Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών
και Μηχανικών Υπολογιστών

Διαχείριση Δικτύων - Ευφυή Δίκτυα

6η Εργαστηριακή Άσκηση

Βρεττός Κωνσταντίνος

A.M: 03119856

Maria_username: netmg026

Άσκηση 1

- Το πρώτο ping έγινε σε κόμβο-προορισμό με ip = 147.102.13.1 και DNS name = avarel.netmode.ece.ntua.gr, ενώ το δεύτερο ping σε κόμβο-προορισμό έχει ip = 147.108.114.2 και DNS name = duth.gr

Πριν από τα 2 αυτά ερωτήματα Ping ανταλλάχθηκαν πακέτα ARP τα οποία είχαν ως στόχο να βρουν τους προορισμούς προς τις διευθύνσεις που θέλησε ο διαχειριστής να επικοινωνήσει, επιπλέον ανταλλάχθηκαν πακέτα DNS, SSH, TCP και άλλα.

- Από το ulysses.noc.ntua.gr ζητήθηκε η πληροφορία σχετικά με τα flag SYN ACK, για την καθίδρυση 3-way handshake. Το πρωτόκολλο μεταφοράς που χρησιμοποιήθηκε είναι το **TCP.**
  Identification numbers :
  Identification: 0xb25a (45658)

  Identification: 0xb25b (45659)

  Identification: 0xb25d (45661)

  Identification: 0xb25e (45662)

  Identification: 0xb25f (45663)

  Identification: 0xb261 (45665)

  Identification: 0xb262 (45666)

Identification: 0xb263 (45667)

Identification: 0xb264 (45668)

Identification: 0xb265 (45669)

Identification: 0xb266 (45670)

Identification: 0xb267 (45671)
Identification: 0xb268 (45672)
Identification: 0xb26a (45674)
Identification: 0xb26c (45676)
Identification: 0xb26d (45677)

Η ακολουθία των πακέτων είναι αποτέλεσμα της εντολής **telnet**.

- Τα data της απάντησης είναι τα κάτωθι:

```
Data (48 bytes)
    Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637
    [Length: 48]
```

  Η ακολουθία των πακέτων είναι αποτέλεσμα της εντολής **dig**.

- Παρατηρούμε πολλαπλά πακέτα ερώτησης / απάντησης καθώς τα πακέτα είναι fragments ενός μεγαλύτερου πακέτου το οποίο όμως ξεπέρναγε την MTU και “τεμαχίστηκε”. Η ακολουθία των πακέτων είναι αποτέλεσμα της εντολής **ssh**.

<u>Άσκηση 2</u>

Πριν ξεκινήσουμε την άσκηση εκτελούμε τις εντολές με την παρακάτω σείρα στο home directory της ομάδας μας:

- mkdir newcerts
- touch ~/index.txt
- touch ~/index.txt.attr
- echo "01" > ~/serial

```
netmg026@maria:~$ pwd
/home/netmg026
netmg026@maria:~$ ls
netmg026@maria:~$ mkdir newcerts
netmg026@maria:~$ touch ~/index.txt
netmg026@maria:~$ touch ~/index.txt.attr
netmg026@maria:~$ echo "01" > ~/serial
netmg026@maria:~$ ls
index.txt  index.txt.attr  newcerts  serial
```

Έπειτα με τη βοήθεια του εργαλείου openssl εκτελούμε το εξής βήματα:

a. Για τη δημιουργία ενός πιστοποιητικού το οποίο να είναι υπογεγραμμένο από την αρχή πιστοποίησης (certificate authority) που βρίσκεται στο μηχάνημα maria.netmode.ntua.gr, εκτελούμε τις ακόλουθες εντολές :

- **Openssl genrsa –out my_file.key**

Με την οποία δημιουργούμε το ιδιωτικό μας κλειδί χρησιμοποιώντας τον αλγόριθμο κρυπρογράφισης RSA.

```
netmg026@maria:~$ openssl genrsa -out my_file.key
Generating RSA private key, 2048 bit long modulus
.............................+++++
.....................................................................+++++
e is 65537 (0x010001)
```

