ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΓΚΟΥΜΕ ΛΑΟΥΡΕΝΤΙΑΝ
ΑΜ: 031 18 014
ΕΞΑΜΗΝΟ: 8^{ο}
ΟΜΑΔΑ: 3

ΕΡΓΑΣΤΗΡΙΟ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 1: ΕΞΟΙΚΕΙΩΣΗ ΜΕ ΤΟ FreeBSD ΚΑΙ VirtualBox

Άσκηση 1: Γνωριμία με το περιβάλλον εργασίας

1.1) IPv4 address: 192.168.56.1

1.2) Mask: /24 ή ισοδύναμα: 255.255.255.0

1.3) Ναι.

1.4) DHCP Server IPv4 address: 192.168.56.100. Περιοχή διευθύνσεων για δυναμική παραχώρηση από 192.168.56.101 (Lower Bound) έως 192.168.56.254 (Upper Bound).

1.5) Εμφανίζεται το παρακάτω prompt:

```
lab@pc:~ %
```

1.6) Με την εντολή “man” λαμβάνουμε την εξής απάντηση:

```
lab@pc:~ % man
What manual page do you want?
```

1.7) Με την εντολή “man man” εμφανίζεται το manual page για την εντολή man.

1.8) Με την εντολή “man hier” εμφανίζεται η προκαθορισμένη ιεραρχία του συστήματος αρχείων του FreeBSD.

1.9) Ο κατάλογος /lib περιέχει κρίσιμες βιβλιοθήκες συστήματος απαραίτητες για τους καταλόγους /bin και /sbin.

1.10) Στον κατάλογο /var/mail.

1.11) Περιηγούμαστε με τα εξής πλήκτρα: άνω/κάτω βελάκι, page up/down, home/end.

1.12) Εάν θέλουμε για παράδειγμα να αναζητήσουμε τη λέξη word, τότε θα εκτελέσουμε την εντολή man less ως εξής: “man less | grep word”.

1.13) Η διαφορά είναι πως το less μας επιτρέπει να κάνουμε backward movement στο αρχείο.

1.14) Όνομα εικονικού μηχανήματος: pc.ntua.lab (εντολή: “hostname”)

1.15) Όνομα χρήστη: lab. (εντολή: “whoami”)

1.16) Αριθμός ταυτότητας (uid): 1001. (εντολή “id”)

1.17) Στις ομάδες: lab(1001) και wheel(0). (εντολή “id”)

1.18) Τρέχων φάκελος εργασίας: /usr/home/lab. (εντολή “pwd”)

1.19) Εμφανίζεται το εξής:

1.20) Αριθμός ταυτότητας (uid): 0.

1.21) Ανήκει στις: wheel(0) και operator(5).

1.22) Είναι 0.

1.23) Είναι /root.

1.24) Αποδόθηκε η IPv4: 192.168.56.101.

1.25) Με την εντολή “ifconfig” βλέπουμε πως διαθέτει 2. (η loopback δεν έχει φυσική μορφή, είναι software διεπαφή).

1.26) em0 MAC: 08:00:27:b7:46:61. (εντολή: “ifconfig”)

1.27) Είναι 1Gbps (1000baseT). (εντολή: “ifconfig”)

1.28) IPv4: 192.168.56.101. (εντολή: “ifconfig”)

1.29) Μάσκα υποδικτύου σε δεκαδική μορφή: 255.255.255.0. (εντολή: “ifconfig”)

1.30) MTU: 1500. (εντολή: “ifconfig”)

1.31) Σχετικά με τις λεπτομέρειες για την loopback, με την εντολή “ifconfig”, βλέπουμε τα παρακάτω:

- 127.0.0.1
- 255.0.0.0
- MTU: 16384

1.32) Όχι, δεν έχουν οριστεί. (εντολή: “cat /etc/resolv.conf”).

