Ονοματεπώνυμο: Πυλιώτης Αθανάσιος	**Όνομα PC:** DESKTOP-5DLG3IF
Ομάδα: 1	**Ημερομηνία:** 01/03/23

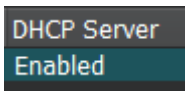
Εργαστηριακή Άσκηση 1
Εξοικείωση με το FreeBSD και το VirtualBox

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

1

1.1 IP Address: 192.168.56.1, το οποίο είναι μια ιδιωτική IP

1.2 Subnet Mask: 255.255.255.0

1.3 

ναι

1.4 **Server address:** 192.168.56.100, **Lower:** 192.168.56.101 , **Upper:** 192.168.56.254

1.5 Μας προτρέπει να δούμε την έκδοση που έχουμε με το freebsd-version ; uname -a

Για introduction to man pages: man man

Για directory layout: man hier

I can also edit /etc/motd to change the login announcement

Lab@PC:~%

1.6 man → Ρωτάει ποιο manual θέλω να δω

1.7 Μας δίνει το όνομα της εντολής, μια σύνοψη του τι μπορούμε να κάνουμε με αυτή και μια πιο αναλυτική περιγραφή (το manual) για την εντολή man

1.8 Μας δίνει αντίστοιχο manual για το hier. (το filesystem)

1.9 Critical system libraries needed for binaries in /bin and /sbin

Geom/ class specific libraries for the geom(8) utility

1.10 /var/mail/ έχει τα user mailbox files

1.11 Τα βελάκια κάτω δεξιά και τα u,k,y, → up, e,j, f,SPACE → down και το u πάει πιο γρήγορα και γενικά όσα λέει κάτω

1.12 / και γράφω αυτό που ψάχνω για forward search και ? για backward search

1.13 Επιτρέπει και backward και forward movement, επίσης δεν διαβάζει όλο το input file πριν ξεκινήσει, άρα ξεκινάει γρηγορότερα όπως στο vi. Έχει και άλλα πλεονεκτήματα βάσει του description της.

1.14 Όνομα εικονικού Μηχανήματος: hostname → PC.ntua.lab

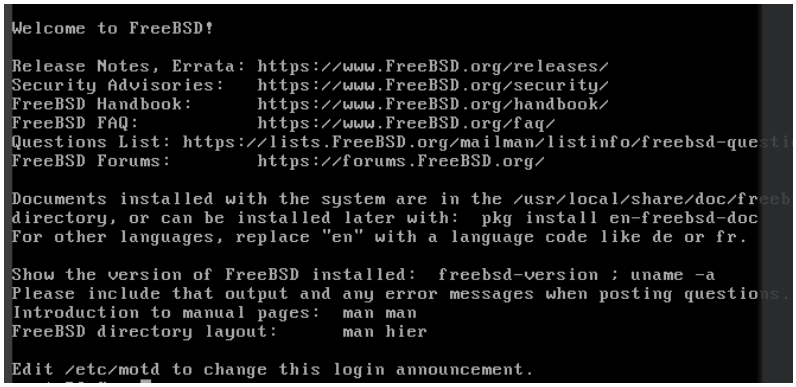
1.15 Όνομα χρήστη: whoami ή id -an → lab

1.16 uid: id lab (ή -u) → 1001(lab)

1.17 Groups: id lab (ή Gn) → gid=0(wheel) έχει δικαιώματα administrator

1.18 Τρέχων φάκελος εργασίας: pwd → /usr/home/lab

1.19



root@PC:~#

1.20 id -u → uid: 0(root)

1.21 id -Gn → 0 (wheel), 5 (operator)

1.22 id -g → gid = 0 for wheel.

1.23 pwd → /root (το βρίσκουμε με pwd)

1.24 dhclient em0 → IPv4 που αποδόθηκε: 192.168.56.101

1.25 ifconfig -a → Δικτυακές διεπαφές: em0 και lo0

1.26 ifconfig -a em0 → MAC of em0: ether: 08:00:27:72:31:bf (ίδιο για όλα τα κάτω)

1.27 Speed: 1000baseT άρα η ταχύτητα του είναι 1000Mbps (1Gbps)

1.28 IPv4: 192.168.56.101

1.29 Subnetwork mask: 255.255.255.0

1.30 MTU Value: 1500 bytes

1.31 ifconfig -a lo0 → IPv4: 127.0.0.1, Subnetwork mask: 255.0.0.0, MTU Value: 16384 bytes

1.32 cat /etc/resolv.conf → Όχι δεν έχουν οριστεί, δεν υπάρχει τέτοιο αρχείο, συνεπώς δεν υπάρχουν εξυπηρετητές DNS ορισμένοι.

