Ονοματεπώνυμο: ΙΟΡΔΑΝΙΔΗΣ ΚΡΙΤΩΝ
Ομαδα: 1
Όνομα PC/OS: Kriton’s Air / MacOS 12.6
Ημερομηνία: 11/10/2022
Διεύθυνση IP: 147.102.238.37
Διεύθυνση MAC: –

ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 2: ΕΝΘΥΛΑΚΩΣΗ ΚΑΙ ΕΠΙΚΕΦΑΛΙΔΕΣ

Άσκηση 1

1.1 Με το φίλτρο απεικόνισης arp or ip εμφανίζονται μόνο τα πακετα με πρωτόκολλο ARP ή IP
1.2 Destination, Source και Type
1.3 Όχι, δεν υπάρχει
1.4 6 bytes
1.5 Είναι 6+6+2=14 bytes
1.6 Το πεδίο type
1.7 Καταλαμβάνει τις θέσεις 13 και 14
1.8 0800 (hex)
1.9 0806 (hex)

Άσκηση 2

2.1 Με το φίλτρο απεικόνισης icmp εμφανίζονται μόνο τα πακέτα με πρωτόκολλο ICMP
2.2 4 bytes
2.3 Version και Header Length
2.4 Και τα δύο πεδια εχουν μήκος 4 bits. Το μεν version έχει τιμή 4, το δε header length έχει τιμη 5
2.5 20 bytes
2.6 Προκύπτει με πολλαπλασιασμό του 5 με το 4 (μια λέξη = 32 bit = 4 byte)
2.7 Το συνολικό μήκος σε bytes προκύπτει 84 bytes αν μετρήσουμε τα byte από τον πίνακα περιεχομένων
2.8 Total Length = 84 bytes. Η τιμή αυτή ταιριάζει με αυτη που βρήκαμε στο προηγούμενο ερώτημα
2.9 Το payload του IPv4 πακέτου είναι 64 bytes, το οποίο υπολογίζεται από το πίνακα περιεχομένων
2.10 Το παραπάνω προκύπτει και απο τη πράξη: 84–20=64 (total length–header length)
2.11 Το πεδίο protocol
2.12 Είναι το 10ο byte
2.13 1

Άσκηση 3

3.1 Με το φίλτρο tcp or udp εμφανίζονται μόνο τα πακέτα με πρωτόκολλα TCP ή UDP
3.2 Παρατηρώ τα ICMPv6, TCP και UDP
3.3 Για το TCP είναι 6 και για το UDP 17
3.4 Κοινά πεδία είναι τα Source Port, Destination Port, Checksum
3.5 Η επικεφαλίδα έχει μήκος 8 bytes

3.6 Ναι, το Length
3.7 Υπάρχει το πεδίο header length στη θέση 13
3.8 Όχι δεν υπάρχει. Για αυτό πρέπει να βρούμε το συνολικό μήκος του πλαισίου IP και να αφαιρέσουμε το μήκος της επικεφαλίδας του.
3.9 Όχι δεν υπάρχει. Ωστόσο οι θύρες προέλευσης ή προορισμού μπορεί να φανερώνουν το πρωτόκολλο εφαρμογής (π.χ. η θύρα 443 αντιστοιχεί στο πρωτόκολλο HTTPS)
3.10 DNS και HTTP

Άσκηση 4

4.1 UDP
4.2 TCP
4.3 το 1ο bit της σημαίας καθορίζει αν πρόκειται για ερώτηση ή απάντηση: για ερώτηση παίρνει την τιμη 0 και για απάντηση την τιμή 1
4.4 Οι ερωτήσεις DNS πηγαίνουν στη θύρα 53
4.5 Οι θύρες πηγής των ερωτήσεων DNS είναι οι 57299, 65305, 58369, 54878, 52903
4.6 Οι θύρα πηγής των απαντήσεων DNS είναι η 53
4.7 Οι θύρες προορισμού των απαντήσεων DNS είναι οι 57299, 65305, 58369, 54878, 52903
4.8 Παρατηρώ ότι οι θύρες πηγής των ερωτήσεων ταυτίζονται με τις θύρες προορισμού των απαντήσεων. Αυτό είναι αναμενόμενο διότι για κάθε ερώτηση που κάνει ο υπολογιστής μου σε μια θύρα, περιμένω μία απάντηση σε αυτή τη θύρα
4.9 Η πασίγνωστη θύρα είναι η 53 το οποίο φαίνεται και από τα παραπάνω ερωτήματα
4.10 Η θύρα προορισμού μηνυμάτων HTTP είναι η 80
4.11 Η θύρα πηγής μηνυμάτων HTTP είναι η 54497
4.12 Η θύρα πηγής απαντήσεων HTTP είναι η 80
4.13 Η θύρα προορισμού απαντήσεων HTTP είναι η 54497
4.14 Η πασίγνωστη θύρα είναι η 80
4.15 Παρατηρώ ότι είναι η ίδια θύρα. Και πάλι είναι λογικό αυτό αφού περιμένουμε μια απάντηση στη θύρα στην οποία στέλνουμε το μήνυμα HTTP
4.16 GET /lab2/ HTTP/1.1\r\n
4.17 200
4.18 Με αυτήν την εντολή καθαρίζεται η cache απο DNS αρχεία. Εάν έχουμε ήδη επισκεφτεί αυτήν την ιστοσελίδα, την επόμενη φορά που θα την επισκεφτούμε τα DNS requests θα απαντηθούν από την cache και όχι απο τον DNS server. Για να το αποφύγουμε αυτό εκτελούμε την εντολη ipconfig / flushdns και ο φυλλομετρητής θα αναγκαστεί να στείλει αιτήματα στον DNS server