****

Department of CSE

**Project 1 Report**

**Course Name:** Cyber Security, Law and Ethics

**Course Code:** CSE487

**Section No:** 03

**Group No:** 109

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

**Submitted To:** Rashedul Amin Tuhin

Senior lecturer,

Department of Computer Science and Engineering,

East West University.

**Submitted by:**

**Amin Talukder**

ID: 2019-3-60-014

**Al Amin**

ID: 2019-1-60-016

**Sayemuzzaman Siam**

ID: 2019-3-60-011

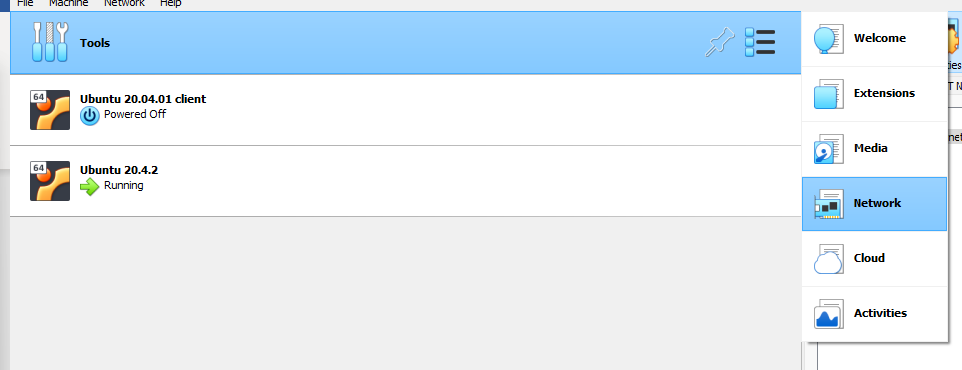
**1.0 Environment Setup:**

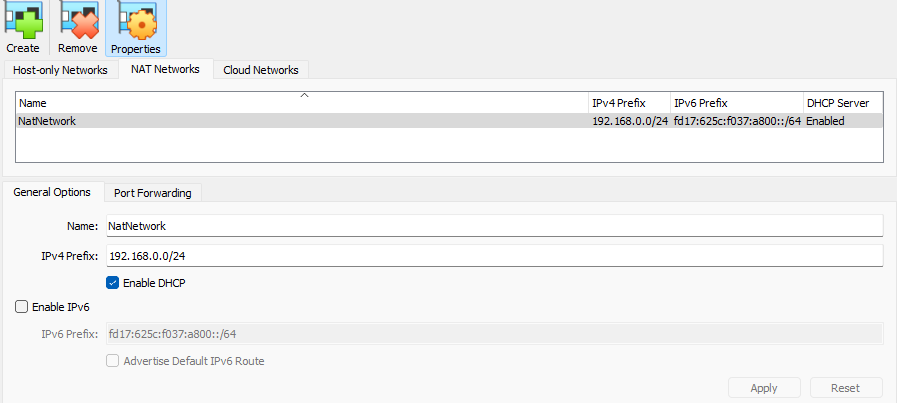
* 1. Download Oracle VM VirtualBox From this website
* <https://www.virtualbox.org/>
* Install it in your pc
  1. Download Ubuntu (Any Version) From this website
* <https://ubuntu.com/download>
* Install it in inside of the VirtualBox

For this project, we need two Ubuntu Operating System, First One we will configure that as a **Server** and the Second one, we will configure that as a **Client.**

**2.0** **Network Setup:**

First, we go to the network option of the VirtualBox and configure the ip address of **NAT Network**.



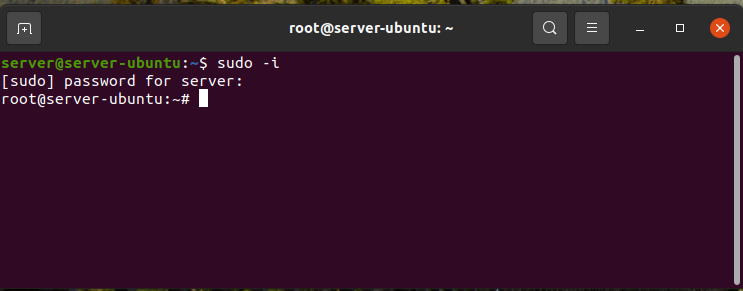


For this project, We will use 2 network adapter in both pc. In Adapter 1, set it as **NAT NETWORK** and In Adapter 2 set is as **NAT.** We will do the same on the both Server and Client PC.

**3.0 Certificate Generation:**

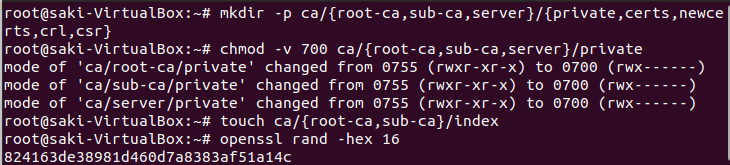
**Step 01:**

First of take root access in the terminal.



Now type the codes in the terminal and run them accordingly as picture:

**Step 02:**





At first, we created three directories named rootCA, subCA, and server . Then we have created sub directories for the three previous directories that we created name private,certs,newcerts,crl,csr . This can be done using the command below :

**mkdir -p ca/{root-ca,sub-ca,server}/{private,certs,newcerts,crl,csr}**

Now we need to change the mode of the files, so that nobody can access those files except the user. This can be done by this command:

**chmod -v 700 ca/{root-ca,sub-ca,server}/private**

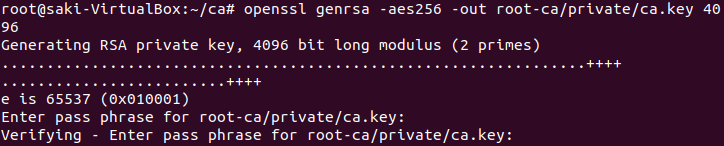
Then we need to create sub directories for RootCA and SubCA named “index”. This directory will be used to keep the index of the certificates . It is done by using this command below:

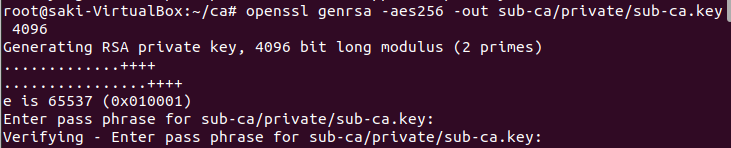
**touch ca/{root-ca,sub-ca}/index**

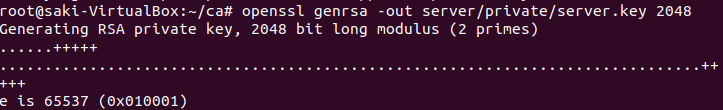
Then we generate for 16 bit random numbers for both rootCA and aubCA.

