

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ
12η Εργαστηριακή Αναφορά
Χρήστος Ηλιακόπουλος
ΑΜ: 03120233

MAC = a0:36:bc:a9:7e:58/8c:c8:4b:7c:5d:73/ B0-22-7A-30-5D-D8

IP = 147.102.131.6/147.102.131.47/υπολογιστής σπιτιού

christos-System-Product-Name/christos-HN-WX9X

LINUX Ubuntu 22.04.3 LTS

ΑΣΚΗΣΗ 1

1.1)Status Code: 401 / Response Phrase: Authorization Required

1.2)WWW-Authenticate: Basic realm="Edu-DY TEST" το πεδίο και η μέθοδος πιστοποίησης είναι η Basic

1.3)Authorization: Basic ...

1.4)Basic ZWR1LWR5OnBhc3N3b3Jk

1.5) edu-dy:password

ZWR1LWR5OnBhc3N3b3Jk\r\n

For encoded binaries (like images, documents, etc.) use the file upload feature.

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supported).

< DECODE > Decodes your data into the area below.

edu-dy:password

1.6) Συμπεραίνουμε ότι η μέθοδος είναι αρκετά απλή και καθόλου ασφαλής καθώς δεν υπάρχει κρυπτογράφηση στα διαπιστευτήρια αλλά αντίθετα κωδικοποίηση σε Base64 και ο οποιοσδήποτε με μία καταγραφή της κίνησης μπορεί να τα αποκτήσει.

ΑΣΚΗΣΗ 2

2.1) TCP

2.2) Θύρα υπολογιστή μας: 52582 / Θύρα εξυπηρετητή: 22

2.3) Η θύρα 22

2.4) SSH

2.5) Protocol: SSH-2.0 / Λογισμικό: -OpenSSH_8.9p1

Ενδεχόμενα σχόλια: Ubuntu-3ubuntu0.6

2.6) Protocol: SSH-2.0 / Λογισμικό: OpenSSH_6.6.1_hpn13v11

Ενδεχόμενα Σχόλια: FreeBSD-20140420

2.7) 305 bytes

- curve25519-sha256
- curve25519-sha256@libssh.org

2.8) 16 αλγόριθμοι

- ssh-ed25519-cert-v01@openssh.com
- ecdsa-sha2-nistp256-cert-v01@openssh.com

2.9)

- chacha20-poly1305@openssh.com
- aes128-ctr

2.10)

- umac-64-etm@openssh.com
- umac-128-etm@openssh.com

2.11) none,zlib@openssh.com, zlib

2.12) curve25519-sha256@libssh.org . Τον εμφανίζει στα επόμενα 2 ssh μηνύματα τύπου elliptic στην επικεφαλίδα Key Exchange (method:curve25519-sha256@libssh.org)

2.13) ssh-ed25519

Προκύπτει από το KEX host key (type: ssh-ed25519)

2.14 SSH Version 2 (encryption:chacha20-poly1305@openssh.com
compression:none)

Άρα ο chacha20-poly1305@openssh.com

2.15) δεν εμφανίζεται κάποιος αλγόριθμος

2.16) none

2.17)

Elliptic Curve Diffie-Hellman Key Exchange Init

Elliptic Curve Diffie-Hellman Key Exchange Reply

New Keys

2.18) Εμφανίζει τον αλγόριθμο κρυπτογράφησης και συμπίεσης

2.19) Όχι, καθώς έχει πραγματοποιηθεί κρυπτογράφηση

2.20) Η ασφάλεια είναι αρκετά μεγαλύτερη σε σύγκριση με το κλασικό telnet και το http basic auth, λόγω της κρυπτογράφησης των δεδομένων που πραγματοποιείται αλλά και της χρήσης του public key που κατέχουν πελάτης και εξυπηρετητής

