Ονοματεπώνυμο: Ιωάννης Γιαννούκος			**Ομάδα:** 3
Όνομα PC/ΛΣ: JohnJohn / Windows 11		**Ημερομηνία:**	**5/12/2022**
Διεύθυνση IP:	**147.102.200.242**	**Διεύθυνση MAC:**	**3C-6A-A7-9A-B3-CF**

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.

Άσκηση 1 (IP: 192.168.1.4)

1.1) TCP

1.2) Στην διαδικασία αυτή παρατηρώ ότι χρησιμοποιούνται οι θύρες 23 και 50916.

1.3) Η θύρα 23 αντιστοιχεί στο πρωτόκολλο εφαρμογής TELNET.

1.4) Φίλτρο απεικόνισης: “telnet”

1.5) Τα 3 προηγούμενα μηνύματα που ανταλλάχθηκαν περιέχουν τις εξής εντολές:
(My PC) → (147.102.40.15) : Will Echo
(147.102.40.15) → (My PC) : Don’t Echo , Will Echo
(My PC) → (147.102.40.15) : Won’t Echo

1.6) Ο εξυπηρετητής ζητά από τον υπολογιστή μου να επαναλαμβάνει τους χαρακτήρες που λαμβάνει με την εντολή `Will Echo`. Ο υπολογιστής μου εγκρίνει το αίτημα αυτό, καθώς δεν στέλνει `Don’t Echo`.

1.7) Ναι, ο εξυπηρετητής με την εντολή `Don’t Echo` ζητά από τον υπολογιστή μου να μην εκτελεί `echo` με τους χαρακτήρες που λαμβάνει από τον εξυπηρετητή, και απαντά με `Won’t Echo` για να δηλώσει ότι εγκρίνει το αίτημα.

1.8) Ναι, ο εξυπηρετητής προτίθεται να επαναλαμβάνει τους χαρακτήρες που λαμβάνει με την εντολή `Will Echo`.

1.9) Ναι, όπως εξηγήθηκε στο προηγούμενο υποερώτημα.

1.10) Καθώς έχει αιτηθεί από τον υπολογιστή μου στον εξυπηρετητή να εκτελείται `echo`, για κάθε χαρακτήρα που στέλνω από τον υπολογιστή μου στέλνεται ο ίδιος χαρακτήρας από τον εξυπηρετητή στον υπολογιστή μου.

1.11) Το φαινόμενο που εξηγείται στο προηγούμενο υποερώτημα, οφείλεται στην δήλωση του edu-dy.cn.ntua.gr για echo.

1.12) Φίλτρο απεικόνισης: “telnet and ip.dst == 147.102.40.15”

1.13) Για να μεταφερθεί η πληροφορία του ονόματος χρειάζονται 5 πακέτα IPv4 από τον υπολογιστή μου στον εξυπηρετητή.

1.14) Για να μεταφερθεί η πληροφορία του κωδικού χρήστη χρειάζονται 5 πακέτα IPv4 από τον υπολογιστή μου στον εξυπηρετητή.

1.15) Όχι, δεν επαναλαμβάνει τους χαρακτήρες του κωδικού που εισάγονται.

1.16) Όχι.

1.17) Λογικά οι χαρακτήρες που εμφανίζονται στην οθόνη του υπολογιστή μου είναι η χαρακτήρες που λαμβάνει από τον εξυπηρετητή, και όχι οι χαρακτήρες που πληκτρολογούνται από εμένα. Αυτό εξηγεί το γεγονός ότι ο κωδικός δεν φαίνεται στην οθόνη μου.

1.18) Η υπηρεσία Telnet δεν έχει επαρκή ασφάλεια στην μεταφορά δεδομένων. Κατ’ αρχάς, η πληροφορία που φέρουν τα πακέτα δεν παρέχουν διαδικασία κρυπτογράφησης και, επιπλέον, κάποιος μπορεί εύκολα να διαβάζει τα πακέτα που στέλνονται από τον υπολογιστή μου στον εξυπηρετητή με επίθεση MiM (Man-In-the-Middle), μαθαίνοντας το όνομα και τον κωδικό μου.

Άσκηση 2

2.1) Φίλτρο σύλληψης: “host 147.102.40.15”

2.2) Ενεργοποιεί την λειτουργία αποσφαλμάτωσης (debugging).

2.3) Μόνο TCP.

2.4) Κατά την διάρκεια όλης της σύνδεσης χρησιμοποιείται η θύρα 21 και η θύρα 20 χρησιμοποιείται μόνο για την τριπλή χειραψία για εκκίνηση της διαδικασίας μεταφοράς δεδομένων.