**Step 03:**

Now we will generate public key for RootC, SubCA and Server and this can be done by this command:







**Why choose 4096 key lengths for RootCA and Sub CA ?**

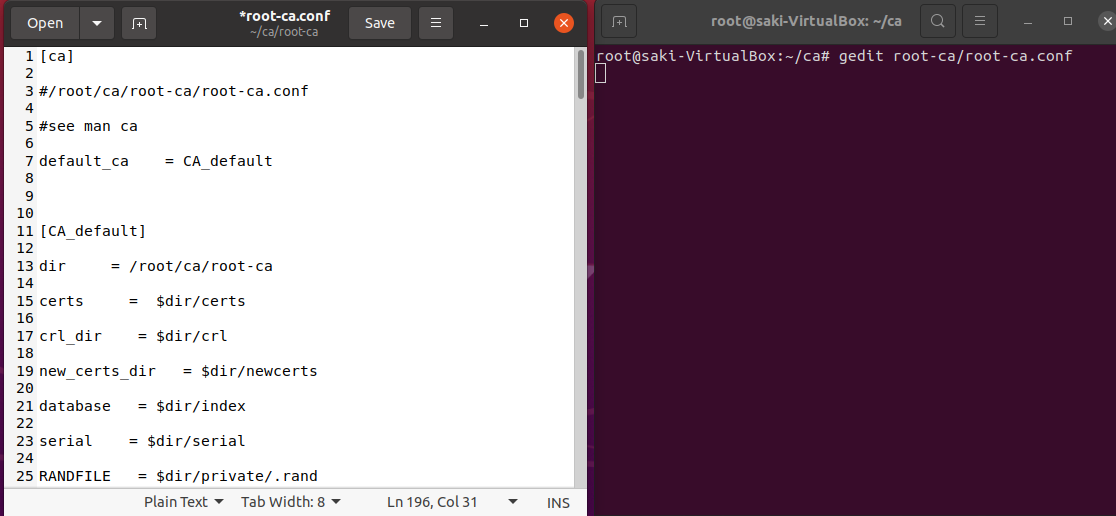
Private key of RootCA and SubCA has to be very strong. If the private key of RootCA or SubCA gets broken or leaked then all the certificated that were singed by these CA’s will be useless. That’s why we choose 2048 key length.

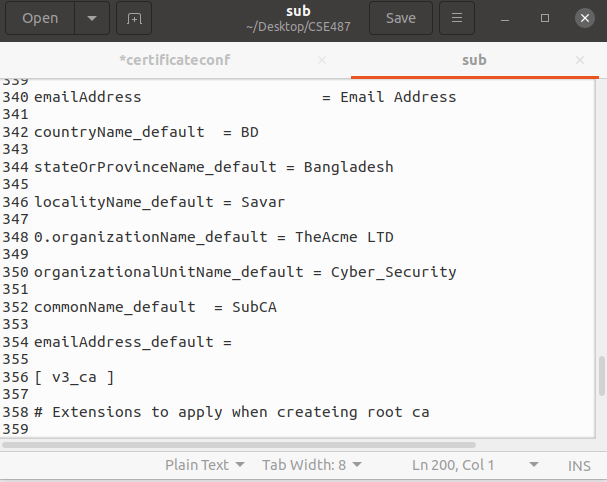
**Why choose 2048 key length for server private key?**

Privat key for server used very frequently. If the private key for server was too big like 4096 then the process of the server will slow.

**Step 04:**

Now we will create the configuration file for both RootC Aans SubCA and edit the files.

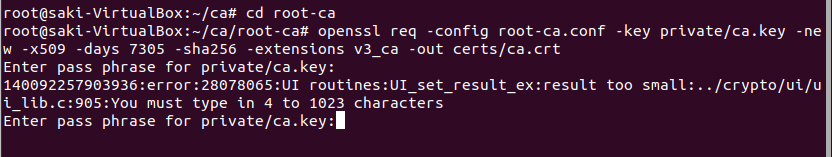


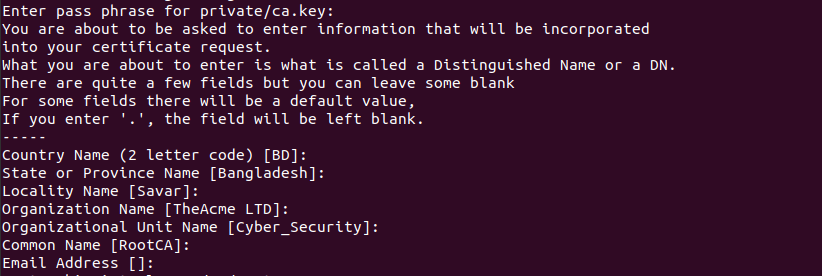


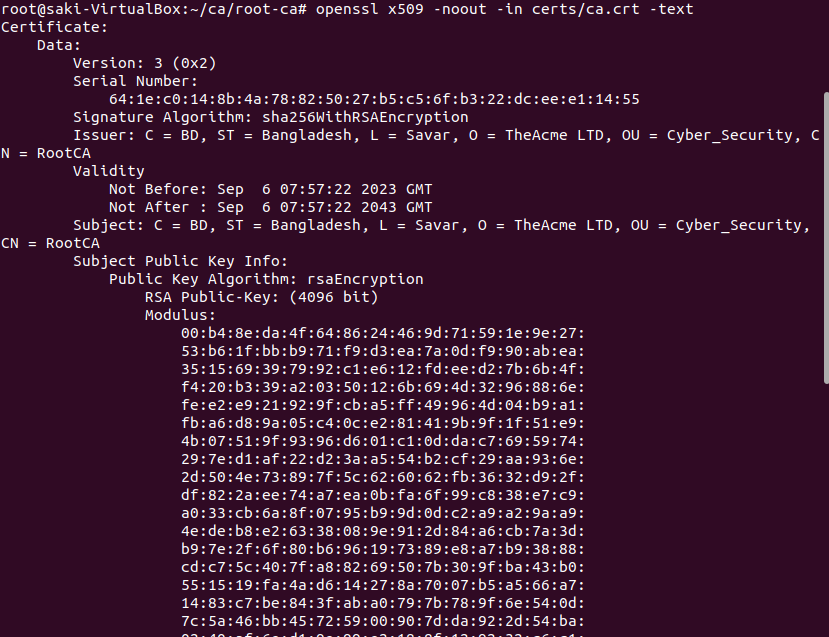
Full text given in **Appendix 1** & **Appendix 2**

