ΕΡΓΑΣΤΗΡΙΟ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

2η ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ

ΠΑΝΑΓΙΩΤΗΣ ΠΑΠΑΔΕΑΣ

A.M el18039

ΑΣΚΗΣΗ 1

SETUP

ΑΣΚΗΣΗ 2

2.1 ifconfig

2.2 ifconfig em0 down

Ifconfig em0 up

2.3 man tcpdump

man pcap

man pcap-filter

2.4 tcpdump -ni em0

2.5 tcpdump -xi em0

2.6 tcpdump -e

2.7 tcpdump -s 68

2.8 tcpdump -ni em0 ‘host 10.0.5.5’

2.9 tcpdump -ni em0 ‘host 10.0.0.1 and host 10.0.0.2’

2.10 tcpdump net 1.1.0.0/16

2.11 tcpdump net not 192.168.1.0/24

2.12 tcpdump -ni em0 ‘broadcast’

2.13 tcpdump -n ‘len > 576’

2.14 tcpdump -n ‘ip[8]<5’

2.15 tcpdump -v

2.16 tcpdump icmp ‘src 10.0.0.1’

2.17 tcpdump tcp ‘dst 10.0.0.2’

2.18 tcpdump udp and port 53

2.19 tcpdump tcp and ‘src or dst 10.0.0.10’

2.20 tcpdump -l > sample_capture tcp ‘port 23 and (src or dst ‘10.0.0.10’)

2.21 tcpdump tcp and ‘tcp[tcpflags] & (tcp-syn) != 0’

2.22 tcpdump tcp and ‘tcp[tcpflags] & (tcp-syn|tcp-ack) != 0’

2.23 tcpdump tcp and ‘tcp[tcpflags] & (tcp-fin) != 0’

2.24 συλλαμβάνει μηνύματα http

2.25 tcpdump -v tcp

2.26 tcpdump -i em1 ‘tcp[((tcp[12:1] & 0xf0) >> 2):4] = 0x47455420 or tcp[((tcp[12:1] & 0xf0) >> 2):4] = 0x504F5354'

2.27 tcpdump -I em0 host 147.102.40.15 and port 23

2.28 tcpdump ip6

ΑΣΚΗΣΗ 3

3.1 192.168.56.1

3.2 192.168.56.2, 192.168.56.101-192.168.56.254

3.3 dhclient em1

3.4 PC1: 192.168.56.102, PC2: 192.168.56.103

3.5 ssh connection από το ένα στο άλλο

3.6 ssh από το command line του pc Μου στα δύο μηχανήματα

3.7 netstat -rn

3.8 link 2, δεν είναι ορισμένη η προκαθορισμένη πύλη καθώς δεν επικοινωνούν τα εξωτερικά μηχανήματα με τα εσωτερικά.

3.9 όχι καθώς έχουμε σύνδεση host-only

3.10 PC.ntua.lab, hostname

3.11 vi rc.conf, hostname =PC1, PC2

3.12 root@pc1

3.13 Διατηρεί το παλιό όνομα και σε περίπτωση επανεκκίνησης το όνομα θα ξαναλλάξει στο PC.ntua.lab

3.14 vi /etc/rc.conf

3.15 Εισαγωγή στο αρχείο /etc/hosts της γραμμής

192.168.56.102 localhost PC1

3.16 ping PC1

3.17 tcpdump -l | tee test

tcpdump -l > test & tail -f test

3.18 length: 64 bytes

Ttl = 64

3.19 ttl = 128

3.20 tcpdump -nv icmp

3.21 32 bytes (windows)

3.22 ttl 128, συμφωνεί

3.23 Δεν παρατηρώ κάποια κίνηση. Πιθανώς να μπορούσα να καταγράψω κάποιο πακέτο ARP.

3.24 λαμβάνω τα πακέτα που στέλνονται στο PC2

ΑΣΚΗΣΗ 4

4.1 ifconfig em1 192.168.56.103

4.2 Δεν εμφανίστηκε μήνυμα λάθους

4.3 tcpdump -vi em1

4.4 Όχι

4.5 Πακέτα arp requests αναζήτησης της διεύθυνσης 192.168.56.103 από τον host

4.6 Όχι

4.7 Όχι

4.8 Ναι

4.9 Όχι καθώς έχω εσωτερικό δίκτυο όπου ο host δεν επικοινωνεί με τα VMs αλλά μόνο τα VMs μεταξύ τους.

4.10 Deny

4.11 ARP request packets από το PC2 για τον Host

4.12 Δεν επικοινωνεί το VM με τον host οπότε νομίζει ότι δεν είναι ενεργός

4.13 Επικοινωνούν

ΑΣΚΗΣΗ 5

5.1 dhclient em0

5.2 10.0.2.15 από 10.0.2.2

5.3 10.0.2.2

5.4 search station

Nameserver 192.168.2.1

5.5 /var/db/dhclient.leases.em0

5.6 Ναι

5.7 Ναι καθώς κάθε μηχάνημα έχει την εντύπωση ότι βρίσκεται στο δικό του ξεχωριστό δίκτυο.

5.8 Απαντούν όλες εκτός από την 10.0.2.1. Η 10.0.2.2 αποτελεί την προκαθορισμένη πύλη όπου βρίσκεται και ο DHCP, η 10.0.2.3 αντιστοιχεί σε proxy DNS και η 10.0.2.4 αντιστοιχεί σε εξυπηρετητή tftp.

5.9 Όχι καθώς κάθε μηχάνημα έχει την εντύπωση πως βρίσκεται σε δικό του δίκτυο και έχουν την ίδια διεύθυνση IPv4

5.10 -I use ICMP ECHO instead of udp

-n print hop addresses numerically

-q set number of probes per hop (1)

5.11 10.0.2.15, ICMP echo request

5.12 192.168.2.7

5.13 192.168.2.1

62.38.28.209

62.38.97.150

185.1.123.10

62.38.28.217

62.38.97.150

62.38.93.221

5.14 192.168.2.7

5.15 10.0.2.2

192.168.2.1

62.38.28.209

62.38.97.150

185.1.123.10

5.16 10.0.2.15

5.17 Όχι διαφέρουν ως προς τον προορισμό και σε κάποιες διευθύνσεις πηγών προέλευσης

5.18 Θα είναι 6 δηλαδή μία λιγότερη καθώς δεν υπάρχει το βήμα από το VM στον host

ΑΣΚΗΣΗ 6

6.1 10.0.2.0/24

6.2 ifconfig em1 delete

6.3 dhclient em1

6.4 10.0.2.4 και 10.0.2.5, διαφέρουν από την προηγούμενη διεύθυνσή τους

6.5 10.0.2.3

6.6 search station

nameserver 192.168.2.1

6.7 10.0.2.1

6.8 Μπορώ

6.9 Μπορώ

6.10 Μπορώ και απαντά το φιλοξενούν μηχάνημα

6.11 Ναι μέσω TCP πάνω από IPv4

6.12 Ναι

6.13 Όχι

6.14 Λαμβάνουμε απάντηση από το 10.0.2.4 ωστόσο δεν αντιστοιχεί στο PC1 αλλά στον εξυπηρετητή tftp. Μπορούμε να το διαπιστώσουμε με tcpdump από το PC1 που δεν καταγράφει τα μηνύματα αυτά.