MMXXIV

PlinkoUniversity

Collegiate Cyber Defense Club

https://plinko.horse

HACK

OpenStack Instructions

- Download OpenVPN config, and connect
- Naviagate to http://192.168.101.25
- Login with the credentials sent to your email
- Generate and add ssh key
- Create VM
- SSH into the box

Create SSH Key

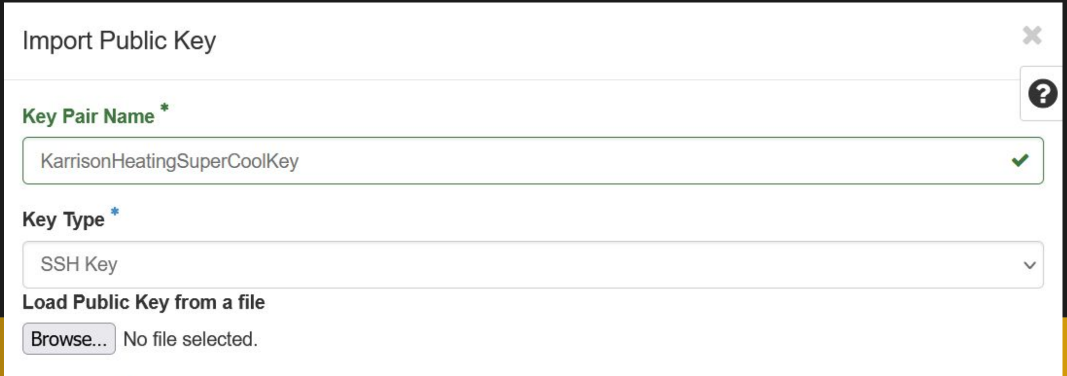
Open a terminal run

```
ssh-keygen -t ed25519
```

Got to the directory it says it put the key and copy the one that is ends in .pub

In OpenStack (under “Compute” -> “Key Pairs”) click “Import Key Pair”.

1. Name it something reasonable.
2. Set “Key Type” to “SSH Key”.
3. Paste the contents of your id_rsa.pub file here, or use “Load Public Key from a file” to upload it.



