Red Hat Full Project Documentation

"Full Enterprise Linux Environment Deployment for a Company."

System Administration & Log Monitoring

Prepared by:

Kerolos Mamdouh Nageh

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: **Build and secure a new internal server** that will serve multiple departments in the company.

Introduction

Objective: Deploy and secure an internal Linux server for a mid-size tech company.

Key Goals:

- Host internal web tools
- Manage department-specific files
- Enforce strict access control
- Automate system maintenance
- Enable secure remote access

Work completed in structured phases:

- System setup and user environment
- Directory and permission configuration
- Storage and LVM setup
- Security hardening
- Internal web hosting
- Automation via scripting
- Troubleshooting and log monitoring

Phase 1: System Preparation and User Environment

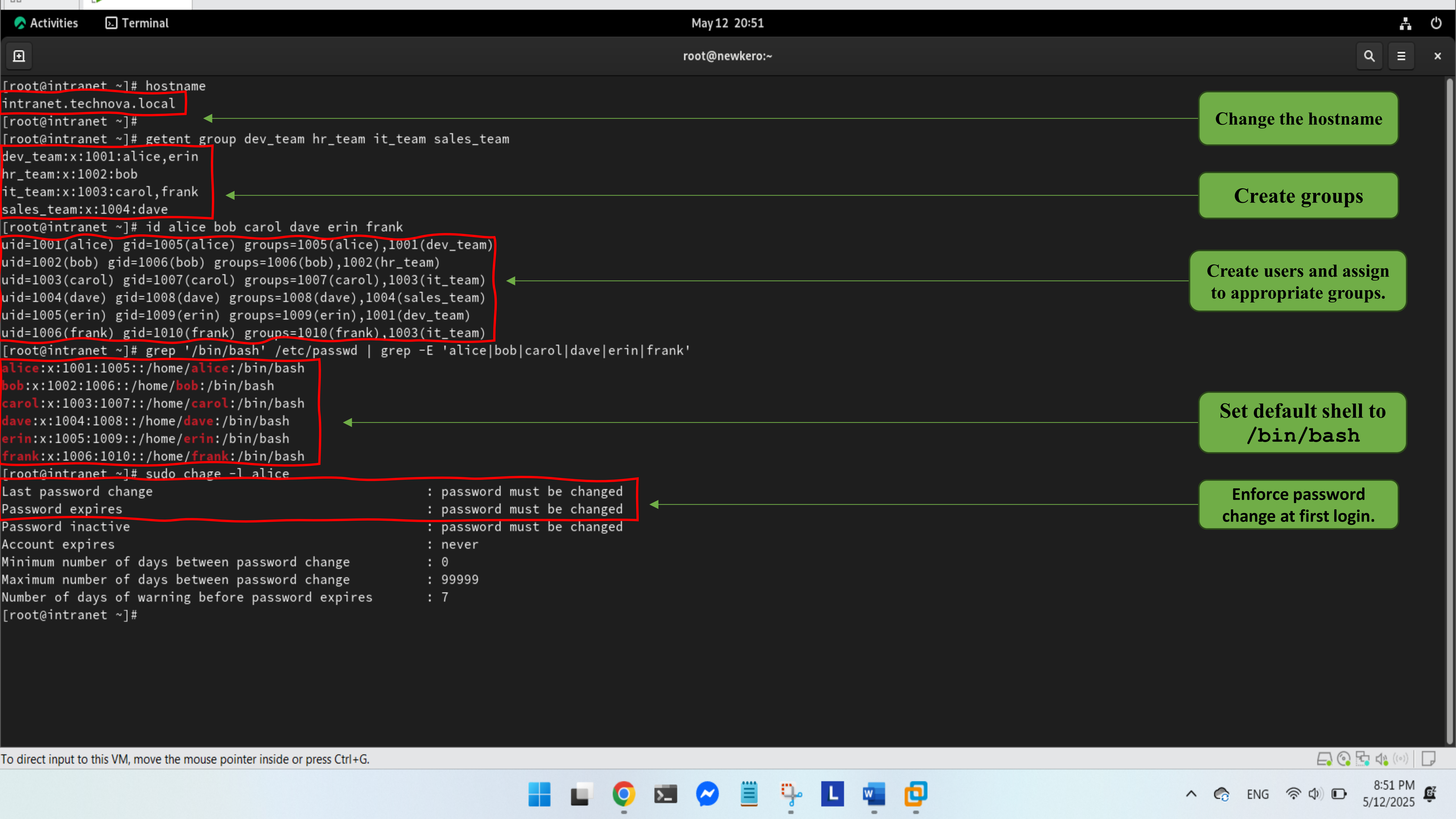
- **Objective:** Prepare the Linux system and organize the user structure.

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**
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.



```
[root@intranet ~]# hostname
intranet.technova.local
[root@intranet ~]#
[root@intranet ~]# getent group dev_team hr_team it_team sales_team
dev_team:x:1001:alice,erin
hr_team:x:1002:bob
it_team:x:1003:carol,frank
sales_team:x:1004:dave
[root@intranet ~]# id alice bob carol dave erin frank
uid=1001(alice) gid=1005(alice) groups=1005(alice),1001(dev_team)
uid=1002(bob) gid=1006(bob) groups=1006(bob),1002(hr_team)
uid=1003(carol) gid=1007(carol) groups=1007(carol),1003(it_team)
uid=1004(dave) gid=1008(dave) groups=1008(dave),1004(sales_team)
uid=1005(erin) gid=1009(erin) groups=1009(erin),1001(dev_team)
uid=1006(frank) gid=1010(frank) groups=1010(frank),1003(it_team)
[root@intranet ~]# grep '/bin/bash' /etc/passwd | grep -E 'alice|bob|carol|dave|erin|frank'
alice:x:1001:1005::/home/alice:/bin/bash
bob:x:1002:1006::/home/bob:/bin/bash
carol:x:1003:1007::/home/carol:/bin/bash
dave:x:1004:1008::/home/dave:/bin/bash
erin:x:1005:1009::/home/erin:/bin/bash
frank:x:1006:1010::/home/frank:/bin/bash
[root@intranet ~]# sudo chage -l alice
Last password change                                    : password must be changed
Password expires                                        : password must be changed
Password inactive                                       : password must be changed
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
[root@intranet ~]#
```

Change the hostname

Create groups

Create users and assign to appropriate groups.

