8η Εργαστηριακή Άσκηση στα Δίκτυα Υπολογιστών

Ονοματεπώνυμο	Γεώργιος Στεφανάκης
Αρ. Μητρώου	el18436
Ομάδα	4
Λειτουργικό Σύστημα	Manjaro Linux x86_64
Διεύθυνση IP	147.102.131.216
Διεύθυνση MAC	b4:69:21:5e:da:03
Ημερομηνία	2022-12-09

1. TELNET

1.1. TCP
1.2. 147.102.40.15 → Port 23, 147.102.131.216 → Port 53779
1.3. Port 23
1.4. Η σύνταξή του είναι “telnet”
1.5. 147.102.40.15 → 147.102.131.216: Do Echo, 147.102.131.216 → 147.102.40.15: Will Echo, 147.102.40.15 → 147.102.131.216: Don’t Echo/Will Echo, 147.102.131.216 → 147.102.40.15: Won’t Echo
1.6. Στην αρχή μας στέλνει Do Echo και ο υπολογιστής μας δέχεται με το Will Echo.
1.7. Στη συνέχεια ο edu-dy.cn.ntua.gr μας στέλνει Don’t Echo και ο υπολογιστής μας το δέχεται (Won’t Echo) συνεπώς δεν θα κάνουμε Echo τα μηνύματα που θα μας στέλνει.
1.8. Ναι αφού μαζί με το Don’t Echo κάνει και Will Echo στο τέλος.
1.9. Ναι έχει προηγηθεί εντολή Telnet με την οποία ο υπολογιστής μας ζητάει Do Echo.
1.10. Παρατηρούμε όπως και φαίνεται παρακάτω ότι οι χαρακτήρες του ονόματος χρήστη επαναλαμβάνονται (Echo) από τον server.
1.11. Αυτό συμβαίνει καθώς ο server όπως είδαμε πριν είχε δηλώσει ότι θέλει να κάνει Echo (Will Echo) και εμείς του απαντήσαμε με Do Echo. Συνεπώς θα μας κάνει Echo τα μηνύματα που του στέλνουμε.
1.12. Η σύνταξή του είναι telnet and ip.src == 147.102.131.216
1.13. Χρειάζονται 5 πακέτα με Data a,b,c,d,\r\n αντιστοίχως.
1.14. Χρειάζονται 5 πακέτα με Data e,f,g,h,\r\n αντιστοίχως.
1.15. Όχι
1.16. Όχι δεν παρατηρήσαμε εντολή Don’t Echo πριν τη μεταφορά του κωδικού.
1.17. Δεν εμφανίζεται ο κωδικός στην οθόνη για λόγους ασφαλείας.
1.18. Δεν υπάρχει ασφάλεια καθώς οποιοσδήποτε που παρακολουθεί τα πακέτα που ανταλλάσσονται μπορεί να υποκλέψει τις πληροφορίες που μεταφέρουν.

2. FTP

2.1. host 147.102.131.216
2.2. Το -d επιτρέπει το debugging (Enables debugging).
2.3. Χρησιμοποιεί το TCP.
2.4. Ο Server χρησιμοποιεί την θύρα 21 ως θύρα ελέγχου και τη θύρα 20 ως θύρα δεδομένων ενώ ο προορισμός χρησιμοποιεί την θύρα 54035 ως θύρα ελέγχου και τη θύρα 54037 ως θύρα δεδομένων.
2.5. Από την πλευρά του εξυπηρετητή.
2.6. Εστειλε τις εξής εντολές,
- USER anonymous
- PASS labuser@cn
- HELP
- PORT 147,102,131,105,209,205
- LIST

- QUIT

2.7. Ναι, ως εξής,
- – – – > USER anonymous
- – – – > PASS XXXX
- – – – > HELP
- – – – > PORT 147,102,131,216,209,205
- – – – > LIST
- – – – > QUIT

