Al Imam Mohammad Ibn Saud Islamic University
College of Computer and Information Sciences

Network Security

PKI using SSL

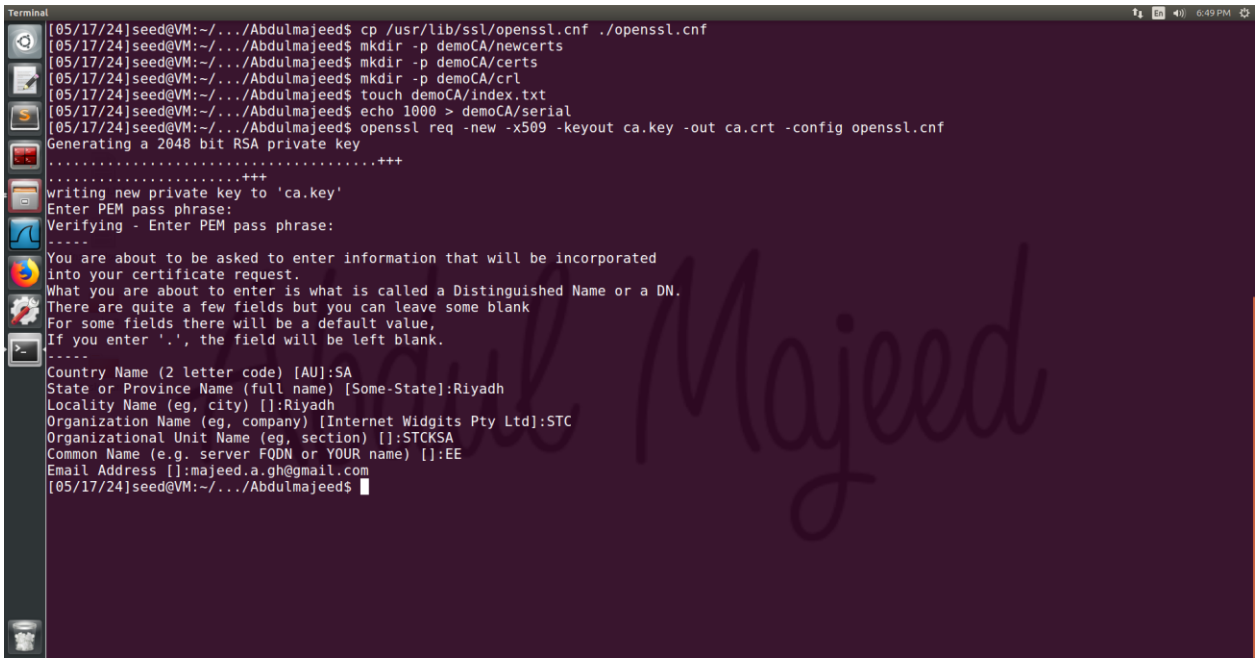
Content

Requirement :

1. Becoming a certificate authority (CA).
2. Creating a certificate.
3. Deploying the certificate in a web server.
4. Deploying certificate in an Apache-based HTTPS website.
5. Launching a Man in the Middle Attack.
6. Launching a Man in the Middle Attack using a compromised CA.

Task 1: Becoming a Certificate Authority (CA):

- First, we Set Up the Configuration File.
- Create the Necessary Directories to storing certificates and other files.
- Use OpenSSL to generate a private key and self-signed Root Certificate , during this process you will have to enter information (The Picture below) , passphrase is important (usually in this lab we make it reverse of seed "dees" but you can choose any) and will be required when we use this Certificate Authority (CA) to sign certificates. After running the command, we will have two files
    - "ca.key " : The private key of the CA
    - "cs.crt" : The self-signed certificate of the CA

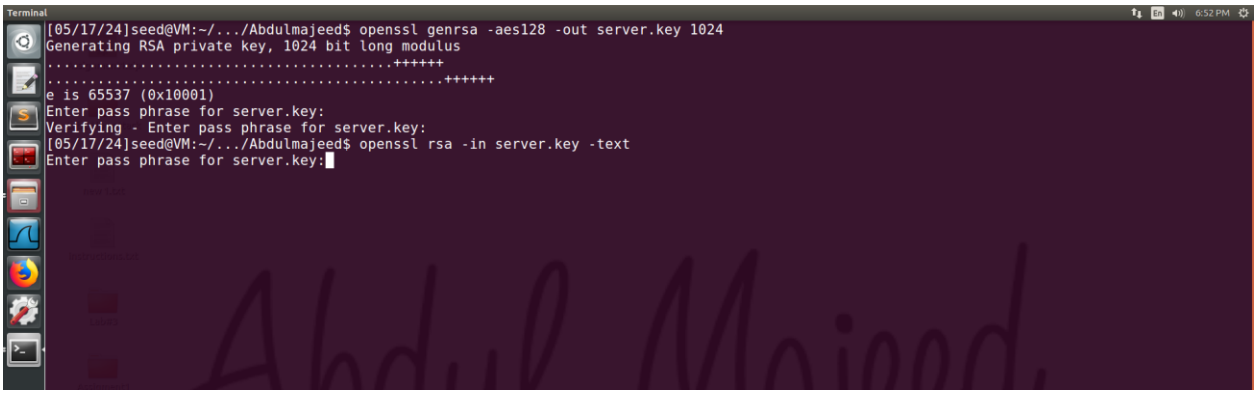


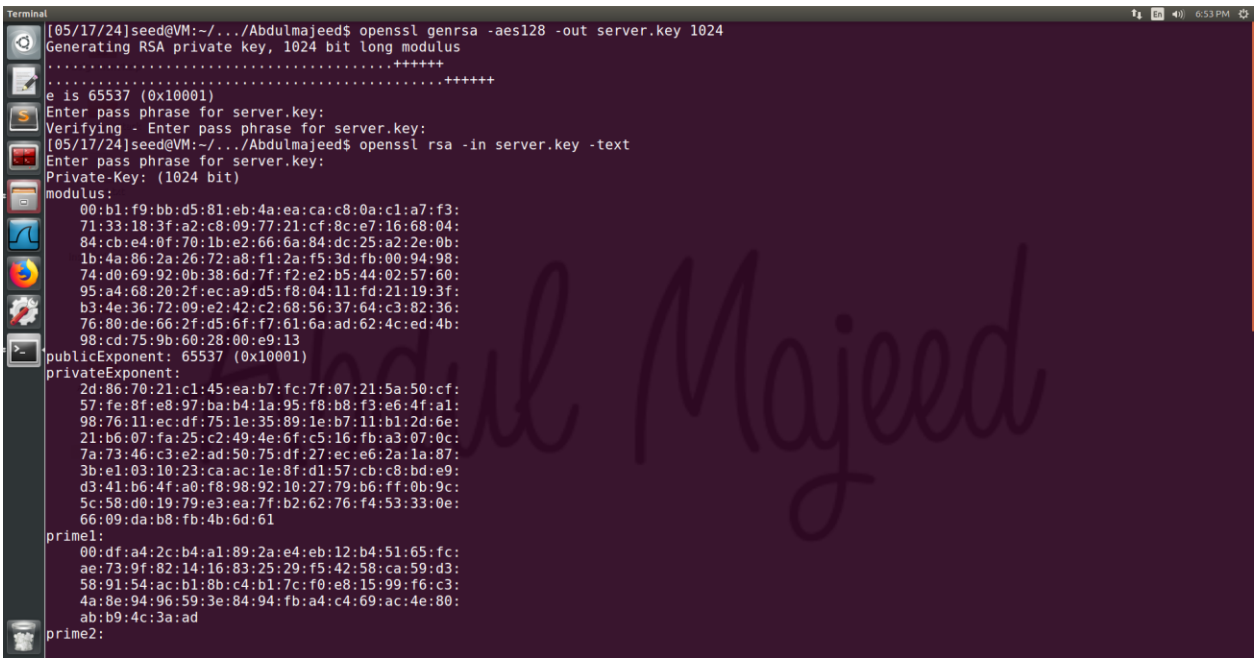
Task 2: Creating a Certificate for SEEDPKILab2020.com

