LAB-02 (Systems networking)

Ονοματεπώνυμο : Νίκος Μπέλλος	Όνομα PC : BELLOS-DELL-G3
Ομάδα : 3	Ημερομηνία : 23/03/2022

Άσκηση 2: Ανάλυση δικτυακών πρωτοκόλλων με το TCPDUMP

1. `ifconfig`
2. `ifconfig em0 down` , `ifconfig em0 up`
3. `man tcpdump` , `man pcap` , `man pcap-filter`
4. `tcpdump -i em0 -n`
5. `tcpdump -i em0 -n -A` → for ASCII, `tcpdump -i em0 -n -x` → for Hex
6. `tcpdump -e` → οι πληροφοριές αυτές εμπεριέχονται στο Ethernet Header
7. `tcpdump -s 68`
8. `tcpdump host 10.0.0.1 -v` → -v stands for network layer header
9. `tcpdump host (10.0.0.1 and 10.0.0.2) -i em0`
10. `tcpdump net 1.1 ip -x`
11. `tcpdump not net 127.0.0.0/8 ip` → my network
12. `tcpdump broadcast -n ip`
13. `tcpdump ip[2:2] > 576` → ip[2:2] represents the ‘Total Length’ in IPv4 Header
14. `tcpdump ip[8] < 5`
15. X
16. `tcpdump src 10.0.0.1 and icmp`
17. `tcpdump dst 10.0.0.2 and tcp`
18. `tcpdump dst port 53 and udp`
19. `tcpdump host 10.0.0.10 tcp ip`
20. `tcpdump host 10.0.0.10 and port 23 and -w sample_capture`
21. `tcpdump tcp[tcpflags] & tcp-syn != 0`
22. `tcpdump (tcp[tcpflags] & tcp-syn != 0) or (tcp[tcpflags] & (tcp-syn|tcp-ack) != 0)` → τοποθετούμε μάσκες πάνω στα bits των tcp flags
23. `tcpdump (tcp[tcpflags] & tcp-fin != 0) or (tcp[tcpflags] & (tcp-fin|tcp-ack) != 0)`
24. Υπολογίζει από το 13ο στη σειρά byte του tcp header τα 4 πρώτα bits, τα οποία αντιστοιχούν στο H**eader** L**ength** και αυτή η τιμή τη διαιρεί με το 4 (slide 2 bits) ώστε να μπορεί να φιλτράρει αν υπάρχουν options (Το tcp header έχει 20 bytes χωρίς τα options)
25. `tcpdump (tcp[12:1] & 0xf0 >> 2) > 5` → 20 bytes / 4 = 5
26. `tcpdump tcp port 80 -A`
27. `tcpdump udp port telnet and dst edu-dy.cn.ntua.gr`
28. `tcpdump ip6`

Άσκηση 3: Δικτύωση Host-only

1. Host-only IPv4 : 192.168.56.1

2. DHCP Server : 192.168.56.100,
   Addresses : 192.168.56.101 - 192.168.56.254
3. Σε κάθε εικονικό μηχάνημα τρέχουμε την `dhclient em0` → λαμβάνεται αυτόματα μία διαθέσιμη διεύθυνση IPv4
4. PC1 → 192.168.56.102
   PC2 → 192.168.56.103
5. Κάνουμε ping από το ένα στο άλλο και βλέπουμε ότι απαντάει
6. Κάνουμε ping από το φιλοξενούν μηχάνημα προς ένα από τα φιλοξενούμενα (βλέπουμε ότι απαντάει)
7. `netstat -r`
8. Όχι, διότι δεν χρειάζεται default gateway στη δικτύωση host-only
9. Όχι, το host μηχάνημα δεν απαντάει στα ping
10. `hostname` → PC.ntua.lab
11. `hostname PC1` , `hostname PC2`
12. Εμφανίζεται όταν κάνουμε logout (πάνω από την προτροπή login οταν κάνουμε CTRL+D)
13. Όχι, δεν το περιέχει, επομένως αν γίνει επανεκκίνηση θα χρησιμοποιηθεί και πάλι το παλιό
14. OK, έκανα την αλλαγή στο αρχείο
15. Προσθέτουμε στο /etc/hosts σε κάθε εικονικό μηχάνημα την εγγραφή [ip] [hostname] που αντιστοιχεί στο άλλο (πχ. στο PC1 προσθέτουμε την γραμμή '192.168.56.102 PC1'
16. `ping PC1`
17. `tcpdump host PC1 -l -w log`
    `tcpdump host 192.168.56.102 -l -w log`
18. Length ; 64 bytes, TTL : 64 bytes (φαίνεται από τη γραμμή εντολών)
19. TTL : 168 bytes
20. `tcpdump icmp -vvv -l | tee dat`
21. Length : 60 bytes → η διαφορά οφείλεται στα διαφορετικά λειτουργικά συστήματα
22. TTL : 64 bytes
23. Δεν παρατηρούμε κάποια καταγραφή
24. Βλέπουμε ότι καταγράφει όλη τη κίνηση του υποδικτύου, όχι μόνο αυτή που έχει ως προορισμό το PC1

