Task 2

Operating System Security Fundamentals (Linux & Windows)

JASHMI KS

Operating System Security

Operating system security focuses on protecting system resources such as files, processes, memory, and network access from unauthorized use or attacks. Both Linux and Windows provide built-in security mechanisms to enforce access control, protect data, and maintain system integrity.

An operating system acts as an intermediary between the computer hardware and the user. In short, it is an interface between computer hardware and the user.

- The purpose of an operating system is to provide an environment in which a user can execute programs conveniently and efficiently.
- The operating system (OS) is a program that runs at all times on a computer. All other programs, including application programs, run on top of the operating system.
- It assigns resources such as memory, processors, and input/output devices to processes that need them. The assignment of resources has to be fair and secure.

Goals of Operating System

Primary Goals

The primary goals of an operating system (OS) are to provide an easy to use and convenient environment for executing user programs.

- **User Convenience:** It should be easy to use, providing a user-friendly interface and making it simple to interact with the system.
- **Program Execution**: It facilitates the execution of user programs, providing the necessary environment and services for them to run**.**
- **Resource Management**: The OS manages and allocates the computer's resources, including the CPU, memory, disk storage and input/output devices, to ensure fair utilization.
- **Security**: The OS protects the system and user data from unauthorized access, ensuring confidentiality, integrity and availability of information.

Secondary Goals

- **Efficient Resource Utilization**: It should aim to maximize the performance and utilization of computer resources like CPU, Memory and I/O devices, ensuring that the system runs smoothly and efficiently.
- **Reliability**: It should be robust and reliable, able to handle errors and exceptions gracefully, ensuring that the system continues to operate smoothly. It should be modular in design and easy to debug.

Components of an Operating System

There are two basic components of an Operating System.

- **Shell** is the outermost layer of the Operating System and handles user interaction. It interprets input for the OS and handles the output from the OS.
- **Kernel** is the core component of the operating system. The kernel is the primary interface between the Operating system and Hardware.

Virtualization

Virtualization is a technology that allows multiple operating systems to run on a single physical machine by creating virtual environments. Each virtual environment, called a Virtual Machine (VM), operates independently with its own operating system, resources, and security controls. Virtualization is widely used in cybersecurity for safe testing and learning.

VirtualBox

VirtualBox is an open-source virtualization software developed by Oracle. It allows users to create and run virtual machines on a host operating system such as Windows or Linux. VirtualBox provides hardware-level virtualization, enabling multiple operating systems to run simultaneously without affecting the host system.

Importance in Security

- Provides isolation from the host system
- Enables safe security testing and experimentation
- Prevents damage to the primary operating system
- Commonly used in penetration testing and system hardening lab

Ubuntu Linux as a Virtual Machine

Ubuntu is a widely used Linux distribution known for its stability and strong security features. When installed as a virtual machine, Ubuntu operates in an isolated environment, making it ideal for learning operating system security concepts such as user management, file permissions, firewalls, and service control.

Security Features of Ubuntu

- Strong permission-based access control
- Root and standard user separation
- Built-in firewall (UFW)
- Regular security updates
- Extensive logging and monitoring support

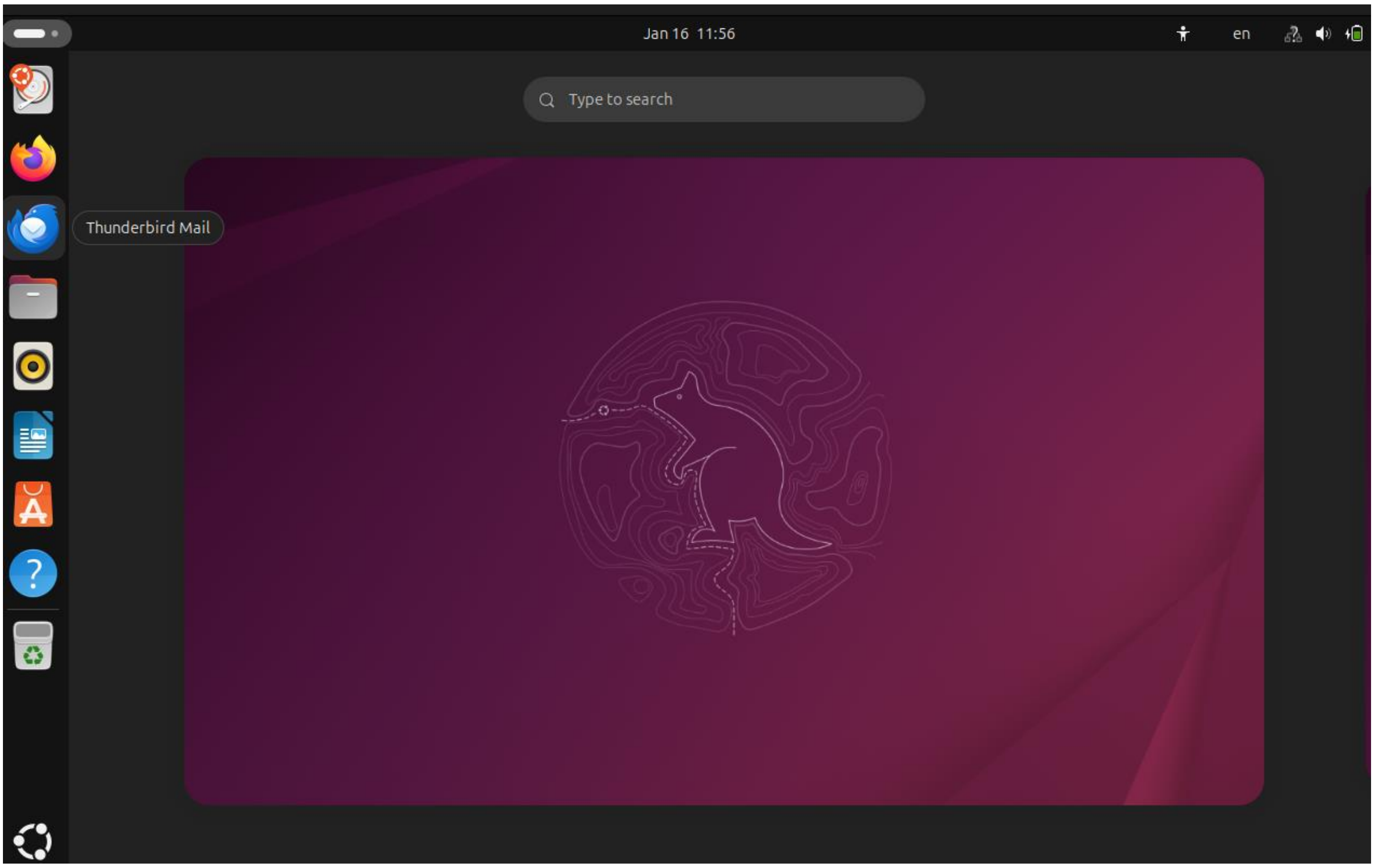
Windows Defender

Windows Defender is the built-in security solution provided by Microsoft for Windows operating systems. It offers real-time protection against malware, viruses, ransomware, and other threats. Windows Defender integrates antivirus, firewall, and threat monitoring features into a single security framework.

Role in Operating System Security

- Provides real-time malware protection
- Monitors system behaviour for threats
- Includes Windows Firewall for network protection
- Helps maintain system integrity and availability

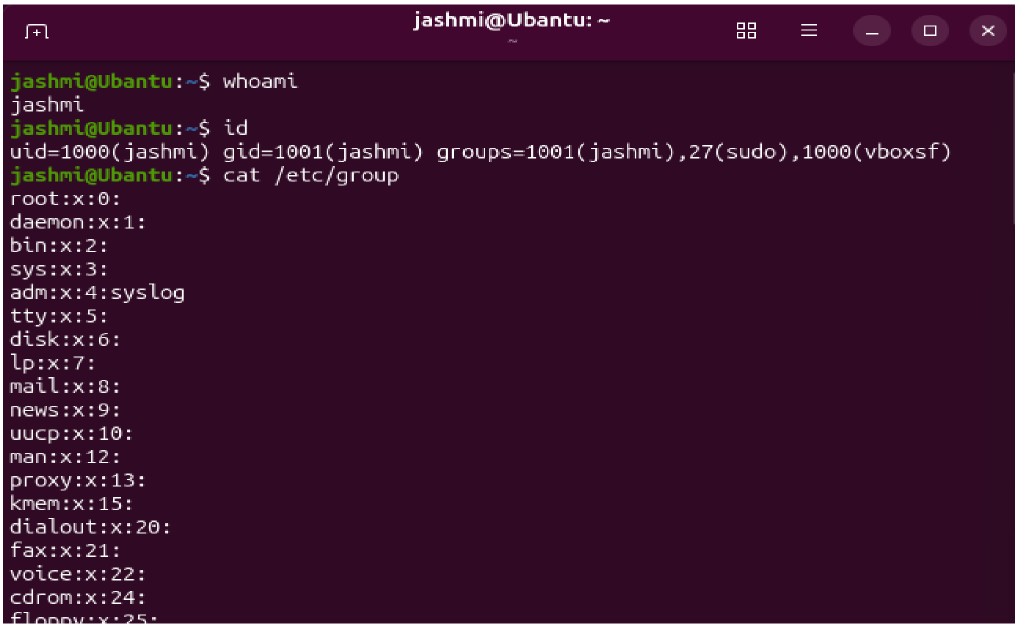
A virtual machine (VM) allows an operating system like Ubuntu Linux to run in isolation from the host system using software like **VirtualBox**.



