Ονοματεπώνυμο: Πυλιώτης Αθανάσιος	**Όνομα PC:** DESKTOP-5DLG3IF
Ομάδα: 1	**Ημερομηνία:** 07/03/23

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 → δείχνει κάρτες δικτύου και κατάσταση.

2.2 #ifconfig em0 down → #ifconfig em0 up

2.3 #man → pcap-filter και tcpdump και pcap και ψάχνουμε το tcpdump.pcap (ή man 3PCAP)

2.4 #tcpdump -v -i em0 -n

-v → το κάνει ανθρωπίνως αναγνώσιμο, -i για interface em0, -n για ναμ ην γίνεται επίλυση IP διευθύνσεων.

2.5 #tcpdump -v -i em0 -XX

-XX → ASCII and HEX

2.6 #tcpdump -v -i em0 -e

-e → Ethernet

2.7 Διαβάζει τα πρώτα 68 bytes: #tcpdump -v -i em0 -s 68 -n -e

2.8 #tcpdump -v -i em0 ip 'host 10.0.0.1'

2.9 #tcpdump -v -i em0 ip 'host 10.0.0.1 and host 10.0.0.2'

2.10 #tcpdump -v -i em0 ip 'dst net 1.1.0.0/16' -X

Το περιεχόμενο εμφανίζεται σε ASCII και HEX.

2.11 #tcpdump -v -i em0 'not net 192.168.1.0/24' -eX

2.12 #tcpdump -v -i em0 ip 'broadcast'

2.13 #tcpdump -v -i em0 ip 'ip[2:2] > 576'

2.14 #tcpdump -v -i em0 ip 'ip[8]<5'

2.15 #tcpdump -v -i em0 ip 'ip[0] & 0xf != 5'

2.16 #tcpdump -v -i em0 'icmp and src 10.0.0.1'

2.17 #tcpdump -v -i em0 'tcp and dst 10.0.0.2'

2.18 #tcpdump -v -i em0 'udp and port 53' ή tcpdump udp and dst port 53

2.19 #tcpdump -v -i em0 'tcp and host 10.0.0.10'

2.20 #tcpdump -v -i em0 '(tcp and host 10.0.0.10) and dst port 23' -w sample_capture

2.21 #tcpdump -v -i em0 'tcp[tcpflags] and tcp-syn!=0'

2.22 #tcpdump -v -i em0 tcp and '(tcp[tcpflags] == tcp-syn) or (tcp[tcpflags] == (tcp-syn + tcp-ack))'

2.23 #tcpdump -v -i em0 'tcp[tcpflags] & tcp-fin != 0'

2.24 tcp[12:1] → Παίρνει αρχικά την τιμή του byte με offset of 12 και πρακτικά παίρνει το “data offset” από το header. Στη συνέχεια, η προσθήκη του & 0xf0 κάνει and 0xf0 και πρακτικά απλά μηδενίζει τα τελευταία 4 bits και διατηρεί τα υπόλοιπα και η προσθήκη του >> 2 το μετακινεί δεξιά κατά 2 bytes. Συνεπώς παίρνουμε το πρώτο μισό του 13^{ου} byte από το TCP Header και το κάνουμε shift δεξιά κατά 2 bit.

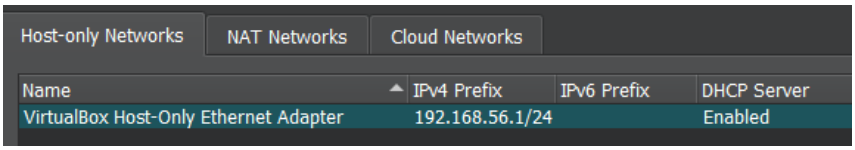
2.25 #tcpdump -v -i em0 ‘tcp and ((tcp[12:1] & 0xf0 >> 2) > 20)’

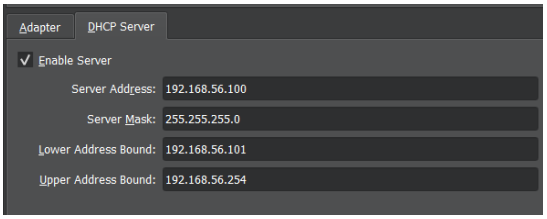
2.26 #tcpdump -v -i em0 -A tcp port 80

2.27 #tcpdump -v -i em0 ‘tcp port 23 and dst edu-dy.cn.ntua.gr’

2.28 #tcpdump -v -i em0 ip6

3

3.1 

3.2 

3.3 dhclient em0

3.4 IPv4: PC1 → 192.168.56.103 , PC2 →192.168.56.102

3.5 κάνω ping την διεύθυνση IPv4 του άλλου

3.6 Αντίστοιχα με ping στις IPv4 από το φιλοξενούν στα φιλοξενούμενα

3.7 netstat -r -4

3.8 Δεν υπάρχει καθώς δεν ορίζεται default gateway γιατί δεν είναι απαραίτητα, υποστηρίζεται μόνο η επικοινωνία στο εσωτερικό του δικτύου.

