Δίκτυα Υπολογιστών

Εργαστηριακή Άσκηση 8
TELNET, FTP και TFTP

Ονοματεπώνυμο: Νικόλαος Παγώνας, el18175	**Ομάδα:** 4 (Τρίτη εξ' αποστάσεως)
Όνομα PC/ΛΣ: nick-ubuntu/Ubuntu 20.04.3 LTS	**Ημερομηνία:** Τρίτη 07/11/2021
Διεύθυνση IP: `192.168.1.15`	**Διεύθυνση MAC:** `3c:2c:30:e1:1c:55`

1. TELNET

1.1

Το TELNET χρησιμοποιεί το πρωτόκολλο TCP.

1.2

Οι θύρες του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την επικοινωνία είναι οι 23 και 38212.

1.3

Στο πρωτόκολλο TELNET αντιστοιχεί η θύρα 23.

1.4

Η σύνταξη του φίλτρου απεικόνισης είναι `telnet`.

1.5

- 147.102.40.15 → 192.168.1.15: Do Echo
- 192.168.1.15 → 147.102.40.15: Won't Echo
- 147.102.40.15 → 192.168.1.15: Will Echo
- 192.168.1.15 → 147.102.40.15: Do Echo

1.6

Ναι, ο edu-dy.cn.ntua.gr ζητάει από τον υπολογιστή μας να επαναλαμβάνει τους χαρακτήρες που λαμβάνει (Do Echo), αλλά ο υπολογιστής μας δεν δέχεται (Won't Echo).

1.7

Όχι, ο edu-dy.cn.ntua.gr δεν ζητάει από τον υπολογιστή μας να μην επαναλαμβάνει τους χαρακτήρες που λαμβάνει.

1.8

Ναι, ο edu-dy.cn.ntua.gr προτίθεται να επαναλαμβάνει τους χαρακτήρες που λαμβάνει (Will Echo).

1.9

Ναι, έχει προηγηθεί (Do Echo).

1.10

Κατά τη μεταφορά του ονόματος χρήστη, βλέπουμε ότι για κάθε χαρακτήρα που πληκτρολογούμε (και άρα στέλνουμε στον edu-dy.cn.ntua.gr), ο edu-dy.cn.ntua.gr μας απαντά αμέσως πίσω με τον ίδιο χαρακτήρα.

1.11

Το παραπάνω γίνεται διότι ο edu-dy.cn.ntua.gr έχει κάνει Will Echo και ο υπολογιστής μας έχει κάνει Do Echo, δηλαδή έχει γίνει η συμφωνία ότι ο edu-dy.cn.ntua.gr θα επαναλαμβάνει τους χαρακτήρες που λαμβάνει.

1.12

Η σύνταξη του φίλτρου είναι:
`ip.version == 4 && telnet && ip.src == 192.168.1.15 && ip.dst == 147.102.40.15`.

1.13

Χρειάζονται 5 πακέτα, ένα για κάθε χαρακτήρα του "abcd" και ένα για το <Enter> (\r)

1.14

Και πάλι χρειάζονται 5 πακέτα, ένα για κάθε χαρακτήρα του "efgh" και ένα για το <Enter> (\r)

1.15

Όχι, δεν την στέλνει.

1.16

Όχι, δεν την παρατηρήσαμε.

1.17

Ο κωδικός δεν εμφανίζεται για λόγους ασφαλείας.

1.18

Η υπηρεσία Telnet δεν είναι ασφαλής, αφού η πληροφορία στέλνεται χωρίς καμία κρυπτογράφηση, και όποιος παρακολουθεί την κίνηση πακέτων μεταξύ των δύο πλευρών μπορεί να υποκλέψει προσωπικά δεδομένα, όπως κάναμε μόλις με το username μέσω του Wireshark.

2. FTP

2.1

Το φίλτρο σύλληψης που χρησιμοποιήσαμε είναι `host edu-dy.cn.ntua.gr`

2.2

Το option `-d` σημαίνει ότι έχουμε κάνει enable το debugging.