Understanding Users & Access Control

Linux uses **Discretionary Access Control (DAC)** where access is controlled by users and groups. Each file, process, and resource is owned by a user and associated with a group.

- Identify current logged-in user: whoamiid
- Display user ID and group ID: id
- View all system users: cat /etc/passwd



```
jashmi@Ubantu:~$ whoami
jashmi
jashmi@Ubantu:~$ id
uid=1000(jashmi) gid=1001(jashmi) groups=1001(jashmi),27(sudo),1000(vboxsf)
jashmi@Ubantu:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:
floppy:x:25:
```

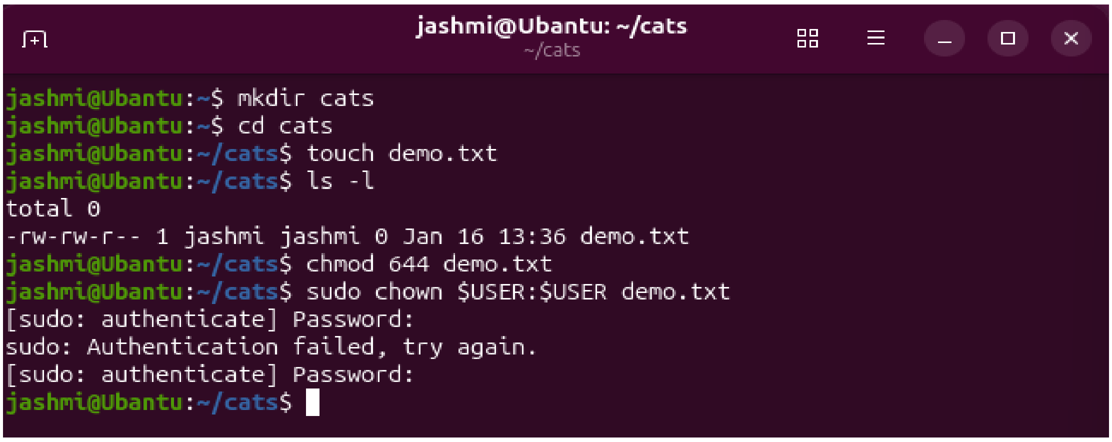
File & Folder Creation and Permission Management

Files and directories must exist before permissions can be applied. Linux permissions control **who can access what and how**, reducing unauthorized access.

Permission format:

-rwxr-xr-x → Owner | Group | Others

- **Create a working directory:** mkdir cats
- **Navigate into it:** cd cats
- **Create a file:** touch demo.txt
- **View permissions:** ls -l
- **Modify permissions:** chmod 644 demo.txt
- **Change ownership:** sudo chown $USER:$USER demo.txt



```
jashmi@Ubantu:~$ mkdir cats
jashmi@Ubantu:~$ cd cats
jashmi@Ubantu:~/cats$ touch demo.txt
jashmi@Ubantu:~/cats$ ls -l
total 0
-rw-rw-r-- 1 jashmi jashmi 0 Jan 16 13:36 demo.txt
jashmi@Ubantu:~/cats$ chmod 644 demo.txt
jashmi@Ubantu:~/cats$ sudo chown $USER:$USER demo.txt
[sudo: authenticate] Password:
sudo: Authentication failed, try again.
[sudo: authenticate] Password:
jashmi@Ubantu:~/cats$ 
```

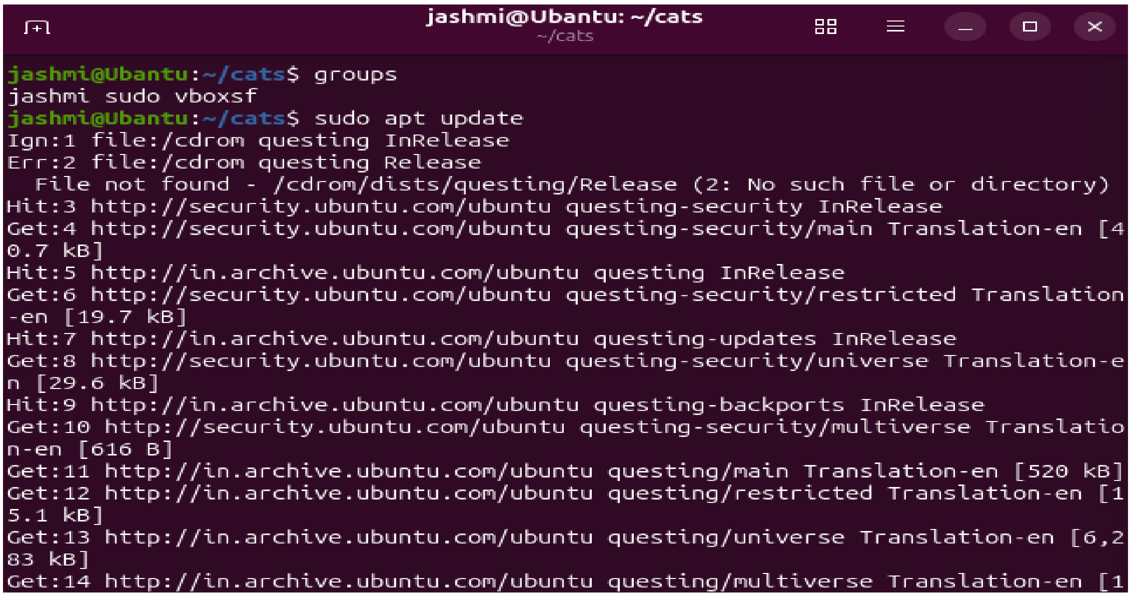
Administrator (Root) vs Standard User Privileges

Root user: Unrestricted access to the entire system

Standard user: Restricted access to protect system integrity

Linux uses the **sudo** mechanism to temporarily elevate privileges.

- **Check group membership:** groups
- **Execute an administrative command:** sudo apt update

