LAB-07 (TCP, UDP)

Ex. 1 | Μετάδοση με TCP

1.1 |
Capture filter : ip host 192.168.1.7

1.2 |
Display filter : ip.addr == 1.1.1.1 or ip.addr == 2.2.2.2 or ip.addr == 147.102.40.1

1.3 |
Προσπαθεί να συνδεθεί στη θύρα 23 που είναι η default θύρα για την επικοινωνία μέσω telnet

1.4 |
Display filter : tcp.port == 23

1.5 |
Η σημαία / flag 'Syn'

1.6 |
Κάνει 5 προσπάθειες στη κάθε περίπτωση

1.7 |
Χρονικές αποστάσεις (σε sec) : 1, 2, 4, 8

1.8 |
Πέρα απο το Sequence number και στις δύο περιπτώσεις A, B παρατηρώ τα ίδια χαρακτηριστικά

1.9 |
Παρατηρώ μόνο το πρώτο βήμα όπου Seq=1, Ack=0

1.10 |
Ο υπολογιστής φαίνεται να εγκαταλείπει τη προσπάθεια, γιατί το flag της απόλυσης σύνδεσης δεν είναι ενεργοποιημένο

1.11 |
Display filter : tcp and ip.host == 147.102.40.1

1.12 |
Κάνει και πάλι 5 προσπάθειες για να εγκαταστήσει σύνδεση TCP

1.13 |
Η διαφορά με το ερώτημα 1.8 είναι ότι πλέον υπάρχουν και απαντήσεις aknowledgement από το άλλο άκρο, στις οποίες είναι ενεργοποιημένο και το flag του RST, δηλαδή της απόρριψης σύνδεσης. Επίσης οι προσπάθειες γίνονται πλέον κάθε 5 δευτερόλεπτα.

1.14 |
1 bit flags : Nonce, CWR, ECN-Echo, Urgent, Acknowledgment, Push, Reset, Syn, Fin

1.15 |
To flag 'Reset'

1.16 |
Header Length : 20 bytes, Data : 0 bytes

DIRECTORY

NOTES

`nslookup <address>`
Finds the ip address throught dns resolver

FTP (CMD)
`bin` → η μεταφορά αρχείων γίνεται σε δυαδική μορφή

`lcd desktop` → επαναορίζουμε τη τοποθεσία που θα αποθηκευτούν τα αρχεία που θα κατέβουν

1.17 |
(1) Source Port (2 bytes), (2) Destination Port (2 bytes), (3) Sequence Number (4 bytes), (4) Acknowledgment Number (4 bytes), (5) Header Length (4 bits), (6) Flags (12 bits), (7) Window (2 bytes), (8) Checksum (2 bytes), (9) Urgent Pointer (2 bytes)

1.18 |
Η ιστοσελίδα χαρακτηρίζει αυτό το πεδίο ως 'Data Offset', ενώ το Wireshark ως 'Header Length'

1.19 |
Το Header Length εχει τιμή 5 HEX → 5 DEC και δηλώνει οτι η επικεφαλίδα έχει μήκος 5 * 4 bytes γιατί πάντα έχει μήκος πολλαπλάσιο των 4 bytes (32 bits)

1.20 |
Οχι, δεν υπάρχει

1.21 |
Το μήκος προκύπτει από το άθροισμα των επικεφαλίδων IPv4 και TCP που είναι 20 bytes η κάθε μία. Άρα συνολικά προκύπτει 40 bytes.

1.22 |
Η επικεφαλίδα TCP έχει μέγεθος 32 bytes

1.23 |
Ναι, υπάρχει διαφορά 12 bytes και οφείλεται στο πεδίο 'Options' το οποίο έχει μέγεθος 12 bytes και περιλαμβάνει τις ρυθμίσεις σύνδεσης.

Ex. 2 | TCP connection, data transfer

2.1 |
Capture filter : tcp and ip host 147.102.40.15

2.2 |
Προσπαθεί να συνδεθεί στη θύρα 21 που είναι η default για το ftp

2.3 |
Η σύνδεση γίνεται με τη θύρα 20

2.4 |
Display filter : tcp.port == 21

2.5 |
Ανταλλάσονται συνολικά 29 τεμάχια στη πόρτα 21 και 3 πακέτα στην αρχή για την εγκατάσταση της σύνδεσης.

2.6 |
Τα flags : SYN, ACK

2.7 |
32 bytes (για τα 2 πρώτα)

2.8 |
Έχουν μηδενικό μέγεθος δεδομένων

2.9 |
Διαρκεί περίπου 0.026 sec

2.10 |
Ναι, συφωνεί

2.11 |
Sequence Number Πελάτη : 0, Sequence Number Εξυπηρετητή : 0

2.12 |
Είναι το Sequence Number Πελάτη + 1, δηλαδή ζητάει το επόμενο τεμάχιο

2.13 |
Το Acknowledgement Number είναι ίδιο με αυτό της αποδοχής σύνδεσης από τον εξυπηρετητή (δηλαδή 1) και το Sequence Number είναι ίδιο με το Acknowledgement Number διότι ο πελάτης αποστέλνει το τεμάχιο που ζήτησε ο εξυπηρετητής.

