| Ονοματεπώνυμο: Μοίρας Αλέξανδρος | Όνομα PC:LAPTOP-5A8R1JQR |
|---|---|
| Ομάδα: 3 | Ημερομηνία: 9/3/2022 |

# 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, 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 -vvv ip and host 10.0.0.1

2.9 tcpdump -i em0 host 10.0.0.1 and host 10.0.0.2

2.10 tcpdump -x ip and net 1.1.0.0/16

2.11 tcpdump -ex ip and tcpnet not 192.168.1.0/24

2.12 tcpdump ip and broadcast

2.13 tcpdump ip and ‘len>576’

2.14 tcpdump ip and ‘ip[8]<5’

2.15 tcpdump ip and ‘ip[0]>4*16+5’ (Version=4 Και header length > 5 που ισοδυναμει με επικεφαλίδα των 20 bytes)

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 src or dst 10.0.0.10

2.20 tcpdump -w sample_capture tcp and src or dst 10.0.0.10 and src or dst port 23

2.21 tcpdump tcp and ‘tcp[13]==2’ (Από το Byte των flags ενεργή μόνο η σημαία SYN)

2.22 tcpdump tcp and ‘tcp[13]&2!=0 or (tcp[13]&16!=0 and tcp[13]&2!=0)’

2.23 tcpdump tcp and ‘tcp[13]&1 != 0’

2.24 Υπολογίζει το μέγεθος της επικεφαλίδας TCP σε Bytes που βρίσκεται στα πρώτα 4 Bits του Byte 12 της επικεφαλίδας TCP εκφρασμένο σε λέξεις των 32 Bits (4 bytes)

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

2.26 tcpdump tcp port 80

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

2.28 tcpdump ip6

**3.**

3.1 192.168.56.1

3.2 Η διεύθυνση του εξυπηρετητή DHCP είναι 192.168.56.100 και η περιοχή διευθύνσεων που μπορεί να εκχωρήσει είναι οι διευθύνσεις από 192.168.56.101 εως 192.168.56.254.

3.3 Αποδώσαμε εκτελώντας dhclient em0 και στα 2 μηχανήματα.

3.4 Είναι οι 192.168.56.102 στο PC1 και 192.168.56.103 στο PC2.

3.5 Εκτελώντας από το PC1 ping -c 3 192.168.56.103 και ελέγχοντας ότι το PC2 αποκρίνεται και λαμβάνουμε πίσω 3 πακέτα και αντίστροφα.

3.6 Εκτελώντας από το τερματικό του ping προς τα δύο φιλοξενούμενα μηχανήματα με ping 192.168.56.102 ή 192.168.56.103 αντίστοιχα και ελέγχοντας ότι αποκρίνονται.

3.7 netstat -r -n | grep default.

3.8 Όχι δεν υπάρχει προεπιλεγμένη πύλη στη συγκεκριμένη κατάσταση δικτύωσης, καθώς δεν παρατηρούμε default διαδρομή στο routing table που εκτυπώνουμε με netstat -r -n. Δεν έχει οριστεί προκαθορισμένη πύλη καθώς στον τρόπο δικτύωσης Host-only εξωτερικά συστήματα δεν μπορούν να επικοινωνήσουν με τα εσωτερικά και δεν έχει νόημα η κίνηση να προωθείται προς ένα default gateway.

3.9 Όχι δεν μπορούμε καθώς το φιλοξενούν σύστημα συμμετέχει στο δίκτυο με μια εικονική κάρτα δικτύου, ενώ η φυσική του δε συμμετέχει σε αυτό και είναι εξωτερική στο σύστημα.

3.10 PC.ntua.lab (εντολή hostname)

3.11 hostname PC1, hostname PC2

3.12 Εμφανίζεται στο Prompt για εντολή του συστήματος (πχ root@PC2:~#)

3.13 Όχι δεν το περιέχει, αντιθέτως περιέχει το παλιό όνομα (cat /etc/rc.conf). Σε ενδεχόμενη επανεκκίνηση του PC1 το όνομά του θα ξαναγίνει PC.ntua.lab, καθώς θα ανακτηθεί από το αρχείο /etc/rc.conf.

