Ονοματεπώνυμο: Παναγιώτης Ζευγολατάκος		Ομάδα: 3
Όνομα PC/ΛΣ: panos/Windows 10		Ημερομηνία: 23/11/2020
Διεύθυνση IP: 192.168.0.18	Διεύθυνση MAC:	30 – 24 – 32 – 79 – 09 – 14

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

1.1 TCP

1.2 23 και 50358.

1.3 Η θύρα 23.

1.4 telnet

1.5 Will echo, Won't echo, Do echo, Don't echo.

1.6 Ναι, ζητάει (Do echo) και ο υπολογιστής μου δέχεται (Will echo).

1.7 Ναι, ζητάει (Don't echo) και ο υπολογιστής μου δέχεται (Won't echo).

1.8 Όχι.

1.9 Ναι.

1.10 Όταν στέλνει ο υπολογιστής μου ένα χαρακτήρα, αυτός ο χαρακτήρας στέλνεται πίσω από τον εξυπηρετητή (echo).

1.11 Ο εξυπηρετητής έχει απαντήσει "Will echo" στο login, επομένως όταν στέλνουμε ένα χαρακτήρα αυτός ο χαρακτήρας θα στέλνεται πίσω (echo), ενώ στο password έχει απαντήσει "Won't echo", επομένως όταν στέλνουμε ένα χαρακτήρα αυτός ο χαρακτήρας δε θα στέλνεται πίσω, το οποίο είναι και λογικό, εκτός κι αν θέλαμε να εμφανίζεται ο κωδικός στην οθόνη.

1.12 telnet and ip.src == 192.168.0.18

1.13 Ένα για τον κάθε χαρακτήρα, άρα 4 (+1 για \r\n).

1.14 Παρομοίως, ένα για τον κάθε χαρακτήρα, άρα 4 (+1 για \r\n).

1.15 Όχι.

1.16 Όχι.

1.17 Ο κωδικός δεν εμφανίζεται στην οθόνη για λόγους ασφάλειας. Παρόλο που ο εξυπηρετητής είναι σε κατάσταση echo, επιλέγει να μην κάνει echo τον κωδικό για λόγους ασφάλειας.

1.18 Η υπηρεσία Telnet δεν έχει ενσωματωμένα μέτρα ασφαλείας, επομένως έχει σοβαρά προβλήματα ασφαλείας. Τα δεδομένα που ανταλλάσσονται δεν είναι κρυπτογραφημένα, επομένως οποιοσδήποτε βρίσκεται στο ίδιο δίκτυο μπορεί με έναν αναλυτή πρωτοκόλλων (όπως κάναμε εμείς τώρα με το Wireshark) να κρυφακούσει. Συνεπώς, εάν το δίκτυο στο οποίο βρίσκεται ο χρήστης δεν είναι ασφαλές, δεν προτείνεται να χρησιμοποιηθεί το πρωτόκολλο Telnet (πόσο μάλλον στο διαδίκτυο). Εναλλακτική (και ασφαλής) επιλογή αποτελεί το πρωτόκολλο SSH (Secure SHell).

2

2.1 host 147.102.40.15

2.2 Ενεργοποιεί το debugging.

2.3 TCP.

2.4 Έλεγχος: θύρες 21 και 65119, Μεταφορά δεδομένων: θύρες 20 65120.

2.5 Από την πλευρά του εξυπηρετητή.

2.6 Ενεργό.

2.7 OPTS UTF8 ON, USER anonymous, PASS labuser@cn, HELP, PORT 147,102,131,212,254,96, NLST, QUIT

2.8 Εμφανίζονται, μετά από τις εντολές που εκτελούμε, με τον παρακάτω τρόπο:

---> OPTS UTF8 ON

2.9 USER

2.10 1.

2.11 PASS

2.12 1.

