

TASK 2

Operating System Security Fundamentals (Linux & Windows)

Installation of Kali Linux in Virtual Box:

Step 1: Installed Oracle VirtualBox on the host system.

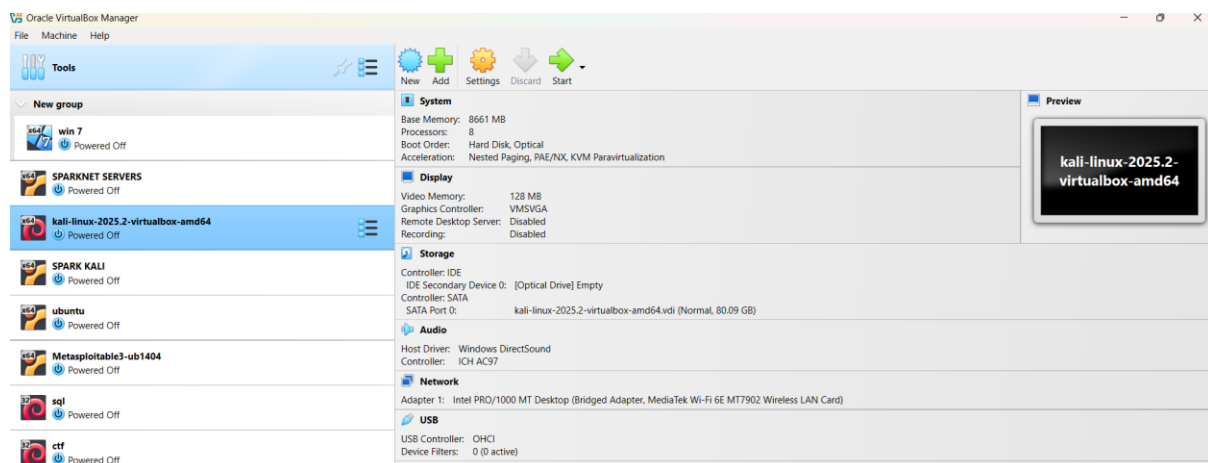
Step 2: Downloaded Ubuntu Linux ISO file.

Step 3: Created a new virtual machine using the ISO file.

Step 4: Allocated required RAM and storage.

Step 5: Completed the Linux OS installation successfully.

Step 6: The virtual machine provides a secure and isolated environment for learning Linux and security.



Explore user accounts, permissions, and access control mechanisms.

User Accounts

- whoami – Displays the current user
- who – Shows logged-in users

- `id` – Displays user ID and group ID
- `cat /etc/passwd` – Lists all user accounts

User & Group Management

- `sudo adduser username` – Create a new user
- `sudo passwd username` – Set/change user password
- `groups username` – Show groups of a user
- `sudo addgroup groupname` – Create a new group

Permissions & Ownership

- `ls -l` – View file permissions
- `chmod 755 filename` – Change file permissions
- `chown user:group filename` – Change file owner and group
- `stat filename` – View detailed permission info

