CSE487: Cybersecurity, Law and Ethics

[Summer 2022]

Section:03

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

Project Report

Submitted to:

Rashedul Amin Tuhin

Senior Lecturer,

Department of Computer Science & Engineering,

East West University

Submitted by:

Student ID	Student Name
2019-1-60-027	Md. Fayjul Islam Nahid
2019-1-60-179	Rifat Sultana Tithy
2018-2-60-127	A.K.M. Sadat
2019-1-60-204	Noshin Faria

Step1: primary DNS Configuration:

Go to - C:\Windows\System32\drivers\etc\hosts:

Paste –

127.0.0.1 localhost

127.0.0.1 acmesecureserver

127.0.0.1 www.acmesecureserver.com

And save it.

Step1.1 : save the file location:

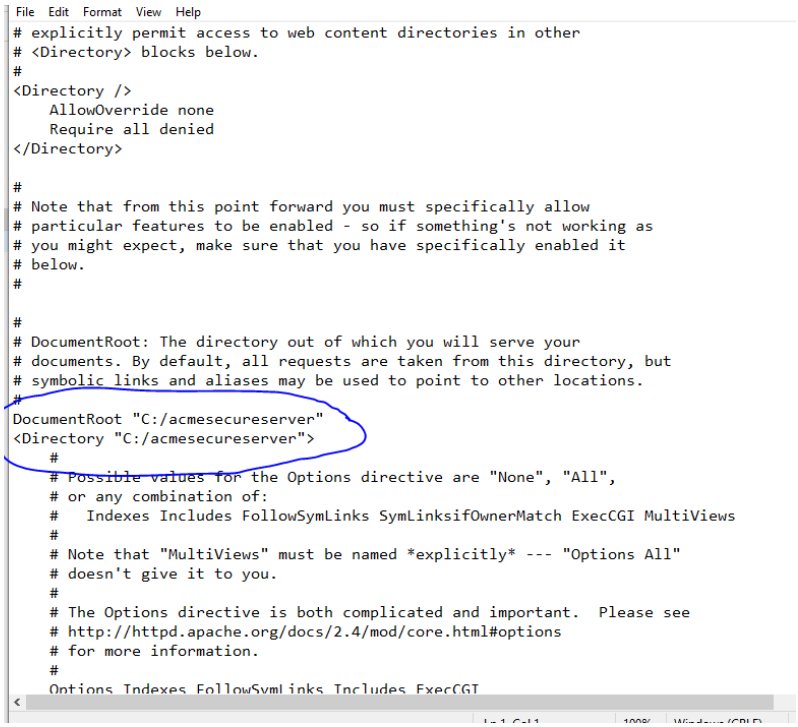
Go to:

Xampp→apache→conf→httpd.conf:

Paste the below part there and save it.

DocumentRoot "C:/acmesecureserver"

<Directory "C:/acmesecureserver">



```
File  Edit  Format  View  Help
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all denied
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "C:/acmesecureserver"
<Directory "C:/acmesecureserver">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important.  Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    Options Indexes FollowSymLinks Includes ExecCGI
```

Step2: Creating certificate

Open cmd and paste the below command.

set OPENSSL_CONF=C:\xampp\apache\conf\openssl.cnf

Step2.1:
go to C:\xampp\apache\bin by the command below.

~ cd..
~ cd..
~ cd xampp
~ cd apache
~ cd bin
~ openssl.exe

Step2.2:
For creating a server certificate –
~ **req -newkey rsa:2048 -nodes -keyout server.key -out server.csr**
then provide all the info. Paste the below part in the common name section.
Common name: www.acmesecureserver.com

~ **x509 -signkey server.key -in server.csr -req -days 365 -out server.crt**
Ctrl c - to close openssl

we can get an error if we don't close it. so it's save to close openssl and open it again
~ openssl.exe

Step2.3:
For creating a sub root CA certificate –
~ **req -newkey rsa:2048 -keyout subrootCA.key -out subrootCA.csr**
then provide all the info. Paste the below part in the common name section.
Common Name(can use any other name): AcmeCA
An optional company name : doesn't need to provide

~ **x509 -signkey subrootCA.key -in subrootCA.csr -req -days 365 -out subrootCA.crt**
Ctrl c - to close openssl

we can get an error if we don't close it. so it's save to close openssl and open it again
~ openssl.exe

Step2.4:

For creating a root CA certificate –
~ **req -x509 -sha256 -days 1825 -newkey rsa:2048 -keyout rootCA.key -out rootCA.crt**
then provide all info
Common Name(can use any other name): Acme-RootCA

Step2.5:
create two ext files-
go to C:\xampp\apache\bin
create - **domain.ext**, **root.ext**

Paste below part in **domain.ext** –
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
subjectAltName = @alt_names
[alt_names]
DNS.1 =www.acmesecureserver.com
DNS.2 =127.0.0.1

Paste below part in **root.ext**–
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:TRUE
subjectAltName = @alt_names
[alt_names]
DNS.1 =www.acmesecureserver.com
DNS.2 =127.0.0.1

Step2.6:
Signing subrootCA certificate with rootCA certificate –
~ **x509 -req -CA rootCA.crt -CAkey rootCA.key -in subrootCA.csr -out subrootCA.crt -days 365 -CAcreateserial -extfile root.ext**

For checking the subrootCa certificate –
~ **x509 -text -noout -in subrootCA.crt**

~ **x509 -in subrootCA.crt -outform der -out subrootCA.der**

Exporting the subrootCA key file in subrootCA pfx file –
~ **pkcs12 -inkey subrootCA.key -in subrootCA.crt -export -out subrootCA.pfx**

Signing server certificate with subrootCA certificate –

~ **x509 -req -CA subrootCA.crt -CAkey subrootCA.key -in server.csr -out server.crt -days 365 -CAcreateserial -extfile domain.ext**

~ **x509 -in server.crt -outform der -out server.der**

Exporting the server key file in the server .pfx file –

~ **pkcs12 -inkey server.key -in server.crt -export -out server.pfx**

Replacing the RSA encryption from the server and subrootCA key for setting the validity –

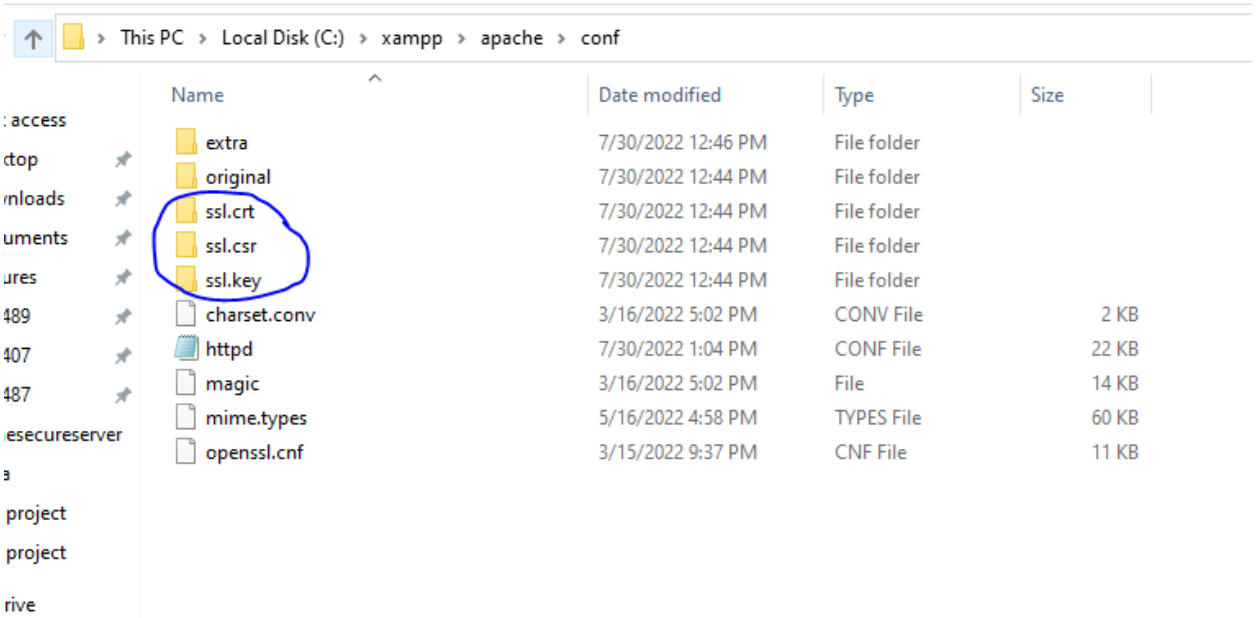
~ **rsa -in server.key -out server.key**