2.13 Μια ομοιότητα στον τρόπο μεταφοράς είναι πως δεν είναι κρυπτογραφημένος ο κωδικός πρόσβασης σε κανένα από τα δύο. Μια διαφορά είναι πως το TELNET μεταφέρει χαρακτήρες ASCII, δηλαδή μεταφέρει το όνομα και τον κωδικό γράμμα-γράμμα, ενώ το FTP τα μεταφέρει σε πακέτα.

2.14 Όχι.

2.15 Η PROT και η AUTH.

2.16 1 από εμένα και 9 από την εξυπηρετητή.

2.17 Η πρώτη γραμμή γράφει "Response: 214-" ενώ η τελευταία γραμμή γράφει "Response: 214 ", δηλαδή η παύλα έχει αντικατασταθεί από κενό και δηλώνει το τέλος της αποστολής.

2.18 Παριστάνουν τη διεύθυνση IP που μου έχει δοθεί.

2.19 **254***256 + **96** = **65120**

2.20 NLST

2.21 Επειδή η εντολή ls μεταφράζεται σε ftp PORT και NLST, με τις οποίες στήνεται η σύνδεση δεδομένων και μεταφέρονται τα δεδομένα αντίστοιχα.

2.22 QUIT

2.23 221 Goodbye.

2.24 tcp.flags.fin == 1

2.25 Η απόλυση των συνδέσεων TCP που αφορούν τις εντολές ελέγχου γίνεται από εμάς, ενώ της σύνδεσης μεταφοράς από τον εξυπηρετητή.

2.26 Έλεγχος: θύρες 21 και 49211, Μεταφορά δεδομένων: θύρες 32318, 49216

2.27 USER anonymous, PASS chrome@example.com, SYST, PWD, TYPE I, SIZE /, CWD /, PASV, LIST –l, QUIT

2.28 Όνομα: anonymous

Κωδικός χρήστη: chrome@example.com

2.29 LIST –l

2.30 Παθητικό, αφού εγώ ξεκίνησα τη σύνδεση των δεδομένων και χρησιμοποιείται η εντολή PASV αντί της PORT.

2.31 227 Entering Passive Mode (147,102,40,15,126,62).

2.32 Από την πλευρά του πελάτη.

2.33 Η απάντηση είναι παρόμοια με το ερώτημα 2.19: **162***256+**62**=**32318**

2.34 Αποτελεί επιλογή του πελάτη.

2.35 Στάλθηκαν δύο πακέτα, μεγέθους 536 και 490 bytes.

2.36 Είναι ίσο με το MSS του εξυπηρετητή.

2.37 Από την πλευρά του εξυπηρετητή.

2.38 Από την πλευρά του πελάτη.

3

3.1 UDP

3.2 Θύρα πηγής: 62114, Θύρα προορισμού: 69.

3.3 Θύρα πηγής: 25119, Θύρα προορισμού: 62114.

3.4 Η θύρα 69.

3.5 Επιλέγονται τυχαία, ενώ ο εξυπηρετητής διαβάζει την τιμή που διάλεξε ο πελάτης από την πρώτη επικοινωνία.

3.6 Σε ASCII.

3.7 Στο πρώτο μήνυμα:

Trivial File Transfer Protocol

Opcode: Read Request (1)

Source File: rfc1350.txt

Type: **netascii**

3.8 Read Request, Data Packet, Acknowledgement

3.9 Το πρόβλημα αυτό αντιμετωπίζεται με το να στέλνει ο πελάτης επιβεβαίωση για κάθε block που λαμβάνεται, και αφού τη λάβει ο εξυπηρετητής θα στείλει το επόμενο block.

3.10 Opcode: Acknowledgement (4)

3.11 516 bytes.

3.12 512 bytes.

3.13 Η σύνδεση απολύεται όταν μήνυμα που θα σταλεί θα έχει μέγεθος μεταξύ 0 και 511 bytes (δηλαδή θα είναι το τελευταίο).