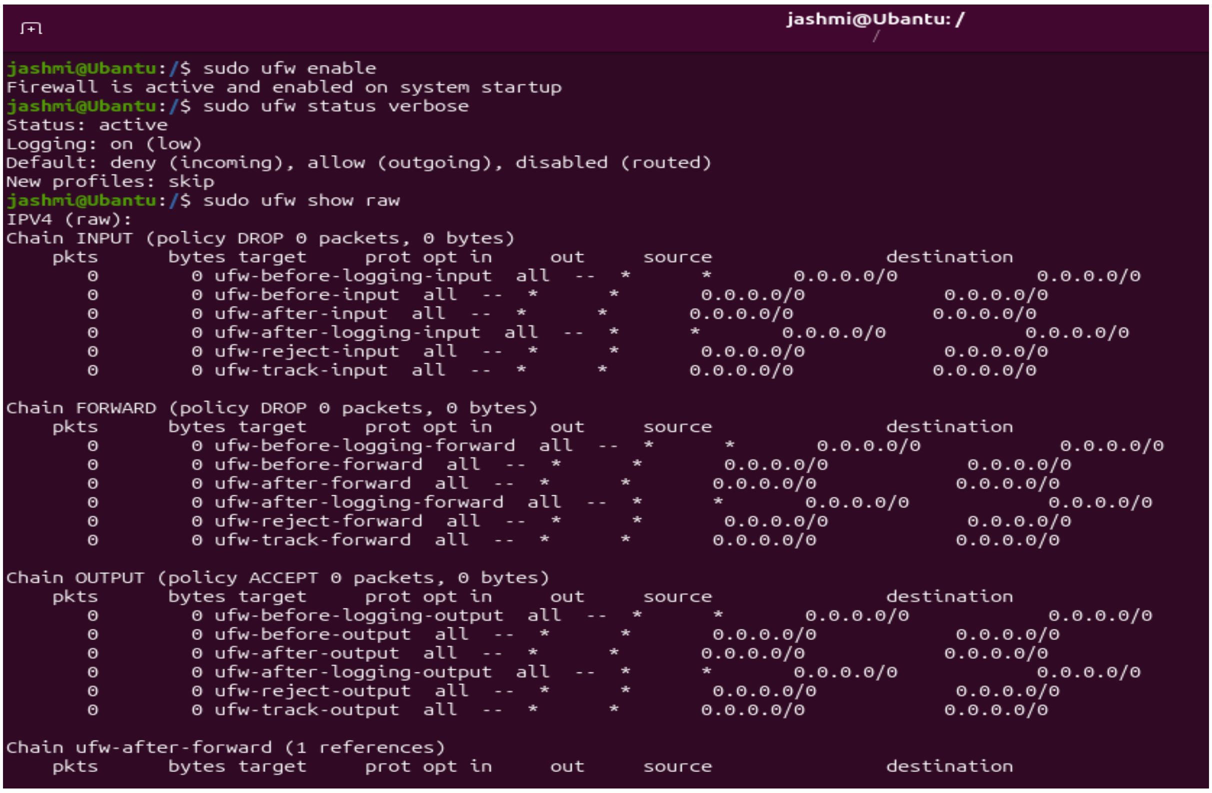


```
jashmi@Ubantu:~/cats$ groups
jashmi sudo vboxsf
jashmi@Ubantu:~/cats$ sudo apt update
Ign:1 file:/cdrom questing InRelease
Err:2 file:/cdrom questing Release
  File not found - /cdrom/dists/questing/Release (2: No such file or directory)
Hit:3 http://security.ubuntu.com/ubuntu questing-security InRelease
Get:4 http://security.ubuntu.com/ubuntu questing-security/main Translation-en [4
0.7 kB]
Hit:5 http://in.archive.ubuntu.com/ubuntu questing InRelease
Get:6 http://security.ubuntu.com/ubuntu questing-security/restricted Translation
-en [19.7 kB]
Hit:7 http://in.archive.ubuntu.com/ubuntu questing-updates InRelease
Get:8 http://security.ubuntu.com/ubuntu questing-security/universe Translation-e
n [29.6 kB]
Hit:9 http://in.archive.ubuntu.com/ubuntu questing-backports InRelease
Get:10 http://security.ubuntu.com/ubuntu questing-security/multiverse Translatio
n-en [616 B]
Get:11 http://in.archive.ubuntu.com/ubuntu questing/main Translation-en [520 kB]
Get:12 http://in.archive.ubuntu.com/ubuntu questing/restricted Translation-en [1
5.1 kB]
Get:13 http://in.archive.ubuntu.com/ubuntu questing/universe Translation-en [6,2
83 kB]
Get:14 http://in.archive.ubuntu.com/ubuntu questing/multiverse Translation-en [1
```

Firewall Configuration (UFW)

A firewall filters network traffic based on predefined rules, preventing unauthorized access and reducing network-based attacks.

- **Enable UFW**: sudo ufw enable
- **Check firewall status:** sudo ufw status verbose
- **List default policies:** sudo ufw show raw

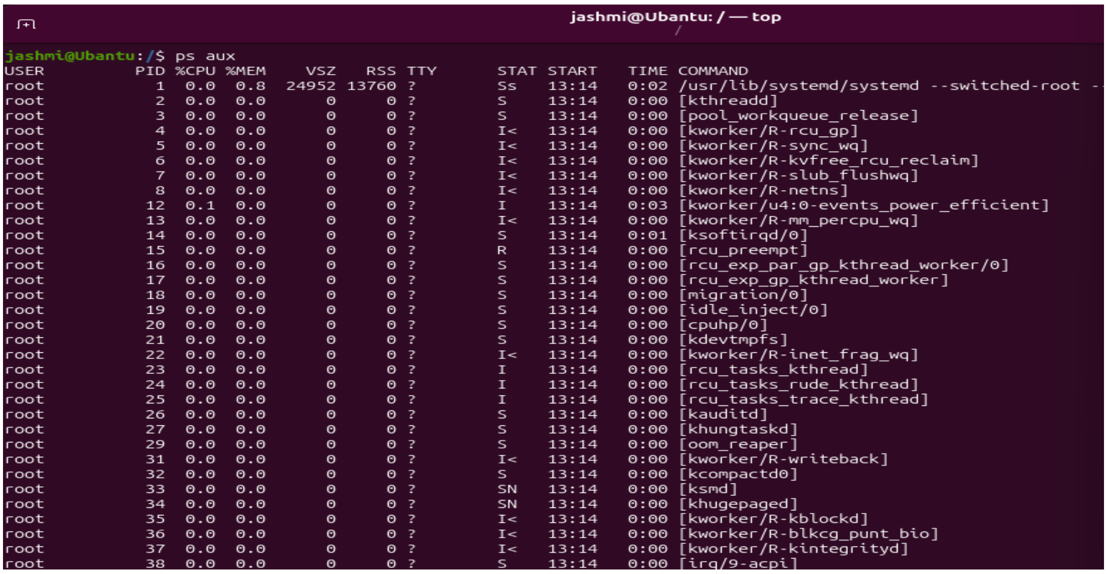


```
jashmi@Ubantu:/$ sudo ufw enable
Firewall is active and enabled on system startup
jashmi@Ubantu:/$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
jashmi@Ubantu:/$ sudo ufw show raw
IPV4 (raw):
Chain INPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ufw-before-logging-input  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-before-input  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-after-input  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-after-logging-input  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-reject-input  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-track-input  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ufw-before-logging-forward  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-before-forward  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-after-forward  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-after-logging-forward  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-reject-forward  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-track-forward  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ufw-before-logging-output  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-before-output  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-after-output  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-after-logging-output  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-reject-output  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ufw-track-output  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain ufw-after-forward (1 references)
    pkts      bytes target     prot opt in     out     source               destination
```

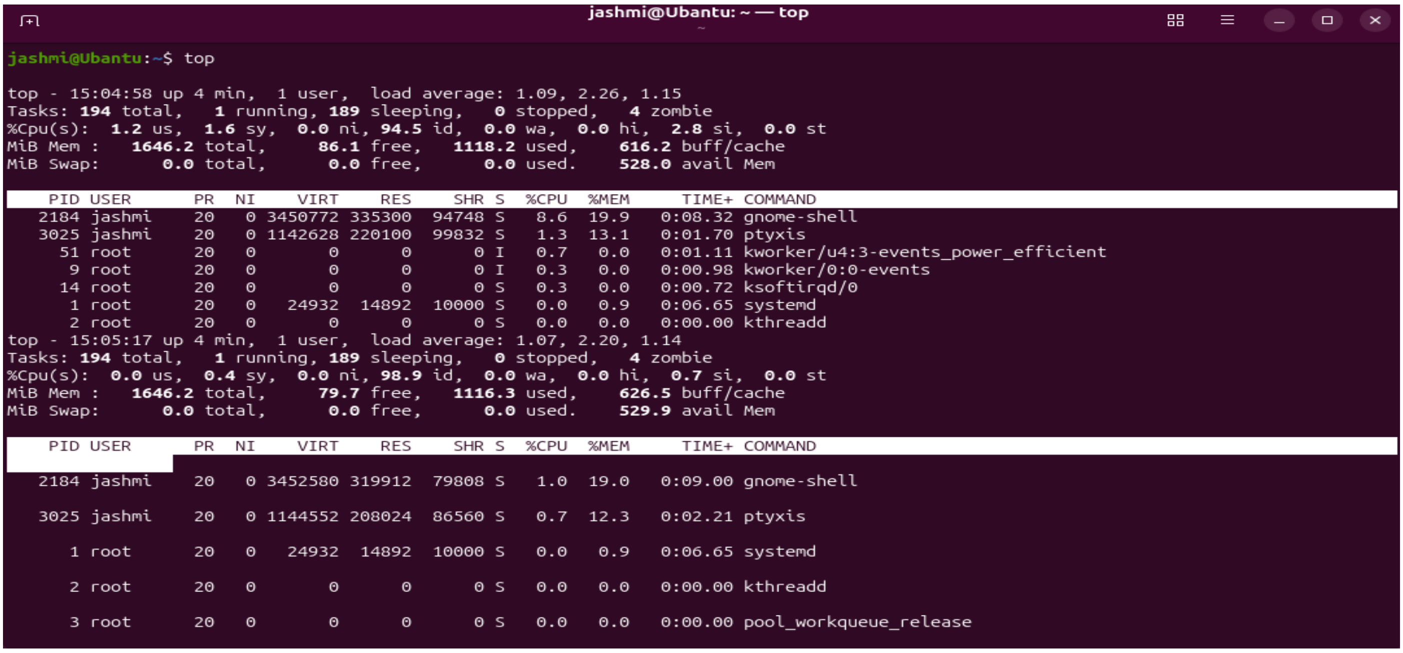
Process and Service Monitoring

Processes are running programs, while services are background processes started by the system. Monitoring them helps detect suspicious or unnecessary activity.

