Ονοματεπώνυμο: Χαράλαμπος Καμπουγέρης

Όνομα PC/ΛΣ: CHARALAMPOSs-MacBook-Air/ macOS 14.0

Διεύθυνση IP:147.102.131.130

Ομάδα: 3, Τετάρτη 10:45-12:30, Αιθ.Α2

Ημερομηνία: 23/01/2024

Διεύθυνση MAC: 0c:e4:41:e1:6c:74

Εργαστηριακή Άσκηση
Αναλυτής Πρωτοκόλλων Wireshark

Άσκηση 1

1.1 401 Authorization Required

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

1.3 Authorization

1.4 ZWR1LWR5OnBhc3N3b3Jk

1.5 edu-dy:password

1.6 Πρόκειται για έναν ανεπαρκή μηχανισμό που πρακτικά δεν παρέχει καμία ασφάλεια για τα σημερινά δεδομένα

Άσκηση 2

2.1 TCP

2.2 49501 και 22

2.3 Η 22

2.4 ssh

2.5 Ο πελάτης χρησιμοποιεί SSH v2.0 και OpenSSH v9.0. Σχόλια δεν υπάρχουν

2.6 Χρησιμοποιείται το SSH v2.0 με λογισμικό OpenSSH v6.6.1. Στα σχόλια αναφέρεται FreeBSD-20140420

2.7 Μήκος συμβολοσειράς kex-algorithms: 276 bytes
11 αλγόριθμοι συνολικά και οι πρώτοι 2 είναι οι: sntrup761x25519 sha512@openssh.com και curve25519-sha256

2.8 12 αλγόριθμοι συνολικά και οι πρώτοι 2 είναι οι: ssh-ed25519-cert-v01@openssh.com και ecdsa-sha2-nistp256-cert-v01@openssh.com

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

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

2.11 none και zlib@openssh.com

2.12 Είναι ο curve25519-sha256@libssh.org. Το wireshark τον εμφανίζει δίπλα απο την επικεφαλίδα Key Exchange

2.13 ecdsa-sha2-nistp256-cert-v01@openssh.com

2.14 Στο πεδίο SSH Version 2 βλέπουμε το **encryption: chacha20-poly1305@openssh.com** Παρατηρούμε πως είναι ο πρώτος από τη λίστα του πελάτη που υπάρχει και στη λίστα του εξυπηρετητή.

2.15 umac-64-etm@openssh.com

2.16 none

2.17 Καταγράφηκαν οι τύποι: Elliptic Curve Diffie-Hellman Key Exchange Init, Elliptic Curve Diffie-Hellman Key Exchange Reply και New Keys

2.18 Εμφανίζει μόνο τον αλγόριθμο κρυπτογράφησης και συμπίεσης

```
> SSH Version 2 (encryption:chacha20-poly1305@openssh.com compression:none)
  [Direction: client-to-server]
```

2.19 Όχι, διότι τα μηνύματα είναι κρυπτογραφημένα

2.20 Το SSH είναι το ασφαλέστερο πρωτόκολλο που έχουμε εξετάσει μέχρι στιγμής διότι τα πάντα κρυπτογραφούνται πριν σταλούν

- Πιστοποίηση αυθεντικότητας: Έχουμε authentication μέσω public-private keys, από τις ασφαλέστερες δηλαδή μεθόδους
- Εμπιστευτικότητα: Λόγω της κρυπτογράφησης, το περιεχόμενο γίνεται κατανοητό μόνο από τον εξυπηρετητή και τον πελάτη.
- Ακεραιότητα δεδομένων: Παρέχονται hashing αλγόριθμοι για data-integrity (MAC)

Άσκηση 3

3.1 host 147.102.222.246

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

3.3 Στην 80 και 443

3.4 Η 80 στο HTTP και η 443 στο HTTPS

3.5 Τόσο για HTTP όσο και για και HTTPS 6 άνοιξαν 6 συνδέσεις

3.6 49890 και 498992

3.7 Είναι τα Content Type (1 byte), Version (2 bytes) και Length (2 bytes)

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

3.9 Client Hello (1), Server Hello (2), Certificate, Server Key Exchange,
Server Hello Done, Client Key Exchange, Encrypted Handshake Message

3.10 6 μηνύματα που αντιστοιχούν στις 6 συνδέσεις TCP

3.11 Version: TLS 1.2 (0x0303)

3.12 Version: TLS 1.0 (0x0301). Διαφέρει από την εγγραφή TLS

3.13 32 bytes και τα 4 πρώτα είναι τα: 0c 45 87 83. Παριστάνουν ημερομηνία
GMT Unix Time: Mar 21, 2072 12:35:47.000000000 EET

3.14 Πλήθος 16. Οι δύο πρώτες έχουν κωδικό (0xdada) και (0x1301) αντίστοιχα

3.15 Δηλώνονται οι εκδόσεις 1.2, 1.3. Η 1.3 έχει αριθμό 0x0304

3.16 h2 και http/1.1

3.17 TLS v1.2

3.18 32 bytes και τα 4 πρώτα είναι τα: c9 95 ad a7. Παριστάνουν ημερομηνία
GMT Unix Time: Mar 3, 2077 22:42:15.000000000 EET. Διαφέρουν άρα παράγονται τυχαία

3.19 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

3.20
Αλγόριθμος ανταλλαγής κλειδιών: Elliptic Curve Diffie-Hellman Ephemeral
(ECDHE)
Αλγόριθμος πιστοποίησης: Rivest Shamir Adleman (RSA)
Αλγόριθμος κρυπτογράφησης: Advanced Encryption Standard with 128bit key
in Galois/Counter mode (AES 128 GCM)
Αλγόριθμος συνάρτησης κατακερματισμού: Secure Hash Algorithm 256
(SHA256)

3.21 Όχι

3.22 6209 bytes

3.23 4 πιστοποιητικά με μήκοι 1930, 1769,1413,1078 bytes αντίστοιχα

3.24 6 πλαίσια ethernet

3.25 Το μήκος του κλειδιού είναι 65 bytes και στις δύο περιπτώσεις. Τα 4 πρώτα γράμματα του κλειδιού του πελάτη είναι 045c2, ενώ του εξυπηρετητή είναι 0448d

3.26 Μήκος μηνύματος 1 byte και μήκος εγγραφής 6 bytes

3.27 40 bytes

3.28 Ναι

3.29 HTTP

3.30 Ναι, στάλθηκαν από την πλευρά του εξυπηρετητή

3.31 Πρόκειται για ένα TLS notification το οποίο στέλνεται για να ειδοποιήσει ότι το session μεταξύ των δύο συσκευών σταματάει καθώς δεν υπάρχουν άλλα δεδομένα να σταλούν.

3.32 Στην περίπτωση του HTTP μπορούμε εύκολα να βρούμε τη πληροφορία που ψάχνουμε. Στο HTTPS τα δεδομένα είναι κρυπτογραφημένα οπότε δεν μπορούμε να βρούμε το πακέτο που περιλαμβάνει αυτή τη φράση

3.33 Το HTTPS είναι σαφώς πολύ πιο ασφαλές διότι όλα τα δεδομένα κρυπτογραφούνται για να σταλθούν. Έτσι, προστατευόμαστε από κακόβουλους χρήστες που ίσως βρίσκονται στο δίκτυο καθώς δεν μπορούν να δουν τα δεδομένα που στέλνουμε και λαμβάνουμε