Εργαστήριο Δικτύων Υπολογιστών

Εργαστηριακή άσκηση 2 (Δικτύωση συστημάτων στο VirtualBox)

Τσάκωνας Παναγιώτης (03119610) Ομάδα: 2

Ακαδημαϊκό Έτος: 2023-2024

Άσκηση 2: Ανάλυση δικτυακών πρωτοκόλλων με το TCPDUMP

2.1) ifconfig

2.2) ifconfig em0 down και ifconfig em0 up

2.3) Με το man πριν από κάθε εντολή για κάθε εντολή.

2.4) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω όλα τα πλαίσια από την κάρτα δικτύου em0 χωρίς επίλυση διευθύνσεων IP είναι η: tcpdump -i em0 -n .

2.5) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω όλα τα πλαίσια από την κάρτα δικτύου em0 και να εμφανίσω τα περιεχόμενα τους σε ASCII είναι: tcpdump -i em0 -n -A και για την δεκαεξαδική μορφή είναι: tcpdump -i em0 -n -x .

2.6) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να βλέπω και τις διευθύνσεις MAC πηγής, προορισμού των πλαισίων που συλλαμβάνω είναι: tcpdump -i em0 -e .

2.7) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω από την κάρτα δικτύου em0 τα πρώτα 68 bytes όλων των πλαισίων είναι: tcpdump -i em0 -s 68 .

2.8) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω πακέτα IPv4 με διεύθυνση 10.0.0.1 και να δω τις λεπτομέρειες της επικεφαλίδας τους είναι: tcpdump -i em0 'ip and src or dst 10.0.0.1'.

2.9) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω στην κάρτα δικτύου em0 πακέτα της επικοινωνίας μεταξύ δύο μηχανημάτων με διευθύνσεις 10.0.0.1 και 10.0.0.2 είναι: tcpdump -i em0 'src or dst(10.0.0.1 or 10.0.0.2)'.

2.10) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω πακέτα IPv4 για το δίκτυο 1.1.0.0/16 και να εμφανίσω στην οθόνη το περιεχόμενό τους είναι: tcpdump -i em0 -X 'ip and net 1.1.0.0/16'.

2.11) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω πακέτα IPv4 που δεν ανήκουν (και δεν έπρεπε ποτέ να έχουν φτάσει) στο τοπικό μου δίκτυο, ας πούμε το 192.168.1.0/24, και να τυπώσω

στην οθόνη το περιεχόμενό τους περιλαμβανομένων των επικεφαλίδων Ethernet είναι: tcpdump -i em0 -XX 'ip and dst net 192.168.1.0/24'.

2.12) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω IPv4 πακέτα εκπομπής ή πολλαπλής διανομής είναι: tcpdump -i em0 'ip broadcast' .

2.13) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω πακέτα IPv4 μήκους μεγαλύτερου των 576 byte είναι: tcpdump -i em0 'ip and greater 576'.

2.14) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω πακέτα IPv4 με τιμές TTL μικρότερες του 5 είναι: tcpdump -i em0 'ip and ip[8] < 5'

2.15) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω πακέτα IPv4 με προαιρετικές επικεφαλίδες είναι: tcpdump -i em0 'ip and ip[0] & 0xf !=5.

2.16) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω πακέτα ICMP με αποστολέα την IP διεύθυνση 10.0.0.1 είναι: tcpdump -i em0 'icmp and src 10.0.0.1'.

2.17) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω τεμάχια TCP με παραλήπτη την IP διεύθυνση 10.0.0.2 είναι: tcpdump -i em0 'tcp and dst 10.0.0.2'.

2.18) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω δεδομενογράμματα UDP με θύρα προορισμού 53 είναι: tcpdump -i em0 'udp and dst port 53'.

2.19) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω τεμάχια TCP με διεύθυνση αποστολέα ή παραλήπτη 10.0.0.10 είναι: tcpdump -i em0 'tcp and (src or dst 10.0.0.10)'.

