

# TASK – 2

## Operating System Security Fundamentals (Linux & Windows)

### Installation of Kali Linux in Virtual Box:

**Step 1:** Installed Oracle VirtualBox on the host system.

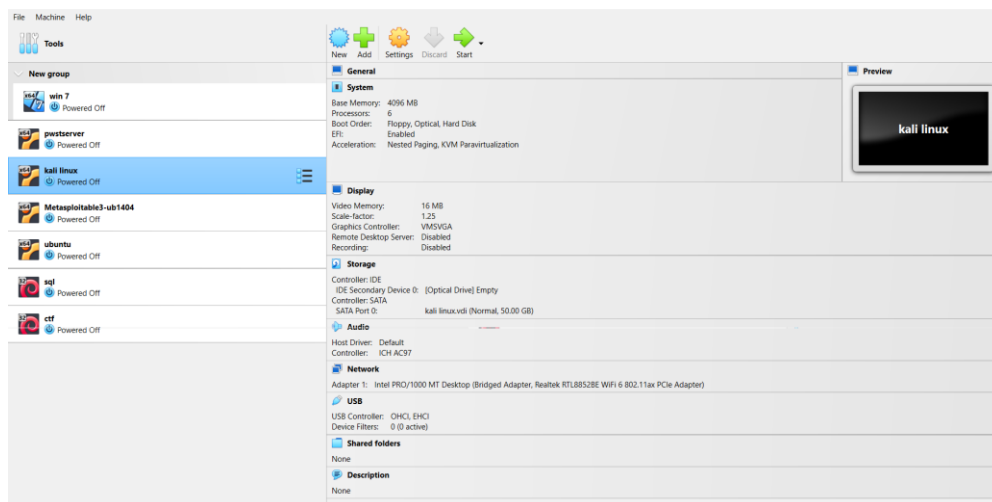
**Step 2:** Downloaded Ubuntu Linux ISO file.

**Step 3:** Created a new virtual machine.

**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.



### User Accounts 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

```
(swetha@pwst-kali)-[~]
$ whoami
swetha

(swetha@pwst-kali)-[~]
$ who
swetha    seat0      2026-01-18 17:41 (:0)

(swetha@pwst-kali)-[~]
$ id
uid=1000(swetha) gid=1000(swetha) groups=1000(swetha),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),116(bluetooth),121(lpadmin),124(wireshark),129(scanner),134(vboxsf),135(kaboxer)

(swetha@pwst-kali)-[~]
$ sudo adduser reni
[sudo] password for swetha:
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for reni
Enter the new value, or press ENTER for the default
  Full Name []: reni
    Room Number []: 2
    Work Phone []: 3
    Home Phone []: 2
      Other []: 2
Is the information correct? [Y/n] y

(swetha@pwst-kali)-[~]
$ ls
-      hosts_up.txt      Public      scan_results.xml  tshark.log
Desktop Music          quick_ports.txt  script.php3       tshark_pid.txt
Documents network-scan-task1  scan_results.html sql                Videos
Downloads Pictures        scan_results.txt Templates         zphisher
```

## 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

```
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 yQrv8sII.jpeg
```

## 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.

```
(swetha@pwst-kali)-[~]
$ whoami
swetha

(swetha@pwst-kali)-[~]
$ sudo su
(root@pwst-kali)-[/home/swetha]
# whoami
root

(root@pwst-kali)-[/home/swetha]
#
```

## 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

```
limit ARGS
delete RULE|NUM
insert NUM RULE
prepend RULE
route RULE
route delete RULE|NUM
route insert NUM RULE
reload
reset
status
status numbered
status verbose
show ARG
version

add limit rule
delete RULE
insert RULE at NUM
prepend RULE
add route RULE
delete route RULE
insert route RULE at NUM
reload firewall
reset firewall
show firewall status
show firewall status as numbered list of RULES
show verbose firewall status
show firewall report
display version information

Application profile commands:
app list
app info PROFILE
app update PROFILE
app default ARG

list application profiles
show information on PROFILE
update PROFILE
set default application policy

(root@pwst-kali)-[/home/swetha]
# sudo ufw status
Status: active

To Action From
--
22 ALLOW Anywhere
22 (v6) ALLOW Anywhere (v6)

(root@pwst-kali)-[/home/swetha]
# 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)

```
(root@pwst-kali)-[/home/swetha]
# ps
  PID TTY          TIME CMD
 2304 pts/1    00:00:00 sudo
 2305 pts/1    00:00:00 su
 2307 pts/1    00:00:01 zsh
 2500 pts/1    00:00:00 ps

(root@pwst-kali)-[/home/swetha]
# ps aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.2  0.3 24776 15916 ?        Ss   17:41   0:01 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    17:41   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    17:41   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   17:41   0:00 [kworker/R-rcu_gp]
root           5  0.0  0.0      0     0 ?        I<   17:41   0:00 [kworker/R-sync_wq]
root           6  0.0  0.0      0     0 ?        I<   17:41   0:00 [kworker/R-kvfree_rcu_rec]
root           7  0.0  0.0      0     0 ?        I<   17:41   0:00 [kworker/R-slab_flushwq]
```

## 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.

```
(root@pwst-kali)-[/home/swetha]
# service --status-all
[ - ] apache-htcacheclean
[ - ] apache2
[ - ] apparmor
[ - ] atftpd
[ - ] bluetooth
[ - ] console-setup.sh
[ + ] cron
[ - ] cryptdisks
[ - ] cryptdisks-early
[ + ] dbus
[ - ] dns2tcp
[ + ] docker
[ - ] inetsim
[ - ] iodined
[ - ] ipsec
[ - ] keyboard-setup.sh
[ + ] lightdm
[ - ] lm-sensors
[ - ] mariadb
```

## 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