- **Openssl req –new –key my_file.key -keyform PEM –out my_file.csr**

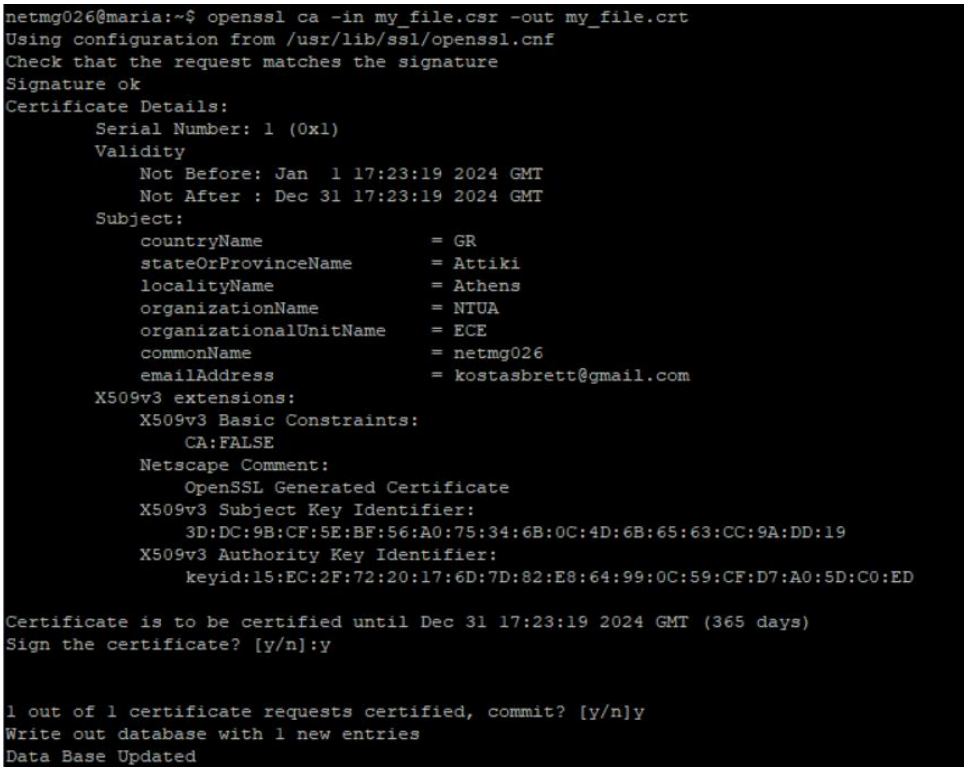
Με την οποία δημιουργούμε μια αίτηση για υπογραφή πιστοποιητικού (Certificate Signing Request – CSR)

```
netmg026@maria:~$ openssl req -new -key my_file.key -keyform PEM -out my_file.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) [AU]:GR
State or Province Name (full name) [Some-State]:Attiki
Locality Name (eg, city) []:Athens
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NTUA
Organizational Unit Name (eg, section) []:ECE
Common Name (e.g. server FQDN or YOUR name) []:netmg026
Email Address []:kostasbrett@gmail.com
```

Μετά από την εκτέλεση της εντολής όπως βλέπουμε και στο στιγμιότυπο από πάνω, μας έγιναν κάποιες ερωτήσεις που χρειάζονται για το Certificate Request που κάναμε.

- **Openssl ca –in my_file.csr -out my_file.crt**

Με την οποία γίνεται η υπογραφή του πιστοποιητικού από την CA (Certification Authority)



Όπως βλέπουμε πήραμε το πιστοποιητικό μας υπογεγραμμένο από την CA με:

Subject Key Identifier:

3D:DC:9B:CF:5E:BF:56:A0:75:34:6B:0C:4D:6B:65:63:CC:9A:DD:19

Authority Key Identifier:

keyid:15:EC:2F:72:20:17:6D:7D:82:E8:64:99:0C:59:CF:D7:A0:5D:C0:ED

b. Προσπαθούμε να συνδεθούμε στον secure web server που λειτουργεί στο μηχάνημα netmg.netmode.ntua.gr (port 443) με την εντολή:

