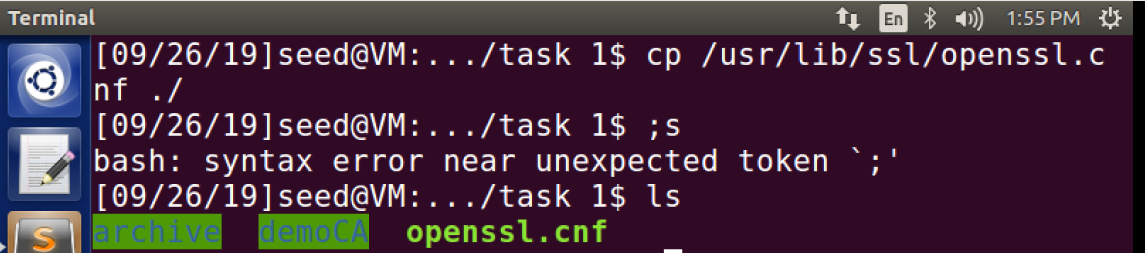
Lab 2

### CMPSC 443

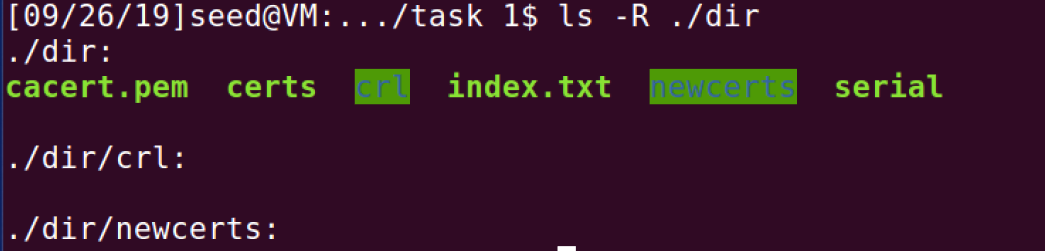
##### Student name:

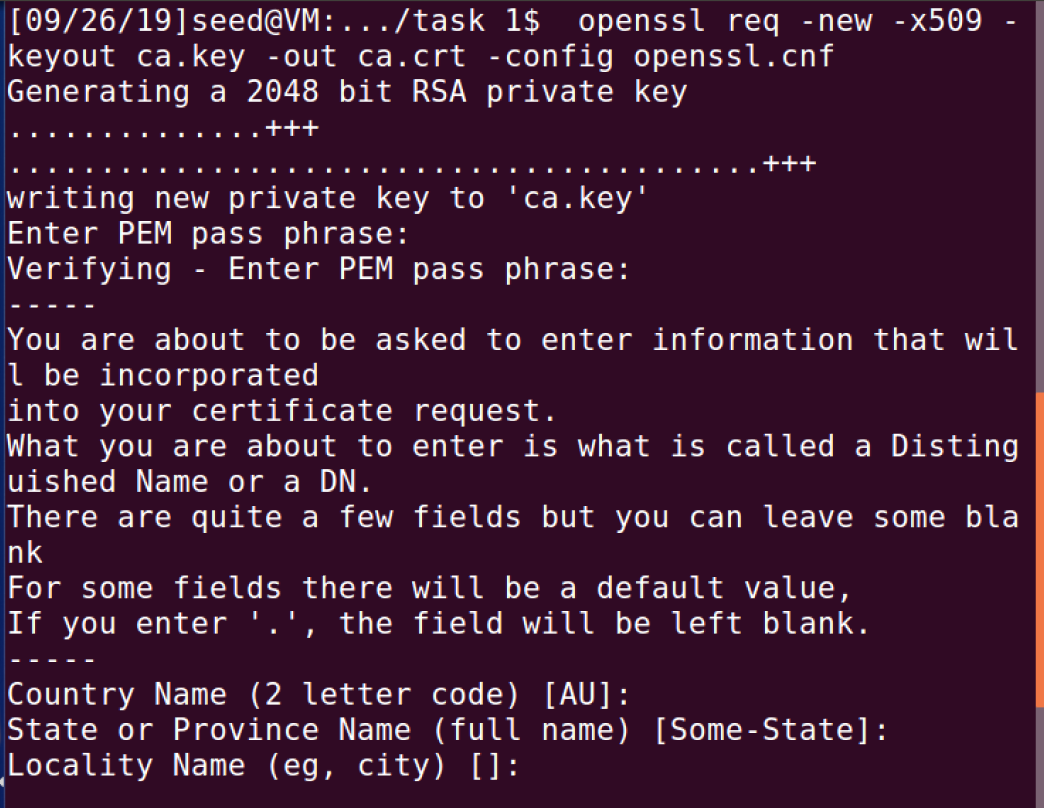
# Task 1: Becoming a Certificate Authority (CA)

Copying the openssl.cnf file

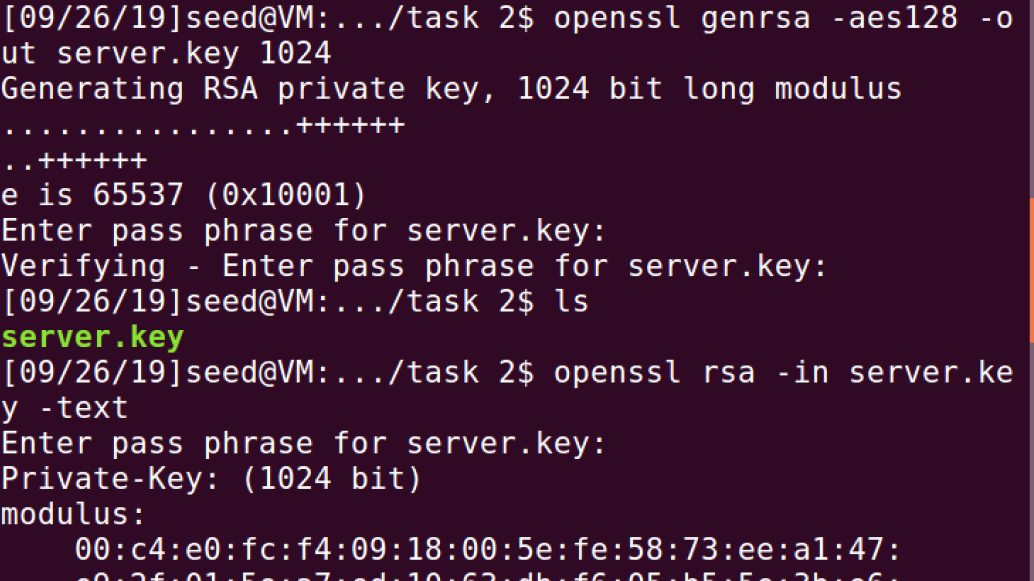


Creating the sub-directories:

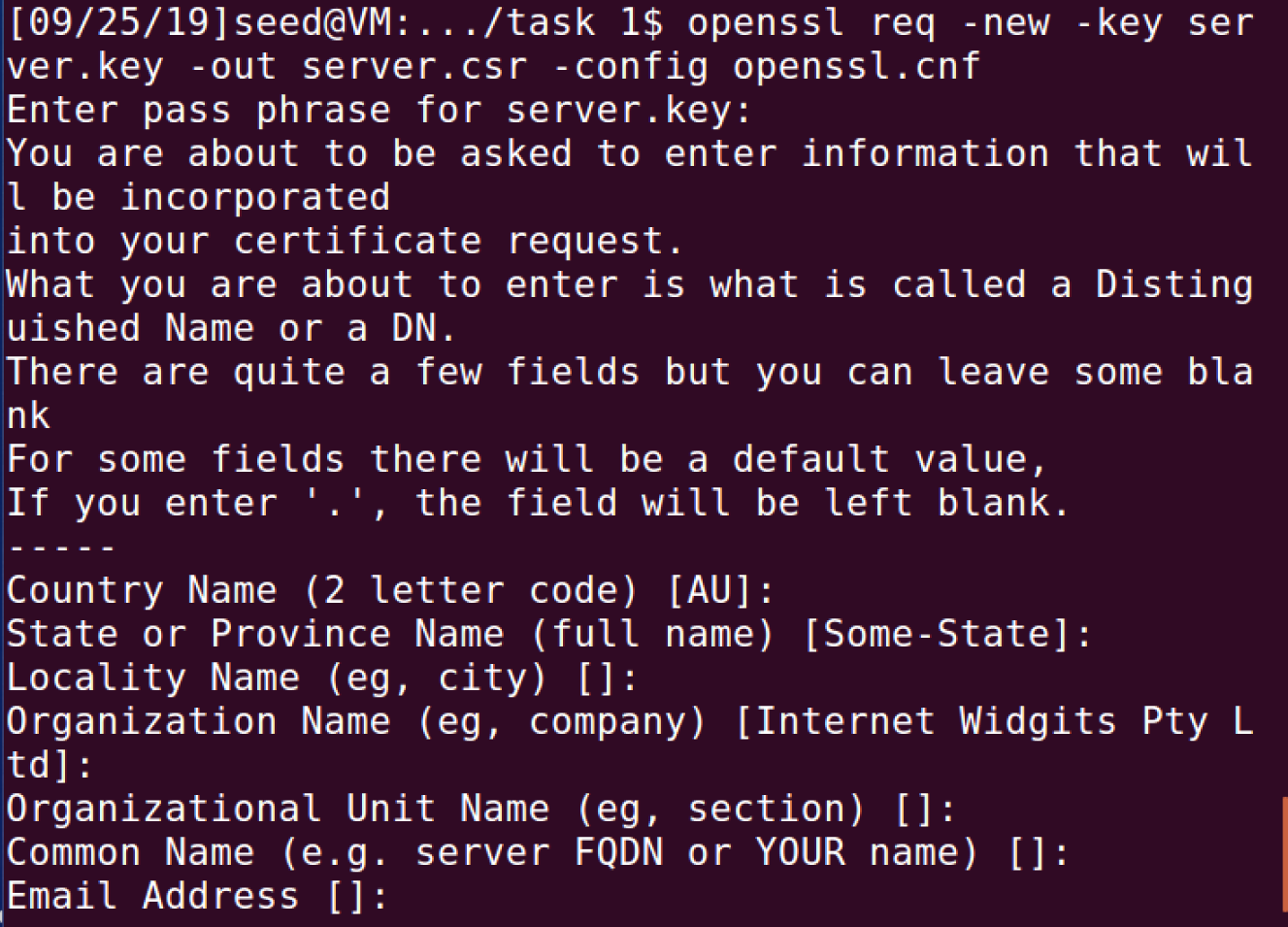


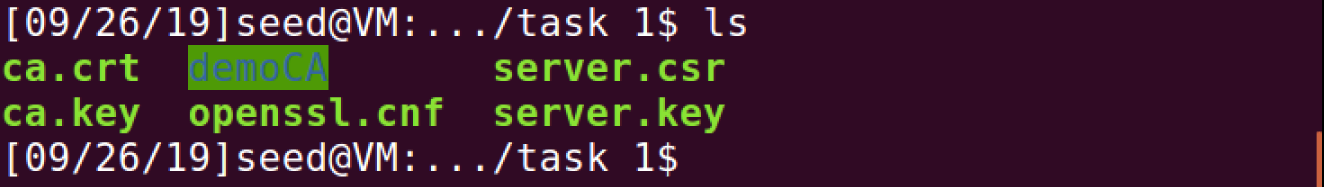
Key created:  


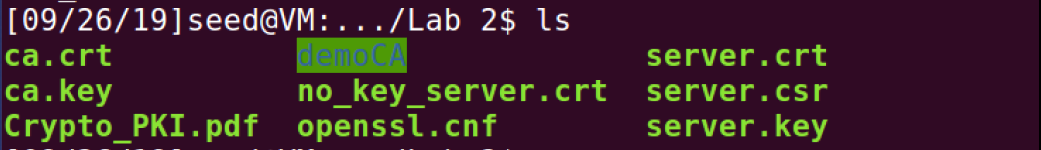
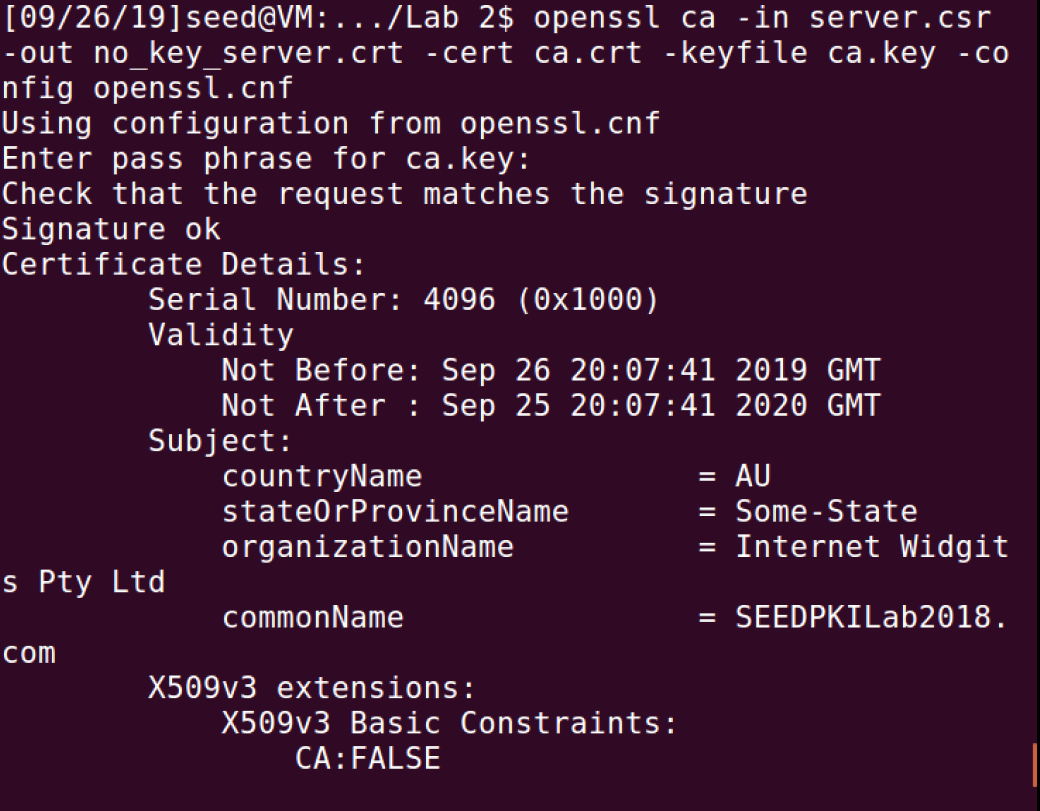
# Task 2 - Creating a Certificate for SEEDPKILab2018.com

