ΕΡΓΑΣΤΗΡΙΟ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
8ο ΕΞΑΜΗΝΟ ΣΗΜΜΥ
Εργαστηριακή Άσκηση 2
Δικτύωση συστημάτων στο VirtualBox

Ιωάννης Αλεξόπουλος (03117001)
Όνομα PC/ΛΣ: thinkpad / Ubuntu 20.04.1
Ομάδα: 1

Άσκηση 2: Βασικές εντολές συστήματος αρχείων

1. ifconfig
2. ifconfig em0 down και ifconfig em0 up
3. man tcpdump, man pcap, man pcap-filter
4. tcpdump -i em0 -n
5. tcpdump -i em0
6. tcpdump -i em0 -x(hex) -A(ascii)
7. tcpdump -i em0 -s 68
8. tcpdump -i em0 -v ‘ip and host 10.0.0.1’
9. tcpdump -i em0 ‘(src 10.0.0.1 or 10.0.0.2) and (dst 10.0.0.1 or 10.0.0.2)’
10. tcpdump ip ‘net 1.1 mask 255.255.0.0’
11. tcpdump -e ‘ip and !(net 192.168.1 and mask 255.255.255.0)’’
12. tcpdump ip ‘multicast’
13. tcpdump ‘ip and (length >= 576)’
14. tcpdump ‘ip[8] < 5’
15. tcpdump ‘ip[0] & 0xf > 5’ (IHL bits 4-7 σε λέξεις των 32 bits)
16. tcpdump ‘icmp and src 10.0.0.1’
17. tcpdump ‘tcp and dst 10.0.0.2’
18. tcpdump ‘udp and src port 53’
19. tcpdump ‘tcp and host 10.0.0.10’
20. tcpdump -w “sample_capture” ‘tcp and dst port 23’
21. tcpdump ‘tcp[13] = 2’
22. tcpdump ‘tcp[13] = 2 or tcp[13] = 18’ (tcpdump ‘tcp[13] & 2 = 2’
23. tcpdump ‘tcp[13] & 1 = 1’
24. Δίνει το tcp header length (((tcp[12:1] & 0xf0) >> 2) τα πρώτα 4 bits του byte 12 * 4
25. tcpdump ‘(tcp[12:1] & 0xf0) >> 2) > 20)’
26. tcpdump -A ‘tcp port 80’
27. tcpdump ‘tcp port 23 and dst host edu-dy.cn.ntua.gr’
28. tcpdump ‘ip6’

Άσκηση 3: Δικτύωση Host-only

1. 192.168.56.1
2. 192.168.56.100 με περιοχή 192.168.56.101 - 192.168.56.254
3. PC1 = 192.168.56.103 και PC2 = 192.168.56.102
4. dhclient em0
5. Με εντολή ping μεταξύ των μηχανών
6. Με εντολή ping από τον φλοιό του φιλοξενούν μηχανήματος
7. netstat -rn
8. Δεν υπάρχει default gateway καθώς δεν προβλέπεται επικοινωνία με το διαδίκτυο ή με κάποιο δρομολογητή
9. Όχι, δεν γίνεται ping καθώς δεν υπάρχει εγγραφή στο routing table
10. PC.ntua.lab
11. hostname PC1/PC2
12. root@PC{1,2}
13. Όχι, περιέχει το παλιό όνομα
14. Έγινε αλλαγή των hostnames στο αρχείο /etc/rc.conf μέσω vim
15. Προσθέτω τις αντίστοιχες γραμμές στα αρχεία /etc/hosts:
    192.168.56.102 PC2
    192.168.56.103 PC1
16. ping PC1
17. tcpdump -i em0 ‘icmp and host 192.168.56.103’ -l | tee test
18. 64 bytes ttl = 64
19. ping -c 4 192.168.56.1
20. tcpdump -i em0 -vv ‘icmp’ -l | tee test
21. Το μήκος είναι το ίδιο, 64 bytes (μαζί με icmp header), unix ping
22. Η τιμή είναι 64 και συμφωνεί με τις προηγούμενες τιμές
23. Δεν παρατήρησα στην καταγραφή κάποια κίνηση
24. Τώρα παρατηρώ όλη την κίνηση ICMP requests και replies μεταξύ του host και PC2