**Step 05:**

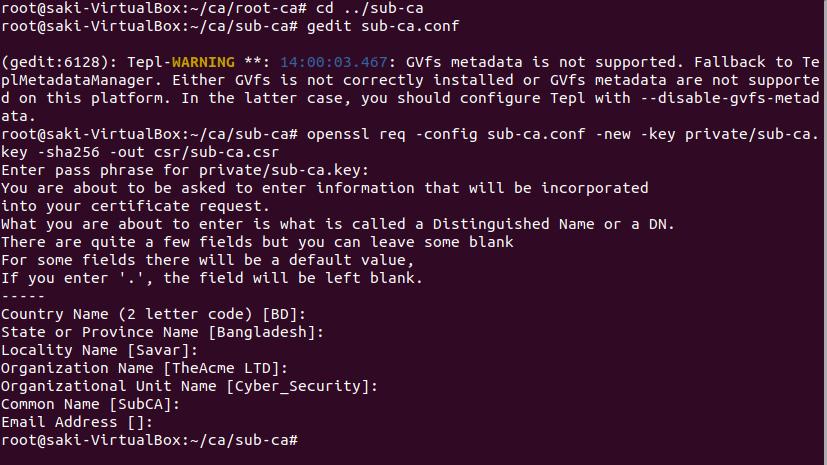
Now We will generate the RootCA Certificate. To do that, type **cd root-ca** and follow the rest given in the image below:



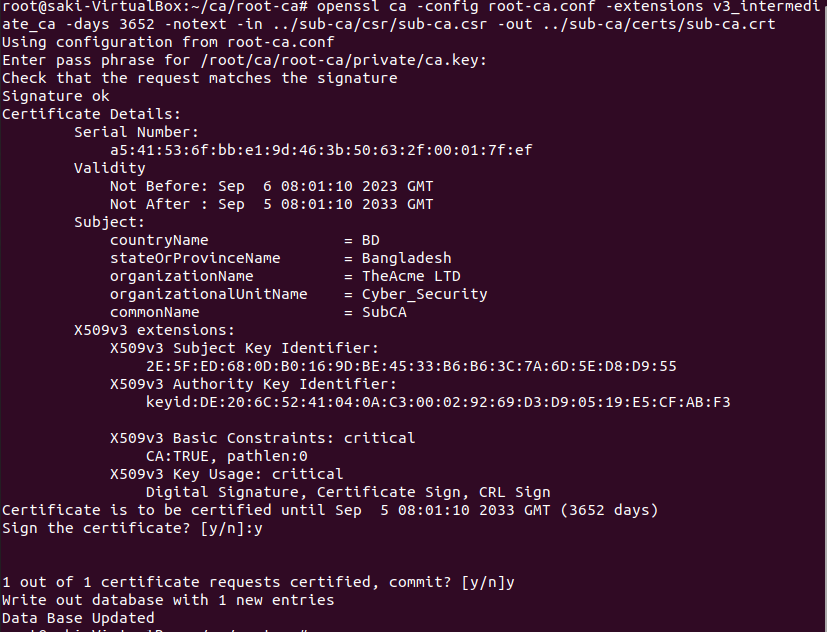




The same procedure we will follow to generate the SubCA certificate. Type **cd ../sub-ca** and follow the instruction given in the image below:



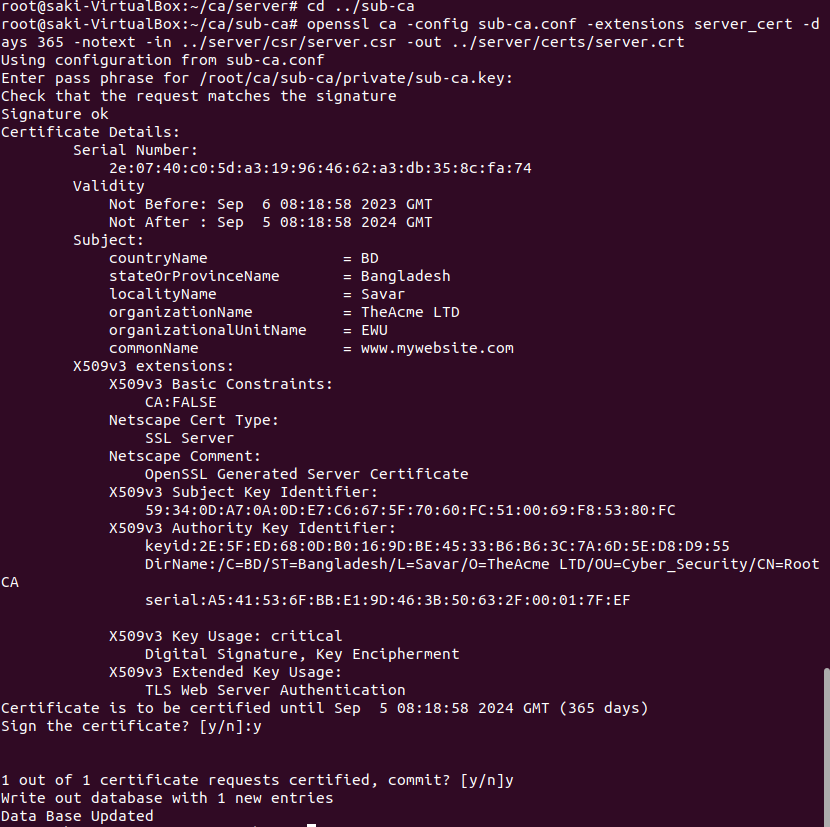
Now the RootCA sign the SubCA and then now anyone request for certification, SubCA will sign them.



