LINUX

BY:-Vivek Kumar

History

- Many events led up to creating the first Linux kernel and, ultimately, the Linux operating system (OS), starting with the Unix operating system's release by Ken Thompson and Dennis Ritchie (whom both worked for AT&T at the time) in 1970. The Berkeley Software Distribution (BSD) was released in 1977, but since it contained the Unix code owned by AT&T, a resulting lawsuit limited the development of BSD. Richard Stallman started the GNU project in 1983. His goal was to create a free Unix-like operating system, and part of his work resulted in the GNU General Public License (GPL) being created. Projects by others over the years failed to result in a working, free kernel that would become widely adopted until the creation of the Linux kernel.

- At first, Linux was a personal project started in 1991 by a Finnish student named Linus Torvalds. His goal was to create a new, free operating system kernel. Over the years, the Linux kernel has gone from a small number of files written in C under licensing that prohibited commercial distribution to the latest version with over 23 million source code lines (comments excluded), licensed under the GNU General Public License v2.

- Linux is available in over 600 distributions (or an operating system based on the Linux kernel and supporting software and libraries). Some of the most popular and well-known being Ubuntu, Debian, Fedora, OpenSUSE, elementary, Manjaro, Gentoo Linux, RedHat, and Linux Mint.

- Linux is generally considered more secure than other operating systems, and while it has had many kernel vulnerabilities in the past, it is becoming less and less frequent. It is less susceptible to malware than Windows operating systems and is very frequently updated. Linux is also very stable and generally affords very high performance to the end-user. However, it can be more difficult for beginners and does not have as many hardware drivers as Windows.

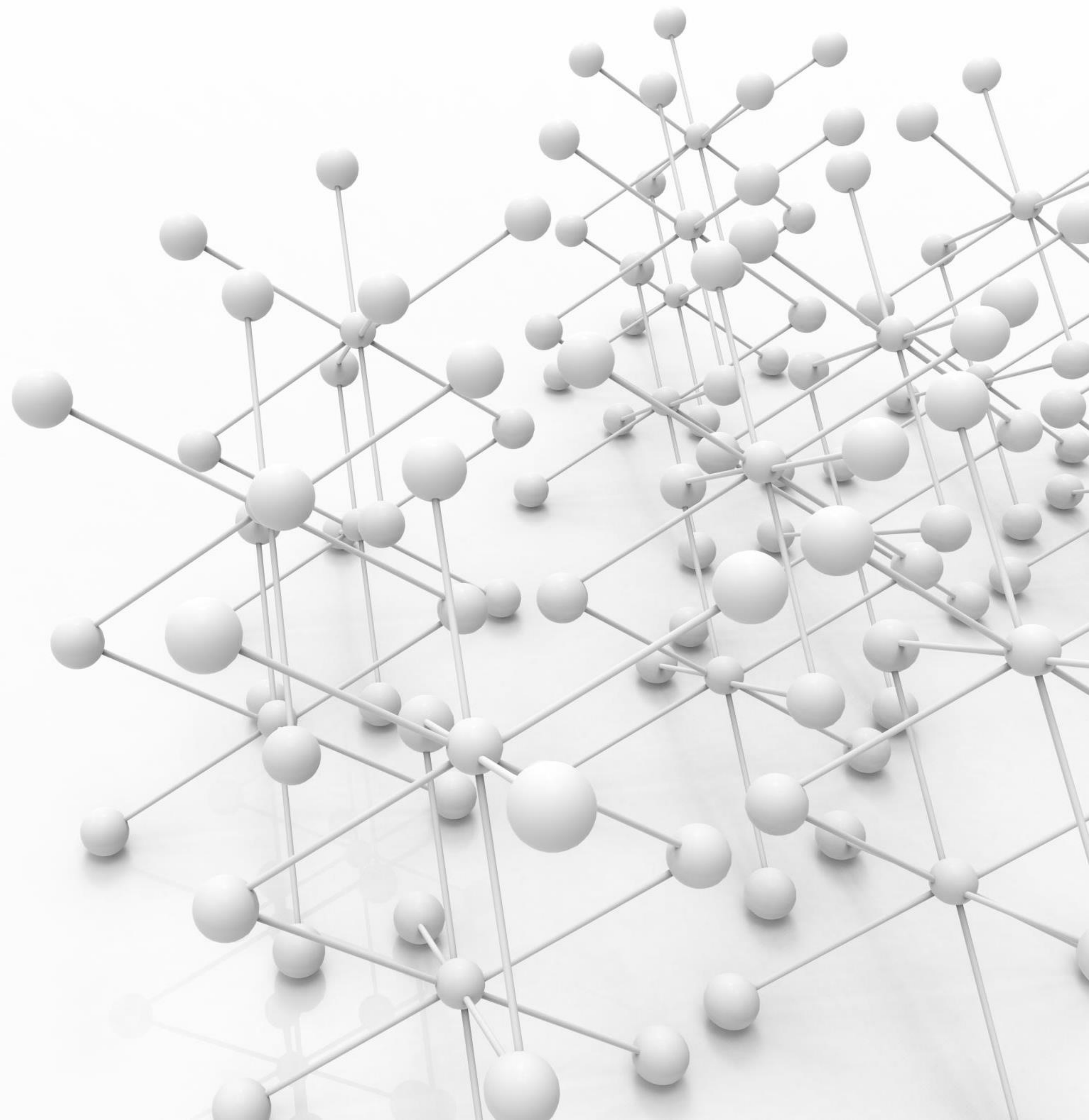
- Since Linux is free and open-source, the source code can be modified and distributed commercially or non-commercially by anyone. Linux-based operating systems run on servers, mainframes, desktops, embedded systems such as routers, televisions, video game consoles, and more. The overall Android operating system that runs on smartphones and tablets is based on the Linux kernel, and because of this, Linux is the most widely installed operating system.

