Cyber Defense Organization

Fall 2018 - Intro to Linux

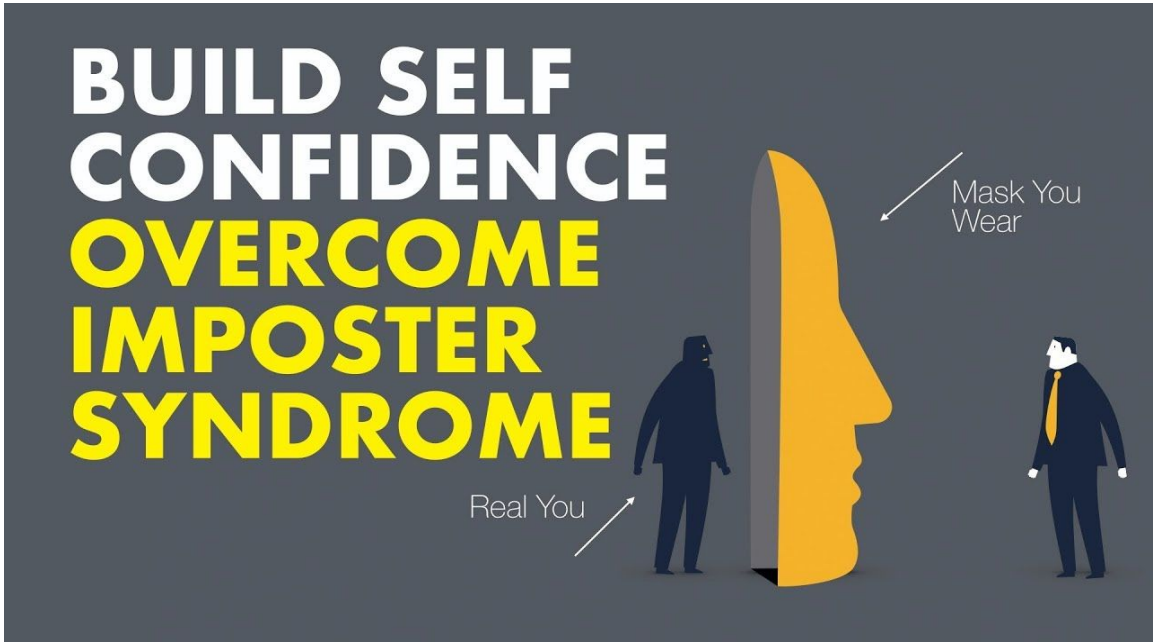
PSA aka NEWS

~~Change facebook password~~ Delete Facebook (Use the UAlbany reddit).

https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

Small Term of the Week: Imposter Syndrome

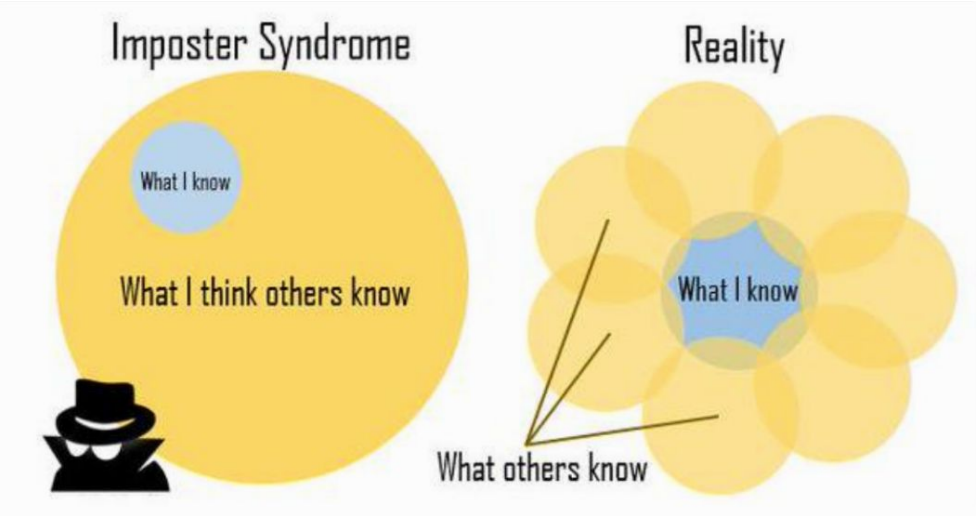
Psychological pattern where an individual doubts their accomplishments, and has a persistent internalized fear of being exposed as fraud.



What is Imposter Syndrome?

Psychological pattern where an individual doubts their accomplishments, and has a persistent internalized fear of being exposed as fraud.

Coined in 1978, is described as a feeling of “phoniness in people who believe that they are not intelligent, **capable** or creative despite evidence of high achievement.” Basically, when you feel **inadequate** despite **evident** success.



Symptoms

Those who believe themselves to be impostors often attribute their accomplishments to luck. They may think, "I was in the right place at the right time" or "That was a fluke."

People with Impostor Syndrome think they're nothing special. Whatever they've achieved, others can too. They'll think to themselves, "Oh, that was nothing. I'm sure my teammate could have done the same thing" or "I don't offer anything special to the company that no one else could."

They may think, "This was really a team project. It wasn't all me" or "Since I didn't do this completely by myself, it doesn't really count as a success."

Use a lot of minimizing language because they don't feel fully confident, like **"I'm pretty sure" or "I kind of think"**

About me

$ Anthony Capece III

$ Junior@DigitalForensics

$ Vice-President@CyberDefenseOrganization

$ Interested in “*Ethical*” Hacking, Linux Security, Networking Security

Introduction to Linux

Introduce you to the fundamentals of Linux

Familiarize you with history of Linux

Groundwork for future workshops/competitions

About Linux

Linux is a Kernel

Operating Systems based off Linux Kernel

a. Ubuntu
b. Kali
c. CentOS
d. Fedora

Why linux

Free and Open Source Software

Command Line Orientated

More Secure (REPOS) (apt, yum etc.)

Stripped Down

Run anything (Services)

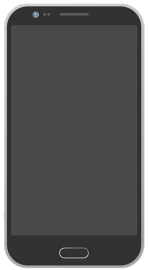

Windows

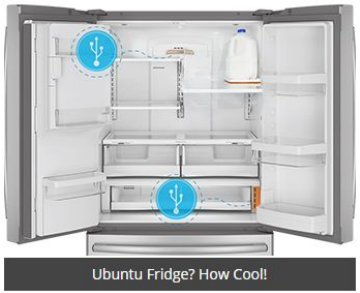

Mac


Linux

Why linux pt 2

POSIX (Portable Software)



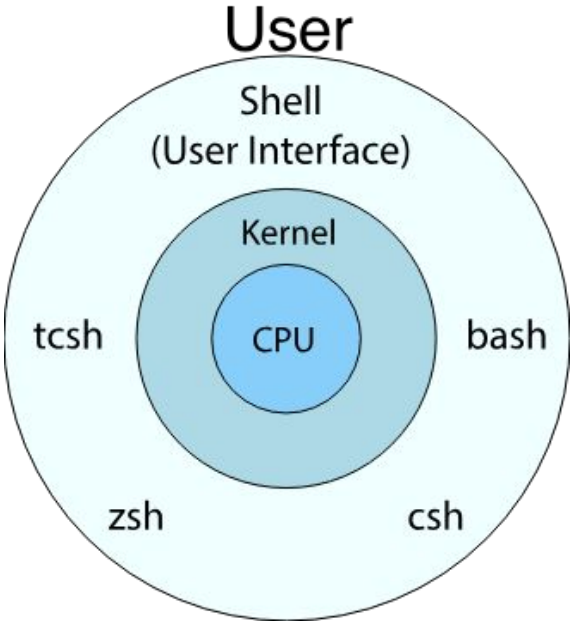


Shells

How you talk to the computer

Different versions

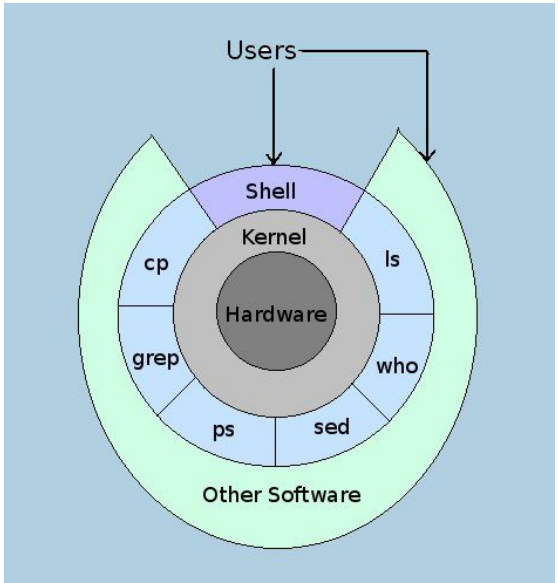
bash, zsh



Prompt:
username@hostname:current/directory$

Shells pt2

Next Time: SSH



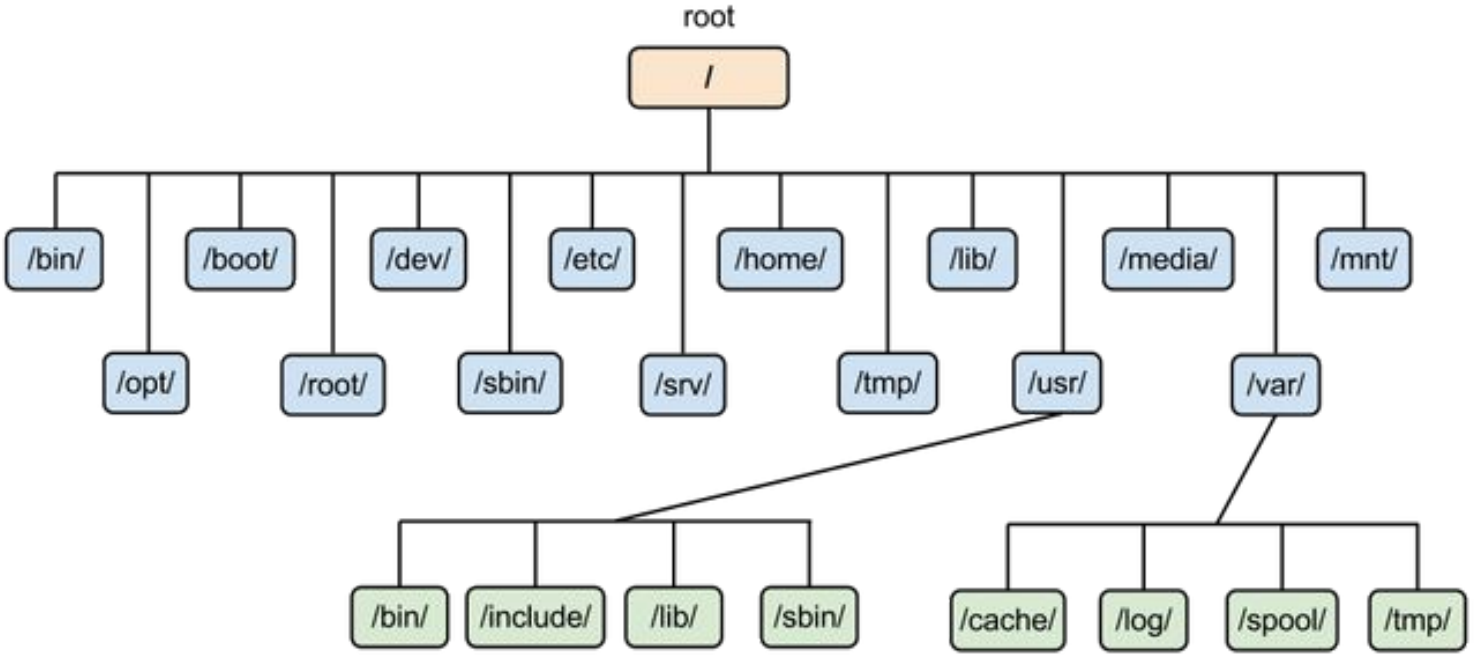
Start em up

Open VirtualBox

Start the Ubuntu Machines

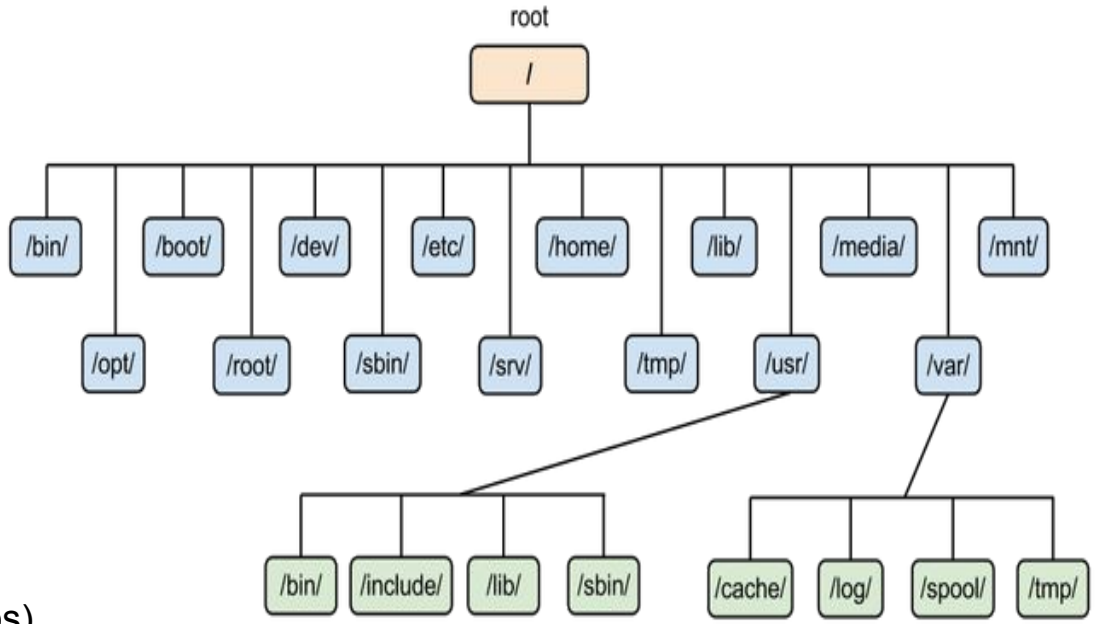
Password: bb123#123

The Hierarchy



The Hierarchy

/ - 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



Getting around

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

ls - list all the files in the current folder
-l : long-listing or more details
-a : list all files (including hidden)

cat - concatenate two files (usually used for printing contents of file)

cd - change directory you are in
cd ..
cd -

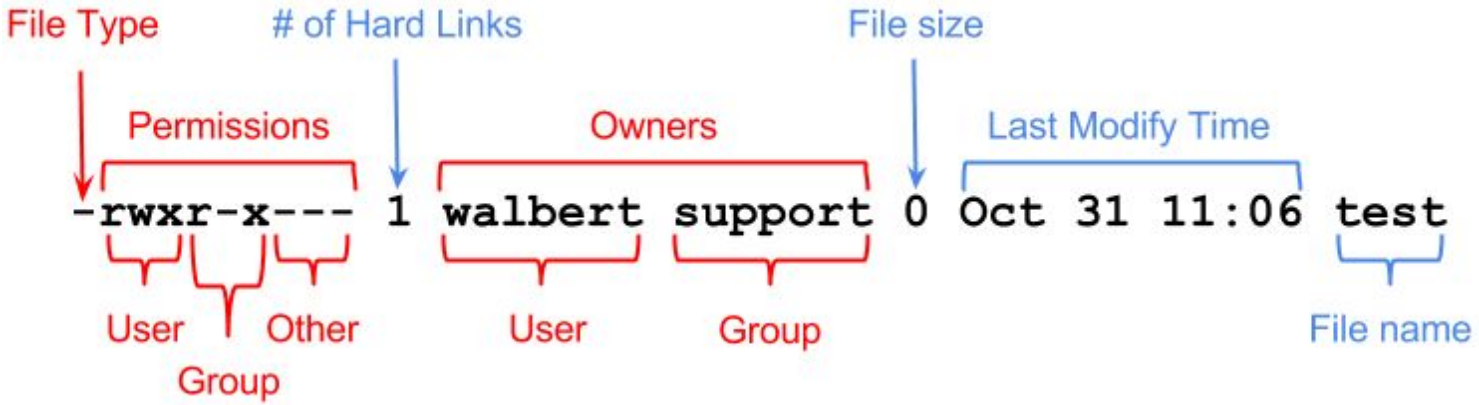
The Users and Groups

Users on linux denoted in /etc/passwd

Every user has a User Identification Number (UID)

Every group has a Group Identification Number (GID)

Permissions



000
421

File Permissions Cont.

Octal	Decimal	Permission	Representation
000	0 (0+0+0)	No Permission	---
001	1 (0+0+1)	Execute	--x
010	2 (0+2+0)	Write	-w-
011	3 (0+2+1)	Write + Execute	-wx
100	4 (4+0+0)	Read	r--
101	5 (4+0+1)	Read + Execute	r-x
110	6 (4+2+0)	Read + Write	rw-
111	7 (4+2+1)	Read + Write + Execute	rwx

Permissions

ROOT - the user name or account that by default has access to all commands and files on a Linux

aka. *root account*, *root user* and the *superuser*.

sudo - Allow for non-privileged users to execute commands with root privileges.

Who can use sudo, /etc/sudoers

File management

chmod - change file permissions; octal or rwx

chown - change owner / group of files

User Management

useradd - add new user
    useradd {username}

deluser - delete user
    deluser {username}

groupadd - create new group
    groupadd {group}

groupdel - delete group
    groupdel {group}
whoami - show logged in
who - who else is logged in

Creating and Destroying

echo - write standard input to output

touch - Allows you to make an empty file.

- touch file

mkdir - Creates (makes) a directory or folder.

- mkdir memes

rm (rmdir) - remove files / directories

QUESTIONS?

How the heck do you manage all that?

<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 - clear the screen

Où est?

find - finding files

grep - search files / folders

which - find binaries

Find

find - used to find files
    find {location} {options}

man {command}

Examples:
    -type f,l,d,c,b
    -user {username} - find all files owned by {username}
    -group {group} - find all files owned by {group}
    -perm ### : find all files with ### permissions

find a file on the ROOT directory named “flag.txt”
HINT: sudo

find a directory on the ROOT directory “flag_challenge”

grep

grep - used for advanced text/file/folder filtering

grep {options} {pattern} {file}

grep -i “string” file.txt

Examples:

-i {case insensitive}

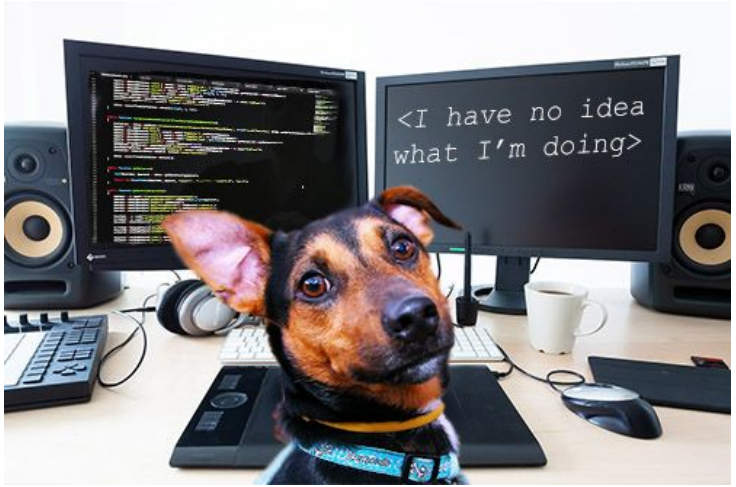
-w {only whole word}

-c {count number of matching lines / suppresses output}

Need Help?

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.



Edit Stuff

Nano - terminal based text editor. Nano is ideal for making small changes to existing configuration files or for writing short plain text files.

Vim- Another terminal based text editor. Vim is much more common and powerful compared to nano.

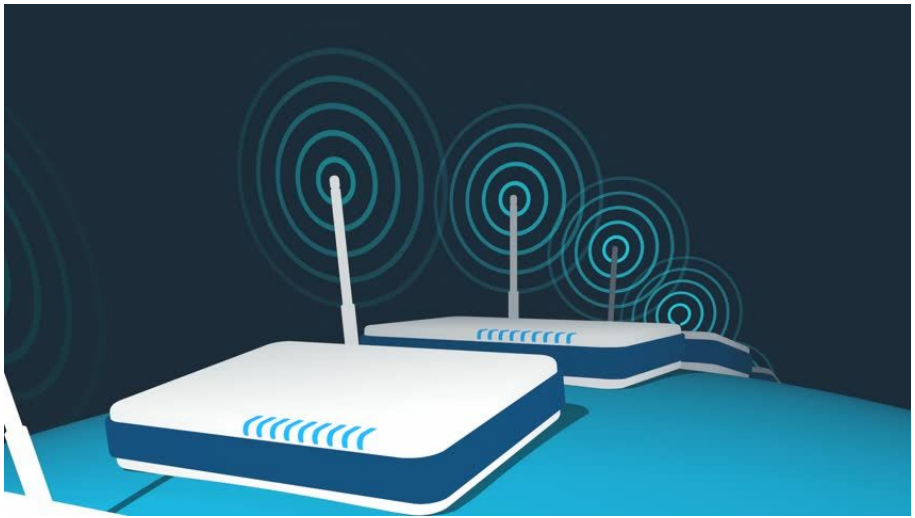
Other useful Linux commands that will be more relevant next week

nslookup

tcpdump

netstat

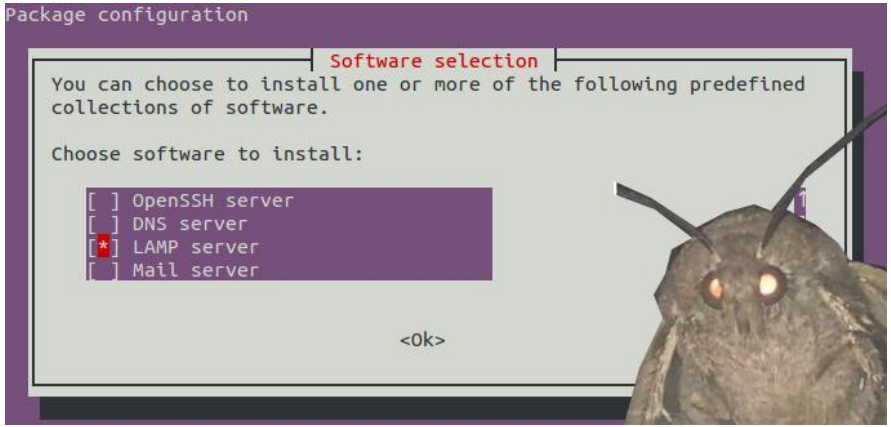
ifconfig



Services

Linux can run

Web Server, DNS, DHCP, Mail, FTP, MYSQL, Anything



Next time linux

Log analysis

Process monitoring

Managing services & Networking with Linux

Linux security

Linux Resources:

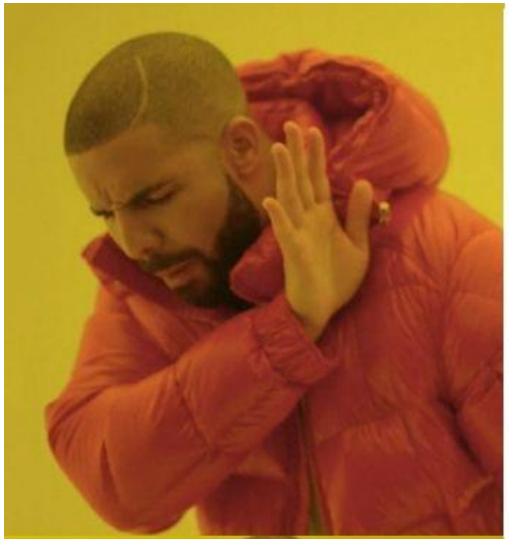
Over the wire - Practice Linux Navigation through SSH.
http://overthewire.org/wargames/

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

Announcements

Working on an interesting project? Have a specialty? Present

If you are interested in a topic/want to present email us! Cyber



Cyber Defense Organization

199 Members

Primary Contact: Liam Smith

Cyber Defense Organization

202 Members

Primary Contact: Liam Smith

Cya Next week!

Thank you to everyone who filled out the survey!

mlim@albany.edu

Follow us on Twitter? Add on myInvolvement?

Grey Castle speakers - Tuesday 7:15? BB129

CCDC! - Monday 7:30

BB123 (Check email).

Introduction to Networking

- **Friday 3pm BB123**