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.

Go to:
Xampp→apache→conf→httpd.conf:
Paste the below part there and save it.

DocumentRoot "C:/acmesecureserver"
<Directory "C:/acmesecureserver">

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**

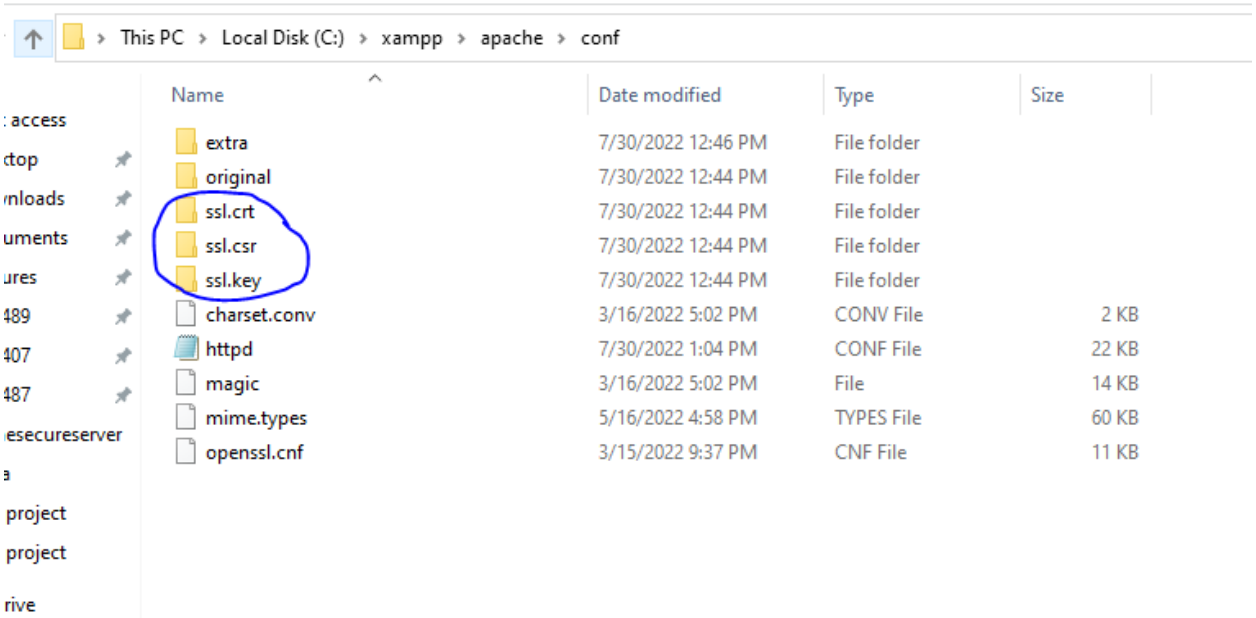
Exporting the server key file in the server .pfx file –
~ **pkcs12 -inkey server.key -in server.crt -export -out server.pfx**

