Intro to Linux

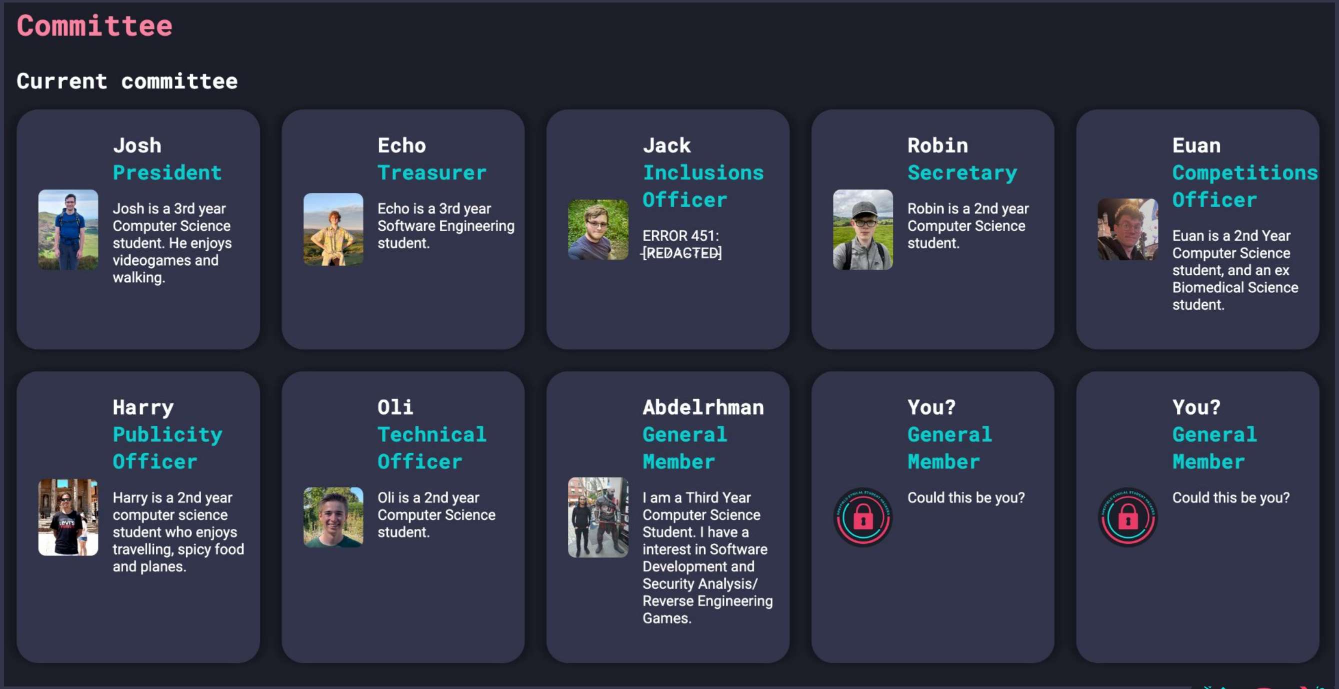
SHEFFIELD ETHICAL STUDENT HACKERS

EGM Time!

We're looking for two new General Members!

- Run sessions
- Help out
- Have fun!

https://forms.gle/RK1PLMm97dX31yC49



Committee

Current committee

Josh
President
Josh is a 3rd year Computer Science student. He enjoys videogames and walking.

Echo
Treasurer
Echo is a 3rd year Software Engineering student.

Jack
Inclusions Officer
ERROR 451: ~~[REDACTED]~~

Robin
Secretary
Robin is a 2nd year Computer Science student.

Euan
Competitions Officer
Euan is a 2nd Year Computer Science student, and an ex Biomedical Science student.

Harry
Publicity Officer
Harry is a 2nd Year computer science student who enjoys travelling, spicy food and planes.

Oli
Technical Officer
Oli is a 2nd year Computer Science student.