2.3

Το FTP χρησιμοποιεί το TCP σαν πρωτόκολλο μεταφοράς.

2.4

- Εντολές ελέγχου: Θύρες 21 και 53396.
- Εντολές μεταφοράς δεδομένων: Θύρες 20 και 47745.

2.5

Η σύνδεση TCP για τη μεταφορά δεδομένων FTP γίνεται από την πλευρά του εξυπηρετητή.

2.6

Ο πελάτης έστειλε τις εντολές:

- USER anonymous
- PASS labuser@cn

- SYST
- HELP
- PORT 147, 102, 131, 25, 186, 129
- LIST
- QUIT

2.7

Οι εντολές αυτές εμφανίζονται αυτούσιες στο παράθυρο εντολών ως εξής:

- - - - > USER anonymous
- - - - > PASS XXXX (εδώ δεν εμφανίζεται το labuser@cn)
- - - - > SYST
- - - - > HELP
- - - - > PORT 147, 102, 131, 25, 186, 129
- - - - > LIST
- - - - > QUIT

2.8

Το όνομα χρήστη μεταφέρεται με την εντολή USER.

2.9

Για να μεταφερθεί το όνομα χρήστη χρειάζεται ένα πακέτο.

2.10

Ο κωδικός χρήστη μεταφέρεται με την εντολή PASS.

2.11

Για να μεταφερθεί ο κωδικός χρήστη χρειάζεται ένα πακέτο.

2.12

Παρατηρούμε ότι το όνομα και ο κωδικός χρήστη μεταφέρονται χωρίς κρυπτογράφηση και στο FTP. Αντίθετα με το TELNET όμως, η πληροφορία στο FTP δεν μεταφέρεται χαρακτήρα-χαρακτήρα, αλλά το όνομα χρήστη μεταφέρεται σαν ολόκληρη συμβολοσειρά σε ένα μόνο πακέτο (το ίδιο ισχύει και για τον κωδικό χρήστη).

2.13

Όχι, η εντολή `help` δεν μεταφράζεται σε εντολή του πρωτοκόλλου FTP.

2.14

Δύο εντολές που δεν υποστηρίζονται από τον εξυπηρετητή είναι η `PBSZ` και η `PROT`. Αυτό φαίνεται επειδή είναι επισημασμένες με αστεράκι.

2.15

Από τον υπολογιστή μας στάλθηκε 1 πακέτο, ενώ από τον εξυπηρετητή στάλθηκαν 9 πακέτα.

2.16

Ο εξυπηρετητής δηλώνει ότι τελείωσε η αποστολή με το να βάλει στην τελευταία γραμμή τον κωδικό απάντησης ακολουθούμενο από ένα κενό διάστημα (και όχι παύλα).

2.17

Οι πρώτοι 4 δεκαδικοί αριθμοί παριστάνουν την IPv4 διεύθυνση του υπολογιστή μας.

2.18

Η θύρα αυτή προκύπτει ως εξής:

$$\text{Θύρα} = \text{5ος δεκαδικός αριθμός εντολής PORT} * 256 + \text{6ος δεκαδικός αριθμός εντολής PORT}.$$

Επιβεβαιώνουμε ότι με αυτόν τον τρόπο η θύρα που προκύπτει είναι αυτή που βρήκαμε προηγουμένως στο ερώτημα 2.4, δηλαδή η 47745.

2.19

Η εντολή LIST.

2.20

Η εντολή PORT προηγείται της LIST διότι πρόκειται να γίνει νέα τριπλή χειραψία για την μετάδοση των δεδομένων.

2.21

Η εντολή bye μεταφράζεται στην εντολή QUIT.

2.22

Ο εξυπηρετητής FTP ανταποκρίνεται με το μήνυμα ”221 Goodbye.”

2.23

Η σύνταξη του φίλτρου είναι `tcp.flags.fin == 1`.

2.24

Η απόλυση των συνδέσεων ελέγχου και δεδομένων έγινε από την πλευρά του πελάτη.

