Ονοματεπώνυμο: Χρήστος Τσούφης		**Ομάδα:** 2
Όνομα PC/ΛΣ: DESKTOP-EUMLCMA/Windows 10		**Ημερομηνία:** 1/12/2020
Διεύθυνση IP: 192.168.1.3	**Διεύθυνση MAC:**	34-F6-4B-07-39-B5

Εργαστηριακή Άσκηση 8
TELNET, FTP και TFTP

1

1.1 Το TELNET χρησιμοποιεί το `TCP` Protocol μεταφοράς.

1.2 Οι θύρες του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την επικοινωνία είναι:

- `Port 23` & `Host: 147.102.40.15`
- `Port 59079` & `Host: 192.168.1.3`

1.3 Από τις θύρες του 1.2, η `Port 23` αντιστοιχεί στο πρωτόκολλο εφαρμογής TELNET.

1.4 Η σύνταξη του φίλτρου απεικόνισης είναι: `telnet` .

1.5 Οι εντολές TELNET τύπου echo και ο αποστολέας τους είναι:

- edu-dy.cn.ntua.gr *sends* `"Do Echo" (Command: Do (253))`
- PC *sends* `"Will Echo" (Command: Will (251))`
- edu-dy.cn.ntua.gr *sends* `"Don't Echo" (Command: Don't (254))` & `"Will Echo" (Command: Will (251))`
- PC *sends* `"Won't Echo" (Command: Won't (252))`

1.6 Ο edu-dy.cn.ntua.gr ζητά από τον υπολογιστή να επαναλαμβάνει (echo) τους χαρακτήρες που λαμβάνει με την εντολή `"Do Echo"` και το PC δέχεται με την εντολή `"Will Echo"`.

1.7 Ο edu-dy.cn.ntua.gr ζητά από τον υπολογιστή να μην επαναλαμβάνει (echo) τους χαρακτήρες που λαμβάνει με την εντολή `"Don't Echo"` και το PC δέχεται με την εντολή `"Won't Echo"`.

1.8 Ο edu-dy.cn.ntua.gr προτίθεται να επαναλαμβάνει τους χαρακτήρες που λαμβάνει από τον υπολογιστή με την εντολή `"Will Echo"`.

1.9 Δεν έχει προηγηθεί του μηνύματος αυτού εντολή TELNET με την οποία ο υπολογιστής ζητά την επανάληψη των χαρακτήρων από τον edu-dy.cn.ntua.gr . Αντιθέτως, ο εξυπηρετητής "αυτοβούλως" στέλνει με την εντολή `"Will Echo"`.

1.10 Κατά την μεταφορά του ονόματος χρήστη που στάλθηκε μετά την πρώτη προτροπή login αυτό που συνέβη είναι ότι επανέλαβε ένα προς ένα τα γράμματα του ονόματος χρήστη.

1.11 Το φαινόμενο που παρατηρείται στο ερώτημα 1.10 είναι ότι ο εξυπηρετητής είχε στείλει με την εντολή `"Will Echo"` και με αυτόν τον τρόπο επανέλαβε τα γράμματα που δέχτηκε.

1.12 Κλείνοντας το παράθυρο Follow TCP Stream και εφαρμόζοντας φίλτρο απεικόνισης, εντοπίζονται τα πακέτα IPv4 που μεταφέρουν μηνύματα TELNET από τον υπολογιστή προς τον εξυπηρετητή. Η σύνταξή του είναι: `ip.src == 192.168.1.3 && telnet` .

1.13 Χρειάζονται 5 (πέντε) πακέτα IPv4 για να μεταφερθεί η πληροφορία για το όνομα (abcd) του χρήστη. Συγκεκριμένα, χρειάζεται 1 (ένα) για κάθε γράμμα και 1 (ένα) για την αλλαγή γραμμής.