~ **rsa -in subrootCA.key -out subrootCA.key**

then install rootCA.crt and server.pfx from C:\xampp\apache\bin
then copy server.crt, server.csr, server.key to C:\xampp\apache\conf\server.crt, C:\xampp\apache\conf\server.csr and C:\xampp\apache\conf\server.key and replace the existing files.

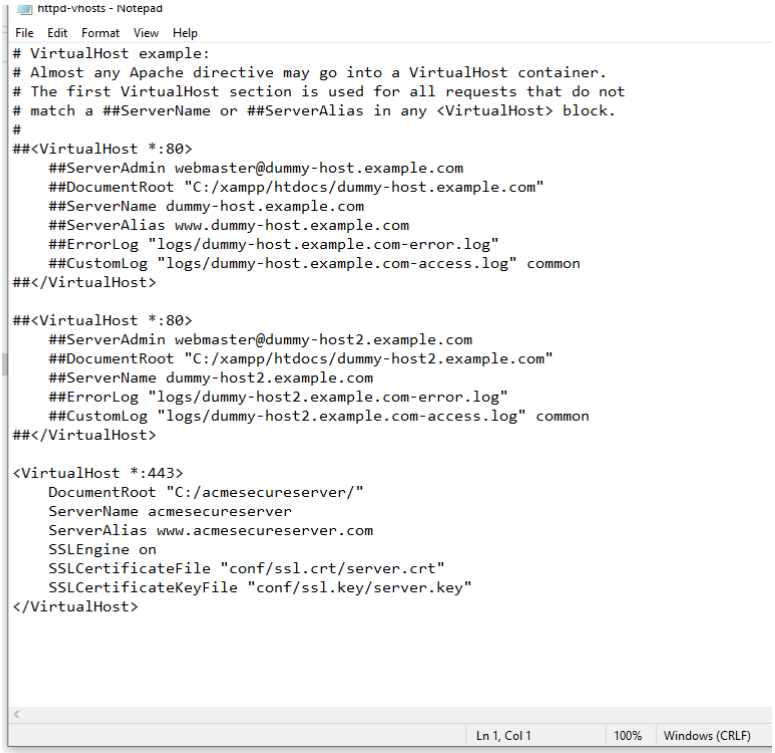
This PC › Local Disk (C:) › xampp › apache › bin

Name	Date modified	Type	Size
icudt70.dll	5/11/2022 3:29 PM	Application exten...	28,779 KB
icuin70.dll	5/11/2022 3:29 PM	Application exten...	2,944 KB
icuio70.dll	5/11/2022 3:29 PM	Application exten...	60 KB
icuuc70.dll	5/11/2022 3:29 PM	Application exten...	2,191 KB
index.txt	7/30/2022 9:32 PM	Text Document	0 KB
jansson.dll	9/12/2021 3:59 PM	Application exten...	55 KB
libapr-1.dll	3/16/2022 5:25 PM	Application exten...	209 KB
libapriconv-1.dll	3/16/2022 5:25 PM	Application exten...	36 KB
libaprutil-1.dll	3/16/2022 5:25 PM	Application exten...	287 KB
libcrypto-1_1-x64.dll	3/16/2022 5:15 PM	Application exten...	3,361 KB
libcurl.dll	2/6/2019 12:58 PM	Application exten...	997 KB
libhttpd.dll	3/16/2022 5:26 PM	Application exten...	449 KB
libsasl.dll	5/11/2022 3:29 PM	Application exten...	190 KB
libssh2.dll	5/11/2022 3:29 PM	Application exten...	372 KB
libssl-1_1-x64.dll	3/16/2022 5:16 PM	Application exten...	672 KB
libxml2.dll	8/23/2021 8:42 PM	Application exten...	1,363 KB
logresolve	3/16/2022 5:27 PM	Application	57 KB
lua52.dll	4/5/2019 8:28 PM	Application exten...	180 KB
nghttp2.dll	3/8/2022 4:35 PM	Application exten...	139 KB
openssl	3/16/2022 5:17 PM	Application	538 KB
pcre.dll	8/23/2021 8:32 PM	Application exten...	392 KB
pcre2-8.dll	2/20/2022 6:45 PM	Application exten...	316 KB
pv	4/16/2012 11:30 PM	Application	60 KB
root.ext	7/30/2022 1:30 PM	EXT File	1 KB
rootCA	7/30/2022 1:27 PM	Security Certificate	2 KB
rootCA.key	7/30/2022 1:26 PM	KEY File	2 KB
rootCA.srl	7/30/2022 1:32 PM	SRL File	1 KB
rotatelogs	3/16/2022 5:27 PM	Application	77 KB
serial.txt	7/30/2022 9:33 PM	Text Document	0 KB
server	7/30/2022 1:34 PM	Security Certificate	2 KB
server.csr	7/30/2022 1:18 PM	CSR File	2 KB
server	7/30/2022 1:35 PM	Security Certificate	2 KB
server.key	7/30/2022 1:36 PM	KEY File	2 KB
server	7/30/2022 1:35 PM	Personal Informati...	3 KB
subrootCA	7/30/2022 9:30 PM	CONF File	3 KB
subrootCA	7/30/2022 1:32 PM	Security Certificate	2 KB
subrootCA.csr	7/30/2022 1:24 PM	CSR File	2 KB
subrootCA	7/30/2022 1:33 PM	Security Certificate	1 KB
subrootCA.key	7/30/2022 1:36 PM	KEY File	2 KB
subrootCA	7/30/2022 1:34 PM	Personal Informati...	3 KB
subrootCA.srl	7/30/2022 1:34 PM	SRL File	1 KB
wintty	3/16/2022 5:27 PM	Application	18 KB



Configuring httpd-vhosts:
go to C:\xampp\apache\conf\extra\httpd-vhosts.conf –
paste below information.

```
<VirtualHost *:443>
    DocumentRoot "C:/acmesecureserver/"
    ServerName acmesecureserver
    ServerAlias www.acmesecureserver.com
    SSLEngine on
    SSLCertificateFile "conf/ssl.crt/server.crt"
    SSLCertificateKeyFile "conf/ssl.key/server.key"
</VirtualHost>
```

