Cyber@UC Meeting 99

// Linux Basics //

If You're New!

- Join our Slack: cyberatuc.slack.com
- **SIGN IN!** *(Slackbot will post the link in slack)*
- Feel free to get involved with one of our committees:

  Content Finance Public Affairs Outreach Recruitment Lab

Cyber@UC

Announcements / Upcoming Events

- **Smash Tournament in lab after the meeting**
- Mason High School Hack club needs help with Cyber Month
    - Tuesdays 2-5 The rest of the Month
- 9.20 NSA Codebreaker opens
- 9.21 CBTS CTF
- 9.24 Northrop Grumman Recruitment Event
    - More information to be distributed in Slack
- 9.27 PicoCTF 2019 opens
- 9.28 OSU CTF Registration Closes
- 10.11 GE Aviation SOC visit
- 10.16 NSA Visit
- Battelle Visiting us later this semester

Cyber@UC

Weekly News

Nuclear Crypto Mining

- Ukrainian nuclear power plant employees hooked up plant to internet
- Attackers might have pivoted through network
- On the admin network and not industrial network
- Ukrainian Secret Service found 11 RX 470 cards in two pc’s

https://www.zdnet.com/article/employees-connect-nuclear-plant-to-the-internet-so-they-can-mine-cryptocurrency/

Eerie Siri

- Apple hired contractors to listen to Siri conversations for “grading”
- Moving forward users have to opt into program
- Include drug deals, sex, and domestic abuse
- Amazon employees listen to 1000 audio clips a shift

https://threatpost.com/apple-updates-privacy-policies-after-siri-audio-recording-backlash/147780/

Twitter Hacks

- Twitter CEO’s account retweeted “nazi germany did nothing wrong”
- SIM swap attack
  - Bribe a cell provider to switch the SIM number
  - Intercept 2FA messages
- Tweets can be sent through text message
- Claimed by “Chuckling Squad”

https://www.wired.com/story/jack-dorsey-twitter-hacked/

Other Stories

- https://news.bitcoin.com/how-big-hydro-power-partners-with-bitcoin-miners-to-prevent-energy-waste/
- https://www.theregister.co.uk/2019/08/29/google_bounties_in_popular_apps/
- https://www.zdnet.com/article/google-launches-bounty-program-to-spot-misuses-of-google-api-chrome-and-android-user-data/

Cyber@UC

Linux

Agenda

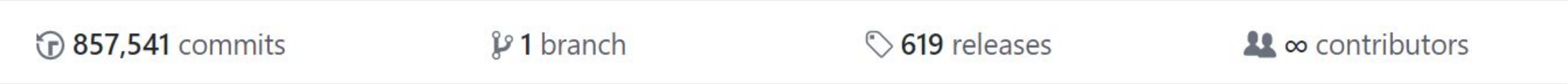
- I wasn’t here last week!
- What ~~the fuck is this shit~~ is Linux?
- Where is Linux?
- Why is ~~Gamora~~ Linux?
- Why isn’t Linux?
- Basic Terminal Commands
- File Hierarchy Standard / where is System32?
- Get help
- Installing useful software (vim) and updates
- More notes on distros

I wasn’t here last week!

- Shame on you
- Previously, we created Linux virtual machines and went over virtual machine concepts
- Google “Windows Linux Subsystem” and get going so you have Linux
    - Use the most recent Ubuntu version in the Windows store
- All of our meetings are on our YouTube channel CyberAtUC

What is Linux?

