Name:_______________________________________Student ID:_______________

You will need:
RedHat Linux 7.3 (VM)
Terminal access to mercury.swin.edu.au
A computer with internet access

COS80013 Internet Security

Lab 1 (week 1)

In this lab you will investigate Linux commands

Before you start, download the Virtual machine – this will always be the slowest part of each lab.

Start the Virtual Machine Launcher on the host PC
Select COS80013/ *RedHat Linux with local network*)
Start the download.
Alternatively zipped copies are on OneDrive here:
Virtual Machines

1. CentOS.

1.1 What is ***CentOS***?
(Look it up with Google). Don't copy and paste – write down what it is - in your own words.

1.2 Using a web browser, go to

https://feenix.swin.edu.au/help/ and click on the links for more info.

(a) What is Mercury? Hint: it is NOT the mail server in XAMPP!

(b) Mercury does not support Telnet. What command must you use to get terminal access (login) to **Mercury**?

(c) How is ssh different to **Telnet**?

(d) What version of **CentOS** is Mercury running?

(e) What is the URL of Mercury?

1.3 If you do have access to putty use redhat linux
When you log in, read the banner.
What version of CentOS is Mercury running?

---no banner?
try **cat /etc/redhat-release** (Redhat only) or
cat /etc/issue (other Linuxes)

1.4 What do the following commands do? (Write down the answers here or in a notebook)
After running the command, try <*command*> *--help*
man <*command*> or **info** <*command*> for more information. Typing **q** will get you out of the **man**ual. Or try Google (keyword + 'linux')

ls
ls –l

pwd *Google can tell you what pwd stands for - look for the wikipedia entry.*

ps
ps -al

Name:______________________________________Student ID:________________

cd /
cd
cd ~
cd ..

uname
uname –a

df
df –hi

echo $PATH
echo $Path

Is Linux case sensitive?

history
history | more
history –c

Try a ping command:
ping opax.swin.edu.au
What does it do?
Use CTRL + C to stop the pings
What is the IP address of opax?

Name:____________________________________**Student ID:**______________

1.5 More advanced commands:

(This might not if you are not using mercury, you can search these command does and put summarize the answer)

dig telstra.com

nslookup telstra.com

netstat
netstat | grep CONNECTED
netstat | grep ESTABLISHED

/usr/sbin/lsof

Note:
Executables in Linux have no extensions.
zip files have tar or gz extensions
To run a program, type it's name. If it is in the current directory, type ./name

Try these commands to find the **ifconfig** program:

```
locate ifconfig
which ifconfig
find / -name ifconfig
```

You can get rid of the error messages this way:

```
find / -name ifconfig 2>/dev/null
```

You must type the instructions EXACTLY as shown. Spaces matter in UNIX/LINUX

Where is ifconfig? What does it show?

1.6 Type in the following command:

who
whoami
Who is logged in at the moment?

Try this command

2. RedHat 7.3 Linux VM:

2.1a Download the Linux VM (COS80013-rh73.zip) from Cloudstor (https://cloudstor.aarnet.edu.au/plus/s/k4fmL4iFEhzkVCx).
Unzip all files to a known location on the hard drive and launch the VM (double-click on the .vmx file). OR
2.1 b Download the Linux VM using VMLauncher (Start/VMLauncher, COS30015/ *RedHat Linux with local network*).
Launch the VM using VMLauncher.

You don't have an account on this Linux server, but you can use the *student* account.

log in as **student** — username
student — password

2.2 Try out these commands:

smbstatus
What does it do?

top
What does it do?
(type **q** to quit)

history | more
What does | *more* do?

Name:____________________________________**Student ID:**______________

ls
ls –l
How many files are executable? (look for **x**)

Type the name of one
e.g **hello1**

Doesn't work?
Use **file hello1** ***to see what sort of file it is.***

Linux uses the search path (type echo $PATH to see it) to decide where an executable program can be found.

Type **pwd** to see where you are.
Is this location in the search path?

Preceding a program with **./** tells Linux to ignore the search path and run the program found in the current directory.

Try:
./hello1
Doesn't work?

