Εργαστήριο Δικτύων Υπολογιστών

Εργαστηριακή Άσκηση 2
Δικτύωση συστημάτων στο VirtualBox

Ονοματεπώνυμο: Νικόλαος Παγώνας, el18175	**Όνομα PC:** nick-ubuntu
Ομάδα: 1 (Τρίτη 10:45)	**Ημερομηνία Εξέτασης:** Τρίτη 08/03/2022

Άσκηση 1 (προετοιμασία): Δημιουργία εικονικού FreeBSD

1.1

Επισκεπτόμαστε την ιστοσελίδα της εκφώνησης και εντοπίζουμε τα VM images για επεξεργαστές `i386`.

1.2

Κατεβάζουμε το αντίστοιχο αρχείο και το αποσυμπιέζουμε.

1.3

Δημιουργούμε ένα νέο εικονικό μηχάνημα στο VirtualBox με τα ζητούμενα χαρακτηριστικά.

1.4

Από το γραφικό περιβάλλον του VirtualBox αλλάζουμε τις ζητούμενες παραμέτρους για μνήμη γραφικών, USB και Network.

1.5

Ξεκινάμε το εικονικό μηχάνημα και κάνουμε login ως root.

1.6

Με τη βοήθεια της εντολής `passwd` ορίζουμε συνθηματικό `ntua` για τον root.

1.7

Με τη βοήθεια της εντολής `adduser` δημιουργούμε έναν νέο χρήστη `lab` που έχει τα ζητούμενα χαρακτηριστικά.

1.8

Στο αρχείο `/etc/rc.conf` προσθέτουμε τις ζητούμενες γραμμές, διαγράφοντας ό,τι υπάρχει.

1.9

Δημιουργούμε το αρχείο `/boot/loader.conf`, το οποίο περιέχει τη ζητούμενη εντολή για επιτάχυνση της διαδικασίας εκκίνησης.

1.10

Επανεκκινούμε το FreeBSD χωρίς προβλήματα και με την εντολή `service -e | grep sshd` βεβαιωνόμαστε ότι η υπηρεσία `sshd` τρέχει.

1.11

Διαγράφουμε το ιστορικό των εντολών που δώσαμε μέχρι το σημείο αυτό με την εντολή `history -c`.

1.12

Διαγράφουμε όποιο αρχείο `/var/db/dhclient.leases.*` έχει δημιουργηθεί κατά την εκκίνηση με την εντολή `rm /var/db/dhclient.leases.*`.

1.13

Κλείνουμε το εικονικό μηχάνημα με την εντολή `poweroff`.

1.14

Από τη διαδρομή File→Export Appliance... δημιουργούμε ένα αρχείο `FreeBSD11.4.ova`.

1.15

Αποθηκεύουμε το αρχείο `.ova` για μελλοντική χρήση και διαγράφουμε το αρχείο `.vhd`, αφού δεν χρειάζεται πλέον.

Άσκηση 2: Ανάλυση δικτυακών πρωτοκόλλων με το TCPDUMP

2.1

Με την εντολή `ifconfig`.

2.2

Με τις εντολές `ifconfig em0 down` και ύστερα `ifconfig em0 up`.

2.3

Με τις εντολές `man tcpdump`, `man pcap` και `man pcap-filter`.

2.4

Η σύνταξη είναι: `tcpdump -i em0 -n`.

2.5

Η σύνταξη είναι: `tcpdump -i em0 -X`.

2.6

Η σύνταξη είναι: `tcpdump -e`.

2.7

Η σύνταξη είναι: `tcpdump -i em0 -s 68`.

2.8

Η σύνταξη είναι:
`tcpdump -v "ip && host 10.0.0.1"` ή `tcpdump -v "ip && (src or dst 10.0.0.1)"`.

2.9

Η σύνταξη είναι:
`tcpdump -i em0 "(src 10.0.0.1 && dst 10.0.0.2) || (src 10.0.0.2 && dst 10.0.0.1)"`.

2.10

Η σύνταξη είναι: `tcpdump -x "ip && net 1.1.0.0/16"`.

