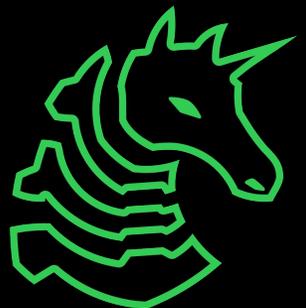


FA2022 Week 01

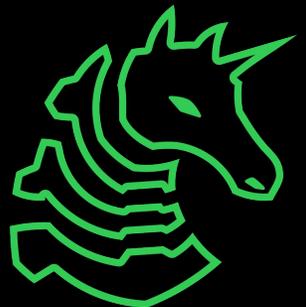
Setup

Anusha and Nathan



Announcements

- CSAW this weekend
 - Free pizza! 🍕
- Fall CTF registration open
 - fallctf.sigpwny.com



What is SIGPwny?

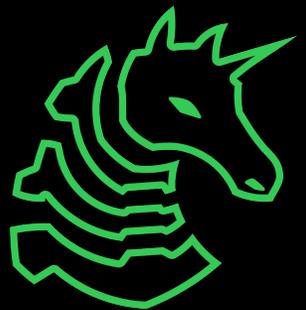
- Computer Security Club at UIUC
- Largest Special Interest Group in ACM@UIUC



Don't talk to me or my child ever again



Two Meetings/Week!



Traditional Thursdays

15 Minutes Talking, 45 Minutes Doing

6-7PM Siebel CS 1404



Seminar Sundays

1+ hours talking, many hours doing

2-3PM Siebel CS 1404



Code of Conduct

1. **Be respectful.**
2. **Be inclusive.**
3. **Nothing illegal.**
4. **No NSFW or suggestive content.**
5. **Don't spam.**
6. **Use common sense.**



Pwny CTF (ctf.sigpwny.com)

- Create an account right now!
- Where we put our challenges for you to build hands on experience
- Solve challenges, find flags, submit flags on website



WARNING before we go any further!

(The “Don’t Get Arrested” Slide)

- We will teach you things that you could use unethically & illegally
- <https://www.law.cornell.edu/uscode/text/18/1030>
 - Read it!
- CFAA TLDR
 - Computer Fraud and Abuse Act
 - Attacking “protected” computers
 - Anywhere between a fine and **TWENTY** years in jail.
- If you don’t have EXPLICIT permission to break into it, **DON’T**
- We are NOT lawyers and CAN’T give you legal advice

We are NOT suggesting, telling, or implying you should actually do these things. By participating in this club and agreeing to our Code of Conduct, you agree that your actions are your own and you will deal with the consequences.



Marcus Hutchins, Controversial Hacker who saved the internet, got arrested for past crimes.

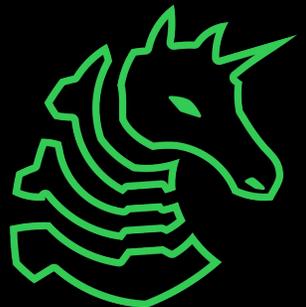


sigpwny{setup}



Table of Contents

- What is a shell
 - I want one
- Getting into the shell
 - OS Differences + Different Shells
 - WSL or Virtual Machines?
 - Installing WSL
- Starter commands
- Tools to install



> The Terminal

"It's where things happen" - Ravi



```
CSAW2020 /dev/tty000
ls
bard      grid      kui_blox1_sol.png
bard.hop  grid_solve.py  libc-2.27.so
ezbreezy  krakme.exe    solve_ezbreezy.py
CSAW2020
```

```
mark@linux-desktop: ~
File Edit View Search Terminal Help
mark@linux-desktop:~$
```

```
tquig@THOMAS-PC: ~
tquig@THOMAS-PC:~$
```



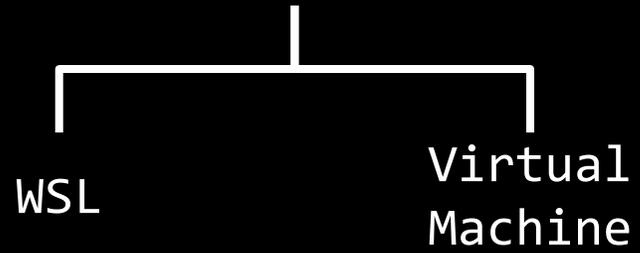
Linux



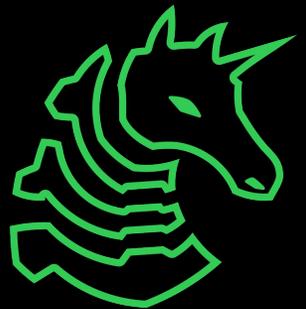
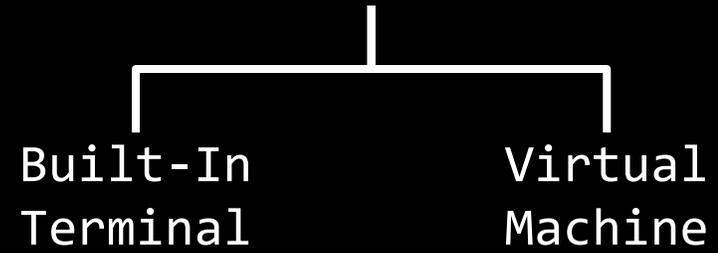
You're good to go!



Windows



macOS



PowerShell? Command Prompt?

- Those are shells too!
- However, they're limited in tools and are Windows-based terminals, not Linux-based



Windows Subsystem for Linux



Installing WSL

- Open command prompt as administrator
 - (Start button → type **cmd** → right click → open as administrator)
- Type **wsl --install**
- Restart computer
- Open command prompt
- Enter WSL by typing **wsl**
- You now have a linux shell

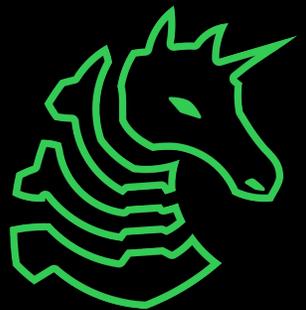
```
Administrator: Windows PowerS... x + v - □ x
PS C:\Users\chris> wsl --install
Installing: Virtual Machine Platform
Virtual Machine Platform has been installed.
Installing: Windows Subsystem for Linux
Windows Subsystem for Linux has been installed.
Downloading: WSL Kernel
Installing: WSL Kernel
WSL Kernel has been installed.
Downloading: GUI App Support
Installing: GUI App Support
GUI App Support has been installed.
Downloading: Ubuntu
[===== 43.3% ]
```



Set a "root" user

Select a username and password for your administrative user.

```
hayden@T470s ~  
Installing, this may take a few minutes...  
Please create a default UNIX user account. The username does not need to match your Windows username.  
For more information visit: https://aka.ms/wslusers  
Enter new UNIX username: hayden  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
Installation successful!  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
hayden@T470s:~$
```



macOS Terminal

Command
+ Space



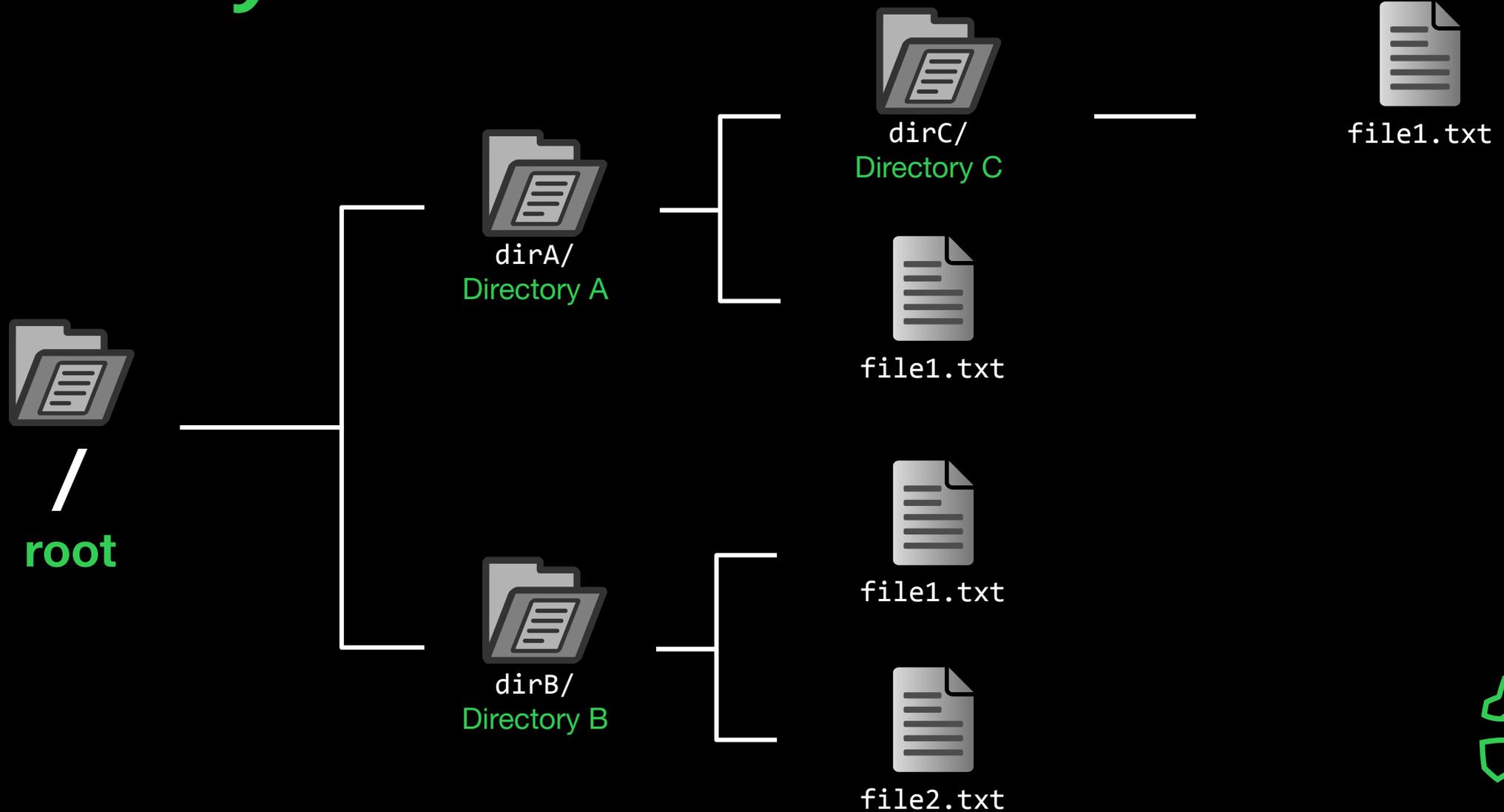
Search "Terminal"