3.9 Όχι γιατί βρίσκεται σε διαφορετικό υποδίκτυο και δεν υπάρχει route για να φτάσει.

3.10 εκτελώ hostname και θεωρεί πως είναι το PC.ntua.lab. Είναι το ίδιο και στα δύο μηχανήματα.

3.11 Θα εκτελέσουμε τις εντολές hostname PC1 και hostname PC2 αντίστοιχα στο κάθε μηχάνημα.

3.12 Η αλλαγή εμφανίζεται στο prompt “root@PC1” και “root@PC2” μετά το login

3.13 όχι δεν έχει αλλάξει το hostname εκεί, σε επανεκκίνηση θα γίνει ξανά PC.ntua.lab

3.14 vi /etc/rc.conf και αλλάζουμε το hostname=”PC.ntua.lab” σε hostname=”PC1” και hostname=”PC2” αντίστοιχα.

3.15 vi /etc/hosts → Πρέπει να υπάρξουν νέες εγγραφές στο κάθε μηχάνημα για το άλλο, δηλαδή πρέπει να προστεθεί γραμμή 192.168.56.102 PC2 και 192.168.56.103 PC1 και στα 2 μηχανήματα.

3.16 ping -c 4 PC2 στο PC1 και αντίστροφα. Απαντάνε οπότε πέτυχε!

3.17 1: tcpdump -i em0 -l host PC1 | tee kati

2: tcpdump -i em0 -l host PC1 >kati & tail -f kati

3.18 Το μήκος είναι 64 bytes και TTL = 64

3.19 ping -c 4 192.168.56.101 (το φιλοξενούν) → TTL = 128

3.20 tcpdump -A -l -n -vvv -i em0 icmp | tee kati

3.21 Το μήκος τώρα είναι 40 bytes μαζί με τη κεφαλίδα. Τα windows στέλνουν by default 40 bytes πακέτα και τα icmp requests έχουν ίδιο μήκος με τα icmp replies

3.22 Τα πακέτα που στέλνει το φιλοξενούν είναι με TTL=128 και τα πακέτα του φιλοξενούμενου είανι TTL=64

3.23 Δεν εμφανίζεται κάποια κίνηση. Η κάρτα δικτύου είναι σε promisquous mode

3.24 Παρατηρούμε πως η καταγραφή έγινε κανονικά, όχι μόνο τα request αλλά και η υπόλοιπη κίνηση που δημιουργήθηκε λόγω του ping.

4

4.1 ifconfig em0 192.168.56.102 (για το PC2)

ifconfig em0 192.168.56.103 (για το PC1)

4.2 Τερματίζει η σύνδεση με τον dhclient και γίνεται στατική

4.3 tcpdump -vvv -I em0

4.4 Όχι, γιατί είναι εσωτερική δικτύωση και ο host δεν επικοινωνεί με το φιλοξενούμενο μηχάνημα.

4.5 Παρατηρούμε ARP μηνύματα από τον host ψάχνοντας την MAC του PC2

4.6 όχι, δεν είναι στο ίδιο υποδίκτυο

4.7 όχι δεν παρατηρήθηκε κάτι σχετικό

4.8 Ναι πλέον μπορούν και επικοινωνούν

4.9 Όχι δεν μπορούμε, Αυτό συμβαίνει επειδή βρίσκονται σε εσωτερικό LAN δίκτυο, το οποίο δεν είναι συνδεδεμένο με το δίκτυο του υπολογιστή μας. Είναι απομονωμένο κι έτσι δεν επικοινωνεί με τον έξω κόσμο.

4.10 tcpdump -vvv -i em0 -n

4.11 arp -ad . ping 192.168.56.1, 3 arp request μηνύματα που έψαχναν τη διεύθυνση του PC1.

4.12 Δεν εμφανίζεται. Το internal network δεν έχει καμία επαφή με τον host και συνεπώς δεν μπορεί να λάβει απάντηση

4.13 ifconfig em0 10.11.12.61 → PC1

ifconfig em0 10.11.12.62 → PC2

4.14 ναι επικοινωνούν

5

5.1 dhclient em0 σε όλα

5.2 10.0.2.15 και τη πήραν από το 10.0.2.2, την default gateway.

5.3 netstat -r: default gateway 10.0.2.2

5.4 cat /etc/resolv.conf

Search home → τα ονόματα που μπορούμε να αναζητήσουμε.

Nameserver 192.168.1.1 → ο DNS server στον οποίο θα στείλουμε για να μάθουμε ονόματα.

