Εθνικό Μετσόβιο Πολυτεχνείο
Δίκτυα Υπολογιστών
Χειμερινό Εξάμηνο 2022-2023
Όνομα:
Ιωάννης Μπασδέκης - 03119198

Όνοματεπώνυμο: Ιωάννης Μπασδέκης	**Ομάδα:** A1
Όνομα PC/ΛΣ: MacBook-Air-Giannes / macOS	**Ημερομηνία:** 14/12/2022
Διεύθυνση IP: 147.102.236.188	**Διεύθυνση MAC:** b0:be:83:20:37:35

12η Εργαστηριακή Αναφορά

Μέρος 1ο

1.1) 401 Authorization Required

1.2)WWW-Authenticate: Basic realm="Edu-DY TEST"\

1.3)Authorization

1.4) Basic ZWR1LWR5OnBhc3N3b3Jk

1.5) edu-dy:password

1.6) Είναι αρκετά unsecure καθώς οποιοσδήποτε μπορεί να βρει τα διαπιστευτήρια αν έχει το πακέτο αυτό

Μέρος 2ο

2.1) TCP

2.2) 22, 51554

2.3) 22

2.4) ssh

2.5) Έκδοση: SSH 2.0
Λογισμικό: OpenSSH_6.6.1_hpn13v11 FreeBSD-20140420
Δεν περιλαμβάνονται σχόλια

2.6) Έκδοση: SSH 2.0
Λογισμικό: OpenSSH 9.0
Δεν περιλαμβάνονται σχόλια

2.7) 10 αλγόριθμοι
sntrup761x25519-sha512@openssh.com
curve25519-sha256

2.8) 12 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

2.12) curve25519-sha256@libssh.org
Εμφανίζεται σε παρένθεση στο πεδίο Key Exchange (method : curve25519-sha256@libssh.org)

2.13) chacha20-poly1305@openssh.com

2.14) umac-64-etm@openssh.com

2.15) none

2.16) Ναι, σε παρένθεση δίπλα στο SSH Version 2

2.17) Elliptic Curve Diffie-Hellman Key Exchange Init
Elliptic Curve Diffie-Hellman Key Exchange Reply
New Keys

2.18) Όχι γιατί έχει γίνει κρυπτογράφηση

2.19) Σε σχέση με άλλα πρωτόκολλα είναι με διαφορά το πιο ασφαλές σε όλους τους τομείς(πιστοποίηση αυθεντικότητας, εμπιστευτικότητα, ακεραιότητα δεδομένων)

3.1) host bbb2.cn.ntua.gr

3.2) (tcp.ack == 0 or tcp.ack == 1) and (tcp.seq == 0 or tcp.seq == 1) and tcp.len ==0

3.3) 80 , 443

3.4) HTTP -> 80
HTTPS -> 443

3.5) Για HTTP -> 6
Για HTTPS -> 1

3.6) client -> server : tcp source port = 52116
server -> client : tcp source port = 443

3.7) Content Type : 1 byte
Version : 2 bytes
Length : 2 bytes

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

3.9) TLS 1.2 : 0x0303

3.10) Client Hello (1)
Server Hello (2)
Certificate (11)
Server Key Exchange (12)
Server Hello Done (14)
Client Key Exchange (16)
New Session Ticket (4)
Encrypted Handshake Message (δεν έχει τιμή γιατί το βγάζει το wireshark)

3.11) ΄Ενα μήνυμα Client Hello αφού έχουμε μόνο μια tcp σύνδεση για HTTPS

3.12) TLS 1.0 : 0x0301
΄Οχι δεν είναι

3.13) 3
Reserved (GREASE) (0x7a7a)
TLS 1.3 (0x0304)
TLS 1.2 (0x0303)

3.14) 2
h2
http/1.1

3.15)32 bytes
Unix GMT timestamp (0xa2ed352f)

3.16) 16
Reserved (GREASE) (0x7a7a)
TLS_AES_128_GCM_SHA256 (0x1301)

3.17) TLS 1.2 : 0x0303

3.18) 32 bytes
Unix GMT timestamp (0x62261af3)

3.19) Όχι (Compression Method: null (0))

3.20) Cipher Suite:
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
KEX: ECDHE
Authentication Mechanism: RSA
Cypher: AES128 (το 128 είναι το μήκος κλειδιού κρυπτογράφησης σε bits
Hash Function:SHA256 (το 256 είναι το Digest Size σε bits)

3.21) 4276 bytes

3.22) 3 πιστοποιητικά
1574 bytes
1306 bytes
1380 bytes

3.23) 4

3.24) Client : 32 bytes , b1f2c
Server: 32 bytes , fc32d

3.25) 6 bytes συνολικά 1 byte το μήνυμα

3.26) 40 bytes

3.27) Ναι

3.28) HTTP

3.29) Όχι

3.30) -

3.31) Η αναζήτηση στην περίπτωση του πρωτοκόλλου HTTPS δεν βρίσκει κάτι σε αντίθεση με το HTTP καθώς τα δεδομένα είναι κρυπτογραφημένα

3.32) Είναι μακράν πιο ασφαλές από το απλό HTTP καθώς όλα είναι κρυπτογραφημένα. Αυτό συμβαίνει χάρης την πιστοποίηση της αυθεντικότητας, την εμπιστευτικότητα και την ακεραιότητα των δεδομένων τα οποία είναι και αυτά ασφαλείς και δεν υπάρχουν στο HTTP