OpenSSL – Αναφορά εργασίας

Φίλιππος Δουραχαλής, 3170045, team23

Apache Configuration)

Αρχικά τροποποιούμε το αρχείο **/etc/httpd/conf.d/httpd.conf** που περιέχει το γενικό configuration του server μας (Virtual Host) που ακούει στη θύρα 80 (HTTP):

- Προσδιορίζουμε το domain name του server μέσω του πεδίου ServerName
- Προσθέτουμε τον κανόνα
  "Redirect / https://snf-883133.vm.okeanos.grnet.gr"
  ώστε όλα τα αιτήματα να ανακατευθύνονται στον virtual host που κάνει χρήση SSL.

Το configuration αυτό θα χρησιμοποιηθεί ώστε να φορτωθεί το configuration του virtual host με SSL όταν προσπαθήσουμε να συνδεθούμε με http.

Στη συνέχεια κάνουμε τις εξής αλλαγές στο αρχείο **/etc/httpd/conf.d/ssl.conf** που χρησιμοποιείται για το configuration των virtual hosts που ακούν στη θύρα 443 (HTTPS) για την επικοινωνία μέσω SSL. Σε αυτό το αρχείο για τον server μας:

- Ορίζουμε το ServerName όπως προηγουμένως
- Θέτουμε το DocumentRoot ίσο με το path στο οποίο περιέχονται τα αρχεία της σελίδας μας, δηλαδή "/var/www/html"
- Θέτουμε το SSLEngine ON ώστε ο server να σερβίρει τις σελίδες με SSL
- Ορίζουμε τη θέση του πιστοποιητικού του server με τον κανόνα
  "SSLCertificateFile /etc/pki/CA/certs/server.crt"
- Τέλος ορίζουμε τη θέση του private key του server που χρησιμοποιείται για την υπογραφή του πιστοποιητικού του με τον κανόνα
  "SSLCertificateKeyFile /etc/pki/CA/private/server.pem"

