VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

SMART BRIDGE – Ethical Hacking

Title: Linux Command List Assessment

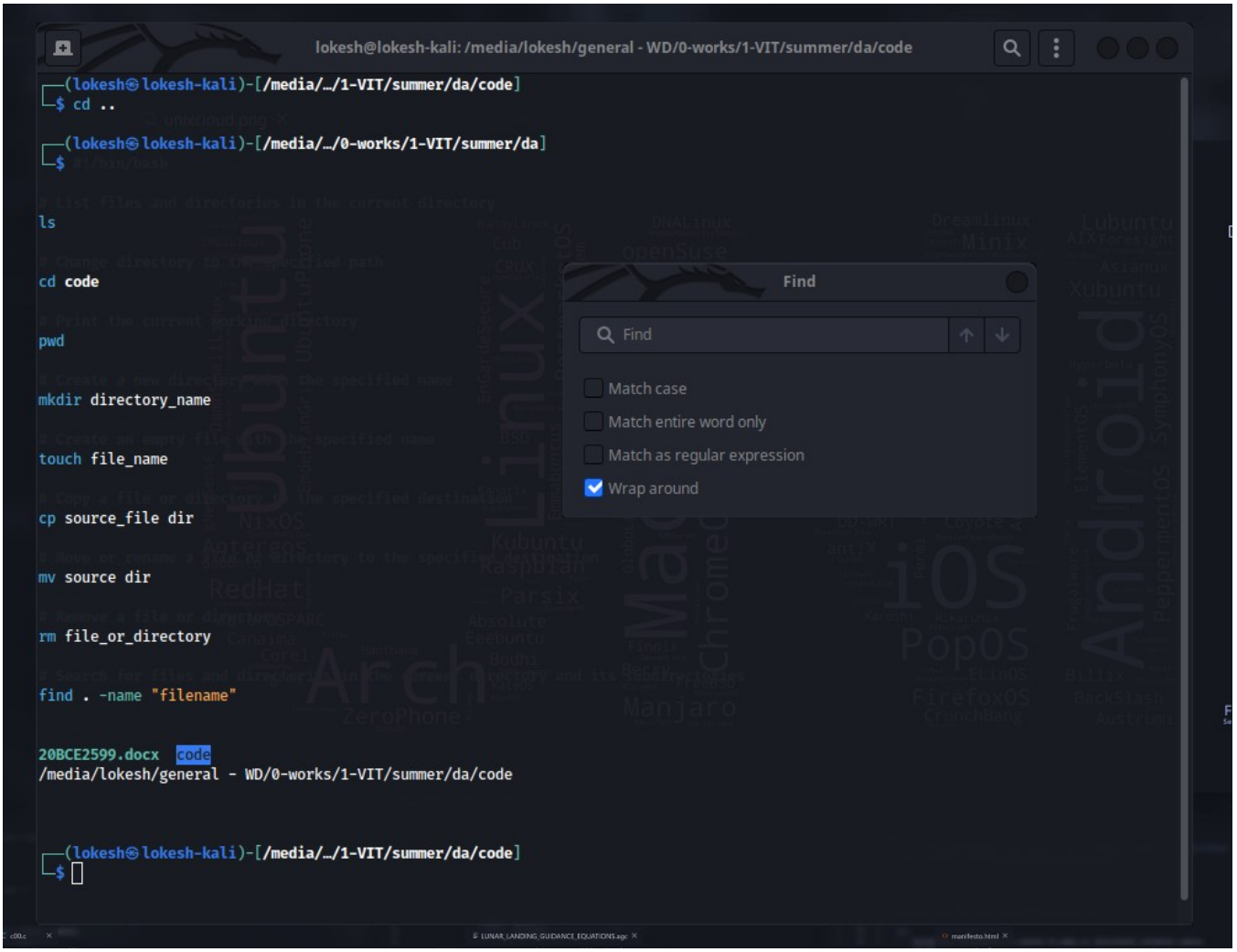
NAME : **LOKESHWARAN M**
REG NO : **20BCE2599**
DATE : **22-5-2023**
SCHOOL : **SCOPE**

File and Directory Operations

Bash script :

```bash
#!/bin/bash

# List files and directories in the current directory
ls

# Change directory to the specified path
cd directory

# Print the current working directory
pwd

# Create a new directory with the specified name
mkdir directory_name

# Create an empty file with the specified name
touch file_name

# Copy a file or directory to the specified destination
cp source_file destination

# Move or rename a file or directory to the specified destination
mv source destination

# Remove a file or directory
rm file_or_directory

# Search for files and directories in the current directory and its subdirectories
find . -name "filename"
```

Output :


lokesh@lokesh-kali: /media/lokesh/general - WD/0-works/1-VIT/summer/da/code
(lokesh㉿lokesh-kali)-[/media/…/1-VIT/summer/da/code]
$ cd ..
(lokesh㉿lokesh-kali)-[/media/…/0-works/1-VIT/summer/da]
$
ls
cd code
pwd
mkdir directory_name
touch file_name
cp source_file dir
mv source dir
rm file_or_directory
find . -name "filename"
20BCE2599.docx code
/media/lokesh/general - WD/0-works/1-VIT/summer/da/code
(lokesh㉿lokesh-kali)-[/media/…/1-VIT/summer/da/code]
$
Find
Find
Match case
Match entire word only
Match as regular expression
Wrap around

Explanition :

This bash script performs various file and directory operations using the following commands:

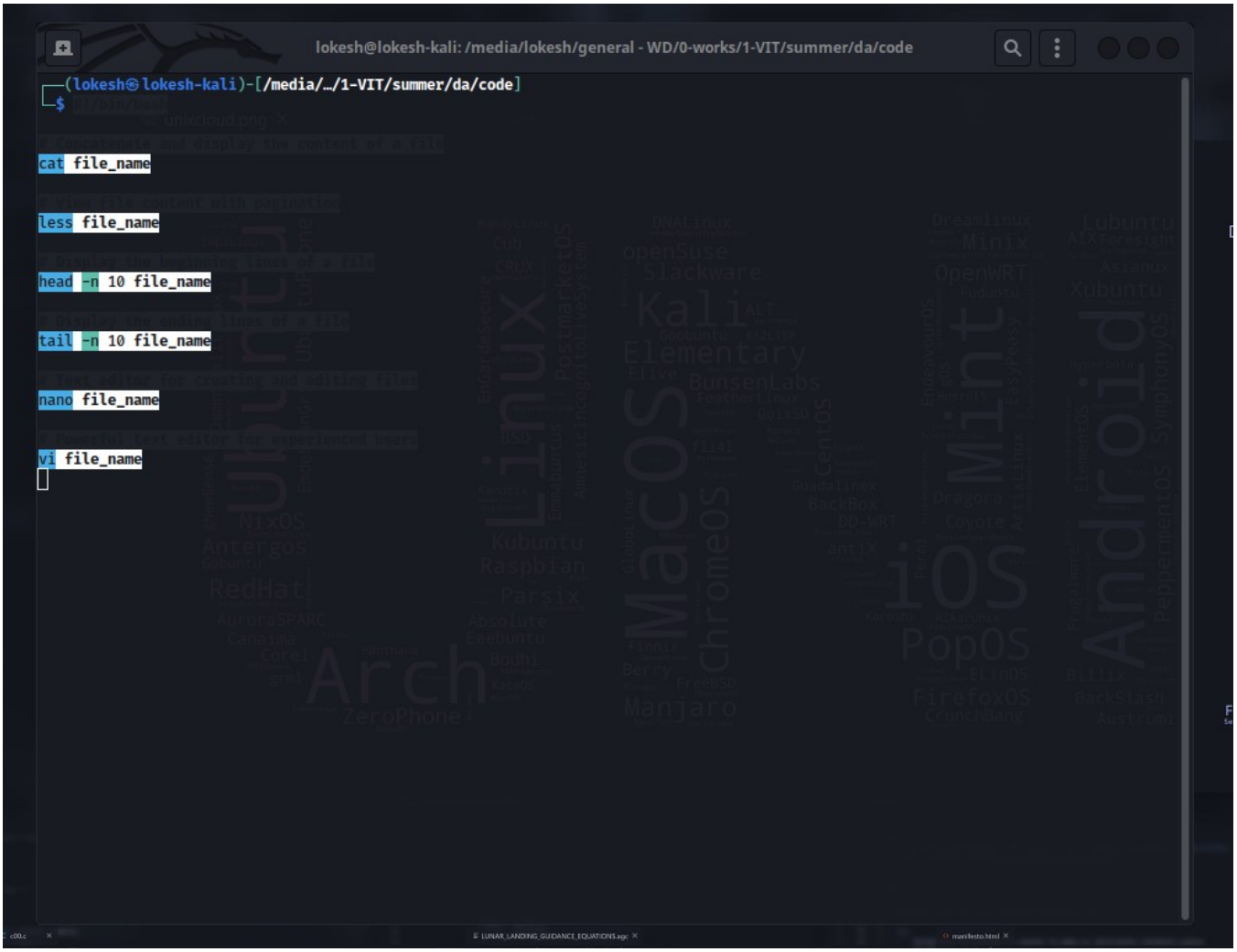
ls: Lists files and directories in the current directory.
cd: Changes the current directory to the specified path.
pwd: Prints the current working directory.
mkdir: Creates a new directory with the specified name.
touch: Creates an empty file with the specified name.
cp: Copies a file or directory to the specified destination.
mv: Moves or renames a file or directory to the specified destination.
rm: Removes a file or directory.
find: Searches for files and directories in the current directory and its subdirectories based on the specified criteria (in this case, searching for a file with a specific filename).