5.5 Οι πληροφορίες είναι στο /var/db/dhclient.leases.em0

5.6 ναι και παρατηρούμε ότι απαντάει

5.7 ναι επικοινωνεί με το internet, και αυτό εξηγείται με την δρομολόγηση των πακέτων του μέσω της default gateway του host που τα προωθεί και τα λαμβάνει όταν pingάρουμε κάποια σελίδα online όπως ping youtube.com

5.8 όλες εκτός 10.0.2.1. 10.0.2.2 → default gateway, 10.0.2.3 → the name server, 10.0.2.4 → tftp server used in NAT

5.9 Δεν επικοινωνούν, το καθένα βρίσκεται στο δικό του ιδιωτικό δίκτυο NAT και επικοινωνεί μόνο μέσα σε αυτό και με τον host και το internet. Τα υπόλοιπα ιδιωτικά δίκτυα δεν εμφανίζονται. Για αυτό το λόγο επίσης μπορούν να υπάρχουν οι ίδιες IP διευθύνσεις σε διαφορετικά υποδίκτυα, πχ η 10.0.2.15 που είναι default.

5.10 -I → ICMP ECHO αντί για UDP

-n → να τυπώσει διευθύνσεις αριθμητικά, όχι ονομαστικά.

-q → Ρύθμισε αριθμό probes ανά hop.

5.11 ICMP Echo request src: 10.0.2.15

5.12 source in Wireshark: είναι 147.102.201.44

5.13 αλλάζει κάθε φορά και είναι οι διευθύνσεις στη διαδρομή

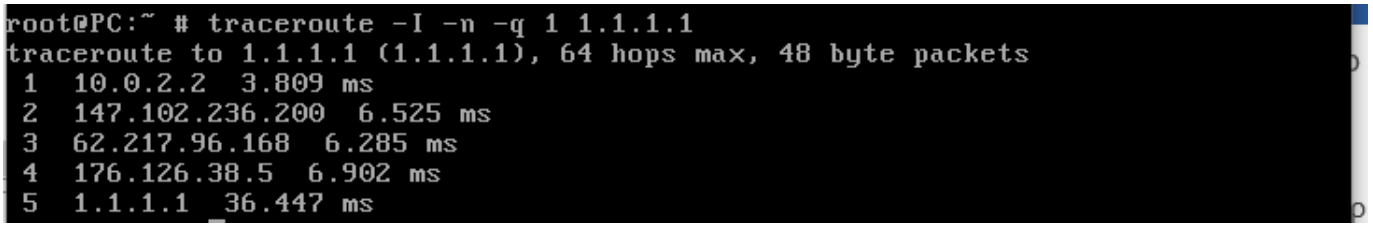
10.0.2.2 (δεν εμφανίστηκε στο wireshark)

147.102.201.44 →

147.102.236.200 →

62.217.96.168 →

176.126.38.5



5.14 dst: 147.102.201.44 η IPv4 του υπολογιστή μου.

5.15 10.0.2.2 →

147.102.236.200 →

62.217.96.168 →

176.126.38.5

5.16 10.0.2.15, η IPv4 του PC3

5.17 ναι γιατί έχουν ίδια τοπολογία. Διαφορετική είναι μονάχα η πηγή, η οποία για το VM είναι η default gateway, ενώ για τον υπολογιστή είναι η διεύθυνση IP του.

5.18 1 λιγότερο γιατί η δικτύωση NAT κρύβει το επίπεδο του default gateway.

6

6.1 NAT Network: 10.0.2.0/24

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

6.3 dhclient em0

6.4 PC1: 10.0.2.4 PC2: 10.0.2.15. Το PC1 αλλάζει τιμή, εφόσον αρχικά ήταν 10.0.2.15.

6.5 DHCP: 10.0.2.3

6.6 search home

nameserver 147.102.224.243, σε αυτή την ip πρέπει να απευθυνθούμε για να μάθουμε το ip ενός μηχανήματος από το όνομα του. Τώρα είναι το default gateway

6.7 netstat -r → default gateway 10.0.2.1

6.8 ναι γίνεται να κάνουμε ping από VM σε default gateway.

6.9 ναι γίνεται να κάνουμε ping από VM σε DHCP Server.

6.10 ναι μπορούμε, αλλά στο arp table βλέπουμε πως η MAC είναι ίδια με του 10.0.2.1, άρα πάλι μας απαντάει το default gateway

6.11 Ναι και επαληθεύεται με το ping youtube.com ή άλλο αντίστοιχο, και μας επιβεβαιώνει πως το NAT επιτρέπει επικοινωνία με τον έξω κόσμο.

6.12 Ναι, το επαληθεύουμε με ping από το ένα στο άλλο, το περιμέναμε από ίδιο NAT Network

6.13 Δεν επικοινωνούν καθώς είναι σε άλλο δίκτυο. Αυτό που απαντάει είναι ο tftp server. Το PC3 δεν λαμβάνει απάντηση από τα PC1, PC2.

6.14 Όχι δεν είναι το ίδιο το PC που απαντάει. Είναι ο tftp server που απαντάει στο 10.0.2.4 ενώ στο 10.0.2.15 απαντάει ο localhost. Με έλεγχο των ARP πινάκων εξακριβώνουμε πως δεν υπάρχουν οι MAC διευθύνσεις των PC1, PC2 στον ARP πίνακα του PC3