**PRACTICA 4 REPORT**

Christoforos Dellios

Konstantinos Ladas

The aim of this practice is to protect the web farm we have created in the past exercises by installing an SSL certificate to configure HTTPS access to the servers and to configure firewall rules.

First, we generate and install an SSL certificate. We execute the following commands:

a2enmod ssl

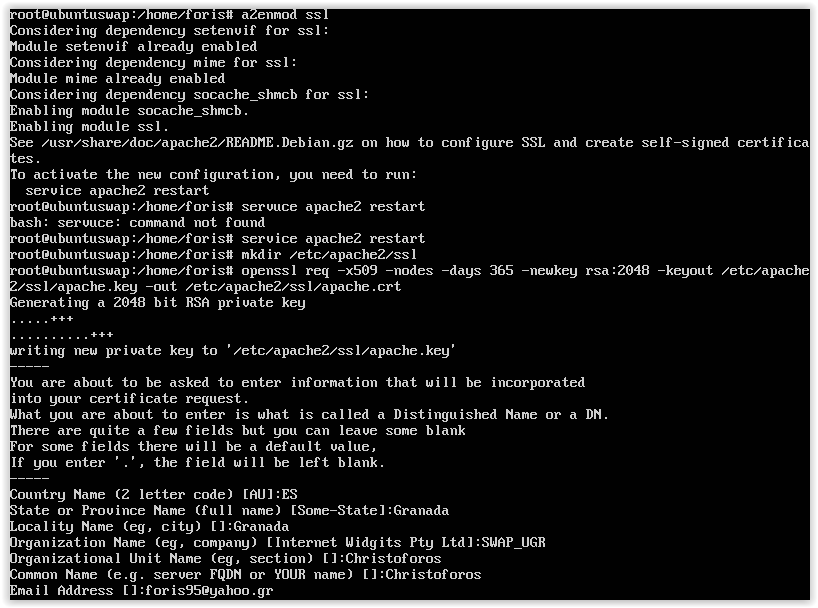
service apache2 restart

mkdir /etc/apache2/ssl

openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout

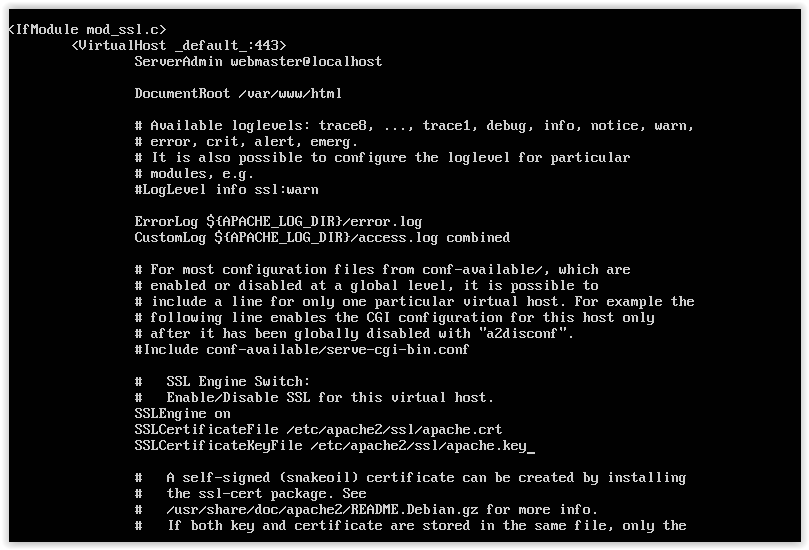
/etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt

And then we complete the form that is generated:



And we add the lines, as instructed under the SSLEngine on, in this file:

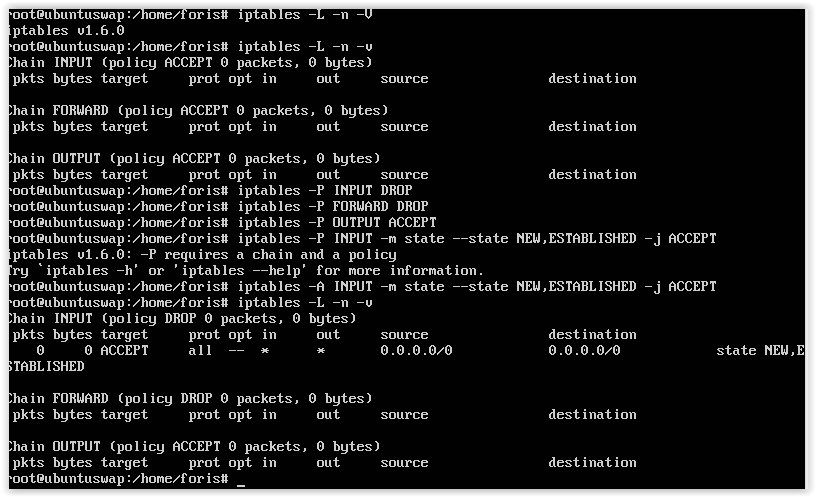
/ etc / apache2 / sites-available / default-ssl



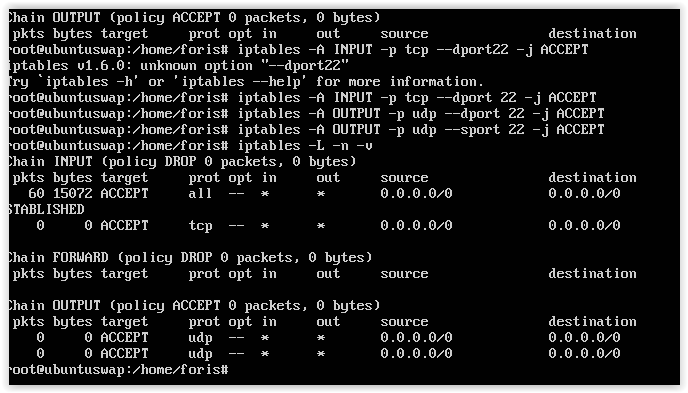
After restarting apache, if we access the server from a browser using its IP, the address bar will be red.

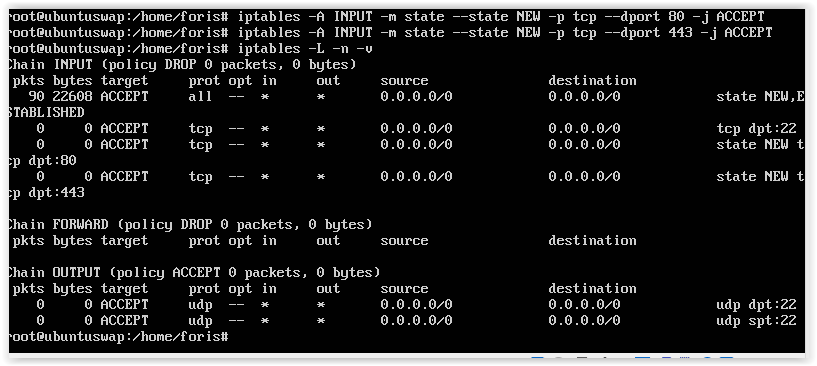
After that, we configure our firewall to block any incoming traffic that doesn’t meet our safety criteria.

To do this we use the iptables application:

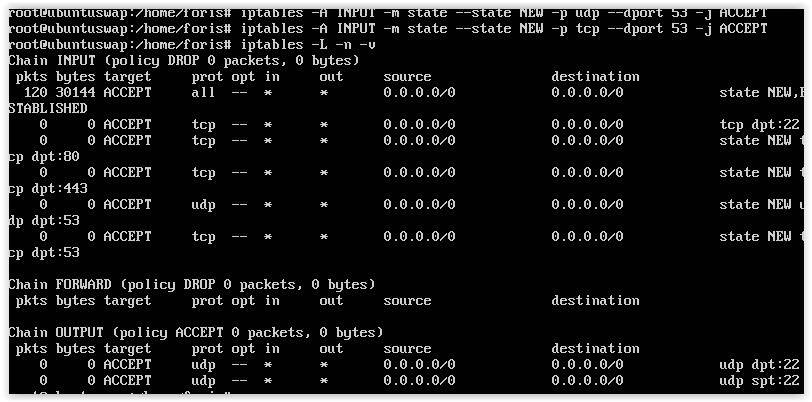


After we test some commands to learn about the iptables application, we have to open certain ports such as port 22 to allow SSH access,



ports 80 and 443 to configure the web server,

and last the port 53 to allow DNS access.



Finally, we test our firewall configuration with the command:

netstat –tulpn

to check if our ports are open. For our commands to run on startup, we made a script that runs on startup.