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>
```

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

Windows Defender Firewall

Control Panel › System and Security › Windows Defender Firewall

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Avengers
Notification state:	Notify me when Windows Defender Firewall blocks a new app

See also

Security and Maintenance

Network and Sharing Center

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall with

Inbound Rules

Outbound Rules

Connection Security Rules

Monitoring

Inbound Rules

Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Au
No	Any	Any	Any	TCP	53, 80, 443	Any	Any	An
No	C:\progr...	Any	Any	UDP	Any	Any	Any	An
No	C:\progr...	Any	Any	TCP	Any	Any	Any	An
No	C:\users\...	Any	Any	UDP	Any	Any	Any	An
No	C:\users\...	Any	Any	TCP	Any	Any	Any	An
No	C:\users\...	Any	Any	TCP	Any	Any	Any	An
No	C:\users\...	Any	Any	UDP	Any	Any	Any	An
No	C:\xamp...	Any	Any	UDP	Any	Any	Any	An
No	C:\xamp...	Any	Any	TCP	Any	Any	Any	An
No	C:\xamp...	Any	Any	UDP	Any	Any	Any	An
No	C:\xamp...	Any	Any	TCP	Any	Any	Any	An
No	C:\Progr...	Any	Any	Any	Any	Any	Any	An
No	C:\progr...	Any	Any	TCP	Any	Any	Any	An
No	C:\progr...	Any	Any	UDP	Any	Any	Any	An
No	C:\app\n...	Any	Any	UDP	Any	Any	Any	An
No	C:\app\n...	Any	Any	TCP	Any	Any	Any	An
No	C:\Progr...	Any	Any	UDP	6004	Any	Any	An
No	C:\xamp...	Any	Any	UDP	Any	Any	Any	An
No	C:\xamp...	Any	Any	UDP	Any	Any	Any	An
No	C:\xamp...	Any	Any	TCP	Any	Any	Any	An
No	C:\xamp...	Any	Any	TCP	Any	Any	Any	An
No	C:\users\...	Any	Any	TCP	Any	Any	Any	An
No	C:\users\...	Any	Any	UDP	Any	Any	Any	An
No	C:\progr...	Any	Any	TCP	Any	Any	Any	An
No	C:\progr...	Any	Any	UDP	Any	Any	Any	An
No	C:\progr...	Any	Any	TCP	Any	Any	Any	An
No	C:\progr...	Any	Any	UDP	Any	Any	Any	An
No	C:\progr...	Any	Any	TCP	Any	Any	Any	An
No	C:\progr...	Any	Any	UDP	Any	Any	Any	An
No	C:\Progr...	Any	Any	UDP	Any	Any	Any	An
No	C:\Progr...	Any	Any	TCP	Any	Any	Any	An
No	C:\Progr...	Any	Any	TCP	Any	Any	Any	An

Actions

Inbound R...

New ...

Filter ...

Filter ...

Filter ...

View

Refresh

Expor...

Help

53, 80, 443

Disabl...

Cut

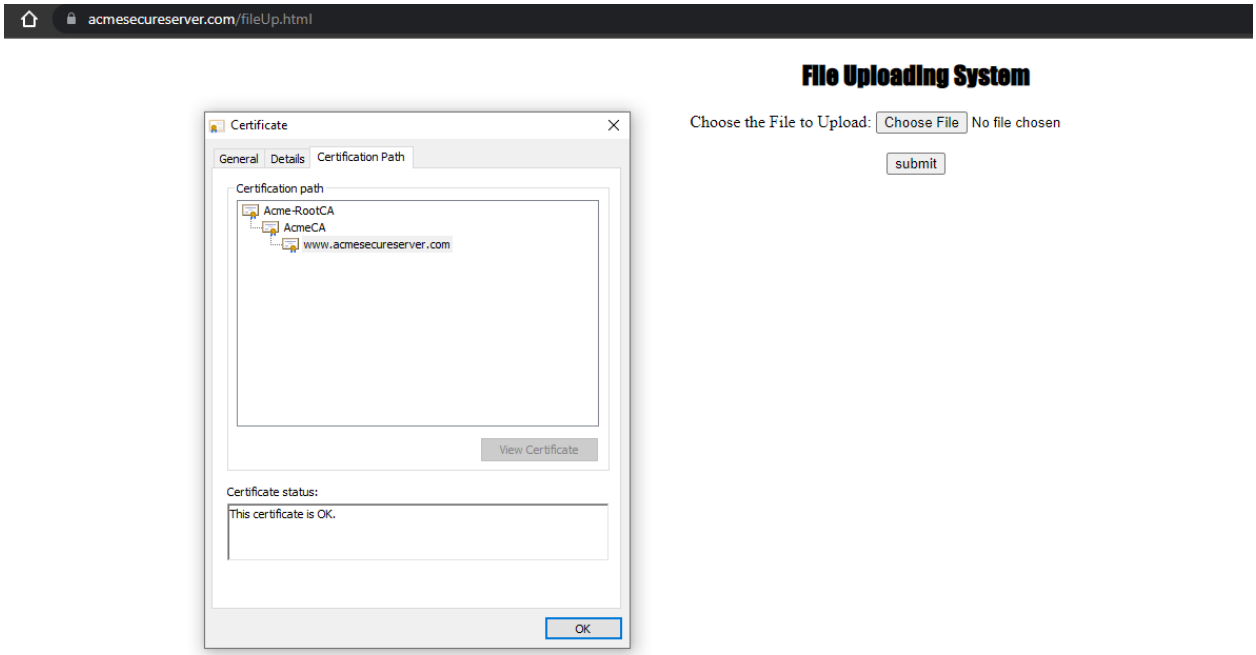
Copy

Delete

Prope...

Help

Finally, we will open our xampp and turn on Apache and go to our website which is running with SSL Certificate. We have also shown our certification path.



Step 3: Revocation of certificate:

Then 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
```

