ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΕΡΓΑΣΙΑ ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Ονοματεπώνυμα :

Ελευθερία Τζαχρήστου

Αριθμός Μητρώου:

21390219

Ημερομηνία Παράδοσης:16/6/2024

ΠΕΡΙΕΧΟΜΕΝΑ

- **Δραστηριότητα 1: Δημιουργία Αρχής Πιστοποίησης**
- **Δραστηριότητα 2: Έκδοση πιστοποιητικού για πελάτη**
- **Δραστηριότητα 3: Χρήση του πιστοποιητικού σε δοκιμαστικό HTTPS Server**
- **Δραστηριότητα 4: Χρήση του πιστοποιητικού σε Apache HTTPS Web server**
- **Δραστηριότητα 5: Επίθεση τύπου Man-In-The-Middle**
- **Δραστηριότητα 6: Επίθεση τύπου Man-In-The-Middle σε περίπτωση παραβιασμένης ΑΠ**

Δραστηριότητα 1: Δημιουργία Αρχής Πιστοποίησης

Η δομή του καταλόγου /pki μετά την κατασκευή των καταλόγων και αρχείων

```
[05/31/24]seed@VM:~/.../pki$ ls -a
.   ..   openssl.cnf   seclabCA
[05/31/24]seed@VM:~/.../pki$ cd seclabCA/
[05/31/24]seed@VM:~/.../seclabCA$ ls -a
.   ..   certs   crl   index.txt   newcerts   serial
[05/31/24]seed@VM:~/.../seclabCA$
```

Κατασκευή αυτό-υπογεγραμμένου πιστοποιητικού της ΑΠ

$ openssl req -new -x509 -keyout ca.key -out ca.crt -days 365 -config openssl.cnf

```
[05/31/24]seed@VM:~/.../pki$ openssl req -new -x509 -keyout ca.key -out ca.crt -days 365 -config openssl.cnf
Generating a 2048 bit RSA private key
.....................+++
.....................................................+++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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) [AU]:GR
State or Province Name (full name) [Some-State]:ATTIKA
Locality Name (eg, city) []:AIGALEO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UNIWA
Organizational Unit Name (eg, section) []:ICE
Common Name (e.g. server FQDN or YOUR name) []:21390219.uniwa.gr
Email Address []:21390219@uniwa.gr
```

Το περιεχόμενο του πιστοποιητικού:

$ openssl x509 -in ca.crt -text –noout

```
[05/31/24]seed@VM:~/.../pki$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            e1:b7:47:aa:0e:cf:67:87
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GR, ST=ATTIKA, L=AIGALEO, O=UNIWA, OU=ICE, CN=21390219.uniwa.gr/emailAddress=21390219@uniwa.gr
        Validity
            Not Before: May 31 22:17:20 2024 GMT
            Not After : May 31 22:17:20 2025 GMT
        Subject: C=GR, ST=ATTIKA, L=AIGALEO, O=UNIWA, OU=ICE, CN=21390219.uniwa.gr/emailAddress=21390219@uniwa.gr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b3:4d:41:91:59:05:22:a6:1b:64:43:25:c8:61:
                    1c:64:5f:b4:99:9f:81:88:b6:ba:9e:6e:ea:b8:07:
                    cc:9f:75:97:3b:46:b6:ed:82:2d:07:27:52:12:76:
                    42:da:a6:7c:08:e2:1c:97:aa:55:41:72:ed:76:79:
                    fb:3e:de:53:33:b8:e4:2a:47:14:f0:06:e4:74:bf:
                    8a:8e:86:74:5f:99:b8:33:7e:46:d1:ef:41:06:98:
                    1a:fb:60:27:41:c7:d6:d9:47:e9:8a:ad:51:be:a5:
                    3c:46:cc:9d:db:14:41:57:f2:88:4f:aa:f5:2b:63:
                    c8:e4:57:18:66:76:fd:4b:a0:8a:d2:0e:3c:ad:98:
                    1d:fd:95:57:9b:b9:8e:02:71:8a:2e:75:37:66:6f:
                    46:45:b0:c8:0f:2e:6d:d2:c8:a7:e8:2f:d7:e5:6c:
                    31:97:8a:3a:de:d6:34:08:3c:ad:4e:c1:db:6e:a8:
                    e4:07:ec:f2:2c:8f:19:3d:bc:79:d2:aa:51:ab:37:
                    e9:0c:f9:be:2f:f9:d1:63:ad:00:30:df:83:34:71:
                    6d:aa:54:41:27:3f:98:c0:69:6c:d8:62:6a:88:b2:
                    c9:9e:81:2b:f1:31:b4:be:c0:da:74:61:43:9f:9c:
                    a7:2b:c7:91:1e:95:df:a6:1f:a0:b8:a7:55:7c:46:
```

Από τον file explorer του συστήματος βλέπουμε το περιεχόμενό του πιστοποιητικού στον κατάλληλο viewer:

eleftheria-tzachristou.com

Identity: eleftheria-tzachristou.com
Verified by: 21390219.uniwa.gr
Expires: 05/31/2025

▾ **Details**

Subject Name

C (Country):	US
ST (State):	NY
L (Locality):	NYC
O (Organization):	MyCompany
OU (Organizational Unit):	IT
CN (Common Name):	eleftheria-tzachristou.com
EMAIL (Email Address):	info@eleftheria-tzachristou.com

Issuer Name

C (Country):	GR
ST (State):	ATTIKA
L (Locality):	AIGALEO
O (Organization):	UNIWA
OU (Organizational Unit):	ICE
CN (Common Name):	21390219.uniwa.gr
EMAIL (Email Address):	21390219@uniwa.gr

