Ονοματεπώνυμο: Μάρκος Δεληγιάννης	Όνομα PC: Lenovo-Laptop
Ομάδα: 1	Ημερομηνία: 28 / 2 / 2023

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

1.1 192.168.56.1

1.2 255.255.255.0

1.3 Ο εξυπηρετητής DHCP είναι ενεργοποιημένος.

1.4 IPv4 διεύθυνση του DCHP: 192.168.56.100
Περιοχή διευθύνσεων προς διάθεση: 192.168.56.101 - 192.168.56.254

1.5 Prompt: “lab@PC:~ %”

1.6 Αποτέλεσμα: “What manual page do you want?”

1.7 Εμφανίζονται οι πληροφορίες του ενσωματωμένου εγχειριδίου για την εντολή “man”. Η δοσμένη περιγραφή είναι: “display online manual documentation pages”.

1.8 Εμφανίζεται η περιγραφή της εντολής hier, η οποία είναι: “layout of file systems”.

1.9 Περιέχει σημαντικές βιβλιοθήκες συστήματος που χρησιμοποιούνται από τα binaries των καταλόγων /bin και /sbin.

1.10 Στον κατάλογο /var/mail.

1.11 Μπορούμε να χρησιμοποιήσουμε τα 4 βελάκια για να περιηγηθούμε στη σελίδα.

1.12 Για forward search: Γράφουμε /, τη λέξη που θέλουμε να αναζητήσουμε, και τέλος enter.
Για backward search: Γράφουμε ?, τη λέξη που θέλουμε να αναζητήσουμε, και τέλος enter.

1.13 Η less μας επιτρέπει να κινούμαστε και προς τα πίσω σε ένα αρχείο, σε αντίθεση με τη more.

1.14 PC.ntua.lab (εντολή hostname)

1.15 lab (εντολή whoami)

1.16 1001 (εντολή id)

1.17 Στην ομάδα “wheel” (εντολή id)

1.18 /usr/home/lab (εντολή pwd)

1.19 Prompt: “root@PC:~ #”

1.20 Το uid του root είναι 0 (εντολή id).

1.21 Στις ομάδες “wheel” και “operator” (εντολή id).

1.22 Το gid της ομάδας wheel είναι 0 (εντολή id).

1.23 /root (εντολή pwd)

1.24 Η διεύθυνση 192.168.56.101 (εμφανίζεται στο terminal με την εκτέλεση της εντολής “dhclient em0”)

1.25 Διαθέτει 2 δικτυακές διεπαφές: Την em0 (ethernet) και την lo0 (loopback). Εντολή: ifconfig

1.26 08:00:27:72:31:bf. Εντολή: ifconfig (ether)

1.27 Η ταχύτητα είναι 1Gbps. Εντολή: ifconfig (media: Ethernet autoselect (1000baseT <full-duplex>))

1.28 Διεύθυνση IPv4: 192.168.56.101. Εντολή: ifconfig (inet)

1.29 Μάσκα υποδικτύου: 255.255.255.0. Εντολή: ifconfig (netmask)

1.30 MTU = 1500. Εντολή: ifconfig (mtu)

1.31 Διεύθυνση IPv4: 127.0.0.1 μάσκα υποδικτύου: 255.0.0.0 mtu: 16384

1.32 Όχι, δεν έχουν ορισθεί εξυπηρετητές. Το αρχείο δεν υπάρχει.

1.33 Όχι, δεν απαντά.

1.34 Ναι, απαντά.

1.35 Η εντολή ping των Windows στέλνει 4 φορές πακέτα από προεπιλογή, ενώ η ping του freeBSD στέλνει από προεπιλογή μέχρι ο χρήστης να τη σταματήσει με ctrl+c.

2

2.1 Το directory είναι: /usr/home/lab. Εντολή: pwd

2.2 Εντολή: mkdir tmp

2.3 Εντολή: mkdir tmp/el19023

2.4 Εντολή: cd tmp/el19023

2.5 Στους φακέλους "/etc/bluetooth/", "/etc/", "/usr/share/examples/etc/", "/var/db/etcupdate/current/etc/" "/var/db/etcupdate/current/etc/bluetooth/". Εντολή: **find / -type f -name hosts |& grep -v "Permission denied"**. Το "/" θέτει ως φάκελο-ρίζα της αναζήτησης το root, το "-type f" οδηγεί στην αναζήτηση μόνο αρχείων, το "-name hosts" θέτει το όνομα των αρχείων που αναζητούνται, και τέλος το "|& grep -v "Permission denied" ανακατευθύνει το stdout και stderr στην grep, επιστρέποντάς μας να φιλτράρουμε τα μηνύματα "Permission denied" που προκύπτουν από την έλλειψη δικαιωμάτων του χρήστη lab.

