Εργαστηριακή Άσκηση 2

Δικτύωση Συστημάτων στο VirtualBox

Ονοματεπώνυμο: Άννα Κουτσώνη	**Όνομα PC:** DESKTOP-90FT571
Ομάδα: 1	**Ημερομηνία:** 20/02/2024

Άσκηση 1

1.1. –
1.2. –
1.3. –
1.4. –
1.5. –
1.6. passwd και ntua ως new password
1.7. –
1.8. –
1.9. –
1.10. reboot και ps aux | grep sshd
1.11. rm /etc/resolv.conf και rm /var/db/dhclient.leases.*
1.12. history -c
1.13. –
1.14. –
1.15. –

Άσκηση 2

2.1. Ifconfig
2.2. Απενεργοποίηση: ifconfig em0 down
Ενεργοποίηση: ifconfig em0 up
2.3. man tcpdump, man pcap, man pcap-filter
2.4. tcpdump -i em0 -n
2.5. ASCII: tcpdump -i em0 -A
HEX: tcpdump -i em0 -x
2.6. tcpdump -e
2.7. tcpdump -i em0 -s
2.8. tcpdump host 10.0.0.1 -v
2.9. tcpdump host (10.0.0.1 and 10.0.0.2) -I em0
2.10. tcpdump ip and net 1.1.0.0/16
2.11. tcpdump ip and not net 192.168.1.0/24
2.12. tcpdump ip broadcast or multicast
2.13. tcpdump ‘(len>576)’ ή tcpdump greater 576
2.14. tcpdump ‘(ip[8]<5)’
2.15. tcpdump ‘(ip[0] & 0x0f>5)’
2.16. tcpdump src 10.0.0.1 and icmp
2.17. tcpdump dst 10.0.0.2 and tcp
2.18. tcpdump dst port 53 and udp

2.19. tcpdump host 10.0.0.10 and tcp
2.20. tcpdump host 10.0.0.10 and tcp port 23 -w sample_capture
2.21. tcpdump tcp and 'tcp[tcpflags] & (tcp-syn) != 0'
2.22. tcpdump '(tcp[tcpflags] & tcp-syn != 0) or (tcp[tcpflags] & (tcp-syn|tcp-ack) != 0)'
2.23. tcpdump '(tcp[tcpflags] & tcp-fin!= 0) or (tcp[tcpflags] & (tcp-fin|tcp-ack) != 0)'
2.24. Αρχικά πηγαίνει στο 13ο byte της επικεφαλίδας και ολισθαίνει δεξιά κατά 2 θέσεις τα 4 πρώτα bit του. Στην ουσία τα διαιρεί με το 4 και τα 4 αυτά bit είναι το Data Offset της επικεφαλίδας (TCP Header Length). Άρα τελικά προκύπτει το μέγεθος της επικεφαλίδας σε byte.
2.25. tcpdump '(tcp[12:1] & 0xf0 >> 2) > 5'
Έτσι μπορούμε και να αποφανθούμε για το αν το πακέτο έχει Options ή όχι, διότι ένα πακέτο χωρίς options έχει TCP Header Length =20 , οπότε αν είναι παραπάνω θα υπάρχουν options.
2.26. tcpdump port 80 -A
2.27. tcpdump port 23 and dst 147.102.40.15
2.28. tcpdump ip6

Άσκηση 3

3.1. 192.168.56.1
3.2. IPv4 του εξυπηρετητή DHCP: 192.168.56.100
Περιοχή διευθύνσεων IPv4 που μπορούν να εκχωρηθούν: 192.168.56.101-192.168.56.254
3.3. dhclient em0 σε κάθε virtual machine
3.4. PC1: 192.168.56.103
PC2: 192.168.56.102
(Η εντολή εκτελέστηκε πρώτα στην PC2 και άρα έλαβε πρώτη IPv4 και για αυτό έχει την αριθμητικά πρώτη κατά σειρά IPv4 και το PC1 ακολουθεί)
3.5. Κάνουμε ping από το ένα μηχάνημα στο άλλο και βλέπουμε ότι απαντάνε και τα δύο, άρα επικοινωνούν.
Από το PC1: ping -c 5 192.168.56.102
Από το PC2: ping -c 5 192.168.56.103
3.6. Κάνουμε ping από το terminal του φιλοξενούν μηχανήματος σε κάθε ένα από τα άλλα δύο και βλέπουμε ότι απαντάνε.
Για το PC1: ping -n 5 192.168.56.102
Για το PC2: ping -n 5 192.168.56.103
3.7. netstat -r
3.8. Όχι δεν χρειάζεται γιατί η δικτύωση είναι host-only που σημαίνει ότι υπάρχει επικοινωνία μόνο μεταξύ μηχανημάτων του εσωτερικού δικτύου και όχι με εξωτερικά.
3.9. Όχι. Κάνοντας ping βλέπουμε ότι δεν λαμβάνεται απάντηση και παίρνουμε μήνυμα 'no route to host'. Αυτό συμβαίνει διότι η φυσική κάρτα δικτύου του host machine ανήκει σε εξωτερικό δίκτυο και λόγω της host-only δικτύωση τα virtual machines επικοινωνούν μόνο εντός του εσωτερικού δικτύου. Από την πλευρά του ο host επικοινωνεί με τα vm μέσω μιας virtual κάρτας δικτύου.

