Ονοματεπώνυμο: ΙΟΡΔΑΝΙΔΗΣ ΚΡΙΤΩΝ
Ομαδα: 1
Όνομα PC/OS: Kriton’s Air / MacOS 13.1
Ημερομηνία: 10/1/2023
Διεύθυνση IP: 147.102.239.189
Διεύθυνση MAC: –

ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 12: ΑΣΦΑΛΕΙΑ

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 52494 και 22
2.3 Η 22
2.4 ssh
2.5 Χρησιμοποιείται το SSH v2.0 με λογισμικό OpenSSH v6.6.1. Στα σχόλια αναφέρεται FreeBSD-20140420
2.6 Ο πελάτης χρησιμοποιεί SSH v2.0 και OpenSSH v9.0. Σχόλια δεν υπάρχουν
2.7 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 aes128-ctr
2.14 umac-64-etm@openssh.com
2.15 none
2.16 Όχι
2.17 Καταγράφηκαν οι τύποι: Elliptic Curve Diffie-Hellman Key Exchange Init, Elliptic Curve Diffie-Hellman Key Exchange Reply και New Keys
2.18 Όχι βέβαια, διότι τα μηνύματα είναι κρυπτογραφημένα
2.19 Το SSH είναι το ασφαλέστερο πρωτόκολλο που έχουμε εξετάσει μέχρι στιγμής διότι τα πάντα κρυπτογραφούνται πριν σταλούν

Άσκηση 3
3.1 host bbb2.cn.ntua.gr
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 Για HTTP ανοιξαν 4 συνδέσεις, ενώ για HTTPS 1 σύνδεση

3.6 61923
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 Είναι η έκδοση 1.2 (0x0303)
3.10 Client Hello, Server Hello, Certificate, Server Key Exchange, Server Hello Done, Client Key Exchange, Encrypted Handshake Message
3.11 1 μήνυμα που αντιστοιχεί στη μια σύνδεση TCP
3.12 Είναι η έκδοση v1.0 με αριθμό 0x0301. Προφανώς διαφέρει με την ερώτηση 3.9
3.13 Δηλώνονται οι εκδόσεις 1.0, 1.1, 1.2, 1.3. Η 1.3 έχει αριθμό 0x0304
3.14 h2 και http/1.1
3.15 32 bytes και τα 4 πρώτα είναι τα: 2c a5 72 b0
3.16 Υπάρχουν 26 σουίτες και 2 εξ' αυτών έχουν κωδικό 0x7a7a και 0x1301
3.17 TLS v1.2
3.18 Είναι 32 bytes. Τα πρώτα 4 είναι: e8 77 5b d0 και διαφέρουν απο αυτά του client άρα παράγονται τυχαία
3.19 Όχι
3.20 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
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 4276 bytes
3.22 1
3.23 4 πλαίσια ethernet]
3.24 Το μήκος του κλειδιού είναι 32 bytes και στις δύο περιπτώσεις. Τα 4 πρώτα γράμματα του κλειδιού του πελάτη είναι 5f7d6, ενώ του εξυπηρετητή είναι bba6d
3.25 Μήκος μηνύματος 1 byte και μήκος εγγραφής 6 bytes
3.26 40 bytes
3.27 Όχι
3.28 HTTP
3.29 Όχι
3.30 -
3.31 Στο HTTPS τα δεδομένα είναι κρυπτογραφημένα οπότε δεν μπορούμε να βρούμε το πακέτο που περιλαμβάνει αυτή τη φράση
3.32 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