Ονοματεπώνυμο: Ανδρέας Στάμος (03120***)	**Όνομα PC:** linux / Ubuntu 22.04.2 LTS
Ομάδα: 1	**Ημερομηνία:** 13/02/2024

Εργαστηριακή Άσκηση 1
Εξοικείωση με το FreeBSD και το VirtualBox

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

Άσκηση 1

1.1 192.168.56.1

1.2 255.255.255.0 (/24)

1.3 Ναι

1.4 Διεύθυνση IPv4 DHCP εξυπηρετητή: 192.168.56.100
Περιοχή διευθύνσεων IPv4 προς παραχώρηση: [192.168.56.101, 192.168.56.254]

1.5 `Password:`

1.6 `What manual page do you want?`

1.7 Εμφανίζεται η man page του προγράμματος `man`.

1.8 Εμφανίζεται η man page για την ιεραρχίαι του συστήματος αρχείου στο FreeBSD.

1.9 Στο `/lib/` υπάρχουν οι πολύ βασικές βιβλιοθήκες (ήτοι τα shared objects τους) (π.χ. libc που χρησιμοποιείται πρακτικά από όλα τα πρόγραμματα)

1.10 Στο `/usr/` βρίσκονται τα αρχεία των περισσότερων εφαρμογών και εργαλείων του χώρου χρήστη.

1.11 Στο `/sbin/` βρίσκονται τα προγράμματα συστήματος και τα εργαλεία διαχείρισης (τρέχουν πάλι σε χώρο χρήστη, όμως απαιτούν να εκτελούνται από τον ΥΠΕΡΧΡΗΣΤΗ)

1.12 `/var/mail/`

1.13 Γενικά γίνεται και με τα βελάκια και με PGUP, PGDOWN. Όμως το `less` υποστηρίζει και πλοήγηση και με απλούς χαρακτήρες χωρίς ειδικά πλήκτρα, προκειμένου να είναι συμβατό με παλαιότερα τερματικά που δεν είχαν ειδικά πλήκτρα.

1.14 `/<SUBSTRING>`

1.15 Το `less` είναι νεότερη εκδόση του `more` πρακτικά, με περισσότερες δυνατότητες (π.χ. πλοήγηση γραμμή-γραμμή, δεν απαιτείται να φορτωθεί όλο το αρχείο στην αρχή).

1.16 `PC.ntua.lab`

1.17 `lab`

1.18 `1001`

1.19 `wheels` με gid `0`.

1.20 `/usr/home/lab`

1.21 Εμφανίζει `/home/lab` διότι το `/home` είναι soft-link στο `/usr/home`.

1.22 `Password:`

1.23 `0`

1.24 `wheels` με gid `0` και `operator` με gid `5`.

1.25 `0`

1.26 `/root`

1.27 192.168.56.101

1.28 `local` και `m0`

1.29 `08:00:27:72:31:bf`

1.30 1 Gbps

1.31 192.168.56.101

1.32 0xffffff00

1.33 1500 bytes

1.34 127.0.0.1, 0xff000000, 16384 bytes

1.35 Όχι.

1.36 Εξαρτάται σε ποια διεπαφή δικτύου του host αναφερόμαστε.

Με την επιλογή host-only network, το VirtualBox δημιούργησε ένα εικονικό δίκτυο, στο οποίο ο host έχει λάβει IP διεύθυνση 192.168.56.1 και ο guest έχει λάβει IP διεύθυνση 192.168.56.101 (με DHCP). Μπόρουμε να επιβεβαιώσουμε την IP διεύθυνση του host τρέχοντας `ip addr` στον host – μάλιστα η αντίστοιχη διεπαφή, στον host, ονομάστηκε `vboxnet0`.

Άρα αν από τον guest κάνουμε ping στον host, αλλά στην διεύθυνση της εικονικής διεπαφής του που αντιστοιχεί στο εικονικό δίκτυο, ο host απαντά.

