Ονοματεπώνυμο: Δημήτρης Βασιλεία	Ομάδα: 3
Όνομα PC/ΛΣ: LAPTOP-N4V173NU	Ημερομηνία: 30 / 11 / 2022
Διεύθυνση IP: 147.102.238.14	Διεύθυνση MAC: 5C - 61 - 99 - 02 - FA - 83

Εργαστηριακή Άσκηση 8
TELNET, FTP και TFTP

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1 (Αυτή η άσκηση πραγματοποιήθηκε από το δίκτυ IPv4: 192.168.1.0, 2-3 είναι από το εργαστήριο)

1.1 Χρησιμοποιεί το TCP

1.2 Οι θύρες 23 και 58.940

1.3 Η θύρα 23

1.4 Πίτες telnet

1.5 Απαντώντας 147.102.40.11 Don't Echo, Will Echo Do Echo

Απαντώντας 192.168.1.7: Won't Echo, Will Echo

1.6 Ναι δίδει υπάρχει Do Echo που ζήτησε. Το PC (ως δέχτης) ζητώ απάντησα Will Echo

1.7 Ναι δίδει ζητάω Don't Echo. Το PC (ως επιβεβαίωσε) για Won't Echo

1.8 Ναι δίδη ~~υπάρχει~~ ζητάω Will Echo.

1.9 Ναι, έχεται ζητάω Do Echo για Server

1.10 Λειτουργούμε ότι για κάθε χαρακτήρα που πλήκτρου, ο εξυπηρετητής τον επαναλαμβάνη.

1.11 Επεις ζητήσαμε για Do Echo από τον εξυπηρετητή να επαναλαφβάνη τον χαρακτήρα και αυτός μας το επιβεβαίωσε για Will Echo.

1.12 telnet and ip.src == 192.168.1.7

1.13 Χρειάζονται 5 πακέτα (μαζί με το <Enter>)

1.14 Χρειάζεται 5 πακέτα (μαζί με το <Enter>)

1.15 Όχι δεν ζητάω.

1.16 Όχι δεν παρατηρήθηκε

1.17 Παρόλο που δεν υπήρχε Ετοίμη Don't Echo, το terminal μπήκε ως το μήνυμα φθάνεται να κλειδώ και γι' αυτό δεν εμφανίζονται οι χαρακτήρες

1.18 Τα μηνύματα μεταφέρθηκαν αυτούσια χωρίς αδρώστα και κρυπτογράφηση, δηλαδή αν υποκλαπή κάποιο μήνυμα, είναι δυνατόν να διαρρεύσουν username και password. Επειδή το terminal κρίθηκε μη ασφαλές.

2

2.1 ip.host == 147.102.40.15

2.2 Ενεργοποιείται το debugging άρα βαθιά σε επίπεδο.

2.3 Χρησιμοποιεί το TCP.

2.4 Για μεταφορά δεδομένων: Source Port: 20 Destination Port:55055
Για εντολές ελέγχου. Source Port 21 Destination Port 55054

2.5 Γίνεται από την πλευρά του εξυπηρετητή.

2.6 Οι εντολές είναι οι OPTS, USER, PASS, HELP, PORT, NLST, QUIT

2.7 Οι εντολές σερβίρονται με ένα βέλος δίπλα τους για να ξεχωρίζουν

2.8 Με την εντολή USER

2.9 Χρειάζεται ένα πακέτο

2.10 Με την εντολή PASS

2.11 Χρειάζεται ένα πακέτο

2.12 Μια ομοιότητα είναι ότι δεν υπάρχει κρυπτογράφηση στα δεδομένα. Διαφορά είναι ότι στο TELNET
οι χαρακτήρες στέλνονται ένας ανά πακέτο, ενώ στο TCP όλοι σε ένα πακέτο (ίσως για name και για password)

2.13 ~~Ναι υπάρχει~~ Όχι δεν υπάρχει.