2.14 |
Έχουν μηδενικό μήκος δεδομένων

2.15 |
Το κάθε ένα από αυτά τα 2 πεδία είναι 4 bytes → 32 bits. Άρα μπορούν να φτάσουν έως και 4 Δισ περίπου (2^32)

2.16 |
Display filter : **tcp.port == 21 and tcp.flags.syn == 1 or (tcp.dstport == 21 and tcp.ack == 1 and tcp.seq == 1)**

2.17 |
Παράθυρο Υπολογιστή : 8192
Παράθυρο Εξυπηρετητή : 65535

2.18 |
Στο πεδίο 'Window'

2.19 |
Μικρότερο μέγεθος παρθύρου έχει ο υπολογιστής μου

2.20 |
MSS : 1460 bytes

2.21 |
Επειδή πρόκειται για πακέτο IPv4 προκύπτει ως MTU - 40 (→ MTU = 1500 bytes)

2.22 |
Στο πεδίο 'Options'

2.23 |
MSS : 536 bytes

2.24 |
Και πάλι, πειδή πρόκειται για πακέτο IPv4 προκύπτει ως MTU - 40

2.25 |
Η MSS είναι 536 bytes αρα 536 + 20 (IPv4 Header) + 20 (TCP Header) = 576 bytes

2.26 |
Το flag FIN

2.27 |
Display filter : tcp.port == 21 and tcp.flags.fin == 1

2.28 |
Την εκκινεί ο εξυπηρετητής

2.29 |
2 τεμάχια, ένα από τον εξυπηρετητή και ένα από τον υπολογιστή μου

2.30 |
Header Length : 20 bytes

2.31 |
Έχουν μηδενικό μέγεθος δεδομένων

2.32 |
Το πακέτο αποτελείται μόνο από επικεφαλίδες / headers, άρα το συνολικό μήκος είναι Ethernet Header + IPv4 Header + TCP Header = 14 + 20 + 20 = 54 bytes

2.33 |
Αντιστοίχως, λόγω έλλειψης δεδομένων, το πακέτο θα έχει μήκος 54 bytes συνολικά

2.34 |
Από τον υπολογιστή μου : 119 bytes
Από τον εξυπηρετητή : 377 bytes

2.35 |
Από τον αριθμό Sequence Number και Acknowledgement Number του τελευταίου πακέτου (διαδικασία απόλυσης)

2.36 |
Display filter : tcp.port == 20

2.37 |
MSS υπολογιστή : 1460 bytes
MSS εξυπηρετητή : 536 bytes

2.38 |
Είναι ίσο με την MSS (1460 bytes) + IPv4 Header (20 bytes) + TCP Header (20 bytes) = 1500 bytes

2.39 |
Είναι περίπου 0.026 sec

2.40 |
Οχι, δεν στέλνει για κάθε τεμάχιο. Στέλνει περίπου κάθε 5 τεμάχια (από 3 μέχρι 9)

2.41 |
Αλλάζει μόνο μία φορά. Η μικρότερη τιμή είναι τα 4097 bytes

2.42 |
Frame : 590 bytes, Ethernet Header : 14 bytes, IPv4 Header : 20 bytes, TCP Header : 32 bytes

2.43 |
Ναι, είναι

2.44 |
Θα τα έστελνε χωρίς να τα κάνει fragment και το gateway του δικτύου του υπολογιστή θα αναγκαζόταν να κάνει fragmentation στο datagram του πακέτου και να το μεταδώσει στουν υπολογιστή / πελάτη

2.45 |
Από τον υπολογιστή : 0 bytes
Από τον εξυπηρετητή : 61441 bytes

2.46 |
525.13 Kbytes/sec

2.47 |
Όχι, δεν υπήρξαν

Ex. 3 | TCP conjestion avoidance

3.1 |
Display filter : tcp.port == 20

3.2 |
IPv4 address : 147.102.40.15

3.3 |
Είναι περίπου 0.015 sec. Είναι ταχύτερο από αυτό του 2.39

3.4 |
Παρατηρούμε κάθε φορά ότι το μέγεθος του παραθύρου μεγαλώνει εκθετικά (2 πλασιάζεται κάθε φορά)

3.5 |
Έστειλε αρχικά 4 τεμάχια. Ναι, το πλήθος είναι σύμφωνο.

3.6 |
Στο δεύτερο έστειλε 6 τεμάχια και στο τρίτο έστειλε 10. Γιατί αυξάνει τον αριθμό, ανάλογα με τα acknowledges που λαμβάνει.

3.7 |
Ναί, είναι σχετικά παρόμοιο. Στο πρώτο έστειλε 4 τεμάχια (δηλαδή όσα και προηγουμένως), στο δεύτερο έστειλε 4 τεμάχια (λιγότερα σε σχέση με πριν) και στο 3 έστειλε 2 τεμάχια (και πάλι λιγότερα σε σχέση με πριν).

Ex. 4 | UDP data transfer

4.1 |
Capture filter : udp

4.2 |
Πεδία : Source Port (2 bytes), Destination Port (2 bytes), Length (2 bytes), Checksum (2 bytes)

4.3 |
UDP Header Length : 8 bytes

4.4 |
Το δεδομενόγραμμα βάσει του Payload Length έχει μήκος 98 bytes

4.5 |
Εκφράζει το μήκος των δεδομένων + το μήκος της επικαφαλίδας UDP

4.6 |
Το ελάχιστο μέγεθος UDP payload είναι να μην υπάρχουν καθόλου δεδομένα, άρα 0. Το μέγιστο μέγεθος καθορίζεται από το μέγιστο μήκος του IPv4 που μπορεί να μεταφερθεί που είναι 576 bytes. Άρα 576 - IPv4 Header (20) - UDP Header (8) = 548 bytes για το UPD payload.

4.7 |
Ισούται με το μέγιστο μέγεθος πακέτου IPv4 πλην την επικεφαλίδα του IPv4, άρα 556 bytes.

4.8 |
Όχι, δεν παρατήρησα.

4.9 |
Display filter : dns

4.10 |
IPv6 Address : fe80::197:6309:6d7b:fba0

4.11 |
Source Port: 61232
Destination Port: 53

4.12 |
Source Port: 53
Destination Port: 61232

4.13 |
Η θύρα 53 (default θύρα DNS)