1.33 ping 192.168.56.1 → όχι δεν απαντάει, 100% packets lost και του στέλνει 1 φορά

1.34 ping 192.168.56.101 → ναι απαντάει

1.35 Τη πρώτη φορά δεν απάντησε αλλά αν απαντούσε θα έστελνε μέχρι να το σταματήσουμε, τη δεύτερη φορά έστειλε μόνο 4 (επειδή είναι προκαθορισμένο στα windows να ζητάνε 4)

2

2.1 pwd → /usr/hom/lab

2.2 mkdir tmp

2.3 mkdir tmp/03119050

2.4 cd tmp/03119050

2.5 lab@PC:~/tmp/03119050 % find / -type f -name 'host' -exec dirname {} \;

/etc/ntp, /var/audit, /var/authpf, /var/cron/tabs, /var/db/entropy, /var/db/freebsd-update, /var/db/hyperv, /var/db/ipf, /var/db/ntp, /var/db/etcupdate/current/etc/ntp, /var/heimdal, /var/run/ppp, /var/spool/opielocks, /var/spool/clientmqueue

2.6 % cp /etc/hosts ./

2.7 % mv hosts hostsfile (απλά αλλάζουμε τα περιεχόμενα σε άλλο όνομα)

2.8 %ls -l → -rw-r--r-- 1 lab wheel 1090 Mar 5 17:04 hostsfile

Αυτό σημαίνει πως ο owner μπορεί να διαβάσει ή να γράψει στο αρχείο, το group permissions μπορεί να διαβάσει μόνο το αρχείο και οι υπόλοιποι μπορούν μόνο να το διαβάσουν.

2.9 % touch test

2.10 % touch .hidden

2.11 % ls -lh /etc/ → 84K bytes (84*1024 = 88064 bytes)

2.12 -h → powers of 1024 and -H → powers of 1000, που είναι θεωρητικά πιο ανθρώπινη μορφή μιας και σκεφτόμαστε σε χιλιάδες.

2.13 %df -h → Συνολικά έχει 19GB, 17GB είναι ελεύθερα και θέλουμε 84KB, οπότε έχουμε παραπάνω από αρκετό χώρο για όλα.

2.14 % cp /etc/services ./

2.15 % gzip services

% ls -lh → 24KB μέγεθος ziparισμένου

2.16 % ls -a →.hidden hostsfile services.gz test

2.17 % find /usr -user lab -type f -print

2.18 % cd ../ → % rm -rfv 03119050/{*,.*} (το v χρησιμοποιείται σε συνδυασμό με τα {*,.*} για να διαγραφούν όλα τα αρχεία που φτιάξαμε (ή ένα ένα)

2.19 % cd ../ → % rm -rf tmp

3

3.1 % cp /etc/hosts ./ , vi, βρίσκουμε το όνομα localhost με τα βελάκια, πατάμε x αρκετές φορές για να διαγράψουμε το localhost και μετά a και μετά γράφουμε ntua-lab. Μετά πατάμε ESC για να βγούμε χωρίς να το αποθηκεύσουμε πατάμε :q!

3.2 % ls -l /etc > filelist

3.3 vi filelist, dd για διαγραφή γραμμής → :wq, μένουν 104 γραμμές και 6089 χαρακτήρες

3.4 total 808 → συνολικό πλήθος blocks για τα directories που εμφανίζονται

3.5 % wc filelist

3.6 % ls /etc | wc -l → 104, άρα πλήθος αρχείων

3.7 % ls -ld /etc/*rc* | wc -l → 15

4

4.1 % cat /var/run/dmesg.boot | grep -i 'CPU:'

CPU: **Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz (2401.51-MHz 686-class CPU)**

4.2 % cat /var/run/dmesg.boot | grep -i 'memory'

real memory = **268369920 (255 MB)**

avail memory = **235118592 (224 MB)**

4.3 % uname -v

FreeBSD 10.4-RELEASE #0 r324094: Fri Sep 29 03:26:46 UTC 2017
root@releng1.nyi.freebsd.org:/usr/obj/usr/src/sys/GENERIC

4.4 % service -e | grep -c . → **16 ενεργοποιημένες υπηρεσίες**

4.5 % ps aux

4.6 % ps | grep (-c) 'syslogd' → αν βάλουμε το -c θέλουμε να είναι 2 το αποτέλεσμα, αλλιώς να υπάρχει η γραμμή /usr/sbin/syslogd -s

4.7 % sockstat -l4 -P tcp,udp

root sendmail 610 4 tcp4 127.0.0.1:25 *:*

root sshd 607 4 tcp4 *:22 *:*

root syslogd 419 7 udp4 *:514 *:*

4.8 % top, δείχνει στο real-time running processes και το CPU Usage.

