ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
Τμήμα Πληροφορικής

ΕΠΛ 371 - Προγραμματισμός Συστημάτων

ΑΣΚΗΣΗ 1 – Βασικές Εντολές UNIX
(σε Virtual Private CentOS Servers)

Διδάσκων: Δημήτρης Ζεϊναλιπούρ

Υπεύθυνος Εργαστηρίου: Παύλος Αντωνίου

Ημερομηνία Ανάθεσης: Τετάρτη 4/2/2015
Ημερομηνία Παράδοσης: Τετάρτη 11/2/2015 και ώρα 13:30 (7 μέρες)

(η λύση να υποβληθεί σε zip μέσω του Moodle και ο κώδικας να να παραδοθεί εκτυπωμένος στο εργαστήριο)

http://www.cs.ucy.ac.cy/courses/EPL371/

Στόχος Άσκησης

Στόχος αυτής της άσκησης είναι η εξοικείωση με βασικές εντολές του λειτουργικού συστήματος UNIX. Συγκεκριμένα, σε αυτή την άσκηση θα πρέπει να κάνετε **χρήση των εντολών του UNIX** με διοχέτευση **ΧΩΡΙΣ** τη χρήση:

1. Εργαλείων ωφελιμότητας *sed* & *awk*;
2. Ενδιάμεσων αρχείων, τα οποία δημιουργούνται με ανακατευθύνσεις; και
3. Τεχνικών προγραμματισμού κελύφους, κάτι το οποίο θα δούμε στη συνέχεια.

Εισηγούμαστε όπως μελετήσετε τις εντολές τις οποίες έχετε διδαχθεί στις διαλέξεις του μαθήματος και μέσω του εγχειριδίου *man,* έτσι ώστε να ανακαλύψετε και χρησιμοποιήσετε νέες παραμέτρους που είναι διαθέσιμες για τις εντολές αυτές.

Virtual Private Servers (VPS)

Ακόμα ένας στόχος είναι η εξοικείωση σας με εικονικές μηχανές (c - VPS). Η υπηρεσία που προσφέρει το Τμήμα Πληροφορικής κάνει χρήση του συστήματος OpenVZ virtualization. Το σύστημα OpenVZ υπάγεται στην κατηγορία του container-based virtualization και αφορά μόνο λειτουργικά συστήματα τύπου Linux. Η εικονική μηχανή που θα έχει στη διάθεσή του ο κάθε φοιτητής τρέχει το λειτουργικό σύστημα Centos 6 64 bit με τις ελάχιστες απαιτήσεις, 2GB quota, και 256MB RAM. Μέσα στο εικονικό αυτό περιβάλλον ο κάθε φοιτητής θα έχει δικαιώματα διαχειριστή (root).

Οι VPS μηχανές που θα σας δοθούν είναι προσβάσιμες μόνο μέσα από το τοπικό δίκτυο του Τμήματος Πληροφορικής. Για να ενωθείτε από σπίτι σας πάνω σε κάποια μηχανή πρέπει προηγουμένως (α) να ενωθείτε με VPN στο Τμήμα Πληροφορικής, (β) να ενωθείτε με SSH (putty από Windows) πάνω σε μια μηχανή είτε του εργαστηρίου 103 ή του B103 και (γ) να ενωθείτε με SSH πάνω στο VPS σας. Το VPS όνομα της μηχανής σας και ο κωδικός του κάθε φοιτητή θα σας αποσταλεί μέσω email. Στο βήμα (γ) η εντολή που θα γράψετε στο terminal είναι:

```
ssh -l root <myVPS>.in.cs.ucy.ac.cy
```

Για να μπορέσετε να εγκαταστήσετε ή να αναβαθμίσετε πακέτα που επιθυμείτε (δείτε την εντολή `yum` μέσω `man yum` στο terminal ή `rpm`) στην μηχανή σας από άλλα εξωτερικά δίκτυα θα πρέπει να τρέξετε προηγουμένως στο terminal την εντολή που ορίζει τον proxy server για να έχουμε πρόσβαση στο διαδίκτυο για κατέβασμα πακέτων:

```
export http_proxy='http://proxy.cs.ucy.ac.cy:8008'
```

ΕΡΩΤΗΜΑΤΑ

Για κάθε ερώτημα που ακολουθεί **δώστε την εντολή (ή σειρά εντολών με διοχέτευση)** που πιστεύετε ότι δίνει πιο αποδοτικά τη ζητούμενη λύση. Επίσης **εξηγήστε εν συντομία** τη δομή της εντολής που έχετε δώσει. Εάν πρόκειται για μια διοχέτευση εντολών τότε περιγράψετε όλους τους επί μέρους όρους της εντολής.