ΑΣΚΗΣΗ 3

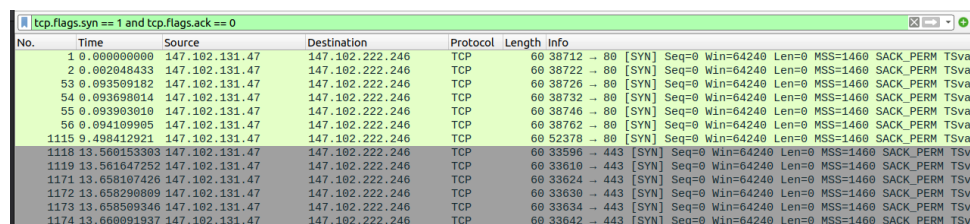
3.1) host www.noc.ntua.gr

3.2) tcp.flags.syn == 1 and tcp.flags.ack == 0

3.3) Στη θύρα 80 και 443

3.4) 80 για HTTP και 443 για HTTPS

3.5) 7 για σύνδεση HTTP και 6 για HTTPS



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	147.102.131.47	147.102.222.246	TCP	60	38712 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva
2	0.002048433	147.102.131.47	147.102.222.246	TCP	60	38722 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva
53	0.093599182	147.102.131.47	147.102.222.246	TCP	60	38726 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva
54	0.093699814	147.102.131.47	147.102.222.246	TCP	60	38732 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva
55	0.093903910	147.102.131.47	147.102.222.246	TCP	60	38746 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva
56	0.094109905	147.102.131.47	147.102.222.246	TCP	60	38762 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva
1115	9.498412921	147.102.131.47	147.102.222.246	TCP	60	52378 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva
1118	13.560153383	147.102.131.47	147.102.222.246	TCP	60	33596 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSV
1119	13.561647252	147.102.131.47	147.102.222.246	TCP	60	33610 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSV
1171	13.658107426	147.102.131.47	147.102.222.246	TCP	60	33624 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSV
1172	13.658290809	147.102.131.47	147.102.222.246	TCP	60	33630 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSV
1173	13.658569346	147.102.131.47	147.102.222.246	TCP	60	33634 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSV
1174	13.660091937	147.102.131.47	147.102.222.246	TCP	60	33642 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSV

3.6) 33596, 33610, 33624, 33630, 33634, 33642

3.7)

Content Type: 1 byte

Version: 2 bytes

Length: 2 bytes

3.8) Handshake(22), Change Cipher Spec(20), Application Data (23), Alert(21)

3.9) Client Hello (1), Server Hello (2), Certificate (11), Server Key Exchange (12), Server Hello Done (14), Client Key Exchange (16), New Session Ticket (4)

3.10) 6 μηνύματα και παρατηρούμε ότι είναι όσες είναι και οι συνδέσεις TCP για HTTPS

3.11)

Version: TLS 1.0 (0x0301)

3.12) Version: TLS 1.0 (0x0301), Όχι η έκδοση που θα χρησιμοποιηθεί από τον εξυπηρετητή είναι η version: TLS 1.2 (0x0303)

3.13) Είναι 32 bytes και τα πρώτα 4 bytes είναι σε 16δική αναπαράσταση 39 48 e6 5e και δείχνουν την ακριβώς από κάτω γραμμή: GMT Unix Time: Jun 15, 2000 17:21:18.000000000 EEST

3.14) Είναι 17 στο σύνολο τους

```
-----
Cipher Suites Length: 34
- Cipher Suites (17 suites)
  Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
  Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
  Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
  Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc030)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
  Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
  Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
  Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
  Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Compression Methods Length: 1
```

Με την πρώτη να έχει hex αναπαράσταση 13 01 και την δεύτερη 13 03

3.15) Υποστηρίζονται 2 tls εκδόσεις. Η tls 1.2 και η tls 1.3 με την tls 1.3 να έχει τιμή (0x0304)

```
- Extension: supported_versions (len=5)
  Type: supported_versions (43)
  Length: 5
  Supported Versions length: 4
  Supported Version: TLS 1.3 (0x0304)
  Supported Version: TLS 1.2 (0x0303)
- Extension: signature_algorithms (len=24)
```

3.16)

```
- Extension: application_layer_protocol_negotiation (len=14)
  Type: application_layer_protocol_negotiation (16)
  Length: 14
  ALPN Extension Length: 12
  - ALPN Protocol
    ALPN string length: 2
    ALPN Next Protocol: h2
    ALPN string length: 8
    ALPN Next Protocol: http/1.1
```

