

Όνοματεπώνυμο: Ναυσικά Αμπατζή		Ομάδα: 2
Όνομα PC/ΛΣ: Dell XPS 15-7590 Windows		Ημερομηνία: 24 /12 /2020
Διεύθυνση IP: 192.168.1.12	Διεύθυνση MAC:24-41-8C-65-26-BF	

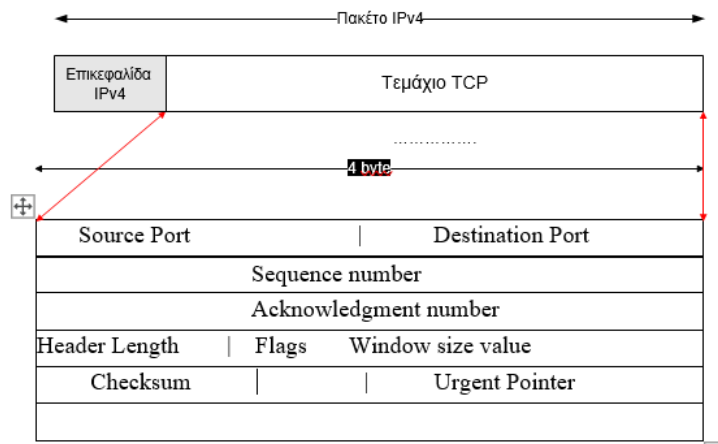
Μέρος 1

- 1.1 Το φίλτρο απεικόνισης που χρησιμοποίησα ώστε να συλλαμβάνονται μόνο πακέτα που περιλαμβάνουν την IPV4 του υπολογιστή μου είναι το : host 192.168.1.12
- 1.2 Προσπαθεί να συνδεθεί στη θύρα 23.
- 1.3 tcp.port == 23
- 1.4 Για την εκκίνηση της εγκατάστασης της σύνδεσης TCP χρησιμοποιείται η σημαία μήκους 1 bit: SYN
- 1.5 Για την περίπτωση A κάνει 5 προσπάθειες και για την περίπτωση B επίσης 5.

tcp.port==23					
No.	Time	Source	Destination	Protocol	Length
1	0.000000	192.168.1.12	1.1.1.1	TCP	
3	1.017616	192.168.1.12	1.1.1.1	TCP	
27	2.010049	192.168.1.12	1.1.1.1	TCP	
36	4.019557	192.168.1.12	1.1.1.1	TCP	
38	8.001799	192.168.1.12	1.1.1.1	TCP	
43	10.112...	192.168.1.12	2.2.2.2	TCP	66 64817 -
46	1.010542	192.168.1.12	2.2.2.2	TCP	66 [TCP Re
47	2.010053	192.168.1.12	2.2.2.2	TCP	66 [TCP Re
54	4.002818	192.168.1.12	2.2.2.2	TCP	66 [TCP Re
59	8.003913	192.168.1.12	2.2.2.2	TCP	66 [TCP Re

- 1.6 Περίπτωση A : 1^η – 2^η : 1.017616 sec, 2^η – 3^η : 2.010049 sec, 3^η – 4^η : 4.019557 sec, 4^η – 5^η : 8.001799 sec
Περίπτωση B : 1^η – 2^η : 1.010542 sec, 2^η – 3^η : 2.010053 sec, 3^η – 4^η : 4.002818 sec, 4^η – 5^η : 8.003713 sec
- 1.7 Παρατηρώ ότι οι χρονικές αποστάσεις ανάμεσα στις προσπάθειες στις περιπτώσεις A και B είναι πολύ παρόμοιες.
- 1.8 Και στις δύο περιπτώσεις σε όλα τα τεμάχια παρατηρώ ότι Ack = 0 και MSS 1460 bytes, επομένως υπάρχει μόνο το πρώτο μέρος της τριμερούς χειραψίας.
- 1.9 Η προσπάθεια απλώς εγκαταλείπεται, καθώς τα πεδία FIN και ACK παραμένουν στο Not set.
- 1.10 ip.addr == 147.102.40.1
- 1.11 Ο υπολογιστής μου κάνει 5 προσπάθειες.
- 1.12 Παρατηρώ ότι ο αριθμός των βημάτων είναι ξανά 5 για την εγκατάσταση της σύνδεσης στην περίπτωση Γ, αλλά πραγματοποιούνται α 2 από τα 3 βήματα της τριμελούς χειραψίας. Επίσης τα retransmissions έχουν χρονική απόσταση περίπου 0.51 sec
- 1.13 Στέλνονται οι σημαίες RST και ACK.
- 1.14 Άρνηση της εγκατάστασης δηλώνει η σημαία RST.
- 1.15 Μέγεθος επικεφαλίδας : 20 byte. Εφόσον δεν μεταφέρονται δεδομένα, το μήκος των δεδομένων θα είναι 0.

