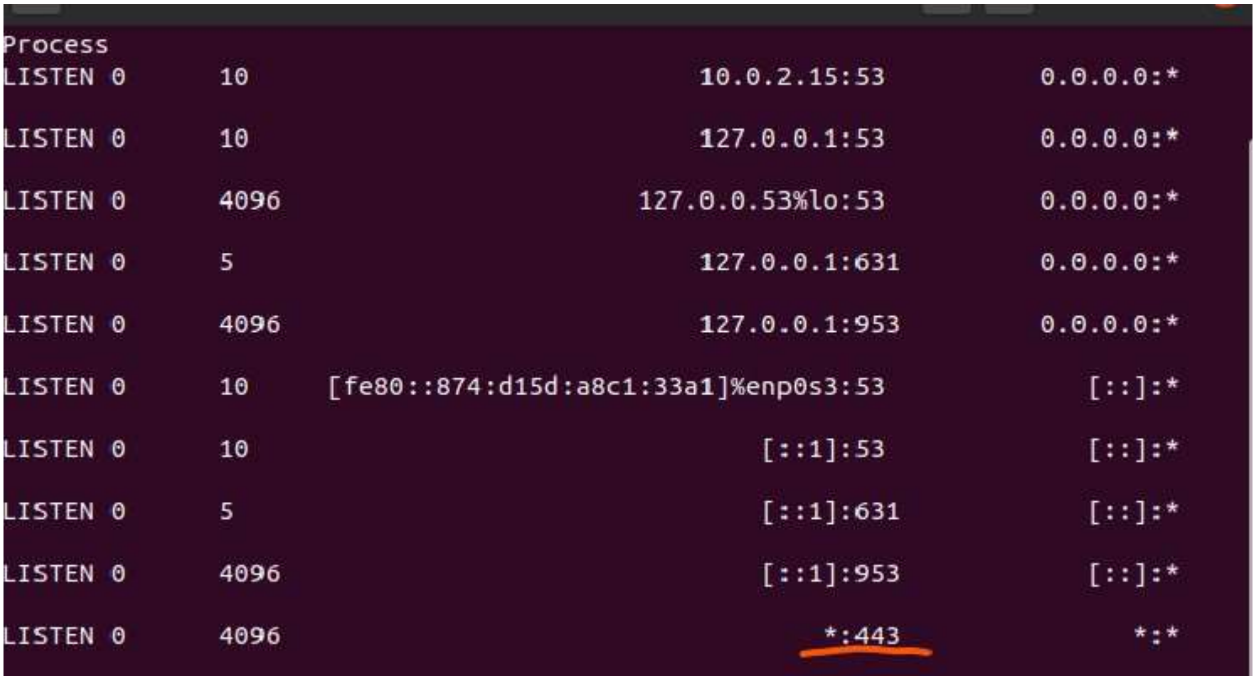
Now, concat sub-ca.crt and server.crt and naming the new file chained.crt -
cat server.crt ../../sub-ca/certs/sub-ca.crt > chained.crt

moving back to server directory
- cd ..

echo "127.0.0.2 www.verysecureserver.com" >> /etc/hosts ping
www.verysecureserver.com

Turning on the ssl port
- openssl s_server -accept 443 -www -key private/server.key -cert certs/server.crt - CAfile ../sub-ca/certs/sub-ca.crt

→Opening new terminal
Again to root
- sudo -i
See the port number used by different Ip addresses -
ss -nt



```
Process
LISTEN 0      10                              10.0.2.15:53          0.0.0.0:*

LISTEN 0      10                              127.0.0.1:53          0.0.0.0:*

LISTEN 0      4096                        127.0.0.53%lo:53          0.0.0.0:*

LISTEN 0      5                               127.0.0.1:631         0.0.0.0:*

LISTEN 0      4096                            127.0.0.1:953         0.0.0.0:*

LISTEN 0      10     [fe80::874:d15d:a8c1:33a1]%enp0s3:53             [::]:*

LISTEN 0      10                                  [::1]:53            [::]:*

LISTEN 0      5                                   [::1]:631           [::]:*

LISTEN 0      4096                                [::1]:953           [::]:*

LISTEN 0      4096                                    *:443              *:*
```

- **sudo apt update** to download or transfer files/data from or to a server using FTP, HTTP, HTTPS, SCP, SFTP, SMB, and other supported protocols, installing curl:

- **sudo apt install curl**

copying the certificate to ca certificate folder
- cp ca/root-ca/certs/ca.crt /usr/local/share/ca-certificates/

Updating ca certificate folder

- update-ca-certificates -v done

Exit_new_terminal

Now we have to install xampp and follow the following proceedure-

At first Download and install xampp-> https://www.apachefriends.org/download.html
----
[In download folder, edit file name xampp.run then open terminal here]

```
$ sudo -s
# sudo chmod a+rwx xampp.run
# ./xampp.run
```

[N.B: If you have apache already, remove it]

```
$ systemctl status apache2
$ sudo apt-get purge apache2 apache2-utils apache2.2-bin apache2-common
$ sudo apt-get autoremove
$ systemctl status apache2
```

TO START XAMPP

```
$ sudo -i
# cd /opt/lampp
# chmod a+rwx manager-linux-x64.run
# ./manager-linux-x64.run
```

Next go to this location from your linux host

----
other Location/Computer/opt/lampp/etc/extra
[open terminal here]

```
$ sudo su
# chmod 777 httpd-ssl.conf
```

line 110 ---------

change server.crt location with your server.crt file location {110 SSLCertificateFile "/home/adri/certificate/server.crt"}

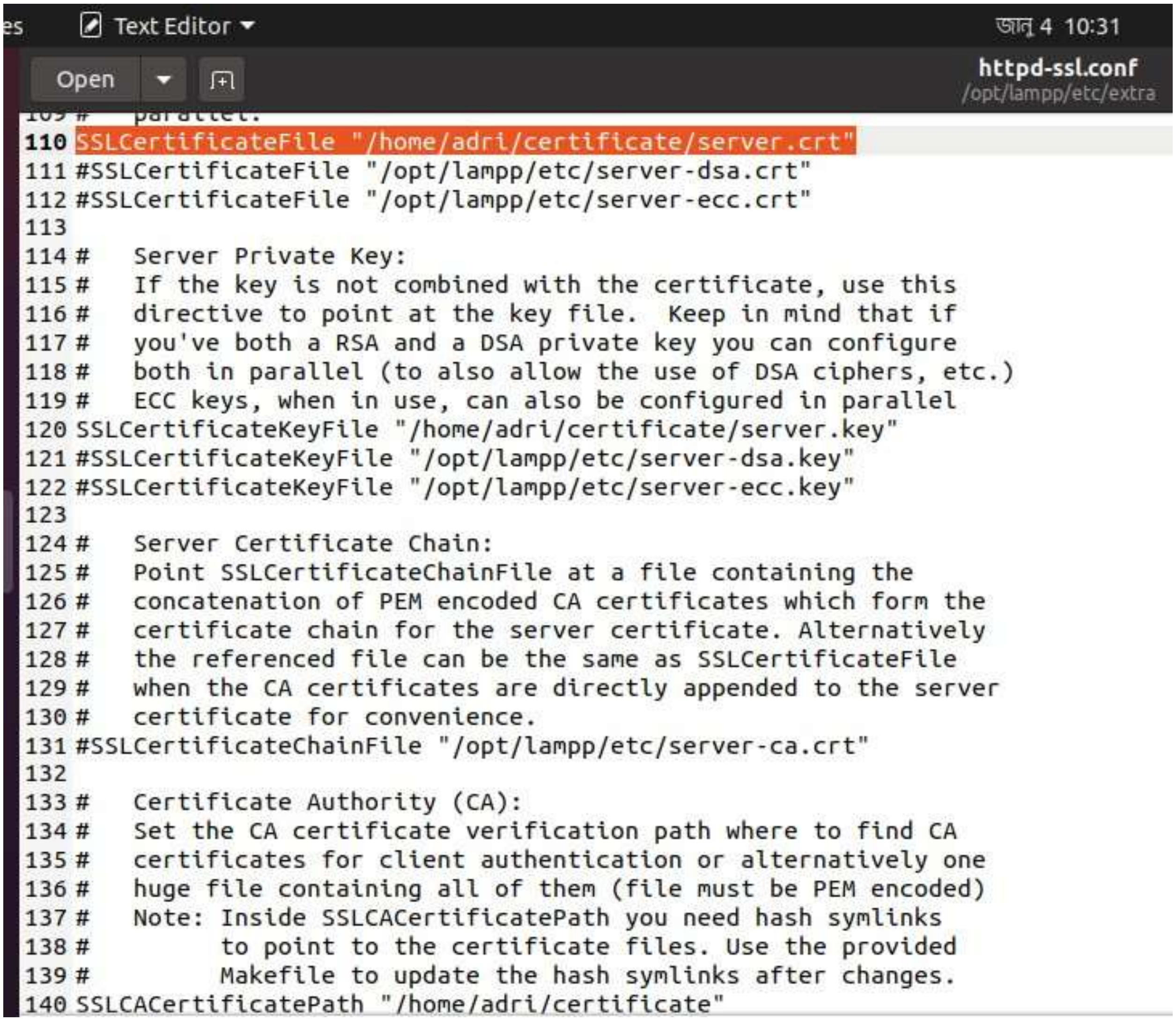
line 120 ---------

change server.key location with your server.key file location {120 SSLCertificateKeyFile "/home/adri/certificate/server.key"}

line 140

----

change full line with your location
{140 SSLCACertificatePath "/home/adri/certificate"}



```
109 #    parallel.
110 SSLCertificateFile "/home/adri/certificate/server.crt"
111 #SSLCertificateFile "/opt/lampp/etc/server-dsa.crt"
112 #SSLCertificateFile "/opt/lampp/etc/server-ecc.crt"
113
114 #   Server Private Key:
115 #   If the key is not combined with the certificate, use this
116 #   directive to point at the key file.  Keep in mind that if
117 #   you've both a RSA and a DSA private key you can configure
118 #   both in parallel (to also allow the use of DSA ciphers, etc.)
119 #   ECC keys, when in use, can also be configured in parallel
120 SSLCertificateKeyFile "/home/adri/certificate/server.key"
121 #SSLCertificateKeyFile "/opt/lampp/etc/server-dsa.key"
122 #SSLCertificateKeyFile "/opt/lampp/etc/server-ecc.key"
123
124 #   Server Certificate Chain:
125 #   Point SSLCertificateChainFile at a file containing the
126 #   concatenation of PEM encoded CA certificates which form the
127 #   certificate chain for the server certificate. Alternatively
128 #   the referenced file can be the same as SSLCertificateFile
129 #   when the CA certificates are directly appended to the server
130 #   certificate for convenience.
131 #SSLCertificateChainFile "/opt/lampp/etc/server-ca.crt"
132
133 #   Certificate Authority (CA):
134 #   Set the CA certificate verification path where to find CA
135 #   certificates for client authentication or alternatively one
136 #   huge file containing all of them (file must be PEM encoded)
137 #   Note: Inside SSLCACertificatePath you need hash symlinks
138 #         to point to the certificate files. Use the provided
139 #         Makefile to update the hash symlinks after changes.
140 SSLCACertificatePath "/home/adri/certificate"
```

Now we have to remove all file from htdocs

-- [open new terminal]

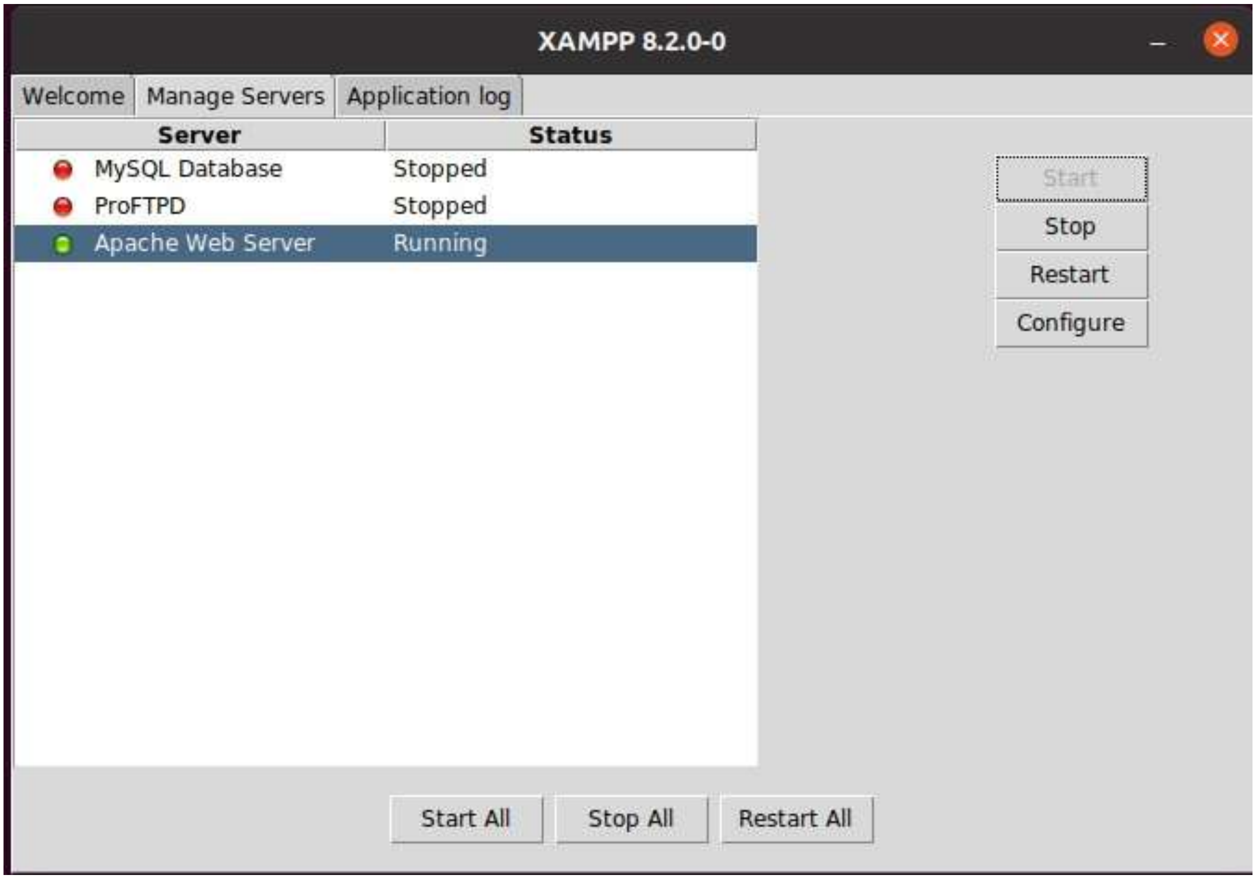
```
$ sudo -i
# cd /opt/lampp/htdocs
# ls
# rm -r dashboard img webalizer
# rm applications.html bitnami.css favicon.ico index.php
```

[Now make a html file and write some html code]
# touch index.html
# gedit index.html
//here I write following html file:

```
<!DOCTYPE html>
<html>
    <head>
        <title> HTML Input type file </title>
        <!--CSS code-->
<style>            h1 {
color: green;
            }
h2,
h3 {
                font-family: Impact;
            }
            body {            text-
align: center;
            }
        </style>
    </head>

    <body>
        <h2> File Upload System </h2>
        <h3>

        </h3>
        <label> Choose the file to upload: </label>
        <input type="submit" value="submit" />
    </body>
</html>
```

save and exit.
Before installation certificate from localhost

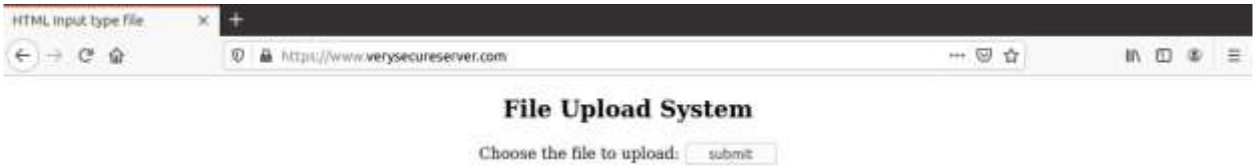
Make sure Xampp Apache server is running before.