Abdelrhman
General Member
I am a Third Year Computer Science Student. I have a interest in Software Development and Security Analysis/ Reverse Engineering Games.

You?
General Member
Could this be you?

You?
General Member
Could this be you?

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

- Relevant UK Law: https://www.legislation.gov.uk/ukpga/1990/18/contents

SHEFFIELD ETHICAL STUDENT HACKERS

Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at **shefesh.com/conduct**

What is Linux?

An Operating System **Kernel**

Kernel:

- Basic core functionality
- Handles allocation of memory, CPU time, and other resources to **processes**
- Provides an **A**pplication **P**rogramming **I**nterface (API) that can be used by processes
    - Communicate with hardware

Distributions

We have the basis (The Kernel)

- Need to put other things on top to build a full OS
- Lots of different software depending on what we want the OS to do

These collections are referred to as ‘Distributions’

- More commonly known as ‘Distros’

There are over 600 actively maintained linux distributions

More Distros Please

Linux is **Free** and **Open-Source**

- Used literally everywhere
    - > 85% of smartphones (Android is Linux based)
    - > 95% of top one million web-servers (AWS, GCP)
    - Top 500 fastest supercomputers

Lots of Distros

- Ubuntu, Fedora, Mint
- Arch, Kali, Qubes
- Red Star, Hannah Montana, Justin Bieber

SSH

SSH - **S**ecure **Sh**ell

Common way to connect to a remote server

Follow the instructions on the whiteboard!

Basic Commands

pwd - **P**rint **W**orking **D**irectory

- Prints current directory you are in

cd [path] - **C**hange **D**irectory

- Allows you to move between directories

ls - **L**i**s**t Directory

- Lists all files within the current directory

mkdir [name] - **M**a**k**e **Dir**ectory

- Makes a new directory

cat [file]

- Prints out the contents of the file

cp [from] [to] - **C**o**p**y

- Used to copy files or directories (use -r for directories)

rm [file/dir] - **R**e**m**ove

- Used to delete files or directories (use -r for directories)

echo [text]

- Prints out the text

nano [file]

- Opens a text editor

mv [from] [to] - **M**o**v**e

- Used to move files or directories (use -r for directories)
- Can also be used to rename files/directories

Changing the output

The output of commands write to the ‘standard output’ (aka stdout)
By default, stdout is shown in your terminal window

- But we can change this (redirect)

a | b

- Sends the result from a into the input of b
- ls | wc -l

a >> b

- Output of a is appended to b
- b is usually a file (i.e “text.txt”)