2.5) Ο εξυπηρετητής ξεκινά την σύνδεση για μεταφορά δεδομένων, έπειτα από την εντολή `ls` που εκτέλεσε ο υπολογιστής μου.

2.6) Ο πελάτης έστειλε τις εξής εντολές:

OPTS UTF8 ON
USER anonymous
PASS labuser@cn
HELP
PORT 147, 102, 200, 242, 195, 51
NLST
QUIT

2.7) Ναι, οι παραπάνω εντολές εμφανίζονται ύστερα από την εκτέλεση της εντολής HELP.

2.8) Με την εντολή USER.

2.9) Χρειάστηκαν 2 πακέτα για να μεταφερθεί το όνομα χρήστη, καθώς το πρώτο από αυτά φαίνεται να μην στάλθηκε επιτυχώς.

2.10) Με την εντολή PASS.

2.11) Χρειάστηκε 1 πακέτο.

2.12) Στο πρωτόκολλο TELNET παρατηρήσαμε ότι τόσο για το όνομα χρήστη όσο και για τον κωδικό χρειάζονταν τόσα πακέτα όσοι και οι χαρακτήρες της συμβολοσειράς που εισήγαγε ο χρήστης, και για το όνομα χρήστη για κάθε ένα από τα πακέτα αυτά ο εξυπηρετητής επαναλάμβανε τον χαρακτήρα για επιβεβαίωση.

2.13) Ναι, η εντολή help μεταφράζεται ως HELP στο πρωτόκολλο FTP.

2.14) Δύο από τις εντολές που δεν υποστηρίζονται από τον εξυπηρετητή είναι οι AUTH και ENC. Αυτό το καταλαβαίνουμε από τον αστερίσκο (*) που σημειώνεται σε αυτές.

2.15) Από τον υπολογιστή μου στάλθηκαν 3 πακέτα: 1 πακέτο για την εκτέλεση της εντολής HELP, και 2 πακέτα Acknowledgement για την πληροφορία που έλαβε. Από τον εξυπηρετητή στάλθηκαν 9 πακέτα.

2.16) Ο εξυπηρετητής για κάθε γραμμή δεδομένων που στέλνει σε ένα πακέτο FTP, πριν τα δεδομένα εισάγει έναν αριθμό και μια παύλα “-”, σημαίνοντας έτσι ότι η γραμμή αυτή είναι μία από πολλές άλλες γραμμές που θα σταλθούν για να ολοκληρωθεί η διαδικασία. Στην τελευταία γραμμή δεδομένων εισάγει στην αρχή τον ίδιο αριθμό με προηγουμένως και, αντί για παύλα “-” εισάγεται κενό “ ”, σημαίνοντας έτσι ότι στάλθηκε η τελευταία γραμμή δεδομένων.

2.17) Οι τέσσερεις πρώτοι αριθμοί παριστάνουν την διεύθυνση IP του υπολογιστή μου στο δίκτυο.

2.18) Η θύρα από την οποία θα διαβάσει ο πελάτης τα δεδομένα που στέλνει ο εξυπηρετητής υπολογίζεται πολλαπλασιάζοντας τον προτελευταίο αριθμό με 256 και προσθέτοντας τον τελευταίο αριθμό στην εντολή PORT. Δηλαδή, στην περίπτωσή μας η θύρα δεδομένων είναι 49971, δηλαδή 195·256+51.

2.19) Η εντολή NLST.

2.20) Επειδή ο υπολογιστής μου με την εντολή PORT ανακοινώνει στον εξυπηρετητή την θύρα στην οποία θα στείλει τα δεδομένα που θα ζητηθούν σε επόμενη εντολή.

2.21) Στην εντολή QUIT.

2.22) Ο εξυπηρετητής ανταποκρίνεται στην εντολή QUIT με το μήνυμα "221Goodbye."

2.23) Φίλτρο απεικόνισης: "tcp.flags.fin == 1".
2.24) Η απόλυση και των 2 συνδέσεων ξεκινούν από τον εξυπηρετητή.

