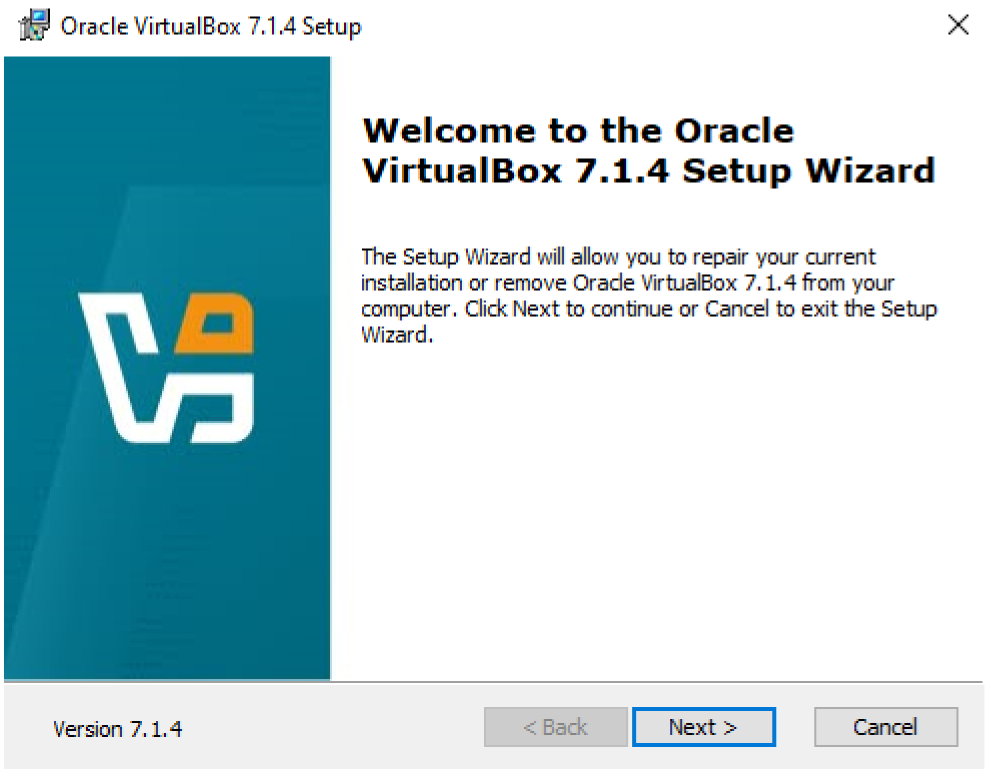
CYBER SECURITY CEH COURSE
Practical Work

17TH September 2025

Installation of Virtual Box:



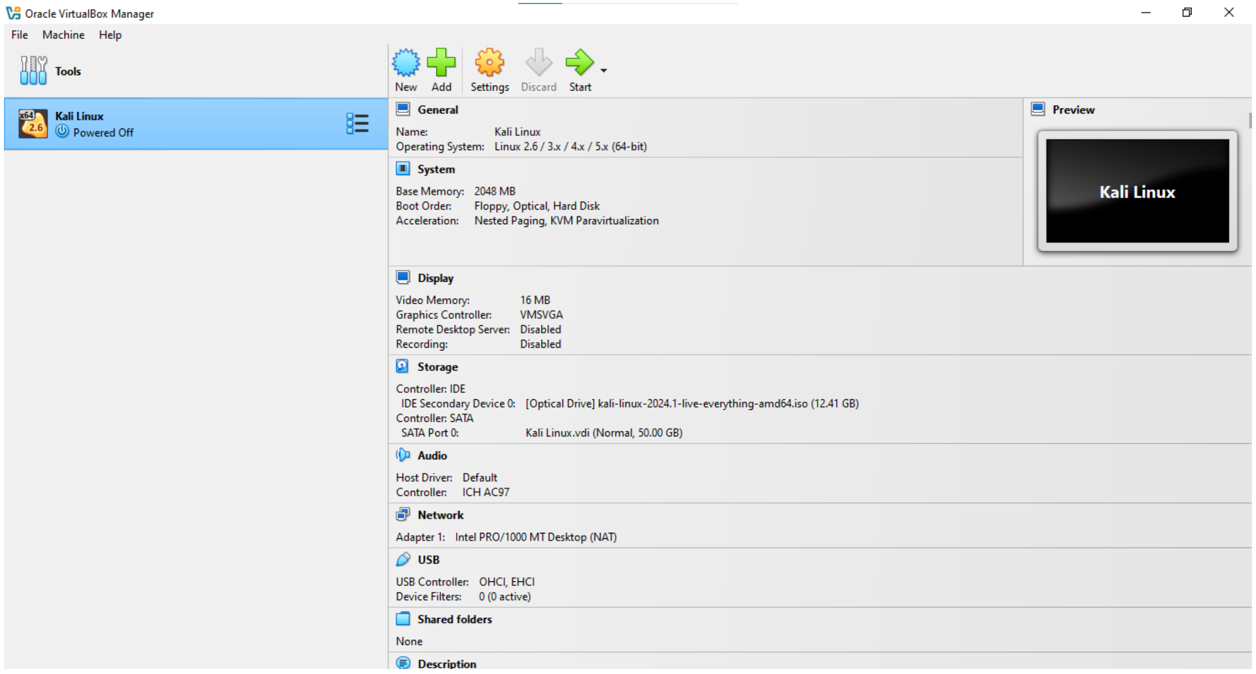
Oracle VirtualBox 7.1.4 Setup

Welcome to the Oracle VirtualBox 7.1.4 Setup Wizard

The Setup Wizard will allow you to repair your current installation or remove Oracle VirtualBox 7.1.4 from your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Version 7.1.4

After Installation:



General
Name: Kali Linux
Operating System: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)

System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] kali-linux-2024.1-live-everything-amd64.iso (12.41 GB)
Controller: SATA
SATA Port 0: Kali Linux.vdi (Normal, 50.00 GB)

Audio
Host Driver: Default
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

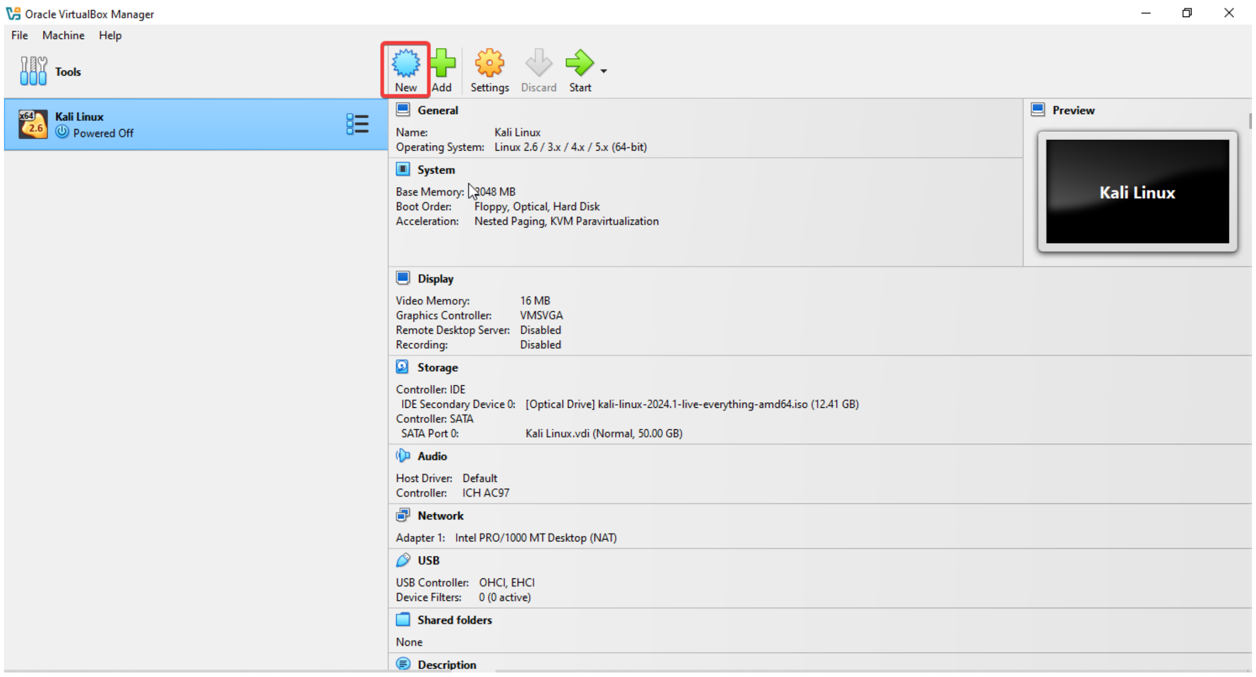
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders
None

Description

Installing Kali Linux:

Click the new Button



General
Name: Kali Linux
Operating System: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)

System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] kali-linux-2024.1-live-everything-amd64.iso (12.41 GB)
Controller: SATA
SATA Port 0: Kali Linux.vdi (Normal, 50.00 GB)

Audio
Host Driver: Default
Controller: ICH AC97

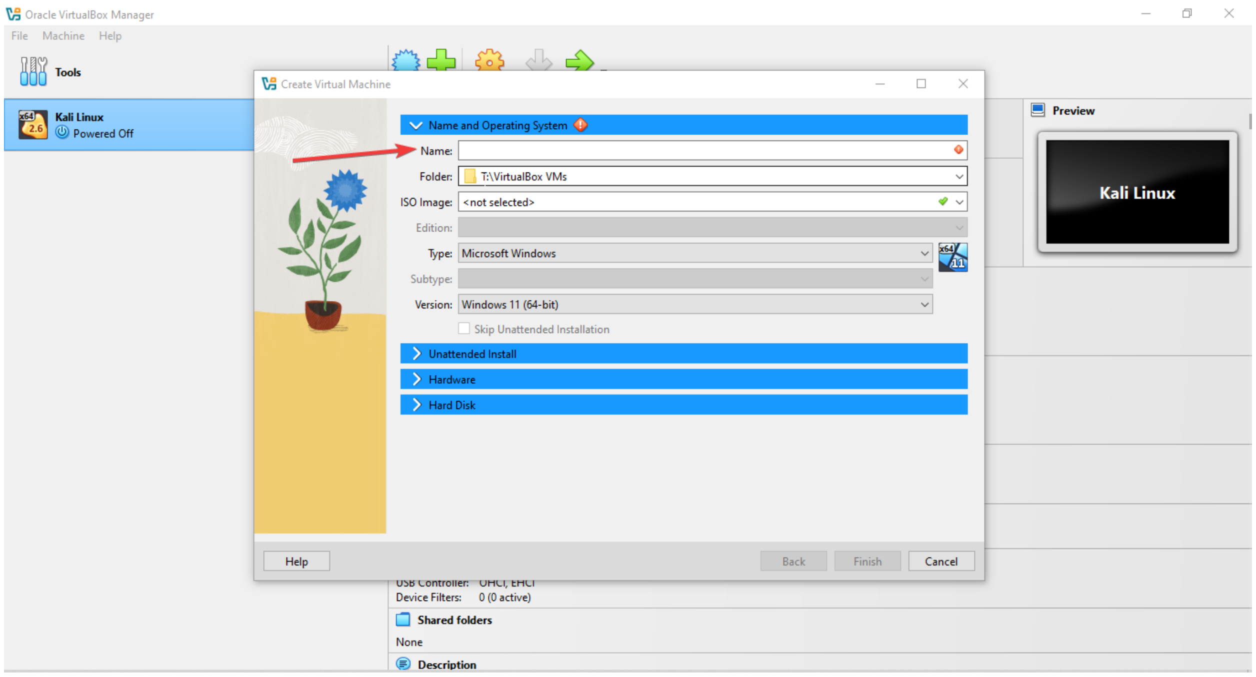
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders
None

Description

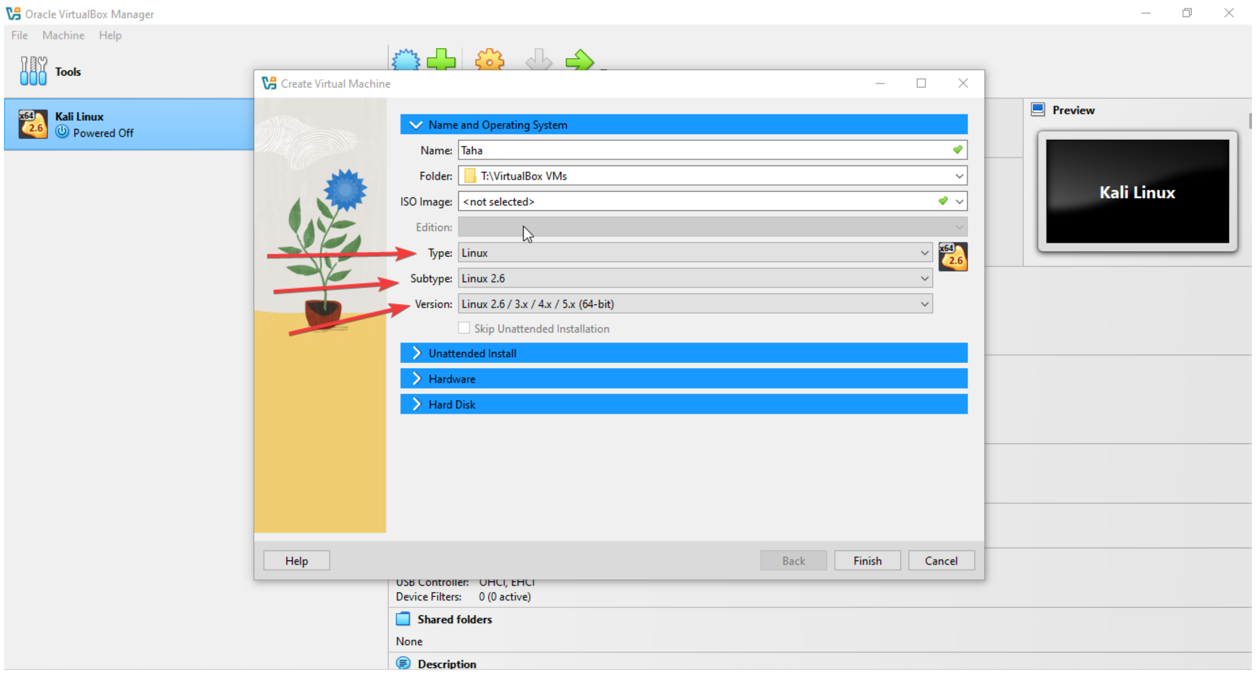
Give name anything you want:



Name:
Folder: T:\VirtualBox VMs
ISO Image: <not selected>
Edition:
Type: Microsoft Windows
Subtype:
Version: Windows 11 (64-bit)
Skip Unattended Installation

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)
None

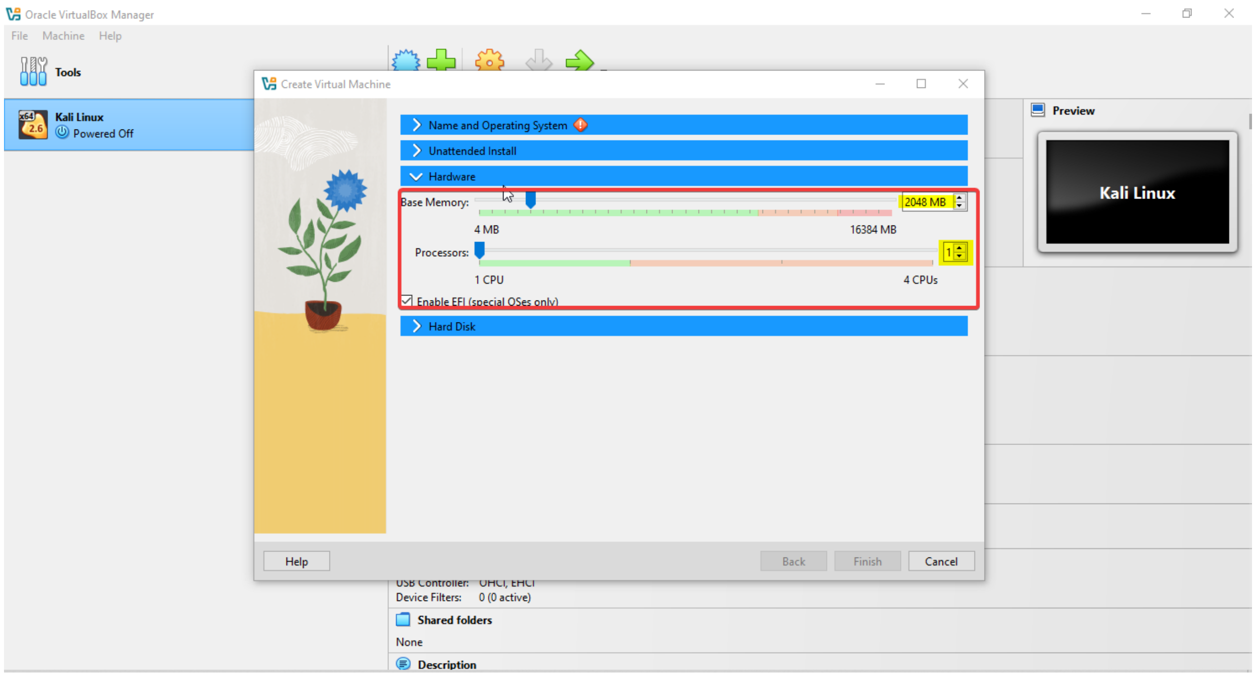
Select these options:



Name: Taha
Folder: T:\VirtualBox VMs
ISO Image: <not selected>
Edition:
Type: Linux
Subtype: Linux 2.6
Version: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)
Skip Unattended Installation

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)
None

Give Ram and CPU as follows:



Base Memory: 2048 MB

4 MB 16384 MB

Processors: 1

1 CPU 4 CPUs

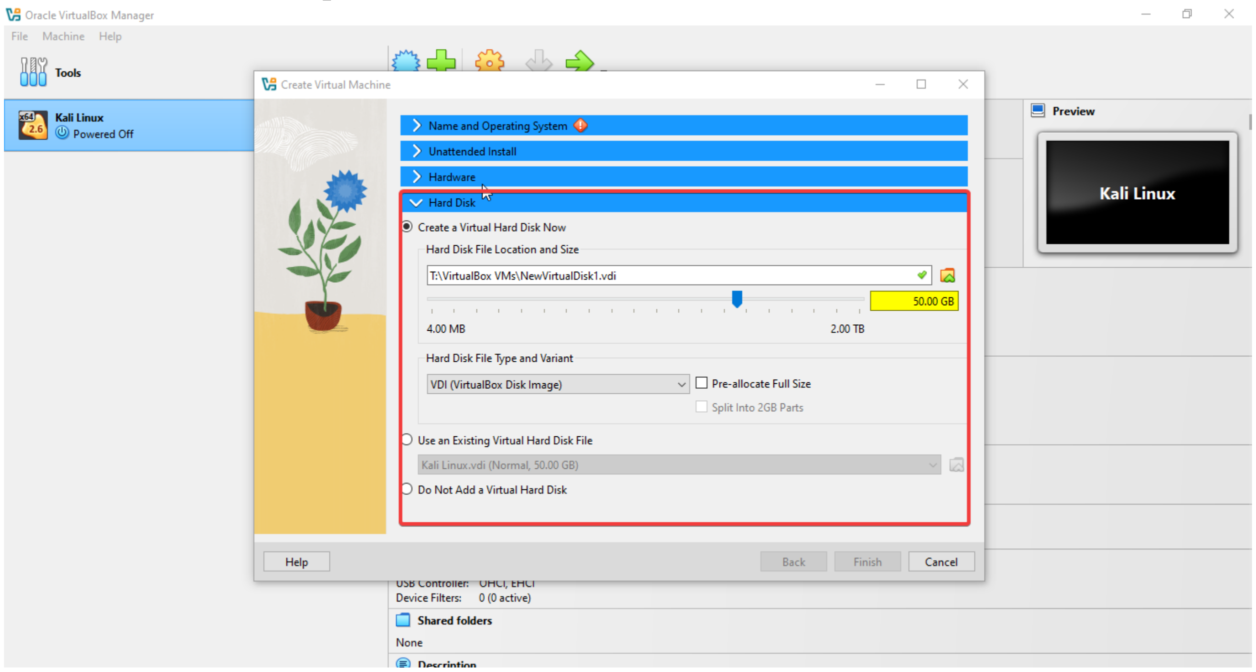
☑ Enable EFI (special OSes only)

USB Controller: OHCI, EHCI

Device Filters: 0 (0 active)

None

Allocate This much space:



● Create a Virtual Hard Disk Now

Hard Disk File Location and Size

T:\VirtualBox VMs\NewVirtualDisk1.vdi

50.00 GB

4.00 MB 2.00 TB

Hard Disk File Type and Variant

VDI (VirtualBox Disk Image) ☐ Pre-allocate Full Size

☐ Split Into 2GB Parts

○ Use an Existing Virtual Hard Disk File

Kali Linux.vdi (Normal, 50.00 GB)

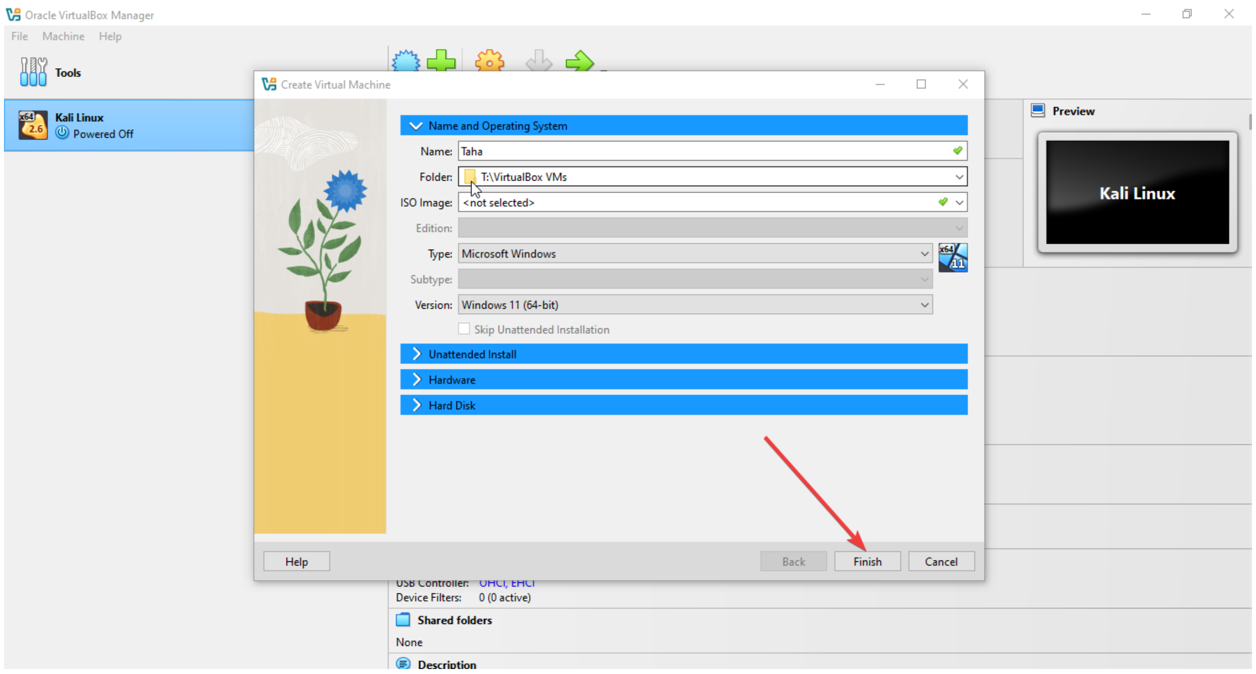
○ Do Not Add a Virtual Hard Disk

USB Controller: OHCI, EHCI

Device Filters: 0 (0 active)

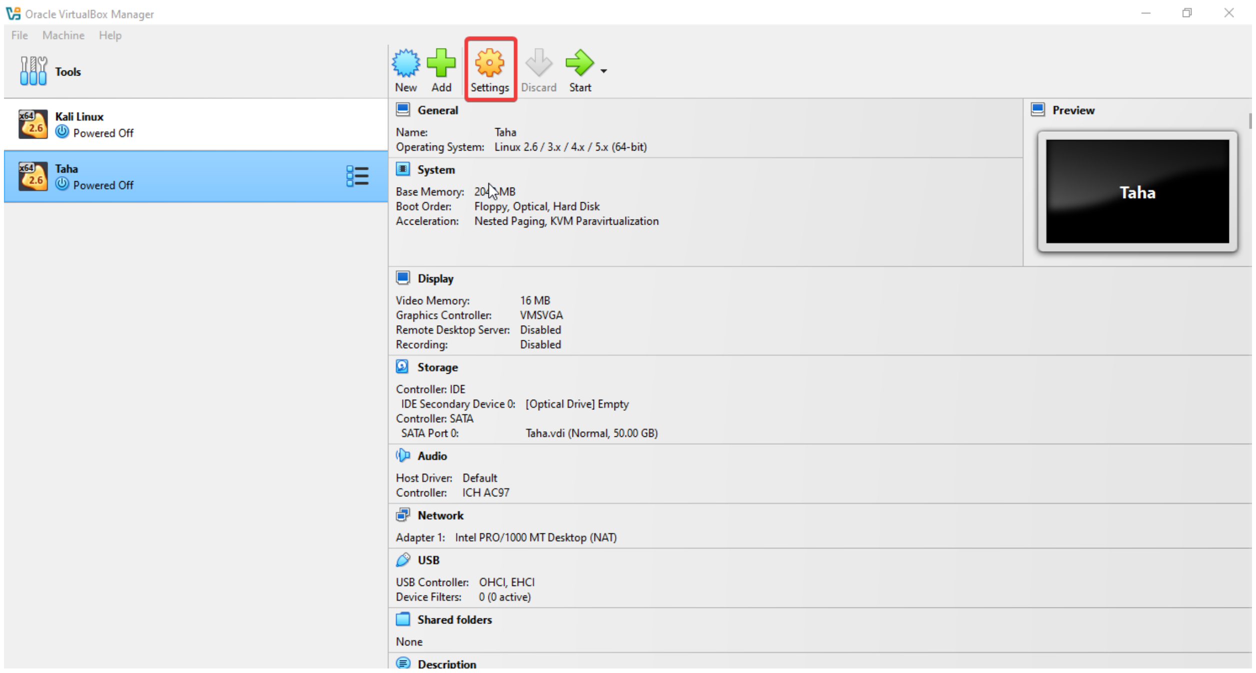
None

After following these steps click on finish:



Name: Taha
Folder: T:\VirtualBox VMs
ISO Image: <not selected>
Edition:
Type: Microsoft Windows
Subtype:
Version: Windows 11 (64-bit)
Skip Unattended Installation

After Finishing click the Settings:



General
Name: Taha
Operating System: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)

System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Taha.vdi (Normal, 50.00 GB)

Audio
Host Driver: Default
Controller: ICH AC97

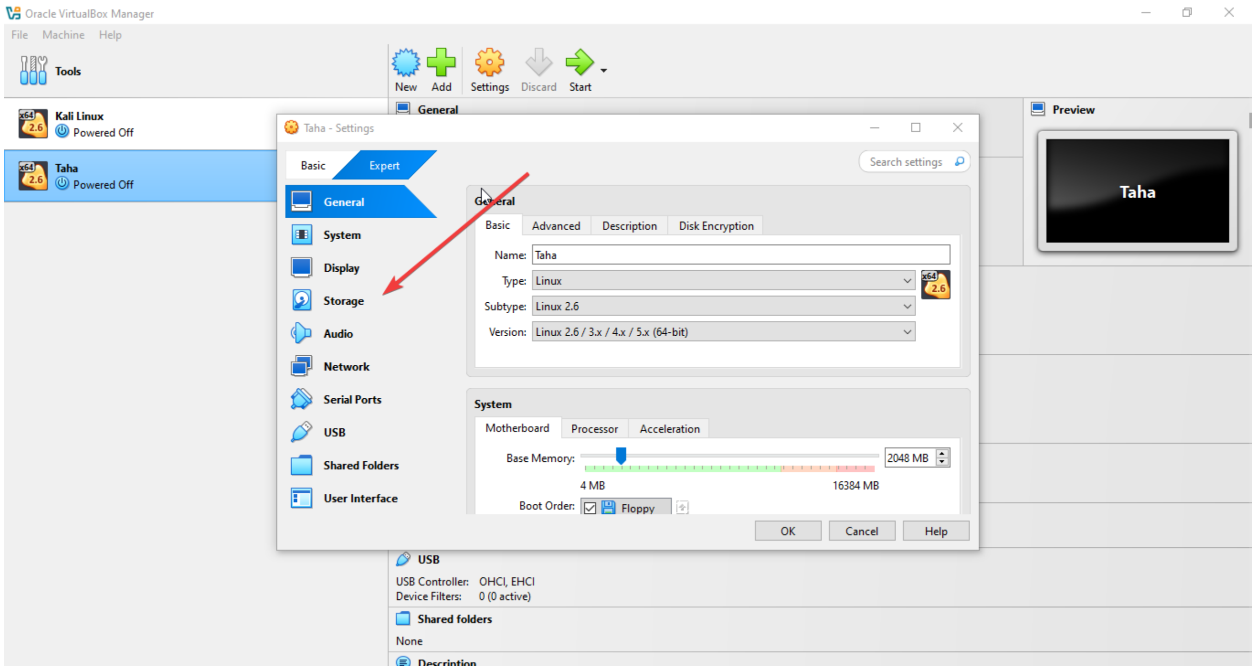
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders
None

Description

Go to the Storage Tab:



Oracle VirtualBox Manager

Taha - Settings

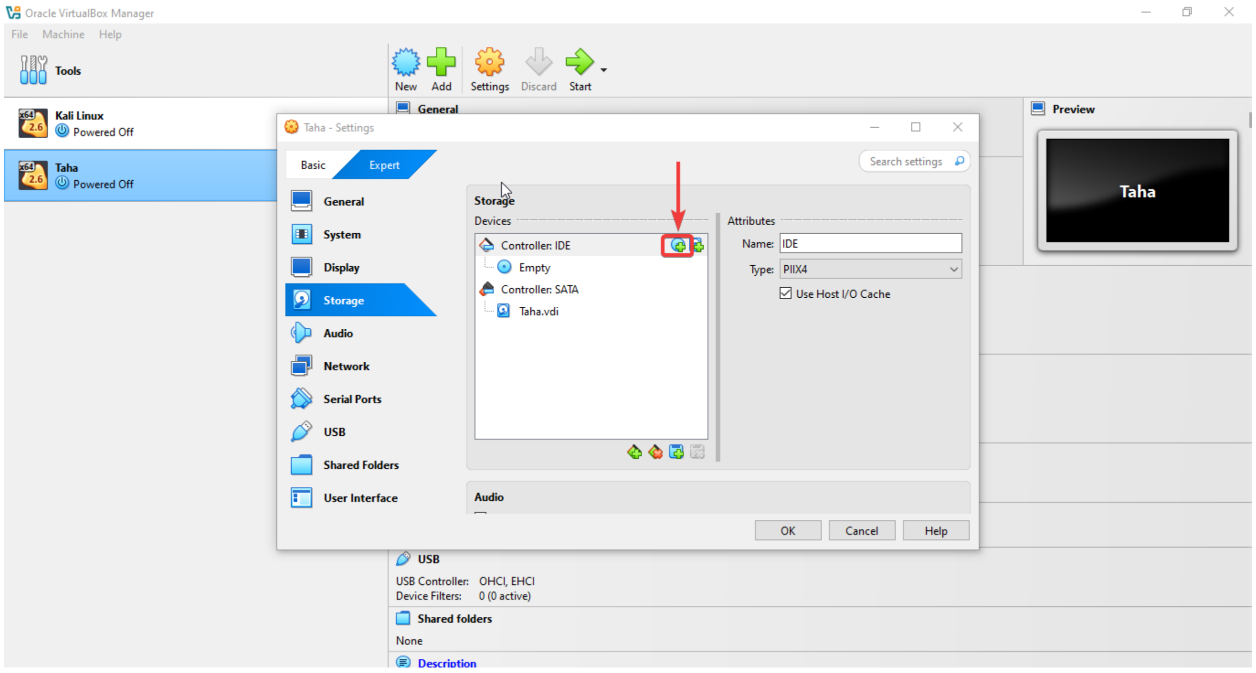
General — Basic: Name: Taha; Type: Linux; Subtype: Linux 2.6; Version: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)

System — Motherboard: Base Memory: 2048 MB; Boot Order: ☑ Floppy

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders: None

Select This Controller IDE and click this:



Oracle VirtualBox Manager

Taha - Settings

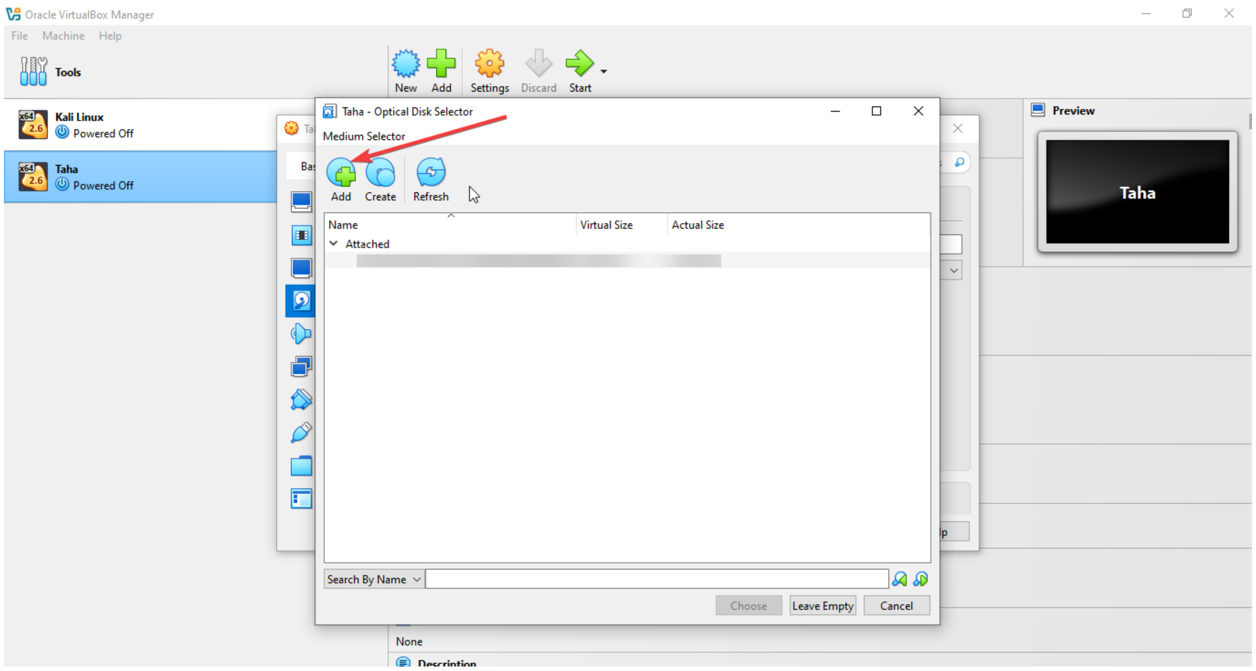
Storage — Devices:
- Controller: IDE
  - Empty
- Controller: SATA
  - Taha.vdi

Attributes: Name: IDE; Type: PIIX4; ☑ Use Host I/O Cache

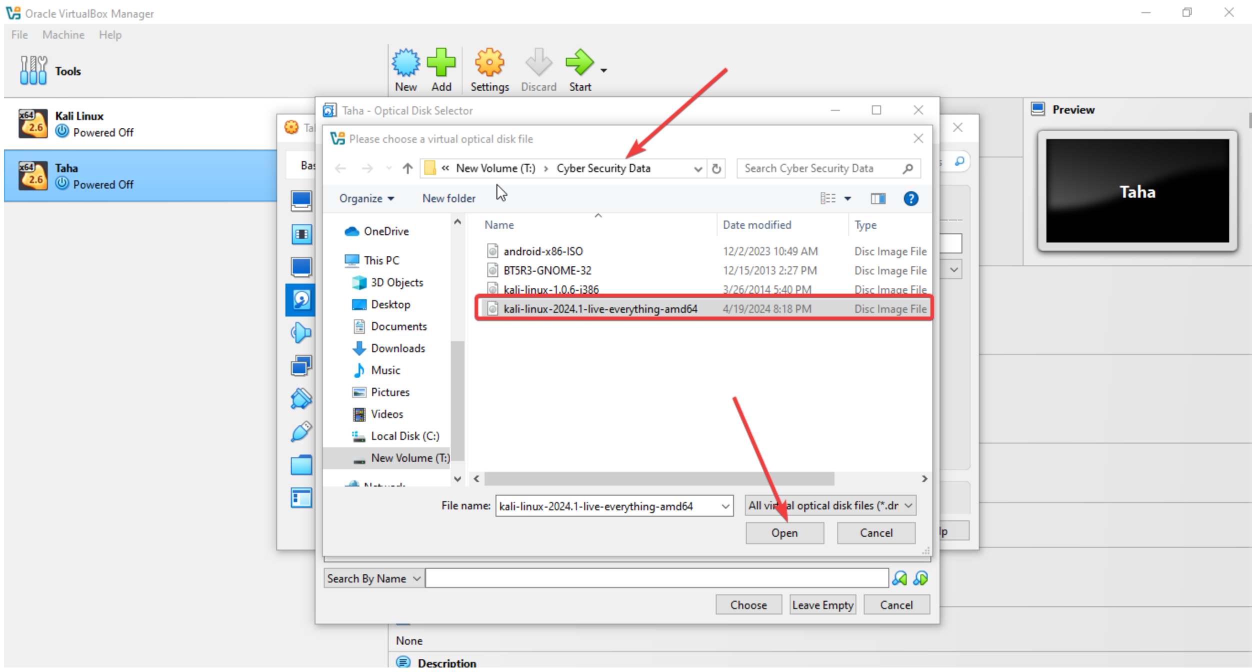
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders: None

Click on this Add Button:



Go to where you put the cyber security data and select kali linux 2024 and press choose:

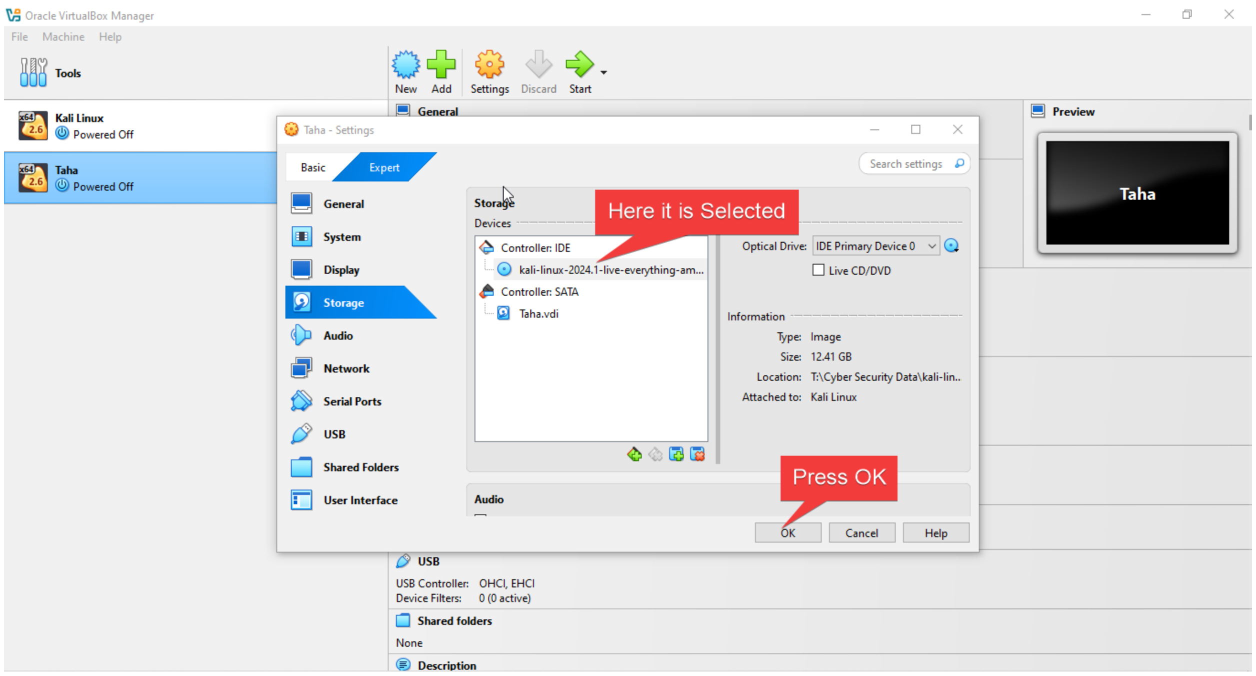


Name	Date modified	Type
android-x86-ISO	12/2/2023 10:49 AM	Disc Image File
BT5R3-GNOME-32	12/15/2013 2:27 PM	Disc Image File
kali-linux-1.0.6-i386	3/26/2014 5:40 PM	Disc Image File
kali-linux-2024.1-live-everything-amd64	4/19/2024 8:18 PM	Disc Image File

File name: kali-linux-2024.1-live-everything-amd64

All virtual optical disk files (*.dr

Now it will be installed:



Storage
Devices
Controller: IDE
kali-linux-2024.1-live-everything-am...
Controller: SATA
Taha.vdi

Optical Drive: IDE Primary Device 0
Live CD/DVD

Information
Type: Image
Size: 12.41 GB
Location: T:\Cyber Security Data\kali-lin..
Attached to: Kali Linux

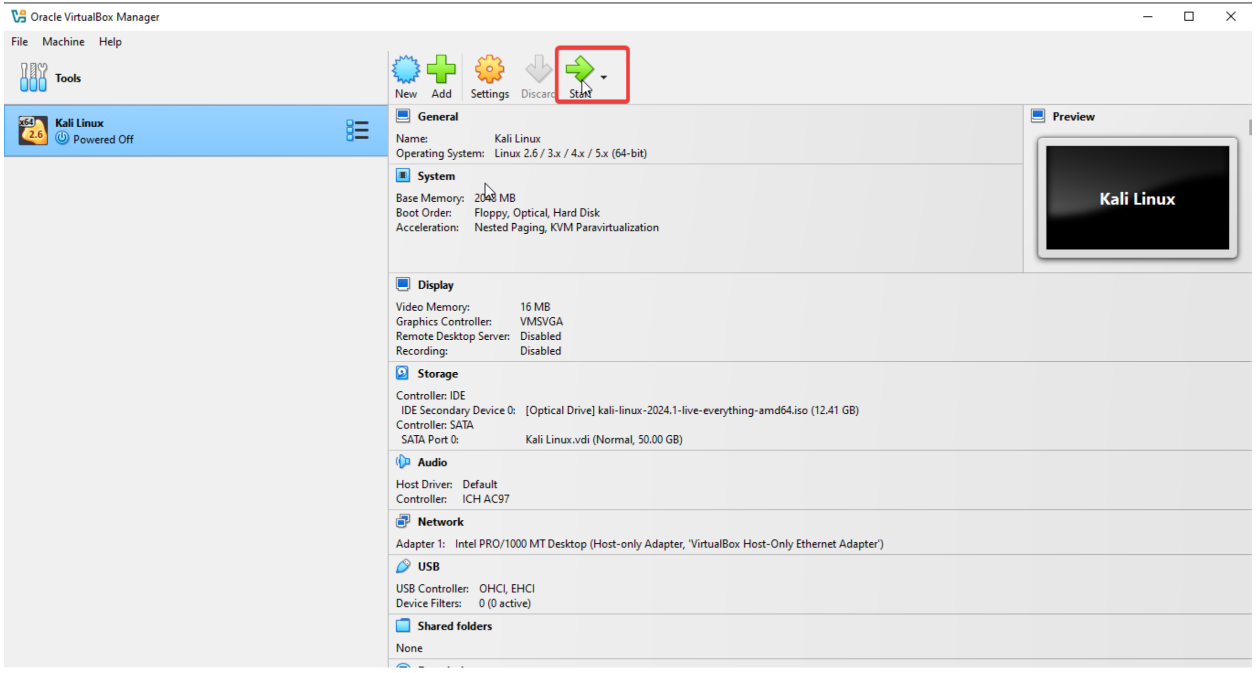
Audio

USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders
None

Description

After That click on this start button to start kali linux:



General
Name: Kali Linux
Operating System: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)

System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

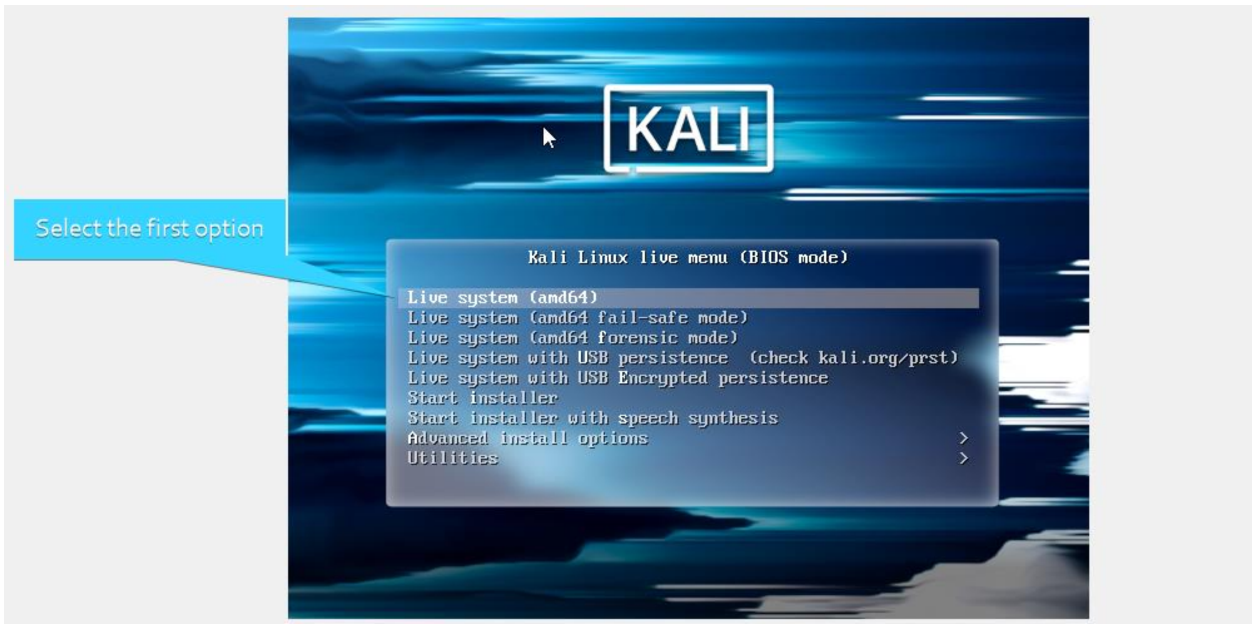
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] kali-linux-2024.1-live-everything-amd64.iso (12.41 GB)
Controller: SATA
SATA Port 0: Kali Linux.vdi (Normal, 50.00 GB)

Audio
Host Driver: Default
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter')

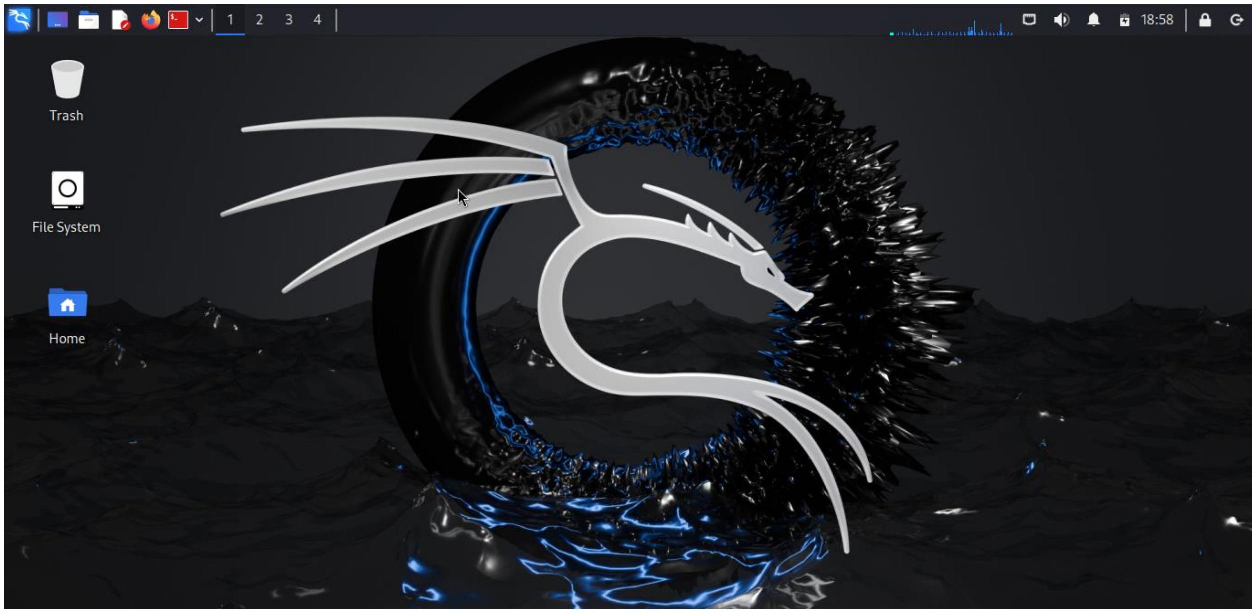
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders
None