Access Control

- `sudo` – Execute commands with admin privileges
- `su username` – Switch user
- `getfacl filename` – View Access Control List
- `setfacl -m u:username:rwx filename` – Set ACL permissions

```

kali@kali:~$ id
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),26(cdrom),25(floppy),27(audio),29(audio),30(dip),44(video),46(plugdev),100(users),101(net)

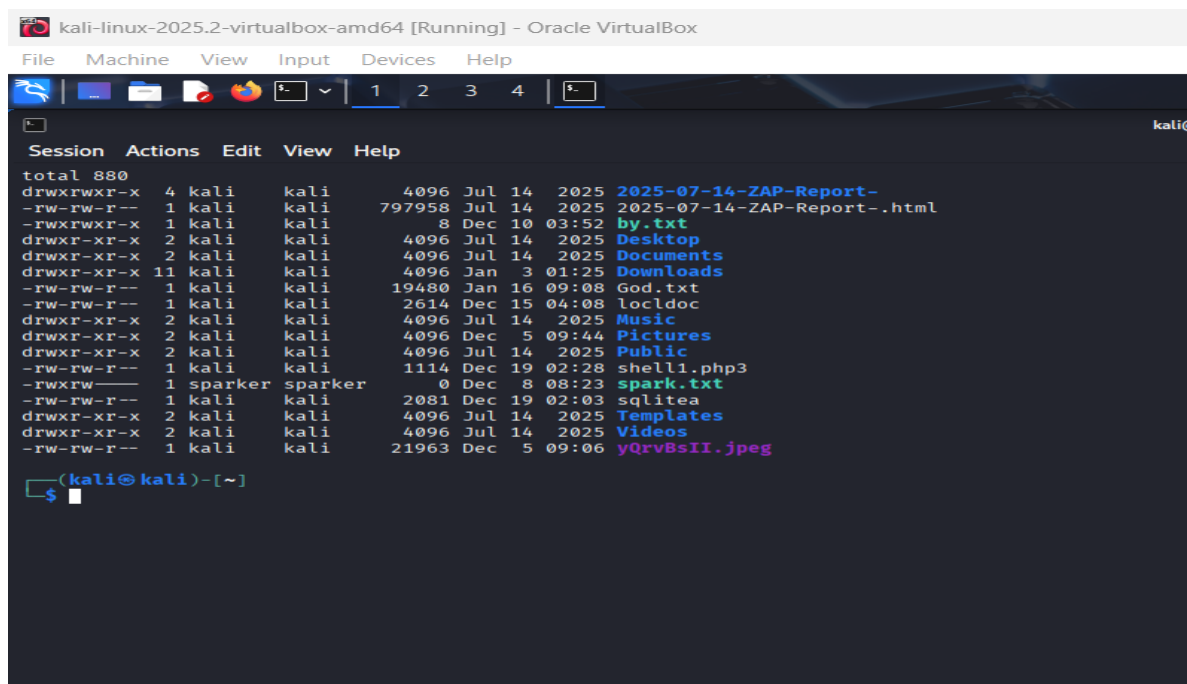
kali@kali:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
cron:x:4:4:cron:/var/spool/cron/:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
kali:x:1000:1000:kali:/:/bin/bash

kali@kali:~$ groups kali
kali : kali adm cdrom floppy plugdev sasl users

```

File Permissions:

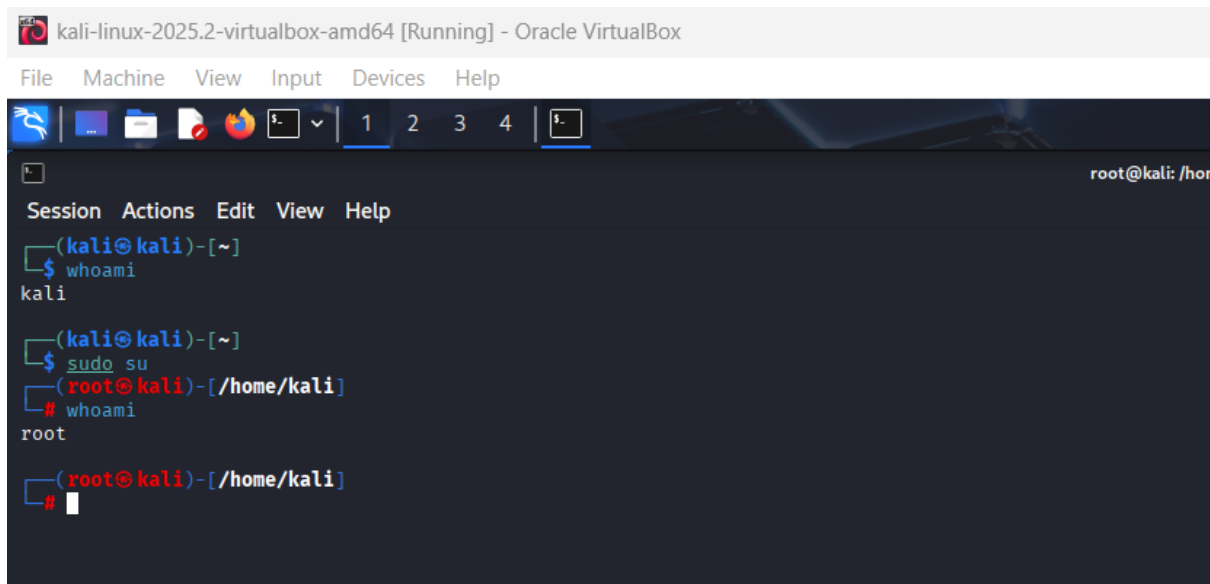
- **ls -l** – Displays file permissions, owner, and group details
- **chmod 755 filename** – Changes file permissions (read, write, execute)
- **chmod u+x filename** – Adds execute permission to the owner
- **chown user filename** – Changes file owner
- **chown user:group filename** – Changes file owner and group



```
kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Session Actions Edit View Help
total 880
drwxrwxr-x 4 kali kali 4096 Jul 14 2025 2025-07-14-ZAP-Report-
-rw-rw-r-- 1 kali kali 797958 Jul 14 2025 2025-07-14-ZAP-Report-.html
-rwxrwxr-x 1 kali kali 8 Dec 10 03:52 by.txt
drwxr-xr-x 2 kali kali 4096 Jul 14 2025 Desktop
drwxr-xr-x 2 kali kali 4096 Jul 14 2025 Documents
drwxr-xr-x 11 kali kali 4096 Jan 3 01:25 Downloads
-rw-rw-r-- 1 kali kali 19480 Jan 16 09:08 God.txt
-rw-rw-r-- 1 kali kali 2614 Dec 15 04:08 locldoc
drwxr-xr-x 2 kali kali 4096 Jul 14 2025 Music
drwxr-xr-x 2 kali kali 4096 Dec 5 09:44 Pictures
drwxr-xr-x 2 kali kali 4096 Jul 14 2025 Public
-rw-rw-r-- 1 kali kali 1114 Dec 19 02:28 shell1.php3
-rwxrwxr-x 1 sparker sparker 0 Dec 8 08:23 spark.txt
-rw-rw-r-- 1 kali kali 2081 Dec 19 02:03 sqlitea
drwxr-xr-x 2 kali kali 4096 Jul 14 2025 Templates
drwxr-xr-x 2 kali kali 4096 Jul 14 2025 Videos
-rw-rw-r-- 1 kali kali 21963 Dec 5 09:06 yQrvBsII.jpeg
(kali@kali)-[~]
$
```