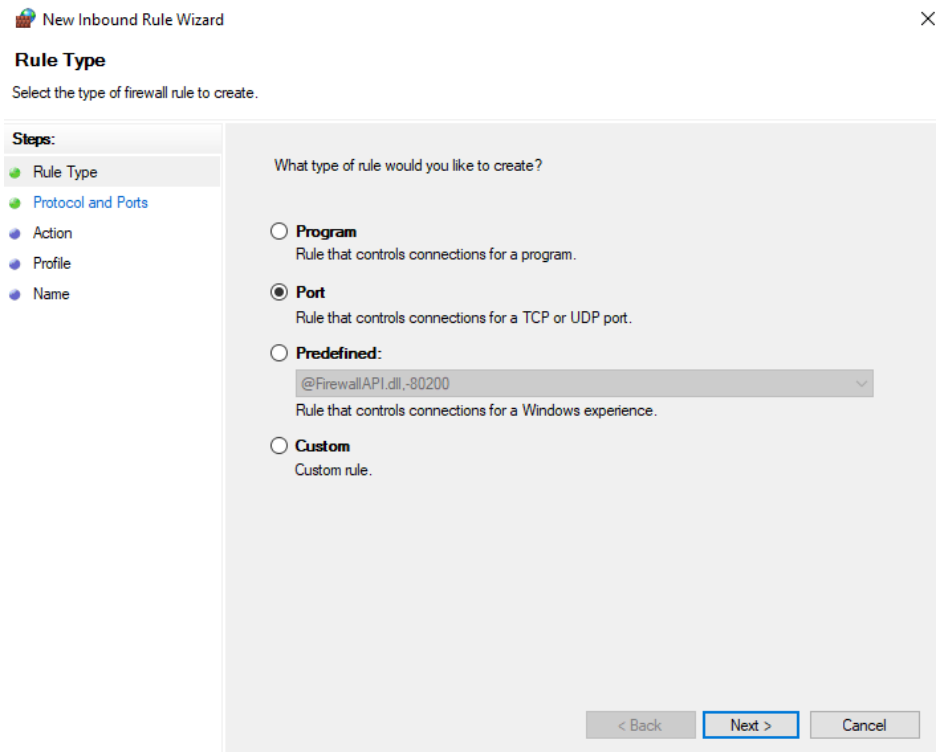


```
# VirtualHost example:
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for all requests that do not
# match a ##ServerName or ##ServerAlias in any <VirtualHost> block.
#
##<VirtualHost *:80>
    ##ServerAdmin webmaster@dummy-host.example.com
    ##DocumentRoot "C:/xampp/htdocs/dummy-host.example.com"
    ##ServerName dummy-host.example.com
    ##ServerAlias www.dummy-host.example.com
    ##ErrorLog "logs/dummy-host.example.com-error.log"
    ##CustomLog "logs/dummy-host.example.com-access.log" common
##</VirtualHost>

##<VirtualHost *:80>
    ##ServerAdmin webmaster@dummy-host2.example.com
    ##DocumentRoot "C:/xampp/htdocs/dummy-host2.example.com"
    ##ServerName dummy-host2.example.com
    ##ErrorLog "logs/dummy-host2.example.com-error.log"
    ##CustomLog "logs/dummy-host2.example.com-access.log" common
##</VirtualHost>

<VirtualHost *:443>
    DocumentRoot "C:/acmesecureserver/"
    ServerName acmesecureserver
    ServerAlias www.acmesecureserver.com
    SSLEngine on
    SSLCertificateFile "conf/ssl.crt/server.crt"
    SSLCertificateKeyFile "conf/ssl.key/server.key"
</VirtualHost>
```

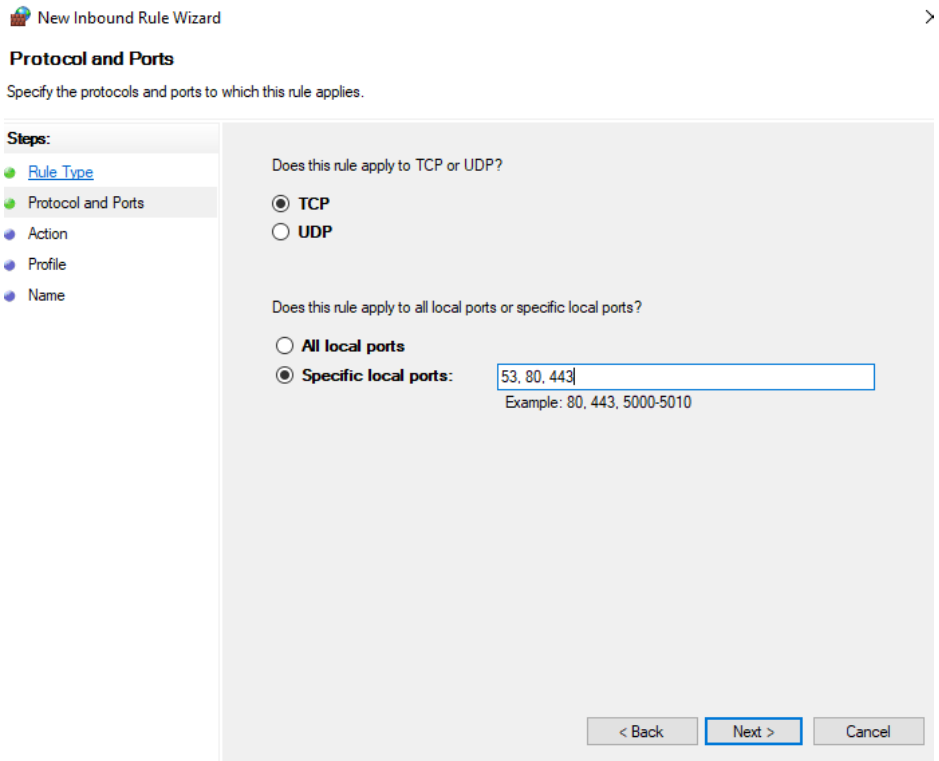
Step2.7: Firewall configuration to allow necessary ports (53, 80, 443) :

Got to control panel > system and security > windows defender firewall > advanced setting > Inbound rules > new rules

