ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΡΟΗ Δ - ΕΡΓΑΣΤΗΡΙΟ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ (COMPUTER NETWORKS LAB)

ΓΕΩΡΓΑΚΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ 03120827

ΑΝΑΦΟΡΑ 2ΗΣ ΕΡΓΑΣΤΗΡΙΑΚΗΣ ΑΣΚΗΣΗΣ

Ομάδα: 1
Λογισμικο: Linux Ubuntu 22.04
Ονομα PC: glaptop

ΑΣΚΗΣΗ 2: Ανάλυση δικτυακών πρωτοκόλλων με το TCPDUMP

2.1 Μπορώ να δω τις κάρτες δικτύου με την εντολή ifconfig
2.2 ifconfig em0 down: απενεργοποίηση
ifconfig em0 up: ενεργοποίηση
2.3 Μπορω να δω περισσότερες πληροφορίες με τις εντολές:
Man tcpdump, man pcap, man pcap-filter
2.4 Θα χρησιμοποιήσω την εντολή tcpdump –i em0 –n
2.5 Θα χρησιμοποιήσω την εντολή tcpdump –i em0 –X
(Σημείωση: -x: hex / -A: ASCII / -X: both hex and ASCII)
2.6 Θα χρησιμοποιήσω την εντολή tcpdump –e
2.7 Θα χρησιμοποιήσω την εντολή tcpdump –s 68
2.8 Θα χρησιμοποιήσω την εντολή tcpdump ip host 10.0.0.1 -v
2.9 Θα χρησιμοποιήσω την εντολή
tcpdump host 10.0.0.1 and host 10.0.0.2 -i em0
2.10 Θα χρησιμοποιήσω την εντολή tcpdump ip net 1.1 -x
2.11 Θα χρησιμοποιήσω την εντολή tcpdump ip not net 192.168.1.0/24 -e
2.12 Θα χρησιμοποιήσω την εντολή tcpdump ip broadcast
2.13 Θα κοιτάξω το Total Length του IP header. Επομένως θα χρησιμοποιήσω την εντολή tcpdump 'ip[2:2] > 576' ή την εντολή tcpdump ip>576
2.14 Θα χρησιμοποιήσω την εντολή tcpdump 'ip[8]<5'
2.15 Θα χρησιμοποιήσω την εντολή tcpdump '((ip[0:1]&0x0f)>>2)>5'
(Αν είναι μεγαλύτερο του 5 τότε έχω Options)
2.16 Θα χρησιμοποιήσω την εντολή tcpdump icmp and src 10.0.0.1
2.17 Θα χρησιμοποιήσω την εντολή tcpdump tcp and dst 10.0.0.2
2.18 Θα χρησιμοποιήσω την εντολή tcpdump udp and dst port 53
2.19 Θα χρησιμοποιήσω την εντολή tcpdump tcp and host 10.0.0.10
2.20 Θα χρησιμοποιήσω την εντολή
tcpdump 'tcp and host 10.0.0.10 and port 23' –w sample_capture
2.21 Θα χρησιμοποιήσω την εντολή tcpdump 'tcp[13]=2'
(Αν μόνο το syn ειναι 1 τότε το 14ο byte θα είναι 00000010)
2.22 Θα χρησιμοποιήσω την εντολή tcpdump 'tcp[13]=2 or tcp[13]=18'

(Τα πρώτα 2 τεμάχια της τριμερούς χειραψίας έχουν ενεργοποιημένο το SYN (2) είτε τα SYN και ACK (18))

2.23 Θα χρησιμοποιήσω την εντολή tcpdump 'tcp[13]&00000001 !=0'
(Χρησιμοποιώ μάσκα για να πάρω μόνο το FIN)

2.24 Η παράσταση αυτή παίρνει τα πρώτα 4 bits του 13ου byte της επικεφαλίδας του tcp (δηλαδή το DO ή αλλιως Header Length) και τα μετατοπίζει κατα 2 θέσεις δεξιά, δηλαδή διαίρεση με το 4. Ετσι μπορώ να κανω τον έλεγχο για τα options