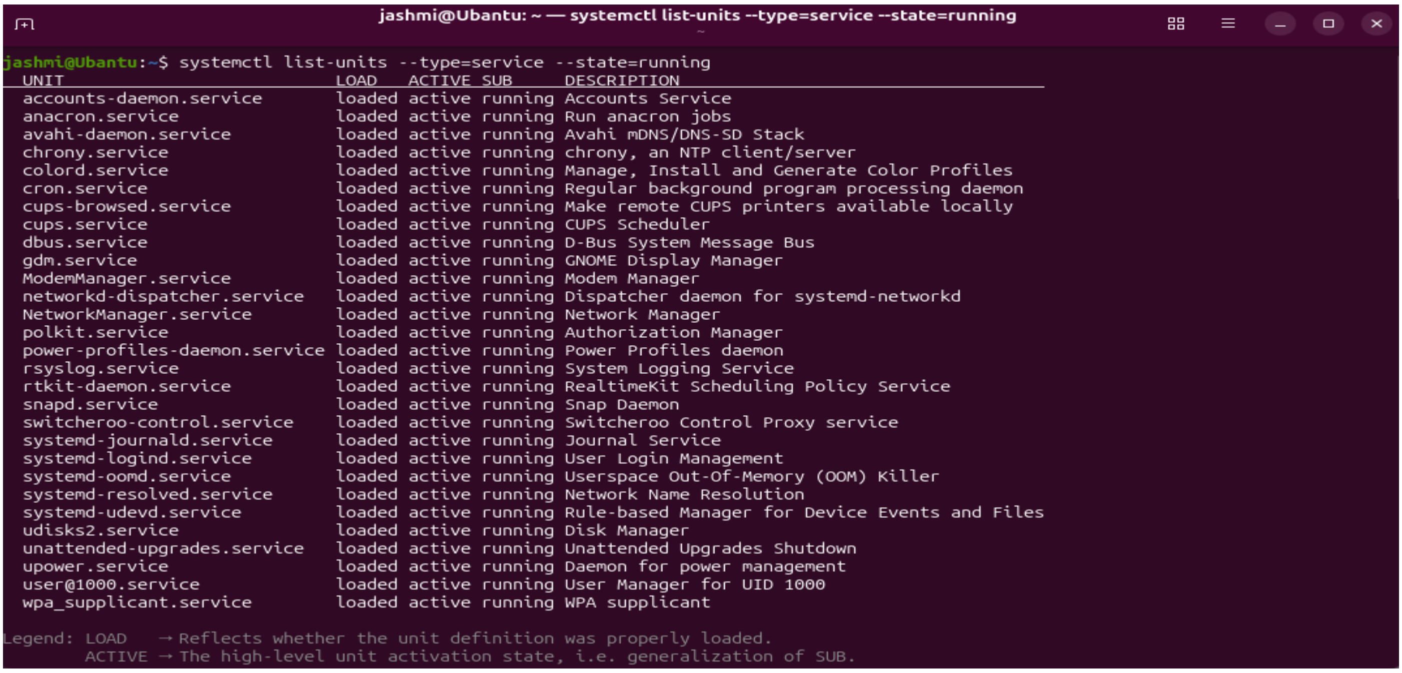
- **Display all running processes**: ps aux
- **Real-time monitoring:** top
- **View active services:** systemctl list-units --type=service --state=running



```
jashmi@Ubantu:/$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.8  24952 13760 ?        Ss   13:14   0:02 /usr/lib/systemd/systemd --switched-root -
root           2  0.0  0.0      0     0 ?        S    13:14   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    13:14   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   13:14   0:00 [kworker/R-rcu_gp]
root           5  0.0  0.0      0     0 ?        I<   13:14   0:00 [kworker/R-sync_wq]
root           6  0.0  0.0      0     0 ?        I<   13:14   0:00 [kworker/R-kvfree_rcu_reclaim]
root           7  0.0  0.0      0     0 ?        I<   13:14   0:00 [kworker/R-slub_flushwq]
root           8  0.0  0.0      0     0 ?        I<   13:14   0:00 [kworker/R-netns]
root          12  0.1  0.0      0     0 ?        I    13:14   0:03 [kworker/u4:0-events_power_efficient]
root          13  0.0  0.0      0     0 ?        I<   13:14   0:00 [kworker/R-mm_percpu_wq]
root          14  0.0  0.0      0     0 ?        S    13:14   0:01 [ksoftirqd/0]
root          15  0.0  0.0      0     0 ?        R    13:14   0:00 [rcu_preempt]
root          16  0.0  0.0      0     0 ?        S    13:14   0:00 [rcu_exp_par_gp_kthread_worker/0]
root          17  0.0  0.0      0     0 ?        S    13:14   0:00 [rcu_exp_gp_kthread_worker]
root          18  0.0  0.0      0     0 ?        S    13:14   0:00 [migration/0]
root          19  0.0  0.0      0     0 ?        S    13:14   0:00 [idle_inject/0]
root          20  0.0  0.0      0     0 ?        S    13:14   0:00 [cpuhp/0]
root          21  0.0  0.0      0     0 ?        S    13:14   0:00 [kdevtmpfs]
root          22  0.0  0.0      0     0 ?        I<   13:14   0:00 [kworker/R-inet_frag_wq]
root          23  0.0  0.0      0     0 ?        I    13:14   0:00 [rcu_tasks_kthread]
root          24  0.0  0.0      0     0 ?        I    13:14   0:00 [rcu_tasks_rude_kthread]
root          25  0.0  0.0      0     0 ?        I    13:14   0:00 [rcu_tasks_trace_kthread]
root          26  0.0  0.0      0     0 ?        S    13:14   0:00 [kauditd]
root          27  0.0  0.0      0     0 ?        S    13:14   0:00 [khungtaskd]
root          29  0.0  0.0      0     0 ?        S    13:14   0:00 [oom_reaper]
root          31  0.0  0.0      0     0 ?        I<   13:14   0:00 [kworker/R-writeback]
root          32  0.0  0.0      0     0 ?        S    13:14   0:00 [kcompactd0]
root          33  0.0  0.0      0     0 ?        SN   13:14   0:00 [ksmd]
root          34  0.0  0.0      0     0 ?        SN   13:14   0:00 [khugepaged]
root          35  0.0  0.0      0     0 ?        I<   13:14   0:00 [kworker/R-kblockd]
root          36  0.0  0.0      0     0 ?        I<   13:14   0:00 [kworker/R-blkcg_punt_bio]
root          37  0.0  0.0      0     0 ?        I<   13:14   0:00 [kworker/R-kintegrityd]
root          38  0.0  0.0      0     0 ?        S    13:14   0:00 [irq/9-acpi]
```



```
jashmi@Ubantu:~$ top

top - 15:04:58 up 4 min,  1 user,  load average: 1.09, 2.26, 1.15
Tasks: 194 total,   1 running, 189 sleeping,   0 stopped,   4 zombie
%Cpu(s):  1.2 us,  1.6 sy,  0.0 ni, 94.5 id,  0.0 wa,  0.0 hi,  2.8 si,  0.0 st
MiB Mem :   1646.2 total,     86.1 free,   1118.2 used,    616.2 buff/cache
MiB Swap:      0.0 total,      0.0 free,      0.0 used.    528.0 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   2184 jashmi    20   0 3450772 335300  94748 S   8.6  19.9   0:08.32 gnome-shell
   3025 jashmi    20   0 1142628 220100  99832 S   1.3  13.1   0:01.70 ptyxis
     51 root      20   0       0      0      0 I   0.7   0.0   0:01.11 kworker/u4:3-events_power_efficient
      9 root      20   0       0      0      0 I   0.3   0.0   0:00.98 kworker/0:0-events
     14 root      20   0       0      0      0 S   0.3   0.0   0:00.72 ksoftirqd/0
      1 root      20   0   24932  14892  10000 S   0.0   0.9   0:06.65 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
top - 15:05:17 up 4 min,  1 user,  load average: 1.07, 2.20, 1.14
Tasks: 194 total,   1 running, 189 sleeping,   0 stopped,   4 zombie
%Cpu(s):  0.0 us,  0.4 sy,  0.0 ni, 98.9 id,  0.0 wa,  0.0 hi,  0.7 si,  0.0 st
MiB Mem :   1646.2 total,     79.7 free,   1116.3 used,    626.5 buff/cache
MiB Swap:      0.0 total,      0.0 free,      0.0 used.    529.9 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND

   2184 jashmi    20   0 3452580 319912  79808 S   1.0  19.0   0:09.00 gnome-shell

   3025 jashmi    20   0 1144552 208024  86560 S   0.7  12.3   0:02.21 ptyxis

      1 root      20   0   24932  14892  10000 S   0.0   0.9   0:06.65 systemd

      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd

      3 root      20   0       0      0      0 S   0.0   0.0   0:00.00 pool_workqueue_release
```