Issued Certificate

Version:	3
Serial Number:	01
Not Valid Before:	2024-05-31
Not Valid After:	2025-05-31

Certificate Fingerprints

SHA1:	BB BA 19 E2 19 39 C1 B3 7B 06 3F 38 FB 93 5E D4 83 64 EA 14
MD5:	9A D5 3A 4E 37 97 E9 21 04 A2 1D ED DC 8C AB 51

Public Key Info

Key Algorithm:	RSA
Key Parameters:	05 00
Key Size:	1024
Key SHA1 Fingerprint:	74 75 1C FF 3D 55 D1 4F 5A 0E 6B 61 FC 91 61 30 39 47 5F C7
Public Key:	30 81 89 02 81 81 00 C7 02 4E F4 E2 87 C5 E0 0A 3F 93 DC 22 7D 6C B3 99 C9 41 58 91 D6 2D C4 46 B6 E3 B5 ED EF B7 F4 71 29 C7 AB 4B 20 B5 8E E3 34 E3 99 44 59 32 4C A5 B5 73 23 7E 56 52 1F 6E C6 89 9F FA DD 4F AF B4 23 E4 46 33 36 BD 35 CD 59 A9 72 36 00 DD BA 4E 32 49 D8 C3 2F CF 26 77 CA F2 AA A9 26 F2 50 ED 18 6E 16 BD 85 67 7A 25 E4 E6 8F E5 34 69 7C EE 89 2C DE CB B6 B8 42 9A 4E F9 C5 4C 9B E7 3D 02 03 01 00 01

Δραστηριότητα 2: Έκδοση πιστοποιητικού για πελάτη

Δημιουργούμε το ζεύγος κλειδιών RSA με την ακόλουθη εντολή στο terminal (μέσα στον κατάλογο /pki).

$ openssl genrsa -aes128 -out server.key 1024

```
[05/31/24]seed@VM:~/.../pki$ openssl genrsa -aes128 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
.................................++++++
.....................++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
```

Βλέπουμε ότι η ενέργεια είναι επιτυχής ,καθώς έχει δημιουργηθεί το αρχείο server.key

```
[05/31/24]seed@VM:~/.../pki$ ls -a
.  ..  ca.crt  ca.key  openssl.cnf  seclabCA  server.key
```

Το αρχείο server.key είναι ένα κρυπτογραφημένο αρχείο, κάτι που σημαίνε ότι δεν θα μπορούμε να δούμε το περιεχόμενο (όπως το modulus N, τα κλειδιά e, d, κ.λπ). Έτσι εκτελούμε την ακόλουθη εντολή στην οποία δίνουμε τον κωδικό πρόσβασης:

$ openssl rsa -in server.key -text

```
[05/31/24]seed@VM:~/.../pki$ openssl rsa -in server.key -text
Enter pass phrase for server.key:
Private-Key: (1024 bit)
modulus:
    00:c7:02:4e:f4:e2:87:c5:e0:0a:3f:93:dc:22:7d:
    6c:b3:99:c9:41:58:91:d6:2d:c4:46:b6:e3:b5:ed:
    ef:b7:f4:71:29:c7:ab:4b:20:b5:8e:e3:34:e3:99:
    44:59:32:4c:a5:b5:73:23:7e:56:52:1f:6e:c6:89:
    9f:fa:dd:4f:af:b4:23:e4:46:33:36:bd:35:cd:59:
    a9:72:36:00:dd:ba:4e:32:49:d8:c3:2f:cf:26:77:
    ca:f2:aa:a9:26:f2:50:ed:18:6e:16:bd:85:67:7a:
    25:e4:e6:8f:e5:34:69:7c:ee:89:2c:de:cb:b6:b8:
    42:9a:4e:f9:c5:4c:9b:e7:3d
publicExponent: 65537 (0x10001)
privateExponent:
    0c:ad:81:f8:29:c2:3a:81:d6:45:4c:97:16:7f:65:
    00:60:08:a9:28:0a:4a:59:aa:0a:53:36:58:6d:aa:
    fa:ce:10:b3:77:ab:da:e2:5f:8e:95:bc:d5:ce:fa:
    c2:af:e8:a0:19:da:16:e5:c2:7c:02:d2:9c:c5:41:
    b2:ca:8c:7b:e9:3a:6b:dd:1d:61:eb:bb:78:bd:94:
    b2:fc:04:ee:ef:58:32:97:ba:ac:79:17:e4:72:b9:
    16:b3:4d:4a:fb:7c:4e:c2:32:6b:f9:e1:c4:92:82:
    5d:99:92:d9:fd:71:3a:06:6d:4e:80:42:db:42:63:
    16:e8:ac:5c:9b:e0:bb:25
prime1:
    00:e7:86:fb:d6:1f:12:aa:0b:d7:68:ea:ae:5d:c2:
    a2:c2:d3:df:da:a0:9e:d5:57:14:7d:d9:3b:8b:9f:
    17:0b:bd:58:88:a1:5c:bd:37:8b:d2:1a:9d:e5:6e:
    c7:4b:0d:c1:87:16:c3:e8:82:74:8f:83:29:32:50:
    83:6b:ec:13:07
prime2:
    00:dc:0b:65:6e:58:c0:bb:d2:ec:20:5c:9f:60:cd:
    49:5b:f8:06:c5:f7:8f:fa:ca:a1:aa:a0:c0:1c:67:
    2f:8d:d5:1d:15:a4:fb:78:31:fd:fa:26:dd:0d:3e:
    15:dc:68:36:4e:29:ef:f2:b5:34:d6:9f:5a:ce:96:
    6a:64:ce:0e:9b
```