Step 1: Generate public/private key pair.

this command will generate RSA key pair and store it in server.key file

Enter the pass phrase we choose it before





Step 2: Generate a Certificate Signing Request (CSR)

Once you has the key file, it should generates a Certificate Signing Request (CSR), The CSR will be sent to the CA, who will generate a certificate for the key

use SEEDPKILab2020.com as the common name of the certificate request.

Step 3: Generating Certificates.

As the CA we will sign the CSR to generate X509 certificate

Task 3: Deploying Certificate in an HTTPS Web Server

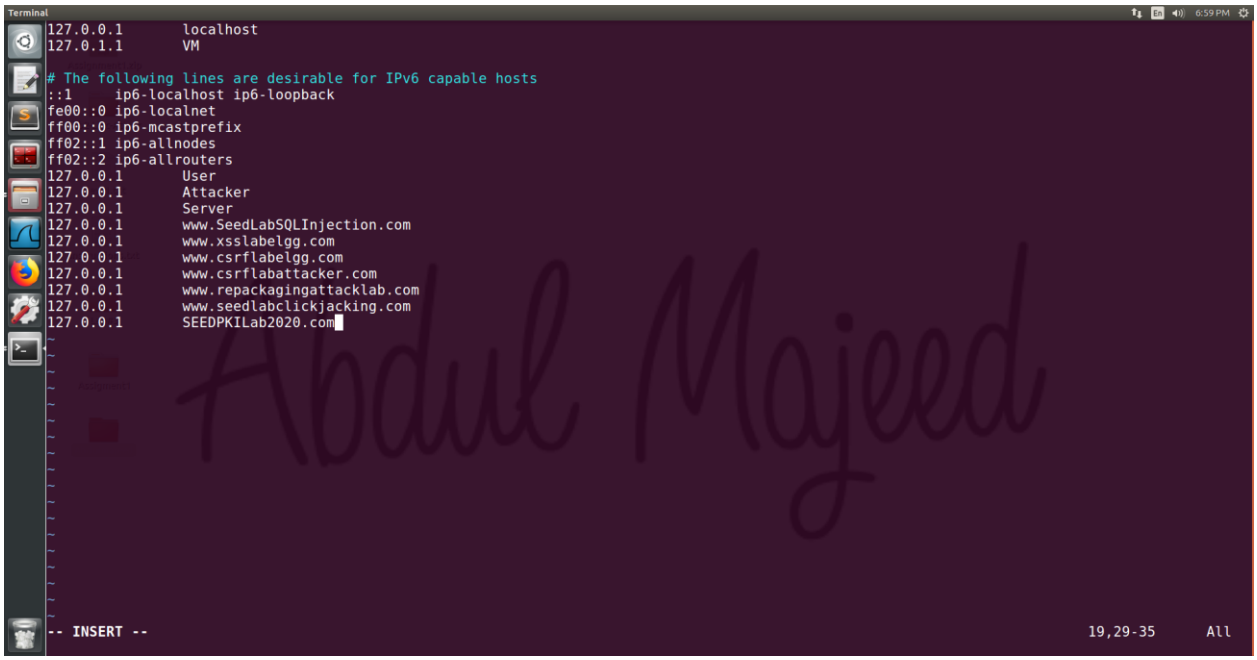
Step 1: Configuring DNS