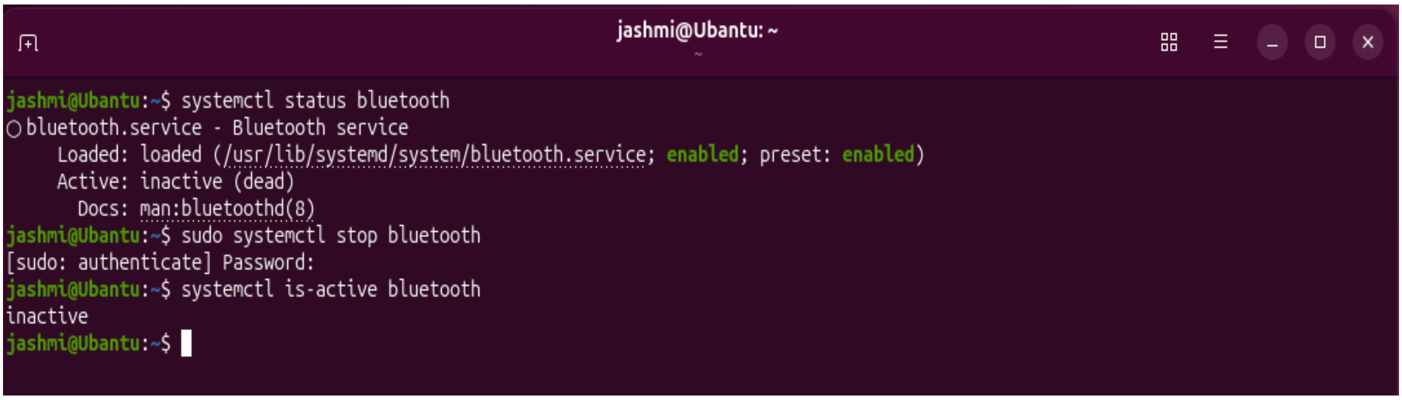

jashmi@Ubantu: ~ — systemctl list-units --type=service --state=running

```
jashmi@Ubantu:~$ systemctl list-units --type=service --state=running
  UNIT                               LOAD   ACTIVE SUB     DESCRIPTION
  accounts-daemon.service            loaded active running Accounts Service
  anacron.service                    loaded active running Run anacron jobs
  avahi-daemon.service               loaded active running Avahi mDNS/DNS-SD Stack
  chrony.service                     loaded active running chrony, an NTP client/server
  colord.service                     loaded active running Manage, Install and Generate Color Profiles
  cron.service                       loaded active running Regular background program processing daemon
  cups-browsed.service               loaded active running Make remote CUPS printers available locally
  cups.service                       loaded active running CUPS Scheduler
  dbus.service                       loaded active running D-Bus System Message Bus
  gdm.service                        loaded active running GNOME Display Manager
  ModemManager.service               loaded active running Modem Manager
  networkd-dispatcher.service        loaded active running Dispatcher daemon for systemd-networkd
  NetworkManager.service             loaded active running Network Manager
  polkit.service                     loaded active running Authorization Manager
  power-profiles-daemon.service      loaded active running Power Profiles daemon
  rsyslog.service                    loaded active running System Logging Service
  rtkit-daemon.service               loaded active running RealtimeKit Scheduling Policy Service
  snapd.service                      loaded active running Snap Daemon
  switcheroo-control.service         loaded active running Switcheroo Control Proxy service
  systemd-journald.service           loaded active running Journal Service
  systemd-logind.service             loaded active running User Login Management
  systemd-oomd.service               loaded active running Userspace Out-Of-Memory (OOM) Killer
  systemd-resolved.service           loaded active running Network Name Resolution
  systemd-udevd.service              loaded active running Rule-based Manager for Device Events and Files
  udisks2.service                    loaded active running Disk Manager
  unattended-upgrades.service        loaded active running Unattended Upgrades Shutdown
  upower.service                     loaded active running Daemon for power management
  user@1000.service                  loaded active running User Manager for UID 1000
  wpa_supplicant.service             loaded active running WPA supplicant

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

Managing and Disabling Unnecessary Services

Unused services expose additional attack surfaces. Temporarily stopping them improves security without permanent system changes.

- **Check service status:** systemctl status bluetooth
- **Stop service (non-permanent):** sudo systemctl stop bluetooth
- **Verify status:** systemctl is-active bluetooth



```
jashmi@Ubantu:~$ systemctl status bluetooth
○ bluetooth.service - Bluetooth service
     Loaded: loaded (/usr/lib/systemd/system/bluetooth.service; enabled; preset: enabled)
     Active: inactive (dead)
       Docs: man:bluetoothd(8)
jashmi@Ubantu:~$ sudo systemctl stop bluetooth
[sudo: authenticate] Password:
jashmi@Ubantu:~$ systemctl is-active bluetooth
inactive
jashmi@Ubantu:~$
```

OS Hardening Best Practices

OS hardening is the process of securing an operating system by reducing vulnerabilities, limiting access, and minimizing the attack surface. It ensures that only authorized users and services can access system resources, thereby improving overall system security.

1. Regular System Updates

Keeps the system protected from known vulnerabilities and security flaws.

```
sudo apt update && sudo apt upgrade
```

2. Strong User Authentication

Using strong passwords and avoiding password reuse prevents unauthorized access.

- Enforce complex passwords
- Lock unused user accounts

3. Principle of Least Privilege

Users and applications should have only the minimum permissions required to perform their tasks.

- Use sudo instead of logging in as root
- Assign limited permissions to users

4. Firewall Configuration

Enabling a firewall blocks unauthorized network traffic.

```
sudo ufw enable
sudo ufw status
```

5. Disable Unnecessary Services

Unused services increase attack surface and should be stopped or disabled.

```
systemctl list-units --type=service
sudo systemctl stop bluetooth
```

6. File and Directory Permission Management

Proper permissions prevent unauthorized access to sensitive files.

```
ls -l
chmod 644 filename
```

7. Monitoring Processes and Logs

Regular monitoring helps detect suspicious activities early.

