ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

3^{Ο} ΕΡΓΑΣΤΗΡΙΟ

Σεραφείμ Τζελέπης AM:el18849,

Huawei MateBook 14, Windows 10,

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

Ομάδα : 4

1)

1.1: > arp -a

1.2: > arp -d

1.3: > ipconfig /all , και βρίσκω ότι η IPv4 διεύθυνση της προκαθορισμένη πύλης είναι 192.168.1.1 την ίδια διεύθυνση έχουν και οι εξυπηρετητές dns

1.4:

Interface: 192.168.1.19 --- 0x5

Internet Address	Physical Address	Type
192.168.1.1	d4-60-e3-b9-96-50	dynamic
192.168.1.11	c2-f6-4e-6c-c1-fa	dynamic
224.0.0.22	01-00-5e-00-00-16	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Interface: 192.168.16.1 --- 0x30

Internet Address	Physical Address	Type
224.0.0.22	01-00-5e-00-00-16	static

239.255.255.250 01-00-5e-7f-ff-fa static

1.5: Υπάρχει η κοινή διεύθυνση προκαθορισμένης πύλης και εξυπηρετητών dns

1.6: Η διεύθυνση από την όποια λήφθηκε απάντηση είναι η 192.168.1.11

1.7: Βλέπουμε ότι μετά το ping ξαναεμφανίζεται το entry 192.168.1.11 στο arp table

1.8: Εμφανίζεται η διεύθυνση 192.168.1.1 η οποία είναι και dns ip address

1.9: Όχι καθώς βρίσκεται σε διαφορετικό υποδίκτυο

2)

2.1: Το Wireshark καταγράφει το MAC header Ethernet II πακέτου, δηλαδή την διεύθυνση προορισμού την διεύθυνση πηγής και τον τύπο.

2.2: Το Wireshark δεν καταγράφει το προοίμιο, το όποιο απλώς αποτελεί έναν μηχανισμό για τον εντοπισμό της έναρξης ενός νέου πλαισίου και δεν μας παρέχει κάποιο δεδομένο

2.3: Το Wireshark εν γένει δεν (μπορεί να καταγράψει)/καταγράφει το FCS(crc) καθώς τα λειτουργικά συστήματα δεν το παρέχουν ως μέρος του πλαισίου.

2.4: 0x0800

2.5: 0x0806

2.6: 0x086dd

2.7: 5c:3a:45:dc:95:1d

2.8: d4:60:e3:b9:96:50

2.9: Όχι δεν είναι

2.10: Η διεύθυνση αυτή είναι του ρούτερ του δικτύου στο οποίο είναι συνδεδεμένος ο προσωπικός μου υπολογιστής και όχι του ιστότοπου όπου βρίσκεται σε διαφορετικό υποδίκτυο

2.11: 486 Bytes

2.12: 54 Bytes

2.13: d4:60:e3:b9:96:50

2.14: Όχι

2.15: Ανήκει στο ρούτερ

2.16: 5c:3a:45:dc:95:1d

2.17: Στον υπολογιστή μου

2.18: 522

2.19: 67 Bytes

3)

3.1: Έχουμε δυο διευθύνσεις πηγών: d4:60:e3:b9:96:50 είναι ατομική και παγκόσμια

5c:3a:45:dc:95:1d είναι ατομική και παγκόσμια

3.2: Σε όλα τα καταγεγραμμένα πακέτα συναντάται μόνο μια διεύθυνση προορισμού η ff:ff:ff:ff:ff:ff η όποια είναι ομαδική και τοπική

3.3: Το πρώτο Byte της διεύθυνσης αποτελείται από 8 bits από αυτά τα 8 bits πρώτο εκπέμπεται το δεξιότερο το 8ο πχ στην 5c:3a:45:dc:95:1d το πρώτο Byte είναι σε δυαδική μορφή 01011100 και το πρώτο bit που εκπέμπεται είναι το δεξιότερο 0 μετά το επόμενο 0 μετά ο άσος κλπ.