1.16 Source port (16 bit), Destination Port (16 bits), Sequence number (32 bits), Acknowledgment number (32 bits), Header Length (8 bits), Flags (8 bits), Window size value (16 bits), Checksum (16 bits), Urgent Pointer(16 bits)



1.17 Σύμφωνα με την ιστοσελίδα το μέγεθος της επικεφαλίδας το καθορίζει το πεδίο Data Offset. Στο wireshark το βλέπουμε από το πεδίο Header Length, το οποίο αντικαθιστά το Data Offset.

1.18 Επιλέγοντας το πακέτο, εάν επιλέξουμε στο πεδίο με τις λεπτομέρειες το Transmission Control Protocol, τότε θα παρατηρήσουμε ότι στα περιεχόμενα έχουν υπογραμμιστεί με μπλε 20 bytes. Έτσι συμπεραίνουμε ότι το μήκος της επικεφαλίδας του TCP είναι 20 bytes.

1.19 Όχι δεν υπάρχει.

1.20 Από την επικεφαλίδα IPV4 $\text{Total Length} - \text{Header Length(IPV4)} - \text{Header Length(TCP)} = 40 - 20 - 20 = 0$ bytes.

1.21 Το μήκος της επικεφαλίδας TCP του πρώτου τεμαχίου TCP που στέλνει ο υπολογιστής μου στον 147.102.40.1 είναι 32 Byte.

1.22 Ναι υπάρχει διαφορά, καθώς το τεμάχιο που στέλνει ο υπολογιστής μου είναι κατά 12 Bytes μεγαλύτερο. Αυτό συμβαίνει διότι στην επικεφαλίδα TCP υπάρχει το πεδίο Options.

Μέρος 2

2.1 Φίλτρο σύλληψης : host 147.102.40.15

2.2 Ο υπολογιστής μου προσπαθεί να συνδεθεί στη θύρα ελέγχου FTP 21 του edu-dy.cn.ntua.gr.

2.3 Η σύνδεση για τη μεταφορά δεδομένων γίνεται με τη θύρα 20

2.4 `tcp.port == 21`

2.5 Κατά την εγκατάσταση της σύνδεσης ελέγχου FTP ανταλλάσσονται 3 τεμάχια TCP (τριμελής χειραψία).

2.6 Σημαίες : ACK,SYN

2.7 Το μέγεθος των πρώτων 2 επικεφαλίδων είναι 32 bytes, ενώ της τρίτης 20 bytes.

2.8 Το μήκος των δεδομένων είναι 0. Αυτό συμβαίνει διότι κατά την τριμερή δεν μεταφέρονται δεδομένα.

2.9 Συνολικός χρόνος : $0.017983 + 0.000109 = 0.018002 \text{ sec}$

2.10 Ναι συμφωνεί, οι τιμές είναι πολύ κοντά.

2.11 Απόλυτος αρχικός αριθμός που ανακοινώνει ο υπολογιστής μου : 3970373601

Απόλυτος αρχικός αριθμός που ανακοινώνει ο server : 1244127161

2.12 Ο Acknowledgement Number του τεμαχίου TCP με το οποίο ο εξυπηρετητής FTP είναι ο Sequence number του παραπάνω ερωτήματος +1.