Import Public Key

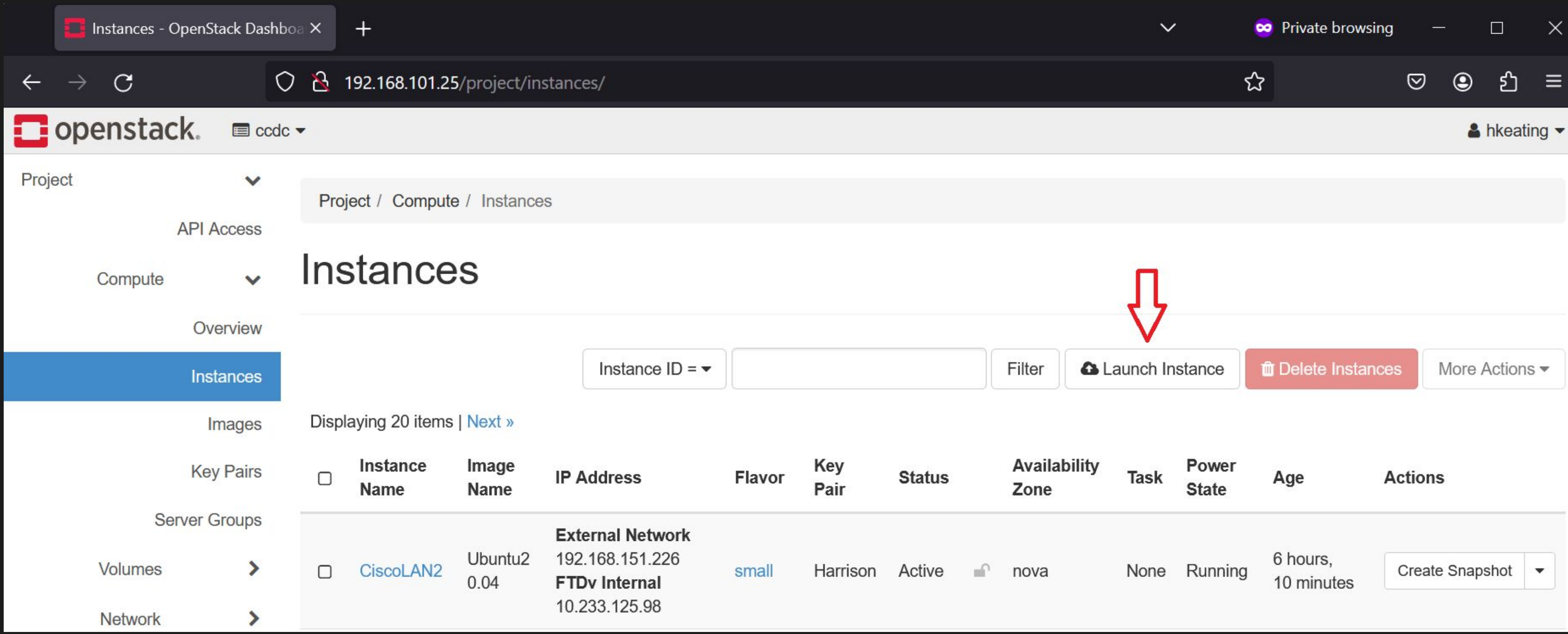
Key Pair Name *

KarrisonHeatingSuperCoolKey

Key Type *

SSH Key

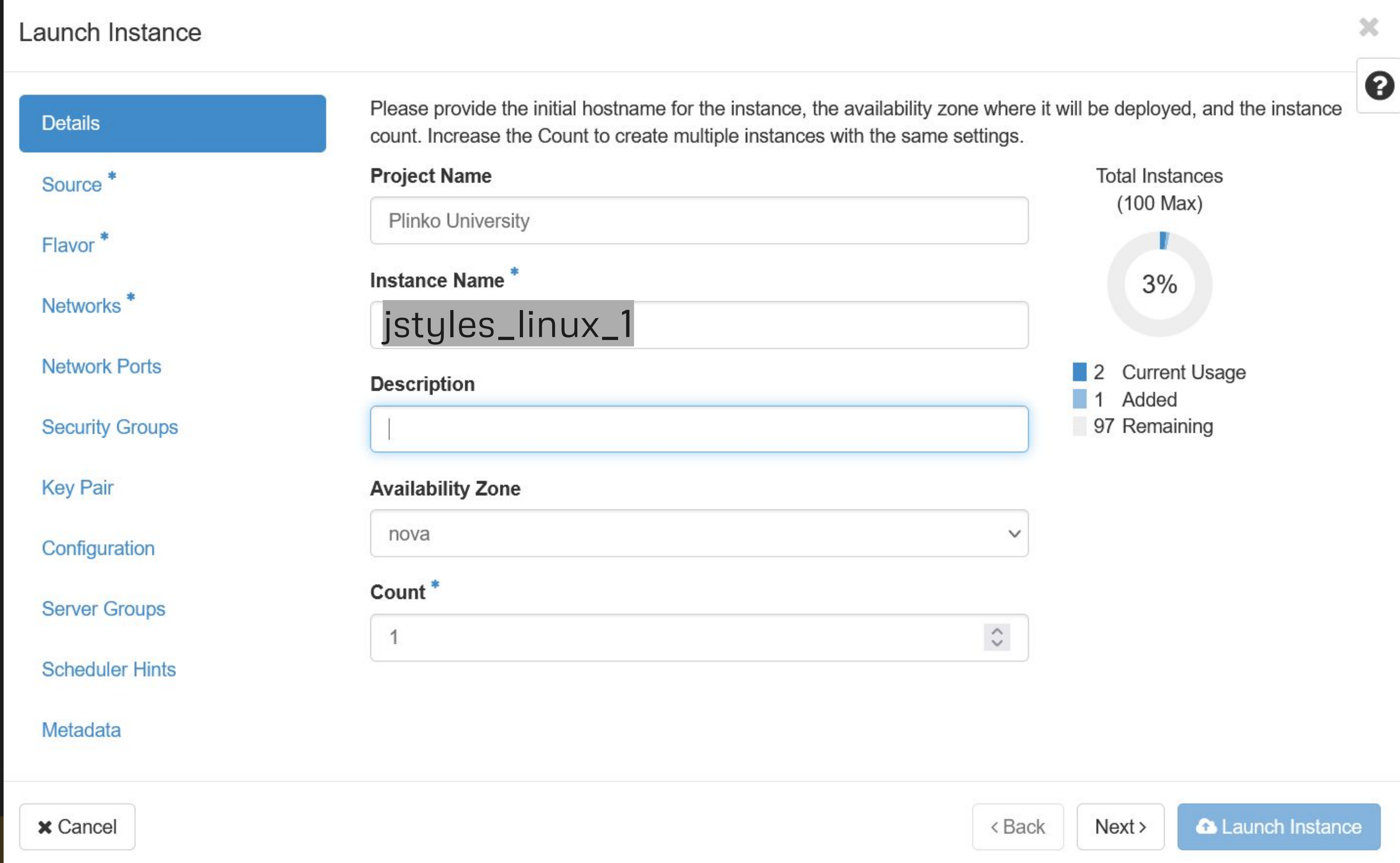
Load Public Key from a file



Instances

Displaying 20 items | Next »

