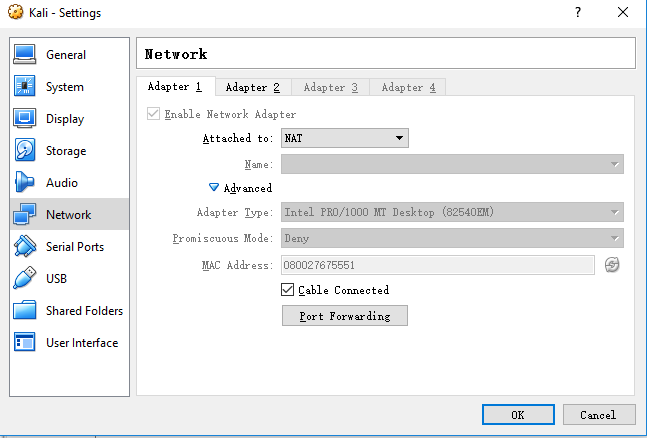
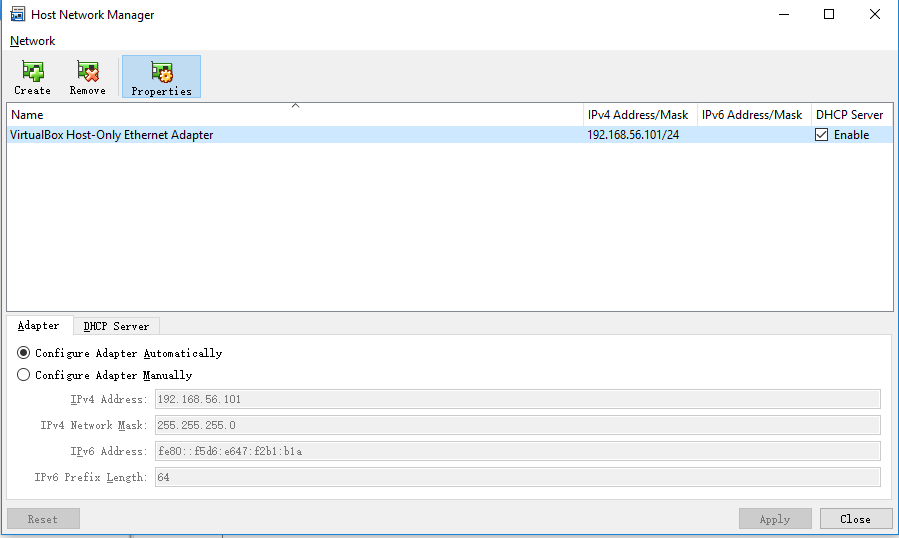
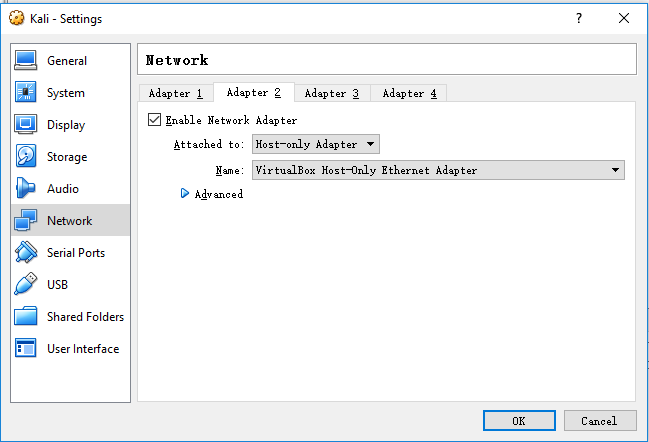
**Linux Commands and Networking**

**Part-1: Setup**

**Creating a Network for Your VMs**

1. We assume that you have created 2 VMs for your Kali and Ubuntu Linux. By default, your VMs should have a “NAT” adapter which makes them connect to the Internet as can be seen below:

However, your two VMs *cannot* talk to each other in this NAT networking mode. To facilitate your lab exercises today, you can create a “Host-only” network, where your VMs can talk to each other, and additionally your host can talk to your VMs.   
As such, a “host-only adapter” is needed for your VMs.

1. In **File → Host Network Manager**, click **Create** to create a new host-only adapter. Select “Configure Adapter Automatically” and enable DHCP Server (unless you are going to specify IP addresses for your VMs).
2. Attach the new host-only adapter to your VMs as their second network adapter.
3. Save your changes and start your two VMs.

**Connectivity Checking**

Now, you want to check if you can reach other machines in your network.

1. Access a VM, and use **ifconfig**/**ip** command to query its IP address:

$ ifconfig # If missing, install net-tools

or

$ ip addr show

It may display multiple IP addresses.   
Which one is the NAT’s and which one is the host-only adapter’s?