Άσκηση 4: Δικτύωση Internal

1. `ifconfig em0 inet 192.168.56.103`
2. Σταματάει η σύνδεση με τον dhclient που υπήρχε
3. OK, `tcpdump -vvv -l | tee dat`
4. Όχι, δεν απαντάει
5. Εμφανίζονται πακέτα ARP
6. Όχι, δεν μπορώ
7. Όχι, δεν παρατηρείται κάποιο πακέτο
8. Ναι, τώρα επικοινωνούν
9. Όχι, δεν μπορώ γιατί τα εικονικά μηχανήματα είναι σε Internal Networking (άρα δεν επικοινωνούν με το host μηχάνημα)
10. `tcpdump -n`

11. `arp -d -a` → Παράγονται μηνύματα ARP τα οποία υποδηλώνουν ότι το PC1 ψάχνει να βρεί πιο μηχάνημα έχει την εικονική IP διεύθυνση του φιλοξενούντος
12. Γιατί κανένα μηχάνημα δεν απαντάει στα ARP request του PC2
13. PC1 → 10.11.12.61/26 (61 → 00111101)
    PC2 → 10.11.12.62/26 (62 → 00111110)
14. Ναι, επικοινωνούν

Άσκηση 5: Δικτύωση NAT

1. `dhclient em0`
2. IPv4 : 10.0.2.15 → αποδόθηκε από την 10.0.2.2
3. `netstat -r` → Default Gateway : 10.0.2.2
4. nameserver 192.168.1.1
5. Στο αρχείο '/var/db/dhclient.leases.em0'
6. Ναι, μπορώ
7. Ναι μπορεί να επικοινωνήσει (δοκιμάζουμε μέσω εντολής ping)
8. Σε όλες εκτός της 10.0.2.1 η οποία δεν αποδίδεται κάπου.
   Η 10.0.2.2 αποδίδεται στο Default Gateway
   Η 10.0.2.3 είναι ο Proxy DNS
   Η 10.0.2.4 είναι ο TFTP Server
9. Ναι, επικοινωνεί, διότι βρίσκονται όλα σε δικτύωση NAT
10. -l : για χρήση ICMP
    -n : για εκτύπωση στη κονσόλα
    -q : για συγκεκριμένο αριθμό από queries
11. IPv4 Source : 10.0.2.15 → ICMP Echo Request
12. IPv4 Source : 192.168.1.13
13. IPv4 Source : 192.168.1.1 → 80.106.125.100 → 79.128.230.202 → 79.128.224.179 → 176.126.38.5
14. IPv4 Destination : 192.168.1.13 (Η IP του υπολογιστή μου)
15. Είναι οι ίδιες, αλλά υπάρχει και η Default Gateway : 10.0.0.2
16. Η IP του εικονικού μηχανήματος 10.0.2.15
17. Ναι, αντιστοιχούν όλα, εκτός του πρώτου
18. Θα είναι ένα λιγότερο hop καθώς το εικονικό μηχάνημα βρίσκεται σε ένα ακόμα υποδίκτυο μέσα στο host

Άσκηση 6: Δικτύωση NAT Network

1. NAT IPv4 : 10.0.2.0
2. `ifconfig em0 delete` → Διαγράφηκαν
3. `dhclient em0`
4. PC1 → 10.0.2.15
   PC2 → 10.0.2.4 (Διαφέρει από τη προηγούμενη)
5. DHCP Server : 10.0.2.3
6. 'nameserver 192.168.1.1' → DNS διευθύνσεις
7. 10.0.2.1
8. Ναί, μπορούμε

9. Ναι, μπορούμε
10. Απαντάει το Host μηχάνημα
11. Ναι επικοινωνούν καθώς η εντολή ping προς εξωτερικές διευθύνσεις είναι επιτυχής
12. Ναι επικοινωνούν (τα ping είναι επιτυχή)
13. Όχι, γιατί δεν έχουν τον ίδιο τρόπο δικτύωσης
14. Το καταλαβαίνουμε από την IP διεύθυνσή του, καθώς το NAT network καθε μηχάνημα έχει την δική του IP