Ονοματεπώνυμο: Περόγαμβρος Γεώργιος	Όνομα PC:
Ομάδα: 2	Ημερομηνία: 17/3/2022

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 Με την εντολή ifconfig.

2.2 Με τις εντολές ifconfig em0 down και ifconfig em0 up αντίστοιχα.

2.3 Με τις εντολές man tcpdump, man pcap, man pcap-filter.

2.4 Με την εντολή tcpdump -i em0 -n.

2.5 Με την εντολή tcpdump -i em0 -X.

2.6 Με την εντολή tcpdump -i em0 -e.

2.7 Με την εντολή tcpdump -i em0 -s 68 .

2.8 Με την εντολή tcpdump -e host 10.0.0.1.

2.9 Με την εντολή tcpdump '(src 10.0.0.1 and dst 10.0.0.2) or (src 10.0.0.2 and dst 10.0.0.1)'.

2.10 Με την εντολή tcpdump -x net 1.1.0.0/16.

2.11 Με την εντολή tcpdump -ex not net 192.168.1.0/24.

2.12 Με την εντολή tcpdump ip broadcast.

2.13 Με την εντολή tcpdump 'ip len > 576'.

2.14 Με την εντολή tcpdump 'ip[8] < 5'.

2.15 Με την εντολή tcpdump 'ip[0] & 31 > 5'.

2.16 Με την εντολή tcpdump 'icmp and src 10.0.0.1'

2.17 Με την εντολή tcpdump 'tcp and dst 10.0.0.2'.

2.18 Με την εντολή tcpdump 'udp and dst port 53'.

2.19 Με την εντολή tcpdump 'tcp and host 10.0.0.10'.

2.20 Με την εντολή tcpdump 'tcp and host 10.0.0.10 and dst port 23' -w sample_capture.

2.21 Με την εντολή tcpdump 'tcp[13] == 2'

2.22 Με την εντολή tcpdump 'tcp[13] == 2 or tcp[13] == 18'

2.23 Με την εντολή tcpdump 'tcp[13] == 2 or tcp[13] == 16'

2.24 Το μήκος της επικεφαλίδας σε bytes (Τα 4 πρώτα bits του DataOffset πολλαπλασιασμένα επί 4).

2.25 Με την εντολή tcpdump '((tcp[12:1] & 0xf0) >> 2) > 20'

2.26 Με την εντολή tcpdump -A port 80.

2.27 Με την εντολή tcpdump 'port 23 and dst edu-dy.cn.ntua.gr'

2.28 Με την εντολή tcpdump ip6.

3

3.1 Η ζητούμενη ip είναι η 192.168.56.1.

3.2 Η ip του εξυπηρετητή DHCP είναι η 192.168.56.100 και μπορεί να εκχωρήσει την περιοχή διευθύνσεων 192.168.56.101-192.168.56.254.

3.3 Αφού συνδέθηκα στο κάθε μηχάνημα ως root, χρησιμοποίησα την εντολή dhclient em0.

3.4 Στο PC1 δώθηκε η διεύθυνση 192.168.56.102 και στο PC2 η διεύθυνση 192.168.56.103.

3.5 Θα προσπαθήσουμε να κάνουμε ping από το ένα στο άλλο. Στο PC1 τρέχουμε ping 192.168.56.103 και στο PC2 τρέχουμε ping 192.168.56.102.

3.6 Κάνουμε ping από ένα από τα εικονικά μηχανήματα στο φιλοξενούν (αφού απαντάει υπάρχει επικοινωνία).

3.7 Η ζητούμενη εντολή είναι η netstat -rn.

3.8 Όχι, αφού στη host-only σύνδεση δεν υπάρχει επικοινωνία εκτός του δικτύου.

3.9 Όχι, αφού το φιλοξενούν είναι στο δίκτυο μέσω της εικονικής και όχι της φυσικής κάρτας.

3.10 Με την εντολή hostname, βρήκα το ζητούμενο όνομα που είναι PC.ntua.lab.