**Step 1:** Generating public/private key pair.  


**Step 2:** Generate a Certificate Signing Request (CSR). (moved the files to another folder)

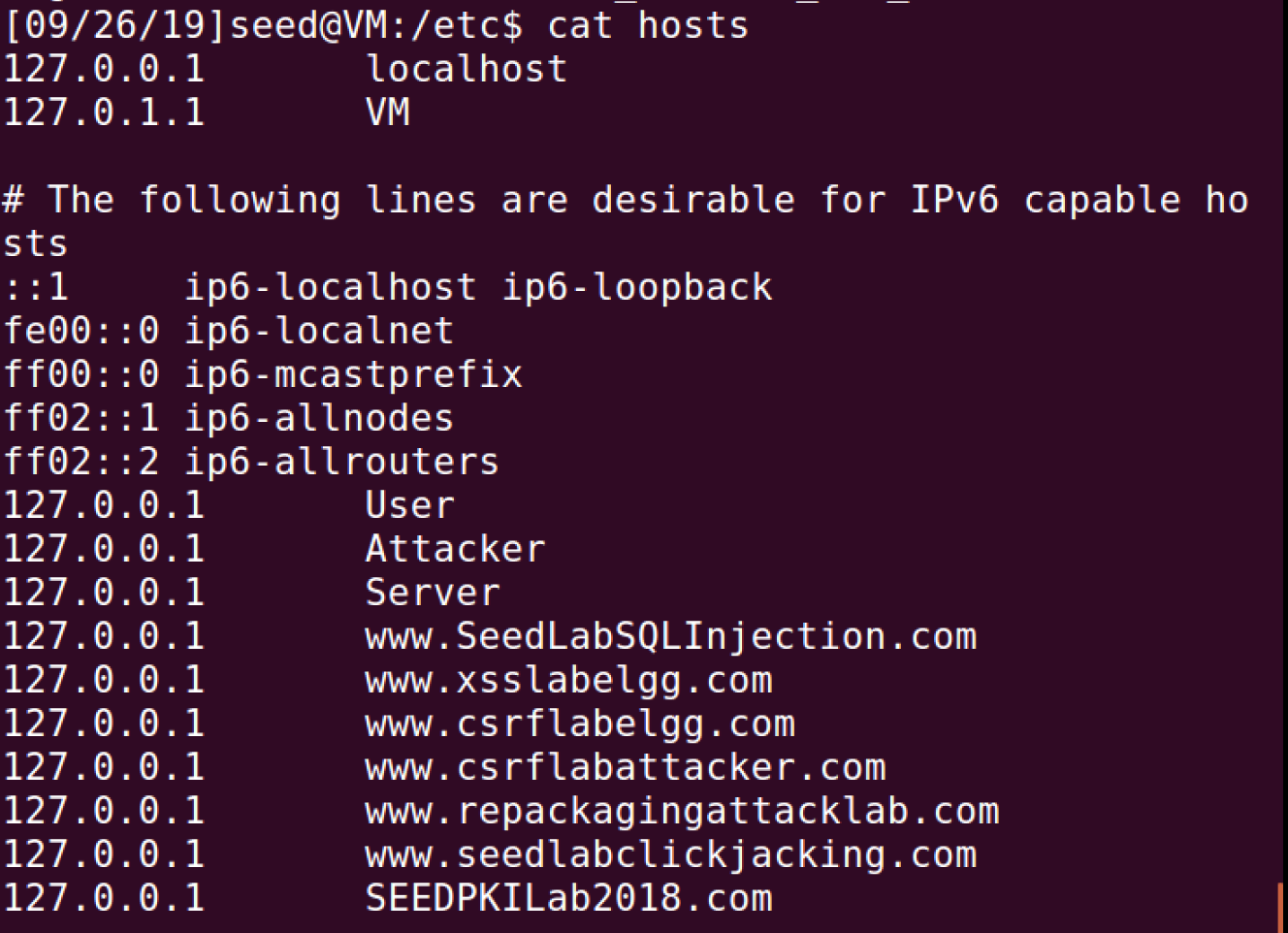




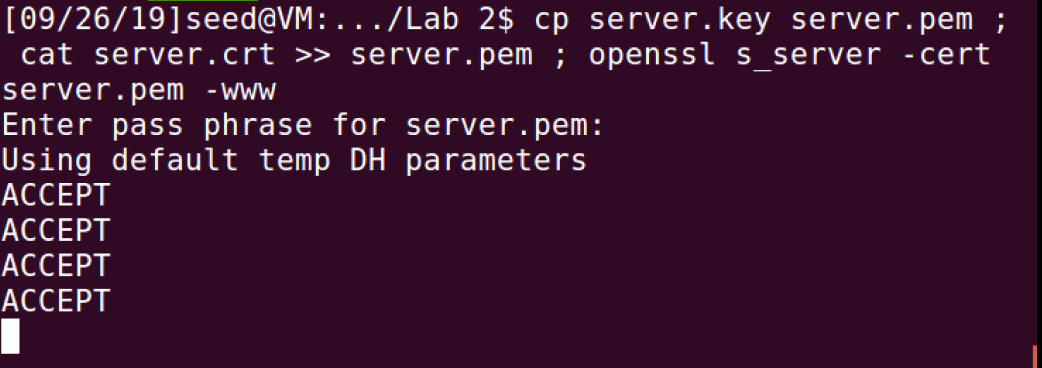
**Step 3:** Generating Certificates. (moved the files to a different folder)  


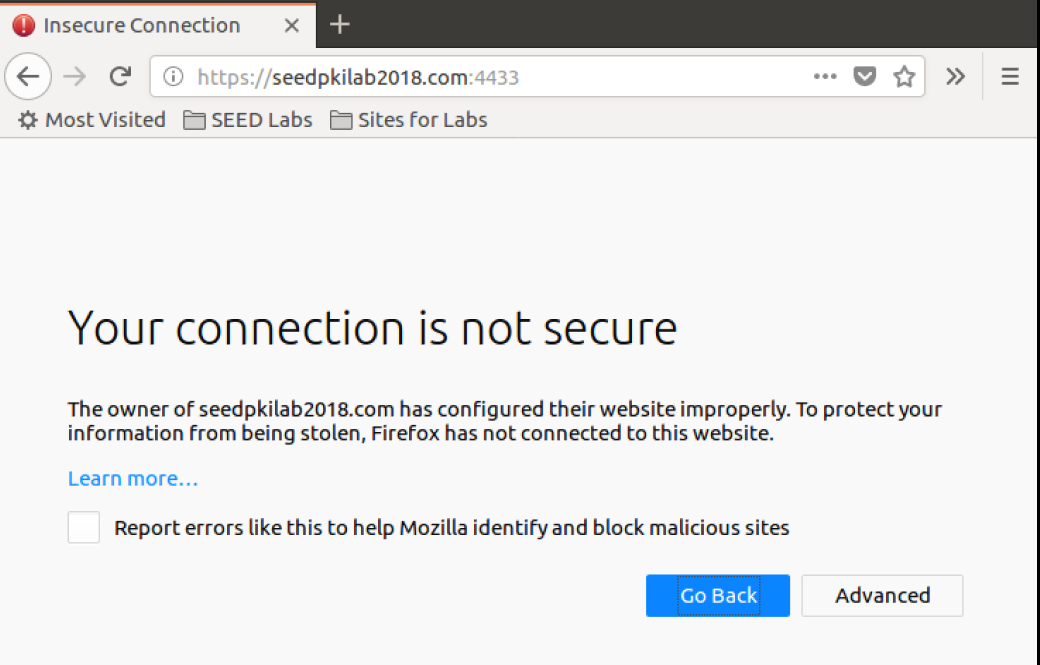
# Task 3 - Deploying Certificate in an HTTPS Web Server

