Free Course Link: https://www.youtube.com/watch?v=Snrh580U3tI&t=6s

Navigating the System

- Windows focus
  - GUI (graphical user interface)
  - CLI (command line interpreter)
- Linux focus
  - The command line interpreter in Linux is called a **shell**, and the language that we'll use to interact with this shell is called **Bash**
- Windows file system
  - In Windows, filesystems are assigned to drive letter, which look like **C:**, or **D:**, or **X:**
  - The **root** directory of C: would be written C:\, and then the root directory of X: would be written X:\
  - Subdirectories are separated by backslashes (\), unlike Linux, which uses forward slashes (/)
  - The C: drive root folder is what we call a **parent directory** and the contents inside are considered **child directories**
- Windows basic commands (in powershell)
  - **Get-Help** _____ = get info about command
  - **ls -Force** = list all files, including hidden
- An **absolute path** is one that starts from the main directory. A **relative path** is the path from your **current directory**.
  - **pwd** = print working directory
  - **cd** = change directory
  - **cd ..** = relative path, take you one level up
  - **cd ~** = root directory
  - Has built in **tab completion**
  - **mkdir** - make new directory
  - **history** = show all commands used
    - **Ctrl + r** = shortcut to search for used command
  - **clear** = clear everything
  - **cp** = copy , **-Recurse** = all files within a directory, **-Verbose** = show text
- A **wildcard** is a character that's used to help select files based on a certain pattern
  - In sell, recurse = **-r**
  - **mv** = move item command, can be used to rename
- In powershell, the command to remove files and directories is **rm** or **remove**
  - Take caution, remove does not use the recycle bin!
  - **cat** = show text in file
    - **-head 10** = show first 10 lines, **-tail 10** = show last 10 lines
  - **more** / **less** (in Linux) command to view text 1 page at a time
  - **Get-alias** _____ = show exact command being used by alias
- **Get-Help** is used for powershell commands life **Get-Help ls**, and **/?** Is used for other commands like dir such as **dir /?** In the cmd
- Windows: Search for files in GUI with **indexing**
  - **sls** [word] [file] = select-string command , used for searching strings in a file(s)
- PS ||| The **-filter** parameter will filter the results for file names that match a pattern

    - The **asterisk** means match anything, and the **.exe** is the file extension for executable files in Windows
    - For Bash, **grep** is used instead of -filter
- PS ||| **Echo** = alias for write-output
    - **>** = redirect output operator
    - **>>** = append operator, does not overwrite - only adds
    - **|** = pipe operator = pass the output of a command to the input or another
    - **1 = stdout** - the output
    - **2 = stderr** - the error
    - **$null** = nothing, black hole operator
        - Bash = /dev/null
- **Regular expressions** are used to help you do advanced pattern-based selection

User, Groups, & Permissions

- **Standard user** - one who is given access to a machine but has restricted access to do things like install software or change certain settings
- **Administrator** (admin) - a user that has complete control over a machine
- Windows - use **computer management** to view users
- **Windows domain** - a network of computers, users, files, etc that are added to a central database
- User Access Control (**UAC**) - a feature in Windows that prevents unauthorized changes to a system
- PS ||| **Get-LocalUser** = show computer user information
    - **Get-LocalGroup** = show computer groups information
    - **Get-LocalGroupMember** _____ = show group members
    - **net** user cindy * = change password for user cindy
    - **net** user victor /logonpasswordchg:yes = user will change password at next logon
- Bash ||| **passwd** (user) = change password
    - sudo passwd **-e** victor = change pass at next logon
    - sudo **useradd** juan = add new user juan
    - sudo **userdel** juan = delete user juan
- In Windows, files and directory permissions are assigned using Access Control Lists or **ACLs**. Specifically, we're going to be working with Discretionary Access Control Lists or **DACLs**.
    - Windows files and folders can also have System Access Control Lists or **SACLs** assigned to them. SACLs are used to tell Windows that it should use an event log to make a note of every time someone accesses a file or folder.
    - **Read**: the Read permission lets you see that a file exists, and allows you to read its contents. It also lets you read the files and directories in a directory.
    - **Read & Execute**: the read and execute permission lets you read files, and if the file is an executable, you can run the file. Read & Execute includes Read, so if you select Read & Execute, Read will be automatically selected.
    - **List folder contents**: List folder contents is an **alias** for Read & Execute on a directory. Checking one will check the other. It means that you can read and execute files in that directory.
    - The **Write** permission also lets you create subdirectories, and write to files in the directory.
    - **Modify**: the Modify permission is an umbrella permission that includes read, execute, and write.
    - **Full Control** - a user or group with full control can do anything they want to the file. It includes all of the permissions of Modify, and adds the ability to take ownership of a file and change its ACLs.