Set default shell to `/bin/bash`

Enforce password change at first login.

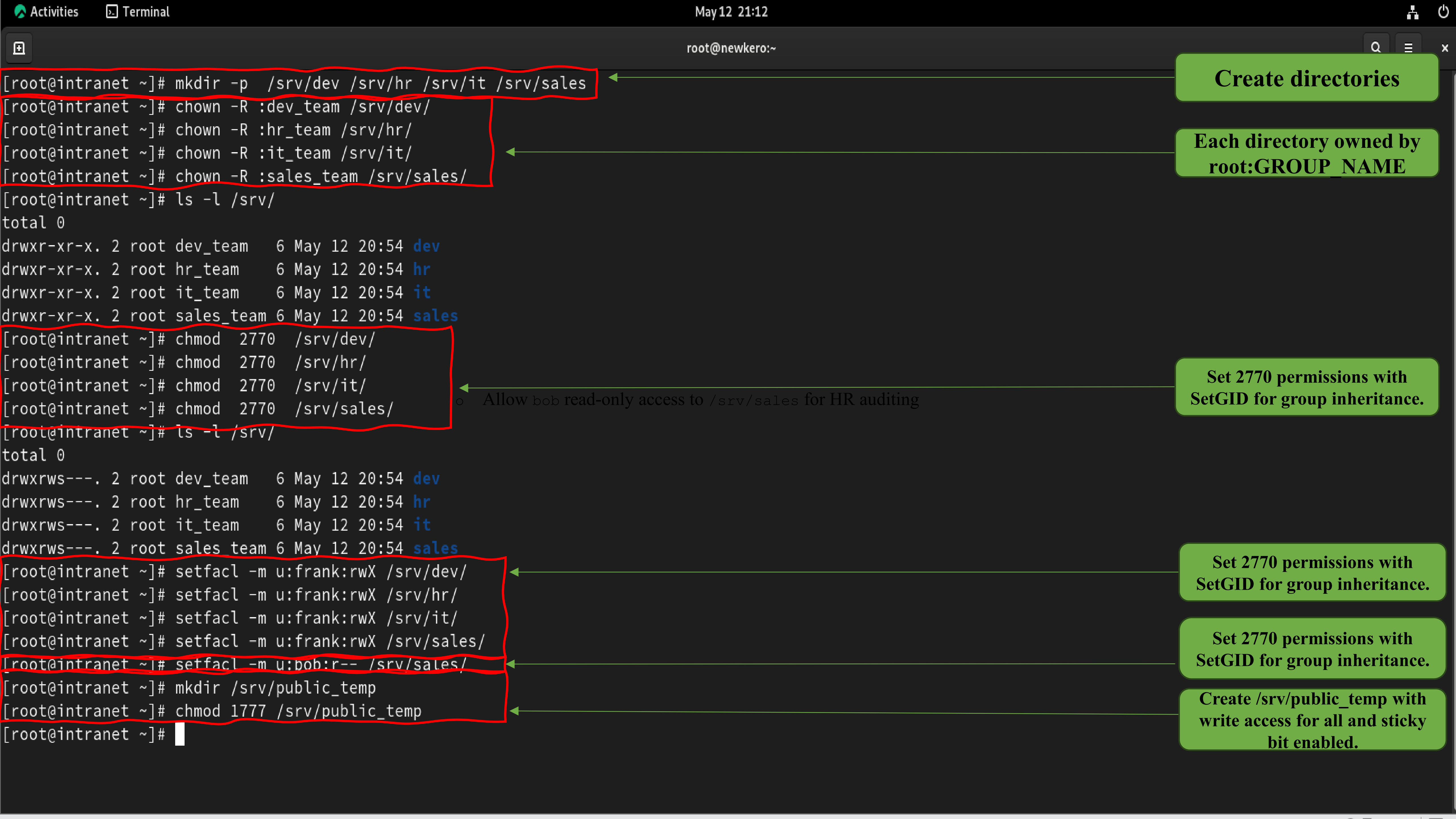
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

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



```
[root@intranet ~]# mkdir -p  /srv/dev /srv/hr /srv/it /srv/sales
[root@intranet ~]# chown -R :dev_team /srv/dev/
[root@intranet ~]# chown -R :hr_team /srv/hr/
[root@intranet ~]# chown -R :it_team /srv/it/
[root@intranet ~]# chown -R :sales_team /srv/sales/
[root@intranet ~]# ls -l /srv/
total 0
drwxr-xr-x. 2 root dev_team   6 May 12 20:54 dev
drwxr-xr-x. 2 root hr_team    6 May 12 20:54 hr
drwxr-xr-x. 2 root it_team    6 May 12 20:54 it
drwxr-xr-x. 2 root sales_team 6 May 12 20:54 sales
[root@intranet ~]# chmod  2770  /srv/dev/
[root@intranet ~]# chmod  2770  /srv/hr/
[root@intranet ~]# chmod  2770  /srv/it/
[root@intranet ~]# chmod  2770  /srv/sales/
[root@intranet ~]# ls -l /srv/
total 0
drwxrws---. 2 root dev_team   6 May 12 20:54 dev
drwxrws---. 2 root hr_team    6 May 12 20:54 hr
drwxrws---. 2 root it_team    6 May 12 20:54 it
drwxrws---. 2 root sales_team 6 May 12 20:54 sales
[root@intranet ~]# setfacl -m u:frank:rwX /srv/dev/
[root@intranet ~]# setfacl -m u:frank:rwX /srv/hr/
[root@intranet ~]# setfacl -m u:frank:rwX /srv/it/
[root@intranet ~]# setfacl -m u:frank:rwX /srv/sales/
[root@intranet ~]# setfacl -m u:bob:r-- /srv/sales/
[root@intranet ~]# mkdir /srv/public_temp
[root@intranet ~]# chmod 1777 /srv/public_temp
[root@intranet ~]# 
```

