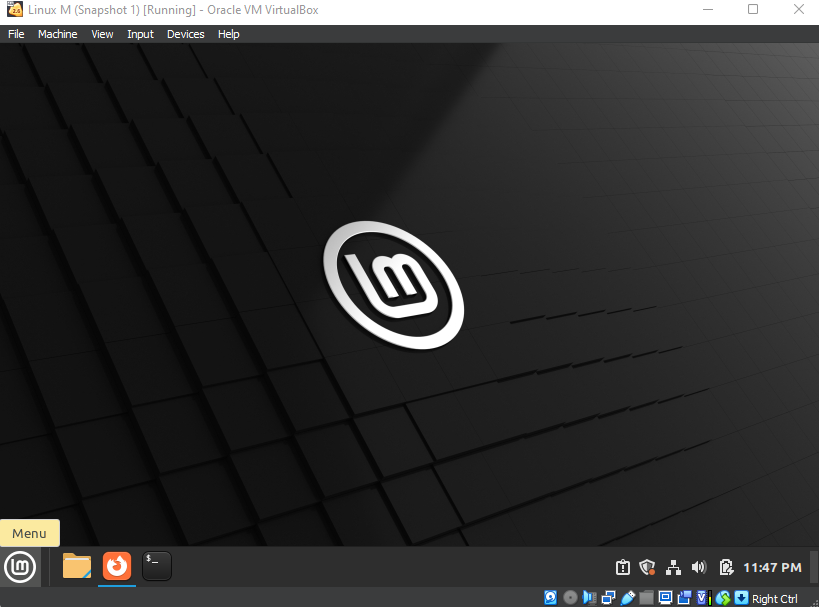
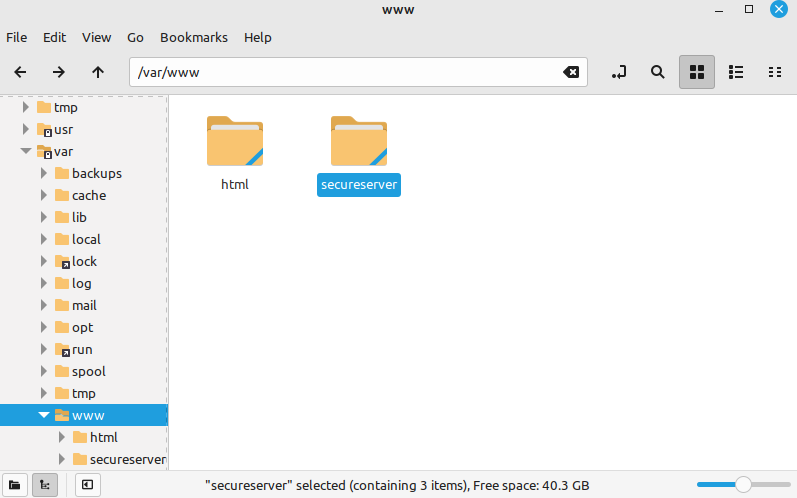
**HOST SERVER**





**Reload main:**

* sudo a2dissite 000-default
* systemctl reload apache2
* sudo a2ensite main
* systemctl reload apache2