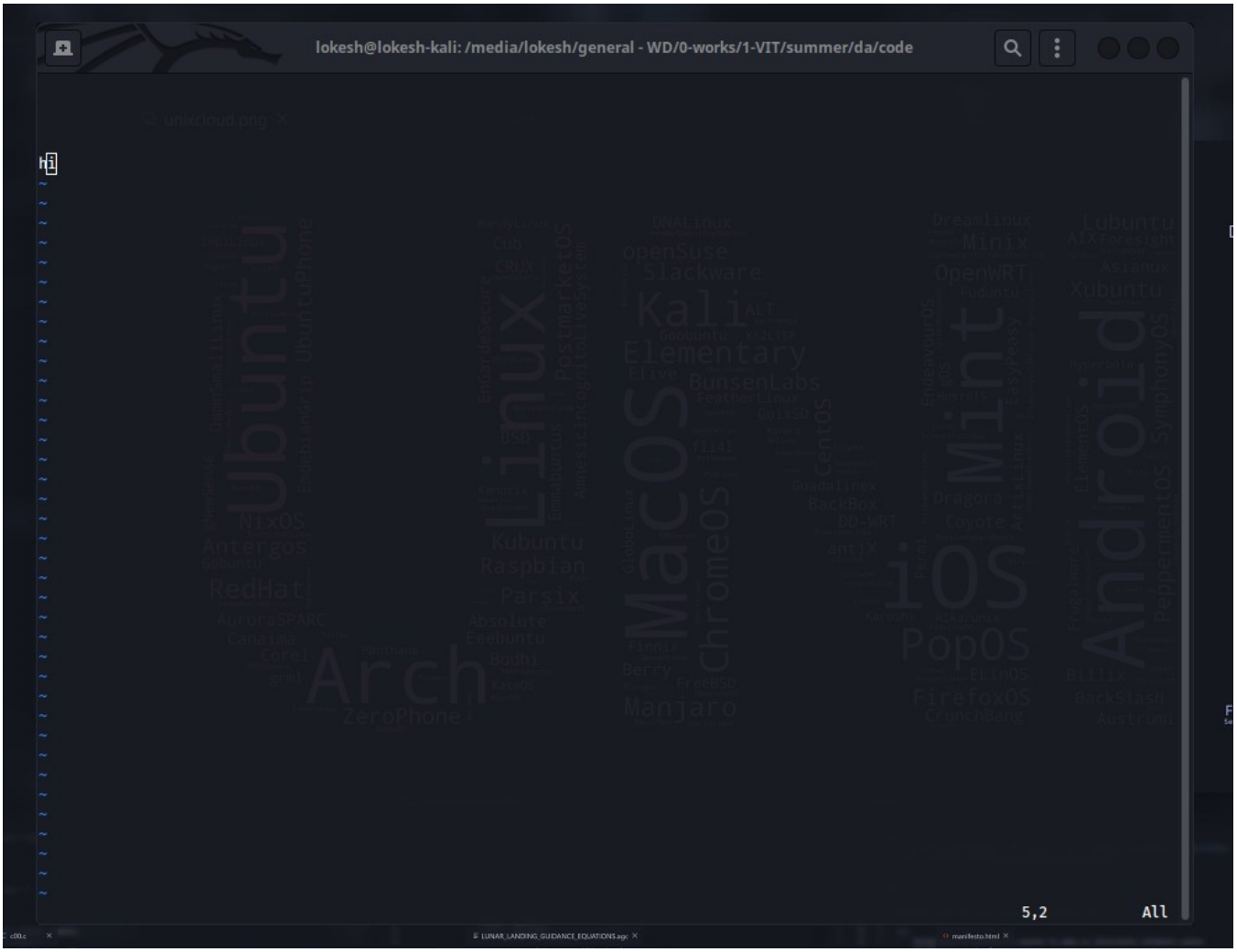
File Viewing and Editing :

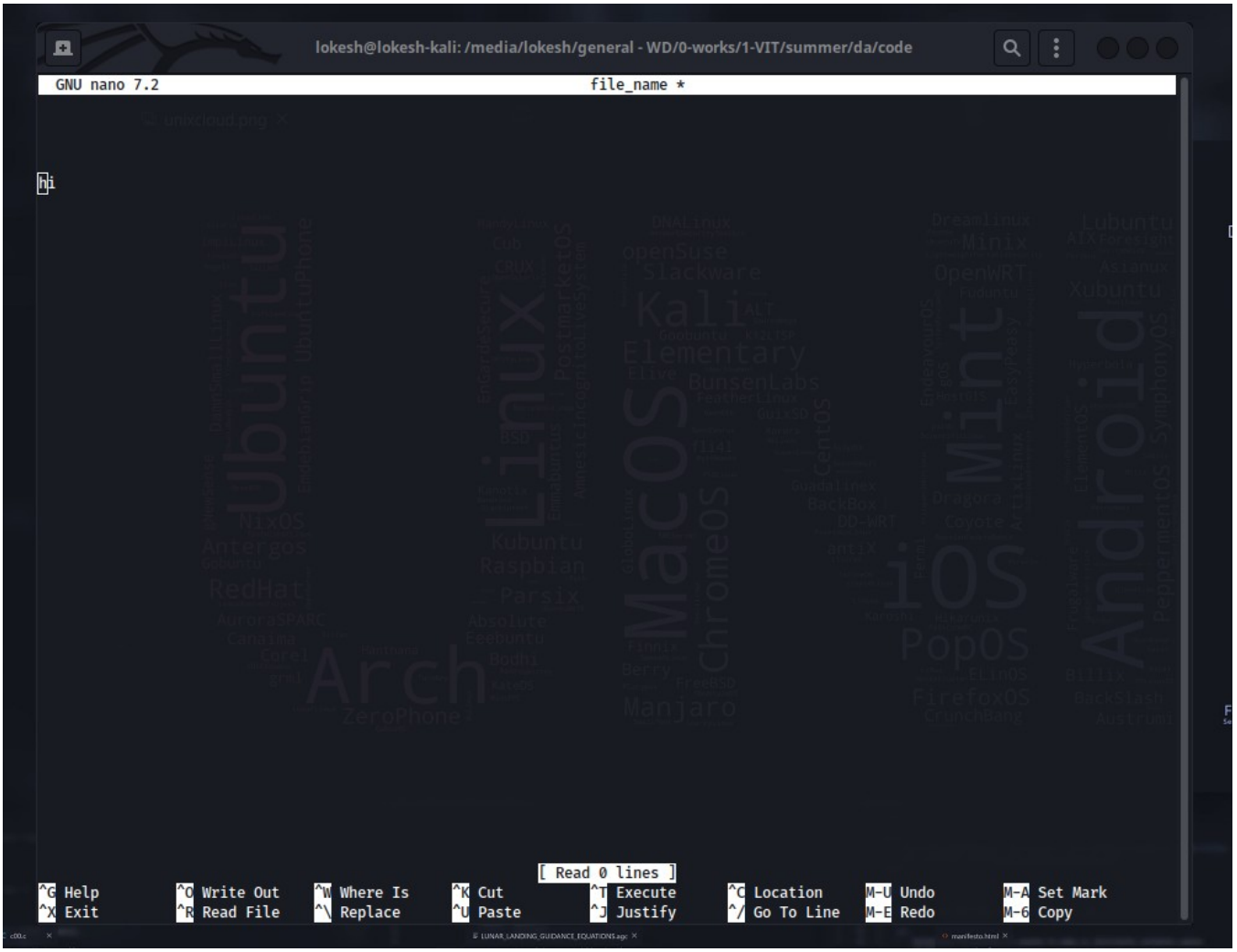
Bash script :

```
#!/bin/bash

# Concatenate and display the content of a file
cat file_name

# View file content with pagination
less file_name

# Display the beginning lines of a file
head -n 10 file_name

# Display the ending lines of a file
tail -n 10 file_name

# Text editor for creating and editing files
nano file_name

# Powerful text editor for experienced users
vi file_name
```