1. Try to ping the other VM:

ping ($other\_ip\_address)

1. (Optional) Copy a file from a VM to another VM over ssh:

$ scp /path/to/file  
 user@server:/path/to/destination

1. (Optional) Mount a remote folder via ssh:

$ sudo apt-get install sshfs

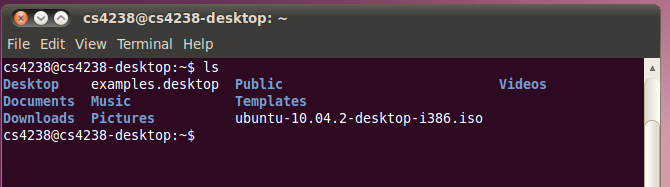
$ sshfs user@server:/remote/dir /local/dir

**Part-2: Recap of Linux Commands**

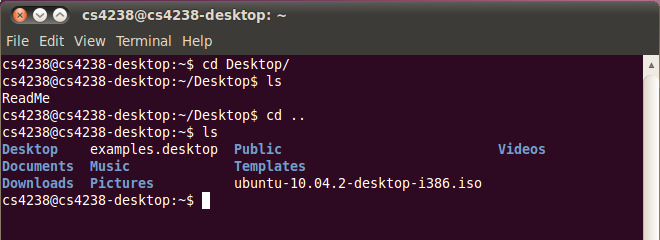
We (need to) assume that you have some familiarity with Linux before.   
If not, please experiment with your Linux setup to get up to speed.   
You can use your Ubuntu machine to practice below.