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 –

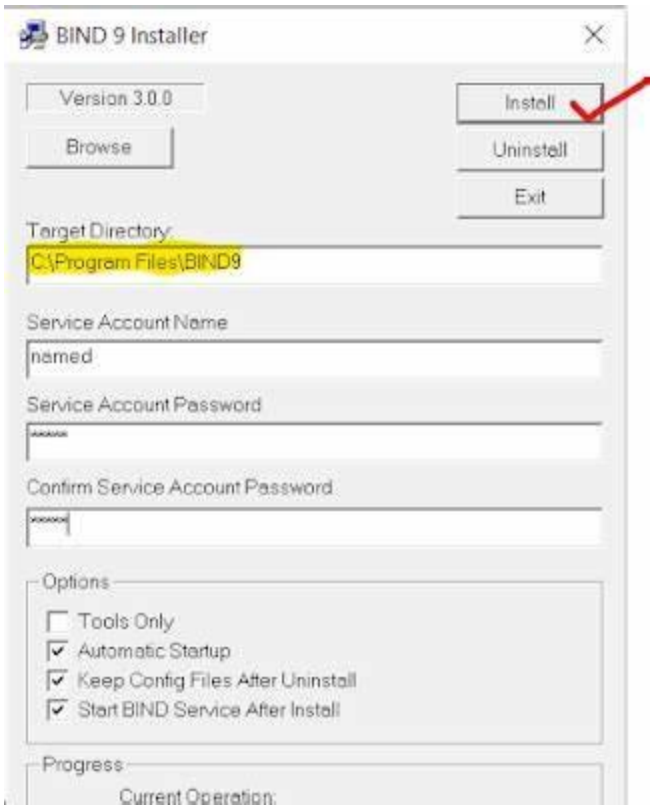
~ **crl -in rev.crl -noout -text**

Step 4: DNS Configuration

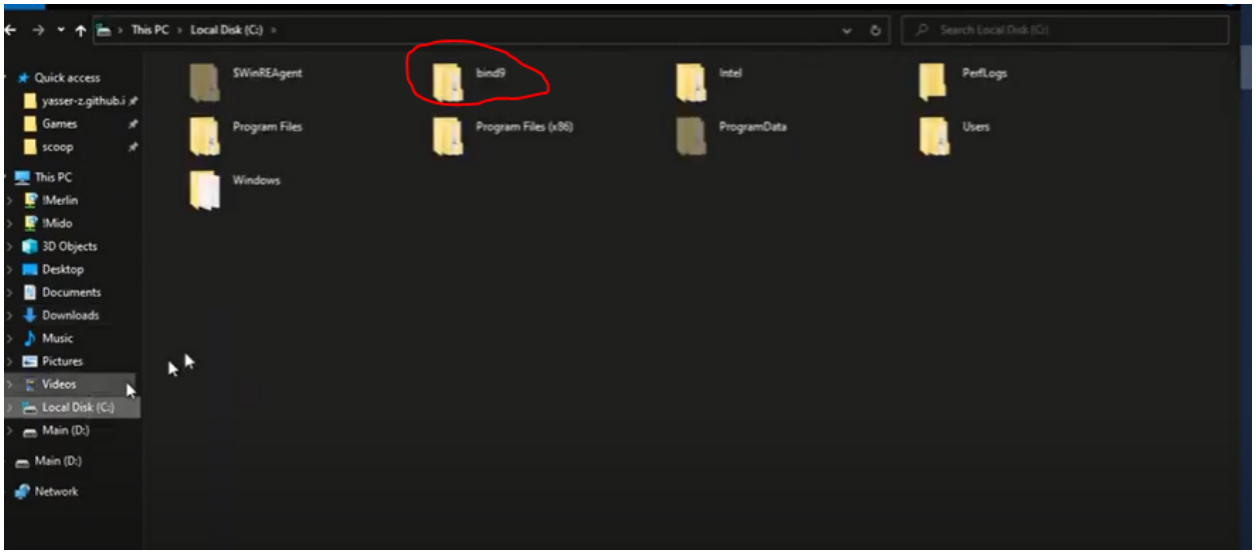
Install bind9 on the PC with necessary information.