2.8. Με την εντολή User.
2.9. Χρειάζεται 1 πακέτο.
2.10. Με την εντολή PASS.
2.11. Χρειάζεται 1 πακέτο.
2.12. Μια διαφορά είναι ότι τα δεδομένα στέλνονται όλα μαζί στο ftp ενώ στο telnet ένα-ένα ενώ μια ομοιότητα είναι ότι δεν υπάρχει κρυπτογράφηση και στα 2.
2.13. Όχι.
2.14. Δύο τέτοιες εντολές είναι οι CCC και MIC.
2.15. Στάλθηκαν 9 από τον εξυπηρετητή και 1 από εμάς.
2.16. Μετά τον κωδικό της απόκρισης (214) δεν υπάρχει παύλα (-) αλλά σκέτο space.
2.17. Παριστάνουν την IPv4 που μας αποδόθηκε από το VPN.
2.18. Προκύπτει αν πολλαπλασιάσουμε το 5ο octet με το 256 και μετά προσθέσουμε το 6ο octet στο σύνολο. Άρα στην περίπτωσή μας είναι 211*256+21 = 54037 άρα επαληθεύεται αυτό που είχαμε βρει στο 2.4.
2.19. Η εντολή NLST.
2.20. Αυτό συμβαίνει γιατί γίνεται σύναψη νέας σύνδεσης με τριμερή χειραψία με την θύρα δεδομένων.
2.21. Στην εντολή Quit.
2.22. Με το μήνυμα 221 Goodbye.
2.23. Η σύνταξή του είναι tcp.flags.fin == 1.
2.24. Την σύνδεση δεδομένων την κλείνει ο server και την σύνδεση ελέγχου την κλείνει ο υπολογιστής μας.
2.25. Σύνδεση ελέγχου: server: port 21 client: 56916
Σύνδεση δεδομένων: server: 18172 (dynamic port) client: 56918
2.26. Εστειλε τις εξής εντολές,
- USER anonymous
- PASS chrome@example.com
- SYST
- PWD
- TYPE I
- SIZE /
- CWD /
- PASV
- LIST -l
- QUIT

2.27. Χρησιμοποιήθηκαν τα: Όνομα: anonymous και password: IEUser@
2.28. Η εντολή LIST.
2.29. Response: 227 Entering Passive Mode (147,102,40,15,70,252).
2.30. Από την δική μας μεριά άρα από την μεριά του πελάτη.
2.31. Προκύπτει ως 70*256+252 = 18172.
2.32. Προκύπτει με τυχαίο τρόπο.
2.33. Παρατηρούμε 2 μηνύματα συνολικού μεγέθους δεδομένων 1026 bytes.
2.34. Είναι το μέγιστο που μπορεί να στείλει ο server δηλαδή ίσο με MSS = 536.
2.35. Η απόλυση σύνδεσης ελέγχου γίνεται από εμάς.
2.36. Η απόλυση σύνδεσης δεδομένων γίνεται από τον server.

3. TFTP

3.1. Το UDP.

3.2. Source (εμείς): Port 58665 και Destination: Port 69.
3.3. Ο υπολογιστής μας χρησιμοποιεί την θύρα 58665 και ο server την θύρα 47709.
3.4. Η θύρα 69.
3.5. Προκύπτουν με τυχαίο τρόπο.
3.6. Μεταφέρεται με ASCII τρόπο.
3.7. Καθορίζεται στο πρώτο μήνυμα που στέλνει ο πελάτης στον εξυπηρετητή και καθορίζεται στο πεδίο Type του TFTP με τιμή netascii.
3.8. Παρατηρούμε στο πεδίο opcode του TFTP ότι έχουμε τα Read request (1), Data Packet (3), Acknowledgment (4).
3.9. Χρησιμοποιούνται πακέτα με opcode = 4 (Acknowledgment) που επιβεβαιώνουν ότι εμείς ως client λάβαμε το πακέτο.
3.10. Χρησιμοποιείται τύπος μηνύματος Acknowledgment και το πεδίο opcode είναι αυτό που το δηλώνει.
3.11. Το μέγεθος τους είναι 516 bytes.
3.12. Το μέγεθος των δεδομένων που μεταφέρονται από αυτά τα μηνύματα είναι 512 bytes.
3.13. Ο client αντιλαμβάνεται το τέλος της μετάδοσης δεδομένων όταν λάβει ένα πακέτο που περιέχει λιγότερα από 512 bytes δεδομένων.