TASK – 2

Operating System Security Fundamentals (Linux & Windows)

Installation of Kali Linux in Virtual Box:

Step 1: Installed Oracle VirtualBox on the host system.

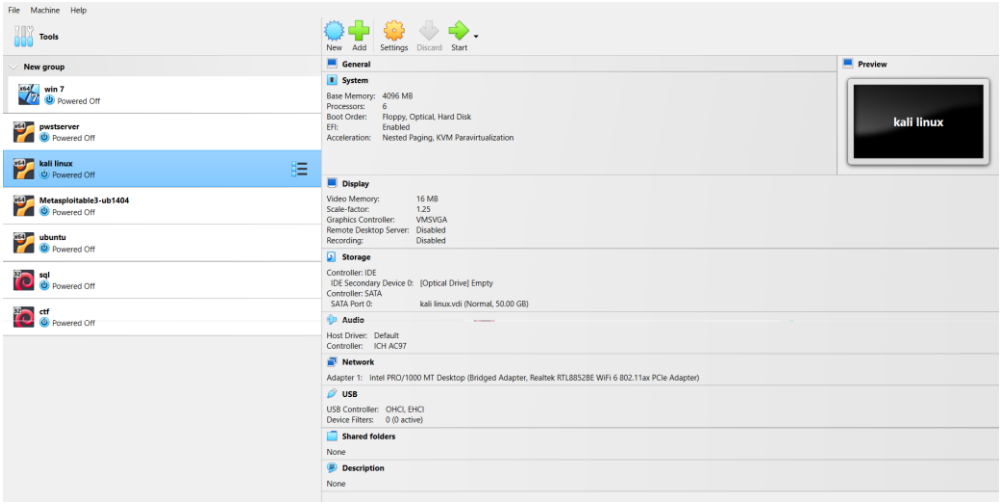
Step 2: Downloaded Ubuntu Linux ISO file.

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

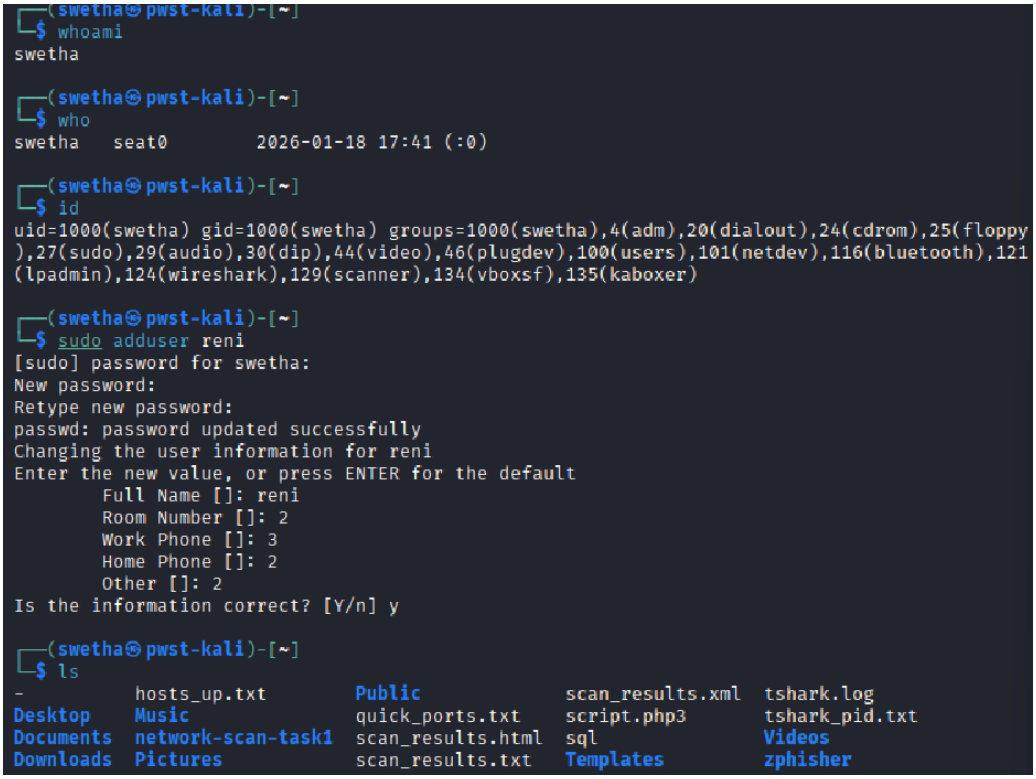
- sudo adduser username – Create a new user
- sudo passwd username – Set/change user password
- groups username – Show groups of a user
- sudo addgroup groupname – Create a new group

