Cyber Defense Organization

Fall 2020 - Intro to Linux

Downloading putty

- Let’s do this now so we are ready for the hands on section!!!
- https://www.putty.org/

already been fixed in those versions.

Package files

You probably want one of these. They include versions of all the PuTTY utilities.

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

MSI (‘Windows Installer’)

32-bit:	putty-0.74-installer.msi	(or by FTP)	(signature)
64-bit:	putty-64bit-0.74-installer.msi	(or by FTP)	(signature)

Unix source archive

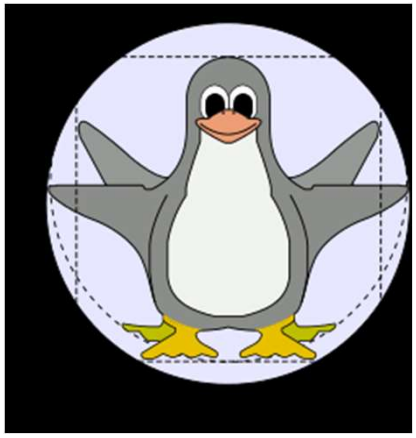
.tar.gz:	putty-0.74.tar.gz	(or by FTP)	(signature)

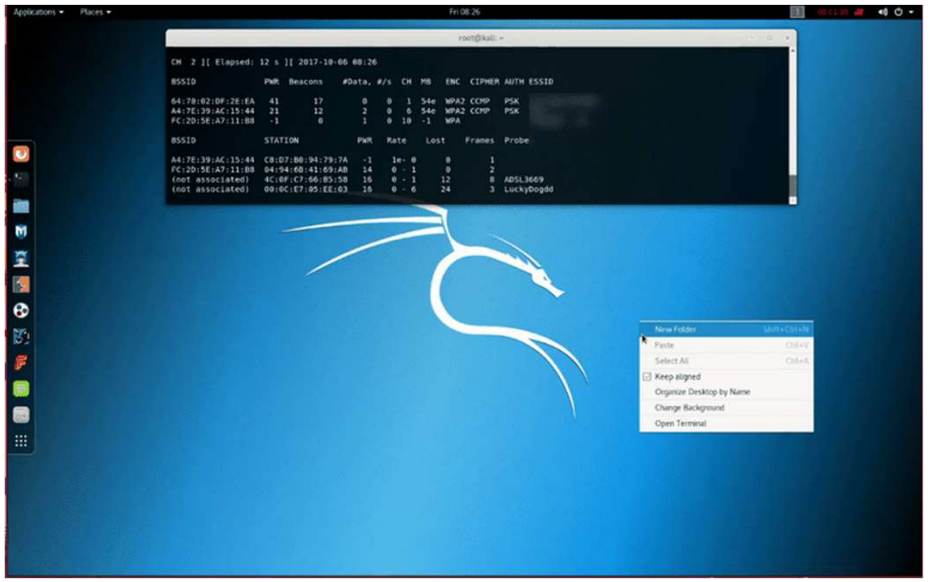
What is Linux?

- Linux is NOT an OS. Linux is a kernel.
- The difference between an OS and kernel is that a kernel interacts directly with the hardware.
- Any OS uses a kernel though.
    - Ubuntu for example is an OS.

Types of Linux?

- These are all “Linux Distributions”
  - Ubuntu
  - Kali (Used in tv show “Mr Robot”)
  - CentOS
  - Mint
  - Cucumber Linux

