Submitted To:

Rashedul Amin Tuhin

Senior Lecturer

Department of Computer Science and Engineering

East West University

Submitted By:

Name	ID
Ronojith Saha Roy Dipta	2019-1-60-103
Mainul Hasan	2019-1-60-130

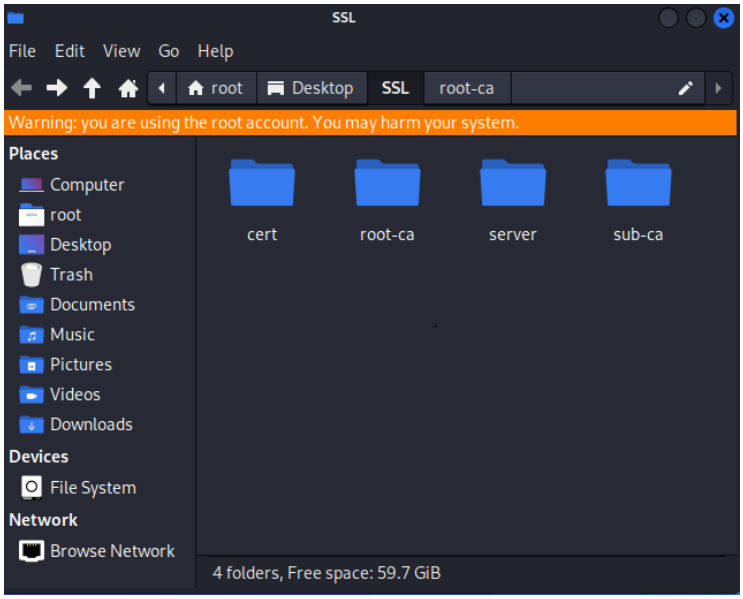
Submission date:

15/10/2022

Certificate Generation:

1. Make directories

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



2. Create index file

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

3. Generate 16 bithexcode for rootca and subca

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

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

4. Generate private key for rootCA

openssl genrsa -aes256 -out root-ca/private/ca.key 4096

5. Generate private key for sub ca

openssl genrsa -aes256 -out sub-ca/private/sub-ca.key 4096

6. Generate private key for server

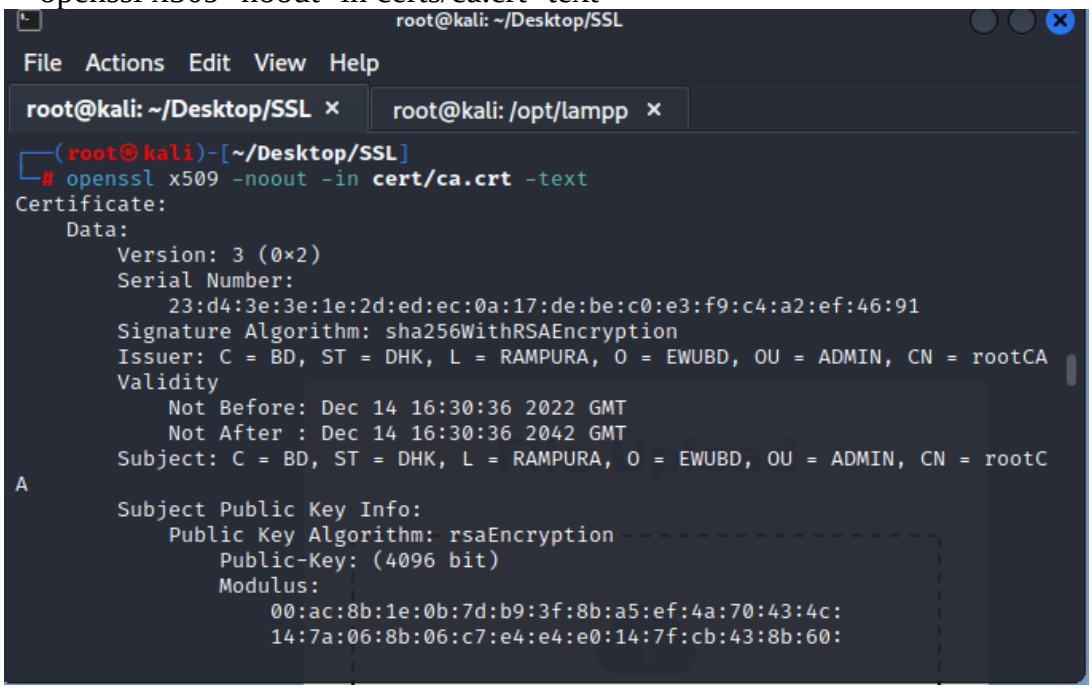
openssl genrsa -out server/private/server.key 2048