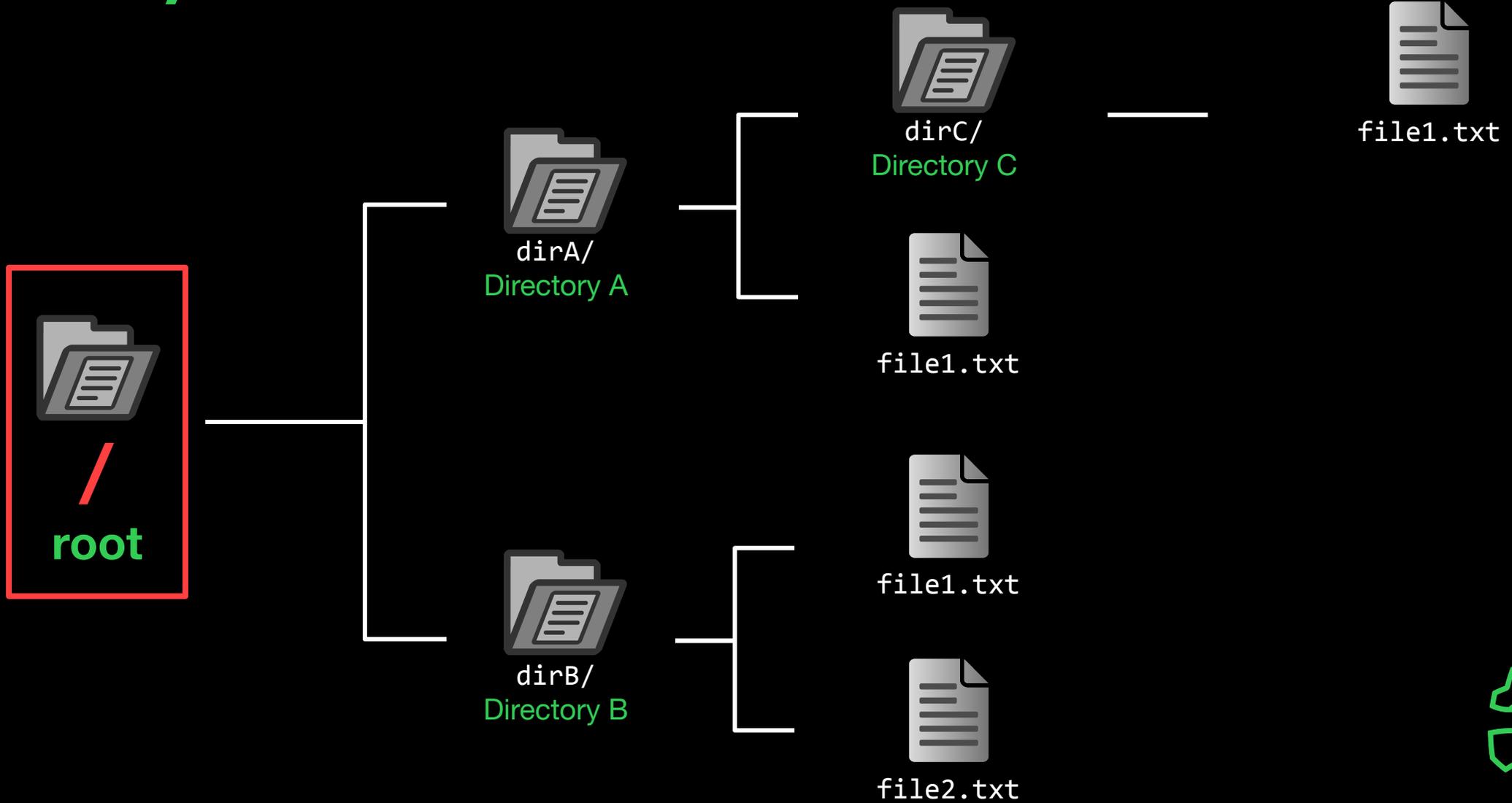
```
→ CSAW2020 ls
bard          grid          kui_blox1_sol.png
bard.hop     grid_solve.py libc-2.27.so
ezbreezy     krakme.exe   solve_ezbreezy.py
→ CSAW2020
```



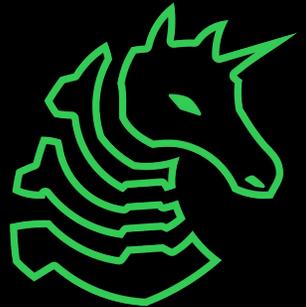
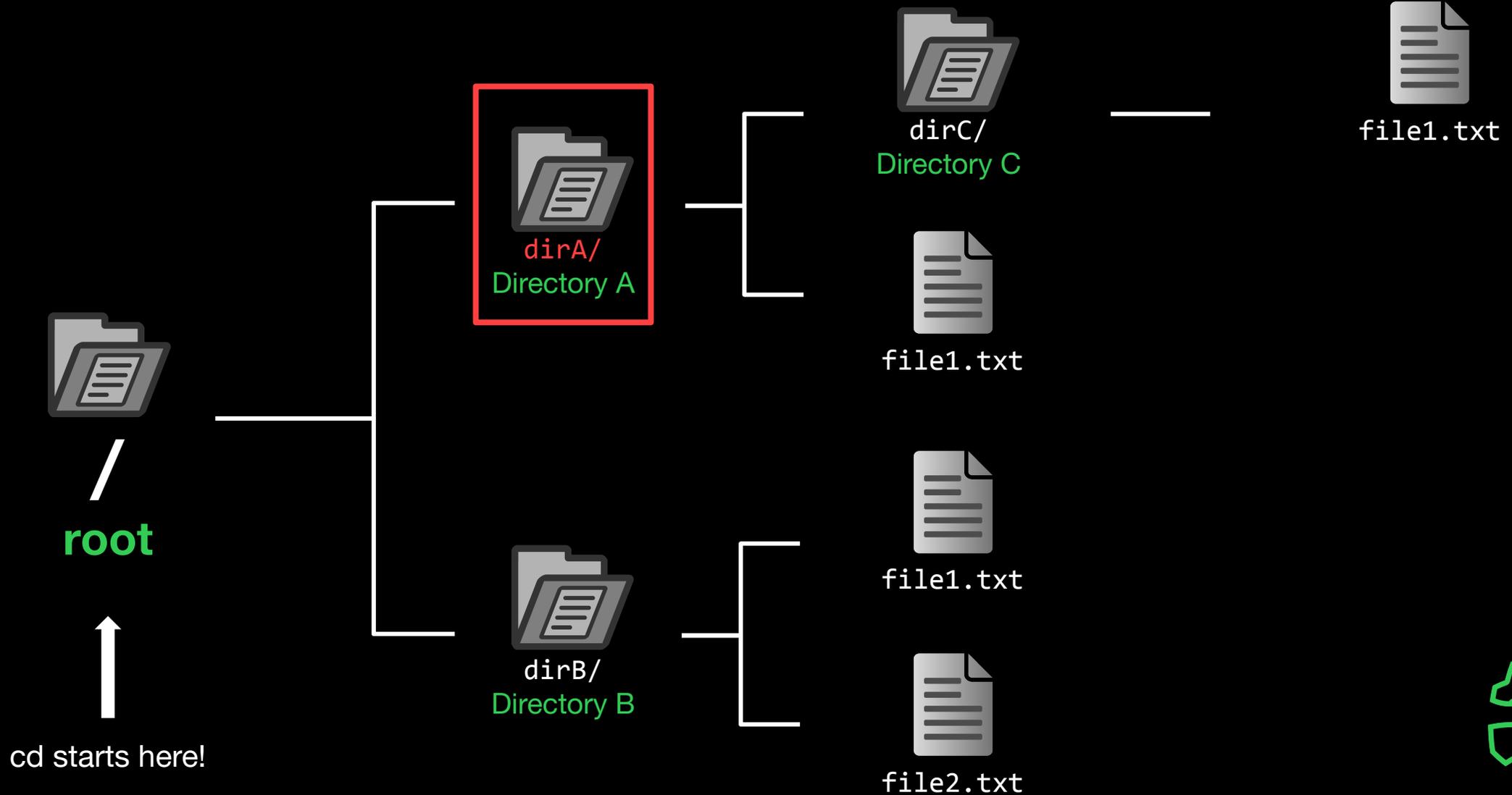
Filesystems