to map the hostname "SEEDPKILab2020.com" to localhost we will use this command

sudo nano /etc/hosts

then Add the following line , Save the file and exit

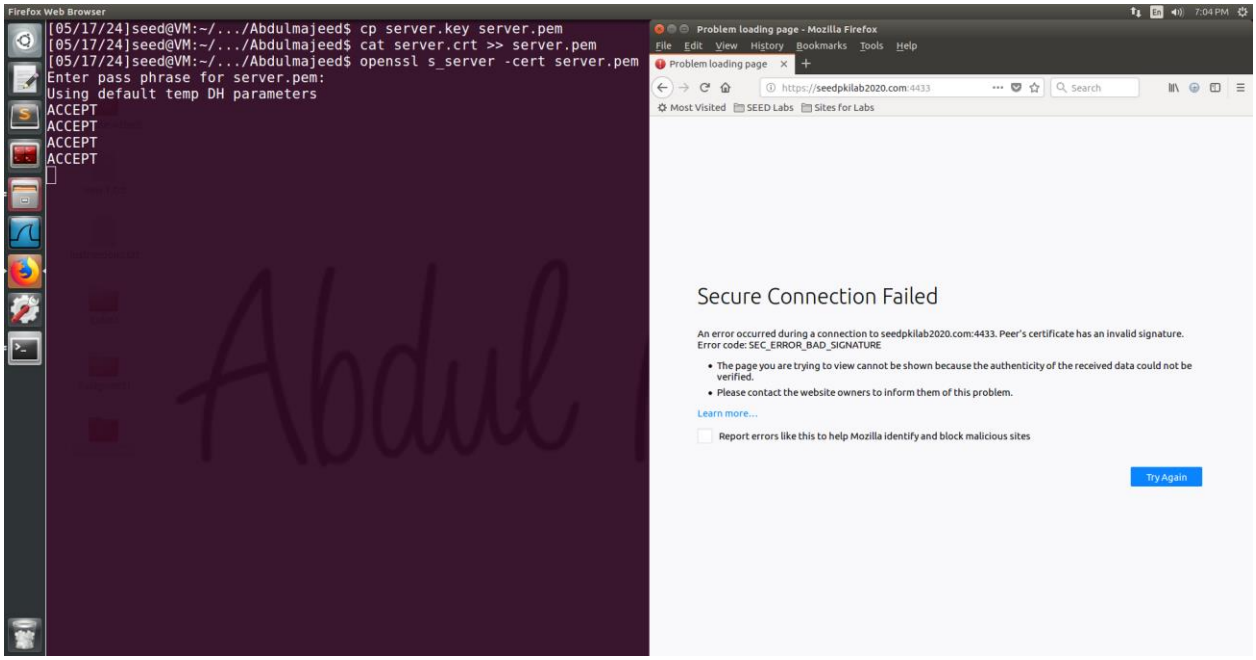
127.0.0.1 SEEDPKILab2020.com



Step 2: Configuring the web server

Combine the secret key and certificate into one file

Then Launch the web server using server.pem



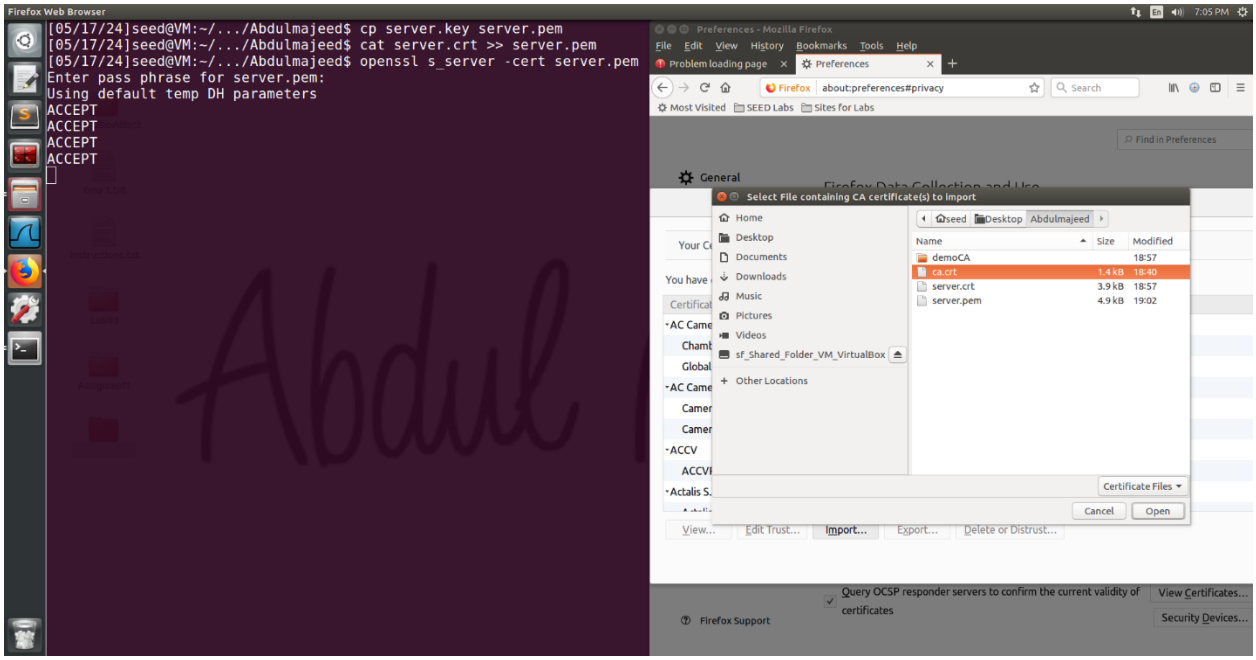
Now we can access the server using this URL "https://seedpkilab2018.com:4433/ "

usually get the error message from the browser , to solve this problem we going to step 3

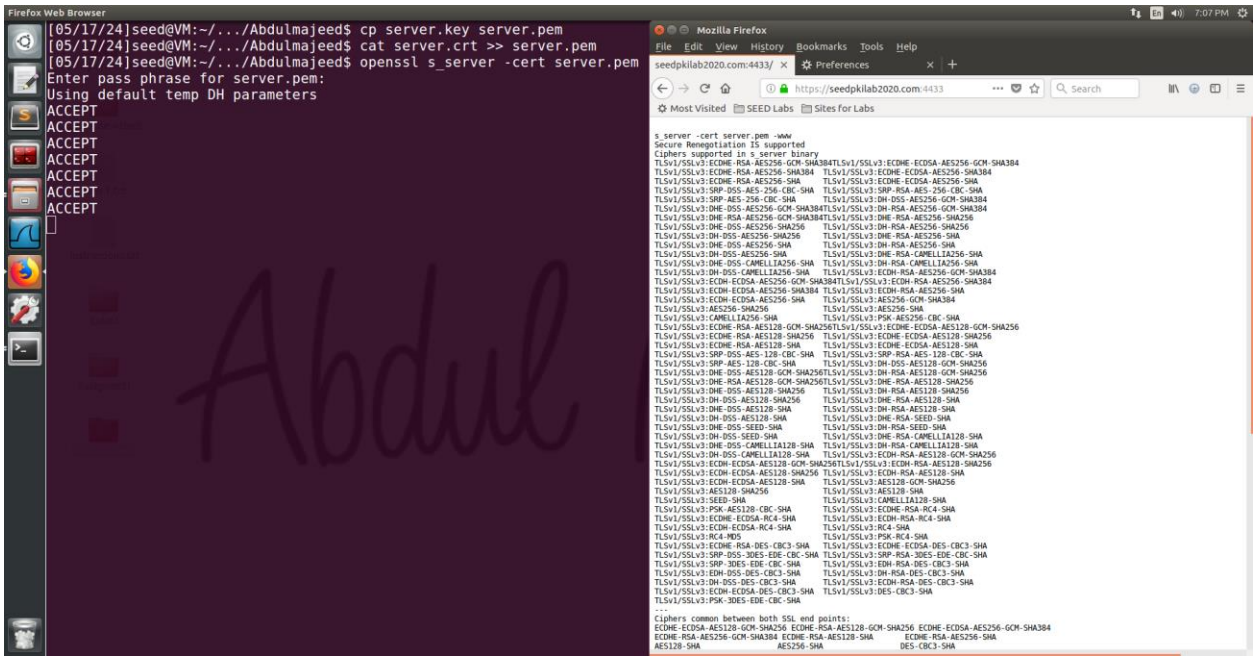
Step 3: Getting the browser to accept our CA certificate