**Step 1**: Configuring DNS

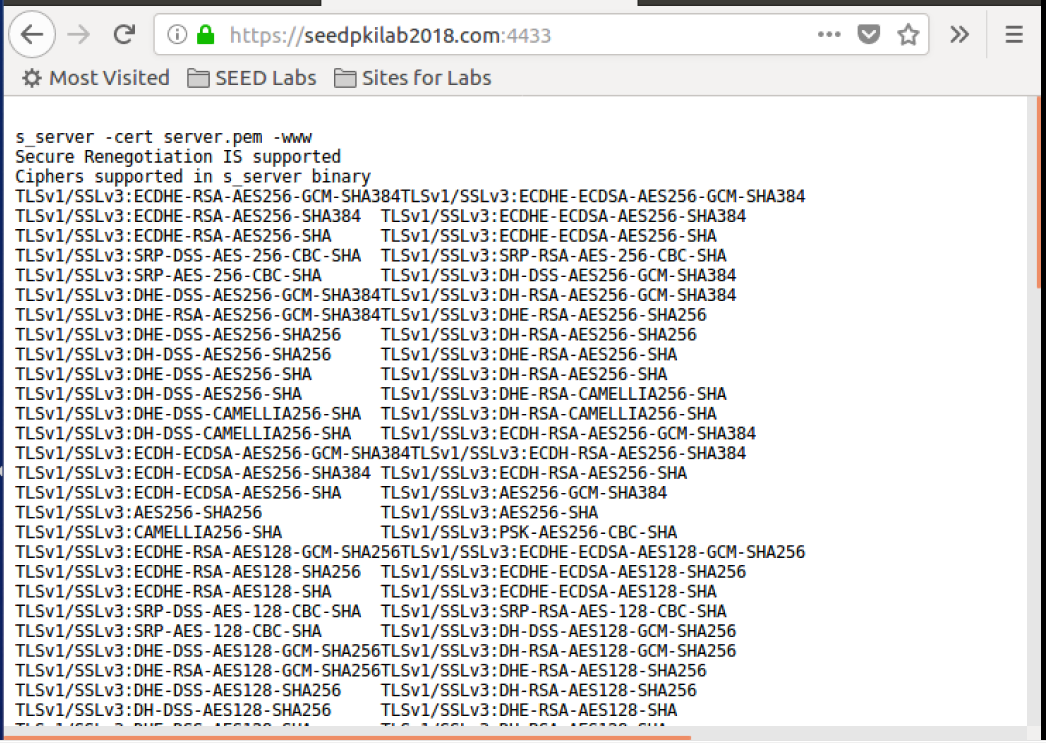


**Step 2:** Configuring the web server



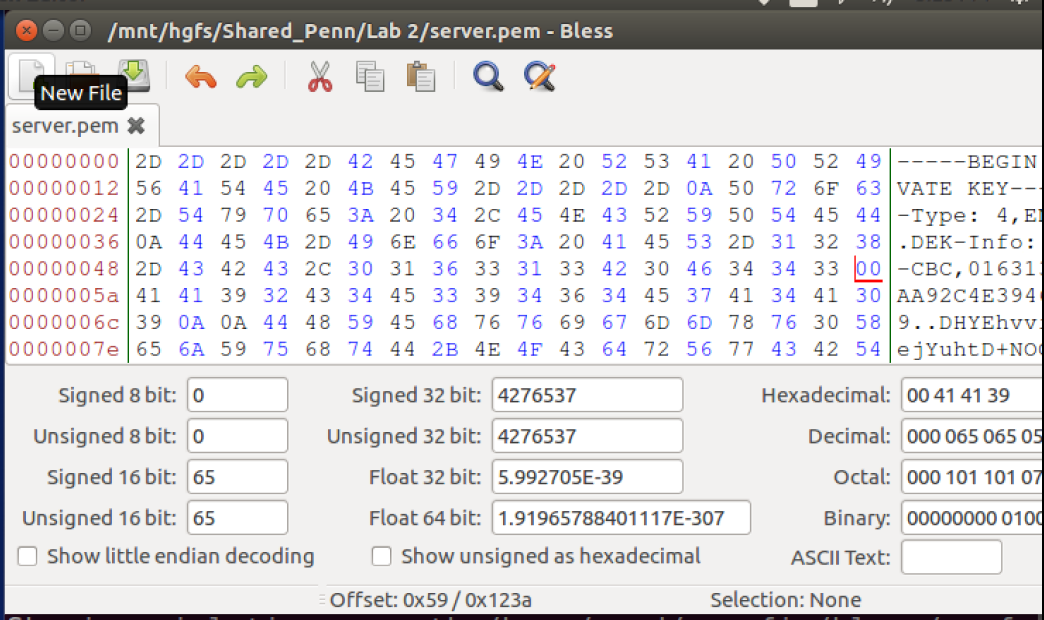
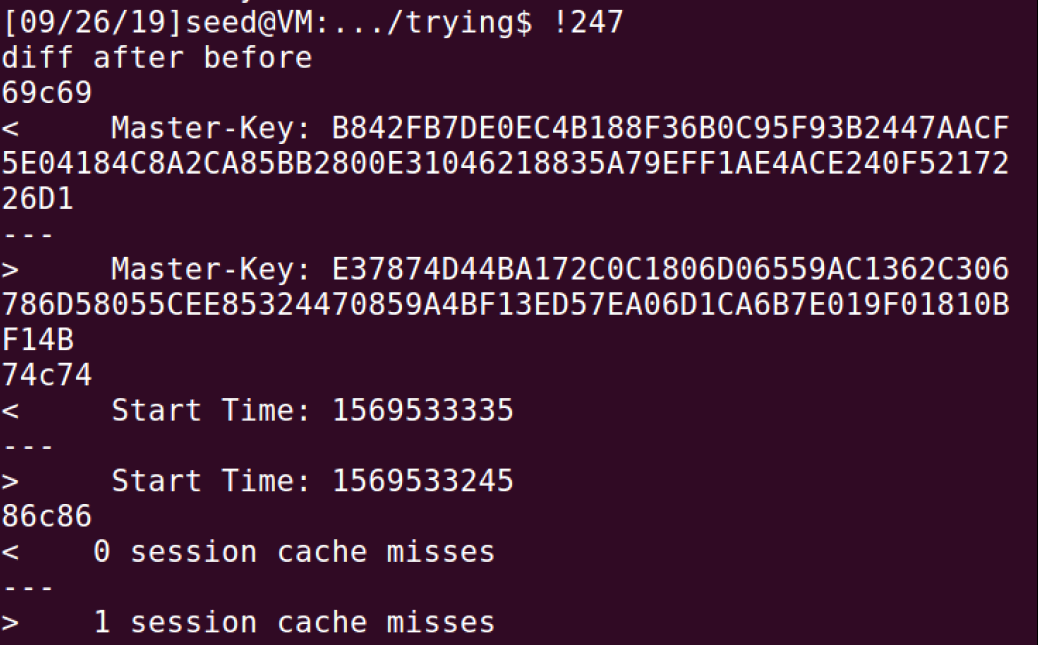