Αν όμως από τον guest κάνουμε ping στον host, αλλά στην διεύθυνση της πραγματικής δικτυακής του διεπαφής, λαμβάνουμε no route to send. Αυτό είναι λογικό, διότι αν στον guest με `netstat -rn` εμφανίσουμε τον πίνακα δρομολόγησης του guest, θα δούμε ότι δεν υπάρχει εγγραφή για δρομολόγηση εκτός του δικτύου 192.168.56.0/24 (και του 127.0.0.1) – δεν υπάρχει default geteway. Με άλλα λόγια, όταν ζητήσουμε από το FreeBSD να κάνουμε ping προς την διεύθυνση 192.168.1.XX που έχει ο host στο "πραγματικό" δίκτυο, το FreeBSD μας λέει, και λογικά, ότι δεν ξέρει που να στείλει αυτό το πακέτο.

1.37 Απαντά.

1.38 ∞, ενώ στα Windows είναι 4 φορές.

Άσκηση 2

2.1
```
lab@PC:~ % pwd
/usr/home/lab
```

2.2
```
lab@PC:~ % mkdir ~tmp
```

2.3
```
lab@PC:~ % mkdir tmp/03120xxx
```

2.4
```
lab@PC:~ % cd tmp/03120xxx
```

2.5
```
lab@PC:~/tmp/03120xxx % cp /etc/hosts .
```

2.6
```
lab@PC:~/tmp/03120xxx % mv hosts hosts.txt
```

2.7
```
lab@PC:~/tmp/03120xxx % ls -l hosts.txt
-rw-r--r-- 1 lab wheel 1090 Feb 13 13:05 hosts.txt
```

Τα δικαιώματα του αρχείου είναι:

- Για τον ιδιοκτήτη του αρχείου, δηλαδή τον χρήστη `lab` είναι ανάγνωσης και εγγραφής.
- Για τα μέλη χρήστες της ομάδας-ιδιοκτητή του αρχείου, δηλαδή την ομάδα `wheel` είναι ανάγνωσης.
- Για όλους τους άλλους χρήστες είναι ανάγνωσης.

2.8
```
lab@PC:~/tmp/03120xxx % touch test
```

2.9
```
lab@PC:~/tmp/03120xxx % touch .hidden
```

2.10
```
lab@PC:~/tmp/03120xxx % ls -l /etc/services
-rw-r--r-- 1 root wheel 86128 Sep 29 2017 /etc/services
```

Άρα το αρχείο έχει μέγεθος 86128 bytes.

2.11
```
lab@PC:~/tmp/03120xxx % du -h -s /usr/games
224K        /usr/games/
```

Άρα ο φάκελος μαζί με τα περιεχόμενα του (ο φάκελος είναι στην πραγματικότητα και αυτός ένα αρχείο) έχει μέγεθος 224KB.

2.12 Το `df -h` χρησιμοποιεί μονάδες Byte, Kibibyte, Mebibyte, Gibibyte, Tebibyte and Pebibyte (δυνάμεις του $1024 = 2^{10}$). Το `df -H` χρησιμοποιεί μονάδες Byte, Kilobyte, Megabyte, Gigabyte, Terabyte and Petabyte (δυνάμεις του $1000 = 10^3$).

2.13
```
lab@PC:~/tmp/03120xxx % df -H
Filesystem         Size    Used   Avail Capacity  Mounted on
/dev/gpt/rootfs     21G    600M     19G     3%    /
devfs              1.0k    1.0k      0B   100%    /dev
```

Άρα υπάρχουν διάθεσιμα 19GB $>$ 2GB.

2.14
```
lab@PC:~/tmp/03120xxx % cp /etc/services .
```

2.15
```
lab@PC:~/tmp/03120xxx % gzip services
lab@PC:~/tmp/03120xxx % gzip services
ls -l services.gz
-rw-r--r-- 1 lab wheel 24570 Feb 13 13:10 services.gz
```

Συνεπώς το συμπιεσμένο αρχείο καταλαμβάνει 24570 bytes.