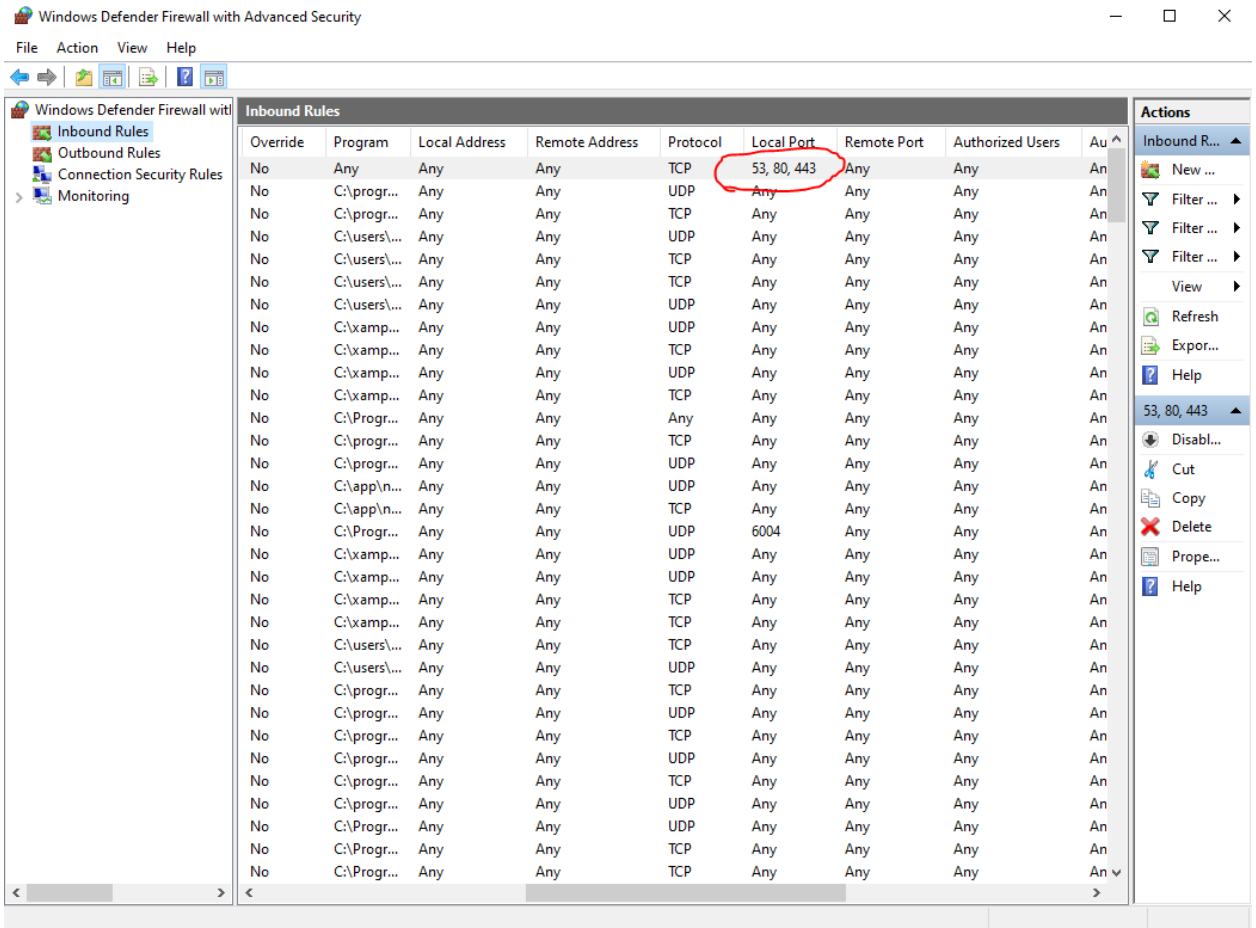
Then choose the port option like below



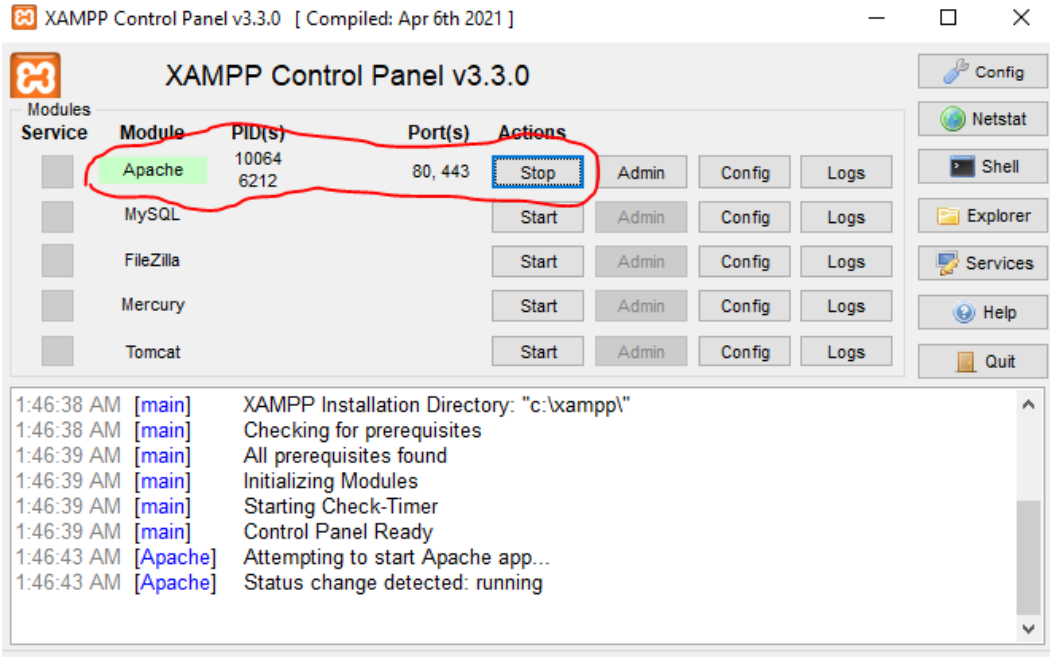
Click on next. Then give the necessary port number. In our case, it's 53, 80, 443. And click on next > next.



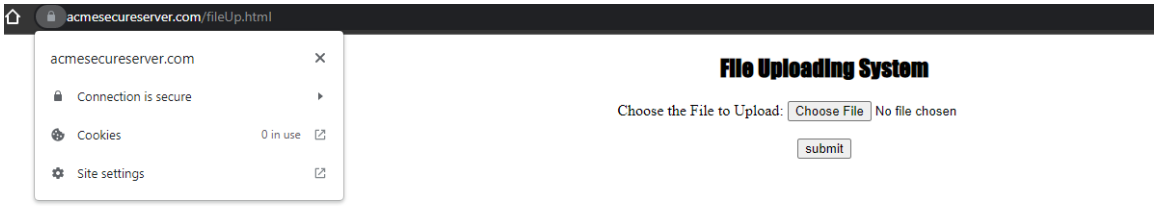
We will able to see our port numbers in the inbound list like below.

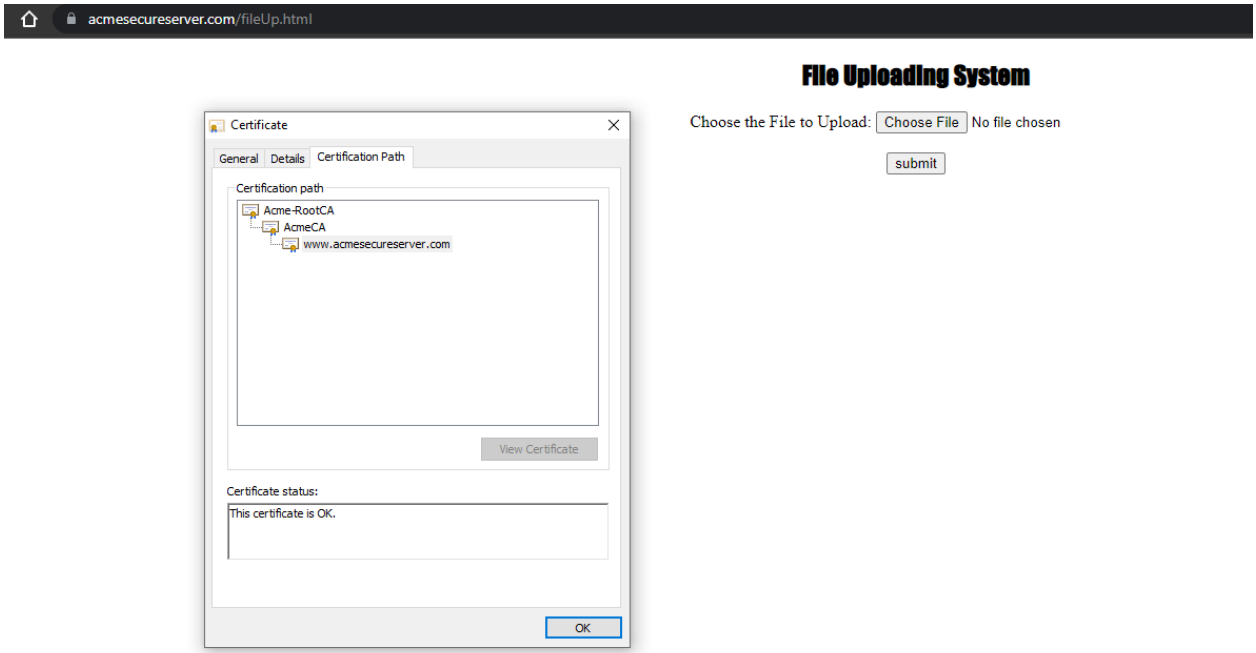


Finally, we will open our xampp and turn on Apache



Open any browser and type " https:\www.acmesecureserver.com" and click on ok. We will see our file is running with SSL Certificate.