Create directories

Each directory owned by root:GROUP_NAME

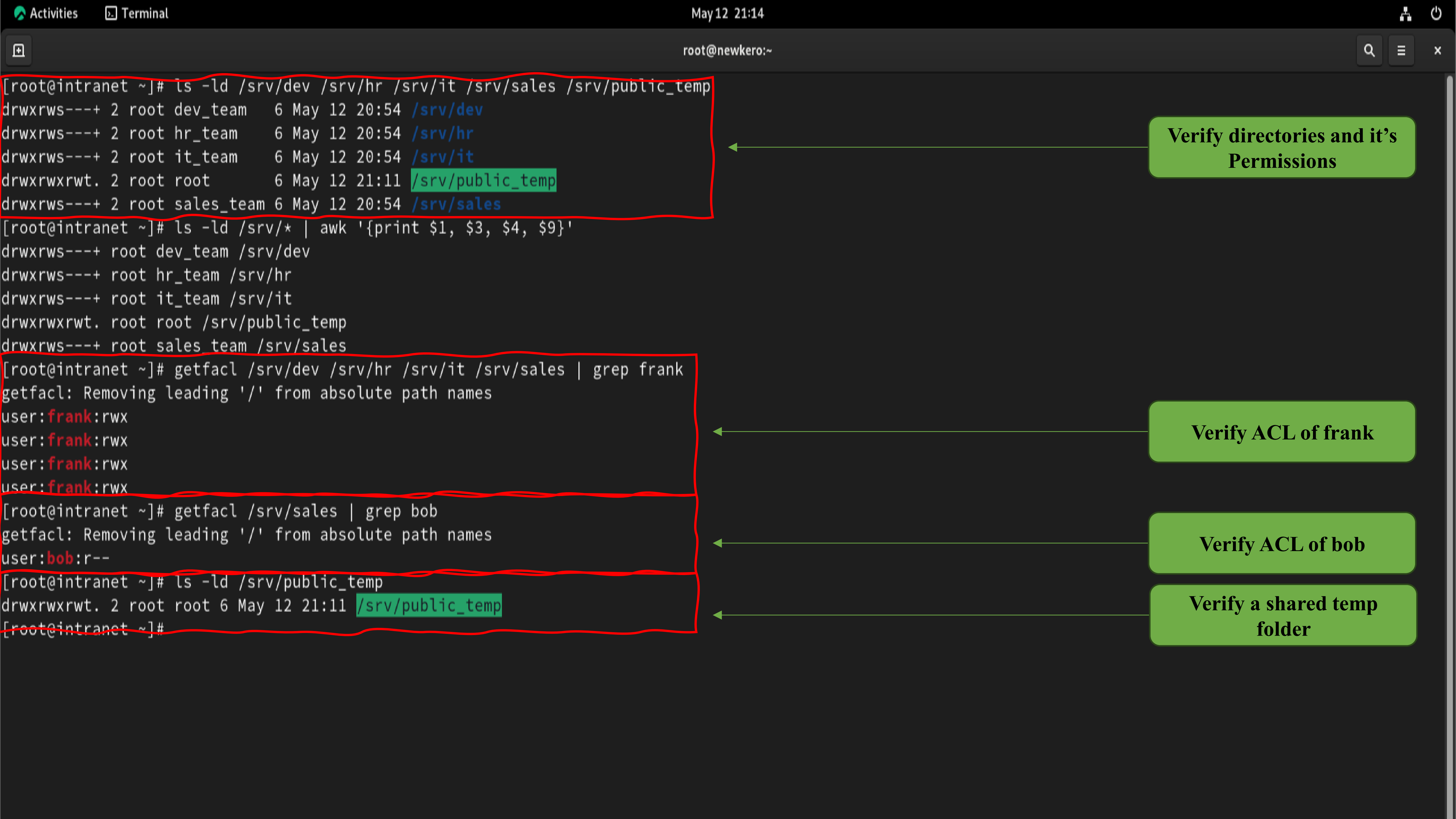
Set 2770 permissions with SetGID for group inheritance.

o Allow bob read-only access to /srv/sales for HR auditing

Set 2770 permissions with SetGID for group inheritance.

Set 2770 permissions with SetGID for group inheritance.

Create /srv/public_temp with write access for all and sticky bit enabled.



```
[root@intranet ~]# ls -ld /srv/dev /srv/hr /srv/it /srv/sales /srv/public_temp
drwxrws---+ 2 root dev_team   6 May 12 20:54 /srv/dev
drwxrws---+ 2 root hr_team    6 May 12 20:54 /srv/hr
drwxrws---+ 2 root it_team    6 May 12 20:54 /srv/it
drwxrwxrwt. 2 root root       6 May 12 21:11 /srv/public_temp
drwxrws---+ 2 root sales_team 6 May 12 20:54 /srv/sales
[root@intranet ~]# ls -ld /srv/* | awk '{print $1, $3, $4, $9}'
drwxrws---+ root dev_team /srv/dev
drwxrws---+ root hr_team /srv/hr
drwxrws---+ root it_team /srv/it
drwxrwxrwt. root root /srv/public_temp
drwxrws---+ root sales_team /srv/sales
[root@intranet ~]# getfacl /srv/dev /srv/hr /srv/it /srv/sales | grep frank
getfacl: Removing leading '/' from absolute path names
user:frank:rwx
user:frank:rwx
user:frank:rwx
user:frank:rwx
[root@intranet ~]# getfacl /srv/sales | grep bob
getfacl: Removing leading '/' from absolute path names
user:bob:r--
[root@intranet ~]# ls -ld /srv/public_temp
drwxrwxrwt. 2 root root 6 May 12 21:11 /srv/public_temp
[root@intranet ~]#
```

