Διαχείριση Δικτύων – Ευφυή Δίκτυα

4η Ομάδα Ασκήσεων

Αλέξανδρος Μαυρογιάννης
Αριστοτέλης Πανάρας

1.
Η λίστα με τα πακέτα που καταγράφησαν σε ένα capture file, μπορεί να φανεί με την εντολή 'tshark -r <input_file>'. Με αυτό τον τρόπο μπορούμε να περιορίσουμε τα πακέτα με όποιο τρόπο θέλουμε, το οποίο πρακτικά σημαίνει ότι μπορούμε να δούμε τα πακέτα που μεταφέρθηκαν μέχρι κάποιο σημείο (και εν προκειμένω μέχρι τη μεταφορά των 2 πρώτων ping requests.
a.
Από το dump στο τέλος της αναφοράς, τα 2 πρώτα ping έγιναν στους:
147.102.13.1 (averel.netmode.ece.ntua.gr)
192.108.114.2 (duth.gr)
Τα πακέτα που μας ενδιαφέρουν είναι τα arp και dns, και μπορούν να φανούν με το display filter 'dns || arp'. Η αποστολή τών arp πακέτων έγινε για την ανακάλυψη του δικτύου, εφόσον είχε γίνει διαγραφή της arp cache, και των πακέτων dns (A queries) έγινε από το ping για να βρεθεί η IP του κόμβου με CNAME αυτό που δόθηκε στο ping.
b.
Με το φίλτρο 'ip.dst == ulysses.noc.ntua.gr' βλέπουμε ότι έγινε ένα AXFR query (DNS domain record request), το οποίο συμβαίνει στην περίπτωση της εντολής dig (ή drill για τους λίγο πιό σοβαρούς). Η μεταφορά των πακέτων έγινε πάνω από TCP/IP. Τα identification fields των IP πακέτων φαίνονται στο dump στο τέλος της αναφοράς.
c.
Το πακέτο απάντησης περιελάμβανε τη διαδρομή που ακολούθησε το πακέτο, το οποίο είναι αποτέλεσμα της χρήσης της record route option του ping.
* Εδώ κάπου υπάρχει ένα bugάκι. Το wireshark αναφέρει το μήκος του σώματος του ICMP πακέτου ως 56 bytes ενώ το dump του tshark ως 48.
d.
Ο λόγος που παρατηρούνται πολλαπλά πακέτα ερωταπάντησς (2 x 1514 + 1 x 82 bytes) είναι λόγω fragmentation. Αυτό οφείλεται στην αλλαγή του packetsize από την default value (56 bytes) σε μέγεθος 3000 bytes.

Η σειρά των εντολών φαίνεται να ήταν η εξής:
ping averel.netmode.ece.ntua.gr
ping duth.gr
dig
ping -R www.uoa.gr
ping -s 3000 www.auth.gr

2.

a.

Αρχικά δημιουργούμε ένα RSA κλειδί, και αφού συμπληρώσουμε την αίτηση για την υπογραφή του, το δίνουμε για υπογραφή στην CA που βρίσκεται στη maria.netmode.ntua.gr.

Οι εντολές που εκτελούμε είναι οι εξής:

openssl genrsa -out gened.key

openssl req -new -key gened.key -keyform PEM -out requed.csr

openssl ca -in requed.csr -out fin.crt

b.

Εκτελώντας την εντολή, δεν συνδεόμαστε στο server, διότι δεν δηλώσαμε ποιό certificate θα έπρεπε να χρησιμοποιηθεί για τη σύνδεση.

c.

Σε αυτή την περίπτωση η σύνδεση στο server γίνεται αποδεκτή, εφόσον έχουμε δηλώσει ποιό certificate θα πρέπει να χρησιμοποιηθεί για τη σύνδεση. Το common name του server είναι sorch.netmode.ntua.gr (του οποίου το certificate είναι self-signed) και τα certificates των χρηστών πρέπει να είναι υπογεγραμμένα από τη CA 'NETMODE COURSE CA - 2008'.

d.

HTTP/1.1 200 OK
Date: Sun, 26 Jan 2014 07:32:46 GMT
Server: Apache/2.2.12 (Ubuntu)
X-Powered-By: PHP/5.2.10-2ubuntu6.10
Vary: Accept-Encoding
Content-Length: 21
Connection: close
Content-Type: text/html

Welcome <canonical_name>!!!

