ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

8^{Ο} ΕΡΓΑΣΤΗΡΙΟ

Σεραφείμ Τζελέπης AM:el18849,

Huawei MateBook 14, Windows 10,

Mac Address: 5C-3A-45-DC-95-1D,

Ομάδα : 4

1)

1.1: TCP

1.2: Οι θύρες που χρησιμοποιούνται είναι οι Port 23 και Port 58421.

1.3: Η θύρα(Port) 23.

1.4: Το φίλτρο απεικόνισης είναι το 'telnet'.

1.5: Οι εντολές τύπου echo μαζί με τον αποστολέα τους που προηγούνται είναι οι:

- Do, 147.102.40.15
- Will, 192.168.1.13
- Don't, 147.102.40.15
- Will, 147.102.40.15
- Won't, 192.168.1.13

1.6: Ναι ο edu-dy.cn.ntua.gr ζητάει με την εντολή Do στον υπολογιστή μου να επαναλαμβάνει τους χαρακτήρες και ο υπολογιστής μου δέχεται με την εντολή Will.

1.7: Ναι ο edu-dy.cn.ntua.gr ζητάει με την εντολή Don't στον υπολογιστή μου να μην επαναλαμβάνει χαρακτήρες και ο υπολογιστής μου δέχεται με την εντολή Won't.

1.8: Ναι όπως αυτό φαίνεται από την εντολή Will.

1.9: Ναι με την χρήση της εντολή Do.

1.10: Ο edu-dy.cn.ntua.gr επαναλαμβάνει κάθε χαρακτήρα του πληκτρολογίου

1.11: Αυτό αιτιολογείται καθώς όπως βλέπουμε στα ερωτήματα 1.8,1.9 ο edu-dy.cn.ntua.gr προτίθεται να επαναλάβει του χαρακτήρες και στην συνέχεια του ζητείται να τους επαναλάβει.

1.12: Το φίλτρο απεικόνισης είναι το 'telnet and ip.src == 192.168.1.13'.

1.13: Χρειάζονται συνολικά 5 πακέτα, ένα για κάθε χαρακτήρα και ένα για το enter.

1.14: Σε απόλυτη αντιστοιχία με το παραπάνω ερώτημα χρειάστηκαν 5 πακέτα στο σύνολο.

1.15: Όχι.

1.16: Όχι.

1.17: Ο κωδικός δεν εμφανίζεται στην οθόνη από το telnet πιθανώς για λόγους ασφαλείας.

1.18: Η ασφάλεια της υπηρεσίας telnet είναι ελάχιστη καθώς δεν υπάρχει καμία κρυπτογράφηση στις εντολές και στα δεδομένα που αποστέλνονται και συνεπώς οι χρήσιμες πληροφορίες είναι εκτεθειμένες.

2)

2.1: Το φίλτρο σύλληψης που χρησιμοποιήθηκε είναι το 'host edu-dy.cn.ntua.gr'.

2.2: Το -d χρησιμοποιείται ώστε να ενεργοποιηθεί το debugging.

2.3: TCP

2.4: Για τις εντολές ελέγχου χρησιμοποιείται η θύρα 21 του εξυπηρετητή και η θύρα 55994 του VPN υπολογιστή, ενώ για τις εντολές μεταφοράς δεδομένων χρησιμοποιείται η θύρα 20 του εξυπηρετητή και η θύρα 55995 του VPN υπολογιστή.

2.5: Από την πλευρά του εξυπηρετητή΄.

2.6:

- OPTS UTF8 ON
- USER anonymous
- PASS labuser@cn
- HELP
- PORT 147,102,131,191,218,187
- NLST
- QUIT

2.7: Ναι εμφανίζονται όλες οι παραπάνω εντολές στον φλοιό με την σύνταξη ---> command.

2.8: USER

2.9: Ένα.

2.10: PASS

2.11: Ένα

2.12: Μια ομοιότητα είναι ότι δεν χρησιμοποιείται κρυπτογράφηση ενώ εκεί που διαφέρουν είναι στην μεταφορά του ονόματος και του κωδικού όπου στο TELNET κάθε χαρακτήρας αποστέλλεται ξεχωριστά ενώ στο ftp χρειάζεται μόνο ένα πακέτο για όλο το όνομα ή τον κωδικό.

2.13: Όχι.

2.14: SMNT, ALLO, AUTH.

2.15: Ένα από τον υπολογιστή μου και 9 από τον εξυπηρετητή.

2.16: Ο εξυπηρετητής δηλώνει ότι τελείωσε η αποστολή πακέτων παραλείποντας μετά τον αριθμό να βάλει το Hyphen “-“.

