Report on VPN (Task 2)

Name Aravindh JAWAHAR

Formation MSS September 2021

Task N° 2

Problem statement:

In this lab, we will create a webserver and a PKI to generate a self-signed certificate. One CentOS 8 virtual machine will be used. A minimal configuration is enough and only 2GB of RAM and 2 CPU's are needed.

Index

Solution:

CentOS 8 has been installed on VMWare workstation player 16.

Installing Webserver:

Apache server has been installed on the VM using the command:

Yum install httpd -y

```
[root@centos8 centos]# yum install httpd -y
CentOS-8 - AppStream                                 1.8 MB/s | 5.8 MB     00:03
CentOS-8 - Base                                      1.3 MB/s | 2.2 MB     00:01
```

And the server has been enabled to start the service with the command:

Systemctl start httpd Systemctl enable httpd

```
Installed:
  apr-1.6.3-9.el8.x86_64
  apr-util-1.6.1-6.el8.x86_64
  apr-util-bdb-1.6.1-6.el8.x86_64
  apr-util-openssl-1.6.1-6.el8.x86_64
  centos-logos-httpd-80.5-2.el8.noarch
  httpd-2.4.37-21.module_el8.2.0+494+1df74eae.x86_64
  httpd-filesystem-2.4.37-21.module_el8.2.0+494+1df74eae.noarch
  httpd-tools-2.4.37-21.module_el8.2.0+494+1df74eae.x86_64
  mailcap-2.1.48-3.el8.noarch
  mod_http2-1.11.3-3.module_el8.2.0+486+c01050f0.1.x86_64

Complete!
[root@centos8 centos]# systemctl start httpd
[root@centos8 centos]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/
httpd.service.
[root@centos8 centos]#
```

```
[root@centos8 centos]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2020-11-27 14:16:02 EST; 25s ago
     Docs: man:httpd.service(8)
 Main PID: 1913 (httpd)
   Status: "Running, listening on: port 80"
    Tasks: 213 (limit: 11484)
   Memory: 27.1M
   CGroup: /system.slice/httpd.service
           ├─1913 /usr/sbin/httpd -DFOREGROUND
           ├─1914 /usr/sbin/httpd -DFOREGROUND
           ├─1915 /usr/sbin/httpd -DFOREGROUND
           ├─1916 /usr/sbin/httpd -DFOREGROUND
           └─1917 /usr/sbin/httpd -DFOREGROUND

Nov 27 14:16:02 centos8.linuxvmimages.local systemd[1]: Starting The Apache HTTP Server...
Nov 27 14:16:02 centos8.linuxvmimages.local systemd[1]: Started The Apache HTTP Server.
Nov 27 14:16:02 centos8.linuxvmimages.local httpd[1913]: Server configured, listening on: port 80
[root@centos8 centos]#
```

Accessing Webserver:

Then the server can be accessed using the **browser** with the help of the **IP address** of the browser. The link to access the server of apache in the browser is http://192.168.132.180. This link has no certificate for encryption so that our task is to enable encryption on the access over the web interface for the apache server by providing the certificates enabling for the access.

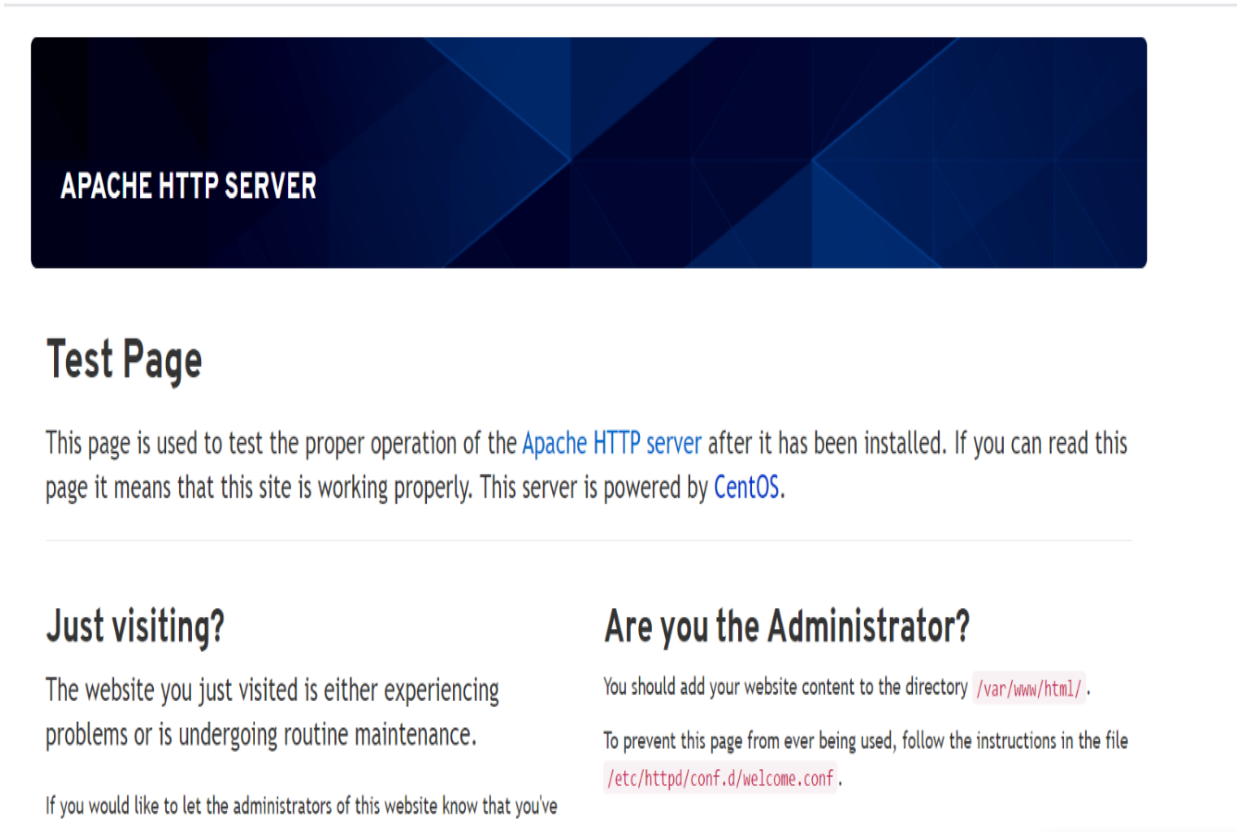
Generating self-signed certificates:

The following are the steps to achieve the encryption:

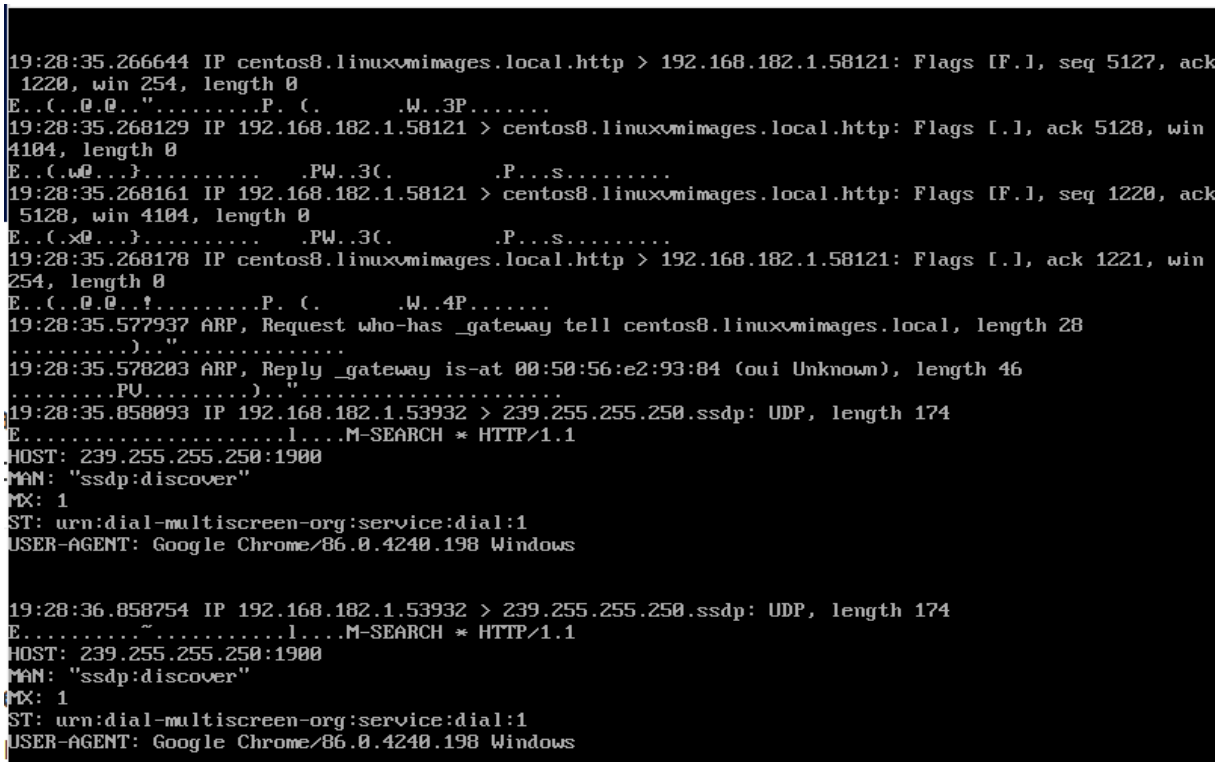
a. Install openssl to create certificate
b. Verify whether the module has been installed
c. Create the certificate:
   Create new directory and type the following command:
   openssl req -x509 -nodes -newkey rsa:2048 -keyout lab.local.key -out lab.local.crt
d. Configure the web server on **ssl.conf** file on **/etc/httpd/conf.d/** and verify the details

Check the server access with the link along side containing the certificates and check it:

https://192.168.182.130



Use the command **tcpdump -i any icmp** to verify whether the traffic is encrypted



Conclusion:

Thus, we created a web server in CentOS 8 and used PKA to generate the self-signed certificates