Ονοματεπώνυμο: Άννα Καστάνη	Ομάδα: 2
Όνομα PC/ΛΣ: DESKTOP-9OFT571/ Windows 11 Home - 64bit	Ημερομηνία: 09/01/2024
Διεύθυνση IP: 147.102.200.81	Διεύθυνση MAC: 1C-BF-CD-41-64-DD

Εργαστηριακή Άσκηση 12
Ασφάλεια

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 Status Code: 401 Response Phrase: 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 ανεπαρκής και δεν προσφέρει αξιοπιστη κρυπτογράφηση

2

2.1 TCP

2.2 Υπηρεσιών: 50820 Εξυπηρετικής: 22

2.3 Η θύρα 22

2.4 ssh

2.5 Έκδοση Πρωτοκόλλου: SSH-2.0
Έκδοση λογισμικού: PuTTY_Release_0.76
Σχόλια δεν υπάρχουν

2.6 Έκδοση Πρωτοκόλλου: SSH-2.0
Έκδοση λογισμικού: OpenSSH_6.6.1_hpn13v11
Σχόλια: FreeBSD-20140420

2.7 kex_algorithms length: 315
13 αλγόριθμοι
Δύο πρώτοι αλγόριθμοι: curve448-sha512, curve25519-sha256

2.8 9 αλγόριθμοι
ssh-ed448, ssh-ed25519

2.9 aes256-ctr, aes256-cbc

2.10 hmac-sha2-256, hmac-sha1

2.11 none, zlib

2.12 curve25519-sha256@libssh.org Είναι ο πρώτος κοινός σαν δυο λίστων. Εμφανίζεται στα πεδία Key-Exchange, αλλά όχι καινα, χειριστά

2.13 ssh-ed25519

2.14 aes256-ctr

2.15 hmac-sha2-256

2.16 none

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

2.18 Ναι στο παρένθεση δίπλα στο πεδίο SSH Version 2

2.19 Όχι, διότι είναι κρυπτογραφημένα.

2.20 Σε σύγκριση με το Telnet είναι ασφαλέστερο, αφού όλο κρυπτογραφείται και χάλιστα με χειριστούς αλγορίθμους

3

3.1 host www.noc.ntua.gr

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

3.3 Στις θύρες 80 και 443

3.4 80 → HTTP, 443 → HTTPS

3.5 6 για http και 6 για https

3.6 51331, 51332, 51333, 51334, 51335, 51336

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), #

3.10 6 μηνύματα Client Hello, όσα δηλαδή και οι συνδέσεις https

3.9. Client Key Exchange (16), Encrypted Handshake Message, New Session Ticket (4)

3.11 Version: TLS 1.0 με τιμή 0x0301

3.12 Version: TLS 1.2 με τιμή 0x0303

3.13 32 bytes. Τα πρώτα 4 bytes: 0a 8d 6c bf και παριστάνουν το GMT Unix Time: Aug 12, 1975 04:56:15.000000000 Ώρινή Ώρα GTB

3.14 16 cipher suites
2 πρώτες: 0x baba, 0x1301

3.15 Δηλώνουν ότι: TLS 1.2, TLS 1.3 → TLS 1.3 → 0x0304

3.16 h2, http/1.1

3.17 TLS 1.2 (0x0303)

3.18 32 bytes, Τα πρώτα 4 bytes: 0c b3 71 63
Παράγονται τυχαία

3.19 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

3.20 Ανταλλαγής Κλειδιών (Key Exchange): ECDHE
Πιστοποίησης Ταυτότητας (Authentication): RSA
Κρυπτογράφησης (Encryption): GCM
Συνάρτηση Κατακερματισμού (Hash function): SHA

3.21 Όχι: Compression Method: null (0)

3.22 6202 bytes

3.23 4 πιστοποιητικά με μήκη: 1930 bytes, 1769 bytes, 1413 bytes, 1078 bytes

3.24 5 πλαίσια

3.25 Εξυπηρετητής: Pubkey Length: 65, 040be
Πελάτης: Pubkey Length: 65, 0455b

3.26 Μήκος Εγγραφής: 6 bytes, Μήκος Μηνύματος: 1 byte

3.27 40 bytes

3.28 Ναι

3.29 HTTP

3.30 Ναι. Από την πλευρά του εξυπηρετητή

3.31 Υποδεικνύει τον τερματισμό της μεταδόσης δεδομένων και αίρει την διασύνδεση TCP

3.32 Στο HTTPS δεν μπορούμε να βρούμε το πακέτο που περιέχει τη φράση γιατί τα δεδομένα είναι κρυπτογραφημένα, ενώ στο HTTP μπορούμε

3.33 Το HTTPS είναι ασφαλέστερο διότι σχεδόν όλα τα δεδομένα είναι κρυπτογραφημένα και προστατεύεται η ακεραιότητα τους