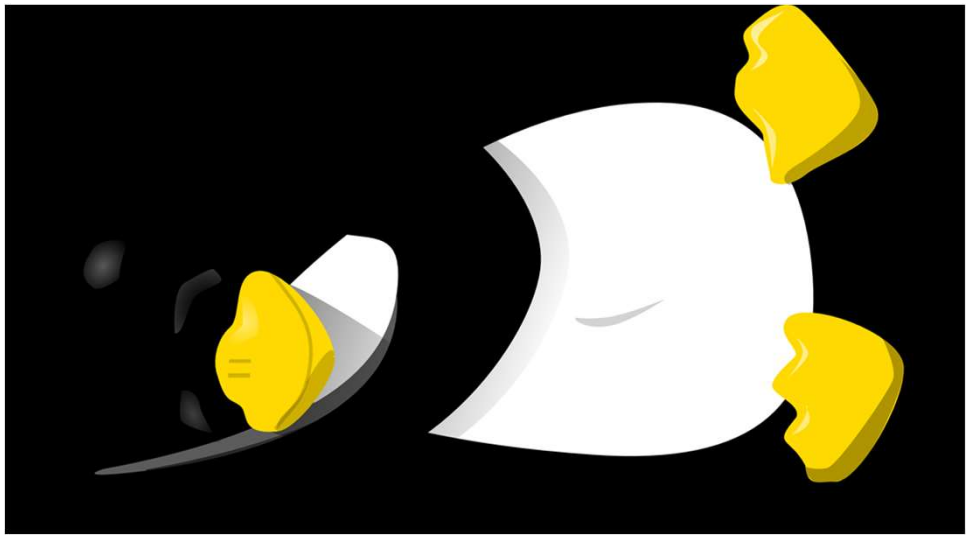




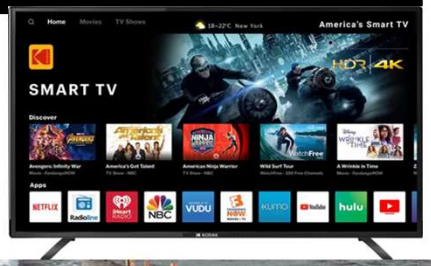
CentOS

Why Linux?

- Free
- Command line based
  - Also has GUI
- Stripped down
- You can directly modify files
- Open source
  - Many different versions of Linux supported by the community.
  - Customization!



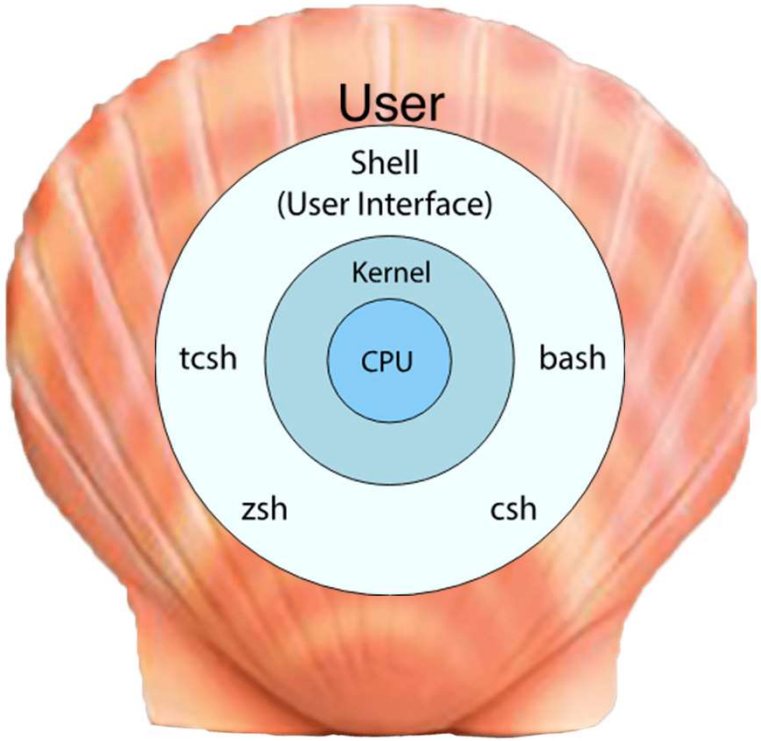
Linux is used in so many things!



The workings on Linux

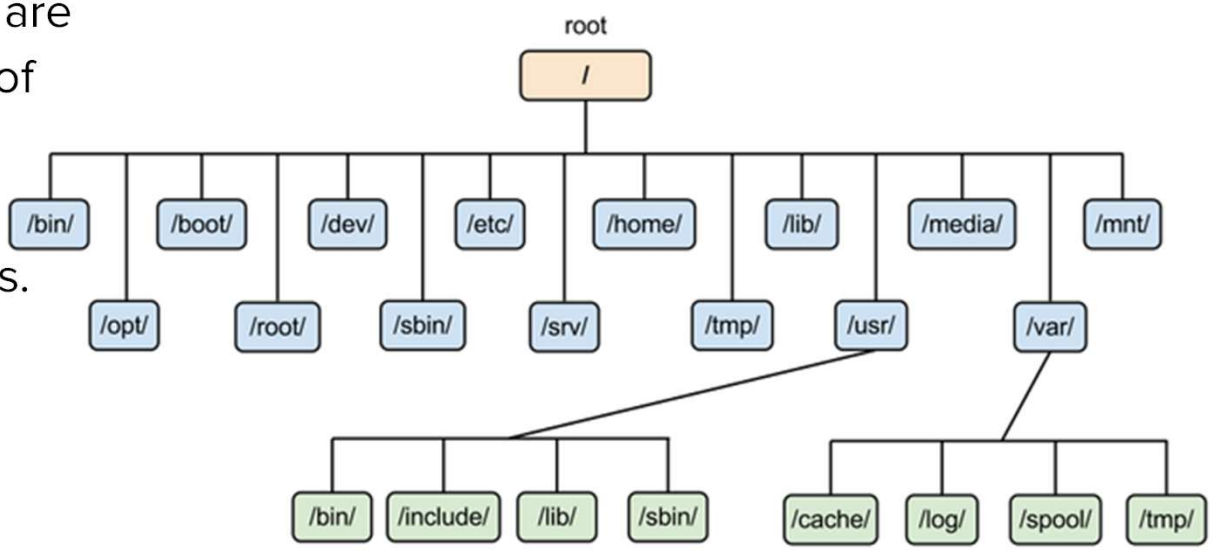
- At its core level linux is a kernel that interacts with your computer's hardware.
- Outside the kernel are the shells.
  - The shell is the user interface that communicates with the kernel.
  - Bash (Bourne-Again SHell)

Fun Fact: When the game Valorant came out people were nervous that it had kernel level permissions!



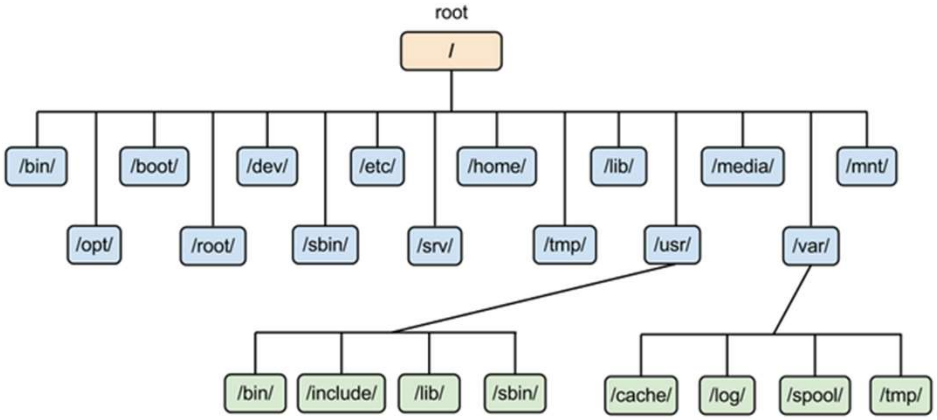
Linux File Structure

- Everything on Linux is a file!
  - That means you can edit everything!
- The file systems in linux are broken up into a bunch of directories.
  - Directories are the equivalent of folders.



Linux framework

/ - filesystem root
/bin - contains programs
/sbin - contains programs for admins
/etc - configuration files for programs
/opt - downloaded programs
/home - each user has files live there
/dev - attached devices information (usbs)
/var - variable files(LOGS!)
/tmp - temporary files
. - current directory
.. - go up one directory
- - go back



Moving around

We use commands to navigate the OS!

pwd - (print working directory) This shows you where you are in the file system

ls - show all the files in the current folder (HINT -a to show hidden files)

Cd <directory name> - Changes the directory (example cd /home moves you to the home directory)

Cat <file name> - shows you the contents of the file

File <filename> - shows you about the file and its type


```
ubuntu@ubuntu:~$ pwd
/home/ubuntu
ubuntu@ubuntu:~$ cd /etc
ubuntu@ubuntu:/etc$ cd calendar
ubuntu@ubuntu:/etc/calendar$ pwd
/etc/calendar
ubuntu@ubuntu:/etc/calendar$ ls
default
ubuntu@ubuntu:/etc/calendar$ file default
default: C source, ASCII text
ubuntu@ubuntu:/etc/calendar$ cat default
/* This is the system-wide default calendar file, used if calendar(1)
 * is invoked by a user without a ~/calendar or ~/.calendar/calendar file.
 * It may be edited or even deleted to reflect local policy.
 *
 * In the standard setup, we simply include the default calendar
 * definitions from /usr/share/calendar/calendar.all.  If you want
 * only some of those definitions, copy calendar.all to /etc/calendar
 * and edit it there.  That way, your changes will be kept next time
 * you upgrade.
 *
 * The search path for include files is:
 *   /etc/calendar
 *   /usr/share/calendar
 */
#include "calendar.all"
ubuntu@ubuntu:/etc/calendar$
```

Manipulating files

Touch <name> - creates a file of designated name in current directory

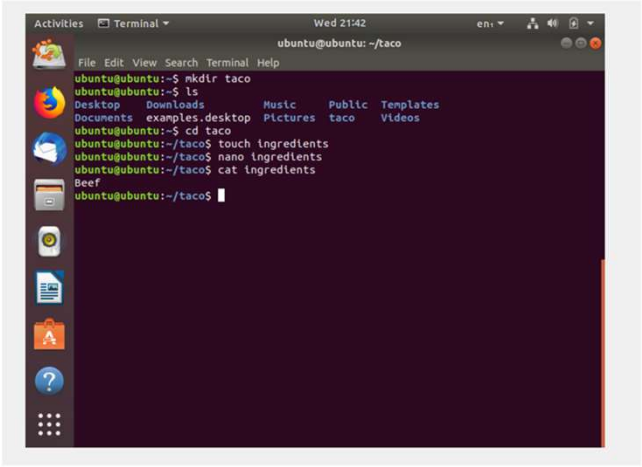
Rm <name> - removes a file of that name in the current directory

