Δίκτυα Υπολογιστών
Εργαστηριακή Άσκηση 2

Ονοματεπώνυμο: Κυριακόπουλος Γεώργιος – el18153
Ομάδα: 4
Όνομα PC/ΛΣ: George – Windows 10 Pro, 21H1
Ημερομηνία: 25/10/2021
Διεύθυνση IP: 192.168.1.8
Διεύθυνση MAC: 60-A4-B7-75-72-0F

Άσκηση 1:

1.1.
Αφού εφαρμόζουμε ένα φίλτρο απεικόνισης *arp or ip*, τότε από τα ήδη περιορισμένα ως προς τη σύλληψη πλαίσια, λόγω του φίλτρου σύλληψης *ether host 60:a4:b7:75:72:0f*, θα εμφανιστούν στη λίστα μόνο αυτά με πρωτόκολλο arp ή ip.

1.2.
Από τις λεπτομέρειες του πλαισίου έχουμε τα ονόματα των πεδίων: Destination, Source και Type.

1.3.
Δεν υπάρχει στην επικεφαλίδα Ethernet, αλλά υπάρχει στη γενικότερη επικεφαλίδα Frame που εμφανίζεται στο Wireshark με όνομα πεδίου Frame Length.

1.4.
Οι διευθύνσεις Ethernet έχουν μήκος 6 bytes.

1.5.
Η επικεφαλίδα Ethernet έχει σταθερό μήκος 14 bytes (6 bytes Destination + 6 bytes Source + 2 bytes Type).

1.6.
Αυτό που καθορίζει το πρωτόκολλο δικτύου είναι το πεδίο Type.

1.7.
Το πεδίο Type βρίσκεται τελευταίο στην επικεφαλίδα Ethernet, καταλαμβάνει δηλαδή τα 2 τελευταία bytes της.

1.8.
Για πακέτα IPv4 η τιμή του είναι 0x0800.

1.9.
Για πακέτα ARP η τιμή του είναι 0x0806.

Άσκηση 2:

2.1.
Εμφανίζονται στη λίστα μόνο τα πλαίσια με πρωτόκολλο ICMP.

2.2.
Οι διευθύνσεις IPv4 έχουν μήκος 4 bytes.

2.3.
Τα πρώτα δύο πεδία της επικεφαλίδας IPv4 είναι τα Version και Header Length.

2.4.
Για το πεδίο Version έχουμε μήκος 4 bit και τιμή 4 (0b0100), ενώ για το πεδίο Header Length έχουμε μήκος 4 bit και τιμή 5 (0b0101).

2.5.
Με βάση το παράθυρο με τα περιεχόμενα, το μήκος της επικεφαλίδας IPv4 είναι 20 bytes.

2.6.
Το πεδίο Header Length εμφανίζει το μήκος της επικεφαλίδας σε 32 bit λέξεις (ή 4 bytes), επομένως έχοντας την τιμή 5 (0b0101) έχουμε 32 bit * 5 = 160 bits ή 20 bytes (5 * 4 bytes), που αποτελεί και την ελάχιστη αποδεκτή τιμή για μία έγκυρη επικεφαλίδα.

2.7.
Με βάση το παράθυρο με τα περιεχόμενα, το μήκος του πακέτου IPv4 (όλου του frame χωρίς το πλαίσιο Ethernet, δηλαδή IPv4 + ICMP) είναι 60 bytes, που συμφωνεί με το συνολικό μήκος του πλαισίου, 74 bytes, μείον το πλαίσιο Ethernet μήκους 14 bytes.

2.8.
Υπάρχει το πεδίο Total Length με τιμή 60, επομένως συμφωνεί με το μήκος που βρήκαμε.

2.9.
Το μήκος των δεδομένων του IPv4 πακέτου είναι 40 bytes.

2.10.
Εάν αφαιρέσουμε από το μήκος του πακέτου IPv4 το μήκος της επικεφαλίδας IPv4 θα μείνει το μήκος των δεδομένων (payload), δηλαδή: Total Length - Header Length = Payload Length (στην περίπτωση μας 60 bytes - 20 bytes = 40 bytes).

2.11.
Αυτό που καθορίζει το πρωτόκολλο στρώματος μεταφοράς είναι το πεδίο Protocol.

2.12.
Το πεδίο Protocol αποτελεί το 10ο byte της επικεφαλίδας (ξεκινάει από το 73ο bit σε σχέση με την αρχή της επικεφαλίδα).

2.13.
Για το πρωτόκολλο ICMP έχει τιμή 1 (0x01).

Άσκηση 3:

3.1.
Εμφανίζει στη λίστα μόνο τα πλαίσια που έχουν στο στρώμα μεταφοράς πρωτόκολλο TCP ή UDP.

3.2.
Στη λίστα των πλαισίων υπάρχουν τα παρακάτω πρωτόκολλα: DNS, HTTP, QUIC, TCP, TLSv1.2, TLSv1.3, UDP.

3.3.
Για το πρωτόκολλο TCP έχουμε τιμή πεδίου Protocol 6 (0x06), ενώ για το πρωτόκολλο UDP έχουμε 17 (0x11).

3.4.
Τα κοινά πεδία μεταξύ των επικεφαλίδων των τεμαχίων TCP και των δεδομενογραμμάτων UDP είναι τα Source Port, Destination Port και Checksum.

3.5.
Το μήκος της επικεφαλίδας των δεδομενογραμμάτων UDP είναι 8 bytes.