2.20) tcpdump -i em0 -w sample_capture 'tcp and (src or dst 10.0.0.10) and dst port 23'

2.21) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω τεμάχια TCP που περιέχουν μόνο τη σημαία SYN είναι: tcpdump -i em0 'tcp and tcp[tcpflags]&tcp-syn!=0'

2.22) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω τα πρώτα 2 τεμάχια της τριμερούς χειραψίας TCP είναι: tcpdump -i em0 'tcp and tcp[13]=2 or tcp[13]=12'

2.23) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω τα σχετικά με την απόλυση μιας σύνδεσης TCP τεμάχια είναι: tcpdump -i em0 'tcp and ((tcp[tcoflags]&tcp-fin !=0) or (tcp[tcpflags]&(tcp-fin|tcp-ack)) !=0)'

2.24) Η παράσταση ((tcp[12:1] & 0xf0) >> 2) χρησιμοποιούμενη ως στοιχείο φίλτρου για τη σύλληψη τεμαχίων TCP υπολογίζει από το 13ο στη σειρά byte του tcp header τα 4 πρώτα bits, τα οποία αντιστοιχούν στο data offset και αυτή τη τιμή την διαιρεί με το 4 (right shift 2 ">>2"), ώστε να βρούμε σε bytes το μέγεθος του tcp header.

2.25) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω τεμάχια TCP που περιλαμβάνουν προαιρετικές επικεφαλίδες (options) είναι: tcpdump -i em0 'tcp and (tcp[12:1] & 0xf0 >> 2) >20'.

2.26) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω μηνύματα HTTP και να δω το περιεχόμενο ως χαρακτήρες ASCII είναι: tcpdump -i em0 -A 'src or dst port 80'

2.27) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω μηνύματα telnet προς το edu-dy.cn.ntua.gr είναι: tcpdump -i em0 'dst host edu-dy.cn.ntua.gr and port telnet'

2.28) Η σύνταξη της εντολής tcpdump που θα μου επιτρέψει να συλλάβω πακέτα IPv6 είναι: tcpdump -i em0 'ip6'

Άσκηση 3: Δικτύωση Host-only

3.1) Host-only IPv4 : 192.168.56.1

3.2) DHCP Server : 192.168.56.100 με περιοχή διευθύνσεων IPv4 που αυτός μπορεί να εκχωρήσει από 192.168.56.101 έως 192.168.56.254

3.3) Σε κάθε εικονικό μηχάνημα τρέχουμε την dhclient em0 και λαμβάνεται αυτόματα μία διαθέσιμη διεύθυνση IPv4.

3.4) PC1 → 192.168.56.102 και PC2 → 192.168.56.103

3.5) Κάνουμε ping από το ένα μηχάνημα στο άλλο και βλέπουμε ότι υπάρχει επικοινωνία.

3.6) Κάνουμε ping από το φιλοξενούν μηχάνημα προς τα 2 άλλα και βλέπουμε ότι υπάρχει επικοινωνία.

3.7) Η σύνταξη της εντολής που θα μου δείξει την προεπιλεγμένη πύλη είναι η: netstat -r

3.8) Όχι δεν υπάρχει προεπιλεγμένη πύλη, διότι δεν χρειάζεται default gateway στη δικτύωση host-only.

3.9) Όχι, το host μηχάνημα δεν απαντάει στα ping, διότι δεν επικοινωνεί με την φυσική διεύθυνση με τα virtual μηχανήματα αλλά με την εικονική διεύθυνση.

3.10) Με χρήση της εντολής hostname είδα ότι το όνομα των μηχανημάτων είναι το: PC.ntua.lab

3.11) hostname PC1 και hostname PC2 αντίστοιχα.

3.12) Το όνομα έχει αλλάξει και αυτό φαίνεται πάνω από το prompt του login.

3.13) Όχι το αρχείο παραμετροποίησης /etc/rc.conf στο PC1 δεν περιέχει το νέο όνομα και σε ενδεχόμενη επανεκκίνηση θα έχει το παλιό όνομα (PC.ntua.lab) δηλαδή αυτό που υπάρχει στο αρχείο.

3.14) Με vi αλλάζουμε τη παράμετρο hostname του αρχείου σε PC1 και PC2 αντίστοιχα.

3.15) Για το PC1 θα πρέπει να προσθέσουμε την γραμμή '192.168.56.103 PC2' και αντίστοιχα για το PC2.

3.16) Πλέον μπορούμε να κάνουμε ping PC1 και ping PC2 χωρίς να χρειάζεται να ορίσουμε τις διευθύνσεις IPv4 των 2 μηχανημάτων.

