CutieHack

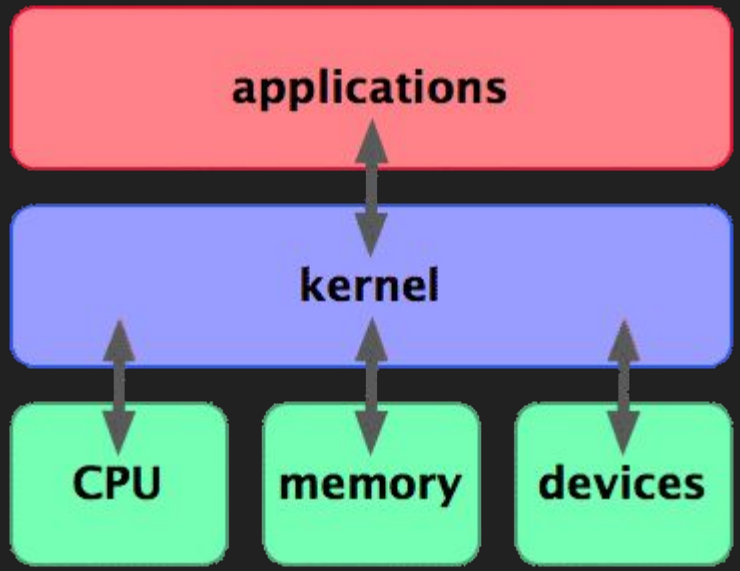
Basic Linux Workshop

What’s a linux?

Linux is a kernel, but we are lazy and don’t care too much so we refer to the whole system as a “linux” system. For this reason, when people are using “Bash” or another shell, it is often just dubbed “Linux” but this is not 100% correct. (MacOS has a terminal and its BSD based)

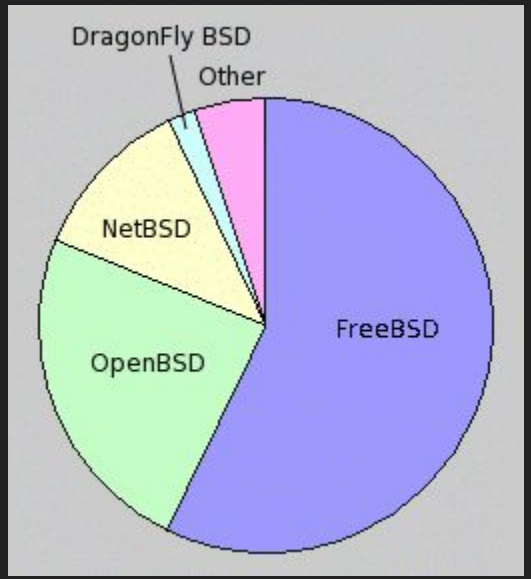
Kernel? Like popcorn?

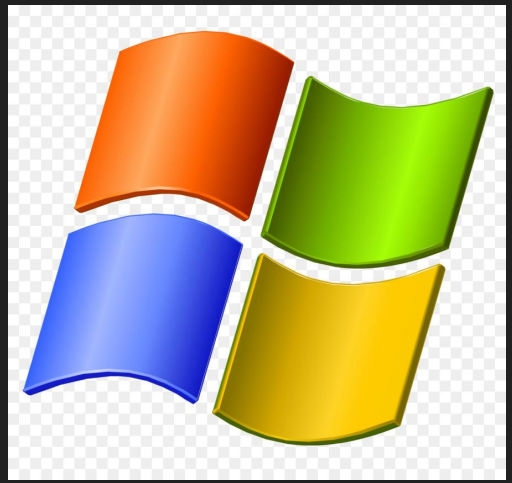
- Serves as the middleman for the OS
- Is one of the first things to boot up
- Comes in two flavors
  - Monolithic kernels, like one big stone
  - Micro kernels, think a bunch of Legos combined
  - (There are hybrids and other types …)
- There are a lot of different versions / types



3 main kernels

- Linux : developed by Linus Torvalds
- Windows : developed by Microsoft
- BSD : Berkeley-Software-Distribution
  - Yes, UC-Berkeley.





So, not the green hacker typer thing?