openssl s_client -state -host netmg.netmode.ntua.gr -port 443 –tls1

```
netmg026@maria:~$ openssl s_client -state -host netmg.netmode.ntua.gr -port 443 -tls1
CONNECTED(00000003)
SSL_connect:before SSL initialization
SSL_connect:SSLv3/TLS write client hello
SSL_connect:SSLv3/TLS write client hello
SSL_connect:SSLv3/TLS read server hello
depth=1 C = GR, ST = ATTICA, L = ATHENS, O = NTUA, OU = NETMODE, CN = maria.netmode.ece.ntua.
gr, emailAddress = admin@netmode.ntua.gr
verify return:1
depth=0 C = GR, ST = ATTICA, L = ATHENS, O = NETMODE, OU = NTUA, CN = netmg.netmode.ntua.gr,
emailAddress = admin@netmode.ntua.gr
verify error:num=10:certificate has expired
notAfter=Dec  7 10:01:25 2023 GMT
verify return:1
depth=0 C = GR, ST = ATTICA, L = ATHENS, O = NETMODE, OU = NTUA, CN = netmg.netmode.ntua.gr,
emailAddress = admin@netmode.ntua.gr
notAfter=Dec  7 10:01:25 2023 GMT
verify return:1
SSL_connect:SSLv3/TLS read server certificate
SSL_connect:SSLv3/TLS read server key exchange
SSL_connect:SSLv3/TLS read server certificate request
SSL_connect:SSLv3/TLS read server done
SSL_connect:SSLv3/TLS write client certificate
SSL_connect:SSLv3/TLS write client key exchange
SSL_connect:SSLv3/TLS write change cipher spec
SSL_connect:SSLv3/TLS write finished
SSL3 alert read:fatal:handshake failure
SSL_connect:error in error
140338313203776:error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure:../
ssl/record/rec_layer_s3.c:1407:SSL alert number 40
---
Certificate chain
 0 s:/C=GR/ST=ATTICA/L=ATHENS/O=NETMODE/OU=NTUA/CN=netmg.netmode.ntua.gr/emailAddress=admin@n
etmode.ntua.gr
   i:/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=maria.netmode.ece.ntua.gr/emailAddress=adm
in@netmode.ntua.gr
 1 s:/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=maria.netmode.ece.ntua.gr/emailAddress=adm
in@netmode.ntua.gr
   i:/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=maria.netmode.ece.ntua.gr/emailAddress=adm
in@netmode.ntua.gr
---
```

```
Server certificate
-----BEGIN CERTIFICATE-----
MIIEKDCCAxCgAwIBAgIBAjANBgkqhkiG9w0BAQsFADCBmjELMAkGA1UEBhMCR1Ix
DzANBgNVBAgMBkF0dGljYTEPMA0GA1UEBwwGQXRoZW5zMQ0wCwYDVQQKDAROVFVB
MRAwDgYDVQQLDAdORVRNT0RFMSIwIAYDVQQDDBltYXJpYS5uZXRtb2RlLmVjZS5u
dHVhLmdyMSQwIgYJKoZIhvcNAQkBFhVhZG1pbkBuZXRtb2RlLm50dWEuZ3IwHhcN
MjIxMjA3MTAwMTIlWhcNMjMxMjA3MTAwMTIlWjCB1jELMAkGA1UEBhMCR1IxDzAN
BgNVBAgMBkFUVElDQTEPMA0GA1UEBwwGQVRIRU5TMRAwDgYDVQQKDAdORVRNT0RF
MQ0wCwYDVQQLDAROVFVBMR4wHAYDVQQDDBVuZXRtZy5uZXRtb2RlLm50dWEuZ3Ix
JDAiBgkqhkiG9w0BCQEWFWFkbWluQG5ldG1vZGUubnR1YS5ncjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMLg/HSUkx3RyswhAuHxUlVX9UzV2fvVw9dn
TuOFUdsPntiudZ6N/xrhCi/5UCC8wrJsjT7lcUruQ/tkg/kd9P89+5wtPE1h/9wU
lpKyxj2x3ZO7Am6tbNF2YhJpEbLBszDLk6mK89W38RxEIKQCIyVCFhyqFt7uDrTf
rlPGfkDslfGnqfPuR+8DNNodkdVHjCbZWaZcu8hQ6Hy8NYokTXq5UdbEPMJ+qY/S
Ciny2T7UM2cZ0lkyduBEXMVmkH4zzvXeUZsEIcFljCpakrU6ikIlzx0IQIYkUk0w
8j+RwHag5OaMiQiggx1GiGLCMu+vDYnR3Qiielc0IlQew2f0vtcCAwEAAaN7MHkw
CQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2Vy
dGlmaWNhdGUwHQYDVR0OBBYEFNac541j2umtfSKBzl0dybVD3kpSMB8GA1UdIwQY
MBaAFBXsL3IgF2l9guhkmQxZz9egXcDtMA0GCSqGSIb3DQEBCwUAA4IBAQAuNiLH
cT0W8aILvbVIVXmyStZ3erd2cBuYnXSnej9aY4LSAegUXZ/s6qabFF8ZVpJhl3FY
LtRPNCXZFTR+ferhR8BlyfOuw4FfOAPl5NGU3lTnI+5OMOZBjxg2/fOMV5g8NFmo
rV0M9eyblCPhmTHKeBD45DeoILkP46nqM77xKkV20RKvZYtD6ZW7++Eca3UOnFoX
lcehJTYCRBJpYEsUUqXNwfjiR+Hj947+9wCK7t53DjbMJY1TInUoZJrwF6EXpohh
pOjxNDcXwznYfMxBPWUtnlUJEMfPcavAZL0kdv0E8o88btMa0hRI6obRkWo9X5/l
l2748cg8y2hQMLc5
-----END CERTIFICATE-----
subject=/C=GR/ST=ATTICA/L=ATHENS/O=NETMODE/OU=NTUA/CN=netmg.netmode.ntua.gr/emailAddress=admi
n@netmode.ntua.gr
issuer=/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=maria.netmode.ece.ntua.gr/emailAddress=a
dmin@netmode.ntua.gr
---
Acceptable client certificate CA names
/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=maria.netmode.ece.ntua.gr/emailAddress=admin@ne
tmode.ntua.gr
Client Certificate Types: RSA sign, DSA sign, ECDSA sign
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 2713 bytes and written 248 bytes
Verification error: certificate has expired
---
New, TLSv1.0, Cipher is ECDHE-RSA-AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1
    Cipher    : ECDHE-RSA-AES256-SHA
    Session-ID:
    Session-ID-ctx:
    Master-Key: 3DC9C36993BB26E47ECDF9B99F2D8DEB044078B67F3EE7D3B08A6A41B0249B6362542565339FB
1F38650F5CF690409E4
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1704131237
    Timeout   : 7200 (sec)
    Verify return code: 10 (certificate has expired)
    Extended master secret: no
---
```

c. Στη συνέχεια εκτελούμε την εντολή

openssl s_client -state –host netmg.netmode.ntua.gr -port 443 –cert my_file.crt -key my_file.key -tls1 ,