2.13 Ο αριθμός σειράς του τελευταίου τεμαχίου TCP της τριμερούς χειραψίας είναι ο ίδιος με τον αριθμό επιβεβαίωσης του προηγούμενου τεμαχίου και ο αριθμός επιβεβαίωσης είναι ο ίδιος με τον sequence number του προτελευταίου επίσης.

2.14 max τιμή : 4,294,967,295

2.15 Το μέγεθος λήψης που ανακοινώνει ο υπολογιστής μου είναι : 8192 bytes και αυτό που ανακοινώνει ο εξυπηρετητής είναι 65535 bytes.

2.16 Στο πεδίο Window size value.

2.17 `max size window = 65535 bytes`

`Min size window = 0 bytes`

2.18 Ο υπολογιστής μου ανακοινώνει τιμή MSS = 1460 bytes.

2.19 Η MTU του υπολογιστή μου είναι ίση με 1500 bytes. Έτσι εάν αφαιρέσω 20 + 20 bytes (τις επικεφαλίδες) προκύπτει η ζητούμενη MTU.

2.20 Η τιμή μεταφέρεται στο πεδίο Options της TCP επικεφαλίδας.

2.21 Ο edu-dy.cn.ntua.gr ανακοινώνει MSS ίση με 536 bytes.

2.22 Ομοίως η τιμή αυτή προκύπτει εάν αφαιρέσουμε από την MTU του server(576) 40 bytes, δηλαδή τα μήκη των Header length των TCP και IPV4.

2.23 536 bytes, καθώς μέχρι αυτό το μέγεθος μπορεί να δεχτεί ο server.

- 2.24 Χρησιμοποιείται η σημαία FIN.
- 2.25 Την διαδικασία της απόλυσης την εκκινεί η πλευρά του server.
- 2.26 Ανταλλάσσονται συνολικά 4 τεμάχια TCP.
- 2.27 20 bytes
- 2.28 0 (στην χειραψία δεν ανταλλάσσονται δεδομένα)
- 2.29 Το μήκος αυτό είναι το μήκος της επικεφαλίδας TCP.
- 2.30 Το μήκος αυτό είναι το μήκος της επικεφαλίδας TCP.
- 2.31 Ο υπολογιστής μου έστειλε 110 bytes. Ο server έστειλε 376 bytes.
- 2.32 Ελέγχω το ACK του FIN για κάθε πλευρά. Ο server στέλνει τεμάχιο απόλυσης με ACK ίσο με 120 άρα έχει λάβει μέχρι και το 119^ο byte. Ο υπολογιστής μου στέλνει τεμάχιο απόλυσης με ACK ίσο με 377, άρα έχει λάβει μέχρι και το 376^ο byte.
- 2.33 $\text{tcp.port} == 20$
- 2.34 Ο υπολογιστής μου ανακοινώνει τιμή MSS = 1460 bytes.
Ο server ανακοινώνει τιμή MSS = 536bytes.
- 2.35 $\text{max TCP segment} = 536 \text{ bytes}$
- 2.36 $\text{RTT} = 0.0009 \text{ sec}$
- 2.37 Όχι, δεν στέλνονται επιβεβαιώσεις για κάθε τεμάχιο αλλά κάθε 2 περίπου.
- 2.38 Όλες οι τιμές των Window size value είναι 512 Bytes, εκτός από την τελευταία που είναι 511 bytes.
- 2.39 Μέγεθος πλαισίου : 590 bytes
Ethernet Header : 14 bytes
IP Header : 20 bytes
TCP Header : 20 bytes
- 2.40 Μέγεθος δεδομένων τεμαχίου TCP = 536 bytes
- 2.41 Εάν δεν υπάρχει το flag Don't fragment, τότε το πακέτο θα θρυμματιστεί πριν σταλεί.
- 2.42 Ο server έχει ACK ίσο με 61441, άρα έχει λάβει 61440bytes.
- 2.43 Ρυθμός μετάδοσης = $61440\text{bytes}/0,4\text{sec} = 153,6 \text{ kbytes/sec}$
- 2.44 Όχι δεν υπήρξαν αναμεταδόσεις τεμαχίων καθώς δεν υπάρχει κάπου πακέτο με το μήνυμα Retransmission.