Άσκηση 4: Δικτύωση Internal

1. ifconfig em0 192.168.56.103/24 αντίστοιχα
2. Η σύνδεση με τον dhcp server απολύεται (dhclient exiting)
3. tcpdump -vv
4. Όχι, δεν απαντάει ο PC2
5. Ναι, φαίνονται τα ARP requests που κάνει ο host για να μάθει την Mac address του PC2
6. Όχι, λαμβάνω μήνυμα host is down
7. Όχι, δεν υπάρχει κίνηση
8. Τώρα επικοινωνούν μεταξύ τους, έλεγχος με ping

9. Όχι, ο host δεν επικοινωνεί με τα εικονικά μηχανήματα. Λογικό γιατί ανήκουν σε internal network (με όνομα LAN) και έτσι ορίζει τη λειτουργία το VirtualBox
10. tcpdump -n -vv
11. arp -d -i em0 -a, ο PC2 παράγει ARP requests στην καταγραφή του PC1
12. Δεν υπάρχει δυνατότητα επικοινωνίας με το host, ο PC2 δεν βρίσκει την MAC address του host για να στείλει το ping request.
13. Οι δύο τελευταίες διαθέσιμες διευθύνσεις είναι οι 10.11.12.61 και 10.11.12.62
14. Ναι, επικοινωνούν (ping)

Άσκηση 5: Δικτύωση NAT

1. dhclient em0 σε κάθε μηχάνημα -> ip 10.0.2.25
2. ip 10.0.2.25 από dhcp server 10.0.2.2
3. 10.0.2.2
4. Το περιεχόμενο είναι το ίδιο με εκείνο του αρχείου /etc/resolv.conf του host
5. /var/db/dhclient.leases.em0
6. Ναι
7. ping www.google.com απαντάει οπότε επικοινωνεί με το Internet
8. Λαμβάνω απάντηση σε όλες εκτός από την 10.0.2.1 η οποία είναι η διεύθυνση υποδικτύου του 10.0.2.0/24
   10.0.2.2 -> gateway
   10.0.2.3 -> DNS server (nameserver)
   10.0.2.4 -> tftp server για remote booting
9. Όχι, δεν επικοινωνεί στο NAT το κάθε μηχάνημα έχει την εντύπωση ότι βρίσκεται στο δικό του ξεχωριστό δίκτυο
10. -I -> icmp , -n δεν κάνει resolve τα names, -q αριθμός δοκιμών ανά hop
11. 10.0.2.15 διεύθυνση πηγής και ICMP echo request
12. πηγή 10.249.137.99 (δηλ ip host)
13. Οι IP των ενδιάμεσων δρομολογητών στα βήματα της traceroute με πρώτη την 10.249.137.25 (δηλαδή του default gateway του host)
14. 10.249.137.99 δηλαδή η διεύθυνση IPv4 του host στο τοπικό δίκτυο
15. Οι διευθύνσεις που εμφανίζονται στο traceroute (ίδιες με 13 + 10.0.2.2)
16. 10.0.2.15
17. Όχι, έχουν διαφορετικές διευθύνσεις και στο tcpdump είναι 6 ενώ στο wireshark 5 σε αριθμό
18. Προφανώς λείπει το πρώτο βήμα του εικονικού μηχανήματος όπου γίνεται το hop με το gateway που τρέχει στον host

Άσκηση 6: Δικτύωση NAT Network

1. 10.0.2.0/24
2. ifconfig em0 delete {ip}
3. dhclient em0
4. PC1 -> 10.0.2.15, PC2 -> 10.0.2.4, πριν σε δικτύωση NAT είχαν την ίδια διεύθυνση 10.0.2.15
5. 10.0.2.3
6. οι DNS servers του host μηχανήματος (περιεχόμενο αρχείου /etc/resolv.conf host
7. 10.0.2.1
8. Ναι
9. Ναι
10. Ναι, το μηχάνημα που απαντάει είναι ο host (ίδια mac με default gateway = host)
11. ping www.google.com
12. Ναι, επικοινωνούν μεταξύ τους
13. Όχι
14. ping σε διεύθυνση 10.0.2.4 (PC2) είναι το φιλοξενούν μηχάνημα, ο tftp server για remote booting. Διαπιστώνω αφού κάνω tcpdump στο PC2, δεν λαμβάνω πακέτο. Επίσης στο arp table του PC3 δεν αντιστοιχεί η MAC διέθυνση του PC2