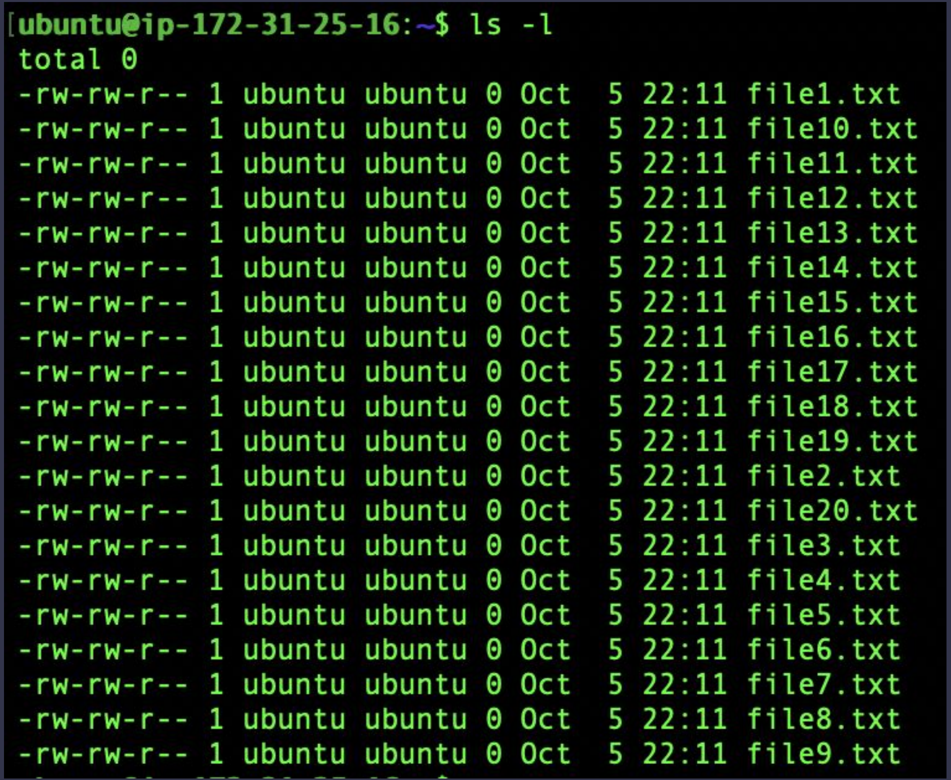
a > b

- Output of a overwrites contents of b

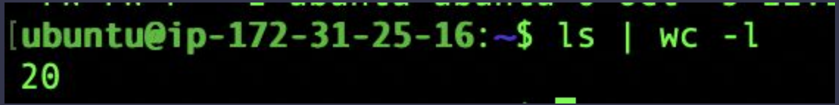
a < b

- Redirects a file (b) into the input of a
- sort < output.txt

Pipe Operator!!!

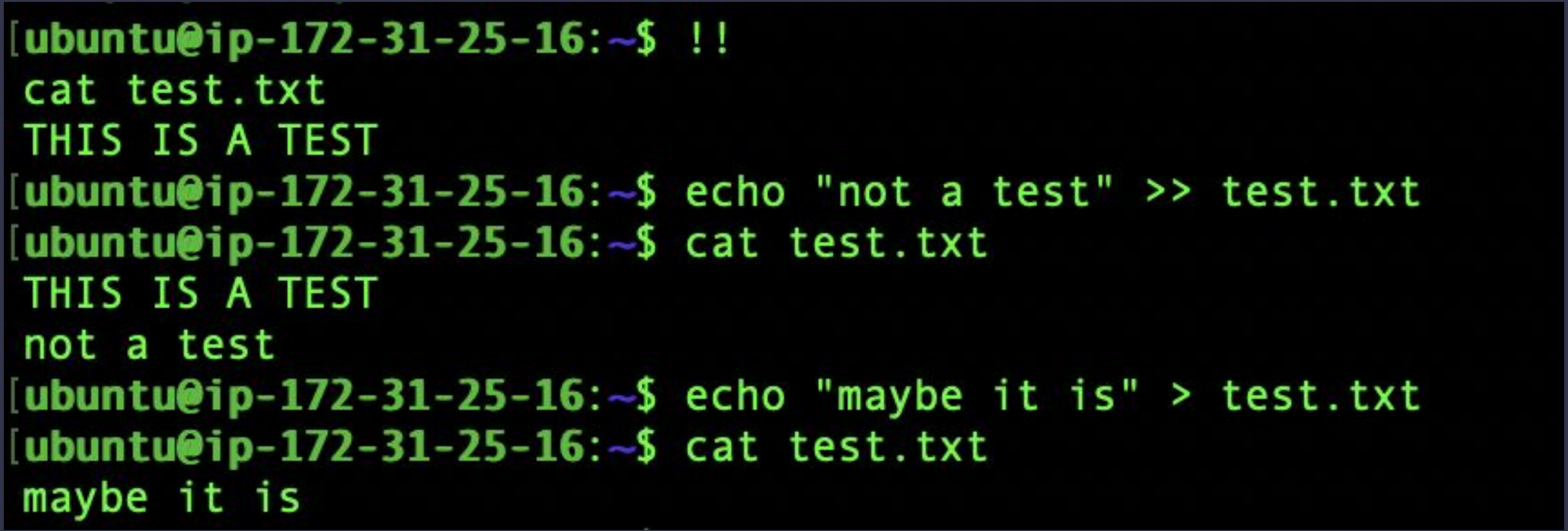


```
[ubuntu@ip-172-31-25-16:~$ ls -l
 total 0
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file1.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file10.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file11.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file12.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file13.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file14.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file15.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file16.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file17.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file18.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file19.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file2.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file20.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file3.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file4.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file5.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file6.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file7.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file8.txt
 -rw-rw-r-- 1 ubuntu ubuntu 0 Oct  5 22:11 file9.txt
```



