ΕΡΓΑΣΙΑ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ 2022-2023

Συντελεστής: Καρλής Κωνσταντίνος(3190077)

1. Οι αλλαγές που έγιναν στο configuration του apache είναι οι εξής:
   i) yum install httpd
   ii) cd /etc/httpd
   iii) cd conf
   iv) ls
   v) vi httpd.conf
   vi) cd /var/www/html
   vii) vi index.html edit index.html
   viii) systemctl status firewalld
   ix) systemctl stop firewalld
   x) systemctl status firewalld
   xi) systemctl status httpd
   xii) systemctl start httpd
   xiii) systemctl enable httpd
   xiv) AFTER GO TO OUR BROWSER AND FILL OUR VM'S IP ADDRESS.
2. Τα rules που χρησιμοποιήθηκαν για το D είναι τα εξής:

```
[root@snf-890411 ~]# firewall-cmd --permanent --zone=public --add-service=http
Warning: ALREADY_ENABLED: http
success
[root@snf-890411 ~]# firewall-cmd --permanent --zone=public --add-service=https
Warning: ALREADY_ENABLED: https
success
[root@snf-890411 ~]# firewall-cmd --permanent --zone=public -add-source=195.51.255.75
usage: see firewall-cmd man page
firewall-cmd: error: unrecognized arguments: -add-source=195.51.255.75
[root@snf-890411 ~]# firewall-cmd --permanent --zone=public --add-source=195.51.255.75
success
[root@snf-890411 ~]# firewall-cmd --permanent --zone=public --add-source=172.39.59.90
Error: ZONE_CONFLICT: 172.39.59.90
[root@snf-890411 ~]# firewall-cmd --permanent --zone=public --remove-service=ssh
Warning: NOT_ENABLED: ssh
success
[root@snf-890411 ~]# firewall-cmd --permanent --zone=public --add-rich-rule='rule family="ipv
4" source address="195.251.255.75" service name="ssh" accept'
Warning: ALREADY_ENABLED: rule family="ipv4" source address="195.251.255.75" service name="ss
h" accept
success
[root@snf-890411 ~]# firewall-cmd --permanent --zone=public --add-rich-rule='rule family="ipv
4" source address="172.39.59.90" service name="ssh" accept'
Warning: ALREADY_ENABLED: rule family="ipv4" source address="172.39.59.90" service name="ssh"
 accept
success
[root@snf-890411 ~]# firewall-cmd --reload
success
[root@snf-890411 ~]#
```

   Τα warnings προκύπτουν επειδή τα έτρεξα συγκεντρωτικά ξανά για να τα έχω μαζεμμένα στο screenshot.
3. Το ερώτημα Ε υλοποιήθηκε ως εξής:
   i) Αρχικά έγινε εγκατάσταση του package openssl με την εντολή:

yum install -y openssl

Για να κάνουμε Public encryption χρειαζόμαστε ένα private key που θα χρησιμοποιηθεί στην δημιουργία του CA.Αυτό συμβαίνει με τις εξής εντολές:

- cd /etc/pki/CA/private/
- openssl genrsa -aes128 -out ourCA.key 2048

Έτσι,δημιουργήσαμε ένα ιδιωτικό κλειδί χρησιμοποιώντας τον αλγόριθμο RSA με μέγεθος κλειδιού 2048 bit για καλύτερη ασφάλεια.

Τώρα πάμε να δημιουργήσουμε την CA με τις εξής εντολές:.

- openssl req -new -x509 -days 1825 -key /etc/pki/CA/private/ourCA.key -out /etc/pki/CA/certs/ourCA.crt

ii) Για να δημιουργήσουμε το CSR εκτελέσαμε την παρακάτω εντολή:

- openssl req -new -key /etc/pki/tls/private/server.key -out /etc/pki/tls/server.csr

iii) Για να πάρουμε το SSL certificate πρώτα στέλνουμε το CSR για ψηφιακή υπογραφή και έπειτα εκτελούμε την υπογραφή του με τις εξής εντολές:

- scp /etc/pki/tls/server.csr root@83.212.106.77:~/server.csr
- openssl x509 -req -in server.csr -CA /etc/pki/CA/certs/ourCA.crt -CAkey /etc/pki/CA/private/ourCA.key -CAcreateserial -out server.crt -days 365

Τέλος,το μόνο που μένει είναι να τοποθετήσουμε το υπογεγραμμενο πιστοποιητικό στο ssl.conf αρχείο με τις εξής εντολές:

- vi /etc/httpd/conf.d/ssl.conf

Σε αυτό το αρχείο απλα θα κάνουμε update τις ακόλουθες τιμές.

SSLCertificateFile /etc/pki/tls/certs/server.crt

SSLCertificateKeyFile /etc/pki/tls/private/server.key

Κάνουμε restart τον apache server και τελειώσαμε.

- systemctl restart httpd.service

Σημείωση 1:Ενδιάμεσα έχουν εκτελεστεί και άλλες εντολές απλώς εδώ παραθέσαμε τις κυριότερες,για οποιαδήποτε απορία κοιτάξτε στο bash history του τελευταίου ερωτήματος.

Σημειώση 2:Στο Organization Unit name έχει χρησιμοποιηθεί ο AM:3190077

4. Η δημιουργία του website έγινε με την χρήση ενός αρχείου Html.Σε αυτό το αρχείο είναι προσαρμοσμένες εντολές css και js αρχείων.Αρχικά,δημιουργούμε το πλαίσιο για το id μας και το κουμπί submit.Με τις εντολές css απλα φτιάχνουμε λίγο το οπτικό και με το js ελέγχουμε το Input Που δίνει κάθε φορά ο χρήστης αν είναι το σωστό AM(3190077) τότε πετάμε alert(“login success”) αλλίως alert(“login fail”).Αυτό το html file το κάνουμε copy paste στο Index.html Που βρίσκεται στο /var/www/html.