όπου τα my_file.crt και my_file.key είναι αυτά που δημιουργήσαμε στην αρχή της άσκησης.

```
netmg026@maria:~$ openssl s_client -state -host netmg.netmode.ntua.gr -port 443 -cert my_file
.crt -key my_file.key -tls1
CONNECTED(00000003)
SSL_connect:before SSL initialization
SSL_connect:SSLv3/TLS write client hello
SSL_connect:SSLv3/TLS write client hello
SSL_connect:SSLv3/TLS read server hello
depth=1 C = GR, ST = ATTICA, L = ATHENS, O = NTUA, OU = NETMODE, CN = maria.netmode.ece.ntua.
gr, emailAddress = admin@netmode.ntua.gr
verify return:1
depth=0 C = GR, ST = ATTICA, L = ATHENS, O = NETMODE, OU = NTUA, CN = netmg.netmode.ntua.gr,
emailAddress = admin@netmode.ntua.gr
verify error:num=10:certificate has expired
notAfter=Dec  7 10:01:25 2023 GMT
verify return:1
depth=0 C = GR, ST = ATTICA, L = ATHENS, O = NETMODE, OU = NTUA, CN = netmg.netmode.ntua.gr,
emailAddress = admin@netmode.ntua.gr
notAfter=Dec  7 10:01:25 2023 GMT
verify return:1
SSL_connect:SSLv3/TLS read server certificate
SSL_connect:SSLv3/TLS read server key exchange
SSL_connect:SSLv3/TLS read server certificate request
SSL_connect:SSLv3/TLS read server done
SSL_connect:SSLv3/TLS write client certificate
SSL_connect:SSLv3/TLS write client key exchange
SSL_connect:SSLv3/TLS write certificate verify
SSL_connect:SSLv3/TLS write change cipher spec
SSL_connect:SSLv3/TLS write finished
SSL_connect:SSLv3/TLS write finished
SSL_connect:SSLv3/TLS read server session ticket
SSL_connect:SSLv3/TLS read change cipher spec
SSL_connect:SSLv3/TLS read finished
---
Certificate chain
 0 s:/C=GR/ST=ATTICA/L=ATHENS/O=NETMODE/OU=NTUA/CN=netmg.netmode.ntua.gr/emailAddress=admin@n
etmode.ntua.gr
   i:/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=maria.netmode.ece.ntua.gr/emailAddress=adm
in@netmode.ntua.gr
 1 s:/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=maria.netmode.ece.ntua.gr/emailAddress=adm
in@netmode.ntua.gr
   i:/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=maria.netmode.ece.ntua.gr/emailAddress=adm
in@netmode.ntua.gr
---
```

```
Server certificate
-----BEGIN CERTIFICATE-----
MIIEKDCCAxCgAwIBAgIBAjANBgkqhkiG9w0BAQsFADCBmjELMAkGA1UEBhMCR1Ix
DzANBgNVBAgMBkF0dGljYTEPMA0GA1UEBwwGQXRoZW5zMQ0wCwYDVQQKDAROVFVB
MRAwDgYDVQQLDAdORVRNT0RFMSIwIAYDVQQDDBltYXJpYS5uZXRtb2RlLmVjZS5u
dHVhLmdyMSQwIgYJKoZIhvcNAQkBFhVhZGlpbkBuZXRtb2RlLm50dWEuZ3IwHhcN
MjIxMjA3MTAwMTI1WhcNMjMxMjA3MTAwMTI1WjCBljELMAkGA1UEBhMCR1IxDzAN
BgNVBAgMBkFUVElDQTEPMA0GA1UEBwwGQVRIRU5TMRAwDgYDVQQKDAdORVRNT0RF
MQ0wCwYDVQQLDAROVFVBMR4wHAYDVQQDDBVuZXRtZy5uZXRtb2RlLm50dWEuZ3Ix
JDAiBgkqhkiG9w0BCQEWFWFkbWluQG51dGlvZGUubnR1YS5ncjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMLg/HSUkx3RyswhAuHxUlVX9UzV2fvVw9dn
TuOFUdsPntiudZ6N/xrhCi/5UCC8wrJsjT7lcUruQ/tkg/kd9P89+5wtPElh/9wU
lpKyxj2x3ZO7Am6tbNF2YhJpEbLBszDLk6mK89W38RxEIKQCIyVCFhyqFt7uDrTf
rlPGfkDslfGnqfPuR+8DNNodkdVHjCbZWaZcu8hQ6Hy8NYokTXq5UdbEPMJ+qY/S
Ciny2T7UM2cZ01kyduBEXMVmkH4zzvXeUZsEIcFljCpakrU6ikIlzx0IQIYkUk0w