3.4: Η διεύθυνση MAC για τα πλαίσια εκπομπής είναι ff:ff:ff:ff:ff:ff

3.5: Μένουν μόνο πλαίσια του προτύπου IEEE 802.3

3.6: Δηλώνει το length του πλαισίου

3.7: Το πλαίσιο IEEE 802.3 χρησιμοποιεί τα 2 Bytes μετα τις διευθύνσεις για το length ενώ το πλαίσιο Ethernet II χρησιμοποιεί αυτά τα δυο Bytes για τον τύπο

3.8: Η επικεφαλίδα LLC έχει μέγεθος 3 Bytes και περιέχει τρεις επικεφαλίδες: DSAP, SSAP, Control field

3.9: Τα πλαίσια IEEE 802.3 μεταφέρουν δεδομένα πρωτοκόλλου STP μεγέθους 39 Bytes

3.10: Το ελάχιστο μέγεθος δεδομένων είναι 46 Bytes συνεπώς από τα 39 που έχουμε χρειάζονται άλλα 7 Bytes παραγέμισμα. Όντως το παραγέμισμα έχει αυτό το μέγεθος και εξυπηρετεί την συμπλήρωση του ελάχιστου αριθμού δεδομένων

4)

4.1: Απεικονίζει τα πακέτα που έχουν ως διεύθυνση πηγής ή προορισμού την MAC address της κάρτας δικτύου μου

4.2: Πλέον το φίλτρο απεικονίζει όσα από τα παραπάνω πακέτα είναι πρωτοκόλλου ARP(Πρακτικά δεν άλλαξε τίποτα γιατί και στην πρώτη καταγραφή όλα τα πλαίσια ήταν πρωτοκόλλου ARP)

4.3: Ανταλλάχθηκαν δυο πακέτα

4.4: Το πεδίο Type(0x0806)

4.5: Hardware type: 2 Bytes, Protocol type: 2 Bytes, Hardware size: 1 Byte, Protocol size: 1 Byte, Opcode: 2 Bytes, Sender MAC address: 6 Bytes, Sender IP address: 4 Bytes, Target MAC address: 6 Bytes, Target IP address: 4 Bytes

4.6: Hardware type: 1, υποδηλώνει κάρτα δικτύου υλικού Ethernet

4.7: Protocol type: 0x0800, υποδηλώνει πρωτόκολλο IPv4

4.8: Το EtherType με τιμή 0x0800 αντιστοιχεί στο πρωτόκολλο IPv4

4.9: Γιατί ο τύπος διεύθυνσης πρωτοκόλλου IPv4 έχει μέγεθος 4 Bytes

4.10: Γιατί ο τύπος διεύθυνσης πρωτοκόλλου Ethernet έχει μέγεθος 6 Bytes

4.11: Η διεύθυνση αυτή ανήκει στον υπολογιστή μου

4.12: Η διεύθυνση του παραλήπτη του πλαισίου αυτού είναι ff:ff:ff:ff:ff:ff δηλαδή είναι η διεύθυνση εκπομπής και λαμβάνεται από όλες τις τοπικές συνδεμένες συσκευές

4.13: Το ARP request είναι 28 Bytes και του πλαισίου Ethernet είναι 42 Bytes

4.14: Προηγούνται 20 Bytes

4.15: Opcode: 0x0001 request

4.16: Sender MAC address

4.17: Sender IP address

4.18: Target IP address

4.19: Target MAC address 00:00:00:00:00:00

4.20: Η διεύθυνση του αποστολέα ανήκει στο ρούτερ και η διεύθυνση του παραλήπτη ανήκει στον υπολογιστή μου

4.21: 0x0002

4.22: Sender IP address

4.23: Sender MAC address

4.24: Target IP address

4.25: Sender MAC address

4.26: ARP: 28 Bytes, Ethernet: 42 Bytes

4:27: ναι

4.28: Αυτό συμβαίνει γιατί το Wireshark θα κάνει capture πριν φτάσουν τα πακέτα στο στρώμα ζεύξης όπου δέχονται και το απαραίτητο padding ενώ στη λήψη το padding για συμπληρωθεί το ελάχιστο μέγεθος θα έχει γίνει από τον αποστολέα και έτσι το Wireshark θα κάνει capture το επαυξημένο πακέτο

4.29: Opcode

4.30: Μια διαφορά είναι στα target και sender mac addresses. Στην πρώτη περίπτωση έχω Sender τον υπολογιστή μου και άγνωστο target ενώ στην συνέχεια έχω sender την mac address που έψαχνα και target τον υπολογιστή μου

4.31: Τότε όλοι όσοι είναι στο δίκτυο θα στέλνουν τα πλαίσια τους σε αυτόν τον κακόβουλο υπολογιστή καθώς οι χρήστες θα το αποθήκευαν στον arp table τους.