Server	Status
🟥 MySQL Database	Stopped
🟥 ProFTPD	Stopped
🟩 Apache Web Server	Running

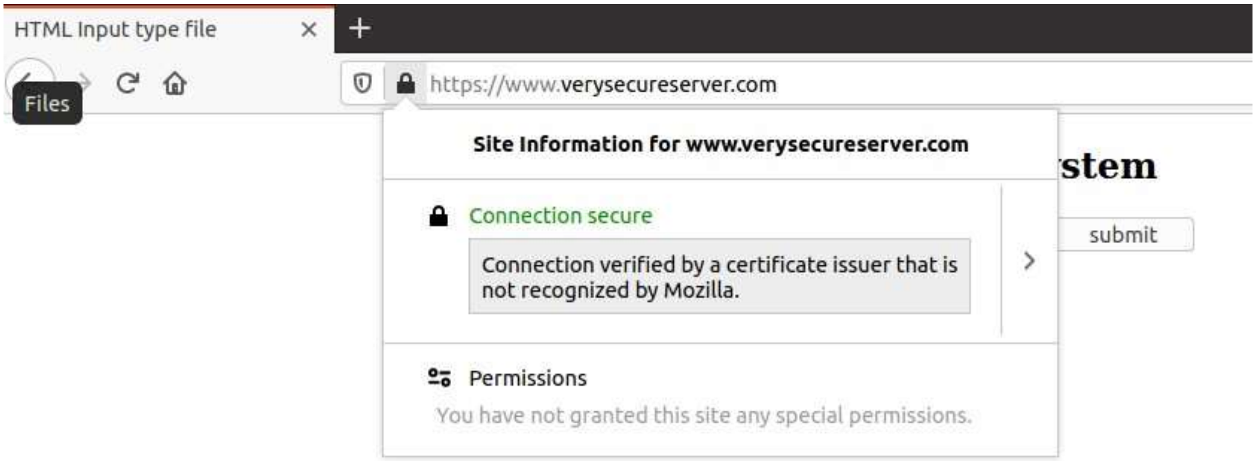
By clicking any browser on ubuntu terminal: www.verysecureserver.com

After install certificate:



File Upload System

Choose the file to upload: submit



Site Information for www.verysecureserver.com

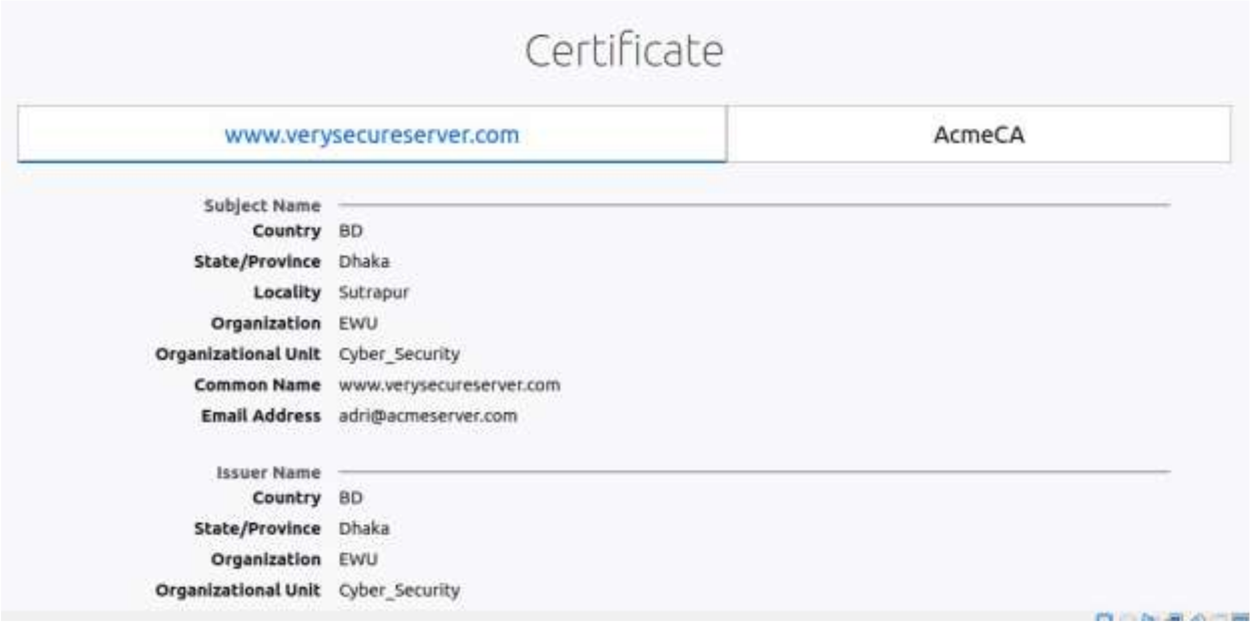
Connection secure

Connection verified by a certificate issuer that is not recognized by Mozilla.

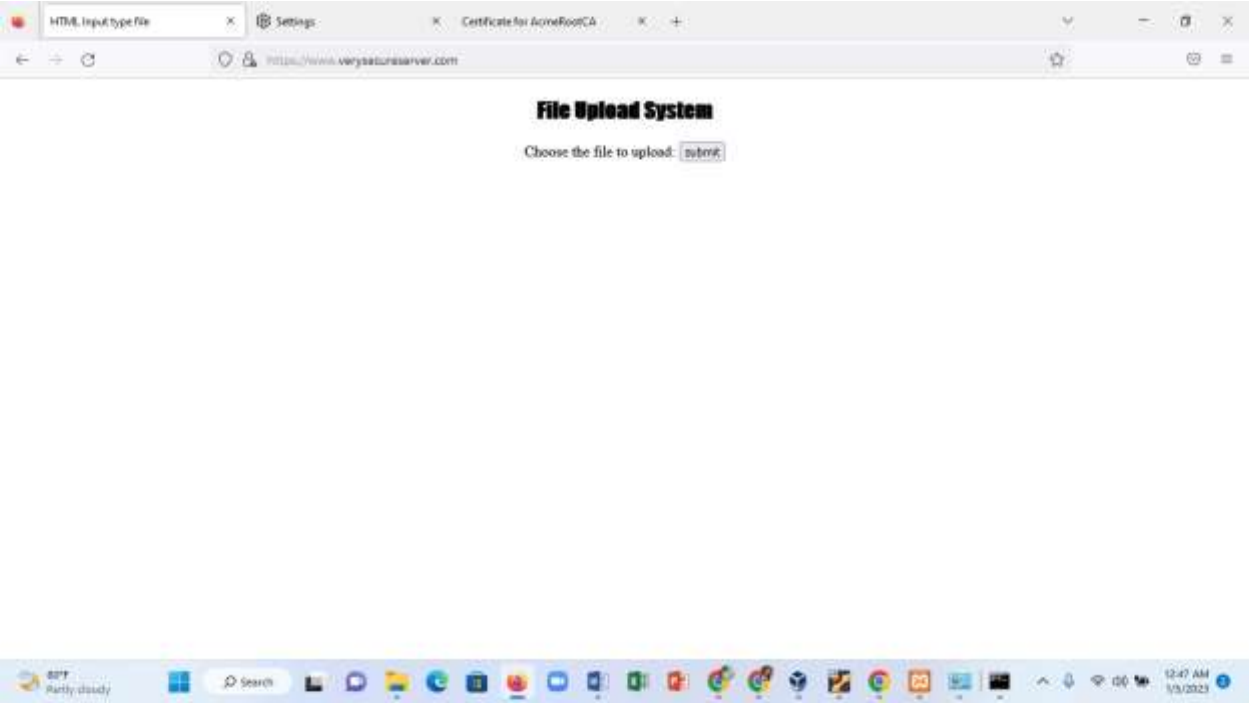
Permissions

You have not granted this site any special permissions.

Certificate:

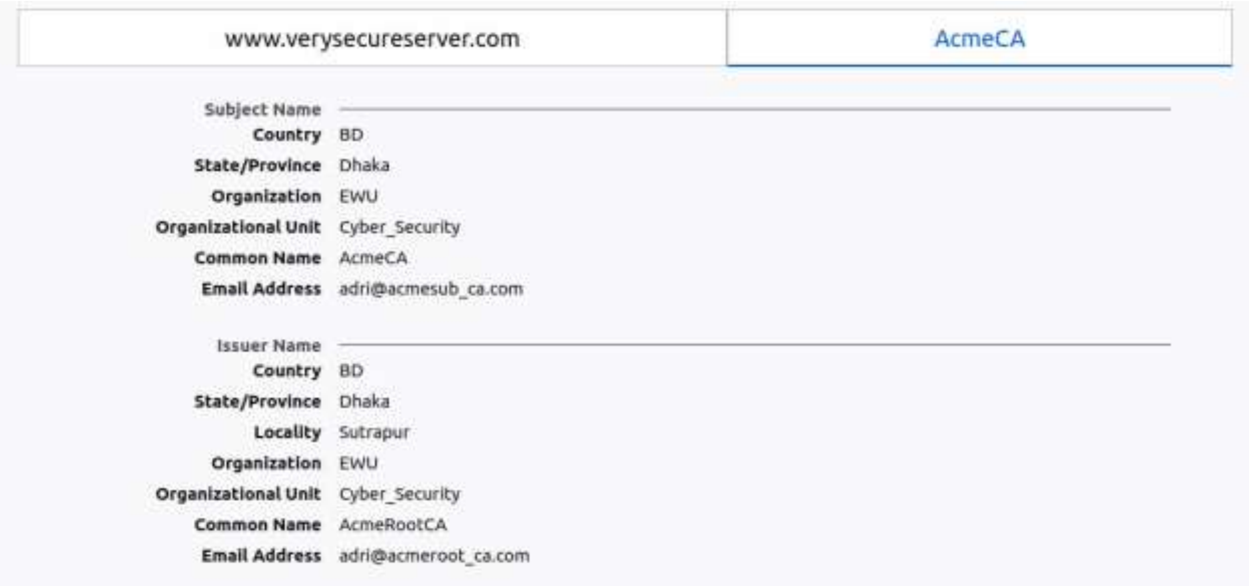


Subject Name	
Country	BD
State/Province	Dhaka
Locality	Sutrapur
Organization	EWU
Organizational Unit	Cyber_Security
Common Name	www.verysecureserver.com
Email Address	adri@acmeserver.com
Issuer Name	
Country	BD
State/Province	Dhaka
Organization	EWU
Organizational Unit	Cyber_Security



File Upload System

Choose the file to upload: submit



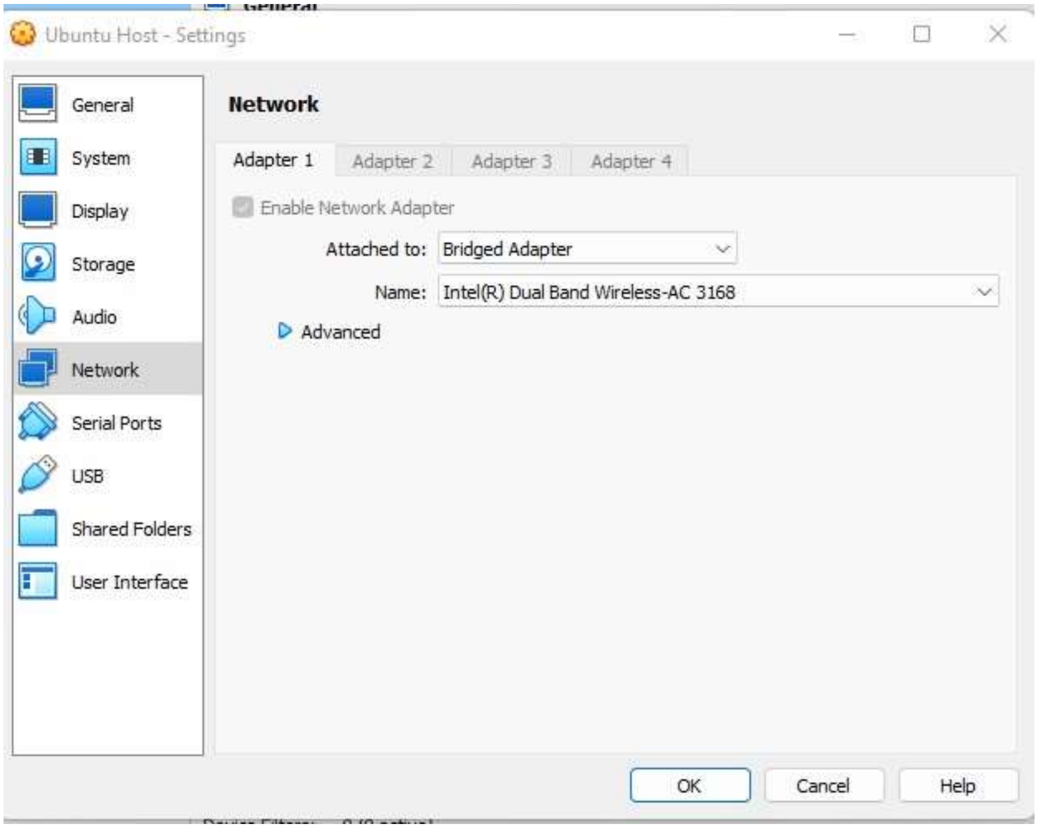
Subject Name	
Country	BD
State/Province	Dhaka
Organization	EWU
Organizational Unit	Cyber_Security
Common Name	AcmeCA
Email Address	adri@acmesub_ca.com
Issuer Name	
Country	BD
State/Province	Dhaka
Locality	Sutrapur
Organization	EWU
Organizational Unit	Cyber_Security
Common Name	AcmeRootCA
Email Address	adri@acmeroot_ca.com

DNS Configuration

In this case, we can go to our domain ‘www.verysecureserver.com’ or IP address of host and find the html page on other server globally by configuring DNS (Domain Name System). In this case, I on my mobile data and connect with my PC’s wifi while configuring DNS to set my mobile internet IP. After host configuring the DNS with client, without any certification, apache server client can access verysecureserver page which is already secured and certified by ROOT CA of hosts.

By following below steps we can do it easily:

Change Virtual Box Network to Bridge Adapter



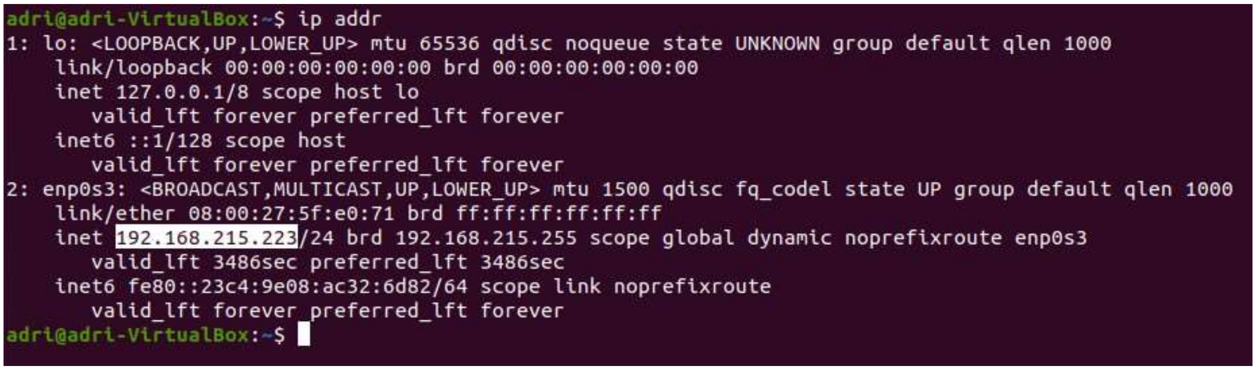
☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: Intel(R) Dual Band Wireless-AC 3168

Step 1: First, check your IP address.