2.16
```
lab@PC:~/tmp/03120xxx % ls -a
.        ..        .hidden        hosts.txt        services.gz        test
```

2.17
```
lab@PC:~/tmp/03120xxx % find /usr -type f -name hosts
/usr/share/examples/etc/hosts
```

2.18
```
lab@PC:~/tmp/03120xxx % find /usr -type f -name hosts
/usr/lib/pam_rhosts.so.5
/usr/share/examples/etc/hosts
/usr/share/examples/etc/hosts.allow
/usr/share/examples/etc/hosts.equiv
/usr/share/examples/etc/hosts.lpd
/usr/share/man/man3/hosts_access.3.gz
/usr/share/man/man3/hosts_ctl.3.gz
/usr/share/man/man5/hosts_access.5.gz
/usr/share/man/man5/hosts_options.5.gz
/usr/share/man/man5/hosts.allow.5.gz
/usr/share/man/man5/hosts.5.gz
/usr/share/man/man5/hosts.equiv.5.gz
/usr/share/man/man5/hosts.lpd.5.gz
/usr/share/man/man5/bluetooth.hosts.5.gz
/usr/share/man/man5/rhosts.5.gz
/usr/share/man/man8/pam_rhosts.8.gz
/usr/share/man/man8/hoststat.8.gz
/usr/share/sendmail/cf/feature/relay_hosts_only.m4
/usr/share/skel/dot.rhosts
/usr/home/lab/.rhosts
/usr/home/lab/tmp/03120xxx/hosts.txt
```

2.19
```
lab@PC:~/tmp/03120xxx % find . -type f
/usr/home/lab/.cshrc
/usr/home/lab/.login
/usr/home/lab/.login_conf
/usr/home/lab/.mailrc
/usr/home/lab/.profile
/usr/home/lab/.shrc
/usr/home/lab/.mail_aliases
/usr/home/lab/.rhosts
/usr/home/lab/.history
/usr/home/lab/.lesshst
```

```
/usr/home/lab/tmp/03120xxx/.hidden
/usr/home/lab/tmp/03120xxx/hosts.txt
/usr/home/lab/tmp/03120xxx/test
/usr/home/lab/tmp/03120xxx/services.gz
```

2.20 `lab@PC:~/tmp/03120xxx % find . -type f | xargs rm`

2.21
```
lab@PC:~/tmp/03120xxx % cd
lab@PC:~ % rm -r tmp
```

Άσκηση 3

Σημείωση: *Ο γράφων χρησιμοποιεί συστηματικά τον επεξεργαστή κειμένου* **vi**. *Μάλιστα, το συγκεκριμένο κείμενο – σε LaTeX – συγγράφτηκε και αυτό με τον επεξεργαστή κειμένου* **vi**.

3.1 `:%s/localhost/ntua-lab/g`

3.2 `lab@PC:~ % ls -l /etc >filelist`

3.3
```
lab@PC:~ % vi filelist
dd
:x
filelist: 104 lines, 6132 characters.
```

3.4 Το πλήθος blocks των αρχείων εντός του φακέλου τα οποία δείχνονται (π.χ. εξαρτάται αν δείχνονται τα κρυφά ή όχι) θεωρώντας μέγεθος block την τιμή της μεταβλητής περιβάλλοντος `$BLOCKSIZE`, που εδώ με `echo $BLOCKSIZE` βλέπουμε ότι έχει `K` που σημαίνει 1024 bytes.

3.5
```
lab@PC:~ % wc filelist
104     944    6132 filelist
```

Άρα αποτελείται από 104 γραμμές ή 944 λέξεις ή 6132 χαρακτήρες.