2.25 Θα χρησιμοποιήσω την εντολή tcpdump '((tcp[12:1]&0xf0)>>2)>5'.
(Χωρις τα options η επικεφαλίδα έχει 20 bytes)

2.26 Θα χρησιμοποιήσω την εντολή tcpdump tcp port 80 -A

2.27 Θα χρησιμοποιήσω την εντολή
tcpdump tcp port 23 and dst edu-dy.cn.ntua.gr

2.28 Θα χρησιμοποιήσω την εντολή tcpdump ip6

ΑΣΚΗΣΗ 3: Δικτύωση Host-only

3.1 Η διεύθυνση IPv4 του Host-only Ethernet adapter είναι 192.168.56.1

3.2 Για τον dhcp server ισχύει ότι:
IPv4: 192.168.56.100
Περιοχή: απο 192.168.56.101 εως 192.168.56.254

3.3 Θα χρησιμοποιήσω την εντολή dhclient em0

3.4 Οι διευθυνσεις είναι:
PC1: 192.168.56.103
PC2: 192.168.56.102

3.5 Κάνοντας ping απο το ένα στο άλλο

3.6 Κάνοντας ping απο το φιλοξενούν στα υπόλοιπα

3.7 Μπορώ να χρησιμοποιήσω την εντολή netstat -r

3.8 Οχι, δεν υπάρχει default gateway στην συγκεκριμένη κατάσταση σύνδεσης καθως δεν υπάρχει ανάγκη για σύνδεση με δίκτυα εκτος αυτων.

3.9 Οχι, δεν μπορώ να κανω ping απο τα VM στο host μηχάνημα

3.10 Και τα δύο εμφανίζουν όνομα PC.ntua.lab (εντολή hostname)

3.11 Θα χρησιμοποιήσω την εντολή hostname PC1 και hostname PC2

3.12 Εμφανίζεται στο όνομα του τερματικου, εκεί που εισάγουμε τις εντολές:
(root@PC1:~#)

3.13 Όχι, δεν το περιέχει. Αν γίνει επανεκκίνηση θα χρησιμοποιηθεί και πάλι το παλιό

3.14 Θα χρησιμοποιήσω το vi

3.15 Θα πρέπει να προσθέσω το μια εγγραφή σε αυτό το αρχείο
(πχ 192.168.56.103 PC1) στο hosts του PC2

3.16 Έπειτα θα μπορώ να εκτελέσω: ping PC1

3.17 ping προς PC2: TTL=64
ping προς εικονική κάρτα host: TTL=64
ping προς dhcp server: TTL=255
Σε όλες τις περιπτώσεις το μήκος ήταν 64 bytes

3.18 Η εντολή που χρησιμοποίησα είναι: tcpdump host PC1 –n -v
3.19 Echo request: length=64bytes
TTL: 64
3.20 Η εντολή που χρησιμοποίησα είναι: tcpdump icmp -vvv
3.21 Echo request: length=84bytes. Το μήκος διαφέρει με αυτό που παρατήρησα πριν λόγω των λειτουργικών συστημάτων.
3.22 Η τιμή του TTL παραμένει 64
3.23 Οι 2 τρόποι είναι:
tcpdump host PC1 –l –w file
tcpdump host 192.168.56.103 –l –w file
3.24 Ναι, παρατηρώ ενα ARP μήνυμα Request who has 192.168.56.1 tell PC2
3.25 Ναι παρατηρώ κίνηση σχετικά με το φιλοξενουν και το δίκτυο
3.26 Δεν παρατηρώ κάτι διαφορετικό σχετικά με το ping.
(Με την αλλαγή που κάναμε θα μπορούσαμε θεωρητικά να δουμε ολα τα πλαίσια της κίνησης του υποδικτύου ανεξαρτήτως της MAC διευθυνσης τους)