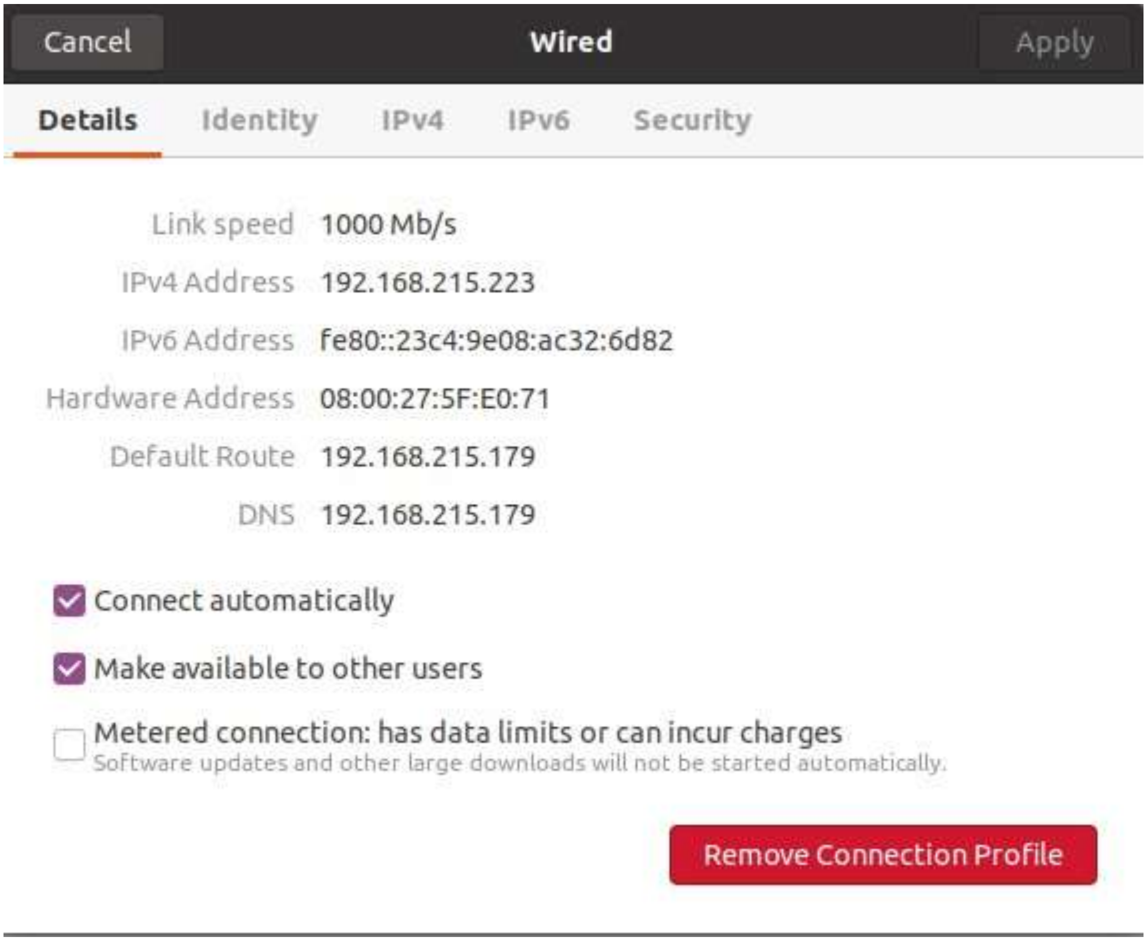
- Ip addr



```
adri@adri-VirtualBox:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5f:e0:71 brd ff:ff:ff:ff:ff:ff
    inet 192.168.215.223/24 brd 192.168.215.255 scope global dynamic noprefixroute enp0s3
       valid_lft 3486sec preferred_lft 3486sec
    inet6 fe80::23c4:9e08:ac32:6d82/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
adri@adri-VirtualBox:~$
```

My IP address is: 192.168.215.223

Check this by the setting option: Here note down IPv4 address, default Route and DNS.



Link speed 1000 Mb/s
IPv4 Address 192.168.215.223
IPv6 Address fe80::23c4:9e08:ac32:6d82
Hardware Address 08:00:27:5F:E0:71
Default Route 192.168.215.179
DNS 192.168.215.179

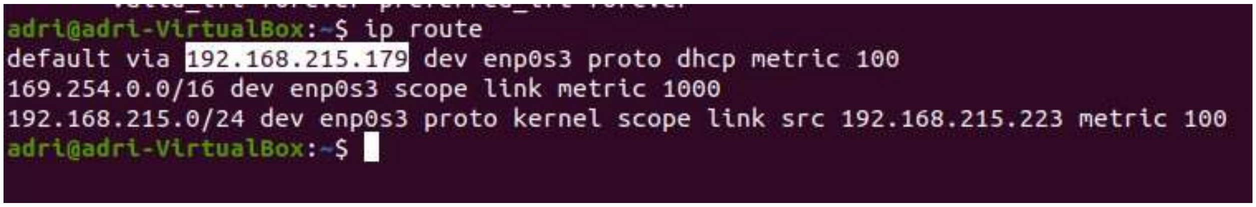
☑ Connect automatically

☑ Make available to other users

□ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.

DNS: 192.168.215.179

- IP route

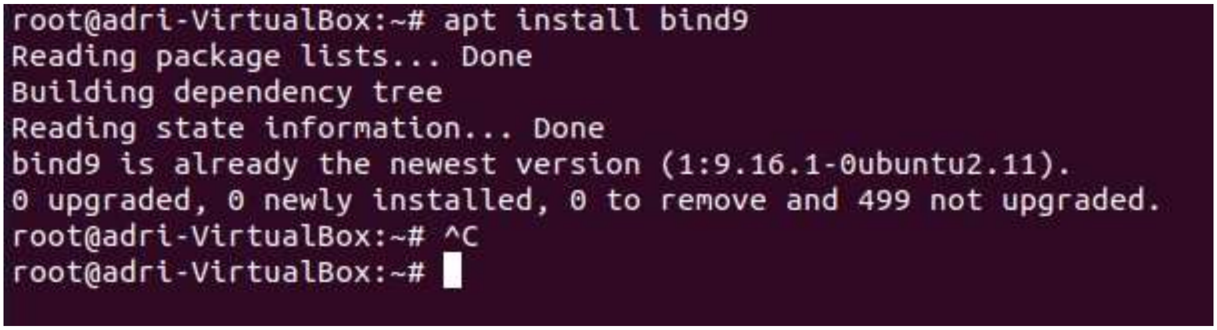


```
       valid_lft forever preferred_lft forever
adri@adri-VirtualBox:~$ ip route
default via 192.168.215.179 dev enp0s3 proto dhcp metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.215.0/24 dev enp0s3 proto kernel scope link src 192.168.215.223 metric 100
adri@adri-VirtualBox:~$ 
```

Default address: 192.168.215.179

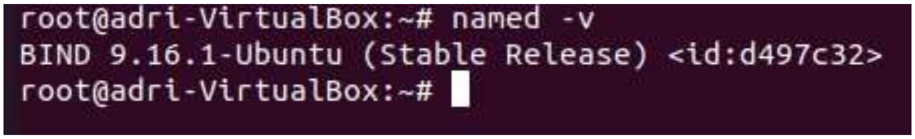
Install bind9:

- apt install bind9



```
root@adri-VirtualBox:~# apt install bind9
Reading package lists... Done
Building dependency tree
Reading state information... Done
bind9 is already the newest version (1:9.16.1-0ubuntu2.11).
0 upgraded, 0 newly installed, 0 to remove and 499 not upgraded.
root@adri-VirtualBox:~# ^C
root@adri-VirtualBox:~# █
```

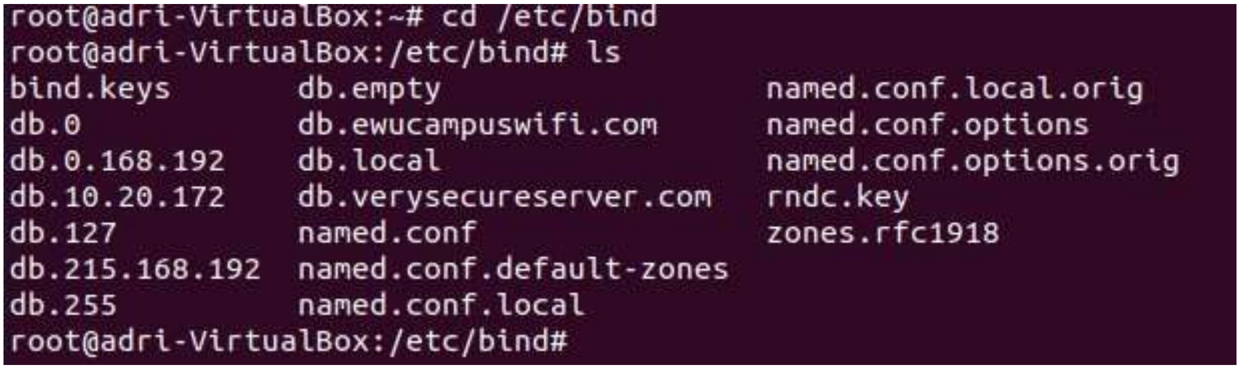
Check version of bind9:
-named -v



```
root@adri-VirtualBox:~# named -v
BIND 9.16.1-Ubuntu (Stable Release) <id:d497c32>
root@adri-VirtualBox:~# █
```

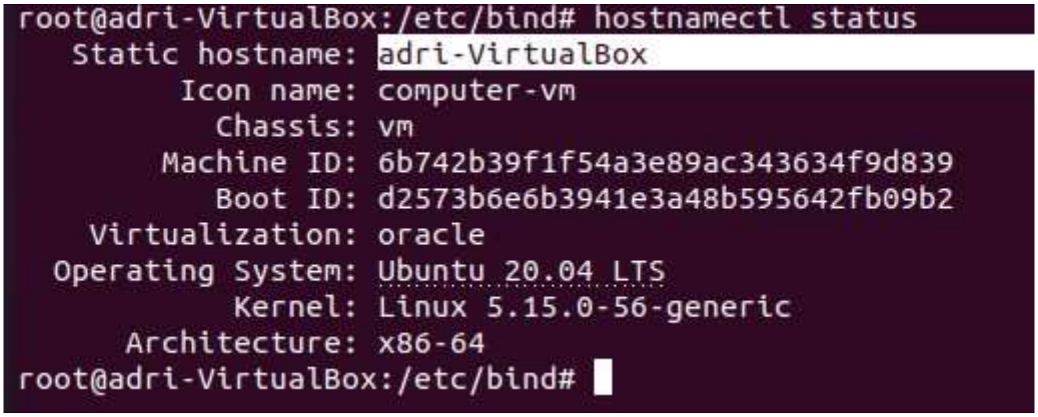
Go to bind folder and check files:

- cd /etc/bind



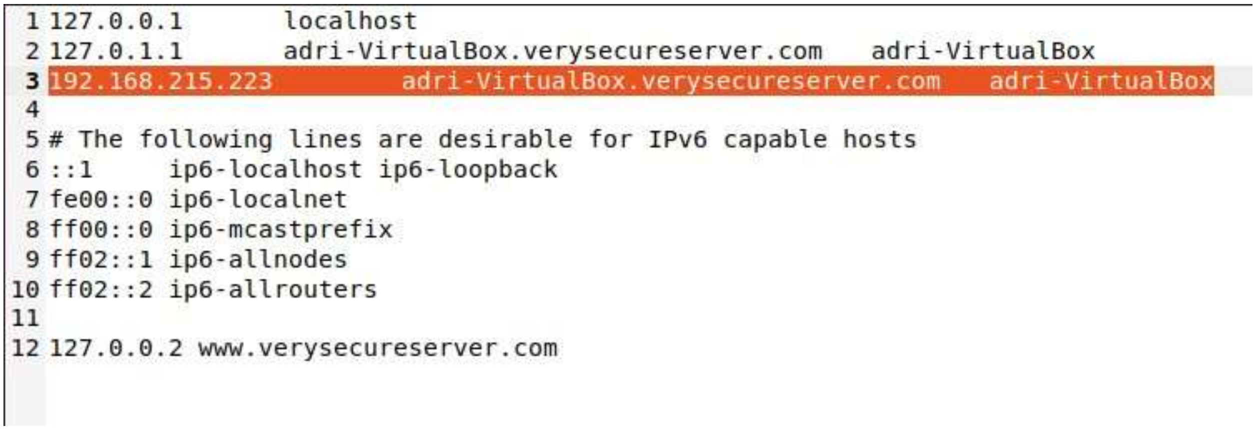
```
root@adri-VirtualBox:~# cd /etc/bind
root@adri-VirtualBox:/etc/bind# ls
bind.keys        db.empty                  named.conf.local.orig
db.0             db.ewucampuswifi.com      named.conf.options
db.0.168.192     db.local                  named.conf.options.orig
db.10.20.172     db.verysecureserver.com   rndc.key
db.127           named.conf                zones.rfc1918
db.215.168.192   named.conf.default-zones
db.255           named.conf.local
root@adri-VirtualBox:/etc/bind#
```

Step 2: Check status if the machine: Here the important thing is static hostname.



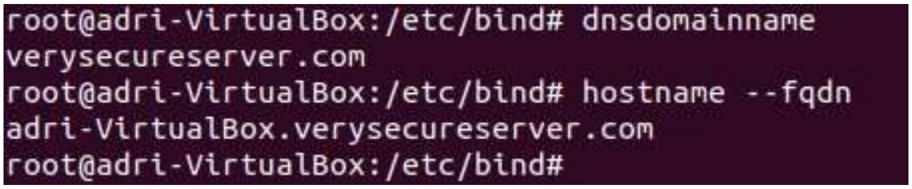
```
root@adri-VirtualBox:/etc/bind# hostnamectl status
   Static hostname: adri-VirtualBox
         Icon name: computer-vm
           Chassis: vm
        Machine ID: 6b742b39f1f54a3e89ac343634f9d839
           Boot ID: d2573b6e6b3941e3a48b595642fb09b2
    Virtualization: oracle
  Operating System: Ubuntu 20.04 LTS
            Kernel: Linux 5.15.0-56-generic
      Architecture: x86-64
root@adri-VirtualBox:/etc/bind# █
```

1. Use the hostname and the domain name to edit the hosts file:



```
127.0.0.1       localhost
127.0.1.1       adri-VirtualBox.verysecureserver.com    adri-VirtualBox
192.168.215.223         adri-VirtualBox.verysecureserver.com    adri-VirtualBox

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

127.0.0.2 www.verysecureserver.com
```

2. Verify hostname, dns domain name, and fully qualified domain name respectively:

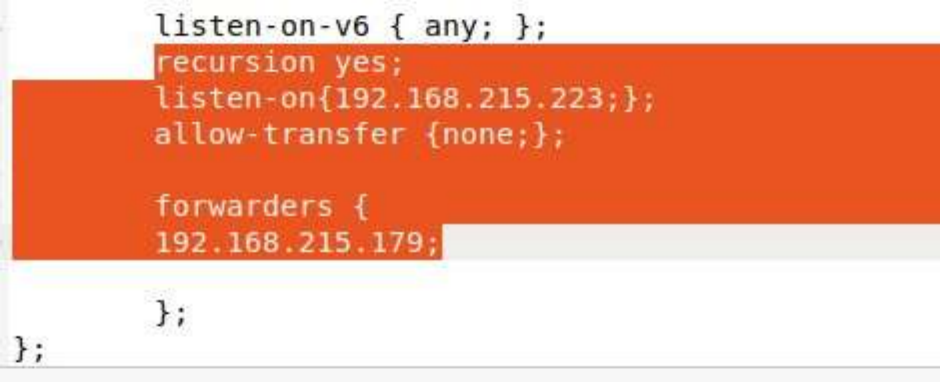


```
root@adri-VirtualBox:/etc/bind# dnsdomainname
verysecureserver.com
root@adri-VirtualBox:/etc/bind# hostname --fqdn
adri-VirtualBox.verysecureserver.com
root@adri-VirtualBox:/etc/bind#
```

Step 3: Configure named.conf.options

- cp named.conf.options named.conf.options.orig

As my default: 192.168.215.179
ipv4: 192.168.215.223/24



```
        listen-on-v6 { any; };
        recursion yes;
        listen-on{192.168.215.223;};
        allow-transfer {none;};

        forwarders {
        192.168.215.179;

        };
};
```

- cp named.conf.local named.conf.local.orig
- gedit named.conf.local

*192.168.215.223 is the machine IP where you are going to configure your server.
*192.168.215.179 is the default gateway for the LAN you created.