we need to add the CA to firefox manually ,

Edit -> Preferences -> Privacy & Security -> View Certificates

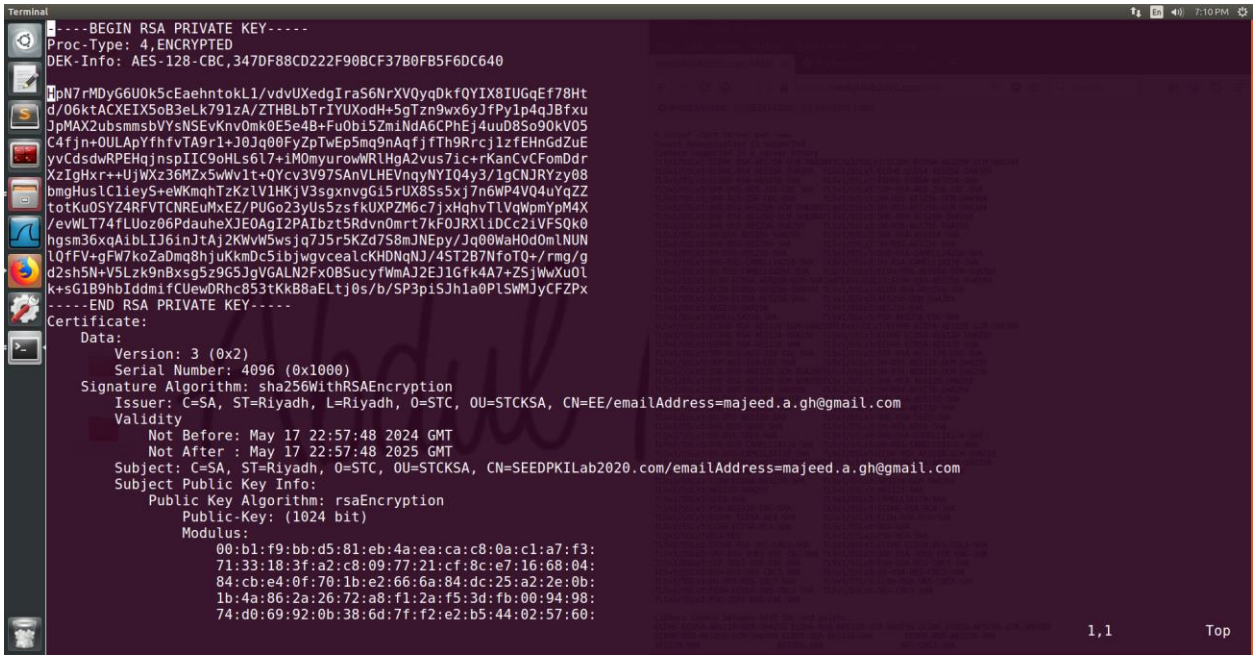


-

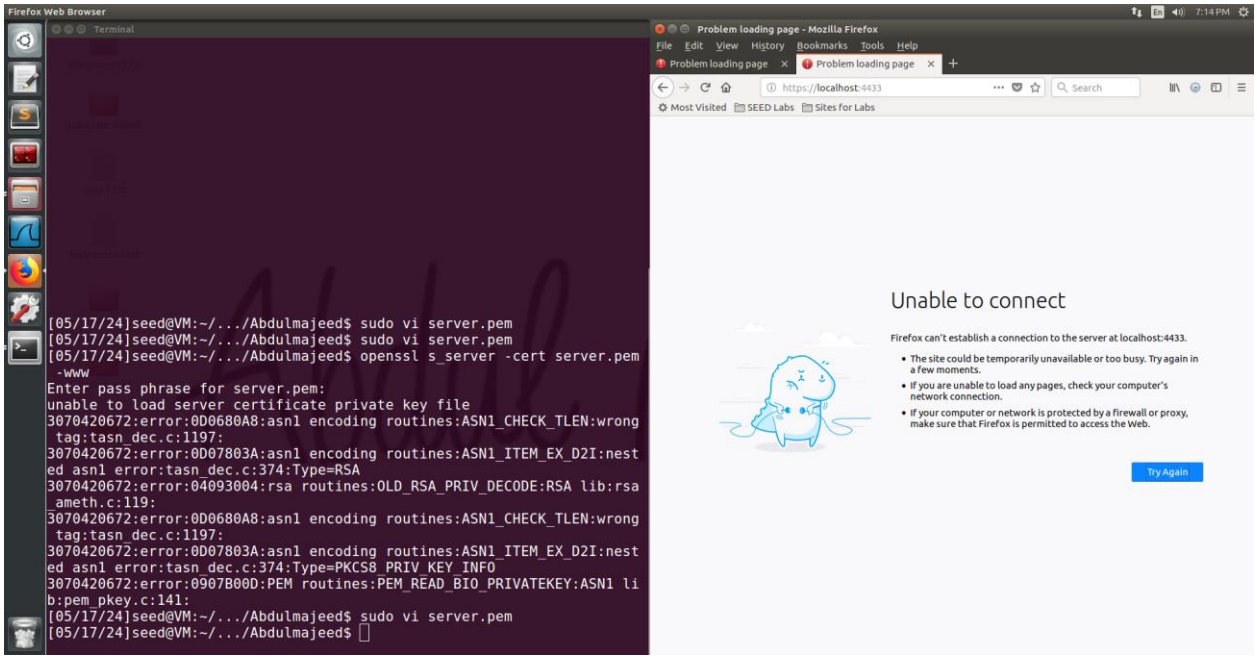


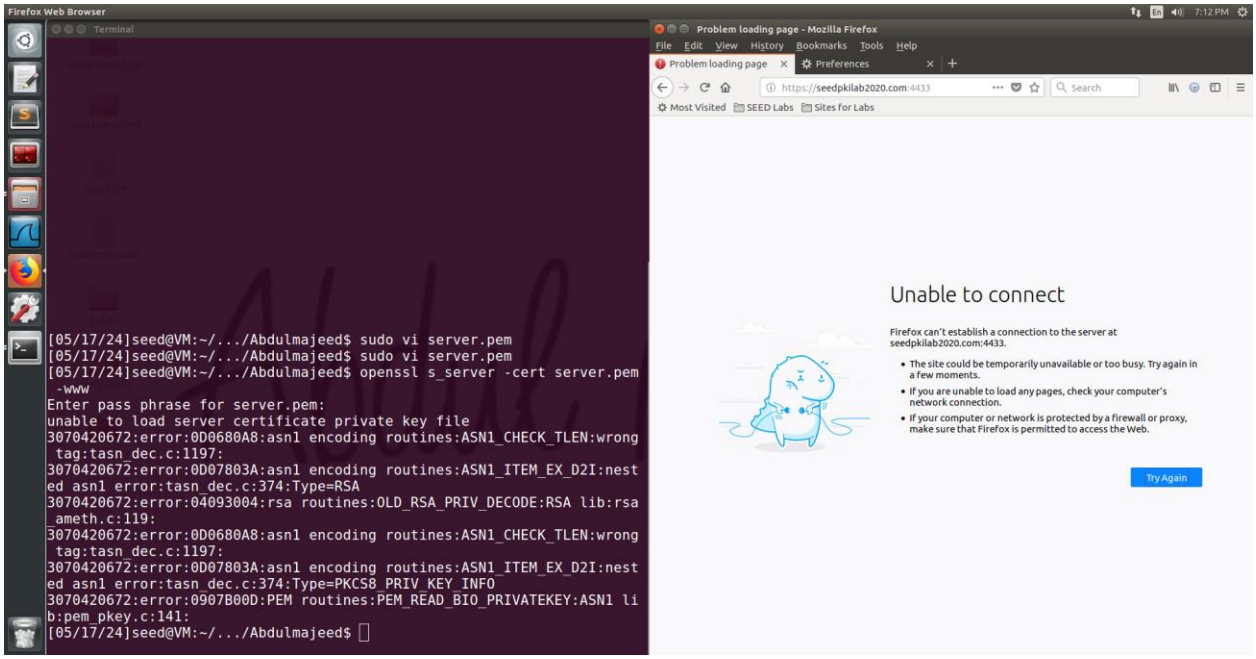
Step 4. Testing our HTTPS website.

Change the first byte of server.pem



Now reopen " https://localhost:4433/ " and " https://seedpkilab2020.com/ :





The reason is modifying a single byte in the server.pem file invalidates the certificate because is change the hash and cryptographic signature and this will prevents browser from verifying the certificate's integrity

Task 4: Deploying Certificate in an Apache-Based HTTPS Website

Create the apache2/ssl directory then move certificate files to it

Edit the default-ssl.cong file to add a VirtualHost entry SEEDPKILab2020.com.

