# Linux for Cyber Security

Class 00

MD Mahmidul Hasan

Sonargaon University Programing Club

# What is Linux?

First and foremost, Linux is an operating system. An operating system is simply a collection of software that manages hardware resources and provides and environment where applications can run. The operating system allows applications to store information, send documents to printers, printers, interact interact with users and other things.

Linux is also a kernel. Typically, when the term “Linux” is used, it refers to the Linux operating system as a whole. However, it can refer to just the Linux kernel as well.

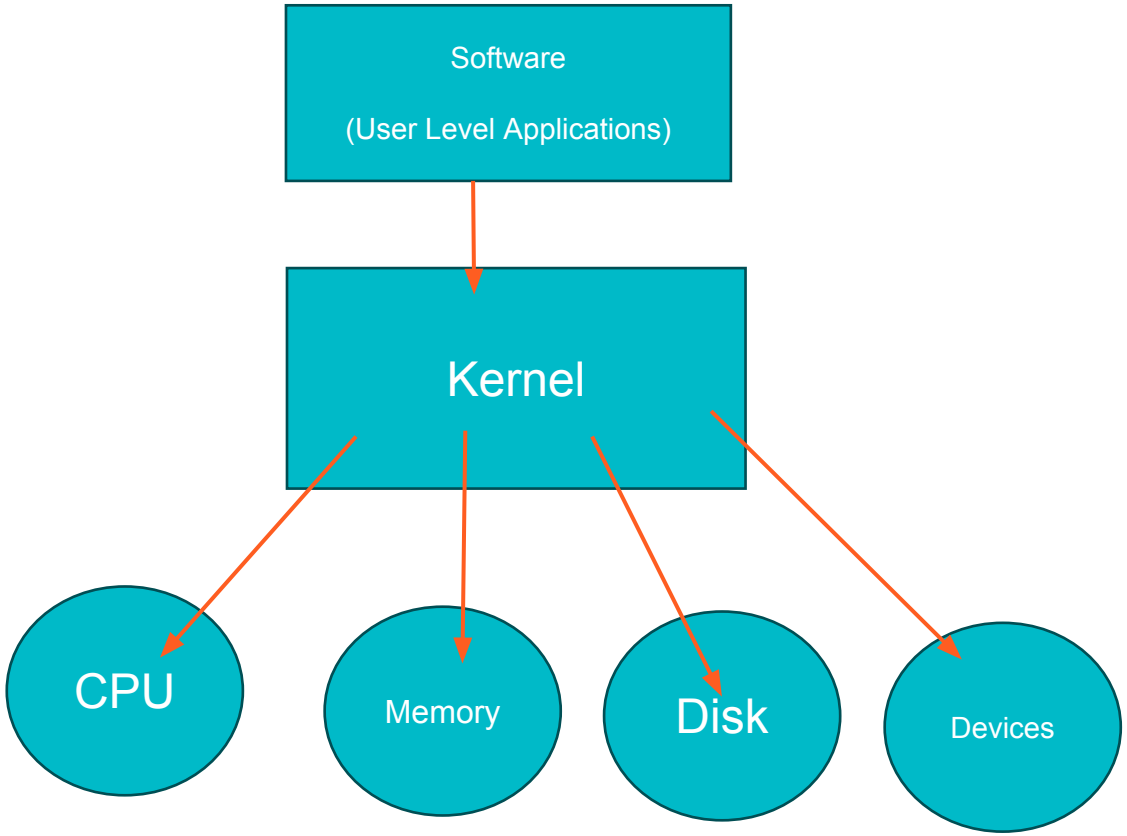
# Who invented Linux?