Target Directory - C:\bind9

Then click on “Install” to install it.

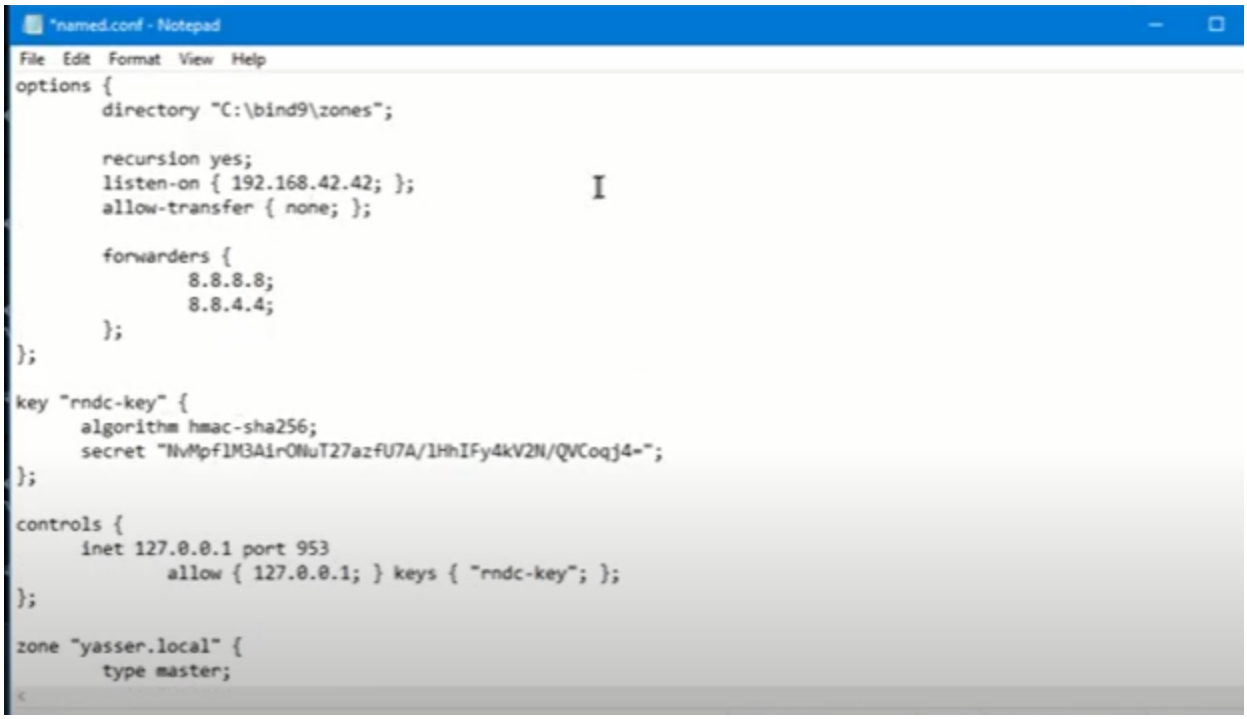


After installation, we get a file in C drive named “bind9”.



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.




```
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)

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.

copy certificates and pfx files in another system then install pfx file. 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 in the author's system. Set up and Open it. You will see the packet is captured.