Ονοματεπώνυμο: Ναυσικά Αμπατζή		Ομάδα: 2
Όνομα PC/ΛΣ: Dell XPS 15-7590 Windows		Ημερομηνία: 1 /12 /2020
Διεύθυνση IP: 192.168.1.12	Διεύθυνση MAC:24-41-8C-65-26-BF	

Μέρος 1

1.1 TCP
1.2 Για την επικοινωνία χρησιμοποιούνται οι θύρες 23 και 55264.
1.3 Η θύρα 23 αντιστοιχεί στο πρωτόκολλο εφαρμογής Telnet.
1.4 telnet
1.5

- Do Echo 147.102.40.15,
- Will Echo 192.168.1.157
- Don't Echo, Will Echo 147.102.40.15
- Won't Echo 192.168.1.157

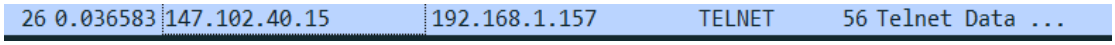
1.6 Όχι ο edu-dy.cn.ntua.gr δεν ζητά από τον υπολογιστή μου να επαναλαμβάνει τους χαρακτήρες που λαμβάνει, καθώς στο παραπάνω ερώτημα έχουμε εντοπίσει την εντολή Do Echo 147.102.40.15.

1.7 Ναι ο edu-dy.cn.ntua.gr ζητά από τον υπολογιστή μου να μην επαναλαμβάνει τους χαρακτήρες που λαμβάνει, καθώς στο παραπάνω ερώτημα έχουμε εντοπίσει την εντολή Don't Echo 147.102.40.15.

1.8 Ναι προτίθεται ο edu-dy.cn.ntua.gr να επαναλαμβάνει τους χαρακτήρες που λαμβάνει από τον υπολογιστή μου, καθώς στο παραπάνω ερώτημα έχουμε εντοπίσει την εντολή Will Echo 147.102.40.15

1.9

Το πρώτο μήνυμα που μεταφέρει τον χαρακτήρα 'a' :




```
Telnet
   Data: a
```

Όχι, δεν έχει προηγηθεί μήνυμα εντολή TELNET (Do Echo), με την οποία ο υπολογιστής μου ζητά την επανάληψη των χαρακτήρων από τον edu-dy.cn.ntua.gr.

1.10 Με την πρώτη προτροπή Login παρατηρώ ότι ενώ εγώ πληρκτρολόγησα ως username το abcd, μετά από κάθε χαρακτήρα που πληκτρολογούσα(κόκκινος) υπάρχει ένας ίδιος μπλε.

1.11 Αυτό σημαίνει ότι ο edu-dy.cn.ntua.gr επαναλάμβανε τους χαρακτήρες που λάμβανε από τον υπολογιστή μου.

1.12 ip.src == 192.168.1.157 && telnet

1.13 5

1.14 5

1.15 Όχι

1.16 Όχι

1.17 Δεν εμφανίζεται ο κωδικός για λόγους ασφάλειας, οπότε ανεξάρτητα σε ποια κατάσταση (Do ή Will Echo) δε θα δούμε χαρακτήρες.

1.18 Η υπηρεσία Telnet δεν είναι αξιόπιστη, καθώς εξ' ορισμού δεν κρυπτογραφεί την πληροφορία. Ο server, δηλαδή δεν ήταν υποχρεωμένος να κρύψει τον κωδικό προηγουμένως.

Μέρος 2

2.1 host 147.102.40.15

2.2 Η παράμετρος -d στην εντολή ftp επιτρέπει το debugging.

2.3 TCP

2.4 Οι θύρες που χρησιμοποιούνται για την επικοινωνία FTP : 65452,21

Οι θύρες που χρησιμοποιούνται για τη μεταφορά δεδομένων είναι οι : 65454,20

2.5 Από τη μεριά του client.

2.6 Στο cmd βλέπουμε το μήνυμα 200 PORT command successful, επομένως πρόκειται για ενεργή σύνδεση.

2.7

```
68 Request: OPTS UTF8 ON
70 Request: USER anonymous
71 Request: PASS labuser@cn
60 Request: HELP
83 Request: PORT 147,102,131,43,255,174
60 Request: NLST
60 Request: QUIT
```

2.8 Ναι οι εντολές αυτές εμφανίζονται στην οθόνη του προγράμματος φλοιού ftp με ένα βέλος(→) να προηγείται.

Πχ. `---> PORT 147,102,131,43,255,174`

2.9 USER [όνομα χρήστη]

2.10 1 πακέτο

2.11 PASS [κωδικός χρήστη]

2.12 1 πακέτο

2.13 Στο πρωτόκολλο TELNET απαιτούνται περισσότερα IPV4 πακέτα για να μεταφερεί το όνομα χρήστη και ο κωδικός αφού κάθε χαρακτήρας του μεταφέρεται σε ξεχωριστό

πακέτο, ενώ στο FTP το όνομα χρήστη και ο κωδικός μεταφέρονται σε ένα IPV4 πακέτο ο καθένας.

Μία ομοιότητα είναι ότι και τα δύο πρωτόκολλα στέλνουν αυτούσιους τους χαρακτήρες χωρίς κάποια κρυπτογραφία.

2.14 Όχι

2.15

```
214-CWD     XCWD    CDUP    XCUP    SMNT*   QUIT    PORT    PASV
214-EPRT    EPSV    ALLO*   RNFR    RNTO    DELE    MDTM    RMD
```

Δεν υποστηρίζονται οι εντολές με αστεράκι, εδώ δύο φαίνονται στο printscreen και είναι οι SMNT και ALLO.

2.16 Αναζητούμε τα μηνύματα HELP. Από τον υπολογιστή μου στάλθηκε 1 πακέτο και από τον εξυπηρετητή στάλθηκαν 9 πακέτα.