cd /

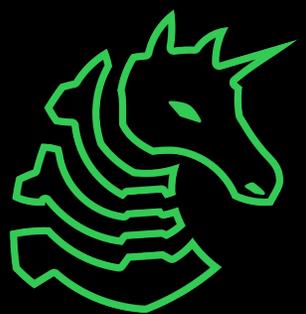
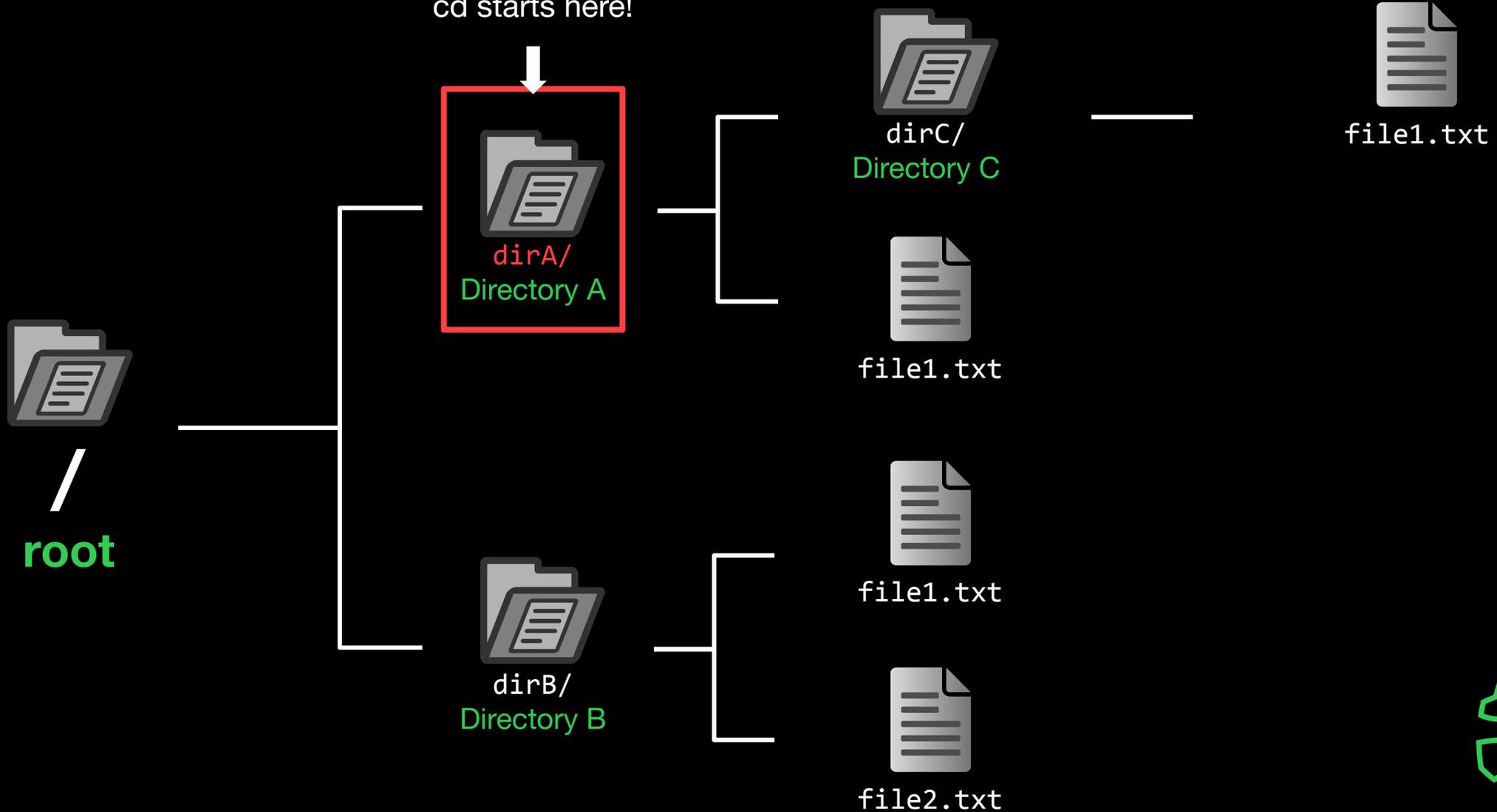


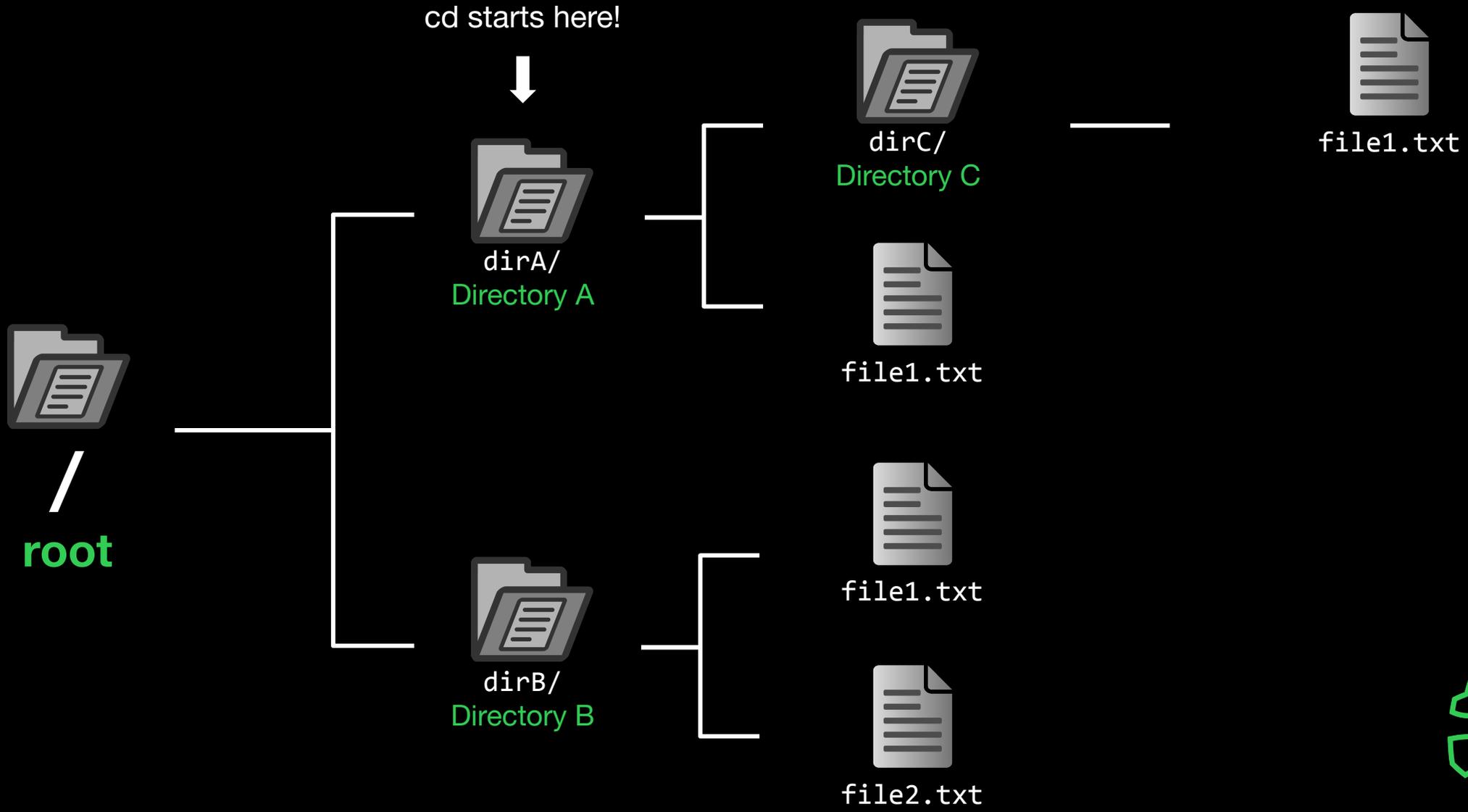
cd dirA



cd dirA

cd starts here!



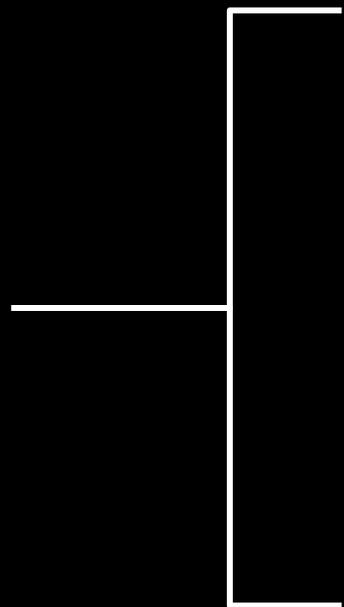


cd dirC

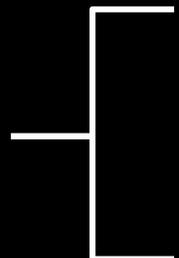
cd starts here!