<VirtualHost \*:80>

    ServerName verysecureserver.com

    ServerAlias www.verysecureserver.com

    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/secureserver

    ErrorLog ${APACHE\_LOG\_DIR}/error.log

    CustomLog ${APACHE\_LOG\_DIR}/access.log combined

</VirtualHost>

<VirtualHost \*:443>

    ServerName verysecureserver.com

    ServerAlias www.verysecureserver.com

    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/secureserver

    ErrorLog ${APACHE\_LOG\_DIR}/error.log

    CustomLog ${APACHE\_LOG\_DIR}/access.log combined

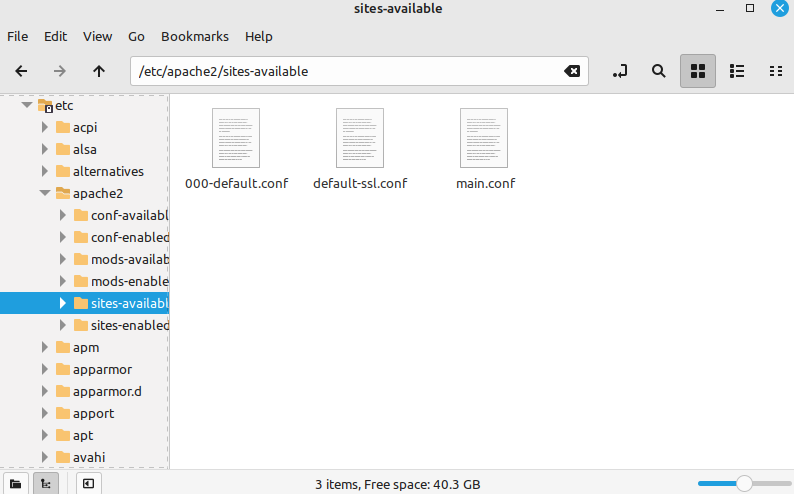
    SSLEngine on

        SSLCertificateFile /home/openssl/server/certs/server.crt

        SSLCertificateKeyFile /home/openssl/server/private/server.key

        SSLCertificateChainFile /home/openssl/chained.crt

</VirtualHost>

****

**Restrat server: Starting And Stopping Apache and Database Server:**

* service apache2 stop
* service apache2 start
* service apache2 status
* service apache2 restart
* service apache2 reload

**DNS Configuration package:**

* sudo apt install bind9
* sudo apt install dnsutils
* sudo systemctl restart bind9.service
* sudo nano /etc/resolv.conf
* sudo nano /etc/named.conf
* sudo nano /etc/bind/verysecureserver.com.zone

**Check DNS Connection:**

* dig verysecureserver.com
* nslookup verysecureserver.com

**Create certificate and sign this site with the certificate:**

1. mkdir {root-ca,sub-ca,server}
2. mkdir {root-ca,sub-ca,server}/{private,certs,newcerts,crl,csr}
3. touch root-ca/index
4. touch sub-ca/index
5. openssl genrsa -aes256 -out root-ca/private/ca.key 4096
6. openssl genrsa -aes256 -out sub-ca/private/sub-ca.key 4096
7. openssl genrsa -out server/private/server.key 2048
8. cd root-ca
9. openssl req -config root-ca.conf -key private/ca.key -new -x509 -days 7200 -sha256 -extensions v3\_ca -out certs/ca.crt

#common name : Acme-RootCA

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

#common name : Acme

1. cd ../root-ca
2. openssl ca -config root-ca.conf -extensions v3\_intermediate\_ca -days 3650 -notext -in ../sub-ca/csr/sub-ca.csr -out ../sub-ca/certs/sub-ca.crt -rand\_serial
3. cd ../server
4. openssl req -config server.conf -key private/server.key -new -sha256 -out csr/server.csr

#common name : verysecureserver.com

1. cd ../sub-ca
2. openssl ca -config sub-ca.conf -extensions server\_cert -days 365 -notext -in ../server/csr/server.csr -out ../server/certs/server.crt -rand\_serial
3. cd ..
4. cat ./server/certs/server.crt ./sub-ca/certs/sub-ca.crt > chained.crt

