ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΣΙΤΩΝ
ΡΟΗ Δ - ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ (COMPUTER NETWORKS)

ΓΕΩΡΓΑΚΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ 03120827

ΑΝΑΦΟΡΑ 8ΗΣ ΕΡΓΑΣΤΗΡΙΑΚΗΣ ΑΣΚΗΣΗΣ

Ομάδα: 2
Λογισμικο: Linux Ubuntu 20.04
Ονομα PC: glaptop
Διεύθυνση IP: 147.102.239.68
Διεύθυνση MAC: 70:9c:d1:03:b0:1

ΑΣΚΗΣΗ 1:

1.1 Το πρωτόκολλο μεταφοράς που χρησιμοποιεί το TELNET είναι το TCP
1.2 Οι θύρες που χρησιμοποιούνται για την επικοινωνία είναι οι 23 και 43916
1.3 Η θύρα που αντιστοιχεί στο πρωτόκολλο εφαρμογής TELNET είναι η 23
1.4 Το φίλτρο απεικόνισης που χρησιμοποίησα είναι το: telnet
1.5 Οι εντολές που κατέγραψα είναι:
Do Echo: Εξυπηρετητής προς τον υπολογιστή μου
Won't Echo: Ο Υπολογιστής μου προς τον Εξυπηρετητή
Will Echo: Εξυπηρετητής προς τον υπολογιστή μου
Do Echo: Ο Υπολογιστής μου προς τον Εξυπηρετητή
1.6 Ναι, ο εξυπηρετητής ζητάει από τον υπολογιστή μου να επαναλαμβάνει τους χαρακτήρες (με την εντολή do echo) και ο υπολογιστής μου αρνείται (με την εντολή won't echo)
1.7 Οχι, ο εξυπηρετητής δεν ζητάει από τον υπολογιστή μου να μην επαναλαμβάνει τους χαρακτήρες
1.8 Ναι, ο εξυπηρετητής προτίθεται να επαναλαμβάνει τους χαρακτήρες που λαμβάνει (με την εντολή will echo)
1.9 Ναι, έχει προηγηθεί εντολή do echo
1.10 Ο εξυπηρετητής επαναλαμβάνει κάθε χαρακτήρα που ο υπολογιστής μου στέλνει
1.11 Με βάση τα ερωτήματα 1.8 και 1.9, ο εξυπηρετητής δηλώνει επιθυμία χρήσης της επιλογής echo και ο υπολογιστής μου ζητα αυτή την επιλογή, επομένως όταν βλεπουμε τον εξυπηρετητή να την χρησιμοποιεί (επαναλαμβάνοντας του χαρακτήρες)
1.12 Το φίλτρο που χρησιμοποίησα είναι: ip.src == 147.102.239.68 and telnet
1.13 Για να μεταφερθεί η πληροφορία για το όνομα χρειάστηκαν 5 πακέτα
1.14 Για να μεταφερθεί η πληροφορία για τον κωδικό χρειάστηκαν 5 πακέτα
1.15 Όχι, ο εξυπηρετητής στέλνει την ηχώ των χαρακτήρων του κωδικού
1.16 Όχι, δεν παρατηρήθηκε εντολή TELNET "Don't Echo" πριν τη μεταφορά του κωδικού

1.17 Ο εξυπηρετητής γνωρίζει ότι πρόκεται για κωδικό.
1.18 Η υπηρεσία TELNET δεν παρέχει καμία ασφάλεια καθώς δεν υπάρχει κρυπτογράφηση. Μέσω του wireshark μπορούμε να δούμε το όνομα και τον κωδικό.