root



dirA/
Directory A



dirC/
Directory C



file1.txt



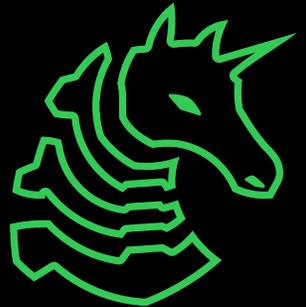
file1.txt



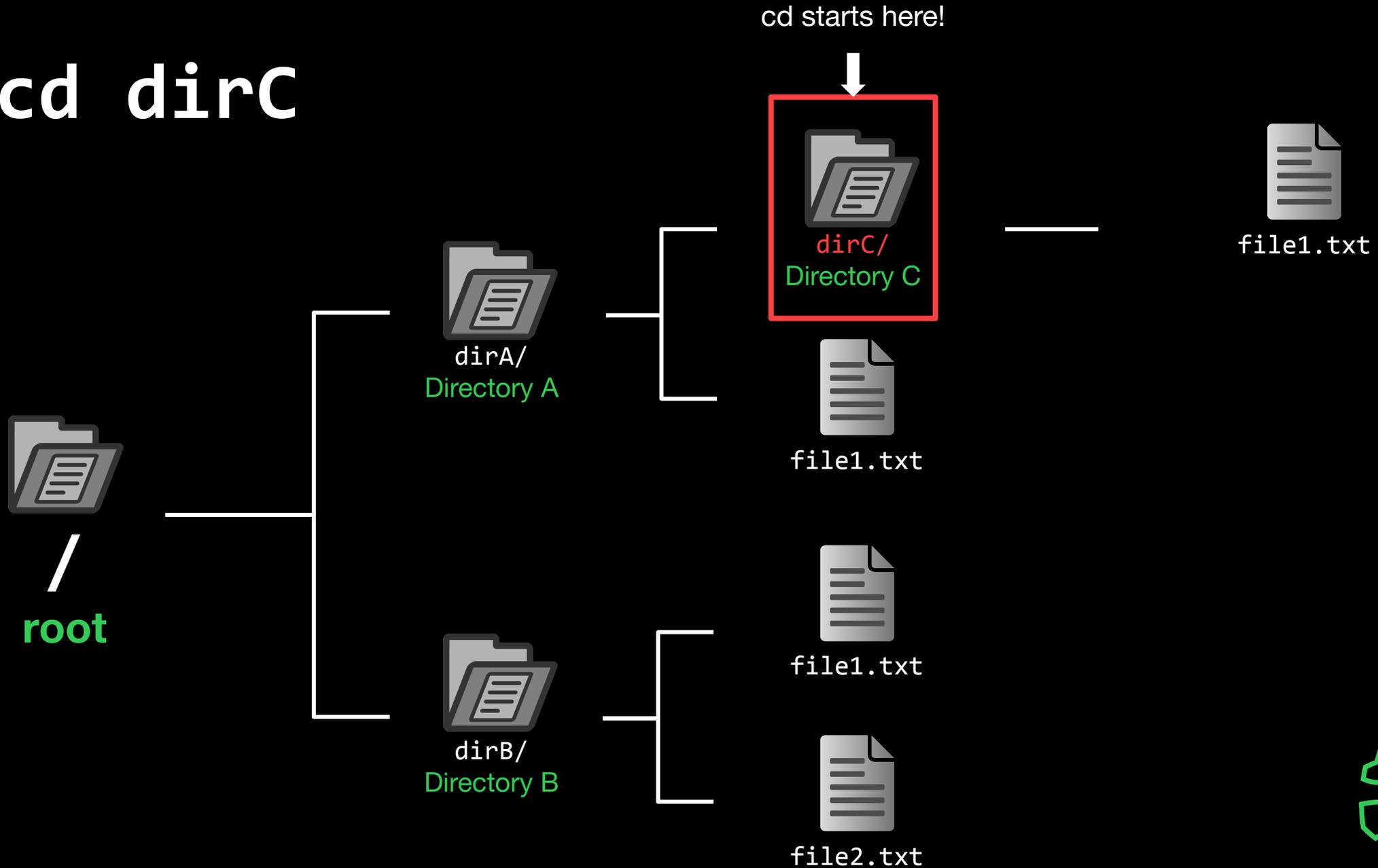
file2.txt

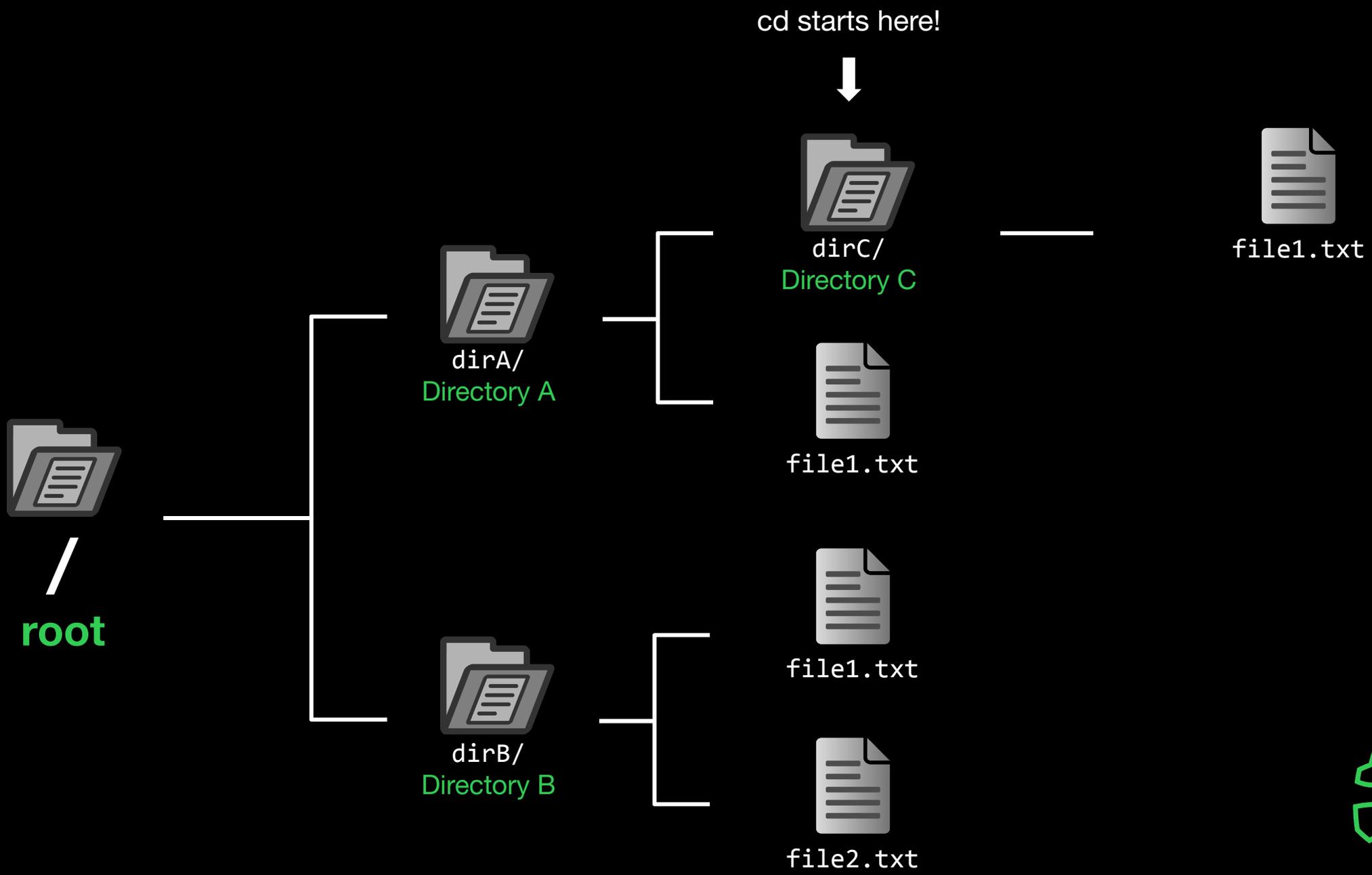


file1.txt



cd dirC





cd dirB

cd starts here!



/
root



dirA/
Directory A



dirC/
Directory C



file1.txt

Error: dirB not found



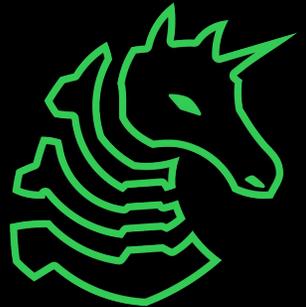
file1.txt



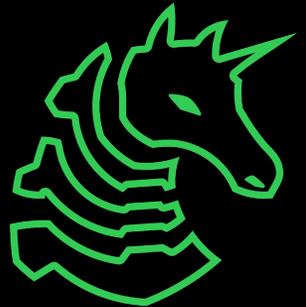
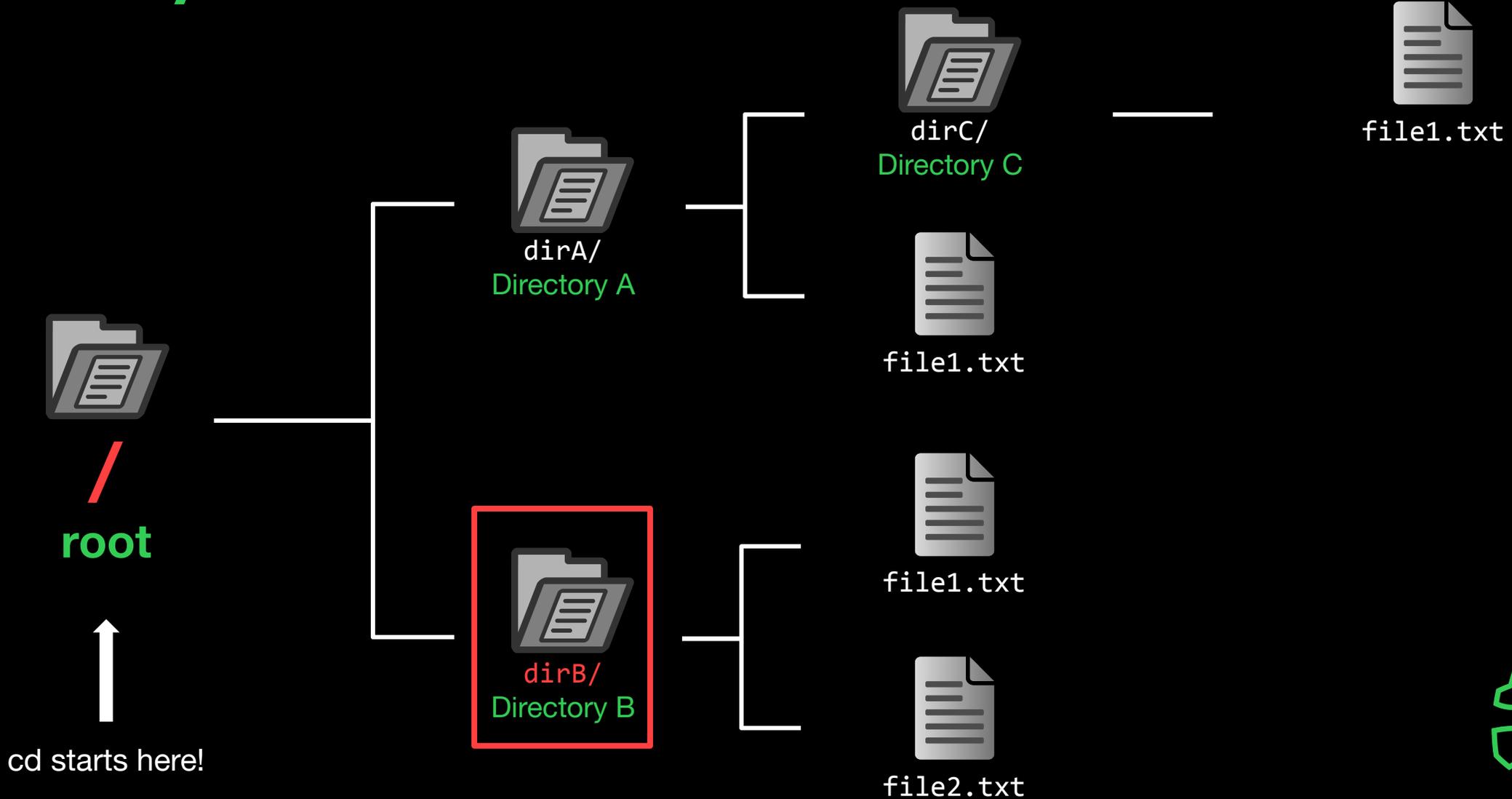
file1.txt