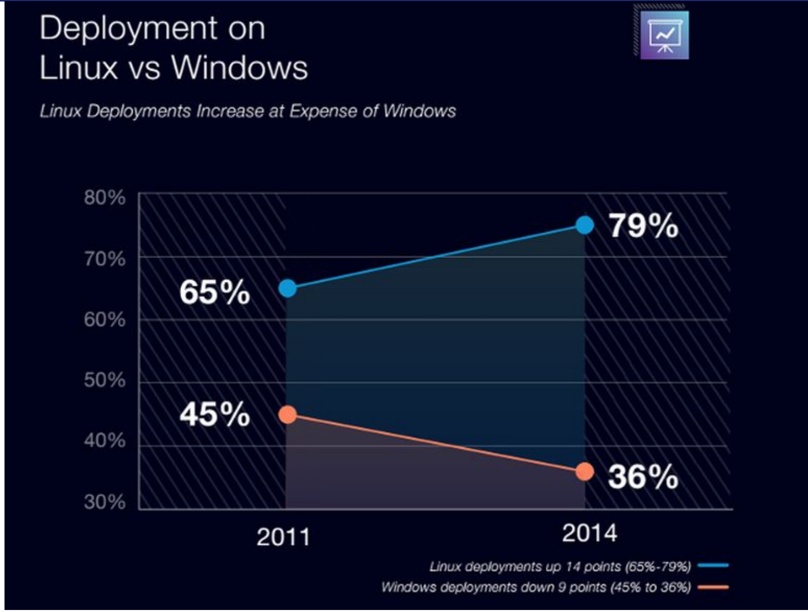
- Free/Open-Source Kernel
  - That’s the software that an OS actually uses to control the hardware
- Used to build operating systems without reinventing the **fork()**
- Doesn’t hide anything from the user by default (unlike Windows/OSX)\
- Open source clone of an old IBM system called Unix
- Mostly C with sprinkles of C++ and Assembly
- Mostly POSIX compliant
  - That means it’s way faster to move a codebase between OS versions than other systems usually are
- Originally made by one programmer in his free time (Linus Torvalds)
- You can download this shit right now (please don’t)
  - https://github.com/torvalds/linux



857,541 commits   1 branch   619 releases   ∞ contributors

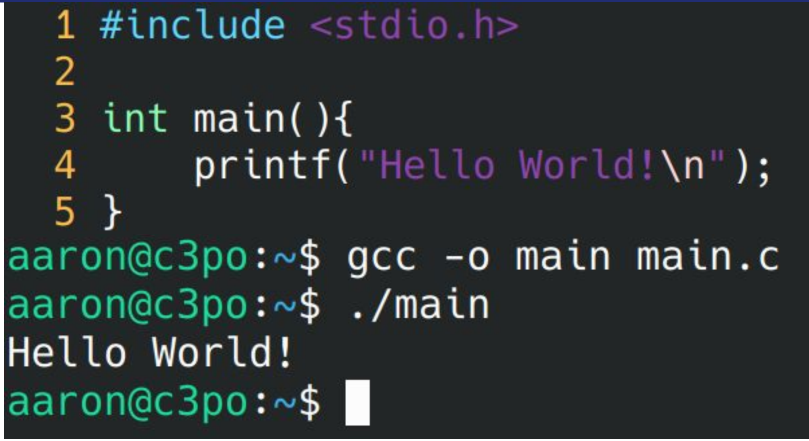
Where is Linux?

- Everywhere
- No really, it's everywhere
  - Our Lab
  - Chrome OS / Android (really just Linux with a specific set of libraries)
  - Game consoles (PS3 OtherOS)
  - Servers
  - Supercomputers
  - NASA spaceships
- There are literally companies who cannot hire enough people who know Linux systems skills because it's in such demand



Why is Linux?

- It’s free
  - Companies will bend over themselves if they can save the money in the long run per server install
  - Think about how much the 1 Million+ servers that Google would cost if it didn’t use a free OS
- It’s open source
  - Because companies are using it, they’re probably also looking for ways to improve it
  - Anyone who wants to can extend/improve it with really only a little effort
- It’s *pure*
  - Being able to instantly have most software that you would ever need immediately install and update itself in seconds by typing a few lines makes Windows update seem suspiciously slow