Output :


lokesh@lokesh-kali: /media/lokesh/general - WD/0-works/1-VIT/summer/da/code
(lokesh㉿lokesh-kali)-[/media/…/1-VIT/summer/da/code]
$
cat file_name
less file_name
head -n 10 file_name
tail -n 10 file_name
nano file_name
vi file_name


lokesh@lokesh-kali: /media/lokesh/general - WD/0-works/1-VIT/summer/da/code
hi
5,2
All



Explanition :

This bash script demonstrates various file viewing and editing operations using the following commands:

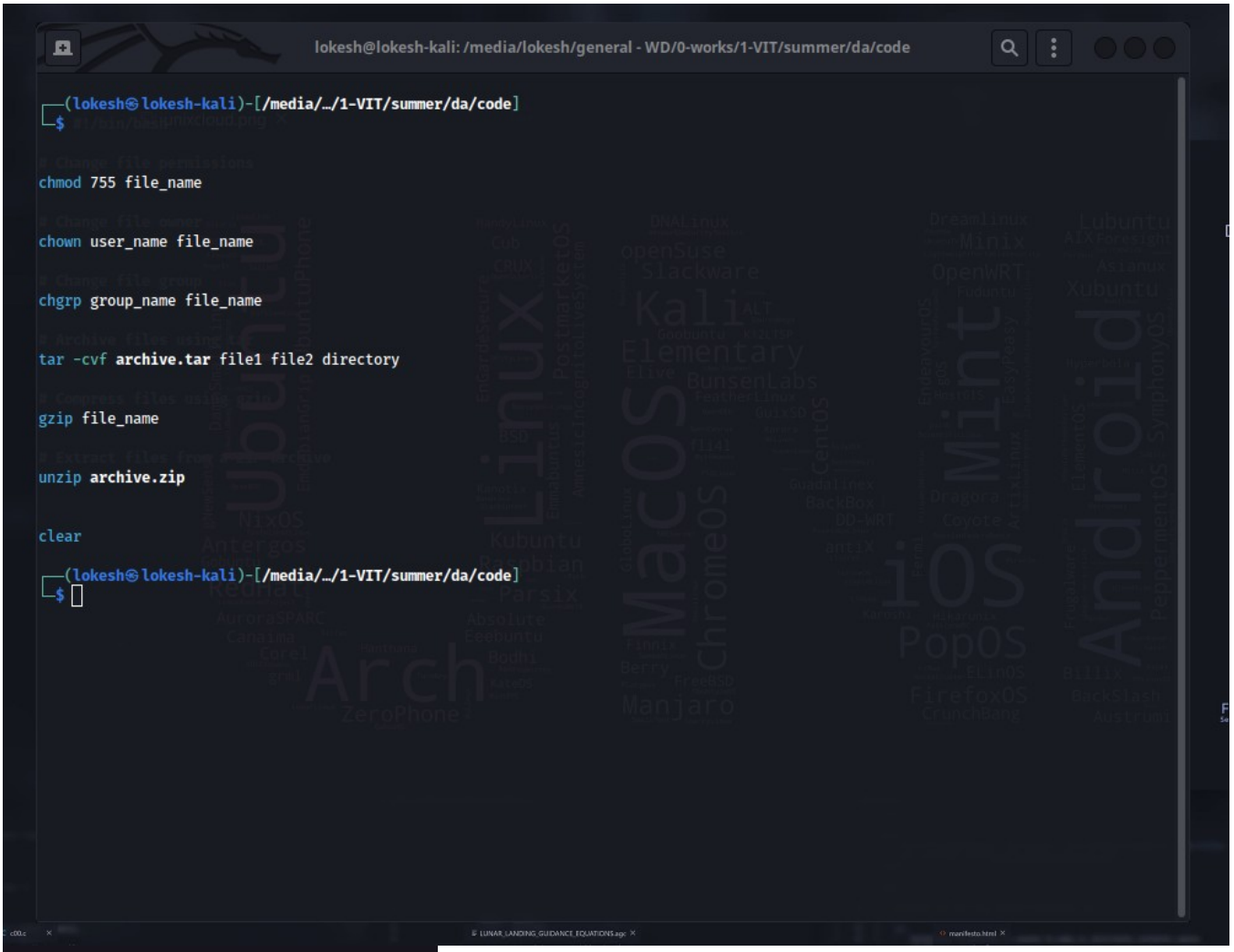
cat: Concatenates and displays the content of a file.
less: Displays the content of a file with pagination, allowing scrolling through the file.
head: Displays the beginning lines of a file. In this example, it shows the first 10 lines of the file.
tail: Displays the ending lines of a file. In this example, it shows the last 10 lines of the file.
nano: Opens the specified file in the nano text editor, which is a simple and user-friendly editor for creating and editing files.
vi/vim: Opens the specified file in the vi or vim text editor, which is a powerful and versatile editor preferred by experienced users.
Each command is accompanied by a comment explaining its purpose within the script.

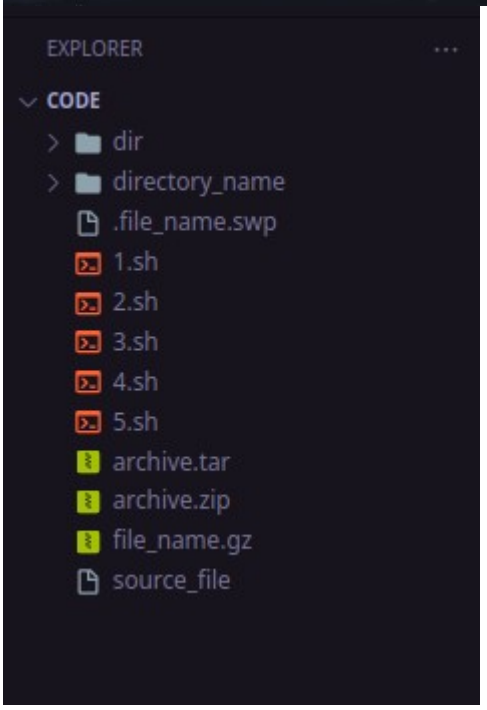
File Permissions abd File Compression and Archiving :

Bash script :

```
#!/bin/bash

# Change file permissions
chmod 755 file_name

# Change file owner
chown user_name file_name

# Change file group
chgrp group_name file_name

# Archive files using tar
tar -cvf archive.tar file1 file2 directory

# Compress files using gzip
gzip file_name

# Extract files from a ZIP archive
unzip archive.zip
```