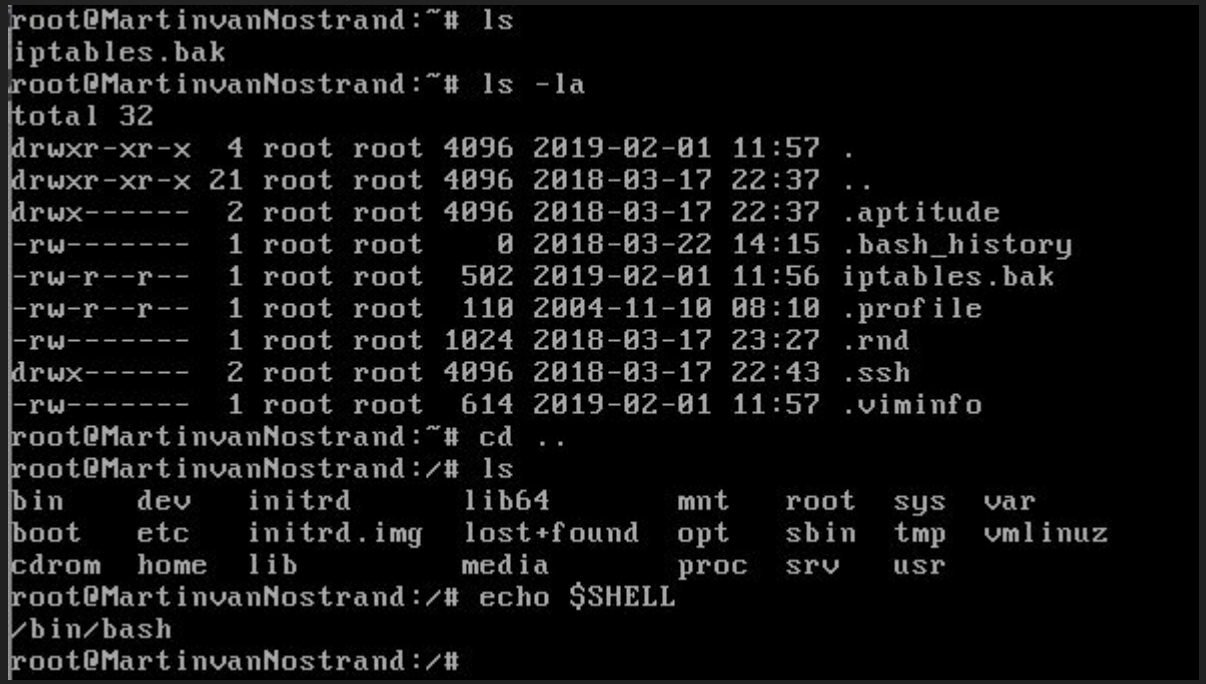
NO!
That’s not Linux (or the other ones we named).

What we will be doing then?

- We will be learning how to use the Shell! Transferable knowledge that you can use on most systems with very little modifying.
- A terminal is the window you use to interact with, the **shell** is the **interpreter** the computer uses to take in user input, **interpret** what you want, execute the proper commands, and give you the output. Repeat until exit is called.
- What you will learn, you can use on Ubuntu, CentOS, MacOS, Fedora, Arch, Windows, … basically any system that you can put Bash on.

Bash?

Bourne-Again-Shell



Basics!

Prompt

Username @ machine : dir $

Username = currently logged in as

Machine = name of the computer

Dir = current directory

$ = just denotes end of prompt, sometimes its #

(technically a difference, we don't care about that right now)

Overview

- Movement and control in the CLI
- System monitoring (featuring logs!)
- Filesystem where typical stuff goes
- How to know normal
- Audit users and groups
- Confused? Me too, so don’t forgot to RTFM when you forget!
- Also, keep track of what has been done and what has not. If you get lost or distracted go back to the list.
- Nothing wrong with not knowing, there is something wrong with not trying.

Commands used

- ls, cd, touch, file, grep, find, locate, which, whoami, pwd, cat, echo
- top, ps, lsof, netstat, systemctl, crontab, ifconfig, ping, kill, w, ss
- Man
- Lsattr, chattr (not standard on all systems), chmod, chown, chgrp (maybe)
- Su, sudo (know the difference!)
- Visudo

But who cares?

- Great way to gather or view lots of information in a quick manner.
- Through the terminal, you have lots of control over the machine through commands rather than clicking through a GUI.
- Often a lot faster than going through the GUI.
- Also you look like a l33t h4ck3r

Time for some hands on experience!

We will be back shortly for your regularly scheduled program!

Quiz time!

1. How do I change the sudoers file?
2. What is /proc for? /etc? /var? /dev? /bin? /sbin?
3. How do you kill a process?
4. How do you find out what processes are running?
5. How do you find out what services are running?
6. What is cron?
7. What is the difference between su and sudo?
8. What do you do if you don’t know / get lost / forget?

Resources!

https://ucrcyber.org

https://ucrcyber.slack.com

https://bash.cyberciti.biz/

https://overthewire.org/wargames/bandit/

Download Oracle VirtualBox + Ubuntu image

Just play around!