Verify directories and it’s Permissions

Verify ACL of frank

Verify ACL of bob

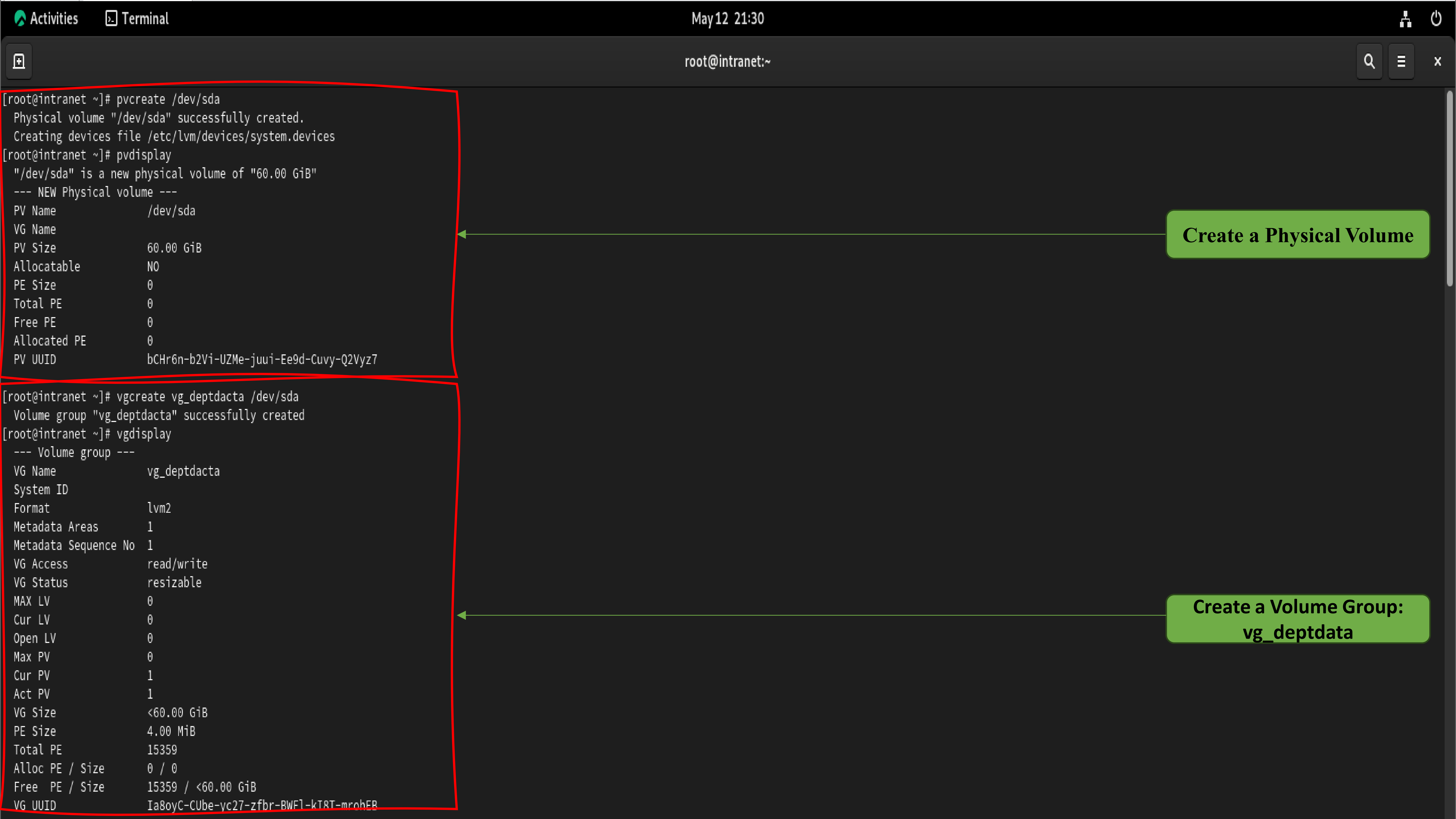
Verify a shared temp folder

Phase 3: Storage and LVM Setup

- **Objective:** Configure dedicated storage using LVM for each department.

Tasks:

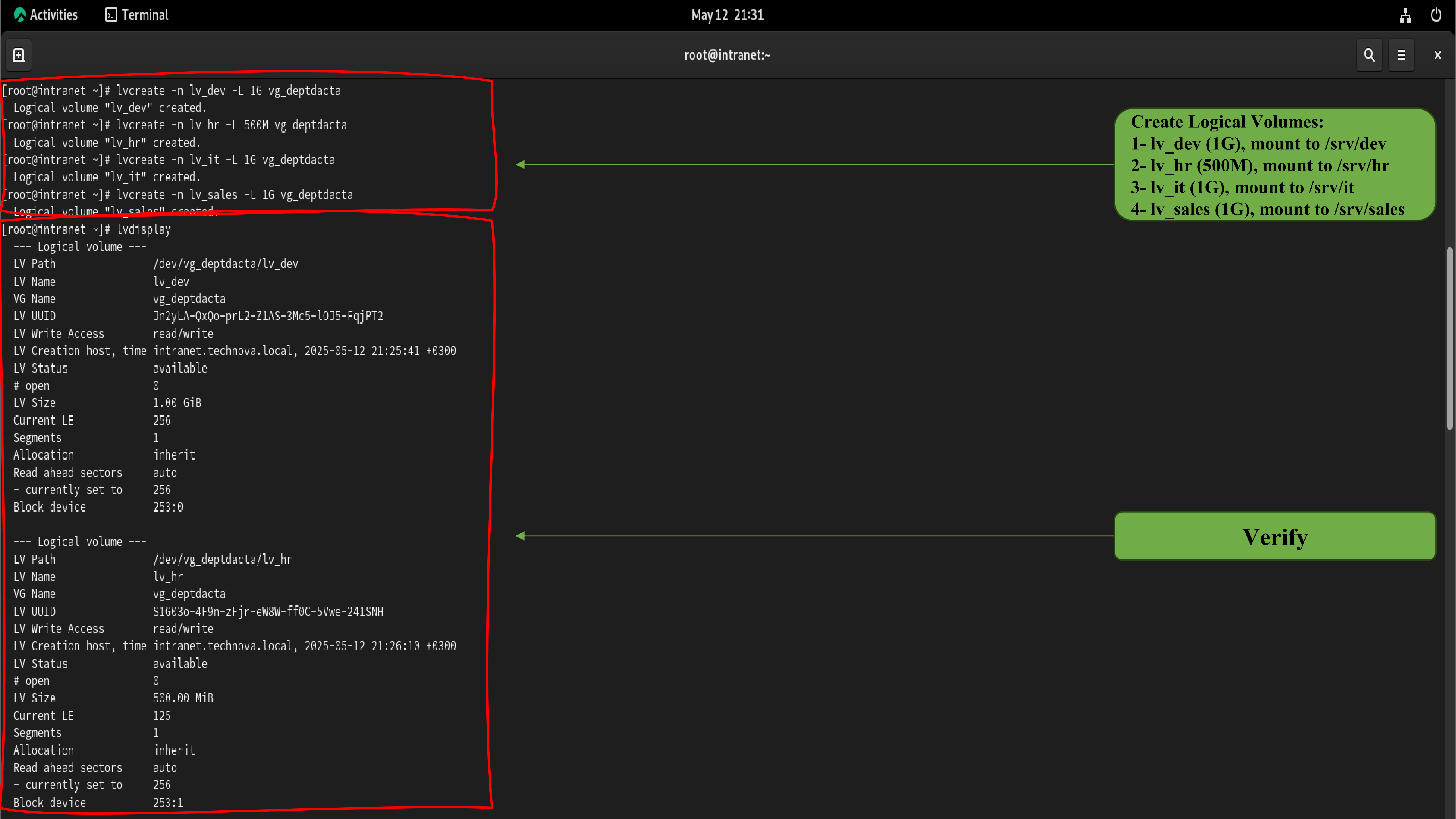
1. Use a second virtual disk `/dev/sdb` to create an LVM setup:
    - Create a Physical Volume
    - Create a Volume Group: `vg_deptdata`
    - Create Logical Volumes:
        - `lv_dev` (1G), mount to `/srv/dev`
        - `lv_hr` (500M), mount to `/srv/hr`
        - `lv_it` (1G), mount to `/srv/it`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



```
[root@intranet ~]# pvcreate /dev/sda
  Physical volume "/dev/sda" successfully created.
  Creating devices file /etc/lvm/devices/system.devices
[root@intranet ~]# pvdisplay
  "/dev/sda" is a new physical volume of "60.00 GiB"
  --- NEW Physical volume ---
  PV Name               /dev/sda
  VG Name
  PV Size               60.00 GiB
  Allocatable           NO
  PE Size               0
  Total PE              0
  Free PE               0
  Allocated PE          0
  PV UUID               bCHr6n-b2Vi-UZMe-juui-Ee9d-Cuvy-Q2Vyz7

[root@intranet ~]# vgcreate vg_deptdacta /dev/sda
  Volume group "vg_deptdacta" successfully created
[root@intranet ~]# vgdisplay
  --- Volume group ---
  VG Name               vg_deptdacta
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  1
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                0
  Open LV               0
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               <60.00 GiB
  PE Size               4.00 MiB
  Total PE              15359
  Alloc PE / Size       0 / 0
  Free  PE / Size       15359 / <60.00 GiB
  VG UUID               Ia8oyC-CUbe-yc27-zfbr-BWFl-kT8T-mrohEB
```

