1/__/____

* DNS.

deb3

① Static IP. - 192.168.80.103

Hostname ser1 (ser1.shuhasilabs.local

address

netmask

network

gateway 80.2

dns

deb1 rootca.shuhari.local
- 192.168.80.101

deb2 subca.shuhari.local
- 192.168.80.102

deb3 ser1.shuhari.local | www.shuhari.local | ns1.shuhari.local
- 192.168.80.103

sudo ~~aptitude~~ apt-get install openssl apache2 tree
sudo apt-get install bind9 dnsutils
cp db.local → db.shuhari.local

SOA ser1.shuhari.local. root.shuhari.local. {
14122022 ; serial.

	IN	NS	ser1.shuhari.local.
ser1	IN	A	192.168.80.103
ns1	IN	CNAME	ser1
www	IN	CNAME	ser1
rootca	IN	A	(92.168.80.101)
subca	IN	A	192.168.80.102

cp /etc/bind/db.127 /etc/bind/db.192. -> reverse.

```
@       SOA     ser1.shuhari.local.  root.shuhari.local. (
        14122022        ; serial.

        IN      NS      ser1.shuhari.local.
        IN      PTR     shuhari.local
101     IN      PTR     rootca.shuhari.local.
102     IN      PTR     subca.shuhari.local.
103     IN      PTR     ser1.shuhari.local.
103     IN      PTR     www.shuhari.local.
103     IN      PTR     ns1.shuhari.local.
```

/etc/bind/named.conf.local.

```
zone "shuhari.local" {
        type master;
        file "/etc/bind/db.shuhari.local";
};

zone "80.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/~~192~~.db.192";
};
```

__/__/____

/etc/resolve.conf

domain shuhari.local
search shuhari.local
nameserver 192.168.80.103

} → 3 same in 3 machines.

→ deb1.
80.101
hostnam → rootca.shuhari~~deb~~.local

→ deb2
80.102
hostname → subca.shuhari.l~~o~~cal

PKI.

Implementation using openssl.

rootca → creating a db for certificates.

* Certificates Lab.

- rootca db machine. (deb1). → login as shuhari.

pwd /home/shuhari.

mkdir ca → store all PKi files.

cd ca/

mkdir -p certs crl newcerts private subca/csr subca/certs/

tree ca/

chmod 700 private/ private folder → for private keys.

4 files

① index file → when certificate is created it will be reflected in index file.

② attribute file → stores configurations of certificates.

serial no. files:-

③ Certificate serial no.

④ CRL no.

pwd

/home/shuhari/ca

touch index.txt

touch index.txt.attr

echo 1000 > serial

echo 1000 > crlnumber

tree ca/

crl

→ index

index.txt.attr

crlnumber

private

-serial.

download rootca.~~conf~~ cnf. (server).
inside ca/ directory
wget.

nano rootca.cnf.
change dir = /home/shuhari/ca. (/root/ca / /home/shuhari/ca).

→ generate private key encrypted for rootca.

→ encryption using aes

openssl genrsa -aes256 \
-out private/ca.key.pem 4096 → key size.

→ give ~~pass~~ pass phrase. (12345)

chmod 400 private/ca.key.pem

Openssl req -config rootca.cnf -key private/ca.key.pem
-new -x509 -days 7300 -sha256
-extensions v3_ca -out certs/ca.cert.pem

→ enter pass phrase (password).

→ SHUHARI.

Commonname → Shuhai Root CA.

chmod 444 certs/ca.cert.pem

In deb2 - SubCA.

pwd
/home/shuhari
mkdir subca
cd subca
mkdir certs crl csr newcerts private
chmod 700 private
touch index.txt
touch index.txt.attr
echo 1000 > serial
echo 1000 > crlnumber

download subca.cnf (server).

wget . .

→ generate private key. openssl genrsa -aes256 -out private/subca.key.pem 4096
→ give password.

chmod 400 private/subca.key.pem

, csr → certificate signing request. (form to request for a certificate).

nano subca.cnf
Change dir → /home/shuhari/subca

give same organization name while generating csr.

* generate csr.

openssl req -config subca.cnf -new -sha256 -key private/subca.key.pem -out csr/subca.csr.pem

→ enter/give password.

Common name → Shuhari Sub CA.

↑ in rootca machine.

get subca.csr.pem to /home/shuhari/ca/subca/csr/->
scp subca.csr.pem shuhari@192.168.80.100:/home/shuhari/ca/subca/csr/
↑ rootca ip.

* In deb1 (rootca)

pwd
/home/shuhari/ca

openssl ca -config rootca.cnf -extensions v3_intermediate_ca -days 3650 -notext -md sha256 -in subca/csr/subca.csr.pem -out subca/certs/subca.cert.pem

→ give password of root private key.

→ 4.

newcerts → 1000.pem
subca/certs → subca.cert.pem
} → both are same as rootca keeps a copy of signed certificate in its db.

serial -no. will increment and replace the old serial file with serial.old.

md5sum newcerts/1000.pem subca/certs/subca.cert.pem
chmod 444 subca/certs/subca.cert.pem

hash value to verify → whether subca certificate is same as our copy.

* Verify relation between rootca & subca. (rootca deb)

Openssl verify -CAfile certs/ca.cert.pem
subca/certs/subca.cert.pem

→ OK.

* Create certificatechain flag. (rootca deb).

cat subca/certs/subca.cert.pem certs/ca.cert.pem >
subca/certs/ca-chain.cert.pem

copy. rootca → subca/certs/ca-chain & subca.cert.pem to.

subca → certs/
folder

In deb2 → subca

In deb3 → ser1.

pwd
/home/shuhari
mkdir certs
cd certs

wget subca.cnf → server.

openssl genrsa -out www.shuhari.local.key.pem 2048

chmod 400 www.shuhari.local.key.pem

website name → www.shuhari.local
↳ this name should be same in Common Name for webserver CSR.

* generate CSR file for webserver.

Openssl ~~req~~ req -config subca.cnf
-key www.shuhari.local.key.pem
-new -sha256 -out www.shuhari.local.csr.pem

Copy ser1's csr file to subca's → csr folder.

In deb2 subca machine

openssl ca -config subca.cnf -extensions server_cert
-days 375 -notext -md sha256
-in csr/www.shuhari.local.csr.pem
-out certs/www.shuhari.local.cert.pem

Copy 2 files www.shuhari.local.cert.pem &
ca-chain.certpem from subca/certs to
ser1/certs

In deb3 → ser1 · cd → certs
Openssl verify -CAfile ca-chain.cert.pem
www.shuhari.local.cert.pem
→ OK

sudo mkdir /etc/~~mkdir~~apache2/ssl
sudo cp ca-chain.cert.pem /etc/apache2/ssl
sudo cp www.shuhari.local.cert.pem /etc/apache2/ssl

sudo cp www.shuhari.local.key.pem /etc/apache2/ssl
sudo chmod 600 /etc/apache2/ssl/*
sudo a2enmod ssl

sudo a2ensite default-ssl

sudo nano /etc/apache2/sites-enabled/default-ssl.conf

ServerName www.shuhari.local

SSLCertificateFile /etc/apache2/ssl/www.shuhari.local.cert.pem.

SSLCertificateKeyFile /etc/apache2/ssl/www.shuhari.local.key.pem.

uncomment SSLCACertificateFile line.
& give path /etc/apache2/ssl/ca-chain.cert.pem

sudo systemctl reload apache2
restart apache2
status

windows base → etc/hosts file.
192.168.80.103 www.shuhari.local.

On ser1 deb.

verify certificate through CLI.
openssl s_client -connect www.shuhari.local:443