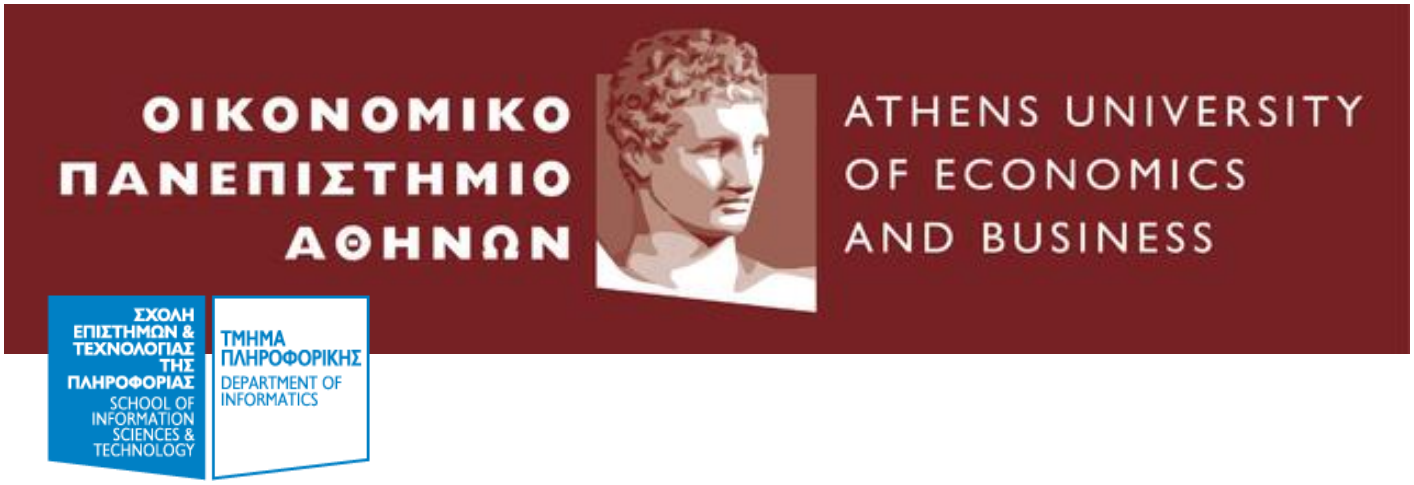

Ασφάλεια Δικτύων
Εργαστηριακή Άσκηση OpenSSL

Ευγένιος Γκρίτσης 3190045

1. Αλλαγές στο configuration του Apache

   - **Αλλαγή στο configuration (/etc/httpd/conf.d/ssl.conf) του Apache #1:**

     SSLCertificateFile /etc/pki/tls/certs/snf-890210.vm.okeanos.grnet.gr.crt

     SSLCertificateKeyFile /etc/pki/tls/private/snf-890210.vm.okeanos.grnet.gr.key

     SSLCertificateChainFile /etc/pki/tls/certs/rootCA.crt

   - **Αλλαγή στο configuration (/etc/httpd/conf.d/ssl.conf) του Apache #2:**
     Προσθήκη του εξής κώδικα

```
<VirtualHost *:80>
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</VirtualHost>
```

2. Screenshot των rules του ερωτήματος (D)

Αρχικά για το public zone απαγορεύουμε την υπηρεσία ssh:

```
[root@snf-890210 firewalld]# firewall-cmd --zone=public --remove-service=ssh
success
```

```
[root@snf-890210 firewalld]# firewall-cmd --zone=public --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:
```

Στην συνέχεια για το internal zone:

```
[root@snf-890210 firewalld]# firewall-cmd --zone=internal --add-source=195.251.255.75
success
[root@snf-890210 firewalld]# firewall-cmd --zone=internal --add-source=195.251.255.77
success
```

```
[root@snf-890210 firewalld]# firewall-cmd --zone=public --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0 eth1
  sources:
  services: dhcpv6-client http https ssh
  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
```

3. Υλοποίηση ερωτήματος (E)