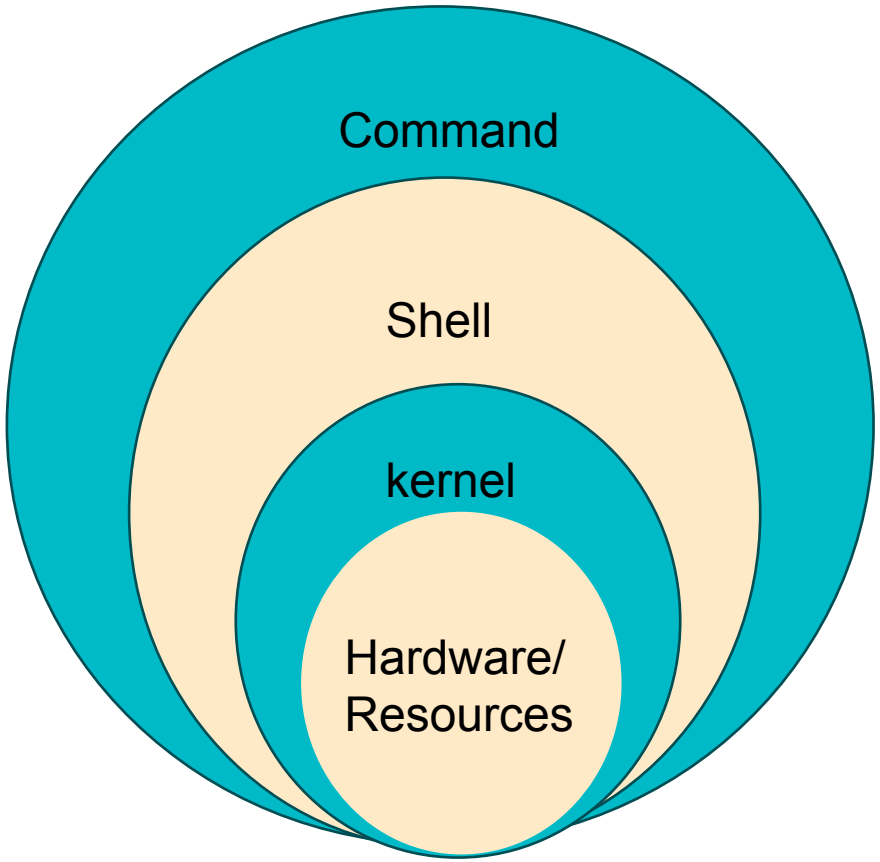
Linus Torvalds created Linux when he was a student at the University of Helsinki studying computer science. In early 1991 he purchased an IBM- compatible personal computer that come with the MS-DOS operating system.

Linus wasn't satisfied with MS-DOS and wanted to use a UNIX operating system like he was accustomed to at the University. When he set out to obtain a copy of UNIX for his personal use, he found that the least expensive UNIX he could buy was about $5,000 USD.

Driven by the desire to run a UNIX-like operating system on his personal computer, he set out to create Linux. Linus and over 100 developers worked on Linux over the next couple of years and in March of 1994, version 1.0 of the Linux kernel was released.

# Operating S. Operating S. vs Kernel



# Operating S. Operating S. vs Kernel

| Operating System | Kernel |
| --- | --- |
| It's a system program that provide interface between user and computer. | A kernel is the core component of OS. Its also a system software. It's a part of OS which convert user commands into machine language. |
| Interface between user and hardware | Interface between application and hardware. |
| Also provide protection and security. | Main purpose is memory management, disk management, process management and task management. |
| Single & Multiuse OS, Real-time OS, Distributed OS. | Monolithic and Micro Kernel. |
| First program to load when computer boots up. | First program to load when operating system loads. |

# Open Source

Linux is open source software. This means that anyone can use, copy, study and change the software in any way they chose so long as the source code is openly shared with others.

To date, thousands of people have made improvements to Linux. With Linux being free and open source software, it has lead to the rise of Linux distributions.

In every case, the source code is free, but in some cases, the distribution is not free,-the binaries, the compiled code in not free. For example, you have to pay a license in order to run Red Hat Enterprise Linux. However, Red Hat releases their source code for anyone to download.

Also, Linux is not a UNIX-derivative. It was written from scratch. However, many of the commands that are found in Linux are also found in UNIX. If you have any experience on UNIX system, you’re going to feel right at home on a Linux system.

# What’s a Distribution? (Linux)

A Linux distribution is the Linux Kernel and a collection of software that together, create an operating system. Each distribution has its own goals and areas of focus. Your choice of distribution will depend on what you are trying to accomplish.

There are distributions that are commercial. These commercial Linux distributions distributions are backed by corporations corporations and you can buy support support from them.