```
ps aux
top
```

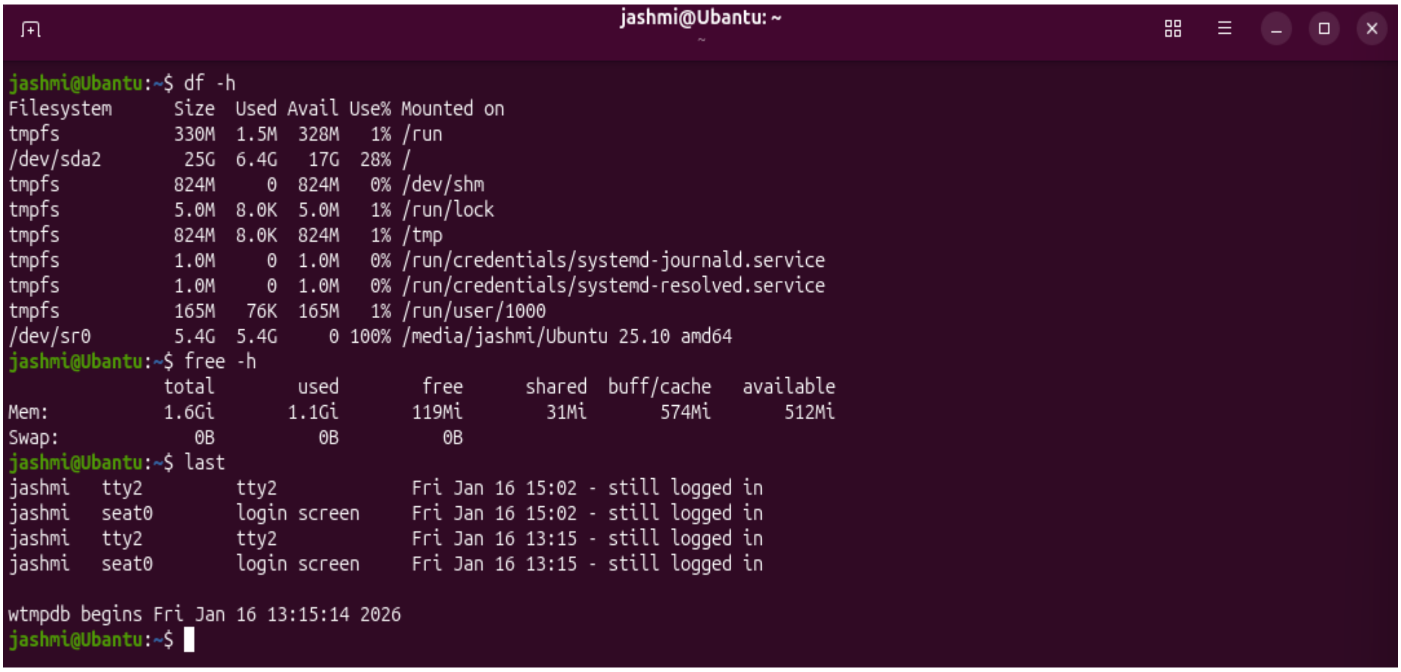
8. Avoid Direct Root Login

Direct root access increases risk. Administrative tasks should be done using sudo.

Additional Security Observations

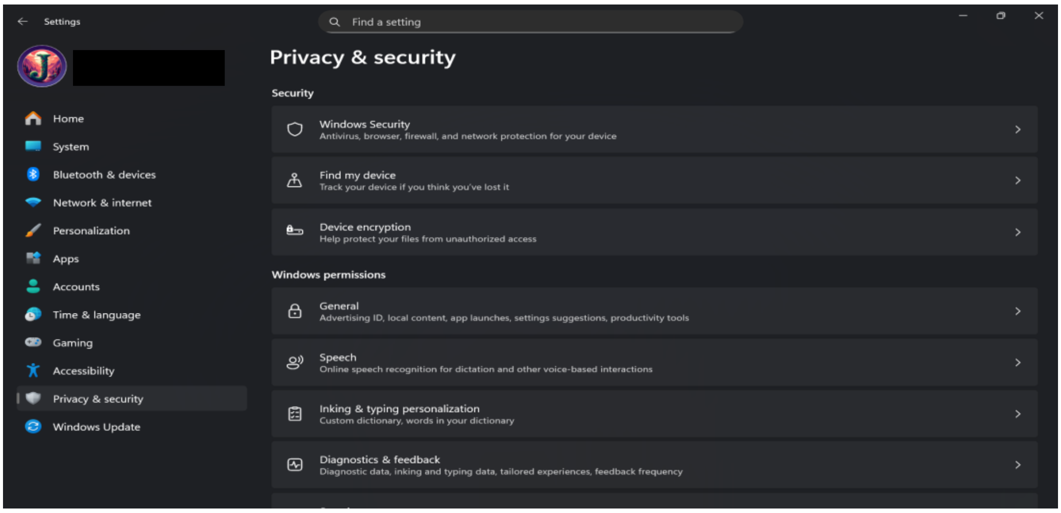
Basic checks further strengthen OS security awareness.

- Check disk usage: df -h
- Check memory usage: free -h
- Check login history: last



```
jashmi@Ubantu:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           330M  1.5M  328M   1% /run
/dev/sda2        25G  6.4G   17G  28% /
tmpfs           824M     0  824M   0% /dev/shm
tmpfs           5.0M  8.0K  5.0M   1% /run/lock
tmpfs           824M  8.0K  824M   1% /tmp
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-journald.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-resolved.service
tmpfs           165M   76K  165M   1% /run/user/1000
/dev/sr0        5.4G  5.4G     0 100% /media/jashmi/Ubuntu 25.10 amd64
jashmi@Ubantu:~$ free -h
               total        used        free      shared  buff/cache   available
Mem:           1.6Gi       1.1Gi       119Mi        31Mi       574Mi       512Mi
Swap:             0B          0B          0B
jashmi@Ubantu:~$ last
jashmi   tty2         tty2             Fri Jan 16 15:02 - still logged in
jashmi   seat0        login screen     Fri Jan 16 15:02 - still logged in
jashmi   tty2         tty2             Fri Jan 16 13:15 - still logged in
jashmi   seat0        login screen     Fri Jan 16 13:15 - still logged in