2.14 Είναι οι εντολές PORT και CONF

2.15 στέλνουμε ένα πακέτο από εμάς και 9 από τον εξυπηρετητή

2.16 Στο τελευταίο response μήνυμα, αυτό που αναφέρεται το 214, υπάρχει μενού.

2.17 Την IP του αποστολέα.

2.18 Προκύπτει από τον εξής τύπο: 55055= 256·215 + 15. 215, 15 είναι
οι δύο τελευταίοι αριθμοί στην εντολή PORT.

2.19 Η εντολή NSLT

2.20 Πρώτα πρέπει να γίνει established η θύρα για τα δεδομένα που θα λάβει ο πελάτης
και έπειτα να εμφανιστεί το περιεχόμενο με την εντολή NSLT.

2.21 Είναι εντολή QUIT

2.22 Με Goodbye

2.23 tcp.flags.fin ==1

2.24 Από την πλευρά του Εξυπηρετητή.

* 2.25 Η θύρα πηγής ήταν η 21 και η θύρα προορισμού η 61.939 για εντολές ελέγχου.
Για μεταφορά δεδομένων, θύρα πηγής είναι η 61940 και προορισμού η 55674

2.26 Είναι οι εντολές USER, PASS, opts, syst, site, PWD, TYPE,
PASV, LIST

2.27 Οι δύο χρήστες είναι anonymous και windows IE User @

2.28 Η εντολή LIST

2.29 Entering Passive Mode (147,102,40,15,45,154)

2.30 Από την πλευρά του πελάτη

2.31 Χρησιμοποιείται η θύρα 11674 από τον εξυπηρετητή για την μεταφορά δεδομένων, προκύπτει από τα δύο τελευταία νούμερα της απάντησης στην 2.29 ως εξής: 11674 = 256·45+154

2.32 Επιλέγεται τυχαία μία διαθέσιμη θύρα.

2.33 3 πακέτα δεδομένων. Τα δύο πρώτα έχουν μέγεθος 536 bytes και το 3ο 307 bytes

2.34 Εφτά το μέγιστο μέγεθος δεδομένων θα έπρεπε να έχουμε 536+20+20 = 576 = MTU, όπου από 20 bytes είναι οι TCP και IPv4 headers.

2.35 Ετέθη από την πλευρά του πελάτη

2.36 Δεδομένων από την πλευρά του εξυπηρετητή Τη.

3

3.1 Το UDP

3.2 Source Port: 53946, Destination Port: 69

3.3 Source port: 16533, Destination Port: 53946

3.4 Η θύρα 69

3.5 Ο πελάτης και ο εξυπηρετητής επιλέγουν τυχαία ένα ID (TID) και αυτά τα TIDs περνιούνται στο UDP σαν θύρα προορισμού και προέλευσης. Επιπλέον σημειώστε ότι αρχικά το PC μας δεν επιλέγει *

3.6 Με ASCII

3.7 Είναι το μήνυμα, δηλαδή το Read Request και το πεδίο Type του TFTP ~~⊙~~ το οποίο είναι netascii

3.8 Read Request, Data Packet, Acknowledgement

3.9 Το TFTP ξαναστέλνει όσα μηνύματα δεν παίσθηκαν, καθώς δεν υπάρχει επιβεβαίωση

3.10 Ο τύπος Read Request και το πεδίο Opcode.

3.11 558 bytes.

3.12 512 bytes.

3.13 Όλα τα μηνύματα που το τελευταίο μεταφέρουν δεδομένα μεγέθους 512 bytes. Το τελευταίο μεταφέρει δεδομένα από 0 έως 511 bytes (εδώ πχ) για να ξέρει ο πελάτης ότι τελείωσε η μετάδοση.

* Είναι TID και source port επίσης την θύρα 69 του εξυπηρετητή. Ο εξυπηρετητής έχει σαν source port το δικό του TID και σαν destination Port το TID του δικού μας PC που δίνει ως πρώτο βήμα. Από μία παρατήρηση για τα υπόλοιπα μηνύματα εναλλάσσονται τα source και destination ports.