3.14 Με vi /etc/rc.conf ανοίγουμε το αρχείο /etc/rc.conf για επεξεργασία και διορθώνουμε το όνομά του PC και για τα δύο μηχανήματα.

3.15 Θα πρέπει στο αρχείο /etc/hosts κάθε μηχανήματος να προσθέσουμε εγγραφή για την IPv4 διευθύνση του άλλου μηχανήματος, η οποία θα αντιστοιχίζει την IPv4 του άλλου με το όνομά του. Πχ:

```
::1                     localhost localhost.my.domain
127.0.0.1               localhost localhost.my.domain
192.168.56.103          PC2
```

3.16 ping -c 3 localhost

3.17 tcpdump -v -l icmp and host 192.168.56.102 | tee test

tcpdump -v -l icmp and host 192.168.56.102 > test & tail -f test

3.18 Το μήκος τους είναι 64 bytes και η τιμή του TTL των αντίστοιχων πακέτων IPv4 είναι 64.

3.19 Η τιμή του πεδίου TTL της απάντησης τώρα είναι 128. Το TTL της απάντησης εξαρτάται από το λειτουργικό σύστημα που κατασκευάζει την απάντηση.

3.20 tcpdump -e -vvv icmp

3.21 Το μήκος των μηνυμάτων ICMP που παράγει το φιλοξενούν μηχάνημα είναι 40 bytes. Η

διαφορά οφείλεται στο γεγονός ότι τα windows κατά το Ping στέλνουν μηνύματα ICMP με δεδομένα 32 Bytes οπότε μαζί με τα 8 bytes της επικεφαλίδας το μήκος τους είναι 40 Bytes, ενώ το Unix-based FreeBSD στέλνει μηνύματα με δεδομένα 56 bytes και μαζί με την επικεφαλίδα το μήκος των πακέτων διαμορφώνεται σε 64 bytes.

3.22 Το TTL των requests που έρχονται από το φιλοξενούν μηχάνημα στο PC2 είναι 128, ενώ το TTL των απαντήσεων από το PC2 στο φιλοξενούν είναι 64. Οι τιμές συμφωνούν με αυτές που βρήκαμε προηγουμένως.

3.23 Όχι δεν παρατηρήσαμε

3.24 Τώρα μπορούμε να δούμε τα πακέτα ICMP echo request και reply που αφορούν το PC2, αφού επιτρέπουμε στην κάρτα δικτύου του PC1 να συλλαμβάνει κίνηση που αφορά το PC2 που αποτελεί άλλο VM του ίδιου δικτύου.

**4**

4.1 Για το PC1 ifconfig em0 add 192.168.56.102 netmask 255.255.255.0 και για το PC2 ifconfig em0 add 192.168.56.103 netmask 255.255.255.0

4.2 Σημαίνει ότι κλείνει η υπηρεσία dhclient καθώς διαγράψαμε τη διεύθυνση που είχε αναθέσει και την αντικαταστήσαμε με μία στατική, οπότε πλέον δεν έχει λόγο να εκτελείται για να ανανεώνει πχ το δάνειο.

4.3 tcpdump -v src port not 54915 (Αυτό το Port έκανε spam arp requests και χαλούσε την καταγραφή).

4.4 Όχι δεν μπορούμε καθώς το PC2 ρυθμισμένο σε internal network δεν επικοινωνεί με το φιλοξενούν μηχάνημα. Ping 192.168.56.103

4.5 Ναι παρατηρούμε μηνύματα ARP για τη διεύθυνση του PC2 (είχαμε κάνει restart το φιλοξενούν μηχάνημα οπότε είχε διαγραφεί το ARP table που είχε δημιουργηθεί από προηγούμενα ερωτήματα).