    - **icacls** = Displays or modifies discretionary access control lists (DACLs) on specified files, and applies stored DACLs to files in specified directories.
- Permissions in Linux:
    - **Read** - this allows someone to read the contents of a file or folder
    - **Write -** " " write information to a file or folder
    - **Execute** - " " execute a program
- **Guest Users** - this is a special type of user that's allowed to use the computer without a password. Guest users are disabled by default. You might enable them in very specific situations.
- Bash ||| **chmod (rwx)** = change permissions
    - Symbolic format:
        - The owner, which is denoted by a "**u**"
        - The group the files belongs to, which is denoted by a "**g**"
        - Other users is denoted by "**o**"
        - **+** or **-** to add / remove
    - Numerical format or rwx is:
        - **4** = read / r
        - **2** = write / w
        - **1** = execute / x
        - ex: chmod 754 (file) = 7 = user permission, 5 = group permission, 4 = other users permissions
    - **chown** = change owner
    - **chgrp** = change group
- **Simple permissions** are actually sets of special or specific permissions
    - **WD**: create files/write data
    - **AD**: create folders/append data
    - **S**: synchronize

Package & Software Management

- .**msi** (Microsoft Install Package) - used to guide a program called the Windows Installer in the installation, maintenance, and removal of programs on the Windows OS.
- **Debian** - packaged as a .deb file for Debian
    - sudo **dpkg -i** (.deb file) = install a file
    - sudo **dpkg -r** (program name) = uninstall program
    - **dpkg -l** = list all debian packages on system
- Windows archives
    - **Archive** - comprised of one or more files that's compressed into a single file
    - **Package archives** - the core or source software files that are compressed into one file
    - **7zip** = popular windows open source tool for handling archives
- Linux Archives
    - 7zip is also on Linux - to extract a file using 7zip, use the command **7z** and the flag **e** for **extract** and then the f**ile you want to extract**
    - **Tar** is native to most linux distros
- Windows Package Dependencies
    - Having **dependencies** = counting on other pieces of software to make an application work, since one bit of code depends on another, in order to work
    - **Library** - a way to package a bunch of useful code that someone else wrote

        - In windows, they are called **DLL** (dynamic link library)
- Linux Package Dependencies
    - **Package managers** = come with the works to make package installation and removal easier, including installing package dependencies
- Windows: package manager
    - **Package manager** = makes sure that the process of software installation, removal, udate, and dependency management is as easy and automatic as possible
    - **Chocolatey** - 3rd party package management / repository for Windows
- Linux Package Manager Apt
    - **sudo apt install** (package name) - install package
    - **sudo apt remove** (package name) - remove package
    - **PPA** (personal package archive) is a software repository for uploading source packages to be built and published as an Advanced Packaging Tool (**APT**) repository by Launchpad
- Windows: add users and groups GUI
    - Computer management > local users and groups > r click > add user
    - PS ||| **net** user andrea * /add = create new user
        - net user andrea /logonpasswordchg:yes = change pass at next login
        - Combined = net user cesar password /add /logonpasswordchg:yes
    - net user andrea /del = delete account
- Linux: devices & drivers (in Linux, everything is a file)
    - **Character devices** - like a keyboard or a mouse, transmit data character by character
    - **Block devices** - like USB drives, hard drives, and CDROMs, transfer blocks of data; a data block is just a unit of data storage
- Windows: OS Updates
    - **Security patch**: software that's meant to fix up a security hole
- Linux: OS Updates
    - **uname -r** = see kernel version
    - **sudo apt full upgrade** = upgrade the kernel if there is a new version

Filesystems

- Review:
    - **Filesystem** is used to keep track of files and file storage on a disk
    - Windows recommended is **NTFS**
    - Linux recommended is **ext4**
- Disk Anatomy
    - **Partition** - the piece of a disk that you can manage
    - **Partition Table** - tells the OS how the disk is partitioned
        - MBR (Master Boot Record), mainly used in Win OS, old school
        - GPT (GUID Partition Table), newer better
- Windows:disk partitioning and formatting a filesystem
    - **Disk Management** utility
    - **Diskpart** - terminal based tool
- Mounting & unmounting a filesystem
    - **Mounting** - making something accessible to the computer, like a filesystem or a hard disk
- Linux: disk partitioning and formatting a filesystem
    - **Parted** tool

        - Sudo parted -l == list out disks info
    - Sudo **mkfs** tool for formatting filesystem
- Linux: Mounting & unmounting a filesystem
    - Sudo **mount** tool, most OS's will do it automatically
    - Sudo **umount** == unmounts the disk
- Windows: swap
    - **Virtual memory:** how our OS provides the physical memory available in our computer (like RAM) to the applications that run on the computer
    - Located in system properties advanced tabs
- Linux: Swap
    - **Swap space** - in linux, the dedicated area of the hard drive used for virtual memory
- Windows Files:
    - NTFS > utilized **MFT (master file table)**
- Windows: Disk usage:
    - **Disk defragmenter** tool
    - The idea behind disk **defragmentation** is to take all the files stored on a given disk, and reorganize them into neighboring locations
- Windows File System repair:
    - **Data Buffer**: a region of RAM that's used to temporarily store data while it's being moved around
    - Command: **chkdsk**
- Linux File System Repair:
    - sudo **fsck**

