PRACTICA 4 REPORT

Christoforos Dellios

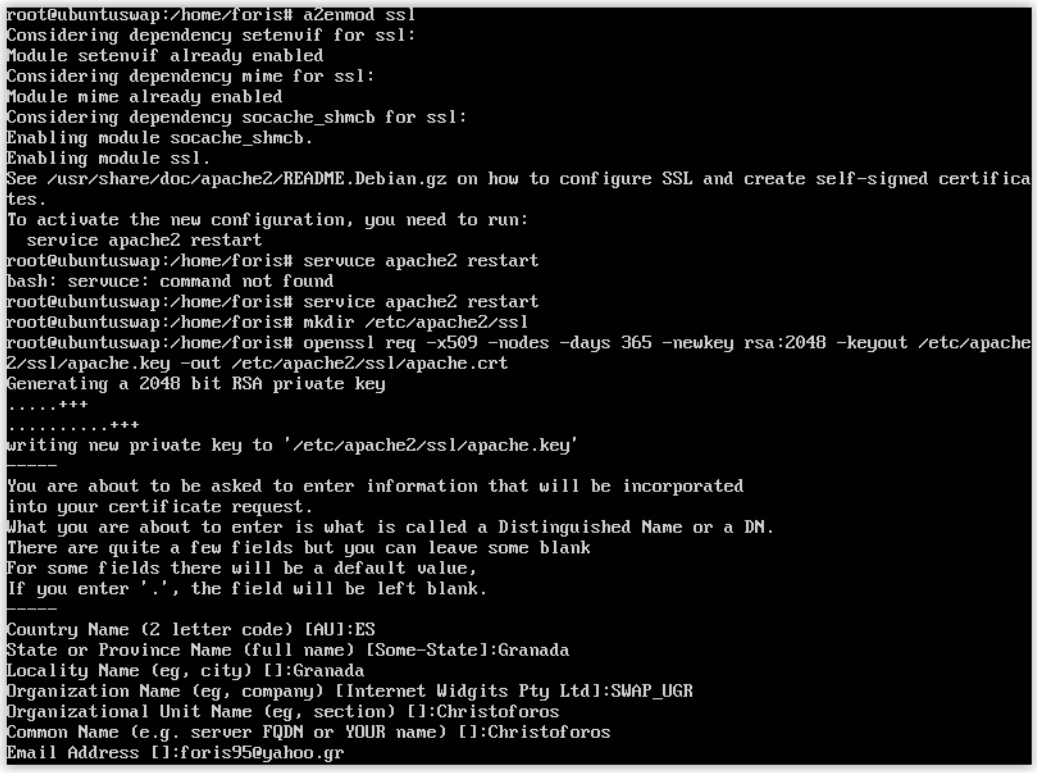
Konstantinos Ladas

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:

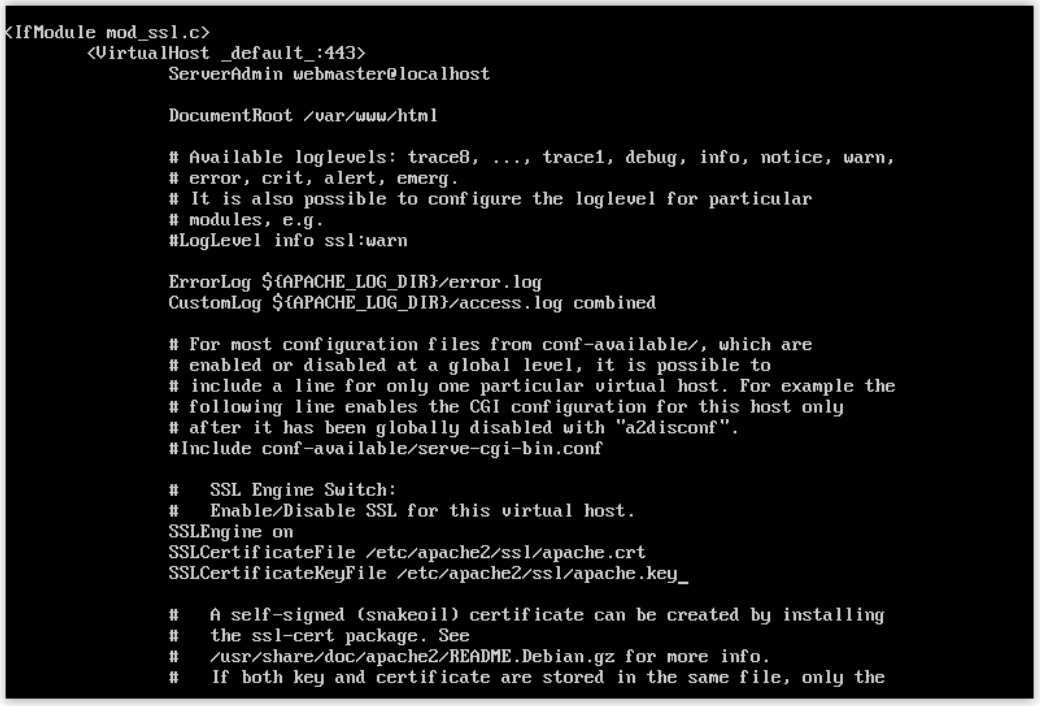
```
a2enmod ssl
service apache2 restart
mkdir /etc/apache2/ssl
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt
```

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.

