ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΙΣΤΩΝ

ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ – 7ο ΕΞΑΜΗΝΟ

Τζομάκα Αφροδίτη – ΑΜ: 03117107

Ονοματεπώνυμο: Τζομάκα Αφροδίτη	**Ομάδα:** 2
Όνομα PC/ΛΣ: DESKTOP-II5SP0K/windows 10	**Ημερομηνία:** 1-12-2020
Διεύθυνση IP: 192.168.0.112	**Διεύθυνση MAC:** A8:6B:AD:73:3E:A5

8η Ομάδα Ασκήσεων

ΑΣΚΗΣΗ 1

1.1. TCP.
1.2. Χρησιμοποιούνται οι θύρες 50049 και 23.
1.3. Η θύρα 23.
1.4. telnet.
1.5. 147.102.40.15 -> 192.168.0.112 : Do Echo
192.168.0.112 -> 147.102.40.15 : Will Echo
147.102.40.15 -> 192.168.0.112 : Don't Echo/Will Echo
192.168.0.112 -> 147.102.40.15 : Won't Echo
1.6. Ναι, ζητάει να επαναλαμβάνονται οι χαρακτήρες μέσω της εντολής Do Echo και ο υπολογιστής μας δέχεται απαντώντας Will Echo.
1.7. Ναι, ζητάει να μην επαναλαμβάνονται οι χαρακτήρες μέσω της εντολής Don't Echo και ο υπολογιστής μας δέχεται απαντώντας Won't Echo.
1.8. Ναι μέσω της εντολής Will Echo.
1.9. Ναι έχει προηγηθεί εντολή Do Echo.
1.10. Παρατηρούμε ότι ο edu-dy.cn.ntua.gr επαναλαμβάνει (echo) τους χαρακτήρες που του αποστέλλουμε.
1.11. Η συμπεριφορά που αναφέρθηκε παραπάνω είναι η αναμενόμενη εφόσον αφενός ο εξυπηρετητής είχε προθυμοποιηθεί να κάνει echo και αφετέρου ο υπολογιστής μας το ζήτησε.

1.12. ip.src == 192.168.0.112 && telnet.
1.13. 5, 1 για κάθε χαρακτήρα + 1 για το Enter.
1.14. 5, 1 για κάθε χαρακτήρα + 1 για το Enter.
1.15. Όχι.
1.16. Όχι.
1.17. Ως γνωστόν για λόγους ασφαλείας ο κωδικός δεν γίνεται ποτέ echo στην οθόνη προκειμένου να μην υποκλαπεί και αυτό δεν χρειάζεται καν κάποια προτοπή τύπου don't echo.
1.18. Γενικά η υπηρεσία TELNET, πέραν των στοιχειωδών όπως η απόκρυψη του κωδικού από την οθόνη όπως αναφέραμε παραπάνω, δεν παρέχει υψηλή ασφάλεια καθώς δεν χρησιμοποιεί κρυπτογράφηση. Επομένως είναι ευάλωτο στις επιθέσεις υποκλοπής κωδικών και δεδομένων ακόμα και μέσω ενός απλού αναλυτή πρωτοκόλλων όπως το Wireshark που χρησιμοποιούμε και εμείς.

ΑΣΚΗΣΗ 2

2.1. host 147.102.40.15.
2.2. Επιτρέπει το debugging (Enables debugging).
2.3. TCP.
2.4. Χρησιμοποιούνται οι θύρες 52761,52762(client), 21(commands) και 20 (data).
2.5. Από την πλευρά του εξυπηρετητή.
2.6. Υλοποιεί τον ενεργό τρόπο λειτουργίας by default.
2.7.

```
Request: OPTS UTF8 ON
Request: USER anonymous
Request: PASS labuser@cn
Request: HELP
Request: PORT 147,102,131,141,206,26
Request: NLST
Request: QUIT
```

2.8. Ναι, εμφανίζονται με το όνομά τους και με τα σύμβολα '--->' να προηγείται.
2.9. Με την εντολή USER.
2.10. 2 πακέτα (το ένα για το ack).
2.11. Με την εντολή PASS.
2.12. 2 πακέτα (το ένα για το ack).
2.13. Μια ομοιότητα των δύο πρωτοκόλλων είναι ότι και τα 2 δεν κάνουν echo το password ενώ μια διαφορά είναι ότι το TELNET χρειάζεται τόσα πακέτα όσα οι χαρακτήρες που «πατήθηκαν» (echo) ενώ το FTP χρειάζεται 2 πακέτα (το ένα για το ack).
2.14. Όχι.
2.15. AUTH, CCC.
2.16. 9 πακέτα από τον εξυπηρετητή και 1 από εμάς.