3. **Make forward lookup zone and reverse lookup zone**

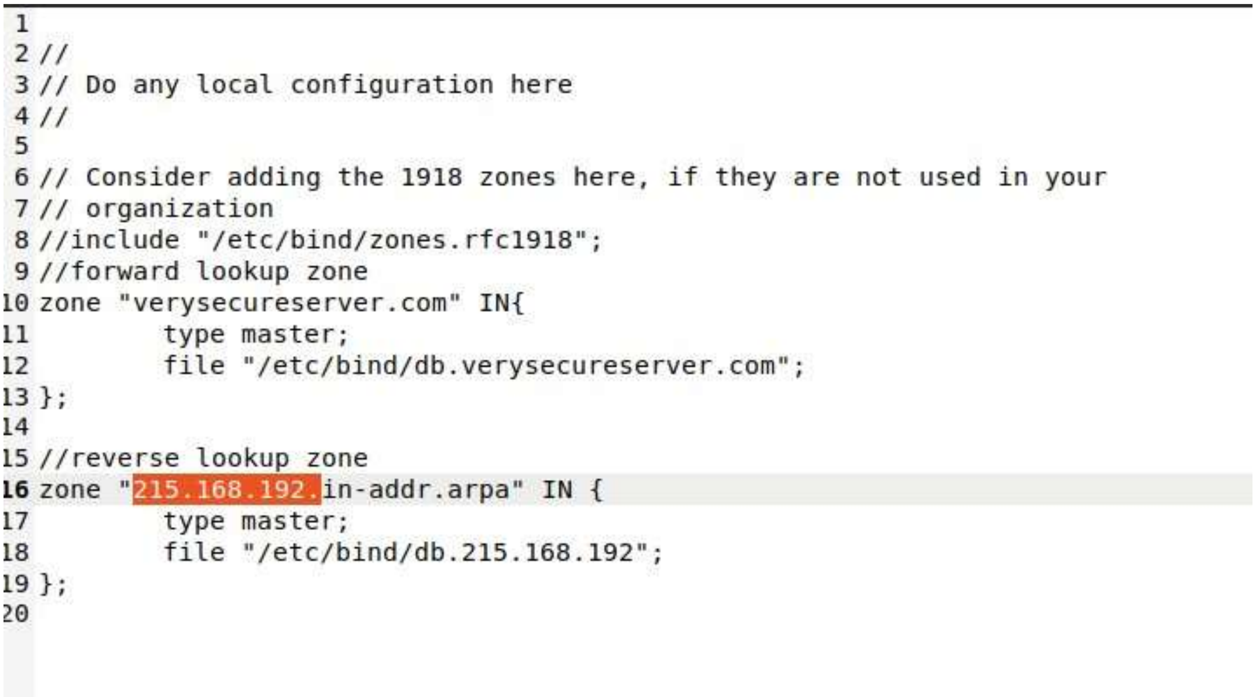
A- make a copy of

- named.conf.local sudo cp named.conf.local named.conf.local.orig

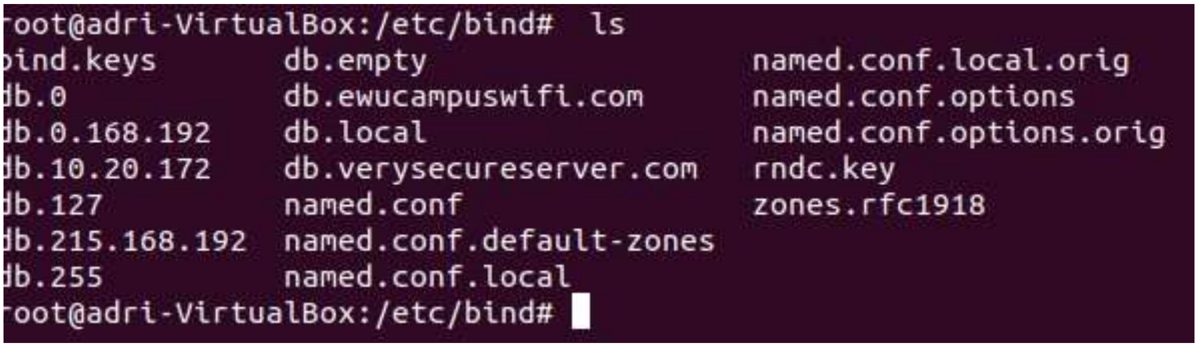
B – edit named.conf.local

- sudo gedit named.conf.local Here, create a forward lookup zone and a reverse lookup zone

Give reverse ip there:



```

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
//forward lookup zone
zone "verysecureserver.com" IN{
        type master;
        file "/etc/bind/db.verysecureserver.com";
};

//reverse lookup zone
zone "215.168.192.in-addr.arpa" IN {
        type master;
        file "/etc/bind/db.215.168.192";
};

```



```
root@adri-VirtualBox:/etc/bind#  ls
bind.keys       db.empty                 named.conf.local.orig
db.0            db.ewucampuswifi.com     named.conf.options
db.0.168.192    db.local                 named.conf.options.orig
db.10.20.172    db.verysecureserver.com  rndc.key
db.127          named.conf               zones.rfc1918
db.215.168.192  named.conf.default-zones
db.255          named.conf.local
root@adri-VirtualBox:/etc/bind# 
```

Step 4:

Make records for forward and reverse lookup zone database

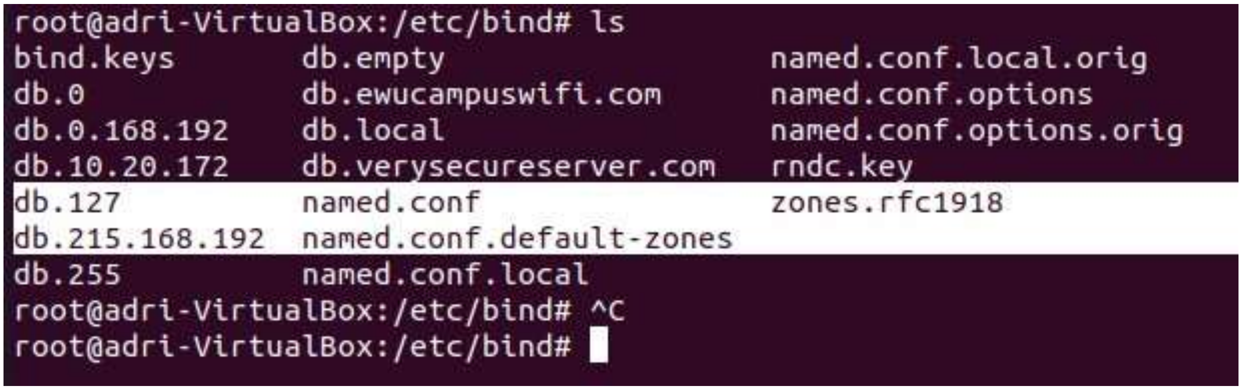
A – copy db.local to db.mysecureserver.com (which you mentioned in named.conf.local) sudo cp db.local db.mysecureserver.com Edit db.mysecureserver.com:
After editing:

- cp db.local db.verysecureserver.com

  Replace full code with:

  ```
  ;
  ; BIND data file for local loopback interface
  ;
  $TTL 604800
  @       IN      SOA     ns1.verysecureserver.com. root.verysecureserver.com. (
                              2           ; Serial
                           604800                 ; Refresh
                            86400                 ; Retry
                          2419200                 ; Expire
                           604800 )       ; Negative Cache TTL
  ;
  @       IN      NS      ns1.verysecureserver.com.
  ns1     IN      A       192.168.215.223
  www IN          A       192.168.215.223
  ftp     IN      A       192.168.215.223
  @       IN      MX      10      mail
  mail    in      A       192.168.0.20
  @       IN      AAAA ::1
  ```

  Check file is ok or not
- named-checkzone verysecureserver.com db.verysecureserver.com



```
root@adri-VirtualBox:/etc/bind# ls
bind.keys        db.empty                  named.conf.local.orig
db.0             db.ewucampuswifi.com      named.conf.options
db.0.168.192     db.local                  named.conf.options.orig
db.10.20.172     db.verysecureserver.com   rndc.key
db.127           named.conf                zones.rfc1918
db.215.168.192   named.conf.default-zones
db.255           named.conf.local
root@adri-VirtualBox:/etc/bind# ^C
root@adri-VirtualBox:/etc/bind# 
```

B- copy db.127 to db.31.168.192 file (which you mentioned in named.conf.local in reverse lookup zone)

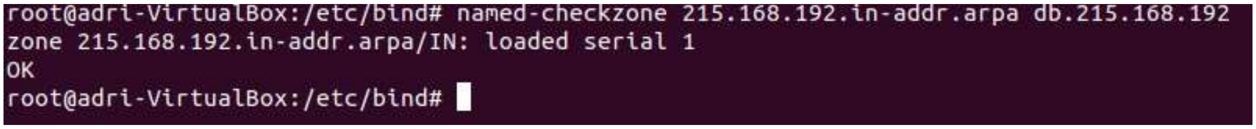
- cp db.127 db.215.168.192
- gedit db.215.168.192

[Replace full file with that text]

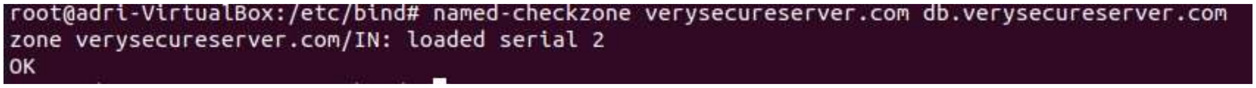
```
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@       IN      SOA     ns1.verysecureserver.com. root.verysecureserver.com. (
                              1           ; Serial
                         604800                 ; Refresh
                          86400                 ; Retry
                        2419200                 ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.verysecureserver.com.
24      IN      PTR     ns1.verysecureserver.com. //here 20 is last host part of your ip 24
IN      PTR     www.verysecureserver.com.
24      IN      PTR     ftp.verysecureserver.com.
24      IN      PTR     mail.verysecureserver.com.
```

[Save and exit]

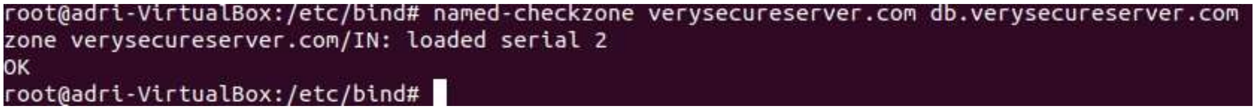
Check:



```
root@adri-VirtualBox:/etc/bind# named-checkzone 215.168.192.in-addr.arpa db.215.168.192
zone 215.168.192.in-addr.arpa/IN: loaded serial 1
OK
root@adri-VirtualBox:/etc/bind# 
```



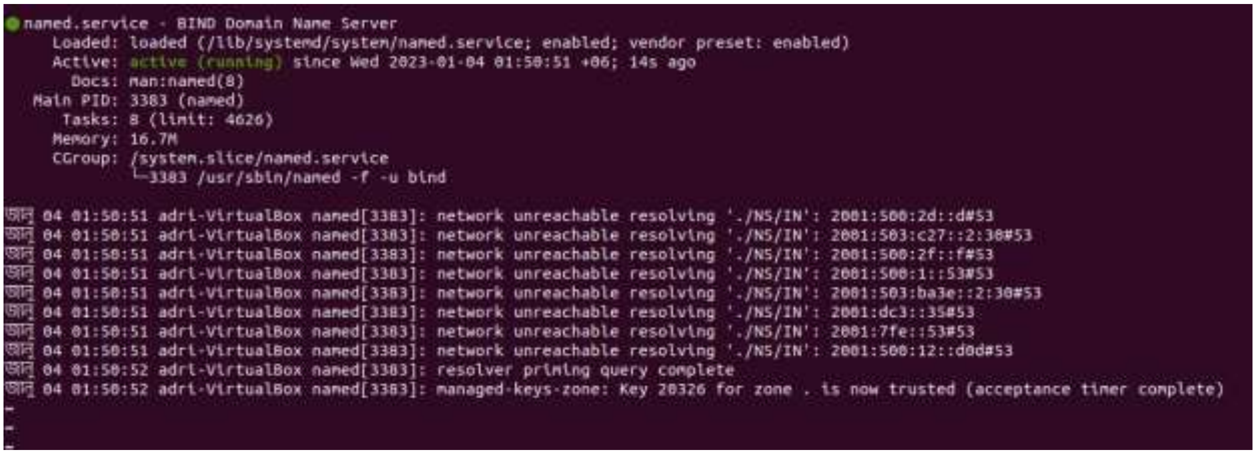
```
root@adri-VirtualBox:/etc/bind# named-checkzone verysecureserver.com db.verysecureserver.com
zone verysecureserver.com/IN: loaded serial 2
OK
```



```
root@adri-VirtualBox:/etc/bind# named-checkzone verysecureserver.com db.verysecureserver.com
zone verysecureserver.com/IN: loaded serial 2
OK
root@adri-VirtualBox:/etc/bind# 
```

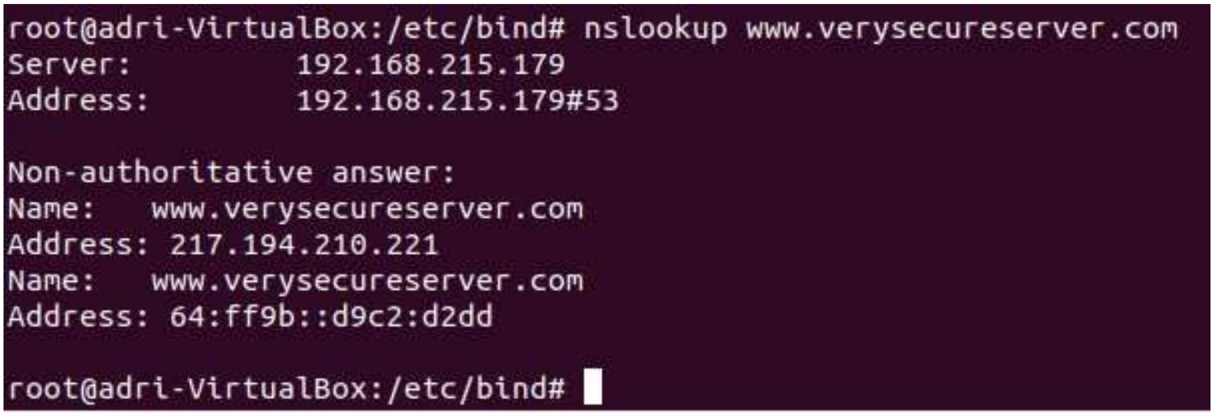
Step 5: Restart bind9 and check status

- service bind9 restart
- service bind9 status

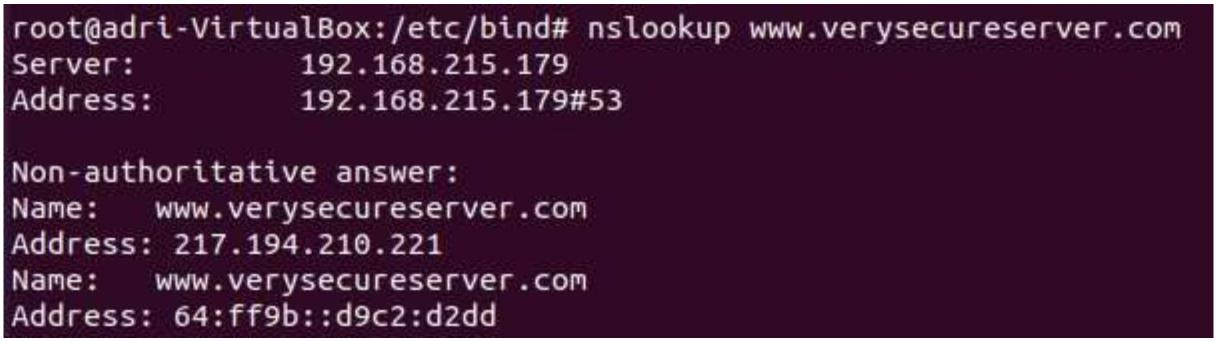


```
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-01-04 01:50:51 +06; 14s ago
       Docs: man:named(8)
   Main PID: 3383 (named)
      Tasks: 8 (limit: 4626)
     Memory: 16.7M
     CGroup: /system.slice/named.service
             └─3383 /usr/sbin/named -f -u bind

জানু 04 01:50:51 adri-VirtualBox named[3383]: network unreachable resolving './NS/IN': 2001:500:2d::d#53
জানু 04 01:50:51 adri-VirtualBox named[3383]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
জানু 04 01:50:51 adri-VirtualBox named[3383]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
জানু 04 01:50:51 adri-VirtualBox named[3383]: network unreachable resolving './NS/IN': 2001:500:1::53#53
জানু 04 01:50:51 adri-VirtualBox named[3383]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
জানু 04 01:50:51 adri-VirtualBox named[3383]: network unreachable resolving './NS/IN': 2001:dc3::35#53
জানু 04 01:50:51 adri-VirtualBox named[3383]: network unreachable resolving './NS/IN': 2001:7fe::53#53
জানু 04 01:50:51 adri-VirtualBox named[3383]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
জানু 04 01:50:52 adri-VirtualBox named[3383]: resolver priming query complete
জানু 04 01:50:52 adri-VirtualBox named[3383]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
~
~
~
```