SCRIPTS

```
#!/usr/bin/env bash

INFILE="lab4_trace.cap"
outfile="lab4_output.text"

#question_template: "command | tee -a $outfile"
questions=(
#Q_4_a
    "tshark -Y "{'"icmp.type == 8" -n','"icmp.type == 8" -N "nNC"','"ip.dst == ulysses.noc.ntua.gr"','"ip.src == ulysses.noc.ntua.gr" -T fields -e ip.id','"ip.src == www.uoa.gr" -PV','"ip.src == www.auth.gr || ip.dst == www.auth.gr"'}" -r \"$INFILE\" | tee -a $outfile"
#Q_4_b
"touch ~/index.txt"
    "echo '01' > ~/serial"
    "openssl "{'genrsa -out gened.key','req -subj "/C=GR/ST=ATTIKI/L=ATHENS/O=MY_MYSELF_I/CN=my.domain.netmode.ntua.gr" -new -key gened.key -keyform PEM -out requed.csr','ca -in requed.csr -out fin.crt','s_client -state -host sorch.netmode.ntua.gr -port 443','s_client -state -host sorch.netmode.ntua.gr -port 443 -cert fin.crt -key gened.key'}" 2>&1 | tee -a $outfile"
#   "openssl s_client -state -host sorch.netmode.ntua.gr -port 443 -cert fin.crt -key gened.key < lab4_ssl_command.txt 2>&1 | tee -a $outfile"
    ####On the last we have to type "GET /netmg.php HTTP/1.0\n\n", since the server has no expect shell.
)
```

```
function report () {
    echo "========" "$1" "========" >> $outfile
    eval "$1"
    echo -e "\n" >> $outfile
}

IFS=""
rm -f "$outfile"
for i in "${questions[@]}"
do
    report "$i"
done
echo "Finished!"
```

OUTPUTS

```
======== tshark -Y "icmp.type == 8" -n -r "lab4_trace.cap" | tee -a lab4_output.text ========
 37   7.424050 147.102.13.30 -> 147.102.13.1 ICMP 98 Echo (ping) request  id=0xae54, seq=0/0, ttl=64
 72  13.432648 147.102.13.30 -> 192.108.114.2 ICMP 98 Echo (ping) request  id=0xb154, seq=0/0, ttl=64
214  25.474019 147.102.13.30 -> 195.134.71.229 ICMP 138 Echo (ping) request  id=0xb654, seq=0/0, ttl=64
319  31.484039 147.102.13.30 -> 155.207.1.12 ICMP 1514 Echo (ping) request  id=0xb854, seq=0/0, ttl=64


======== tshark -Y "icmp.type == 8" -N "nNC" -r "lab4_trace.cap" | tee -a lab4_output.text ========
 37   7.424050 cornuto.netmode.ece.ntua.gr -> averel.netmode.ece.ntua.gr ICMP 98 Echo (ping) request
id=0xae54, seq=0/0, ttl=64
 72  13.432648 cornuto.netmode.ece.ntua.gr -> duth.gr      ICMP 98 Echo (ping) request  id=0xb154, seq=0/0,
ttl=64
214  25.474019 cornuto.netmode.ece.ntua.gr -> sites.uoa.gr ICMP 138 Echo (ping) request  id=0xb654,
seq=0/0, ttl=64
319  31.484039 cornuto.netmode.ece.ntua.gr -> www.ccf.auth.gr ICMP 1514 Echo (ping) request  id=0xb854,
seq=0/0, ttl=64


======== tshark -Y "ip.dst == ulysses.noc.ntua.gr" -r "lab4_trace.cap" | tee -a lab4_output.text
========
107  19.452339 cornuto.netmode.ece.ntua.gr -> ulysses.noc.ntua.gr TCP 78 57950 > domain [SYN] Seq=0
Win=65535 Len=0 MSS=1460 WS=2 TSval=800963077 TSecr=0 SACK_PERM=1
109  19.452560 cornuto.netmode.ece.ntua.gr -> ulysses.noc.ntua.gr TCP 66 57950 > domain [ACK] Seq=1
Ack=1 Win=66608 Len=0 TSval=800963077 TSecr=1094416294
110  19.452615 cornuto.netmode.ece.ntua.gr -> ulysses.noc.ntua.gr DNS 105 Standard query 0x20e4  AXFR
netmode.ece.ntua.gr
114  19.454049 cornuto.netmode.ece.ntua.gr -> ulysses.noc.ntua.gr TCP 66 57950 > domain [ACK] Seq=40
Ack=1535 Win=65160 Len=0 TSval=800963078 TSecr=1094416294
120  19.455244 cornuto.netmode.ece.ntua.gr -> ulysses.noc.ntua.gr TCP 66 57950 > domain [ACK] Seq=40
Ack=3747 Win=64206 Len=0 TSval=800963080 TSecr=1094416295
126  19.456143 cornuto.netmode.ece.ntua.gr -> ulysses.noc.ntua.gr TCP 66 57950 > domain [ACK] Seq=40
Ack=5997 Win=62682 Len=0 TSval=800963081 TSecr=1094416297
134  19.457049 cornuto.netmode.ece.ntua.gr -> ulysses.noc.ntua.gr TCP 66 57950 > domain [ACK] Seq=40
Ack=8181 Win=61308 Len=0 TSval=800963081 TSecr=1094416297
141  19.457938 cornuto.netmode.ece.ntua.gr -> ulysses.noc.ntua.gr TCP 66 57950 > domain [ACK] Seq=40
Ack=10398 Win=59844 Len=0 TSval=800963082 TSecr=1094416298
147  19.458838 cornuto.netmode.ece.ntua.gr -> ulysses.noc.ntua.gr TCP 66 57950 > domain [ACK] Seq=40
Ack=12582 Win=58518 Len=0 TSval=800963083 TSecr=1094416299
```

153 19.461316 cornuto.netmode.ece.ntua.gr -> ulysses.noc.ntua.gr TCP 66 57950 > domain [ACK] Seq=40 Ack=12803 Win=61226 Len=0 TSval=800963086 TSecr=1094416300
162 19.463987 cornuto.netmode.ece.ntua.gr -> ulysses.noc.ntua.gr TCP 66 [TCP Window Update] 57950 > domain [ACK] Seq=40 Ack=12803 Win=64144 Len=0 TSval=800963088 TSecr=1094416300
169 19.466571 cornuto.netmode.ece.ntua.gr -> ulysses.noc.ntua.gr TCP 66 57950 > domain [FIN, ACK] Seq=40 Ack=12803 Win=66608 Len=0 TSval=800963091 TSecr=1094416300
174 19.466831 cornuto.netmode.ece.ntua.gr -> ulysses.noc.ntua.gr TCP 66 57950 > domain [ACK] Seq=41 Ack=12804 Win=66606 Len=0 TSval=800963091 TSecr=1094416308

======== tshark -Y "ip.src == ulysses.noc.ntua.gr" -T fields -e ip.id -r "lab4_trace.cap" | tee -a lab4_output.text ========
0xb25a
0xb25b
0xb25d
0xb25e
0xb25f
0xb261
0xb262
0xb263
0xb264
0xb265
0xb266
0xb267
0xb268
0xb26a
0xb26c
0xb26d

======== tshark -Y "ip.src == www.uoa.gr" -PV -r "lab4_trace.cap" | tee -a lab4_output.text ========
216 25.475515 sites.uoa.gr -> cornuto.netmode.ece.ntua.gr ICMP 138 Echo (ping) reply   id=0xb654, seq=0/0, ttl=62 (request in 214)
Frame 216: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 5, 2010 17:17:11.607529000 EET
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1288970231.607529000 seconds
    [Time delta from previous captured frame: 0.001383000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 25.475515000 seconds]
    Frame Number: 216
    Frame Length: 138 bytes (1104 bits)
    Capture Length: 138 bytes (1104 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:icmp:data]
Ethernet II, Src: router.netmode.ece.ntua.gr (00:08:7c:63:e4:00), Dst: cornuto.netmode.ece.ntua.gr (00:0c:6e:ba:d1:41)
    Destination: cornuto.netmode.ece.ntua.gr (00:0c:6e:ba:d1:41)
        Address: cornuto.netmode.ece.ntua.gr (00:0c:6e:ba:d1:41)
        .... ..0. .... = LG bit: Globally unique address (factory default)
        ....0 .... = IG bit: Individual address (unicast)
    Source: router.netmode.ece.ntua.gr (00:08:7c:63:e4:00)
        Address: router.netmode.ece.ntua.gr (00:08:7c:63:e4:00)
        .... ..0. .... = LG bit: Globally unique address (factory default)

```
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Type: IP (0x0800)
Internet Protocol Version 4, Src: sites.uoa.gr (195.134.71.229), Dst: cornuto.netmode.ece.ntua.gr
(147.102.13.30)
   Version: 4
   Header length: 60 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
   Total Length: 124
   Identification: 0xbced (48365)
   Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
   Fragment offset: 0
   Time to live: 62
   Protocol: ICMP (1)
   Header checksum: 0x45d3 [correct]
      [Good: True]
      [Bad: False]
   Source: sites.uoa.gr (195.134.71.229)
   Destination: cornuto.netmode.ece.ntua.gr (147.102.13.30)
   Options: (40 bytes), Record Route, End of Options List (EOL)
      Record Route (39 bytes)
         Type: 7
            0... .... = Copy on fragmentation: No
            .00. .... = Class: Control (0)
            ...0 0111 = Number: Record route (7)
         Length: 39
         Pointer: 28
         Recorded Route: ntua-uoa.core.ntua.gr (147.102.224.33)
         Recorded Route: 195.134.71.1 (195.134.71.1)
         Recorded Route: sites.uoa.gr (195.134.71.229)
         Recorded Route: sites.uoa.gr (195.134.71.229)
         Recorded Route: 147.102.224.34 (147.102.224.34)
         Recorded Route: router.netmode.ece.ntua.gr (147.102.13.200)
         Empty Route: 0.0.0.0 <- (next)
         Empty Route: 0.0.0.0 (0.0.0.0)
         Empty Route: 0.0.0.0 (0.0.0.0)
      End of Options List (EOL)
         Type: 0
            0... .... = Copy on fragmentation: No
            .00. .... = Class: Control (0)
            ...0 0000 = Number: End of Option List (EOL) (0)
Internet Control Message Protocol
   Type: 0 (Echo (ping) reply)
   Code: 0
   Checksum: 0xb297 [correct]
   Identifier (BE): 46676 (0xb654)
   Identifier (LE): 21686 (0x54b6)
   Sequence number (BE): 0 (0x0000)
   Sequence number (LE): 0 (0x0000)
   [Request frame: 214]
   [Response time: 1.496 ms]
   Timestamp from icmp data: Nov  5, 2010 17:17:11.606012000 EET
```

```
    [Timestamp from icmp data (relative): 0.001517000 seconds]
    Data (48 bytes)

0000  08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17   ................
0010  18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27   ........ !"#$%&'
0020  28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37   ()*+,-./01234567
        Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...
        [Length: 48]



======== tshark -Y "ip.src == www.auth.gr || ip.dst == www.auth.gr" -r "lab4_trace.cap" | tee -a
lab4_output.text ========
319  31.484039 cornuto.netmode.ece.ntua.gr -> www.ccf.auth.gr ICMP 1514 Echo (ping) request  id=0xb854,
seq=0/0, ttl=64
320  31.484043 cornuto.netmode.ece.ntua.gr -> www.ccf.auth.gr IPv4 1514 Fragmented IP protocol
(proto=ICMP 1, off=1480, ID=7b2a)
321  31.484045 cornuto.netmode.ece.ntua.gr -> www.ccf.auth.gr IPv4 82 Fragmented IP protocol (proto=ICMP
1, off=2960, ID=7b2a)
323  31.492408 www.ccf.auth.gr -> cornuto.netmode.ece.ntua.gr ICMP 1514 Echo (ping) reply    id=0xb854,
seq=0/0, ttl=60 (request in 319)
324  31.492415 www.ccf.auth.gr -> cornuto.netmode.ece.ntua.gr IPv4 1514 Fragmented IP protocol
(proto=ICMP 1, off=1480, ID=ed0e)
325  31.492419 www.ccf.auth.gr -> cornuto.netmode.ece.ntua.gr IPv4 82 Fragmented IP protocol (proto=ICMP
1, off=2960, ID=ed0e)


======== touch ~/index.txt ========


======== echo '01' > ~/serial ========


======== openssl genrsa -out gened.key 2>&1 | tee -a lab4_output.text ========
Generating RSA private key, 512 bit long modulus
.....................................++++++++++++
.............++++++++++++
e is 65537 (0x10001)


======== openssl req -subj
"/C=GR/ST=ATTIKI/L=ATHENS/O=MY_MYSELF_I/CN=my.domain.netmode.ntua.gr" -new -key gened.key
-keyform PEM -out requed.csr 2>&1 | tee -a lab4_output.text ========


======== openssl ca -in requed.csr -out fin.crt 2>&1 | tee -a lab4_output.text ========
Using configuration from /etc/ssl/openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Jan 26 12:13:55 2014 GMT
            Not After : Jan 26 12:13:55 2015 GMT
        Subject:
            countryName               = GR
```

```
        stateOrProvinceName     = ATTIKI
        organizationName        = MY_MYSELF_I
        commonName              = my.domain.netmode.ntua.gr
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            D7:78:71:49:13:A0:BD:97:AD:EB:24:A5:AC:14:39:BE:8F:9D:EC:C0
        X509v3 Authority Key Identifier:
            DirName:/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=NETMODE COURSE CA -
2008/emailAddress=root@netmode.ntua.gr
            serial:92:C5:2F:BC:2E:8F:01:13

Certificate is to be certified until Jan 26 12:13:55 2015 GMT (365 days)
Sign the certificate? [y/n]:

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


======== openssl s_client -state -host sorch.netmode.ntua.gr -port 443 2>&1 | tee -a lab4_output.text
========
SSL_connect:before/connect initialization
SSL_connect:SSLv2/v3 write client hello A
SSL_connect:SSLv3 read server hello A
depth=0 /C=GR/ST=ATTICA/L=Athens/O=NETMODE/CN=sorch.netmode.ntua.gr
verify error:num=18:self signed certificate
verify return:1
depth=0 /C=GR/ST=ATTICA/L=Athens/O=NETMODE/CN=sorch.netmode.ntua.gr
verify error:num=10:certificate has expired
notAfter=Dec 20 14:14:50 2013 GMT
verify return:1
depth=0 /C=GR/ST=ATTICA/L=Athens/O=NETMODE/CN=sorch.netmode.ntua.gr
notAfter=Dec 20 14:14:50 2013 GMT
verify return:1
SSL_connect:SSLv3 read server certificate A
SSL_connect:SSLv3 read server key exchange A
SSL_connect:SSLv3 read server certificate request A
SSL_connect:SSLv3 read server done A
SSL_connect:SSLv3 write client certificate A
SSL_connect:SSLv3 write client key exchange A
SSL_connect:SSLv3 write change cipher spec A
SSL_connect:SSLv3 write finished A
SSL_connect:SSLv3 flush data
SSL3 alert read:fatal:handshake failure
SSL_connect:failed in SSLv3 read finished A
58484:error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake
failure:/usr/src/secure/lib/libssl/../../../crypto/openssl/ssl/s3_pkt.c:1102:SSL alert number 40
58484:error:140790E5:SSL routines:SSL23_WRITE:ssl handshake
failure:/usr/src/secure/lib/libssl/../../../crypto/openssl/ssl/s23_lib.c:188:
CONNECTED(00000003)
```

======== openssl s_client -state -host sorch.netmode.ntua.gr -port 443 -cert fin.crt -key gened.key 2>&1 | tee -a lab4_output.text ========
SSL_connect:before/connect initialization
SSL_connect:SSLv2/v3 write client hello A
SSL_connect:SSLv3 read server hello A
depth=0 /C=GR/ST=ATTICA/L=Athens/O=NETMODE/CN=sorch.netmode.ntua.gr
verify error:num=18:self signed certificate
verify return:1
depth=0 /C=GR/ST=ATTICA/L=Athens/O=NETMODE/CN=sorch.netmode.ntua.gr
verify error:num=10:certificate has expired
notAfter=Dec 20 14:14:50 2013 GMT
verify return:1
depth=0 /C=GR/ST=ATTICA/L=Athens/O=NETMODE/CN=sorch.netmode.ntua.gr
notAfter=Dec 20 14:14:50 2013 GMT
verify return:1
SSL_connect:SSLv3 read server certificate A
SSL_connect:SSLv3 read server key exchange A
SSL_connect:SSLv3 read server certificate request A
SSL_connect:SSLv3 read server done A
SSL_connect:SSLv3 write client certificate A
SSL_connect:SSLv3 write client key exchange A
SSL_connect:SSLv3 write certificate verify A
SSL_connect:SSLv3 write change cipher spec A
SSL_connect:SSLv3 write finished A
SSL_connect:SSLv3 flush data
SSL_connect:SSLv3 read finished A
CONNECTED(00000003)

