ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΙΣΤΩΝ

ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ – 7ο ΕΞΑΜΗΝΟ

Τζομάκα Αφροδίτη – ΑΜ: 03117107

2η Ομάδα Ασκήσεων

Ονοματεπώνυμό: Τζομάκα Αφροδίτη	**Ομάδα:** 2
Όνομα PC/ΛΣ: DESKTOP-II5SP0K/windows 10	**Ημερομηνία:** 13-10-2020
Διεύθυνση IP: 192.168.1.4/24	**Διεύθυνση MAC:** A8:6B:AD:73:3E:A5

ΑΣΚΗΣΗ 1

1.1. Με το φίλτρο απεικόνισης arp or ip βλέπουμε μόνο τα πακέτα με πρωτόκολλο ζεύξης arp ή πρωτόκολλο δικτύου ip.
1.2. Source, Destination, Type.
1.3. Όχι, τέτοια πληροφορία μπορεί να βρεθεί στο τμήμα Frame των Λεπτομερειών.
1.4. 6 byte.
1.5. 6(src)+6(dst)+2(type)=14 bytes
1.6. Το πεδίο type.
1.7. 13ο-14ο MSbyte.
1.8. 0x0800.
1.9. 0x0806.

ΑΣΚΗΣΗ 2

2.1. Φιλτράρει μόνο τα icmp echo packets.
2.2. 4 bytes.
2.3. Version και header length.
2.4. Καθένα από τα πεδία αυτά έχει μέγεθος 4 bits. Οι τιμές τους είναι: version = 0100=4, header length = 5.
2.5. Header length = 20bytes.
2.6. Header length = 5*32bits = 160bits = 20bytes.
2.7. 60bytes = 20 ipv4 bytes + 40 icpm bytes.

2.8. Ναι, το πεδίο total length = 60. Όπως βλέπουμε συμφωνεί με τις προηγούμενες παρατηρήσεις μας.
2.9. Το μήκος δηλαδή του icpm που ακολουθεί: 40bytes.
2.10. Προκύπτει ως εξής: total length – header length.
2.11. Το πεδίο protocol.
2.12. 10ο MSByte.
2.13. 1.

ΑΣΚΗΣΗ 3

3.1. Εμφανίζει τα πλαίσια με πρωτόκολλα tcp, udp ή πρωτόκολλα του επιπέδου εφαρμογής που χρησιμοποιούν τα δύο προηγούμενα.
3.2. UDP, TCP.
3.3. TCP: 6, UDP: 17.
3.4. Source, destination, checksum.
3.5. 8bytes.
3.6. Ναι, το πεδίο length.
3.7. Το πεδίο data offset ως εξής: data offset = header length = 5 = 20 bytes. Βρίσκεται στα 4 πρώτα bits του 13ου byte.
3.8. Όχι. Για να βρούμε το συνολικό μήκος των πακέτων TCP προσθέτουμε το μέγεθος της επικεφαλίδας μαζί με το μέγεθος μηνύματος που ενθυλακώνει. Για το προκείμενο πακέτο δεν ακολουθεί κάποιο data message μετά την tcp επικεφαλίδα οπότε θα είναι 20 bytes.
3.9. Πρόκειται για τις θύρες dest, src. Αυτές καθορίζουν το αντίστοιχο πρωτόκολλο.
3.10. TLSv1.2, TLSv1.3, DNS, HTTP, STUN.

ΑΣΚΗΣΗ 4

4.1. Το UDP.
4.2. Το TCP.
4.3. Το 16ο bit (QR). Για QR = 0 έχουμε query, ενώ για QR = 1 έχουμε response.
4.4. 53.
4.5. 53076, 60576, 62189, 53579, 49944, 56438, 59552, 56355, 59559, 49663, 64628.
4.6. 53.
4.7. 53076, 60576, 62189, 53579, 49944, 56438, 59552, 56355, 59559, 49663, 64628.
4.8. Είναι τα ακριβώς αντίστοιχα, δηλαδή έχουμε ότι ο προορισμός της ερώτησης είναι η πηγή της απάντησης και αντίστροφα.
4.9. Η 53.

4.10. 80.
4.11. 62952.
4.12. 80.
4.13. 62952.
4.14. Η 80.
4.15. Ομοίως με τα πορίσματα μας στην 4.8. βλέπουμε πλήρη αντιστοιχία.
4.16. GET /lab2/ HTTP/1.1.
4.17. 200 – OK.
4.18. Η εντολή ipconfig/flushdns αδειάζει την dns cache η οποία κρατάει το αρχείο των αντιστοιχιών ανάμεσα σε domain names και IP addresses. Το βήμα αυτό είναι αναγκαίο για να ανακληθεί ξανα το dns και να ανιχνεύσει τα κατάλληλα πακέτα προς ανάλυση το wireshark.