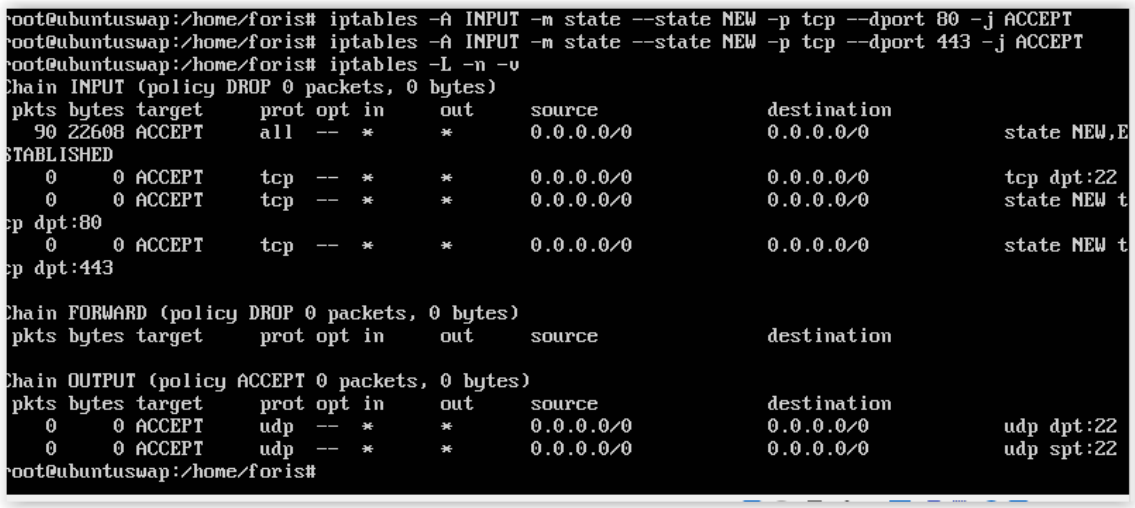
To do this we use the iptables application:

```
root@ubuntuswap:/home/foris# iptables -L -n -V
iptables v1.6.0
root@ubuntuswap:/home/foris# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@ubuntuswap:/home/foris# iptables -P INPUT DROP
root@ubuntuswap:/home/foris# iptables -P FORWARD DROP
root@ubuntuswap:/home/foris# iptables -P OUTPUT ACCEPT
root@ubuntuswap:/home/foris# iptables -P INPUT -m state --state NEW,ESTABLISHED -j ACCEPT
iptables v1.6.0: -P requires a chain and a policy
Try `iptables -h' or 'iptables --help' for more information.
root@ubuntuswap:/home/foris# iptables -A INPUT -m state --state NEW,ESTABLISHED -j ACCEPT
root@ubuntuswap:/home/foris# iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state NEW,E
STABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@ubuntuswap:/home/foris# _
```

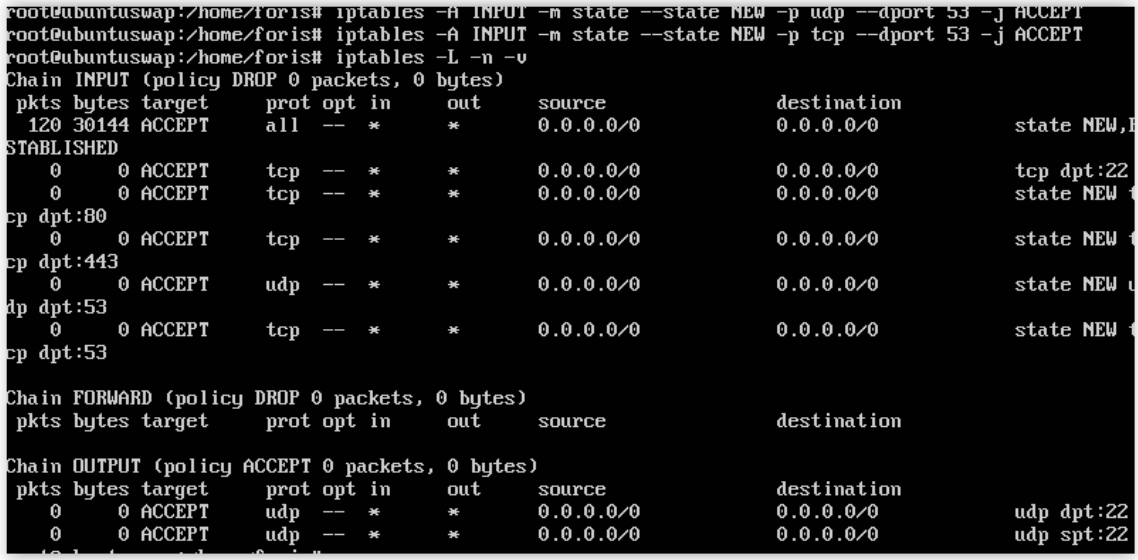
After we test some commands to learn about the iptables application, we have to open certain ports such as port 22 to allow SSH access,

```
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@ubuntuswap:/home/foris# iptables -A INPUT -p tcp --dport22 -j ACCEPT
iptables v1.6.0: unknown option "--dport22"
Try `iptables -h' or 'iptables --help' for more information.
root@ubuntuswap:/home/foris# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
root@ubuntuswap:/home/foris# iptables -A OUTPUT -p udp --dport 22 -j ACCEPT
root@ubuntuswap:/home/foris# iptables -A OUTPUT -p udp --sport 22 -j ACCEPT
root@ubuntuswap:/home/foris# iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   60 15072 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
STABLISHED
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0
root@ubuntuswap:/home/foris#
```

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.