2.25) Για την επικοινωνία για τις εντολές ελέγχου χρησιμοποιούνται οι εξής θύρες:
Source Port (My PC) : 50550
Destination Port (Server) : 21
Για την επικοινωνία για μεταφορά δεδομένου χρησιμοποιούνται οι εξής θύρες:
Source Port (My PC) : 50551
Destination Port (Server) : 56488

2.26) Οι εντολές που κάλεσε ο πελάτης είναι οι εξής (καταγράφονται και τα ορίσματα των εντολών, καθώς η κάθε εντολή καλείται με μόνο την πρώτη λέξη, πχ. USER):
USER anonymous
PASS IEUser@
opts utf8 on
syst
site help
PWD
noop
CWD /
TYPE A
PASV
LIST

2.27) Χρησιμοποιήθηκε ως όνομα "anonymous" και ως κωδικός χρήστη "IEUser@".

2.28) Η εντολή "LIST".

2.29) Ο εξυπηρετητής αποκρίνεται στην εντολή "PASV" με το μήνυμα "227 Entering Passive Mode (147,102,40,15,220,168).".

2.30) Από την πλευρά του υπολογιστή μου.

2.31) Χρησιμοποιείται η θύρα 56488.

2.32) Έστω A,B ο προτελευταίος και ο τελευταίος αριθμός, αντίστοιχα, που δίνεται στην απάντηση του εξυπηρετητή στην εντολή PASV (υποερώτημα 2.29).Ο αριθμός θύρας της σύνδεσης TCP για μεταφορά δεδομένων FTP υπολογίζεται από την εξής σχέση: $PORT = A \cdot 256 + B$. Στην περίπτωσή μας είναι: $56488 = 220 \cdot 256 + 168$.

2.33) Συνολικά στάλθηκαν 2 μηνύματα δεδομένων των 536 bytes και 1 μήνυμα μεγέθους 380 bytes.

2.34) Καθώς η MTU είναι 576 bytes, και κάθε μία από τις επικεφαλίδας IP και TCP είναι 20 bytes, το μέγεθος των δεδομένων FTP δεν μπορεί να ξεπερνά την τιμή

$$576 - 20 - 20 = 536\ bytes$$

2.35) Η απόλυση σύνδεσης TCP για εντολές ελέγχου FTP ξεκινούν από τον υπολογιστή μου.

2.36) Η απόλυση σύνδεσης TCP για μεταφορά δεδομένων FTP ξεκινούν από τον εξυπηρετητή.

Άσκηση 3

3.1) UDP

3.2) Το πρώτο πακέτο που στέλνεται από τον πελάτη στον εξυπηρετητή TFTP έχει:

Source Port :	62938
Destination Port :	69

3.3) Κατά την μεταφορά δεδομένων τα πακέτα που στέλνονται από τον εξυπηρετητή έχουν:

Source Port :	45323
Destination Port :	62938

3.4) Η θύρα 69.

3.5) Κατά την εκκίνηση της διαδικασίας μεταφοράς δεδομένων η θύρα που επιλέγει ο εξυπηρετητής για να στείλει τα δεδομένα είναι η θύρα από την οποία επικοινώνησε αρχικά ο πελάτης και η θύρα από την οποία στέλνει τα δεδομένα διαλέγεται τυχαία από τον εξυπηρετητή.

3.6) Η μεταφορά του αρχείου γίνεται σε ascii τρόπο.

3.7) Το παραπάνω καθορίζεται στο πρώτο πακέτο από τον πελάτη στον εξυπηρετητή στην τιμή του πεδίου Transfer Type, που είναι netascii.

3.8) Παρατηρούνται μόνο 3 τύποι μηνυμάτων: στον πρώτο ανήκει το μήνυμα με το οποίο ζητείται από τον εξυπηρετητή το αρχείο “rfc1350.txt”, στον δεύτερο ανήκουν τα μηνύματα που μεταφέρουν δεδομένα από τον εξυπηρετητή στον πελάτη, και στον τρίτο ανήκουν τα μηνύματα που στέλνονται από τον πελάτη για επιβεβαίωση των δεδομένων που έλαβε.

3.9) Παρόλο που το πρωτόκολλο UDP δεν παρέχει μηχανισμό επιβεβαιώσεων, το πρωτόκολλο TFTP αναγκάζει τον πελάτη να στέλνει μηνύματα επιβεβαίωσης που πληροφορεί τον εξυπηρετητή πόσα πακέτα έχει λάβει με επιτυχία.

3.10) Χρησιμοποιείται ο τύπος “Data” του οποίου το πεδίο “Data” έχει τον παραπάνω σκοπό.

3.11) 524 bytes

3.12) 516 bytes

3.13) Ο πελάτης καταλαβαίνει ότι έλαβε το τελευταίο πακέτο μετάδοσης δεδομένων αν αυτό έχει μέγεθος δεδομένων μεταξύ 0 και 511 bytes.