Μέρος 3

3.1 IPV4 = 94.65.141.44

3.2 RTT = 0.000097 sec. Ο χρόνος αυτός είναι μικρότερος.

3.3 Παρατηρώντας το διάγραμμα καταλήγουμε στα εξής συμπεράσματα:

Αρχικά στέλνονται ένα ένα τα τεμάχια της τριμελούς χειραψίας. Αυτό συμβαίνει καθώς για να σταλεί το 3^ο από τον edu-dy.cn.ntua.gr πρέπει να λάβει απάντηση με τις σημαίες [SYN,ACK] από τον υπολογιστή με την παραπάνω IPV4 διεύθυνση. Στη συνέχεια αρχίζουν και στέλνονται τεμάχια με FTP δεδομένα κάθε φορά που στέλνεται επαλήθευση [σημαία ACK] είτε από τον server είτε από τον client. Σε κάθε επαλήθευση στέλνονται σειριακά δεδομένα μέχρι το μέγεθος τους σε Byte να φτάσει τον αριθμό του window size που καθορίζεται από την επαλήθευση.

3.4 Στο πρώτο RRT στάλθηκε μόνο το τεμάχιο με τη σημαία SYN από τον edu-dy.cn.ntua.gr. Σύμφωνα με το RFC 5681 το MSS= 563 < 1095 Bytes κι έτσι επιτρέπεται να σταλούν το πολύ 4 τεμάχια, άρα υπάρχει συμφωνία.

3.5 Στο δεύτερο RRT έστειλε πάλι 1 τεμάχιο, την επαλήθευση ACK στο τεμάχιο[SYN,ACK] που είχε στείλει ο υπολογιστής με την παραπάνω IPV4. Στο τρίτο RRT(τόρα η τριμερής χειραψία έχει τελειώσει) έστειλε 5 τεμάχια, κάτι το οποίο φαίνεται από το διάγραμμα με αποστολέα την IPV4 94.65.141.44, όπου το πρώτο τεμάχιο που στέλνει έχει νούμερο 21 και το επόμενο 28, επομένως παρεμβάλλονται 7 τεμάχια.

3.6 Παρατηρώ ότι στο δικό μου διάγραμμα(από το part 2) στέλνονται λιγότερα τεμάχια σειριακά, επομένως στέλνονται περισσότερες επαληθεύσεις ACK. Όσον αφορά τα τεμάχια στα RRT, στα πρώτα δύο είναι τα ίδια καθώς πρόκειται για τη χειραψία. Στο τρίτο RRT στέλνονται 3 τεμάχια πριν την επαλήθευση ACK, αντί για 5 όπως πριν.

Μέρος 4

4.1 ether host 24-41-8C-65-26-BF

4.2 udp

4.3 Πεδία επικεφαλίδας UDP:

- Source Port (2 bytes)
- Destination Port (2 bytes)
- Length (2 bytes)
- Checksum (2 bytes)

4.4 8 Bytes

4.5 Το μέγεθος του πακέτου IPV4 είναι 247 Bytes. Αφαιρώντας τα 20 Bytes της επικεφαλίδας του και τα 8 bytes της επικεφαλίδας του UDP προκύπτει το μέγεθος των δεδομενογραμμάτων ίσο με 219 bytes.

4.6 Το πεδίο Length της επικεφαλίδας είναι το άθροισμα του μεγέθους της επικεφαλίδας συν το μέγεθος των ενθυλακωμένων δεδομένων.

4.7 Ελάχιστο μήκος : 0 bytes

Μέγιστο μήκος : $2^{16} - 1 - 8(\text{header length}) - 20 = 65507$ bytes

4.8 Αφαιρώντας από τα 576 bytes τα 20 Bytes της επικεφαλίδας του IPV4, το μέγιστο μήκος προκύπτει ίσο με 556 bytes.

4.9 DNS IPV4 : 192.168.1.78

4.10 Source Port : 53

Destination Port = 64703

4.11 Source Port : 64703

Destination Port = 53

4.12 Η θύρα 53.