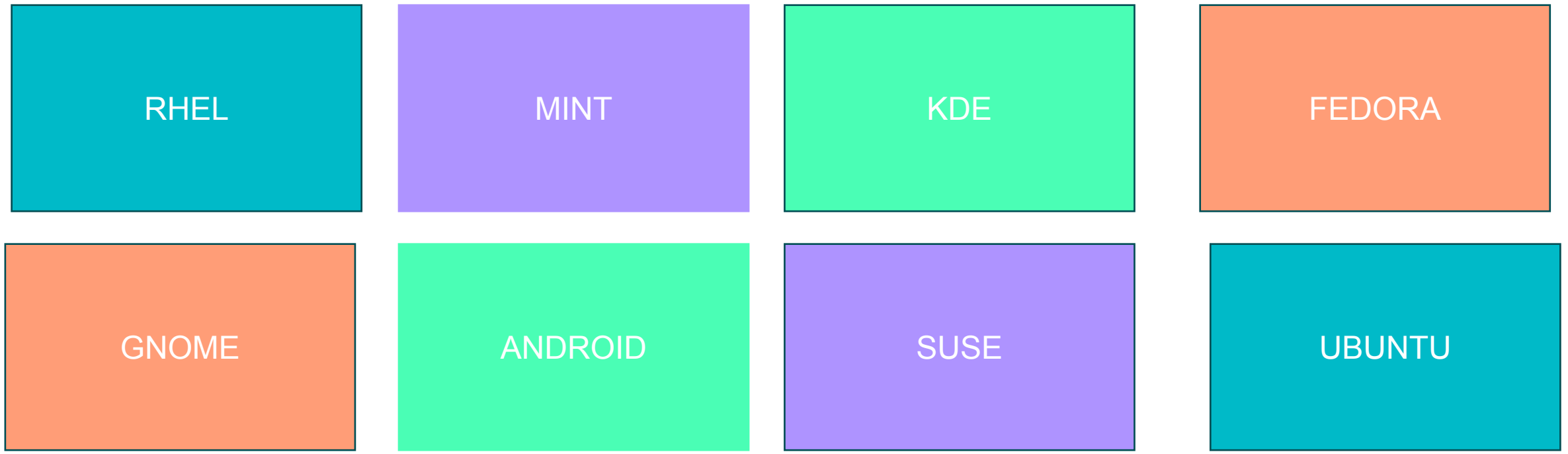
There are non-commercial Linux distributions. These are maintained by a community of volunteers.

You have Linux distro that are designed for server use, others that aredesigned for desktop use, some that are focus on research and science. There are others that are focused on multimedia production.

There are literally hundreds of Linux distributions.

# Linux Distributions

Example:



# RHEL (May 1995)


In 2003 Red Hat Linux merged with the community-based Fedora Project.

Introduced a graphical installer called Anaconda and Lokkit for configuring the firewall capabilities.

Developed by: Bob Young, Marce Ewing and Red Hat Inc.

# Fedora (November 2003)

Focuses on innovation, integrating new technologies early on and working

closely with Linux communities.

Linus Torvalds uses Fedora on all of his computers.

Developed by: Fedora Project. (Owned by Red Hat Inc.)

# Ubuntu (October 2004)


Community to open source development; encouraged to use free software, study how it works, improve upon it, and distribute it.

Named after the Southern African philosophy of Ubuntu (literally, “human- ness”.

Developed by: Mark Shuttleworth and Canonical Ltd.

# Debian (Sept. 1993)

debian

The Debian Project's policies focus on collaborative software development

and testing processes. (Kali Linux, Parrot)

New release every two years.

Developed by: Ian Murdock and the Debian Project.