Δημιουργούμε αίτημα υπογραφής πιστοποιητικού (CSR)

Εκτελούμε την ακόλουθη εντολή στο terminal (μέσα στον κατάλογο /pki)

$ openssl req -new -key server.key -out server.csr -config openssl.cnf

```
[05/31/24]seed@VM:~/.../pki$ openssl req -new -key server.key -out server.csr -config openssl.cnf
Enter pass phrase for server.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) [AU]:US
State or Province Name (full name) [Some-State]:NY
Locality Name (eg, city) []:NYC
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MyCompany
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:eleftheria-tzachristou.com
Email Address []:info@eleftheria-tzachristou.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[05/31/24]seed@VM:~/.../pki$
```

Εφόσον η διαδικασία πραγματοποιηθεί , θα έχει δημιουργηθεί το αρχείο server.csr. Μπορούμε να το δούμε με την εντολή:

$ openssl req -text -noout -verify -in server.cs

```
[05/31/24]seed@VM:~/.../pki$ openssl req -text -noout -verify -in server.csr
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, ST=NY, L=NYC, O=MyCompany, OU=IT, CN=eleftheria-tzachristou.com/emailAddress=info@eleftheria-tzachristou.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c7:02:4e:f4:e2:87:c5:e0:0a:3f:93:dc:22:7d:
                    6c:b3:99:c9:41:58:91:d6:2d:c4:46:b6:e3:b5:ed:
                    ef:b7:f4:71:29:c7:ab:4b:20:b5:8e:e3:34:e3:99:
                    44:59:32:4c:a5:b5:73:23:7e:56:52:1f:6e:c6:89:
                    9f:fa:dd:4f:af:b4:23:e4:46:33:36:bd:35:cd:59:
                    a9:72:36:00:dd:ba:4e:32:49:d8:c3:2f:cf:26:77:
                    ca:f2:aa:a9:26:f2:50:ed:18:6e:16:bd:85:67:7a:
                    25:e4:e6:8f:e5:34:69:7c:ee:89:2c:de:cb:b6:b8:
                    42:9a:4e:f9:c5:4c:9b:e7:3d
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         86:46:f4:ef:a2:89:06:ae:22:19:8a:80:7c:2e:8e:bd:ed:d2:
         ba:c1:87:61:28:d0:f5:3a:cb:c1:c2:fe:83:53:aa:85:93:68:
         a4:d9:93:f5:8a:35:79:03:e3:fb:32:8b:4a:b1:97:50:e6:2a:
         f3:e8:e4:3a:77:06:90:41:88:19:1b:e9:47:78:f2:49:4e:ba:
         85:60:ea:b7:fa:b6:81:6a:e1:d0:78:4b:22:49:aa:16:0d:05:
         98:37:20:1c:b7:ce:40:f3:81:c9:98:99:57:c4:59:fe:b1:ae:
         59:27:8a:cd:83:45:11:06:b8:42:16:71:87:e8:75:a3:21:66:
         d9:a2
```

Εκδίδουμε πιστοποιητικό για τον πελάτη

$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf

```
[05/31/24]seed@VM:~/.../pki$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: May 31 22:43:41 2024 GMT
            Not After : May 31 22:43:41 2025 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = NY
            localityName              = NYC
            organizationName          = MyCompany
            organizationalUnitName    = IT
            commonName                = eleftheria-tzachristou.com
            emailAddress              = info@eleftheria-tzachristou.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                5E:33:8D:19:0E:52:EE:4E:34:7D:0C:96:DC:D2:46:87:37:B5:B3:26
            X509v3 Authority Key Identifier:
                keyid:82:96:C8:F7:DD:4D:C9:64:4E:F0:55:98:D8:9B:A0:6D:EC:8E:1D:2C

Certificate is to be certified until May 31 22:43:41 2025 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Όταν η διαδικασία ολοκληρωθεί , τότε δημιουργείται το πιστοποιητικό του πελάτη (αρχείο server.crt), το οποίο μπορούμε να δούμε με την εντολή:

$ openssl x509 -in server.crt -text –noout

```
[05/31/24]seed@VM:~/.../pki$ openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GR, ST=ATTIKA, L=AIGALEO, O=UNIWA, OU=ICE, CN=21390219.uniwa.gr/emailAddress=21390219@uniwa.gr
        Validity
            Not Before: May 31 22:43:41 2024 GMT
            Not After : May 31 22:43:41 2025 GMT
        Subject: C=US, ST=NY, L=NYC, O=MyCompany, OU=IT, CN=eleftheria-tzachristou.com/emailAddress=info@eleftheria-tzachristou.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c7:02:4e:f4:e2:87:c5:e0:0a:3f:93:dc:22:7d:
                    6c:b3:99:c9:41:58:91:d6:2d:c4:46:b6:e3:b5:ed:
                    ef:b7:f4:71:29:c7:ab:4b:20:b5:8e:e3:34:e3:99:
                    44:59:32:4c:a5:b5:73:23:7e:56:52:1f:6e:c6:89:
                    9f:fa:dd:4f:af:b4:23:e4:46:33:36:bd:35:cd:59:
                    a9:72:36:00:dd:ba:4e:32:49:d8:c3:2f:cf:26:77:
                    ca:f2:aa:a9:26:f2:50:ed:18:6e:16:bd:85:67:7a:
                    25:e4:e6:8f:e5:34:69:7c:ee:89:2c:de:cb:b6:b8:
                    42:9a:4e:f9:c5:4c:9b:e7:3d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                5E:33:8D:19:0E:52:EE:4E:34:7D:0C:96:DC:D2:46:87:37:B5:B3:26
            X509v3 Authority Key Identifier:
                keyid:82:96:C8:F7:DD:4D:C9:64:4E:F0:55:98:D8:9B:A0:6D:EC:8E:1D:2C