Output :


lokesh@lokesh-kali: /media/lokesh/general - WD/0-works/1-VIT/summer/da/code
(lokesh㉿lokesh-kali)-[/media/…/1-VIT/summer/da/code]
$
chmod 755 file_name
chown user_name file_name
chgrp group_name file_name
tar -cvf archive.tar file1 file2 directory
gzip file_name
unzip archive.zip
clear
(lokesh㉿lokesh-kali)-[/media/…/1-VIT/summer/da/code]
$


EXPLORER
CODE
dir
directory_name
.file_name.swp
1.sh
2.sh
3.sh
4.sh
5.sh
archive.tar
archive.zip
file_name.gz
source_file

Explanition :

This bash script demonstrates various file permission, compression, and archiving operations using the following commands:

File Permissions:

chmod: Changes the permissions of a file. In this example, it sets the permissions to 755 for the specified file, allowing read, write, and execute permissions for the owner, and read and execute permissions for group and others.
File Ownership:

chown: Changes the owner of a file. It assigns the specified user_name as the owner of the file_name.
File Group:

chgrp: Changes the group ownership of a file. It assigns the specified group_name as the group owner of the file_name.
File Compression and Archiving:

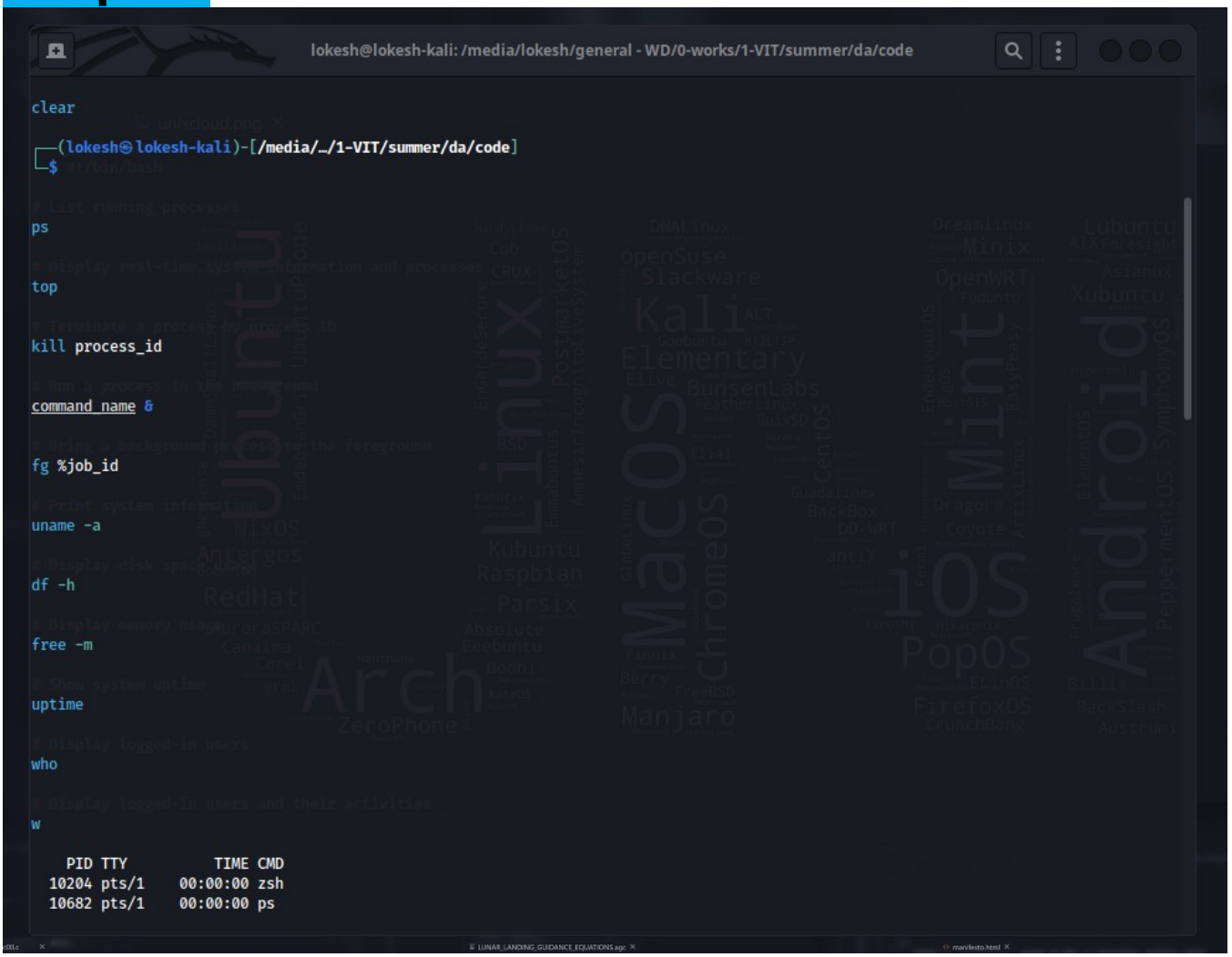
tar: Archives files and directories into a tar archive. In this example, it creates an archive named archive.tar containing file1, file2, and directory.
gzip: Compresses a file using the gzip algorithm. The file_name specified will be compressed and renamed with the extension .gz.
unzip: Extracts files from a ZIP archive. It unzips the contents of archive.zip into the current directory.

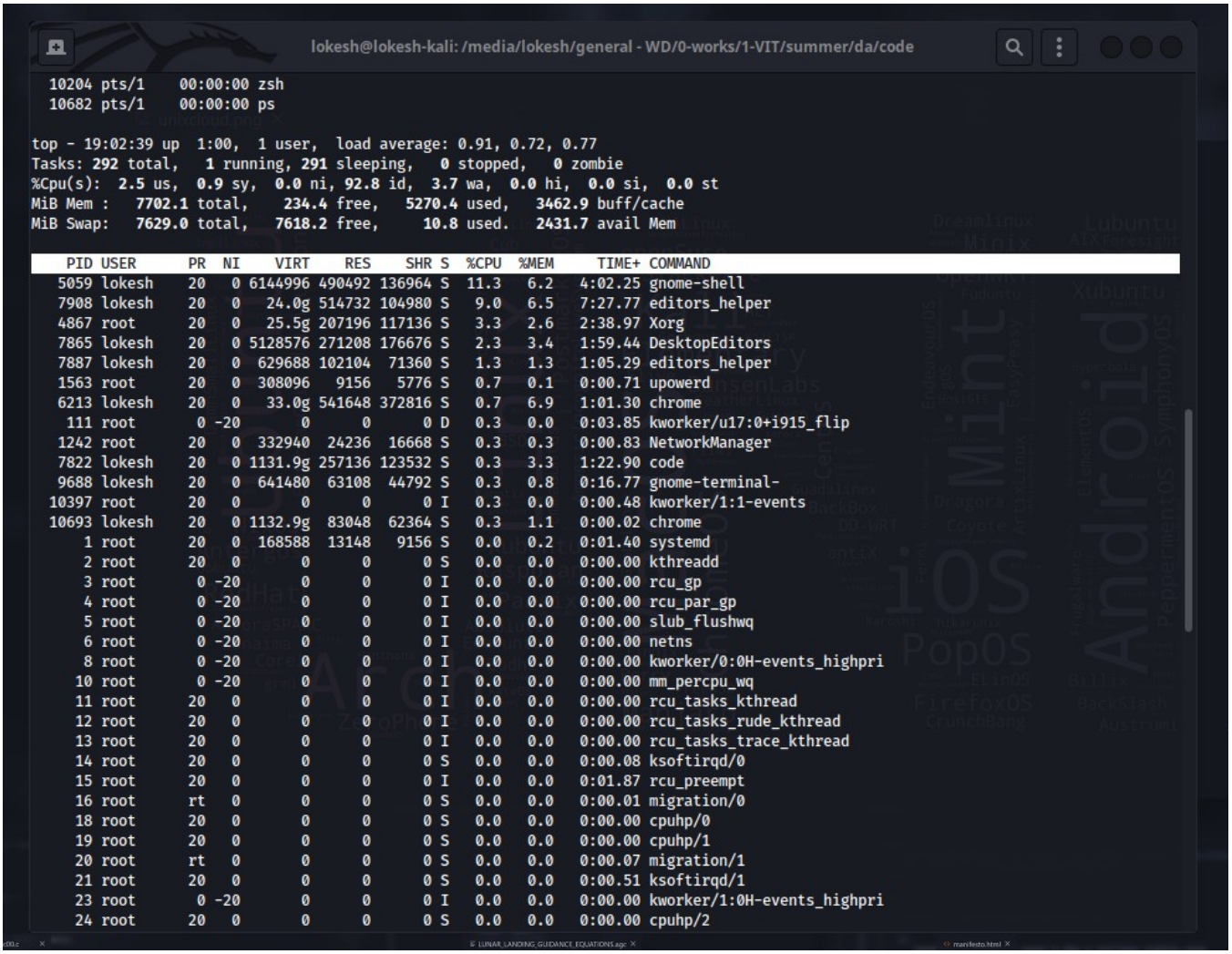
Process Management and System Information:

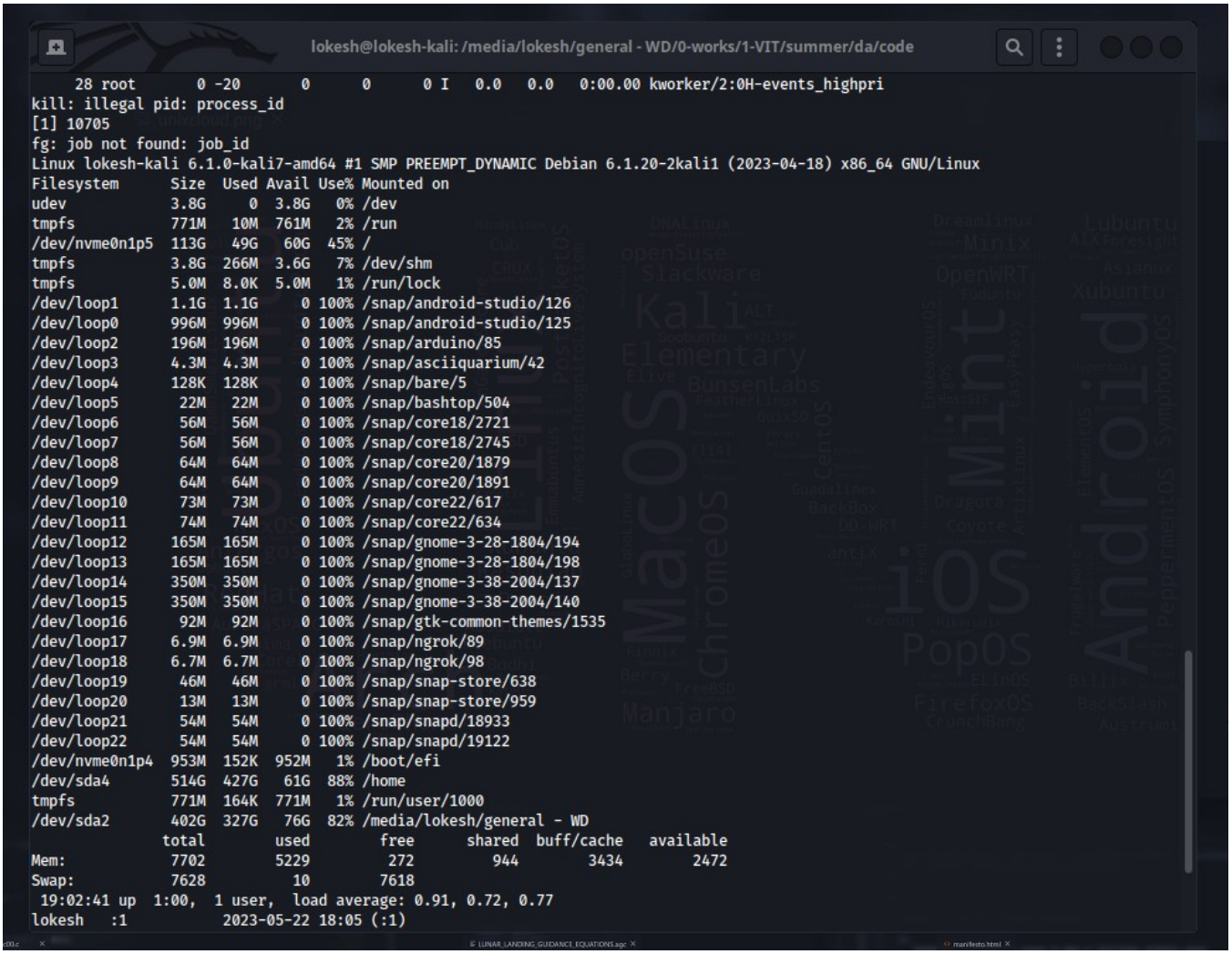
Bash script :

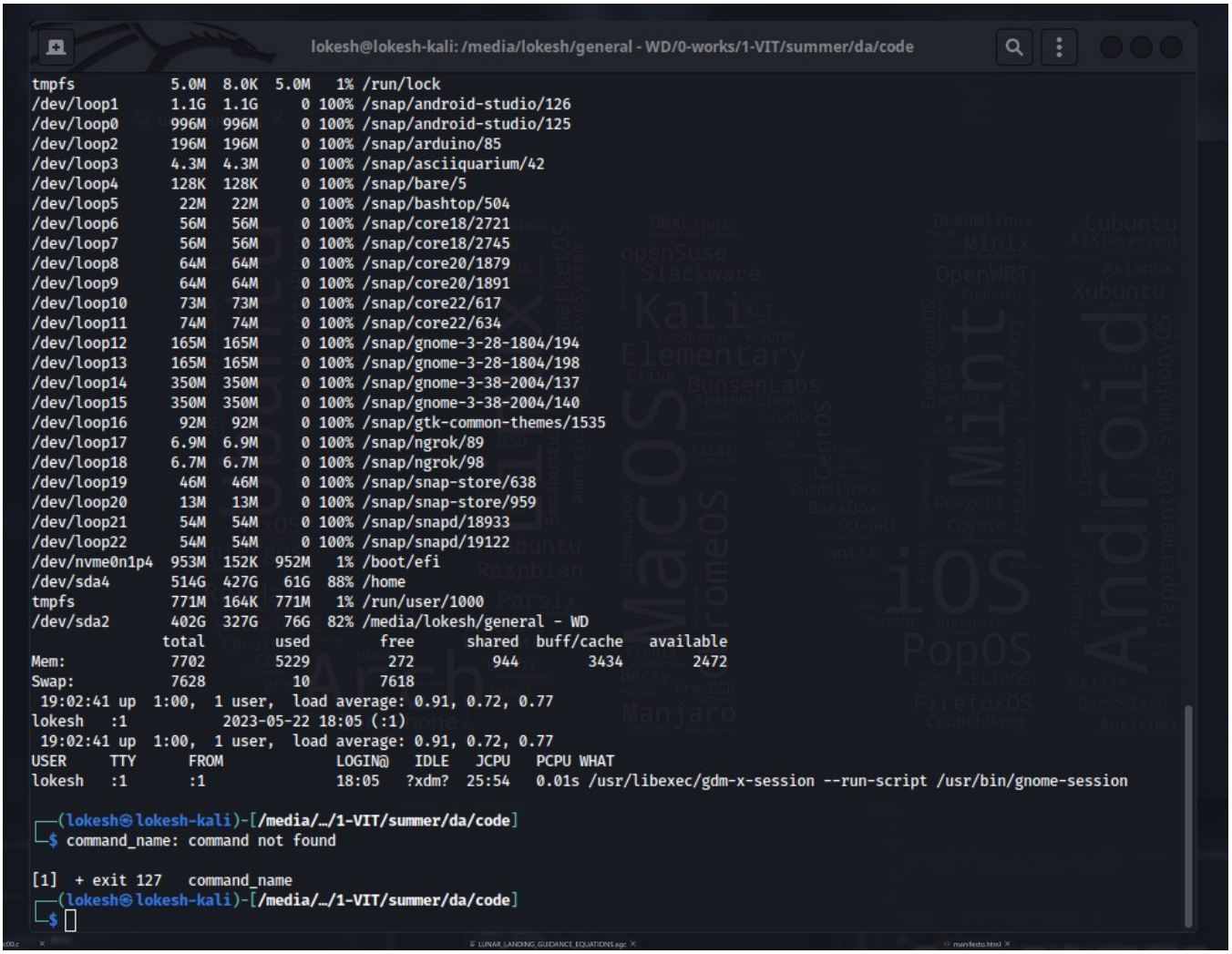
```
#!/bin/bash

# List running processes
ps

# Display real-time system information and processes
top

# Terminate a process by process ID
kill process_id

# Run a process in the background
command_name &

# Bring a background process to the foreground
fg %job_id

# Print system information
uname -a

# Display disk space usage
df -h

# Display memory usage
free -m

# Show system uptime
uptime

# Display logged-in users
who

# Display logged-in users and their activities
w
```