1.33) Όχι, δε μας απαντάει. (εντολή “ping -c 4 10.3.20.60”, από το guest machine). Δοκιμάζοντας να απενεργοποιήσουμε το firewall στα Windows, είχαμε το ίδιο αποτέλεσμα.

```
root@pc:~ # ping -c 4 10.3.20.60
PING 10.3.20.60 (10.3.20.60): 56 data bytes
ping: sendto: No route to host
ping: sendto: No route to host
ping: sendto: No route to host
ping: sendto: No route to host

--- 10.3.20.60 ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
```

1.34) Ναι, μας απαντάει. (εντολή: “ping 192.168.56.101” από το host machine).

```
C:\Users\Αλεξ>ping 192.168.56.101

Pinging 192.168.56.101 with 32 bytes of data:
Reply from 192.168.56.101: bytes=32 time=2ms TTL=64
Reply from 192.168.56.101: bytes=32 time=1ms TTL=64
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64
Reply from 192.168.56.101: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.56.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

1.35) Στέλνει πακέτα επ’ άπειρον, μέχρι να τη διακόψουμε εμείς, για αυτό και τη χρησιμοποιήσαμε με το όρισμα -c 4, ώστε να στείλει μόνο 4, όπως και στα Windows.

Άσκηση 2: Βασικές εντολές συστήματος αρχείων

2.1) Βρισκόμαστε στο φάκελο /usr/home/lab. (εντολή: “pwd”)

2.2) Εντολή: “mkdir tmp”.

2.3) Αρχικά πηγαίνουμε στον φάκελο tmp με “cd tmp”, και στη συνέχεια κάνουμε “mkdir el18014”.

2.4) Εκτελούμε “cd el18014”.

2.5) Με την εντολή “find / -name hosts” βρίσκουμε τα παρακάτω αρχεία με όνομα hosts:

- /etc/bluetooth/hosts
- /etc/hosts
- /usr/share/examples/etc/hosts
- /var/db/etcupdate/current/etc/bluetooth/hosts
- /var/db/etcupdate/current/etc/hosts

2.6) Μεταβαίνουμε στον φάκελο tmp και εκεί εκτελούμε την εντολή “cp /etc/hosts el18014”.

2.7) Εκτελούμε την εντολή “mv hosts hostsfile”.

2.8) Με την εντολή “ls -la” όντας στον φάκελο el18014, βλέπουμε τα παρακάτω:

```
-rw-r--r--  1 lab  wheel  1090 Mar  2 14:22 hostsfile
```

Επομένως, ο χρήστης έχει δικαιώματα ανάγνωσης και εγγραφής (rw), η ομάδα του χρήστη δικαιώματα ανάγνωσης (r), ενώ για οποιονδήποτε άλλο έχει πρόσβαση στο αρχείο, επιτρέπεται επίσης μόνο η ανάγνωση (r).

2.9) Εκτελούμε “touch test”, όντας στον φάκελο el18014.

2.10) Εκτελούμε “touch .hidden”.

2.11) Εκτελούμε την εντολή “ls -l /etc/services” και βλέπουμε πως έχει μέγεθος 86128 bytes.

```
lab@PC:~/tmp/el18014 % ls -l /etc/services
-rw-r--r--  1 root  wheel  86128 Sep 29  2017 /etc/services
```

2.12) Η διαφορά των 2 εντολών είναι πως η df -h εκφράζει το output στις μονάδες Byte, Kibibyte, Mebibyte, Gibibyte κ.λπ. (δυνάμεις τους 1024), ενώ η df -H στις μονάδες Byte, Kilobyte, Megabyte, Gigabyte κ.λπ. (δυνάμεις του 1000). Εάν για παράδειγμα έχουμε έναν χώρο αποθήκευσης 500Gigabyte = 500.000Megabyte = 500.000.000Kilobyte = 500.000.000.000 bytes, τότε με την εντολή df -H θα πάρουμε ως αποτέλεσμα 500G, ενώ με την εντολή df -h θα πάρουμε ως αποτέλεσμα 465.66G ($500.000.0000.000 / (1024)^3$, αντί του $500.000.000.000 / (1000)^3$ στην πρώτη περίπτωση). Για αυτό μάλιστα, εάν συνδέσουμε έναν σκληρό δίσκο στον υπολογιστή μας βλέπουμε πως αντί για 500Gigabyte που θα αναμέναμε, εμφανίζονται 465.66Gigabyte, καθώς ο υπολογισμός έχει γίνει στη βάση του 1024.

2.13) Εκτελούμε “df”.

2.14) Όντας στον φάκελο tmp, εκτελούμε “cp /etc/services el18014”.

2.15) Εκτελούμε όντας στον φάκελο el18014 την εντολή “gzip services”, οπότε και δημιουργείται το services.gz με μέγεθος 24.570 bytes.

2.16) Εκτελούμε ls -la:

```
lab@PC:~/tmp/el18014 % ls -la
total 36
drwxr-xr-x  2 lab  wheel    512 Mar  2 18:21 .
drwxr-xr-x  3 lab  wheel    512 Mar  2 14:12 ..
-rw-r--r--  1 lab  wheel      0 Mar  2 14:31 .hidden
-rw-r--r--  1 lab  wheel   1090 Mar  2 14:22 hostsfile
-rw-r--r--  1 lab  wheel  24570 Mar  2 18:15 services.gz
-rw-r--r--  1 lab  wheel      0 Mar  2 14:30 test
```

2.17) Παρατηρούμε πως κανένα αρχείο δεν ανήκει στον user με την εντολή “ls -la” (ή και “ls -la | grep user”, ώστε να μη λάβουμε κανένα αποτέλεσμα).

```
lab@PC:/usr % ls -la
total 84
drwxr-xr-x  15 root  wheel    512 Feb 16  2018 .
drwxr-xr-x  18 root  wheel    512 Mar  2 14:09 ..
drwxr-xr-x   2 root  wheel   8192 Sep 29  2017 bin
drwxr-xr-x   2 root  wheel    512 Sep 29  2017 games
drwxr-xr-x   3 root  wheel    512 Feb 16  2018 home
drwxr-xr-x  55 root  wheel   6144 Sep 29  2017 include
drwxr-xr-x   9 root  wheel  13312 Sep 29  2017 lib
drwxr-xr-x   5 root  wheel    512 Sep 29  2017 lib32
drwxr-xr-x   6 root  wheel    512 Sep 29  2017 libdata
drwxr-xr-x   8 root  wheel   1536 Sep 29  2017 libexec
drwxr-xr-x   2 root  wheel    512 Sep 29  2017 local
drwxr-xr-x   2 root  wheel    512 Sep 29  2017 obj
drwxr-xr-x   2 root  wheel   5632 Sep 29  2017 sbin
drwxr-xr-x  33 root  wheel   1024 Sep 29  2017 share
drwxr-xr-x   2 root  wheel    512 Sep 29  2017 src
```

2.18) Όντας στον φάκελο el18014 εκτελούμε την εντολή “rm hostsfile test services.gz .hidden”.

2.19) Εκτελούμε την εντολή “rm -R tmp”.

Άσκηση 3: Επεξεργασία κειμένου, ανακατεύθυνση εντολών

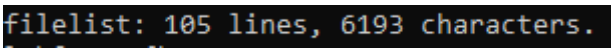
3.1) Η αλληλουχία βημάτων που εκτελούμε είναι η εξής:

1. **pwd** για να δούμε το directory που βρισκόμαστε. Είμαστε στο /usr/home/lab
2. **cd ..** για να μεταφερθούμε ένα directory πίσω, δηλαδή στο /usr/home.
3. **cp /etc/hosts lab** για να αντιγράψουμε το /etc/hosts στον φάκελο lab

4. **cd lab** για να μεταφερθούμε στον φάκελο lab
5. **vi hosts** για να ανοίξουμε το hosts με τον vi editor
6. **ESC** για να μεταφερθούμε σε command mode εντός του editor
7. **:%s /localhost/ntua-lab/ g** για να αλλάξουμε κάθε localhost με ntua-lab
8. **ESC** για να μεταφερθούμε σε command mode εντός του editor
9. **:q!** για να κλείσουμε το αρχείο χωρίς να αποθηκεύσουμε τις αλλαγές

3.2) Εκτελούμε την εντολή “touch filelist | ls -l /etc > filelist” (ή εναλλακτικά, σε μία γραμμή: “touch filelist; ls -l /etc > filelist)

