

## Εργαστηριακή Άσκηση 8

Θοδωρής Φρίξος Παπαρρηγόπουλος  
el18040  
Ομάδα 4η.  
Ipn6: 2a02:587:4f0e:2b65:34b0:9e4a:d912:2f8a  
MAC: 40-1C-83-38-F7-20  
Λειτουργικό: Windows  
DESKTOP-1403ER3

### Άσκηση 1

1.1) TCP

1.2)

192.168.1.9 → 147.102.40.15: Port 23

147.102.40.15 → 192.168.1.9: Port 52893

184	0.000000	192.168.1.9	147.102.40.15	TCP	66	52893 → 23	[SYN]
185	0.012107	147.102.40.15	192.168.1.9	TCP	66	23 → 52893	[SYN]

1.3) Η θύρα 23

1.4) telnet

1.5)

147.102.40.15 → 192.168.1.9: Do Echo

192.168.1.9 → 147.102.40.15: Will Echo

147.102.40.15 → 192.168.1.9: Don't Echo

147.102.40.15 → 192.168.1.9: Will Echo

192.168.1.9 → 147.102.40.15: Won't Echo

1.6) Ναι και ο υπολογιστής μου δέχεται να τους επαναλαμβάνει

1.7) Ναι, και ο υπολογιστής μου δέχεται να μην τους επαναλαμβάνει

1.8) Ναι, προτίθεται

1.9) Ναι έχει προηγηθεί

1.10) Ο εξυπηρετητής επαναλαμβάνει κάθε γράμμα που πληκτρολογώ

```
..%..%..%.....%.....&.... ..#..'..$..&..... ..#..'..$.....'.....x.
+....'.....ANSI.....".....!.....".....!.....
.
FreeBSD/amd64 (edu-dy.cn.ntua.gr) (pts/0)
.
login: ...aabbccdd

Password for abcd@edu-dy.cn.ntua.gr:efgh

Login incorrect
login:
```

1.11) Το φαινόμενο είναι λογικό καθώς ο edu-dy.cn.ntua.gr προτίθεται να επαναλαμβάνει τους χαρακτήρες που λαμβάνει από τον υπολογιστή μου

1.12) telnet and ip.src == 192.168.1.9

1.13) Χρειάζονται 4 πακέτα για τα γράμματα (1 για κάθε γραμμα/χαρακτήρα που πληκτρολογώ) και 1 για το ENTER (την αλλαγή γραμμής \r\n). Δηλαδή συνολικά 5 πακέτα

1.14) Ομοίως χρειάζονται 5 πακέτα, 1 για κάθε χαρακτήρα και 1 για την αλλαγή γραμμής

1.15) Το φίλτρο: telnet and ip.src == 147.102.40.9

1.16) Όχι

1.17) Το Telnet, για λόγους ασφαλείας δεν επαναλαμβάνει τον κωδικό του χρήστη

1.18) Η ασφάλεια που παρέχει η υπηρεσία Telnet είναι ανύπαρκτη, καθώς οποιοσδήποτε μπορεί να παρακολουθήσει την συνομιλία των συσκευών καθώς και να υποκλέψει ευαίσθητα στοιχεία

## Άσκηση 2

2.1) host 147.102.40.15

2.2) Σημαίνει ότι είναι σε debug mode

2.3) TCP

2.4)

Για τις εντολές ελέγχου:

Source Port: 58354

Destination Port: 21

Για τη μεταφορά δεδομένων:

Source Port: 58383

Destination Port: 20

2.5) Από την πλευρά του εξυπηρετητή

2.6)

OPTS UTF8 ON, USER anonymous, PASS labuser@cn, HELP, PORT 147,102,131,110,239,132, NLST, QUIT

ftp.request==1						
No.	Time	Source	Destination	Protocol	Length	Info
5	0.000000	147.102.131.48	147.102.40.15	FTP	68	Request: OPTS UTF8 ON
8	4.624187	147.102.131.48	147.102.40.15	FTP	70	Request: USER anonymous
11	7.265401	147.102.131.48	147.102.40.15	FTP	71	Request: PASS labuser@cn
14	4.679123	147.102.131.48	147.102.40.15	FTP	60	Request: HELP
29	3.969704	147.102.131.48	147.102.40.15	FTP	82	Request: PORT 147,102,131,48,228,15
31	0.020058	147.102.131.48	147.102.40.15	FTP	60	Request: NLST
43	3.313365	147.102.131.48	147.102.40.15	FTP	60	Request: QUIT

2.7)