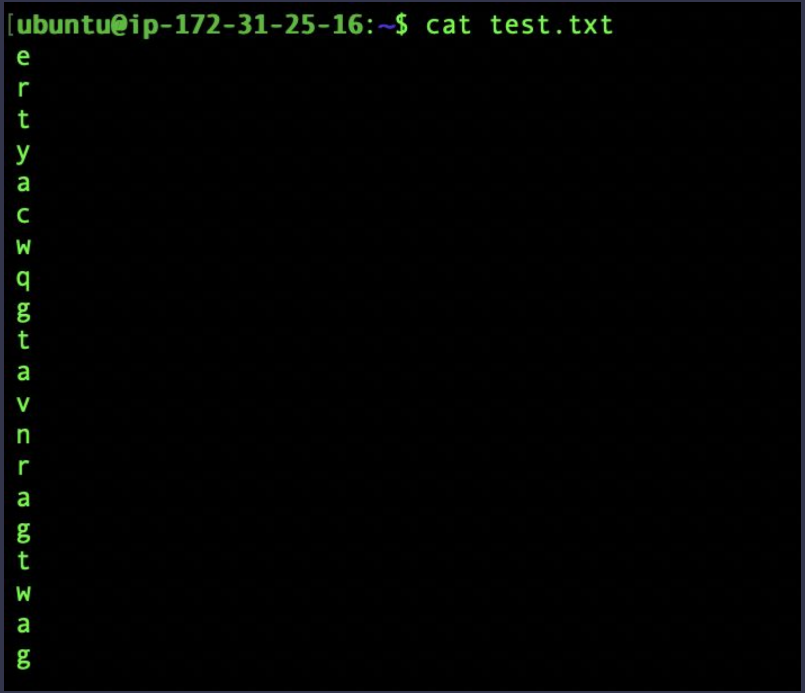
```
[ubuntu@ip-172-31-25-16:~$ ls | wc -l
 20
```

Redirections

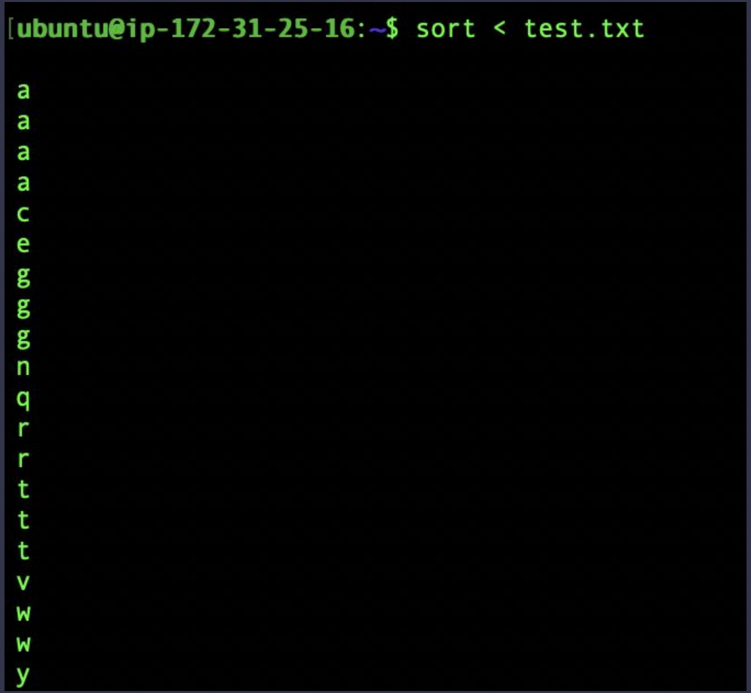


```
[ubuntu@ip-172-31-25-16:~$ !!
 cat test.txt
 THIS IS A TEST
[ubuntu@ip-172-31-25-16:~$ echo "not a test" >> test.txt
[ubuntu@ip-172-31-25-16:~$ cat test.txt
 THIS IS A TEST
 not a test
[ubuntu@ip-172-31-25-16:~$ echo "maybe it is" > test.txt
[ubuntu@ip-172-31-25-16:~$ cat test.txt
 maybe it is
```