2.11

Η σύνταξη είναι: `tcpdump -e -x "ip && (!net 192.168.1.0/24)"`.

2.12

Η σύνταξη είναι: `tcpdump "ip && broadcast"`.

2.13

Η σύνταξη είναι: `tcpdump "ip[2:2] > 576"`.

2.14

Η σύνταξη είναι: `tcpdump "ip[8:1] < 5"`.

2.15

Η σύνταξη είναι: `tcpdump "ip[0:1] & 0x0f > 5`.

2.16

Η σύνταξη είναι: `tcpdump "icmp && (src 10.0.0.1)"`.

2.17

Η σύνταξη είναι: `tcpdump "tcp && (dst 10.0.0.2)"`.

2.18

Η σύνταξη είναι: `tcpdump "udp && (dst port 53)"`.

2.19

Η σύνταξη είναι: `tcpdump "tcp && (src or dst 10.0.0.10)"`.

2.20

Η τροποποιημένη σύνταξη είναι:
`tcpdump -w sample_capture "tcp && (src or dst 10.0.0.10) && (dst port 23)"`.

2.21

Η σύνταξη είναι: `tcpdump "tcp[13:1] & 0xff == 2"`.

2.22

Η σύνταξη είναι: `tcpdump "tcp[13:1] & 0xff == 2 || tcp[13:1] & 0xff == 18"`.

2.23

Η σύνταξη είναι: `tcpdump "tcp[13:1] & 0xff == 17"`.

2.24

Η παράσταση αυτή απομονώνει την τιμή του Data Offset, και λόγω τις δεξιάς ολίσθησης κατά 2 θέσεις μας δίνει τελικά το μέγεθος του TCP Header μετρημένο σε bytes.

2.25

Η σύνταξη είναι: `tcpdump "((tcp[12:1] & 0xf0) >> 2) > 20"`.

2.26

Η σύνταξη είναι: `tcpdump -A "port 80"`.

2.27

Η σύνταξη είναι: `tcpdump "dst edu-dy.cn.ntua.gr && dst port 23"`.

2.28

Η σύνταξη είναι: `tcpdump "ip6"`.

Άσκηση 3: Δικτύωση Host-only

3.1

Από τη διαδρομή: "File→Host Network Manager→Adapter" βρίσκουμε ότι η IPv4 διεύθυνση του Host-only Ethernet adapter είναι `192.168.56.1`.

3.2

Από τη διαδρομή "File→Host Network Manager→DHCP Server" βρίσκουμε ότι η IPv4 διεύθυνση του DHCP Server είναι `192.168.56.100`, ενώ η περιοχή διευθύνσεων που μπορεί να εκχωρήσει είναι `192.168.56.101-192.168.56.254`.

3.3

Με την εντολή `dhclient em0` αποδίδουμε διευθύνσεις μέσω DHCP στα εικονικά μηχανήματα.

3.4

Στο PC1 αποδόθηκε η διεύθυνση `192.168.56.102`, ενώ στο PC2 αποδόθηκε η διεύθυνση `192.168.56.103`.

3.5

Θα εκτελέσουμε `ping 192.168.56.102` από το PC2 ή `ping 192.168.56.103` από το PC1.

Εναλλακτικά για να έχουμε καλύτερη εποπτεία της επικοινωνίας θα μπορούσαμε να τρέξουμε και `nc -l <port>` από το ένα μηχάνημα (πχ το PC1), και από το άλλο να τρέξουμε `nc <PC1 ip> <port>`, όπου `port > 1024`. Ύστερα γράφουμε ένα μήνυμα (πχ hello) και πατάμε <enter> σε οποιαδήποτε από τις δύο κονσόλες. Το μήνυμα θα πρέπει να μεταφέρεται αυτούσιο στην κονσόλα του άλλου vm.

3.6

Θα εκτελέσουμε `ping 192.168.56.102` ή `ping 192.168.56.103` από το φιλοξενούν μηχάνημα.