3.17) ping PC2 → στέλνει 64 bytes με ttl=64

ping 192.168.56.1 → στέλνει 64 bytes με ttl=128

ping 192.168.56.100 → στέλνει 64 bytes με ttl=255

3.18) tcpdump -i em0 -n -v 'src or dst 192.168.56.103'

3.19) Το μήκος των μηνυμάτων ICMP echo request που λαμβάνει το PC2 είναι 64 Bytes και η τιμή του πεδίου TTL είναι 64.

3.20) tcpdump -i em0 -vvv icmp

3.21) Το μήκος των μηνυμάτων ICMP echo request που παράγει το φιλοξενούν μηχάνημα είναι 40 bytes και αυτό συμβαίνει επειδή είναι διαφορετικό το λειτουργικό σύστημα.

3.22) Η τιμή του πεδίου TTL των πακέτων IPv4 που ανταλλάσσουν τα δύο μηχανήματα είναι 64 και είναι η ίδια.

3.23) tcpdump -i em0 -n -vvv -l 'icmp' | tee dat και `tcpdump -i em0 -n -vvv -l 'icmp' | dat & tail -f dat

3.24) Δεν παρατήρησα κάποια καταγραφή.

3.25) Παρατηρώ ότι κάθε 300s δημιουργείται κίνηση DHCP ώστε να ανανεώνονται αν χρειαστεί οι διευθύνσεις των μηχανών καθώς και μια κίνηση UDP πακέτων.

3.26) Αφού επιτρέπεται η κίνηση που αφορά τα VMs βλέπουμε και τα ICMP πακέτα με προορισμό το PC2.

Άσκηση 4: Δικτύωση Internal

4.1) ifconfig em0 192.168.56.103

4.2) Το μήνυμα λάθους που εμφανίσθηκε όταν όρισα στατικές διευθύνσεις είναι ότι θα έπρεπε να προσδιορίσω και μάσκα δικτύου, η οποία αφού δεν προσδιορίστηκε χρησιμοποιήθηκε by default η συνήθης 255.255.255.0 .

4.3) tcpdump -i em0 -vvv

4.4) Όχι δεν μπορώ να κάνω από το φιλοξενούν μηχάνημα ping στο PC2, εμφανίζει μήνυμα 'Destination Host Unreachable'.

4.5) Ναι παρατηρώ κίνηση, η οποία αφορά τα ARP πακέτα.

4.6) Όχι, δεν μπορώ από το PC2 να κάνετε ping στο PC1.

4.7) Όχι δεν παρατηρώ από την καταγραφή κίνηση σχετική με το ping προς το PC1.

4.8) Ναι επικοινωνούν τώρα τα 2 μηχανήματα.

4.9) Όχι δεν μπορώ να επικοινωνήσω από το φιλοξενούν μηχάνημα, διότι σε Internal mode τα δίκτυα που δημιουργούμε είναι ορατά μόνο μεταξύ των VMs.

4.10) tcpdump -i em0 -n

4.11) Διαγράφουμε τα entries με arp -d -a και βλέπουμε ότι το PC2 στέλνει ARP μηνύματα προς όλους ώστε να βρει την φυσική διεύθυνση του 192.168.56.1. αυτό δεν μπορεί να γίνει, αφού δεν είναι δυνατή η επικοινωνία με το φιλοξενούν μηχάνημα και έτσι δεν θα πάρει απάντηση ποτέ.

4.12) Αφού δεν παίρνει απάντηση μετά από κάποιο διάστημα συμπεραίνει πως δεν υπάρχει επικοινωνία με τον host και έτσι εμφανίζει το μήνυμα host is down.

4.13) ifconfig em0 10.11.12.62 για το PC1 και ifconfig em0 10.11.12.63 για το PC2

4.14) Ναι επικοινωνούν τα 2 μηχανήματα.

Άσκηση 5: Δικτύωση NAT

5.1) dhclient em0

5.2) Όλα τα μηχανήματα έλαβαν τη διεύθυνση 10.0.2.15 από τον 10.0.2.2

5.3) Η προεπιλεγμένη πύλη στον πίνακα δρομολόγησης είναι η 10.0.2.2 και την βρήκα με την εντολή: netstat -r

5.4) Το περιεχόμενο του αρχείου /etc/resolv.conf είναι: 'nameserver 1.0.0.2' , 'nameserver 1.1.1.2'

5.5) Η διεύθυνση IPv4 που αποδόθηκε προηγουμένως μέσω DHCP καθώς και οι πληροφορίες που περιέχει το resolv.conf υπάρχουν στο αρχείο /var/db/dhclient.leases.em0

5.6) Ναι μπορούμε να κάνουμε από τα εικονικά μηχανήματα ping στη διεύθυνση IPv4 της προεπιλεγμένης πύλης.

