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')

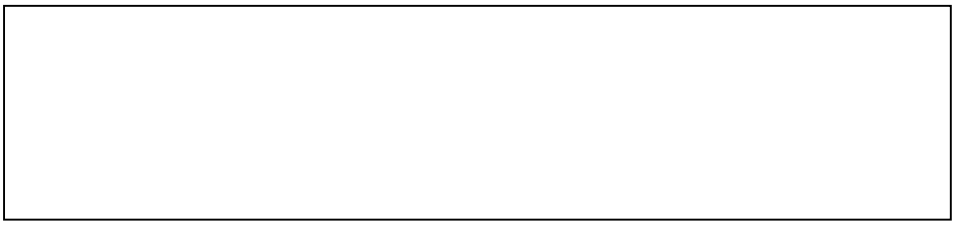
ls
ls –l

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*>

***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

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

<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.

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

the root password

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.

Try those commands again.

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

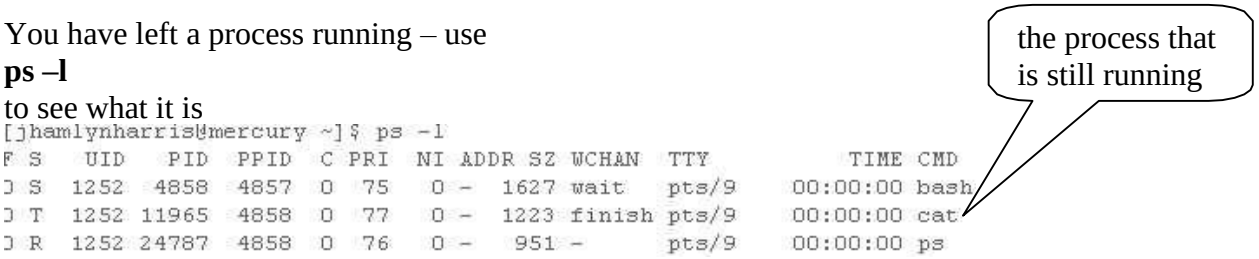
If you did anyway, use the VMWare menu - *Player – Power – Shut down guest*.

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



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.

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.

Internet Security-COS80013 Lab Report Template

Student ID	
Student Name	
Lab Name	
Lab Date	
Tutor	

Title:

The title should be descriptive of the experiments that were done in the lab session. Create a title that reflects the main purpose of the lab.

Introduction:

What is the overall purpose of the lab activity?

What do you expect to learn in this lab?

What are the main hypothesis (predicted outcomes) of the experiment?

Methodology:

What are the key techniques, topics and tools did you need for this lab?

Group them together into a tree-based structure or lists with headings.

Describe how these materials were used to complement the lab experiment.

Data Recording.

Demonstrates key observations or results of your lab. (You can include key results or screenshots which illustrates key experimental results.)

Discussion.

How you can implement the knowledge of this lab in Cyber-security landscape?