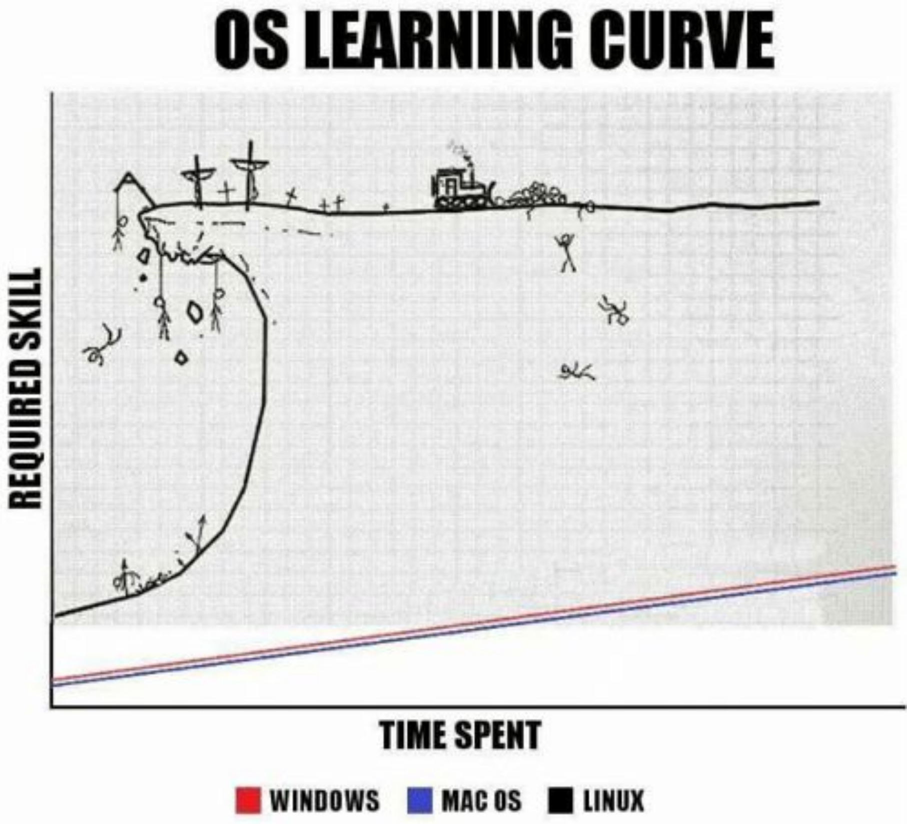


```
#include <stdio.h>

int main(){
    printf("Hello World!\n");
}
aaron@c3po:~$ gcc -o main main.c
aaron@c3po:~$ ./main
Hello World!
aaron@c3po:~$ 
```

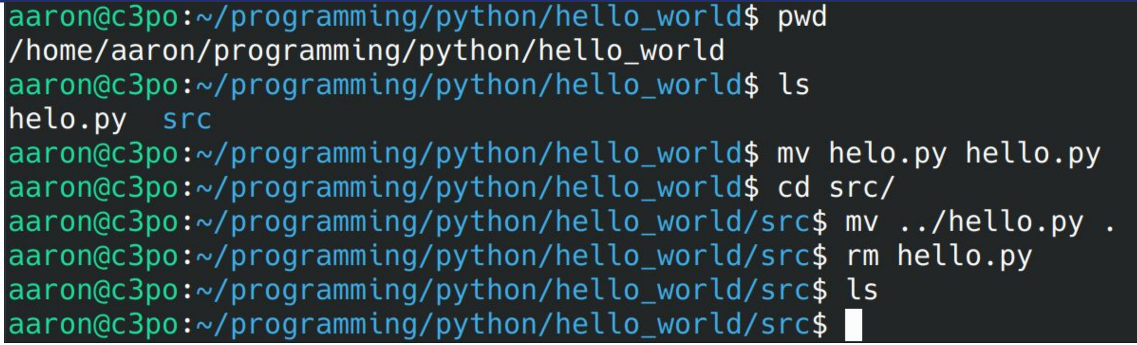
Why isn’t Linux?

- Not usually a consumer go-to unless the consumer is a highly technical person
- Requires learning how to use the command line to be effective
- High initial learning investment