    Signature Algorithm: sha256WithRSAEncryption
```

Το αρχείο κάθως ανοίγουμε τον file explorer και βλέπουμε το περιεχόμενό του στον κατάλληλο viewer:

eleftheria-tzachristou.com

Identity: eleftheria-tzachristou.com
Verified by: 21390219.uniwa.gr
Expires: 05/31/2025

▾ **Details**

Subject Name

C (Country):	US
ST (State):	NY
L (Locality):	NYC
O (Organization):	MyCompany
OU (Organizational Unit):	IT
CN (Common Name):	eleftheria-tzachristou.com
EMAIL (Email Address):	info@eleftheria-tzachristou.com

Issuer Name

C (Country):	GR
ST (State):	ATTIKA
L (Locality):	AIGALEO
O (Organization):	UNIWA
OU (Organizational Unit):	ICE
CN (Common Name):	21390219.uniwa.gr
EMAIL (Email Address):	21390219@uniwa.gr

Issued Certificate

Version:	3
Serial Number:	01
Not Valid Before:	2024-05-31
Not Valid After:	2025-05-31

Certificate Fingerprints

SHA1:	BB BA 19 E2 19 39 C1 B3 7B 06 3F 38 FB 93 5E D4 83 64 EA 14
MD5:	9A D5 3A 4E 37 97 E9 21 04 A2 1D ED DC 8C AB 51

Public Key Info

Key Algorithm:	RSA
Key Parameters:	05 00
Key Size:	1024
Key SHA1 Fingerprint:	74 75 1C FF 3D 55 D1 4F 5A 0E 6B 61 FC 91 61 30 39 47 5F C7
Public Key:	30 81 89 02 81 81 00 C7 02 4E F4 E2 87 C5 E0 0A 3F 93 DC 22 7D 6C B3 99 C9 41 58 91 D6 2D C4 46 B6 E3 B5 ED EF B7 F4 71 29 C7 AB 4B 20 B5 8E E3 34 E3 99 44 59 32 4C A5 B5 73 23 7E 56 52 1F 6E C6 89 9F FA DD 4F AF B4 23 E4 46 33 36 BD 35 CD 59 A9 72 36 00 DD BA 4E 32 49 D8 C3 2F CF 26 77 CA F2 AA A9 26 F2 50 ED 18 6E 16 BD B5 67 7A 25 E4 E6 8F E5 34 69 7C EE 89 2C DE CB B6 B8 42 9A 4E F9 C5 4C 9B E7 3D 02 03 01 00 01

Δραστηριότητα 3: Χρήση του πιστοποιητικού σε δοκιμαστικό HTTPS Server

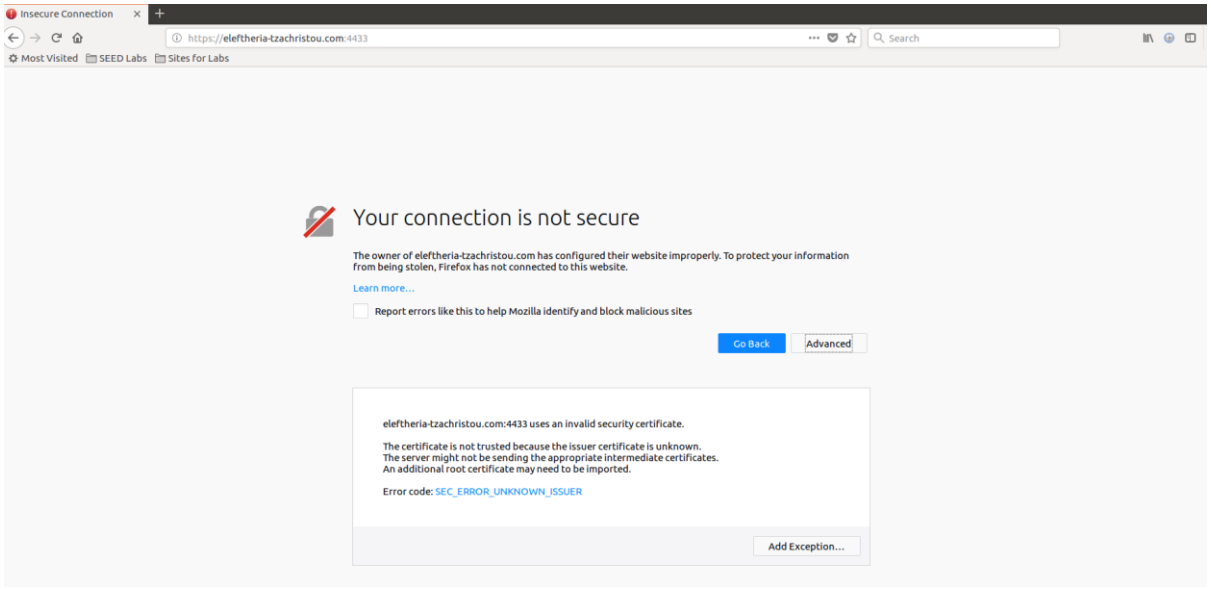
Διαμορφώνουμε DNS

Στην συνέχεια διαμορφώνουμε web server και δοκιμάζουμε