4.6 ping -c 4 PC1. Όχι δεν μπορούμε.

4.7 Όχι δεν παρατηρούμε. Τα μηνύματα του PC2 δεν φτάνουν ποτέ στο PC1

4.8 Ναι τώρα τα δύο μηχανήματα επικοινωνούν αφού βρίσκονται στο ίδιο εσωτερικό δίκτυο. ping PC2 από το PC1.

4.9 Όχι δεν μπορούμε (Από το φιλοξενούν ping 192.168.56.102 και ping 192.168.56.103). Όπως εξηγήθηκε παραπάνω σε αυτόν τον τρόπο δικτύωσης το φιλοξενούν μηχάνημα δε συμμετέχει στο δίκτυο, με αποτέλεσμα να μην επικοινωνεί με τα εικονικά μηχανήματα.

4.10 tcpdump -n

4.11 arp -d -a. ping -c 4 192.168.56.1. Το PC2 παράγει πακέτα ARP Broadcast αναζητώντας τη φυσική διεύθυνση του φιλοξενούντος μηχανήματος.

4.12 Εφόσον το PC2 δεν επικοινωνεί με το φιλοξενούν μηχάνημα, αυτό δεν απαντά στα ARP requests του, με αποτέλεσμα το PC2 να υποθέτει ότι το μηχάνημα που προσπαθεί να κάνει ping δε λειτουργεί.

4.13 Οι δύο τελευταίες διαθέσιμες διευθύνσεις αυτού του υποδικτύου θα είναι οι 10.11.12.61 και 10.11.12.62 καθώς η 10.11.12.63 θα αποτελεί τη διεύθυνση εκπομπής του υποδικτύου.

Στο PC1 εκτελούμε: ifconfig em0 add 10.11.12.61 netmask 255.255.255.192

Και στο PC2: ifconfig em0 add 10.11.12.62 netmask 255.255.255.192

4.14 Ναι επικοινωνούν κανονικά (PC1: ping -c 4 10.11.12.62, PC2: ping -c 4 10.11.12.61)

***5***

5.1 dhclient em0

5.2 Έχουν λάβει όλοι τη διεύθυνση 10.0.2.15 η οποία τους αποδόθηκε από τον 10.0.2.2.

5.3 Η προεπιλεγμένη πύλη στον πίνακα δρομολόγησης είναι η 10.0.2.2. (netstat -rn)

5.4 Περιέχει λίστα για αναζήτηση ονομάτων host, στη συγκεκριμένη περίπτωση το search domain home και τις διεύθυνσεις IP των nameservers που θα χρησιμοποιεί για την επίλυση ονομάτων η οποία στην συγκεκριμένη περίπτωση είναι μία και είναι η 192.168.1.1.

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

5.6 Ναι μπορούμε.

5.7 Ναι επικοινωνεί με το διαδίκτυο. Η κίνηση από το φιλοξενούμενο μηχάνημα προς το διαδίκτυο στέλνεται μέσω της πύλης με τις διευθύνσεις IPv4 να μεταφράζονται ώστε να φαίνεται ότι η κίνηση ξεκινά από το φιλοξενούν μηχάνημα, ενώ τα πακέτα που προκύπτουν ως απάντηση επιστρέφονται στο φιλοξενούμενο μηχάνημα σαν να προέρχονταν από το διαδίκτυο. Χωρίς Port Forwarding δεν είναι δυνατή η επικοινωνία από το διαδίκτυο προς το φιλοξενούμενο μηχάνημα.

5.8 Λαμβάνουμε απάντηση στις εξής διευθύνσεις:

10.0.2.2: Παριστάνει το default gateway και τον DHCP Server.

10.0.2.3: Παριστάνει τον proxy DNS Server

10.0.2.4: Παριστάνει έναν εξυπηρετητή tftp για εκκίνηση του φιλοξενούμενου μηχανήματος από το δίκτυο.