Output :


lokesh@lokesh-kali: /media/lokesh/general - WD/0-works/1-VIT/summer/da/code
clear
(lokesh㉿lokesh-kali)-[/media/.../1-VIT/summer/da/code]
$
ps
top
kill process_id
command_name &
fg %job_id
uname -a
df -h
free -m
uptime
who
w
PID TTY TIME CMD
10204 pts/1 00:00:00 zsh
10682 pts/1 00:00:00 ps


lokesh@lokesh-kali: /media/lokesh/general - WD/0-works/1-VIT/summer/da/code
10204 pts/1 00:00:00 zsh
10682 pts/1 00:00:00 ps
top - 19:02:39 up 1:00, 1 user, load average: 0.91, 0.72, 0.77
Tasks: 292 total, 1 running, 291 sleeping, 0 stopped, 0 zombie
%Cpu(s): 2.5 us, 0.9 sy, 0.0 ni, 92.8 id, 3.7 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 7702.1 total, 234.4 free, 5270.4 used, 3462.9 buff/cache
MiB Swap: 7629.0 total, 7618.2 free, 10.8 used. 2431.7 avail Mem
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
5059 lokesh 20 0 6144996 490492 136964 S 11.3 6.2 4:02.25 gnome-shell
7908 lokesh 20 0 24.0g 514732 104980 S 9.0 6.5 7:27.77 editors_helper
4867 root 20 0 25.5g 207196 117136 S 3.3 2.6 2:38.97 Xorg
7865 lokesh 20 0 5128576 271208 176676 S 2.3 3.4 1:59.44 DesktopEditors
7887 lokesh 20 0 629688 102104 71360 S 1.3 1.3 1:05.29 editors_helper
1563 root 20 0 308096 9156 5776 S 0.7 0.1 0:00.71 upowerd
6213 lokesh 20 0 33.0g 541648 372816 S 0.7 6.9 1:01.30 chrome
111 root 0 -20 0 0 0 D 0.3 0.0 0:03.85 kworker/u17:0+i915_flip
1242 root 20 0 332940 24236 16668 S 0.3 0.3 0:00.83 NetworkManager
7822 lokesh 20 0 1131.9g 257136 123532 S 0.3 3.3 1:22.90 code
9688 lokesh 20 0 641480 63108 44792 S 0.3 0.8 0:16.77 gnome-terminal-
10397 root 20 0 0 0 0 I 0.3 0.0 0:00.48 kworker/1:1-events
10693 lokesh 20 0 1132.9g 83048 62364 S 0.3 1.1 0:00.02 chrome
1 root 20 0 168588 13148 9156 S 0.0 0.2 0:01.40 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kthreadd
3 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_gp
4 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_par_gp
5 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 slub_flushwq
6 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 netns
8 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kworker/0:0H-events_highpri
10 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 mm_percpu_wq
11 root 20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_kthread
12 root 20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_rude_kthread
13 root 20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_trace_kthread
14 root 20 0 0 0 0 S 0.0 0.0 0:00.08 ksoftirqd/0
15 root 20 0 0 0 0 I 0.0 0.0 0:01.87 rcu_preempt
16 root rt 0 0 0 0 S 0.0 0.0 0:00.01 migration/0
18 root 20 0 0 0 0 S 0.0 0.0 0:00.00 cpuhp/0
19 root 20 0 0 0 0 S 0.0 0.0 0:00.00 cpuhp/1
20 root rt 0 0 0 0 S 0.0 0.0 0:00.07 migration/1
21 root 20 0 0 0 0 S 0.0 0.0 0:00.51 ksoftirqd/1
23 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kworker/1:0H-events_highpri
24 root 20 0 0 0 0 S 0.0 0.0 0:00.00 cpuhp/2


lokesh@lokesh-kali: /media/lokesh/general - WD/0-works/1-VIT/summer/da/code
28 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kworker/2:0H-events_highpri
kill: illegal pid: process_id
[1] 10705
fg: job not found: job_id
Linux lokesh-kali 6.1.0-kali7-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.20-2kali1 (2023-04-18) x86_64 GNU/Linux
Filesystem Size Used Avail Use% Mounted on
udev 3.8G 0 3.8G 0% /dev
tmpfs 771M 10M 761M 2% /run
/dev/nvme0n1p5 113G 49G 60G 45% /
tmpfs 3.8G 266M 3.6G 7% /dev/shm
tmpfs 5.0M 8.0K 5.0M 1% /run/lock
/dev/loop1 1.1G 1.1G 0 100% /snap/android-studio/126
/dev/loop0 996M 996M 0 100% /snap/android-studio/125
/dev/loop2 196M 196M 0 100% /snap/arduino/85
/dev/loop3 4.3M 4.3M 0 100% /snap/asciiquarium/42
/dev/loop4 128K 128K 0 100% /snap/bare/5
/dev/loop5 22M 22M 0 100% /snap/bashtop/504
/dev/loop6 56M 56M 0 100% /snap/core18/2721
/dev/loop7 56M 56M 0 100% /snap/core18/2745
/dev/loop8 64M 64M 0 100% /snap/core20/1879
/dev/loop9 64M 64M 0 100% /snap/core20/1891
/dev/loop10 73M 73M 0 100% /snap/core22/617
/dev/loop11 74M 74M 0 100% /snap/core22/634
/dev/loop12 165M 165M 0 100% /snap/gnome-3-28-1804/194
/dev/loop13 165M 165M 0 100% /snap/gnome-3-28-1804/198
/dev/loop14 350M 350M 0 100% /snap/gnome-3-38-2004/137
/dev/loop15 350M 350M 0 100% /snap/gnome-3-38-2004/140
/dev/loop16 92M 92M 0 100% /snap/gtk-common-themes/1535
/dev/loop17 6.9M 6.9M 0 100% /snap/ngrok/89
/dev/loop18 6.7M 6.7M 0 100% /snap/ngrok/98
/dev/loop19 46M 46M 0 100% /snap/snap-store/638
/dev/loop20 13M 13M 0 100% /snap/snap-store/959
/dev/loop21 54M 54M 0 100% /snap/snapd/18933
/dev/loop22 54M 54M 0 100% /snap/snapd/19122
/dev/nvme0n1p4 953M 152K 952M 1% /boot/efi
/dev/sda4 514G 427G 61G 88% /home
tmpfs 771M 164K 771M 1% /run/user/1000
/dev/sda2 402G 327G 76G 82% /media/lokesh/general - WD
total used free shared buff/cache available
Mem: 7702 5229 272 944 3434 2472
Swap: 7628 10 7618
19:02:41 up 1:00, 1 user, load average: 0.91, 0.72, 0.77
lokesh :1 2023-05-22 18:05 (:1)



Explanition :

This bash script demonstrates various process management and system information operations using the following commands:

Process Management:

ps: Lists the currently running processes.
top: Displays real-time system information, including processes, CPU usage, and memory usage.
kill: Terminates a process using its process ID.
bg: Runs a process in the background.
fg: Brings a background process to the foreground.
System Information:

uname: Prints system information, including the kernel version, machine architecture, and operating system.
df: Displays disk space usage, showing the total size, used space, and available space for each mounted filesystem.