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



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
-rwxrw----  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
```

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.

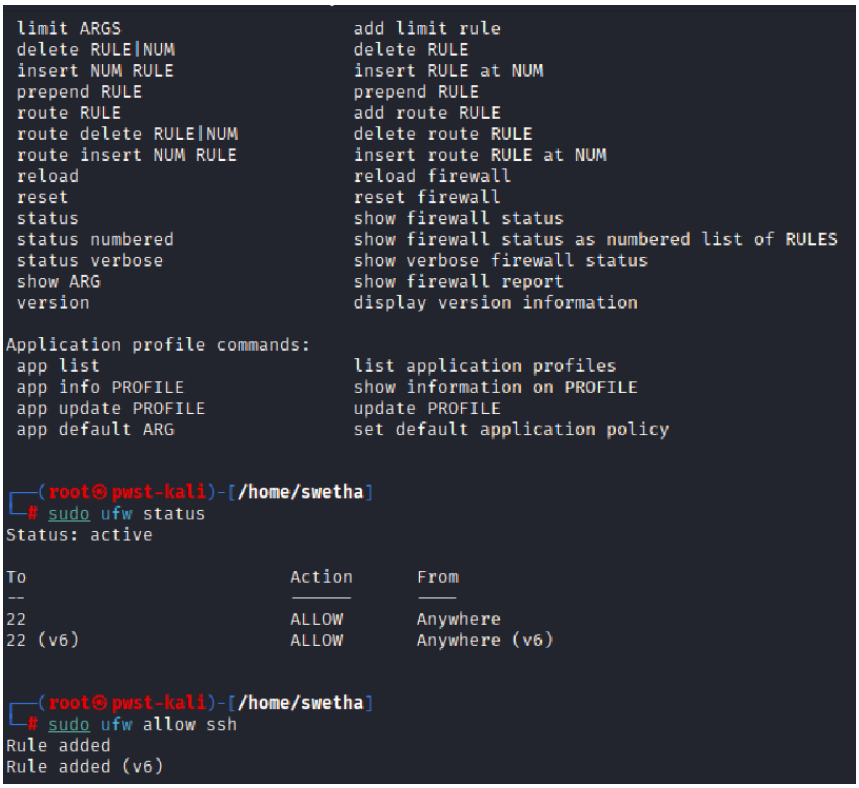
```
┌──(swetha㉿pwst-kali)-[~]
└─$ whoami
swetha

┌──(swetha㉿pwst-kali)-[~]
└─$ sudo su
┌──(root㉿pwst-kali)-[/home/swetha]
└─# whoami
root

┌──(root㉿pwst-kali)-[/home/swetha]
└─#
```

Enable Firewall in Linux (UFW):

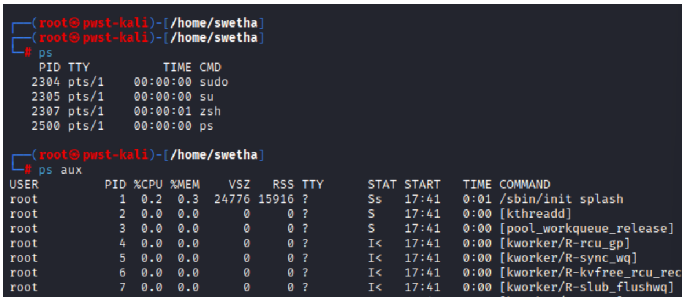
1. sudo apt install ufw – Install UFW
2. sudo ufw enable – Enable the firewall
3. sudo ufw status – Check firewall status
4. sudo ufw allow ssh – Allow SSH connections



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)



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.

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