Step 3: Revocation of certificate:

go to C:\xampp\apache\bin
create a file **subrootCA.conf**
paste the below code -

```
[ca]
default_ca = CA_default
[CA_default]
dir =C:/xampp/apache/bin
certs = $dir
crl_dir = $dir
new_certs_dir = $dir
database = $dir/index.txt
serial = $dir/serial.txt
RANDFILE = $dir/private/.rand
private_key = $dir/subrootCA.key
certificate = $dir/subrootCA.crt
crlnumber = $dir/crlnumber.txt
crl = $dir/crl/ca.crl
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 = supplied
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
0.organizationName_default = Acme
[ 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
crlDistributionPoints = @crl_dist_points
[ server_cert ]
# Extensions for server certificates
basicConstraints = CA:FALSE
```

nsComment = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = www.acmesecureserver.com
DNS.2 = 127.0.0.1

libcrypto-1_1-x64.dll	3/27/2021 5:13 PM	Application exten...	3,357 KB
libcurl.dll	2/6/2019 12:58 PM	Application exten...	997 KB
libhttpd.dll	5/18/2021 4:45 PM	Application exten...	438 KB
libsasl.dll	6/2/2021 7:20 AM	Application exten...	190 KB
libssh2.dll	6/2/2021 7:20 AM	Application exten...	275 KB
libssl-1_1-x64.dll	3/27/2021 5:14 PM	Application exten...	671 KB
libxml2.dll	2/17/2020 6:25 PM	Application exten...	1,359 KB
logresolve	5/18/2021 4:47 PM	Application	57 KB
lua52.dll	4/5/2019 8:28 PM	Application exten...	180 KB
nghttp2.dll	4/24/2021 4:17 PM	Application exten...	145 KB
openssl	3/27/2021 5:15 PM	Application	537 KB
pcre.dll	2/17/2020 6:44 PM	Application exten...	386 KB
pv	4/16/2012 11:30 PM	Application	60 KB
rev	8/21/2022 10:46 AM	Certificate Revoca...	1 KB
root.ext	8/6/2022 6:08 PM	EXT File	1 KB
rootCA	8/20/2022 10:12 PM	Security Certificate	2 KB
rootCA.key	8/20/2022 10:11 PM	KEY File	2 KB
rootCA.srl	8/20/2022 10:13 PM	SRL File	1 KB
rotatelogs	5/18/2021 4:47 PM	Application	77 KB
serial	8/21/2022 10:23 AM	Text Document	0 KB
server	8/20/2022 10:15 PM	Security Certificate	2 KB
server.csr	8/20/2022 9:56 PM	CSR File	2 KB
server	8/20/2022 10:16 PM	Security Certificate	2 KB
server.key	8/20/2022 10:16 PM	KEY File	2 KB
server	8/20/2022 10:16 PM	Personal Informati...	3 KB
subrootCA.conf	8/21/2022 10:47 AM	CONF File	3 KB
subrootCA	8/20/2022 10:13 PM	Security Certificate	2 KB
subrootCA.csr	8/20/2022 9:58 PM	CSR File	2 KB
subrootCA	8/20/2022 10:14 PM	Security Certificate	1 KB
subrootCA.key	8/20/2022 10:16 PM	KEY File	2 KB
subrootCA	8/20/2022 10:14 PM	Personal Informati...	3 KB
subrootCA.srl	8/20/2022 10:15 PM	SRL File	1 KB
wintty	5/18/2021 4:47 PM	Application	18 KB

hosts | project1.txt | httpd-vhosts.conf | subrootCA.conf | root.ext | domain.ext | index.txt | serial.txt | crlnumber.txt

```
[ca]
default_ca = CA_default
[CA_default]
dir =C:/xampp/apache/bin
certs = $dir
crl_dir = $dir
new_certs_dir = $dir
database = $dir/index.txt
serial = $dir/serial.txt
RANDFILE = $dir/private/.rand
private_key = $dir/subrootCA.key
certificate = $dir/subrootCA.crt
crlnumber = $dir/crlnumber.txt
crl = $dir/crl/ca.crl
default_crl_days = 0
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 = supplied
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
```

Open openssl.exe to revoke the certificate issued to acmesecureserver.com from the AcmeCA–

~ **ca -config subrootCA.conf -revoke server.crt**

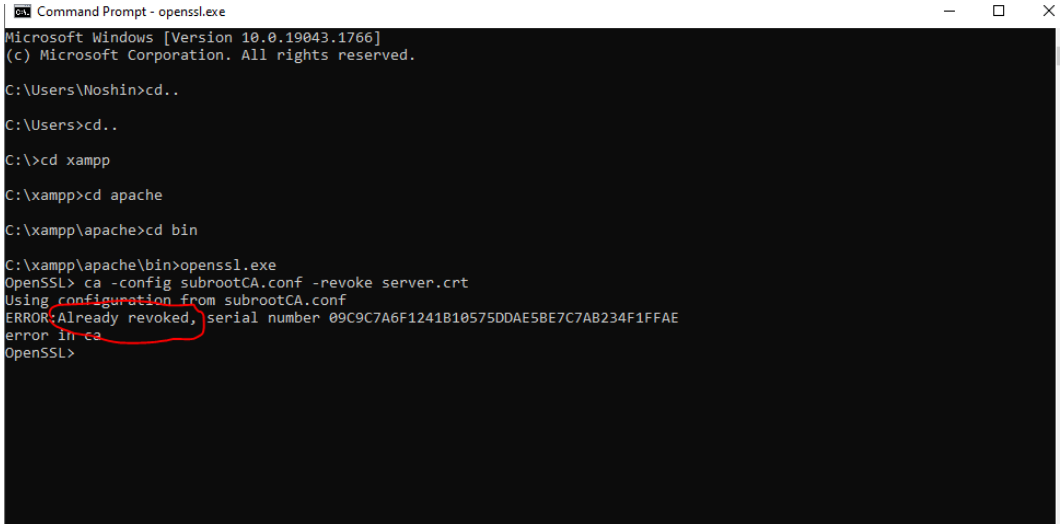
To generate revocation crl file –

~ **ca -config subrootCA.conf -gencrl -out rev.crl**

To see the revocation file in the form of text –

~ **crl -in rev.crl -noout -text**

The certificate is revoked successfully. Then again give the first command of revocation. You will see the status “already revoked”.