5.9 Όχι δεν επικοινωνεί καθώς τα εικονικά μηχανήματα βρίσκονται σε ξεχωριστά εικονικά δίκτυα.

5.10 -I: Χρήση ICMP ECHO αντί για δεδομενογράμματα UDP. -n: Εκτύπωση αριθμητικών διευθύνσεων για τα hops αντί για μετάφρασή τους σε ονόματα. -q 1: Αποστολή ενός πακέτου (probe) ανά hop.

5.11 Η διεύθυνση πηγής είναι η 10.0.2.15 και ο τύπος των μηνυμάτων που παράγει η traceroute είναι ICMP Echo Request. (tcpdump -n -w data icmp, tcpdump -n -r data)
5.12 Η διεύθυνση IPv4 πηγής των αντίστοιχων μηνυμάτων ICMP όπως αυτά εμφανίζονται στην καταγραφή του wireshark είναι 147.102.237.116 δηλαδή η IPv4 της φυσικής κάρτας δικτύου του υπολογιστή.

5.13 147.102.236.200

62.217.96.168

176.126.38.5

5.14 Η διεύθυνση προορισμού των μηνυμάτων αυτών είναι η 147.102.237.116

5.15 10.0.2.2

147.102.236.200

62.217.96.168

176.126.38.5

5.16 Η διεύθυνση προορισμού των μηνυμάτων αυτών είναι η 10.0.2.15

5.17 Όχι υπάρχει ένα παραπάνω στην καταγραφή του tcpdump από το εικονικό μηχάνημα, αυτό που αντιστοιχεί στο hop από το εικονικό μηχάνημα στο default gateway που παρέχεται από το φιλοξενούν.

5.18 Το πλήθος των hops θα είναι 4 ενώ στο εικονικό μηχάνημα η Traceroute εμφάνισε 5 hops. Όπως εξηγήθηκε παραπάνω αυτό το έξτρα Hop αντιστοιχεί στο Hop από το εικονικό μηχάνημα στο default gateway Που παρέχεται από το φιλοξενούν μηχάνημα.

## *6*

6.1 10.0.2.0/24

6.2 ifconfig em0 delete, rm /var/db/dhclient.leases.em0

6.3 dhclient em0.

6.4 Αποδόθηκαν οι 10.0.2.4 kai 10.0.2.15. Η μία διαφέρει από την 10.0.2.15 που είχαν προηγουμένων τα PC1, PC2.

6.5 10.0.2.3

6.6 Περιέχει λίστα για αναζήτηση ονομάτων host, στη συγκεκριμένη περίπτωση το search domain ntua.gr και τις διεύθυνσεις IP των nameservers που θα χρησιμοποιεί για την επίλυση ονομάτων η οποία στην συγκεκριμένη περίπτωση είναι μία και είναι η 147.102.224.243.

6.7 10.0.2.1

6.8 Ναι μπορούμε

6.9 Ναι μπορούμε.

6.10 Ναι μπορούμε. Απαντά το φυσικό μηχάνημα.

6.11 Ναι επικοινωνούν μέσω του default gateway χρησιμοποιώντας TCP και UDP πάνω από IPv4 και IPv6 αλλά συστήματα του διαδικτύου δεν μπορούν να έχουν άμεση πρόσβαση εντός του δικτύου NAT.

6.12 Ναι επικοινωνούν.

6.13 Όχι δεν μπορούμε.

6.14 Όχι δεν είναι το αντίστοιχο PC. Στην περίπτωση που κάνουμε ping το 10.0.2.4 απαντά ο tftp server του NAT ενώ αν κάνουμε ping το 10.0.2.15 απαντά ο ίδιος ο υπολογιστής μας. Για να το διαπιστώσουμε μπορούμε να ξεκινήσουμε μία καταγραφή στα αντίστοιχα PC που κάνουμε ping κάθε φορά και θα παρατηρήσουμε ότι δεν καταγράφουν κανένα πακέτο.