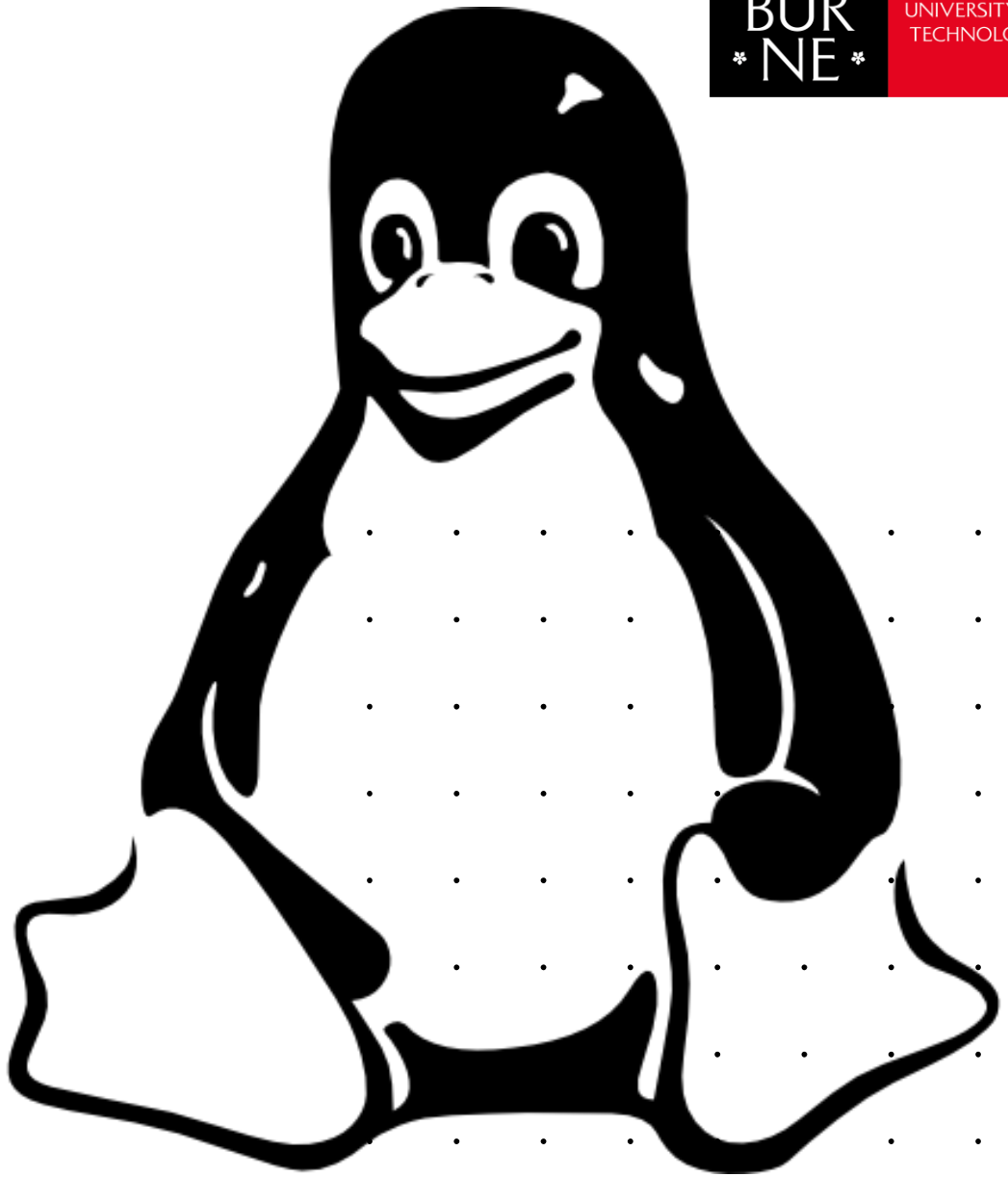
(What cyber-security related issues will be addressed using the techniques, tools and topics used in this lab.)

What are the limitations (if any) to this lab experiment?