192.168.1.1

```
PS C:\Users\papar>
PS C:\Users\papar> ftp -d edu-dy.cn.ntua.gr
Connected to edu-dy.cn.ece.ntua.gr.
220 ProFTPD 1.3.4a Server (ProFTPD Default Installation) [147.102.40.15]
---> OPTS UTF8 ON
200 UTF8 set to on
User (edu-dy.cn.ece.ntua.gr:(none)): anonymous
---> USER anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
---> PASS labuser@cn
230 Anonymous access granted, restrictions apply
ftp> help
Commands may be abbreviated.  Commands are:

!           delete          literal          prompt          send
?           debug           ls              put             status
append      dir                  mdelete        pwd            trace
ascii       disconnect        mdir           quit           type
bell        get                  mget           quote          user
binary      glob                mkdir          recv           verbose
bye         hash                mls            remotehelp
cd          help                mput           rename
close       lcd                open           rmdir

ftp> remotehelp
---> HELP
214-The following commands are recognized (* =>'s unimplemented):
214-CWD      XCWD      CDUP      XCUP      SMNT*    QUIT      PORT      PASV
214-EPRT     EPSV      ALLO*     RNFR      RNT0     DELE      MDTM      RMD
214-XRMD     MKD        XMKD      PWD       XPWD     SIZE      SYST      HELP
214-NOOP     FEAT       OPTS      AUTH*     CCC*     CONF*     ENC*      MIC*
214-PBSZ*    PROT*     TYPE      STRU      MODE     RETR      STOR      STOU
214-APPE     REST      ABOR      USER     PASS     ACCT*     REIN*     LIST
214-NLST     STAT      SITE      MLSD      MLST
214 Direct comments to root@edu-dy.cn.ece.ntua.gr
ftp> ls
---> PORT 147,102,131,48,228,15
200 PORT command successful
---> NLST
150 Opening ASCII mode data connection for file list
FreeBSD10.4.ova
PCATTCP.exe
lab6.cap
router.ova
FreeBSD.ova
firewall.ova
MagicAdb.exe
Asterisk.ova
TDIQ.exe
MacAddr2.exe
putty.exe
FreeBSD11.3.ova
psftp.exe
pcattcp.pcap
icmpv6.pcap
226 Transfer complete
ftp: 200 bytes received in 0.01Seconds 16.67Kbytes/sec.
ftp> bye
---> QUIT
221 Goodbye.
PS C:\Users\papar>
```

2.8) Με την εντολή USER

- 2.9) Ένα  
 2.10) Με την εντολή PASS  
 2.11) Ένα  
 2.12) Η ομοιότητα τους είναι ότι κανένα από τα δύο δεν χρησιμοποιεί κρυπτογράφηση. Και μια διαφορά τους, είναι ότι με το telnet στέλνεται κάθε χαρακτήρας ξεχωριστά ενώ στο FTP πάνε όλοι μαζί (σε ένα πακέτο)  
 2.13) Όχι  
 2.14) PROT και AUTH  
 2.15) Από τον υπολογιστή μου στάλθηκε ένα, από τον εξυπηρετητή στάλθηκαν 9 πακέτα  
 2.16) Το δηλώνει με το να μη βάλει "-" (Hyphen) στην αρχή της γραμμής  
 2.17) Την IPv4 διεύθυνση του υπολογιστή μου  
 2.18) Προκύπτει αν πολλαπλασιάσουμε το 50 byte με το  $2^8=256$  και προσθέσουμε στο αποτέλεσμα το 60  
 2.19) Η εντολή LIST  
 2.20) Αυτό συμβαίνει επειδή γίνεται σύναψη νέας σύνδεσης (τριμερής χειραψίας με την θύρα δεδομένων)  
 2.21) Στην εντολή QUIT  
 2.22) Με το μήνυμα "221 Goodbye."  
 2.23) `tcp.flags.fin == 1`  
 2.24) Η απόλυση των συνδέσεων έγινε από την πλευρά του πελάτη, τόσο για τις εντολές ελέγχου όσο και για τα μηνύματα δεδομένων  
 2.25) assigned IP: 147.102.131.48

Για τις εντολές ελέγχου:

Θύρα πηγής: 52250

Θύρα προορισμού: 21

Για τη μεταφορά δεδομένων:

Θύρα πηγής: 52382

Θύρα προορισμού: 45230

2.26)

ftp.request==1						
No.	Time	Source	Destination	Protocol	Length	Info
6	0.000000	147.102.131.48	147.102.40.15	FTP	70	Request: USER anonymous
9	0.143006	147.102.131.48	147.102.40.15	FTP	69	Request: PASS password
12	0.131904	147.102.131.48	147.102.40.15	FTP	68	Request: opts utf8 on
15	0.124127	147.102.131.48	147.102.40.15	FTP	60	Request: syst
18	0.130503	147.102.131.48	147.102.40.15	FTP	65	Request: site help
29	0.141942	147.102.131.48	147.102.40.15	FTP	59	Request: PWD
32	0.028253	147.102.131.48	147.102.40.15	FTP	62	Request: TYPE A
35	0.041185	147.102.131.48	147.102.40.15	FTP	60	Request: PASV
41	0.234754	147.102.131.48	147.102.40.15	FTP	60	Request: LIST

