Ονοματεπώνυμο: Δημήτριος Βασιλείου		Ομάδα: 3
Όνομα PC/ΛΣ: LAPTOP-N4VI73NU/Windows 10	Ημερομηνία: 12/10/2022	
Διεύθυνση IP: 147.102.238.249	Διεύθυνση MAC: 5C-61-99-02-FA-83	

Εργαστηριακή Άσκηση 2
Ενθυλάκωση και Επικεφαλίδες

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 Εξαμήνουσα πακέτα ARP ή IP.

1.2 Destination, Source, Type

1.3 0x1

1.4 6 bytes

1.5 6(Destination) + 6(Source) + 2(Type) = 14 bytes

1.6 Το πεδίο Type

1.7 Τα 2 τελευταία bytes

1.8 Type: IPv4 (0x0800)

1.9 Δεν βρέθηκαν πακέτα ARP

2

2.1 Εξαμήνουσα μόνο αυτά τα περιλαμβάνουν το πρωτόκολλο ICMP

2.2 4 bytes.

2.3 b: Version, 2ο: Header Length 0101

2.4 Version είναι 4 bit και έχει τιμή 0100. Header Length είναι 4 bit και έχει τιμή

2.5 Είναι 20 bytes.

2.6 Κοιτάξτε το πεδίο Header Length της επικεφαλίδας IPv4.

2.7 ~~10 bytes~~ 60 bytes

2.8 Είναι το πεδίο Total Length το οποίο έχει τιμή 60 άρα δίχνουμε.

2.9 40 bytes payload.

2.10 Payload = Total Length − Header Length = 60 − 20 = 40

2.11 Το πεδίο Protocol

2.12 Θυμόμαστε ότι η αρχή της επικεφαλίδας (το πρώτο byte της) είναι στη θέση 1, το Protocol βρίσκεται στη θέση 10.

2.13 01 hex.

3

3.1 Εμφανίζονται ίδιο τεμάχια/δεδομενογράμματα TCP/UDP αντίστοιχα

3.2 TCP και UDP

3.3 06 hex για TCP, 11 hex για UDP

3.4 Source Port, Destination Port, Checksum

3.5 8 bytes

3.6 Το πεδίο Length

3.7 Το πεδίο Header Length. Θέση 13 της επικεφαλίδας (13ο byte δηλαδή θα βρίσκεται στη θέση 13)

3.8 Δεν υπάρχει τέτοιο πεδίο. Για να βρούμε το συνολικό μήκος του τεμαχίου TCP αθροίζουμε το Header Length με το TCP payload

3.9 Κοιτάμε τα πεδία Source Port, Destination Port. Το HTTP χρησιμοποιεί την port 80, το HTTPS την port 443 και το DNS την port 53.

3.10 HTTP, DNS

4.1 Το UDP

4.2 Το TCP

4.3 Το 1ο bit του Flag. 0: query, 1: response

4.4 Θύρα προορισμού ερωτήσεων DNS: 53

4.5 Θύρες προέλευσης ερωτήσεων DNS: 64314, 50899, 61760, 51661, 62311

4.6 Θύρα προέλευσης απαντήσεων DNS: 53

4.7 Θύρες προορισμού απαντήσεων DNS: 50899, 64314, 61760, 51661, 62311

4.8 Παρατηρώ ότι είναι ίδιες οι θύρες.

4.9 Η port 53 για το DNS

4.10 Dst Port: 80 } από τον PC

4.11 Src port: 50149

4.12 Src Port: 80 } εξυπηρετητής

4.13 Dst Port: 50149

4.14 Η port 80 για το HTTP

4.15 Οι θύρες ταιριάζουν

4.16 GET (πλήρες GET /lab2/HTTP/1.1

4.17 200 OK (πλήρες HTTP/1.1 200 OK)

4.18 Με την εντολή ipconfig/flushdns διαγράφονται οι αντιστοιχίσεις ονομάτων DNS σε διευθύνσεις IP. Έτσι, όταν επισκεπτόμαστε πρώτη φορά την σελίδα βλέπουμε ότι πριν από τα HTTP requests, υπάρχουν DNS requests για να αντιστοιχηθούν τα ονόματα σε IP. Ωστόσο, όταν επισκεπτόμαστε δεύτερη φορά την σελίδα, τα ονόματα έχουν αποθηκευτεί και οι αιτήσεις DNS δεν γίνονται, αλλά γίνονται μηνύματα αιτήσεων HTTP. Αν εκτελέσουμε πάλι την εντολή ipconfig /flushdns θα γίνουν πάλι τα DNS requests.