**Step 06:**

Now for the server certification we will move to the server folder, generate certificate, which will be signed by the SubCA. The detailed procedure will given below:





**Step 07:**

Now we move to Server Certificate folder and merge the certificate by tyoing the following command:

**cd ../server/certs/**

**cat server.crt ../../sub-ca/certs/sub-ca.crt ../../root-ca/certs/ca.crt > mywebsite.crt**

**Step 08:**

At this stage we turn on SSL port which is 443.

**openssl s\_server -accept 443 -www -key private/server.key -cert certs/server.crt -CAfile ../sub-ca/certs/sub-ca.crt**

**Step 09:**

Now we update our certificates by typing the following commands in the terminal.

**cp ca/root-ca/certs/ca.crt /usr/local/share/ca-certificates/**

**update-ca-certificates -v**

**Step 10:**

Copying Certificates:

**cp /root/ca/root-ca/certs/ca.crt /home/[username]/[folder\_name]**

**cp /root/ca/sub-ca/certs/sub-ca.crt /home/[username] /[folder\_name]/**

**cp /root/ca/server/certs/verysecureserver.crt /[username] /server/[folder\_name]/**

**cp /root/ca/server/certs/server.crt /home/[username] /[folder\_name]/**

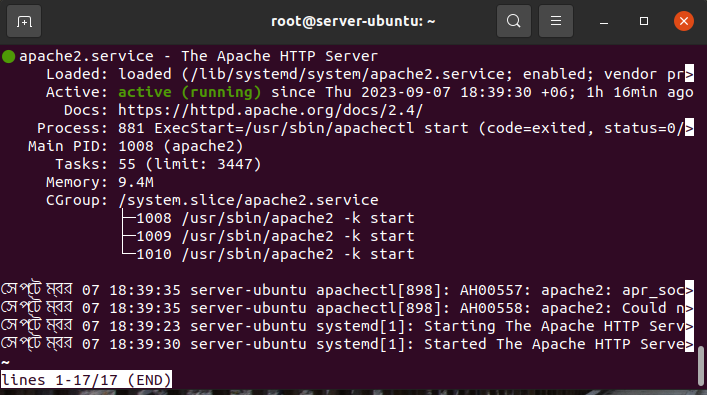
**cp /root/ca/server/private/server.key /home/[username] /[folder\_name]/**

**Step 11:**

Open a new terminal and type:

**sudo apt install apache2**

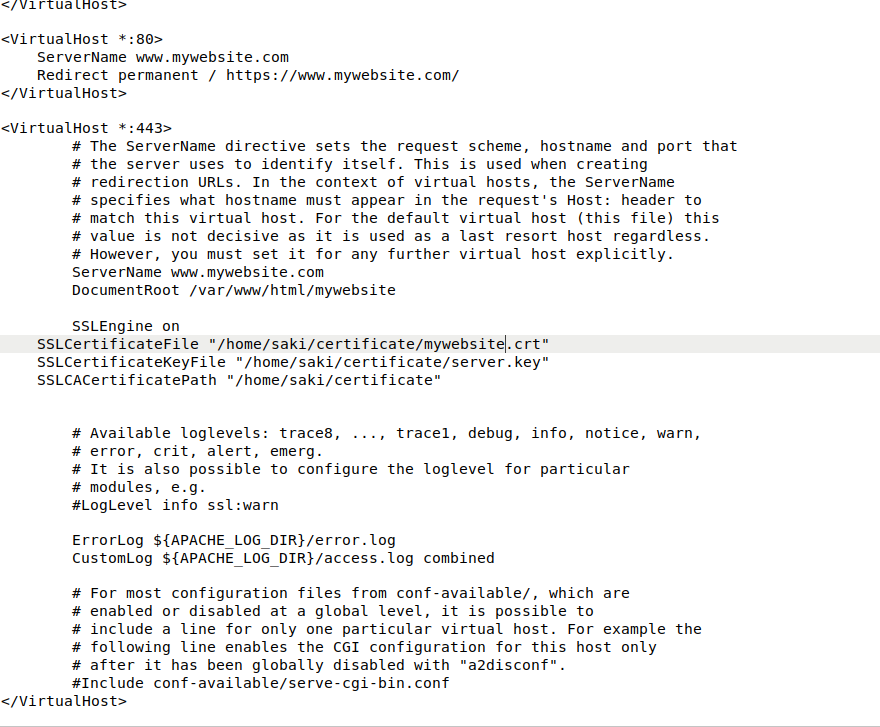
**systemctl status apache2**



Check the status of apache2, if apache2 is not showing active, then type the following command:

**sudo start apache2.** This will start your apache server.

Now go to this location: **/etc/apache2/sites-enabled** and paste the following code in 000-default.conf file.



**Step 12:**

Now go to this location: **var/www/html** and create a folder named **mywebsite** and make a html file for your website inside of this folder.

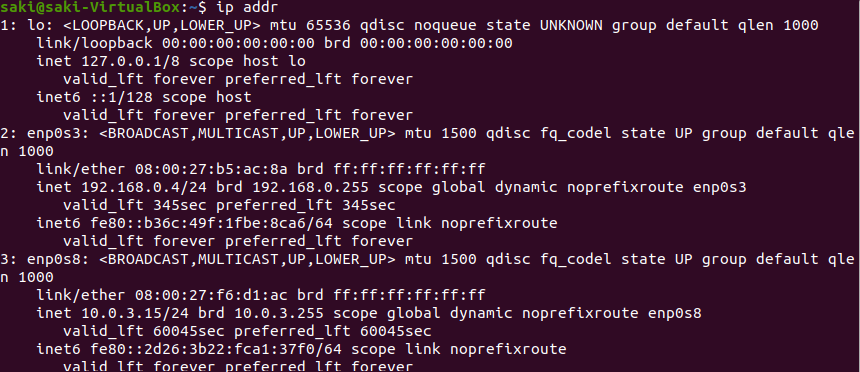
**4.0 DNS SETUP (Server)**

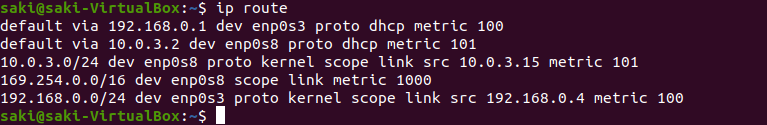
First install the following commands:

**sudo apt install net-tools**

**sudo apt install bind9**

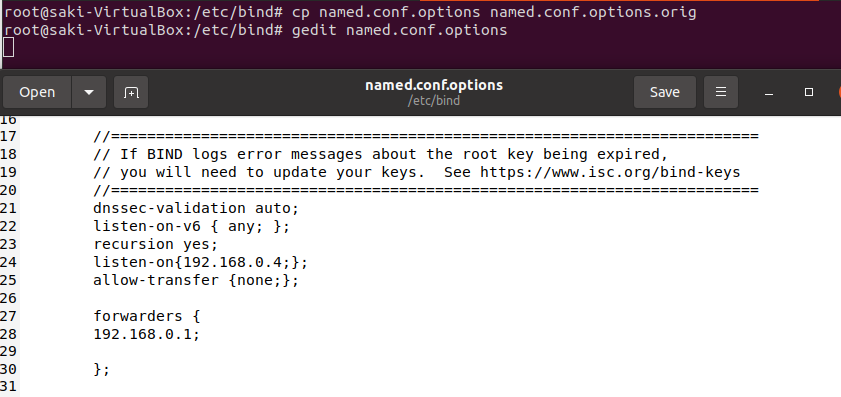
**sudo apt-get install bind9 bind9utils bind9-doc**

****

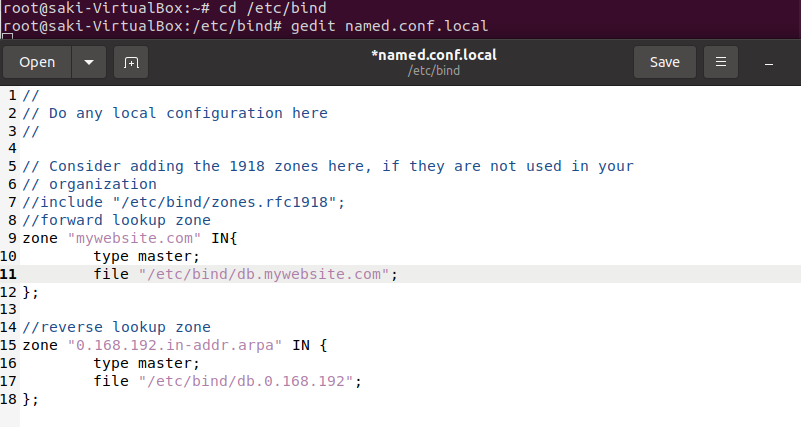


Here we can see, our ip address is 192.168.0.4 and our default route is 192.168.0.1, using this ip and route, we will configure our DNS server.

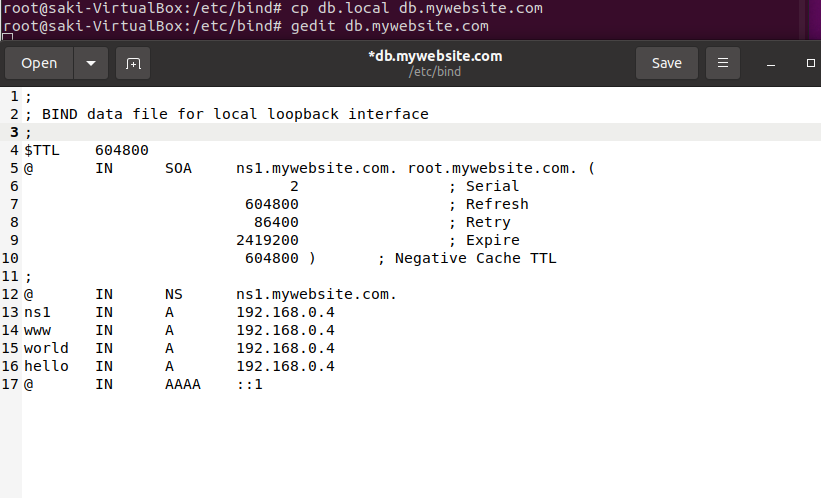
Next go to this location: **sudo /etc/bind** and edit the **named.conf.options** file.



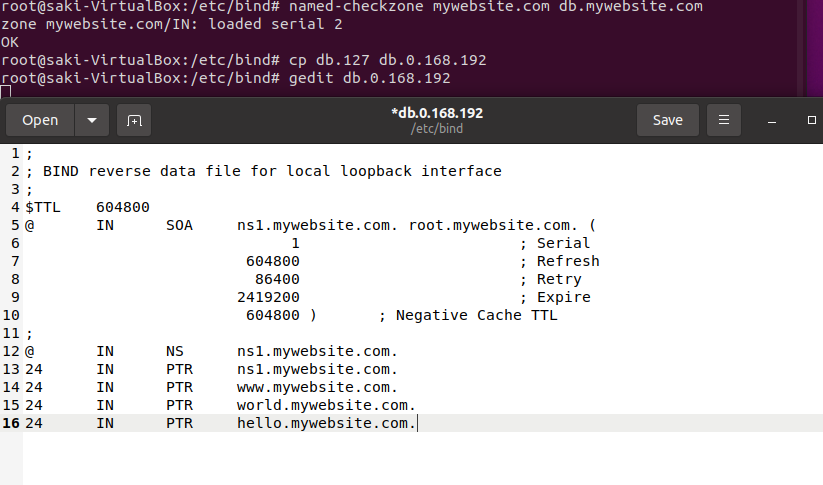
Then edit the **named.conf.local** file.