Επισκεπτόμενοι την σελίδα του server το certificate chain που εμφανίζεται είναι το εξής:

```
[root@snf-883133 ~]# openssl s_client -showcerts -connect snf-883133.vm.okeanos.grnet.gr:443
CONNECTED(00000003)
depth=1 C = GR, ST = Attiki, L = Marousi, O = AUEB, OU = team23, CN = snf-883133.vm.okeanos.grnet.gr, emailAddress = p3170045@au
eb.gr
verify return:1
depth=0 C = GR, ST = Attiki, O = AUEB, OU = team23, CN = snd-883133.vm.okeanos.grnet.gr, emailAddress = p3170045@aueb.gr
verify return:1
---
Certificate chain
 0 s:/C=GR/ST=Attiki/O=AUEB/OU=team23/CN=snd-883133.vm.okeanos.grnet.gr/emailAddress=p3170045@aueb.gr
   i:/C=GR/ST=Attiki/L=Marousi/O=AUEB/OU=team23/CN=snf-883133.vm.okeanos.grnet.gr/emailAddress=p3170045@aueb.gr
-----BEGIN CERTIFICATE-----
MIIEHDCCAwSgAwIBAgIDIyMjMA0GCSqGSIb3DQEBCwUAMIGaMQswCQYDVQQGEwJH
UjEPMA0GA1UECAwGQXR0aWtpMRAwDgYDVQQHDAdNYXJvdXNpMQ0wCwYDVQQKDARB
VUVCMQ8wDQYDVQQLDAZ0ZWFtMjMxJzAlBgNVBAMMHnNuZi04ODMxMzMudm0ub2tl
YW5vcy5ncm5ldC5ncjEfMB0GCSqGSIb3DQEJARYQcDMxNzAwNDVAYXVlYi5ncjAe
Fw0yMTA1MTkxODA1NTlaFw0yMjA1MTkxODA1NTlaMIGIMQswCQYDVQQGEwJHUjEP
MA0GA1UECAwGQXR0aWtpMQ0wCwYDVQQKDARBVUVCMQ8wDQYDVQQLDAZ0ZWFtMjMx
JzAlBgNVBAMMHnNuZC04ODMxMzMudm0ub2tlYW5vcy5ncm5ldC5ncjEfMB0GCSqG
SIb3DQEJARYQcDMxNzAwNDVAYXVlYi5ncjCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAORz4VhtjeqBRmB+TWsZ2koLzKtGbmQHLHgJ/JG7MB0QiVpB8al8
T/jaqD8tAcH7WN1vuB8zHnFmePfaRFZwYemM5yI0uEWusPdBfRitsJqE+cveT+SD
Dunbgf6XUrYdzENs5wh0opxZo6yYuxh3Ou4ky3fzAmBdimNI9R2ZosNFxdyEO1Bp
L+A33SWJiTC25dQipVjePISsX8W19qZxupJM8x882Ns51EH7XAqrS2dWMeqEBiVU
OZzq0s7e1oWWPniq4Xy2kE/BgtIXGSO7FGap/am2DPKUnvbxswYJh95JGghKtKPh
FQE1yRPjMIFP4xGFch+Sj7K/ylLnrFkd4QsCAwEAAaN7MHkwCQYDVR0TBAIwADAs
BglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYD
VR0OBBYEFHLxjOZur4bblNwvTUx+nLtvuE98MB8GA1UdIwQYMBaAFLyPljQcO0xc
toJdOFlG79ErZNr2MA0GCSqGSIb3DQEBCwUAA4IBAQAvH5JnxrL/5OyaSOfqwdHh
oZ2f9RQSQDuml0IllKi8evCI/nUPzK3X7FdqrvOGUI5K479zACfxc20yZxojGK0U
IXZ4XW3mfvvwLckOsILXPJtDJgBLIWkNGCK5U7Z3HGIEjMl5AVhSfHGkkW2OXBHe
9cGEnu8J+gSVlNKSwG41F7W/bRp7N2FD0SNDfuRZn7gCy+6sYmY6LPXGiap3hXfb
l7nVCd/uWqKg/zhJQ/T0ioHlRcnKvxLQDFbDecVmzp8ZJkRNDm2RiBOHYEnGDSm8
hP5B8zjAmbmHMq8qeSrum+BOxKiFggKBq6oTAumEYTI5HZxrSoCT5uDU/62EkYbQ
-----END CERTIFICATE-----
---
Server certificate
subject=/C=GR/ST=Attiki/O=AUEB/OU=team23/CN=snd-883133.vm.okeanos.grnet.gr/emailAddress=p3170045@aueb.gr
issuer=/C=GR/ST=Attiki/L=Marousi/O=AUEB/OU=team23/CN=snf-883133.vm.okeanos.grnet.gr/emailAddress=p3170045@aueb.gr
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 1747 bytes and written 415 bytes
```

Firewall Rules)

Τροποποιούμε κατάλληλα τις ζώνες public και internal του firewall.

1. Ζώνη Public
   Η συγκεκριμένη ζώνη προορίζεται για χρήση σε δημόσια δίκτυα όπου δεν εμπιστευόμαστε τους υπόλοιπους υπολογιστές.
   Εδώ ορίζουμε κανόνες ώστε να επιτρέπονται οι συνδέσεις http και https (ports 80 και 443) από όλες τις IP, όπως φαίνεται στην εικόνα:

```
<?xml version="1.0" encoding="utf-8"?>
<zone>
  <short>Public</short>
  <description>For use in public areas. You do not trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.</description>
  <service name="dhcpv6-client"/>
  <service name="ftp"/>
  <service name="http"/>
  <service name="https"/>
  <port protocol="tcp" port="80"/>
  <port protocol="tcp" port="443"/>
  <port protocol="tcp" port="21"/>
</zone>
```