8j+RwHag5OaMiQiggxlGiGLCMu+vDYnR3Qiie1c0IlQew2f0vtcCAwEAAaN7MHkw
CQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2Vy
dGlmaWNhdGUwHQYDVR0OBBYEFNac541j2umtfSKBzl0dybVD3kpSMB8GA1UdIwQY
MBaAFBXsL3IgF2l9guhkmQxZz9egXcDtMA0GCSqGSIb3DQEBCwUAA4IBAQAuNiLH
cT0W8aILvbVIVXmyStZ3erd2cBuYnXSnej9aY4LSAegUXZ/s6qabFF8ZVpJhl3FY
LtRPNCXZFTR+ferhR8BlyfOuw4FfOAPl5NGU3lTnI+5OMOZBjxg2/fOMV5g8NFmo
rV0M9eyblCPhmTHKeBD45DeoILkP46nqM77xKkV20RKvZYtD6ZW7++Eca3UOnFoX
lcehJTYCRBJpYEsUUqXNwfjiR+Hj947+9wCK7t53DjbMJYlTInUoZJrwF6EXpohh
pOjxNDcXwznYfMxBPWUtnlUJEMfPcavAZL0kdv0E8o88btMa0hRI6obRkWo9X5/l
l2748cg8y2hQMLc5
-----END CERTIFICATE-----
subject=/C=GR/ST=ATTICA/L=ATHENS/O=NETMODE/OU=NTUA/CN=netmg.netmode.ntua.gr/emailAddress=admi
n@netmode.ntua.gr
issuer=/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=maria.netmode.ece.ntua.gr/emailAddress=a
dmin@netmode.ntua.gr
---
```

```
Acceptable client certificate CA names
/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=maria.netmode.ece.ntua.gr/emailAddress=admin@ne
tmode.ntua.gr
Client Certificate Types: RSA sign, DSA sign, ECDSA sign
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 4028 bytes and written 2612 bytes
Verification error: certificate has expired
---
New, TLSv1.0, Cipher is ECDHE-RSA-AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1
    Cipher    : ECDHE-RSA-AES256-SHA
    Session-ID: BFF08A8CE5B2F78CEDCC089503AC951C1D9F306B3F0099CDCFA74EADA629F664
    Session-ID-ctx:
    Master-Key: 8E1FDAA120D5C85E68BEC397F511262EDEDD22A785ABEDE043777736841A9B5B16ECF812EC70A
C7B5F3A8F504CF42E01
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
```

```
0150 - 19 01 99 f7 d8 cf f2 a0-48 d6 ce a5 d4 61 1a b9   ........H....a..
0160 - d2 f4 cf b9 91 4e f6 9c-f1 de f5 28 33 7c 61 a6   .....N.....(3|a.
0170 - ba bb e3 2e 6f e2 8e a9-9f 7b f7 1f 30 ee bc 94   ....o....{..0...
0180 - 66 76 81 70 b9 3f fb e8-f6 e6 22 92 d4 58 dc ad   fv.p.?....".X..
0190 - a9 91 d4 9b 54 13 28 ca-3b c2 4c a7 d9 83 ae 27   ....T.(.;.L....'
01a0 - de 9d 9f 05 3a cc b8 4b-9d f9 35 20 87 43 86 94   ....:..K..5 .C..
01b0 - 28 d8 8d 08 f6 96 fb 36-60 0e 82 9e 1c a1 c8 42   (......6`......B
01c0 - 48 ce 30 28 65 2d 22 1b-25 3f 27 8b 83 5a be 64   H.0(e-".%?'..Z.d
01d0 - 36 76 11 4e 1c e0 31 02-3e 51 68 ad 6d 73 75 4a   6v.N..1.>Qh.msuJ
01e0 - c0 26 3c b2 1c 5f 7c bf-3c df 91 64 26 86 68 14   .&<.._|.<..d&.h.
01f0 - 8f 9a 66 68 94 c2 65 2b-a0 c8 c0 6a e8 9f 08 b1   ..fh..e+...j....
0200 - f1 68 24 95 64 d2 8a 9f-1a b8 85 17 34 02 21 78   .h$.d.......4.!x
0210 - 55 7d 1e ce 09 9e 8e c4-43 09 f4 92 43 4a 67 61   U}......C...CJga
0220 - d0 a0 d7 83 61 db 12 e3-fb 15 a5 9f 5d 31 09 3a   ....a.......]1.:
0230 - f3 06 d0 b1 9e 04 df 3f-94 1d 1b 42 3c 9e 1f d2   .......?...B<...
0240 - 79 4c b8 9b f8 c8 ed be-cc fa 37 0b a8 42 69 5c   yL........7..Bi\
0250 - 17 5e 85 98 49 d1 e1 f7-71 18 9d 50 55 e1 e7 5b   .^..I...q..PU..[
0260 - 0d cb 30 0c 9d 59 45 35-82 6f ec fc 6d f4 8a c6   ..0..YE5.o..m...
0270 - 5c 62 b6 2a 4d 11 e7 f0-54 e4 a1 ef cd 0d ca cf   \b.*M...T.......