file2.txt

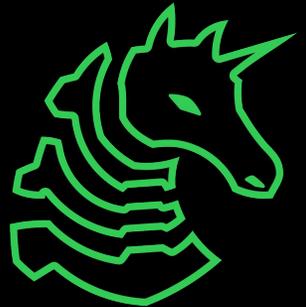
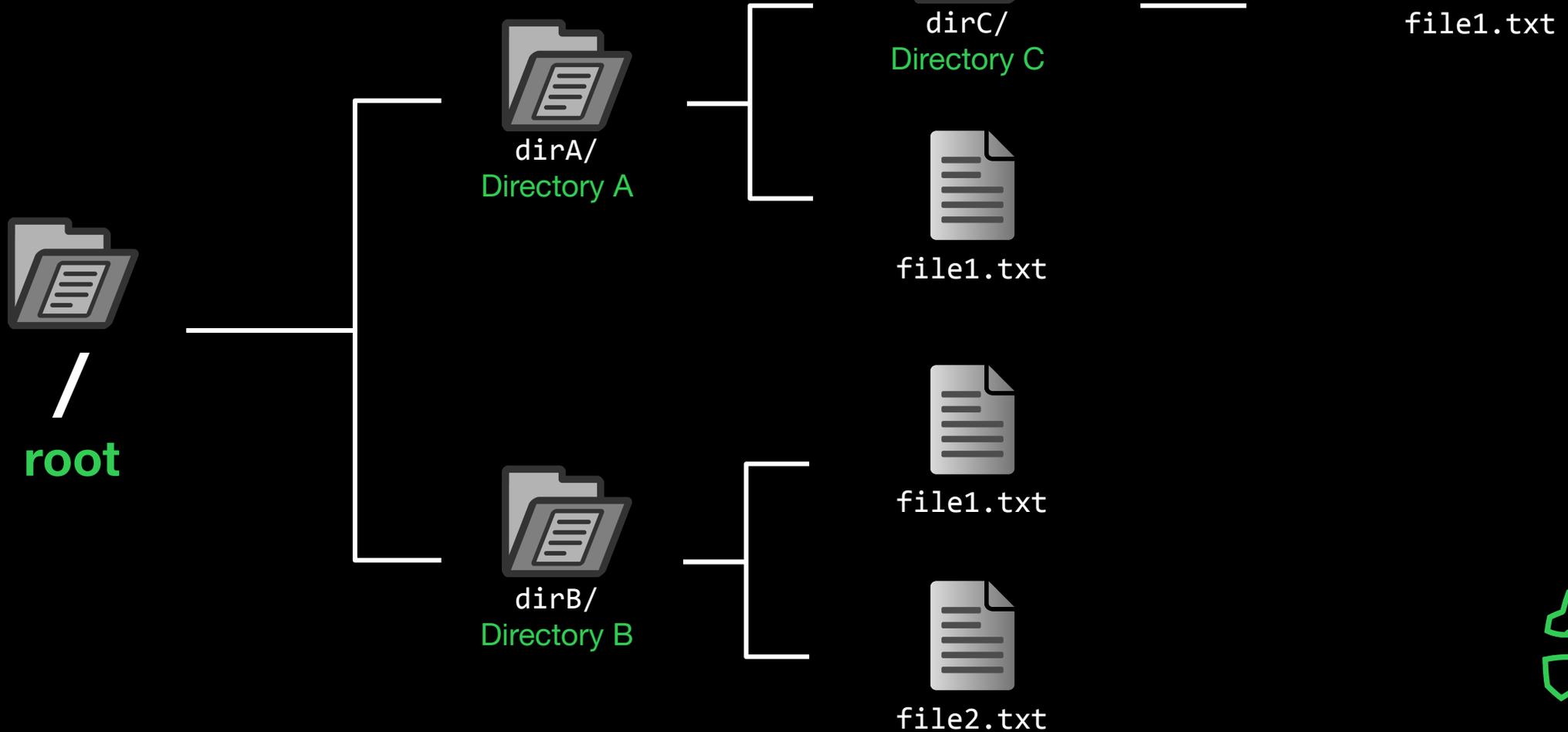


cd /dirB



`cd ../../../dirB`

cd starts here!



```
cd ../../dirB
```

cd starts here!



dirC/
Directory C



file1.txt



dirA/
Directory A



/
root



file1.txt



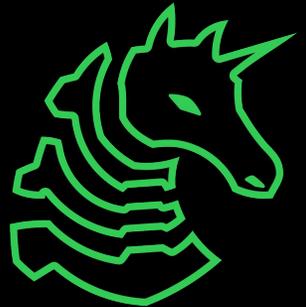
file1.txt



dirB/
Directory B

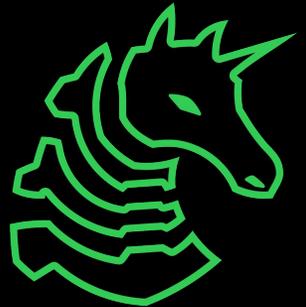
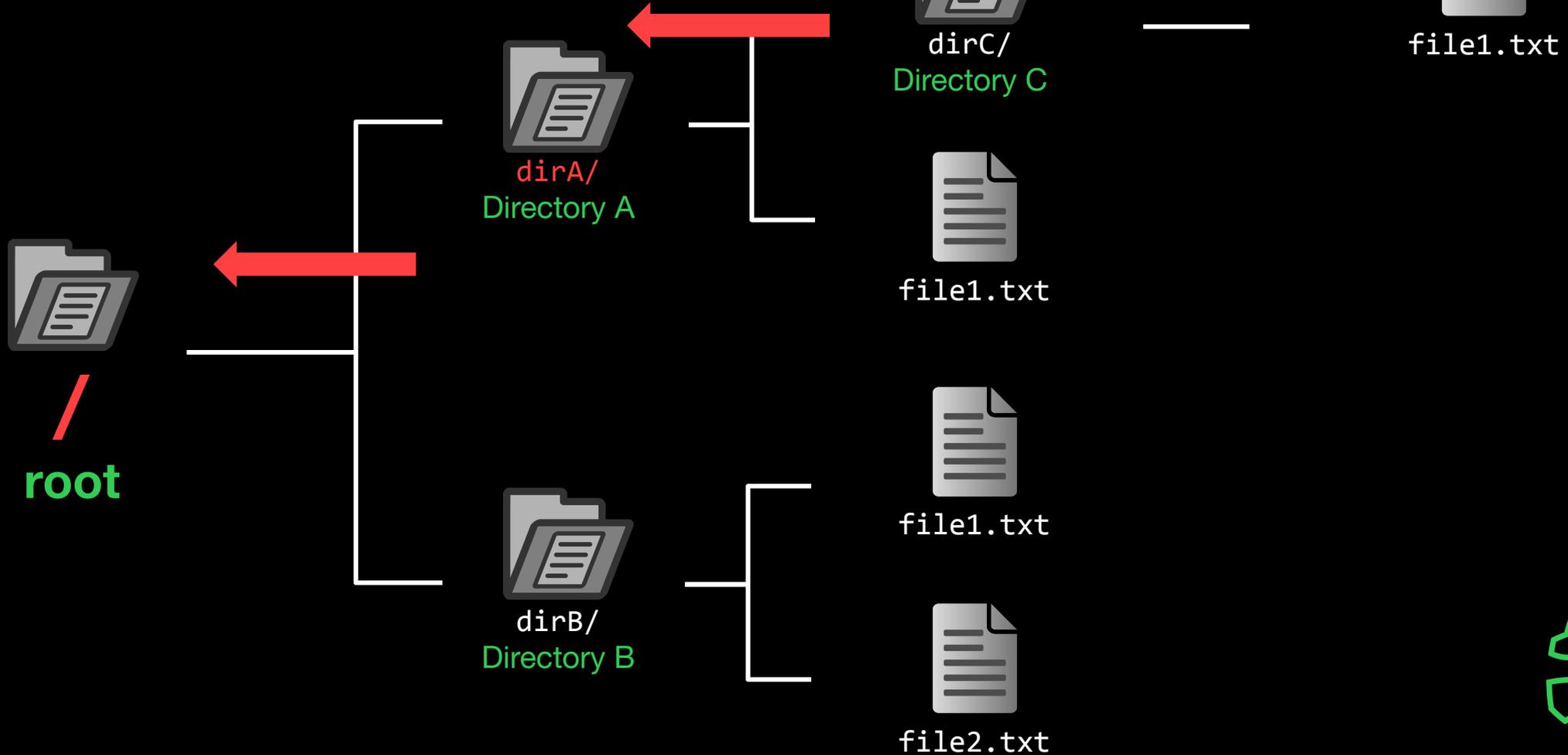