Basic Navigation

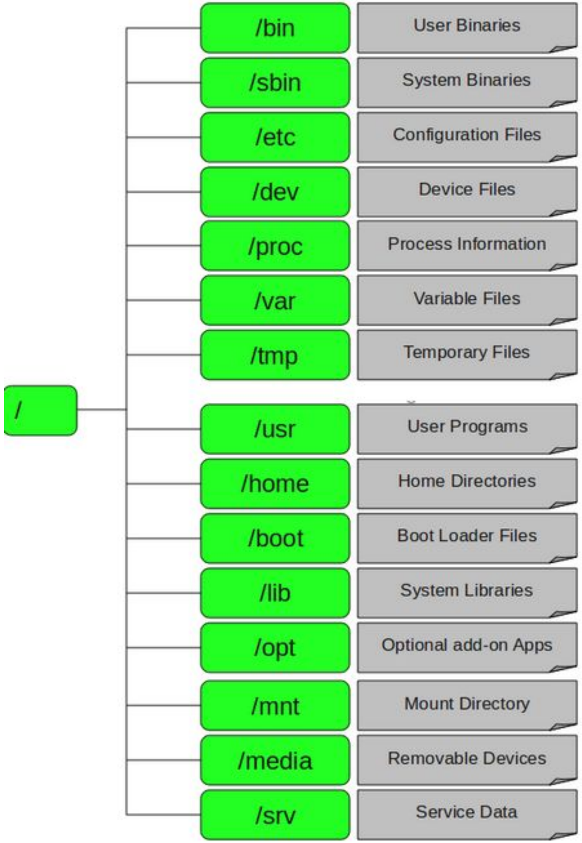
- **Open that terminal**
- Where am I?
  - pwd
- What’s here?
  - ls [directory]
- Rename files
  - mv <old_name> <new_name>
- Let’s go somewhere
  - cd <directory>
- Deleting
  - rm <file>
  - rm -r <directory>
- **! Pressing TAB usually autocompletes whatever you are trying to type !**



```
aaron@c3po:~/programming/python/hello_world$ pwd
/home/aaron/programming/python/hello_world
aaron@c3po:~/programming/python/hello_world$ ls
helo.py   src
aaron@c3po:~/programming/python/hello_world$ mv helo.py hello.py
aaron@c3po:~/programming/python/hello_world$ cd src/
aaron@c3po:~/programming/python/hello_world/src$ mv ../hello.py .
aaron@c3po:~/programming/python/hello_world/src$ rm hello.py
aaron@c3po:~/programming/python/hello_world/src$ ls
aaron@c3po:~/programming/python/hello_world/src$ 
```

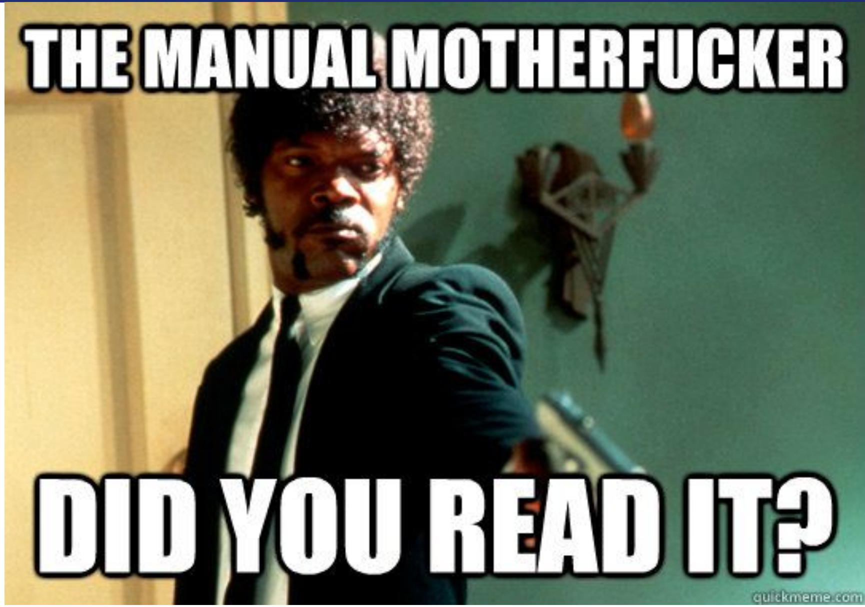
File Hierarchy Standard and more terms

- **/** - the root of the drive
- **root** - “admin” equivalent user
- Multiple Drives are put into the same hierarchy and can be viewed with **lsblk**
- Every device connected to the machine will appear as a file in **/dev/**
- **~** is usually a shortcut for **/home/<username>/** for the current user
  - Ex **cd ~** should take you home



Get help (Manual Pages)

- RTFM
- **man <program>** - the manual command, 90% of programs have a page
  - **man man**
  - 99% of the C programming language on Linux is also there
- **<program> --help**
  - For the remaining programs and for the short help message