3.3) Αφού εκτελέσουμε “vi filelist”, διαγράφουμε την πρώτη γραμμή, και στη συνέχεια, αφού αποθηκεύσουμε με “:wq” βλέπουμε πως μας εμφανίζεται στο τέλος του αρχείου η παρακάτω γραμμή:



Επομένως, το νέο πλήθος γραμμών και χαρακτήρων του filelist είναι πλέον 105 και 6.193 αντίστοιχα.

3.4) Διαγράψαμε τη γραμμή που έλεγε “total 812”. Όπως διαβάζουμε από το documentation της ls, ο αριθμός αυτός αφορά το πλήθος των blocks που χρησιμοποιούνται από το filesystem από τα αρχεία που υπάρχουν στο directory που του δώσαμε ως όρισμα (στο /etc εν προκειμένω).

3.5) Με την εντολή “wc filelist” βλέπουμε πως το αρχείο αποτελείται από 105 γραμμές, 953 λέξεις και 6.193 χαρακτήρες.

3.6) Εκτελούμε την εντολή “ls -l /etc | wc -l”, οπότε και μας εμφανίζεται ο αριθμός 106, και αφαιρώντας 1 για την πρώτη γραμμή που δεν αναπαριστά αρχείο, λαμβάνουμε το επιθυμητό πλήθος (μη κρυφών) αρχείων, ίσο με 105.

3.7) Εκτελούμε την εντολή “ls -l /etc | grep rc | wc -l” ως lab user και λαμβάνουμε ως αποτέλεσμα 15, αποτέλεσμα που αφορά αρχεία φακέλους/αρχεία που είναι ακριβώς μέσα στο /etc και όχι σε κάποιον υποφάκελο. Εκτελώντας “ls -l -R /etc | grep rc | wc -l” λαμβάνουμε ως αποτέλεσμα 21, αλλά και μήνυμα για αδυναμία πρόσβασης στο αρχείο /etc/ntp. Το αποτέλεσμα αυτό αφορά ολόκληρο το “δένδρο” καταλόγων και αρχείων κάτω από το /etc και όχι μόνο το πρώτο επίπεδο όπως πριν. Εκτελώντας ως root την εντολή “ls -l -R /etc | grep rc | wc -l” λαμβάνουμε 21 χωρίς το μήνυμα αδυναμίας πρόσβασης όπως πριν, επομένως το αποτέλεσμα είναι 21.

Άσκηση 4: Βασικές πληροφορίες συστήματος

4.1) Βλέπουμε τα παρακάτω:

```
lab@PC:~ % cat /var/run/dmesg.boot | grep CPU
CPU: AMD Ryzen 5 2500U with Radeon Vega Mobile Gfx   (1997.09-MHz 686-class CPU)
```

4.2) Βλέπουμε τα παρακάτω:

```
lab@PC:~ % cat /var/run/dmesg.boot | grep memory
real memory  = 268369920 (255 MB)
avail memory = 235118592 (224 MB)
```

4.3) Βρίσκουμε με “uname -sr” ότι χρησιμοποιείται η έκδοση 10.4 του FreeBSD.

```
lab@PC:~ % uname -sr
FreeBSD 10.4-RELEASE
```

4.4) Εκτελούμε την εντολή “ps aux | wc -l”, η οποία και μας επιστρέφει 41, και δεδομένου ότι η πρώτη γραμμή του ps ax περιέχει τους τίτλους για την κάθε στήλη, οι συνολικές υπηρεσίες του συστήματος είναι 40.

4.5) Με την εντολή “ps aux”.

4.6) Εκτελώντας “ps aux | grep syslogd” μας εμφανίζεται αποτέλεσμα που σημαίνει πως εκτελείται η syslogd.

4.7) Με την εντολή “sockstat -4 -l”.