- Linux is an operating system like Windows, iOS, Android, or macOS. An OS is software that manages all of the hardware resources associated with our computer. That means that an OS manages the whole communication between software and hardware. Also, there exist many different distributions (distro). It is like a version of Windows operating systems.

- With the interactive instances, we get access to the Pwnbox, a customized version of Parrot OS. This will be the primary OS we will work with through the modules. Parrot OS is a Debian-based Linux distribution that focuses on security, privacy, and development

File System Hierarchy

- The Linux operating system is structured in a tree-like hierarchy and is documented in the Filesystem Hierarchy Standard (FHS). Linux is structured with the following standard top-level directories:



/

- The top-level directory is the root filesystem and contains all of the files required to boot the operating system before other filesystems are mounted as well as the files required to boot the other filesystems. After boot, all of the other filesystems are mounted at standard mount points as subdirectories of the root.

/bin

- **Contains essential command binaries.**

/boot

- **Consists of the static bootloader, kernel executable, and files required to boot the Linux OS.**

/dev

- Contains device files to facilitate access to every hardware device attached to the system.

/etc

- Local system configuration files. Configuration files for installed applications may be saved here as well.

/home

- **Each user on the system has a subdirectory here for storage.**

/lib

- **Shared library files that are required for system boot.**

/media

- External removable media devices such as USB drives are mounted here.

/mnt

- **Temporary mount point for regular filesystems.**

/opt

- Optional files such as third-party tools can be saved here.

/root

- The home directory for the root user.

/sbin

- **This directory contains executables used for system administration (binary system files).**

/tmp

- The operating system and many programs use this directory to store temporary files. This directory is generally cleared upon system boot and may be deleted at other times without any warning.

/usr

- Contains executables, libraries, man files, etc.

/var

- This directory contains variable data files such as log files, email in-boxes, web application related files, cron files, and more.

Linux Distributions

- **Linux distributions - or distros - are operating systems based on the Linux kernel. They are used for various purposes, from servers and embedded devices to desktop computers and mobile phones. Each Linux distribution is different, with its own set of features, packages, and tools. Some popular examples include:**

- [Ubuntu]
- [Fedora]
- [CentOS]
- [Debian]
- [Red Hat Enterprise Linux]

- **Many users choose Linux for their desktop computers because it is free, open source, and highly customizable. Ubuntu and Fedora are two popular choices for desktop Linux and beginners. It is also widely used as a server operating system because it is secure, stable, and reliable and comes with frequent and regular updates. Finally, we, as cybersecurity specialists, often prefer Linux because it is open source, meaning its source code is available for scrutiny and customization. Because of such customization, we can optimize and customize our Linux distribution the way we want and configure it for specific use cases only if necessary.**
- **We can use those distros everywhere, including (web) servers, mobile devices, embedded systems, cloud computing, and desktop computing. For cyber security specialists, some of the most popular Linux distributions are but are not limited to:**