```
[05/31/24]seed@VM:~/.../pki$ cp server.key server.pem
[05/31/24]seed@VM:~/.../pki$ cat server.crt >> server.pem
[05/31/24]seed@VM:~/.../pki$ ls -a
.   ca.crt  openssl.cnf  server.crt  server.key
..  ca.key  seclabCA     server.csr  server.pem
[05/31/24]seed@VM:~/.../pki$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
```

Βλέπουμε την ένδειξη ACCEPT, κάτι που σημαίνει οτι server είναι σε λειτουργία και περιμένει εισερχόμενα αιτήματα. Δοκιμάζουμε, χρησιμοποιώντας την ακόλουθη διεύθυνση URL στον browser:

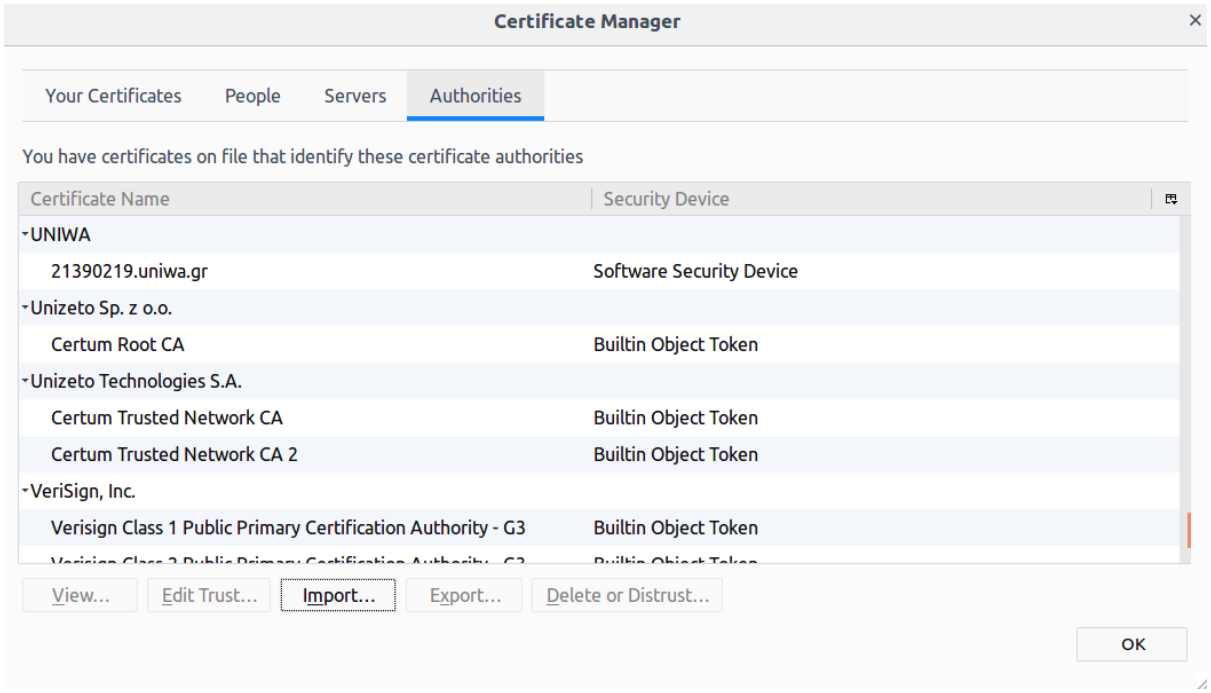
https://eleftheria-tzachristou.com:4433/



Πραγματοποιήση αποδοχής του πιστοποιητικού της ΑΠ από το πρόγραμμα περιήγησης

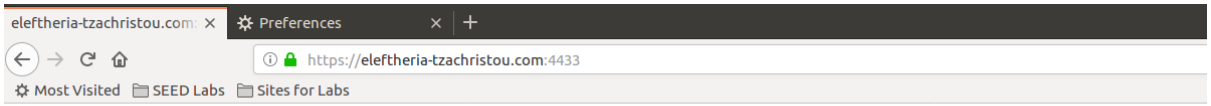
Προσθέτουμε χειροκίνητα το πιστοποιητικό της δικής σας ΑΠ (ca.crt) στο πρόγραμμα περιήγησης Firefox, κάνοντας κλικ στην ακόλουθη σειρά μενού: Edit -> Preferences -> Privacy & Security -> View Certificates

Εμφανίζετε μια λίστα με τα πιστοποιητικά που είναι ήδη αποδεκτά από τον Firefox και εισάγουμε το δικό μας πιστοποιητικό.



Το πιστοποιητικό της ΑΠ σας βρίσκεται στη λίστα των έμπιστων πιστοποιητικών του Firefox.

Δοκιμάζουμε ασφαλούς website




