Ονοματεπώνυμο: Χαράλαμπος Καμπουγέρης **Ομάδα:** 3, Τετάρτη 10:45-12:30, Αιθ.Α2

Όνομα PC/ΛΣ: CHARALAMPOSs-MacBook-Air/ macOS 14.0 **Ημερομηνία:** 11/10/2023

Διεύθυνση IP: 147.102.237.77 **Διεύθυνση MAC:** 0c:e4:41:e1:6c:74

Εργαστηριακή Άσκηση 2
Ενθυλάκωση και Επικεφαλίδες

Άσκηση 1

1.1 Με το φίλτρο απεικόνισης **arp or ip** εμφανίζονται όλα τα πακέτα που περιέχουν επικεφαλίδες ARP(Address Resolution Protocol) ή IP (internet Protocol).

1.2 Destination, Source, Type.

1.3 Όχι δεν υπάρχει.

1.4 6 bytes.

1.5 14 bytes (6-> Destination, 6 -> Source, 2 -> Type).

1.6 Το πεδίο Type του πλαισίου Ethernet.

1.7 Καταλαμβάνει τα δύο τελευταία bytes (τις θέσεις 13 και 14).

1.8 0800 (HEX).

1.9 0806 (HEX).

Άσκηση 2

2.1 Με το φίλτρο απεικόνισης **icmp** εμφανίζονται όλα τα πακέτα με πρωτόκολλο ICMP (Internet Control Message Protocol).

2.2 Μια διεύθυνση IPv4 έχει μήκος διεύθυνσης 4 bytes.

2.3 Πρώτο πεδίο: Version / Δεύτερο πεδίο: Header Length.

2.4 Και τα δύο πεδία έχουν μήκος 4 bits. Το πρώτο πεδίο (Version) έχει τιμή 4 και το δεύτερο πεδίο (Header Length) έχει τιμή 5.

2.5 Το συνολικό μήκος της επικεφαλίδας IPv4 είναι 20 byte.

2.6 Ταυτίζεται με την τιμή που φαίνεται στο πεδίο Header Length της επικεφαλίδας IPv4.

2.7 Μήκος πακέτου IPv4 (με βάση τα περιεχόμενα): 84 bytes.

2.8 Ναι υπάρχει πεδίο, το Total Length, και η τιμή του συμφωνεί με βάση αυτά που βρήκαμε προηγουμένως (84bytes).

2.9 Το payload του πακέτου IPv4 είναι το μήκος σε byte του ICMP, δηλαδή 64 bytes.

2.10 Το παραπάνω προκύπτει και από την πράξη: 84-20 (Total Length – Header Length).

2.11 Το πεδίο που ονομάζεται Protocol.

2.12 Βρίσκεται στο 10^{ο} byte.

2.13 01(HEX)

Άσκηση 3

3.1 Εμφανίζει όλα τα πακέτα που περιέχουν επικεφαλίδες TCP ή UDP.

3.2 Παρατηρώ τα TCP, UDP, TLS.

3.3 Για το πρωτόκολλο TCP: 06(HEX) / Για το πρωτόκολλο UDP: 11(HEX).

3.4 Κοινά πεδία είναι τα Source Port, Destination Port, Checksum.

3.5 Η επικεφαλίδα έχει μήκος 8 bytes.

3.6 Ναι, υπάρχει το πεδίο Length.

3.7 Υπάρχει το πεδίο Header Length και βρίσκεται στη θέση 13 (13^{ο} byte από την αρχή της επικεφαλίδας)

3.8 Όχι δεν υπάρχει. Προκύπτει από το άθροισμα σε bytes του Header Length και του TCP Payload.

3.9 Όχι δεν υπάρχει. Ωστόσο οι θύρες προέλευσης ή προορισμού μπορεί να φανερώνουν το πρωτόκολλο εφαρμογής (η θύρα 443 αντιστοιχεί στο πρωτόκολλο HTTPS).

3.10 DNS, HTTP

Άσκηση 4

4.1 Το πρωτόκολλο μεταφοράς για DNS είναι το UPD.

4.2 Το πρωτόκολλο μεταφοράς για HTTP είναι το TCP.

4.3 Το πρώτο bit. 0 για ερώτηση και 1 για απάντηση.

4.4 Destination port (DNS query): 53

4.5 Source port (DNS query): 62696

4.6 Source port (DNS response): 53

4.7 Destination port (DNS query): 62696

4.8 Παρατηρώ ότι οι θύρες πηγής των ερωτήσεων ταυτίζονται με τις θύρες προορισμού των απαντήσεων.

4.9 Η πασίγνωστη θύρα είναι η 53.

4.10 Θύρα προορισμού για HTTP request: Destination Port: 80.

4.11 Θύρα προέλευσης για HTTP request: Source Port: 49215.

4.12 Θύρα προέλευσης για HTTP response: Source Port: 80.

4.13 Θύρα προορισμού για HTTP response: Destination Port: 49215.

4.14 Η πασίγνωστη θύρα που ακούει ο εξυπηρετητής HTTP είναι η 80.

4.15 Παρατηρώ ότι οι θύρες πηγής των ερωτήσεων ταυτίζονται με τις θύρες προορισμού των απαντήσεων.

4.16 Ονομασία του πρώτου μηνύματος HTTP από τον υπολογιστή: GET /lab2/ HTTP/1.1

4.17 Κωδικός απάντησης από web-server: HTTP/1.1 200 OK

4.18 Η εντολή **ipconfig/flushdns** χρειάζεται για τον καθαρισμό της cache από DNS αρχεία, καθώς αν έχουμε επισκεφθεί ήδη αυτήν την ιστοσελίδα, την επόμενη φορά που θα την επισκεφθούμε τα DNS requests θα απαντηθούν από την cache και όχι από τον DNS server (ο κωδικός απάντησης από τον web-server θα είναι: HTTP/1.1 304 Not Modified).