# Android (Sept. 2008)

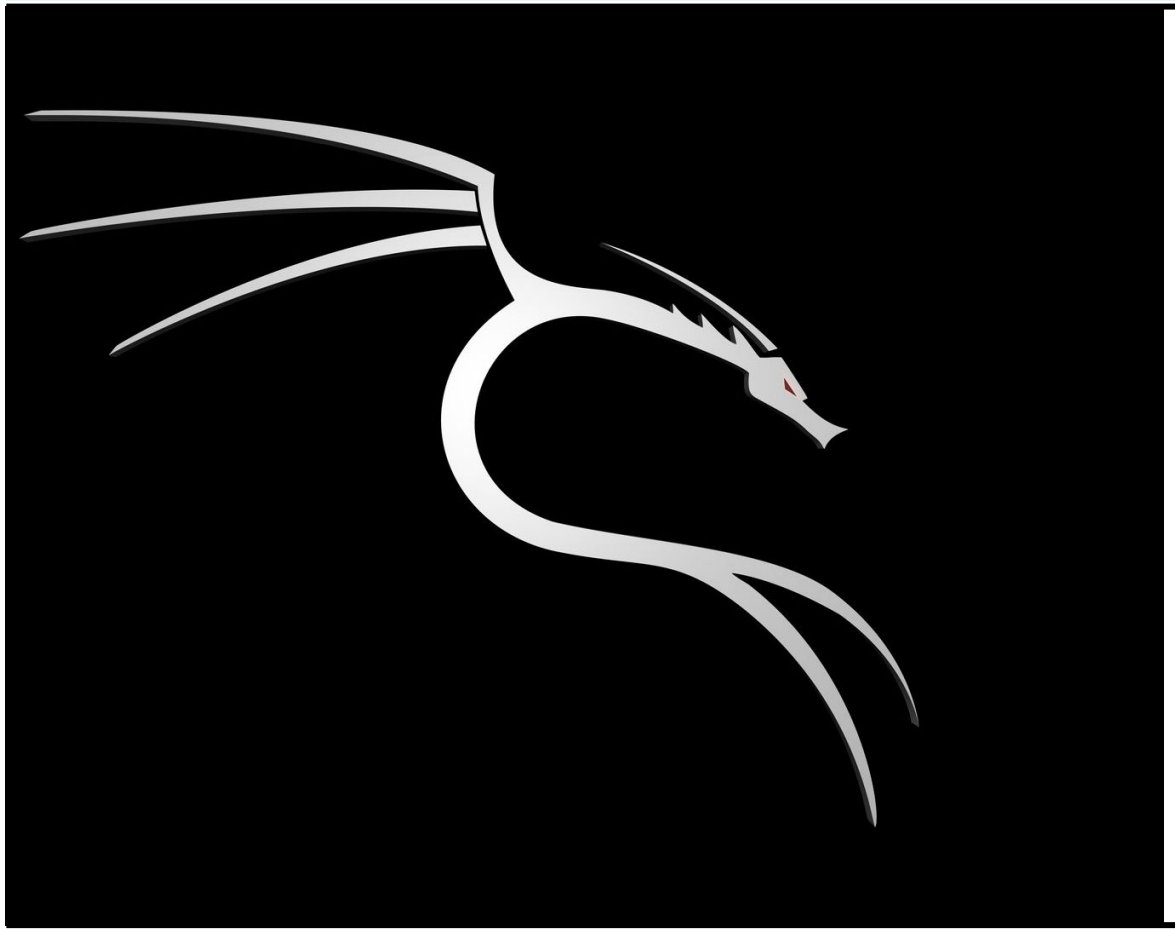
Android is designed primarily for touchscreen mobile devices such as

smartphones and tablet computers.

The most widely used mobile OS.

Developed by: Google and Open Handset Alliance.

# Kali Linux



The most advanced Penetration Testing Distribution.

More than 600 penetration testing tools included:

Free (as in beer) and always will be:

Kali Linux is an open-source, Debian-based Linux distribution geared

towards various information security tasks, such as Penetration Testing,

Security Research, Computer Forensics and Reverse Engineering.

# Why should we know Linux

In September 2008 Steve Ballmer (Microsoft CEO) claimed 60% of servers run Linux and 40% run Windows Server. According to IDC's report covering Q2 2013, Linux was up to 23.2% of worldwide server revenue.

Linux is used as: - Server (HTTP, FTP, DNS, File Server, etc)

- Desktop (It's a free alternative to Microsoft windows)

- Supercomputer Operating System:

--According to Wikipedia & top500.org over 95% of

Supercomputers use Linux as their host OS.