Administrator vs Standard user privileges:

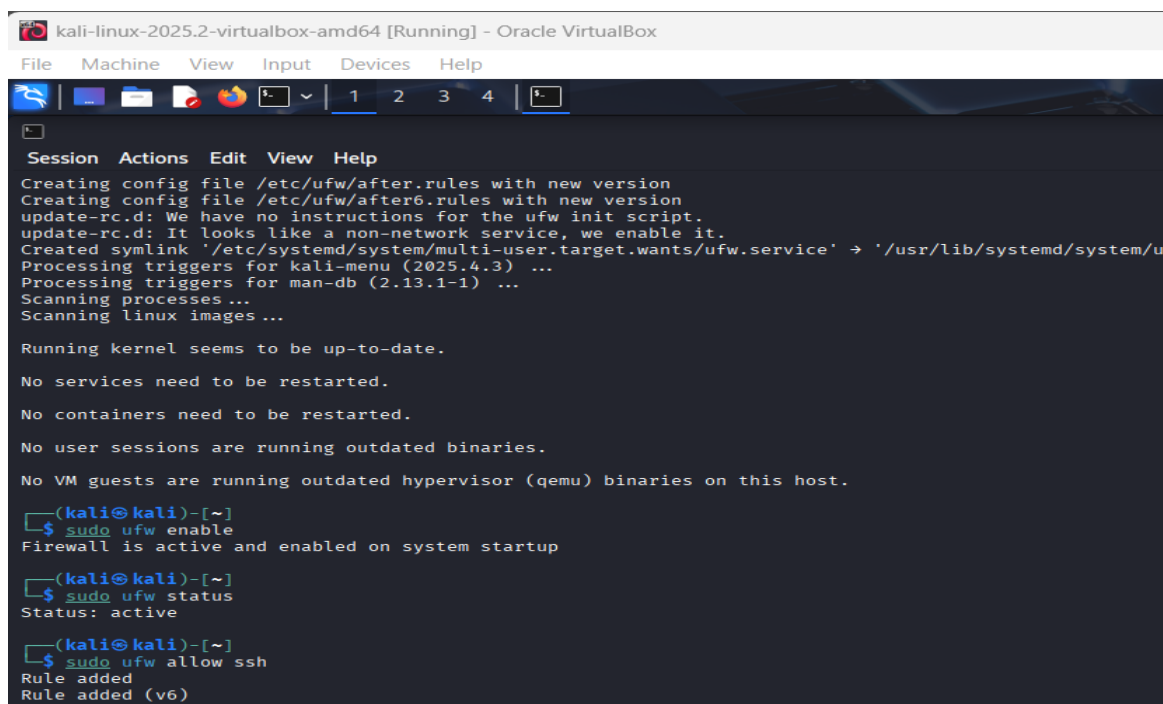
- Administrator (root/sudo user) has full system access and can install software, modify system files, and manage users.
- Standard user has limited privileges and can access only permitted files and applications.
- Administrative tasks are performed using the sudo command.
- This separation of privileges improves system security and prevents accidental system damage.



```
kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali: /home/kali
Session Actions Edit View Help
(kali@kali)-[~]
$ whoami
kali
(kali@kali)-[~]
$ sudo su
(root@kali)-[/home/kali]
# whoami
root
(root@kali)-[/home/kali]
#
```