file2.txt



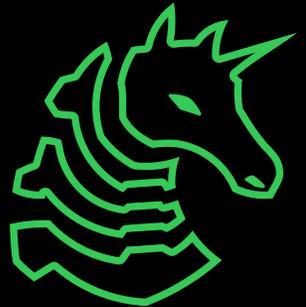
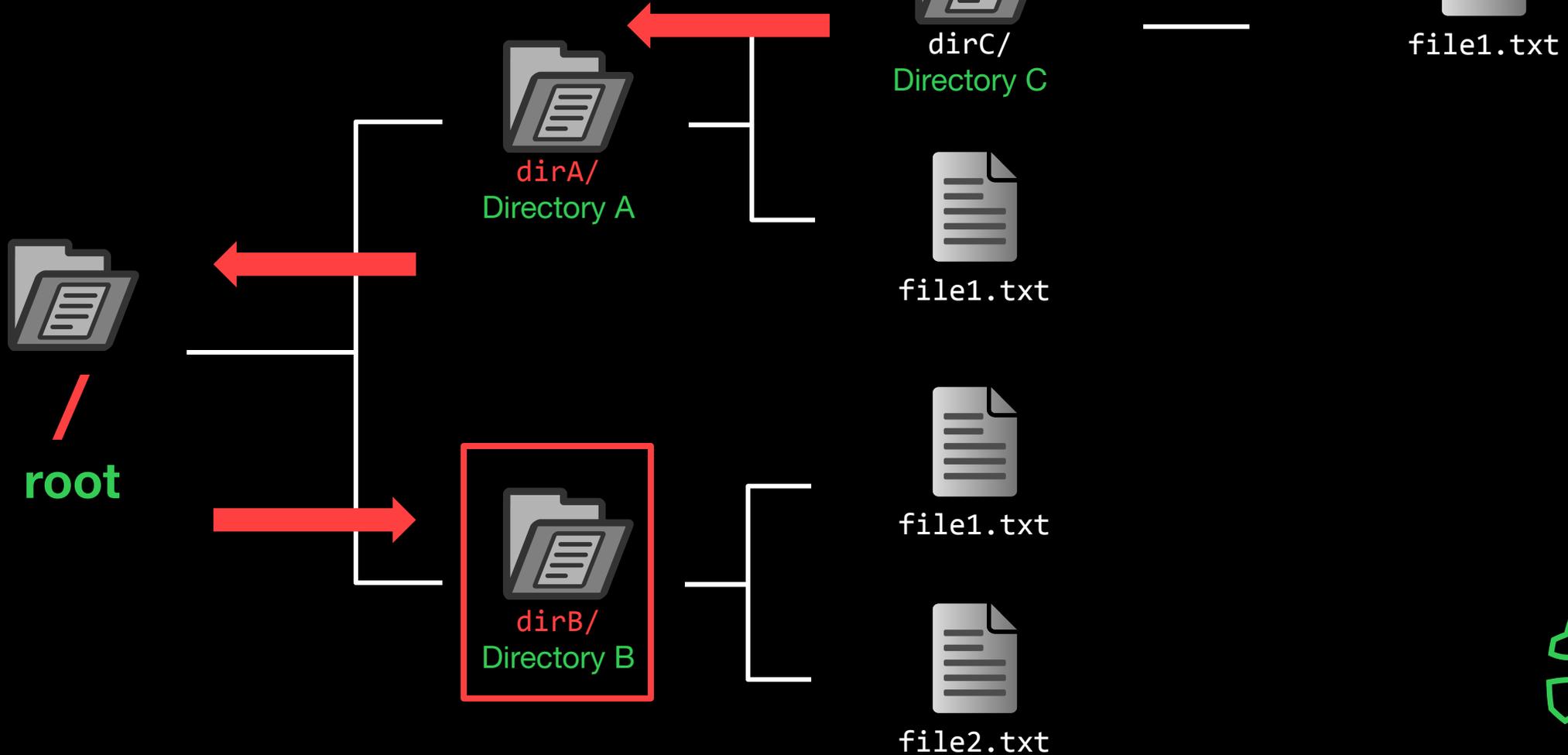
`cd ../.. /dirB`

cd starts here!

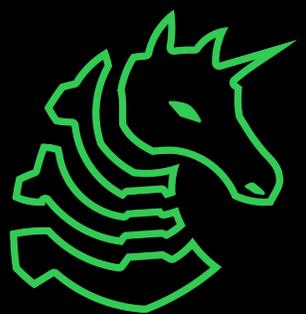
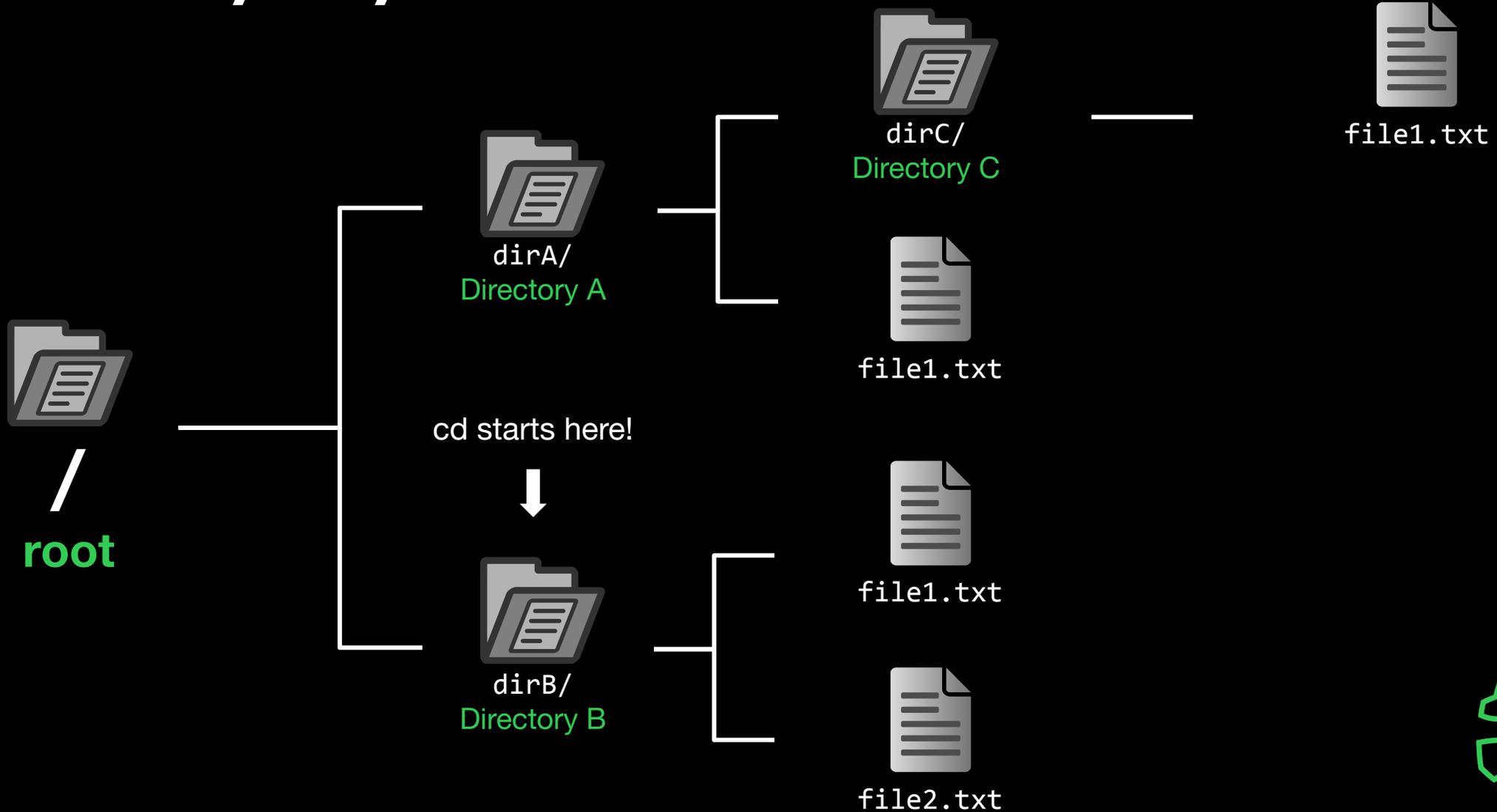


`cd ../../dirB`

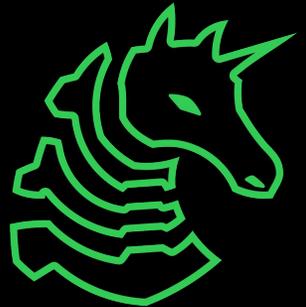
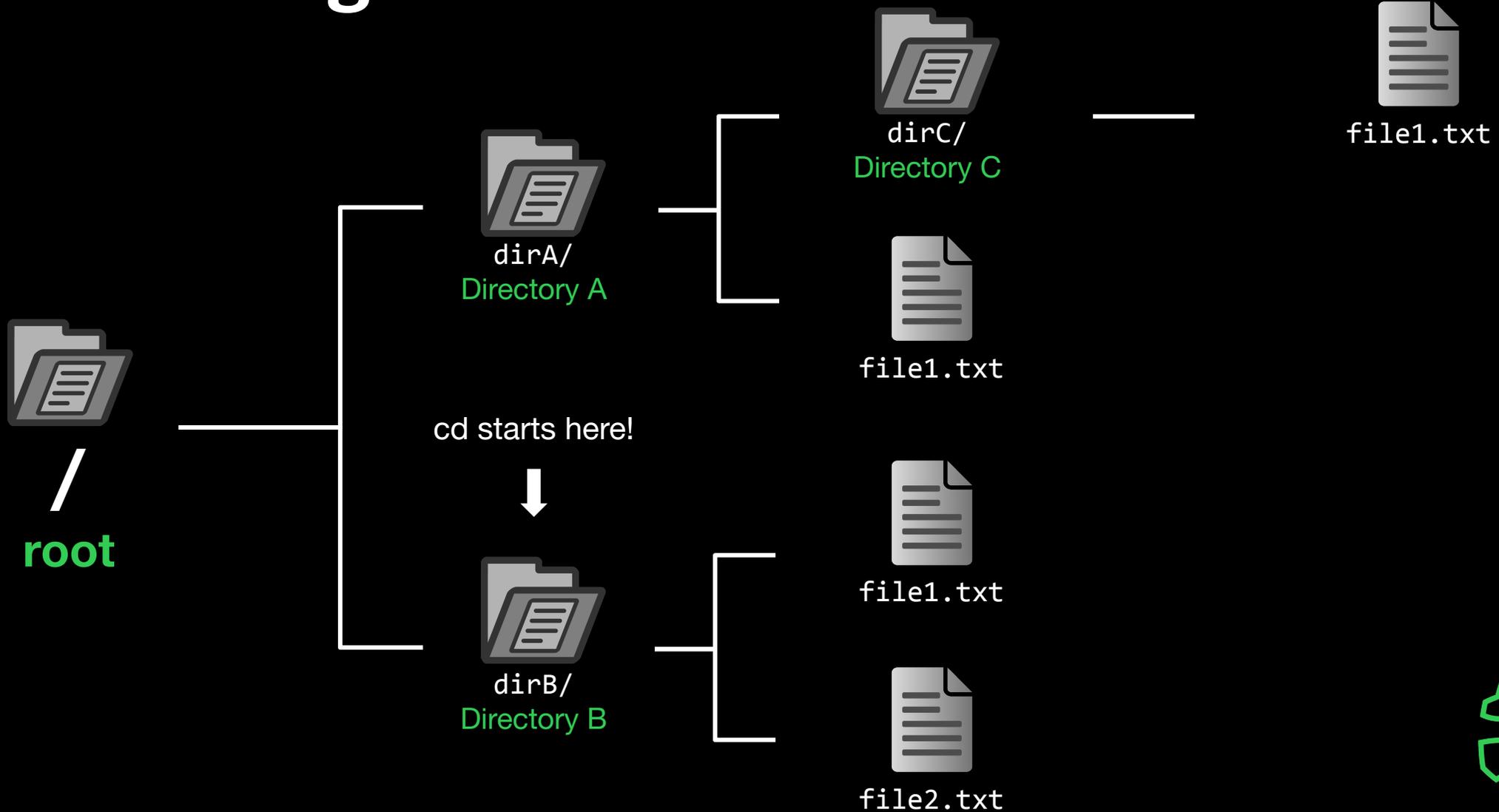
cd starts here!



