Ονοματεπώνυμο: Παναγιώτης Ζευγολατάκος	**Όνομα PC:** panos-PC
Ομάδα: 1	**Ημερομηνία:** 26/02/2021

Εργαστηριακή Άσκηση 2

Δικτύωση συστημάτων στο VirtualBox

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

2

2.1 ifconfig

2.2 ifconfig em0 down

ifconfig em0 up

2.3 man tcpdump

man pcap (στο manual αυτό βρίσκουμε και το pcap-filter, εφόσον δεν έχει δικό του manual entry)

2.4 tcpdump -i em0 -n

2.5 tcpdump -i em0 -XX

2.6 tcpdump -i em0 -e -XX

2.7 tcpdump -i em0 -s 68 -e -XX

2.8 tcpdump -v 10.0.0.1

2.9 tcpdump -i em0 '(src 10.0.0.1 and dst 10.0.0.2)' or '(dst 10.0.0.1 and src 10.0.0.2)'

2.10 tcpdump ip and net 1.1.0.0/16

2.11 tcpdump -e ip and not net 192.168.1.0/24

2.12 tcpdump ip and broadcast

2.13 tcpdump ip and greater 576

2.14 tcpdump ip and 'ip[8]<5'

2.15 tcpdump ip and '((ip[0]&0x0f)>5)'

2.16 tcpdump icmp and src 10.0.0.1

2.17 tcpdump tcp and dst 10.0.0.2

2.18 tcpdump udp and dst port 53

2.19 tcpdump tcp and host 10.0.0.10

2.20 tcpdump -w sample_capture tcp and host 10.0.0.10 and dst port 23

2.21 tcpdump '(tcp[tcpflags] & tcp-syn)!=0'

2.22 tcpdump -c 2 '(tcp[tcpflags] & (tcp-syn|tcp-ack))!=0'

2.23 tcpdump '(tcp[tcpflags] & tcp-fin)!=0'

2.24 Με το κομμάτι tcp[12:1] επιλέγουμε 1 byte από το TCP Segment με offset 12, δηλαδή το byte που περιέχει το πεδίο Data Offset (4 bits) και του εφαρμόζουμε μάσκα για να κρατήσουμε τα πρώτα 4 bit του octet (δηλαδή μόνο το πεδίο Data Offset). Στη συνέχεια το κάνουμε shift right 2, δηλαδή το διαιρούμε με το 4 (εφόσον είναι ήδη ολισθημένο κατά 4, άρα ουσιαστικά το πολλαπλασιάζουμε με το 4), για να μπορέσουμε να βρούμε το μέγεθος της επικεφαλίδας tcp σε bytes.

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

2.26 tcpdump tcp and port 80

2.27 tcpdump tcp and port 23 and dst edu-dy.cn.ntua.gr

2.28 tcpdump ip6

3

3.1 192.168.56.1

3.2 DHCP IPv4:192.168.56.100

Range:192.168.56.101 – 192.168.56.254

3.3 dhclient em0 και στα 2 μηχανήματα

3.4 PC1: 192.168.56.104

PC2: 192.168.56.103

3.5 Θα κάνω ping από το ένα μηχάνημα στο άλλο, πχ. Από το PC1: ping 192.168.56.103 (έχοντας εκτελέσει την εντολή tcpdump στο μηχάνημα PC2)

3.6 Θα κάνω ping από το μηχάνημά μου σε ένα από τα δύο VM, πχ. Από cmd στο PC2: ping 192.168.56.103 (έχοντας εκτελέσει την εντολή tcpdump στο μηχάνημα PC2)

3.7 netstat -nr

3.8 Χρησιμοποιώ την εντολή netstat -r για να δούμε τα περιεχόμενα των routing tables και παρατηρώ πως δεν υπάρχει προεπιλεγμένη πύλη στη συγκεκριμένη κατάσταση δικτύωσης.

