Ονοματεπώνυμο : Ιωάννης Μπασδέκης
Ομάδα: 3
‘Ονομα PC: DESKTOP-0BU537U
Ημερομηνία: 14/3/2023

**Μέρος 2ο**

2.1) ifconfig

2.2) ifconfig em0 down
ifconfig em0 up

2.3) man tcpdump
man pcap
man pcap-filter

2.4) tcpdump -i em0 -n

2.5) tcpdump -i em0 -X

2.6) tcpdump -i em0 -e

2.7) tcpdump -i em0 -s 68

2.8) tcpdump -i em0 -v ‘ip and src or dst 10.0.0.1’

2.9) tcpdump -i em0 ‘src or dst(10.0.0.1 or 10.0.0.2)’

2.10) tcpdump -i em0 -X ‘ip and net 1.1.0.0/16’

2.11) tcpdump -i em0 -XX ‘ip and dst net 192.168.1.0/24’

2.12) tcpdump -i em0 ‘ip broadcast’

2.13) tcpdump -i em0 ‘ip and greater 576’

2.14) tcpdump -i em0 ‘ip and ip[8] < 5’

2.15) tcpdump -i em0 ‘ip and ip[0] & 0xf !=5’

2.16) tcpdump -i em0 ‘icmp and src 10.0.0.1’

2.17) tcpdump -i em0 ‘tcp and dst 10.0.0.2’

2.18) tcpdump -i em0 ‘udp and dst port 53’

2.19) tcpdump -i em0 ‘tcp and (src or dst 10.0.0.10)’

2.20) tcpdump -i em0 -w sample_capture ‘tcp and (src or dst 10.0.0.10) and dst port 23’

2.21) tcpdump -i em0 ‘tcp and tcp[tcpflags]&tcp-syn!=0’

2.22) tcpdump -i em0 ‘tcp and tcp[13]=2 or tcp[13]=12’

2.23) tcpdump -i em0 ‘tcp and ((tcp[tcoflags]&tcp-fin !=0) or (tcp[tcpflags]&(tcp-fin|tcp-ack)) !=0 )’

2.24) Δίνει το 13ο σε σειρα byte στο tcp header και συγκεκριμένα τα 4 πρώτα που είναι το data offset(μηδενίζουμε τα άλλα). Με το right shift 2 ( >>2) βρίσκουμε σε bytes το μέγεθος του  tcp header

2.25) tcpdump -i em0 ‘tcp and (tcp[12:1] & 0xf0 >> 2) >20’

2.26) tcpdump -i em0 -A ‘src or dst port 80’

2.27) tcpdump -i em0 ‘dst host edu-dy.cn.ntua.gr and port telnet’

2.28) tcpdump -i em0 ‘ip6’

**Μέρος 3ο**

3.1) 192.168.56.1

3.2) 192.168.56.100
Lower bound: 192.168.56.101
Upper bound: 192.168.56.254

3.3) dhclient em0

3.4)PC1 -> 192.168.56.102
PC2 -> 192.168.56.103

3.5) Με ping

3.6) Με ping

3.7) netstat -r

3.8) Όχι γιατι με αυτήν την δικτύωση δεν υπάρχει gateway

3.9) Όχι γιατι δεν επικοινωνει με την φυσική διευθυνση με τα virtual μηχανήματα αλλά με την εικονική (είναι δηλαδή σε διαφορετικό δίκτυο)

3.10) hostname PC.ntua.lab

3.11) hostname PC1
hostname PC2

3.12) Πάνω απο το prompt του login φαίνεται το νέο όνομα

3.13) Όχι και αν κάνω επανεκκίνηση θα έχει το παλίο όνομα (PC.ntua.lab) δηλαδή αυτό που έχει στο αρχείο

3.14)-

3.15)Για το PC1 θα πρέπει να προσθέσουμε την γραμμή 192.168.56.103 PC2
Το αντίστοιχο για το PC2

3.16)ping PC2

3.17)tcpdump -i em0 -l ‘src or dst PC1’ | tee test
tcpdump -i em0 -l ‘src or dst 192.168.56.102’ | tee test