**Step 3:** Getting the browser to accept our CA certificate.  
Done in firefox.

**Step 4.** Testing our HTTPS website.  


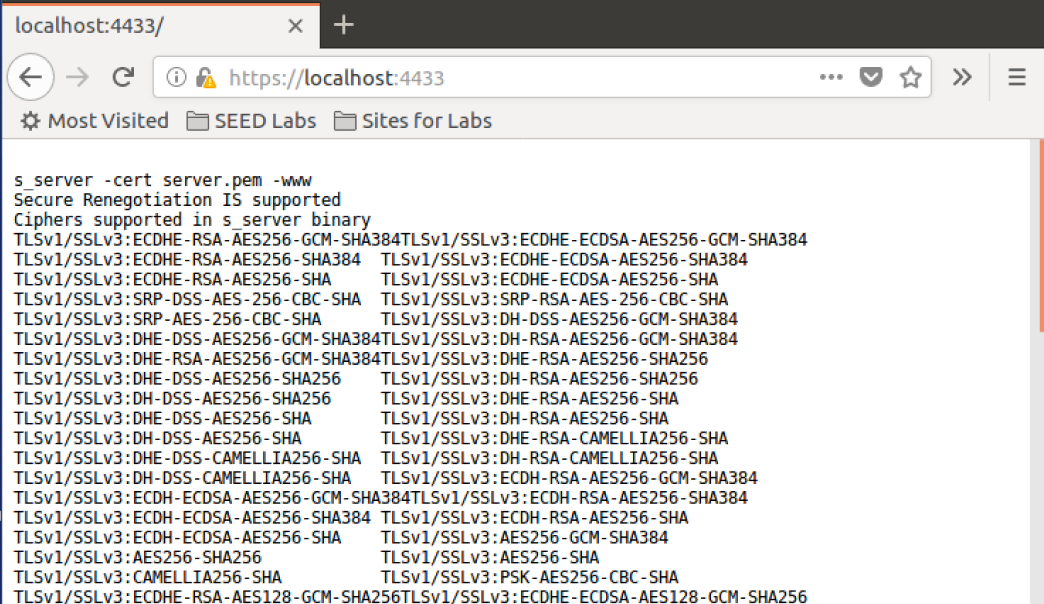
##### Question 1

Changing 1 bit.

  
Things all across the page has changed   


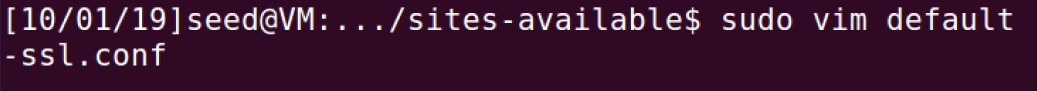
##### Question 2

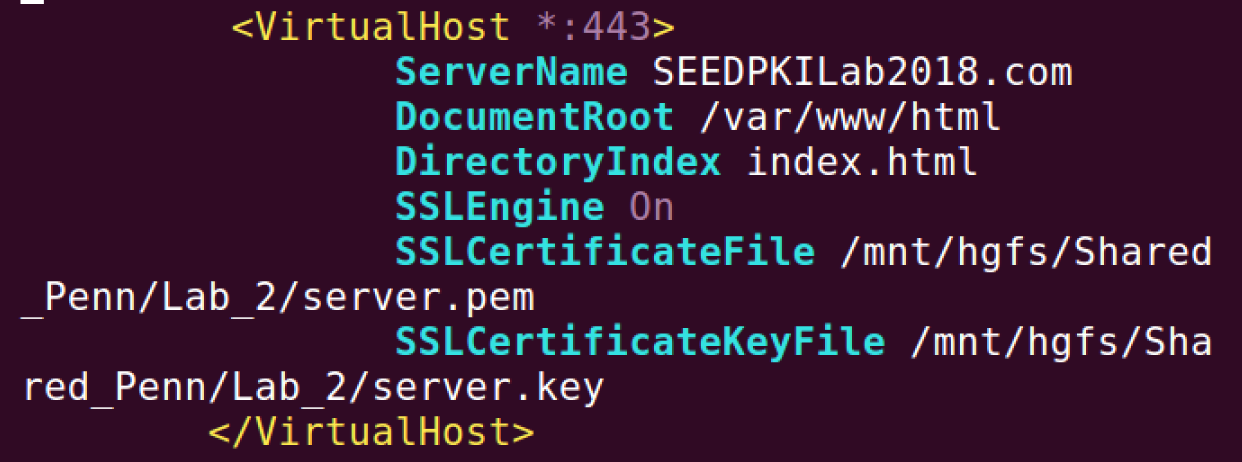
When I tried connecting to “https://localhost:4433” I was asked to add the URL to the exceptions.  
after doing so, I could connect to the site.



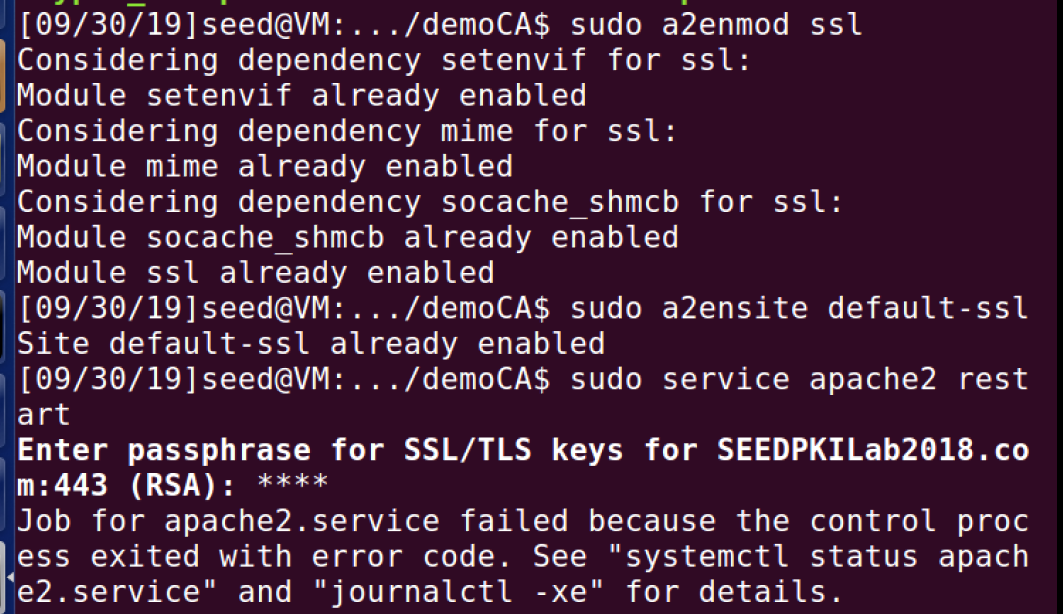
# Task 4 - Deploying Certificate in an Apache-Based HTTPS Website.

Editing the “default-ssl.conf” file.