- **The main differences between the various Linux distributions are the included packages, the user interface, and the tools available. Kali Linux is the most popular distribution for cyber security specialists, including a wide range of security-focused tools and packages. Ubuntu is widespread for desktop users, while Debian is popular for servers and embedded systems. Finally, red Hat Enterprise Linux and CentOS are popular for enterprise-level computing.**

Debian

- Debian is a widely used and well-respected Linux distribution known for its stability and reliability. It is used for various purposes, including desktop computing, servers, and embedded system. It uses an Advanced Package Tool (apt) package management system to handle software updates and security patches. The package management system helps keep the system up-to-date and secure by automatically downloading and installing security updates as soon as they are available. This can be executed manually or set up automatically.

- **Debian can have a steeper learning curve than other distributions, but it is widely regarded as one of the most flexible and customizable Linux distros. The configuration and setup can be complex, but it also provides excellent control over the system, which can be good for advanced users. The more control we have over a Linux system, the more complex it feels to become. However, it just feels that way compared to the options and possibilities we get. Without learning it with the required depth, we might spend way more time configuring “easy” tasks and processes than when we would learn to use a few commands and tools more in-depth. We will see it in the Filter Contents and Find Files and Directories sections.**

- **Stability and reliability are key strengths of Debian. The distribution is known for its long-term support releases, which can provide updates and security patches for up to five years. This can be especially important for servers and other systems that must be up and running 24/7. It has had some vulnerabilities, but the development community has quickly released patches and security updates. In addition, Debian has a strong commitment to security and privacy, and the distribution has a well-established security track record. Debian is a versatile and reliable Linux distribution that is widely used for a range of purposes. Its stability, reliability, and commitment to security make it an attractive choice for various use cases, including cyber security.**

Introduction to Shell

Getting Help

- Man (manual)
- --help (for getting help)
- -h (help)
- Whatis
- https://explainshell.com/

System Information

- **whoami Displays current username.**
- **hostname Sets or prints the name of current host system.**
- **uname Prints basic information about the operating system name and system hardware.**
- **Pwd Returns working directory name.**
- **ifconfig The ifconfig utility is used to assign or to view an address to a network interface and/or configure network interface parameters.**
- **ip Ip is a utility to show or manipulate routing, network devices, interfaces and tunnels.**

- **Top – show running services**

- **Kill – kill the task**

- **W – login details**

Navigation

- Ls
- dir
- Cd
- Cd ..

Complete ls

- **Ls –a (to see hide files)**
- **Ls –l (to see the permissions of file)**
- **Ls –t (shorted by modification date)**
- **Ls –r (list file in reversed fashion)**
- **Ls –i (show index node number)**

Linux Links

- **iNode :**
- **•	Every file in the system has an inode(Index Node)**
- **•	Contains all the file information except the file contents & name.**
- **•	Just like a personal ID or a passport(Without a name!)**

- **They contain the following -**
- **➢	Inode number**
- **➢	File size**
- **➢	Owner information**
- **➢	Permissions**
- **➢	File type**
- **➢	Number of links etc.**

- **Types of Links :**

- **1. Soft Links :**
- **✓ Just like a shortcut in Window**
- **✓ It is a pointer to the original file**
- **✓ Different iNode number**
- **✓ Smaller file size**

- **Note :- If we delete the original file then softlink will become useless!**

- **2. Hard Links :**
- **✓ Different name of the same file**
- **✓ Same file size**
- **✓ Same iNode number**

- **Note :- If the original File is deleted, the Hard link will still contain the data that were in the original file.**

Creating hard link and soft link

- Ln (for creating link)
- Ln (then file name) (then new file name)
- If inode number is same then it’s a hard link
- Ln –s (file name) (new file name)

- You create a soft link for dir

Working with Files and Directories

- **Touch**
- **Mkdir**
- **rmdir**
- **Rm**
- **File (**Determine the type of a file)
- **Tree**
- **Cp give path (ex /home/kali/more path)**
- **Mv give path (ex /home/kali/more path)**
- **For rename we use mv (file name) (new file name)**

Change extension & space in file & more commands

- Mv (filename) (new file) for changing extension
- Mkdir “file name” (for space in file name)
- Mkdir “   file name “ (give more space for getting space in dir)

- 2 method
- Mkdir “filename \complete name”

- Echo

Editing Files

- There are several ways to edit a file. One of the most common text editors for this is Vi and Vim. More rarely, there is the Nano editor.