- nslookup www.verysecureserver.com

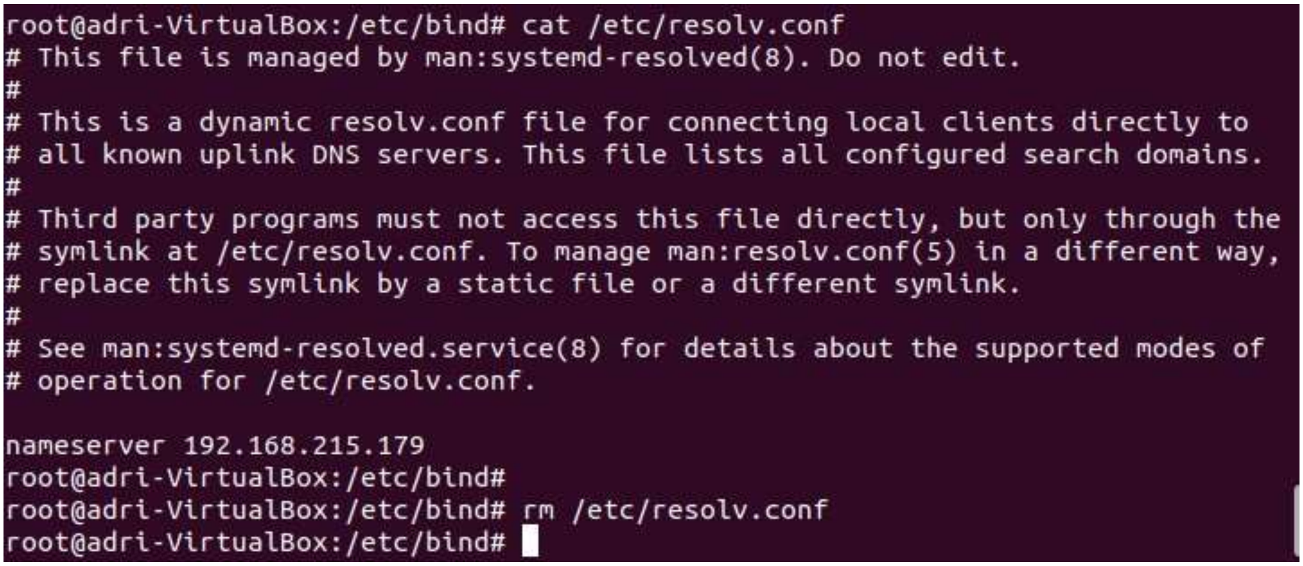


```
root@adri-VirtualBox:/etc/bind# nslookup www.verysecureserver.com
Server:         192.168.215.179
Address:        192.168.215.179#53

Non-authoritative answer:
Name:   www.verysecureserver.com
Address: 217.194.210.221
Name:   www.verysecureserver.com
Address: 64:ff9b::d9c2:d2dd

root@adri-VirtualBox:/etc/bind# 
```



```
root@adri-VirtualBox:/etc/bind# nslookup www.verysecureserver.com
Server:         192.168.215.179
Address:        192.168.215.179#53

Non-authoritative answer:
Name:   www.verysecureserver.com
Address: 217.194.210.221
Name:   www.verysecureserver.com
Address: 64:ff9b::d9c2:d2dd
```

Step 6: Didn’t match with IP. So, remove the resolv.conf file. -
sudo rm /etc/resolv.conf



```
root@adri-VirtualBox:/etc/bind# cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients directly to
# all known uplink DNS servers. This file lists all configured search domains.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 192.168.215.179
root@adri-VirtualBox:/etc/bind#
root@adri-VirtualBox:/etc/bind# rm /etc/resolv.conf
root@adri-VirtualBox:/etc/bind# 
```

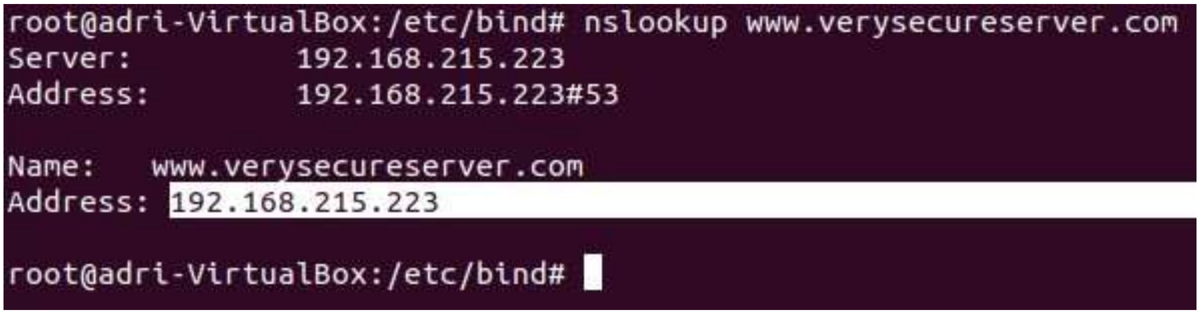
Step 7: Link up resolv.conf: ln -sf
/run/systemd/resolve/resolv.conf /etc/resolv.conf

gedit /etc/resolv.conf

[Replace last line with that text]

nameserver 192.168.215.223 //ipv4
nameserver 192.168.215.179 //default search
verysecureserver.com

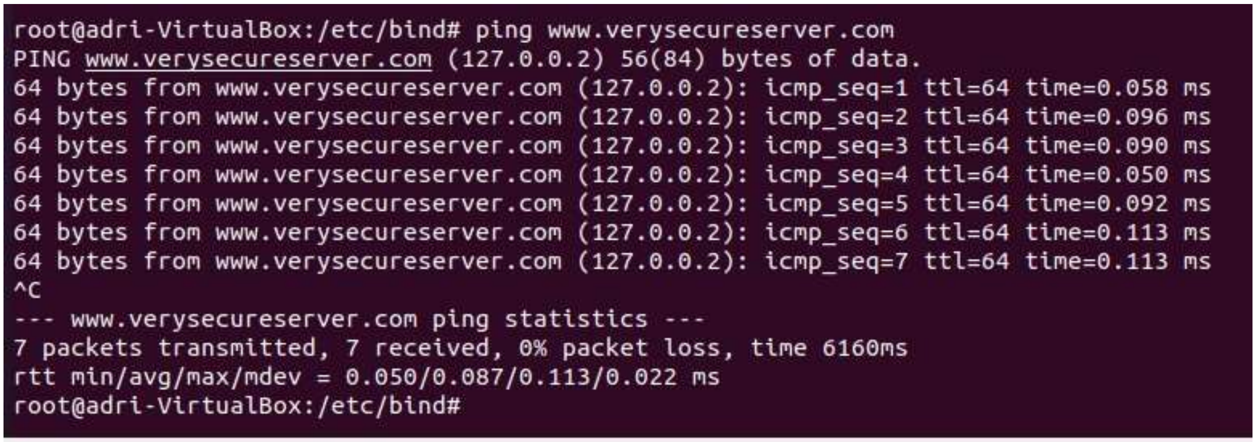
[Save and exit]



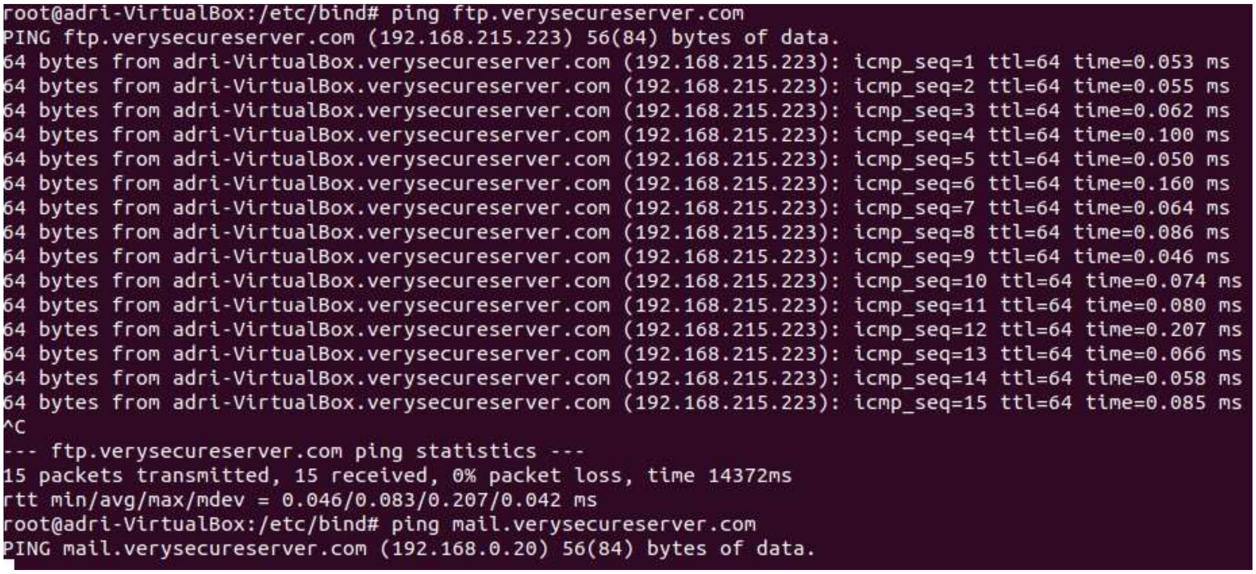
```
root@adri-VirtualBox:/etc/bind# nslookup www.verysecureserver.com
Server:         192.168.215.223
Address:        192.168.215.223#53

Name:   www.verysecureserver.com
Address: 192.168.215.223

root@adri-VirtualBox:/etc/bind# 
```

Step 8: Checking

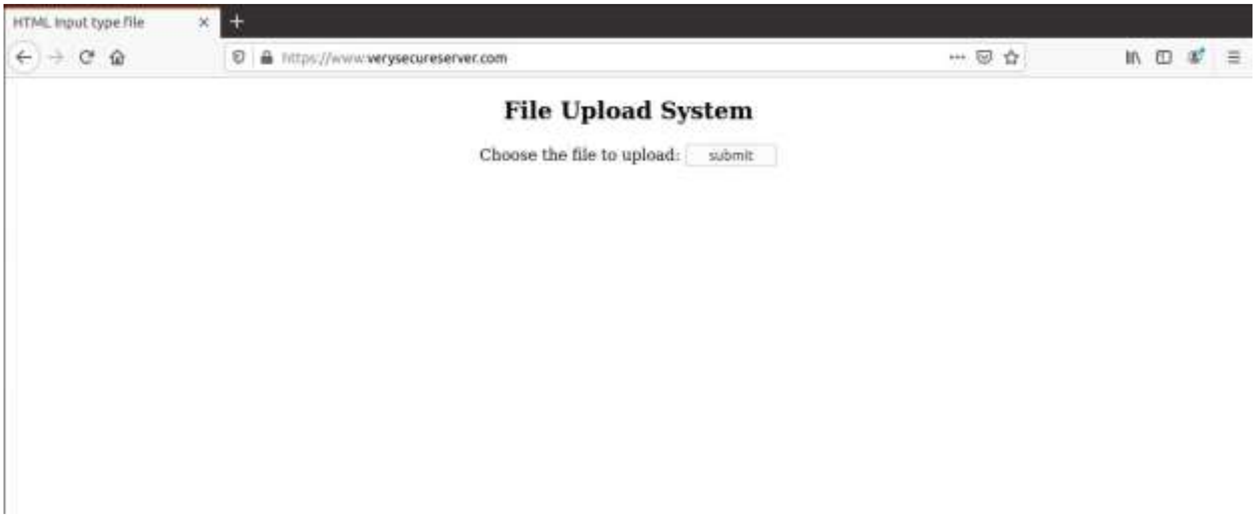
- ping www.verysecureserver.com
- ping ftp.verysecureserver.com
- ping mail.verysecureserver.com



```
root@adri-VirtualBox:/etc/bind# ping www.verysecureserver.com
PING www.verysecureserver.com (127.0.0.2) 56(84) bytes of data.
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=1 ttl=64 time=0.058 ms
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=2 ttl=64 time=0.096 ms
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=3 ttl=64 time=0.090 ms
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=4 ttl=64 time=0.050 ms
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=5 ttl=64 time=0.092 ms
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=6 ttl=64 time=0.113 ms
64 bytes from www.verysecureserver.com (127.0.0.2): icmp_seq=7 ttl=64 time=0.113 ms
^C
--- www.verysecureserver.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6160ms
rtt min/avg/max/mdev = 0.050/0.087/0.113/0.022 ms
root@adri-VirtualBox:/etc/bind#
```



```
root@adri-VirtualBox:/etc/bind# ping ftp.verysecureserver.com
PING ftp.verysecureserver.com (192.168.215.223) 56(84) bytes of data.
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=1 ttl=64 time=0.053 ms
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=2 ttl=64 time=0.055 ms
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=3 ttl=64 time=0.062 ms
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=4 ttl=64 time=0.100 ms
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=5 ttl=64 time=0.050 ms
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=6 ttl=64 time=0.160 ms
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=7 ttl=64 time=0.064 ms
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=8 ttl=64 time=0.086 ms
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=9 ttl=64 time=0.046 ms
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=10 ttl=64 time=0.074 ms
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=11 ttl=64 time=0.080 ms
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=12 ttl=64 time=0.207 ms
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=13 ttl=64 time=0.066 ms
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=14 ttl=64 time=0.058 ms
64 bytes from adri-VirtualBox.verysecureserver.com (192.168.215.223): icmp_seq=15 ttl=64 time=0.085 ms
^C
--- ftp.verysecureserver.com ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14372ms
rtt min/avg/max/mdev = 0.046/0.083/0.207/0.042 ms
root@adri-VirtualBox:/etc/bind# ping mail.verysecureserver.com
PING mail.verysecureserver.com (192.168.0.20) 56(84) bytes of data.
```

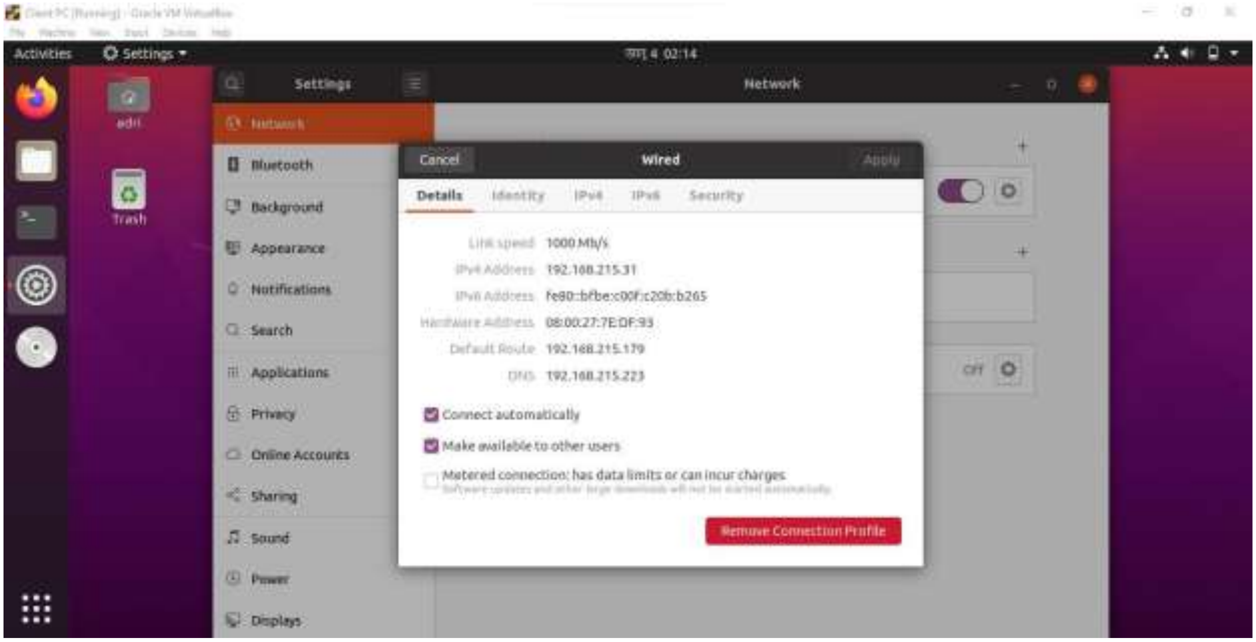


File Upload System

Choose the file to upload: submit

Step 9 Client PC:

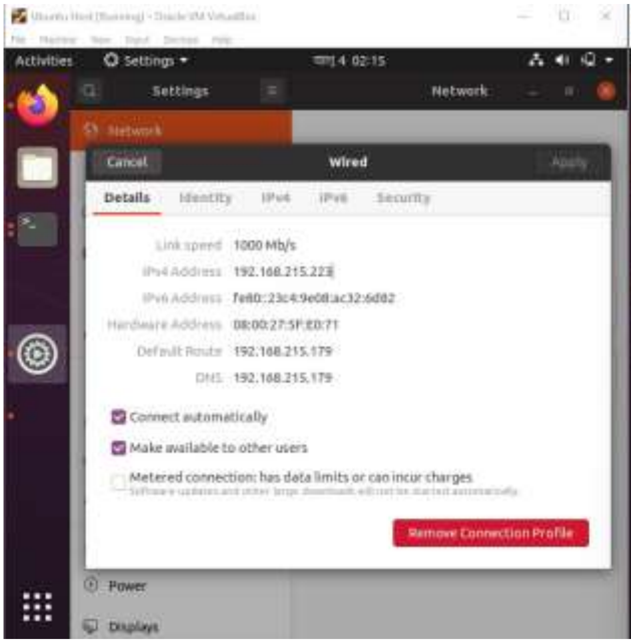
We already made a clone of ubuntu named ‘Client PC’. So now open the Client PC. Make network: Bridge Adapter.



Link speed 1000 Mb/s
IPv4 Address 192.168.215.31
IPv6 Address fe80::bfbe:c00f:c20b:b265
Hardware Address 08:00:27:7E:DF:93
Default Route 192.168.215.179
DNS 192.168.215.223

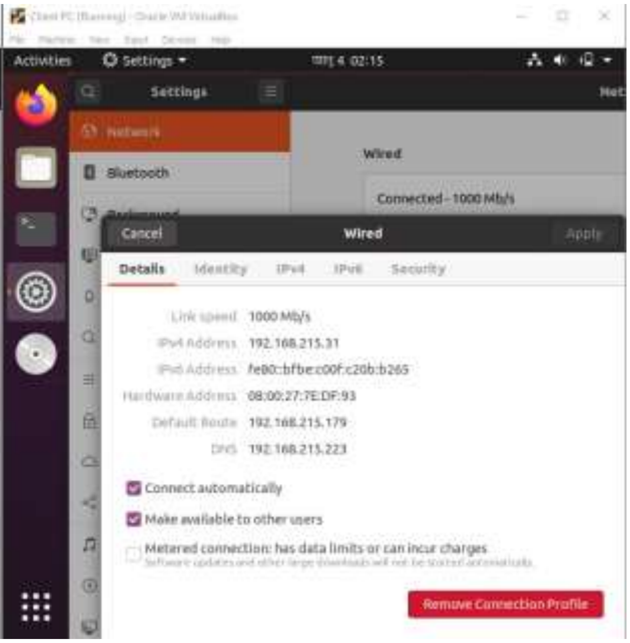
☑ Connect automatically
☑ Make available to other users
□ Metered connection: has data limits or can incur charges

Check host & ubuntu addresses:



Link speed 1000 Mb/s
IPv4 Address 192.168.215.223
IPv6 Address fe80::23c4:9e08:ac32:6d82
Hardware Address 08:00:27:5F:E0:71
Default Route 192.168.215.179
DNS 192.168.215.179

☑ Connect automatically
☑ Make available to other users
□ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically



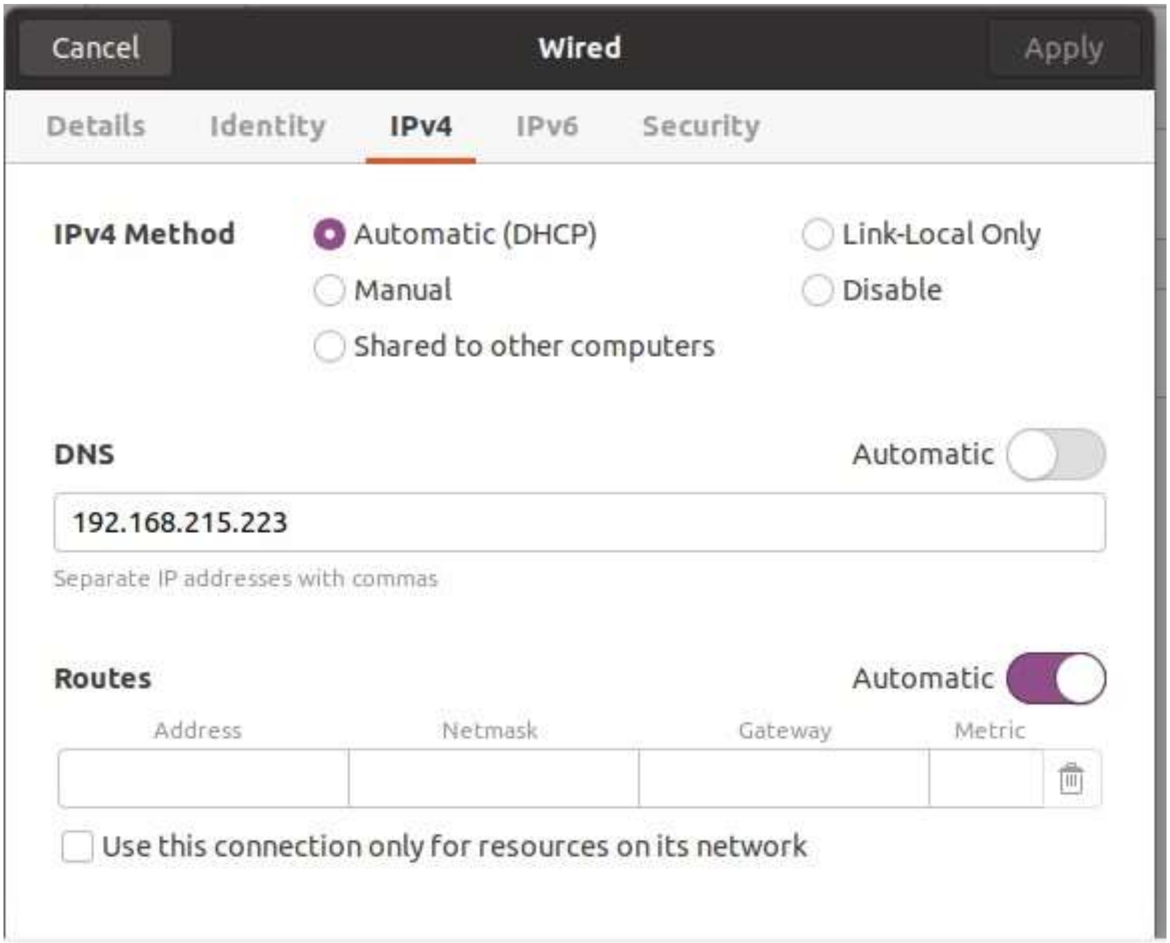
Link speed 1000 Mb/s
IPv4 Address 192.168.215.31
IPv6 Address fe80::bfbe:c00f:c20b:b265
Hardware Address 08:00:27:7E:DF:93
Default Route 192.168.215.179
DNS 192.168.215.223

☑ Connect automatically
☑ Make available to other users
□ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically

Both default route is same which is: 192.168.215.179

Set the Client’s DNS = Host PC’s IPv4 address
DNS: 192.168.215.223

Change client’s DNS with host’s IPv4 address:



IPv4 Method

● Automatic (DHCP) ○ Link-Local Only
○ Manual ○ Disable
○ Shared to other computers

DNS Automatic ○

192.168.215.223

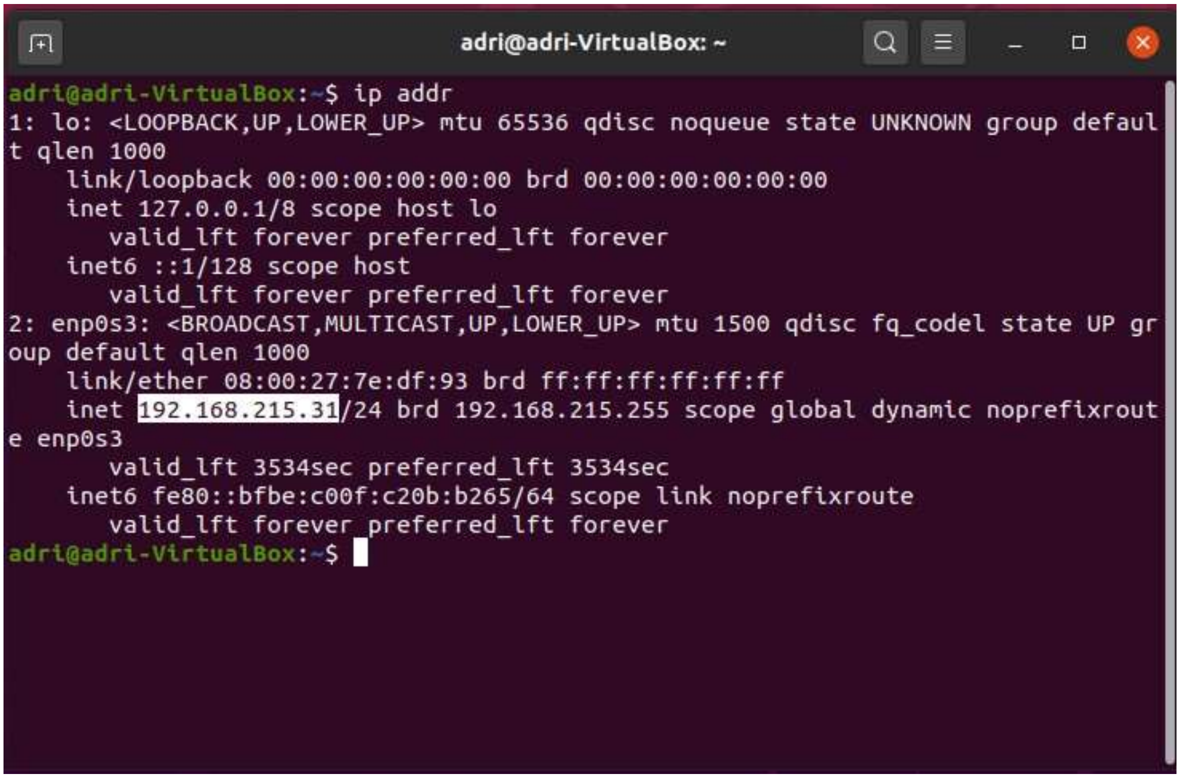
Separate IP addresses with commas

Routes Automatic ●

Address	Netmask	Gateway	Metric

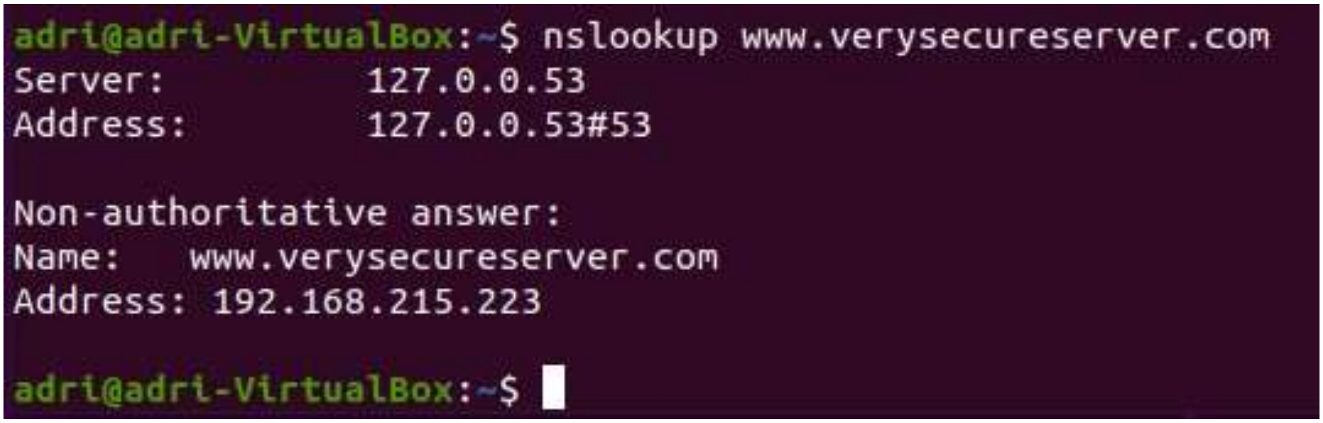
□ Use this connection only for resources on its network

Check client PC’s IP address:



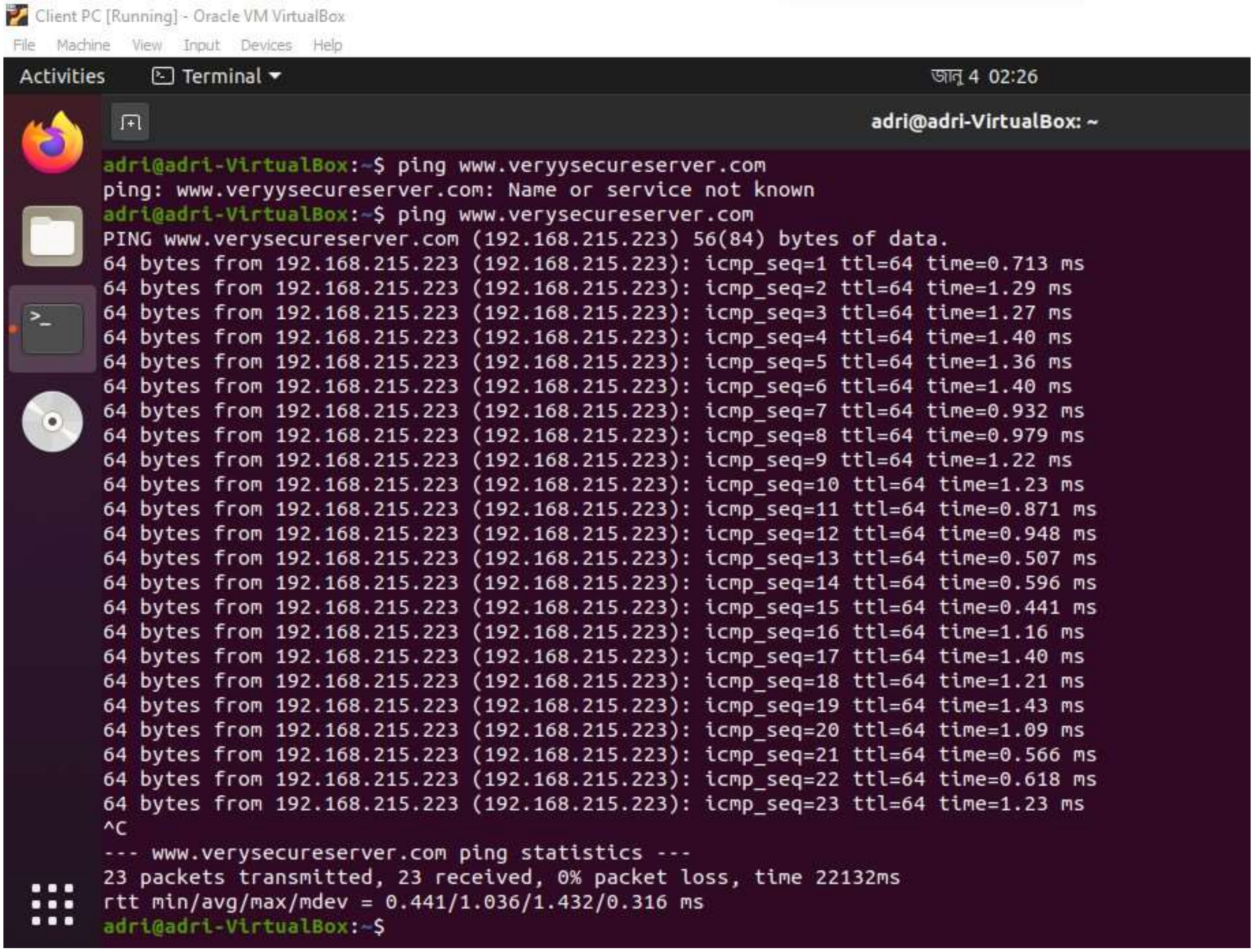
```
adri@adri-VirtualBox:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:7e:df:93 brd ff:ff:ff:ff:ff:ff
    inet 192.168.215.31/24 brd 192.168.215.255 scope global dynamic noprefixrout
e enp0s3
       valid_lft 3534sec preferred_lft 3534sec
    inet6 fe80::bfbe:c00f:c20b:b265/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
adri@adri-VirtualBox:~$ 
```