**Revoke certificate:**

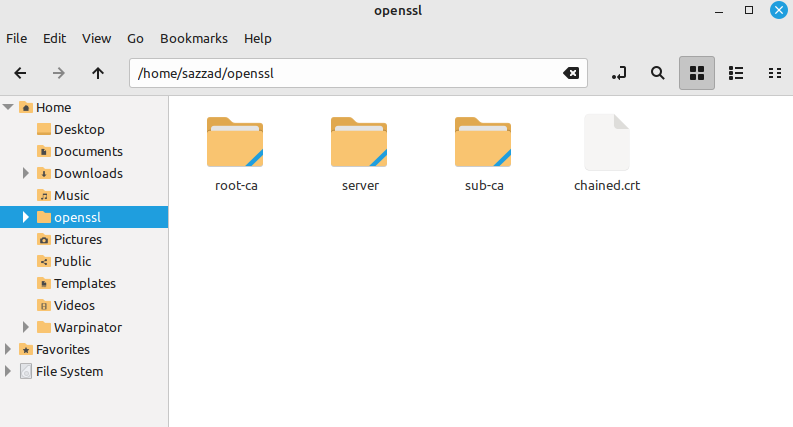
* cd sub-ca
* openssl ca -config sub-ca.conf -revoke ../server/certs/server.crt