- **Sudo su –grant root privileges**

- **Cat – show contant of file**

- **Nano –linux file editor**

- **Vim –linux file editor**

- **Gedit –file editor software**

- **Chmod –change directory permissions**

Find Files and Directories

- **Which – (locate a command) *limited value**
- **Find – (search for files in a directory hierarchy)**
- **Example find . –name (filename)**
- **Find . –type f –name (filename)**
- **Locate – (list files in databases that match a pattern)**

Filter Contents

- **Wc**
- **ex-Line,sentence,words**
- **Sort**
- **Short –r**
- **Short –n (for numeric shorting)**
- **Grep**
- **cat filename | Grep (text)**

Permission Management

- **Ls –l**
- **Chmod**
- **(r) - Read**
- **(w) - Write**
- **(x) – Execute**

- drwxr
- - (file)
- D – directory
- L – link
- Owner
- Group
- User
- Rwx – (read write execute)
- Chmod +ugo
- Chmod + -

SUID & SGID

- Besides assigning direct user and group permissions, we can also configure special permissions for files by setting the Set User ID (SUID) and Set Group ID (SGID) bits. These SUID/SGID bits allow, for example, users to run programs with the rights of another user. Administrators often use this to give their users special rights for certain applications or files. The letter "s" is used instead of an "x". When executing such a program, the SUID/SGID of the file owner is used.

- It is often the case that administrators are not familiar with the applications but still assign the SUID/SGID bits, which leads to a high-security risk. Such programs may contain functions that allow the execution of a shell from the pager, such as the application "journalctl."

- If the administrator sets the SUID bit to "journalctl," any user with access to this application could execute a shell as root. More information about this and other such applications can be found at GTFObins.

Suid

- Chmod u+s then filename
- Chmod u-s then filename
- Cd Desktop
- Ls – la /usr/bin/passwd
- First create a user and entre on it
- Ls –l /root
- Ls –l /usr/bin/ls
- Chmod u+s /usr/bin/ls
- Gtfobins use for explotitaion
- Cat /etc/passwd

Sgid

Useradd new
Useradd new1
Gropadd bit
Usermod –aG bit new
And 2 usr new1
/home
Mkdir test
Chown root:bit test/
Ll
Chmod 2775 test
Ll
Su new
Cd test
Mkdir hi
Touch hi
Path is your test
Cd test
Touch hi2.txt
Mkdir hi2
Sudo su
Touch nake files
Go to root and see the bit

4 uid
2 gid
1 sticky

Sticky Bit

- Sticky bits are a type of file permission in Linux that can be set on directories. This type of permission provides an extra layer of security when controlling the deletion and renaming of files within a directory. It is typically used on directories that are shared by multiple users to prevent one user from accidentally deleting or renaming files that are important to others.
- For example, in a shared home directory, where multiple users have access to the same directory, a system administrator can set the sticky bit on the directory to ensure that only the owner of the file, the owner of the directory, or the root user can delete or rename files within the directory. This means that other users cannot delete or rename files within the directory as they do not have the required permissions. This provides an added layer of security to protect important files, as only those with the necessary access can delete or rename files. Setting the sticky bit on a directory ensures that only the owner, the directory owner, or the root user can change the files within the directory.

- When a sticky bit is set on a directory, it is represented by the letter “t" in the execute permission of the directory's permissions. For example, if a directory has permissions “rwxrwxrwt", it means that the sticky bit is set, giving the extra level of security so that no one other than the owner or root user can delete or rename the files or folders in the directory.
- In this example, we see that both directories have the sticky bit set. However, the reports folder has an uppercase T, and the scripts folder has a lowercase t.