7. Create CA certificate using rootCA config file and private key

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

#Enter organization name, unit name, and common name.

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



8. Generate signing request using subCA config file and subCA private key

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

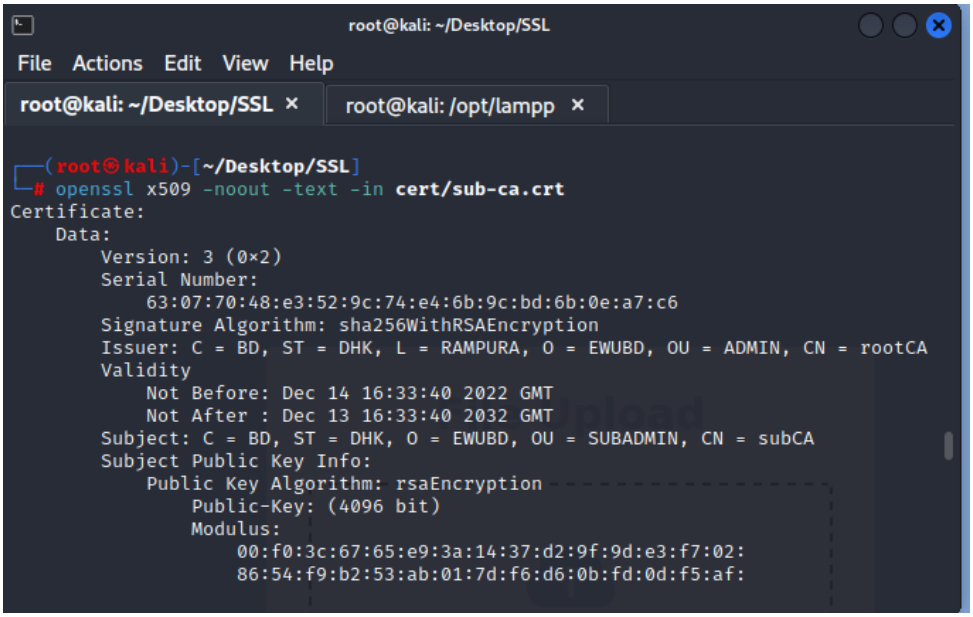
9. Sign subCA certificate using the rootCA certificate

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

Check if the certificate is signed:

cat index

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



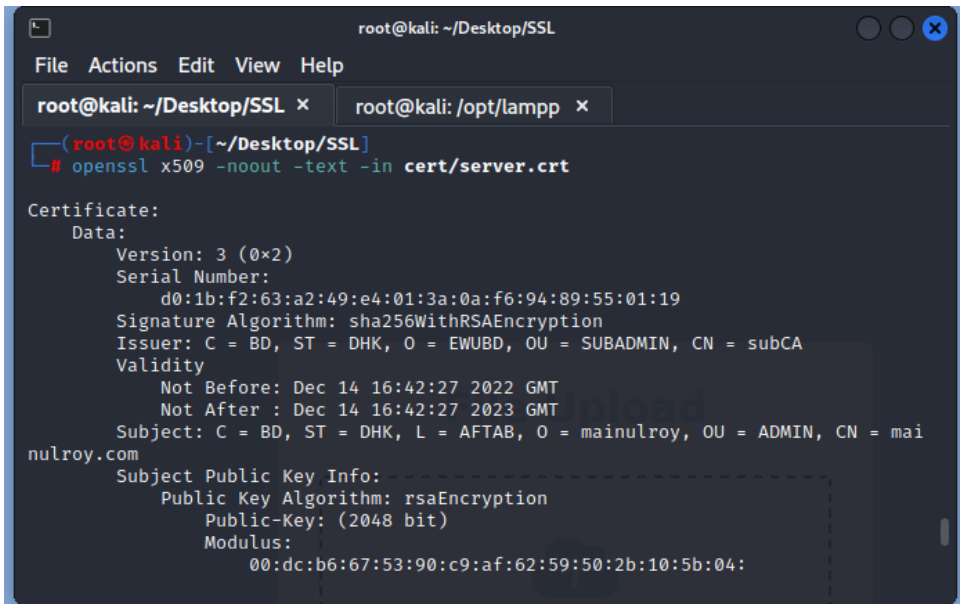
10. Create server request

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

mainulroy.com

11. Sign server certificate using sub-ca

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



12. Map 127.0.0.1 to our website

echo "127.0.0.1 www.mysecureserver.com" >> /etc/hosts

13. In another terminal check:

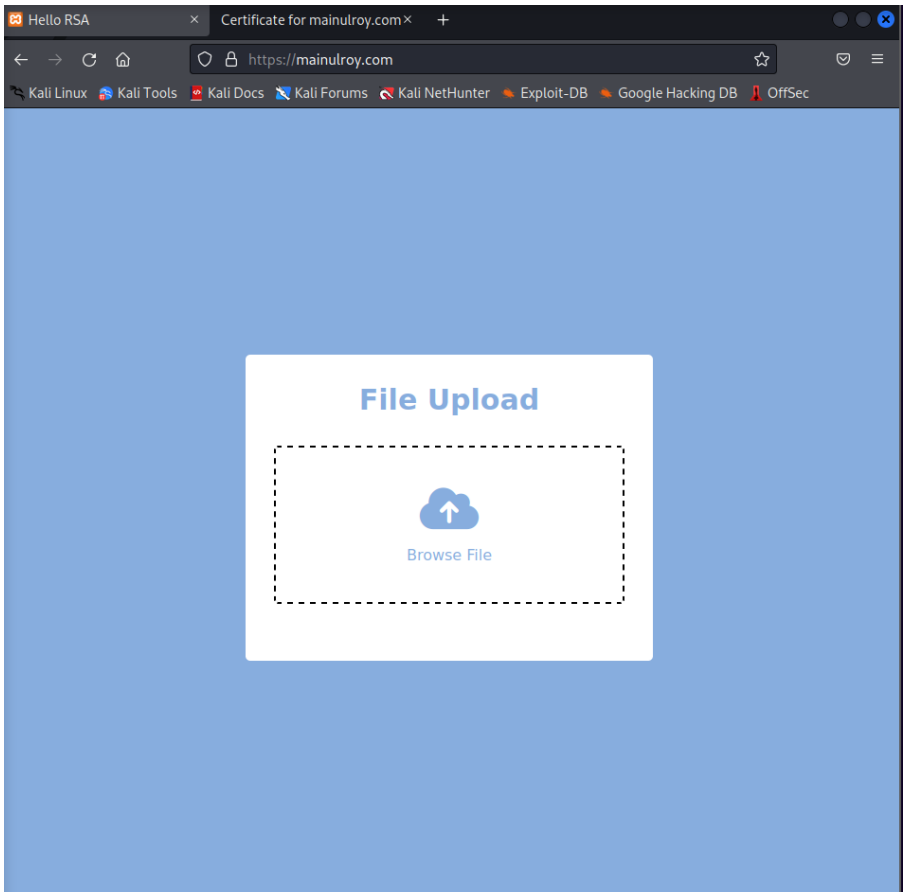
curl https://mainulroy.com

*You will see that you cannot connect to the website securely.

You have to update the ca-certificates folder.