☐	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status		Availability Zone	Task	Power State	Age	Actions
☐	CiscoLAN2	Ubuntu20.04	**External Network** 192.168.151.226 **FTDv Internal** 10.233.125.98	small	Harrison	Active	🔓	nova	None	Running	6 hours, 10 minutes	Create Snapshot ▾



Launch Instance

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

Project Name
Plinko University

Instance Name *
jstyles_linux_1

Description

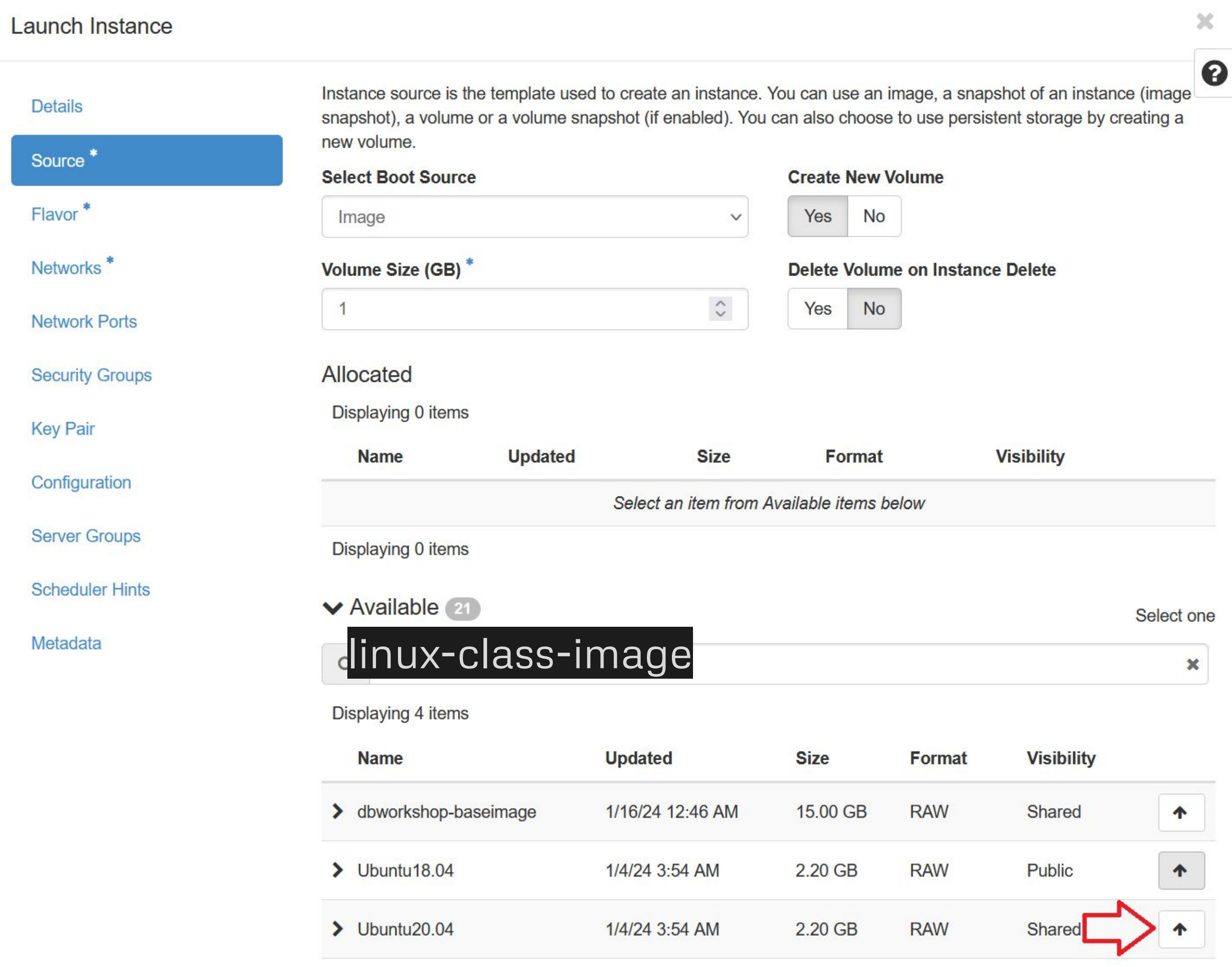
Availability Zone
nova

Count *
1

Total Instances
(100 Max)

3%

🟦	2	Current Usage
🟦	1	Added
⬜	97	Remaining



Launch Instance

Instance source is the template used to create an instance. You can use an image, a snapshot of an instance (image snapshot), a volume or a volume snapshot (if enabled). You can also choose to use persistent storage by creating a new volume.