- If the sticky bit is capitalized (T), then this means that all other users do not have execute (x) permissions and, therefore, cannot see the contents of the folder nor run any programs from it. The lowercase sticky bit (t) is the sticky bit where the execute (x) permissions have been set.

Sticky bit (set on dir) 1

```
Cat /etc/passwd
/home
Pwd
Mkdir sticky
Chmod 777 sticky/
Ll
Su new
Cd sticky
Mkdir a
Touch a.txt
Su new 1
Touch b.txt
Mkdir b
Rm a.txt
/home
Ll
Chmod +t sticky
Su new1
Rmdir a
Rm a.txt
```

Protect files

User Management

- Sudo
- Su
- Useradd
- Userdel
- Addgroup
- Delgroup
- Passwd

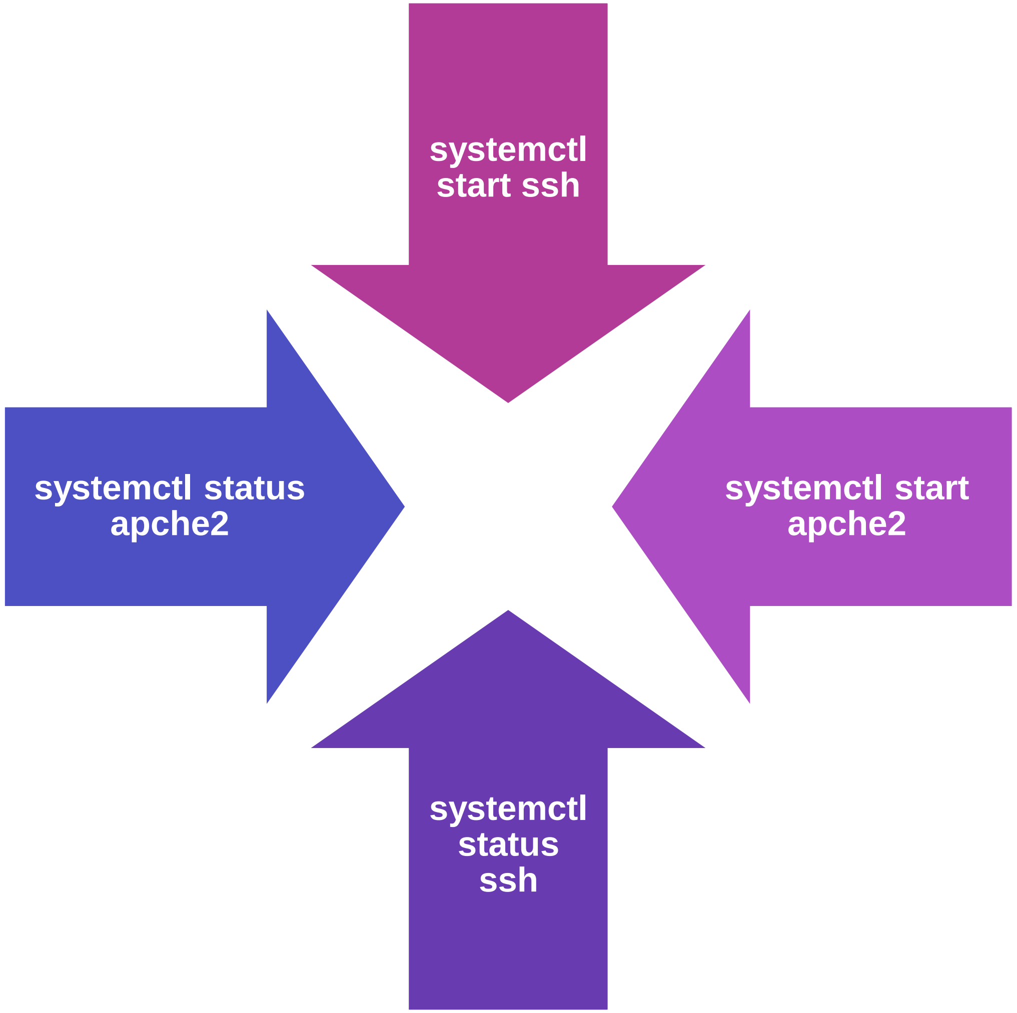
useradd

- Useradd then username
- Grep (username) /etc/passwd
- Cat naman /etc/passwd
- Passwd
- Del user

