Project Title:

"Full Enterprise Linux Environment Deployment for Company."

Scenario Background:

Welcome to your new job at **Company**, a mid-size technology company. You are joining the **Linux Infrastructure Team** as a Junior Linux System Administrator. Your team lead has assigned you a critical task: **to build and secure a new internal server that will serve multiple departments within** the company.

This server will be used to:

- Host internal web tools
- Store and manage department-specific files
- Enforce strict access control
- Automate system maintenance
- Be ready for secure remote access

Project Phases & Tasks:

Phase 1: System Preparation and User Environment

Objective: Prepare the Linux system and organize the user structure.

Tasks:

1. **Change the hostname** of the system to `intranet.technova.local`.
2. **Set a static IP**:
3. **Create groups** for each department:
   - `dev_team`, `hr_team`, `it_team`, `sales_team`
4. **Create the following users and assign them to the correct groups:**

Username	Group	Role
alice	dev_team	Developer
bob	hr_team	HR Assistant
carol	it_team	IT Technician

Username	Group	Role
dave	sales_team	Sales Rep
erin	dev_team	Developer Lead
frank	it_team	IT Manager

5. **Set default shell to `/bin/bash`** for all users and create a secure password for each.
6. **Force password change** on first login for security.

Phase 2: Directory & Permission Setup

Objective: Create shared department folders with proper access control.

Tasks:

1. Create the following directories:
   - `/srv/dev`
   - `/srv/hr`
   - `/srv/it`
   - `/srv/sales`
2. Set **ownership and permissions**:
   - Each directory owned by `root:GROUP_NAME`
   - Permission: `2770` (SetGID for group inheritance)
3. **Use ACLs**:
   - Allow `frank` (IT Manager) to read/write all folders
   - Allow `bob` read-only access to `/srv/sales` for HR auditing
4. Create a shared temp folder `/srv/public_temp`:
   - All users can write
   - Enable sticky bit so users can't delete each other's files

---

Phase 3: Storage and LVM Setup

Objective: Configure dedicated storage using LVM for each department.

Tasks:

1. Use a second virtual disk `/dev/sdb` to create an LVM setup:
   - Create a Physical Volume
   - Create a Volume Group: `vg_deptdata`
   - Create Logical Volumes:
     - `lv_dev` (1G), mount to `/srv/dev`
     - `lv_hr` (500M), mount to `/srv/hr`

        - `lv_it` (1G), mount to `/srv/it`
        - `lv_sales` (1G), mount to `/srv/sales`
2. Format each LV with `xfs` and mount it permanently via `/etc/fstab`.
3. Enable **disk quotas** on `/srv/hr` and `/srv/sales`:
    - Limit each user to 100MB soft, 150MB hard.

Phase 4: Security Hardening

Objective: Secure the server and control access.

Tasks:

1. **Configure `sudo`** access:
    - Allow `frank` to use `sudo` for user management and system updates.
    - Use `/etc/sudoers.d/` for custom rules.
2. **Configure SSH access**:
    - Allow only `it_team` to connect via SSH.
    - Disable root login.
    - Setup **SSH key-based login** for `frank`.
3. **Apply SELinux policies**:
    - Ensure SELinux is enforcing.
    - Allow HTTPD to access `/var/www/html/intranet`.
4. **Configure the firewall** to allow:
    - SSH (port 22)
    - HTTP (port 80)
    - ICMP (ping)

Phase 5: Internal Web Portal

Objective: Host a simple internal company web page.

Tasks:

1. Install and enable the `httpd` service.
2. Create a basic `index.html` page:

    ```
    html
    CopyEdit
    <h1>Welcome to TechNova Internal Portal</h1>
    <p>Only accessible inside the company.</p>
    ```

3. Place the file under `/var/www/html/` and set correct SELinux context if needed.

4. Ensure the service starts on boot and is accessible at `http://192.168.100.10`.

Phase 6: Automation & Scripting

Objective: Automate routine maintenance tasks.

Tasks:

1. Write a script `/usr/local/bin/backup_dept.sh` that:
   - Archives each `/srv/DEPT` folder to `/backups/DEPT_$(date +%F).tar.gz`
2. Create a cron job to run the script **daily at 1:00 AM**.
3. Use `logger` inside the script to log backup success to `/var/log/messages`.
4. Schedule a one-time `at` job to send a broadcast system message at 5 PM:

> "System maintenance will occur tonight at 1:00 AM. Save your work!"

Phase 7: Troubleshooting & Logs

Objective: Practice system recovery and log monitoring.

Tasks:

1. Introduce an error in `/etc/fstab` (mount a missing disk) and reboot.
   - Fix it using GRUB rescue or single-user mode.
2. Check logs for:
   - Failed SSH logins (`/var/log/secure`)
   - Backup success messages
3. Use `last`, `who`, and `journalctl` to review recent activity.

Final Deliverables:

- Working Linux system with all tasks completed
- Screenshot proof of:
  - Directory permissions
  - LVM and mounted partitions
  - Web portal in browser
  - Cron logs
- A **report** (text or markdown) including:
  - User and group structure

- LVM layout
- ACL and permission strategy
- Security configurations (firewall, sudo, SSH, SELinux)
- Scripts used and their output