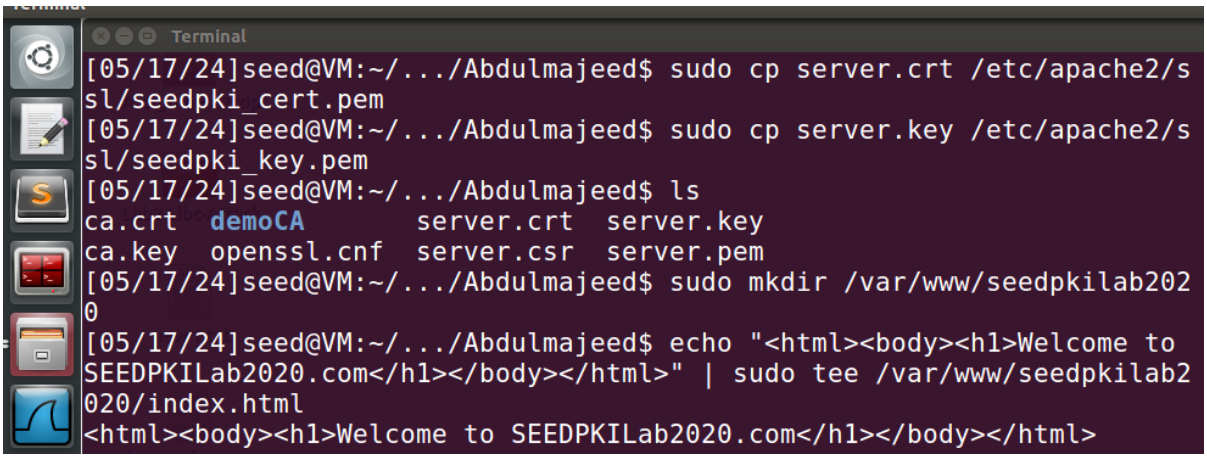
```
[05/17/24]seed@VM:.../apache2$ ls
apache2.conf    envvars         mods-enabled     sites-enabled
conf-available  magic           ports.conf       ssl
conf-enabled    mods-available  sites-available
[05/17/24]seed@VM:.../apache2$ cd ssl
[05/17/24]seed@VM:.../ssl$ ls
seedpki_cert.pem  seedpki_key.pem
[05/17/24]seed@VM:.../ssl$ sudo nano /etc/apache2/sites-available/defa
ult-ssl.conf
[05/17/24]seed@VM:.../ssl$ sudo nano /etc/apache2/sites-available/000-
default.conf
[05/17/24]seed@VM:.../ssl$ sudo apachectl configtest
AH00112: Warning: DocumentRoot [/var/www/seedlabclickjacking] does not
 exist
AH00558: apache2: Could not reliably determine the server's fully qual
ified domain name, using 127.0.1.1. Set the 'ServerName' directive glo
bally to suppress this message
Syntax OK
[05/17/24]seed@VM:.../ssl$ sudo service apache2 restart
Enter passphrase for SSL/TLS keys for SEEDPKILab2020.com:443 (RSA): **
**
[05/17/24]seed@VM:.../ssl$
```

FEdit the default-ssl.conf

```
Terminal
<IfModule mod_ssl.c>
<VirtualHost *:443>
    ServerName SEEDPKILab2020.com
    DocumentRoot /var/www/seedpki
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /etc/apache2/ssl/cert.pem
    SSLCertificateKeyFile /etc/apache2/ssl/key.pem
</VirtualHost>


        <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost

                DocumentRoot /var/www/html

                # Available loglevels: trace8, ..., trace1, debug, inf
o, notice, warn,
                # error, crit, alert, emerg.
                # It is also possible to configure the loglevel for pa
rticular
                # modules, e.g.
                #LogLevel info ssl:warn

                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined

                # For most configuration files from conf-available/, w
hich are
                # enabled or disabled at a global level, it is possibl
e to
                # include a line for only one particular virtual host.
 For example the
                # following line enables the CGI configuration for thi
s host only
```