3.6
```
lab@PC:~ % ls /etc | wc -l
104
```

3.7 Υπάρχουν κάποια προβλήματα με τα permissions. Πιο συγκεκριμένα ο χρήστης `lab` δεν έχει δικαιώματα ανάγνωσης στον φάκελο `/etc/ntp` οπότε δεν μπορεί να τον ανοίξει και να δει τι περιέχει. (επίσης δεν έχει και δικαίωματα εκτέλεσης οπότε ακόμα και αν μπορούσε να δει τι περιέχει δεν θα μπορούσε να ανοίξει τα περιεχόμενα, π.χ. αν υπήρχαν υποφάκελοι δεν θα μπορούσε να τους ανοίξει)

Για αυτό, τρέχουμε:

```
lab@PC:~ % su root -c "find /etc -name '*rc*' | wc -l"
Password:
19
```

Συνεπώς υπάρχουν 19 τέτοια αρχεία.

Άσκηση 4

4.1
```
lab@PC:~ % grep CPU /var/run/dmesg.boot
CPU: Intel(R) Core(TM) i7 CPU K 875 @ 2.93GHz (2942.61-MHz 686-class CPU)
```

4.2
```
lab@PC:~ % grep memory /var/run/dmesg.boot
real memory = 268369920 (255 MB)
avail memory = 235118592 (224 MB)
```

4.3
```
lab@PC:~ % uname -s -r
FreeBSD 10.4-RELEASE
```

4.4
```
lab@PC:~ % uptime
17:05PM up 2 mins, 1 user, load averages: 0.29, 0.25, 0.11
```

4.5
```
lab@PC:~ % service -e | wc -l
16
```

Άρα υπάρχουν 16 ενεργοποιημένες υπηρεσίες.

4.6
```
lab@PC:~ % ps ax | wc -l
36
```

Άρα υπάρχουν 36 διεργασίες που τρέχουν. (με την ευρύτερη έννοια τρέχουν. διότι μετράμε και διεργασίες που ενδεχομένως κοιμούνται περιμένοντας να συμβεί κάτι, που είναι suspended ή ακόμα και που είναι zombie, δηλαδή που περιμένουν κάποια διεργασία να τις κάνει `wait` για να διαγραφούν).

4.7
```
lab@PC:~ % service syslogd status
Password:
syslogd is running as pid 432.
```

Συνεπώς η υπηρεσία `syslogd` τρέχει.

4.8
```
lab@PC:~ % netstat -ss -p tcp
tcp:
        7066 packets sent
                6992 data packets (539552 bytes)
                67 ack-only packets (33 delayed)
                7 control packets
        8926 packets received
                6197 acks (for 539567 bytes)
                7 duplicate acks
                3799 packets (173100 bytes) received in-sequence
        8 connection accepts
        8 connections established (including accepts)
        16 connections closed (including 0 drops)
                7 connections updated cached RTT on close
                7 connections updated cached RTT variance on close
        6197 segments updated rtt (of 5494 attempts)
        4895 correct ACK header predictions
        2714 correct data packet header predictions
        8 syncache entries added
                8 completed
        8 cookies sent
        1 hostcache entry added
```

4.9
```
lab@PC:~ % sockstat -l -4
USER     COMMAND    PID   FD PROTO  LOCAL ADDRESS         FOREIGN ADDRESS
root     sshd       3049  4  tcp4   *:22                  *:*
root     syslogd    432   7  udp4   *:514                 *:*
```

Με `service -l` επιβεβαιώνουμε (αν και ήδη γνωστό), πως τα `sshd` και `syslogd` είναι πράγματι υπηρεσίες:

```
lab@PC:~ % service -l | egrep 'sshd|syslogd'
sshd
syslogd
```

Συνεπώς, κίνηση IPv4 αναμένει ο δαίμονας του ssh στην TCP θύρα 22 και ο syslogd στην UDP θύρα 514.