## File system commands

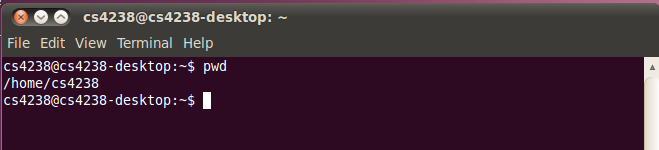
**ls -** list directory contents



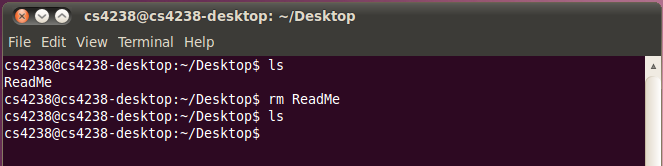
**cd** – enter a directory

****

**pwd -** print name of current/working directory

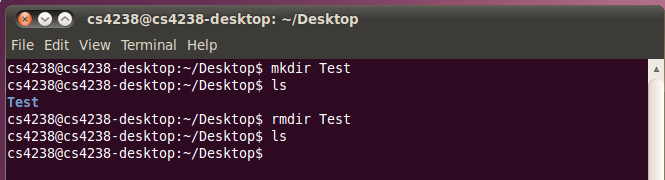


**rm -** remove files or directories



**mkdir -** make directories

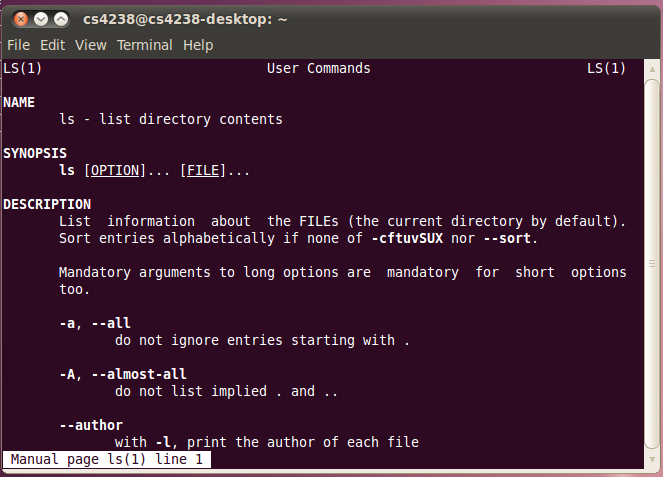
**rmdir -** remove empty directories

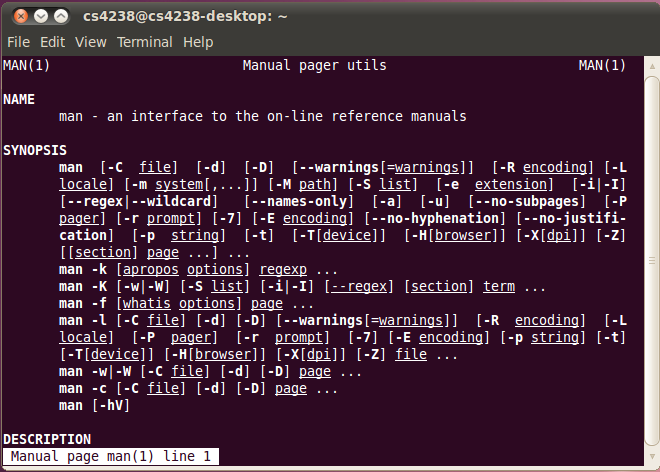


## Interface to the on-line reference manuals: man

**man** - an interface to the on-line reference manuals

Example: man ls

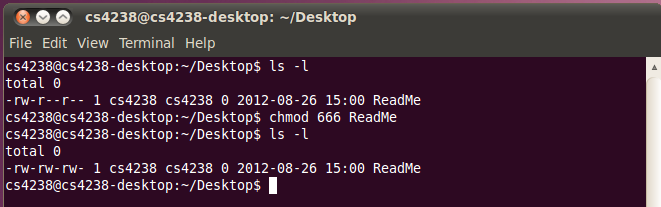


Example: man man**

## File system access control: chmod, chown, chgrp

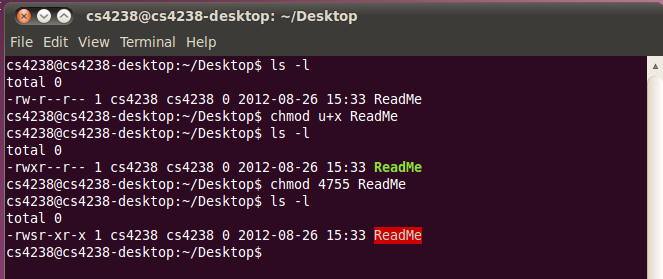
**chmod** - change file mode bits

Example: add write permission of *ReadMe* to all users



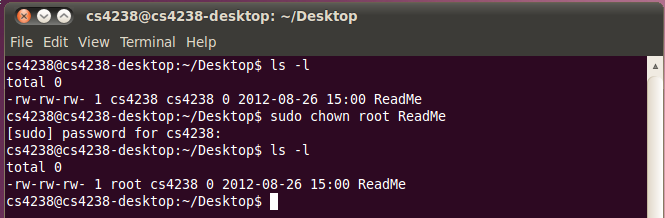
Example: another way to add permission through ‘+’ operator;

add set-uid permission, from *rwx* to *rws*



**chown** - change file owner and group

Example: change owner of *ReadMe* from *cs4238* to *root*



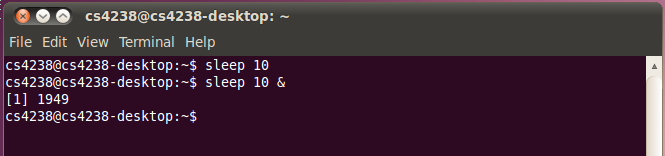
**chgrp** - change group ownership

**Example**: change group of *ReadMe* from *cs4238* to *root*

## Process control: &, ps, kill, fg, bg

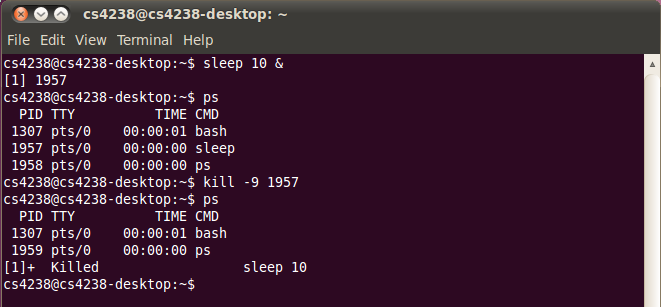
**&** - run program in background

Example: see the difference between “*sleep 10*” and “*sleep 10 &*”



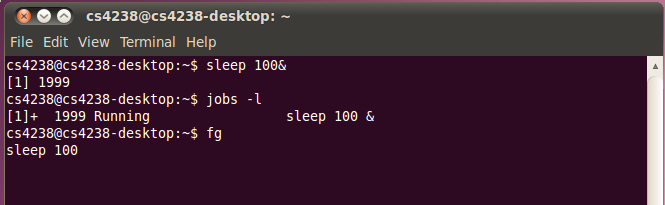
**ps** - report a snapshot of the current processes.