```
lab@PC:~ % sockstat -4 -l
USER     COMMAND    PID   FD PROTO  LOCAL ADDRESS         FOREIGN ADDRESS
root     sendmail   629   4  tcp4   127.0.0.1:25          *:*
root     sshd       626   4  tcp4   *:22                  *:*
root     syslogd    436   7  udp4   *:514                 *:*
```

4.8) Με την εντολή “top”.

4.9) Με την εντολή “iostat ada0” βλέπουμε τα παρακάτω:

```
lab@PC:~ % iostat ada0
      tty            ada0             cpu
 tin  tout  KB/t tps  MB/s  us ni sy in id
   1   100 15.35   2  0.02   0  0  0  0 100
```

Αναλυτικά, οι στήλες δείχνουν:

- tin: χαρακτήρες που διαβάστηκαν από το terminal
- tout: χαρακτήρες που γράφτηκαν στο terminal
- KB/t: Kilobytes ανά transfer
- tps: transfers ανά second

- us: %cpu time σε user mode
- ni: %cpi time σε user mode που αξιοποιείται σε niced διεργασίες
- sy: %cpu time σε system mode
- in: %cpu time σε interrupt mode
- id: %cpu time σε idle mode

4.10) Με την εντολή “vmstat -w 2”.

```
lab@PC:~ % vmstat -w 2
 procs      memory      page                    disks     faults         cpu
 r b w      avm    fre   flt  re  pi  po    fr  sr ad0 cd0   in   sy   cs us sy id
 1 0 0    219M   186M    30   0   0   0    30   4   0   0  404  134  131  0  0 100
 0 0 0    219M   186M     0   0   0   0     0   3   0   0  401   62  123  0  0 100
 0 0 0    219M   186M     0   0   0   0     0   3   0   0  404   70  127  0  0 100
 0 0 0    219M   186M     0   0   0   0     0   3   0   0  405   73  127  0  0 100
```

Άσκηση 5: Πρόσβαση ως root

5.1) Για λόγους ασφαλείας απαγορεύεται η πρόσβαση ως root μέσω ssh, καθώς εάν επιτρεπόταν θα μπορούσε κάποιος να δοκιμάσει με brute force πιθανούς κωδικούς μέχρι να καταφέρει να συνδεθεί με πλήρη δικαιώματα.

5.2) Με την εντολή “hostname” βλέπουμε πως το όνομα του εικονικού μηχανήματος είναι “PC.ntua.lab”. Από το documentation της hostname, διαβάζουμε ότι το hostname μπορεί να το αλλάξει μόνο ο superuser δίνοντας κατάλληλο όρισμα στο script /etc/rc.d/hostname κατά το boot time, επομένως ο lab user δε μπορεί να αλλάξει το όνομα σε virtualmachine.

5.3) Εκτελούμε την εντολή “ping -c 5 -i 2 192.168.56.100”.

5.4) Για χρόνους ενδιάμεσης παύσης μικρότερους από 1 δευτερόλεπτο έχει δικαίωμα μόνο ο root.

5.5) Μπορούμε να επιτύχουμε τα παραπάνω όντας root user.

5.6) Με την εντολή “who” βλέπουμε πως συνδεδεμένος είναι ένας χρήστης lab και ένας χρήστης root.

5.7) Εκτελώντας την εντολή “su”, εάν έχουμε ήδη δικαιώματα διαχειριστή δε γίνεται τίποτα, ενώ εάν δεν έχουμε τέτοια δικαιώματα μας ζητείται κωδικός, ώστε να γίνουμε root.

5.8) Κάνοντας “cat /var/log/auth.log” ως lab λαμβάνουμε μήνυμα σφάλματος “Permission denied”, ενώ ως root λαμβάνουμε έναν κατάλογο σχετικά με τα login που πραγματοποιήθηκαν.