```
s_server -cert server.pem -www
Secure Renegotiation IS supported
Ciphers supported in s_server binary
TLSv1/SSLv3:ECDHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDHE-ECDSA-AES256-GCM-SHA384
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA384  TLSv1/SSLv3:ECDHE-ECDSA-AES256-SHA384
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES256-SHA
TLSv1/SSLv3:SRP-DSS-AES-256-CBC-SHA  TLSv1/SSLv3:SRP-RSA-AES-256-CBC-SHA
TLSv1/SSLv3:SRP-AES-256-CBC-SHA      TLSv1/SSLv3:DH-DSS-AES256-GCM-SHA384
TLSv1/SSLv3:DHE-DSS-AES256-GCM-SHA384TLSv1/SSLv3:DH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3:DHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:DHE-RSA-AES256-SHA256
TLSv1/SSLv3:DHE-DSS-AES256-SHA256    TLSv1/SSLv3:DH-RSA-AES256-SHA256
TLSv1/SSLv3:DH-DSS-AES256-SHA256     TLSv1/SSLv3:DHE-RSA-AES256-SHA
TLSv1/SSLv3:DHE-DSS-AES256-SHA       TLSv1/SSLv3:DH-RSA-AES256-SHA
TLSv1/SSLv3:DH-DSS-AES256-SHA        TLSv1/SSLv3:DHE-RSA-CAMELLIA256-SHA
TLSv1/SSLv3:DHE-DSS-CAMELLIA256-SHA  TLSv1/SSLv3:DH-RSA-CAMELLIA256-SHA
TLSv1/SSLv3:DH-DSS-CAMELLIA256-SHA   TLSv1/SSLv3:ECDH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3:ECDH-ECDSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDH-RSA-AES256-SHA384
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA384 TLSv1/SSLv3:ECDH-RSA-AES256-SHA
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA    TLSv1/SSLv3:AES256-GCM-SHA384
TLSv1/SSLv3:AES256-SHA256            TLSv1/SSLv3:AES256-SHA
TLSv1/SSLv3:CAMELLIA256-SHA          TLSv1/SSLv3:PSK-AES256-CBC-SHA
TLSv1/SSLv3:ECDHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:ECDHE-ECDSA-AES128-GCM-SHA256
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA256  TLSv1/SSLv3:ECDHE-ECDSA-AES128-SHA256
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES128-SHA
TLSv1/SSLv3:SRP-DSS-AES-128-CBC-SHA  TLSv1/SSLv3:SRP-RSA-AES-128-CBC-SHA
TLSv1/SSLv3:SRP-AES-128-CBC-SHA      TLSv1/SSLv3:DH-DSS-AES128-GCM-SHA256
TLSv1/SSLv3:DHE-DSS-AES128-GCM-SHA256TLSv1/SSLv3:DH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3:DHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:DHE-RSA-AES128-SHA256
TLSv1/SSLv3:DHE-DSS-AES128-SHA256    TLSv1/SSLv3:DH-RSA-AES128-SHA256
TLSv1/SSLv3:DH-DSS-AES128-SHA256     TLSv1/SSLv3:DHE-RSA-AES128-SHA
TLSv1/SSLv3:DHE-DSS-AES128-SHA       TLSv1/SSLv3:DH-RSA-AES128-SHA
TLSv1/SSLv3:DH-DSS-AES128-SHA        TLSv1/SSLv3:DHE-RSA-SEED-SHA
TLSv1/SSLv3:DHE-DSS-SEED-SHA         TLSv1/SSLv3:DH-RSA-SEED-SHA
TLSv1/SSLv3:DH-DSS-SEED-SHA          TLSv1/SSLv3:DHE-RSA-CAMELLIA128-SHA
TLSv1/SSLv3:DHE-DSS-CAMELLIA128-SHA  TLSv1/SSLv3:DH-RSA-CAMELLIA128-SHA
TLSv1/SSLv3:DH-DSS-CAMELLIA128-SHA   TLSv1/SSLv3:ECDH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3:ECDH-ECDSA-AES128-GCM-SHA256TLSv1/SSLv3:ECDH-RSA-AES128-SHA256
TLSv1/SSLv3:ECDH-ECDSA-AES128-SHA256 TLSv1/SSLv3:ECDH-RSA-AES128-SHA
TLSv1/SSLv3:ECDH-ECDSA-AES128-SHA    TLSv1/SSLv3:AES128-GCM-SHA256
TLSv1/SSLv3:AES128-SHA256            TLSv1/SSLv3:AES128-SHA
TLSv1/SSLv3:SEED-SHA                 TLSv1/SSLv3:CAMELLIA128-SHA
TLSv1/SSLv3:PSK-AES128-CBC-SHA       TLSv1/SSLv3:ECDHE-RSA-RC4-SHA
TLSv1/SSLv3:ECDHE-ECDSA-RC4-SHA      TLSv1/SSLv3:ECDH-RSA-RC4-SHA
TLSv1/SSLv3:ECDH-ECDSA-RC4-SHA       TLSv1/SSLv3:RC4-SHA
TLSv1/SSLv3:RC4-MD5                  TLSv1/SSLv3:PSK-RC4-SHA
TLSv1/SSLv3:ECDHE-RSA-DES-CBC3-SHA   TLSv1/SSLv3:ECDHE-ECDSA-DES-CBC3-SHA
TLSv1/SSLv3:SRP-DSS-3DES-EDE-CBC-SHA TLSv1/SSLv3:SRP-RSA-3DES-EDE-CBC-SHA
TLSv1/SSLv3:SRP-3DES-EDE-CBC-SHA     TLSv1/SSLv3:EDH-RSA-DES-CBC3-SHA
TLSv1/SSLv3:EDH-DSS-DES-CBC3-SHA     TLSv1/SSLv3:DH-RSA-DES-CBC3-SHA
TLSv1/SSLv3:DH-DSS-DES-CBC3-SHA      TLSv1/SSLv3:ECDH-RSA-DES-CBC3-SHA
TLSv1/SSLv3:ECDH-ECDSA-DES-CBC3-SHA  TLSv1/SSLv3:DES-CBC3-SHA
TLSv1/SSLv3:PSK-3DES-EDE-CBC-SHA
---
---
Ciphers common between both SSL end points:
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-SHA       ECDHE-RSA-AES256-SHA
AES128-SHA                  AES256-SHA                 DES-CBC3-SHA
Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:0x04+0x08:0x05+0x08:0x06+0x08:RSA+SHA256:RSA+SHA384:RSA+SHA512:ECDSA+SHA1:RSA+SHA1
Shared Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:RSA+SHA256:RSA+SHA384:RSA+SHA512:ECDSA+SHA1:RSA+SHA1
Supported Elliptic Curves: 0x001D:P-256:P-384:P-521:0x0100:0x0101
Shared Elliptic curves: P-256:P-384:P-521
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID:
    Session-ID-ctx: 01000000
    Master-Key: 4CD94BFF2A9D5071E9BB13D2B382DD5085BAB67681AE9BE39D93A1AA9ECB80454892A268299C8558FEA41142B6BC726A
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1717198722
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
---
   0 items in the session cache
   0 client connects (SSL_connect())
   0 client renegotiates (SSL_connect())
   0 client connects that finished
   7 server accepts (SSL_accept())
   0 server renegotiates (SSL_accept())
   7 server accepts that finished
   0 session cache hits
   7 session cache misses
   0 session cache timeouts
   0 callback cache hits
   0 cache full overflows (128 allowed)
---
no client certificate available
```

Δραστηριότητα 4: Χρήση του πιστοποιητικού σε Apache HTTPS Web server

Αρχικά μεταφέρουμε τα αρχεία του website στον Apache server

Έπειτα ρυθμίζουμε το Apache για HTTPS