Εναλλακτικά μπορούμε να ακολουθήσουμε την ίδια διαδικασία με το `nc` που περιγράψαμε παραπάνω.

3.7

Η σύνταξη της εντολής που δείχνει την προεπιλεγμένη πύλη είναι `netstat -rn`.

3.8

Όχι, δεν υπάρχει προεπιλεγμένη πύλη, αφού έχουμε Host-only networking, οπότε δεν υπάρχει επικοινωνία με εξωτερικά δίκτυα, αλλά μόνο με μηχανήματα που υπάρχουν στο εσωτερικό δίκτυο (συμπεριλαμβανομένου του host).

3.9

Όχι, δεν μπορούμε να κάνουμε ping στην φυσική κάρτα δικτύου του φιλοξενούντος μηχανήματος, αφού έχουμε λειτουργία Host-only networking και η φυσική κάρτα δικτύου θεωρείται ότι ανήκει σε εξωτερικό δίκτυο.

3.10

Το όνομα των μηχανημάτων όπως το αντιλαμβάνεται το λειτουργικό τους σύστημα είναι `PC.ntua.lab`, το οποίο βρέθηκε με την εντολή `hostname`.

3.11

Με την εντολή `hostname PC1` και την εντολή `hostname PC2` μετονομάζουμε τα εικονικά μηχανήματα σε `PC1` και `PC2` αντίστοιχα.

3.12

Με το που κάνουμε logout εμφανίζεται το εξής μήνυμα στον PC1 και τον PC2 αντίστοιχα, χωρίς εμείς να εκτελέσουμε κάποια επιπλέον εντολή:

Σε κάθε μηχάνημα, το νέο όνομα που αποδώσαμε φαίνεται στην παρένθεση.
Αφού κάνουμε login, αυτό φαίνεται και στο prompt:

```
root@PC1:~ #

root@PC2:~ #
```

3.13

Το `/etc/rc.conf` στο PC1 δεν περιέχει το νέο όνομα, οπότε σε περίπτωση επανεκκίνησής του το όνομα θα γίνει `PC.ntua.lab`.

3.14

Με `vi /etc/rc.conf` αντικαθιστούμε το `PC.ntua.lab` με `PC1`, `PC2` αντίστοιχα.

3.15

Πρέπει να προσθέσουμε στο `/etc/hosts` τις γραμμές:

```
192.168.56.102 PC1
192.168.56.103 PC2
```

3.16

Ένα σύνηθες παράδειγμα είναι η χρήση του `localhost`, πχ `ping localhost`.

3.17

Δύο τρόποι είναι:

- `tcpdump -l "icmp && host PC1" | tee test`
- `tcpdump -l "icpm && host PC1" > test & tail -f test`

3.18

Το μήκος των μηνυμάτων ICMP είναι 64 bytes και το TTL τους είναι 64.

3.19

Η τιμή του πεδίου TTL της απάντησης είναι 64.

3.20

Η σύνταξη της εντολής `tcpdump` που χρησιμοποιήσαμε είναι: `tcpdump -v "icmp"`. Θα μπορούσαμε να βάλουμε παραπάνω verbosity (πχ. `tcpdump -vv "icmp"`), αλλά δεν θα έκανε διαφορά στην συγκεκριμένη περίπτωση.

3.21

Το μήκος των μηνυμάτων ICMP που παράγει το φιλοξενούν μηχάνημα είναι 64 bytes, όπως και πριν.

3.22

Η τιμή του TTL είναι 64 και συμφωνεί με την τιμή που βρήκαμε προηγουμένως.

3.23

Όχι, δεν παρατηρήθηκε κάποια κίνηση σχετική με το ping, αφού το PC1 καταγράφει κίνηση που αφορά μόνο την κάρτα δικτύου του.

3.24

Αυτή τη φορά παρατηρούμε την σχετική με το ping κίνηση, αφού με το Allow VMs καταγράφεται στο PC1 και κίνηση που αφορά και τις άλλες εικονικές μηχανές που βρίσκονται στο ίδιο δίκτυο.

