Δίκτυα Υπολογιστών
Εργαστηριακή Άσκηση 8

Ονοματεπώνυμο: Κυριακόπουλος Γεώργιος – el18153
Ομάδα: 4
Όνομα PC/ΛΣ: George – Windows 10 Pro, 21H1
Ημερομηνία: 13/12/2021
Διεύθυνση IP: 192.168.1.5
Διεύθυνση MAC: 60-A4-B7-75-72-0F

Άσκηση 1:

1.1.
Το TELNET χρησιμοποιεί το TCP πρωτόκολλο μεταφοράς.

1.2.
Από τη μεριά του υπολογιστή μου χρησιμοποιείται η θύρα 63886, ενώ από τη μεριά του εξυπηρετητή edu-dy.cn.ntua.gr χρησιμοποιείται η θύρα 23.

1.3.
Η θύρα 23 αποτελεί τη θύρα για το πρωτόκολλο εφαρμογής TELNET.

1.4.
Χρησιμοποίησα το φίλτρο απεικόνισης *telnet*.

1.5.
Οι εντολές τύπου echo που προηγούνται του πρώτου μηνύματος που μεταφέρει την προτροπή για login είναι: Do (253) Echo από 147.102.40.15, Will (251) Echo από τον υπολογιστή μου, Don’t (254) Echo από 147.102.40.15, Will (251) Echo από 147.102.40.15 και, τέλος, Won’t (252) Echo από τον υπολογιστή μου.

1.6.
Ναι, ο edu-dy.cn.ntua.gr ζητάει από τον υπολογιστή μου να επαναλαμβάνει τους χαρακτήρες που λαμβάνει (Do Echo) και παρότι αρχικά δέχεται ο υπολογιστής μου (Will Echo), βλέπουμε με την τελευταία εντολή πριν την προτροπή για το login ότι τελικά, αφότου ο edu-du.cn.ntua.gr ζητήσει να μην τους επαναλαμβάνει (Don’t Echo), ο υπολογιστής μου δέχεται να μην τους επαναλαμβάνει (Won’t Echo).

1.7.
Ναι, όπως ειπώθηκε και στο ερώτημα 1.6, ο edu-dy.cn.ntua.gr ζητάει από τον υπολογιστή μου να μην επαναλαμβάνει τους χαρακτήρες που λαμβάνει (Don't Echo) και ο υπολογιστής μου δέχεται να μην τους επαναλαμβάνει (Won't Echo).

1.8.
Ναι, με το Don't Echo που στέλνει στον υπολογιστή μου, στέλνει και ένα Will Echo μήνυμα, δηλαδή προτροπή για να επαναλαμβάνει τους χαρακτήρες που λαμβάνει από τον υπολογιστή μου.

1.9.
Ναι, ακριβώς πριν από το μήνυμα που μεταφέρει τον πρώτο χαρακτήρα "a" του ονόματος χρήστη προηγείται εντολή Do Echo από τον υπολογιστή μου προς τον edu-dy.cn.ntua.gr.

1.10.
Κατά τη μεταφορά του ονόματος χρήστη, παρατηρούμε ότι κάθε χαρακτήρας του ονόματος επαναλαμβάνεται από τον edu-dy.cn.ntua.gr.

1.11.
Ο edu-dy.cn.ntua.gr είχε δηλώσει προτροπή να επαναλαμβάνει τους χαρακτήρες που λαμβάνει από τον υπολογιστή μου (Will Echo). Επίσης, πριν την προτροπή για το login, ο υπολογιστής μου είχε ζητήσει και αυτός από τον edu-dy.cn.ntua.gr να επαναλαμβάνει τους χαρακτήρες που λαμβάνει (Do Echo), κάτι που συμβαδίζει με αυτά που βλέπουμε στο παράθυρο Follow TCP Stream.

1.12.
Χρησιμοποίησα το φίλτρο απεικόνισης *telnet and ip.src == 192.168.1.5 and ip.dst == 147.102.40.15.*

1.13.
Χρειάστηκαν 5 πακέτα IPv4 για να μεταφερθεί το όνομα (abcd) του χρήστη, ένα πακέτο IPv4 για κάθε χαρακτήρα (σύνολο 4) και ένα πακέτο για το New Line - Enter.

