Ασφάλεια Δικτύων - Άσκηση 3
Αργυρόπουλος Χρήστος - 3170010
Τσολάκου Διογένης - 3170164

Ερώτημα Α:

1. adduser teacher
2. mkdir /home/teacher/.ssh
3. chown -R teacher:teacher /home/teacher
4. chmod 705 -R /home
5. chmod 705 -R /root

Ερώτημα Β:

1. sudo yum install httpd
2. sudo firewall-cmd --permanent --add-service=http
3. sudo firewall-cmd --permanent --add-service=https
4. sudo firewall-cmd --reload
5. sudo systemctl start http

Ερώτημα C:

1. firewall-cmd --permanent --remove-service=ssh
2. firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source address="195.251.255.77" port port=22 protocol="tcp" accept'
3. firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source address="195.251.255.75" port port=22 protocol="tcp" accept'

```
[root@snf-883459 services]# firewall-cmd --permanent --remove-service=ssh
success
```

```
[root@snf-883459 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0 eth1
  sources:
  services: dhcpv6-client http https
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
        rule family="ipv4" source address="195.251.255.77" port port="22" protocol="tcp" accept
        rule family="ipv4" source address="195.251.255.75" port port="22" protocol="tcp" accept
[root@snf-883459 ~]#
```

Ερώτημα D:

1. yum install -y openssl
2. openssl genrsa -aes128
   -out /etc/pki/CA/private/team28CA.key 2048
3. openssl req -new -x509 -days 1825
   -key /etc/pki/CA/private/team28CA.key
   -out /etc/pki/CA/certs/team28CA.crt
4. yum install -y mod_ssl
5. openssl genrsa
   -out /etc/pki/tls/private/team28website.key 1024
6. openssl req -new
   -key /etc/pki/tls/private/team28website.key
   -out /etc/pki/tls/team28website.csr
7. openssl x509 -req
   -in /etc/pki/tls/team28website.csr
   -CA /etc/pki/CA/certs/team28CA.crt
   -CAkey /etc/pki/CA/private/team28CA.key -CAcreateserial
   -out /etc/pki/tls/certs/team28website.crt -days 365
8. systemctl restart httpd.service
9. firewall-cmd --reload

Αρχικά εγκαταστήσαμε το openssl package[1] και δημιουργήσαμε το κλειδί του Certificate Authority (CA)[2]. Έπειτα με αυτό το κλειδί παράξαμε το πιστοποιητικό του CA με διάρκεια 5 χρόνων δίνοντας τα απαραίτητα στοιχεία[3]. Εγκαταστήσαμε το mod_ssl ώστε να κάνουμε τον Apache από HTTP σε HTTPS και να μπορεί να χρησιμοποιήσει το SSL certificate[4]. Δημιουργήσαμε το κλειδί της ιστοσελίδας[5] και το χρησιμοποιήσαμε για να παράξουμε το Certificate Signing Request (CSR) της ιστοσελίδας[6]. Στη συνέχεια, συνδυάσαμε το CSR με το πιστοποιητικό και το κλειδί του CA ώστε να παράξουμε το πιστοποιητικό της ιστοσελίδας με διάρκεια 1(ένα) έτος[7]. Τέλος, επεξεργαστήκαμε το δημιουργημένο ssl.conf αρχείο στο path /etc/httpd/conf.d/ βάζοντας τα path προς το πιστοποιητικό της ιστοσελίδας και το κλειδί της. Κάναμε restart το httpd service[8] και reload το firewall[9] ώστε να εφαρμοστούν οι αλλαγές μας.

Οι αλλαγές στο ssl.conf αρχείο μπορούν να φανούν στα screenshots του ερωτήματος Ε.

```
[root@snf-883459 ~]# cd /etc/pki/CA/private/
[root@snf-883459 private]# openssl genrsa -aes128 -out team28CA.key 2048
Generating RSA private key, 2048 bit long modulus
...........................+++
.+++
e is 65537 (0x10001)
Enter pass phrase for team28CA.key:
Verifying - Enter pass phrase for team28CA.key:
[root@snf-883459 private]# ls
team28CA.key
[root@snf-883459 private]# openssl req -new -x509 -days 1825 -key /etc/pki/CA/private/team28CA.key -out /etc/pki/CA/certs/team28CA.crt
Enter pass phrase for /etc/pki/CA/private/team28CA.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:GR
State or Province Name (full name) []:ATH
Locality Name (eg, city) [Default City]:.
Organization Name (eg, company) [Default Company Ltd]:AUEB
Organizational Unit Name (eg, section) []:team28
Common Name (eg, your name or your server's hostname) []:AUEBteam28
Email Address []:.
```

```
[root@snf-883459 CA]# openssl genrsa -out /etc/pki/tls/private/team28website.key 1024
Generating RSA private key, 1024 bit long modulus
....++++++
.........++++++
e is 65537 (0x10001)
[root@snf-883459 CA]# openssl req -new -key /etc/pki/tls/private/team28website.key -out /etc/pki/tls/team28website.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:GR
State or Province Name (full name) []:ATH
Locality Name (eg, city) [Default City]:.
Organization Name (eg, company) [Default Company Ltd]:AUEB
Organizational Unit Name (eg, section) []:team28
Common Name (eg, your name or your server's hostname) []:team28website
Email Address []:.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Ερώτημα E:

```
#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/team28website.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/team28website.key
```

```
<VirtualHost *:80>
  ServerName 83.212.110.142

  Redirect permanent / https://83.212.110.142
</VirtualHost>

<VirtualHost *:443>

# General setup for the virtual host, inherited from global configuration
DocumentRoot "/var/www/html"
ServerName 83.212.110.142
```

Ανακατεύθυνση από http σε https

Ερώτημα F:

Φτιάξαμε ένα html αρχείο στα Windows στο οποίο βάλαμε μία φόρμα υποβολής η οποία περιέχει ένα πεδίο για την εισαγωγή username και το κάναμε υποχρεωτικό (required). Βάλαμε και το απαιτούμενο κουμπί για την υποβολή του username και με μία απλή μέθοδο Javascript ελέγχουμε αν το δοσμένο username είναι το σωστό και εμφανίζει το κατάλληλο μήνυμα. Αφού ελέγξαμε τοπικά ότι η ιστοσελίδα λειτουργεί, αντιγράψαμε τον κώδικα σε ένα νέο αρχείο στο VM μας στο path /var/www/html με το όνομα index.html ώστε να λειτουργεί η ιστοσελίδα εισάγοντας την IP του VM μας σε κάποιον browser.