0280 - 3e 6b a4 0b 2d 63 a3 18-5b 49 49 dd 64 4e 3c b7   >k..-c..[II.dN<.
0290 - 94 cf 15 b1 75 bd 5d ef-93 6e a4 0c fb 20 a2 e4   ....u.]..n... ..
02a0 - 1b bc 6d f7 b8 e4 9e b4-0b af fe f1 4d de e0 3f   ..m.........M..?
02b0 - d7 ab c8 ed 47 02 43 0d-53 3e 10 b0 5f 80 1e f1   ....G.C.S>.._...
02c0 - 60 0a af 36 77 0a 8b c0-12 d1 68 fe 0a 5b 46 fc   `..6w.....h..[F.
02d0 - 84 8d 3d 64 0e 4d e0 fc-c5 69 63 ad 7d 6e 63 b2   ..=d.M...ic.}nc.
02e0 - ab 44 a5 b8 32 de ec 00-b8 d1 1d 7f e2 c3 b3 5d   .D..2..........]
02f0 - 53 a3 07 a6 f5 72 3c 21-72 ee e1 3e d5 59 9f 63   S....r<!r..>.Y.c
0300 - 51 5f ad 8e 52 48 80 f7-aa d0 94 e3 19 f4 d9 e3   Q_..RH..........
0310 - 10 99 47 75 dc 8e f8 45-40 47 ef e9 a0 aa 0d 24   ..Gu...E@G.....$
0320 - 92 61 33 f6 fa 3d 30 4b-fd 0c c4 29 e5 61 3d c2   .a3..=0K...).a=.
0330 - bc e1 c4 bc af 38 4e 51-73 ce 5a 0a ae cc 79 95   .....8NQs.Z...y.
0340 - 0c 2c e2 43 0c 37 99 20-98 5f d0 b2 56 bd a0 6e   .,.C.7. ._..V..n
0350 - 10 ec 54 7b 79 67 78 35-e4 11 92 f5 35 c5 56 dd   ..T{ygx5....5.V.
0360 - f6 a9 98 c4 08 4c bf 9f-dc 30 fc 50 e6 05 b1 56   .....L...0.P...V
0370 - ef d6 c8 4b 5c 86 05 fe-6c dc 6a fe 7d 60 24 8a   ...K\...l.j.}`$.
0380 - 1a 3e 8a 0d 69 2b f4 76-4c 79 f2 00 31 4a 9a be   .>..i+.vLy..1J..
0390 - 4f 29 61 bf 31 2f ba 6f-53 5d 2f d3 0c 40 ca 0b   O)a.1/.oS]/..@..
03a0 - b5 91 19 7f 01 27 28 22-1f 82 76 00 88 cf 46 59   .....'("..v...FY
03b0 - d5 07 65 cf 99 04 70 db-bc 8f 6d f3 24 f8 46 c2   ..e...p...m.$.F.
03c0 - dd ad ce 18 5e e4 32 48-0a a8 8f 09 ec bd 1e d0   ....^.2H........
03d0 - 74 9f 61 f3 d7 d8 f8 f2-70 ab 87 e3 9b 7a b4 a0   t.a.....p....z..
03e0 - 2b 7a d3 ab 76 c2 ee 31-82 8c b1 ae 30 24 bc 29   +z..v..1....0$.)
03f0 - 50 02 48 51 86 2b 51 bf-07 e1 ca 70 fc d7 6c 98   P.HQ.+Q....p..l.
0400 - 67 b2 f7 b9 41 fa 9b a4-d5 38 43 22 50 22 30 7b   g...A....8C"P"0{
0410 - 2d 1f c9 9b 00 41 89 2c-32 1a 2d ae 2d 8c 4b 50   -....A.,2.-.-.KP
0420 - 70 af 73 20 e6 89 15 05-38 74 00 ee 0d ee f7 00   p.s ....8t......
0430 - 93 a8 8a cf 50 b7 5e 17-01 dc 43 0e 26 ab 17 80   ....P.^...C.&...
0440 - 94 0f 52 9e c6 47 f6 4f-86 65 65 e8 df ff 6f 24   ..R..G.O.ee...o$
0450 - c3 a8 76 a0 59 e3 06 34-0a e7 71 e3 cf 4c 2c 93   ..v.Y..4..q..L,.
0460 - 8b 3c 2d ab 5b d2 91 6a-38 3d 9f bf c1 c2 29 42   .<-.[..j8=....)B
0470 - cb f2 39 25 d0 31 95 07-b5 0d 6c 3e 8d 8f 9d 84   ..9%.1....l>....
0480 - 53 44 2a 03 b8 48 38 76-21 6d 48 1e 85 fa 22 87   SD*..H8v!mH...".
0490 - ac 53 57 30 1b d9 d6 0a-0e 0f 91 0b 39 ba 57 7d   .SW0........9.W}
04a0 - 6c 9c e5 9f d2 02 c9 41-26 38 a3 98 28 0a 29 d4   l......A&8..(.).
04b0 - 94 5f 6d d9 d8 8b 38 42-4a 2e d7 0c 55 e3 60 6f   ._m...8BJ...U.`o
04c0 - 8c bb 05 6f 8b ef c4 e8-64 ac ea 36 47 26 b9 bc   ...o....d..6G&..
04d0 - 70 89 97 3a dd b5 61 8c-71 1a b8 58 b7 9e b5 66   p..:..a.q..X...f

Start Time: 1704131998
Timeout   : 7200 (sec)
Verify return code: 10 (certificate has expired)
Extended master secret: no
```