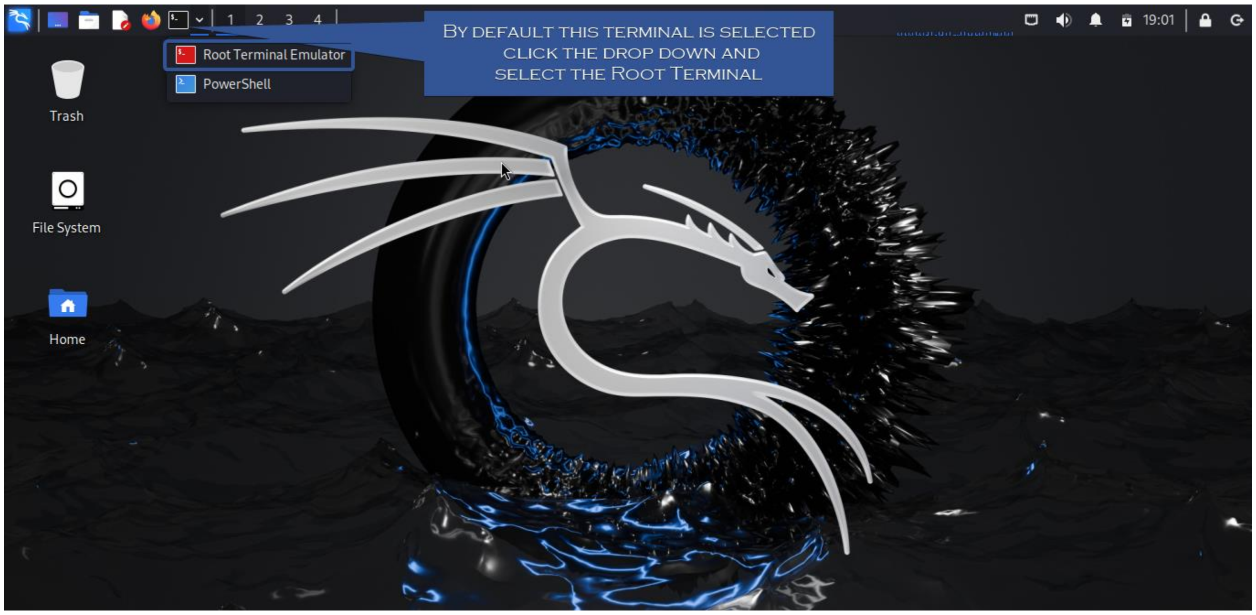


```
Kali Linux live menu (BIOS mode)

Live system (amd64)
Live system (amd64 fail-safe mode)
Live system (amd64 forensic mode)
Live system with USB persistence  (check kali.org/prst)
Live system with USB Encrypted persistence
Start installer
Start installer with speech synthesis
Advanced install options                                >
Utilities                                               >
```

This is the Home Screen of the Kali Linux:

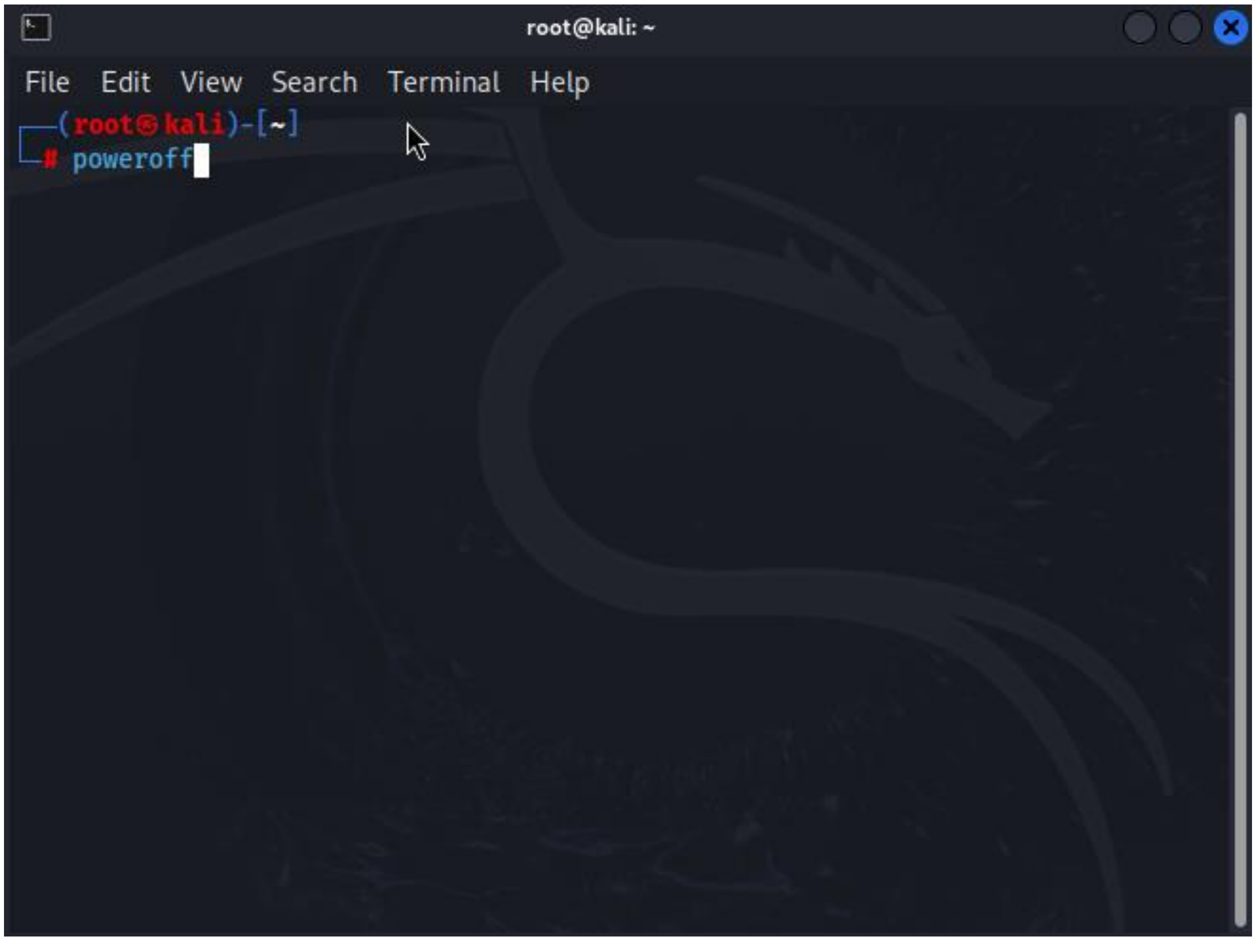


Select the Root Terminal Emulator



BY DEFAULT THIS TERMINAL IS SELECTED CLICK THE DROP DOWN AND SELECT THE ROOT TERMINAL

Run this command to Power off the VM:



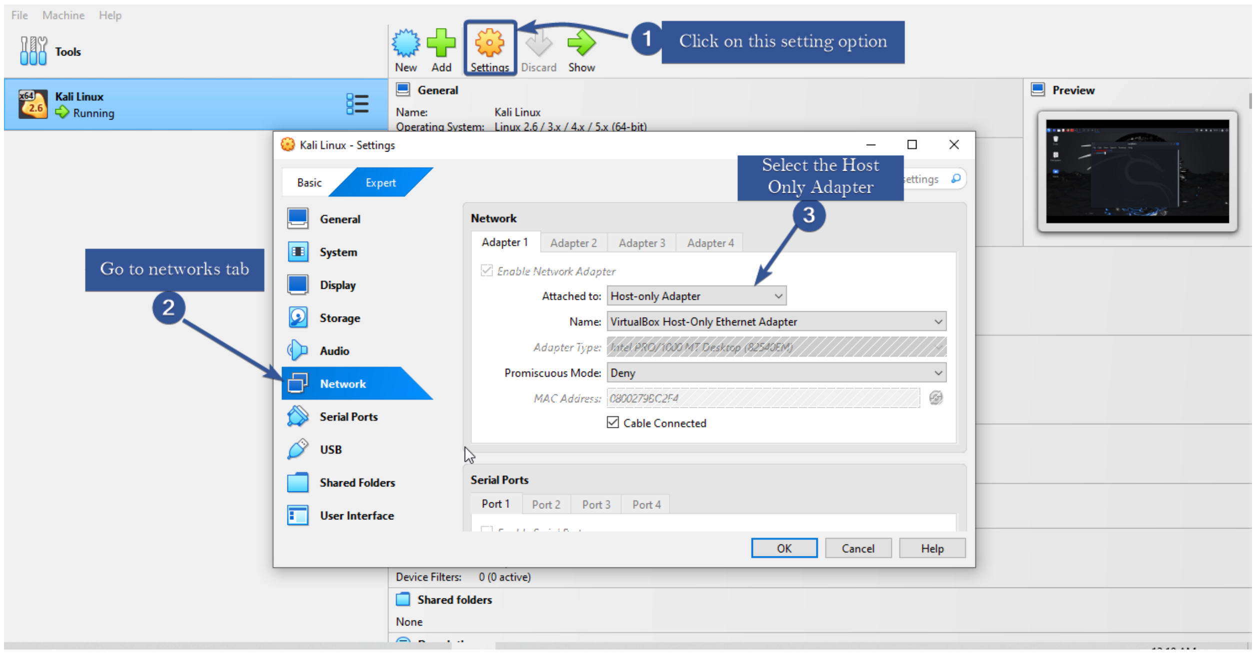
```
┌──(root㉿kali)-[~]
└─# poweroff
```

18TH September 2025

➢ Host – only Adapter:-

If we select **Host-only Adapter** for networking in VirtualBox/VMware, then all the machines (VMs) that have chosen **Host-only Adapter** will be able to communicate with each other.

- **Key Point:-**
  These machines **can only talk to each other** but will **not have internet access** through this adapter.



Name: Kali Linux
Operating System: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)

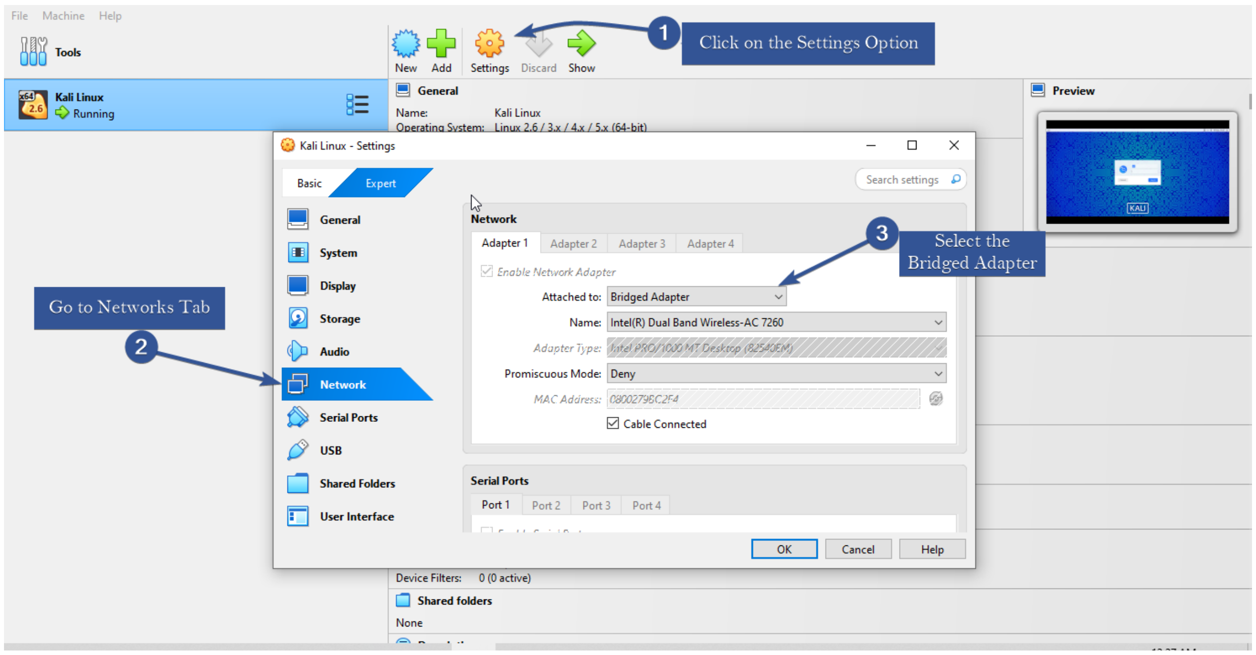
Enable Network Adapter ✓
Attached to: Host-only Adapter
Name: VirtualBox Host-Only Ethernet Adapter
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 08002796C2F4
✓ Cable Connected

Device Filters: 0 (0 active)
Shared folders
None

➢ Bridged Adapter:

If we select **Bridged Adapter**, then all the machines (VMs) that have chosen **Bridged Adapter** will be connected to each other **and** they will also connect to the **same physical network as the host machine**.

- **Key Points:-**
  - If the **physical machine has internet access**, then all the connected VMs will also have internet access.
  - If the **physical machine loses internet**, then the VMs will also lose internet.



Network

Adapter 1

Enable Network Adapter

Attached to: Bridged Adapter

Name: Intel(R) Dual Band Wireless-AC 7260

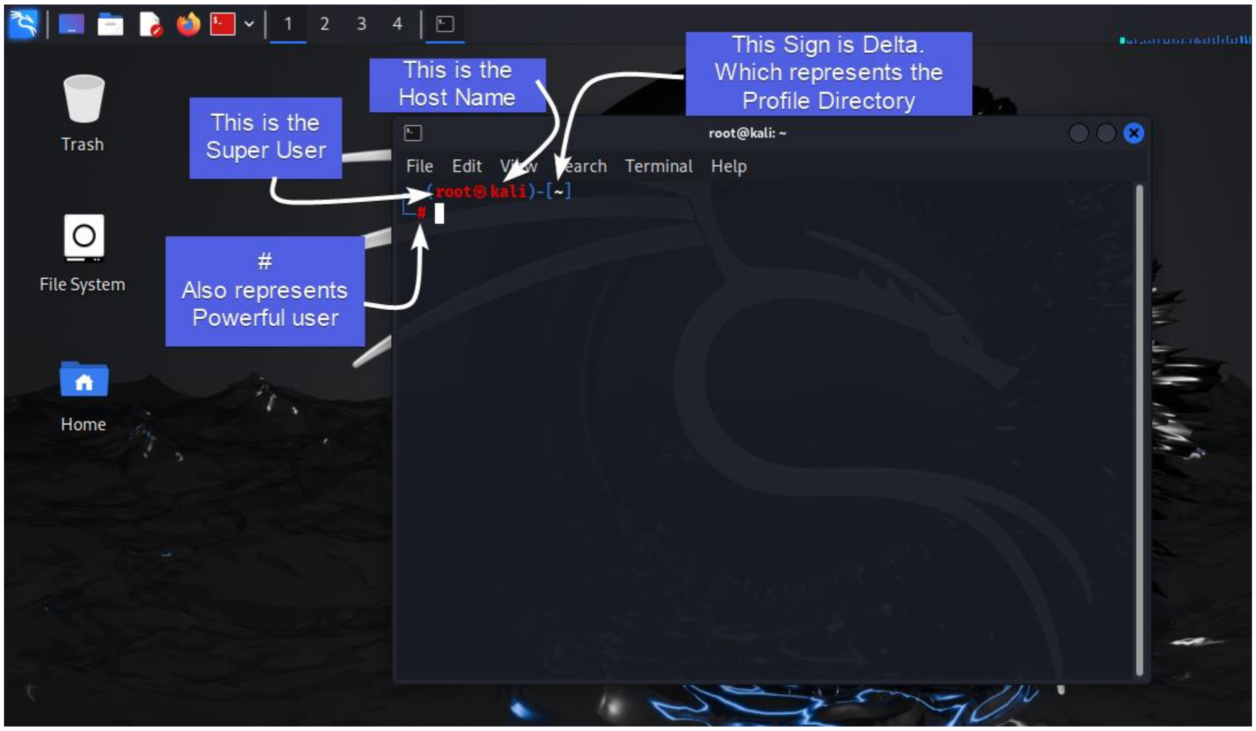
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 0800279BC2F4

Cable Connected

Kali Linux Shell Prompt Explained:


This is the Host Name
This Sign is Delta. Which represents the Profile Directory
This is the Super User
# Also represents Powerful user
Trash
File System
Home
root@kali: ~
File Edit View Search Terminal Help

```
┌──(root㉿kali)-[~]
└─#
```

➢ Commands Learned:-

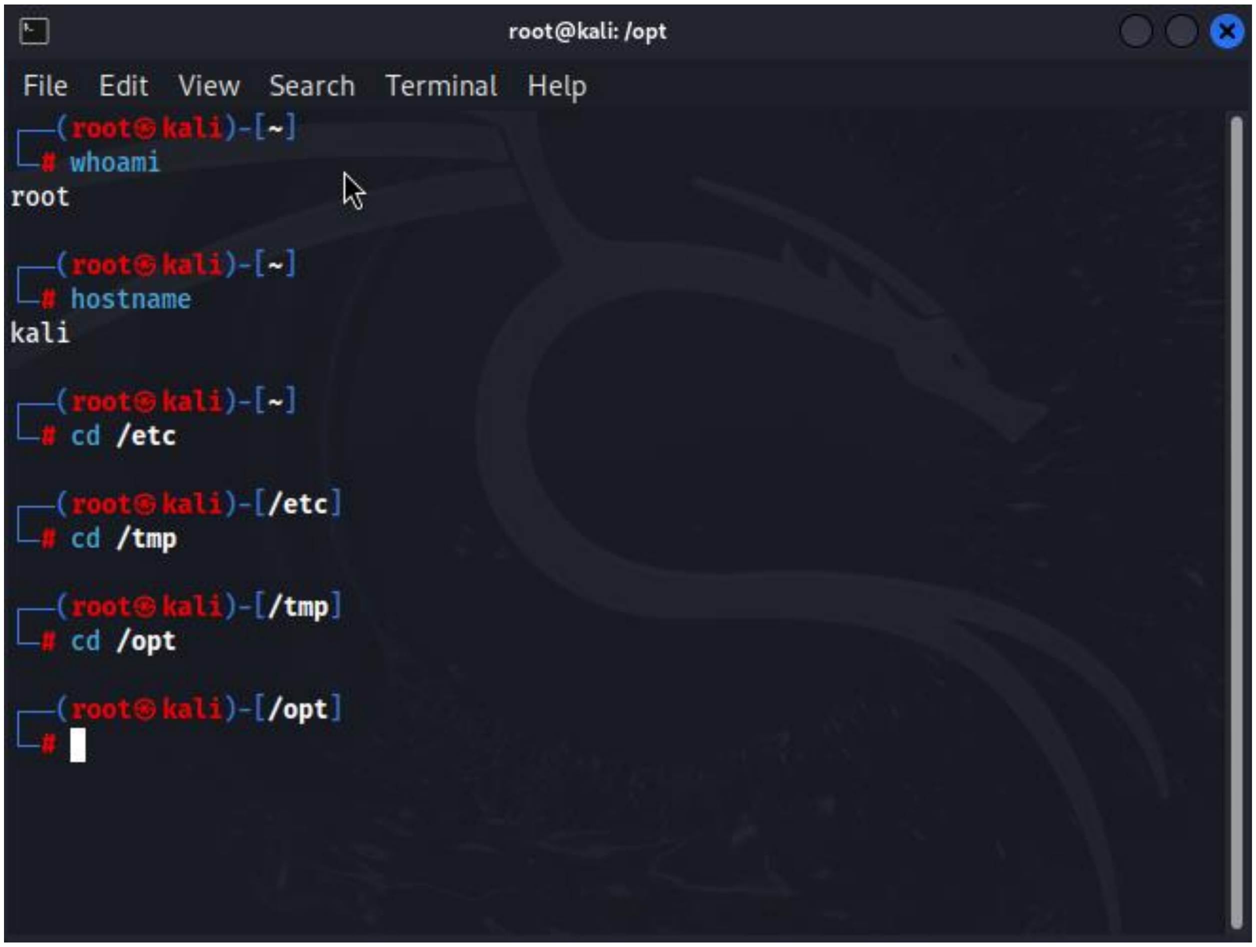
1. whoami → Shows the currently logged-in user (Linux is **case sensitive**).
2. hostname → Shows the host name of the system

Navigating in root Terminal:-

3. cd /etc
4. cd /tmp
5. cd /opt

➢ When in the root Terminal:-

- ~ changes to the folder name when moving, e.g., cd /etc replaces ~ with /etc.
- pwd → Shows the **present working directory**.