**Add CRL to server**

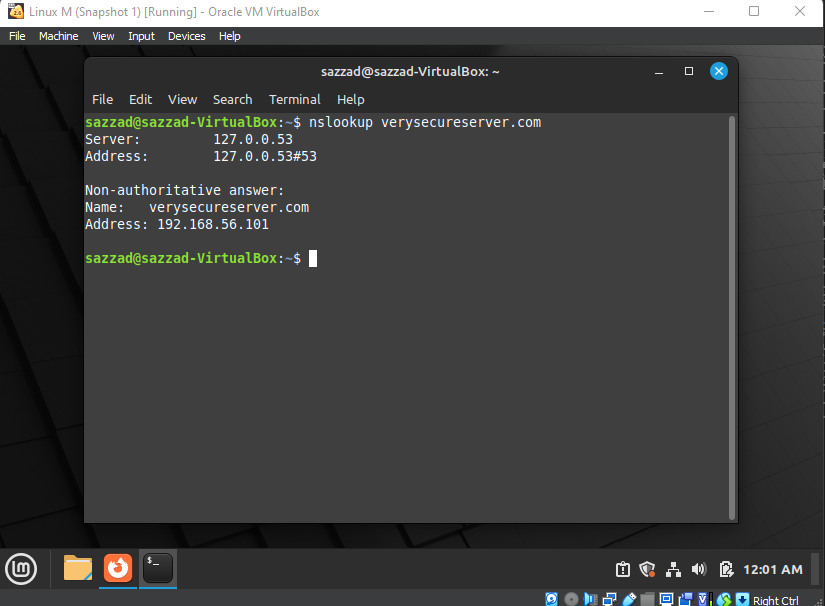
* cd sub-ca
* nano crlnumber

#type: 1002

* openssl ca -config sub-ca.conf -gencrl -out crl/rev.crl

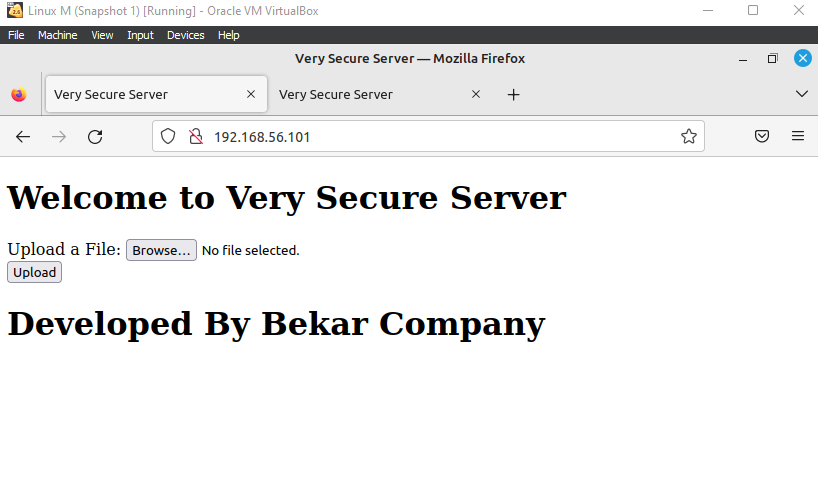


**Figure: Certificate and sign this site with the Certificate.**

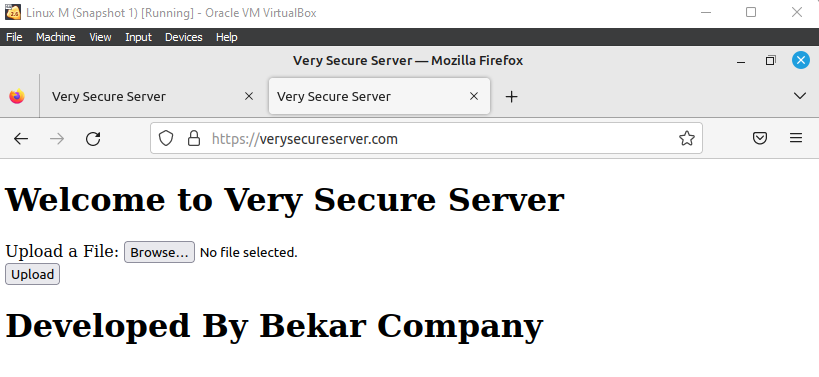