ΑΣΚΗΣΗ 2:
2.1 Το φίλτρο που χρησιμοποίησα είναι: host 147.102.40.15
2.2 Το –d στη γραμμή εντολής ενεργοποιεί το debugging mode
2.3 Το FTP χρησιμοποιεί για πρωτόκολλο μεταφοράς το TCP
2.4 Οι θύρες που χρησιμοποιήθηκαν είναι:
Έλεγχος: 21 (Εξυπηρετητής) και 48780 (ο υπολογιστής μου)
Μεταφορά Δεδομένων: 20 (Εξυπηρετητής) και 44947 (ο υπολογιστής μ)
2.5 Ο αριθμός θύρας TCP για την εγκατάσταση σύνδεσης ελέγχου είναι 21 και για την μεταφορά δεδομένων είναι 20
2.6 Η σύνδεση TCP για τη μεταφορά δεδομένων FTP γίνεται από την πλευρά του εξυπηρετητή
2.7 Οι εντολές FTP που έστειλε ο πελάτης είναι:
USER / PASS / SYST / FEAT / HELP / EPRT / LIST / QUIT
2.8 Ναι, οι εντολές αυτές εμφανίζονται στην οθόνη του προγράμματος φλοιού και διαφοροποιούνται από τις εντολές φλοιού που εκτελούμε εμείς.
2.9 Το όνομα χρήστη μεταφέρεται με την εντολή USER
2.10 Για να μεταφερθεί το όνομα του χρήστη χρειάστηκε ένα πακέτο.
2.11 Ο κωδικός χρήστη μεταφέρεται με την εντολή PASS
2.12 Για να μεταφερθεί ο κωδικός χρήστη χρειάστηκε ένα πακέτο.
2.13 Ομοιότητα: Οι εντολές φλοιού μεταφράζονται σε εντολές πρωτοκόλλου.
Διαφορά: Στο telnet το όνομα και ο κωδικός μεταφέρονται σε πολλά πακέτα (ένα για κάθε byte) ενώ στο ftp χρειάζεται μόνο 1 πακετο.
2.14 Όχι, η εντολή help του προγράμματος φλοιού ftp δεν μεταφράζεται σε εντολή του πρωτοκόλλου
2.15 Δύο εντολές FTP που δεν υποστηρίζονται από τον εξυπηρετητή είναι:
ALLO και AUTH
2.16 Στάλθηκαν 9 πακέτα από την εξυπηρετητή και 1 πακέτο από τον υπολογιστή μου, σχετικά με την εντολή rhelp
2.17 Στο τελευταίο πακέτο μετά τον κωδικό δεν έχει παυλα (hyphen ‘-’) αλλά κενό <SP>
2.18 Αντί για PORT, έχω EPRT (Extended Port Command) και επομένως δεν βλέπω τους 4 πρώτους δεκαδικους αριθμούς που ζητούνται. Αυτοι οι αριθμοι θα έδειχναν την IP του αποστολέα. (Η EPRT δείχνει όλη την IP σε ένα κελι)
2.19 Και πάλι, στην EPRT φαίνεται κατευθείαν ο ακριβής αριθμός της θύρας. Στην PORT δείχνει 2 αριθμούς X και Y και ο η θύρα είναι X*256+Y
2.20 Η εντολή του πρωτοκόλλου FTP που εμφανίζει τα περιεχόμενα του τρέχοντος καταλόγου είναι η LIST
2.21 Η εντολή PORT προηγείται της LIST καθώς πρέπει να καθοριστεί πρώτα η data port