2.17. Προκειμένου να δηλωθεί ότι ακολουθούν πακέτα για εμφάνιση μηνυμάτων σε πολλαπλές γραμμές, το φορμάτ έχει ως εξής: «αριθμός '–' κείμενο». Το τελευταίο πακέτο του μηνύματος δεν έχει την παύλα (–) και δηλώνει το τέλος της αποστολής πακέτων.

2.18. Αποτελούν τη διεύθυνση IP του πελάτη.

2.19. Προκύπτει πολλαπλασιάζοντας τον πρώτο αριθμό επί το 256 και προσθέτοντας τον δεύτερο.

2.20. NLST.

2.21. Σύνδεση ξεχωριστά για μεταφορά δεδομένων. Για να γνωστοποιηθεί η θύρα προορισμού (πελάτη) που θα εκτυπωθεί η λίστα των δεδομένων για την νέα αυτή σύνδεση.

2.22. QUIT.

2.23. Goodbye.

2.24. tcp.flags.fin == 1.

2.25. Ελέγχου από την πλευρά του πελάτη και δεδομένων από την πλευρά του εξυπηρετητή.

2.26. 57628, 21 (ελέγχου), 57629, 40429 (δεδομένων).

2.27.

```
Request: USER anonymous
Request: PASS mozilla@example.com
Request: SYST
Request: FEAT
Request: OPTS UTF8 ON
Request: PWD
Request: TYPE I
Request: PASV
Request: CWD /
Request: LIST
```

2.28. Ως όνομα χρησιμοποιήθηκε το anonymous και ως κωδικός το mozilla@example.com.

2.29. LIST.

2.30. Παθητικό.

2.31. 227 Entering Passive Mode (147,102,40,15,157,237).

2.32. Ο πελάτης.

2.33. Χρησιμοποιείται η θύρα 40429.

2.34. Προσθέτοντας 1 στην θύρα ελέγχου.

2.35. 2 πακέτα δεδομένων, το πρώτο 536 και το δεύτερο 490.

2.36. Διότι η MTU του εξυπηρετητή είναι 576.

2.37. Του πελάτη.

42	5.481570	147.102.40.15	147.102.131.220	FTP-DATA	544	FTP Data: 490 bytes (PASV) (CWD /)
44	0.000437	147.102.131.220	147.102.40.15	TCP	54	57629 → 40429 [FIN, ACK] Seq=1 Ack=1028 Win=131072 Len=0
45	0.011341	147.102.131.220	147.102.40.15	TCP	54	57628 → 21 [FIN, ACK] Seq=101 Ack=782 Win=131072 Len=0
50	0.186407	147.102.40.15	147.102.131.220	TCP	54	21 → 57628 [FIN, ACK] Seq=805 Ack=102 Win=65920 Len=0

2.38. Του εξυπηρετητή (όπως φαίνεται και παραπάνω).

ΑΣΚΗΣΗ 3

3.1. UDP.
3.2. Source Port: 50603, Destination Port: 69.
3.3. Source Port: 28566, Destination Port: 50603.
3.4. Η 69.
3.5. Η θύρα του host μηχανήματος επιλέγεται τυχαία ώστε να προληφθεί η επιλογή της ίδιας θύρας 2 φορές συνεχόμενα. Το αρχικό request στέλνεται στην γνωστή θύρα 69 του server ενώ στην συνέχεια ο server διαλέγει και εκείνος (τυχαία) μια θύρα για την μετέπειτα επικοινωνία/ανταλλαγή δεδομένων.
3.6. ASCII.
3.7. Ο τρόπος αυτός καθορίζεται στο πρώτο μήνυμα επικοινωνίας πελάτη – εξυπηρετητή με την προτροπή Transfer type: netascii (πεδίο type επικεφαλίδας tftp = netascii).
3.8. Read request, Data Packet, Acknowledgement.
3.9. Στέλνει το ίδιο πακέτα Aknowledgement.
3.10. Τα acknowledgement πακέτα, ταυτοποιώντας (επαναλαμβάνοντας) το πεδίο block που προσδιορίζει το block number κάθε πακέτου.
3.11. 516 bytes.
3.12. 512 bytes δεδομένων.
3.13. Μέσω της μετάδοσης πακέτου δεδομένων με μήκος 0 έως 511 byte δεδομένων (Datagram length < 516).