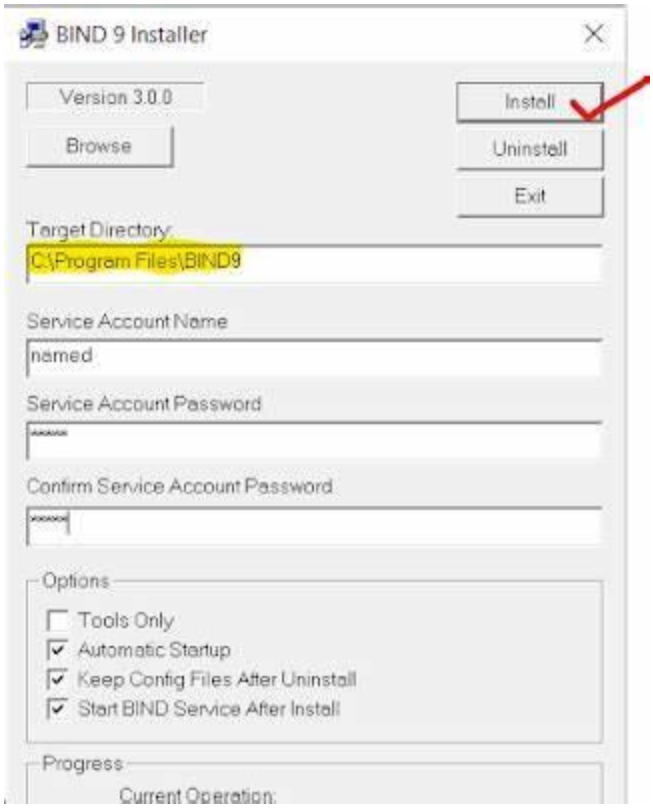


Step 4: DNS Configuration

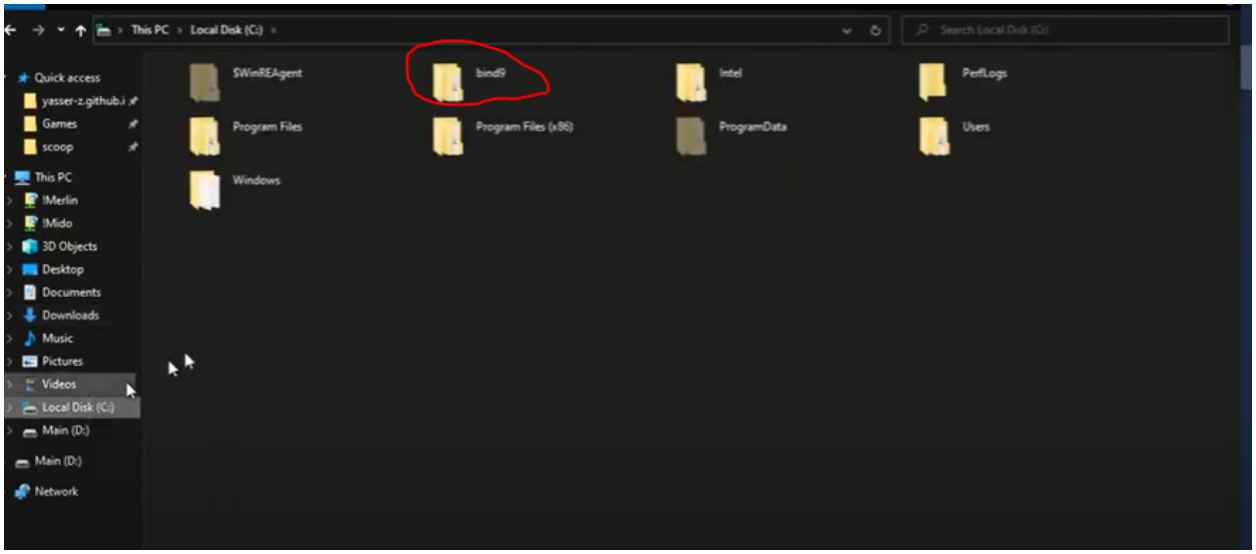
Install bind9 on the PC with necessary information.

Here , Target Directory - C:\bind9

Give a password and click on “Install” to install it.



After installation, we get a file in C drive named “bind9”.



Go to bind9\etc and create files named "**named.conf**" and "**rndc.key**".
Open the cmd and go to C:\bind9\bin. Then give this command -
~ **rndc-confgen**
You will get a part of the code called "rndc-key". Paste that part inside the "rndc.key" file.

Write the below code in the "named.conf" file where inside "listen-on{}" put your IP address. Here, ours is **192.168.42.42**

```
options {
        directory "C:\bind9\zones";

        recursion yes;
        listen-on { 192.168.42.42; };
        allow-transfer { none; };

        forwarders {
                8.8.8.8;
                8.8.4.4;
        };
};

key "rndc-key" {
      algorithm hmac-sha256;
      secret "NvMpflM3AirONuT27azfU7A/1HhIFy4kV2N/QVCoqj4=";
};

controls {
      inet 127.0.0.1 port 953
              allow { 127.0.0.1; } keys { "rndc-key"; };
};

zone "yasser.local" {
        type master;
```

```
named.conf - Notepad
File  Edit  Format  View  Help
        forwarders {
                8.8.8.8;
                8.8.4.4;
        };
};

key "rndc-key" {
      algorithm hmac-sha256;
      secret "NvMpflM3AirONuT27azfU7A/lHhIFy4kV2N/QVCoqj4=";
};

controls {
      inet 127.0.0.1 port 953
              allow { 127.0.0.1; } keys { "rndc-key"; };
};

zone "yasser.local" {
        type master;
        file "yasser.local.zone";
};

zone "42.168.192.in-addr.arpa" {
        type master;
        file "192.168.42.rev";
};
Ln 32, Col 3    100%    Windows (CRLF)    UT
```

Put the marked part from your cmd in the “named.conf” file.

```
Command Prompt

C:\bind9\bin>rndc-confgen
# Start of rndc.conf
key "rndc-key" {
        algorithm hmac-sha256;
        secret "NvMpflM3AirONuT27azfU7A/lHhIFy4kV2N/QVCoqj4=";
};

options {
        default-key "rndc-key";
        default-server 127.0.0.1;
        default-port 953;
};
# End of rndc.conf

# Use with the following in named.conf, adjusting the allow list as needed:
# key "rndc-key" {
#       algorithm hmac-sha256;
#       secret "NvMpflM3AirONuT27azfU7A/lHhIFy4kV2N/QVCoqj4=";
# };
#
# controls {
#       inet 127.0.0.1 port 953
#               allow { 127.0.0.1; } keys { "rndc-key"; };
# };
# End of named.conf

C:\bind9\bin>csl
```

And save it. Create a new folder inside bind9 named “zones”. Create two files using the below names, provided in the **named.conf** file. In our case it’s **192.168.42.rev** and **yasser.local.zone.** 192.168.42 is the fst three parts of the IP address and yasser.local is our html file name.

named.conf - Notepad

File Edit Format View Help

```
        forwarders {
                8.8.8.8;
                8.8.4.4;
        };
};

key "rndc-key" {
      algorithm hmac-sha256;
      secret "NvMpf1M3AirONuT27azfU7A/1HhIFy4kV2N/QVCoqj4=";
};

controls {
      inet 127.0.0.1 port 953
              allow { 127.0.0.1; } keys { "rndc-key"; };
};

zone "yasser.local" {
        type master;
        file "yasser.local.zone";
};

zone "42.168.192.in-addr.arpa" {
        type master;
        file "192.168.42.rev";
};
```

Search in google writing “default zone bind9”

default zone bind9

All Images Videos News Maps More Tools

About 63,700 results (0.66 seconds)

https://github.com › bind9 › blob › master › debian › n...

bind9/named.conf.default-zones at master - GitHub

bind9/debian/named.conf.**default-zones** · Go to file T · Go to line L · Copy path · Copy permalink.

https://wiki.debian.org › Bind9

Bind9 - Debian Wiki

File /etc/bind/named.conf.**default-zones** — ... Debian 7 "Wheezy" **bind9** ships with a file containing **default** forward, reverse, and broadcast **zones**.