Select Boot Source: Image

Create New Volume: [✓ Yes] No

Volume Size (GB) *: 1

Delete Volume on Instance Delete: Yes [✓ No]

Allocated

Displaying 0 items

Name	Updated	Size	Format	Visibility
Select an item from Available items below				

Displaying 0 items

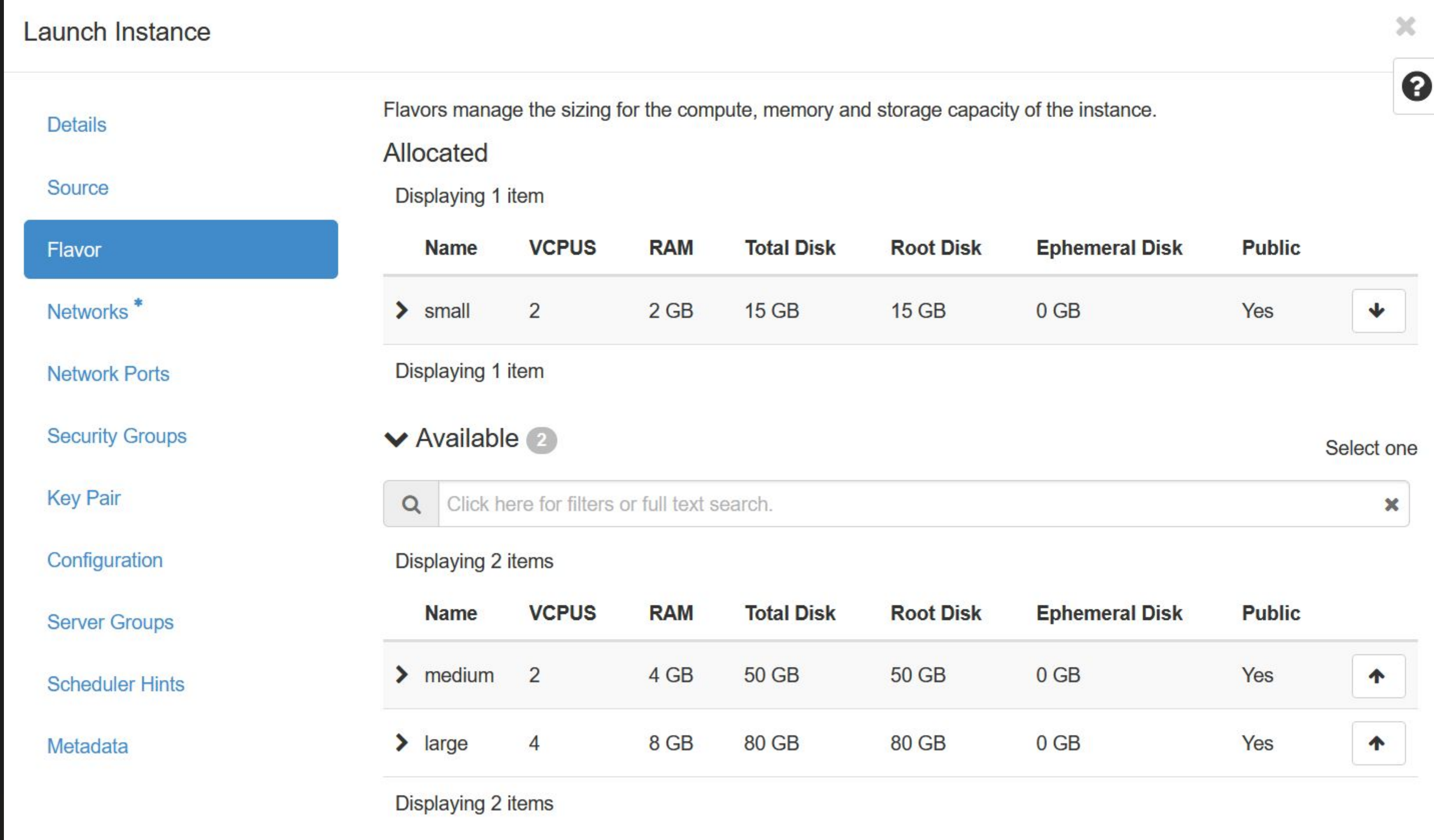
Available 21

Select one

linux-class-image

Displaying 4 items

Name	Updated	Size	Format	Visibility	
dbworkshop-baseimage	1/16/24 12:46 AM	15.00 GB	RAW	Shared	↑
Ubuntu18.04	1/4/24 3:54 AM	2.20 GB	RAW	Public	↑
Ubuntu20.04	1/4/24 3:54 AM	2.20 GB	RAW	Shared	↑



Launch Instance

Flavors manage the sizing for the compute, memory and storage capacity of the instance.