3.9 Όχι, δεν μπορώ, εφόσον δεν υπάρχει gateway για το φιλοξενούν μηχάνημα (το οποίο το βλέπουμε από το routing table). Χρησιμοποίησα την εντολή ping προς την IPv4 διεύθυνση του φιλοξενούντος μηχανήματος:

```
root@PC:~ # ping 192.168.2.17
PING 192.168.2.17 (192.168.2.17): 56 data bytes
ping: sendto: No route to host
ping: sendto: No route to host
ping: sendto: No route to host
ping: sendto: No route to host
^C
--- 192.168.2.17 ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
```

3.10 Χρησιμοποιώ την εντολή ‘hostname’ και λαμβάνω την απάντηση ‘PC.ntua.lab’.

3.11 hostname PC1

hostname PC2

3.12 Εμφανίζεται στο prompt: root@PC2:

3.13 Όχι, το όνομα είναι “PC.ntua.lab”

3.14 Και στα δύο μηχανήματα κάνω edit το αρχείο /etc/rc.conf και θέτω:

hostname=”PC1.ntua.lab” και

hostname=”PC2.ntua.lab”

3.15 Προσθέτω στα αρχεία του καθενός:

PC1: “192.168.56.103 PC2”

PC2: “192.168.56.104 PC1”

3.16 ping PC1 (από το μηχάνημα PC2)

3.17 tcpdump -l icmp and host PC1 | tee test

tcpdump -l icmp and host PC1 > test & tail -f test

3.18 Το μήκος των ICMP πακέτων που λαμβάνει το PC1 είναι 64 bytes και η τιμή του πεδίου TTL είναι 64.

3.19 Η τιμή του πεδίου TTL είναι 128.

3.20 tcpdump -e -XX -vvv icmp | tee 3_2

3.21 Το μήκος των πακέτων είναι 40 bytes εφόσον τα παράγουν τα Windows

3.22 TTL = 64 και παρατηρώ πως είναι το ίδιο με πριν.

3.23 Όχι δεν παρατήρησα

3.24 Παρατηρώ πως εμφανίζεται η κίνηση που έγινε με το ping, εφόσον επιτρέψαμε πρόσβαση και στα άλλα εικονικά μηχανήματα (το promiscuous mode επιτρέπει να παραδίδεται στην κάρτα δικτύου και η κίνηση που αφορά και άλλα VMs του ίδιου δικτύου).

4

4.1 ifconfig em0 192.168.56.104/24

ifconfig em0 192.168.56.103/24

4.2 Σημαίνει πως εφόσον θα χρησιμοποιηθεί μια στατική διεύθυνση IPv4 παύει να χρησιμοποιείται το DHCP (ή το BOOTP), όντας δυναμικά πρωτόκολλα.

```
ifconfig em0 192.168.56.104/24
root@PC:/etc # Mar  3 22:06:05 PC dhclient[684]: My address (192.168.56.104) was
 deleted, dhclient exiting
Mar  3 22:06:05 PC dhclient[669]: connection closed
Mar  3 22:06:05 PC dhclient[669]: exiting.
```

4.3 tcpdump -e -XX -vvv

4.4 Ναι

4.5 Όχι

4.6 Όχι

4.7 Όχι

4.8 Ναι

4.9 Όχι, εφόσον δημιουργείται ένα εσωτερικό δίκτυο μεταξύ των δύο, πλήρως απομονωμένο από το φιλοξενούν μηχάνημα.

4.10 tcpdump -n

4.11 Στο PC1 παρατηρώ πως το PC2 έχει κάνει ARP Requests για να δει σε ποιον ανήκει η διεύθυνση του φιλοξενούντος μηχανήματος.

4.12 Εφόσον δεν έλαβε κάποια απόκριση θεωρεί πως ο host είναι απενεργοποιημένος.