Άσκηση 4: Δικτύωση Internal

4.1

Η σύνταξη της εντολής που χρησιμοποιήσαμε για να ορίσουμε τις στατικές διευθύνσεις είναι: `ifconfig em0 192.168.56.102/24` (για το PC1) και `ifconfig em0 192.168.56.103/24` (για το PC2).

4.2

Το μήνυμα λάθους που εμφανίστηκε όταν ορίσαμε στατικές διευθύνσεις οφείλεται στο ότι ακόμα λειτουργεί ο dhcp client. Αν ξαναεκτελέσουμε την παραπάνω εντολή, δεν θα εμφανιστεί το μήνυμα λάθους διότι έχει πλέον απενεργοποιηθεί η υπηρεσία dhcp για το συγκεκριμένο μηχάνημα.

4.3

Με `tcpdump -v` στο PC1 ξεκινάμε τη ζητούμενη καταγραφή.

4.4

Όχι, δεν μπορούμε να κάνουμε `ping 192.168.56.103` (δηλαδή στο PC2).

4.5

Παρατηρούνται μόνο ARP Requests από το φιλοξενούν μηχάνημα, το οποίο θέλει να μάθει την φυσική διεύθυνση του PC2.

4.6

Όχι, δεν μπορούμε να κάνουμε `ping PC1`.

4.7

Όχι, δεν παρατηρούμε κίνηση σχετική με το ping προς το PC1.

4.8

Ναι, πλέον τα δύο εικονικά μηχανήματα επικοινωνούν, αφού βρίσκονται στο ίδιο εσωτερικό δίκτυο.

4.9

Όχι, δεν μπορούμε να επικοινωνήσουμε με κανένα από τα δύο εικονικά μηχανήματα, αφού στο mode ”Internal Network” δεν συμμετέχει καθόλου ο host.

4.10

Με την εντολή `tcpdump -n` ξεκινάμε μία νέα καταγραφή στο PC1, χωρίς επίλυση διευθύνσεων IPv4 σε ονόματα.

4.11

Με την εντολή `arp -d -a` αδειάζουμε τον πίνακα arp του PC2, και ύστερα κάνουμε ping από το PC2 προς την εικονική κάρτα δικτύου του host. Παρατηρούμε στην καταγραφή πλαίσια ARP Request που θέλουν να μάθουν την φυσική διεύθυνση της εικονικής κάρτας του host.

4.12

Επειδή τώρα ο host δεν συμμετέχει στο δίκτυο των εικονικών μηχανών, δεν απαντάει κανείς στο ping, εξού και το μήνυμα `host is down`, αφού θεωρείται ότι ο host είναι απενεργοποιημένος.

4.13

Με την εντολή `ifconfig em0 10.11.12.61/26` δίνουμε την προτελευταία διαθέσιμη διεύθυνση του υποδικτύου στο PC1, ενώ με την εντολή `ifconfig em0 10.11.12.62/26` δίνουμε την τελευταία διαθέσιμη διεύθυνση του υποδικτύου στο PC2. Η διεύθυνση `10.11.12.63/26` είναι η διεύθυνση broadcast, και άρα δεν είναι διαθέσιμη.

4.14

Ναι, τα δύο μηχανήματα επικοινωνούν μεταξύ τους με τις νέες διευθύνσεις που ορίσαμε προηγουμένως.

Άσκηση 5: Δικτύωση NAT

5.1

Με την εντολή `dhclient em0` σε καθένα από τα PC{1,2,3}, αποδίδουμε IPv4 διεύθυνση στην διεπαφή `em0` των εικονικών μηχανημάτων, με DHCP.

5.2

Και τα 3 μηχανήματα έχουν λάβει τη διεύθυνση IPv4 `10.0.2.15`, η οποία αποδόθηκε από τη διεύθυνση `10.0.2.2`, δηλαδή από τον host, ο οποίος λειτουργεί και ως DHCP Server.

5.3

Με την εντολή `netstat -rn` βλέπουμε ότι η προεπιλεγμένη πύλη είναι η διεύθυνση `10.0.2.2`, δηλαδή ο host.