Allocated

Displaying 1 item

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
small	2	2 GB	15 GB	15 GB	0 GB	Yes

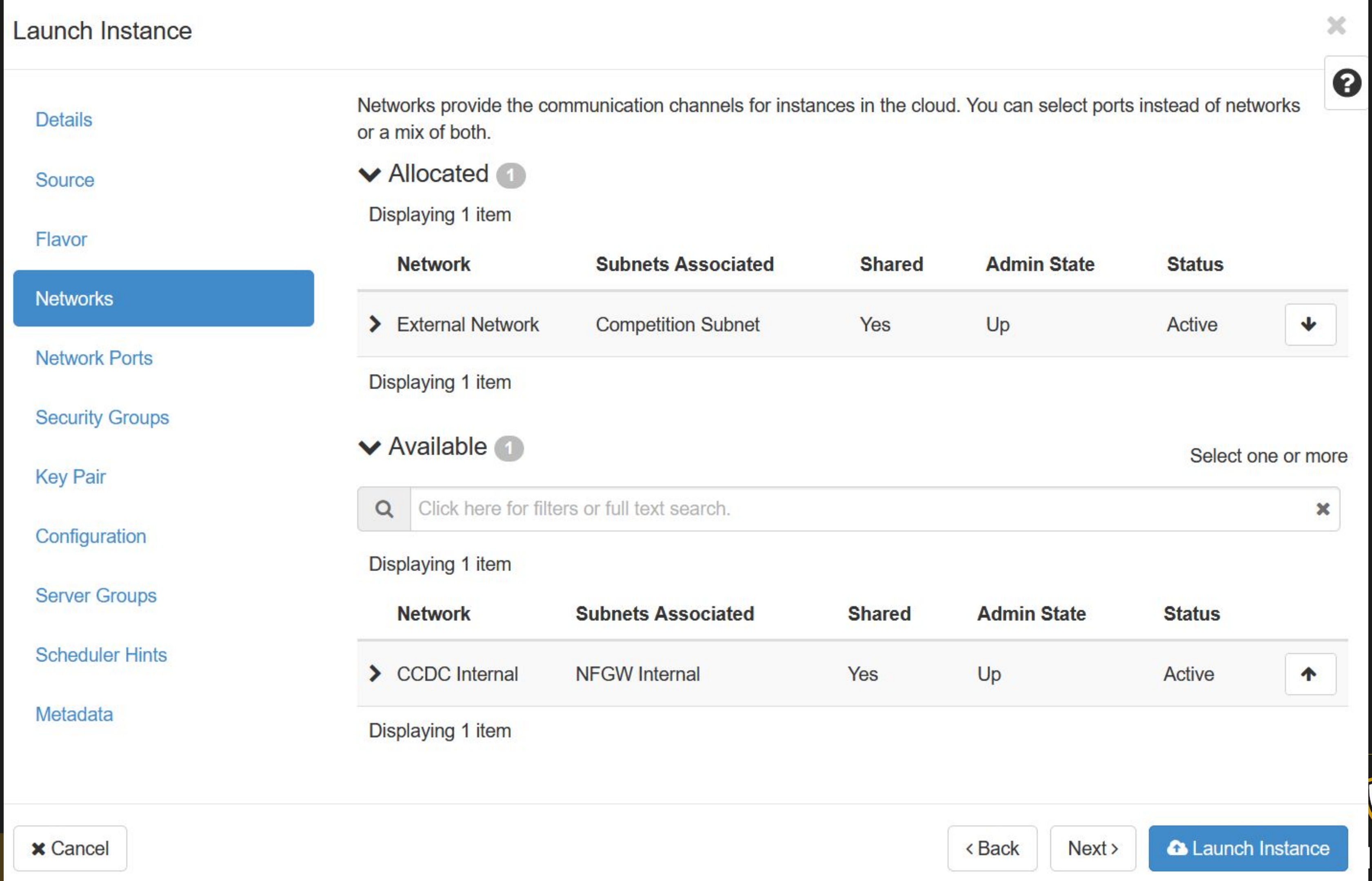
Displaying 1 item

Available 2

Displaying 2 items

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
medium	2	4 GB	50 GB	50 GB	0 GB	Yes
large	4	8 GB	80 GB	80 GB	0 GB	Yes

Displaying 2 items



Networks provide the communication channels for instances in the cloud. You can select ports instead of networks or a mix of both.