SWINBURNE UNIVERSITY OF TECHNOLOGY

Demo Week 1

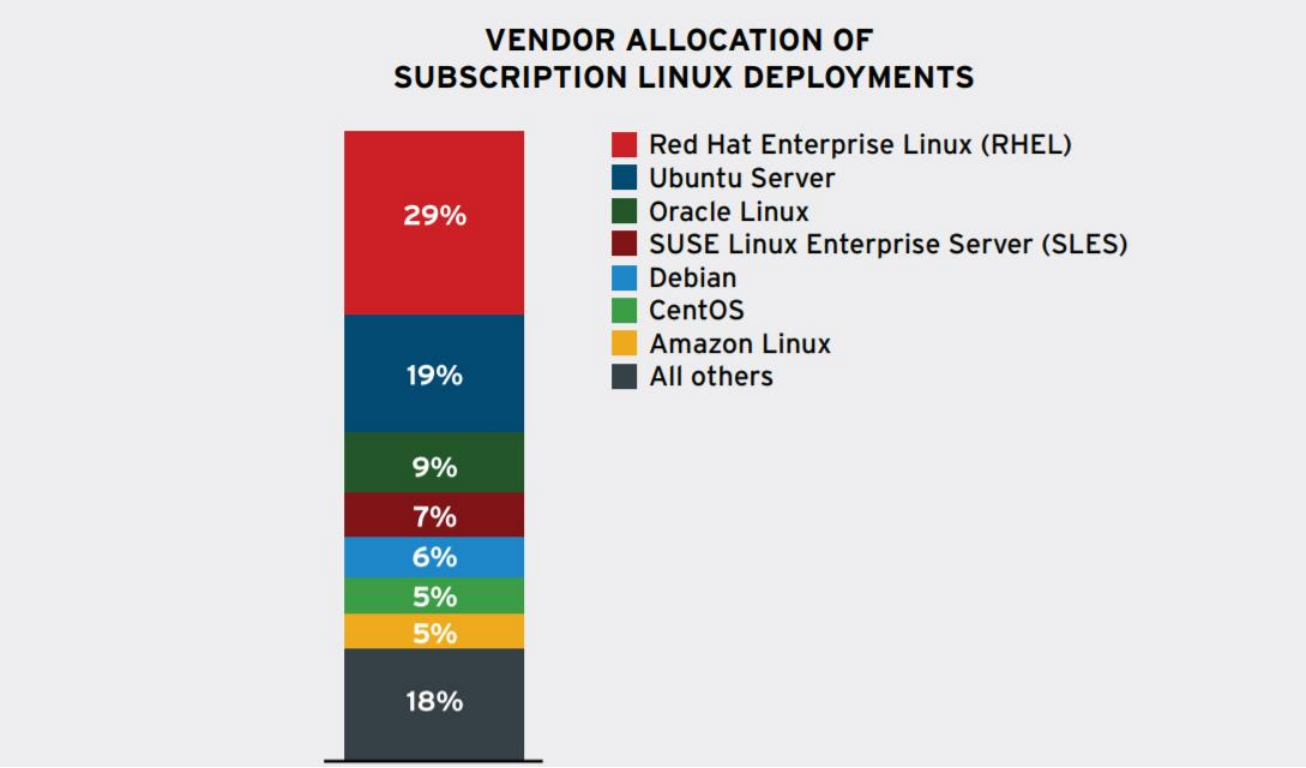
Linux Basics



Investigation of Linux commands

The relevancy

Linux is the most popular operating system for servers and web infrastructure.



The Role of Linux in Cybersecurity

Attacker's PoV	Defender's Pov
• Port scanning • Exploitation • Privilege escalation • Covering tracks • Botnet creation	• System Administration (routers, firewalls) • Vulnerability Scanning (namp, tcpdump) • Forensics (grep-log files) • Automation

Learning Outcomes

- **Familiarization with lab environment.**
  - ✓ Personal lab setup help
  - ✓ Extending Vmware player interface
- **Identifying Linux commands.**

SWINBURNE UNIVERSITY OF TECHNOLOGY

Login for Red hat:- student

Password: student

Login for kali:-root

Password:- toor

What is Red-Hat?

It’s a commercial enterprise Linux distribution

Available through subscription

Customer focused,

- Patches
- Bug fixes
- Updates
- Upgrades
- Technical support

What is Mercury?

Mercury is a distributed main-memory cache management system.

A cache is a high-speed data storage layer which store a subset of data to increase data revival speed.

Swinburne's CentOS server

SWINBURNE UNIVERSITY OF TECHNOLOGY

What command you must use to get secure terminal access (login) to Mercury?