Check



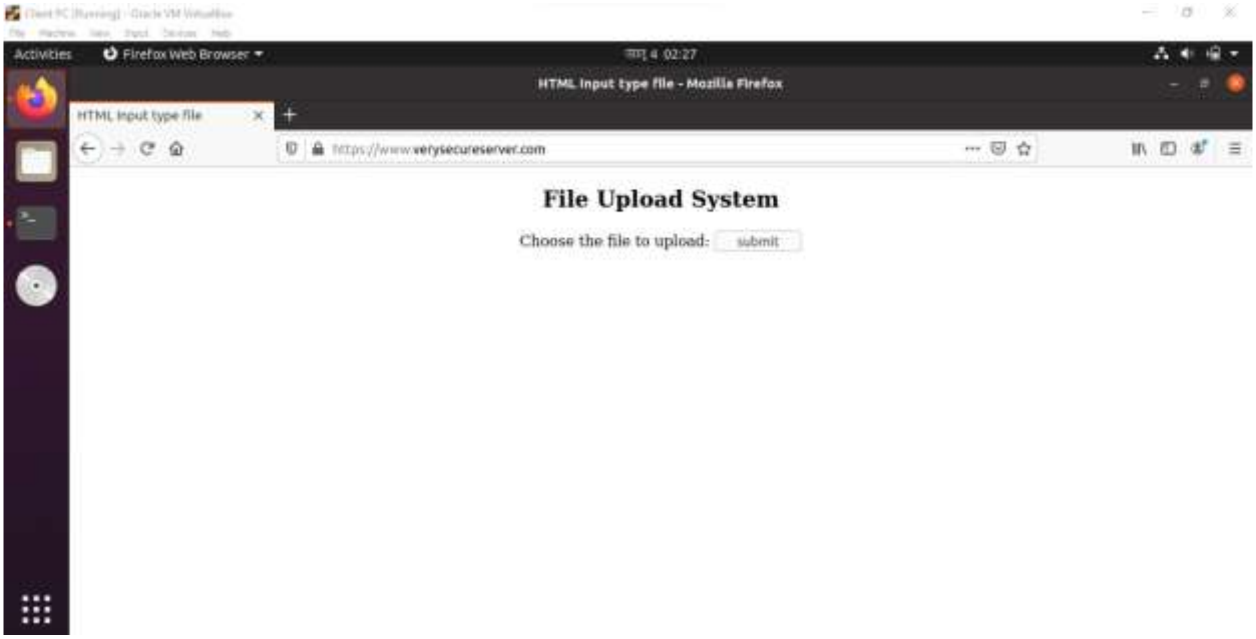
```
adri@adri-VirtualBox:~$ nslookup www.verysecureserver.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.verysecureserver.com
Address: 192.168.215.223

adri@adri-VirtualBox:~$ 
```

Step 10: Ping


Client PC [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
জানু 4 02:26
adri@adri-VirtualBox: ~

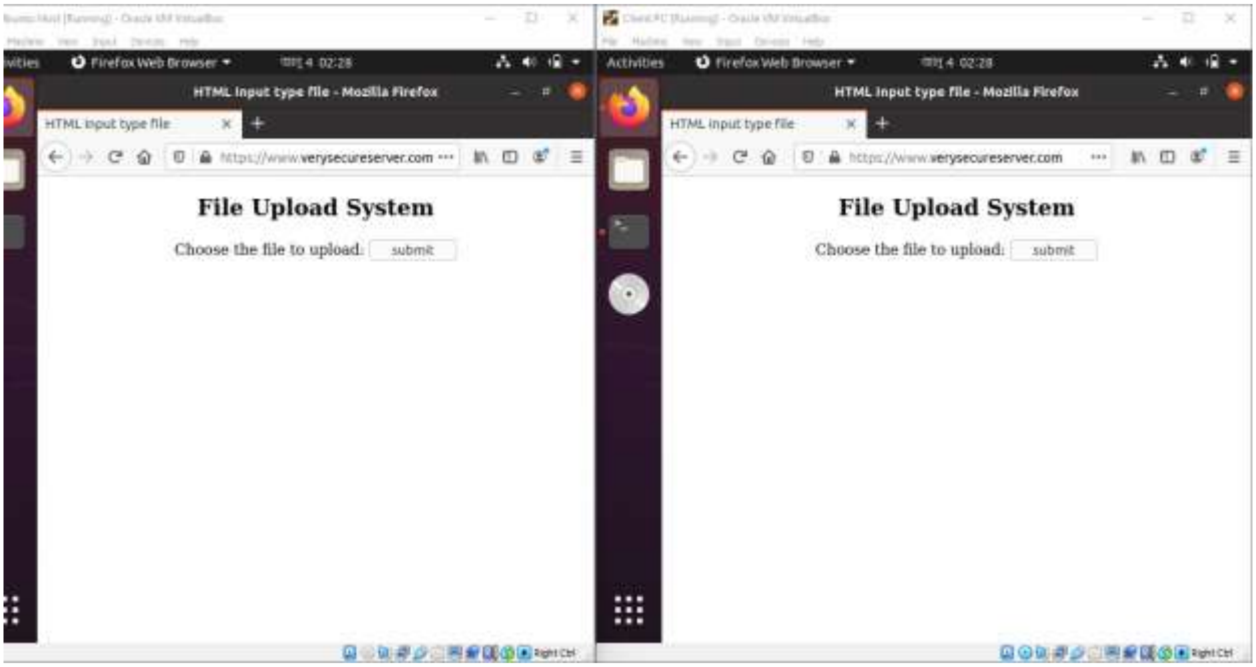
```
adri@adri-VirtualBox:~$ ping www.veryysecureserver.com
ping: www.veryysecureserver.com: Name or service not known
adri@adri-VirtualBox:~$ ping www.verysecureserver.com
PING www.verysecureserver.com (192.168.215.223) 56(84) bytes of data.
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=1 ttl=64 time=0.713 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=2 ttl=64 time=1.29 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=3 ttl=64 time=1.27 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=4 ttl=64 time=1.40 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=5 ttl=64 time=1.36 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=6 ttl=64 time=1.40 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=7 ttl=64 time=0.932 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=8 ttl=64 time=0.979 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=9 ttl=64 time=1.22 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=10 ttl=64 time=1.23 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=11 ttl=64 time=0.871 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=12 ttl=64 time=0.948 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=13 ttl=64 time=0.507 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=14 ttl=64 time=0.596 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=15 ttl=64 time=0.441 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=16 ttl=64 time=1.16 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=17 ttl=64 time=1.40 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=18 ttl=64 time=1.21 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=19 ttl=64 time=1.43 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=20 ttl=64 time=1.09 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=21 ttl=64 time=0.566 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=22 ttl=64 time=0.618 ms
64 bytes from 192.168.215.223 (192.168.215.223): icmp_seq=23 ttl=64 time=1.23 ms
^C
--- www.verysecureserver.com ping statistics ---
23 packets transmitted, 23 received, 0% packet loss, time 22132ms
rtt min/avg/max/mdev = 0.441/1.036/1.432/0.316 ms
adri@adri-VirtualBox:~$
```

Output Results


Activities
Firefox Web Browser
HTML Input type file - Mozilla Firefox
HTML Input type file
https://www.verysecureserver.com

File Upload System

Choose the file to upload: submit


Firefox Web Browser
HTML Input type file - Mozilla Firefox
HTML Input type file
https://www.verysecureserver.com
Activities
Firefox Web Browser
HTML Input type file - Mozilla Firefox
HTML Input type file
https://www.verysecureserver.com
Right Ctrl

File Upload System

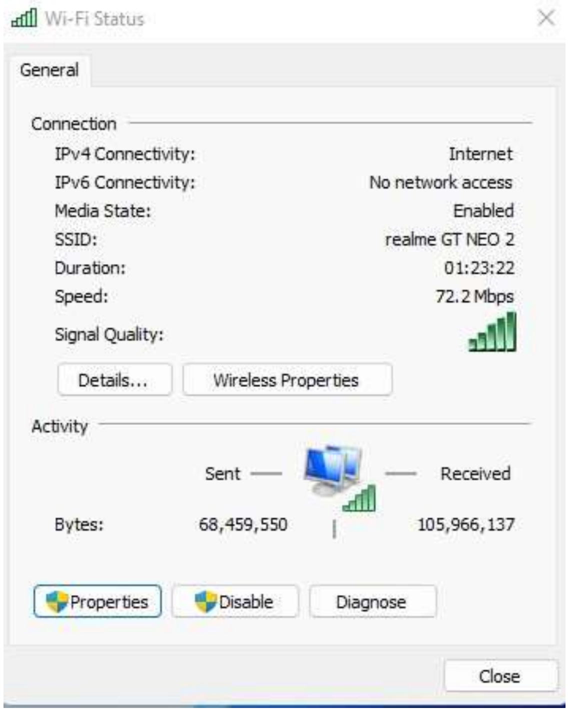
Choose the file to upload: submit

File Upload System

Choose the file to upload: submit

Here, we see by typing host's IP address or domain name on both server, file shows up with low and configured the certificate. So, DNS configuration for www.verysecureserver.com has been done.

Select your internet connection and right click and go to properties
->Double click TCP/IPv4



Wi-Fi Status

General

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No network access

Media State: Enabled

SSID: realme GT NEO 2

Duration: 01:23:22

Speed: 72.2 Mbps

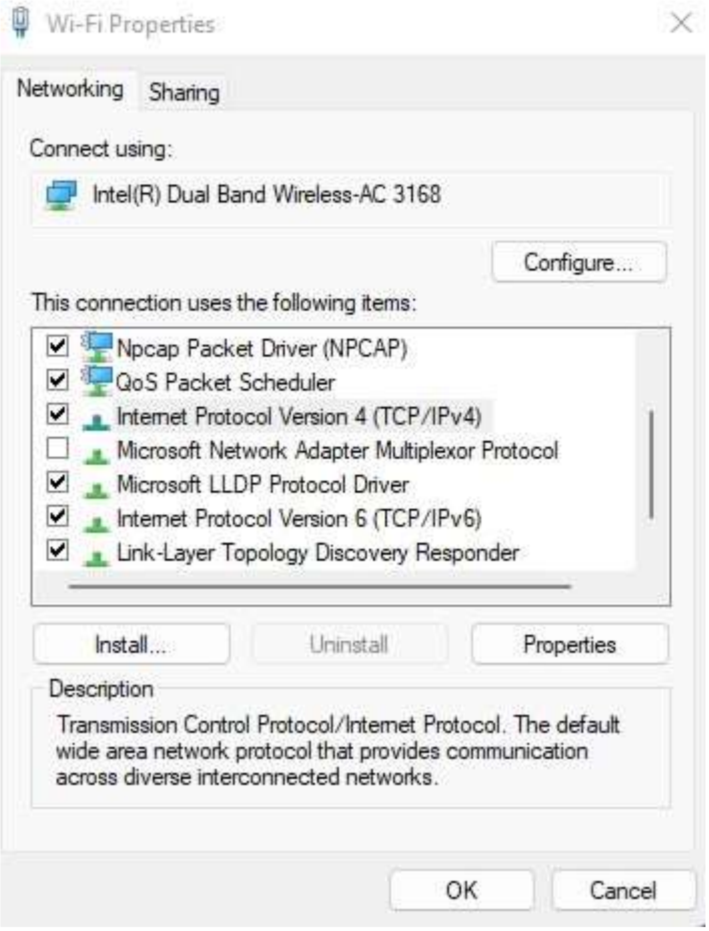
Signal Quality:

Activity

Sent — Received

Bytes: 68,459,550 | 105,966,137

>Change DNS with nameserver ip (192.168.31.44)



Connect using:

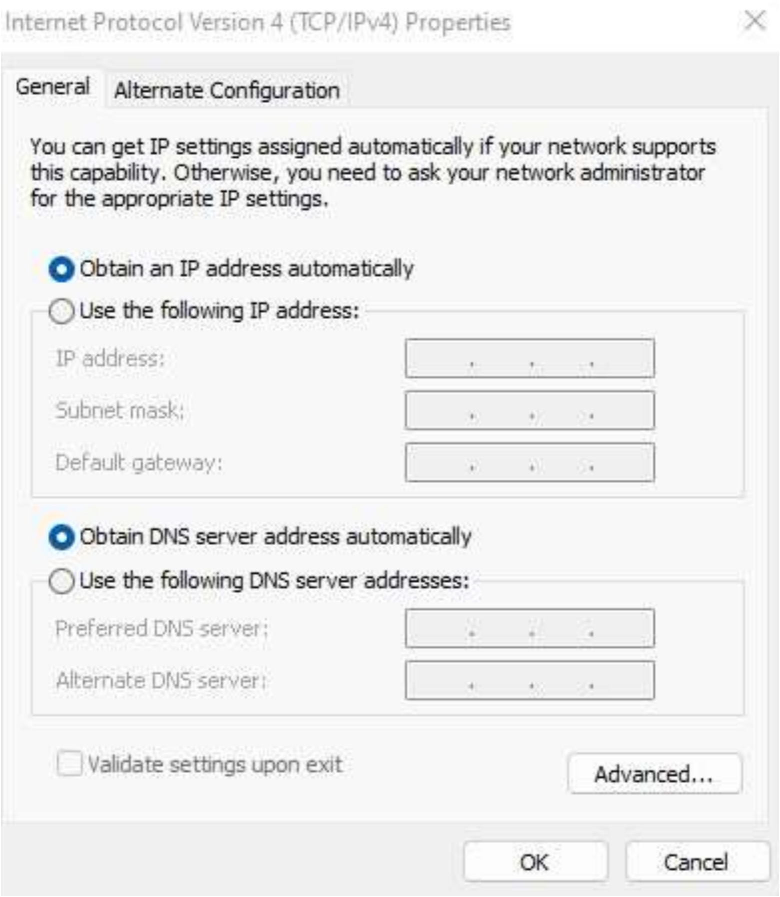
Intel(R) Dual Band Wireless-AC 3168

This connection uses the following items:

☑ Npcap Packet Driver (NPCAP)
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.



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: . . .