Enable Firewall in Linux (UFW):

1. **sudo apt install ufw** – Install UFW
2. **sudo ufw enable** – Enable the firewall
3. **sudo ufw status** – Check firewall status
4. **sudo ufw allow ssh** – Allow SSH connections



```
kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Session Actions Edit View Help
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 (2025.4.3) ...
Processing triggers for man-db (2.13.1-1) ...
Scanning processes ...
Scanning linux images ...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

(kali@kali)-[~]
$ sudo ufw enable
Firewall is active and enabled on system startup
(kali@kali)-[~]
$ sudo ufw status
Status: active
(kali@kali)-[~]
$ sudo ufw allow ssh
Rule added
Rule added (v6)
```

Identify running processes and services:

Identify Running Processes

- `ps` – Displays current running processes
- `ps aux` – Shows all running processes in detail
- `top` – Displays real-time running processes
- `htop` – Interactive process viewer (if installed)

```
(kali@kali)-[~]
$ ps
  PID TTY          TIME CMD
 1873 pts/0    00:00:03 zsh
 3126 pts/0    00:00:00 ps

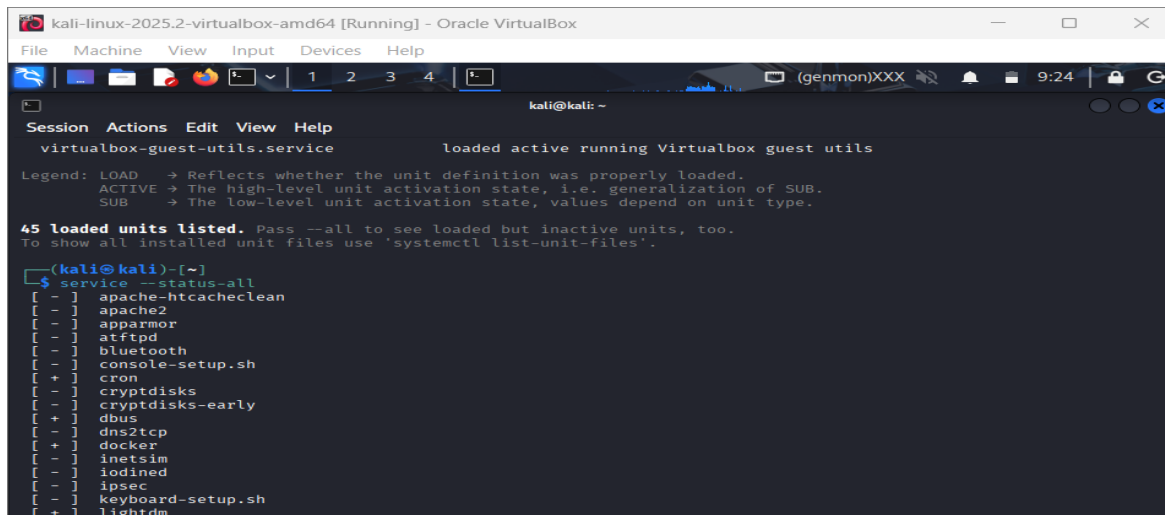
(kali@kali)-[~]
$ ps aux
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1   0.5  0.1 25000 15424 ?        Ss   09:03   0:05 /sbin/init splash
root         2   0.0  0.0      0     0 ?        S    09:03   0:00 [kthreadd]
root         3   0.0  0.0      0     0 ?        S    09:03   0:00 [pool_workqueue_release]
root         4   0.0  0.0      0     0 ?        I<   09:03   0:00 [kworker/R-rcu_gp]
root         5   0.0  0.0      0     0 ?        I<   09:03   0:00 [kworker/R-sync_wq]
root         6   0.0  0.0      0     0 ?        I<   09:03   0:00 [kworker/R-kvfree_rcu_reclaim]
root         7   0.0  0.0      0     0 ?        I<   09:03   0:00 [kworker/R-slub_flushwq]
root         8   0.0  0.0      0     0 ?        I<   09:03   0:00 [kworker/R-netns]
root        10   0.0  0.0      0     0 ?        I<   09:03   0:00 [kworker/0:0H-kblockd]
root        12   0.0  0.0      0     0 ?        I    09:03   0:00 [kworker/u32:0-events_unbound]
root        13   0.0  0.0      0     0 ?        I<   09:03   0:00 [kworker/R-mm_percpu_wq]
```