1.14 Χρειάζονται 5 (πέντε) πακέτα IPv4 για να μεταφερθεί η πληροφορία για το κωδικό (efgh) του χρήστη. Συγκεκριμένα, χρειάζεται 1 (ένα) για κάθε γράμμα και 1 (ένα) για την αλλαγή γραμμής.

1.15 Ο εξυπηρετητής δεν στέλνει την ηχώ των χαρακτήρων efgh του κωδικού χρήστη προς τον πελάτη.

1.16 Δεν παρατηρήθηκε εντολή TELNET "Don't Echo" πριν την μεταφορά του κωδικού.

1.17 Ο κωδικός δεν εμφανίζεται στην οθόνη ο κωδικός διότι ο εξυπηρετητής γνωρίζει ότι πρόκειται για password και δεν στέλνει echo.

1.18 Όσον αφορά την ασφάλεια της υπηρεσίας TELNET, δεν είναι πολύ αξιόπιστη διότι τα δεδομένα αποστέλλονται σε plain text χωρίς κρυπτογράφηση.

2

2.1 Η σύνταξη του φίλτρου σύλληψης είναι: `host 147.102.40.15`.

2.2 Το – d στην γραμμή εντολής σημαίνει ότι γίνεται `enable debugging`.

2.3 Το FTP χρησιμοποιεί το `TCP` Protocol μεταφοράς.

2.4 Οι θύρες πηγής & προορισμού που χρησιμοποιούνται για την επικοινωνία FTP τόσο για τις εντολές ελέγχου όσο και για τη μεταφορά δεδομένων είναι:

- Για έλεγχο: `Port 55277 (στο PC)` & `Port 21 (στο host 147.102.40.15)`.
- Για δεδομένα: `Port 55287 (στο PC)` & `Port 20 (στο host 147.102.40.15)`.

2.5 Η σύνδεση TCP γίνεται από την πλευρά του πελάτη για την μεταφορά των δεδομένων FTP.

2.6 Η εντολή φλοιού ftp υλοποιεί τον ενεργό τρόπο λειτουργίας του FTP Protocol εφόσον χρησιμοποιεί την `Port 20`.

2.7 Οι εντολές FTP που έστειλε ο πελάτης στον εξυπηρετητή είναι:

```
Request: OPTS UTF8 ON
Request: USER anonymous
Request: PASS labuser@cn
Request: HELP
Request: PORT 147,102,131,149,215,247
Request: NLST
Request: QUIT
```

2.8 Αυτές οι εντολές FTP εμφανίζονται στις πληροφορίες αποσφαλμάτωσης (debugging) στην οθόνη του προγράμματος φλοιού ftp. Αυτό συμβαίνει με --->.

2.9 Η εντολή του FTP Protocol με την οποία μεταφέρεται το όνομα χρήστη είναι:

`Request command: USER`.

2.10 Για να μεταφερθεί το όνομα χρήστη χρειάζεται 1 (ένα) πακέτο.

2.11 Η εντολή του FTP Protocol με την οποία μεταφέρεται ο κωδικός χρήστη είναι:

`Request command: PASS`.

2.12 Για να μεταφερθεί ο κωδικός χρήστη χρειάζονται 1 (ένα) πακέτο.

2.13 Τα FTP Protocol & TELNET Protocol μοιάζουν ως προς το γεγονός ότι αποστέλλουν plain text χωρίς κρυπτογράφηση, οπότε δεν θεωρούνται απολύτως ασφαλή. Όμως, διαφέρουν ως προς το γεγονός ότι το TELNET αποστέλλει ένα πακέτο ανά γράμμα ενώ το FTP μπορεί να αποστείλει ολόκληρο το username που δίνει ο χρήστης σε ένα IP πακέτο.

2.14 Η εντολή help του προγράμματος φλοιού ftp δεν μεταφράζεται σε εντολή του πρωτοκόλλου FTP. Η εντολή `Request command: HELP` είναι για remotehelp.

