Windows 10

Ονοματεπώνυμο: Δημήτρης Βασιλάκης	**Ομάδα:** 3
Όνομα PC/ΛΣ: LAPTOP-NMV173NU	**Ημερομηνία:** 11 / 01 / 2023
Διεύθυνση IP: 147.102.202.252	**Διεύθυνση MAC:** 5C-61-99-02-FA-83

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

Για άσκ 1: IPv4: 192.168.1.7

1.1 Μήνυμα 401. Authorization Required

1.2 Το πεδίο είναι WWW-Authenticate και περιέχει πιστοποίηση η Basic

1.3 Authorization

1.4 Credentials: edu-lab: password

1.5 ZWR1LWR5OnBhc3N3b3Jk

1.6 Συμπεραίνουμε ότι ο μηχανισμός ασφάλειας δεν είναι πολύ καλός, διότι τα credentials δεν κρυπτογραφούνται και φαίνονται κανονικά

2

Για άσκ 2: IPv4: 147.102.202.252

2.1 Το TCP

2.2 Source Port: 63087 (τυχαία) , Destination Port: 22

2.3 Η 22

2.4 SSH

2.5 έκδοση πρωτοκόλλου SSH: SSH-2.0
έκδοση λογισμικού: OpenSSH_6.6.1_hpn13v11
έχουν: FreeBSD-20140420

2.6 έκδοση πρωτοκόλλου SSH: SSH-2.0
έκδοση λογισμικού: PuTTY_Release_0.76
Ο πελάτης δεν έχει κάτι.

2.7 Υποστηρίζονται 14 αλγόριθμοι. Οι πρώτοι δύο είναι οι curve448-sha512, curve25519-sha256.

2.8 Υποστηρίζονται 8 αλγόριθμοι. Οι πρώτοι δύο είναι οι ssh-ed448, ssh-ed25519

2.9 aes256-ctr, aes256-cbc

2.10 hmac-sha2-256, hmac-sha1

2.11 zlib, zlib@openssh.com

2.12 Ο αλγόριθμος είναι ο curve25519-sha256@libssh.org. Εμφανίζεται στο πεδίο key Exchange

2.13 O aes256-ctr

2.14 O hmac-sha2-256

2.15 Δεν χρησιμοποιείται συμπίεση (compression: none)

2.16 Εμφανίζονται με παρενθέσεις στο πεδίο SSH Version 2 του SSH protocol.

2.17 Βλέπουμε τους τύπους μηνυμάτων: Elliptic Curve Diffie-Hellman key Exchange Init, Elliptic Curve Diffie-Hellman key Exchange Reply και New keys.

2.18 Δεν μπορούμε, διότι όλα τα μηνύματα έχουν κρυπτογραφηθεί.

Για αυτή ↓ IP: 192.168.1.7

2.19 Στο telnet ό,τι δίνει ο χρήστης, μεταφέρεται αυτούσιο χωρίς κρυπτογράφηση στον εξυπηρετητή. Στο SSH γίνεται ισχυρή κρυπτογράφηση και έτσι προστατεύεται η εμπιστευτικότητα. Επίσης με το μηχανισμό ψηφιακού κλειδιού, πιστοποιείται η αυθεντικότητα κάθε πλευράς.

3

3.1 host 147.102.40.19

3.2 tcp.seq==0 and tcp.ack==0

3.3 Στις 80 και 443

3.4 Η 80 για http και η 443 για https

3.5 Ανοίχτηκαν 6 συνδέσεις για https και 2 για https

3.6 Source Port: 57386, 57387, 57389, 57390, 57391, 57392

3.7 Πεδία Content-Type: 2 bytes, Version: 4 bytes και Length: 4 bytes.

3.8 Handshake(22), Application Data(23),

3.9 TLS 1.2

3.10 Client Hello(1), Client key Exchange(16), Server Hello(2), Certificate(11), New Session Ticket(4)

3.11 2 πακέτα Client Hello, ίδια κρυπτ. για τη σύνδεση TCP στο HTTPS

3.12 Έκδοση TLS 1.0. Δεν είναι ασφαλής

3.13 Υποστηρίζει 5 εκδόσεις: TLS 1.3, TLS 1.2, TLS 1.0, TLS 1.1, SSL 3.0
Για TLS 1.3 η τιμή είναι 0x0304

3.14 Τα http/1.1 και h2

3.15 32 bytes. f4 0c 75 69. Παρατήρησα τη τρίτη έκδοση για προηγούμενα SSL/TLS που υποστηρίζει ο πελάτης.

3.16 Πλήθος 16. Δύο τιμές: 0x1301, 0x1302

3.17 Version: TLS 1.2

3.18 32 bytes. Δεν δεν το βλέπω.

3.19 Όχι, δεν χρησιμοποιείται

3.20 Cipher Suite: TLS-ECDHE-RSA-WITH-AES_128-GCM-SHA256, 0xC02f.
key exchange: ~~ECDHE~~ ECDHE, Auth: RSA, Bulk Encryption: GCM,
Hash: SHA256

3.21 Length: 4216 bytes

3.22 Μεταφέρονται 3 πιστοποιητικά. 1ο: 1574 bytes, 2ο: 1306 bytes,
3ο: 1380 bytes

3.23 Η πλαίσια Ethernet

3.24 Μήκος πλαισίου πελάτη: 326 bytes, Μήκος πλαισίου εξυπηρετητή: 326 bytes
f556 6707

3.25 Μήκος εγγραφής: 6 bytes, Μήκος μηνύματος: 1 byte

3.26 Μήκος 45 bytes.

3.27 Ναι

3.28 Του TCP.

3.29 Όχι

3.30 Δεν υπήρχαν

3.31 Δεν μπορούμε να βρούμε αυτό το πακέτο. Από εδώ και πέρα, όσα πακέτα κρυπτογραφούνται, οι απαντήσεις για το HTTP, όπου η εύρεση είναι εύκολη.

3.32 Στο HTTPS οι τιμές κρυπτογράφησης και αυθεντικότητας προφέρουν ασφάλεια και εμπιστευτικότητα, ό.ε απ' όσα για το HTTP όπου είναι εύκολη η υκλοπή πληροφοριών.