**kill** - send a signal to a process



**jobs** - check the status of the all background jobs

**fg** – run a job in foreground

****

**Ctrl-Z** – pause a job in background

**bg** – run a job in background

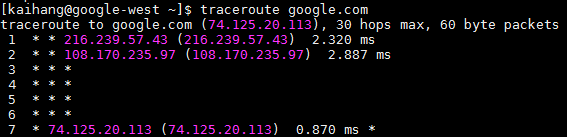
**Part-3: Linux Commands**

Try the following:

* Try “ls” and “ls -la”. What’s the difference?
* Create a folder, put a file there, and delete the folder including the file within one command.
* Try man 1 write; man 2 write. See the difference.
* Create a folder and change its permission and owner.   
  What will happen if a directory does not have executable permission?   
  Can you cd into it? Can you access the file inside the folder?
* Try “ps -aux” and “top”.   
  What’s their difference and which one do you prefer?

**Part-4: Traceroute**

**traceroute** - show the route taken by packets across an IP network



Using Traceroute

Install traceroute on your VM:  
sudo apt install inetutils-traceroute

Try to traceroute comp.nus.edu.sg, google.com, and scanme.nmap.org.

**Part-5: Nmap**

***Important Notes:***

* **Double check every nmap command you’re going to execute**:

Nmap is very powerful and may cause serious harm when executed with incorrect parameters, e. g. you may incidentally run a TCP SYN flood (DoS attack) against innocent victim.

* **Do not scan any host without explicit permission obtained beforehand**!

Some organizations and countries consider network scanning as a *violation* of their security policy or even law and your activity might have disciplinary/legal consequences!

* **Hint**:   
  See [10 useful nmap commands](http://bencane.com/2013/02/25/10-nmap-commands-every-sysadmin-should-know/)

Scanning with Nmap

Install [nmap](https://nmap.org/) on your VM:  
sudo apt install nmap

Install some services for scanning, e.g. ssh server, telnetd server, apache2 server:  
sudo apt install openssh-server telnetd apache2

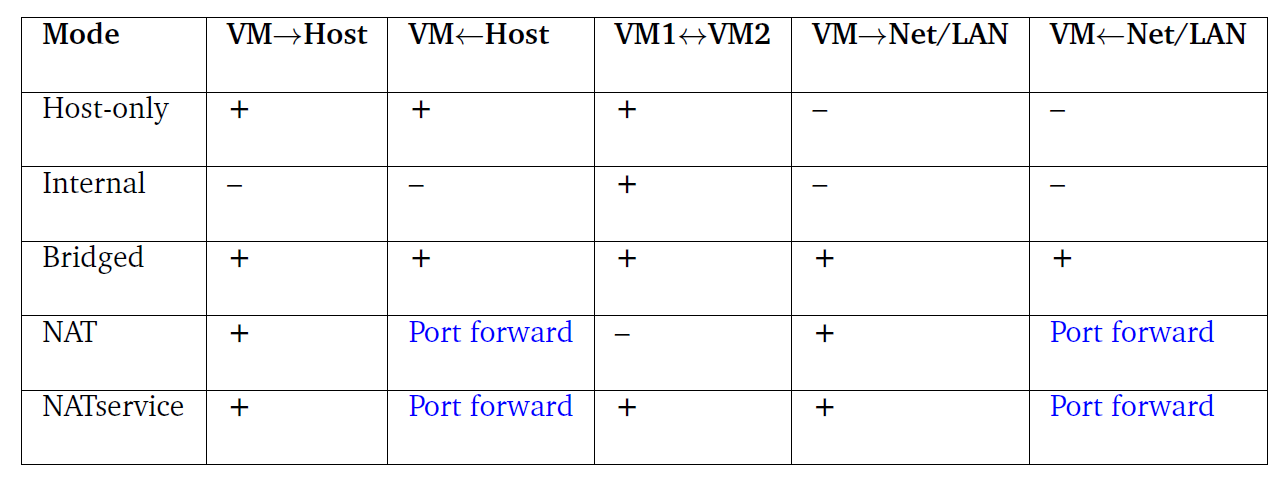
Scanning tasks:

1. Use nmap to scan localhost with various options (e.g. different type of scans, OS and service fingerprinting, timing):  
   nmap -T4 -A –v localhost
2. Scan your VM network. (x.x.x.0/24)
   1. What are the OSes of discovered machines?
   2. What services are running on them?
   3. How many ports are open on the PC?   
      How many TCPs and UDPs?
   4. What do MAC addresses tell about the infrastructure of the VM network?
3. (Optional) If you prefer a graphical interface, install [zenmap](https://nmap.org/zenmap/) and run it:

sudo apt install zenmap

**Part-6: VirtualBox Networking Modes**

Try out the different networking modes and ensure that the connectivity provided by VirtualBox matches that specified in the table below.



**Part-7: Which mode do you use?**

For CS4238, the TAs want to create a network of 50 VMs, where each VM is connected to every other VM. The TAs are provided with two physical server, each of which can support 25 VMs due to memory constraints. Use a network diagram to show how they will achieve this setup along with the Virtualbox network mode they should be using.