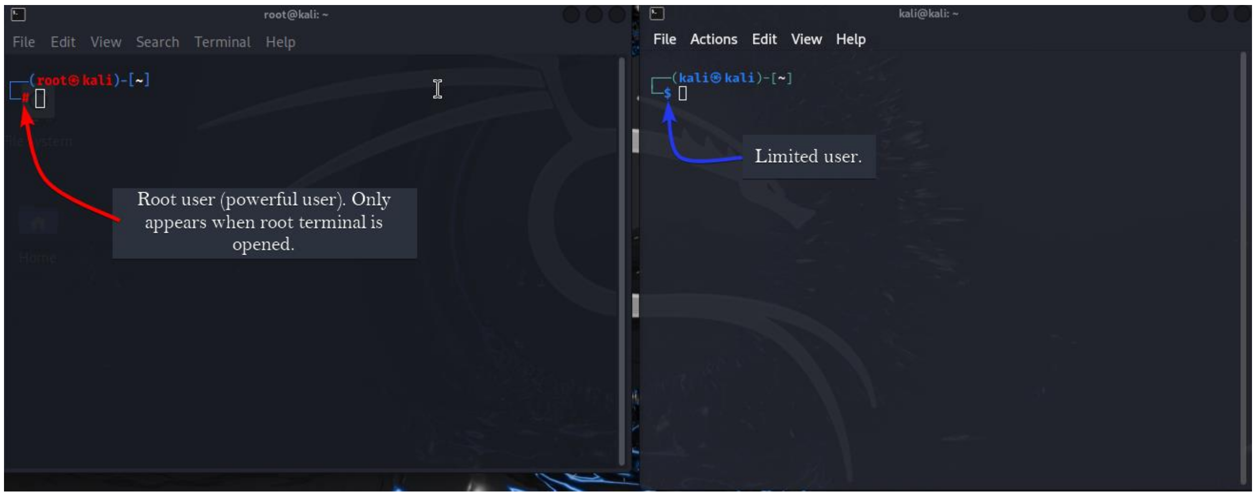


```
┌──(root㉿kali)-[~]
└─# whoami
root

┌──(root㉿kali)-[~]
└─# hostname
kali

┌──(root㉿kali)-[~]
└─# cd /etc

┌──(root㉿kali)-[/etc]
└─# cd /tmp

┌──(root㉿kali)-[/tmp]
└─# cd /opt

┌──(root㉿kali)-[/opt]
└─# 
```

➢ Symbols in Linux:-

# → Root user (powerful user). Only appears when root terminal is opened.
$ → Limited User

- In Windows: you can create any user and give **administrator rights**.
- In Linux: **only root** has administrator rights.


root@kali: ~
File Edit View Search Terminal Help
Root user (powerful user). Only appears when root terminal is opened.
kali@kali: ~
File Actions Edit View Help
Limited user.

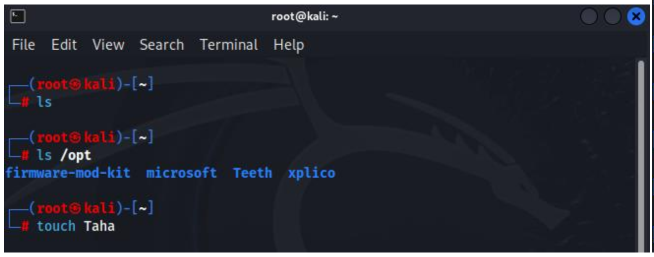
```
┌──(root㉿kali)-[~]
└─#
```

```
┌──(kali㉿kali)-[~]
└─$
```

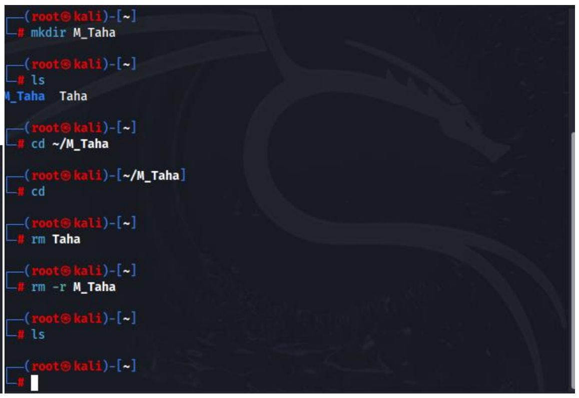
- **User Privileges:-**
  1. **Root User:** Can perform administrative tasks, no limitations.
  2. **Normal User:** Can only perform basic tasks, not everything is possible.

- **File & Directory Commands**

  - ls → Lists contents of the current directory.
  - ls /tmp → Lists contents of /tmp without entering it.
  - touch [filename] → Creates a file.
  - mkdir [foldername] → Creates a folder (e.g., mkdir M_Taha).
  - cd ~/M_Taha → Access the created folder.
  - rm [filename] → Removes a file.
  - rm –r [foldername] → Removes a folder.



```
┌──(root㉿kali)-[~]
└─# ls

┌──(root㉿kali)-[~]
└─# ls /opt
firmware-mod-kit  microsoft  Teeth  xplico

┌──(root㉿kali)-[~]
└─# touch Taha
```



```
┌──(root㉿kali)-[~]
└─# mkdir M_Taha

┌──(root㉿kali)-[~]
└─# ls
_Taha  Taha

┌──(root㉿kali)-[~]
└─# cd ~/M_Taha

┌──(root㉿kali)-[~/M_Taha]
└─# cd

┌──(root㉿kali)-[~]
└─# rm Taha

┌──(root㉿kali)-[~]
└─# rm -r M_Taha

┌──(root㉿kali)-[~]
└─# ls

┌──(root㉿kali)-[~]
└─#
```

  - Files appear in white and folders appear in blue

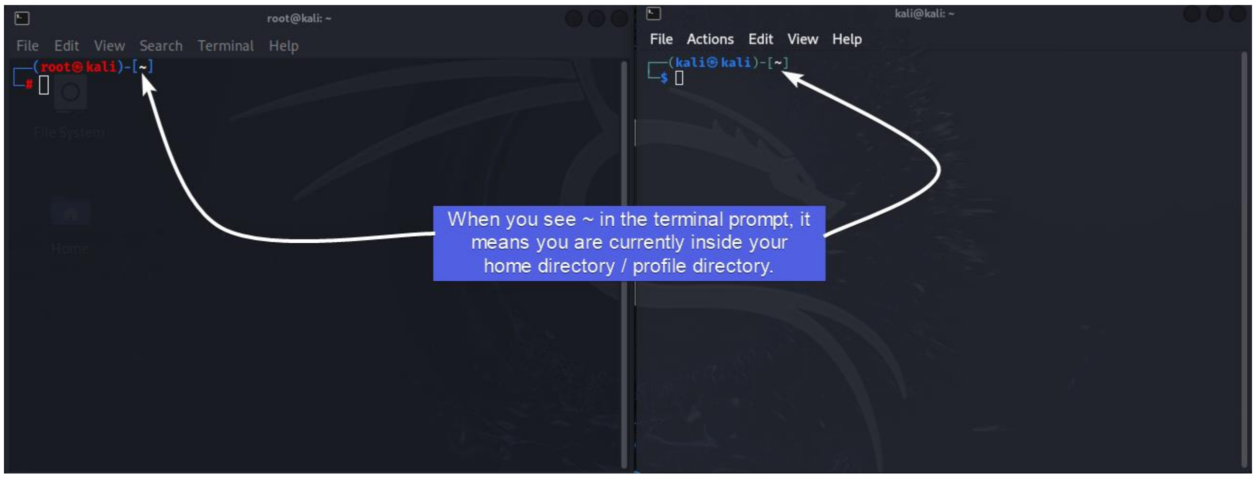
- **History:-**

  history → Shows the list of previously used commands.

19TH September 2025

➢ Home Directory (~):

- In Linux, the **tilde symbol (~)** represents the **home directory / profile directory** of the currently logged-in user.
- Example: If you're logged in as user kali, then ~ points to /home/kali. If you're logged in as root, ~ points to /root.
- When you see ~ in the terminal prompt, it means you are currently inside your **home directory / profile directory**.


root@kali: ~
File Edit View Search Terminal Help
kali@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─#
```

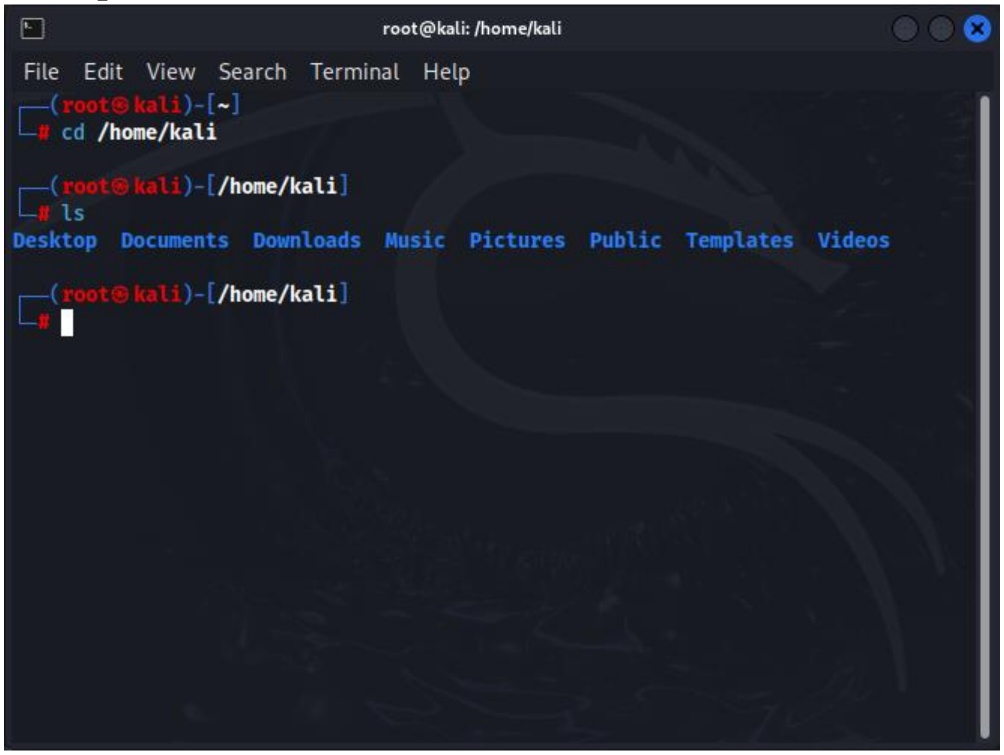
```
┌──(kali㉿kali)-[~]
└─$
```

When you see ~ in the terminal prompt, it means you are currently inside your home directory / profile directory.

➢ Automatic Folders:

- When a user logs in graphically for the first time, Linux automatically creates some default folders (like **Desktop, Downloads, Documents, Music, Pictures, Videos**) in their **home directory**.

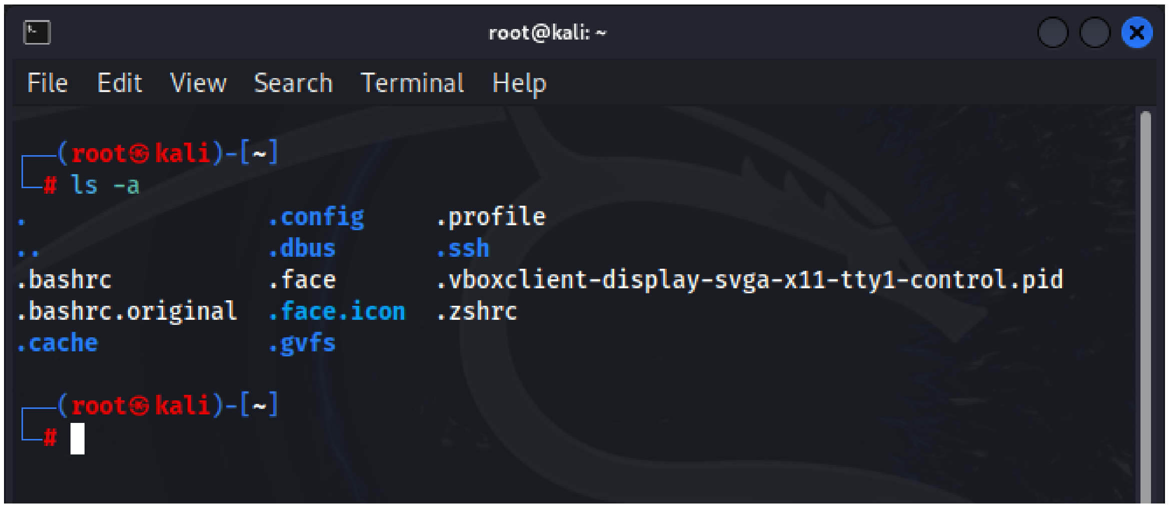
- **Example: Run:**



```
┌──(root㉿kali)-[~]
└─# cd /home/kali

┌──(root㉿kali)-[/home/kali]
└─# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(root㉿kali)-[/home/kali]
└─# 
```

➢ Hidden Files:

- To view **hidden files**, use:



```
┌──(root㉿kali)-[~]
└─# ls -a
.                  .config     .profile
..                 .dbus       .ssh
.bashrc            .face       .vboxclient-display-svga-x11-tty1-control.pid
.bashrc.original   .face.icon  .zshrc
.cache             .gvfs

