2^o Εργαστήριο στα Δίκτυα Υπολογιστών
Ενθυλάκωση και Επικεφαλίδες

Όνοματεπώνυμο: **Αλέξανδρος Κυριακάκης (03112163)**
Ομάδα: **2**
Όνομα PC/ΛΣ: **MacBook Pro - Alexandros, macOS Catalina**
Ημερομηνία: **17/10/2020**
Διεύθυνση IP: **192.168.1.8**
Διεύθυνση MAC: **a4:83:e7:97:af:31**

1 Στρώμα ζεύξης δεδομένων

1.1

Το φίλτρο απεικόνισης που εφαρμόσαμε επιτρέπει μόνο πακέτα με πρωτόκολλο arp ή ip.

1.2

Destination, Source, Type

1.3

Όχι, δεν υπάρχει αντίστοιχο πεδίο.

1.4

Έχουν μήκος 6 bytes.

1.5

Έχει συνολικό μήκος 14 bytes.

1.6

Το πεδίο Type.

1.7

Τα τελευταία δύο bytes.

1.8

0x0800

1.9

0x0806

2 Στρώμα Δικτύου

2.1

Επιτρέπει την απεικόνιση μόνο πρωτοκόλλων ICMP στο στρώμα δικτύου.

2.2

Είναι 4 bytes.

2.3

Τα πρώτα δύο πεδία είναι: Version, Header Length.

2.4

Είναι 4 bit το καθένα και η τιμή τους είναι:

- Version: $0b0100$
- Header Length: $0b0101$

2.5

Είναι 20 bytes.

2.6

Γνωρίζουμε ότι η τιμή της αντίστοιχου πεδίου της επικεφαλίδας είναι Header Length: $0b0101 = 5$ και πολλαπλασιάζοντας με το 4 βρίσκουμε το μήκος της επικεφαλίδας.

2.7

Είναι 84 bytes.

2.8

Στην επικεφαλίδα IPv4 υπάρχει το πεδίο Total Length με τιμή 84.

2.9

Το μήκος των δεδομένων του πακέτου IPv4 είναι 64 bytes.

2.10

Αν αφαιρέσουμε απο το συνολικό μήκος (Total Length) το μήκος της επικεφαλίδας IPv4 (Header Length) $Total\ Length - Header\ Length = 84 - 20 = 64\ bytes$

2.11

Το πεδίο Protocol.

2.12

Βρίσκεται στο 10^o *byte* της επικεφαλίδας.

2.13

Η τιμή για ICMP είναι $0x01$

3 Στρώμα Μεταφοράς

3.1

Επιτρέπει την απεικόνιση μόνο πακέτων με πρωτόκολλο TCP, UDP στο στρώμα μεταφοράς.

3.2

Παρατηρώ τα εξής πρωτόκολλα του στρώματος μεταφοράς: HTTP, DNS, ICMP, SSL, TCP, TLSV1.2, UDP.

3.3

Για TCP είναι Protocol: TCP ($6 = 0x06$) και για UDP Protocol: UDP ($17 = 0x11$)

3.4

Τα κοινά πεδία είναι τα Src Port, Dst Port.

3.5

Είναι 8 bytes.

3.6

Ναι υπάρχει το Length.

3.7

Το Header Length και βρίσκεται στα 4 MSB του $13^{ου}$ byte της επικεφαλίδας.

3.8

Δεν υπάρχει αντίστοιχο πεδίο. Προκύπτει από το άθροισμα των IPv4 Header Length + TCP Header Length.

3.9

Υπάρχει και αυτό είναι το συνδεδεμένο με το Destination Port που βάση του πίνακα της ιστοσελίδας http://www.networksorcery.com/enp/default.htm συμπεραίνουμε και το αντίστοιχο πρωτόκολλο εφαρμογής.

3.10

DNS, MDNS, HTTP, SSDP

4 Στρώμα Εφαρμογής

4.1

Το UDP.

4.2

Το TCP.

4.3

Το καθορίζει το πρώτο bit της σημαίας (flag) όπου το 0 σημαίνει ότι είναι ερώτηση (Query) ενώ το 1 απάνρηση (Response).

4.4

Destination Port: 53

4.5

Source Port: 49486, 60595, 51010, 54739, 60595, 55180

4.6

Source Port: 53

4.7

Destination Port: 49486, 60595, 51010, 54739, 60595, 55180

4.8

Παρατηρώ ότι είναι οι ίδιες ακριβώς θύρες (Ports), δηλαδή από όποια θύρα γίνεται η ερώτηση στην ίδια θύρα αναμένεται και η απάντηση της ερώτησης αυτής.

4.9

Είναι η θύρα (Port) 53.

4.10

Είναι η θύρα Destination Port: 80

4.11

Source Port: 49847,49848

4.12

Είναι η θύρα Source Port: 80

4.13

Destination Port: 49847,49848

4.14

Είναι η θύρα Port: 80

4.15

Παρατηρώ ότι είναι οι ίδιες ακριβώς θύρες (Ports), δηλαδή από όποια θύρα γίνεται η ερώτηση στην ίδια θύρα αναμένεται και η απάντηση της ερώτησης αυτής.

4.16

Το όνομα του πρώτου μυνήματος είναι: GET /lab2/ HTTP/1.1

4.17

Ο κωδικός απάντησης είναι: HTTP/1.1 200 OK

4.18

Παρατηρώ ότι δεν γίνονται DNS Queries πριν την λήψη του πακέτου "GET /lab2/ HTTP/1.1" αφού το DNS αποτέλεσμα είναι αποθυκευμένο στην DNS cache του υπολογιστή μου. Έτσι για να δω αυτά τα πακέτα πρέπει να εκτελέσω την εντολή **dscacheutil -flushcache** (για MacOS) ώστε να διαγράψω την μνήμη των DNS αποτελεσμάτων.