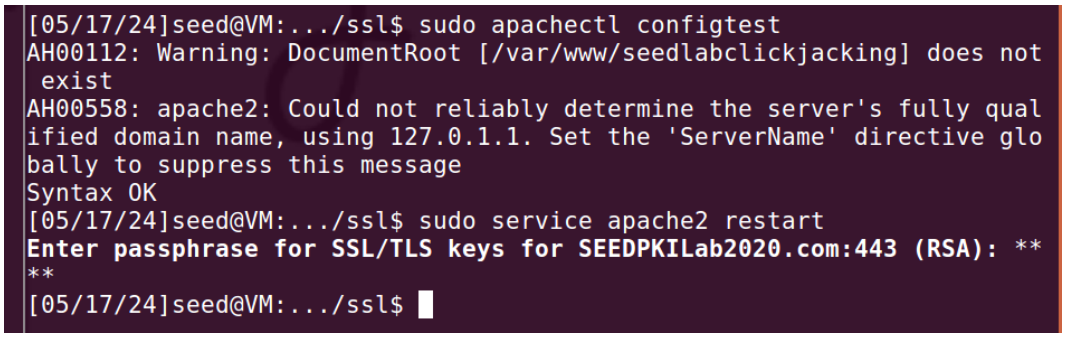
Add the VirtualHost

create simple HTML file for testing

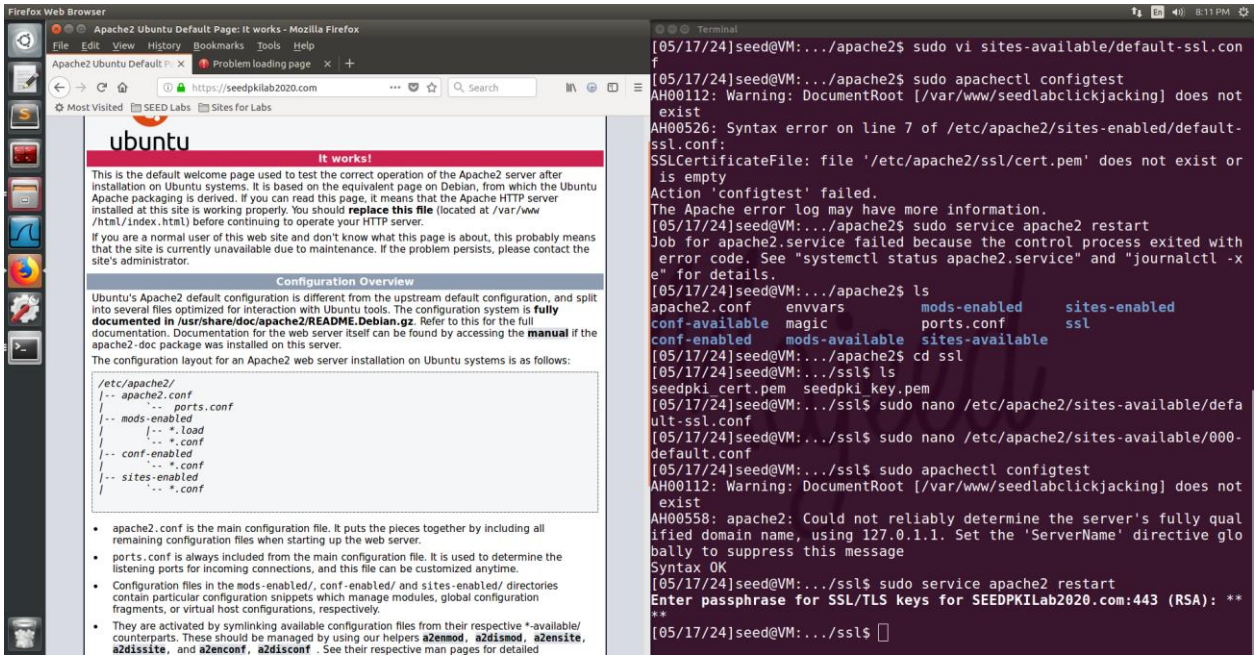


Enable SSL and the Site Configuration

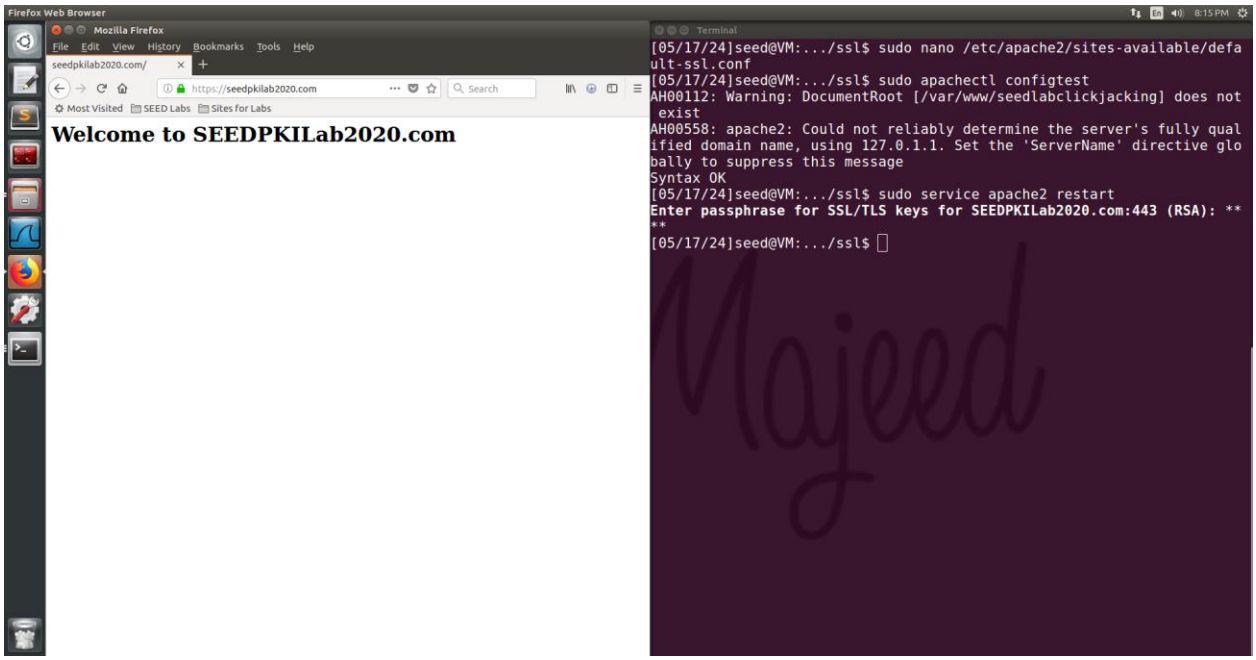
```
// Test the Apache configuration file for errors
$ sudo apachectl configtest

// Enable the SSL module
$ sudo a2enmod ssl

// Enable the site we have just edited
$ sudo a2ensite default-ssl

// Restart Apache
$ sudo service apache2 restart
```



Navigate to https://SEEDPKILab2020.com and its work



in previous we cerate simple HTML file so if we change the Document Root in virtual Host to our file

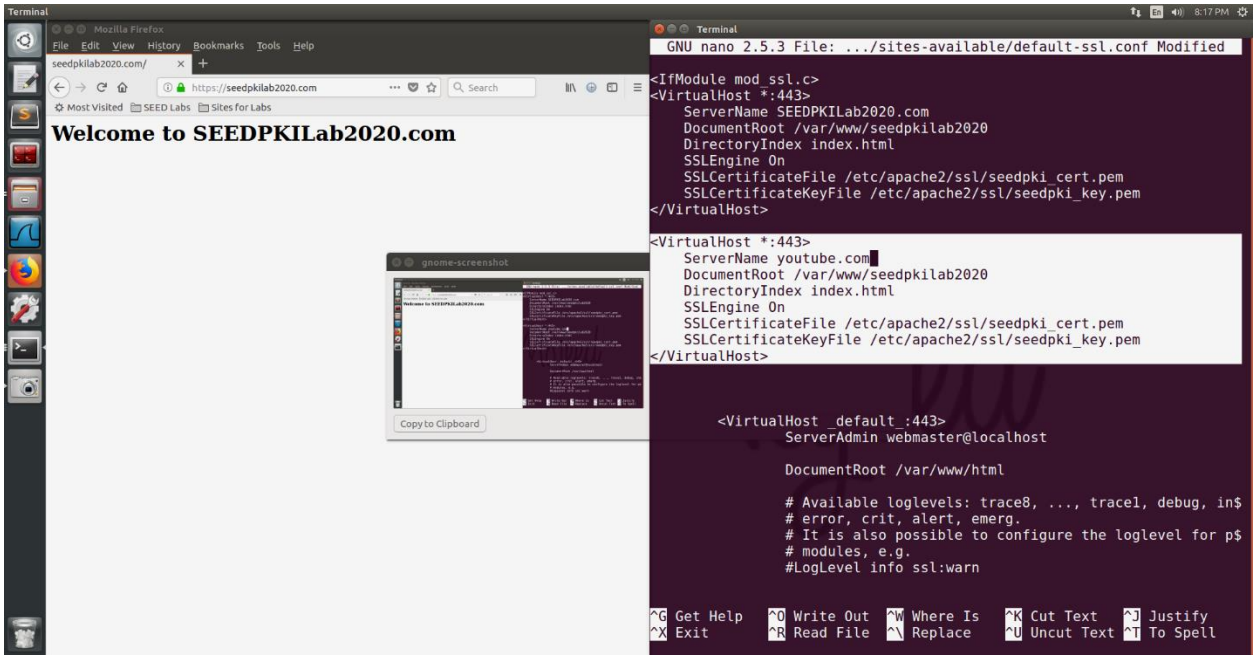


Task 5: Launching a Man-In-The-Middle Attack

Step 1: Setting up the malicious website.

setting up the malicious website , by do same instructions from task 4 to set up a Virtual Host