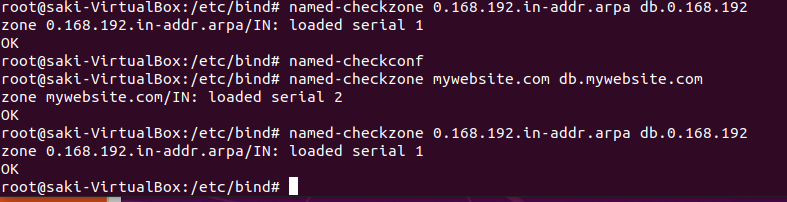
Edit db.mywebsite.com file-



Edit db.0.168.192 file-



To Check all the files working fine or not



Now restart the bind9 service by typing command: **service bind9 restart**

**Edit the resolve.conf file:**

**sudo systemctl status resolvconf.service**

**sudo apt update**

**sudo apt install resolvconf**

**sudo systemctl status resolvconf.service**

**(if resolveconf isn't running, enable then start it)**

**sudo systemctl enable resolvconf.service**

**sudo systemctl start resolvconf.service**

**(check resolveconf status)**

**sudo systemctl status resolvconf.service**

**(edit the head file)**

**sudo nano /etc/resolvconf/resolv.conf.d/head**

**(enter your nameservers below the comments)**

**nameserver 192.168.0.4**

**nameserver 192.168.0.1**

**search localdomain**

**(update resolve.conf file)**

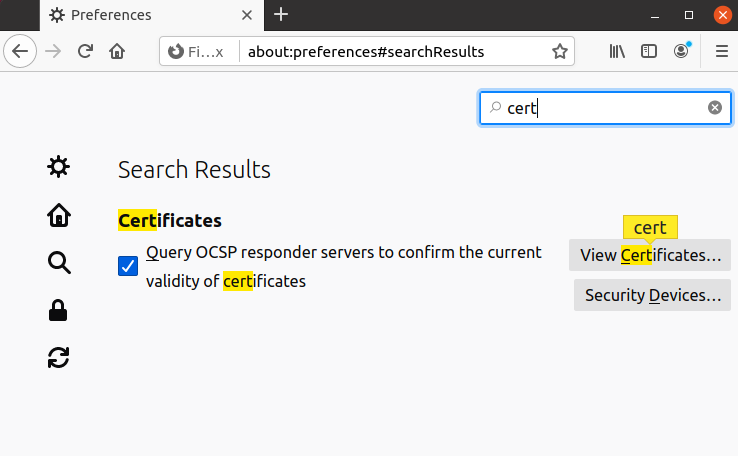
**sudo resolvconf --enable-updates**

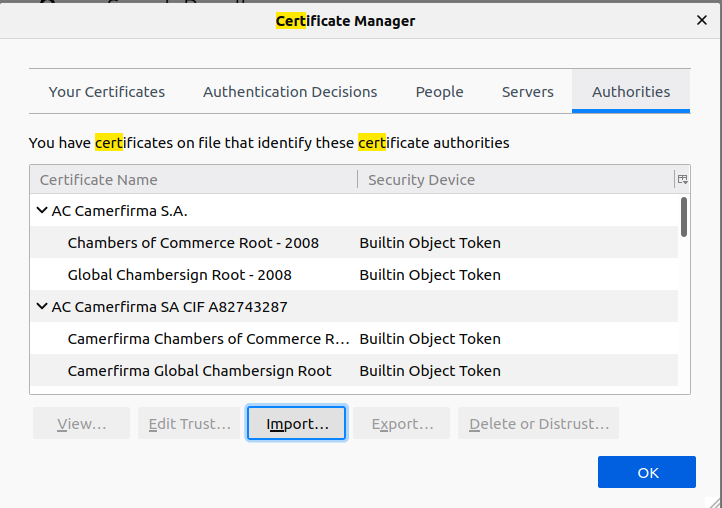
**sudo resolvconf -u**

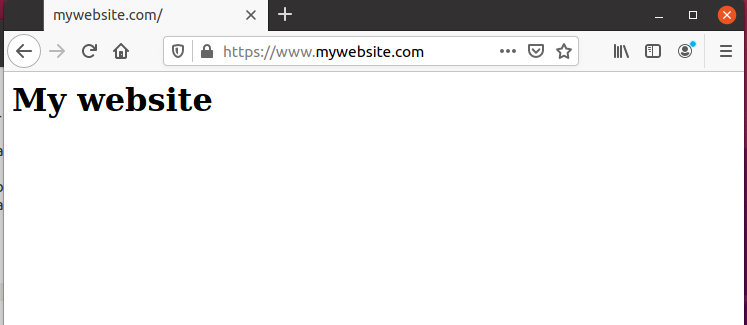
**(check if changes we successful)**

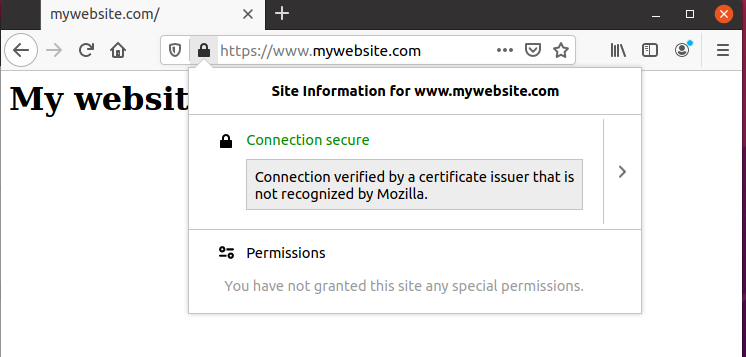
**sudo nano /etc/resolv.conf**

Now command nslookup [**www.mywebsite.com**](http://www.mywebsite.com) **and this will show you that the reply is coming from your ip. Now Paste root certificate in the browser and search for your website, this will show your website with padlock icon.**



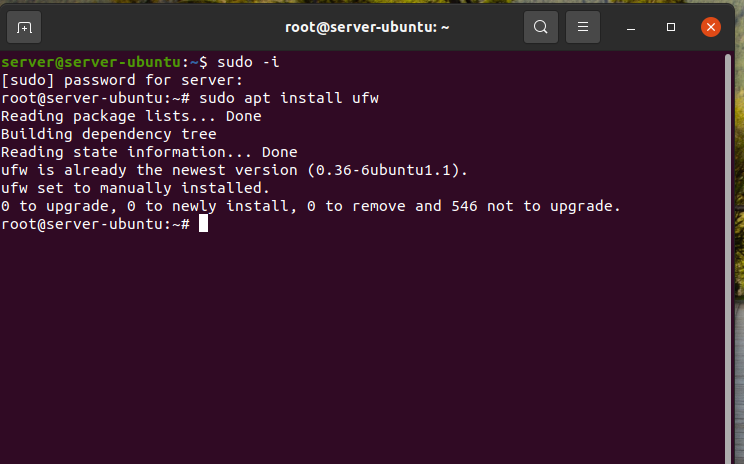






**5.0 Firewall Setup (Server Machine)**

To install firewall on servr pc, first take root access in terminal then type “**sudo apt install ufw**”. This will install firewall in your machine.