(More) Redirections



```
[ubuntu@ip-172-31-25-16:~$ cat test.txt
e
r
t
y
a
c
w
q
g
t
a
v
n
r
a
g
t
w
a
g
```



```
[ubuntu@ip-172-31-25-16:~$ sort < test.txt

a
a
a
a
c
e
g
g
g
n
q
r
r
t
t
t
v
w
w
y
```

Directories

Directories on linux based systems start from ‘/’

- There is no concept of ‘drives’ (No C: drive like Windows)

Your user accounts home directory is located at ‘/home/<username>’

- Often shown on terminals as ‘~’

Usually your personal files go in your user directory

- On distros with a ‘Desktop Environment’, you typically have folders like ‘Download’, ‘Documents’, premade
- You can do the same on distros without desktops, just make a folder using mkdir command

File paths

/home/ubuntu - same as ~

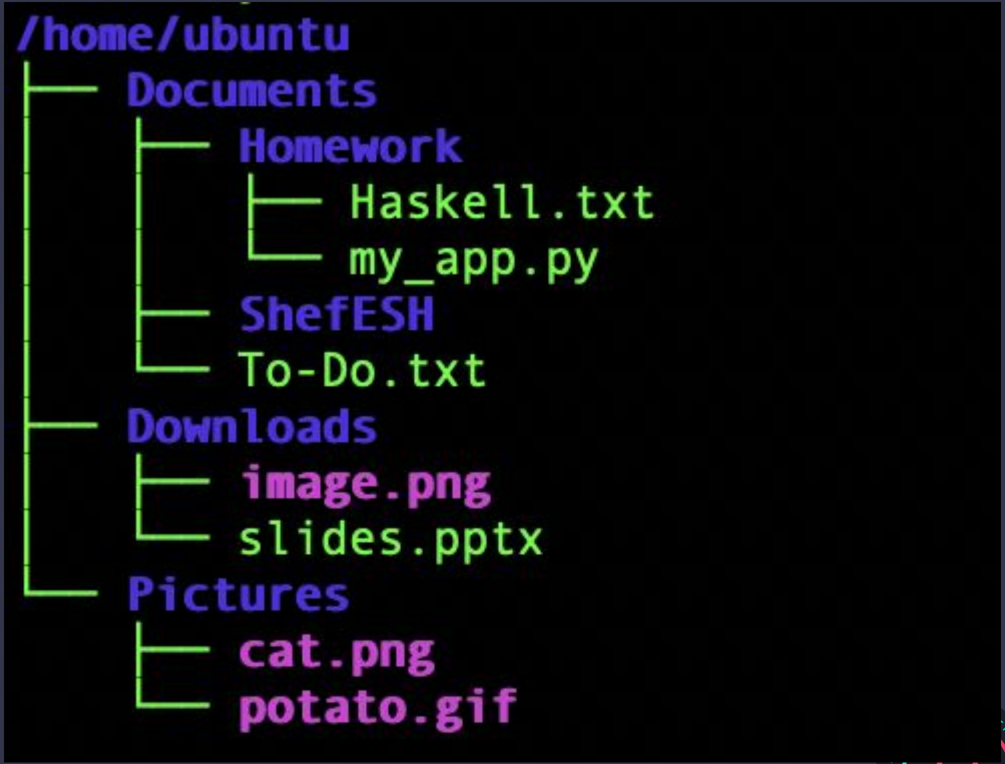
- As my user account is 'ubuntu'