```
</VirtualHost>
<VirtualHost *:443>
    ServerName eleftheria-tzachristou.com
    DocumentRoot /var/www/eleftheria-tzachristou
    DirectoryIndex index.html
        SSLEngine On
        SSLCertificateFile /home/seed/Desktop/pki/server.pem
        SSLCertificateKeyFile /home/seed/Desktop/pki/server.pem
</VirtualHost>
```

Αφού τροποποιηθεί το αρχείο default-ssl.conf, πρέπει να εκτελέσετε μια σειρά από εντολές στο terminal για να ενεργοποιήσετε το πρωτόκολλο SSL:

// Test the Apache configuration file for errors

$ sudo apachectl configtest

// Enable the SSL module

$ sudo a2enmod ssl

// Enable the site we have just edited

$ sudo a2ensite default-ssl

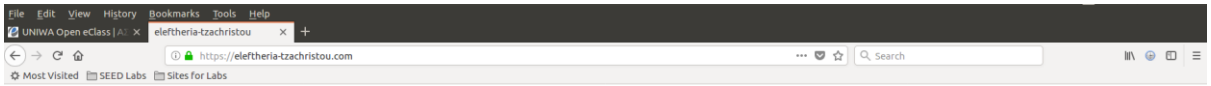
// Restart Apache

$ sudo service apache2 restart

```
[06/01/24]seed@VM:~$ sudo apachectl configtest
AH00112: Warning: DocumentRoot [/var/www/seedlabclickjacking] does not exist
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
[06/01/24]seed@VM:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
```

```
[06/01/24]seed@VM:~$  sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  service apache2 reload
[06/01/24]seed@VM:~$ sudo service apache2 restart
Enter passphrase for SSL/TLS keys for eleftheria-tzachristou.com:443 (RSA): **********
[06/01/24]seed@VM:~$
```

Πλέον μπορούμε να περιηγηθούμε στο ασφαλές website από τον browser.



eleftheria-tzachristou

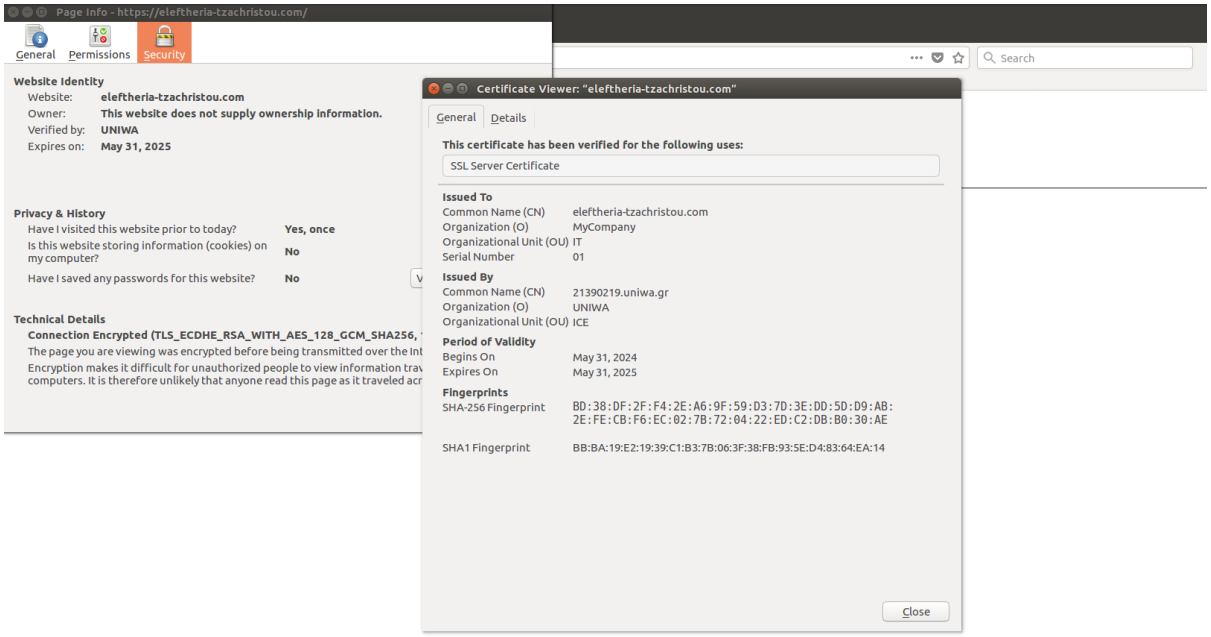
Owner

Lastname:Tzachristou

Firstname:Eleftheria

AM:21390219

Date:1/6/24



Δραστηριότητα 5: Επίθεση τύπου Man-In-The-Middle

Αρχικά ρυθμίζουμε το κακόβουλο ιστότοπο