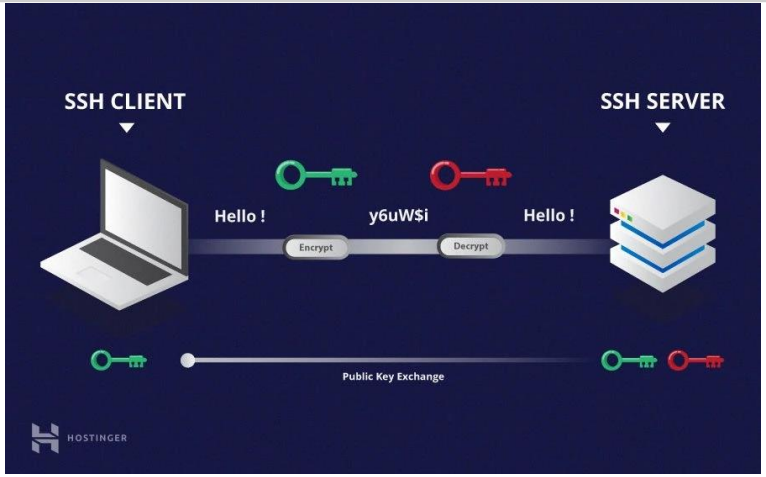
SSH

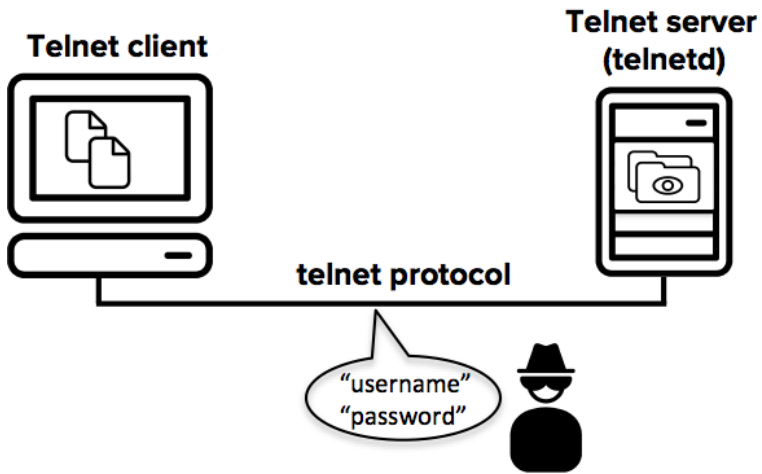
Secure Shell Protocol

-It will unable two computers to communicate using http and share data in an encrypted way.

SSH vs Telnet

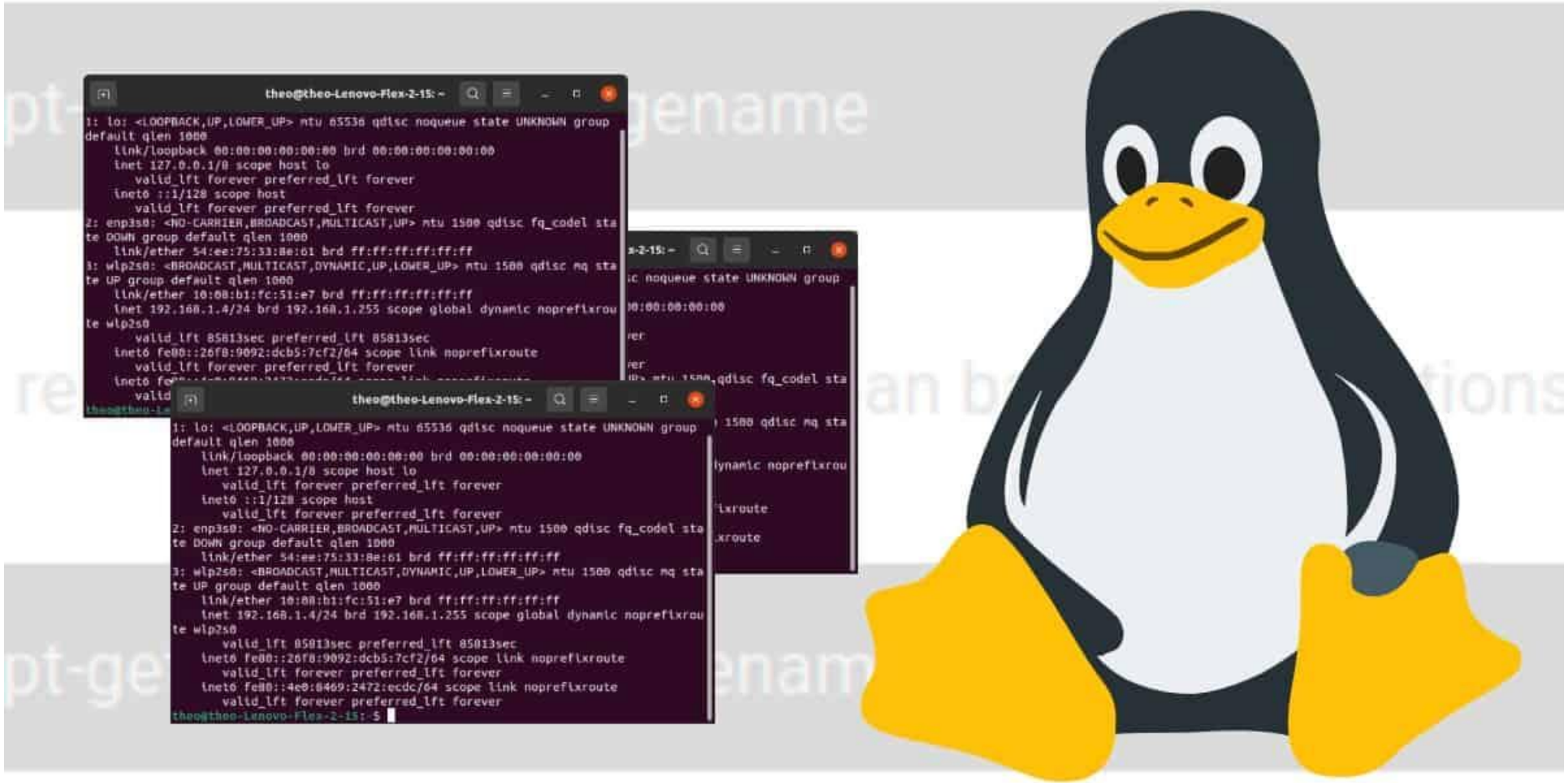
SSH	Telnet
Sends encrypted data	Send data as plain text
Uses public key encryption in order to authenticate	No authentication mechanisms
Mostly used in public networks	Used in private networks
Usually the TCP port number will be 22	Usually the TCP port number will be 23