2.22 Στην εντολή πρωτοκόλλλου QUIT
2.23 Ο εξυπηρετητής FTP αποκρίνεται με το μήνυμα: Goodbye
2.24 Το φίλτρο που χρησιμοποίησα είναι: tcp.flags.fin == 1
2.25 Η απόλυση των συνδέσεων TCP γίνεται:
Εντολές ελέγχου: Από τον υπολογιστή μου
Μηνύματα Δεδομένων: Από τον εξυπηρετητή
Για να το συμπεράνουμε αυτό κοιτάμε το πρώτο πακετο με fin flag
2.26 Το φίλτρο που χρησιμοποίησα είναι:
ip.addr == 147.102.40.15 and tcp.flags.syn == 1
2.27 Θυρες:
Δεδομένων: 39359 (Ο υπολογιστής μου) / 35273 (Ο εξυπηρετητής)
Έλεγχος: 50198 (Ο υπολογιστής μου) / 21 (Ο εξυπηρετητής)
2.28 Η εγκατάσταση της σύνδεσης TCP για τη μεταφορά δεδομένων FTP γίνεται από την πλευρά του πελάτη (ο υπολογιστής μου) και χρησιμοποιείται η θύρα 35273 (η οποία ανακοινώθηκε από την πλευρά του εξυπηρετητή)
2.29 Εντολές FTP που έστειλε ο πελάτης στον εξυπηρετητή:
AUTH TLS / AUTH SSL / USER / PASS / SYST / FEAT / OPTS / PWD / TYPE I / PASV / MLSD
2.30 Όνομα: anonymous / Κωδικός: anonymous@example.com
2.31 Για την εμφάνιση λίστας αρχείων χρησιμοποιήθηκε η εντολή MLSD
2.32 Στην εντολή PASV ο εξυπηρετητής απαντάει:
227 Entering Passive Mode (147,102,40,15,137,201)
2.33 Η θύρα 35273 προκύπτει από την παραπάνω απάντηση ως εξής:
137*256 + 201 = 35273
2.34 Ο αριθμός θύρας της σύνδεσης TCP για μεταφορά δεδομένων FTP στην πλευρά του πελάτη είναι τυχαίος (ubuntu linux)
2.35 Κάθε μήνυμα δεδομένων έχει μήκος 536 bytes, εκτός του τελευταίου που έχει 121 (σύνολο 4409 bytes) και παρατηρούμε 9 μηνύματα.
2.36 Τα πρώτα μηνύματα έχουν μήκος ίσο με την MTU
2.37 Η απόλυση της σύνδεσης TCP που αφορά τη μεταφορά δεδομένων FTP γίνεται από την πλευρά του πελάτη
2.38 Η απόλυση της σύνδεσης TCP που αφορά τις εντολές ελέγχου FTP γίνεται από την πλευρά του εξυπηρετητή

ΑΣΚΗΣΗ 3:
3.1 Το TFTP χρησιμοποιεί για πρωτόκολλο μεταφοράς το UDP
3.2 Τύποι μηνυμάτων TFTP:
Read Request / Data Packet / Acknowledgement
3.3 Το πεδίο της επικεφαλίδας TFTP που καθορίζει τον τύπο του μηνύματος είναι το opcode και έχει μήκος 2 byte
3.4 Πρώτη Επικοινωνία:
Θύρα Πηγής: 50493 / Θύρα Προορισμού: 69
(Πηγή ο Υπολογιστής μου και Προορισμός ο Εξυπηρετητής)

3.5 Μεταφορα Δεδομένων:
Θύρα Πηγής: 40402 / Θύρα Προορισμού: 50493
(Πηγή ο Εξυπηρετητής και Προορισμός ο Υπολογιστής μου)
3.6 Η θύρα που αντιστοιχεί στο πρωτόκολλο εφαρμογής TFTP είναι η 69
3.7 Οι αριθμοί θυρών, που χρησιμοποιούνται κατά την μεταφορά δεδομένων, προκύπτουν τυχαία.
3.8 Η μεταφορα του αρχείου rfc13550.txt γίνεται σε ASCII
3.9 Αυτό καθορίζεται στο μήνυμα Read Request στο πεδίο Type το οποίο τώρα έχει τιμή: netascii
3.10 Το TFTP για να αντιμετωπίσει αυτό το πρόβλημα, χωρίζει τα πακέτα σε blocks και για κάθε ένα που στέλνει περιμένει acknowledgement
3.11 Για τον σκοπό αυτό τα μηνύματα TFTP περιέχουν το πεδίο Block το οποίο περιέχει έναν αριθμό, ο οποίος μετά από κάθε acknowledgement με ίδια τιμή Block, μεγαλώνει. Ο αριθμός αυτός δείχνει δηλαδή την σειρά των μηνυμάτων
3.12 Το μέγεθος των TFTP μηνυμάτων είναι 558 bytes. (πλην του τελευταίου)
3.13 Το μέγεθος των δεδομένων που μεταφέρονται από αυτά τα μηνύματα TFTP είναι 512 bytes
3.14 Το πλαίσιο Ethernet, για αυτά τα μηνύματα TFTP είναι 14 bytes
3.15 Ο πελάτης αντιλαμβάνεται το τέλος της μετάδοσης δεδομένων από το γεγονός ότι το τελευταίο πακέτο έχει μήκος δεδομένων μεταξύ 0 και 511 bytes.