Identify Running Services

- `systemctl list-units --type=service` – Lists active services
- `systemctl status servicename` – Checks service status
- `service --status-all` – Displays all services and their status

These commands help monitor system activity and resource usage.

```
kali@kali:~$ systemctl list-units --type=service
UNIT                                LOAD    ACTIVE SUB    DESCRIPTION
accounts-daemon.service            loaded active running Accounts Service
colord.service                     loaded active running Manage, Install and Generate Color Profiles
console-setup.service              loaded active exited Set console font and keymap
containerd.service                 loaded active running containerd container runtime
cron.service                       loaded active running Regular background program processing daemon
dbus.service                      loaded active running D-Bus System Message Bus
docker.service                    loaded active running Docker Application Container Engine
getty@tty1.service                 loaded active running Getty on tty1
haveged.service                   loaded active running Entropy Daemon based on the HAVEGE algorithm
ifupdown-pre.service              loaded active exited Helper to synchronize boot up for ifupdown
keyboard-setup.service             loaded active exited Set the console keyboard layout
kmod-static-nodes.service          loaded active exited Create List of Static Device Nodes
lightdm.service                   loaded active running Light Display Manager
ModemManager.service              loaded active running Modem Manager
networking.service                loaded active exited Raise network interfaces
NetworkManager-wait-online.service loaded active exited Network Manager Wait Online
NetworkManager.service            loaded active running Network Manager
plymouth-quit-wait.service         loaded active exited Hold until boot process finishes up
plymouth-read-write.service        loaded active exited Tell Plymouth To Write Out Runtime Data
```



The screenshot shows a terminal window titled 'kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox'. The terminal output shows the status of the 'virtualbox-guest-utils.service' as 'loaded active running Virtualbox guest utils'. It also displays a legend for unit states: LOAD (unit definition loaded), ACTIVE (high-level activation state), and SUB (low-level activation state). Below this, it lists 45 loaded units. The command 'service --status-all' is executed, showing the status of various services like apache2, apparmor, atftpd, bluetooth, console-setup.sh, cron, cryptdisks, cryptdisks-early, dbus, dns2tcp, docker, inetsim, iodined, ipsec, keyboard-setup.sh, and lightdm.

```
kali@kali: ~  
$ service --status-all  
[ - ] apache2-htcacheclean  
[ - ] apache2  
[ - ] apparmor  
[ - ] atftpd  
[ - ] bluetooth  
[ - ] console-setup.sh  
[ + ] cron  
[ - ] cryptdisks  
[ - ] cryptdisks-early  
[ + ] dbus  
[ - ] dns2tcp  
[ + ] docker  
[ - ] inetsim  
[ - ] iodined  
[ - ] ipsec  
[ - ] keyboard-setup.sh  
[ + ] lightdm
```

Disable Unnecessary Services:

- `systemctl list-unit-files --type=service` – List all services
- `systemctl status servicename` – Check service status
- `sudo systemctl stop servicename` – Stop a running service
- `sudo systemctl disable servicename` – Disable service at boot
- `sudo systemctl is-enabled servicename` – Verify service is disabled