****

**Figure:** DNS configuration is Done.

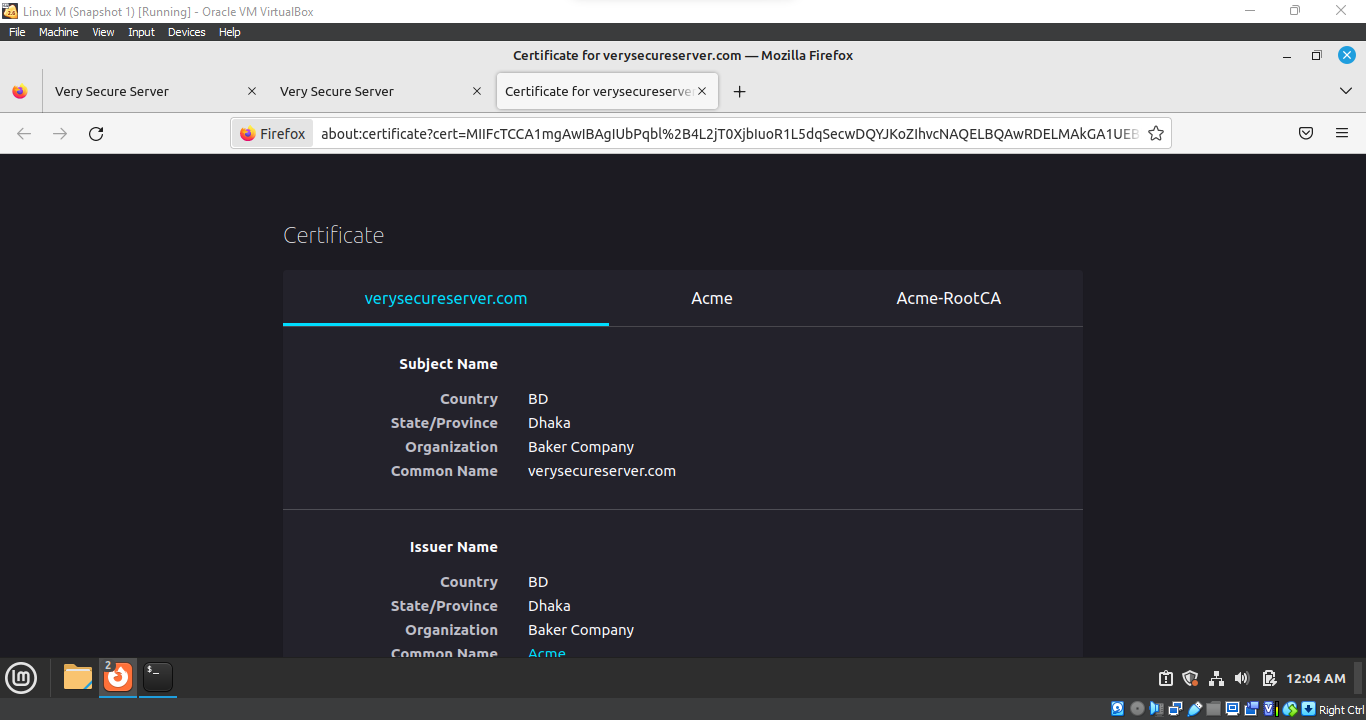
**IP ADDRESS:**

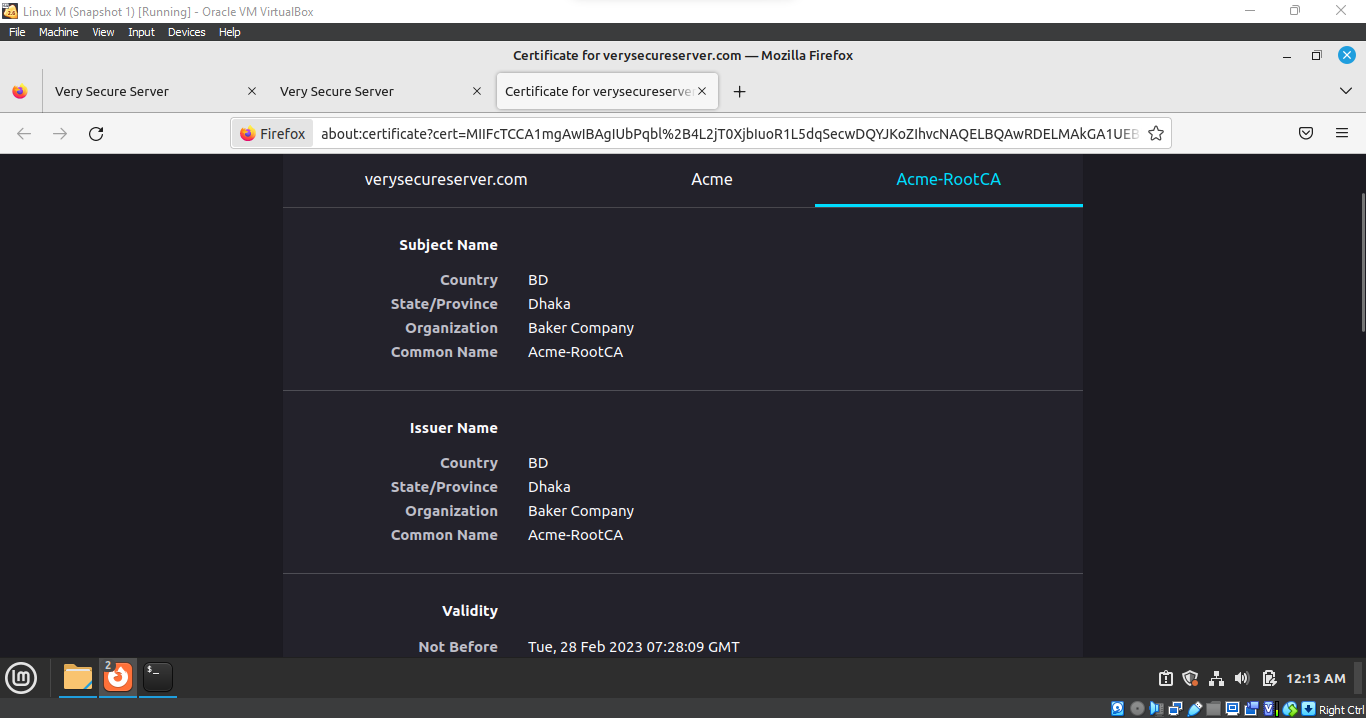
****

**Domain verysecureserver.com:**

****

**Certificate:**

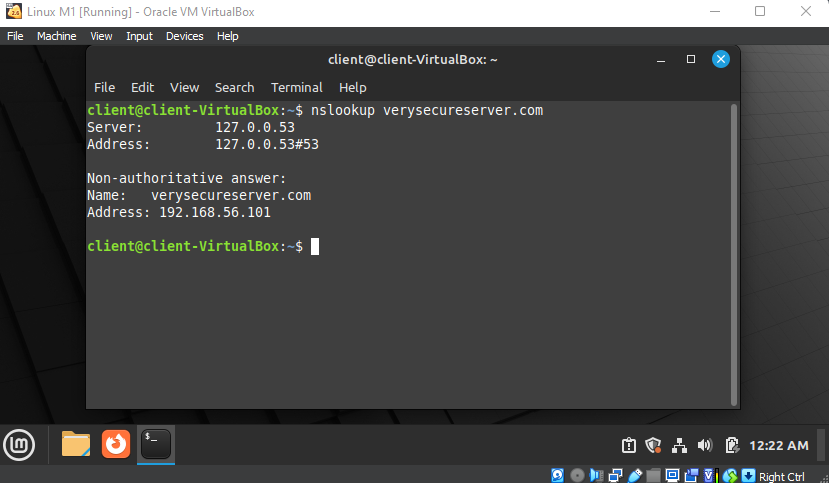
****

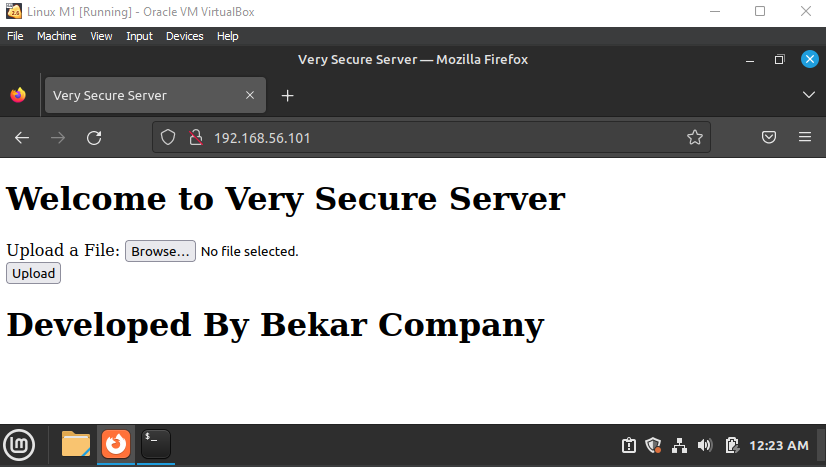