5.7) Κάνοντας ping 1.1.1.1 βλέπουμε ότι μπορούμε να επικοινωνήσουμε με το Internet, αυτό συμβαίνει επειδή βρισκόμαστε σε NAT network mode και τα μηχανήματα μπορούν να κάνουν μόνο εξερχόμενες συνδέσεις.

5.8) Απάντηση λαμβάνουμε σε όλες εκτός από την 10.0.2.1. Η 10.0.2.2 είναι το default gateway, η 10.0.2.3 είναι ο nameserver (DNS) και η 10.0.2.4 είναι ο TFTP server.

5.9) Όχι το νέο μηχάνημα (PC3) δεν επικοινωνεί με τα άλλα 2, καθώς κάθε μηχάνημα βλέπει ότι ανήκει σε ένα δικό του δίκτυο και όλα έχουν την ίδια διεύθυνση.

5.10) Το -I option αναγκάζει το traceroute να χρησιμοποιεί ICMP ECHO μηνύματα αντί για UDP datagrams, το -n τυπώνει τις hop διευθύνσεις ως νούμερα, οι οποίες δεν γίνονται resolve και το -q 1 ορίζει το πλήθος των προσπαθειών ανά hop σε 1.

5.11) Έχουμε ένα ICMP ECHO request από την 10.0.2.15.

5.12) Στο Wireshark η διεύθυνση πηγής του ICMP ECHO request είναι η 192.168.1.2

5.13) 192.168.1.1, 80.106.125.100, 79.128.240.188, 79.128.224.179, 176.126.38.5

5.14) 192.168.1.2

5.15) Είναι οι ίδιες απλά υπάρχει και η 10.0.2.2

5.16) 10.0.2.15

5.17) Όχι δεν υπάρχει ένα προς ένα αντιστοιχία, υπάρχει ένα επιπλέον, αυτό που στάλθηκε από τη default gateway προς το VM το οποίο είναι αναμενόμενο να μην είναι ορατό στον host.

5.18) Η traceroute -n 9.9.9.9 στον host εμφάνισε ένα λιγότερο hop αφού πλέον δεν υπάρχει στη διαδρομή η default gateway του VM.

Άσκηση 6: Δικτύωση NAT Network

6.1) Η διεύθυνση του δικτύου NAT που έχει οριστεί στο VirtualBox είναι η 10.0.2.0

6.2) ifconfig em0 delete

6.3) dhclient em0

6.4) Το PC1 έχει την ίδια με πριν την 10.0.2.15, ενώ το PC2 λαμβάνει διαφορετική, την 10.0.2.4

6.5) Η διεύθυνση IPv4 του εξυπηρετητή DHCP είναι η: 10.0.2.3

6.6) Το περιεχόμενο του αρχείου /etc/resolv.conf είναι: 'nameserver 192.168.2.1'

6.7) Η προεπιλεγμένη πύλη στον πίνακα δρομολόγησης είναι η: 10.0.2.1

6.8) Ναι μπορώ να κάνω ping στην IPv4 διεύθυνση της προεπιλεγμένης πύλης από τα εικονικά μηχανήματα PC1, PC2.

6.9) Ναι μπορώ να κάνω ping στην IPv4 διεύθυνση του εξυπηρετητή DHCP από τα εικονικά μηχανήματα PC1, PC2.

6.10) Ναι μπορώ να κάνω ping στην διεύθυνση 10.0.2.2 από τα εικονικά μηχανήματα PC1, PC2 και αυτός που απαντά είναι ο host.

6.11) Ναι υπάρχει επικοινωνία με το διαδίκτυο, διότι είμαστε σε NAT δίκτυο.

6.12) Ναι επικοινωνούν τα PC1, PC2 μεταξύ τους, διότι βρίσκονται στο ίδιο Internal Network.

6.13) Ναι μπορώ από το PC3 να κάνω ping στα PC1, PC2 και απαντάει ο tftp server για τη διεύθυνση που τελειώνει σε 15.

6.14) Ναι, αυτό φαίνεται με χρήση της traceroute το οποίο μας δείχνει ότι υπάρχει ένα μόνο hop για να έρθει η απάντηση.