14. Now check with curl:

https://www.mainulroy.com



DNS Setup:

sudo apt install bind9

#192.168.253.129 is the machine IP in your LAN where your server is going to be.

gedit named.conf.local

Make forward lookup zone and reverse lookup zone

```
zone    "mainulroy.com" {
        type master;
        file "/etc/bind/db.forward.com";
};

zone    "253.168.192.in-addr-arpa"      {
        type master;
        file "/etc/bind/db.reverse.com";
};
```

Here, create a forward lookup zone and a reverse lookup zone.

Make records for forward and reverse lookup zone database

```
$TTL    604800
@       IN      SOA     ns1.mainulroy.com. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.mainulroy.com
ns1     IN      A       192.168.253.129
server  IN      A       192.168.253.129
```

```
$TTL    604800
@       IN      SOA     ns1.mainulroy.com. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS1     ns1.
129     IN      PTR     ns1.mainulroy.com.
129     IN      PTR     server.mainulroy.com.
```

Restart bind9 and check status

sudo service bind9 restart

sudo service bind9 status

```
┌──(root㉿kali)-[/etc/bind]
└─# sudo service bind9 status
× named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: >
     Active: failed (Result: signal) since Thu 2022-12-15 12:08:07 EST; 36min ago
   Duration: 5ms
       Docs: man:named(8)
    Process: 307198 ExecStart=/usr/sbin/named -f $OPTIONS (code=killed, signal=A>
   Main PID: 307198 (code=killed, signal=ABRT)
        CPU: 5ms

Dec 15 12:08:07 kali systemd[1]: named.service: Scheduled restart job, restart c>
Dec 15 12:08:07 kali systemd[1]: Stopped BIND Domain Name Server.
Dec 15 12:08:07 kali systemd[1]: named.service: Start request repeated too quick>
Dec 15 12:08:07 kali systemd[1]: named.service: Failed with result 'signal'.
Dec 15 12:08:07 kali systemd[1]: Failed to start BIND Domain Name Server.
lines 1-14/14 (END)
```

ping

ping www.mainulroy.com

```
┌──(root㉿kali)-[~/Desktop]
└─# ping www.mainulroy.com
PING www.mainulroy.com (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.062 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.060 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.039 ms
64 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.063 ms
64 bytes from localhost (127.0.0.1): icmp_seq=6 ttl=64 time=0.045 ms
64 bytes from localhost (127.0.0.1): icmp_seq=7 ttl=64 time=0.045 ms
64 bytes from localhost (127.0.0.1): icmp_seq=8 ttl=64 time=0.057 ms
64 bytes from localhost (127.0.0.1): icmp_seq=9 ttl=64 time=0.043 ms
64 bytes from localhost (127.0.0.1): icmp_seq=10 ttl=64 time=0.056 ms
64 bytes from localhost (127.0.0.1): icmp_seq=11 ttl=64 time=0.053 ms
64 bytes from localhost (127.0.0.1): icmp_seq=12 ttl=64 time=0.043 ms
64 bytes from localhost (127.0.0.1): icmp_seq=13 ttl=64 time=0.043 ms
64 bytes from localhost (127.0.0.1): icmp_seq=14 ttl=64 time=0.046 ms
64 bytes from localhost (127.0.0.1): icmp_seq=15 ttl=64 time=0.046 ms
64 bytes from localhost (127.0.0.1): icmp_seq=16 ttl=64 time=0.036 ms
64 bytes from localhost (127.0.0.1): icmp_seq=17 ttl=64 time=0.038 ms
```

Firewall Configuration:

Install ufw package

sudo apt install ufw

Set default rules for ufw firewall

ufw default allow outgoing

ufw default deny incoming

ufw allow ssh

ufw enable

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

ufw allow 80

ufw allow 443

ufw allow 53

```
┌──(root㉿kali)-[/etc/bind]
└─# ufw allow ssh
Rule added
Rule added (v6)

┌──(root㉿kali)-[/etc/bind]
└─# ufw allow 53
Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(root㉿kali)-[/etc/bind]
└─# netstat -an | grep "LISTEN "
tcp6       0      0 :::443                  :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN

┌──(root㉿kali)-[/etc/bind]
└─#
```