2.27) anonymous για username και password ως κωδικό

2.28) LIST

2.29)

ftp						
No.	Time	Source	Destination	Protocol	Length	Info
4	0.000000	147.102.40.15	147.102.131.48	FTP	128	Response: 220 ProFTPD 1.3.4a Server (ProFTPD Default Installation) [147.102.40.15]
6	0.000146	147.102.131.48	147.102.40.15	FTP	70	Request: USER anonymous
7	0.142686	147.102.40.15	147.102.131.48	FTP	129	Response: 331 Anonymous login ok, send your complete email address as your password
9	0.000320	147.102.131.48	147.102.40.15	FTP	69	Request: PASS password
10	0.131567	147.102.40.15	147.102.131.48	FTP	104	Response: 230 Anonymous access granted, restrictions apply
12	0.000337	147.102.131.48	147.102.40.15	FTP	68	Request: opts utf8 on
13	0.123803	147.102.40.15	147.102.131.48	FTP	74	Response: 200 UTF8 set to on
15	0.000324	147.102.131.48	147.102.40.15	FTP	60	Request: syst
16	0.130162	147.102.40.15	147.102.131.48	FTP	73	Response: 215 UNIX Type: L8
18	0.000341	147.102.131.48	147.102.40.15	FTP	65	Request: site help
19	0.128828	147.102.40.15	147.102.131.48	FTP	125	Response: 214-The following SITE commands are recognized (* =>'s unimplemented)
21	0.012561	147.102.40.15	147.102.131.48	FTP	64	Response: 214-HELP
23	0.000144	147.102.40.15	147.102.131.48	FTP	65	Response: 214-CHGRP
25	0.000075	147.102.40.15	147.102.131.48	FTP	65	Response: 214-CHMOD
27	0.000069	147.102.40.15	147.102.131.48	FTP	105	Response: 214 Direct comments to root@edu-dy.cn.ece.ntua.gr
29	0.000265	147.102.131.48	147.102.40.15	FTP	59	Request: PWD
30	0.027888	147.102.40.15	147.102.131.48	FTP	88	Response: 257 "/" is the current directory
32	0.000365	147.102.131.48	147.102.40.15	FTP	62	Request: TYPE A
33	0.040720	147.102.40.15	147.102.131.48	FTP	73	Response: 200 Type set to A
35	0.000465	147.102.131.48	147.102.40.15	FTP	60	Request: PASV
36	0.127084	147.102.40.15	147.102.131.48	FTP	106	Response: 227 Entering Passive Mode (147,102,40,15,248,234).
41	0.107670	147.102.131.48	147.102.40.15	FTP	60	Request: LIST
42	0.123497	147.102.40.15	147.102.131.48	FTP	108	Response: 150 Opening ASCII mode data connection for file list
50	0.193444	147.102.40.15	147.102.131.48	FTP	77	Response: 226 Transfer complete

2.30) Από τον υπολογιστή μου (από την πλευρά του πελάτη)

2.31) 52839

2.32) Είναι απλά η πρώτη διαθέσιμη θύρα (προκύπτει τυχαία)

2.33) Στάλθηκαν 2 μηνύματα από 590 και 544 bytes αντίστοιχα

ftp-data						
No.	ftp-data	Source	Destination	Protocol	Length	Info
44	0.000000	147.102.40.15	147.102.131.48	FTP-DA...	590	FTP Data: 536 bytes (PASV) (LIST)
46	0.000049	147.102.40.15	147.102.131.48	FTP-DA...	544	FTP Data: 490 bytes (PASV) (LIST)

2.34) Περιέχει ονομαστικά τα περιεχόμενα του καταλόγου του ανταποκρινόμενου υπολογιστή

2.35) Από την πλευρά του εξυπηρετητή

2.36) Από την πλευρά του πελάτη

### Άσκηση 3

3.1) UDP

3.2)

Source Port: 61361

Destination Port: 69

3.3)

Source Port: 12712

Destination Port: 61361

3.4) 69

3.5) Είναι οι πρώτες διαθέσιμες θύρες (η θύρα προορισμού είναι η θύρα με την οποία επικοινωνήσε αρχικά ο υπολογιστής μου)

3.6) Με ASCII

3.7) Στο πρώτο μήνυμα που στέλνει ο πελάτης στον εξυπηρετητή και κάνει το request (καθορίζεται στο πεδίο Type με τιμή netascii)

3.8) Read Request, Data Packet και Acknowledgement

3.9) Χωρίζει τα πακέτα με ένα αριθμό Block και για κάθε ένα που στέλνει ο εξυπηρετητής, ο πελάτης απαντά με ένα πακέτο τύπου Acknowledgement με το αντίστοιχο αριθμό Block

3.10) Ο τύπος Acknowledgement στο πεδίο επικεφαλίδας Opcode

3.11) Ολόκληρο το μήνυμα TFTP έχει μέγεθος 516 bytes (512bytes των Data συν 4 της επικεφαλίδας)

3.12) 512 bytes

3.13) Ο πελάτης το αντιλαμβάνεται με το που λάβει πακέτο TFTP που έχει λιγότερα από 512 bytes δεδομένων, και διπλα από τον αριθμό του Block γράφει (Last)