3.18) 64 bytes TTL=64

3.19) TTL = 128

3.20) tcpdump -i em0 -vvv icmp

3.21)40 bytes . Διαφορετικό λειτουργικό σύστημα
3.22) TTL=64 συμφωνεί

3.23) Δεν παρατήρησα καταγραφή

3.24) Παρατηρώ όλη την κίνηση στο υποδίκτυο(και τα arp)

**Μέρος 4ο**

4.1) PC2:  ifconfig em0 192.168.56.103
PC1:  ifconfig em0 192.168.56.102

4.2) Δεν εμφανίστηκε κάποιο μήνυμα

4.3) tcpdump -i em0 -vvv

4.4) όχι

4.5) Ναι κίνηση ARP

4.6) Όχι

4.7) Όχι

4.8) Ναι

4.9) Όχι γιατι τα virtual machines βρίσκονται σε Interal network και δεν επικοινωνούν με το host

4.10) tcpdump -i em0 -n

4.11) arp -d -a
Παράγονται ARP request . Το PC2 ψάχνει να βρει το 192.168.56.1

4.12) Ενώ υπάρχει η διαδρομή το host δεν απαντάει

4.13) PC2:  ifconfig em0 10.11.12.63
PC1:  ifconfig em0 10.11.12.62

4.14) όχι

**Μέρος 5ο**

5.1) dhclient em0

5.2) 10.0.2.15 from 10.0.2.2

5.3) 10.0.2.2 (netstat -r)

5.4)# Generated by resolvconf

nameserver 1.1.1.1
nameserver 1.0.0.1

5.5) /var/db/dhclient.leases.em0

5.6) Ναι

5.7) Ναι δοκιμάζουμε με το ping 1.1.1.1 . Εξάλλου στην NAT δικτύωση μπορούμε να ξεκινήσουμε συνδέσεις προς το διαδίκτυο(δεν μπορούμε να δεχτούμε)

5.8) Σε όλες εκτός της 10.0.2.1 η οποία δεν αποδίδεται κάπου.
10.0.2.2 -> Default Gateway
10.0.2.3 -> DNS
10.0.2.4 -> TFTP Server

5.9) Όχι γιατί βρίσκονται σε NAT δικτύωση και κάθε μηχάνημα νομίζει ότι είναι μόνο του στο δίκτυο

5.10) -I : ICMP
-n : να μην γίνει resolve των ονομάτων
-q 1 :  ορίζει το πλήθος των προσπαθειών ανα hop σε 1
1.1.1.1 :  destination

5.11) 10.0.2.15 → 1.1.1.1 ICMP Echo request

5.12) 192.168.1.2 → 1.1.1.1 Echo (ping) request

5.13) 192.168.1.1
80.106.125.100
79.128.230.202
79.128.224.179
176.126.38.5

5.14) 192.168.1.2

5.15) Οι ίδιες

5.16) 10.0.2.15

5.17) Ναι

5.18) Λόγω του NAT για εξωτερικά δίκτυα ότι request κάνουν τα VMs φαίνεται ότι έγιναν απο τον υπολογιστή μας οπότε θα είναι το ίδιο

**Μέρος 6ο**

6.1) 10.0.2.0 (αφου το prefix είναι 10.0.2.0/24)

6.2) ifconfig em0 delete

6.3) dhclient em0

6.4) PC1 → 10.0.2.15 (ίδια)
PC2 → 10.0.2.4 (άλλαξε)

6.5) 10.0.2.3

6.6) # Generated by resolvconf

nameserver 1.1.1.1
nameserver 1.0.0.1

6.7) 10.0.2.1

6.8) Ναι

6.9) Ναι

6.10) Ναι , απαντά ο host

6.11) Ναι αφού είναι σε NAT δίκτυο

6.12) Ναι, αφου βρίσκονται στο ίδιο internal network

6.13) Όχι. Δεν βρίσκεται στο ίδιο internal network.

6.14) Θα απαντά ο TFTP server. Το καταλαβαίνουμε απο τις ip διευθύνσεις καθώς στο NAT network έχουν διαφορετικές κάθε μηχάνημα