Allocated 1

Displaying 1 item

Network	Subnets Associated	Shared	Admin State	Status
External Network	Competition Subnet	Yes	Up	Active

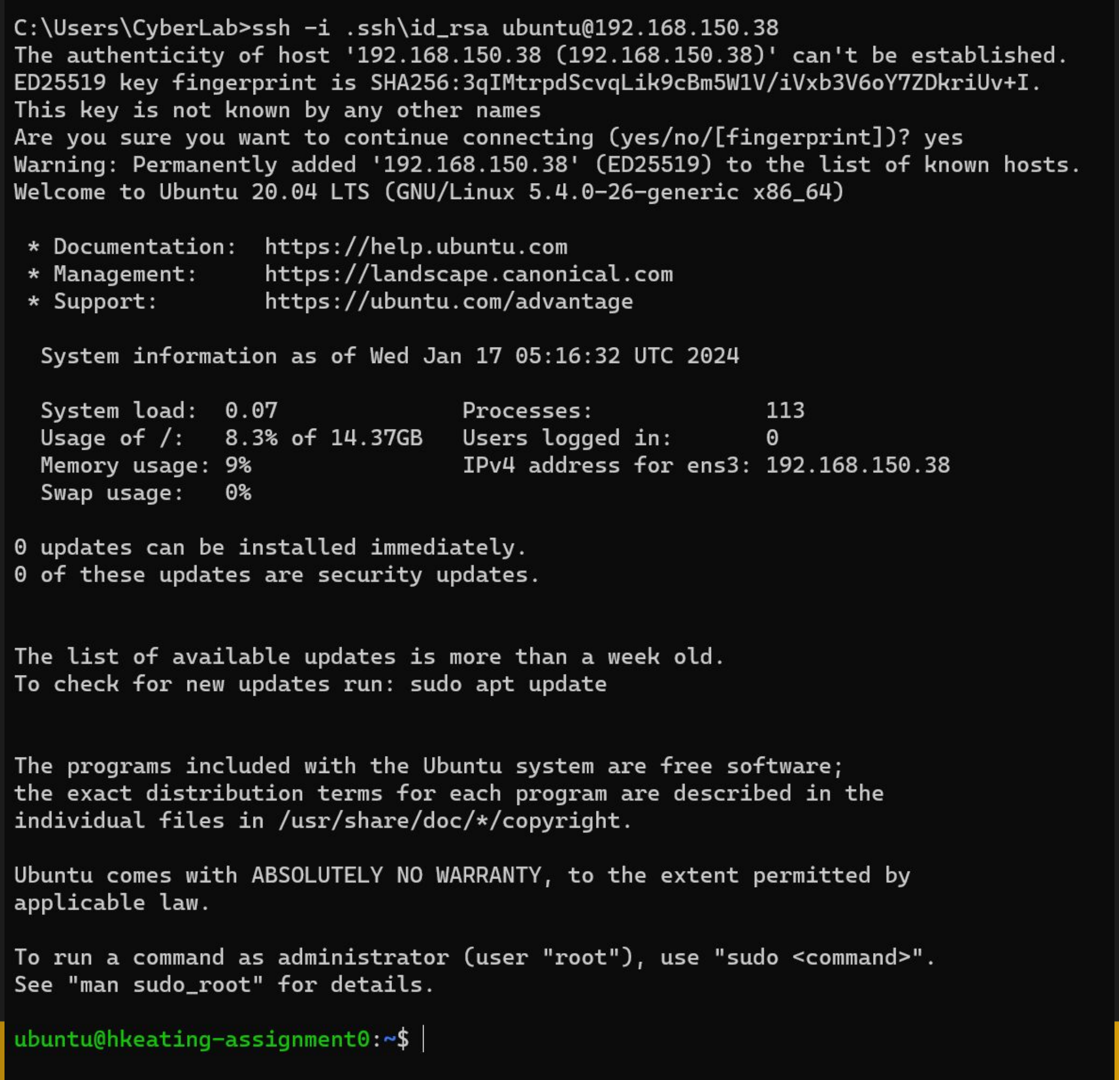
Displaying 1 item

Available 1

Displaying 1 item

Network	Subnets Associated	Shared	Admin State	Status
CCDC Internal	NFGW Internal	Yes	Up	Active