SWINBURNE UNIVERSITY OF TECHNOLOGY

Introduction to Linux commands



cat command

1. Create a file (cat > filename)

```
sofija@sofija-VirtualBox:~$ cat >test1.txt
This is test file #1.
sofija@sofija-VirtualBox:~$
```

2. To view the contents of a file

```
sofija@sofija-VirtualBox:~$ cat test3.txt
This is test file #1.
```

3. The more and less options(cat file.txt | more)
4. Can view line umbers of a file(cat b-n file.txt)
5. To differentiate end of a file (cat e file)
6. View tab separated lines in file (cat –T test)
7. Use ; at the end of the command you can view multiple files
8. Use standard output with redirection (cat file1 > file2)
9. Append outputs(cat file1 >> file2)

```
sofija@sofija-VirtualBox:~$ cat test1.txt test2.txt > test3.txt
sofija@sofija-VirtualBox:~$ cat test3.txt
This is test file #1.
This is test file #2.
```

10. Sort (| sort > file4)

SWINBURNE UNIVERSITY OF TECHNOLOGY

ls command

1. List
2. Long list
3. View hidden files (ls –a)
4. Find readable files (ls –lh)
5. Directories with ‘/’ at the end[trailing slash] (ls –F)
6. To list file sin reverse order(ls –r)
7. Recursively list sub directories(ls –R)
8. View files and directories in reverse order (ls –ltr)
9. Sort files by size(ls –lS)
10. View inode umbers(ls –i)

```
maverick@maverick-Inspiron-5548:~$ ls -1
1.c
a.out
ass8_1.c
binary.txt
cfile.c
c++file.cpp
cfile.o
cfile.so
client.c
Desktop
Documents
Downloads
end.txt
Exam
examples.desktop
FALCONN-1.2
fifo1.c
fifo2.c
first.txt
glove.cc
google-chrome-stable_current_amd64.deb
kv
libCfile.so
```

Search for more

pwd- (Print working directory)

- When you open a terminal window in Linux, the working directory is your home directory by default.
- The pwd command displays the current directory path on the terminal.
- The pwd command has no options or arguments.
- pwd simply displays the current working directory path.
- The pwd command can be useful for verifying your current working directory .
- The output of the pwd command is the absolute path of the current working directory.