Create a Physical Volume

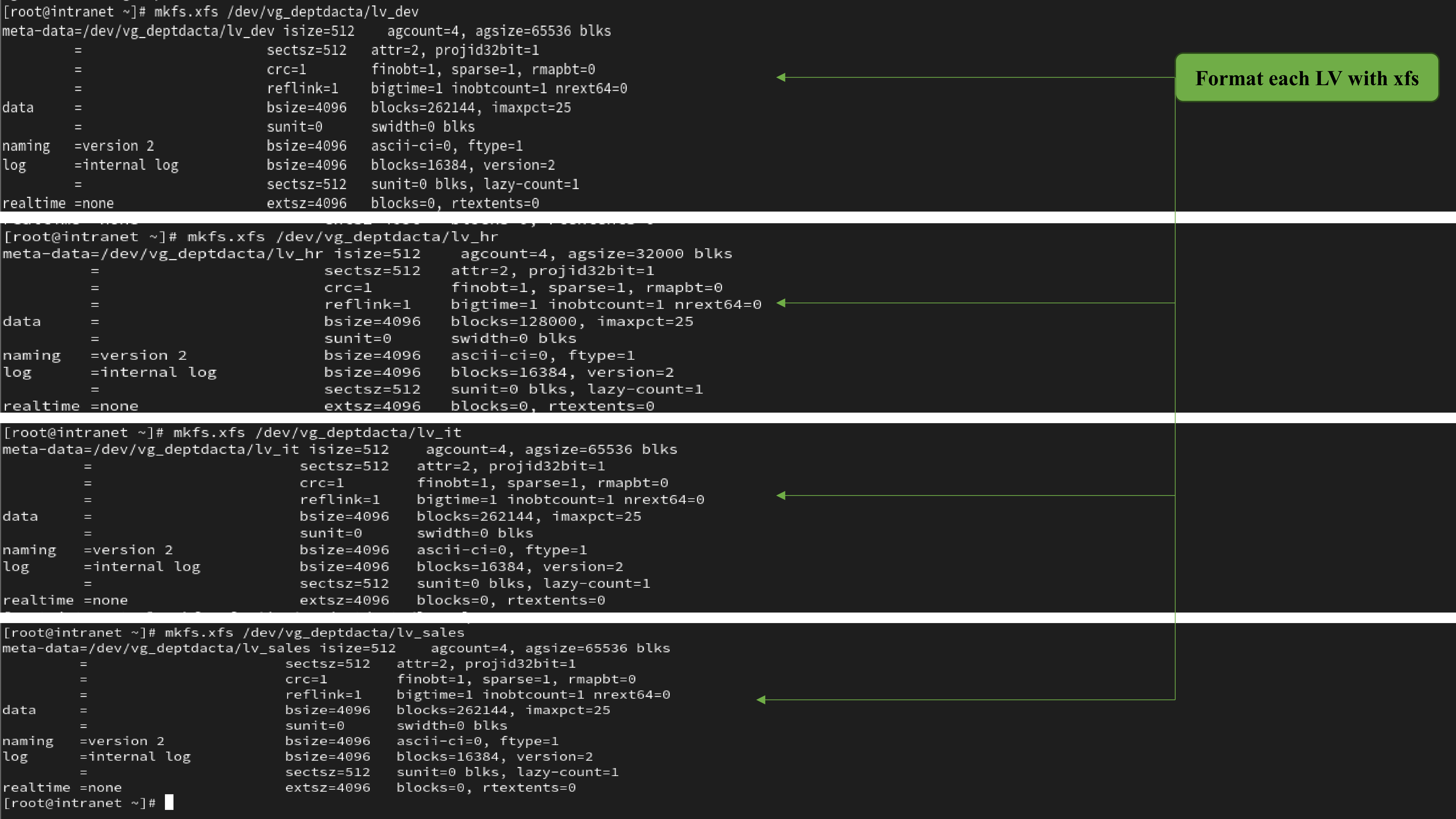
Create a Volume Group: vg_deptdata



```
[root@intranet ~]# lvcreate -n lv_dev -L 1G vg_deptdacta
  Logical volume "lv_dev" created.
[root@intranet ~]# lvcreate -n lv_hr -L 500M vg_deptdacta
  Logical volume "lv_hr" created.
[root@intranet ~]# lvcreate -n lv_it -L 1G vg_deptdacta
  Logical volume "lv_it" created.
[root@intranet ~]# lvcreate -n lv_sales -L 1G vg_deptdacta
  Logical volume "lv_sales" created.
[root@intranet ~]# lvdisplay
  --- Logical volume ---
  LV Path                /dev/vg_deptdacta/lv_dev
  LV Name                lv_dev
  VG Name                vg_deptdacta
  LV UUID                Jn2yLA-QxQo-prL2-Z1AS-3Mc5-lOJ5-FqjPT2
  LV Write Access        read/write
  LV Creation host, time intranet.technova.local, 2025-05-12 21:25:41 +0300
  LV Status              available
  # open                 0
  LV Size                1.00 GiB
  Current LE             256
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           253:0

  --- Logical volume ---
  LV Path                /dev/vg_deptdacta/lv_hr
  LV Name                lv_hr
  VG Name                vg_deptdacta
  LV UUID                S1G03o-4F9n-zFjr-eW8W-ff0C-5Vwe-241SNH
  LV Write Access        read/write
  LV Creation host, time intranet.technova.local, 2025-05-12 21:26:10 +0300
  LV Status              available
  # open                 0
  LV Size                500.00 MiB
  Current LE             125
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           253:1
```

Create Logical Volumes:
1- lv_dev (1G), mount to /srv/dev
2- lv_hr (500M), mount to /srv/hr
3- lv_it (1G), mount to /srv/it
4- lv_sales (1G), mount to /srv/sales

Verify



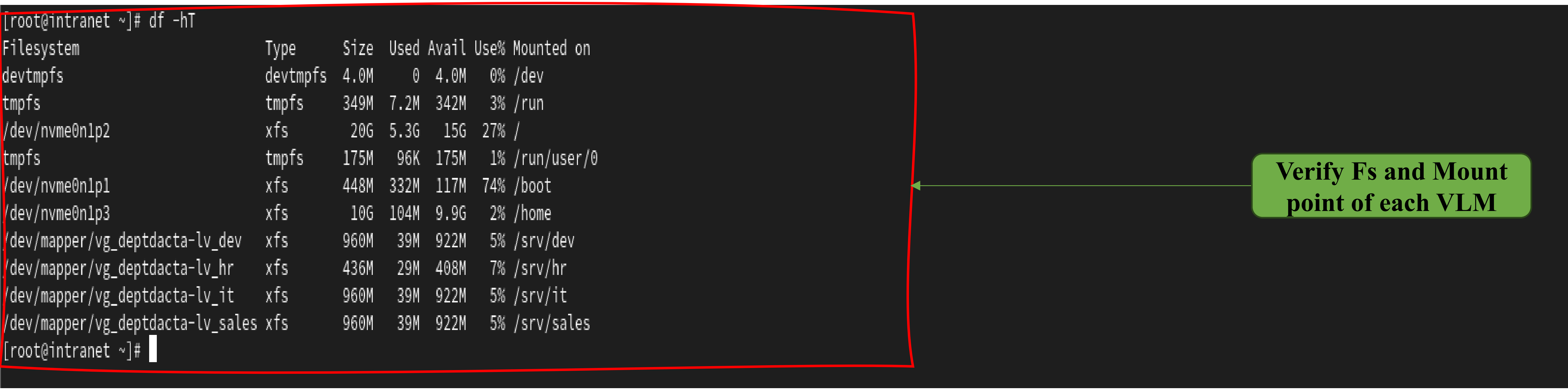
```
[root@intranet ~]# mkfs.xfs /dev/vg_deptdacta/lv_dev
meta-data=/dev/vg_deptdacta/lv_dev isize=512    agcount=4, agsize=65536 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=1 inobtcount=1 nrext64=0
data     =                       bsize=4096   blocks=262144, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=16384, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