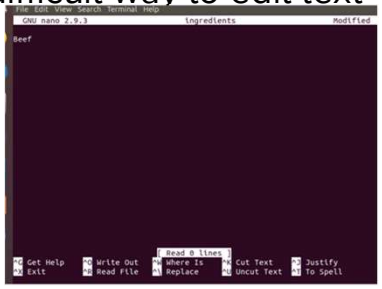
Mkdir <name> - create a directory with that name

Rmdir <name> - remove the directory with that name.

Nano <file name> - edit the text inside of a file

Vi <file name> - the more difficult way to edit text





Users and groups!

- Linux uses users and groups to manage access
- Each user gets an identification called a UID
- Each group gets a GID
- Use the id command to see the UID and GID
- Id <user or group>
- User and Group Files!!!
  - /etc/passwd
  - /etc/group


```
ubuntu@ubuntu:~$ id mail
uid=8(mail) gid=8(mail) groups=8(mail)
```

Modifying users and groups!

useradd <username> - add new user

deluser <username>- delete user

groupadd <groupname>- create new group

groupdel <groupname>- delete group

usermod -aG <groupname> <username> - Add user to group.

whoami - show logged in

who - who else is logged in

```
ubuntu@ubuntu:/$ sudo useradd joe
ubuntu@ubuntu:/$ sudo groupadd joe_group
ubuntu@ubuntu:/$ sudo usermod -aG joe_group joe
ubuntu@ubuntu:/$ id joe
uid=1000(joe) gid=1000(joe) groups=1000(joe),1001(joe_group)
ubuntu@ubuntu:/$
```

Ease of use commands

<ctrl-c> : kill current process

<ctrl-z>: put current process in background

<tab>: complete the command

!!: re-run recent command

jobs : view background processes

history - view recent commands

clear or <ctrl-L) - clear the screen

Curious about a command?

Just use the man command!

This gives you a manual of what that command is and does!!!

Who doesn't like free knowledge! (Jon Matza doesn't)

Linux Resources!

1. Linux Handbook! (Major work in progress, but has such good content)
    a. https://tinyurl.com/cdo-linux-handbook
2. Linux Resources!
    a. https://tinyurl.com/cdo-linux-folders
3. Linux Books!
    a. Reach out to Max Kirby (mkirby@albany.edu) for access to CDO Linux Books!

Coming up this week!

Monday 9/14 @ 7:00 pm: Blue Team Practice - **Discord**

Tuesday 9/15 @ 5:00 pm: Security + Cert Study - **Discord**

Thursday 9/17 @ 7:20 pm: Red Team Practice - **Discord & Twitch**

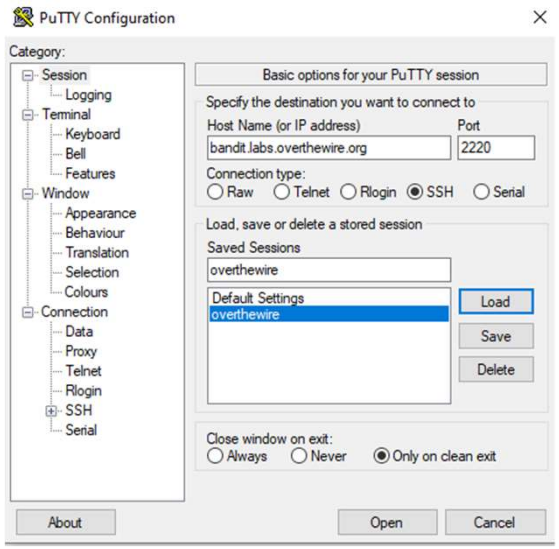
Friday 9/18 @ 3:30 pm: Into to Windows - **Discord & Twitch**

Next Time: Intro To Windows with Collin

Hands On!!

GO TO: https://overthewire.org/wargames/

OPEN PUTTY:



Username and password for level 0 is bandit0

As stated on site look for the first password in a file called readme.

Use that password in a new putty session with the username bandit1

And so on!!

Add us on Social Media!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Myinvolvement: **Cyber Defense Org**

Twitch: UACyberDef

We have a discord!

(discord is for UAlbany Students & Alumni only)