Το h2 και το http/1.1

3.17) Θα χρησιμοποιηθεί η έκδοση 1.2

Version: TLS 1.2 (0x0303)

3.18) Είναι ξανά 32 bytes και τα 4 πρώτα bytes έχουν την hex μορφή: c1 fb fe 9e. Παρατηρώ ότι δεν είναι ίδια η μορφή τους με το ερώτημα 3.13. Δεν προκύπτει κάποιο συμπέρασμα, εκτός ίσως ότι η παραγωγή τους είναι random

3.19) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) με hex τιμή c02f

3.20)

Key exchange/agreement: ECDH

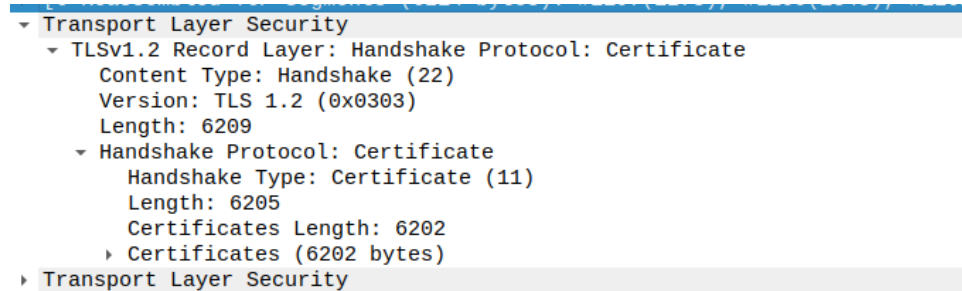
Authentication: RSA

Encryption: GCM

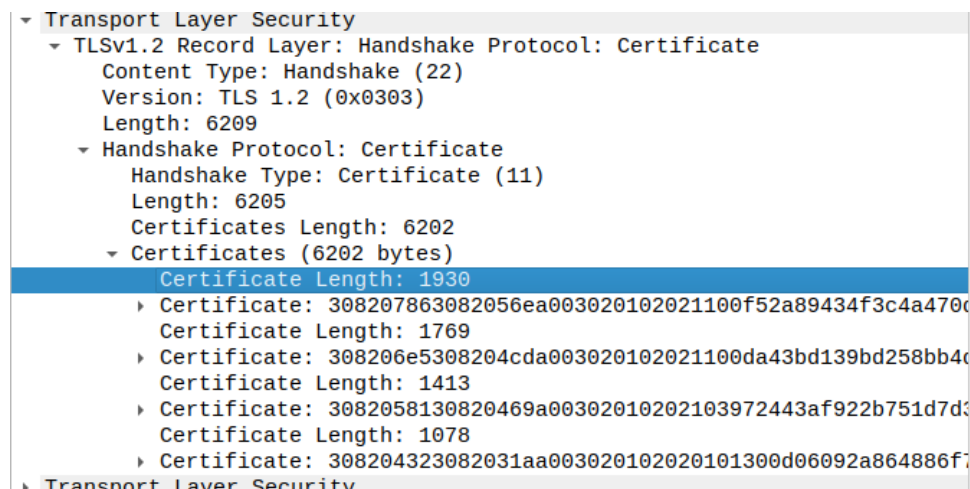
Hash Function: SHA256

3.21) Όχι, Compression Method: null (0)

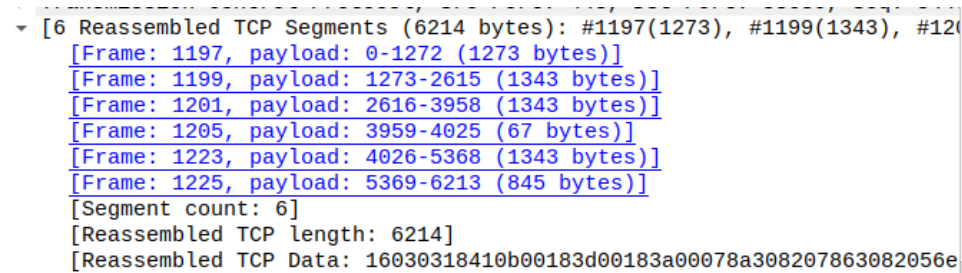
3.22) Length: 6209



3.23) 4 πιστοποιητικά με μήκη 1930, 1769, 1413, 1078 bytes αντίστοιχα το κάθε ένα