Displaying 1 item

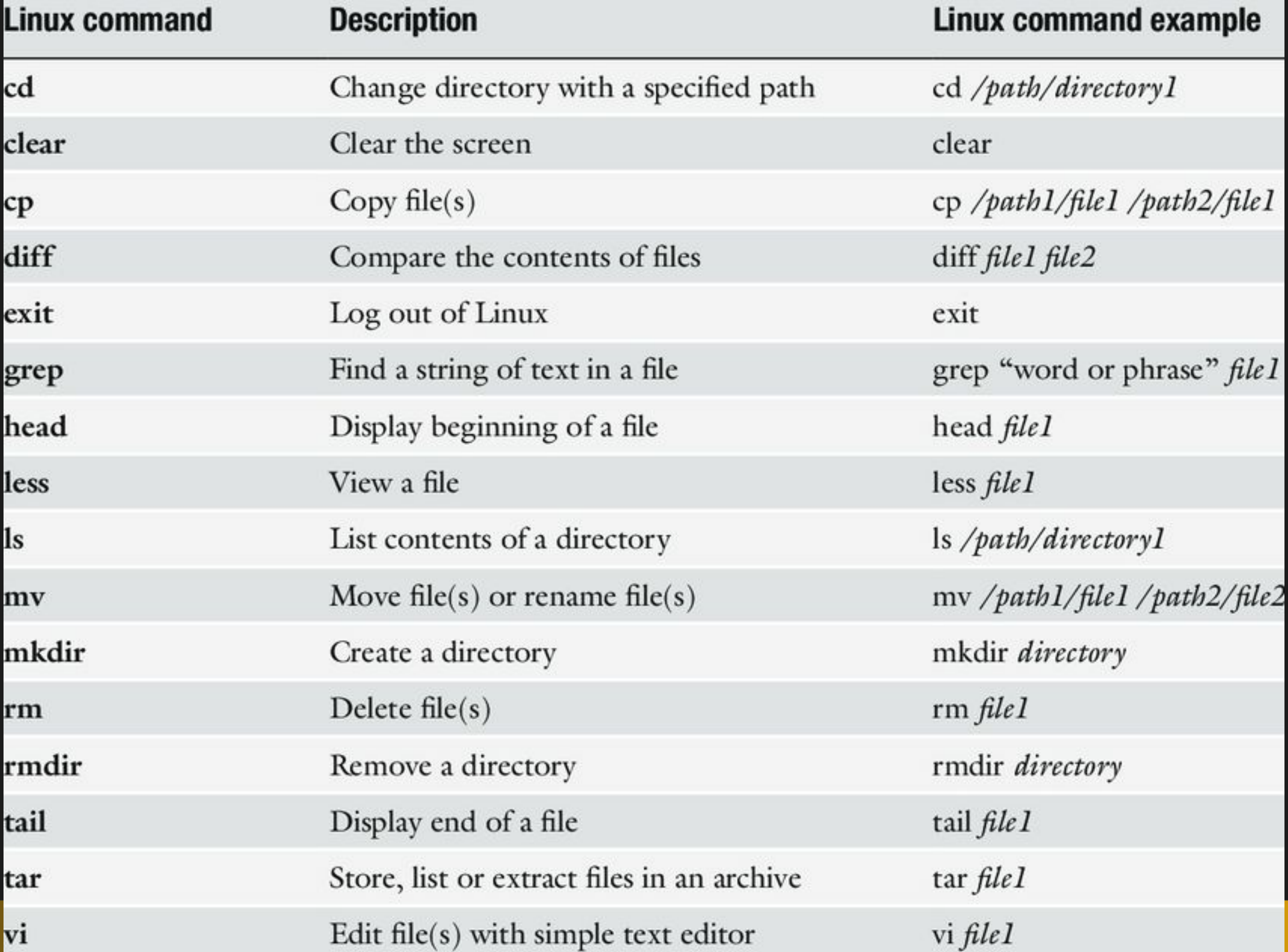


```
C:\Users\CyberLab>ssh -i .ssh\id_rsa ubuntu@192.168.150.38
The authenticity of host '192.168.150.38 (192.168.150.38)' can't be established.
ED25519 key fingerprint is SHA256:3qIMtrpdScvqLik9cBm5W1V/iVxb3V6oY7ZDkriUv+I.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.150.38' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-26-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Jan 17 05:16:32 UTC 2024

  System load:  0.07              Processes:             113
  Usage of /:   8.3% of 14.37GB   Users logged in:       0
  Memory usage: 9%                IPv4 address for ens3: 192.168.150.38
  Swap usage:   0%

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@hkeating-assignment0:~$
```