Package Management

- Apt
- Pip
- Git
- wget

Service and Process Management



systemctl start ssh

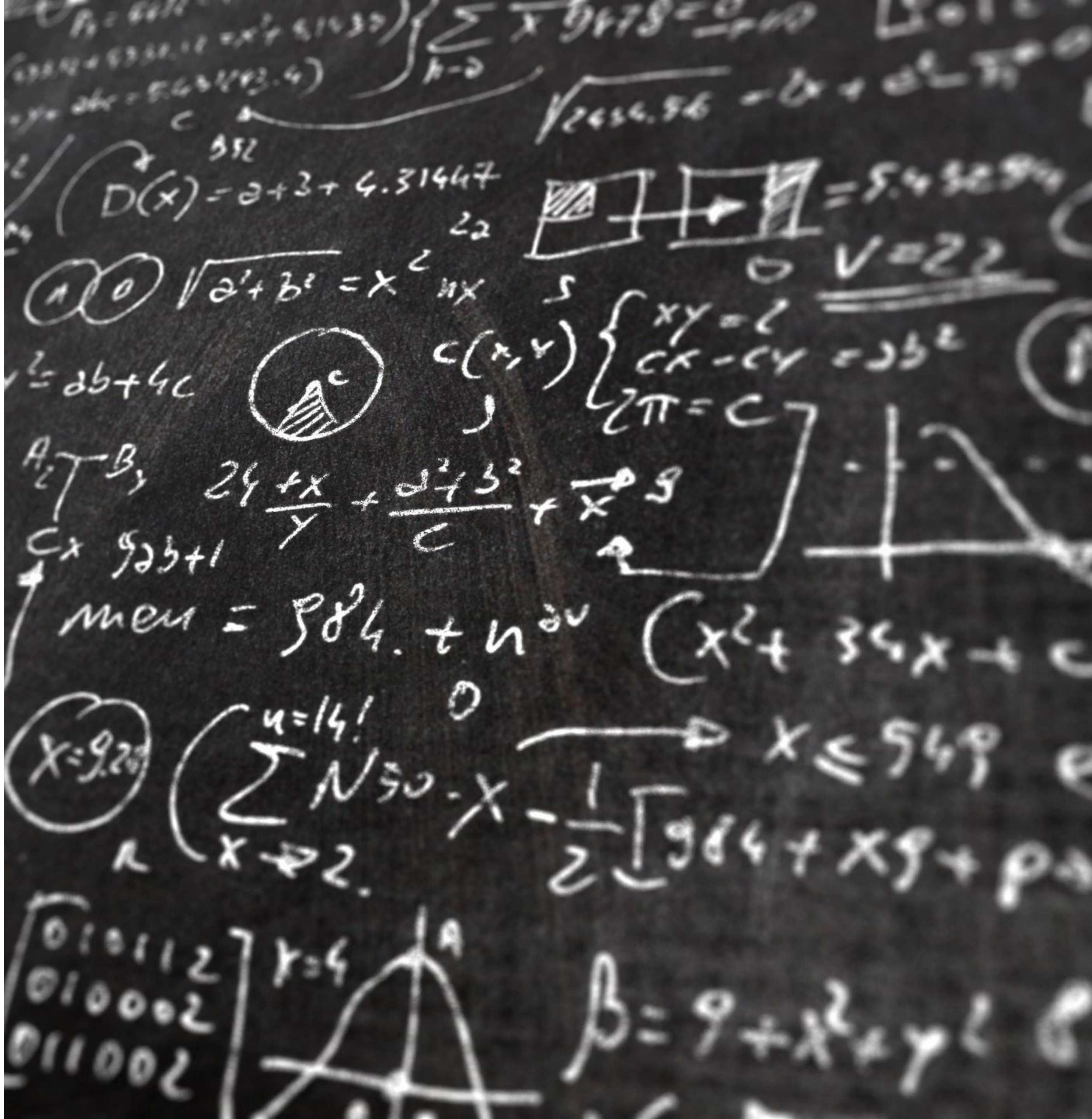
systemctl status apche2

systemctl start apche2

systemctl status ssh

Alias command

- Type (is use for which type of command is this)
- Alias (commandname) =“”