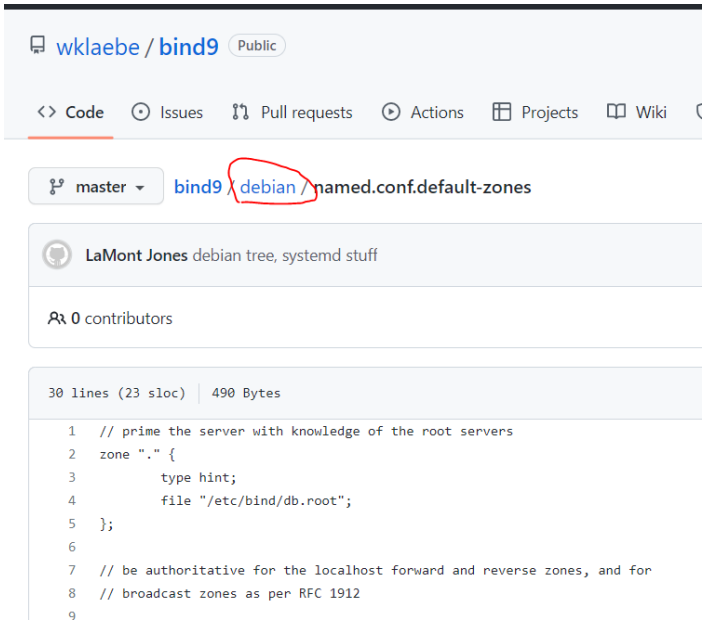
Configuration · File /etc/bind/named.conf... · File /etc/bind/named.conf.options

https://bind9.readthedocs.io › latest › chapter3

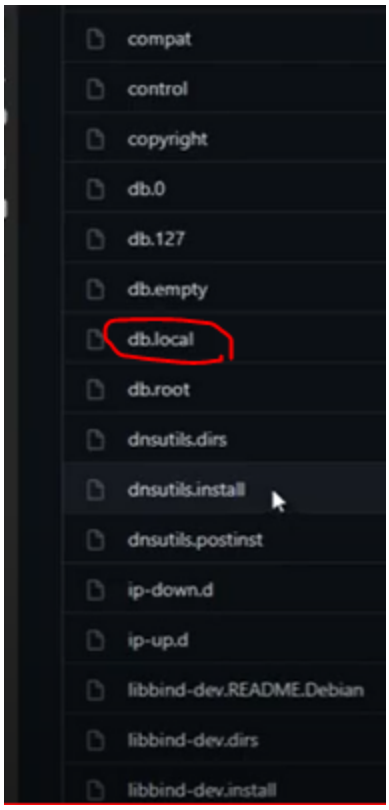
3. Configurations and Zone Files — BIND 9 9.19.5-dev ...

Zone files consist of Resource Records (RR), which describe the **zone's** characteristics or properties. 1; base **zone** file for example.com 2$TTL 2d ; **default** TTL ...

Visit this github profile.



Click on “debian”



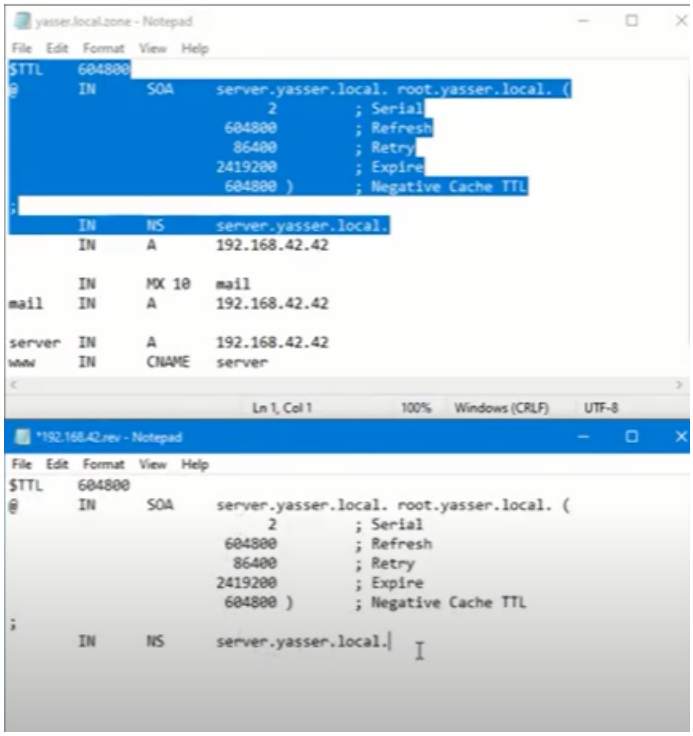
You will get a file named “db.local”. Go inside it and copy the highlighted code.

```
14 lines (14 sloc)   270 Bytes

;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
```

Paste it inside the “yasser.local.zone” file and modify it like in the image below.

```
*yasser.local.zone - Notepad
File  Edit  Format  View  Help
@       IN      SOA     server.yasser.local. root.yasser.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
        IN      NS      server.yasser.local
        IN      A       192.168.42.42

        IN      MX 10   mail
mail    IN      A       192.168.42.42

server  IN      A       192.168.42.42
www     IN      CNAME   server
ftp     IN      CNAME   server
```

Then copy the highlighted part from “yasser.local.zone” and paste it in “192.168.42.rev” like in the image below.



Paste this code in the “192.168.42.rev” file.

```
42    IN    NS    server.yasser.local.
42    IN    PTR   yasser.local.
42    IN    PTR   mail.yasser.local.
42    IN    PTR   www.yasser.local
42    IN    PTR   ftp.yasser.local.
```

Here, 42 is the last digit of the IP address. It will vary.

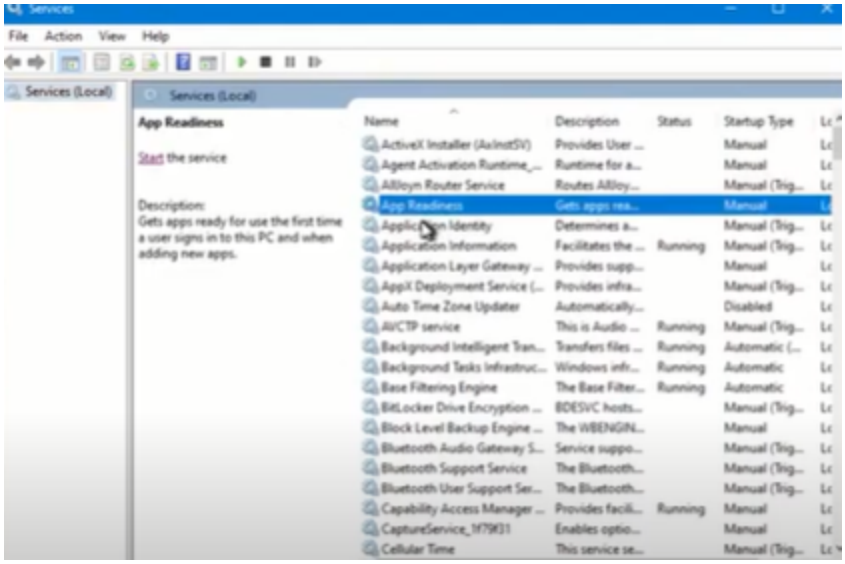
then , go to cmd and C:\bind9\bin path. Give the following command. If everything is okay, it will show no error.