5.9) Όντας root χρήστης στο εικονικό μηχάνημα, εκτελούμε “su lab”, οπότε και γινόμαστε απλός χρήστης χωρίς αυξημένα δικαιώματα χωρίς να μας ζητηθεί κωδικός κατά την αλλαγή. Αυτό δικαιολογείται από το γεγονός πως ο root είχε ήδη περισσότερο δικαιώματα από τον lab, οπότε τα δικαιώματα του lab στα οποία θα έχει πρόσβαση πλέον ο root είναι υποσύνολο αυτών που ήδη είχε, επομένως δε τίθεται θέμα ασφαλείας.

Άσκηση 6: Μεταφορά αρχείων

6.1) Χρησιμοποιώντας κατάλληλα τις εντολές “cd” και “lcd” μεταβαίνουμε στους φακέλους /usr/home/lab και c:\users\MyName\downloads του απομακρυσμένου και του τοπικού μηχανήματος αντίστοιχα. Στη συνέχεια εκτελούμε την εντολή “get -r lab c:\users\MyName\downloads\tmp”, ώστε να κατεβάσουμε όλο τον φάκελο lab του απομακρυσμένου μηχανήματος στον φάκελο tmp κάτω από το downloads του τοπικού μηχανήματος.

6.2) Μεταφερόμαστε με τη χρήση της “lcd” στο directory C:\users\MyName\ Downloads\tmp του τοπικού μηχανήματος. Όντας εκεί, εκτελούμε διαδοχικά “get /etc/hosts” και “get /etc/rc.conf”.

6.3) Όντας στο /usr/home/lab του remote μηχανήματος, εκτελούμε την εντολή “mkdir tmp”.

6.4) Αρχικά, μεταφερόμαστε στο /usr/home/lab/tmp του remote μηχανήματος με κατάλληλη χρήση της εντολής cd. Αντίστοιχα, μεταφερόμαστε στον φάκελο Downloads του τοπικού μηχανήματος. Εκεί, εκτελούμε την εντολή “put -r tmp”.

6.5) Όντας στο /usr/home/lab/tmp, εκτελούμε την εντολή “rm *”. Ωστόσο, παραμένουν τα κρυφά αρχεία (., .., .ssh). Εάν εκτελέσουμε “rm .*” τότε παίρνουμε σφάλμα για απαγόρευση πρόσβασης. Άρα αδυνατούμε να διαγράψουμε όλα τα περιεχόμενα.

6.6) Καθώς δε μπορούμε να διαγράψουμε όλα τα περιεχόμενα, δε μπορούμε να εκτελέσουμε το “rmdir tmp”, αφού το tmp δεν είναι άδειο.

6.7) Όντας στο c:\users\MyName\Downloads του local μηχανήματος, εκτελούμε την εντολή “get -r /etc c:\users\MyName\downloads\local_etc”, ώστε να αντιγράψουμε τον φάκελο etc (remote) στο local_etc (local).

6.8) Η μεταφορά δεν ολοκληρώνεται, καθώς κατά το κατέβασμα των αρχείων, προηγείται το άνοιγμα καθενός εξ αυτών (open(“etc/filename”), το οποίο και αποτυγχάνει σε κάποια λόγω περιορισμένων δικαιωμάτων.

6.9) Αρχικά, μεταφερόμαστε κατάλληλα στο /usr/home/lab. Εκεί, εκτελούμε “mkdir remote_etc”, ώστε να δημιουργήσουμε τον φάκελο όπου θα αντιγράψουμε το local_etc από το Download directory του τοπικού μας μηχανήματος. Στη συνέχεια, κάνουμε “put -r local_etc remote_etc”.

6.10) Εκτελούμε “rename remote_etc tmp”.

6.11) Δοκιμάζοντας να κάνουμε “rm *” εντός του φακέλου tmp, παρατηρούμε πως δε μπορούμε να διαγράψουμε πολλά από τα αρχεία (Permission denied).

6.12) Δε μπορούμε να διαγράψουμε τον φάκελο tmp (“rmdir tmp”), καθώς αυτό προϋποθέτει τη διαγραφή αρχείων που δε μπορούν να διαγραφούν, όπως είδαμε στο 6.11.