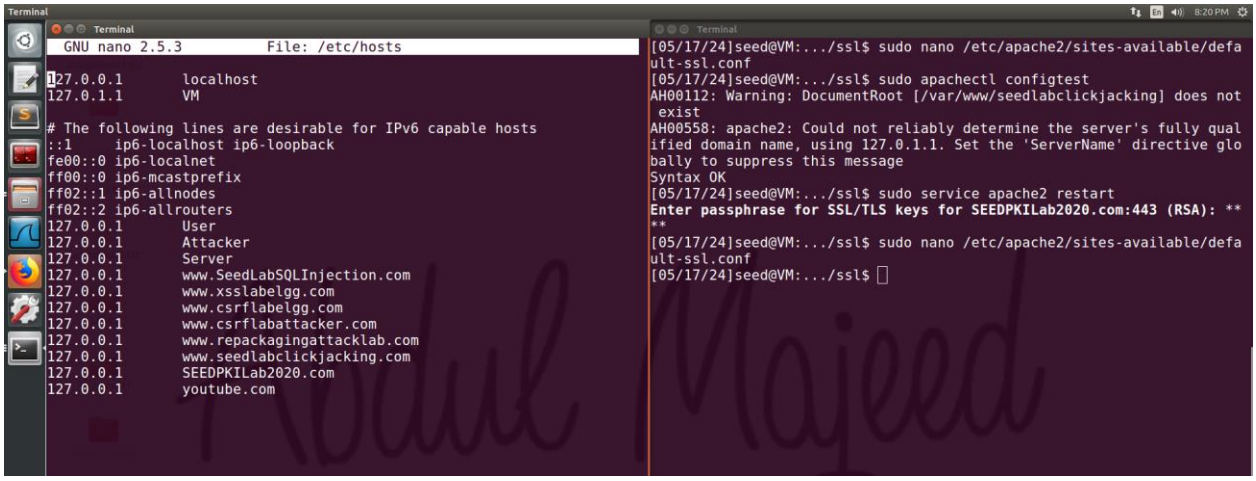
Entery , but in ServerName we will choose anywebsite for example in my case I use youtube.com



Step 2: Becoming the man in the middle

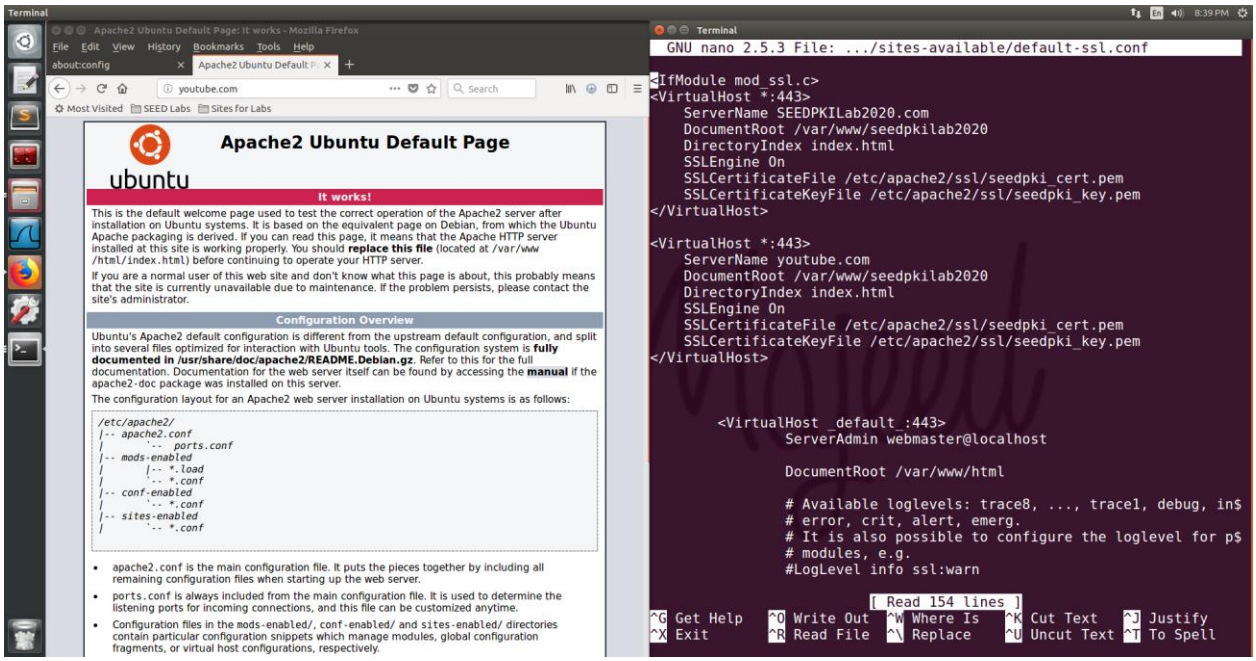
modyfiy the victm /etc/hosts file to redirect request for the target website to our malicious

IP server use command 'sudo nano /etc/hosts' and Add the ip and malicious website we chose



Step 3: Browse the target website

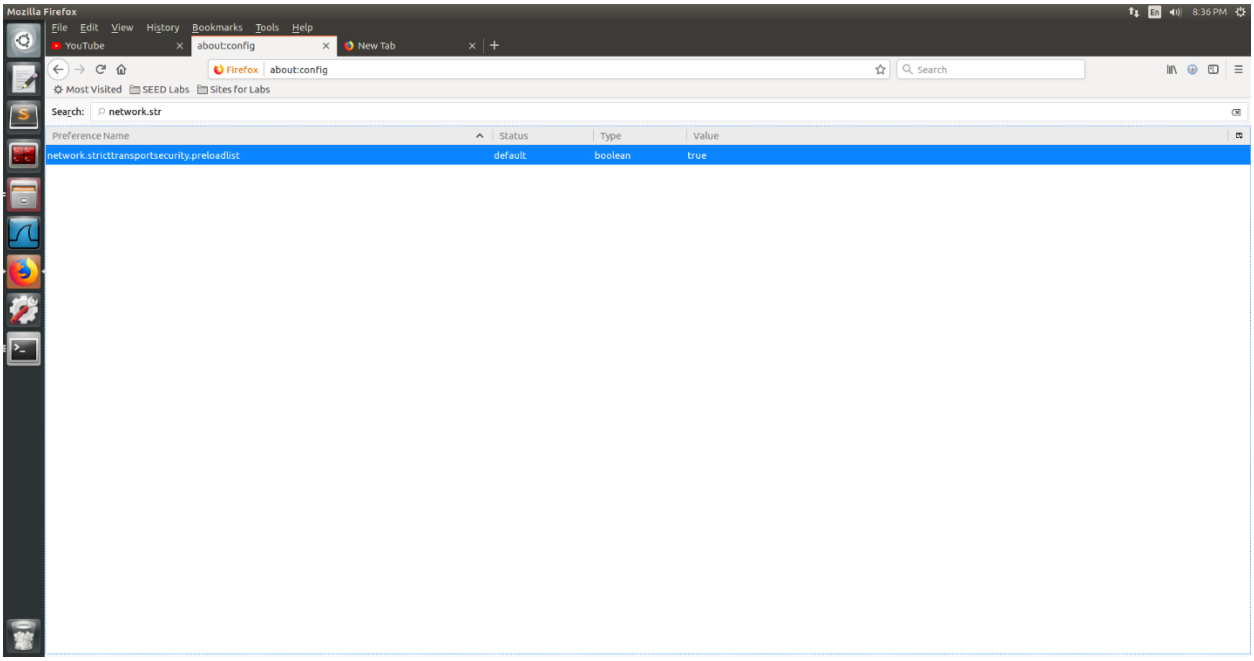
Navigate to the target website its will redirect to our malicious server