┌──(root㉿kali)-[~]
└─# 
```

- The -a option means **all**, including hidden files.
- InLinux (and UNIX-like systems), hidden files and folders start with a **dot (.)**.
  Example: .bashrc, .profile, .config/

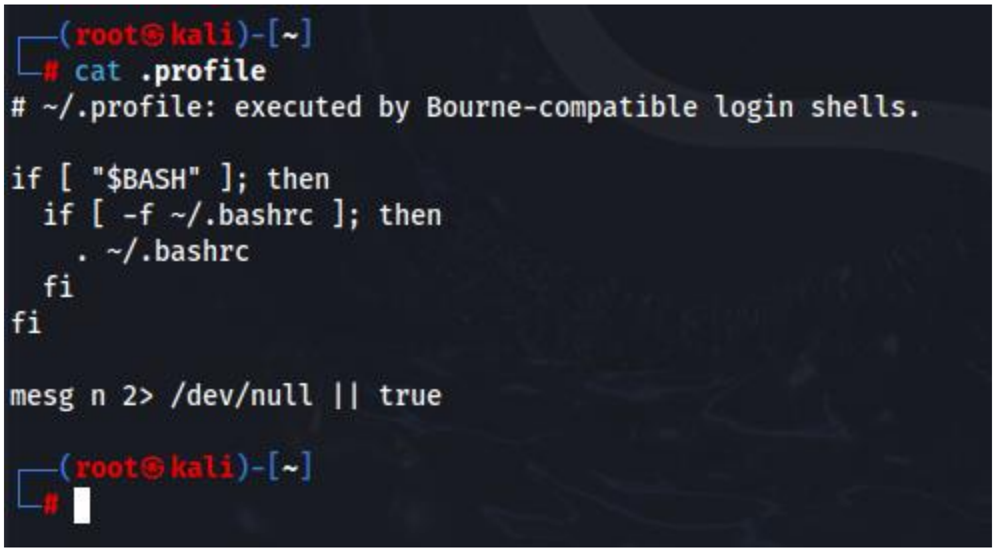
➢ **In Windows**, hidden files are controlled by system attributes, not by starting the name with a dot.

➢ File Extensions:

- In **Windows**, file extensions are important (.txt, .zip, .exe, etc.).
- In **Linux**, file extensions are **optional**. Files are recognized by their **content**, not extension.
- Example: A shell script may not have .sh extension but can still be executed if it has executable permissions.
- In **Linux** the color **White** represents a **text file** and the color **Blue** represents a **directory**.

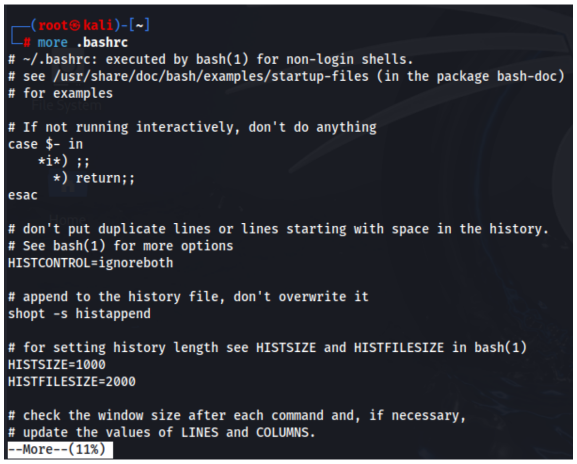
➢ Viewing File Contents:

- To view contents of a file use:
  cat filename



```
┌──(root㉿kali)-[~]
└─# cat .profile
# ~/.profile: executed by Bourne-compatible login shells.

if [ "$BASH" ]; then
  if [ -f ~/.bashrc ]; then
    . ~/.bashrc
  fi
fi

mesg n 2> /dev/null || true

┌──(root㉿kali)-[~]
└─# █
```

- **Only use cat for small files** (otherwise the output will overflow).
- To view large files use page by page using this command:
  more filename



```
┌──(root㉿kali)-[~]
└─# more .bashrc
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
case $- in
    *i*) ;;
      *) return;;
esac

# don't put duplicate lines or lines starting with space in the history.
# See bash(1) for more options
HISTCONTROL=ignoreboth

# append to the history file, don't overwrite it
shopt -s histappend

# for setting history length see HISTSIZE and HISTFILESIZE in bash(1)
HISTSIZE=1000
HISTFILESIZE=2000

# check the window size after each command and, if necessary,
# update the values of LINES and COLUMNS.
--More--(11%)
```

- Press **Enter** to move line by line.

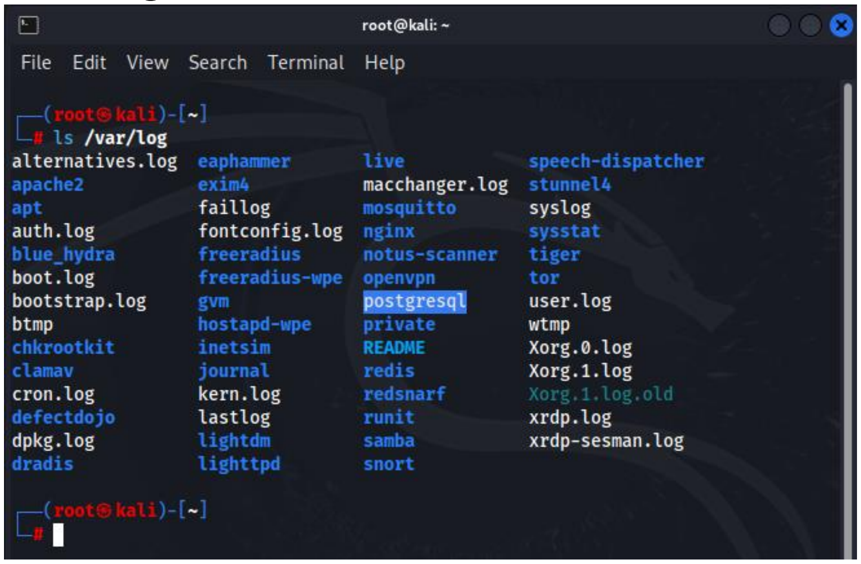
- Press **Spacebar** to move page by page.
- To view first 10 lines of a file use this command:
  head filename
- To view the last 10 lines of a file use this command:
  tail filename
- Custom Number of lines let's say first 15 lines:
  head –n 15 filename
- Custom number of lines let's say last 15 lines:
  tail –n 15 filename
- Get the first line of the file only:
  head –n 1 filename
- Get the last line of the file only:
  tail –n 1 filename

➢ System Information:

- To check CPU details:
  cat /proc/cpuinfo
- To check ram details:
  cat /proc/meminfo

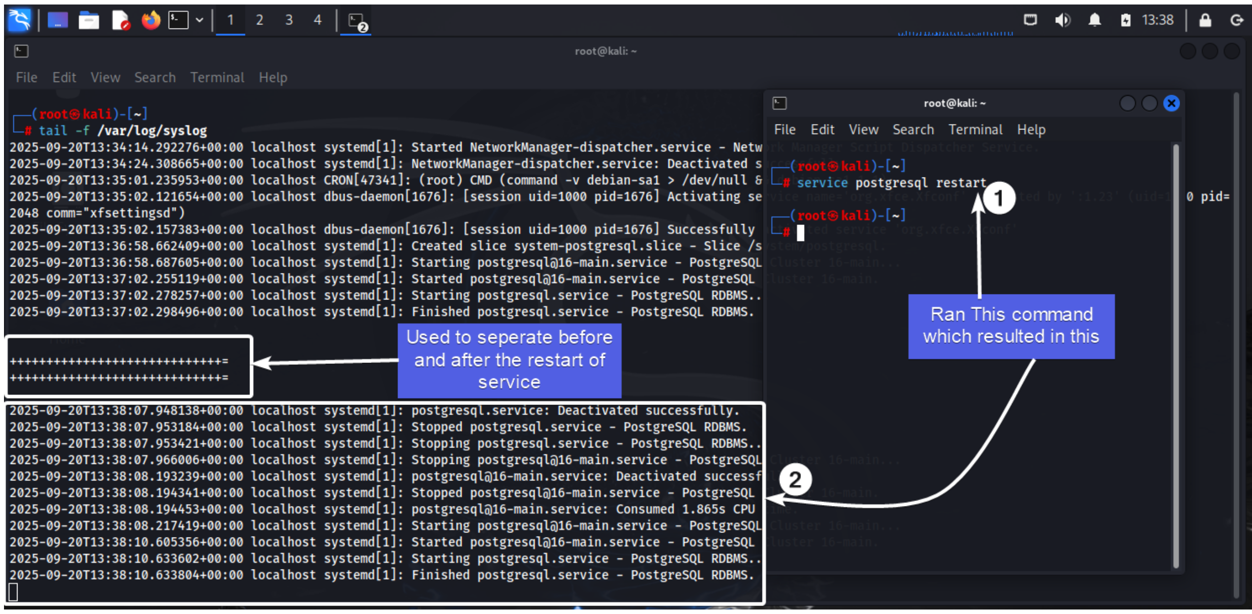
➢ Logs

- Linux System logs are stored in ***/var/log*** To see them:
  ls /var/log



```
┌──(root㉿kali)-[~]
└─# ls /var/log
alternatives.log  eaphammer         live             speech-dispatcher
apache2           exim4             macchanger.log   stunnel4
apt               faillog           mosquitto        syslog
auth.log          fontconfig.log    nginx            sysstat
blue_hydra        freeradius        notus-scanner    tiger
boot.log          freeradius-wpe    openvpn          tor
bootstrap.log     gvm               postgresql       user.log
btmp              hostapd-wpe       private          wtmp
chkrootkit        inetsim           README           Xorg.0.log
clamav            journal           redis            Xorg.1.log
cron.log          kern.log          redsnarf         Xorg.1.log.old
defectdojo        lastlog           runit            xrdp.log
dpkg.log          lightdm           samba            xrdp-sesman.log
dradis            lighttpd          snort

┌──(root㉿kali)-[~]
└─#
```

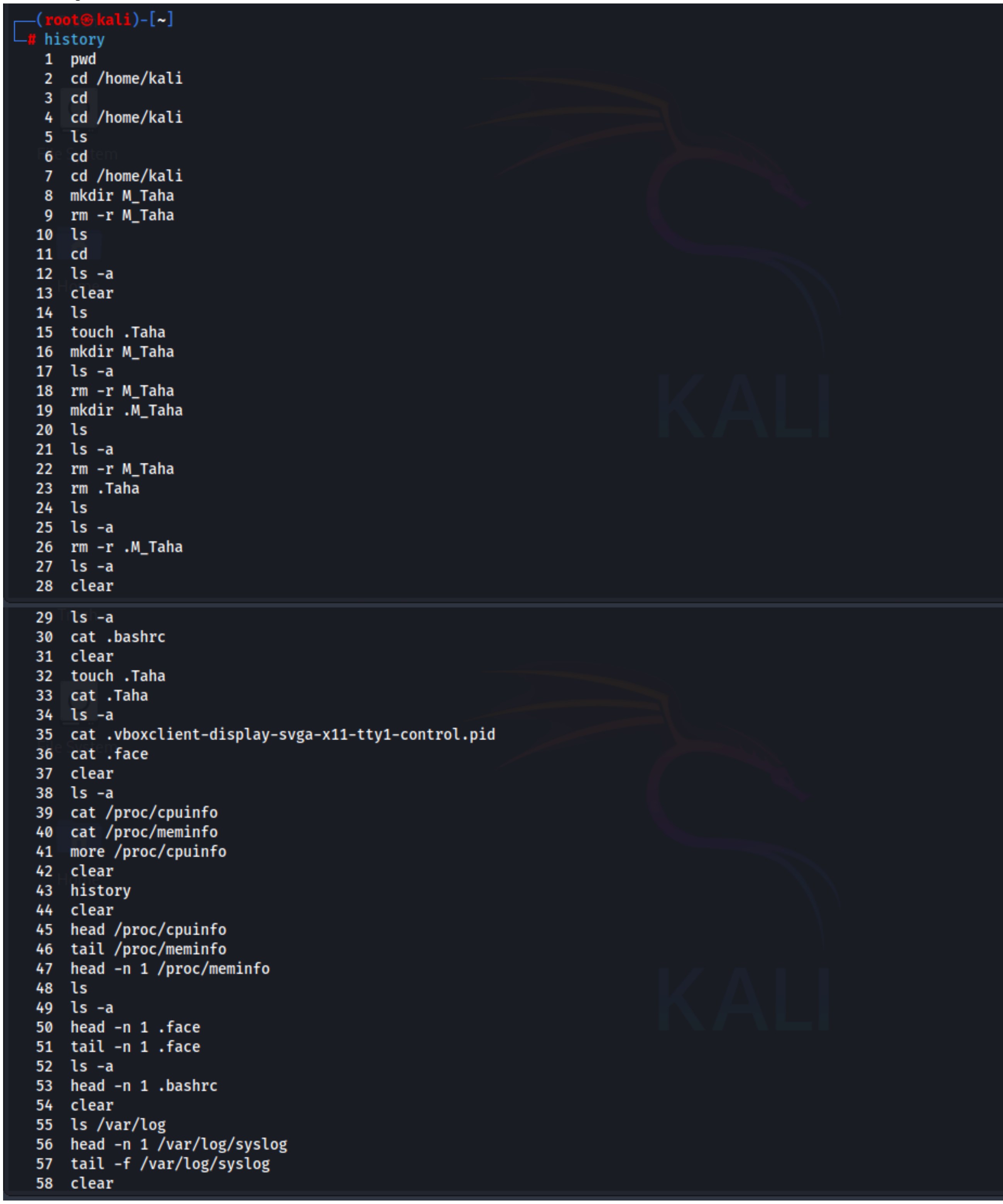
- To monitor a log file continuously (live updates)
  tail -f /var/log/syslog
- **Example:**
  - Run in one Terminal:
    tail -f /var/log/syslog (This will keep new logs as they are added)
  - In another terminal restart a service like PostgreSQL
    service postgresql restart
  - You will immediately see the related logs in the first terminal


root@kali: ~
File Edit View Search Terminal Help
Used to seperate before and after the restart of service
Ran This command which resulted in this
1
2

```
┌──(root㉿kali)-[~]
└─# tail -f /var/log/syslog
2025-09-20T13:34:14.292276+00:00 localhost systemd[1]: Started NetworkManager-dispatcher.service - Netw
2025-09-20T13:34:24.308665+00:00 localhost systemd[1]: NetworkManager-dispatcher.service: Deactivated s
2025-09-20T13:35:01.235953+00:00 localhost CRON[47341]: (root) CMD (command -v debian-sa1 > /dev/null &
2025-09-20T13:35:02.121654+00:00 localhost dbus-daemon[1676]: [session uid=1000 pid=1676] Activating se
2048 comm="xfsettingsd")
2025-09-20T13:35:02.157383+00:00 localhost dbus-daemon[1676]: [session uid=1000 pid=1676] Successfully
2025-09-20T13:36:58.662409+00:00 localhost systemd[1]: Created slice system-postgresql.slice - Slice /s
2025-09-20T13:36:58.687605+00:00 localhost systemd[1]: Starting postgresql@16-main.service - PostgreSQL
2025-09-20T13:37:02.255119+00:00 localhost systemd[1]: Started postgresql@16-main.service - PostgreSQL
2025-09-20T13:37:02.278257+00:00 localhost systemd[1]: Starting postgresql.service - PostgreSQL RDBMS..
2025-09-20T13:37:02.298496+00:00 localhost systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.

++++++++++++++++++++++++++++++=
++++++++++++++++++++++++++++++=

2025-09-20T13:38:07.948138+00:00 localhost systemd[1]: postgresql.service: Deactivated successfully.
2025-09-20T13:38:07.953184+00:00 localhost systemd[1]: Stopped postgresql.service - PostgreSQL RDBMS.
2025-09-20T13:38:07.953421+00:00 localhost systemd[1]: Stopping postgresql.service - PostgreSQL RDBMS..
2025-09-20T13:38:07.966006+00:00 localhost systemd[1]: Stopping postgresql@16-main.service - PostgreSQL
2025-09-20T13:38:08.193239+00:00 localhost systemd[1]: postgresql@16-main.service: Deactivated successf
2025-09-20T13:38:08.194341+00:00 localhost systemd[1]: Stopped postgresql@16-main.service - PostgreSQL
2025-09-20T13:38:08.194453+00:00 localhost systemd[1]: postgresql@16-main.service: Consumed 1.865s CPU
2025-09-20T13:38:08.217419+00:00 localhost systemd[1]: Starting postgresql@16-main.service - PostgreSQL
2025-09-20T13:38:10.605356+00:00 localhost systemd[1]: Started postgresql@16-main.service - PostgreSQL
2025-09-20T13:38:10.633602+00:00 localhost systemd[1]: Starting postgresql.service - PostgreSQL RDBMS..
2025-09-20T13:38:10.633804+00:00 localhost systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.
```