3.10. Εντολή: hostname
Όνομα: PC.ntua.lab

3.11. hostname PC1
hostname PC2

3.12. Αμέσως μετά το logout εμφανίζεται το εξής ‘FreeBSD/i386 (PC1) (ttyv0)’ στον PC1 και αντίστοιχα ‘FreeBSD/i386 (PC2) (ttyv0)’ στον PC2. Επίσης μετά το login η προτροπή έχει αλλάξει σε root@PC1 και root@PC2

3.13. Όχι δεν το περιέχει άρα μετά από επανεκκίνηση το όνομα θα επανέλθει σε PC.ntua.lab

3.14. vi /etc/rc.conf και αλλάζουμε το hostname σε PC1 και PC2 αντίστοιχα

3.15. vi /etc/hosts και σε κάθε vm αντίστοιχα προσθέτουμε στο /etc/hosts του PC1 την γραμμή 192.168.56.102 PC2 και στο /etc/hosts του PC2 192.168.56.103 PC1

3.16. ping PC1
ping PC2

3.17. ping -c 3 PC1 : ttl=64
ping -c 3 192.168.56.100 : ttl=255

3.18. tcpdump -n host PC1

3.19. length=64
ttl=64

3.20. tcpdump icmp -vvv

3.21. length=40
Η διαφορά οφείλεται στα λειτουργικά συστήματα.

3.22. TTL=64
Συμφωνεί με τις τιμές προηγουμένως

3.23. tcpdump host PC1 -l -w log
tcpdump host 192.168.56.103 -l -w log

3.24. Όχι δεν παρατηρώ κάποια κίνηση.

3.25. Δεν παρατηρείται κίνηση.

3.26. Καταγράφει όλη την κίνηση του υποδικτύου και όχι μόνο αυτή που αφορά τον PC1 και λαμβάνει τα πακέτα που στέλνονται στον PC2 .

Άσκηση 4

4.1. Για το PC2: ifconfig em0 192.168.56.102
Για το PC1: ifconfig em0 192.168.56.103

4.2. Αφορά τη διακοπή της σύνδεσης με τον DHCP Server και την αποδέσμευση της δυναμικά καταχωρημένης διεύθυνσης από αυτόν.

4.3. tcpdump -vvv

4.4. Όχι, δεν μπορούμε.

4.5. Ναι εμφανίζονται ARP requests για την αναζήτηση της IP του PC2.

4.6. Όχι, δεν μπορούμε.

4.7. Όχι, δεν παρατηρούμε.

4.8. Ναι, επικοινωνούν, αφού βρίσκονται πλέον στο ίδιο εσωτερικό δίκτυο.

4.9. Όχι, γιατί έχουμε Internal Network και το φιλοξενούν μηχάνημα δεν συμμετέχει στο εσωτερικό δίκτυο και δεν επικοινωνεί άρα με τα PC1,PC2.

4.10. tcpdump -n

4.11. ARP Requests με τα οποία ο PC2 αναζητά την MAC Adress του 192.168.56.1 δηλαδή της εικονικής κάρτας του φιλοξενούντος μηχανήματος.

4.12. Ο PC2 δεν παίρνει απάντηση στα ARP Requests και θεωρεί ότι ο host είναι απενεργοποιημένος.

4.13. Οι δύο τελευταίες διαθέσιμες IP του υποδικτύου 10.11.12.0/26 είναι οι 10.11.12.61 και 10.11.12.62 (η 10.11.12.63 είναι broadcast και άρα δεν είναι διαθέσιμη). Εκτελούμε στον PC1 ifconfig em0 10.11.12.61/26 και στον PC2 ifconfig em0 10.11.12.62/26.

4.14. Κάνουμε ping 10.11.12.61 από τον PC2 και ping 10.11.12.62 από τον PC1 και βλέπουμε ότι επικοινωνούν κανονικά.

Άσκηση 5

5.1. dhclient em0

5.2. Είναι η 10.0.2.15 και αποδόθηκε από την διεύθυνση 10.0.2.2

5.3. netstat -r
Default Gateway: 10.0.2.2

5.4. cat /etc/resolv.conf
Το περιεχόμενο του είναι: # Generated by resolvconf
search home
nameserver 192.168.1.1

5.5. Στο αρχείο /var/db/dhclient.leases.em0

5.6. Ναι, μπορούμε

5.7. Ναι επικοινωνεί. Κάνουμε ping www.ntua.gr και βλέπουμε ότι παίρνουμε απάντηση. Η επικοινωνία γίνεται μέσω της προκαθορισμένης πύλης.