2. Ζώνη Internal
   Σε αυτή τη ζώνη προσθέτουμε κανόνες που αφορούν την επικοινωνία με υπολογιστές που εμπιστευόμαστε. Επομένως ορίζουμε ο server να αποδέχεται συνδέσεις ssh από τις δύο IP που προσδιορίζουμε:

```
<?xml version="1.0" encoding="utf-8"?>
<zone>
  <short>Internal</short>
  <description>For use on internal networks. You mostly trust the other computers on the networks to not harm your computer. Only selected incoming connections are accepted.</description>
  <source address="195.251.255.77"/>
  <source address="130.43.62.33"/>
  <service name="ssh"/>
  <service name="mdns"/>
  <service name="samba-client"/>
  <service name="dhcpv6-client"/>
</zone>
```

Certificates)

1. Αρχικά δημιουργούμε το ζεύγος δημοσίου-ιδιωτικού κλειδιού της Certificate Authority (CA), με την εντολή:

   “openssl genrsa -aes256 -out /etc/pki/CA/private/cakey.pem”

2. Στη συνέχεια δημιουργούμε και το πιστοποιητικό της CA με το ιδιωτικό κλειδί που μόλις δημιουργήσαμε, εισάγοντας τα απαραίτητα στοιχεία. Εφόσον δεν προσδιορίσαμε ημερομηνία λήξης, το πιστοποιητικό θα είναι έγκυρο για 30 μέρες:

   “openssl req -new -x509 -key /etc/pki/CA/private/cakey.pem -out /etc/pki/CA/cacert.pem”

3. Έχοντας δημιουργήσει τη δική μας CA, προχωράμε στην δημιουργία ενός δημοσίου και ιδιωτικού κλειδιού μήκους 2048 bits για τον server:

   “openssl genrsa -aes256 -out /etc/pki/CA/requests/server.pem 2048”

4. Εκδίδουμε ένα Αίτημα Υπογραφής Πιστοποιητικού (CSR), που θα σταλεί στο επόμενο βήμα στην CA, με την εντολή:

   “openssl req -new -key /etc/pki/CA/requests/server.pem -out /etc/pki/CA/requests/server.csr”

5. Τέλος στέλνουμε το αίτημα στην CA ώστε να το υπογράψει και να λάβουμε το υπογεγραμμένο πιστοποιητικό (SSL Certificate) του server :

   “openssl ca -in /etc/pki/CA/requests/server.csr -out /etc/pki/CA/requests/server.crt”

HTML)

Για την δημιουργία του site, χρησιμοποιήθηκε μια απλή φόρμα html η οποία περιέχει ένα πεδίο input, όπου ο χρήστης δίνει τον κωδικό ή το όνομα της ομάδας, και ένα κουμπί για την υποβολή της φόρμας. Επίσης κάτω από την φόρμα έχουν οριστεί δύο ακόμα στοιχεία: Ένα στοιχείο div που περιλαμβάνει το κείμενο που θα εμφανίζεται κατά την υποβολή και μια εικόνα η οποία εμφανίζεται αν δοθεί η σωστή τιμή. Στο ίδιο html έγγραφο έχει οριστεί και ένα script το οποίο ελέγχει την ορθότητα της εισόδου που δόθηκε στη φόρμα. Στο script έχουμε έναν listener στο κουμπί υποβολής, ώστε όταν ο χρήστης το πατήσει να εκτελεστεί μια συνάρτηση, η οποία ελέγχει αν η τιμή που δόθηκε στο πεδίο αντιστοιχεί στην ομάδα 23. Αν ναι, εμφανίζει κατάλληλο μορφοποιημένο μήνυμα επιτυχίας στο στοιχείο div

καθώς και την εικόνα. Αν όχι, εμφανίζει μήνυμα αποτυχίας (Η εικόνα παραμένει κρυμμένη μέχρι να δοθεί η σωστή είσοδος). Τέλος δημιουργούμε και ένα αρχείο css για να δώσουμε στυλ στην φόρμα και να προσδιορίσουμε την διάταξή της για να εμφανίζεται στο κέντρο της οθόνης.

Βάζουμε τα αρχεία .html, .css και την εικόνα στον φάκελο /var/www/html που έχουμε προσδιορίσει και στο ssl.conf ώστε ο server να εμφανίζει τη σελίδα μας.