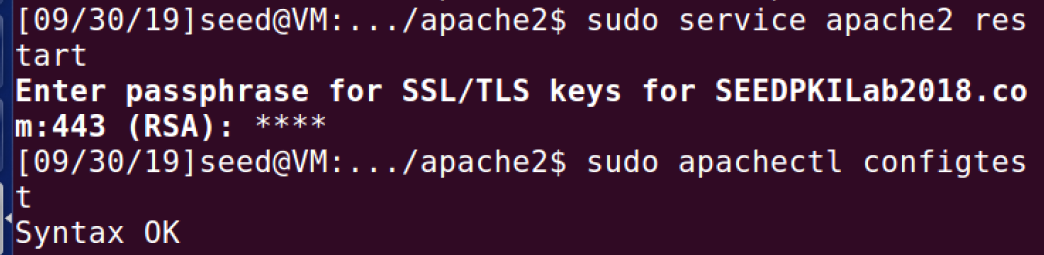




Enabling the SSL module and the site we have just edited.

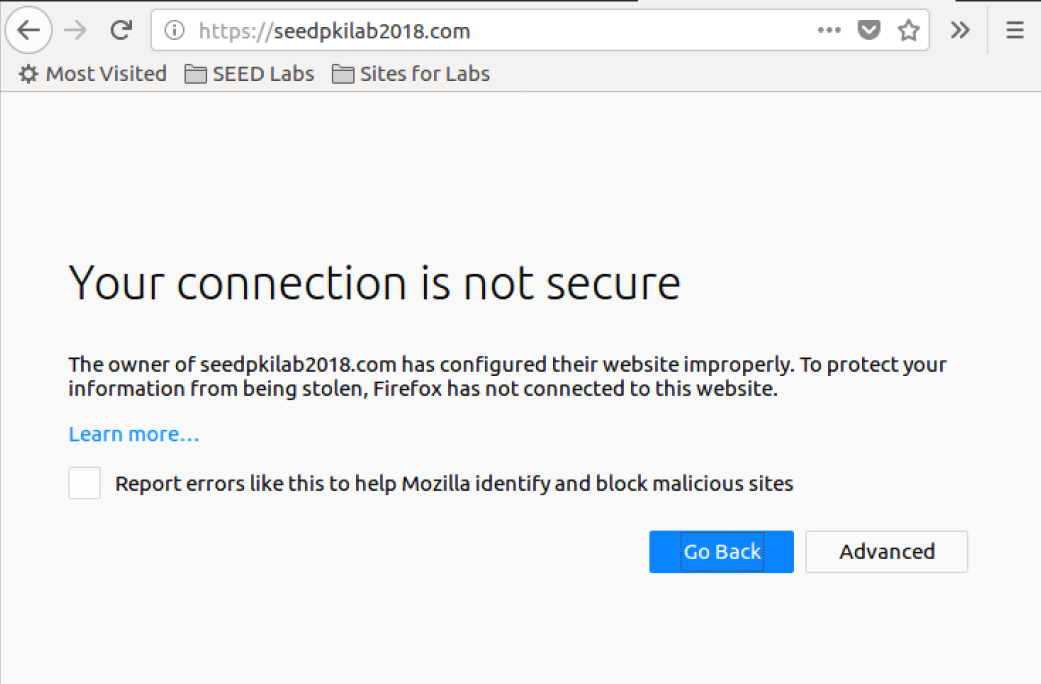


Restarting and testing the system

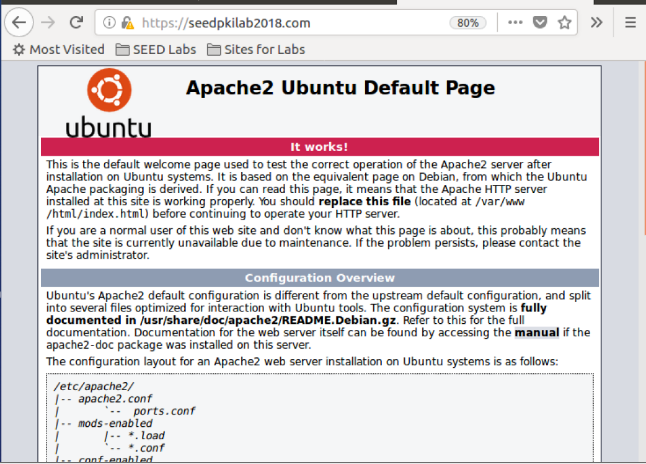


The webpage

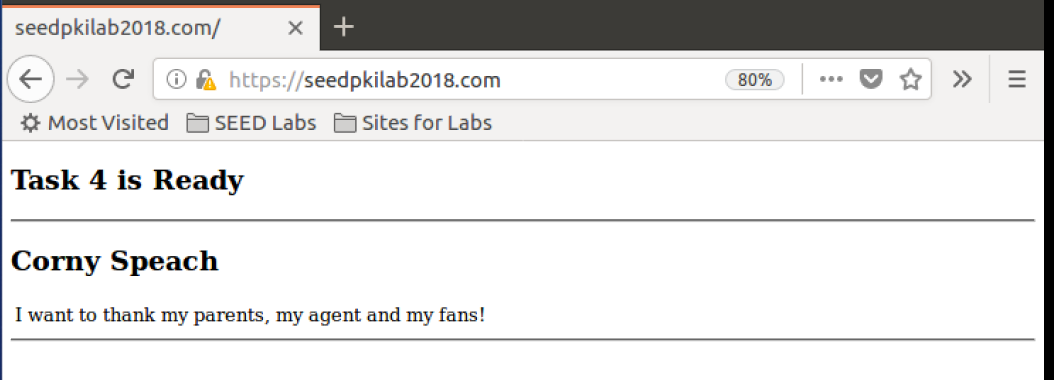
* I got message: “your connection is not secure”, even when the cert is imported.



The site, after adding an exception.

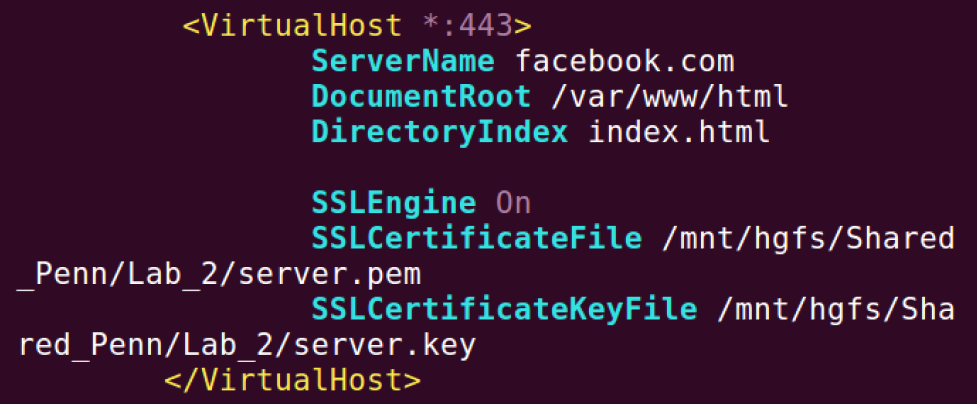


After editing the site

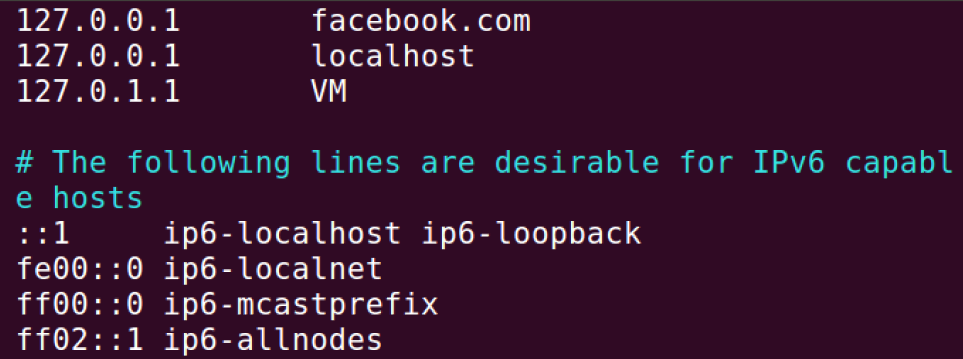


# Task 5 - Launching a Man-In-The-Middle Attack

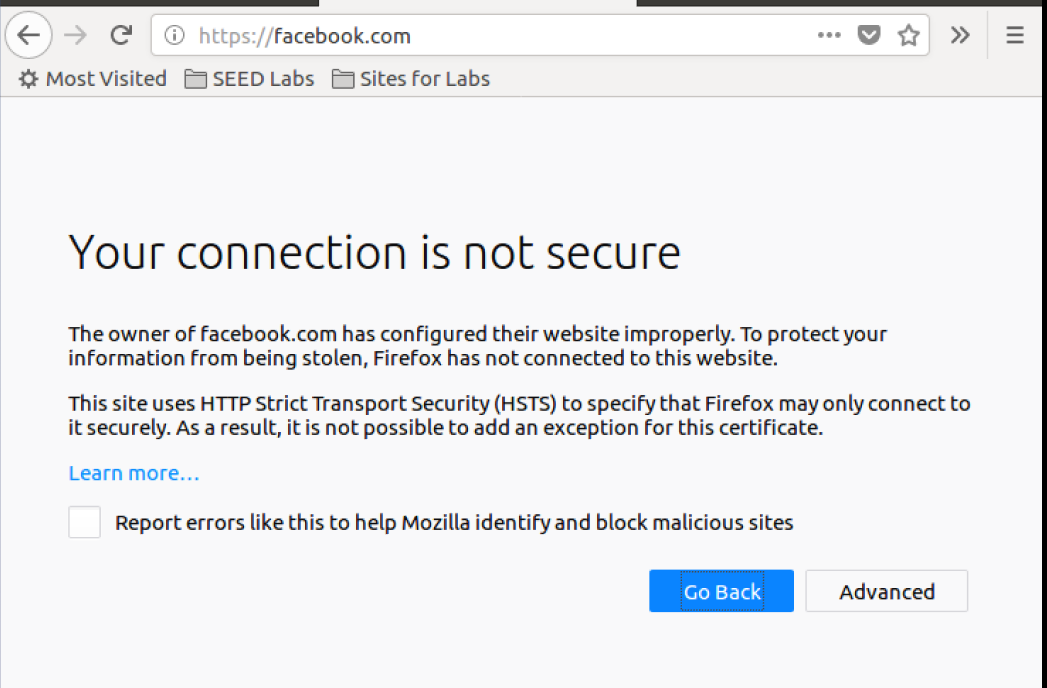
**Step 1: Setting up the malicious website.** I will use “facebook.com” for the task.

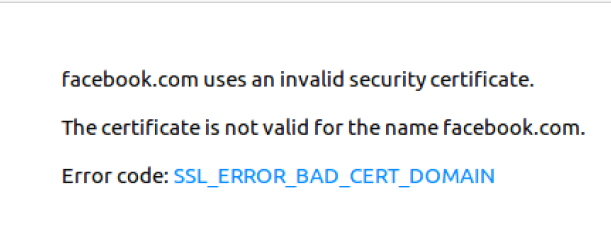


**Step 2: Becoming the man in the middle.**Adding “facebook.com” into the hosts file with the IP of our malicious site



**Step 3: Browse the target website.** I am getting “your connection is not secure” message.

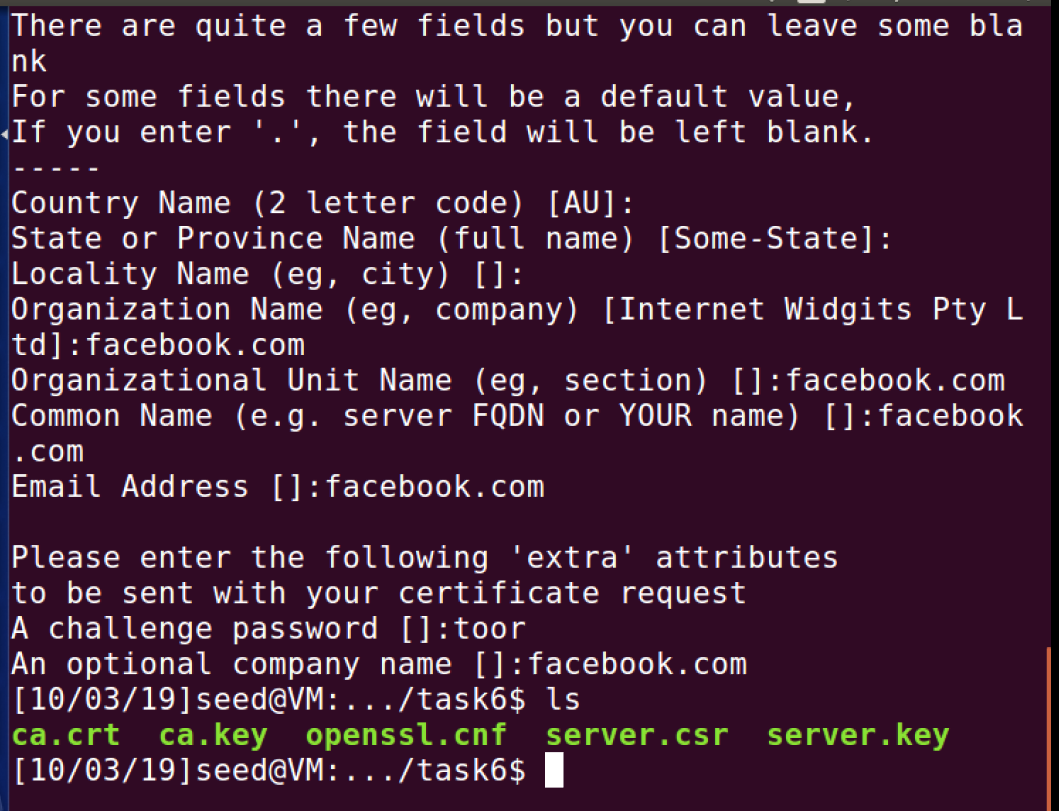


And if we will try to add the Cert file as an exception, we will get this message-