To read my Haskell Homework

- cat ~/Documents/Homework/Haskell.txt

To delete my cat image

- rm ~/Pictures/cat.png



```
/home/ubuntu
├── Documents
│   ├── Homework
│   │   ├── Haskell.txt
│   │   └── my_app.py
│   ├── ShefESH
│   └── To-Do.txt
├── Downloads
│   ├── image.png
│   └── slides.pptx
└── Pictures
    ├── cat.png
    └── potato.gif
```

Default Directories

/bin	Contains essential binaires to launch the system
/boot	Stores files needed to boot the system
/dev	Device files - linux treats keyboards, mice, etc as files
/etc	System config files
/home	User directories
/lib	Shared libraries
/mnt	Temporary mount point for filesystems
/media	Mount point for removable media (USBs, CDs, etc)
/root	Home directory for superuser account
/sbin	System binaries
/temp	Temporary files - lost on reboot
/usr	User system resources - applications, binaries, etc

Permissions and Ownership

Ownership

Every file and folder has three ‘ownership’ parts

- ‘Owner’ - typically the user that created the file/folder
- ‘Group’ - the group the user belongs to
    - On larger systems / servers you would have groups for developers, database admins, etc
    - On personal systems you would likely belong to groups such as ‘sudo’
- ‘Other’ - Everyone else on the system who isn’t the owner or in the group

Permissions

There are three types of permissions for every file and folder

- Read - Do I have permission to read the contents of this file/folder
- Write - Do I have permission to write to (including renaming, moving and deleting) this file/folder
- Execute - Do I have permission to execute this file/folder

Permissions are **NOT** suitable to protect sensitive files

Changing Permissions and Ownership

chown [user][:group] [path]

- **Ch**ange **own**ership of a file or folder, to the specified user or group
- chown user1 file.txt - Change owner
- chown group1 file.txt - Change group
- chown user1:group1 file.txt - Change both owner and group

chmod [mode] [path]

- **Ch**ange file **mod**e bits
- Can be done using characters or a number code
- u = users g = group o = others “ = all
- + = grant - = remove ‘=’ = set
- r = read w = write x = execute

https://chmod-calculator.com/

Sudo

Sudo - Superuser Do

- Basically ‘run as administrator’ on Windows

Can be very dangerous

- Usually requires a password
- May leave an audit log

Temporary elevation

- Usually only for that command or the current session

Allows you to modify system files, install software

- Can easily break things
- Most of the time it won’t stop you!

grep

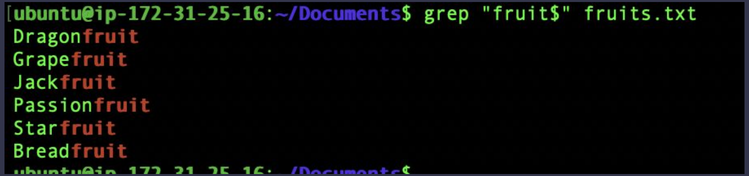
Grep is a handy command for searching for text patterns in files