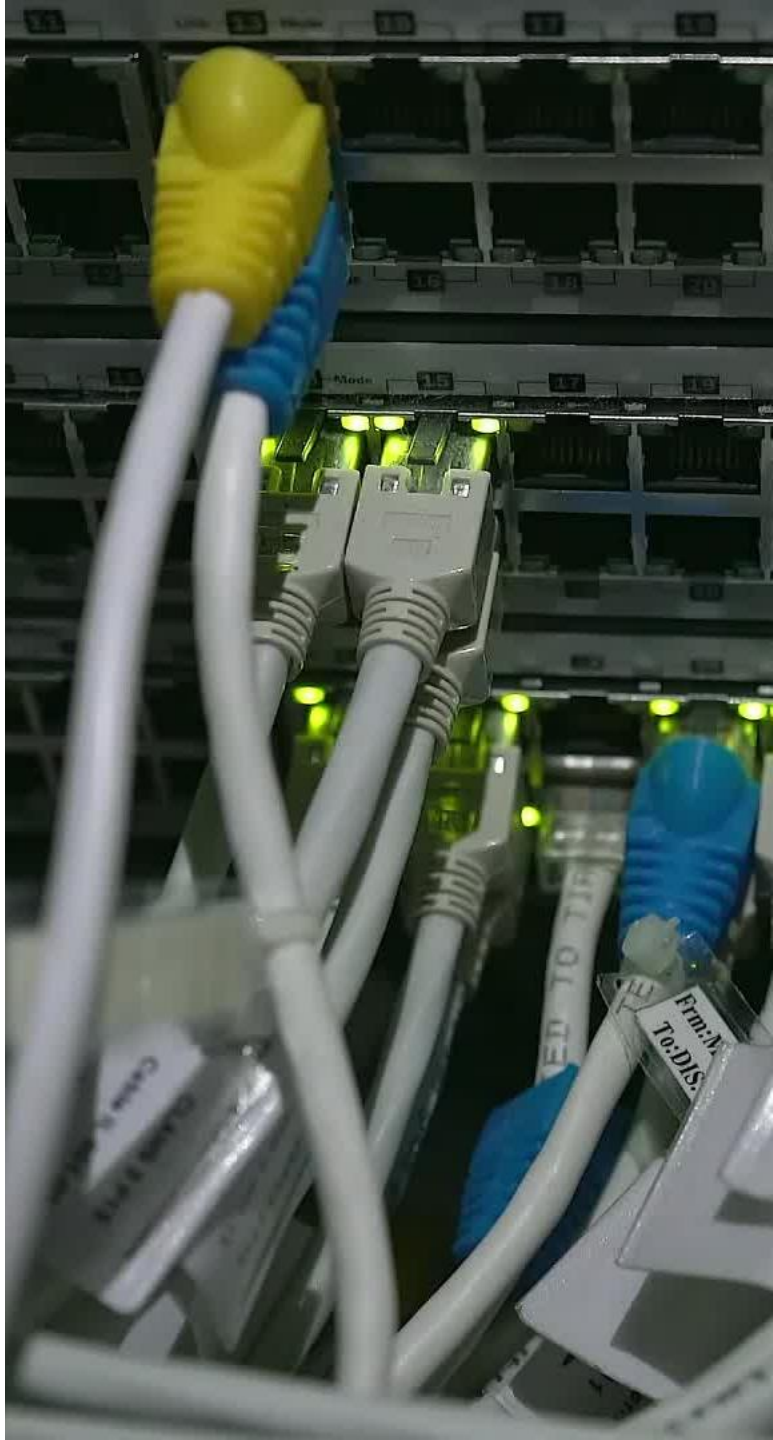


Network Services

- Ssh

- Apche

- vpn



Network Configuration

- Ifconfig
- Ip a

Shortcuts

- [CTRL] + A - Move the cursor to the beginning of the current line.
- [CTRL] + E - Move the cursor to the end of the current line.
- [CTRL] + [←] / [→] - Jump at the beginning of the current/previous word.
- [ALT] + [TAB] - Switch between opened applications.
- Ctrl+c
- [CTRL] + [+] - Zoom in.
- [CTRL] + [-] - Zoom out.