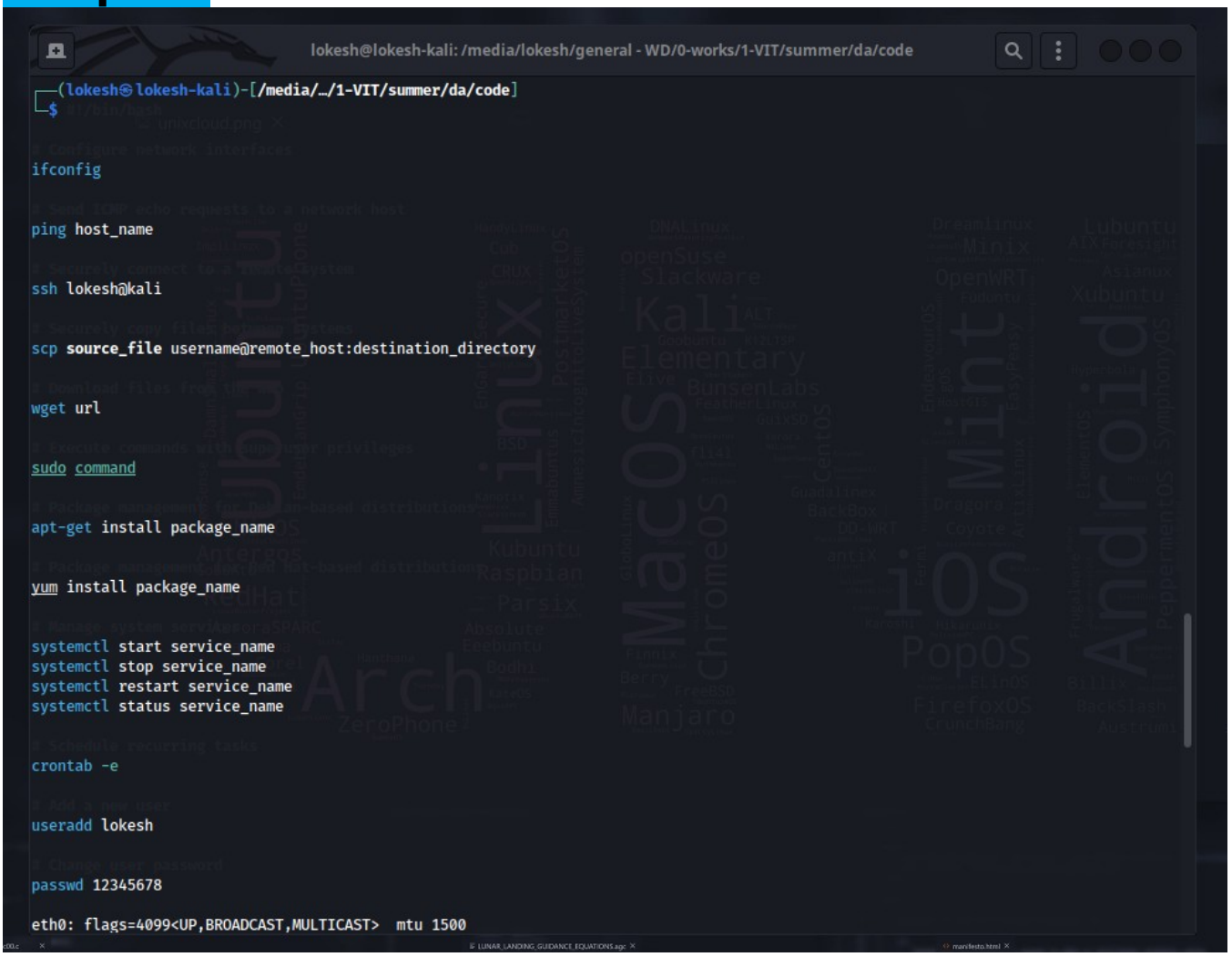
free: Displays memory usage, including the total, used, and free memory on the system.
uptime: Shows the system's uptime, indicating how long the system has been running.
who: Displays the currently logged-in users.
w: Displays the logged-in users and their activities, including the time they logged in, idle time, and the commands they are currently running.

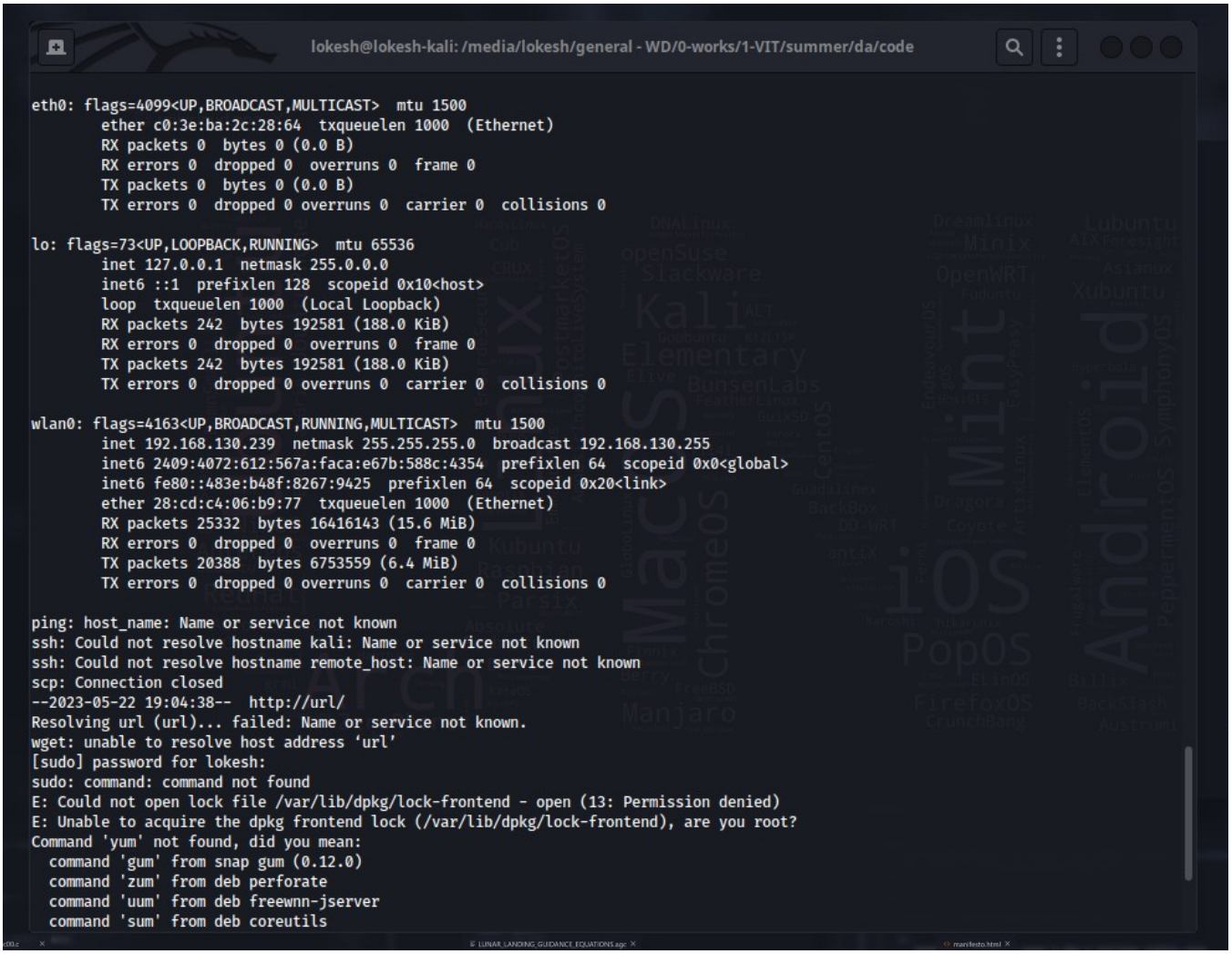
Networking and System Administration :