2.17 Για τα πολλαπλά μηνύματα απάντησης η πρώτη γραμμή έχει hyphen ανάμεσα απο το reply code και το text, όπως και οι επόμενες μέχρι και την προτελευατία. Η τελευταία δεν έχει αυτό το hyphen και κι έτσι δηλώνεται ότι ότι τελειώνει η αποστολή των πολλαπλών απαντήσεων.

2.18 Οι 4 πρώτοι δεκαδικοί αριθμοί του μηνύματος PORT αποτελούν τη source διεύθυνση του μηνύματος.

2.19 Ο αριθμός 65452 του ερωτήματος 2.4, προκύπτει εάν πολλαπλασιάσουμε με τον προτελευταίο αριθμό (255) με το 256 και στο αποτέλεσμα προσθέσουμε τον τελευταίο αριθμό (174). Δηλαδή : 255*256 = 65280 + 174 = 65452

2.20 Η εντολή NLST.

2.21 Διότι πρώτα πρέπει να έλεγχος της σύνδεση και μετά να εξεταστούν τα δεδομένα.

2.22 QUIT

2.23 Ο εξυπηρετητής αποκρίνεται με το μήνυμα 221 Goodbye στην εντολή bye του προγράμματος φλοιού ftp.

2.24 tcp.flags.fin == 1

2.25 Από τη μεριά του client.

2.26 Χρησιμοποιούνται οι θύρες 21,49321,(εντολές ελέγχου) και 49322,15322(μεταφορά δεδομένων).

2.27

Protocol	Length	Info
FTP	70	Request: USER anonymous
FTP	79	Request: PASS chrome@example.com
FTP	60	Request: SYST
FTP	59	Request: PWD
FTP	62	Request: TYPE I
FTP	62	Request: SIZE /
FTP	61	Request: CWD /
FTP	60	Request: PASV
FTP	63	Request: LIST -l
FTP	60	Request: QUIT

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

2.29 Εντολή : LIST -l

2.30 Ο πλοηγός χρησιμοποιεί παθητικό τρόπο λειτουργίας του πρωτοκόλλου TCP και αυτό φαίνεται από το Request 60 του ερωτήματος 2.27, όπου υπάρχει το μήνυμα PSV.

2.31

105 Response: 227 Entering Passive Mode (147,102,40,15,59,218).

2.32 Από τη μεριά του πελάτη (υπολογιστή μου).

2.33 Χρησιμοποιείται η θύρα 15322 και αυτό προκύπτει με παρόμοιο τρόπο όπως στο 2.19 από την πράξη 256*59 + 218.

2.34 Βρισκόμαστε σε passive mode κι έτσι ο client ανοίγει το ftp data σε θύρα με αριθμό που προκύπτει εάν προσθέσει +1 στον αριθμό της θύρας που χρησιμοποιεί ο server.

2.35 Στάλθηκαν 2 μηνύματα δεδομένων από τον εξυπηρετητή και το μέγεθος των δεδομένων για το πρώτο ισούται με length IPV4 – header IPV4 – header TCP = 576 – 20 – 20 = 536 bytes και το μέγεθος του δεύτερου ισούται ομοίως με 530-20-20 = 490 bytes

2.36 Το πρώτο πακέτο έχει μήκος όσο το μέγεθος της MTU.

2.37 Η απόλυση συνδέσεων που αφορούν τις εντολές ελέγχου γίνεται από τη μεριά του εξυπηρετητής.

2.38 Η απόλυση συνδέσεων που αφορούν τα μηνύματα δεδομένων γίνεται από τη μεριά του εξυπηρετητή.

Μέρος 3

3.1 UDP

3.2
```
Source Port: 53800
Destination Port: 69
```

3.3
```
Source Port: 31908
Destination Port: 53800
```

3.4 Η θύρα 69 αντιστοιχεί στο πρωτόκολλο TFTP.

3.5 Θύρες που χρησιμοποιούνται για τη μεταφορά δεδομένων σύμφωνα με το RFC 1350:

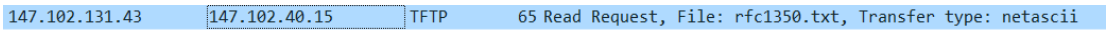
- Για το πρώτο Read Request η source port είναι το TID του υπολογιστή μου(53800) και το destination port η 69.
- Ο server απαντά με source port το TID του και destination port το TID του υπολογιστή μου.

Σε αυτό το σημείο πραγματοποιείται η σύνδεση και ο υπολογιστής μου μπορεί να στείλει το πρώτο πακέτο δεδομένων.

- Στη συνέχεια η επικοινωνία γίνεται με θύρες τα αντίστοιχα TIDs του server και client.

3.6 Η μεταφορά γίνεται σε ascii mode. Transfer type: netascii

3.7 Καθορίζεται στο πρώτο TFTP μήνυμα που στέλνει ο πελάτης στον server ως εξής:



3.8 Τύποι TFTP: Read Request, Data Packet, Acknowledgement.

3.9 Το TFTP αντιμετωπίζει το πρόβλημα της επιβεβαίωσης του UDP, πραγματοποιώντας σε ανώτερο επίπεδο(Acknowledgement) την επιβεβαίωση.

3.10 Χρησιμοποιείται ο τύπος μηνύματος Acknowledgement και το πεδίο Opcode της επικεφαλίδας.

3.11 558 Bytes

3.12 Το μέγεθος των δεδομένων των πακέτων αυτών είναι 512 bytes.

3.13 Ο πελάτης αντιλαμβάνεται το τέλος της μετάδοσης δεδομένων με το TFTP Data Packet μεγέθους 175 bytes.