4.10
```
lab@PC:~ % top
```

Δείχνει σε πραγματικό χρόνο τις διεργασίες ταξινομημένες από προεπιλογή με βάση το ποσοστό χρήσης της CPU. (ανανεώνει την οθόνη από προεπιλογή ανά 2 δευτερόλεπτα, αν και αυτό μπορεί να ρυθμιστεί με `-s<χρόνος σε δευτερόλεπτα>`)

4.11
```
lab@PC:~ % iostat -d ada0
             ada0
  KB/t tps  MB/s
 16.64   2  0.03
```

4.12
```
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   185M    55   0   0   0    58   4   0   0  405  286  132  0  0 100
 0 0 0    219M   185M     0   0   0   0     0   4   0   0  405   70  131  0  0 100
 0 0 0    219M   185M     0   0   0   0     0   4   0   0  403   63  116  0  0 100
```

Άσκηση 5

5.1 Το ssh σε root επιτρέπεται μόνο αν υπάρχει η σχετική ρύθμιση `PermitRootLogin` στο αρχείο `/etc/ssh/sshd_config`.

Από το man page του FreeBSD (εδώ) παρατηρούμε ότι το default (αν δεν υπάρχει ρύθμιση) είναι `no`. Στο αρχείο δεν υπάρχει ρύθμιση. Οπότε ισχύει το `no`.

5.2 Απαιτούνται δικαιώματα ΥΠΕΡΧΡΗΣΤΗ.

Πράγματι τρέχοντας χωρίς δικαιώματα υπερχρήστη:

```
lab@PC:~ % hostname testhostname hostname: sethostname: Operation not permitted
```

Αντίθετα, τρέχοντας με δικαιώματα υπερχρήστη:

```
lab@PC:~ % su
Password:
root@PC:/home/lab # hostname testhostname
root@PC:/home/lab # hostname
testhostname
```

5.3
```
lab@testhostname:~ % ping -i 2 -c 5 192.168.56.1
PING 192.168.56.1 (192.168.56.1): 56 data bytes
64 bytes from 192.168.56.1: icmp_seq=0 ttl=64 time=1.037 ms
64 bytes from 192.168.56.1: icmp_seq=1 ttl=64 time=0.420 ms
64 bytes from 192.168.56.1: icmp_seq=2 ttl=64 time=0.381 ms
64 bytes from 192.168.56.1: icmp_seq=3 ttl=64 time=0.492 ms
64 bytes from 192.168.56.1: icmp_seq=4 ttl=64 time=0.469 ms

--- 192.168.56.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.381/0.560/1.037/0.242 ms
```

5.4 Για να δοθούν χρόνοι αναμονής κάτω του 1 sec πρέπει ο χρήστης να έχει δικαιώματα ΥΠΕΡΧΡΗΣΤΗ.

Πράγματι τρέχοντας χωρίς δικαιώματα υπερχρήστη:

```
lab@testhostname:~ % ping -i 0.1 -c 5 192.168.56.1
ping: -i interval too short: Operation not permitted
```

Αντίθετα, τρέχοντας με δικαιώματα υπερχρήστη:

```
lab@testhostname:~ % su
Password:
root@testhostname:/home/lab # ping -i 0.1 -c 5 192.168.56.1
PING 192.168.56.1 (192.168.56.1): 56 data bytes
64 bytes from 192.168.56.1: icmp_seq=0 ttl=64 time=0.470 ms
64 bytes from 192.168.56.1: icmp_seq=1 ttl=64 time=0.338 ms
64 bytes from 192.168.56.1: icmp_seq=2 ttl=64 time=0.442 ms
64 bytes from 192.168.56.1: icmp_seq=3 ttl=64 time=0.639 ms
64 bytes from 192.168.56.1: icmp_seq=4 ttl=64 time=0.470 ms

--- 192.168.56.1 ping statistics --- 5 packets transmitted, 5 packets received, 0.0%
packet loss round-trip min/avg/max/stddev = 0.338/0.472/0.639/0.097 ms
```

5.5 Τις τρέχουμε ως υπερχρήστες, εκτελώντας `su` πρώτα. (στα ερωτήματα έχει δοθεί και η εκτέλεση αυτή)

5.6 Για να βρούμε ποιοι είναι:

```
lab@testhostname:~ % w
 6:18PM  up 49 mins, 2 users, load averages: 0.19, 0.09, 0.02
USER       TTY      FROM                    LOGIN@  IDLE WHAT
lab        v0       -                       5:30PM     - w
lab        pts/0    192.168.56.1            6:06PM     - -csh (csh)
```