```
</VirtualHost>
<VirtualHost *:443>
    ServerName seclab-2024.com
    DocumentRoot /var/www/eleftheria-tzachristou
    DirectoryIndex index.html
        SSLEngine On
        SSLCertificateFile /home/seed/Desktop/pki/server.pem
        SSLCertificateKeyFile /home/seed/Desktop/pki/server.pem
</VirtualHost>
```

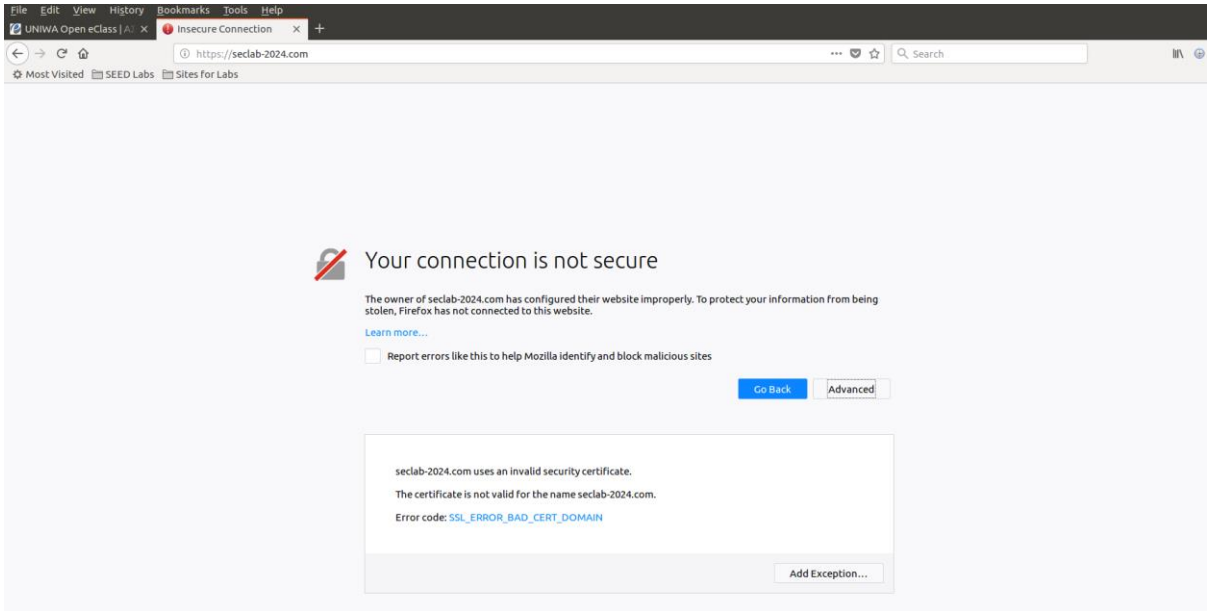
Ανακατευθύνουμε το θύμα

Χρησιμοποιηούμε την επίθεση στον DNS. Όμως δεν πραγματοποιείται πραγματική επίθεση DNS ,αλλά θα την προσομοιώσουμε, τροποποιώντας το αρχείο /etc/hosts στο μηχάνημα του θύματος.

```
127.0.0.1       localhost
127.0.1.1       VM

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1       User
127.0.0.1       Attacker
127.0.0.1       Server
127.0.0.1       www.SeedLabSQLInjection.com
127.0.0.1       www.xsslabelgg.com
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
127.0.0.1       seclab-2024.com
```

Έπειτα από τον browser (του θύματος) συνδεόμαστε στο νόμιμο website https://seclab-2024.com και λαμβάνουμε ένα μήνυμα σφάλματος:


File Edit View History Bookmarks Tools Help
UNIWA Open eClass | A
Insecure Connection
https://seclab-2024.com
Search
Most Visited
SEED Labs
Sites for Labs
Your connection is not secure
The owner of seclab-2024.com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.
Learn more...
Report errors like this to help Mozilla identify and block malicious sites
Go Back
Advanced
seclab-2024.com uses an invalid security certificate.
The certificate is not valid for the name seclab-2024.com.
Error code: SSL_ERROR_BAD_CERT_DOMAIN
Add Exception...

Δραστηριότητα 6: Επίθεση τύπου Man-In-The-Middle σε περίπτωση παραβιασμένης ΑΠ

Προσθέτουμε μια καταχώρηση στο αρχείο, όπως φαίνεται παρακάτω./etc/apache2/sites-available/default-ssl.conf

```
</VirtualHost>
<VirtualHost *:443>
    ServerName seclab-2024.com
    DocumentRoot /var/www/eleftheria-tzachristou
    DirectoryIndex index.html
        SSLEngine On
        SSLCertificateFile /home/seed/Desktop/pki/server.pem
        SSLCertificateKeyFile /home/seed/Desktop/pki/server.pem
</VirtualHost>

IfModule>
```

Θα χρησιμοποιήσουμε το αρχείο html

Ο ιστότοπος προορισμού μπορεί να προσπελαστεί στο θύμα χωρίς να ειδοποιήσει το πρόγραμμα περιήγησης, όπως φαίνεται παρακάτω.