Ονοματεπώνυμο: Παναγιώτης Σταματόπουλος		**Ομάδα:** 6
Όνομα PC/ΛΣ: TakisAsus/Windows 10	**Ημερομηνία:** 16/1/24	
Διεύθυνση IP: 192.168.2.4	**Διεύθυνση Mac:** D4-5D-64-59-27-5F	

ΑΜ: el20096

Εργαστηριακή Άσκηση 12
Ασφάλεια

Άσκηση 1:

*Στον προσωπικό υπολογιστή

1.1: 401 Authorization Required
1.2: WWW-Authenticate
1.3: Authorization
1.4: Authorization: Basic ZWR1LWR5OnBhc3N3b3Jk..
1.5: edu-dy:password
1.6: Ο βασικός μηχανισμός πιστοποίησης αυθεντικότητας δεν παρέχει ασφάλεια λόγω έλλειψης εμπιστευτικότητας, αφού τα δεδομένα δεν κρυπτογραφούνται, απλά κωδικοποιούνται

Άσκηση 2:

*Στον προσωπικό υπολογιστή με σύνδεση VPN στο δίκτυο της σχολής IP: 147.102.131.132, MAC: 00-FF-43-66-F7-C9

2.1: TCP
2.2: 62892, 22
2.3: 22
2.4: ssh
2.5: Version: 2.0, Software: PuTTY_Release_0.74 δεν περιλαμβάνονται σχόλια
2.6: Version: 2.0, Software: OpenSSH_6.6.1_hpn13v11, Comments: FreeBSD-20140420
2.7: 270 χαρακτήρες: curve25519-sha256@libssh.org, ecdh-sha2-nistp256 κλπ
2.8: 6 αλγόριθμοι: ssh-ed25519, ecdsa-sha2-nistp256
2.9: aes256-ctr και aes256-cb
2.10: hmac-sha2-256 και hmac-sha1
2.11: none και zlib

2.12: curve25519-sha256@libssh.org, εμφανίζεται στο πεδίο Key Exchange (method)
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
New Keys
2.18: Στο SSH Version 2 εμφανίζεται το encryption, mac και compression
2.19: Δεν μπορούμε γιατί τα πακέτα έχουν κρυπτογραφηθεί
2.20: Η πιστοποίηση της αυθεντικότητας γίνεται με κλειδιά, η εμπιστευτικότητα με κρυπτογράφηση που είναι γνωστή μόνο από τον πελάτη και τον εξυπηρετητή και η ακεραιότητα με hashing, καθιστώντας έτσι το SSH πιο ασφαλές από άλλα πρωτόκολλα, όπως το Telnet και το HTTP

Άσκηση 3:

*Στον προσωπικό υπολογιστή IP: 192.168.2.2

3.1: host www.noc.ntua.gr

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

3.3: 80 και 443

3.4: HTTP: 80, HTTPS: 443

3.5: 6 HTTP και 6 HTTPS

3.6: 50605, 50606, 50607, 50608, 50609, 50610

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,
Client Key Exchange 16, New Session Ticket 4

3.10: 6 όσες και οι TCP συνδέσεις για HTTPS όπως περιμέναμε

3.11: TLS 1.0 (0x0301)

3.12: TLS 1.2 (0x0303) δεν είναι ταυτόσημες

3.13: 32 bytes, f1 3b b4 d6 GMT Unix Time

3.14: 16: 0x4a4a και 0x1301

3.15: 2 Versions: TLS 1.3 (0x0304) και TLS 1.2 (0x0303)

3.16: h2 και http/1.1

3.17: TLS 1.2

3.18: 32 bytes, 85 75 e4 a0 GMT Unix Time, τα 4 πρώτα bytes
είναι τα δευτερόλεπτα που προσθέτουμε στη χρονική
στιγμή 00:00:00 UTC, 1 Ιανουαρίου 1970 και παίρνουμε
το GMT Unix Time σαν αποτέλεσμα

3.19: Cipher Suite:
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
(0xc02f)

3.20: Ανταλλαγή Κλειδιών: ECDHE
Πιστοποίηση Ταυτότητας: RSA
Κρυπτογράφηση: AES (128 bits)
Συνάρτηση Κατακερματισμού: SHA (256 bits)

3.21: null (0)

3.22: 6209 bytes

3.23: 4 Certificates: 1930, 1769, 1413 και 1078 bytes αντίστοιχα
3.24: 5
3.25: Client: 65 bytes (04779), Server: 65 bytes (04804)
3.26: 6 bytes, 1 byte
3.27: 40 bytes
3.28: Ναι
3.29: HTTP
3.30: Ναι, από τον εξυπηρετητή
3.31: Απόλυση της σύνδεσης
3.32: Μπορούμε να το εντοπίσουμε για HTTP αλλά όχι για HTTPS, αφού είναι encrypted
3.33: Στο HTTPS επαληθεύεται η γνησιότητα του πελάτη με την ανταλλαγή κλειδιών, τα δεδομένα στέλνονται κρυπτογραφημένα και η ακεραιότητα των δεδομένων ελέγχεται με τον αλγόριθμο MAC, καθιστώντας το έτσι ασφαλέστερο πρωτόκολλο από το HTTP