4.13 ifconfig em0 10.11.12.61/26

ifconfig em0 10.11.12.62/26

4.14 Ναι

5

5.1 dhclient em0

5.2 Έχουν λάβει τη διεύθυνση IPv4 10.0.2.15 η οποία αποδόθηκε από την IPv4 10.0.2.2

5.3 netstat -nr

```
Internet:
Destination        Gateway            Flags     Netif Expire
default            10.0.2.2           UGS         em0
```

5.4

```
root@PC:~ # cat /etc/resolv.conf
# Generated by resolvconf
nameserver 192.168.2.1
```

5.5 Στο αρχείο /var/db/dhclient.leases.em0

5.6 Ναι

5.7 Ναι (ping google.com)

5.8 Λαμβάνω απάντηση από τις διευθύνσεις 10.0.2.2 (προκαθορισμένη πύλη), 10.0.2.3 (DNS) και 10.0.2.4 (TFTP Server)

5.9 Δεν επικοινωνεί, εφόσον με τη χρήση NAT, κάθε φιλοξενούμενο μηχάνημα έχει την εντύπωση ότι βρίσκεται στο δικό του ξεχωριστό δίκτυο (για αυτόν το λόγο παίρνουν και την ίδια διεύθυνση IPv4)

5.10 -I: ICMP

-n: μη επίλυση διευθύνσεων

-q 1: 1 probe packet ανά hop

5.11 Η πηγή είναι η 10.0.2.15 και ο τύπος των μηνυμάτων ICMP echo request

5.12 192.168.2.17 (η διεύθυνση του φιλοξενούντος)

5.13 192.168.2.1

62.38.0.170

62.38.28.109

62.38.37.81

62.38.96.150

176.126.38.5

5.14 192.168.2. 17 (η διεύθυνση του φιλοξενούντος)

5.15 10.0.2.2

192.168.2.1

62.38.0.170

62.38.28.109

62.38.37.81

62.38.96.150

176.126.38.5

5.16 10.0.2.15

5.17 Ναι (με εξαίρεση την προκαθορισμένη πύλη στην καταγραφή με την εντολή tcpdump)

5.18 Το πλήθος των αναπηδήσεων που προκύπτει από το φιλοξενούν μηχάνημα είναι κατά ένα λιγότερο από την εικονική μηχανή, μιας και αυτή απέχει ένα hop από αυτό (το φιλοξενούν μηχάνημα).

```
C:\Users\panos>tracert -d 1.1.1.1

Tracing route to 1.1.1.1 over a maximum of 30 hops

  1     1 ms    <1 ms    <1 ms  192.168.2.1
  2     8 ms    10 ms     8 ms  62.38.0.170
  3    10 ms     9 ms     9 ms  62.38.28.109
  4     9 ms    10 ms    10 ms  62.38.37.81
  5    10 ms    10 ms     9 ms  62.38.96.150
  6    10 ms    10 ms    10 ms  176.126.38.5
  7     9 ms     9 ms     9 ms  1.1.1.1

Trace complete.
```

6

6.1 10.0.2.0/24

6.2 ifconfig em0 10.0.2.15 delete

rm /var/db/dhclient.leases.em0

6.3 dhclient em0

6.4 Δόθηκαν οι 10.0.2.4 (PC2) και 10.0.2.5 (PC1) – δε διαφέρουν

6.5 10.0.2.3

6.6

```
root@PC1:~ # cat /etc/resolv.conf
# Generated by resolvconf
nameserver 192.168.2.1
```

6.7

```
root@PC1:~ # netstat -nr
Routing tables

Internet:
Destination        Gateway            Flags     Netif Expire
default            10.0.2.1           UGS         em0
10.0.2.0/24        link#1             U           em0
10.0.2.5           link#1             UHS         lo0
127.0.0.1          link#2             UH          lo0
```

6.8 Ναι

6.9 Ναι

6.10 Απαντάει το φιλοξενούν μηχάνημα (οι διευθύνσεις 10.0.2.1 (προκαθορισμένη πύλη) και 10.0.2.2 αντιστοιχούν στο ίδιο μηχάνημα).

6.11 Ναι (ping google.com)

6.12 Ναι (ping 10.0.2.5 από το PC2)

6.13 Όχι (ping 10.0.2.4 και ping 10.0.2.5 από το PC3), εφόσον το PC3 δε βρίσκεται στο ίδιο NAT Network με τις άλλες 2 εικονικές μηχανές.

6.14 Εκτελώντας την εντολή tcpdump στα PC1, PC2 και κάνοντας ping σε αυτά από το PC3, βλέπουμε πως δε λαμβάνουν κάποιο πακέτο, επομένως αν ληφθεί κάποια απάντηση δε θα είναι από τα μηχανήματα αυτά.