wtmpdb begins Fri Jan 16 13:15:14 2026
jashmi@Ubantu:~$ 
```

Using Windows Security Settings



Privacy & security

Security

Windows Security
Antivirus, browser, firewall, and network protection for your device

Find my device
Track your device if you think you've lost it

Device encryption
Help protect your files from unauthorized access

Windows permissions

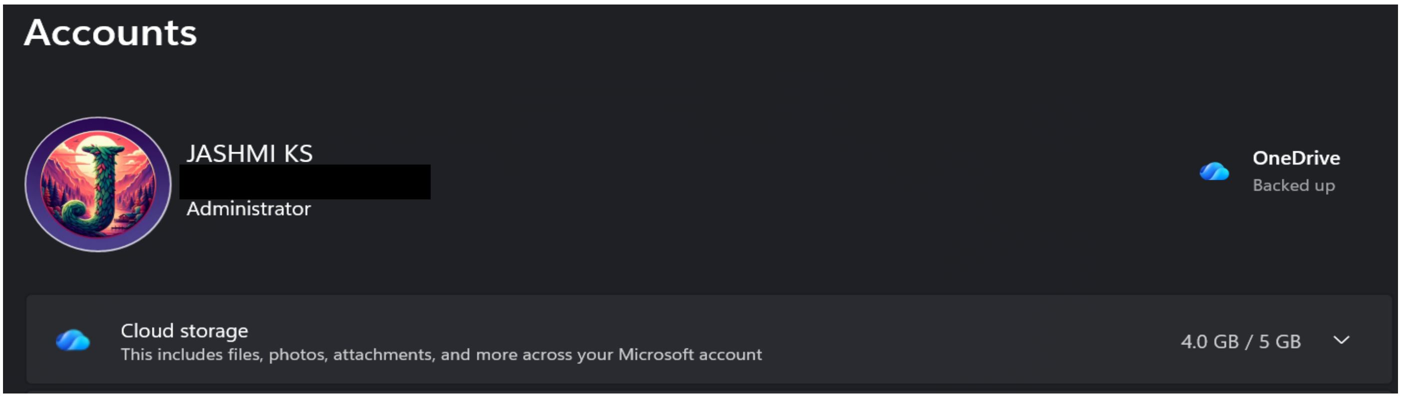
General
Advertising ID, local content, app launches, settings suggestions, productivity tools

Speech
Online speech recognition for dictation and other voice-based interactions

Inking & typing personalization
Custom dictionary, words in your dictionary

Diagnostics & feedback
Diagnostic data, inking and typing data, tailored experiences, feedback frequency

User Accounts & Access Control



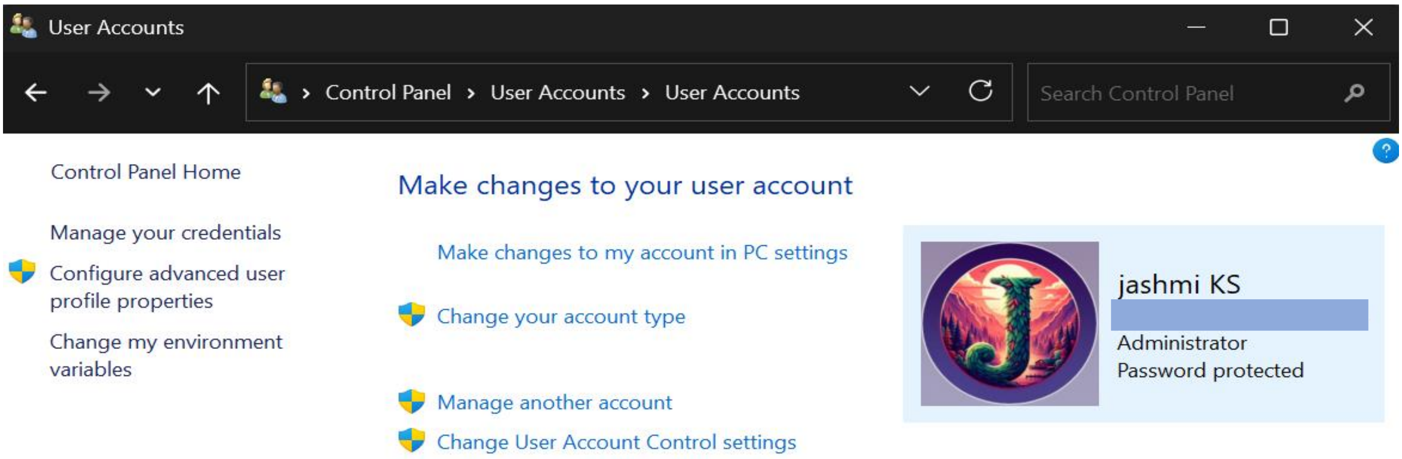
Accounts

JASHMI KS
[redacted]
Administrator

OneDrive
Backed up

Cloud storage
This includes files, photos, attachments, and more across your Microsoft account

4.0 GB / 5 GB



User Accounts

Control Panel › User Accounts › User Accounts

Search Control Panel

Control Panel Home

Manage your credentials

Configure advanced user profile properties

Change my environment variables

Make changes to your user account

Make changes to my account in PC settings

Change your account type

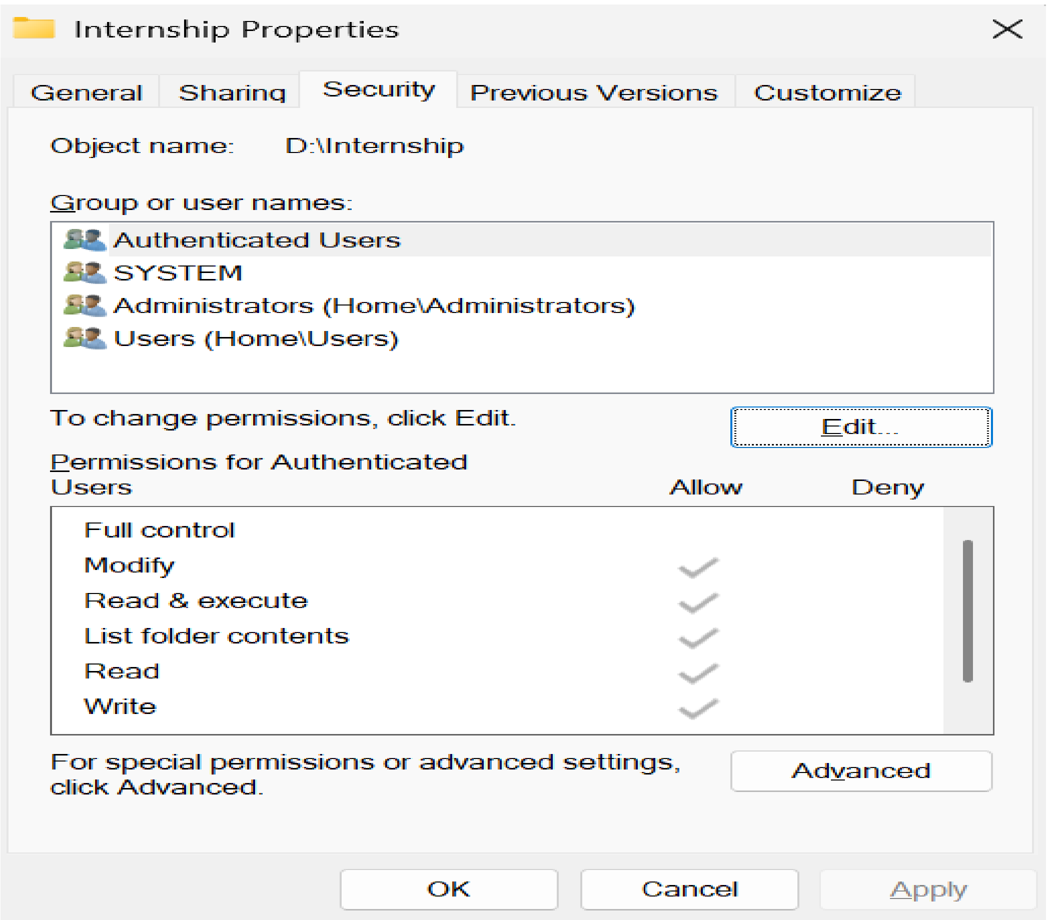
Manage another account

Change User Account Control settings

jashmi KS
[redacted]
Administrator
Password protected

File & Folder Permissions

Windows uses **NTFS permissions** instead of chmod.



Internship Properties

General | Sharing | Security | Previous Versions | Customize

Object name: D:\Internship

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (Home\Administrators)
- Users (Home\Users)

To change permissions, click Edit. [Edit...]

Permissions for Authenticated Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced. [Advanced]

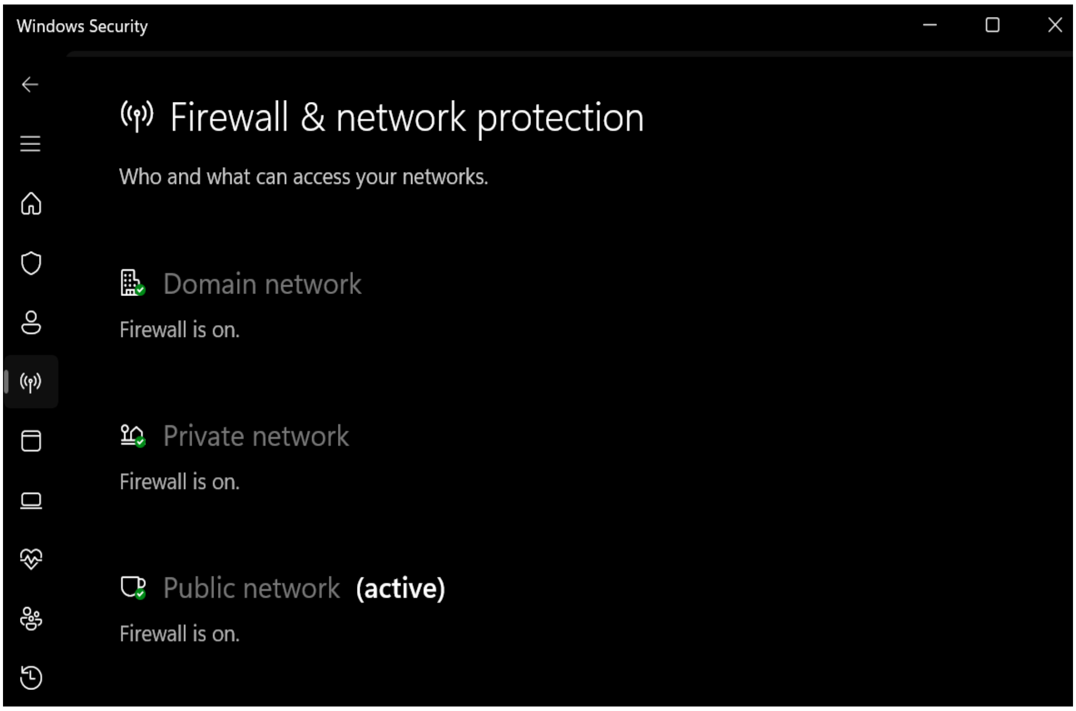
[OK] [Cancel] [Apply]

Administrator vs Standard User

- **Administrator:** Full system control
- **Standard User:** Limited access for safety

Enabling Windows Firewall

Firewall protects the system from unauthorized network access.



Firewall & network protection

Who and what can access your networks.

Domain network

Firewall is on.

Private network

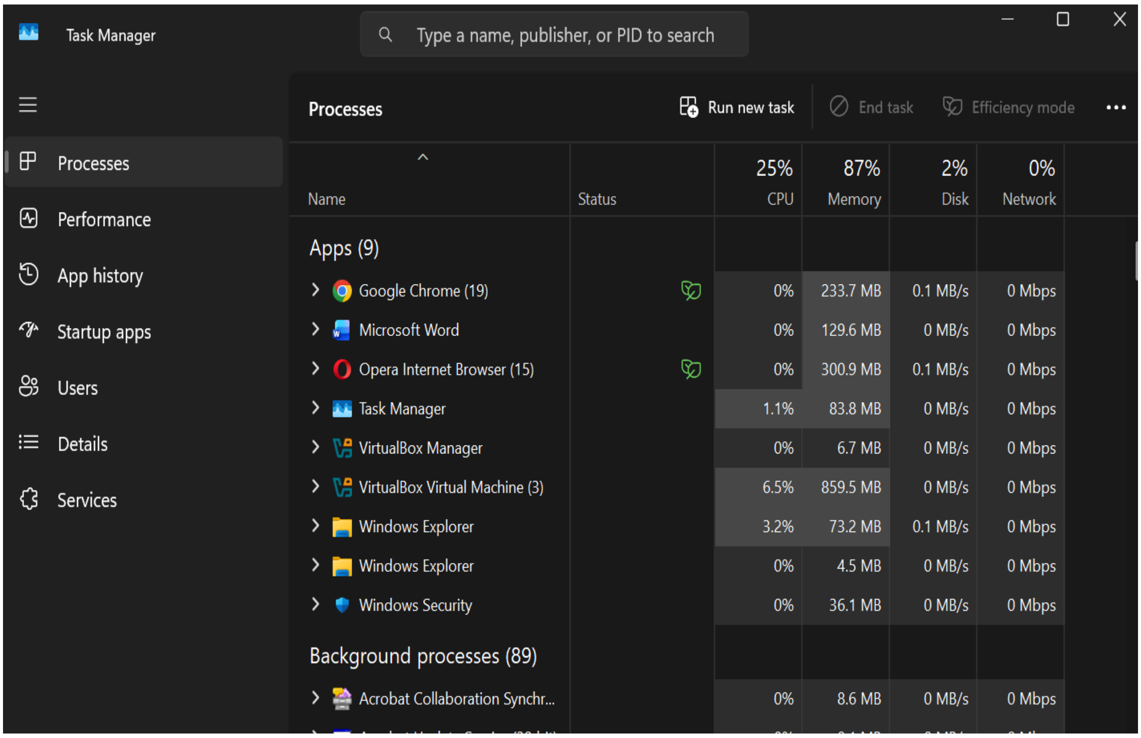
Firewall is on.

Public network (active)

Firewall is on.

Identifying Running Processes & Services

Running processes show active programs and background services.

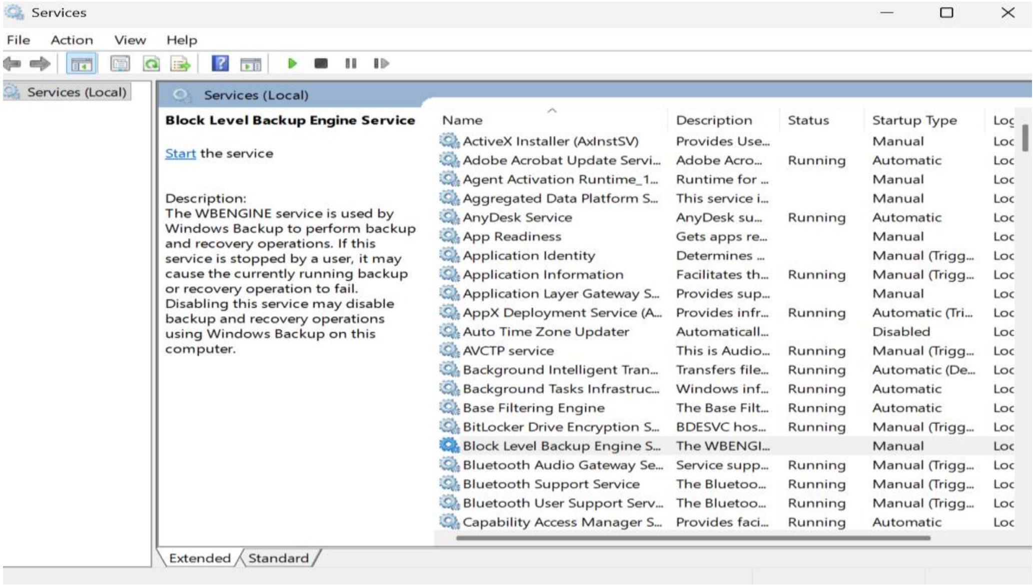


Processes

Name	Status	25% CPU	87% Memory	2% Disk	0% Network
Apps (9)					
Google Chrome (19)		0%	233.7 MB	0.1 MB/s	0 Mbps