Assignments

4 mini assignments

1. Linux scavenger hunt
2. My Brand New Website
3. Game Time
4. Blockgame



Linux command	Description	Linux command example
cd	Change directory with a specified path	cd */path/directory1*
clear	Clear the screen	clear
cp	Copy file(s)	cp */path1/file1 /path2/file1*
diff	Compare the contents of files	diff *file1 file2*
exit	Log out of Linux	exit
grep	Find a string of text in a file	grep "word or phrase" *file1*
head	Display beginning of a file	head *file1*
less	View a file	less *file1*
ls	List contents of a directory	ls */path/directory1*
mv	Move file(s) or rename file(s)	mv */path1/file1 /path2/file2*
mkdir	Create a directory	mkdir *directory*
rm	Delete file(s)	rm *file1*
rmdir	Remove a directory	rmdir *directory*
tail	Display end of a file	tail *file1*
tar	Store, list or extract files in an archive	tar *file1*
vi	Edit file(s) with simple text editor	vi *file1*

Anatomy of a Linux command

Positional Arguments

```
cp [source] [destination]
```

Flag

`cp -r [source] [destination]` or

`ls -laR or mysql -h 127.0.0.1 -u bob -p` or `docker -- help`

Sub command

```
docker --tlsverify run -rm hello-world
```

Sudo

Privilege escalation

If it doesn't work, try it with sudo

```
sudo cat /etc/shadow
```

You can also become other users

```
sudo -u test echo $USER
```

What is Linux?

Linux kernel

- Developed by the open source community
- Lead by Linus Torvalds

+ Open source projects

- Like Gnu Coreutils and systemd

+ Distribution Maintainers

- Combine all the above things into a single cohesive operating system
- Responsible for choosing what packages and which versions to include

= Linux

Assignment 1

In Webcourses you will find a quiz with hints for when flags are located. Using your basic knowledge of Linux commands and copious amounts of googling, find the flags.

Note: using any kind of grep find ripgrep is considered academic misconduct and will result in a plinking

Cool Demo

Use `ip a` to find the ip of your linux box. In your browser navigate to http://ip:80 to see the beautiful website

Whoops it's broken (Assignment 2)

In assignment 2 document the steps we take in order to fix the webserver and how we updated the site.

Systemd Basics

Systemd is the init process for most Linux distributions

That means it starts all the other services when the linux server starts.

```
systemctl status *service-name*
systemctl enable *service-name*
systemctl start/stop/restart *service-name*
```

Editing Files

There are lots of different cli text editors

The best one is neovim (fight me)

If you don’t have a favorite use nano

```
nano /path/to/filename
```

Ctrl-x to exit (hit y to write the file)

Downloading files

Download an image to add to your website

Copy the link and use wget to download the url

```
wget https://upload.wikimedia.org/wikipedia/commons/d/d2/Uluguru_Mountain_Ranges.jpg
```

Permissions

A well setup Linux box will have different users for different applications and roles.

Any non-root user will be limited by the permissions on a file

Using `ls -l` will show you the permissions on all files and folders in a directory

```
chown user02 file1
chown :groupA file1
chown user02:groupA file2
```

Permissions Pt. 2

There are three permission and the ways these permissions can be applied

- User, Group, Other
- Read, Write, Execute
- Read 4, Write 2, Execute 1\

So `chmod 740 file2` would,

- The 7 is assigned to the user and is the sum of 4+2+1 or read+write+execute (full access)
- The 4 is assigned to the group and is the sum of 4+0+0 (read-only)
- The 0 is assigned to others and is the sum of 0+0+0 (no access)

Assignment 3 - Game Time

- Update Server
- Install terminal Game
- Create a user for your friend
- Have friend ssh into your server and play your game
- Uninstall Game
- Lock User

Apt Package Management

`sudo apt update` - updates list of packages

`sudo apt upgrade` - downloads all the packages install them with dpkg

`sudo apt search *item*` - search for a list of packages

`sudo apt install *item*` - installs package

`sudo apt reinstall *item*` - reinstalls package

Sudo apt autoremove *item*

Other way to

Snap - garbage

Flatpak - basically the same as snap but not garbage

Dnf - basically the same as apt but newer and for RHEL based distros

Pacman - for arch based

User Management

`useradd -m *name* `add user with name and create home directory

`sudo passwd *user* `change user password

`sudo groupadd games` create games group

`sudo usermod -a -G games *user* `Add user to games group

`sudo usermod -L *user*` prevent user from logging in

`sudo userdel *user*` remove user

`sudo mkhomedir_helper username` when you forget to add a home directory

Assignment 4 - Blockgame (the knockoff)

Fix the blockgame

Find listening ports

```
ss -peanut
netstat -planet
```

Reading logs

```
sudo journalctl -u minetest-server
sudo systemctl status minetest-server
```

Postgres (basically the bare min)

```
sudo -u postgres psql
ALTER USER user_name WITH PASSWORD 'new_password';
\q
```

Thank you!

MMXXIV

PlinkoUniversity

https://plinko.horse