~ **named-checkconf**

~ **named-checkzone yasser.local ..\zones\yasser.local.zone**

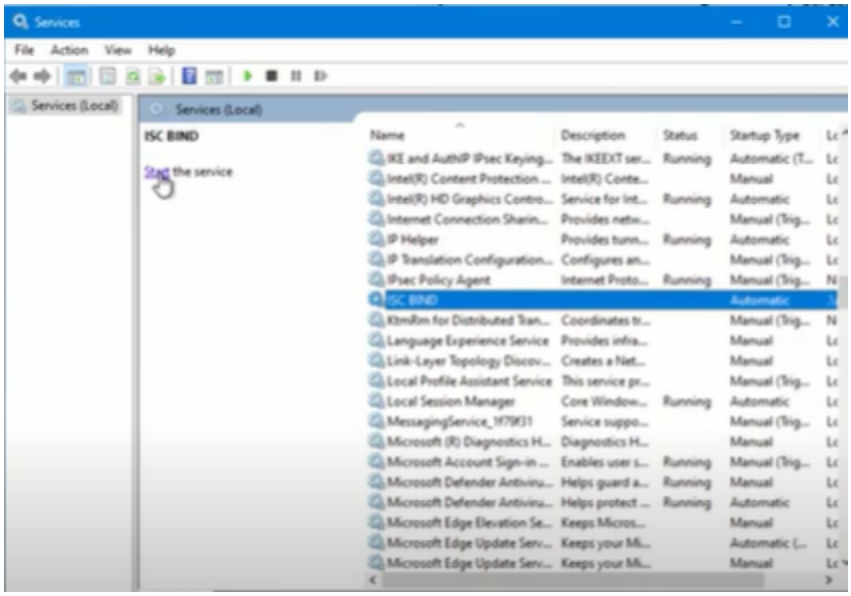
~ **named-checkzone 42.168.192.in-addr.arpa ..\zones\192.168.42.rev**

Then go to **service**. Choose **app Readiness** and click on **start**.



Then choose **ISC BIND** and click on properties >log on > click on local system account. And then start. It will install.

.



Then go to setting > change adapter option. Choose your network. Go to properties > Internet protocol version 4 > advanced > DNS and add DNS server address and suffix. Then press ok. Disable your network and enable it again.
Repeat this 3 lines for client DNS also and configuration will complete.

copy certificates and pfx files in the client system then install pfx files. Also, modify the necessary options and will be able to see the lock from a different system.

Step 6: DOS attack
Install kali linux in virtualbox . go to the terminal.paste the following command:
~ **sudo apt update**
Then provide a password
~ **sudo apt install kali-root-login**
~ **sudo passwd**
Then provide a password and finally close the terminal.

Go to following path:
Application > vulnerability analysis > legion(root) > add host

Provide host's IP address,
Mode selection: hard
Port scan options: TCP
Host discovery option: ICMP

Then submit it. It will start to attack.

Step 7: observe the attack with snort

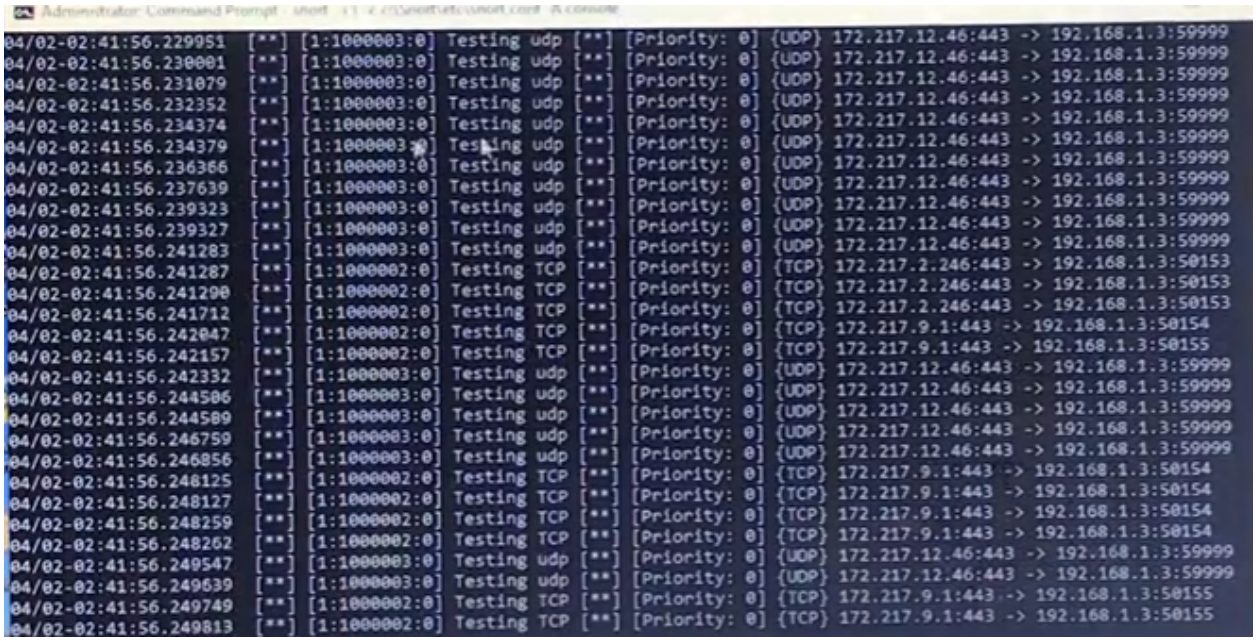
Install snort and rules in the author's system. Set up and Open it. Open cmd and give the following command.

Go to cd c:\Snort\bin

~ **snort -i 1 -c c:\Snort\etc\snort.conf -T**

~ **snort -i 1 -c c:\Snort\etc\snort.conf -A console**

You will see the packet is captured.



```
04/02-02:41:56.229951  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.230001  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.231079  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.232352  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.234374  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.234379  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.236366  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.237639  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.239323  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.239327  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.241283  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.241287  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 172.217.2.246:443 -> 192.168.1.3:50153
04/02-02:41:56.241290  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 172.217.2.246:443 -> 192.168.1.3:50153
04/02-02:41:56.241712  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 172.217.2.246:443 -> 192.168.1.3:50153
04/02-02:41:56.242047  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 172.217.9.1:443 -> 192.168.1.3:50154
04/02-02:41:56.242157  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 172.217.9.1:443 -> 192.168.1.3:50155
04/02-02:41:56.242332  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.244506  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.244589  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.246759  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.246856  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.248125  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 172.217.9.1:443 -> 192.168.1.3:50154
04/02-02:41:56.248127  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 172.217.9.1:443 -> 192.168.1.3:50154
04/02-02:41:56.248259  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 172.217.9.1:443 -> 192.168.1.3:50154
04/02-02:41:56.248262  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 172.217.9.1:443 -> 192.168.1.3:50154
04/02-02:41:56.249547  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.249639  [**] [1:1000003:0] Testing udp [**] [Priority: 0] {UDP} 172.217.12.46:443 -> 192.168.1.3:59999
04/02-02:41:56.249749  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 172.217.9.1:443 -> 192.168.1.3:50155
04/02-02:41:56.249813  [**] [1:1000002:0] Testing TCP [**] [Priority: 0] {TCP} 172.217.9.1:443 -> 192.168.1.3:50155
```