Installing useful software and updates

- Package manager is like the app store
  - Debian = APT
  - RHEL/CentOS = yum
- Update package list
  - `apt update`
- Install updates
  - `apt upgrade`
- Search
  - `apt search <package_name>`
- More detail
  - `apt show <package_name>`
- Install
  - `apt install <package_name>`

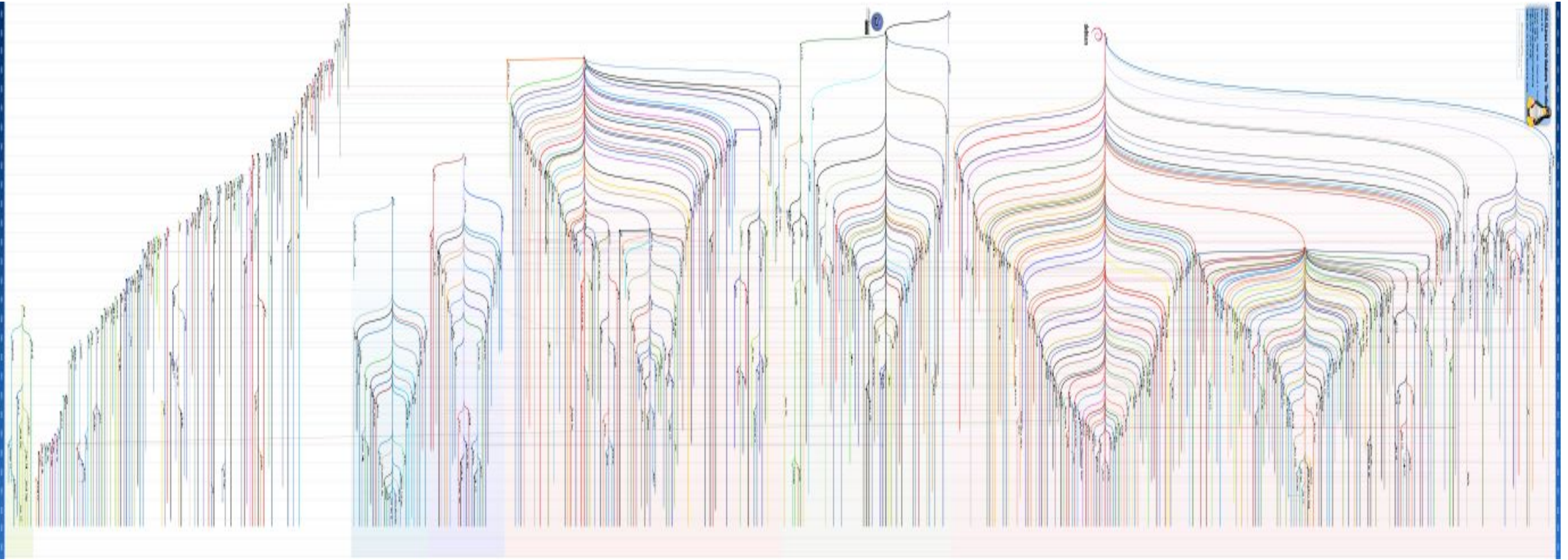
VIM

- It’s a command line text editor
- Exit = ESC + :q + ENTER
- Three main modes
  - Normal (Command)
    - Run commands
  - Insert
    - Writing text
  - Visual
    - Highlighting text
- VERY powerful text editor
- Breakup with that whimpy mouse

LIVE
BREAKING NEWS
HACKERS MANAGED TO EXIT VIM
18:44
ASKED HOW THEY DID IT, THEY SAID "IT'S BECAUSE WE ALL USE ARCH".

Linux Distributions

- There's a lot of distributions



Linux Distributions (cont.)

The Few that we care about

- Debian: a simple base OS
- Ubuntu: based on Debian, tries to be more user/beginner friendly
- Kali: also Debian based, comes with a lot of “Hacking” tools

Some More:

- Red Hat Enterprise Linux (RHEL): Super stable server distro, Fedora based
- CentOS: Stable, infrequent releases
- Arch: Less configured than other systems, helps with in-depth knowledge, fosters deep knowledge about your packages, for advanced users willing to see their stuff break all the time (Clif)