ps command

ps- Process Status

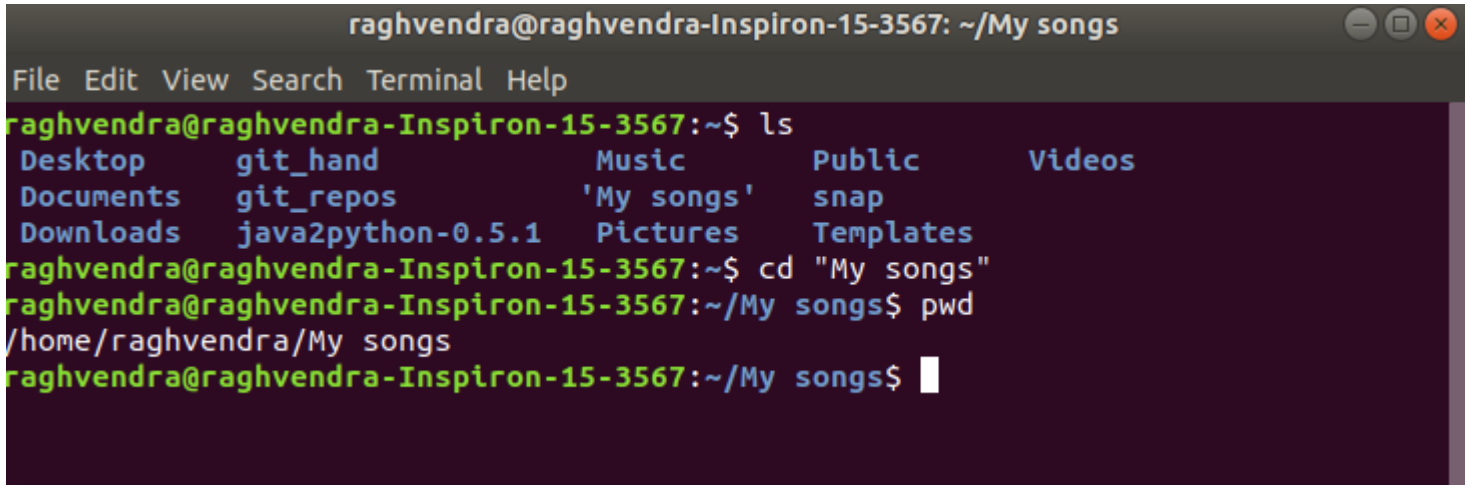
ps –a all running processes
ps –d processes that are running in a particular session or on a particular terminal
ps –T processes running on a Linux system, organized by thread
ps –r processes on a Linux system, sorted by their CPU usage

Process Selection- How we can use ps to select different processes?

cd command

Used for change the directories,

-	Switch back to previous directory
--	Show last working directory
../	Move two directories up
~/Documents && ls	Change current working directory to Documents and list all its setting at once



df command
df –hi command

df: Shows file system space usage details

df -hi: shows file system space usage inode information with sizes in power of 1000

```
echo $PATH
echo $Path
```

echo $PATH: directories where paths are looked for when a command is entered

history
history | more
history –c

History : print all the previous commands used by the user

History | more : shows page by page with more option

History –c : clear history

dig command – (domain information groper)

We can use “dig” command to view query information about Domain Name Systems

Try using *dig –t NS telstra.com*

nslookup command

nslookup -> used for troubleshooting DNS servers as it

Try using *nslookup –type=NS telstra.com*

nslookup [-option] [name | -] [server]

nslookup -type=soa redhat.com

netstat command

netstat -> shows status of current TCP, UDP, UNIX and listening ports

Command	Description
netstat	show a relatively simple list of all active TCP connections
-a	This switch displays active TCP connections
-b	Will display the process's actual file name
-e	show statistics about your network connection
-f	force the netstat command to display the Fully Qualified Domain Name
-o	displays the process identifier (PID)
-p	show connections or statistics only for a particular protocol
-n	prevent netstat from attempting to determine host names for foreign IP addresses

Locate ifconfig	Shows the location of ifconfig
updatedb	unauthorized
Find / -name ifconfig	
find / -name msf > temp && more temp	Locate files with name msf
Which ifconfig	Views the actual location of ifconfig

Thank you