****

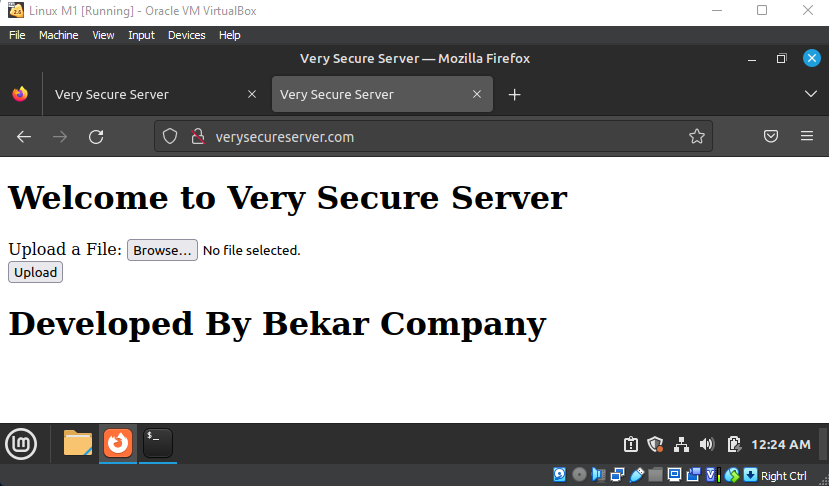
**CLIENT SERVER**

**Configure client server:**

* sudo nano /etc/netplan/1-network-manager-all.yaml
* sudo netplan try
* sudo resolvectl status
* nslookup host/client ip







**Firewall:**

* sudo ufw status verbose
* sudo ufw default allow outgoing