```
┌──(root㉿kali)-[~]
└─# service postgresql restart

┌──(root㉿kali)-[~]
└─#
```

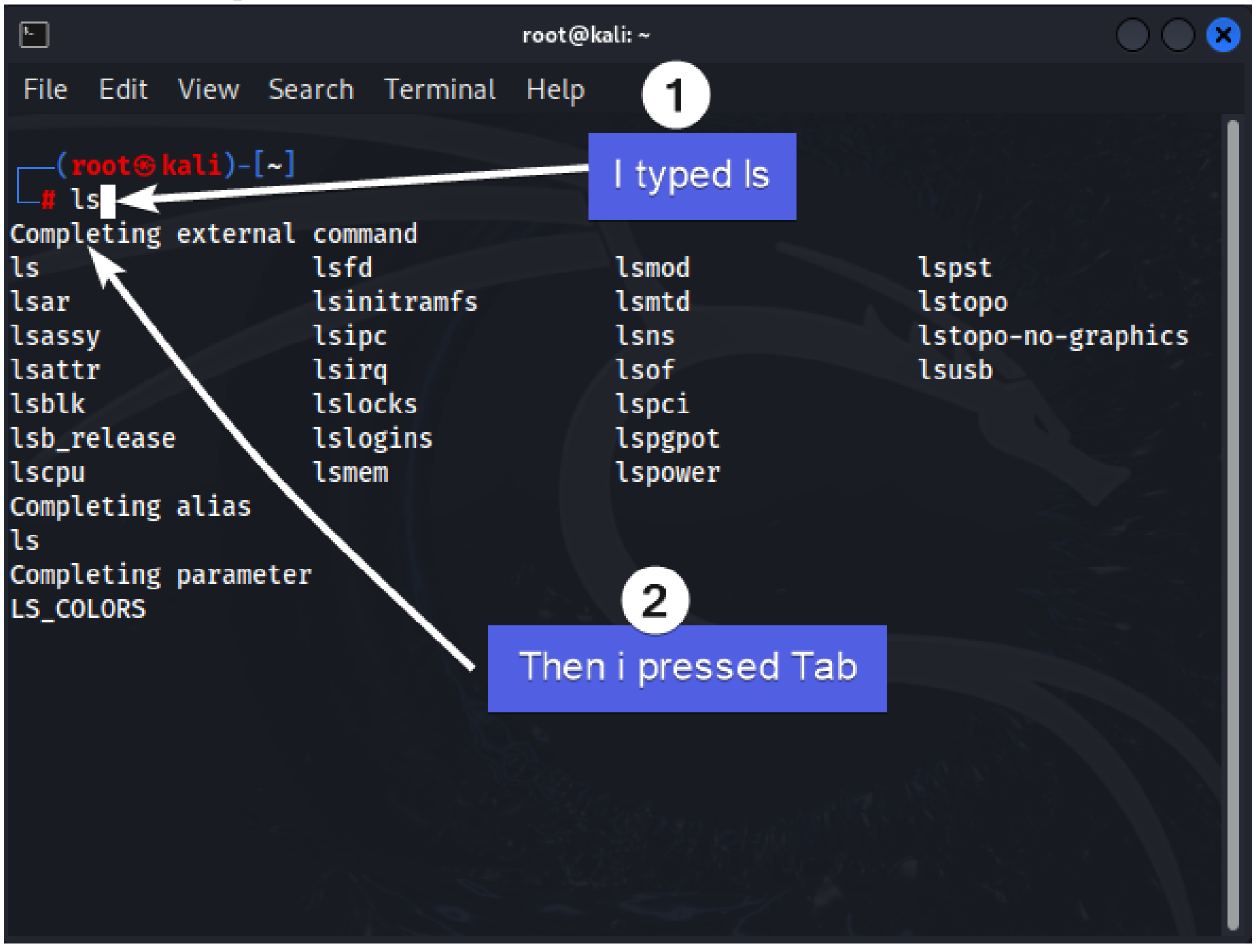
- You can check the history of the commands you've run using:
  history



```
┌──(root㉿kali)-[~]
└─# history
    1  pwd
    2  cd /home/kali
    3  cd
    4  cd /home/kali
    5  ls
    6  cd
    7  cd /home/kali
    8  mkdir M_Taha
    9  rm -r M_Taha
   10  ls
   11  cd
   12  ls -a
   13  clear
   14  ls
   15  touch .Taha
   16  mkdir M_Taha
   17  ls -a
   18  rm -r M_Taha
   19  mkdir .M_Taha
   20  ls
   21  ls -a
   22  rm -r M_Taha
   23  rm .Taha
   24  ls
   25  ls -a
   26  rm -r .M_Taha
   27  ls -a
   28  clear
   29  ls -a
   30  cat .bashrc
   31  clear
   32  touch .Taha
   33  cat .Taha
   34  ls -a
   35  cat .vboxclient-display-svga-x11-tty1-control.pid
   36  cat .face
   37  clear
   38  ls -a
   39  cat /proc/cpuinfo
   40  cat /proc/meminfo
   41  more /proc/cpuinfo
   42  clear
   43  history
   44  clear
   45  head /proc/cpuinfo
   46  tail /proc/meminfo
   47  head -n 1 /proc/meminfo
   48  ls
   49  ls -a
   50  head -n 1 .face
   51  tail -n 1 .face
   52  ls -a
   53  head -n 1 .bashrc
   54  clear
   55  ls /var/log
   56  head -n 1 /var/log/syslog
   57  tail -f /var/log/syslog
   58  clear
```

22nd September 2025

- **Getting Help in Linux:**
  - If you need technical help, you can use **Google** or **ChatGPT** but **Linux** itself provide multiple ways to get help about commands.
- **Command Line vs GUI:**
  - **Command line** is the **professional approach.**
  - A **Cybersecurity professional** mainly works on the command line, since most powerful tools and administrative tasks are handled there.
- **Tab Completion:**
  - If you type the **first few letters** of a command and then press **Tab**, Linux will try to auto-complete the command or list all the possible commands related to that specific command.



```
┌──(root㉿kali)-[~]
└─# ls
Completing external command
ls                  lsfd                lsmod               lspst
lsar                lsinitramfs         lsmtd               lstopo
lsassy              lsipc               lsns                lstopo-no-graphics
lsattr              lsirq               lsof                lsusb
lsblk               lslocks             lspci
lsb_release         lslogins            lspgpot
lscpu               lsmem               lspower
Completing alias
ls
Completing parameter
LS_COLORS
```

➢ Where Commands Are Stored:

- Linux Commands are stored in specific directories:
  - ls /bin
  - ls /usr/bin
  - ls /usr/local/bin
  - ls /sbin
  - ls /usr/sbin
  - ls /usr/local/sbin

➢ bin vs sbin:

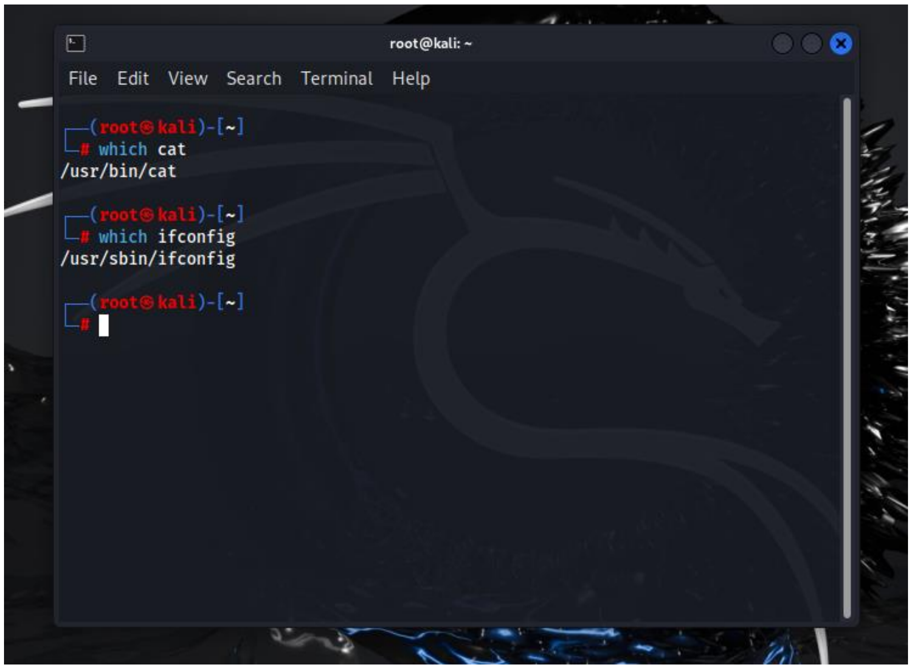
bin	**sbin**
Contains **basic commands** that all users can run.	Contains **administrative commands**, usually only run by the root user

Even if you use sudo, not every command in sbin will be accessible unless your account has the required privillages.

Administrative commands affect the **whole system.**

➢ Finding Where a Command Lives:

- To check whether a command is basic or administrative use:
  - **which [command name]**
  - **Example:**



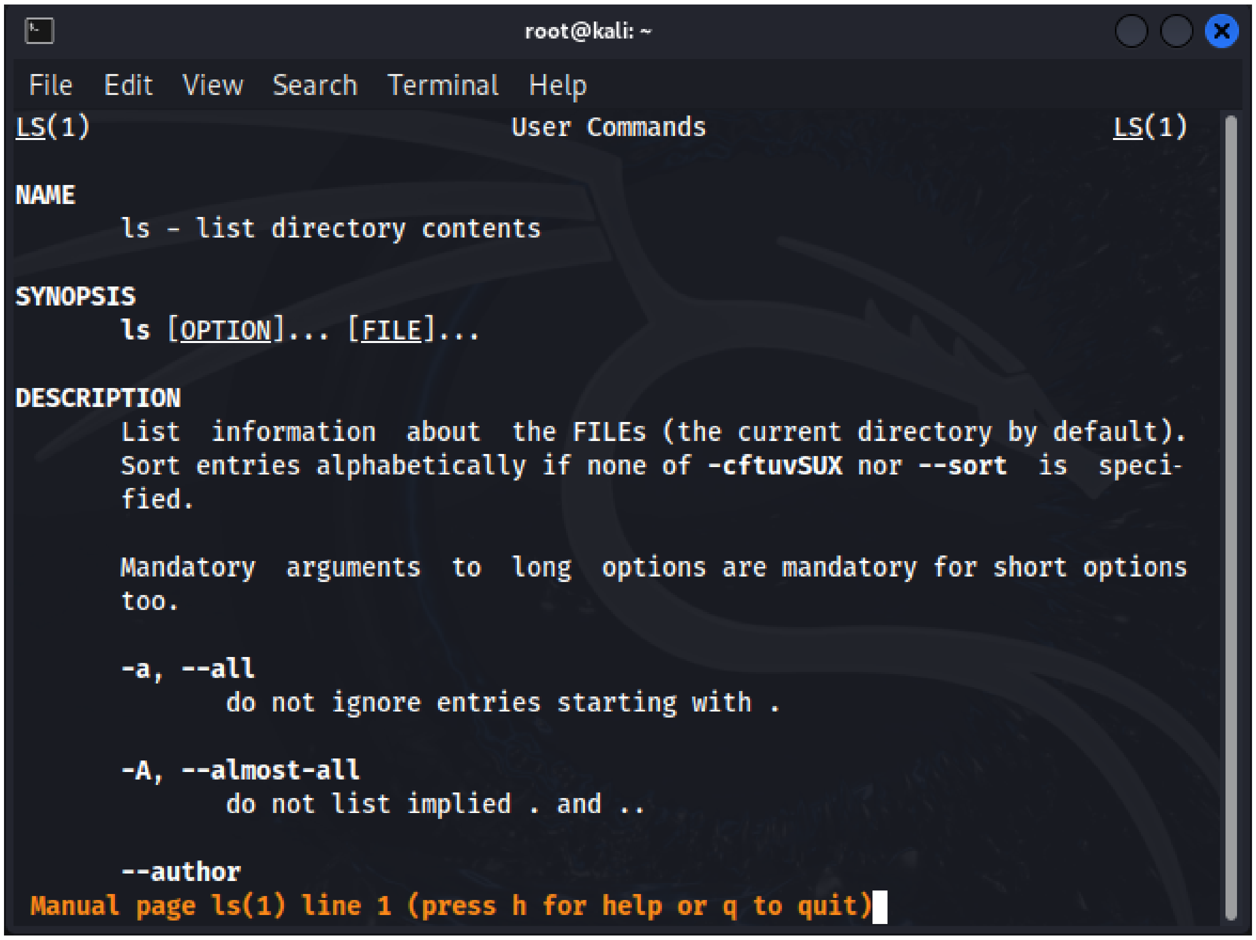
```
┌──(root㉿kali)-[~]
└─# which cat
/usr/bin/cat

┌──(root㉿kali)-[~]
└─# which ifconfig
/usr/sbin/ifconfig

┌──(root㉿kali)-[~]
└─#
```

➢ Sudo & Root:

- **Sudo** is used to run commands with administrative permissions.
- Root can run all commands in /sbin.
- A non-root user can run them only if root has granted permission.

➢ Manual Pages (man):

- Every command in linux has a **manual page** (documentation).
- **Example: man ls**

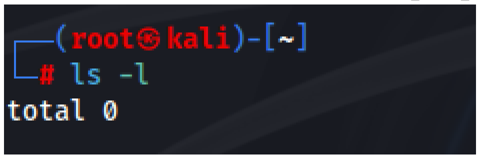


```
LS(1)                        User Commands                        LS(1)

NAME
       ls - list directory contents

SYNOPSIS
       ls [OPTION]... [FILE]...

DESCRIPTION
       List  information  about  the FILEs (the current directory by default).
       Sort entries alphabetically if none of -cftuvSUX nor --sort  is  speci-
       fied.

       Mandatory  arguments  to  long  options are mandatory for short options
       too.

       -a, --all
              do not ignore entries starting with .

       -A, --almost-all
              do not list implied . and ..

       --author
 Manual page ls(1) line 1 (press h for help or q to quit)
```

- In the **Synopsis** section of the manual, the **bold text means mandatory arguments.**

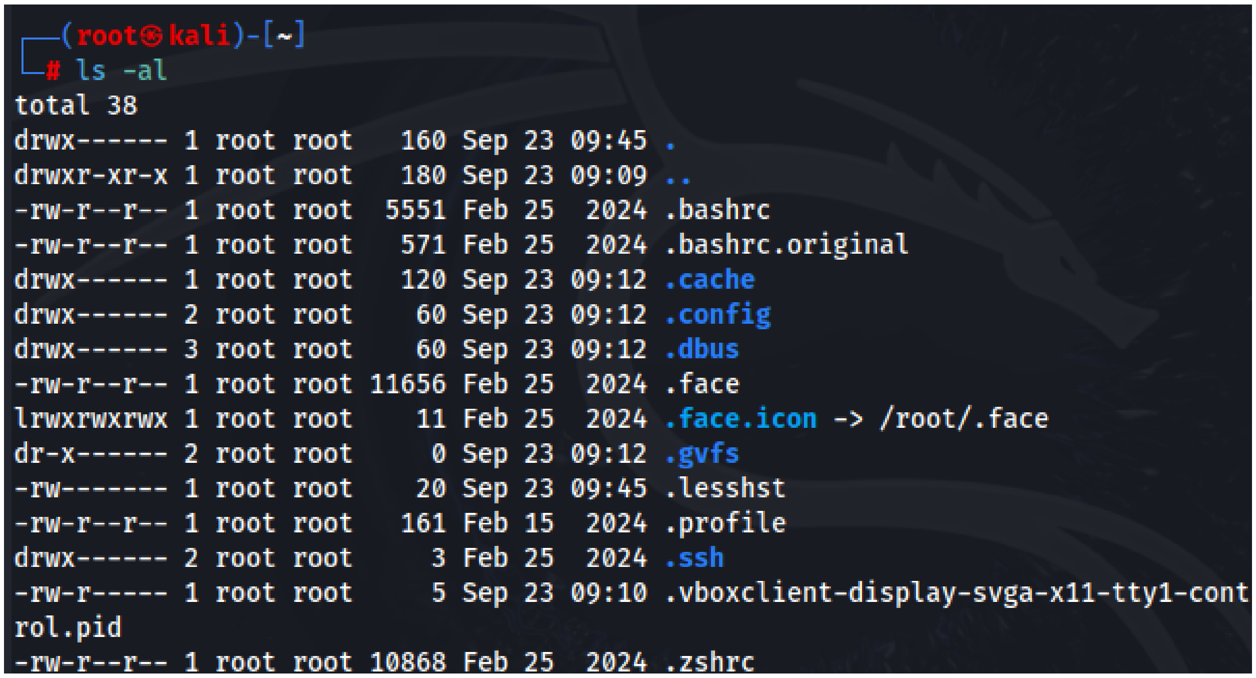
➢ File Properties:

- To see file and directories properties **ls –l:**



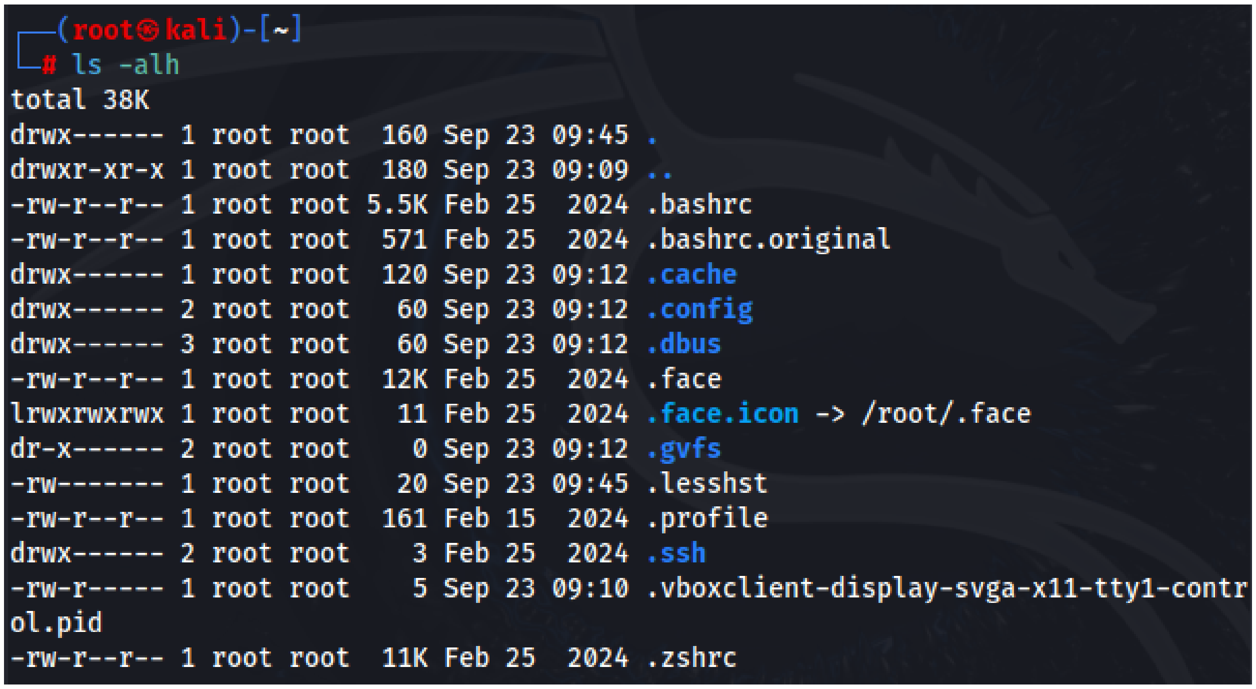
```
┌──(root㉿kali)-[~]
└─# ls -l
total 0
```

- To include hidden files **ls –al:**