2.6 Εντολή: "cp /etc/hosts ."

2.7 Εντολή: "mv hosts hostsfile"

2.8 Η εντολή "ls -l hostsfile" δίνει "-rw-r--r--", το οποίο σημαίνει ότι ο χρήστης lab έχει δικαιώματα ανάγνωσης, εγγραφής αλλά όχι εκτέλεσης (rw-), ενώ οι υπόλοιποι χρήστες εντός και εκτός του group wheel έχουν μόνο δικαίωμα ανάγνωσης (r--). Εξαίρεση φυσικά αποτελεί ο root.

2.9 Εντολή: "touch test"

2.10 Εντολή: "touch .hidden"

2.11 Το μέγεθος του αρχείου είναι 86.128 bytes. Εντολή: "ls -l /etc/services"

2.12 -h: Χρήση μονάδων Byte, Kibibyte, Mebibyte κλπ. -H: Χρήση μονάδων Byte, Kilobyte, Megabyte κλπ.

2.13 Υπάρχουν 19 Gigabytes ελεύθερα στον δίσκο, οπότε υπάρχει χώρος. Εντολή: "df -H /"

2.14 Εντολή: "cp /etc/services ."

2.15 Το νέο μέγεθος του αρχείου είναι 24.570 bytes. Εντολή: "gzip services"

2.16 Εντολή: "ls -a"

2.17 Εντολή: "find /usr -user lab -type f"

2.18 Εντολή: "rm -r ~/tmp/el19023/*"

2.19 Εντολή: "rm -r ~/tmp"

3

3.1 1) **vi hosts** 2) **:%s /localhost/ntua-lab/ g** 3) **:x**

3.2 ls -l /etc > filelist

3.3 **vi filelist** και **dd** και **:x** (Η πληροφορία για το πλήθος γραμμών και χαρακτήρων εμφανίζεται στην έξοδο)

3.4 Η γραμμή ("Total 808") περιέχει την πληροφορία για τον αριθμό blocks που χρησιμοποιούνται στο file system από τα αρχεία που περιέχονται στο directory.

3.5 **wc filelist** (Εμφανίζονται με τη σειρά γραμμές, λέξεις, χαρακτήρες (bytes))

3.6 **ls /etc | wc -l**

3.7 **ls /etc | grep rc -c**

4

4.1 Εντολή: **cat /var/run/dmesg.boot** και επισκόπηση 6 γραμμής / Τύπος CPU: i386 (x86)

4.2 Εντολή: **cat /var/run/dmesg.boot | grep -i memory** / Συν. Μνήμη: 255MB Διαθ. Μνήμη: 224MB

4.3 Εντολή: **uname -v** / Αποτέλεσμα: FreeBSD 10.4-RELEASE #0

4.4 Εντολή: **service -e | wc -l** / Αποτέλεσμα: 16

4.5 Εντολή: **ps aux**

4.6 Εντολή: **service -e | grep syslogd** / Αποτέλεσμα: /etc/rc.d/syslogd, συνεπώς **η υπηρεσία είναι ενεργή**.

4.7 Εντολή: **sockstat -4l**

4.8 Εντολή: **top**. Εμφανίζονται οι διεργασίες με τη μεγαλύτερη χρήση CPU.

4.9 Εντολή: **iostat -d ada0**

4.10 Εντολή: **vmstat -w 2** και επισκόπηση της στήλης **memory**

5

5.1 Για λόγους ασφαλείας η προεπιλεγμένη ρύθμιση στο εικονικό μηχάνημα είναι να απαγορεύει το login ως root από το SSH με χρήση συνθηματικού.

5.2 Χρησιμοποιούμε την εντολή **hostname virtualmachine**. Το σύστημα δεν μας επιτρέπει να αλλάξουμε το όνομα του εικονικού μηχανήματος ως χρήστης lab.

5.3 Εντολή: **ping -i 2 -c 5 192.168.56.100**

5.4 Λαμβάνουμε μήνυμα λάθους **ping: -i interval too short: Operation not permitted**, έχουμε βάλει δηλαδή πολύ μικρό χρονικό διάστημα παύσης.

5.5 Θα εκτελέσουμε τις εντολές που απέτυχαν ως διαχειριστής (root), με χρήση της εντολής **su -**.

5.6 Εκτελούμε την εντολή **who**. Παρατηρούμε ότι 2 χρήστες είναι συνδεδεμένοι στο σύστημα, ο root και ο lab.

5.7 Ναι, στην κονσόλα του μηχανήματος όταν έχουμε συνδεθεί ως root και κάποιος κοινός χρήστης αποκτήσει δικαιώματα διαχειριστή εμφανίζεται μήνυμα: **[timestamp] PC su: lab to root on [terminal]**. Επιπλέον, ένας λιγότερο αξιόπιστος τρόπος είναι να εκτελέσουμε την εντολή w ως διαχειριστής και να εστιάσουμε στη στήλη "WHAT". Εάν ο χρήστης που έχει χρησιμοποιήσει την εντολή su δεν εκτελεί εκείνη τη στιγμή κάποια άλλη εντολή (όπως την ping), τότε στη στήλη WHAT θα εμφανιστεί "su (csh)".

5.8 Εντοπίζουμε τις ειδοποιήσεις που λάμβανε ο root στο terminal κάθε φορά που ένας απλός χρήστης αποκτούσε δικαιώματα διαχειριστή.

5.9 Χρησιμοποιούμε την εντολή **su – lab**. Φυσικά δεν απαιτείται κωδικός, καθώς μεταβαίνουμε από ρόλο διαχειριστή (που ήδη έχει τον πλήρη έλεγχο στο σύστημα) σε άλλον ρόλο, οπότε δεν υπάρχει νόημα να ζητηθεί κωδικός.

6

6.1 Εντολές: 1) **!mkdir tmp**
2) **get -r . tmp** (εκτελέσαμε το terminal από τον φάκελο Downloads)

6.2 Εντολές: 1) **mget /etc/hosts /etc/rc.conf**

6.3 Εντολή: **mkdir tmp** (αφού βεβαιωθούμε με **pwd** ότι είμαστε στο σωστό remote directory)

6.4 Εντολή: **put -r .\tmp tmp**

6.5 Εντολή: **rm tmp/***

6.6 Εντολή: **ls tmp**, βρίσκουμε τα directories (το entry τους ξεκινά με d) και για κάθε ένα από αυτά εκτελούμε την εντολή **rm tmp/[dir-name]/***

6.7 Εντολή: **rmdir tmp/***

6.8 Εντολή: **rmdir tmp**

6.9 Εντολές: 1) **!mkdir etc**
2) **get -r /etc etc**

6.10 Λαμβάνουμε το μήνυμα λάθους: **/etc/bluetooth/hcsecd.conf: open for read: permission denied**. Αυτό σημαίνει ότι δεν έχουμε δικαίωμα ανάγνωσης αυτού του αρχείου, οπότε δεν μπορούμε να το αντιγράψουμε.

6.11 Εντολές: 1) **mkdir etc**
2) **put -r etc etc**

6.12 Εντολή: **ren etc tmp**

6.13 Ναι, μπορούμε με την εντολή **rm tmp/***. Έτσι μένουν μόνο τα subdirectories του tmp.

6.14 Δεν μπορούμε να διαγράψουμε κατευθείαν τον tmp εκτελώντας την εντολή **rmdir tmp** (λαμβάνουμε failure), επειδή δεν είναι άδειος (περιέχει τα subdirectories που δεν διαγράψαμε). Μπορούμε όμως να διαγράψουμε “από μέσα προς τα έξω” τα directories ως εξής:
1) Αν ένα directory περιέχει μόνο αρχεία, τότε εκτελούμε **rm [path_to_dir]/*** και **rmdir [path_to_dir]** για να το διαγράψουμε.
2) Αν ένα directory περιέχει και subdirectories, εκτελούμε τις εντολές του 1, διαγράφοντας τα αρχεία του, και μετά διαγράφουμε ένα-ένα τα subdirectories ακολουθώντας αναδρομικά τη μεθοδολογία που περιγράψαμε. Τέλος, διαγράφουμε το ίδιο το directory.