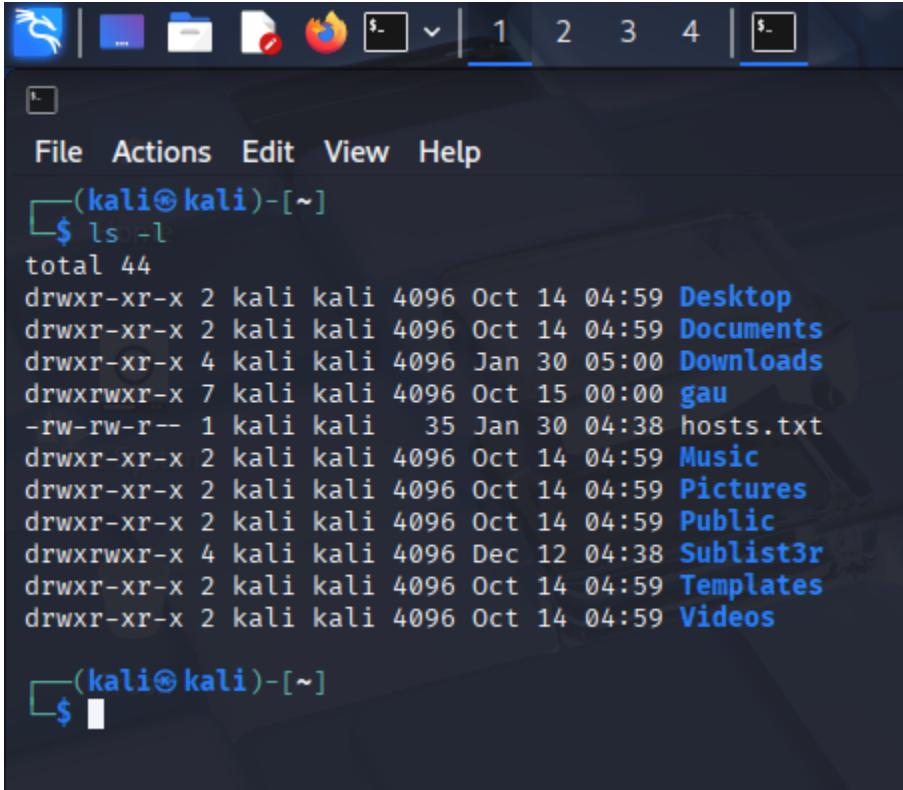


TASK 2

1. View Permissions



A screenshot of a Linux desktop environment, likely Kali Linux, showing a terminal window. The terminal window has a dark background with light-colored text. It displays the output of the 'ls -l' command, listing various directories and files in the current directory. The terminal window is titled '(kali㉿kali)-[~]'. The desktop interface includes a dock with icons for a web browser, file manager, terminal, and other applications. A taskbar at the top shows several open windows.

```
(kali㉿kali)-[~]
$ ls -l
total 44
drwxr-xr-x 2 kali kali 4096 Oct 14 04:59 Desktop
drwxr-xr-x 2 kali kali 4096 Oct 14 04:59 Documents
drwxr-xr-x 4 kali kali 4096 Jan 30 05:00 Downloads
drwxrwxr-x 7 kali kali 4096 Oct 15 00:00 gau
-rw-rw-r-- 1 kali kali 35 Jan 30 04:38 hosts.txt
drwxr-xr-x 2 kali kali 4096 Oct 14 04:59 Music
drwxr-xr-x 2 kali kali 4096 Oct 14 04:59 Pictures
drwxr-xr-x 2 kali kali 4096 Oct 14 04:59 Public
drwxrwxr-x 4 kali kali 4096 Dec 12 04:38 Sublist3r
drwxr-xr-x 2 kali kali 4096 Oct 14 04:59 Templates
drwxr-xr-x 2 kali kali 4096 Oct 14 04:59 Videos

(kali㉿kali)-[~]
$
```

2. Change Permission (chmod):

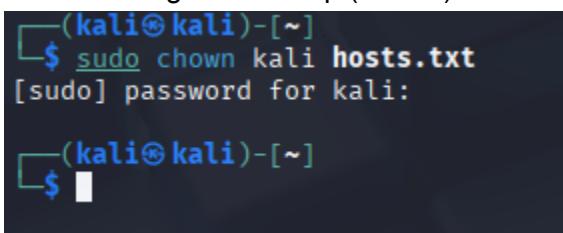


A screenshot of a terminal window showing two commands used to change file permissions. The first command uses 'chmod u+x' to add execute permission for the user on the 'hosts.txt' file. The second command uses 'chmod 755' to set the permissions to 755. Both commands are run by the user '(kali㉿kali)-[~]'.

```
(kali㉿kali)-[~]
$ chmod u+x hosts.txt

(kali㉿kali)-[~]
$ chmod 755 hosts.txt
```

3. Change ownership (chown)



A screenshot of a terminal window showing the 'chown' command being run. The user '(kali㉿kali)-[~]' runs 'sudo chown kali hosts.txt' to change the ownership of the 'hosts.txt' file to the 'kali' user. A password prompt '[sudo] password for kali:' is visible. The terminal window is titled '(kali㉿kali)-[~]'.

```
(kali㉿kali)-[~]
$ sudo chown kali hosts.txt
[sudo] password for kali:

(kali㉿kali)-[~]
$
```