```
[root@intranet ~]# mkfs.xfs /dev/vg_deptdacta/lv_hr
meta-data=/dev/vg_deptdacta/lv_hr isize=512    agcount=4, agsize=32000 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=1 inobtcount=1 nrext64=0
data     =                       bsize=4096   blocks=128000, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=16384, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

```
[root@intranet ~]# mkfs.xfs /dev/vg_deptdacta/lv_it
meta-data=/dev/vg_deptdacta/lv_it isize=512    agcount=4, agsize=65536 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=1 inobtcount=1 nrext64=0
data     =                       bsize=4096   blocks=262144, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=16384, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

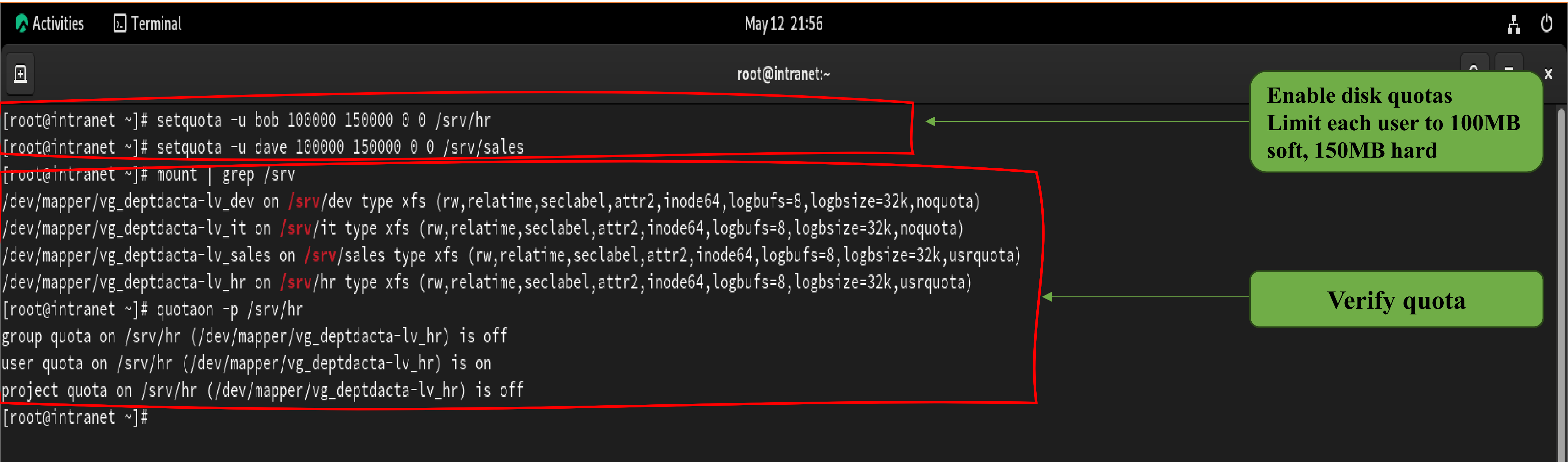
```
[root@intranet ~]# mkfs.xfs /dev/vg_deptdacta/lv_sales
meta-data=/dev/vg_deptdacta/lv_sales isize=512    agcount=4, agsize=65536 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=1 inobtcount=1 nrext64=0
data     =                       bsize=4096   blocks=262144, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=16384, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
[root@intranet ~]#
```

Format each LV with xfs



```
[root@intranet ~]# df -hT
Filesystem                      Type      Size  Used Avail Use% Mounted on
devtmpfs                        devtmpfs  4.0M     0  4.0M   0% /dev
tmpfs                           tmpfs     349M  7.2M  342M   3% /run
/dev/nvme0n1p2                  xfs        20G  5.3G   15G  27% /
tmpfs                           tmpfs     175M   96K  175M   1% /run/user/0
/dev/nvme0n1p1                  xfs       448M  332M  117M  74% /boot
/dev/nvme0n1p3                  xfs        10G  104M  9.9G   2% /home
/dev/mapper/vg_deptdacta-lv_dev xfs       960M   39M  922M   5% /srv/dev
/dev/mapper/vg_deptdacta-lv_hr  xfs       436M   29M  408M   7% /srv/hr
/dev/mapper/vg_deptdacta-lv_it  xfs       960M   39M  922M   5% /srv/it
/dev/mapper/vg_deptdacta-lv_sales xfs     960M   39M  922M   5% /srv/sales
[root@intranet ~]#
```

Verify Fs and Mount point of each VLM