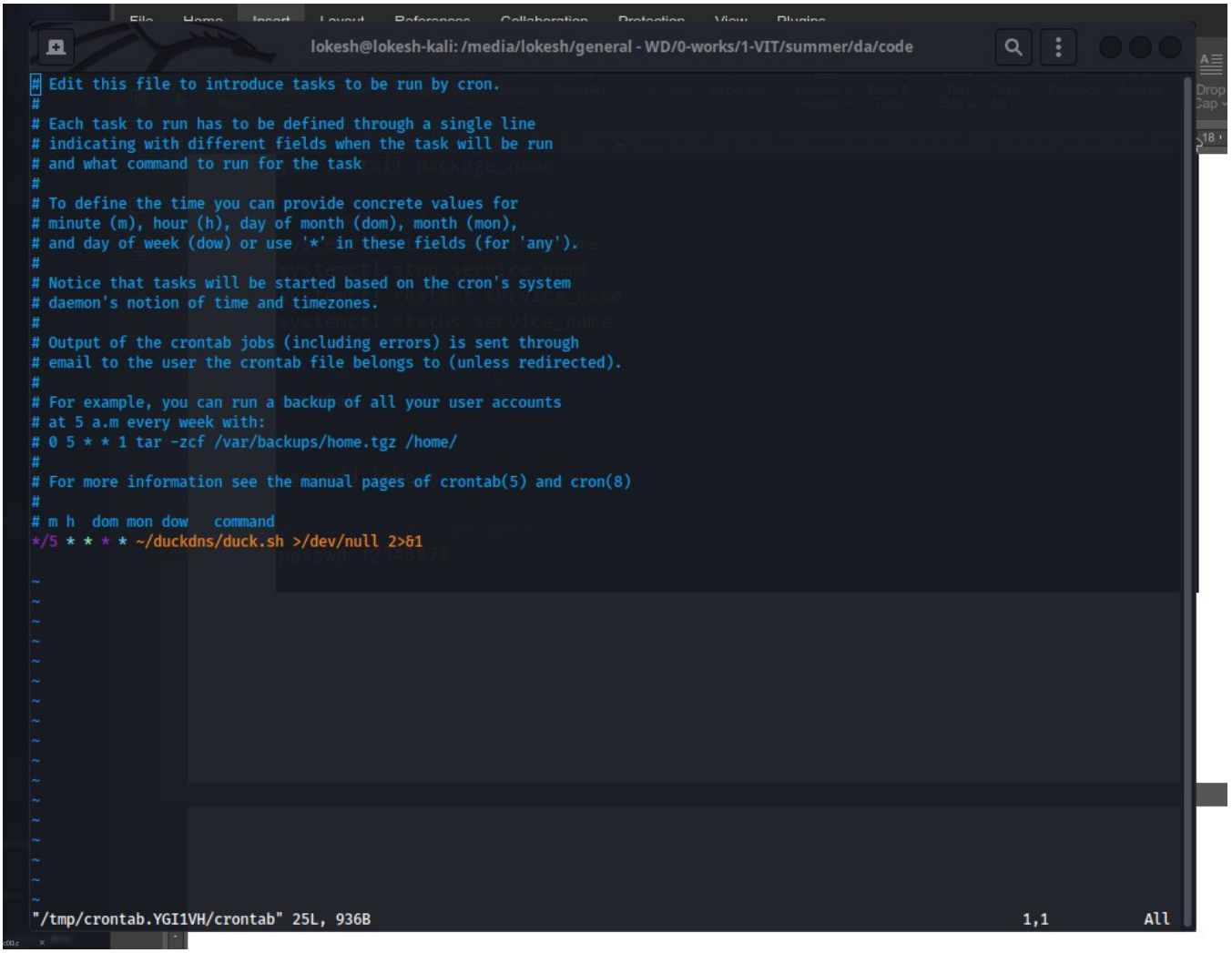
Bash script :

```
#!/bin/bash

# Configure network interfaces
ifconfig

# Send ICMP echo requests to a network host
ping host_name

# Securely connect to a remote system
ssh lokesh@kali

# Securely copy files between systems
scp source_file username@remote_host:destination_directory

# Download files from the web
wget url

# Execute commands with superuser privileges
sudo command

# Package management for Debian-based distributions
apt-get install package_name

# Package management for Red Hat-based distributions
yum install package_name

# Manage system services
systemctl start service_name
systemctl stop service_name
systemctl restart service_name
systemctl status service_name

# Schedule recurring tasks
crontab -e

# Add a new user
useradd lokesh

# Change user password
passwd 12345678
```

Output :


lokesh@lokesh-kali: /media/lokesh/general - WD/0-works/1-VIT/summer/da/code
(lokesh㉿lokesh-kali)-[/media/.../1-VIT/summer/da/code]
$
ifconfig
ping host_name
ssh lokesh@kali
scp source_file username@remote_host:destination_directory
wget url
sudo command
apt-get install package_name
yum install package_name
systemctl start service_name
systemctl stop service_name
systemctl restart service_name
systemctl status service_name
crontab -e
useradd lokesh
passwd 12345678
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500


lokesh@lokesh-kali: /media/lokesh/general - WD/0-works/1-VIT/summer/da/code
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether c0:3e:ba:2c:28:64 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 242 bytes 192581 (188.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 242 bytes 192581 (188.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.130.239 netmask 255.255.255.0 broadcast 192.168.130.255
inet6 2409:4072:612:567a:faca:e67b:588c:4354 prefixlen 64 scopeid 0x0<global>
inet6 fe80::483e:b48f:8267:9425 prefixlen 64 scopeid 0x20<link>
ether 28:cd:c4:06:b9:77 txqueuelen 1000 (Ethernet)
RX packets 25332 bytes 16416143 (15.6 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 20388 bytes 6753559 (6.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
ping: host_name: Name or service not known
ssh: Could not resolve hostname kali: Name or service not known
ssh: Could not resolve hostname remote_host: Name or service not known
scp: Connection closed
--2023-05-22 19:04:38-- http://url/
Resolving url (url)... failed: Name or service not known.
wget: unable to resolve host address ‘url’
[sudo] password for lokesh:
sudo: command: command not found
E: Could not open lock file /var/lib/dpkg/lock-frontend - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), are you root?
Command 'yum' not found, did you mean:
command 'gum' from snap gum (0.12.0)
command 'zum' from deb perforate
command 'uum' from deb freewnn-jserver
command 'sum' from deb coreutils



Explanition :

This bash script demonstrates various networking and system administration operations using the following commands:

Networking:

ifconfig: Configures network interfaces, displaying network interface information such as IP addresses, network masks, and network activity.
ping: Sends ICMP echo requests to a network host to check its availability and measure the network latency.
ssh: Securely connects to a remote system using the SSH (Secure Shell) protocol.
scp: Securely copies files between systems over SSH.
wget: Downloads files from the web using HTTP, HTTPS, or FTP protocols.
System Administration:

sudo: Executes commands with superuser (root) privileges.

apt-get: Package management command for Debian-based distributions, used to install, upgrade, or remove software packages.
yum: Package management command for Red Hat-based distributions, used to install, upgrade, or remove software packages.
systemctl: Manages system services, including starting, stopping, restarting, and checking the status of services.
crontab: Schedules recurring tasks using the cron daemon. It opens the user's crontab file for editing.
useradd: Adds a new user to the system.
passwd: Changes the password of a user