5.4

Με `cat /etc/resolv.conf` βλέπουμε ότι το περιεχόμενο του αρχείου είναι:

```
# Generated by resolvconf
nameserver 10.0.2.3
```

5.5

Οι πληροφορίες αυτές έχουν καταγραφεί στο `/var/db/dhclient.leases.em0`.

5.6

Ναι, μπορούμε να κάνουμε `ping 10.0.2.2`.

5.7

Ναι, το νέο μηχάνημα επικοινωνεί με το Internet. Αν κάνουμε πχ `ping google.com`, βλέπουμε ότι στέλνονται επιτυχώς πακέτα. Αυτό συμβαίνει διότι στο NAT mode γίνεται μετάφραση των διευθύνσεων IP ώστε η προέλευση των πακέτων να φαίνεται ότι είναι η προκαθορισμένη πύλη (`10.0.2.2`).

5.8

Αν κάνουμε ping στις 4 αυτές διευθύνσεις, λαμβάνουμε απάντηση από όλες εκτός από την `10.0.2.1`. Οι διευθύνσεις αυτές παριστάνουν:

- `10.0.2.1` → Τίποτα
- `10.0.2.2` → Host/Default Gateway/DHCP Server
- `10.0.2.3` → Proxy DNS server
- `10.0.2.4` → TFTP Server για εκκίνηση του φιλοξενούμενου μηχανήματος από το δίκτυο

5.9

Όχι, δεν επικοινωνεί, διότι κάθε εικονικό μηχάνημα βρίσκεται σε δικό του δίκτυο, το οποίο έχει προκαθορισμένη πύλη τον host.

5.10

Η σημασία των παραμέτρων στην εντολή `traceroute` είναι:

- `-I` → χρήση πακέτων ICMP για τις ανάγκες τις εντολής
- `-n` → μη αντιστοίχιση των διευθύνσεων IP σε ονόματα
- `-q 1` → χρήση ενός πακέτου σε κάθε διαδοχική προσπάθεια της εντολής (αντί για 3 που είναι το default)
- `1.1.1.1` → η διεύθυνση-στόχος

5.11

Σύμφωνα με την καταγραφή του tcpdump, η διεύθυνση πηγής των μηνυμάτων ICMP που παράγει η `traceroute` είναι `10.0.2.15`, δηλαδή η διεύθυνση της διεπαφής του guest, και ο τύπος τους είναι `ICMP Echo Request`.

5.12

Σύμφωνα με την καταγραφή του Wireshark, η διεύθυνση πηγής των αντίστοιχων μηνυμάτων ICMP είναι `192.168.1.42`, δηλαδή η διεύθυνση της διεπαφής του host.

5.13

Οι διευθύνσεις πηγής των μηνυμάτων ICMP τύπου "TTL exceeded in transit" στην καταγραφή του Wireshark είναι `192.168.1.1` και `62.38.0.170`.

5.14

Η διεύθυνση προορισμού των μηνυμάτων αυτών είναι η `192.168.1.42`.

5.15

Σύμφωνα με την καταγραφή του tcpdump, οι διευθύνσεις IPv4 πηγής των μηνυμάτων ICMP τύπου "TTL exceeded in transit" είναι `10.0.2.2`, `192.168.1.1` και `62.38.0.170`.

5.16

Η διεύθυνση προορισμού των μηνυμάτων αυτών είναι η `10.0.2.15` .

5.17

Τα 2 από τα 3 μηνύματα "TTL exceeded in transit" της καταγραφής του tcpdump έχουν αντιστοίχιση σε αυτά της καταγραφής του Wireshark. Το πρώτο από τα τρία μηνύματα (αυτό με διεύθυνση πηγής `10.0.2.2`) όμως, εμφανίζεται μόνο στην καταγραφή του tcpdump, αφού γίνεται αντιληπτό μόνο από το φιλοξενούμενο μηχάνημα (επειδή μηδενίζεται το TTL στην προκαθορισμένη πύλη `10.0.2.2`).

