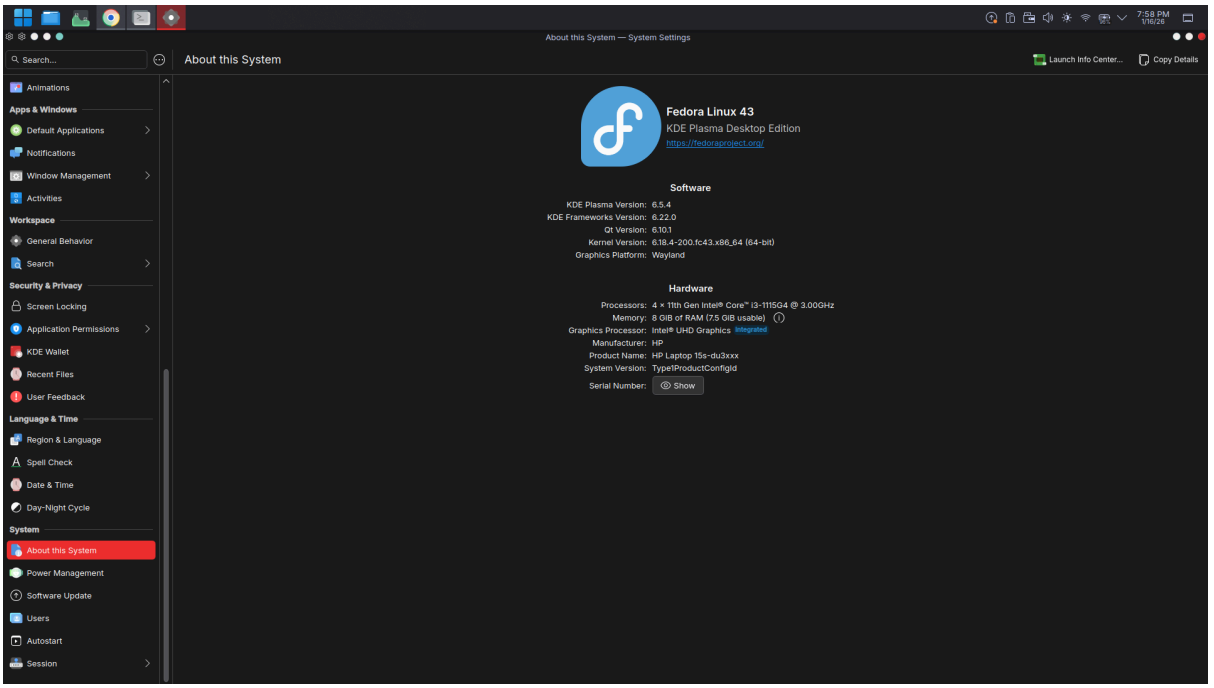
Task day-2

16/1/2026

☑ 1.Installed Fedora



☑ 2.Explore user accounts, permissions, and access control mechanisms.

☑ 2.1 User controls

- Add user - sudo user <username>
- Set password - sudo passwd <username>
- Give sudo access -> sudo usermod -aG wheel <username>

☑ 2.2 permissions

- UGO(User, Group, Others): every file and directory has 3 type permissions for three distinct categories of users
- permission types:
  - read(r) to view contents
  - write(w) to edit or delete the file
  - Execute (x) to run as a program/script
  - These will have different commands for files and directories

☑ 2.3 Access control mechanisms

- Access control mechanisms in Fedora are maintained by using several specialised access control mechanisms that go beyond simple file permissions. Those are :
  1.SELinux
  2.Polkit(formely policykit)
  3.Linux Capabilities
  4.Linux Audit Framework

☑ 3. File permissions

- ls -l is used for viewing file and directory permissions

- Chmod (chnage mode) is used to modify what users can do with a file.
  Eg: adding/removing permissions for a specific group of users or a user
- Chown(chnage owner) is used to transfer a file to a different user or group. Usually requires sudo

☑ 4. Administrator vs Standard user privileges

1. Standard user

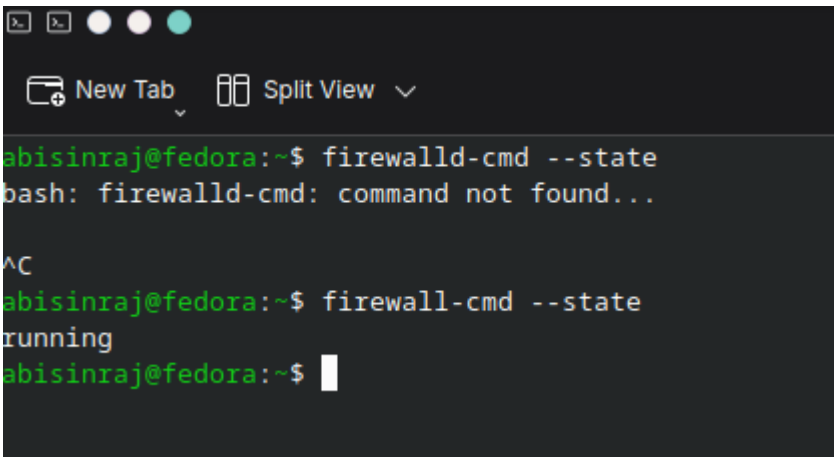
- A standard user is intended for everyday computing tasks,so they can only access and modify files within their own home directory
- Cant install/uninstall apps system wide
- Safety isnt a compromise , malware running in standard account is restricted to that user's files only and wont compromise the entire os

2. Administrator

- Usually, an administrator is a standard user who belongs to the special wheel group
- They can manage other user accounts, install system-wide hardware or software, and modify critical security settings
- Needs authentication while performing sensitive tasks (their own password, not root password) to confirm the action

☑ 5. Enabling Fedora firewall

- Fedora by default uses firewalld as their default firewall . we can install ufw by manually installing. By default its turned on
- To turn it on, use sudo systemctl enable firewalld
  Sudo systemctl start firewalld
- To install ufw on fedora use the command ,sudo dnf install ufw
- Enable ufw and start, sudo systemctl enable ufw
  Sudo systemctl enable ufw
- To check their status use —state on firewalld and status in ufw command
  Eg: firewall-cmd –state ,ufw status



☑ 6.Identify running processes and services.

Fedora uses systemd for service management and standard linux utilities for process monitoring

1. Identifying Running Services

->Services (or daemons) are background tasks managed by the system. Use the systemctl utility to inspect them.

->List all active services:

systemctl list-units --type=service

->List only currently running services:

systemctl list-units --type=service --state=running

->Check the detailed status of a specific service:

systemctl status <service_name> (e.g., systemctl status sshd)

->List all installed service files (enabled or disabled):

systemctl list-unit-files --type=service

2. identifying running processes.

Processes are individual instances of running programs. fedora offers several tools for both static snapshots and real-time monitoring.

->standard snapshot (ps): Use ps aux to see a detailed list of all processes from all users, including those without a terminal.

->interactive real-time monitoring (top / htop): top: the default, built-in real-time monitor. htop: a more user-friendly, interactive alternative (install via sudo dnf install htop). ->visualizing process hierarchy (pstree): use pstree -p to see processes organized in a tree structure showing parent-child relationships.

->searching for a specific process (pgrep): use pgrep -l <name> to quickly find the process id (pid) and name of a specific program.