Ερώτημα 1

Να δώσετε την εντολή (ή σειρά εντολών με διοχέτευση) που να παρουσιάζει πόσα user ids στο αρχείο `/etc/passwd` βρίσκονται μεταξύ 10 και 20 συμπεριλαμβανομένου. Για παράδειγμα, μια καταχώρηση μέσα στο αρχείο `/etc/passwd` μπορεί να είναι: `ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin` όπου το user id είναι το 14. Υποθέστε ότι τα user ids δεν αντιστοιχούν ποτέ σε αριθμό που ξεκινά από 0 π.χ. 013.

Ερώτημα 2

Στα συστήματα Linux τα αρχεία συμβάντων (log files) αποθηκεύονται στο /var/log και μόνο ο χρήστης root μπορεί να έχει πρόσβαση σε αυτά. Μερικά αρχεία που βρίσκονται στον κατάλογο αυτό είναι:

```
/var/log/message: General message and system related stuff
/var/log/boot.log: System boot log
/var/log/mysqld.log: MySQL database server log file (if database exists)
/var/log/secure: Authentication log
/var/log/utmp or /var/log/wtmp : Login records file
/var/log/yum.log: Yum log files
```

Το αρχείο `yum.log` συνδέεται με την εντολή `yum` η οποία χρησιμοποιείται στα συστήματα Linux για την εγκατάσταση, την αφαίρεση και την ενημέρωση του λογισμικού ενός συστήματος που λειτουργεί με RPM διανομές (π.χ., Centos 6.6 – Redhat - στην περίπτωση μας). Μέσα στο αρχείο `yum.log` υπάρχει το ιστορικό των πιο πάνω διαδικασιών. Για να δημιουργηθεί το αρχείο αυτό (αν δεν υπάρχει) πρέπει να καλέσετε την εντολή: "`yum update`" (αφού πρώτα εκτελέσετε την εντολή που ορίζει τον proxy server). Η εντολή "`yum update`" θα αναβαθμίσει όλα τα εγκατεστημένα πακέτα στη μηχανή σας δημιουργώντας ταυτόχρονα και το αρχείο yum.log.

Ένα παράδειγμα μιας γραμμής του αρχείου αυτού είναι η πιο κάτω:

```
Jan 09 05:33:44 Updated: finger-0.17-40.el6.x86_64
```

που λέει ότι στις 9 Ιανουαρίου και ώρα 05:33:44 ενημερώθηκε (Updated) το πρόγραμμα (package) finger-0.17-40.el6.x86_64. Το x86_64 δείχνει ότι το πρόγραμμα αυτό είναι συμβατό με αρχιτεκτονικές 64 bit.

Δώστε την εντολή (ή σειρά εντολών με διοχέτευση) που να εμφανίζει ταξινομημένα κατά αύξουσα αλφαβητική σειρά τα προγράμματα που ενημερώθηκαν (Updated), των οποίων το όνομα αρχίζει από li **ή** gli. Το κάθε πρόγραμμα (package) να εμφανίζεται μόνο μια φορά.

Ερώτημα 3

Να δώσετε την εντολή (ή σειρά εντολών με διοχέτευση) που να τυπώνει τον συνολικό αριθμό γραμμών που βρίσκονται σε όλα τα αρχεία .log στον τρέχων κατάλογο και σε οποιοδήποτε υποκατάλογο (κάτω από τον τρέχων).

Ερώτημα 4

Δώστε την εντολή (ή σειρά εντολών με διοχέτευση) που να εμφανίζει ταξινομημένα κατά αύξουσα αλφαβητική σειρά τα usernames των χρηστών που είναι συνδεδεμένοι στο σύστημα, των οποίων το username αρχίζει από sp **ή** τελειώνει σε 1. Το username κάθε χρήστη να εμφανίζεται μόνο μια φορά (δοκιμάστε το καλύτερα στις μηχανές του εργαστηρίου όπου θα υπάρχουν και άλλοι χρήστες ενωμένοι)

Ερώτημα 5

Μέσα στο HOME κατάλογο κάθε χρήστη υπάρχει ένα κρυφό (hidden) αρχείο με το όνομα `.bash_history` το οποίο περιέχει τις προηγούμενες εντολές που εκτέλεσε ο χρήστης (ιστορικό εντολών) στο κέλυφος bash. Σε κάθε γραμμή του αρχείου υπάρχει μια εντολή ή ένα σύνολο εντολών με διοχέτευση ή/και ανακατεύθυνση. Οι HOME κατάλογοι των χρηστών (εκτός του root) βρίσκονται μέσα στον κατάλογο `/home`. Για παράδειγμα ο χρήστης με username "johnsmith" έχει σαν HOME κατάλογο το `/home/johnsmith`. Ο HOME κατάλογος του root που είναι προσπελάσιμος μόνο από τον root βρίσκεται στο /root.