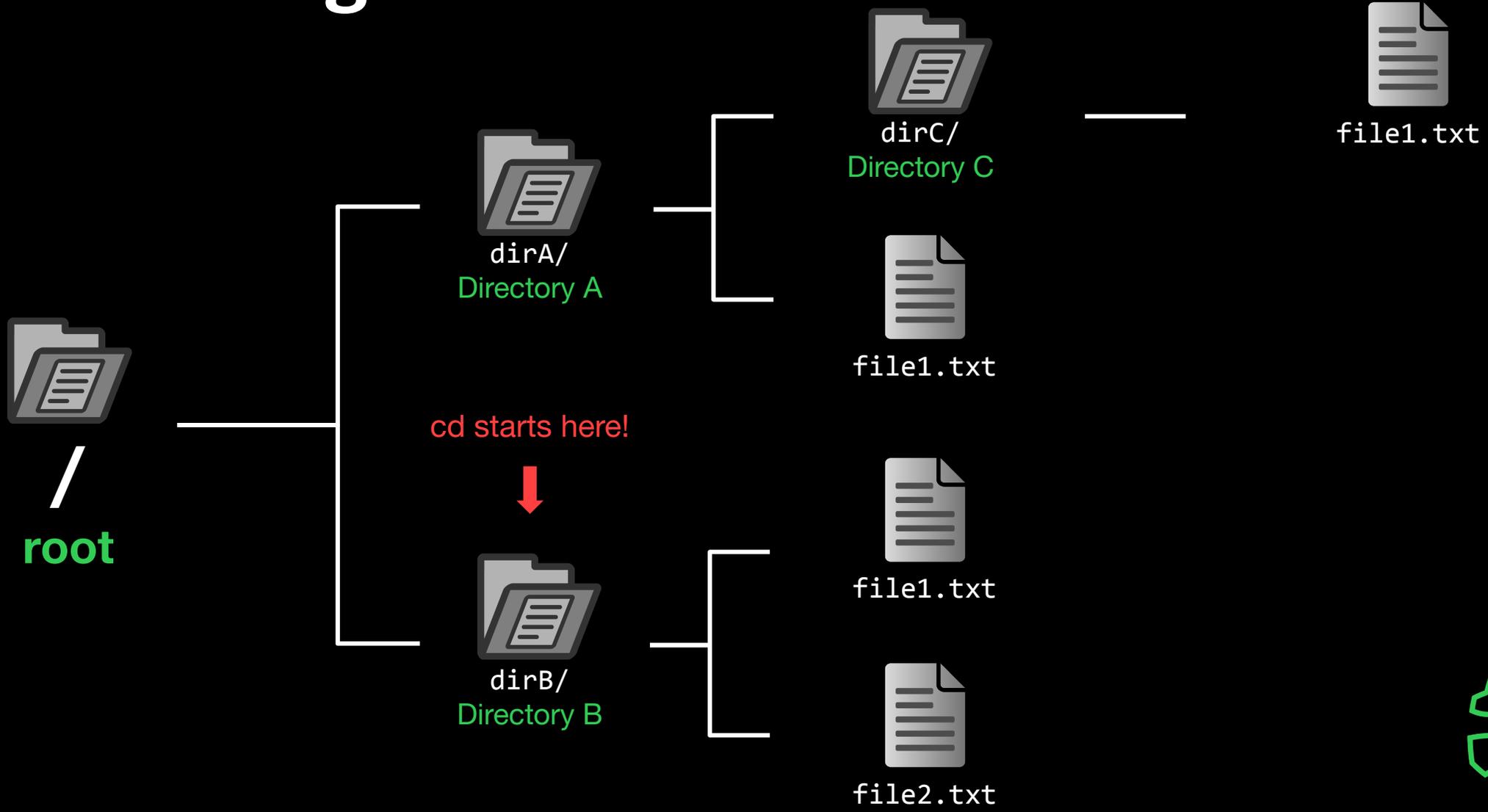
cd ../../dirB



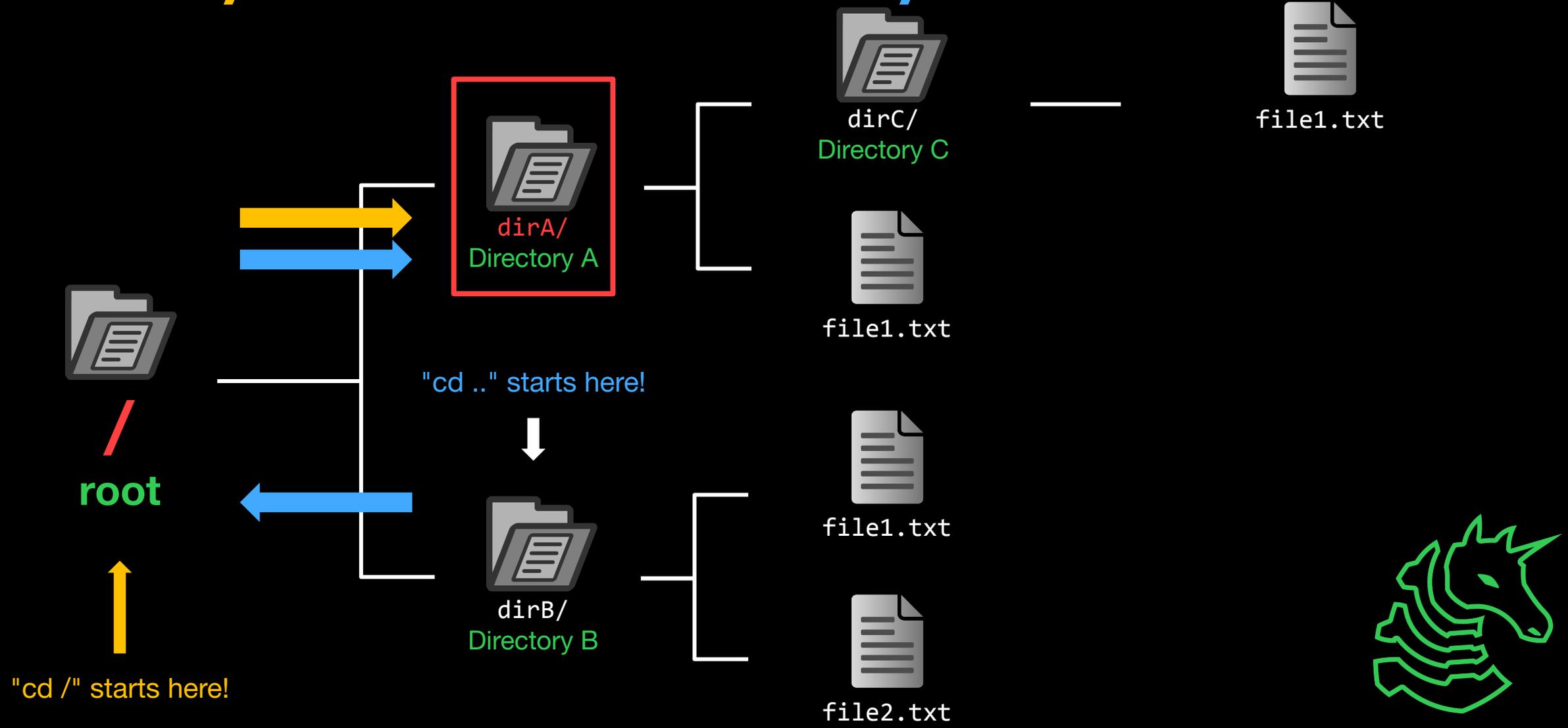
How to get to dirA?



How to get to dirA?