Σε αυτή την περίπτωση βλέπουμε ότι συνδεόμαστε στον secure web server επιτυχώς.

CN του Web Server :

```
Acceptable client certificate CA names
/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=maria.netmode.ece.ntua.gr/emailAddress=admin@ne
tmode.ntua.gr
```

Certification Authority :

```
subject=/C=GR/ST=ATTICA/L=ATHENS/O=NETMODE/OU=NTUA/CN=netmg.netmode.ntua.gr/emailAddress=admi
n@netmode.ntua.gr
issuer=/C=GR/ST=Attica/L=Athens/O=NTUA/OU=NETMODE/CN=maria.netmode.ece.ntua.gr/emailAddress=a
dmin@netmode.ntua.gr
```

Τα πιστοποιητικά πρέπει να είναι υπογεγραμμένα από την πιστοποιημένη αρχή netmg.netmode.ntua.gr

d. Έχοντας επιτύχει την σύνδεση εκτελούμε την εντολή :

- **GET /netmg.php HTTP/1.0**

Και το αποτέλεσμα που παίρνουμε από αυτήν είναι “**HTTP/1.1 200 OK**” , το οποίο σημαίνει ότι το αίτημα μας ήταν επιτυχές,βλέπουμε κιόλας ότι στο παρακάτω screenshot κάτω από το πεδίο Content-Type το οποίο είναι text/html, υπάρχει ένα μήνυμα το οποίο γράφει “**Welcome netmg026**” το οποίο είναι το μήνυμα το οποίο εμφανίζεται στον secure web server στον οποίο έχουμε συνδεθεί.

```
GET /netmg.php HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 01 Jan 2024 21:29:42 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.5
Content-Length: 21
Connection: close
Content-Type: text/html

Welcome netmg026!!!

read:errno=0
SSL3 alert write:warning:close notify
```