Για την δημιουργία CA, CSR και SSL Certificate με openssl ακολουθήθηκαν τα εξής βήματα:

a. **Δημιουργία ιδιωτικού κλειδιού για το domain snf-890210.vm.okeanos.grnet.gr:**
openssl genrsa -des3 -out snf-890210.vm.okeanos.grnet.gr.key 2048

(#passphrase=1234)

b. **Δημιουργία ενός Certificate Signing Request (CSR):**
openssl req -key snf-890210.vm.okeanos.grnet.gr.key -new -out snf-890210.vm.okeanos.grnet.gr.csr

c. **Δημιουργία ενός self-signed Certificate με το ήδη υπάρχων ιδιωτικό κλειδί και CSR που παρήχθησαν από τα προηγούμενα βήματα:**
openssl x509 -signkey snf-890210.vm.okeanos.grnet.gr.key -in snf-890210.vm.okeanos.grnet.gr.csr -req -days 365 -out snf890210.vm.okeanos.grnet.gr.crt

d. **Δημιουργία ενός self-signed Root CA:**
openssl req -x509 -sha256 -days 365 -newkey rsa:2048 -keyout rootCA.key -out rootCA.crt

e. **Υπογραφή του CSR με το νέο self-signed Root CA:**

- Δημιουργία νέου configuration text-file snf-890210.vm.okeanos.grnet.gr.ext με τις παρακάτω ρυθμίσεις εντός του:

  authorityKeyIdentifier=keyid,issuer

  basicConstraints=CA:FALSE

  subjectAltName = @alt_names
  [alt_names]
  DNS.1 = snf-890210.vm.okeanos.grnet.gr

- Στην συνέχεια υπογράφουμε το CSR με το Root CA certificate και το private key του:
  openssl x509 -req -CA rootCA.crt -CAkey rootCA.key -in snf-890210.vm.okeanos.grnet.gr.csr -out snf-890210.vm.okeanos.grnet.gr.crt -days 365 -CAcreateserial -extfile snf-890210.vm.okeanos.grnet.gr.ext

Στην συνέχεια, εφαρμόζονται τα παρακάτω βήματα με στόχο διαμόρφωση του Apache HTTP Server για χρήση πιστοποιητικών SSL:

I. **Εγκατάσταση mod_ssl:**

```
yum install -y mod_ssl
```

II. **Τροποποίηση των ρυθμίσεων του SSL configuration file (/etc/httpd/conf.d/ssl.conf) ως εξής:**

```
SSLCertificateFile /etc/pki/tls/certs/snf-890210.vm.okeanos.grnet.gr.crt
SSLCertificateKeyFile /etc/pki/tls/private/snf-890210.vm.okeanos.grnet.gr.key
SSLCertificateChainFile /etc/pki/tls/certs/rootCA.crt
```

4. Υλοποίηση ερωτήματος (F)

Για να σερβίρει ο Apache Web Server το πιστοποιητικό μας σε HTTPS και να ανακατευθύνει τα HTTP σε HTTPS προστέθηκαν οι εξής αλλαγές στο /etc/httpd/conf.d/ssl.conf:

```
<VirtualHost *:80>
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</VirtualHost>
```

Το παραπάνω κομμάτι κώδικα είναι γραμμένο σε Apache configuration language. Συγκεκριμένα, ο virtualhost ακούει σε όλες τις διαθέσιμες IP διευθύνσεις (*) και στην θύρα 80 (:80). Η εντολή RewriteEnginer On ενεργοποιεί την μονάδα mod_rewrite του Apache, η οποία χρησιμοποιείται για την επανεγγραφή διευθύνσεων URL. Η λειτουργία RewriteCond ορίζει μια συνθήκη για την εντολή RewriteRule. Στην περίπτωση αυτή, η συνθήκη είναι όταν η σύνδεση HTTPS είναι απενεργοποιημένη -δηλαδή ο πελάτης δεν χρησιμοποιεί HTTPS- και με την εντολή RewriteRule ανακατευθύνεται η σύνδεση από HTTP σε HTTPS με αποτέλεσμα η κυκλοφορία μεταξύ του πελάτη και του διακομιστή να είναι κρυπτογραφημένη και ασφαλής.

Το SSL Certificate chain εμφανίζεται σωστά: