Ονοματεπώνυμο: Βρεζάς Κωνσταντίνος | Όνομα PC: LAPTOP-RLR92PLC
Ομάδα: 2 | Ημερομηνία: 06/03/2023

Εργαστηριακή Άσκηση 2

Δικτύωση Συσκευών στο VirtualBox.

Άσκηση 2

2.1| ifconfig

2.2| ifconfig eth0 down
ifconfig eth0 up

2.3| man tcpdump
man pcap
man pcap-filter

2.4| tcpdump -i eth0 -n

2.5| tcpdump -i eth0 -n -A ⇝ ASCII
tcpdump -i eth0 -n -x ⇝ Hex.

2.6| tcpdump -e

2.7| tcpdump -s 68

2.8| tcpdump host 10.0.0.1 -v

2.9| tcpdump host 10.0.0.1 and 10.0.0.2 -i eth0

2.10| ~~tcpdump ip -x net 1.1.0.0/16~~ tcpdump ip -x net 1.1.0.0/16

2.11| tcpdump not net 127.0.0.1

2.12|

2.13| tcpdump ip[2:2] > 576

2.14| tcpdump ip[8] < 5

2.15|

2.16| tcpdump src 10.0.0.1 and icmp.

2.17| tcpdump dst 10.0.0.2 and tcp.

2.18| tcpdump dst port 53 and udp.

2.19| tcpdump src or dst 10.0.0.10 tcp.

2.20| tcpdump src or dst 10.0.0.10 and port 23 -w sample_captur

2.21| tcpdump tcp[tcpflags] & tcp-syn != 0

2.22| tcpdump tcp[tcpflags] & tcp-syn != 0 or tcp[tcpflags] & tcp-syn | tcp-ack != 0

2.23| tcpdump tcp[tcpflags] & tcp-fin != 0 or tcp[tcpflags] & tcp-fin | tcp-ack != 0

2.24| Υποδηλώνει από το 13ο στερό byte του tcp header τα 4 πρώτα bits, τα οποία αντιστοιχούν στο Header Length και αυτή η τιμή τα διαιρεί με το 4 ώστε να μπορεί να φιλτράρει όποια πακέτα υπήρχαν.

2.25|

2.26| tcpdump tcp port 80 -A

2.27|

2.28| tcpdump ip6.

Άσκηση 3

3.1| IPv4 Host Only Ethernet Adapter: 192.168.56.1/24

3.2| DHCP Server Address: 192.168.56.100
Lower-Upper bound: 192.168.56.101 - 192.168.56.254

3.3| Εκτέλεση την εντολή "dhclient em0" και στα 2 μηχανήματα
3.4| και έχω PC2: 192.168.56.102
PC1: 192.168.56.103

3.5| κάναμε ping από το ένα μηχάνημα στο άλλο και βλέπουμε ότι απαντάει
(PC1: ping 192.168.56.102)
(PC2: ping 192.168.56.103).

3.6| Ομοίως κάνουμε ping από το φιλοξενούν στα εικονικά και βλέπουμε ότι απαντάνε

3.7| netstat -r

3.8| Όχι, στη host-only δικτύωση δεν χρειάζεται default gateway.

3.9| Το host μηχάνημα (φιλοξενών) δεν απαντάει στα ping.

3.10| hostname ~> PC.ntua.lab.

3.11| hostname PC1
hostname PC2

3.12| Εμφανίζεται δίπλα από το είδος του λειτουργικού και πάνω από την προτροπή login.

3.13| Όχι, στο αρχείο rc.conf περιέχεται το πεδίο hostname, έτσι σε ενδεχόμενη επανεκκίνηση το hostname θα ξανά γίνει το PC.ntua.lab.

3.14| Μέσω vi rc.conf αλλάζω τα hostnames σε PC1 και PC2 αντίστοιχα.

3.15| Στο PC1 : 192.168.56.102 PC2
Στο PC2 : 192.168.56.103 PC1

3.16| Ping PC2

3.17| tcpdump -d host PC1 -l -w test
tcpdump -d host 192.168.56.103 -l -w test.

3.18| ping statistics: Length: 64 bytes
ttl = 64

3.19| ttl = 128

3.20| tcpdump icmp -vvv -l

3.21| length = 60 bytes. Η διαφορά που παρατηρούμε οφείλεται στα διαφορετικά O.S.

3.22| src: 192.168.56.102 ⇝ ttl = 128, src: 192.168.56.1 ⇝ ttl = 64.