Certificate chain
 0 s:/C=GR/ST=ATTICA/L=Athens/O=NETMODE/CN=sorch.netmode.ntua.gr
   i:/C=GR/ST=ATTICA/L=Athens/O=NETMODE/CN=sorch.netmode.ntua.gr
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICOTCCAaICCQC233p1hG6DwzANBgkqhkiG9w0BAQUFADBhMQswCQYDVQQGEwJH
UjEPMA0GA1UECBMGQVRUSUNBMQ8wDQYDVQQHEwZBdGhlbnMxEDAOBgNVBAoTB05F
VE1PREUxHjAcBgNVBAMTFXNvcmNoLm5ldG1vZGUubnR1YS5ncjAeFw0xMjEyMjAx
NDE0NTBaFw0xMzEyMjAxNDE0NTBaMGExCzAJBgNVBAYTAkdSMQ8wDQYDVQQIEwZB
VFRJQ0ExDzANBgNVBAcTBkF0aGVuczEQMA4GA1UEChMHTkVUTU9ERTEeMBwGA1UE
AxMVc29yY2gubmV0bW9kZS5udHVhLmdyMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQCwBKO+Nt0lRQ83cXPaAG0fOSHWuklKwsLWIfpfLmbOBdF40oLOeBtwHTrb
5M4oRIXen+swsVII6Qb6HV130r0Sinzrj1lNzk5PE8ZJEuE3CZ616hX2d3UcPPvJ
JSbekNHk5g951ItKmnTSeuCULa95ph+GeRy+r5o8ArITwHAS1QIDAQABMA0GCSqG
SIb3DQEBBQUAA4GBAAzpFw06KGVXEZQ2YZwnJVZ+8JHLyknhPug1DsUN4Xcd6w1s
XlJe/LlJVhsWOvPi+HrSQHVSNdkRXvFM6SQCugs4+nTOCbJhdsiJUnwHAwLp4PVW
cg0xNyOWGf5jhumfanxIoIvQ4W1KOX567AxQ/s7IdmUkFOmBf5GQtnT2qog5
-----END CERTIFICATE-----
subject=/C=GR/ST=ATTICA/L=Athens/O=NETMODE/CN=sorch.netmode.ntua.gr
issuer=/C=GR/ST=ATTICA/L=Athens/O=NETMODE/CN=sorch.netmode.ntua.gr
---
Acceptable client certificate CA names
/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=NETMODE COURSE CA - 2008/emailAddress=root@netmode.ntua.gr
---
SSL handshake has read 1313 bytes and written 1258 bytes

New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol : TLSv1
    Cipher   : DHE-RSA-AES256-SHA
    Session-ID: 7CE1CCB48903DB0E28549616E5F608DD52730B5705732495153511FE3E21B496
    Session-ID-ctx:
    Master-Key:
725041DCFA5AA408A7EC8BC1D90D7A7218E9798FFD9EC50CBD21E1C47E1227CD3D34354C90AEDDC41729E
B379F506C9E
    Key-Arg   : None
    Start Time: 1390738438
    Timeout   : 300 (sec)
    Verify return code: 10 (certificate has expired)

HTTP/1.1 200 OK
Date: Sun, 26 Jan 2014 12:14:08 GMT
Server: Apache/2.2.12 (Ubuntu)
X-Powered-By: PHP/5.2.10-2ubuntu6.10
Vary: Accept-Encoding
Content-Length: 38
Connection: close
Content-Type: text/html

Welcome my.domain.netmode.ntua.gr!!!

SSL3 alert read:warning:close notify
SSL3 alert write:warning:close notify
closed