Ονοματεπώνυμο: Παναγιώτης Ζευγολατάκος	**Ομάδα: 3**
Όνομα PC/ΛΣ: panos/Windows 10	**Ημερομηνία: 9/1/2021**
Διεύθυνση IP: 192.168.0.7	**Διεύθυνση MAC: 30–24–32–79–09–14**

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

1.1 401 Authorization Required

1.2 Authorization

1.3 Authorization: Basic edu-dy:password

1.4 edu-dy:password

1.5 Δεν μπορούμε να πούμε πως ο βασικός μηχανισμός πιστοποίησης αυθεντικότητας που παρέχει το HTTP είναι ασφαλής, εφόσον μπορέσαμε να το αποκρυπτογραφήσουμε με ευκολία χρησιμοποιώντας ένα online calculator.

2

2.1 TCP

2.2 Χρησιμοποιούνται οι θύρες 57121 και 22.

2.3 Η θύρα 22.

2.4 ssh

2.5 Protocol: SSH-2.0 (έκδοση πρωτοκόλλου) - OpenSSH_5.8p2_hpn13v11 (έκδοση λογισμικού) FreeBSD -20110503 (σχόλια)

2.6 Protocol: SSH-2.0 (έκδοση πρωτοκόλλου) - PuTTY_Release_0.74 (έκδοση λογισμικού)

2.7 Είναι 11 και οι πρώτοι δύο είναι: curve25519-sha256@libssh.org, ecdh-sha2-nistp256

2.8 Είναι 6 και ο πρώτος είναι: ecdsa-sha2-nistp256

2.9 aes256-ctr, aes256-cbc

2.10 hmac-sha2-256, hmac-sha1

2.11 none, zlib

2.12 Επέλεξε τον 1^{ο} από τη λίστα αλγορίθμων του πελάτη και εμφανίζεται στο method του Key Exchange:
Key Exchange (method:ecdh-sha2-nistp256)

2.13 aes128-ctr

2.14 hmac-sha1

2.15 none

2.16 Εμφανίζονται δίπλα στο SSH Version 2 σε όλα τα επόμενα πακέτα:
SSH Version 2 (encryption:aes256-ctr mac:hmac-sha1 compression:none)

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

2.18 Λογικά θα βρίσκονται σε κάποιο Encrypted Packet, εφόσον η σύνδεση έχει γίνει και τα μηνύματα μεταφέρονται πλέον κρυπτογραφημένα.

2.19 Το SSH είναι ασφαλές, εφόσον η πιστοποίηση της αυθεντικότητας εξασφαλίζεται με το Authentication Protocol και η εμπιστευτικότητα και η ακεραιότητα εξασφαλίζονται μέσω της κρυπτογράφησης, σε αντίθεση με άλλα πρωτόκολλα, όπως το HTTP που είδαμε προηγουμένως.

3

3.1 host 147.102.222.242

3.2 tcp.flags.syn == 1

3.3 Στις θύρες 80 και 443.

3.4 HTTP → θύρα 80
HTTPS → θύρα 443

3.5 Για την HTTP ανοίχθηκαν 5 συνδέσεις ενώ για την HTTPS ανοίχθηκαν 6 συνδέσεις.

3.6 Χρησιμοποιήθηκαν οι θύρες: 57831-57836.

3.7 Content → 1 byte, Version → 2 bytes, Length → 2 bytes

3.8 Content Type: Handshake (22)
Content Type: Change Cipher Spec (20)
Content Type: Application Data (23)
Content Type: Alert (21)

3.9 Handshake Type: Client Hello (1)
Handshake Type: Server Hello (2)
Handshake Type: Certificate (11)
Handshake Type: Server Key Exchange (12)
Handshake Type: Server Hello Done (14)
Handshake Type: Client Key Exchange (16)
Handshake Type: New Session Ticket (4)
Encrypted Handshake Message

3.10 Ο πελάτης έστειλε 6 μηνύματα Client Hello, δηλαδή τόσα όσα και οι συνδέσεις TCP.

3.11 Version: TLS 1.2 (0x0303)

3.12 Το μήκος του τυχαίου αριθμού που περιέχει είναι 32 bytes και τα πρώτα 4 είναι: d8, 36, 01, c3, τα οποία παριστάνουν την ημερομηνία:
GMT Unix Time: Dec 12, 2084 02:07:31.000000000 GTB Standard Time

3.13 Είναι 16 και τα δύο πρώτα από αυτά είναι:
Cipher Suite: Reserved (GREASE) (0x7a7a)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

3.14 Version: TLS 1.2 (0x0303)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

3.15 Το μήκος του τυχαίου αριθμού που περιέχει είναι 32 bytes και τα 4 πρώτα είναι: 71, fa, fd, bd, τα οποία παριστάνουν την ημερομηνία:
GMT Unix Time: Aug 6, 2030 22:19:25.000000000 GTB Daylight Time

3.16 Όχι, εφόσον ο πελάτης δηλώνει 'null' ως μέθοδο συμπίεσης.

3.17 Ανταλλαγή κλειδιών: EC Diffie-Hellman
Πιστοποίηση ταυτότητας: RSA
Κρυπτογράφηση: AES 256 GCM
Συνάρτηση κατακερματισμού: SHA 384

3.18 Certificates Length: 6297

3.19 Μεταφέρονται 4 πιστοποιητικά:
my.ntua.gr
GEANT OV RSA CA 4
USERTrust RSA Certification Authority
uTF8String: AAA Certificate Services

3.20 5

3.21 Και τα δύο έχουν μήκος 65 bytes και τα πρώτα 5 γράμματα του δημόσιου κλειδιού του πελάτη είναι 0401d ενώ του εξυπηρετητή είναι 045a2.

3.22 6 bytes

3.23 45 bytes

3.24 Ναι

3.25 Ναι, από τη μεριά του εξυπηρετητή.

3.26 Λογικά υπάρχουν επειδή έκλεισα τη σελίδα, εφόσον είναι οι τελευταίες εγγραφές στη συγκεκριμένη σύνδεση TCP.

3.27 Στην περίπτωση του πρωτοκόλλου HTTP μπορούμε να το βρούμε, ενώ στην περίπτωση του πρωτοκόλλου HTTPS δεν είναι εφικτό λόγω κρυπτογράφησης.

3.28 Σε αντίθεση με το πρωτόκολλο HTTP που δεν είναι ασφαλές όσον αφορά την πιστοποίηση της αυθεντικότητας, την εμπιστευτικότητα και την ακεραιότητα, το πρωτόκολλο HTTPS φροντίζει για όλα: Κρυπτογράφηση → εμπιστευτικότητα/ακεραιότητα, Certificates → πιστοποίηση της αυθεντικότητας.