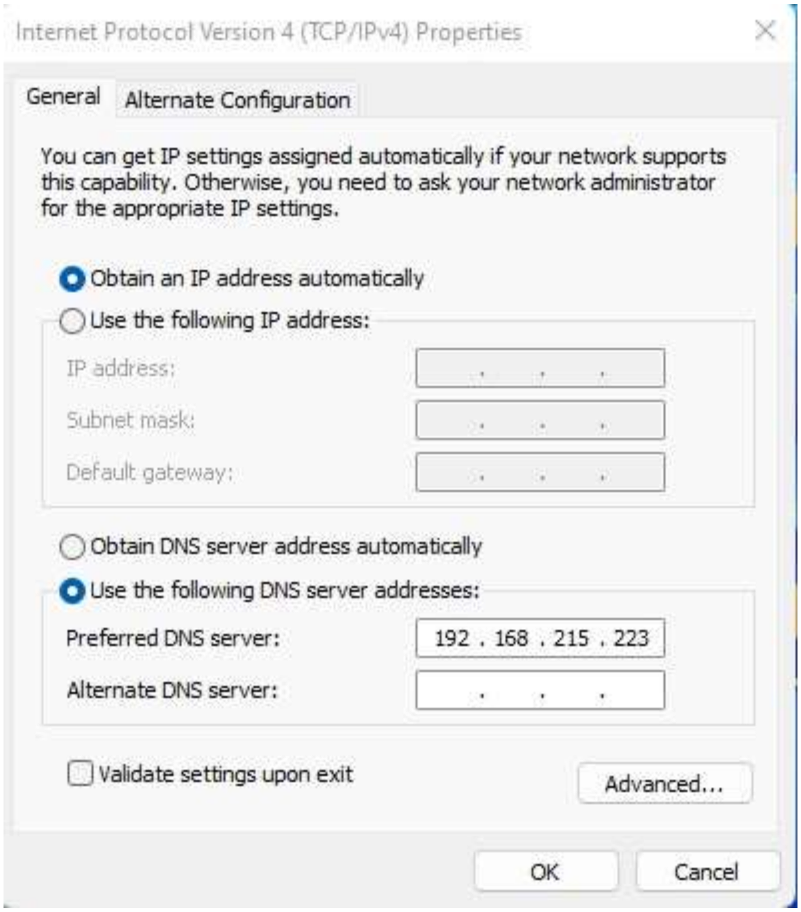
● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit



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: . . .

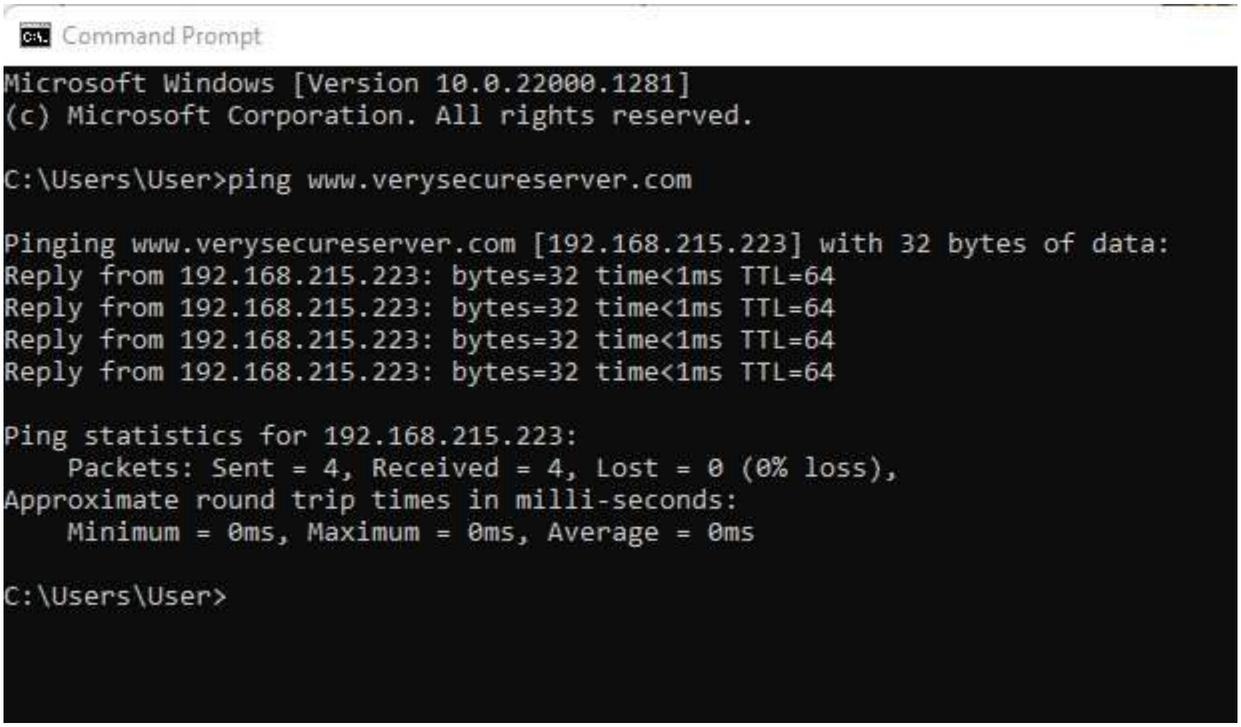
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

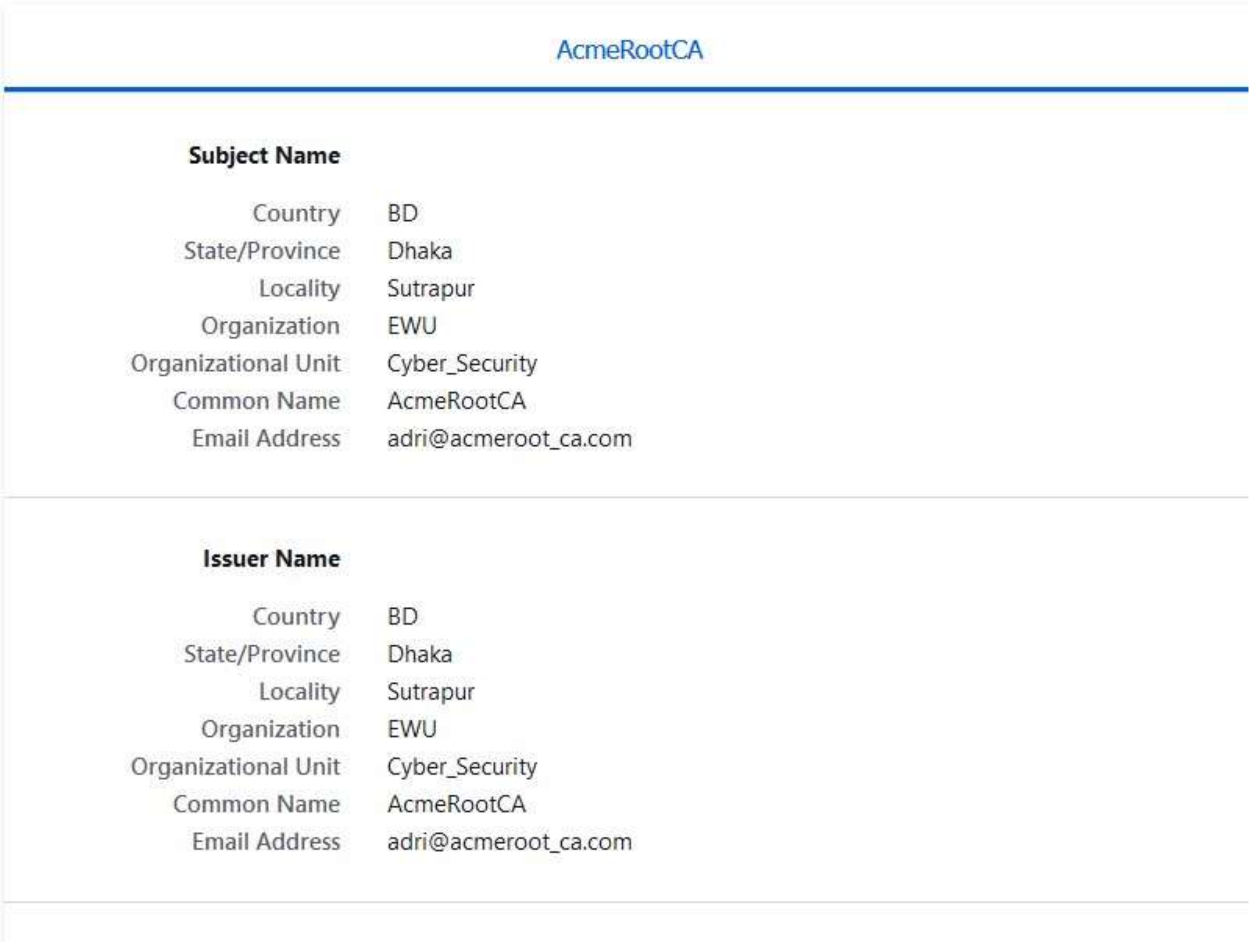
Preferred DNS server: 192 . 168 . 215 . 223

Alternate DNS server: . . .

□ Validate settings upon exit



```
Microsoft Windows [Version 10.0.22000.1281]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User>ping www.verysecureserver.com

Pinging www.verysecureserver.com [192.168.215.223] with 32 bytes of data:
Reply from 192.168.215.223: bytes=32 time<1ms TTL=64
Reply from 192.168.215.223: bytes=32 time<1ms TTL=64
Reply from 192.168.215.223: bytes=32 time<1ms TTL=64
Reply from 192.168.215.223: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.215.223:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\User>
```



AcmeRootCA

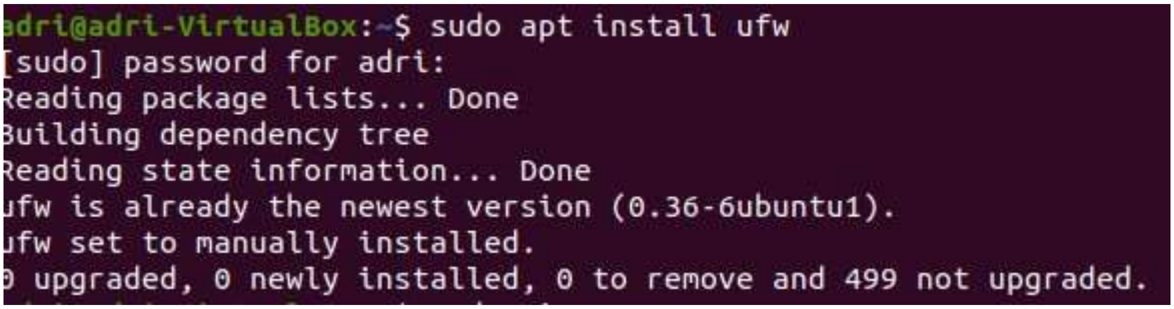
Subject Name	
Country	BD
State/Province	Dhaka
Locality	Sutrapur
Organization	EWU
Organizational Unit	Cyber_Security
Common Name	AcmeRootCA
Email Address	adri@acmeroot_ca.com

Issuer Name	
Country	BD
State/Province	Dhaka
Locality	Sutrapur
Organization	EWU
Organizational Unit	Cyber_Security
Common Name	AcmeRootCA
Email Address	adri@acmeroot_ca.com

Firewall Configuration

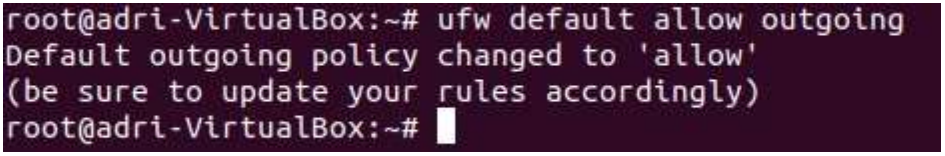
Firewalls defend any computer or network from outside cyberattacks by blocking malicious or unnecessary network traffic. Additionally, firewalls can prevent harmful software from connecting to a computer or network over the internet. By following below steps we can configure firewall.

1.**Install ufw package**
- sudo apt install ufw



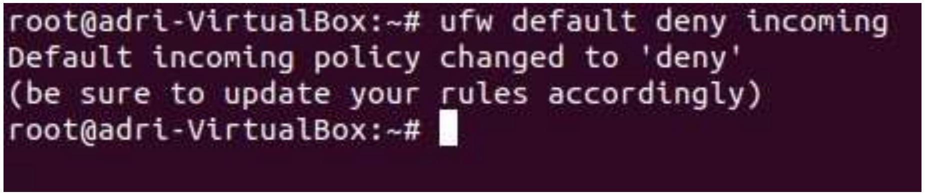
```
adri@adri-VirtualBox:~$ sudo apt install ufw
[sudo] password for adri:
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.36-6ubuntu1).
ufw set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 499 not upgraded.
```

2. **Set default rules for ufw firewall**
- ufw default allow outgoing



```
root@adri-VirtualBox:~# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
root@adri-VirtualBox:~# █
```

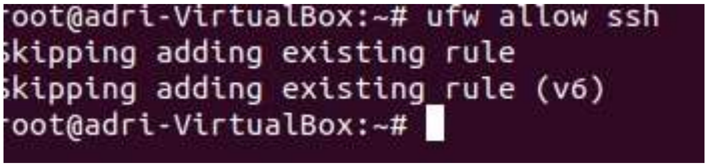
ufw default deny incoming



```
root@adri-VirtualBox:~# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@adri-VirtualBox:~# █
```

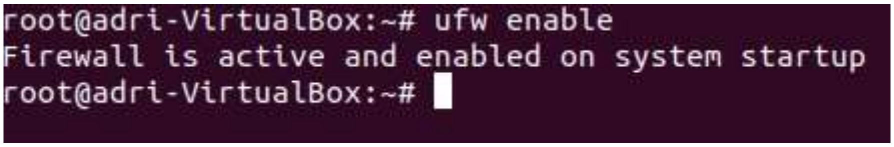
3. **Enable ssh**

- ufw allow ssh



```
oot@adri-VirtualBox:~# ufw allow ssh
kipping adding existing rule
kipping adding existing rule (v6)
oot@adri-VirtualBox:~# █
```

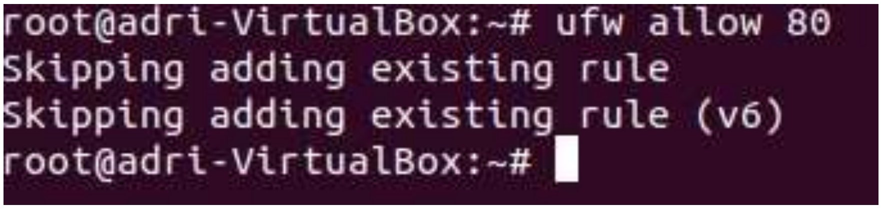
4. **Enable ufw** ufw
enable



```
root@adri-VirtualBox:~# ufw enable
Firewall is active and enabled on system startup
root@adri-VirtualBox:~# █
```

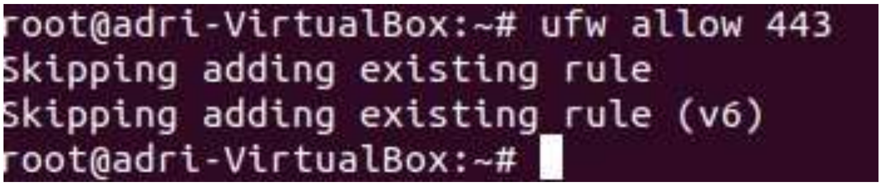
4. Allow port 80 (http), 443(https), and 53(DNS)

- ufw allow 80



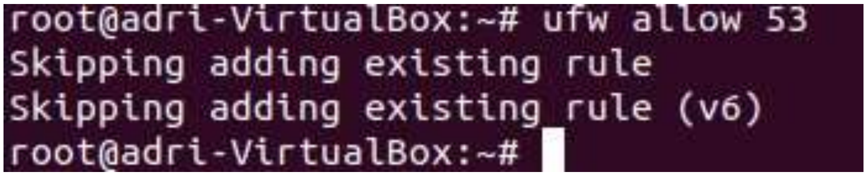
```
root@adri-VirtualBox:~# ufw allow 80
Skipping adding existing rule
Skipping adding existing rule (v6)
root@adri-VirtualBox:~# █
```

- ufw allow 443



```
root@adri-VirtualBox:~# ufw allow 443
Skipping adding existing rule
Skipping adding existing rule (v6)
root@adri-VirtualBox:~#
```

- ufw allow 53



```
root@adri-VirtualBox:~# ufw allow 53
Skipping adding existing rule
Skipping adding existing rule (v6)
root@adri-VirtualBox:~#
```

Certificate Revocation

To revoke certificates used following commands:

- openssl ca –keyfile ca.key –cert ca.crt –revoke server.crt
- openssl ocsp –Cafile ca.crt –issuer ca.crt –cert server.crt –url
- http://www.verysecureserver.com:8080 –resp_text –noverify