5.8. Σε όλες εκτός από την 10.0.2.1 η οποία δεν παριστάνει τίποτα
10.0.2.2 →Default Gateway
10.0.2.3 →Proxy DNS Server
10.0.2.4 →TFTP Server

5.9. Ναι, επικοινωνεί. Κάνουμε ping και βλέπουμε ότι λαμβάνουμε απάντηση.

5.10. -I → Χρήση ICMP
-n → μη αντιστοίχιση των διευθύνσεων σε ονόματα
-q 1 → 1 request ανά βήμα πριν από κάθε αύξηση το TTL
9.9.9.9 → τελική διεύθυνση πακέτων

5.11. ICMP Requests με διεύθυνση πηγής 10.0.2.15

5.12. Είναι η 192.168.1.4 δηλαδή η IPv4 του υπολογιστή στο οικιακό δίκτυο

5.13. Καταγράφηκε μόνο η 192.168.1.1

5.14. 192.168.1.4

5.15. 10.0.2.2 (Default Gateway)
192.168.1.1

5.16. 10.0.2.15 (η IP του εικονικού μηχανήματος)

5.17. Το μήνυμα με διεύθυνση πηγής 192.168.1.1 αντιστοιχεί ναι , ενώ το μήνυμα με διεύθυνση πηγής 10.0.2.2 δεν αντιστοιχεί.

5.18. Προκύπτουν 6 hops δηλαδή 1 λιγότερο από ότι με την traceroute με την οποία προέκυπταν 7 hops. Αυτό συμβαίνει διότι τα πακέτα στο εικονικό μηχάνημα πρέπει να περάσουν και από το gateway του virtual machine και από το gateway του host. Ενώ στο φιλοξενούν μηχάνημα το hop αυτό παραλείπεται.

Άσκηση 6

6.1. 10.0.2.0/24

6.2. Για την διαγραφή της IPv4 από την κάρτα δικτύου: ifconfig em0 delete
Για την διαγραφή του αρχείου: rm /var/db/dhclient.leases.em0

6.3. dhclient em0

6.4. PC1 → 10.0.2.15 (ίδια με πριν)
PC2 → 10.0.2.4 (διαφορετική)

6.5. 10.0.2.3

6.6. cat /etc/resolv.conf
Το περιεχόμενο του είναι: # Generated by resolvconf
search home
nameserver 192.168.1.1

6.7. 10.0.2.1

6.8. Ναι μπορούμε. Κάνουμε ping 10.0.2.1 και λαμβάνουμε απάντηση

6.9. Ναι μπορούμε. Κάνουμε ping 10.0.2.3 και λαμβάνουμε απάντηση

6.10. Ναι μπορούμε. Απαντά το host μηχάνημα αφού βλέπουμε ότι 10.0.2.2 και 10.0.2.1 έχουν την ίδια MAC Address.

6.11. Ναι επικοινωνούν. Κάνουμε ping ww.ntua.gr και λαμβάνουμε απάντηση. Έχουμε NAT Network και η επικοινωνία γίνεται μέσω του Default Gateway.

6.12. Ναι επικοινωνούν. Κάνουμε από τον PC1 ping 10.0.2.4 και από τον PC2 10.0.2.15 και λαμβάνουμε απαντήσεις και στα δύο.

6.13. Ναι μπορούμε. Κάνουμε ping από το PC3 και λαμβάνουμε απάντηση. (Αναμέναμε ότι δεν θα ήταν δυνατό καθώς το PC3 έχει δικτύωση NAT και τα PC1,PC2 δικτύωση NAT Networking)

6.14. Όχι δεν είναι το αντίστοιχο PC που απαντάει. Το διαπιστώνουμε πρώτον κάνοντας tcpdump κατά τη διάρκεια του ping αντίστοιχα σε PC1, PC2 και βλέπουμε ότι παρόλο που ο PC3 λαμβάνει απάντηση στους PC1,PC2 δεν καταγράφεται καμία σχετική κίνηση. Δεύτερον ελέγχοντας

τον arp πίνακα βλέπουμε ότι οι διευθύνσεις MAC που έχουν αντιστοιχιστεί στις IP 10.0.2.15 και 10.0.2.4 δεν ταυτίζονται με τις διευθύνσεις MAC των PC1 και PC2 που βρίσκουμε στους αντίστοιχους πίνακες arp. Η απάντηση στα ping προέρχεται από τον εξυπηρετητή TFTP.