Μαρίνα Σαμπροβαλάκη
3180234

1. Apache Configuration

   Πάμε στο /**etc/httpd/conf/httpd.conf**
   Στη συνέχεια, αλλάζουμε την ip διεύθυνση που θέλουμε να ακούει ο server μας στην δική μας.

```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 83.212.97.16:80
Listen 80
```

   Η εγκατάσταση του Apache, δημιούργησε το path **/var/www/html**. Σε αυτό το path, δημιουργούμε το index.html στο οποίο υπάρχει ο κώδικας που εμφανίζεται στην σελίδα μας.

2. Για το πρώτο μέρος, τα inbound rules στο service FirewallD του CentOS , ώστε τα http και https να είναι προσπελάσιμα από παντού φαίνονται παρακάτω

```
[root@snf-885682 ~]# firewall-cmd --permanent --zone=public --add-service=http
Warning: ALREADY_ENABLED: http
success
[root@snf-885682 ~]# firewall-cmd --permanent --zone=public --add-service=https
Warning: ALREADY_ENABLED: https
success
[root@snf-885682 ~]# firewall-cmd --reload
success
```

   Στη συνέχεια για να επιτρέψουμε την είσοδο μόνο από το VPN του AUEB, δημιουργούμε έναν rich-rule, αφού πρώτα αφαιρέσουμε την υπηρεσία ssh από την public zone με την εντολή

   firewall-cmd --zone=public --remove-service=ssh

   Στις επιτρεπόμενες ip, προσθέτουμε την δική μας ip και αυτή που αναφέρεται στην εκφώνηση.

```
[root@snf-885682 ~]# firewall-cmd --zone=public --add-rich-rule=' rule family="ipv4" source address="195.251
.255.75" port protocol="tcp" port="22" accept'
success
[root@snf-885682 ~]# firewall-cmd --zone=public --add-rich-rule=' rule family="ipv4" source address="195.251
.255.77" port protocol="tcp" port="22" accept'
success
```

Μαρίνα Σαμπροβαλάκη
3180234

Μπορούμε να επαληθεύσουμε ότι οι πύλες είναι ανοικτές εκτελώντας

nmap 83.212.97.16

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-30 18:40 Libya Standard Time
Nmap scan report for snf-885682.vm.okeanos.grnet.gr (83.212.97.16)
Host is up (0.048s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-30 18:39 Libya Standard Time
Nmap scan report for snf-885682.vm.okeanos.grnet.gr (83.212.97.16)
Host is up (0.085s latency).
Not shown: 996 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
113/tcp closed ident
443/tcp open   https
```

Το port 22 είναι ανοικτό μόνο αν τρέξουμε **nmap 83.212.97.16** και είμαστε στο VPN του AUEB.

3. Μία Certificate Authority χρησιμοποιεί το δικό της private key για να υπογράφει τα πιστοποιητικά, συνεπώς πρέπει να δημιουργήσουμε ένα private key για την CA μας και στην συνέχεια να δημιουργήσουμε την CA μας. Στη συνέχεια, προχωράμε στο επόμενο βήμα που είναι η δημιουργία του Certificate Signing Request (CSR). Το CSR χρησιμοποιείται για να ζητήσουμε κάποιο πιστοποιητικό. Το αίτημα για πιστοποιητικό θα γίνει με το δικό μας private key, συνεπώς πρέπει πρώτα να δημιουργήσουμε ένα private key για εμάς και μετά να κάνουμε το αίτημα μας. Τέλος, θα ζητήσουμε μέσω του CSR ένα SSL Certificate το οποίο θα υπογράφεται από την CA μας. Είναι σημαντικό να αποθηκευτούν τα πιστοποιητικά μας σε ένα directory με chmod 700 ώστε μόνο ο owner να έχει πρόσβαση σε αυτά.

<u>Για το Certificate Authority:</u>
Η εντολή που θα χρησιμοποιήσουμε για το private key είναι η
openssl genrsa -des3 -out CAPrivate.key 2048
Η εντολή που θα χρησιμοποιήσουμε για το root certificate είναι η
openssl req -x509 -new -nodes -key CAPrivate.key -sha256 -days 365 -our CAPrivate.pem
Σε αυτό το σημείο πρέπει να αναφέρουμε ότι η προηγούμενη εντολή θα μας επιστρέψει κάποια πεδία για να συμπληρώσουμε, με το πιο σημαντικό το Organizational Unit Name όπου βάλαμε τον αριθμό μητρώου.

<u>Για το CSR:</u>
Η εντολή που θα χρησιμοποιήσουμε για το private key είναι η
openssl genrsa -out MyPrivate.key 2048
Η εντολή που θα χρησιμοποιήσουμε για να δημιουργήσουμε το CSR είναι η
openssl req -new -key MyPrivate.key -out MyRequest.csr
Σε αυτό το σημείο πρέπει να αναφέρουμε ότι η προηγούμενη εντολή θα μας επιστρέψει κάποια πεδία για να συμπληρώσουμε, με το πιο σημαντικό το Organizational Unit Name όπου βάλαμε τον αριθμό μητρώου.

Μαρίνα Σαμπροβαλάκη
3180234

Για το SSL:
Για να δημιουργήσουμε το πιστοποιητικό, χρησιμοποιήσαμε την εντολή
openssl x509 -req -in MyRequest.csr -CA CAPrivate.pem -CAkey CAPrivate.key -CAcreateserial -out X509Certificate.crt -days 365 -sha256

Βλέπουμε ότι **Signature ok** οπότε το πιστοποιητικό μας είναι έτοιμο.

4. Αρχικά ανοίγουμε το αρχείο index.html χρησιμοποιώντας την παρακάτω εντολή

```
sudo nano /var/www/html/index.html
```

Στην συνέχεια, χρησιμοποιήσαμε HTML και JavaScript για να φτιάξουμε ένα πεδίο για το username και ένα κουμπί submit. Μετέπειτα, φτιάξαμε μια συνάρτηση με όνομα isValid() η οποία ελέγχει αν το input που δίνει ο χρήστης είναι ίδιο με τον αριθμό μητρώου που του έχουμε δώσει, στην συγκεκριμένη περίπτωση είναι ο αριθμός 3180234. Αν είναι ίδιος εμφανίζεται alert με μήνυμα success, ενώ σε κάθε άλλη περίπτωση εμφανίζεται alert με μήνυμα fail.