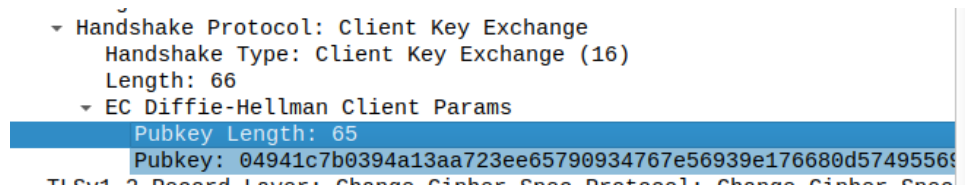


3.24) 6 tcp segments συνολικά άρα και 6 πλαίσια ETHERNET

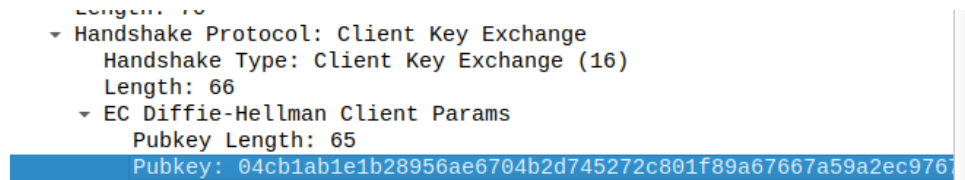


3.25)

Client: 65 bytes με 04941 τα 5 πρώτα γράμματα



Server: 65 bytes με 04cb1 τα 5 πρώτα γράμματα



3.26) 6 bytes το μήκος της εγγραφής και 1 byte του αντίστοιχου μηνύματος

3.27) Length: 40 bytes

3.28) Ναι

3.29) HTTP

3.30) Ναι. Και από τις δύο μεριές στάλθηκαν

3.31) Τα μηνύματα Alert στο πρωτόκολλο TLS χρησιμοποιούνται για να επικοινωνήσουν σημαντικές πληροφορίες σχετικά με την ασφάλεια της σύνδεσης. Το "Encrypted Alert" είναι ένα είδος Alert που μεταφέρει ενημερώσεις σχετικά με τον τρόπο που η συνδεσιμότητα κρυπτογραφίας (encryption) χειρίζεται μεταξύ του πελάτη (client) και του διακομιστή (server) σε μια σύνδεση TLS. Μερικοί λόγοι που μπορεί να σταλθεί είναι

- Σφάλμα κρυπτογραφίας (Cryptographic Errors)
- Αλλαγές στο Κλειδί (Key Changes)
- Λήξη Σύνδεσης (Connection Closure)

Εδώ πέρα παρατηρούμε πως τα κλειδιά στέλνονται μετά το τέλος της τριπλής χειραψίας από την κάθε μεριά για κάποιον από τους προηγούμενους λόγους

3.32) Το κείμενο webmail εμφανίζεται στο πακέτο που στάλθηκε μόνο στην http σύνδεση. Αυτό συμβαίνει γιατί στην https είναι κρυπτογραφημένο

3.33) Το πρωτόκολλο HTTPS (Hypertext Transfer Protocol Secure) αποτελεί μια ασφαλέστερη έκδοση του πρωτοκόλλου HTTP, προσφέροντας προηγμένη ασφάλεια στη μεταφορά δεδομένων μεταξύ του πελάτη και του διακομιστή. Υπάρχει πιστοποίηση της αυθεντικότητας με την χρήση των certificates, εμπιστευτικότητα καθώς η μεταφορά των δεδομένων γίνεται με κρυπτογράφηση και τέλος ακεραιότητα λόγω των ψηφιακών υπογραφών και checksums που ελέγχονται για την διασφάλιση ότι δεν υπάρχει αλλοίωση των δεδομένων κατά τη μετάδοση.