3.6.
Το πεδίο Length μας δίνει το συνολικό μήκος των δεδομενογραμμάτων UDP.

3.7.
Το πεδίο Header Length (Data Offset) είναι αυτό που καθορίζει το μήκος της επικεφαλίδας του τεμαχίου TCP και βρίσκεται στην αρχή του 13ου bit, συγκεκριμένα αποτελεί τα 4 πρώτα bit του, δηλαδή τα 4 MSBs.

3.8.
Δεν υπάρχει τέτοιο πεδίο στην επικεφαλίδα TCP. Το συνολικό μήκος των τεμαχίων TCP προκύπτει από την αφαίρεση του IPv4 Header Length πεδίου της επικεφαλίδας IPv4 από το Total Length πεδίο της ίδιας επικεφαλίδας. Για παράδειγμα, στην περίπτωση μας: 40 bytes - 20 bytes = 20 bytes μήκος τεμαχίων TCP.

3.9.
Με βάση το πεδίο Destination Port μπορούμε να προσδιορίσουμε τον τύπο του πρωτοκόλλου εφαρμογής, με τη βοήθεια και της σελίδας που δίνεται, όπου αναγράφονται ποιο πρωτόκολλο χρησιμοποιούν συνήθως ορισμένες θύρες με βάση τη σύμβαση της IANA.

3.10.
Δεν παρατήρησα κάποιο άλλο πρωτόκολλο στρώματος εφαρμογής.

Άσκηση 4:

4.1.
Το DNS χρησιμοποιεί το UDP πρωτόκολλο μεταφοράς.

4.2.
Το HTTP χρησιμοποιεί το TCP πρωτόκολλο μεταφοράς.

4.3.
Το 1ο bit της σημαίας (flag) στην επικεφαλίδα DNS καθορίζει εάν πρόκειται για ερώτηση (query με τιμή 0) ή απάντηση (response με τιμή 1).

4.4.
Η θύρα προορισμού των ερωτήσεων DNS (Destination Port) είναι η θύρα 53.

4.5.
Οι θύρες πηγής των ερωτήσεων DNS (Source Port) είναι οι θύρες 50685, 65290, 54718, 58467.

4.6.
Η θύρα πηγής των απαντήσεων DNS (Source Port) είναι η θύρα 53.

4.7.
Οι θύρες προορισμού των απαντήσεων DNS (Destination Port) είναι οι θύρες 50685, 65290, 54718, 58467.

4.8.
Ουσιαστικά όταν μια ερώτηση (query) γίνεται από μία θύρα X (Source Port) προς μία θύρα Y (Destination Port), τότε η απάντηση της (response) έρχεται από τη θύρα Y (Source Port) στη θύρα X (Destination Port). Επομένως, οι θύρες X και Y ανταλλάζουν ρόλους σε ένα γεγονός ερώτησης-απάντησης.

4.9.
Πρόκειται για τη θύρα 53.

4.10.
Η θύρα προορισμού (Destination Port) των μηνυμάτων HTTP που παράγει ο υπολογιστής μας (δηλαδή όπου Source είναι η IPv4 του υπολογιστή μας -192.168.1.8 στην περίπτωση μας) είναι η θύρα 80.

4.11.
Η θύρα προέλευσης (Source Port) των μηνυμάτων HTTP που παράγει ο υπολογιστής μας είναι η θύρα 59794.

4.12.
Η θύρα προέλευσης (Source Port) της αντίστοιχης απάντησης του εξυπηρετητή ιστού είναι η θύρα 80.

4.13.
Η θύρα προορισμού (Destination Port) της αντίστοιχης απάντησης του εξυπηρετητή ιστού είναι η θύρα 59794.

4.14.
Πρόκειται για τη θύρα 80.

4.15.
Παρατηρώ ότι ισχύει μία παρόμοια σχέση με αυτή που εξήγησα στο ερώτημα 4.8. για τις θύρες προέλευσης και προορισμού των ερωτήσεων-απαντήσεων DNS. Συνοπτικά, η θύρα προέλευσης του μηνύματος HTTP γίνεται θύρα προορισμού της απάντησης και η θύρα προορισμού του μηνύματος HTTP γίνεται θύρα προέλευσης της απάντησης.

4.16.
Το μήνυμα που στέλνει ο υπολογιστής μας είναι το: GET /lab2/ HTTP/1.1, επομένως το όνομα του είναι GET.

4.17.
Το μήνυμα που επιστρέφει έχει όνομα: HTTP/1.1 200 OK, επομένως ο κωδικός απάντησης είναι ο 200 OK.

4.18.
Παρατηρούμε πως δεν υπάρχουν ερωτήσεις και επομένως απαντήσεις DNS, παρά μόνο HTTP μηνύματα, καθώς τα προηγούμενα αποτελέσματα από τις αντίστοιχες DNS ερωτήσεις και απαντήσεις έχουν αποθηκευτεί στην DNS cache του υπολογιστή μου. Επομένως, προηγουμένως χρειάστηκε η εντολή *$ ipconfig /flushdns*, ώστε να εκκαθαριστεί η DNS cache του υπολογιστή μου και να τρέξουν κανονικά οι DNS ερωτήσεις και απαντήσεις, ώστε να είναι δυνατή η μελέτη τους, αφού δεν θα βρισκόταν η απάντηση στην DNS cache μου.