Δώστε την εντολή (ή σειρά εντολών με διοχέτευση) η οποία θα παρουσιάζει τις πρώτες 20 σελίδες **man** της εντολής που εκτέλεσε τις περισσότερες φορές ο χρήστης root και ΔΕΝ περιλαμβάνει διοχέτευση (|) ή ανακατεύθυνση (>, <). Σε περίπτωση περισσότερων από μια χρησιμοποιήστε όποια εντολή επιθυμείτε.

Για παράδειγμα εάν το αρχείο `/root/.bash_history` περιέχει τις πιο κάτω εντολές

ls
mv mylist.c list.c
ls | sort | uniq
man sort
cat lab3.c > lab4.c
grep –v "include" lab4.c
ls -ltr
ls -l
rm test1.txt
ls –a

τότε εκτελώντας τις εντολές σας θα πρέπει να παρουσιάζει τις πρώτες 20 γραμμές του ***man ls***, εφόσον η εντολή αυτή παρουσιάζεται 4 φορές. Οι εντολές με έντονα γράμματα λαμβάνονται υπόψη και οι γραμμές με κόκκινα γράμματα πρέπει να αγνοηθούν.

Ερώτημα 6

Αρκετές φορές ο διαχειριστής του συστήματος (root) χρειάζεται να κάνει backup κάποια αρχεία. Έστω ότι θέλει να κάνει backup το αρχείο notes αντιγράφοντας το σε ένα νέο αρχείο με το όνομα notes.HHMM όπου HHMM είναι η παρούσα ώρα (HH είναι οι ώρες και MM τα λεπτά). Ο διαχειριστής θέλει να διαγράψει τα παλαιότερα πέντε αρχεία του με τη χρήση μιας εντολής και χωρίς να γράφει το όνομα του κάθε αρχείου ξεχωριστά. Να δώσετε την εντολή (ή σειρά εντολών με διοχέτευση) που διαγράφει τα παλαιότερα πέντε αρχεία που έγιναν backup.

Ερώτημα 7

Το `/proc` είναι ένα εικονικό σύστημα αρχείων το οποίο μας δίνει τη δυνατότητα να πάρουμε πληροφορίες από τις δομές δεδομένων του πυρήνα (kernel). Είναι εικονικό με την έννοια ότι τα αρχεία που βλέπουμε δεν έχουν κάποια φυσική υπόσταση (π.χ. δεν βρίσκονται σε κάποια συσκευή). Τα περισσότερα αρχεία μπορούν να ανοιχτούν μόνο για ανάγνωση. Στο βασικό κατάλογο `/proc` υπάρχει ένα πλήθος από αρχεία και καταλόγους. Κάποια από αυτά περιέχουν ολόκληρες δομές πληροφοριών, ενώ άλλα απλώς την τιμή μιας συγκεκριμένης μεταβλητής του πυρήνα. Τα περισσότερα αρχεία έχουν ονόματα αυτό-επεξηγηματικά. Πιο συγκεκριμένα το αρχείο `/proc/cpuinfo` περιέχει πληροφορίες για τον επεξεργαστή του συστήματος.

Να δώσετε την εντολή που βρίσκει τα flags του επεξεργαστή (σε περίπτωση πολυπύρηνου επεξεργαστή να δείξετε τα flags μόνο του πρώτου πυρήνα) ταξινομημένα σε αντίστροφη αλφαβητική σειρά (ως προς το όνομά) και τα αποθηκεύει στο αρχείο `/root/cpuflags.txt` (το αρχείο δεν πρέπει να περιέχει καμία κενή γραμμή).

Ερώτημα 8

Η εντολή `tcpdump` μας βοηθά να συλλέξουμε (capture) τα πακέτα που στέλνονται ή λαμβάνονται από το σύστημα μας για κάποιο χρονικό διάστημα (αντίστοιχα με το Wireshark – winpcap library ειδικότερα - στα Windows). Χρησιμοποιώντας τους κατάλληλους διακόπτες μπορούμε:

(α) να δούμε πλήρεις πληροφορίες για κάθε πακέτο π.χ. τα περιεχόμενα των κεφαλίδων των πρωτοκόλλων (διακόπτης `-v`)

(β) να λάβουμε μόνο συγκεκριμένο αριθμό πακέτων (διακόπτης `-c` ακολουθούμενος από ένα νούμερο π.χ. `-c 100` σημαίνει ότι θέλουμε να λάβουμε μόνο 100 πακέτα),

(γ) να αναλύσουμε το περιεχόμενο των πακέτων σε δεκαεξαδική μορφή (διακόπτης -XX),