- It allows us to use regex (Regular Expression) to find these patterns

> grep “pattern” file

> grep “fruit$” fruits.txt

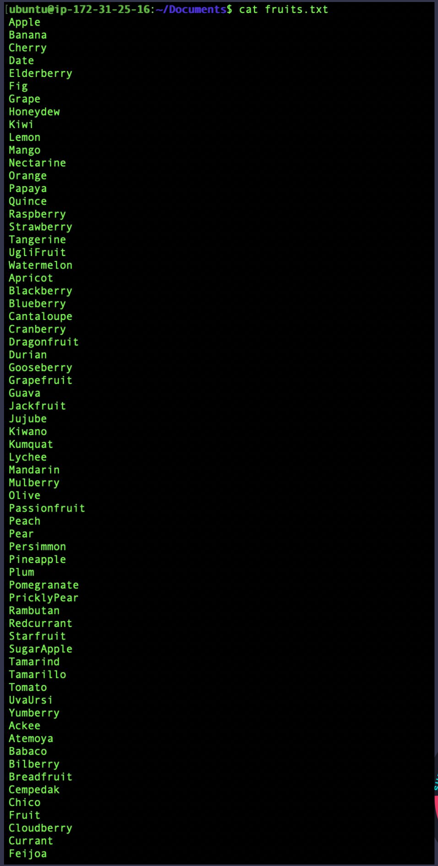
- The $ means any line that ends in “fruit”



```
[ubuntu@ip-172-31-25-16:~/Documents$ grep "fruit$" fruits.txt
Dragonfruit
Grapefruit
Jackfruit
Passionfruit
Starfruit
Breadfruit
ubuntu@ip-172-31-25-16:~/Documents$
```

https://regex101.com/

[Mozilla Regex Cheatsheet]()



```
[ubuntu@ip-172-31-25-16:~/Documents$ cat fruits.txt
Apple
Banana
Cherry
Date
Elderberry
Fig
Grape
Honeydew
Kiwi
Lemon
Mango
Nectarine
Orange
Papaya
Quince
Raspberry
Strawberry
Tangerine
UgliFruit
Watermelon
Apricot
Blackberry
Blueberry
Cantaloupe
Cranberry
Dragonfruit
Durian
Gooseberry
Grapefruit
Guava
Jackfruit
Jujube
Kiwano
Kumquat
Lychee
Mandarin
Mulberry
Olive
Passionfruit
Peach
Pear
Persimmon
Pineapple
Plum
Pomegranate
PricklyPear
Rambutan
Redcurrant
Starfruit
SugarApple
Tamarind
Tamarillo
Tomato
UvaUrsi
Yumberry
Ackee
Atemoya
Babaco
Bilberry
Breadfruit
Cempedak
Chico
Fruit
Cloudberry
Currant
Feijoa
```

Commands, Commands, Commands

uptime

- Shows how long your system has been running

ping

- Used to send a request to a webserver
- Try ‘ping google.com’

seq [start] [step] [end]

- Used to generate a sequence of numbers

man [command]

- Shows an inbuilt manual on how to use a command
- Google is probably better but if you don’t have internet it can be helpful

stat [file]

- Detailed stats about a file

find

- Searches for files or directories
- Can use regex, just like grep

top

- Bit like task manager
- Shows running processes, memory, etc

yes

- Prints a string repeatedly
- Can be piped into installers to agree ‘yes’ to any questions

Flags

Most commands accept flags

- Extra instructions
- Modify behaviour of command

Common flags

- ‘--force’ or ‘-f’ -> tries to force something
- ‘--verbose’ or ‘-v’ -> print out as much information as possible
- ‘--quiet’ or ‘-q’ -> print out as little information as possible
- ‘--recursive’ or ‘-r’ -> recursively run the command - used for copying/moving/deleting directories
- ‘-c’ -> count - can be used to either limit something or to get the count of something

Challenges

1. Make a folder - call it whatever you want
2. Rename this folder
3. Delete this folder
4. List all files in your current directory
   - Can you send the output to a text file?

5. Make a new text file
   - Write something in it and print this out to the terminal
   - Can you modify the permissions so that you can not read it anymore?

6. Can you print out your name to the terminal?
   - Can you save this to a file called <yourname>.txt

7. Can you ping ‘shefesh.com’?
   - Can you write its output to a file?
   - Make sure to pass ‘-c’ flag to limit responses

8. Find the secret folder
   - Find the secret FLAG{} inside the file in this folder
   - First one gets a sticker!

9. Make a new folder and Download the tar at shefesh.com/rp/intro_to_linux_25.tar
   - Extract it and read its contents

10. Follow the instructions from Q9

SHEFFIELD ETHICAL STUDENT HACKERS