```
┌──(root㉿kali)-[~]
└─# ls -al
total 38
drwx------ 1 root root   160 Sep 23 09:45 .
drwxr-xr-x 1 root root   180 Sep 23 09:09 ..
-rw-r--r-- 1 root root  5551 Feb 25  2024 .bashrc
-rw-r--r-- 1 root root   571 Feb 25  2024 .bashrc.original
drwx------ 1 root root   120 Sep 23 09:12 .cache
drwx------ 2 root root    60 Sep 23 09:12 .config
drwx------ 3 root root    60 Sep 23 09:12 .dbus
-rw-r--r-- 1 root root 11656 Feb 25  2024 .face
lrwxrwxrwx 1 root root    11 Feb 25  2024 .face.icon -> /root/.face
dr-x------ 2 root root     0 Sep 23 09:12 .gvfs
-rw------- 1 root root    20 Sep 23 09:45 .lesshst
-rw-r--r-- 1 root root   161 Feb 15  2024 .profile
drwx------ 2 root root     3 Feb 25  2024 .ssh
-rw-r----- 1 root root     5 Sep 23 09:10 .vboxclient-display-svga-x11-tty1-cont
rol.pid
-rw-r--r-- 1 root root 10868 Feb 25  2024 .zshrc
```

- To see **human-readable sizes** (KB, MB, GB) **ls –alh:**

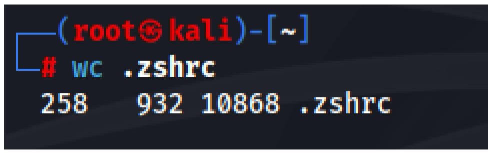


```
┌──(root㉿kali)-[~]
└─# ls -alh
total 38K
drwx------ 1 root root  160 Sep 23 09:45 .
drwxr-xr-x 1 root root  180 Sep 23 09:09 ..
-rw-r--r-- 1 root root 5.5K Feb 25  2024 .bashrc
-rw-r--r-- 1 root root  571 Feb 25  2024 .bashrc.original
drwx------ 1 root root  120 Sep 23 09:12 .cache
drwx------ 2 root root   60 Sep 23 09:12 .config
drwx------ 3 root root   60 Sep 23 09:12 .dbus
-rw-r--r-- 1 root root  12K Feb 25  2024 .face
lrwxrwxrwx 1 root root   11 Feb 25  2024 .face.icon -> /root/.face
dr-x------ 2 root root    0 Sep 23 09:12 .gvfs
-rw------- 1 root root   20 Sep 23 09:45 .lesshst
-rw-r--r-- 1 root root  161 Feb 15  2024 .profile
drwx------ 2 root root    3 Feb 25  2024 .ssh
-rw-r----- 1 root root    5 Sep 23 09:10 .vboxclient-display-svga-x11-tty1-contr
ol.pid
-rw-r--r-- 1 root root  11K Feb 25  2024 .zshrc
```

-rw-r--r-- 1 root root 10868 Feb 25 2024 .zshrc						
-rw-r--r--	**1**	**root**	**root**	**10868**	**Feb 25 2024**	**.zshrc**
File Permissions	Number of links	Owner	Group Member Ship	File size (bytes)	Last Modified Date and Time	File Name

➢ Word Count (wc):

- To count lines, words, and characters in a file **wc filename:**

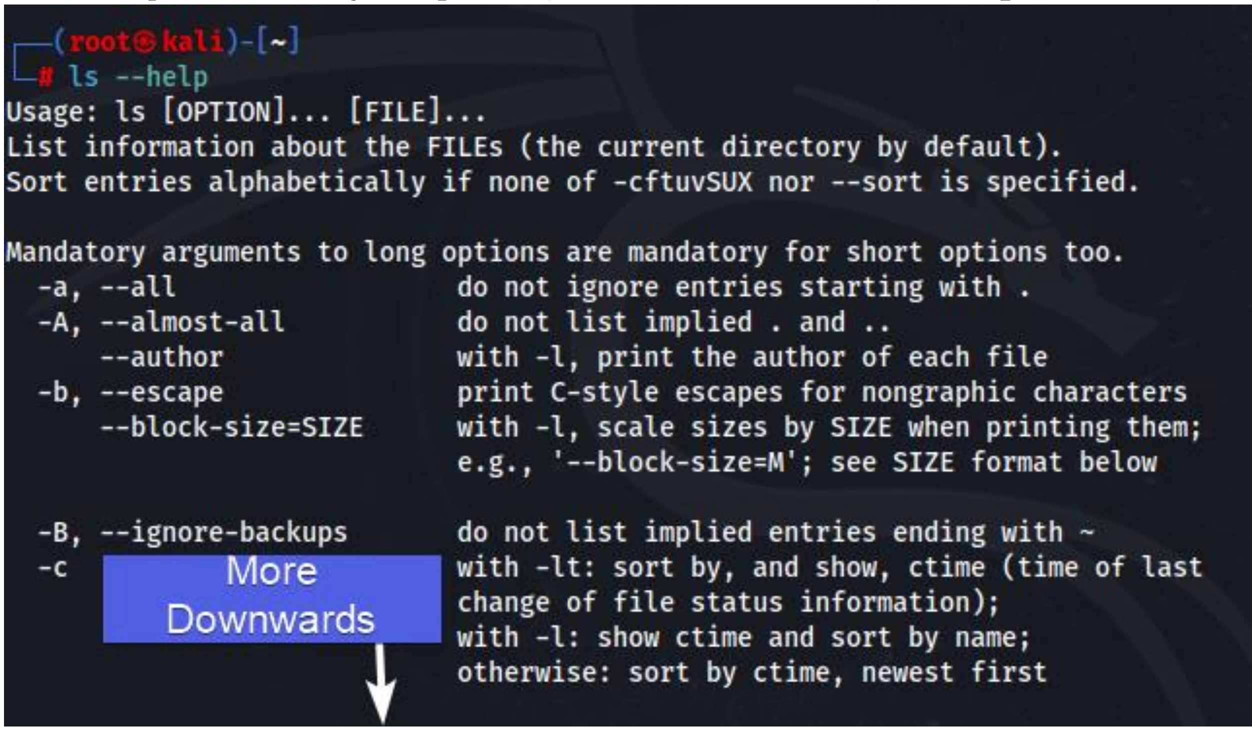


```
┌──(root㉿kali)-[~]
└─# wc .zshrc
 258   932 10868 .zshrc
```

258 932 10868 .zshrc		
258	**932**	**10868**
Lines	Words	Characters

➢ Quick Help:

- To see a quick summary of options (instead of full manual) **ls –help:**



```
┌──(root㉿kali)-[~]
└─# ls --help
Usage: ls [OPTION]... [FILE]...
List information about the FILEs (the current directory by default).
Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.

Mandatory arguments to long options are mandatory for short options too.
  -a, --all                  do not ignore entries starting with .
  -A, --almost-all           do not list implied . and ..
      --author               with -l, print the author of each file
  -b, --escape               print C-style escapes for nongraphic characters
      --block-size=SIZE      with -l, scale sizes by SIZE when printing them;
                             e.g., '--block-size=M'; see SIZE format below

  -B, --ignore-backups       do not list implied entries ending with ~
  -c                         with -lt: sort by, and show, ctime (time of last
                             change of file status information);
                             with -l: show ctime and sort by name;
                             otherwise: sort by ctime, newest first
```

Processes and Services:

- To list running services/processes:
  - **Ps -aux**
- To view output **page by page:**
  - **Ps -aux | more**
- To monitor system performance in real time:
  - **top**
  - This shows processes sorted by **CPU** and **memory usage.**
  - To quit **top,** press **q.**

Zombie Process:

- A **zombie process** is a child process whose **parent process has already terminated.**
- Since it has no parent to clean it up, it lingers until the system reclaims it.

Quit Commands:

- In most Linux help/manual/programs (like man, more, top), you can quit by pressing:
  - **q**

23RD September 2025.

Permissions Overview:

- In Linux file and directory permissions are represented like this:
  - **-rw-r--r--**
- This string has a total of 10 characters:
  - The **first character** is the **file type (nature)**, not part of permissions.

-	**d**	**l**
regular file	directory	symbolic link

  - The next **9 characters** represent permissions.

Permission Types:

r	**w**	**x**	**-**
Read	Write	Execute	No Permission

The order is always the same: **read → write → execute**

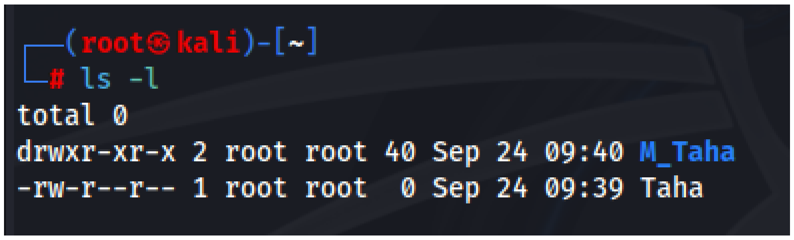
Permission Groups:

- Permissions are divided into three sets:
  - **Owner (user)** → the user who owns the file.
  - **Group** → other users in the same group.
  - **Others** → all other users.
- **Example:**

rw-	**r--**	**r--**
Owner can read and write	Group can only read	Other users can only read

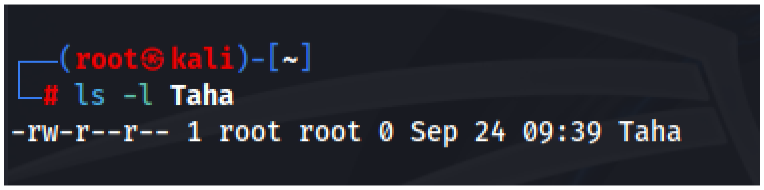
➢ Checking Permissions:

- To see file and directories permissions **ls –l:**



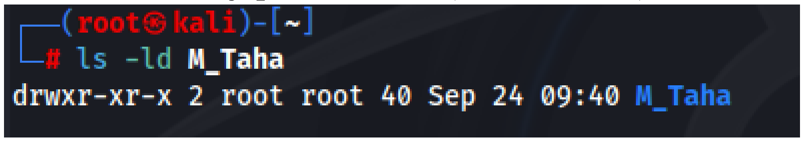
```
┌──(root㉿kali)-[~]
└─# ls -l
total 0
drwxr-xr-x 2 root root 40 Sep 24 09:40 M_Taha
-rw-r--r-- 1 root root  0 Sep 24 09:39 Taha
```

- To see file permissions **ls –l [filename].**



```
┌──(root㉿kali)-[~]
└─# ls -l Taha
-rw-r--r-- 1 root root 0 Sep 24 09:39 Taha
```

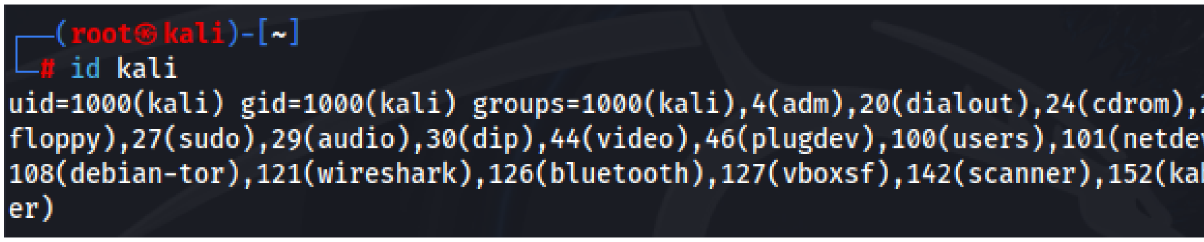
- To see directory permissions (not contents) **ls -ld [dirname].**



```
┌──(root㉿kali)-[~]
└─# ls -ld M_Taha
drwxr-xr-x 2 root root 40 Sep 24 09:40 M_Taha
```

➢ Groups in Linux:

- In **Windows,** new users are added to predefined groups.
- In **Linux,** when new user is created, a **new group with the same name** is also created by default.
- To check which group a user belongs to:
    - **id username**



```
┌──(root㉿kali)-[~]
└─# id kali
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),
floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netde
108(debian-tor),121(wireshark),126(bluetooth),127(vboxsf),142(scanner),152(kal
er)
```

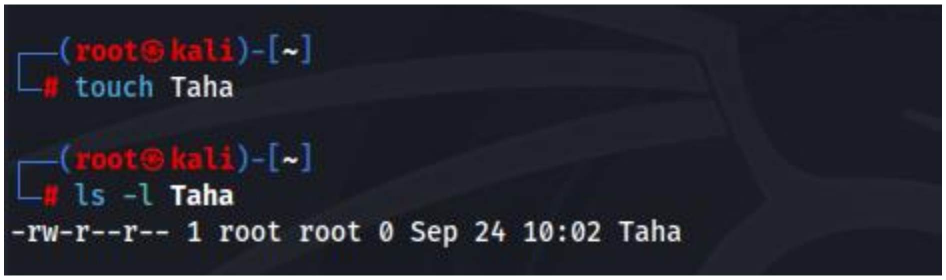
➢ Changing Permissions:

- Permissions can be represented by numbers:

Read(r)	**Write(w)**	**Execute(x)**	**No Permission(-)**
4	**2**	**1**	**0**

- Add the values together for each group.
- **Example:**
    1. **Create a file:**

- **touch Taha**
- Default Permissions are: **-rw-r--r—**

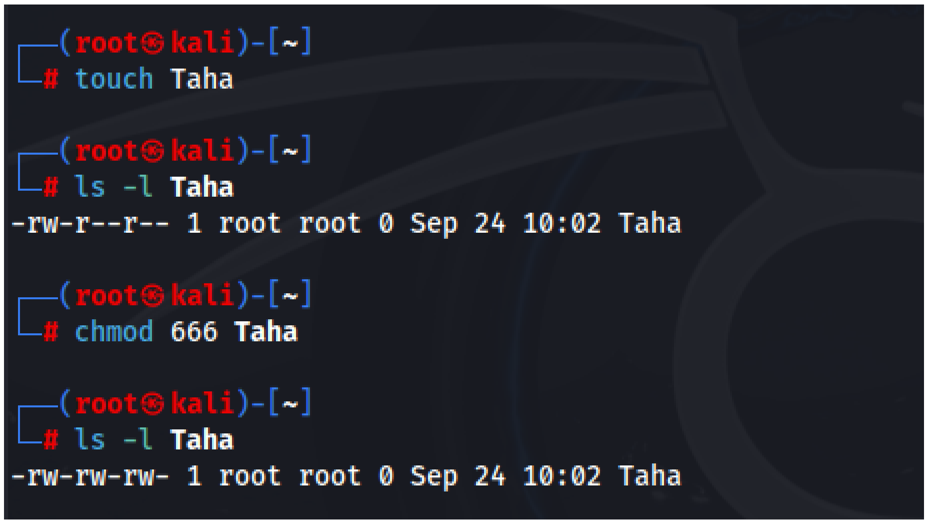


```
┌──(root㉿kali)-[~]
└─# touch Taha

┌──(root㉿kali)-[~]
└─# ls -l Taha
-rw-r--r-- 1 root root 0 Sep 24 10:02 Taha
```

2. If we want **owner, group, and others to have read + write (rw- rw- rw-):**

Owner	Group	Others
r(4)+w(2)	**r(4)+w(2)**	**r(4)+w(2)**
6	**6**	**6**

3. **Change Permissions:**
   - **chmod 666 Taha**
   - New Permissions: **-rw-rw-rw-**



```
┌──(root㉿kali)-[~]
└─# touch Taha

┌──(root㉿kali)-[~]
└─# ls -l Taha
-rw-r--r-- 1 root root 0 Sep 24 10:02 Taha

┌──(root㉿kali)-[~]
└─# chmod 666 Taha

┌──(root㉿kali)-[~]
└─# ls -l Taha
-rw-rw-rw- 1 root root 0 Sep 24 10:02 Taha
```