3.11 Χρησιμοποίησα τις εντολές hostname PC1 και hostname PC2 στο αντίστοιχο μηχάνημα.

3.12 Εμφανίζονται στην προτροπή root@PC1 και root@PC2.

3.13 Δεν το περιέχει. Σε περίπτωση επανεκκίνησης θα έχει το όνομα PC.ntua.lab.

3.14 Αλλάξα το hostname στο αρχείο /etc/rc.conf

3.15 Πρέπει να προσθέσουμε τα ζευγάρια IPv4-όνομα vm για τα δύο μηχανήματα στο αρχείο /etc/hosts

3.16 Από το PC1 ping PC2.

3.17 Μπορώ να χρησιμοποιήσω τις εντολές tcpdump -l | tee test και tcpdump -l > tee & tail -f test

3.18 Το μήκος είναι 64 bytes και η τιμή του ttl είναι 64.

3.19 Το ttl έχει τιμή 128.

3.20 Χρησιμοποίησα την εντολή tcpdump ‘icmp’ -v.

3.21 Το μήκος είναι 40 bytes. Η διαφορά οφείλεται ότι στα windows το μήκος είναι 40 ενώ στο freeBSD 64.

3.22 Τα μηνύματα από το φιλοξενούν έχουν ttl 64, ενώ από το PC2 128, όπως και πριν.

3.23 Όχι, δεν παρατηρείται κίνηση.

3.24 Καταγράφονται κανονικά τα μηνύματα που ανταλλάζουν το φιλοξενούν με το PC2.

4

4.1 Χρησιμοποίησα τις εντολές ifconfig em0 192.168.56.102 και ifconfig em0 192.168.56.103 αντίστοιχα.

4.2 Το μήνυμα σφάλματος που εμφανίζεται σημαίνει πως χάθηκε η σύνδεση με τον dhclient.

4.3 Χρησιμοποίησα την εντολή tcpdump -v.

4.4 Όχι, δεν μπορώ.

4.5 Ναι, παρατηρώ.

4.6 Όχι, δεν μπορώ.

4.7 Όχι, δεν παρατηρώ.

4.8 Ναι, επικοινωνούν.

4.9 Όχι, αφού στο εσωτερικό δίκτυο δεν συμμετέχει το φιλοξενούν μηχάνημα και όλη η κίνηση του εσωτερικού δικτύου παραμένει στο εσωτερικό δίκτυο.

4.10 Χρησιμοποίησα την εντολή tcpdump -e.

4.11 Χρησιμοποίησα την εντολή arp -da. Το PC2 στέλνει arp requests για να μάθει ποιος έχει τη διεύθυνση 192.168.56.1.

4.12 Είναι λογικό αφού δεν παίρνει απάντηση στο request που έκανε και δεν υπάρχει επικοινωνία μεταξύ τους.

4.13 Οι δύο ζητούμενες διευθύνσεις είναι οι 10.11.12.61 και οι 10.11.12.62, αφού η τελευταία διεύθυνση 10.11.12.63 είναι δεσμευμένη για broadcast.

4.14 Ναι, επικοινωνούν.

5

5.1 Χρησιμοποίησα την εντολή dhclient em0.

5.2 Και οι τρεις έλαβαν την 10.0.2.15 από την 10.0.2.2.

5.3 Η διεύθυνση της προκαθορισμένης πύλη είναι η 10.0.2.2. Βρέθηκε χρησιμοποιώντας την εντολή netstat -rn.

5.4 Το περιεχόμενο του αρχείου είναι:

#Generated by resolvconf

nameserver 192.168.1.254

Η διεύθυνση αυτή είναι η default gateway του φυσικού μηχανήματος.

5.5 Είναι το αρχείο /var/db/dhclient.leases.em0.

5.6 Ναι, μπορούμε.

5.7 Ναι, υπάρχει επικοινωνία με το διαδίκτυο. Σε ένα NAT δίκτυο τα φιλοξενούμενα μηχανήματα στέλνουν μέσω του φιλοξενούν τα μηνύματα προς το διαδίκτυο (με IP διεύθυνση αυτή του φιλοξενούν). Όταν έχουμε εισερχόμενη κίνηση, οι απαντήσεις φαίνεται σαν να προέρχονται από το διαδίκτυο.