4. Firewall Configuration

```
(kali㉿kali)-[~]
$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.7 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.0 M
B]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [117 kB]
Get:5 http://kali.download/kali kali-rolling/non-free amd64 Packages [190 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [90
5 kB]
Fetched 73.9 MB in 23s (3,261 kB/s)

2039 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali㉿kali)-[~]
$ sudo apt install ufw
The following packages were automatically installed and are no longer required
:
  libwireshark18  libwiretap15  libwsutil16
Use 'sudo apt autoremove' to remove them.

Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 2039
  Download size: 169 kB
  Space needed: 880 kB / 63.3 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169
kB]
Fetched 169 kB in 1s (253 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 412740 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36.2-9_all.deb ...
Unpacking ufw (0.36.2-9) ...
Setting up ufw (0.36.2-9) ...
Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions for the ufw init script.
update-rc.d: It looks like a non-network service, we enable it.
Created symlink '/etc/systemd/system/multi-user.target.wants/ufw.service' → '/
usr/lib/systemd/system/ufw.service'.
Processing triggers for kali-menu (2025.2.7) ...
Processing triggers for man-db (2.13.1-1) ...
```

```
[kali㉿kali)-[~]
└─$ sudo ufw status
Status: inactive
```

5. Hardening

```
[kali㉿kali)-[~]
└─$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

[kali㉿kali)-[~]
└─$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)

[kali㉿kali)-[~]
└─$ sudo ufw allow ssh
Rules updated
Rules updated (v6)

[kali㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

[kali㉿kali)-[~]
└─$ █
```

6. Identify and disable unnecessary services

```
(kali㉿kali)-[~]
$ systemctl list-units --type=service --state=running
UNIT                  LOAD   ACTIVE SUB   DESCRIPTION
accounts-daemon.service    loaded active running Accounts Service
colord.service             loaded active running Manage, Install and Ge>
cron.service               loaded active running Regular background pro>
dbus.service                loaded active running D-Bus System Message Bus
getty@tty1.service          loaded active running Getty on tty1
haveged.service            loaded active running Entropy Daemon based o>
lightdm.service             loaded active running Light Display Manager
ModemManager.service        loaded active running Modem Manager
NetworkManager.service      loaded active running Network Manager
polkit.service              loaded active running Authorization Manager
rtkit-daemon.service       loaded active running RealtimeKit Scheduling>
systemd-journald.service   loaded active running Journal Service
systemd-logind.service     loaded active running User Login Management
systemd-udevd.service      loaded active running Rule-based Manager for>
udisks2.service             loaded active running Disk Manager
upower.service              loaded active running Daemon for power manag>
user@1000.service           loaded active running User Manager for UID 1000
virtualbox-guest-utils.service loaded active running Virtualbox guest utils

Legend: LOAD → Reflects whether the unit definition was properly loaded.
        ACTIVE → The high-level unit activation state, i.e. generalization of >
lines 1-22 ... skipping ...
UNIT                  LOAD   ACTIVE SUB   DESCRIPTION
accounts-daemon.service    loaded active running Accounts Service
colord.service             loaded active running Manage, Install and Generate Color Profiles
cron.service               loaded active running Regular background program processing daemon
dbus.service                loaded active running D-Bus System Message Bus
getty@tty1.service          loaded active running Getty on tty1
haveged.service            loaded active running Entropy Daemon based on the HAVEGE algorithm
lightdm.service             loaded active running Light Display Manager
ModemManager.service        loaded active running Modem Manager
NetworkManager.service      loaded active running Network Manager
polkit.service              loaded active running Authorization Manager
rtkit-daemon.service       loaded active running RealtimeKit Scheduling Policy Service
systemd-journald.service   loaded active running Journal Service
systemd-logind.service     loaded active running User Login Management
systemd-udevd.service      loaded active running Rule-based Manager for Device Events and Files
udisks2.service             loaded active running Disk Manager
upower.service              loaded active running Daemon for power management
user@1000.service           loaded active running User Manager for UID 1000
virtualbox-guest-utils.service loaded active running Virtualbox guest utils

Legend: LOAD → Reflects whether the unit definition was properly loaded.
        ACTIVE → The high-level unit activation state, i.e. generalization of SUB.
        SUB   → The low-level unit activation state, values depend on unit type.

18 loaded units listed.
```

```
(kali㉿kali)-[~] units --type=service --state=running
└─$ sudo systemctl stop colord.service   ACTIVE SUB    DESCRIPTION
    accounts-daemon.service     loaded active running Accounts Service
└─(kali㉿kali)-[~]                   loaded active running Manage, Install and Ge>
└─$ sudo systemctl disable colord.service  active running Regular background prox>
The unit files have no installation config (WantedBy=, RequiredBy=, UpheldBy=, Also=, or Alias= settings in the [Install] section, and DefaultInstance= for template units). This means they are not meant to be enabled or disabled using systemctl.
Possible reasons for having these kinds of units are:
• A unit may be statically enabled by being symlinked from another unit's .wants/, .requires/, or .upholds/ directory.
• A unit's purpose may be to act as a helper for some other unit which has a requirement dependency on it.
• A unit may be started when needed via activation (socket, path, timer, D-Bus, udev, scripted systemctl call, ...).
• In case of template units, the unit is meant to be enabled with some instance name specified.
```