1.14.
Ομοίως, χρειάστηκαν 5 πακέτα IPv4 για να μεταφερθεί ο κωδικός (efgh) του χρήστη, ένα πακέτο IPv4 για κάθε χαρακτήρα (σύνολο 4) και ένα πακέτο για το New Line - Enter.

1.15.
Όχι, ο εξυπηρετητής δε στέλνει την ηχώ των χαρακτήρων efgh του κωδικού χρήστη προς τον πελάτη (τον υπολογιστή μου).

1.16.
Όχι, δεν υπήρξε καμία εντολή TELNET *Don't Echo* πριν τη μεταφορά του κωδικού.

1.17.
Ο κωδικός δεν εμφανίζεται στην οθόνη για λόγους ασφαλείας. Είναι μια πρακτική που χρησιμοποιεί by default το πρωτόκολλο TELNET.

1.18.
Δεν υπάρχει ιδιαίτερη ασφάλεια κατά τη χρήση της υπηρεσίας TELNET, αφού δε χρησιμοποιείται κάποιου είδους κρυπτογράφηση και επομένως οποιοσδήποτε μπορεί, έχοντας πρόσβαση στη συνομιλία των δύο άκρων, να υποκλέψει πληροφορίες, όπως, για παράδειγμα, τον κωδικό του χρήστη.

Άσκηση 2:

2.1.
Χρησιμοποίησα το φίλτρο σύλληψης *host 147.102.40.15*.

2.2.
Το -d που πληκτρολόγησα στη γραμμή εντολής ενεργοποιεί το debugging mode για την FTP σύνδεση.

2.3.
Το FTP χρησιμοποιεί το TCP πρωτόκολλο μεταφοράς.

2.4.
Για την επικοινωνία FTP σχετικά με τις εντολές ελέγχου χρησιμοποιούνται η θύρα πηγής 58793 και η θύρα προορισμού 21, ενώ για την επικοινωνία FTP σχετικά με τη μεταφορά δεδομένων χρησιμοποιούνται η θύρα πηγής 20 και θύρα προορισμού 58803.

2.5.
Η σύνδεση TCP για τη μεταφορά δεδομένων FTP γίνεται από την πλευρά του εξυπηρετητή edu-dy.cn.ntua.gr.

2.6.
Ο πελάτης (δηλαδή ο υπολογιστής μου μέσω της σύνδεσης στη διεπαφή του Πολυτεχνείου με χρήση OpenVPN) έστειλε τις παρακάτω εντολές: *OPTS, USER, PASS, HELP, PORT, NLST, QUIT.*

2.7.
Οι εντολές αυτές που έστειλε ο πελάτης εμφανίζονται στο παράθυρο εντολών ως πληροφορίες αποσφαλμάτωσης (debugging) με τη χρήση ενός βέλους ($---->$), ακολουθούμενο από την αντίστοιχη εντολή.

2.8.
Το όνομα χρήστη μεταφέρεται με χρήση της εντολής *USER*.

2.9.
Χρησιμοποιείται μόλις ένα πακέτο IP για να μεταφερθεί το όνομα χρήστη.

2.10.
Ο κωδικός χρήστη μεταφέρεται με χρήση της εντολής *PASS.*

2.11.
Χρησιμοποιείται μόλις ένα πακέτο IP για να μεταφερθεί ο κωδικός χρήστη.

2.12.
Μια διαφορά στον τρόπο λειτουργίας των πρωτοκόλλων FTP και TELNET είναι ότι στο πρωτόκολλο FTP χρησιμοποιείται ένα πακέτο για τη μεταφορά του ονόματος ή/και του κωδικού χρήστη, ενώ στο πρωτόκολλο TELNET χρησιμοποιούνται περισσότερα πακέτα,

συγκεκριμένα τόσα όσα το μέγεθος του ονόματος ή/και του κωδικού συν ένα ακόμα για το New Line - Enter. Μια ομοιότητα στον τρόπο λειτουργίας των πρωτοκόλλων FTP και TELNET είναι ότι και στα δύο πρωτόκολλα δεν παρατηρείται χρήση κρυπτογράφησης κατά τη μεταφορά αυτών των στοιχείων.

2.13.
Η εντολή help του προγράμματος φλοιού ftp δε μεταφράζεται σε εντολή του πρωτοκόλλου FTP, όμως η εντολή remotehelp μεταφράζεται στην εντολή HELP του πρωτοκόλλου FTP.