You can also find Linux distros in:

- Routers, Firewalls, Switch

- Smartphones (See Android)

- Gaming consoles (Sony PlayStation, Valve SteamBox)

# Linux File System

The Linux file-system structure is somewhat different from that of Windows. Linux doesn't have a physical drive (such as the C: drive) at the base of the file-system but uses a logical file-system instead. At the very top
of the file-system structure is /, which is often referred to as the root of thefile-system, as if it were an up

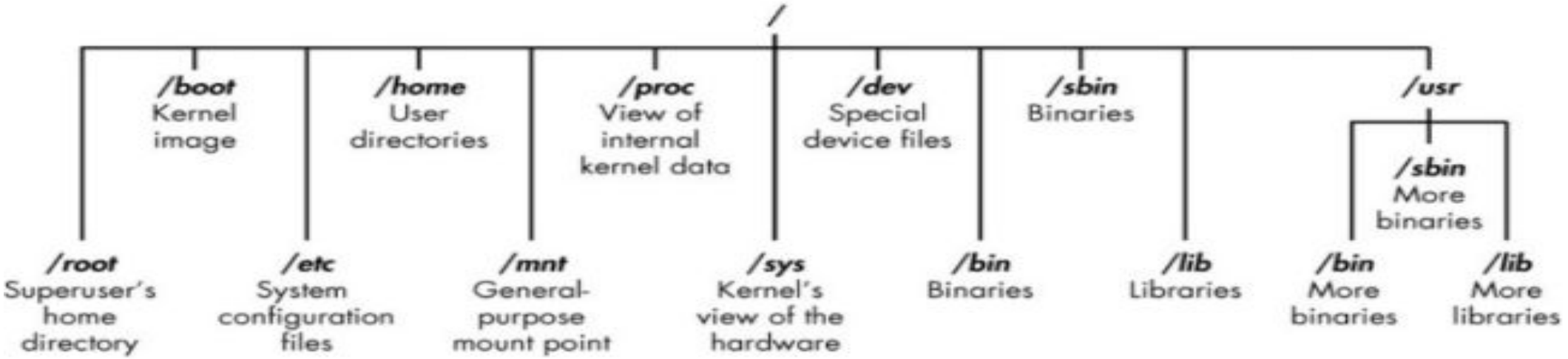



*Figure 1-4: The Linux filesystem*

# Getting Started

Binaries:

Ø Case Sensitivity:

Ø Directories:

Ø Home:

Ø Kali:

Ø Root:

Ø Script

Ø Terminal (CLI)

# Very Basic Command in Linux

- pwd
- whoami
- cd
- ls
- man
- --h or –help
- locate
- whereis
- find
- vim

# Modify file and directories

- Ps aux
- Ps aux | grep apache2
- Cat
- Touch newfile
- Mkdir newdirectory
- Cp oldfile /root..... (copy on this directory)
- Mv old_file_name new_file_name
- Rm file_name
- Rmdir directory_name
- Rm –r directory_name

# Text Manipulation

cat /etc/snort/snort.conf

head /etc/snort/snort.conf

tail /etc/snort/snort.conf

Head -20 /etc/snort/snort.conf

Tail -20 /etc/snort/snort.conf

nl /etc/snort/snort.conf

cat /etc/snort/snort.conf | grep output

nl /etc/snort.conf | grep output

cat /etc/snort/snort.conf | grep mysql

less /etc/snort/sonrt.conf

# Analyzing and Managing Network

- ifconfig
- iwconfig
- ifconfig eth0 192.168.11.12
- iconfig eth0 192.168.11.12 netmask 255.255.0.0 broadcast 192.16.11.1
- ifconfig eth0 down
- ifconfig eth0 up
- ip a
- Ip addr
- netstat –p
- netsat –s
- netstat –r

# Adding and Managing Software

- apt-get update
- apt-get upgrade
- apt-get update && upgrade
- vim /etc/apt/sources.list
- apt-get install synaptic
- apt-get remove synaptic

Installing package with github(GIT)

- www.github.com
- git clone https://www.gitbub.com/balle/bluediving.git
- ls –l

# File, User & Directory Permissions

Useradd

Userdel

# Process Management

Ps

Ps aux

Ps aux | grep msfconsole

Top

Kill 6994

Killall -9 zombieprocess

# Using & Using & Abusing Services

Service apache2 status

Service apache2 start

Service apache2 stop

Service apache2 restart

Services (ssh,mysql,webserver and others service)

# Compress
# Compress &
# Archive &
# Archive

tar cvf name.tar file_path

tar xvf name.tar file_path

gzip

gzip –d file_name

gunzip compressed_file_name

bzip2

bzip2 file_name

bunzip2 compressed_file_name

# Tryhackme content link

https://tryhackme.com/room/linuxfundamentalspart1

https://tryhackme.com/room/linuxfundamentalspart2

https://tryhackme.com/room/linuxfundamentalspart3

# Thank You