2.15 Με βάση τα αποτελέσματα από την εκτέλεση της εντολής remotehelp που πληκτρολογήθηκε στο παράθυρο της γραμμής εντολών, καταγράφηκαν οι εξής εντολές FTP που δεν υποστηρίζονται από τον εξυπηρετητή: `MIC & AUTH`.

2.16 Σχετικά με την εντολή remotehelp, στάλθηκε 1 (ένα) πακέτο με `Request command: HELP` από το PC και 9 (εννιά) πακέτα από τον εξυπηρετητή (ένα για κάθε γραμμή του παραθύρου εντολών).

2.17 Ο εξυπηρετητής δηλώνει ότι τελείωσε η αποστολή πακέτων σχετικών με την εντολή remotehelp με τον εξής τρόπο: η τελευταία γραμμή έχει τον ίδιο κωδικό με τις προηγούμενες αλλά αυτή τη φορά υπάρχει " " (κενό) και όχι "–" (παύλα) μετά το password.

2.18 Στην λίστα καταγεγραμμένων πακέτων εντοπίζεται το μήνυμα που μεταφέρει την εντολή PORT. Οι 4 πρώτοι δεκαδικοί αριθμοί παριστάνουν την IP Address του PC.

2.19 Αυτός ο αριθμός προκύπτει από τα δεδομένα της εντολής PORT ως εξής:

`215*256 + 247 = 55.287.`

2.20 Τα περιεχόμενα του τρέχοντος καταλόγου εμφανίζονται με την εντολή:

`Request: NLST.`

2.21 Η εντολή PORT του FTP Protocol προηγείται της εντολής της ερώτησης 2.20 διότι με αυτήν την εντολή ο πελάτης ενημερώνει τον εξυπηρετητή που να συνδεθεί.

2.22 Η εντολή `bye` του προγράμματος φλοιού ftp μεταφράζεται στην εντολή:

`Request: QUIT.`

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

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

2.25 Η απόλυση των συνδέσεων TCP που αφορούν τις εντολές ελέγχου και τα μηνύματα δεδομένων του FTP γίνεται από την πλευρά του εξυπηρετητή.

2.26 Οι θύρες πηγής & προορισμού που χρησιμοποιούνται για την επικοινωνία FTP τόσο για εντολές ελέγχου όσο και για την μεταφορά δεδομένων είναι:

- Για έλεγχο: `Port 53124 (στο PC)` & `Port 21 (στο host 147.102.40.15).`
- Για δεδομένα: `Port 53127 (στο PC)` & `Port 57023 (στο host 147.102.40.15).`

2.27 Οι εντολές FTP που έστειλε ο πελάτης στον εξυπηρετητή είναι:

```
Request: USER anonymous
Request: PASS chrome@example.com
Request: SYST
Request: PWD
Request: TYPE I
Request: SIZE /
Request: CWD /
Request: PASV
Request: LIST -l
Request: QUIT
```

2.28 Η σύνδεση μέσω της διεύθυνσης ftp://user:password@edu-dy.cn.ntua.gr οδήγησε στην χρήση:

`anonymous` ως όνομα χρήστη & `chrome@example.com` ως κωδικός χρήστη.

2.29 Ο πλοηγός χρησιμοποίησε για την εμφάνιση της λίστας αρχείων την εντολή:

`Request: LIST -l`.

2.30 Ο πλοηγός υλοποιεί το παθητικό τρόπο λειτουργίας. Αυτό συμβαίνει διότι δεν χρησιμοποιεί την Port 20 αλλά και λόγω της ύπαρξης της PASV.

2.31 Ο εξυπηρετητής αποκρίνεται στην εντολή PASV με το μήνυμα:

`227 Entering Passive Mode (147,102,40,15,222,191).`

2.32 Η εγκατάσταση της σύνδεσης TCP γίνεται από την πλευρά του πελάτη.

2.33 Χρησιμοποιείται η θύρα Port 57.023. Ο αριθμός της προκύπτει από τα στοιχεία της απάντησης που καταγράφηκε στο ερώτημα 2.31 ως εξής:

`222*256 + 191 = 57023`.