In some case we will facing some issue whenever navigate to youtube.com

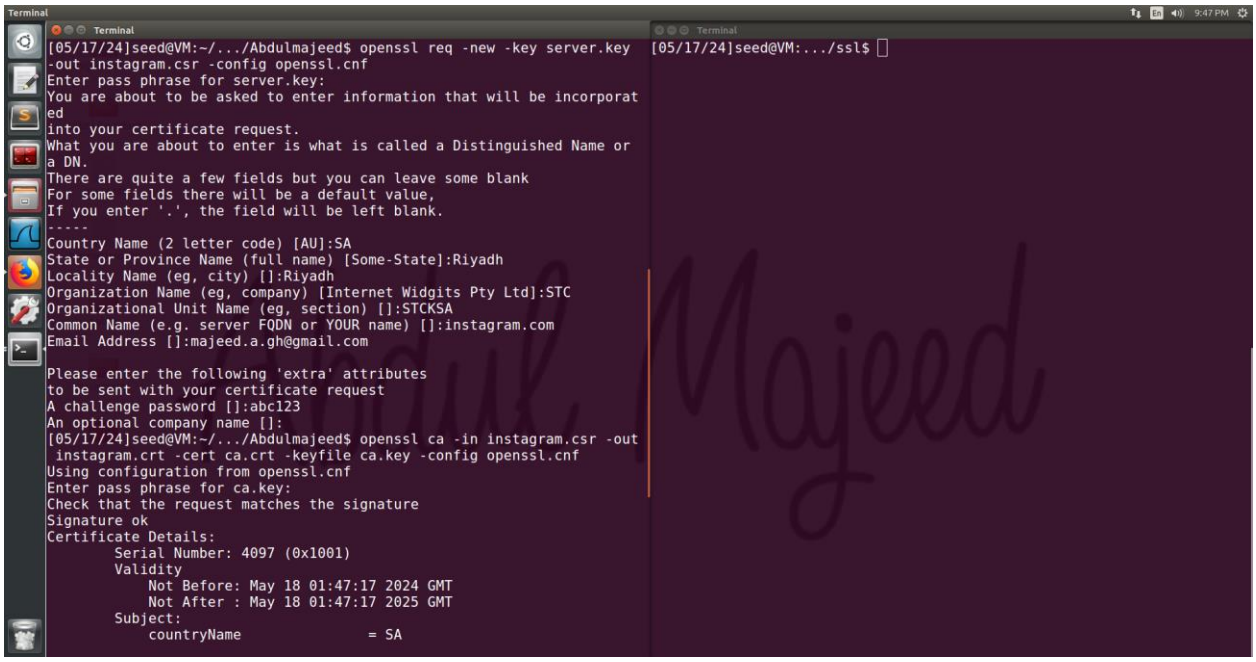
So I search for the reason and I found this :
"When you navigate to youtube.com , it automatically redirects to https://youtube.com because YouTube, like many modern websites, enforces HTTPS for all connections to ensure secure communication between the user and the website. This is achieved through HTTP Strict Transport Security (HSTS), which instructs browsers to only interact with the site over a secure connection. "

I disable the HSTS and its now work correctly

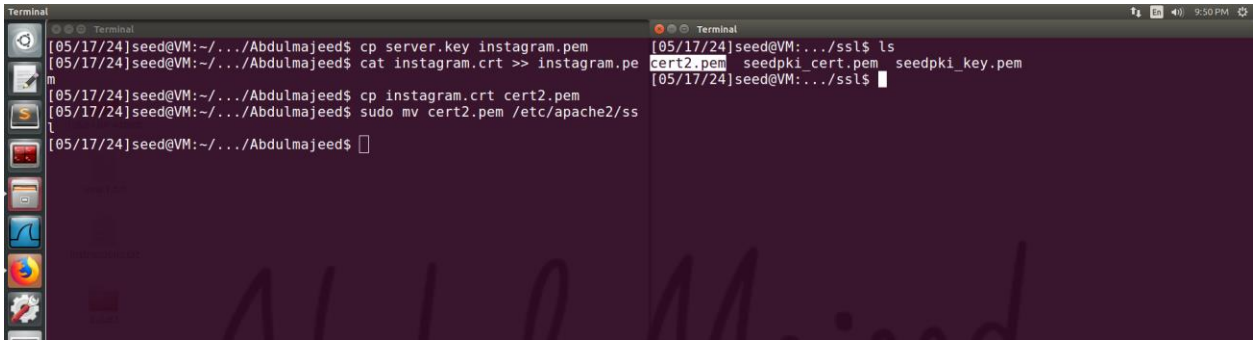


Task 6: Launching a Man-In-The-Middle Attack with a Compromised CA

generate a certificate using a Certificate Signing Request (CSR) file named "instagram.csr and compromised CA private key to sign the CSR and generate the certificate

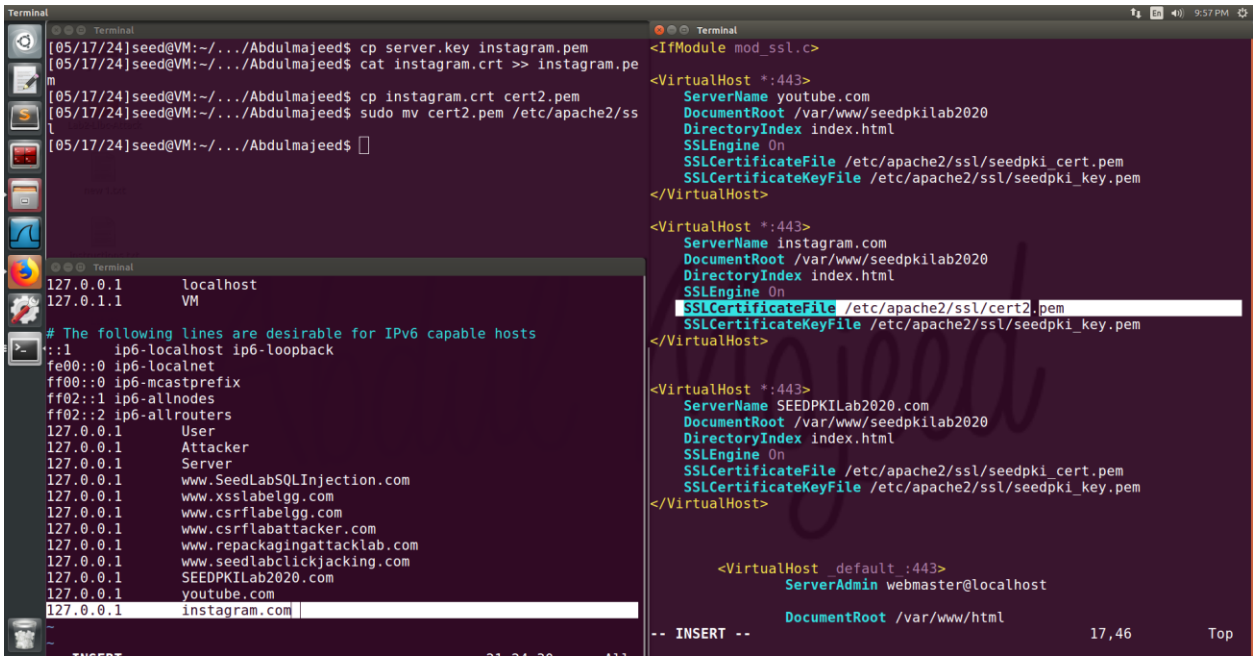


combine the secret key and certificate



Configuring DNS as we did before , and in the Virtualhost we add the website (notice SSLCertificateFile)

the path navigation to new cert2 we create for Instagram



navigate in the browser Instagram.com