3.23| Δεν παρατηρήσαμε καταπτώσεις πακέτων

3.24| Παρατηρούμε ότι καταπίπτονται πακέτα από όλο το υποδίκτυο, όχι μόνο όσα έχουν ως προορισμό το PC1.

Άσκηση 4|

4.1| ifconfig em0 inet "192.168.56.103" ή "192.168.56.102" για PC1 και PC2 αντίστοιχα

4.2| Χάνει η προ-υπάρχουσα σύνδεση με τον dhclient.

4.3| tcpdump -vvv -l

4.4| Όχι

4.5| Ναι, καταγράφονται πακέτα ARP

4.6| Όχι, δεν μπορώ να κάνω ping από το PC2 στο PC1

4.7| Όχι, δεν καταγράφονται πακέτα

4.8| Ναι, επικοινωνούν (ping PC1)

4.9| Όχι, δεν μπορώ καθώς τα VM's είναι σε Internal Networking, συνεπώς δεν υπάρχει επικοινωνία με το host μηχάνημα.

4.10| tcpdump -n

4.11| arp -d -a ~> Καταγράφονται μηνύματα ARP

4.12|

Άσκηση 5|

5.1| dhclient em0

5.2| Και στα 3 μηχανήματα έχει αποδοθεί η 10.0.2.15, αποδόθηκε από την 10.0.2.2

5.3| netstat -r → Default gateway: 10.0.2.2

5.4| # Generated by resolv.conf
search Home
nameserver 192.168.1.1

5.5| Στο /var/db/dhclient.leases.em0

5.6| Ναι

5.7| Ναι μπορεί να επικοινωνήσει. Το διαπιστώσαμε αυτό κάνοντας ping www.google.com.

5.8| Απάντηση από ping πήραμε σε όλες τις διευθύνσεις εκτός από την 10.0.2.1
Η 10.0.2.2 παρέχει το Default gateway
Η 10.0.2.3 ~~παρέχει~~ το name server
Η 10.0.2.4 είναι ο TFTP server

5.9| Ναι επικοινωνεί, διότι βρίσκονται και τα 3 μηχανήματα σε δικτύωση NAT

5.10| -I : Για χρήση ICMP
-n : Για εμφάνιση απλά κανονικά
-q : Για ορισμένο αριθμό από probes

5.11| Πηγή IPv4 : 10.0.2.15
Τύπος μηνύματος: ICMP Echo request.

5.12| Πηγή IPv4 : 192.168.1.102

5.13| Πηγές IPv4 : 192.168.1.1, 10.13.255.62, 185.3.220.116, 185.3.220.5
10.13.255.185, 62.169.252.250, 176.126.38.5

5.14| IPv4 Destination : 192.168.1.102

5.15| ίδιες με αυτές που καταγράφηκαν και στο wireshark αν και default gateway

5.16| Η ip του εικονικού μηχανήματος 10.0.2.15

5.17| Ναι ενώ είναι και default gateway.

5.18| Στο φιλοξενούν μηχάνημα θα είναι 9 hops ενώ στο εικονικό μηχάνημα είναι 10. Αυτό το ένα παραπάνω είναι επειδή το vm είναι σε ξεχωριστό υποδίκτυο

Άσκηση 6

6.1| NAT IPv4: 10.0.2.0

6.2| ifconfig em0 delete
rm dhclient.leases.em0

6.3| dhclient em0

6.4| PC1 ~> 10.0.2.15, ίδια με πριν
PC2 ~> 10.0.2.4, διαφορετική από πριν.

6.5| DHCP server: 10.0.2.3

6.6| # Generated by resolvconf
search Home
nameserver 192.168.1.1

6.7| netstat -r ~> 10.0.2.1

6.8| Ναι.

6.9| Ναι

6.10| Αναγράφει το host μηχάνημα (ether: 08:00:27:25:30:45) ίδια με πίνακα απ

6.11| Ναι επικοινωνούν τα μηχανήματα με το internet. Τα ping προς την www.google.com ήταν επιτυχής

6.12| Ναι επικοινωνούν

6.13| Όχι, καθώς έχουν διαφορετικό τρόπο δικτύωσης

6.14| Το διαπιστώνουμε από την απάντηση που επιστρέφει κάθε ping καθώς στη δικτύωση NAT network κάθε μηχάνημα έχει διαφορετική IP.