Cyber Defense Organization

Spring 19’ - Intro to Linux

Sign in?

Spring 19’ - Intro to Linux

Hacking on our Campus?!

UNIVERSITY AT ALBANY
State University of New York

INFORMATION SECURITY ALERT

Dear Students,

Here is some additional information about the incident that occurred this morning. The campus experienced a distributed denial of service attack that is designed to make on-line resources unavailable by flooding them with a high volume of network traffic. The confidentiality of campus information systems was not impacted by this event.

In response to this activity, we have made some changes to our firewall rules that are designed to protect the targeted resources (e.g., Blackboard) from these types of attacks.

Anthony Capece

Junior

From upstate NY

Linux Coach

Competition i've been to...

- A lot

Max Kirby

Freshman

From Long Island

Linux Specialty

Competitions that I've been too...

- Cny Hackathon
- UBNet Def
- CCDC Qualifiers

Daunte Kinsey

Freshman, Digital Forensics Major

Linux Specialty

Competitions that I've been too...

- Cny Hackathon
- UBNet Def
- CCDC Qualifiers

Small “Term” of the Week:

Blue Team - The team in a cyber security competition that is given a network to defend. (You!)

Red Team - The team in a cyber security competition that is tasked with attacking the blue team’s networks. (Boo!)

White Team - The people that will help you along the way during the competition. They do not compete.

Black Team - Helped create the infrastructure for the competition and are tasked with making sure everything is running correctly.

Introduction to Linux

Introduce you to the fundamentals of Linux

Familiarize you with history of Linux

Groundwork for future workshops/competitions

What is Linux?

Linux is an NOT an operating system. It’s a kernel! Operating systems are based of linux.

There are many different operating systems based of original Linux:

- Ubuntu
- Kali (Used in tv show “Mr Robot”)
- CentOS
- Fedora

What makes Linux Awesome?

It’s free.

Command-line format. (Which makes you feel like a real hacker)

More secure.

Stripped down.

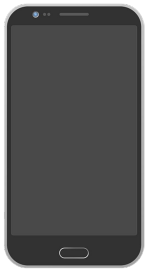
Direct modification of Configuration Files.

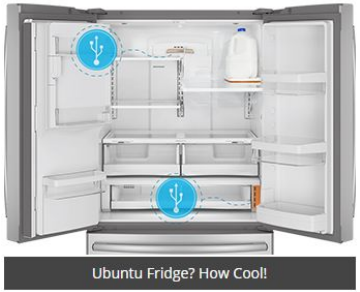
Can run all services.

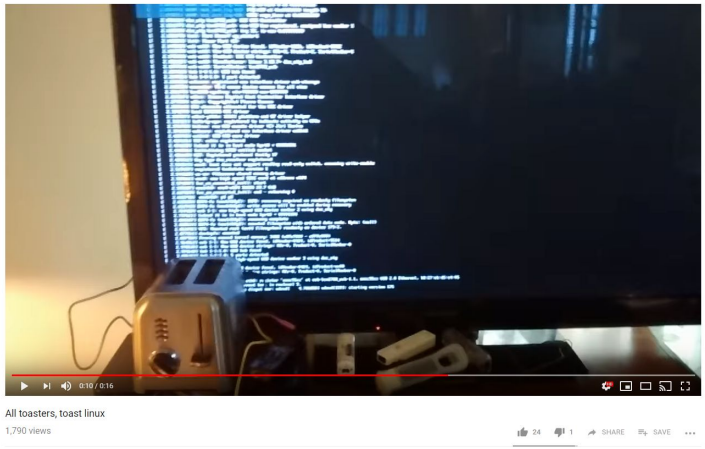
What makes Linux Awesome pt. 2?

Linux can become a portable operating system and is used in many devices.

POSIX (Portable Software)

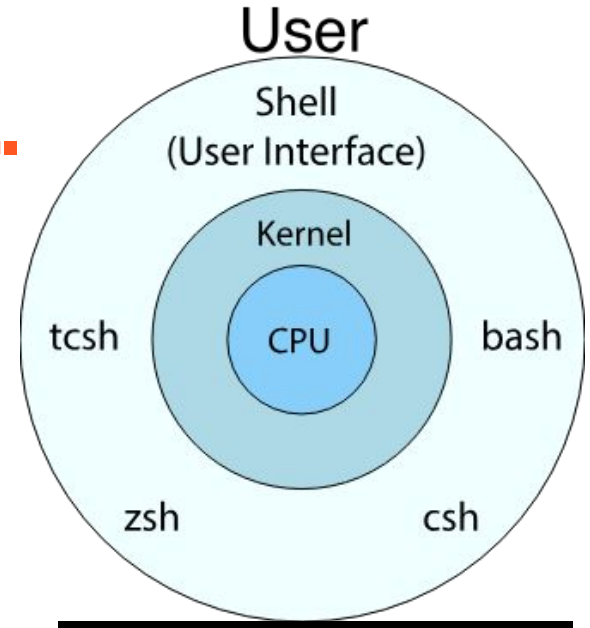


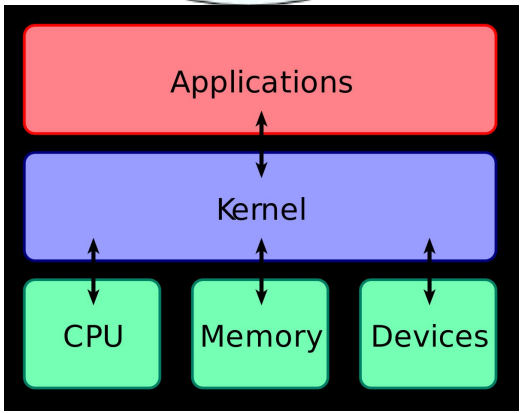




The Nuts and Bolts of Linux.

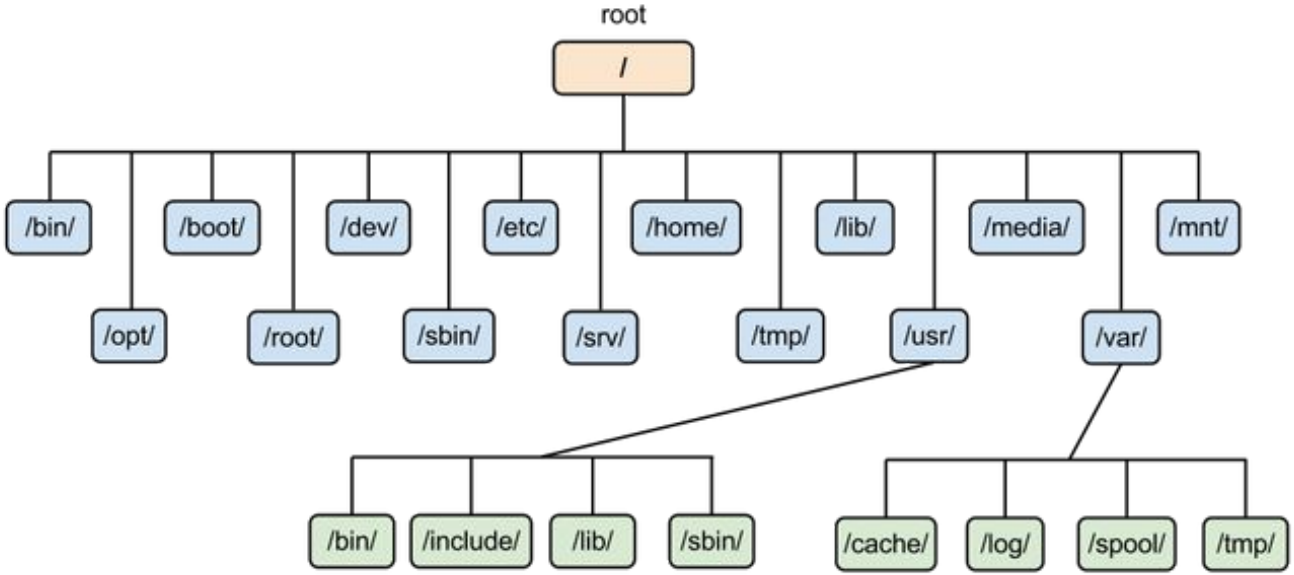
- At its core level linux is a kernel that interacts with your computer's hardware.
  - A kernel is the programming of the core operating system.
- Outside the kernel are the shells.
  - The shell is the user interface that communicates with the kernel.





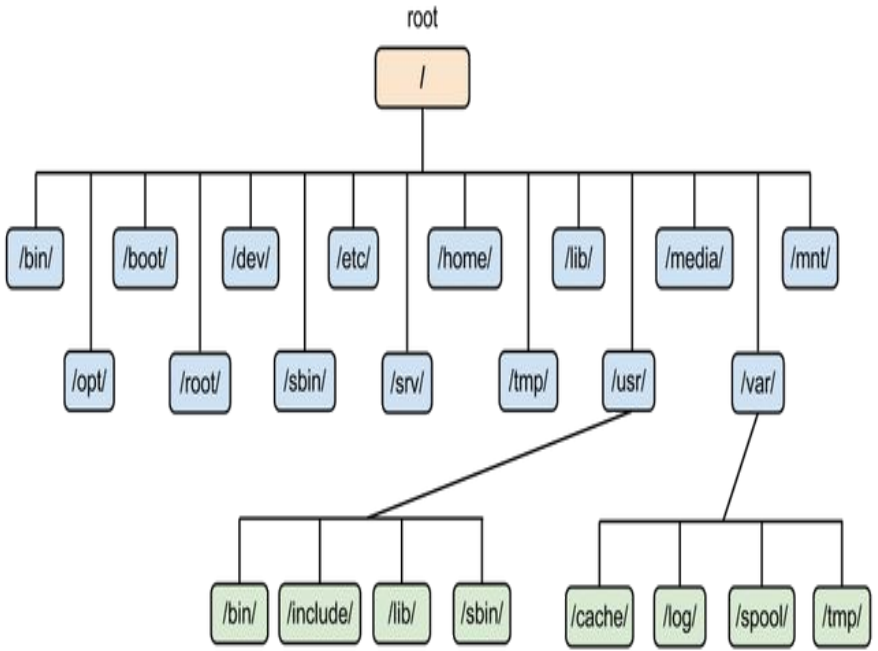
Linux's Hierarchy

- The file systems in linux are broken up into a bunch of directories.
  - Directories are the equivalent of folders.
- For example, /home is a directory in the Linux file system.



Linux's Hierarchy pt. 2

/ - 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 Linux

Since Linux is in command-line format, we use commands to navigate our file system.

pwd - Print working directory, shows where you currently are in the system i.e the working directory

cd <directoryname> - Change directory you are in
    cd /home : Moves you to the “home” directory

ls - list all the files in the current folder
    -a : list all files (including hidden)

Cat <filename> - Used for printing contents of file

File <filename> - Will tell you what the file type is.

Start em up!

- Log into machine
- Password - bb123#123
- The objective is to navigate to the calendar directory, which is in the etc directory.
    - Open terminal
    - Use the pwd command to see your working directory.
    - Then, use the cd command to navigate to the /etc directory.
    - Use pwd to print out file path.
    - Then cd into the /calendar directory
    - Use pwd again to print out the full file path.
    - Once in the calendar directory, use ls to display the contents of the directory.
    - Then, use file to see what type of file default is.
    - Use **cat** to print out contents of file default.

This is what you should see...

```
kirby@kirby-VirtualBox:~$ pwd
/home/kirby
kirby@kirby-VirtualBox:~$ cd /etc
kirby@kirby-VirtualBox:/etc$ pwd
/etc
kirby@kirby-VirtualBox:/etc$ cd calendar
kirby@kirby-VirtualBox:/etc/calendar$ pwd
/etc/calendar
kirby@kirby-VirtualBox:/etc/calendar$ ls
default
kirby@kirby-VirtualBox:/etc/calendar$ file default
default: C source, ASCII text
kirby@kirby-VirtualBox:/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"
kirby@kirby-VirtualBox:/etc/calendar$
```

Manipulating your System.

touch <filename> - This command is used to create a file in whatever directory you are in.

rm <filename>- This command is used to remove or delete a file

mkdir <directoryname> - Used to create a directory

rmdir <directoryname>- Used to remove the specified directory.

nano <filename>- This is a text editor. Text editors are used to edit the contents of a file.

vi <file- Another text editor. (The inferior one).

Give it a Try!

Now that we have gone over how to directly create things in your system, let's test it out.

- Go back to your home directory by just typing **cd**.
- First create a directory with the **mkdir** command. You can name it whatever you want.
  - Use **ls** to see if it worked
- Next, **cd** into that directory.
- Then create a file using the **touch** command. Again, name it anything.
- Edit the file using **nano**. Type "Linux is cool." in the file.
  - Use the commands listed on the bottom of **nano** to save and exit. (Ctrl + X >
- Lastly, burn it all down. Delete the file with the **rm** command, then delete the directory with the **rmdir** command.
  - You can't delete a directory from within, so make sure you **cd** somewhere else first.

It should look like this...

```
cdo@cdo-VirtualBox:~$ mkdir test
cdo@cdo-VirtualBox:~$ ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  test  Videos
cdo@cdo-VirtualBox:~$ cd test
cdo@cdo-VirtualBox:~/test$ touch test
cdo@cdo-VirtualBox:~/test$
```

```
 GNU nano 2.9.3                          test                          Modified

Linux is cool!
```

```
cdo@cdo-VirtualBox:~/test$ rm test
cdo@cdo-VirtualBox:~/test$ cd
cdo@cdo-VirtualBox:~$ rmdir test
cdo@cdo-VirtualBox:~$ ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  Videos
cdo@cdo-VirtualBox:~$
```

Users and Groups

Linux also has users and groups to help manage its system.

Users are given an identification number called a UID.

Groups are given an identification number called a GID.

id <user or group> - command used to show the id of a specified user or group.

Commands for User/Group Management.

As we know, commands are used to do things in linux. So, these commands are used to manage users and groups.

useradd <username> - add new user

deluser <username>- delete user

groupadd <groupname>- create new group

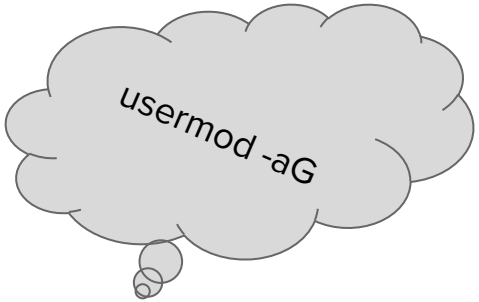
groupdel <groupname>- delete group

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

whoami - show logged in

who - who else is logged in

Your turn!



Let's give it a try.

- Create a user with the useradd command. Call them “bob”.
- Then, create a group with groupadd. Call the group “bob_group”
- Next, add bob to bob_group with the usermod -aG command.
- To check if it worked type “id bob”.
- Now let's break it with groupdel and userdel.

Ask questions if you’re having problems.

Take a look...

```
root@cdo-VirtualBox:~# useradd bob
root@cdo-VirtualBox:~# groupadd bob_group
root@cdo-VirtualBox:~# usermod -aG bob_group bob
root@cdo-VirtualBox:~# id bob
uid=1001(bob) gid=1001(bob) groups=1001(bob),1002(bob_group)
root@cdo-VirtualBox:~# userdel bob
root@cdo-VirtualBox:~# groupdel bob_group
root@cdo-VirtualBox:~#
```

Questions so far?

How to manage everything?

<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

Wondering what a Command Does?

The manual pages are built in to your Linux operating system to help you find out the usage of commands.

man - User manual for Linux distributions

man {option}

man find

If you keep getting an error on the command you are typing, always check the manual to see if you are doing it correctly!

Services

Linux can run a bunch of services. Each do their own thing and have different purposes.

Examples:

Mail Servers: Postfix,Dovecot

Web Servers: Apache/Apache2, nginx

Databases: MYSQL, MariaDB

And more!

Linux Resources

Over the wire - Practice Linux Navigation through SSH.
http://overthewire.org/wargames/

Linux Academy - Practice for CTF, Certifications, Hands-on Labs
https://linuxacademy.com/

Next time with Linux...

Something Cool :)

Announcements

Working on an interesting project? Have a specialty? Present

If you are interested in a topic/want to present email us!
Cyberdefenseorg@albany.edu

OTHER STUFF?

Join a Competition Team!

Monday nights at 7:15 in bb123.

Open training for competitions. Find out what specialty you're interested in.

Linux, Windows, Firewall. They're all super fun and interesting!

Multiple competitions! Cny, UBNet Def, CCDC, RIT Sec.

Certification Study Group - Security +

Tuesday nights at 7:15 in bb123.

Study as a group

Talk to Mark

J-Board Applications!

OPEN POSITIONS:

Treasurer
IT-Chief Technology Officer
Competition Captain
Competition Co-Captain

EVERYONE SHOULD APPLY (:

Other Updates!

CEHC Drone Lab Launch; Wednesday, February 27

Page Hall, basement Downtown Campus, University at Albany

3 pm Pre-fly event, student demos

4:15 Open house

4:45 Official ribbon cutting

Cya Next week!

If you have any good memes send them to the email below.

wcsmith@albany.edu

Follow us on Twitter? Add on myInvolvement?

PC Assembly Workshop- February 19th(?)

CCDC! - Monday 7:30

BB123 (Check email).

MyInvolve

Twitter

Discord

https://discord.gg/9Dh6R5R

Sal didn't clear his command history showing red team where all his backup files were, and that makes him tonight's biggest loser!