Για να βρούμε πόσοι είναι:

```
lab@testhostname:~ % w -h | wc -l
       2
```

5.7 Θα ανιχνεύσουμε τις διεργασίες `su` και θα βρούμε τους χρήστες των γονικών διεγασιών (δηλ. του `csh` που εκτέλεσε το `su`).

```
lab@testhostname:~ % ps ax -o command,ppid | egrep '^su( )+[0-9]+$' | awk '{print $2}' |
xargs ps -o user= -p
lab
```

Η κανονική παράσταση `^su( )+[0-9]+$` *έχει σκοπό να πιάσουμε την λέξη su στην αρχή της γραμμής με τουλάχιστον ένα κένο μετά και να ακολουθεί ακριβώς ένας αριθμός (το ppid, δηλ. το pid της γονικής διεργασίας).*

5.8 Βλέπουμε τις χρονικές στιγμές που έγιναν απόπειρες αυθεντικοποίησης (είτε με su, είτε με ssh, είτε με login σε κονσόλα tty) είτε επιτυχείς είτε ανεπιτυχείς. Όμως, δεν υπάρχουν οι χρονικές στιγμές αποσυνδέσεις, αν κάποιος τρέξει `su`. Συνεπώς, μπορούμε να ξέρουμε αν κάποτε ή/και πρόσφατα κάποιος χρήστης επιχείρησε να λάβει δικαιώματα ΥΠΕΡΧΡΗΣΤΗ, όμως, δεν μπορούμε να ξέρουμε αν τα διαθέτει ακόμα την τρέχουσα χρονική στιγμή.

5.9 Όχι δεν ζητείται. Ο υπερχρήστης `root` έχει όλα τα δικαιώματα που θα μπορούσε να έχει κάποιος χρήστης (δηλ. ότι θα μπορούσε να κάνει κάποιος από τον χώρο χρήστη του ΛΣ – κάποια πράγματα παραμένουν που γίνονται μόνο σε χώρο πυρήνα, τουλάχιστον στο Linux). Συνεπώς, δεν θα είχε νόημα να του ζητηθεί ο κωδικός πρόσβασης ένος χρήστη, αφού ούτως ή άλλως έχει δικαιώμα να κάνει ό,τι θα μπορούσε να κάνει και εκείνος ο χρήστης. Αν απαιτούνταν να δοθεί κωδικός πρόσβασης, ο υπερχρήστης δυνητικά θα μπορούσε κιόλας απλά να αλλάξει το password του και να συνδεθεί έπειτα σε αυτόν.

Άσκηση 6

6.1 `ls -a /home/lab/`

6.2 `get -r /home/lab/`

6.3 `get /etc/hosts Downloads/temp`

`get /etc/rc.conf Downloads/temp`

6.4 `mkdir /home/lab/tmp`

6.5 `put -r Downloads/temp /home/lab/tmp`

6.6 Όχι. Το `rmdir` απαιτεί ο φάκελος να είναι κενός, που δεν είναι.

6.7 `rm /home/lab/tmp/temp/*`

6.8 Ναι με `rmdir /home/lab/tmp/temp`.

6.9 Δεν υπήρχαν κρυφά αρχεία.

6.10 Η διαγραφή είχε πετύχει.

6.11 `get -r /etc Downloads/`

6.12 Η μεταφορά ολοκληρώνεται χωρίς να έχουν μεταφερθεί όλα τα αρχεία, για το οποία λαμβάνουμε το σφάλμα Permission Denied.

Ο λόγος που συμβαίνει αυτό είναι διότι συνδεθήκαμε στο guest μηχάνημα με τον χρήστη `lab`, ο οποίος δεν έχει δικαιώματα ανάγνωσης σε κάποια αρχεία του `/etc`.

6.13 `put -r Downloads/etc/ /home/lab/`

6.14 `rename /home/lab/etc /home/lab/tmp`