2.34 Ο αριθμός θύρας της σύνδεσης TCP για την μεταφορά δεδομένων FTP στην πλευρά του πελάτη προκύπτει από τον της θύρας για τον έλεγχο προσθέτοντας 3 (τρία) καθώς αυτός ήταν ο επόμενος διαθέσιμος αριθμός.

2.35 Στάλθηκαν 2 (δύο) μηνύματα δεδομένων FTP από τον εξυπηρετητή. Το μέγεθος των δεδομένων που μεταφέρουν είναι:

`590 bytes` & `544 bytes`.

2.36 Το μέγεθος του πρώτου διαφέρει από τα προηγούμενα μηνύματα δεδομένων FTP διότι:

`Ethernet Header (14 bytes) + MTU (576 Bytes) = 590 bytes`

Όπου

`MTU (576 Bytes) = MSS (536 bytes) + IPv4 Header Length (20 bytes) + TCP Header Length (20 bytes)`

2.37 Η απόλυση των συνδέσεων TCP που αφορούν τις εντολές ελέγχου FTP γίνεται από την πλευρά του εξυπηρετητή.

2.38 Η απόλυση της σύνδεσης TCP που αφορά τα μηνύματα δεδομένων FTP γίνεται από την πλευρά του εξυπηρετητή.

3

3.1 Το TFTP χρησιμοποιεί το `UDP` Protocol.

3.2 Οι θύρες πηγής & προορισμού του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την πρώτη επικοινωνία του πελάτη με τον εξυπηρετητή TFTP είναι:

`Source Port: 54456` (του πελάτη) & `Destination Port: 69` (του εξυπηρετητή)

3.3 Οι θύρες πηγής & προορισμού του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται κατά την μεταφορά δεδομένων είναι:

`Source Port: 54456` (του πελάτη) & `Destination Port: 54200` (του εξυπηρετητή)

3.4 Η θύρα `Port 69` αντιστοιχεί στο πρωτόκολλο της εφαρμογής TFTP.

3.5 Οι αριθμοί θυρών που χρησιμοποιούνται κατά τη μεταφορά δεδομένων προκύπτουν με τυχαίο τρόπο ώστε η πιθανότητα να επιλεχθεί ο ίδιος αριθμός δύο διαδοχικές φορές να είναι μικρή.

3.6 Η μεταφορά του αρχείου *rfc1350.txt* γίνεται σε `ASCII`.

3.7 Αυτό καθορίζεται στο πρώτο μήνυμα TFTP με την τιμή του πεδίου Type: netascii στην επικεφαλίδα TFTP όταν αποστέλλεται από τον πελάτη στον εξυπηρετητή.

3.8 Οι τύποι μηνυμάτων TFTP που παρατηρήθηκαν είναι:

`Read Request, Data Packet` & `Acknowledgement`.

3.9 Το πρωτόκολλο μεταφοράς UDP είναι αναξιόπιστο. Αυτό αντιμετωπίζεται από το TFTP με τη χρήση μηνυμάτων `ack` στο ανώτερο επίπεδο.

3.10 Για τον σκοπό αυτό, χρησιμοποιείται ο τύπος μηνύματος `Acknowledgement(4)` και το πεδίο επικεφαλίδας `opcode`.

3.11 Το μέγεθος των μηνυμάτων TFTP (πλην του τελευταίου) που μεταφέρουν τα προς μετάδοση δεδομένα είναι:

`558 bytes`.

3.12 Το μέγεθος των δεδομένων που μεταφέρονται από αυτά τα μηνύματα TFTP είναι:

`512 bytes`.

3.13 Ο πελάτης αντιλαμβάνεται το τέλος της μετάδοσης δεδομένων καθώς το τελευταίο μήνυμα μετάδοσης δεδομένων περιέχει δεδομένα μήκους από 0 έως 511 data.