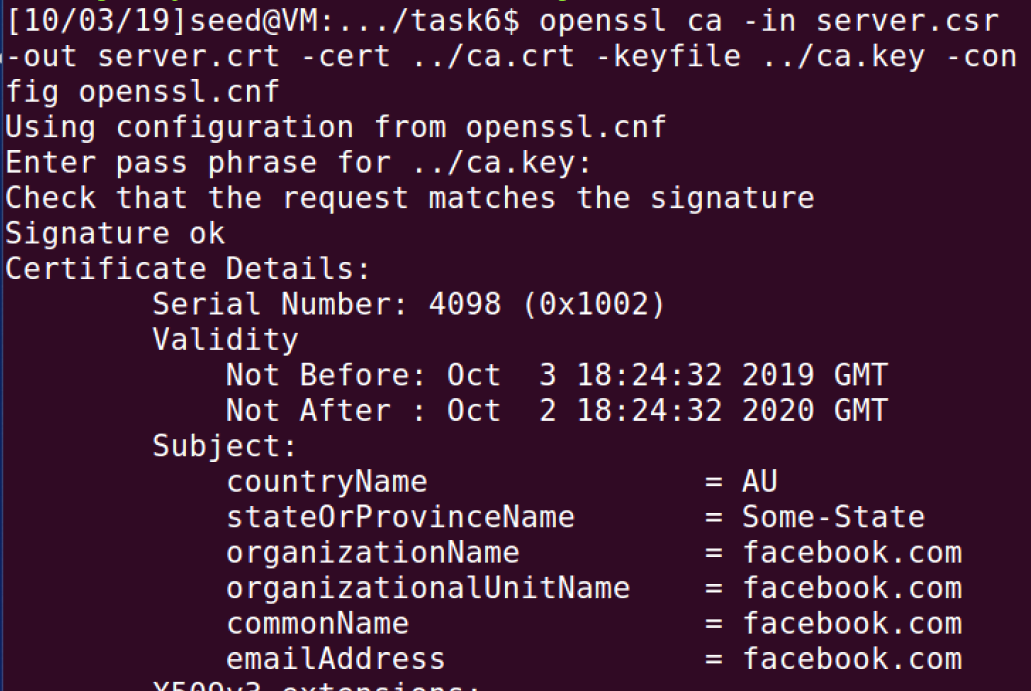
I am assuming that our browser has the list of sites of which he knows what the Cert file is suppose to be, and the browser can detect that we are directed to a site that does not match the original site, by the cert files (because they are public).

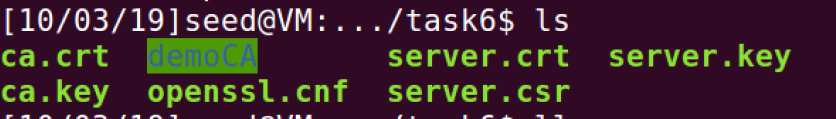
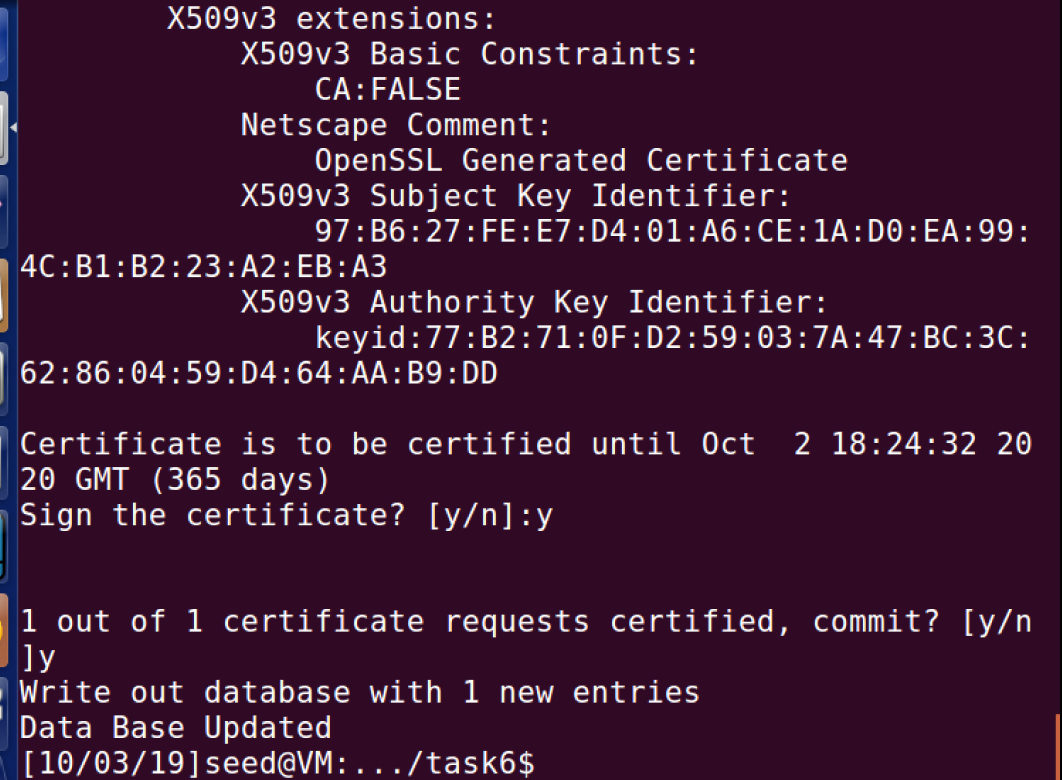
# Task 6: Launching a Man-In-The-Middle Attack with a Compromised CA

Creating new server files-

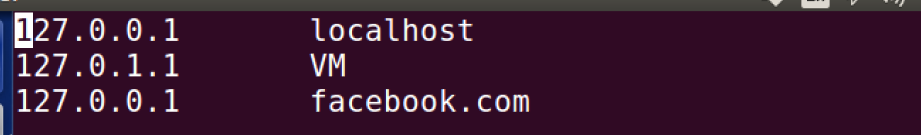


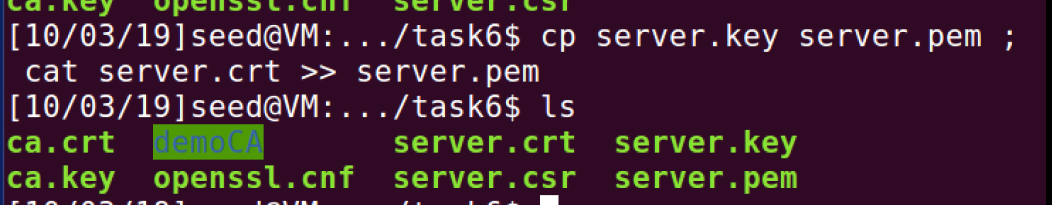
Creating the server.crt file



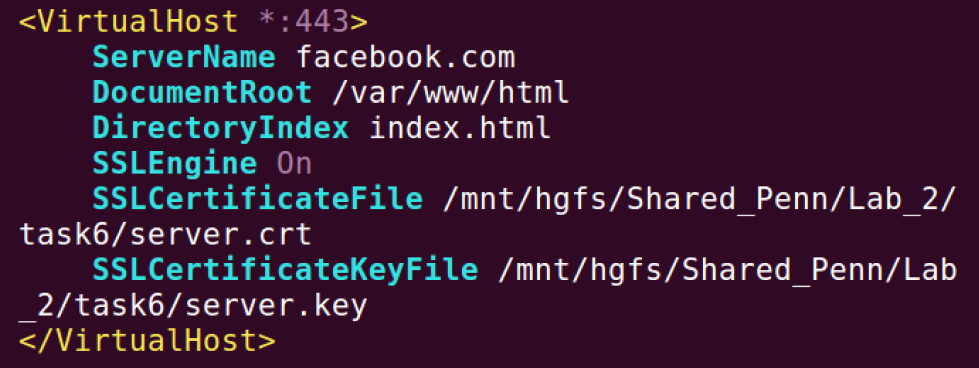


DNS file-



Creating the server.pem file-

Editing the Virtual Host entry-



* **We are now using “server.crt” file and not the “server.pem” file.**

Restarting Apache and browsing the target website-