Microsoft Word		0%	129.6 MB	0 MB/s	0 Mbps
Opera Internet Browser (15)		0%	300.9 MB	0.1 MB/s	0 Mbps
Task Manager		1.1%	83.8 MB	0 MB/s	0 Mbps
VirtualBox Manager		0%	6.7 MB	0 MB/s	0 Mbps
VirtualBox Virtual Machine (3)		6.5%	859.5 MB	0 MB/s	0 Mbps
Windows Explorer		3.2%	73.2 MB	0.1 MB/s	0 Mbps
Windows Explorer		0%	4.5 MB	0 MB/s	0 Mbps
Windows Security		0%	36.1 MB	0 MB/s	0 Mbps
Background processes (89)					
Acrobat Collaboration Synchr...		0%	8.6 MB	0 MB/s	0 Mbps

Disabling Unnecessary Services

Unused services increase attack surface.



Block Level Backup Engine Service

Start the service

Description:
The WBENGINE service is used by Windows Backup to perform backup and recovery operations. If this service is stopped by a user, it may cause the currently running backup or recovery operation to fail. Disabling this service may disable backup and recovery operations using Windows Backup on this computer.

Name	Description	Status	Startup Type	Log
ActiveX Installer (AxInstSV)	Provides Use...		Manual	Loc
Adobe Acrobat Update Servi...	Adobe Acro...	Running	Automatic	Loc
Agent Activation Runtime_1...	Runtime for ...		Manual	Loc
Aggregated Data Platform S...	This service i...		Manual	Loc
AnyDesk Service	AnyDesk su...	Running	Automatic	Loc
App Readiness	Gets apps re...		Manual	Loc
Application Identity	Determines ...		Manual (Trigg...	Loc
Application Information	Facilitates th...	Running	Manual (Trigg...	Loc
Application Layer Gateway S...	Provides sup...		Manual	Loc
AppX Deployment Service (A...	Provides infr...	Running	Automatic (Tri...	Loc
Auto Time Zone Updater	Automaticall...		Disabled	Loc
AVCTP service	This is Audio...	Running	Manual (Trigg...	Loc
Background Intelligent Tran...	Transfers file...	Running	Automatic (De...	Loc
Background Tasks Infrastruc...	Windows inf...	Running	Automatic	Loc
Base Filtering Engine	The Base Filt...	Running	Automatic	Loc
BitLocker Drive Encryption S...	BDESVC hos...	Running	Manual (Trigg...	Loc
Block Level Backup Engine S...	The WBENGI...		Manual	Loc
Bluetooth Audio Gateway Se...	Service supp...	Running	Manual (Trigg...	Loc
Bluetooth Support Service	The Bluetoo...	Running	Manual (Trigg...	Loc
Bluetooth User Support Serv...	The Bluetoo...	Running	Manual (Trigg...	Loc
Capability Access Manager S...	Provides faci...	Running	Automatic	Loc

OS Hardening Best Practices (Windows)

OS hardening improves system security.

Best Practices

- Keep Windows updated
- Enable firewall & antivirus
- Use strong passwords
- Disable unnecessary services
- Use standard user accounts

I learned basic OS security using **Ubuntu and Windows**, including users, permissions, and admin vs standard users. I also learned how firewalls, process monitoring, and OS hardening protect a system.