2.14.
Η εντολή ALLO και η εντολή AUTH είναι δύο εντολές του πρωτοκόλλου FTP που δεν υποστηρίζονται από τον εξυπηρετητή.

2.15.
Από τον υπολογιστή μου στάλθηκε μόλις ένα πακέτο σχετικά με την εντολή remotehelp, ενώ από τον εξυπηρετητή στάλθηκαν 9 πακέτα.

2.16.
Γενικά για απαντήσεις που αποτελούνται από πολλές γραμμές, η πρώτη αυτών πρέπει να ξεκινάει με τον κωδικό απάντησης ακολουθούμενο από το σύμβολο - (hyphen), ενώ η τελευταία πρέπει να ξεκινάει με τον ίδιο κωδικό απάντησης ακολουθούμενο από ένα κενό.

2.17.
Οι πρώτοι 4 δεκαδικοί αριθμοί του μηνύματος FTP που μεταφέρει την εντολή PORT αποτελούν τη διεύθυνση IPv4 της διεπαφής που χρησιμοποιεί ο υπολογιστής μου για την επικοινωνία με τον εξυπηρετητή FTP.

2.18.
Η θύρα προορισμού προκύπτει από τους άλλους 2 δεκαδικούς αριθμούς πολλαπλασιάζοντας τον πρώτο με 256 και προσθέτοντας μετά στο αποτέλεσμα το δεύτερο. Στη δική μου περίπτωση, οι δύο αριθμοί είναι οι 229 και 179 και έχουμε $229 * 256 + 179 = 58803$, που είναι και η θύρα που έχω καταγράψει στο ερώτημα 2.4.

2.19.
Η εντολή του πρωτοκόλλου FTP που εμφανίζει τα περιεχόμενα του τρέχοντος καταλόγου είναι η NLST.

2.20.
Πριν εμφανιστούν τα αποτελέσματα σχετικά με τα περιεχόμενα του τρέχοντος καταλόγου, πρέπει να υπάρχει σύνδεση με τη θύρα δεδομένων. Για αυτό προηγείται η εντολή PORT, ώστε να γίνει πρώτα αυτή η σύνδεση και στη συνέχεια να εμφανιστούν τα δεδομένα της NLST.

2.21.
Η εντολή bye του προγράμματος φλοιού ftp μεταφράζεται στην εντολή QUIT του πρωτοκόλλου FTP.

2.22.
Ο εξυπηρετητής FTP αποκρίνεται στην εντολή bye με το μήνυμα *221 Goodbye*.

2.23.
Χρησιμοποίησα το φίλτρο απεικόνισης *tcp.flags.fin == 1.*

2.24.
Η απόλυση της σύνδεσης TCP σχετικά με τα μηνύματα δεδομένων του FTP γίνεται από την πλευρά του εξυπηρετητή, ενώ η απόλυση της σύνδεσης TCP σχετικά με τις εντολές ελέγχου γίνεται από την πλευρά του πελάτη.

2.25.
Για την επικοινωνία FTP σχετικά με τις εντολές ελέγχου χρησιμοποιούνται η θύρα πηγής 55258 και η θύρα προορισμού 21, ενώ για την επικοινωνία FTP σχετικά με τη μεταφορά δεδομένων χρησιμοποιούνται η θύρα πηγής 55259 και θύρα προορισμού 13678.

2.26.
Ο πελάτης (δηλαδή ο υπολογιστής μου μέσω της σύνδεσης στη διεπαφή του Πολυτεχνείου με χρήση OpenVPN) έστειλε τις παρακάτω εντολές: *USER, PASS, opts, syst, site, PWD, noop, CWD, TYPE, PASV, LIST.*

2.27.
Ως όνομα χρήστη φαίνεται το anonymous, ενώ ως κωδικός χρήστη ο IEUser@.

2.28.
Χρησιμοποιήθηκε η εντολή *LIST* του πρωτοκόλλου FTP.

2.29.
Ο εξυπηρετητής ανταποκρίνεται στην εντολή *PASV* με το μήνυμα *227 Entering Passive Mode (147,102,40,15,53,110).*

2.30.
Η εγκατάσταση της σύνδεσης TCP που αφορά τα μηνύματα δεδομένων του FTP γίνεται από την πλευρά του πελάτη.