ΑΣΚΗΣΗ 4: Δικτύωση Internal
4.1 Η εντολή που χρησιμοποίησα είναι: ifconfig em0 inet 192.168.56.102
4.2 Το μήνυμα που έβγαλε ήταν: My address was deleted, dhclient exiting.
Ουσιαστικά αναφέρει ότι κλείνει η σύνδεση με τον dhclient απο την άσκηση 3
4.3 Η εντολή που χρησιμοποίησα είναι: tcpdump –v –l
(Option –l: Make stdout line buffered. Useful if you want to see the data while capturing it)
(Option –v: Λεπτομέρειες)
4.4 Οχι, δεν μπορώ να κάνω ping:
Destination Host Unreachable
4.5 Το μόνο που εμφανίζεται είναι κάποια πακέτα ARP
4.6 Οχι, δεν μπορώ να κανω ping απο το PC2 στο PC1
(διαφορετικό τρόπο δικτύωσης)
4.7 Οχι, δεν παρατηρώ κανένα μηνυμα στην καταγραφή
4.8 Αφότου αλλάξαμε την ρύθμιση δικτύου του PC1 σε Internal Network, τα δύο μηχανήματα επικοινωνούν κανονικά μεταξύ τους
4.9 Οχι, απο το φιλοξενούν μηχάνημα δεν μπορώ να επικοινωνήσω με κανένα απο τα μηχανήματα. Αυτό συμβαίνει γιατι τα μηχανήματα βρίσκονται σε Internal Network και άρα δεν επικοινωνούν με κανένα εξωτερικό δίκτυο πέρα απο αυτο μεταξύ τους.
4.10 Για την καταγραφή χρησιμοποιώ την εντολή tcpdump –n
(Option –n: Don't convert addresses to names)
4.11 Για την διαγραφή στοιχείων του arp πίνακα χρησιμοποιώ την εντολή arp –d –a (delete all entries).
Στην κατγραφή του PC1 παρατηρώ ARP Request who has 192.168.56.1 μηνύματα. Ως απάντηση στο ping του PC2 παίρνω Host is down
4.12 Το μήνυμα αυτό προκύπτει καθώς το PC2 δεν παίρνει καμία απάντηση,

εφόσον δεν μπορεί να επικοινωνήσει με το φιλεξενούν μηχάνημα

4.13 Χρησιμοποίησα τις εντολές:
ifconfig em0 inet 10.11.12.63 (για το PC1)
ifconfig em0 inet 10.11.12.62 (για το PC2)

4.14 Ναι τα μηχανήματα επικοινωνούν με τις νέες διευθύνσεις

ΑΣΚΗΣΗ 5: Δικτύωση NAT

5.1 Θα χρησιμοποιήσω την εντολή: dhclient em0

5.2 Η διεύθυνση που δόθηκε είναι η 10.0.2.15 και δόθηκε απο την 10.0.2.2
(Ολα τα μηχανήματα λαμβάνουν την ίδια διευθυνση καθώς καθε ένα θεωρεί ότι βρίσκεται στο δικό του ξεχωριστό δίκτυο)

5.3 Η προεπιλεγμένη πύλη είναι: Default Gateway = 10.0.2.2
(Χρησιμοποίησα την εντολή netstat -r)

5.4 Το αρχείο αυτό περιέχει:
#Generated bt resolvconf
nameserver 10.0.2.3
(Ουσιαστικά περιέχει τους DNS εξυπηρετητές)

5.5 Οι πληροφορίες αυτές περιέχονται στο αρχείο /var/db/dhclient.leases.em0

5.6 Ναι, μπορώ να κάνω ping απο τα VMs στην Default Gateway

5.7 Ναι, τα VMs επικοινωνούν με το internet μέσω της Default Gateway
Πχ η εντολή ping edu-dy.cn.ntua.gr πετυχαίνει

5.8 Η μόνη διεύθυνση για την οποία δεν λαμβάνω απάντηση είναι η 10.0.2.1
Για τις υπόλοιπες λαμβάνω
(2: Default Gateway / 3: DNS server / 4: TFTP server)