(δ) να τυπώσουμε το χρόνο (timestamp) σε πιο εύληπτη μορφή (διακόπτης -tttt)

Για να παράξουμε κάποια επιπλέον κίνηση (πέρα από την συνήθη TCP/UDP κίνηση που θα βλέπει η NIC του host σας), θα μπορούσαμε προαιρετικά να τρέχουμε την εντολή:

```
ping www.cs.ucy.ac.cy -c 100 > /dev/null  &
```

η οποία (ping) αποτελεί μια μέθοδο για τον εντοπισμό της διαθεσιμότητας και της απόδοσης ενός απομακρυσμένου πόρου του δικτύου και αποτελείται από κάποια REQUESTs και κάποια RESPONSEs. Αμέσως μετά την πιο πάνω εντολή τρέχουμε το πιο κάτω:

```
tcpdump -c 100 -XX -tttt -vv > /root/packet
```

για να ξεκινήσει η συλλογή των πακέτων (δεν σημαίνει ότι θα προλάβουμε να δούμε και τα 100 ICMP πακέτα που στάλθηκαν με το ping). Ειδικότερα το transport πρωτόκολλο του κάθε IP πακέτου αναγράφεται στο σημείο «proto X» (όπου X είναι ICMP, TCP ή UDP). Τα περιεχόμενα του αρχείου `/root/packet` έχουν την πιο κάτω μορφή (πιο κάτω φαίνονται πληροφορίες μόνο για 2 πακέτα):

```
2015-01-29 10:07:33.189005 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto ICMP (1), length
84)
    Asia > clio.cs.ucy.ac.cy: ICMP echo request, id 9759, seq 15, length 64
        0x0000:  0004 ffff 0000 0000 0000 0000 0000 0800  ................
        0x0010:  4500 0054 0000 4000 4001 4d7b 0a10 0f6d  E..T..@.@.M{...m
        0x0020:  c22a 1187 0800 567b 261f 000f b54c ca54  .*....V{&....L.T
        0x0030:  0000 0000 3ae2 0200 0000 0000 1011 1213  ....:...........
        0x0040:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0050:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0060:  3435 3637                                4567
```

```
2015-01-29 10:07:33.189878 IP (tos 0x0, ttl 61, id 11862, offset 0, flags [none], proto ICMP (1),
length 84)
    clio.cs.ucy.ac.cy > Asia: ICMP echo reply, id 9759, seq 15, length 64
        0x0000:  0000 ffff 0000 0000 0000 0000 0000 0800  ................
        0x0010:  4500 0054 2e56 0000 3d01 6225 c22a 1187  E..T.V..=.b%.*..
        0x0020:  0a10 0f6d 0000 5e7b 261f 000f b54c ca54  ...m..^{&....L.T
        0x0030:  0000 0000 3ae2 0200 0000 0000 1011 1213  ....:...........
        0x0040:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0050:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0060:  3435 3637
```

Όταν τελειώσει η πιο πάνω εντολή δώστε την εντολή (ή σύνολο εντολών) που βρίσκει και τυπώνει στην οθόνη πόσα TCP πόσα UDP και πόσα ICMP πακέτα στάλθηκαν. Για παράδειγμα:

```
92 ICMP
 6 UDP
 2 TCP
```

Ερώτημα 9

Έστω ότι έχετε ένα αρχείο `input.txt` το οποίο περιέχει και κάποιες ορθογραφικά λανθασμένες λέξεις, δηλαδή οι λέξεις αυτές δεν υπάρχουν στο λεξικό του συστήματος το οποίο βρίσκεται στον κατάλογο `/usr/share/dict/words` (οι πεζοί και οι κεφαλαίοι χαρακτήρες πρέπει να θεωρούνται το ίδιο στη σύγκριση αυτή). Στόχος είναι να εμφανιστούν οι λανθασμένες λέξεις ταξινομημένες και χωρίς διπλά αντίγραφα. (θεωρήστε ότι οι λέξεις είναι όλες γραμμένες με Λατινικούς, δηλ., Αγγλικούς, χαρακτήρες).

Ερώτημα 10

Δημιουργήστε μια λίστα από ΟΛΕΣ τις διεργασίες που εκτελούνται στο σύστημα και φυλάξετε τις στο αρχείο processes.txt. Παράλληλα εκτυπώστε στην οθόνη τις τελευταίες οκτώ (8) γραμμές ταξινομημένες (σε αύξουσα αλφαβητική σειρά) ως προς το όνομα της διεργασίας. Η εντολή δεν γίνεται να χρησιμοποιεί ανακατεύθυνση αλλά μόνο διοχέτευση.

Καλή Επιτυχία !