2.25

- Εντολές ελέγχου: Θύρες 21, 53974
- Εντολές μεταφοράς δεδομένων: Θύρες 33832, 47957

2.26

Οι εντολές είναι οι εξής:

- FEAT
- USER anonymous
- PASS gvfsd-ftp-1.44.1@example.com
- TYPE I
- OPTS UTF8-ON
- SYST
- SITE HELP
- PWD
- CWD /
- PASV
- LIST -a

2.27

Στην δική μας περίπτωση χρησιμοποιήθηκε ως όνομα χρήστη το `anonymous`, ενώ ως κωδικός χρήστη το `gvfsd-ftp-1.44.1@example.com`.

2.28

Για την εμφάνιση της λίστας αρχείων χρησιμοποιήθηκε η εντολή `LIST -a`.

2.29

Ο εξυπηρετητής ανταποκρίνεται με το μήνυμα:
`227 Entering Passive Mode (147,102,40,15,187,85).`

2.30

Η εγκατάσταση της σύνδεσης TCP γίνεται από την πλευρά του υπολογιστή μου.

2.31

Η θύρα του εξυπηρετητή που χρησιμοποιείται για τη μεταφορά δεδομένων FTP είναι η 47957. Αυτός ο αριθμός μπορεί να προκύψει και μέσω της εντολής PORT ως εξής:

Θύρα = 5ος δεκαδικός αριθμός εντολής PORT $*$ 256 + 6ος δεκαδικός αριθμός εντολής PORT.

2.32

Η θύρα από την πλευρά του πελάτη είναι η πρώτη διαθέσιμη.

2.33

Στάλθηκαν 4 μηνύματα από τον εξυπηρετητή, με μέγεθος δεδομένων 524, 524, 524 και 155 bytes αντίστοιχα.

2.34

Τα περιεχόμενα του καταλόγου έχουν θρυμματιστεί, γι' αυτό έχουμε 3 πακέτα μήκους ακριβώς 576 bytes και ένα 155.

2.35

Η απόλυση της σύνδεσης που αφορά τις εντολές ελέγχου γίνεται από τον εξυπηρετητή.

2.36

Η απόλυση της σύνδεσης που αφορά τα μηνύματα δεδομένων γίνεται από τον πελάτη.

3. TFTP

3.1

Το TFTP χρησιμοποιεί το πρωτόκολλο μεταφοράς UDP.

3.2

- Θύρα πηγής: 34175
- Θύρα προορισμού: 69

3.3

- Θύρα πηγής (εξυπηρετητής): 16799
- Θύρα προορισμού (πελάτης): 34175

3.4

Στο TFTP αντιστοιχεί η θύρα 69.

3.5

Οι αριθμοί θυρών που χρησιμοποιούνται κατά την μεταφορά δεδομένων επιλέγονται τυχαία.

3.6

Η μεταφορά του αρχείου rfc1350.txt γίνεται με ASCII.

3.7

Ο τρόπος μεταφοράς καθορίζεται από το πρώτο μήνυμα που στέλνει ο πελάτης, μέσω του πεδίου Type του TFTP, το οποίο έχει την τιμή `netascii`.

3.8

Οι τύποι μηνυμάτων που παρατηρήσαμε είναι:

- Read Request
- Data Packet
- Acknowledgment

3.9

Στο TFTP ο πελάτης στέλνει μηνύματα επιβεβαίωσης (Acknowledgment) όπου αναγράφεται το block δεδομένων που λήφθηκε με επιτυχία.

3.10

Γι' αυτόν τον σκοπό χρησιμοποιείται ο τύπος μηνυμάτων Acknowledgment, του πεδίου Opcode.

3.11

Το μέγεθος των μηνυμάτων TFTP (πλην του τελευταίου) είναι 516 bytes.

3.12

Το μέγεθος δεδομένων είναι 512 bytes.

3.13

Ο πελάτης αντιλαμβάνεται το τέλος της μετάδοσης δεδομένων αν λάβει ένα μήνυμα με μέγεθος δεδομένων μικρότερο από 512 bytes.