5.8 Απαντάνε όλες εκτός από την 10.0.2.1. Η 10.0.2.2 είναι η default gateway, η 10.0.2.3 είναι nameserver και η 10.0.2.4 είναι tftp server.

5.9 Όχι αφού στο NAT τα μηχανήματα δεν επικοινωνούν μεταξύ τους. Στο NAT το κάθε μηχάνημα είναι σαν να βρίσκεται στο δικό του ξεχωριστό δίκτυο.

5.10 Έχουμε τις εξής σημαίες: -I: χρησιμοποίησε icmp echo αντί για udp diagrams, -n: τύπωσε τις διευθύνσεις αριθμητικά και όχι συμβολικά και αριθμητικά, -q: το πλήθος των probes σε κάθε hop.
5.11 Παράγονται ICMP echo request μηνύματα από την 10.0.2.15.

5.12 Η πηγή είναι η 192.168.1.215, η οποία είναι η διεύθυνση της φυσικής κάρτας.

5.13 Οι πήγες είναι οι 192.168.1.254, 10.13.255.59, 185.3.220.70, 62.169.252.230, 10.13.255.101, 62.169.252.233

5.14 Ο προορισμός είναι η 192.168.1.215.

5.15 Οι πήγες είναι οι 10.0.2.2, 192.168.1.254, 10.13.255.59, 185.3.220.70, 62.169.252.230, 10.13.255.101, 62.169.252.233

5.16 Ο προορισμός είναι η 10.0.2.15.

5.17 Όχι, λείπει το πρώτο ttl exceeded in transit από την 10.0.2.2 (default gateway του εικονικού δικτύου) προς το 10.0.2.15.

5.18 Έχουμε ένα λιγότερο βήμα από πριν, καθώς δεν υπάρχει το βήμα της 10.0.2.2 (εικονική default gateway).

6

6.1 Είναι η 10.0.2.0/24.

6.2 Χρησιμοποίησα τις εντολές ifconfig em0 delete και rm /var/db/dhclient.leases.em0.

6.3 Χρησιμοποίησα την εντολή dhclient em0.

6.4 Για το PC1 έχουμε την 10.0.2.15 και για το PC2 την 10.0.2.4. Του PC1 είναι ίδια με πριν, ενώ του PC2 όχι.

6.5 Η διεύθυνση του DHCP είναι η 10.2.3.

6.6 Το περιεχόμενο του αρχείου είναι:

#Generated by resolvconf

nameserver 192.168.1.254

Η διεύθυνση αυτή είναι η default gateway του φυσικού μηχανήματος.

6.7 Είναι η 10.0.2.1.

6.8 Ναι, μπορώ.

6.9 Ναι, μπορώ.

6.10 Μπορώ να κάνω ping. Όπως βλέπουμε από τον πίνακα arp η mac της διεύθυνσης που απαντάει είναι αυτή της εικονικής κάρτας δικτύου του φιλοξενούν.

6.11 Στο δίκτυο NAT υπάρχει επικοινωνία με το διαδίκτυο χρησιμοποιώντας TCP και UDP πάνω από IPv4 και IPv6.

6.12 Ναι, επικοινωνούν.

6.13 Ναι, μπορώ.

6.14 Σε καμία από τις δύο περιπτώσεις δεν απαντάει το αντίστοιχο PC (δεν θα μπορούσε, αφού είναι NAT). Στην περίπτωση του PC1 που κάναμε ping στη διεύθυνση 10.0.2.15, το PC3 έκανε ping στον εαυτό του, αφού στο δικό του δίκτυο, έχει αυτή τη διεύθυνση. Στην περίπτωση της 10.0.2.4 η απάντηση προήλθε από το φυσικό υπολογιστή (από τον πίνακα arp είδα πως η mac είναι ίδια με αυτή του 6.10)