2.17: Οι πρώτοι 4 αριθμοί αποτελούν την IPv4 διεύθυνση του υπολογιστή μου.

2.18: Οι τελευταίοι δύο αριθμοί μπορούν να χρησιμοποιηθούν για την εύρεση της θύρας στην όποια ανακοινώνει ο πελάτης ότι θέλει να λάβει τα δεδομένα. Πιο συγκεκριμένα προκύπτει ο αριθμός αυτός πολλαπλασιάζοντας τον $5^{ο}$

αριθμό,218, με το 216 και προσθέτοντας στο γινόμενο αυτό τον 6^{ο} αριθμό, 187. Πράγματι (216 x 256) + 187 = 55995.

2.19: NLST

2.20: Γιατί γίνεται σύνδεση με την θύρα δεδομένων του πελάτη η οποία βρίσκεται μέσω της εντολής PORT.

2.21: QUIT.

2.22: Απαντάει με '221 Goodbye'.

2.23: 'tcp.flags.fin == 1'.

2.24: Η απόλυση των συνδέσεων και για τις εντολές ελέγχου όσο και για τα μηνύματα δεδομένων γίνεται από την πλευρά του πελάτη.

2.25: Για τα μηνύματα ελέγχου έχουμε ότι θύρα πηγής είναι η 54609 και θύρα προορισμού η 21, ενώ για τα μηνύματα δεδομένων έχουμε θύρα πηγής 54611 και θύρα προορισμού 29391.

2.26:

- USER anonymous
- PASS IEUser@
- Opts utf8 on
- syst
- site help
- PWD
- noop
- CWD /
- TYPE A
- PASV
- LIST

2.27: Όνομα: anonymous, Κωδικός: IEUser@.

2.28: LIST.

2.29: Ο εξυπηρετητής αποκρίνεται ως εξής: 227 Entering Passive Mode (147,102,40,15,114,207).

2.30: Από την πλευρά του πελάτη.

2.31: Ο εξυπηρετητής χρησιμοποιεί την θύρα 29391,η οποία προκύπτει από τους δύο τελευταίους αριθμούς του 2.29 όπως έχει εξηγηθεί και προηγουμένως, (256 x 114) + 207 = 29391.

2.32: Σύμφωνα με το πρωτόκολλο για την παθητική σύνδεση η θύρα πηγής για την μεταφορά δεδομένων είναι η θύρα πηγής για έλεγχο αυξημένη κατά ένα. Στην προκειμένη περίπτωση πιθανώς να είναι κατειλημμένη αύτη η θύρα(54610) συνεπώς η θύρα πηγής για τα δεδομένα είναι 54611 = 54609(θύρα πηγής ελέγχου) + 2.

2.33: Στάλθηκαν δύο μηνύματα δεδομένων με μέγεθος 536 και 490 Bytes αντίστοιχα.

2.34: Το MSS του 147.102.40.15 είναι 536 Bytes συνεπώς το πρώτο πακέτο έχει μέγεθος 536 Bytes και τα υπόλοιπα δεδομένα στέλνονται με το δεύτερο πακέτο.

2.35: Η απόλυση σύνδεσης που αφορά τις εντολές ελέγχου γίνεται από την πλευρά του πελάτη.

2.36: Η απόλυση σύνδεσης που αφορά τα μηνύματα δεδομένων γίνεται από την πλευρά του πελάτη.

3)

3.1: UDP.

3.2: Η θύρα πηγής είναι η 64524, ενώ η θύρα προορισμού είναι η 69.

3.3: Η θύρα πηγής είναι η 28871, ενώ η θύρα προορισμού είναι η 64524.

3.4: Η θύρα 69.

3.5: Τυχαία.

3.6: Σε ASCII.

3.7: Στο read request στο πεδίο Type, όπου έχει τιμή netascii, της επικεφαλίδας TFTP.

3.8: Read Request, Data Packet, Acknowledgment.

3.9: Για κάθε πακέτο που στέλνει ο εξυπηρετητής ο πελάτης απαντάει με ένα Acknowledgment.

3.10: Ο τύπος του μηνύματος αυτού είναι Acknowledgment και αυτό φαίνεται στο opcode της TFTP επικεφαλίδας.

3.11: Το συνολικό μέγεθος των TFTP πακέτων είναι 516 Bytes.

3.12: Το μέγεθος των δεδομένων είναι 512 Bytes.

3.13: Το μέγεθος του τελευταίου πακέτου ο πελάτης το αντιλαμβάνεται καθώς αυτό έχει μέγεθος δεδομένων μικρότερο των 512 Bytes.