2.3 To create a text file:

cat > ***<filename>*** where <*filename*> is the name of a new file
...type stuff...
Ctrl+C (stop)

To see what's in a file:
cat *<filename>*

rm -i *<filename>* (delete the file)

You can also create an empty file this way:

touch *<filename>*

2.4 Edit the file:

vi *<filename>*

vi commands:

<insert> - toggle between insert and replace mode
<esc> - go back to command mode

Linux does not use file extensions to determine file type. There are no .exe files in Linux.
Linux uses commands like **chmod** to set permissions which include read, write and execute. Any file can be marked as executable, but only files which contain recognisable bash script or compiled code will actually run.
Type this to remove *exe* rights from the source files:
chmod –x *.asm *.c *.txt *.s

<delete> - delete characters
: - enter a command

e.g.

:w - write file
:q - quit file
:wq - write and then quit a file

Try editing **hello1.asm** - what sort of file is it?

To exit, enter:
<esc>:wq<enter>

2.5 Linux Directories are equivalent to Windows folders.

mkdir <*dirname*>

rmdir <*dirname*>

2.6 Which of these commands can you access? Write down what they do.

locate access_log

updatedb &

find / -name access_log

find / -name ifconfig > temp && more temp
(this takes a while)

which ifconfig

If you are refused permission, tru 'su' (substitute user) to escalate your privileges to root.

the root password

type in
su root
security (logs you in as a the root user)

Try those commands again.

Note: **su** is not a user name. It only works after you have logged in. It changes your current user name to **root** (default) or whatever you type after su.
e.g. **su <enter>** -changes you to root,
su jim <enter> – changes you to jim.
You still need the password.

3. Shut down

3.1 Try these:

exit - logs you out of the **su** shell

halt - shuts the Linux VM down. –but this leaves the VM running with the OS shut down. DON'T USE IT

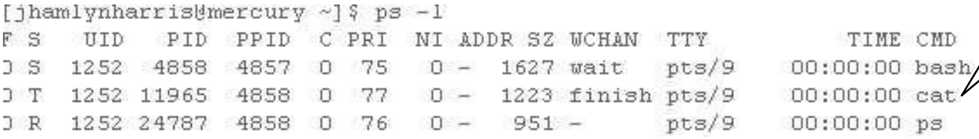
If you did anyway, use the VMWare menu - *Player – Power – Shut down guest*.

While in Linux, try **poweroff** – the best way to shut down
halt –p does the same as **poweroff.**

3.2 If you get this:

There are stopped jobs.

You have left a process running – use
ps –l
to see what it is



```
[jhamlynharris@mercury ~]$ ps -l
F S   UID   PID  PPID  C PRI  NI ADDR SZ WCHAN  TTY          TIME CMD
0 S  1252  4858  4857  0  75   0 -  1627 wait   pts/9    00:00:00 bash
0 T  1252 11965  4858  0  77   0 -  1223 finish pts/9    00:00:00 cat
0 R  1252 24787  4858  0  76   0 -   951 -      pts/9    00:00:00 ps
```

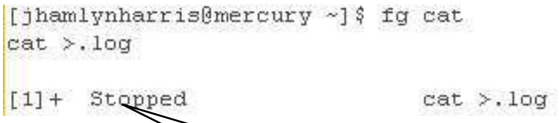
the process that is still running

then type
fg <CMD> where <CMD> is the name of the process you started (what you typed to run it)

to bring the process into the foreground.

e.g. **fg cat**

Stop it the correct way: Ctrl+C for most programs.



```
[jhamlynharris@mercury ~]$ fg cat
cat >.log

[1]+  Stopped                 cat >.log
```

look for this

If this doesn't work, use **ps** to get the PID number, and try

kill <PID>
where <PID> is the PID of the process you want to kill

Name:______________________________________Student ID:______________

Report (COS80013)

Write a one-page report on this lab covering the following:

1. Summarize the topics you explored and the activities you did during this lab.
2. Classify (group) these topics and actions under appropriate headings. Do not just copy the headings used in the instructions. For example, which are the network tools? Which are the file system tools? Which tools manipulate processes? Search tools?
3. Discuss the relevance of these topics and actions in terms of Internet security. i.e. How do the things in this lab contribute to your understanding of Internet security and the IT industry overall?
4. Why do you need to understand (and use) Linux commands?

This report is worth 2 % towards your unit assessment.