2.31.
Ο εξυπηρετητής χρησιμοποιεί τη θύρα 13678 για τη μεταφορά των δεδομένων FTP, το οποίο προκύπτει και από τους δύο τελευταίους δεκαδικούς του μηνύματος του ερωτήματος 2.29. Συγκεκριμένα $53 * 256 + 110 = 13678$.

2.32.
Η θύρα σύνδεσης TCP για τη μεταφορά των δεδομένων FTP στην πλευρά του πελάτη προκύπτει με τυχαία επιλογή από τις διαθέσιμες θύρες.

2.33.
Στάλθηκαν 2 μηνύματα δεδομένων FTP από τον εξυπηρετητή με μέγεθος δεδομένων 536 και 490 byte αντίστοιχα.

2.34.
Το πρώτο αυτό μήνυμα δεδομένων FTP έχει μέγεθος ίσο με το μέγιστο δυνατό με βάση το MTU της διεπαφής του εξυπηρετητή (576) και το MSS που επικοινώνησε και με τον αποστολέα, χωρίς να χρειάζεται να γίνει κάποιος θρυμματισμός, ώστε να μπορέσουν να φύγουν τα πακέτα από τον εξυπηρετητή.

2.35.
Η απόλυση της σύνδεσης TCP σχετικά με τις εντολές ελέγχου γίνεται από την πλευρά του πελάτη.

2.36.
Η απόλυση της σύνδεσης TCP σχετικά με τα μηνύματα δεδομένων του FTP γίνεται από την πλευρά του εξυπηρετητή.

Άσκηση 3:

3.1.
Το TFTP χρησιμοποιεί το UDP πρωτόκολλο μεταφοράς.

3.2.
Για την πρώτη επικοινωνία του πελάτη με τον εξυπηρετητή TFTP χρησιμοποιούνται η θύρα πηγής 53888 και η θύρα προορισμού 69.

3.3.
Για τη μεταφορά των δεδομένων χρησιμοποιούνται η θύρα πηγής 20929 και η θύρα προορισμού 53888.

3.4.
Η θύρα 69 αντιστοιχεί στο πρωτόκολλο εφαρμογής TFTP.

3.5.
Οι αριθμοί των θυρών που χρησιμοποιούνται κατά τη μεταφορά δεδομένων επιλέγονται τυχαία από τους διαθέσιμους, ώστε να ελαχιστοποιηθεί η πιθανότητα να επιλεγεί ο ίδιος αριθμός θύρας δύο διαδοχικές φορές.

3.6.
Η μεταφορά του αρχείου rfc1350.txt γίνεται σε mode ASCII.

3.7.
Στο πρώτο μήνυμα TFTP μεταξύ πελάτη και εξυπηρετητή καθορίζεται το mode της μεταφοράς του αρχείου, συγκεκριμένα στο πεδίο Type της TFTP επικεφαλίδας, με τιμή *netascii*.

3.8.
Όλοι οι τύποι των TFTP μηνυμάτων που παρατηρώ είναι οι εξής: Read Request (1), Data Packet (3), Acknowledgement (4).

3.9.
Το πρωτόκολλο TFTP αντιμετωπίζει το πρόβλημα αξιοπιστίας του πρωτοκόλλου μεταφοράς UDP με τη χρήση Acknowledgement μηνυμάτων τα οποία περιέχουν τον αριθμό Block κάθε μηνύματος που λαμβάνει.

3.10.
Για τον παραπάνω σκοπό χρησιμοποιείται ο τύπος μηνύματος TFTP Acknowledgement, το οποίο καθορίζεται από την τιμή του πεδίου Opcode της επικεφαλίδας TFTP και συγκεκριμένα με τιμή 4 (0x0004).

3.11.
Το μέγεθος των μηνυμάτων TFTP που μεταφέρουν τα προς μετάδοση δεδομένα είναι 558 byte.

3.12.
Τα παραπάνω μηνύματα TFTP (με εξαίρεση του τελευταίου) μεταφέρουν το καθένα 512 byte δεδομένων.

3.13.
Ο πελάτης αντιλαμβάνεται το τέλος της μετάδοση των δεδομένων όταν λάβει ένα μήνυμα TFTP με μέγεθος δεδομένων μικρότερο των 516 byte.