"cd /dirA" or "cd ../dirA"



Paths

Absolute Path

The full path that always starts at root (/)

`/dirA/file1.txt`

`/dirA/dirC/file1.txt`

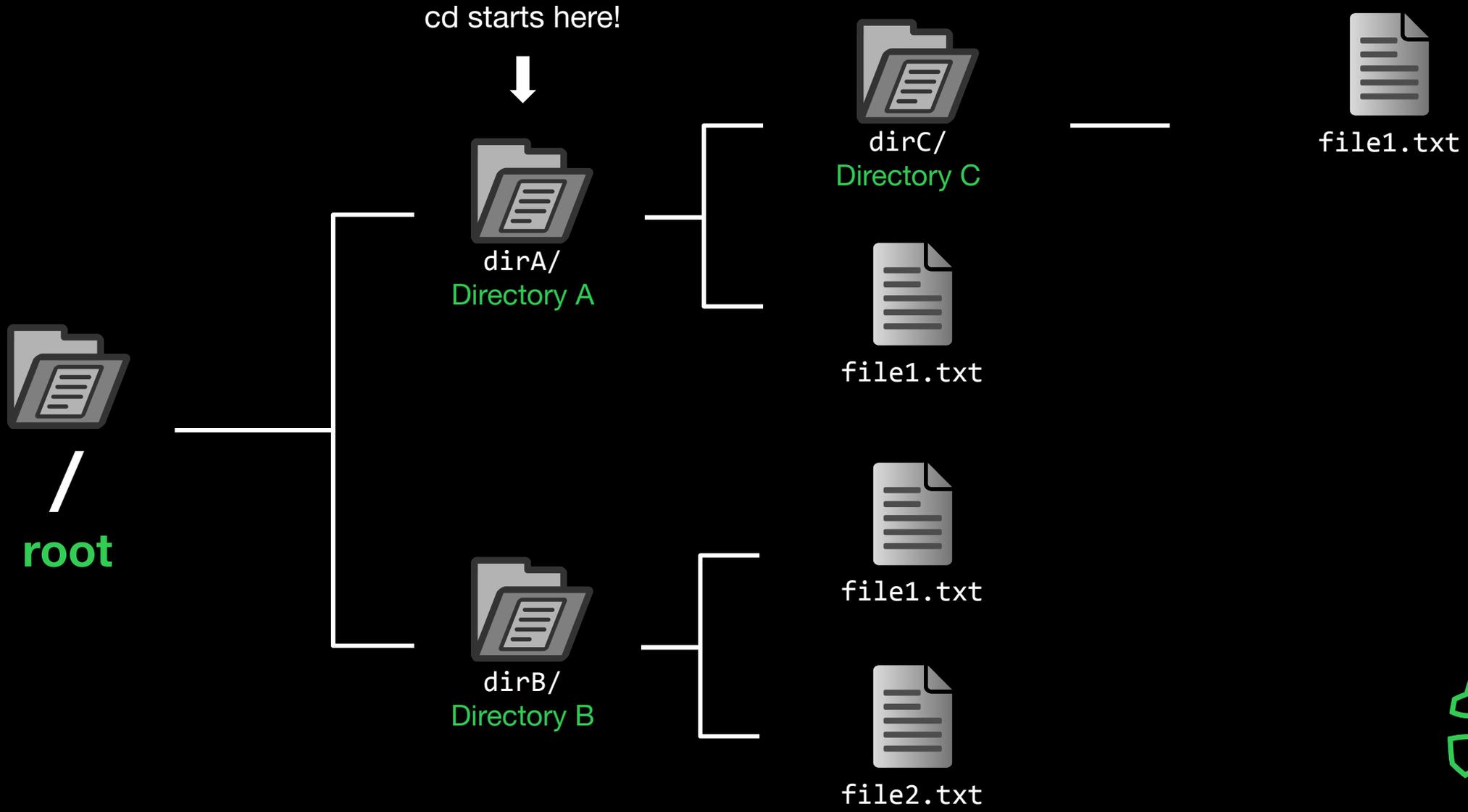
Relative Path

The partial path relative to where you are currently in the terminal

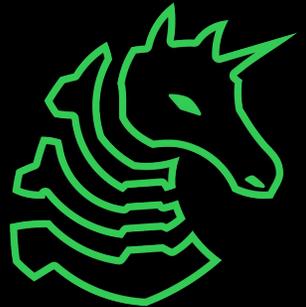
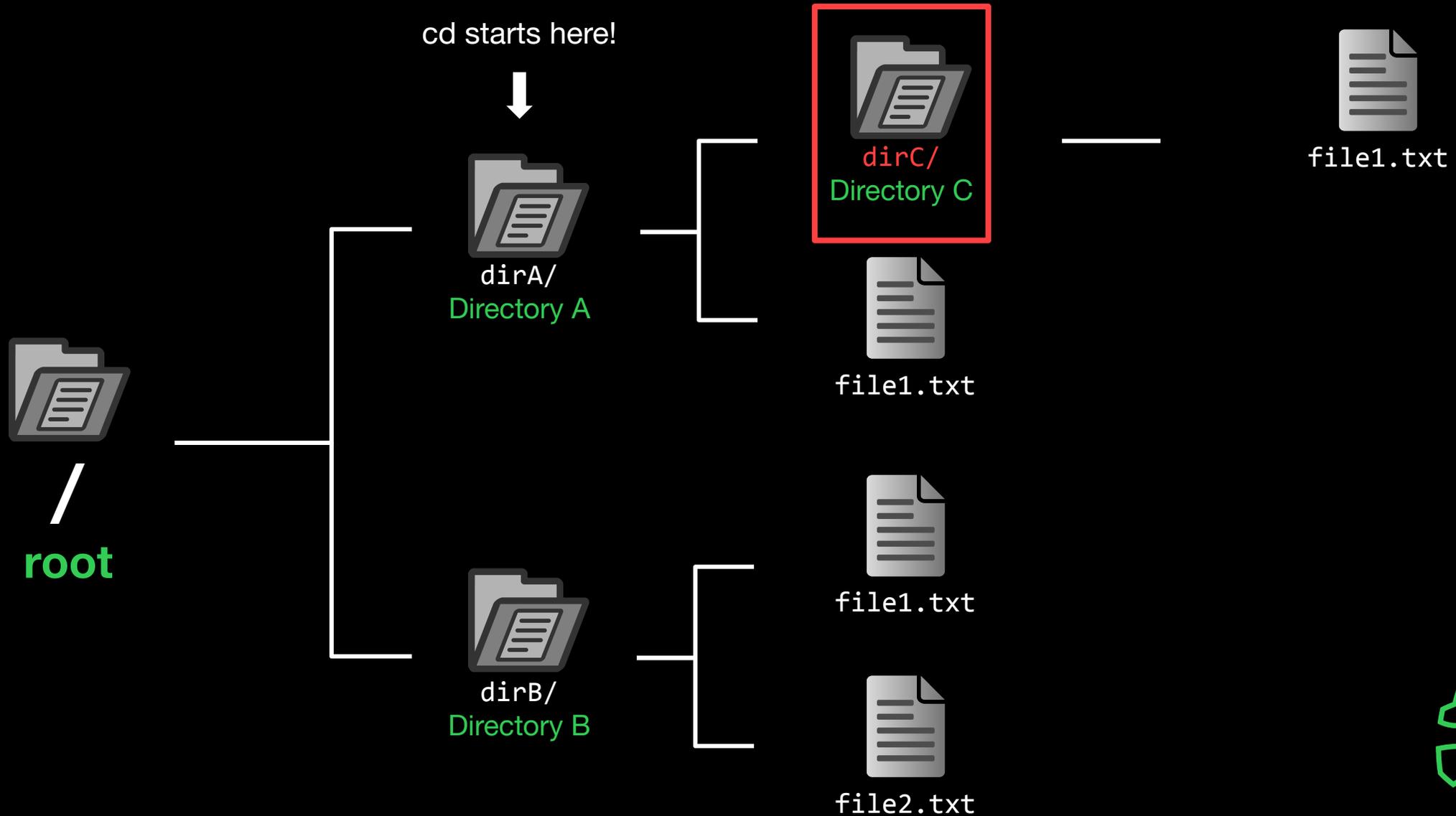
(Relative to dirA)

`file1.txt`

`dirC/file1.txt`



"cd dirC" or "cd ./dirC" or "cd dirC/"



`./dirC == dirC == dirC/`

Also `../dirC` and `../../dirC` and `../../../dirC` and...

These are just conventions!



Useful Commands - Filesystem

ls [directory]: lists files in your current directory or specified directory

cd <directory>: changes your current directory to specified directory

mv <source> <dest>: moves file from source to dest (rename), if dest is a directory, move source

rm <file>: removes file (**NOT REVERSIBLE**)

cat <file>: prints the contents of file (sometimes it prints gibberish, think why that might happen)

./file: executes whatever is at file

man <command>: lets you see info about a command and all of its parameters/options

<parameter> means it's a required parameter

[parameter] means it's an optional parameter



Useful Commands - Networking

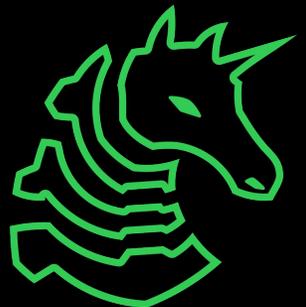
`nc <ip> <port>`: netcat, connect to ip on port port. (First Command - netcat)

`ssh <user@ip> [port]`: secure remote shell, run an instance of a shell as user at the IP address

`ping <ip>`: see if an IP address is up using ICMP (usually blocked by firewalls)

`curl <url>`: network access tool that is mainly used to access websites from the terminal

`wget <url>`: Simplified/modern curl that downloads the file with relevant name

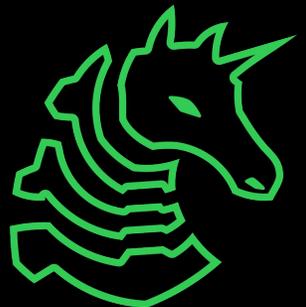


Networking Fundamentals

`nc -l <port>`: open a network socket to listen on specified port

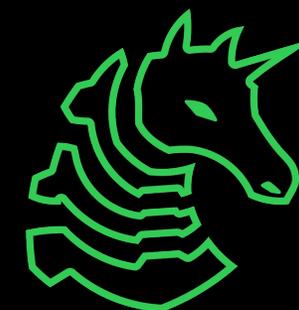
`nc <ip> <port>`: open a connection to the specified IP and port

Ports - communication endpoints on your computer (1-65535)



Next Steps - Bandit

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```



Next Steps - Bandit

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

command

user

IP

port



Next Meetings

2022-09-08 - This Thursday

- Web I
- Intro to Web Hacking

2022-09-09 - This Friday

- CSAW CTF '22 Qualifying Round
- We will be playing in this weekend long CTF - come join us!

2022-09-11 - Next Sunday

- Web II
- Advanced Web Hacking