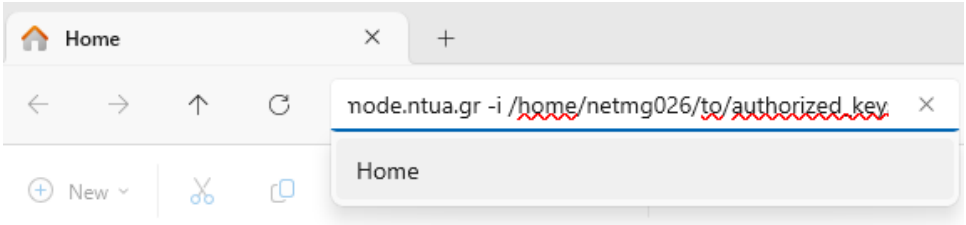
Άσκηση 3

Εκτελώντας την εντολή “ssh-keygen” δημιουργούμε ένα ζεύγος κλειδιών RSA, με την εκτέλεση της εντολής καλούμαστε να συμπληρώσουμε κάποια πεδία, ένα από αυτά είναι το σε ποιό αρχείο θα αποθηκευτεί το public key, εκεί συμπληρώνουμε το αρχείο authorized_keys. Όπως βλέπουμε και παρακάτω το public key έχει αποθηκευτεί στο αρχείο authorized_keys.pub

```
netmg026@maria:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/netmg026/.ssh/id_rsa): authorized_keys
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in authorized_keys.
Your public key has been saved in authorized_keys.pub.
The key fingerprint is:
SHA256:131TPQh9q0sFFxGSL9hG/QWkNuq9bpARkQHgSYLQ4xg netmg026@maria
The key's randomart image is:
+---[RSA 2048]----+
|.o .. o...o=.o==+|
|E +  + .  o .*o+o|
| + .  o    .B.=.*|
|. .       .* = =o|
|        S +oo *  |
|         oo. + . |
|          ..o .  |
|            .o   |
|           oo    |
+----[SHA256]-----+
netmg026@maria:~$ ls
authorized_keys      index.txt.attr      my_file.crt  newcerts
authorized_keys.pub  index.txt.attr.old  my_file.csr  serial
index.txt            index.txt.old       my_file.key  serial.old
```

```
netmg026@maria:~$ cat authorized_keys
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA+XzCfOfXb7Pezj2BWm+W99mEuL8p5xdCW8Q7CiqJxQ83slKD
whK4TJcnv9OYXhKiujx/zqJWLzYa02pPowPIEBi7uokP9jRV6TCDBEa65Sv0tixE
eXjOfxXWM1dR6l8DlZlsthegaN8hiEmV6E0039eQhOTr8mn+4u4UBdlplJkXOziH
tmxKQSYtzcylIF9zk6gyDbr8uTsByTb3ROlg3Vk8sj8MfNq8HKRxrb7bnyV4vIVB
5BPkTqJWDjASRSeRJ4hibvwzILVsbYt6RoaRf5jFr0fkdFb6a8Mt6ohly/O5XcOD
bBZfm9jqbrefnorx5n6vQOvfZsiJGxAdbi79JQIDAQABAoIBABsEWKdgD+NnzhPl
cyGQ/f8/DfFXujjtOuFnIaGbM6okWLqlltDYaB7bK5HJXzGowPh7/rcouz6HlGYa
mB8mFK8xjnrHxvO5fSgwea+n3SteFDT6HDwvSeVXPwfajuNbgLXMQ26Apn1U1HPG
zDYIzlYDKQJLLAXnVpPKhl6QOJO/vZh932RnOlmtzBcKmkzYxHM4MH0x4GGWRxIB
aY+gPWiKmmw9H7ykBWczb8619YItBtGZ4aQT0tOT86oK04VCXSAl+GWKXDw//06Y
xGBiE82x3jGjN4fLLGcLlgJVF8z5zx+weh/xXzF7JWtkxrz0IJ/r+Nll3n7NHUtW
ceQEK6ECgYEA/uUbAWDA89Eh0/8k0aplrEh9vntH6ue5LmwXMccHnI2WbNpqHB+t
MI0ibat/mDgdmJystbYgU3DDrvHykCe6b6nA89SZ8rbNsJ+Ser0+WM6+cXWehrnt
kFlvXpdlinDPaiDZ7YAxjkshzn2Hwt+nvVu2NY/4vewan0fmhoddwk0CgYEA+pGn
EeK5DcG2u6zeGfbt3TnBmhUo4rpvAjXlmod2s4KV3jSNVnR9J09FKaBI/qUprLxf
DLl2p0npgGfdW3Fw8Ma2Wbw6Sto5RXfnN0LtGRB0UpVy7ZTMv5LkDuK0/mpFGFGr
AhXBSD+kI5sc9L40/qY/hROUX+UaxiI9oxPCojkCgYAvseD+vgL83GoPCBP0o4TI
2vukc97+JoPxGsqwRsS2l4uJLMlkH8lBY3dIvClw6zcmglKS4dRkqJoFF0LDFJv/
Hul68pIn52rPnNxE2TpcVbsu8cpK/WlldQZMldxpnjhBbIo6tZ0QOiDGSZjorv7t
IMcUeK8boplMpqCNFbFGlQKBgQCVDlQ+lYrUHipgFoPBGl2BvrvmtzOtPI6Q2BMQ
DAmW29Xfa4+woHdbDRLtokYKBaJ2+U/pukN9XMCk/CR4IlG2Sd9sHkbnBE4RfzRy
cUOuJlWrUvAdWOk8BVvZZw+YUQttXhfGk755BjLUY4+kIApSef9LYMxhBl8YAoJ8
ImMkMQKBgD88AB+epugIJaA/esLsDCTL0HfHPm4fLRXDw4FrFTqLVRACkVlxCRx7
3nalD0vPLIV9YnFvR9EcC3Hza+R346Ugvh4B8HsocvcLNg2glvW5D9AVX0Xu5XPY
elLeTy0Tdamj2aPKrMBC74EpKAueRDtx+n4dD23QDpM5MWFIw8yl
-----END RSA PRIVATE KEY-----
netmg026@maria:~$ cat authorized_keys.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQD5fMJ859dvs97OPYFab5b32YS4vynnF0JbxDsKKonFDzeyUoPCErhM1
ye/05heEqK6PH/OolYvNhrTak+jA8gQGLu6iQ/2NFXpMIMERrrlK/S2LER5eM5/FdYyV1HqXwPVnWy2F6Bo3yGISZXoTT
Tfl5CE5Ovyaf7i7hQF3WmUmRc7OIe2bEpBJi3NzKUgX3OTqDINuvy5OwHJNvdE7WDdWTyyPwx82rwcpHGtvtufJXi8hUH
kE+ROolYOMBJFJ5EniGJu/DMgtWxti3pGhpF/mMWvR+R0Vvprwy3qiGXL87ldw4NsFl+b2Oput5+eivHmfq9A699myIkb
EBluLv01 netmg026@maria
```

Έχοντας δημιουργήσει το αρχείο authorized_keys.pub πάμε στα αρχεία του υπολογιστή μας και γράφουμε το εξής :



Πατώντας enter μας ανοίγει το cmd στο οποίο λαμβάνουμε ένα μήνυμα για το αν είμαστε σίγουροι ότι θέλουμε να συνδεθούμε, πατάμε yes και μετά enter στο επόμενο βήμα έχουμε μια προτροπή να συνδεθούμε με τους κωδικούς μας, πληκτρολογώντας τον συνδεόμαστε στο maria μέσω sftp client.