4.9 % iostat -dw 1 ada0

4.10 % vmstat -w 2 → memory avm and free

5

5.1 Επειδή διαθέτει μόνο public key και όχι το private key. Η εικονική μηχανή δεν αφήνει κανένα να μπει στο σύστημα ως root για λόγους ασφάλειας του συστήματος, γιατί μπορεί κάποιος κακόβουλος να έχει βρει το συνθηματικό μας χωρίς το private key μας.

5.2 % hostname virtualmachine

hostname: sethostname: Operation not permitted

Δεν το καταφέραμε επειδή δεν ανήκουμε στην ομάδα που έχει permissions για να κάνει τις αλλαγές (sudo). Με τη χρήση του sudo ενδέχεται να γίνεται, αν έχουμε την άδεια αυτή.

5.3 % ping -i 2 -c 5 192.168.56.100

5.4 % ping -i 0.1 -c 5 192.168.56.100

ping: -i interval too short: Operation not permitted

Συνεπώς απλά είναι πολύ μικρό χρονικό διάστημα μεταξύ της παραλαβής πακέτων. Πρέπει να είναι τουλάχιστον 1 sec.

5.5 Με το να γίνουμε διαχειριστής λογικά. Ο διαχειριστής έχει την ικανότητα να κάνει όπως θέλει. Εκτελούμε %su και γινόμαστε root και μετά η εντολή % ping -i 0.1 -c 5 192.168.56.100

τρέχει χωρίς κανένα πρόβλημα.

5.6 # w → δείχνει και users (πλήθος) και ονόματα, και TTY, και IP για όσους είναι με ssh και ώρα που έκαναν login και τις εντολές που έτρεξαν. Είναι 2 χρήστες και είναι ο root και ο lab → 192.168.56.1.

5.7 Ναι, στο What (τελευταία στήλη) γράφει πως ο lab εκτέλεσε την εντολή su, η οποία του δίνει δικαιώματα διαχειριστή. Συγκεκριμένα γράφει _su (csh).

5.8 # cat /var/log/auth.log → βρίσκουμε πως λίγα λεπτά πριν ο lab έτρεξε την εντολή su και έγινε από lab root, su: lab to root on /dev/pts/0

5.9 #su - lab, όχι δεν ζητήθηκε συνθηματικό, πιθανότατα επειδή ο root είναι ο διαχειριστής που έχει access στα πάντα. Πολλές φορές στα συστήματα πρέπει να υπάρχει κάποιος με πλήρη πρόσβαση χωρίς την ανάγκη για συνθηματικό, με σκοπό την επιδιόρθωση χωρίς να είναι απαραίτητη η αλλαγή συνθηματικού κάθε φορά για τον χρήστη. Με το exit επανήλθε.

6

6.1 πάμε στο Downloads/tmp. Εκεί κάνουμε:

>sftp lab@192.168.56.101

Sftp> cd ../ → sftp> get -r * και έτσι αντιγράφουμε όλα τα περιεχόμενα του home του lab στο tmp.

6.2 sftp> get /etc/hosts → sftp> get /etc/rc.conf

6.3 sftp> cd lab

sftp> mkdir tmp

6.4 sftp> cd tmp → sftp> put -r *

6.5 sftp> rm ./tmp/*

6.6 sftp> rm tmp/{dir}/*

6.7 sftp> rmdir tmp/*

6.8 sftp> rmdir -r ./tmp

6.9 sftp> !cd ../ → sftp> !mkdir etc → sftp> get -r /etc etc

6.10 Δεν ολοκληρώνεται επειδή /etc/bluetooth/hcsecd.conf: open for read: permission denied

6.11 sftp> put -r ./etc etc

6.12 sftp>ren ./etc emp

6.13 rm ./tmp/* → έχω permission denied για αρκετά από τα αρχεία. Τα υπόλοιπα διαγράφονται κανονικά.

6.14 rmdir ./tmp → αποτυχία επειδή υπάρχουν αρχεία χωρίς write permission που συνεπάγεται και πως δεν μπορούν να διαγραφούν κι όλας.