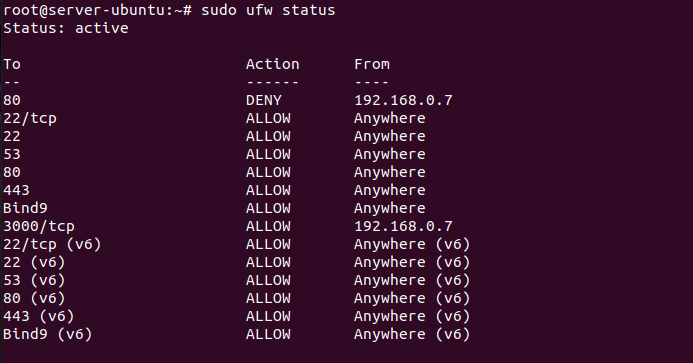
Then set some rules for firewall:

* ufw default allow outgoing
* ufw default deny incoming
* ufw allow ssh
* ufw enable
* sudo ufw allow 22
* sudo ufw allow 53
* sudo ufw allow 80 (for http)
* sudo ufw allow 443(for https)

You can check the rules that you set for your firewall:

Type: **sudo ufw status**. This will show you all the rules that you have set for your firewall.

If you want delete some rules just type in terminal: **sudo ufw delete 1** [Here I want to delete the 1st rule which is denying 192.168.0.7 ip to port 80].



**6.0 Wireshark and Snort installation (Server)**

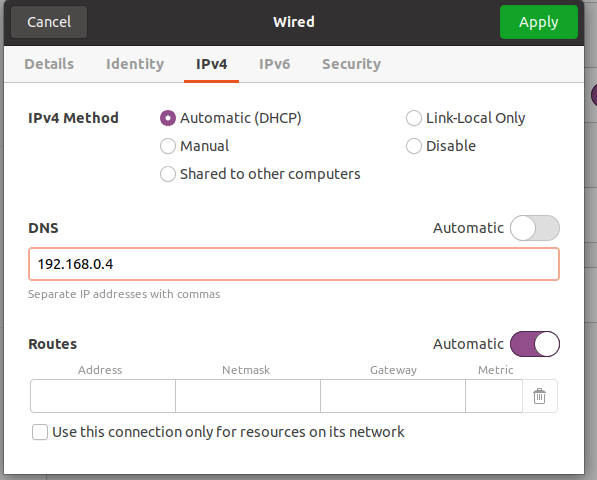
To install wireshark, first take root access in the terminal and type **sudo apt install wireshark**

and to install snort command: **sudo apt-get install snort.**

After installing the snort, set rules for the possible SYN Flood Attack. To do this, go to this location: **/etc/snort/rules**  and edit file named local.rules for identifying SYN Flood Attack.  
Again Now open a new terminal and take the root access and type the following to run the snort.  
**sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s3**[As we use enp0s3 network for our DNS Configuration and configure and set snort rules on enp0s3 network]

**7.0 Server PC Configuration:**

Our Server machine’s ip is 192.168.0.4 which we will as our DNS address in our client machine. To do this edit the network file of client pc and set server’s ip as Client pc DNS address.

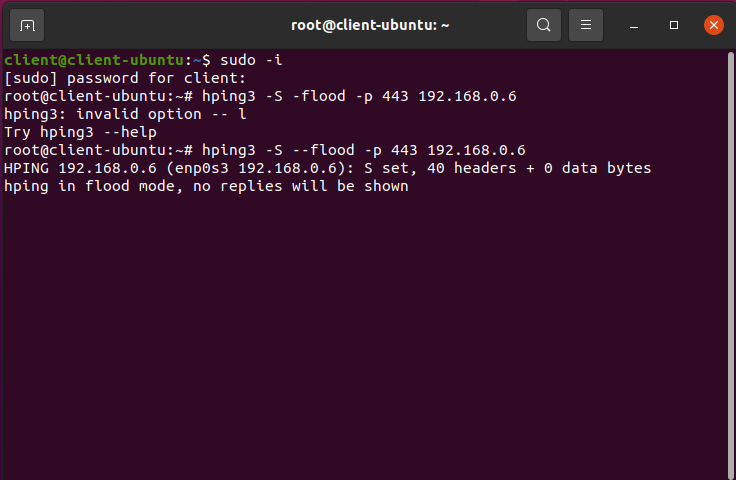


Now Open a terminal and type the following commands:  
**sudo apt install wireshark**

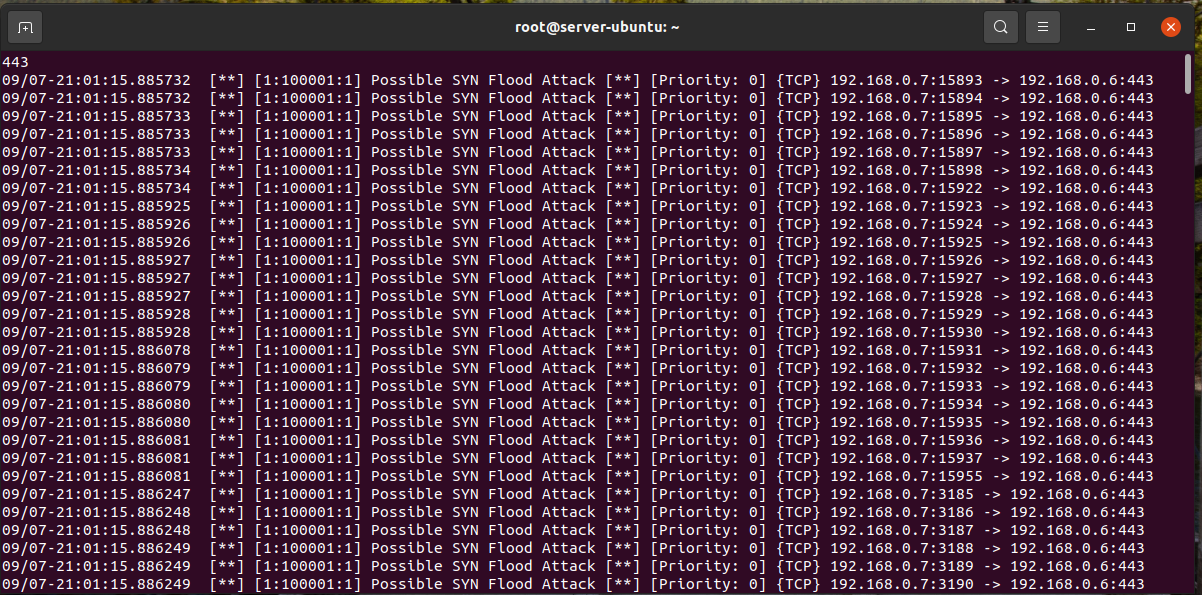
**sudo apt install hping3**

**sudo apt install ssh**

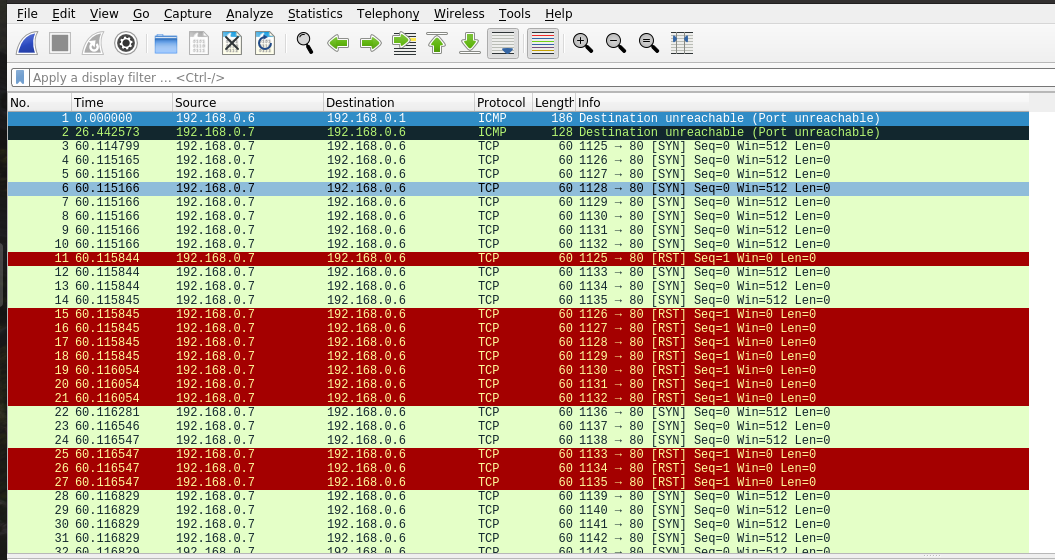
**Performing attack from Client PC:**



Attack from Client PC.



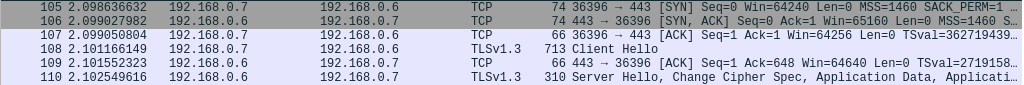
Attack Detection from Server PC. Now if we want block the attacker IP, we need to see the snort log file to see the attacker ip. To do this go to this location of your server pc: **/var/log/snort**  from here you can see the log file. Now open that log file with Wireshark and you can see the Attacker ip.

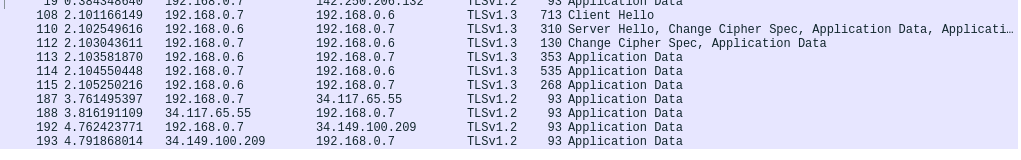


Here In source column, We can see the attacker ip, now using firewall block the attacker ip from server. To to do that type:  
**sudo ufw insert 1 deny from 192.168.0.7 to any port** **80** and save it.

**8.0 TCP & TLS Handshake:**

From the client pc open wireshark and starting capture packet from enp0s3 adapter. Now hit the website from Client pc bowser.





**9.0 OPENSSH SERVER:**

install on both pc.

**sudo apt install openssh-server**

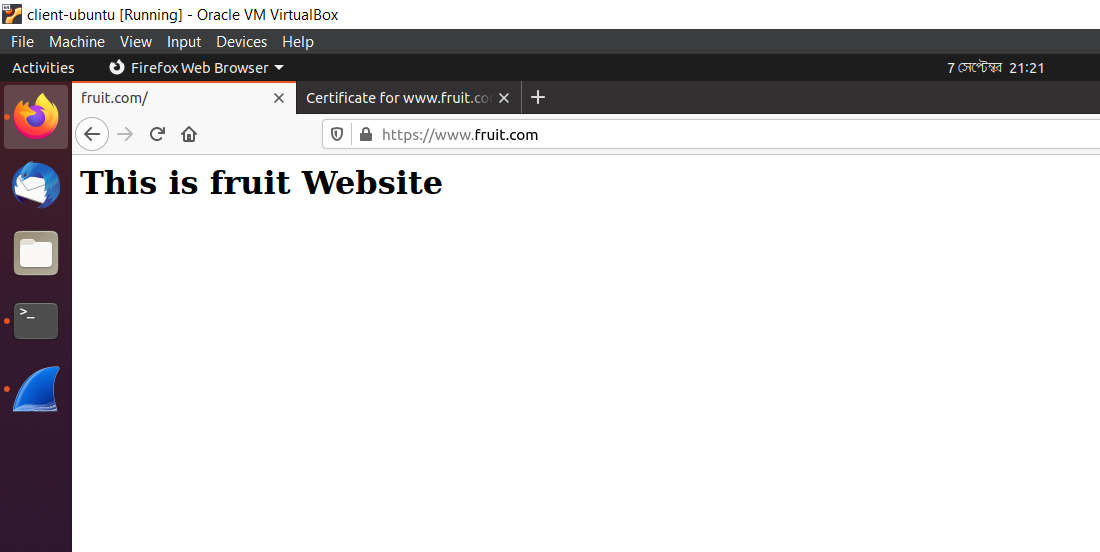
now from client pc type:

**ssh** [**server@192.168.0.7**](mailto:server@192.168.0.7)

If Firewall configured correctly in server, then using this command you can access the server pc from client pc.

**10.0 Client PC VIEW:**

Copy the Root Certificate file and paste the file in Client PC. Now Install the certificate in Client pc browser and after paste the certificate, the padlock icon should appear in the Client pc too.



View From Client Website