5.18

Εκτελούμε την εντολή `traceroute -n 1.1.1.1` (η αντίστοιχη της `tracert -d 1.1.1.1` σε Linux) από το φιλοξενούν μηχάνημα. Το πλήθος των hops που προκύπτει είναι κατά 1 μικρότερο από αυτό που εμφάνισε η traceroute στο εικονικό μηχάνημα (7 αντί για 8), επειδή στο εικονικό μηχάνημα γίνεται και το επιπλέον hop guest $\rightarrow$ host.

Άσκηση 6: Δικτύωση NAT Network

6.1

Η διεύθυνση του δικτύου NAT που έχει οριστεί στο VirtualBox είναι `10.0.2.0/24`.

6.2

Με `ifconfig em0 delete` στα μηχανήματα PC{1,2} διαγράφουμε τη διεύθυνση IPv4 από την κάρτα δικτύου, ενώ διαγράφουμε (με `rm`) και το αρχείο `/var/db/dhclient.leases.em0`.

6.3

Με την εντολή `dhclient em0` δίνουμε μέσω DHCP διευθύνσεις IPv4 στα εικονικά μηχανήματα PC1, PC2.

6.4

Στο PC1 αποδόθηκε η διεύθυνση `10.0.2.15` (ίδια με πριν), ενώ στο PC2 αποδόθηκε η διεύθυνση `10.0.2.4` (διαφορετική απ' ό,τι πριν).

6.5

Η διεύθυνση του DHCP Server είναι `10.0.2.3`.

6.6

Κάνοντας `cat /etc/resolv.conf` βλέπουμε ότι το περιεχόμενο του αρχείου είναι:

```
# Generated by resolvconf
search home
nameserver 10.0.2.1
```

6.7

Κάνοντας `netstat -r` βλέπουμε ότι η προεπιλεγμένη πύλη στον πίνακα δρομολόγησης είναι η `10.0.2.1`

6.8

Ναι, μπορούμε να κάνουμε `ping` στην IPv4 διεύθυνση της προεπιλεγμένης πύλης από τα PC{1,2}.

6.9

Ναι, μπορούμε να κάνουμε `ping` στην IPv4 διεύθυνση του εξυπηρετητή DHCP και από τα δύο μηχανήματα.

6.10

Από τα PC{1,2} μπορούμε να κάνουμε `ping` στη διεύθυνση `10.0.2.2`, και απαντά το φιλοξενούν μηχάνημα, όπως φαίνεται και από τον πίνακα `arp`.

6.11

Ναι, τα δύο μηνύματα επικοινωνούν, γιατί αν πχ κάνουμε `ping google.com` θα είναι επιτυχές. Αυτό είναι λογικό, διότι στο mode NAT Network τα εικονικά μηχανήματα επικοινωνούν με το Internet μέσω του default gateway.

6.12

Ναι, τα PC1, PC2 επικοινωνούν μεταξύ τους, αφού στο mode NAT Network βρίσκονται στο ίδιο δίκτυο.

6.13

Όχι, δεν μπορούμε από το PC3 να κάνουμε `ping` στα άλλα δύο μηχανήματα, διότι το PC3 είναι ακόμη σε NAT Mode, και βρίσκεται απομονωμένο από το NAT Network των άλλων δύο.

6.14

Αφού κάνουμε `ping 10.0.2.15` (υποτίθεται στο PC1) και `ping 10.0.2.4` (υποτίθεται στο PC2), παίρνουμε απάντηση και στα δύο. Όμως, αν παρατηρήσουμε τον πίνακα `arp` του PC3, θα δούμε ότι οι φυσικές διευθύνσεις που αντιστοιχούν στις `10.0.2.4` και `10.0.2.15` δεν είναι ίδιες με αυτές των μηχανημάτων PC{1,2}. Συγκεκριμένα, η φυσική διεύθυνση που αντιστοιχεί στην `10.0.2.15` είναι του ίδιου του μηχανήματος PC3, ενώ η φυσική διεύθυνση που αντιστοιχεί στην `10.0.2.4` είναι αυτή του εξυπηρετητή TFTP.