Process Management

- Programs vs Processes
    - **Programs** - the applications that we can run, like the Chrome web browser
    - **Processes** - programs that are running
    - **PID** = process ID

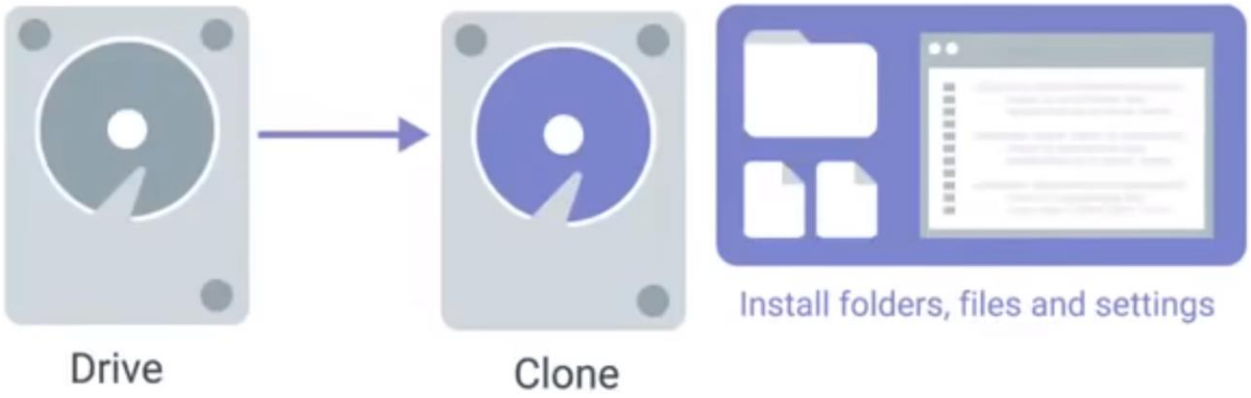
- Windows: process creation & termination
    - To start in cmd === (program name).exe
    - To kill in cmd === **taskkill /pid (process number)**
- Linux: process creation & termination
    - When you start up your computer the kernel creates a process called **init**, which has a **PID of 1**
- Windows: reading process information

    - Task Manager
        - Get PID by clicking on Details tab
    - In cmd , use **tasklist** to show all running processes
        - **Get-Process** in powershell
- Linux: reading process information
    - In shell: **ps -x**
        - R == running, T == stopped, S == interruptible sleep
    - In shell: **ps -ef** ; for all processes even by other users
- Windows: managing processes
    - **Process Explorer** - a utility Microsoft created to let IT Support specialists, system admins, and other users look at running processes (must be downloaded from microsoft website)
- Linux: managing processes
    - Terminate processes using **kill** command; kill (PID)
    - kill **-TSTP** (PID) == pause the process; kill **-CONT** (PID) == continue
- Windows resource monitoring
    - **Resource monitor**
    - In powershell: Get-Process
- Linux resource monitoring
    - **Top** command ; Q key to quit
    - **uptime** command to see machine uptime info
    - **lfos** == list open files and what processes are using them

Operating Systems in Practice

- Remote Access:
    - Remote connection & SSH:
        - **Remote connection** allows us to manage multiple machines from anywhere in the world
        - **Secure shell (SSH)** - a protocol implemented by other programs to securely access one computer from another
        - **Virtual private network (VPN)** - allows you to connect to a private network, like your work network, over the internet
    - Remote connection on Windows
        - Through powershell: https://www.howtogeek.com/336775/how-to-enable-and-use-windows-10s-built-in-ssh-commands/
        - **PuTTY** - a free, open source software that you can use to make remote connections through several network protocols, including SSH
        - **RDP**
    - Remote connection file transfer
        - **Secure copy (SCP)** - a command you can use in Linux to copy files between computers on a network (**WinSCP** for Windows)
            - scp (file) user@(IP address)
        - Fir Windows, Putty supports SCP; PSCP
            - Windows has Shared folders
            - From cmd, use **net share** command
- Virtualization
        - **Virtual instance** : a single virtual machine
- Logging

    - System Monitoring
        - **Logging** - the act of creating log events
    - The Windows **Event Viewer**
        - eventvwr.msc
        - Utilize custom views and filtering capabilities
    - Linux logs:
        - stored in **/var/log** directory
            - /var, var stands for **Variable**, so files that are constantly changing are kept in this directory
        - /var/log/syslog file logs everything, usually the first stop
        - **logrotate** tool
    - Working with logs
        - Search for **errors**: less var/log/syslog | grep error (searches log for errors)
- Operating System Deployment
    - Imaging Software
        - **Imaging**: to format a machine with an image of another machine, includes everything - from the OS to the settings
    - Deployment methods
        - Disc cloning tools, i.e. Clonezilla



        - Network initiated deployments - can utilize scripts; keep hardware standardization