5.9 Οχι, δεν επικοινωνούν γιατι το καθε ένα θεωρεί ότι βρίσκεται στο δικό του ξεχωριστό δίκτυο. Δοκιμάζοντας ping 10.0.2.15 απο το PC3 ενω κάνουμε καταγραφή στα PC1 και PC2, δεν βλέπουμε καποια κίνηση, παρότι το ping πετυχαίνει

5.10 Στην εντολή traceroute:
-I: ICMP messages
-n: Display in console
-q 1: number of queries is 1

5.11 Απο την καταγραφή του tcpdump παίρνουμε ότι:
Διευθυνση πηγής: 10.0.2.15
Τύπος Μηνυνάτων: ICMP echo request

5.12 Στο wireshark βλέπουμε:
Διεύθυνση πηγής: 192.168.2.8

5.13 Τα μηνύματα TTL exceeded in transit έχουν διευθύνσεις πηγης, σύμφωνα με το wireshark:
192.168.2.1 / 62.38.0.170 / 176.126.38.118

5.14 Τα μηνύματα αυτά έχουν διεύθυνση προοσιμού, σύμφωνα με το wireshark: 192.168.2.8

5.15 Τα μηνύματα TTL exceeded in transit έχουν διευθύνσεις πηγης, σύμφωνα με το tcpdump:

10.0.2.2 / 192.168.2.1 / loopback2004.med01.ds1.ho1.gr

5.16 Τα μηνύματα αυτά έχουν διεύθυνση προοσιμού, σύμφωνα με το tcpdump: 10.0.2.15

5.17 Ναι, αντιστοιχουν 1 προς 1 εκτός απο το 1ο μήνυμα

5.18 Παραηρώ ενα λιγότερο hop οταν κανω traceroute απο το φιλοξενούν μηχάνημα (δηλαδή 5 αντί για 6 που είχα στα VMs). Αυτό συμβαίνει καθώς απο τα VMs πρέπει πρώτα να επικοινωνήσω και με το host

ΑΣΚΗΣΗ 6: Δικτύωση NAT NETWORK

6.1 Το δίκτυο NAT που έχει ορίσει το Virtual Box έχει διεύθυνση: 10.0.2.0/24

6.2 Χρησιμοποίησα τις εντολές

ifconfig em0 –alias (ιδια με την ifconfig em0 delete)

rm /var/db/dhclient.leases.em0

6.3 Χρησιμοποίησα την εντολή dhclient em0

6.4 Αποδόθηκαν οι διευθύνσεις:

PC1: 10.0.2.15 (ίδια με πριν)

PC2: 10.0.2.4 (διαφορετική με πριν)

6.5 Ο εξυπηρετητής DHCP έχει διεύθυνση: 10.0.2.3

6.6 Το αρχείο /etc/resolv.conf περιέχει:

#Generated bt resolvconf

nameserver 10.0.2.1

6.7 Η προεπιλεγμένη πυλη έχει διεύθυνση: 10.0.2.1

6.8 Ναι, μπορώ να κανω ping 10.0.2.1 απο τα εικονικά μηχανήματα (Οπως και στο απλό NAT)

6.9 Ναι, μπορώ να κάνω ping 10.0.2.3 απο τα εικονικά μηχανήματα

6.10 Ναι, μπορώ να κάνω ping 10.0.2.2 απο τα εικονικά μηχανήματα και απαντάει το φιλοξενούν μηχάνημα

6.11 Ναι, τα VMs επικοινωνούν με το internet μέσω της Default Gateway Πχ η εντολή ping edu-dy.cn.ntua.gr πετυχαίνει

6.12 Ναι τα PC1 και PC2 επικοινωνούν μεταξύ τους

6.13 Οχι, το PC3 δεν μπορέι να κάνει ping στα PC1 και PC2

6.14 Ναι, καθώς λόγω του NAT Network τα PC έχουν διαφορετικές IP. Επίσης μπορώ να το διαπιστώσω και ξεκινώντας καταγραφές tcpdump στο μηχάνημα που θέλω να κανω ping