```
[root@intranet ~]# setquota -u bob 100000 150000 0 0 /srv/hr
[root@intranet ~]# setquota -u dave 100000 150000 0 0 /srv/sales
[root@intranet ~]# mount | grep /srv
/dev/mapper/vg_deptdacta-lv_dev on /srv/dev type xfs (rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota)
/dev/mapper/vg_deptdacta-lv_it on /srv/it type xfs (rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota)
/dev/mapper/vg_deptdacta-lv_sales on /srv/sales type xfs (rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,usrquota)
/dev/mapper/vg_deptdacta-lv_hr on /srv/hr type xfs (rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,usrquota)
[root@intranet ~]# quotaon -p /srv/hr
group quota on /srv/hr (/dev/mapper/vg_deptdacta-lv_hr) is off
user quota on /srv/hr (/dev/mapper/vg_deptdacta-lv_hr) is on
project quota on /srv/hr (/dev/mapper/vg_deptdacta-lv_hr) is off
[root@intranet ~]#
```

Enable disk quotas
Limit each user to 100MB soft, 150MB hard

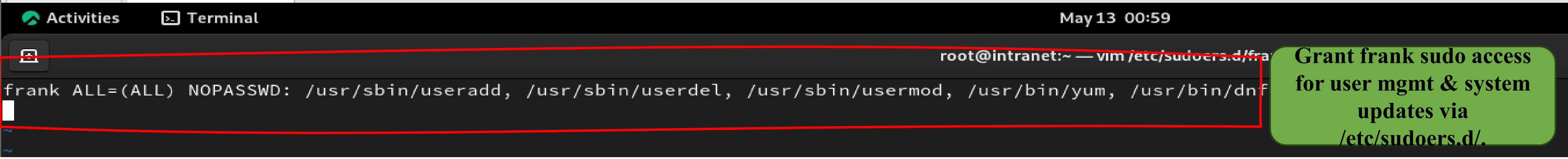
Verify quota

Phase 4: Security Hardening

- **Objective:** Secure the server and control access.

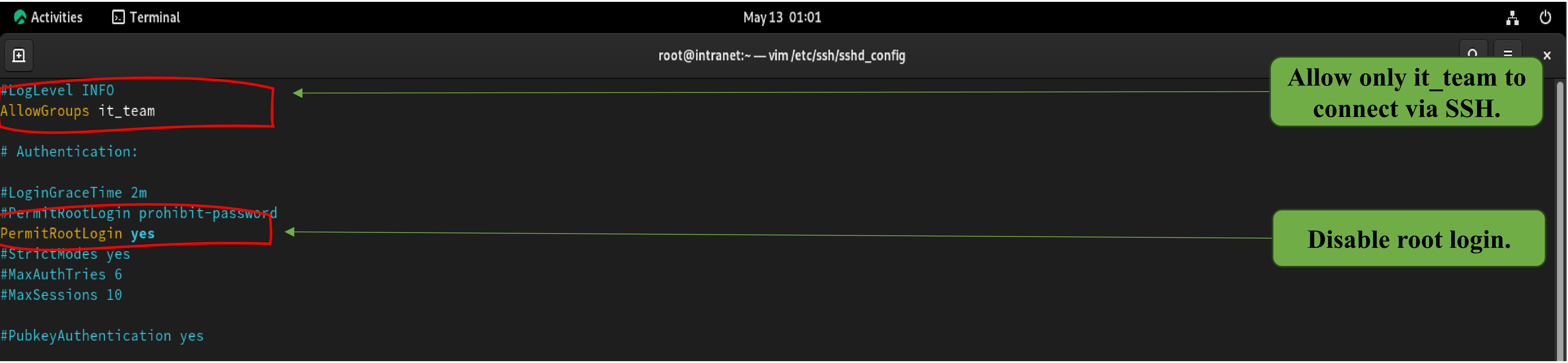
  Tasks:

  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)



```
frank ALL=(ALL) NOPASSWD: /usr/sbin/useradd, /usr/sbin/userdel, /usr/sbin/usermod, /usr/bin/yum, /usr/bin/dnf
~
~
```

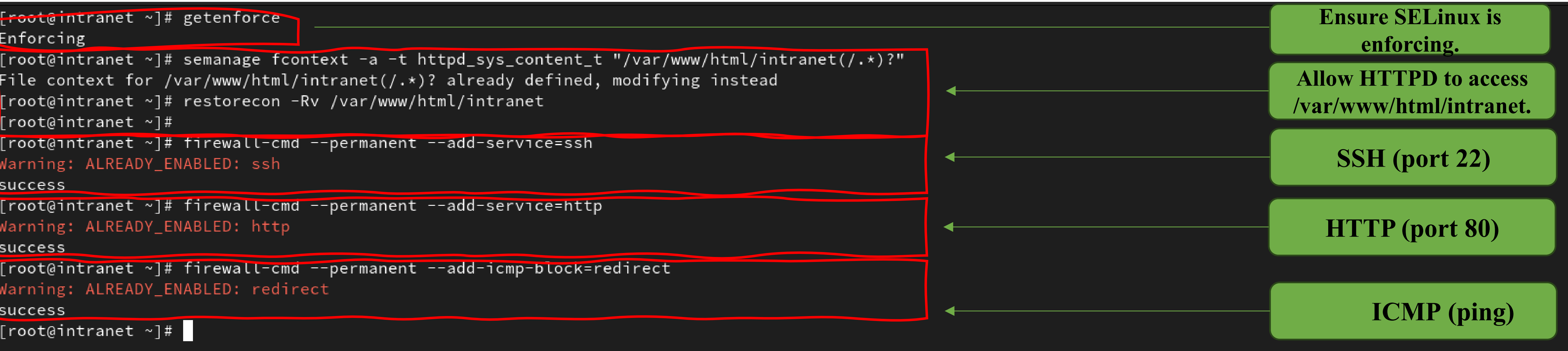
Grant frank sudo access for user mgmt & system updates via /etc/sudoers.d/.



```
#LogLevel INFO
AllowGroups it_team

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes
```

Allow only it_team to connect via SSH.

Disable root login.



```
[root@intranet ~]# getenforce
Enforcing
[root@intranet ~]# semanage fcontext -a -t httpd_sys_content_t "/var/www/html/intranet(/.*)?"
File context for /var/www/html/intranet(/.*)? already defined, modifying instead
[root@intranet ~]# restorecon -Rv /var/www/html/intranet
[root@intranet ~]#
[root@intranet ~]# firewall-cmd --permanent --add-service=ssh
Warning: ALREADY_ENABLED: ssh
success
[root@intranet ~]# firewall-cmd --permanent --add-service=http
Warning: ALREADY_ENABLED: http
success
[root@intranet ~]# firewall-cmd --permanent --add-icmp-block=redirect
Warning: ALREADY_ENABLED: redirect
success
[root@intranet ~]#
```

Ensure SELinux is enforcing.

Allow HTTPD to access /var/www/html/intranet.

SSH (port 22)

HTTP (port 80)

ICMP (ping)

Phase 5: Internal Web Portal

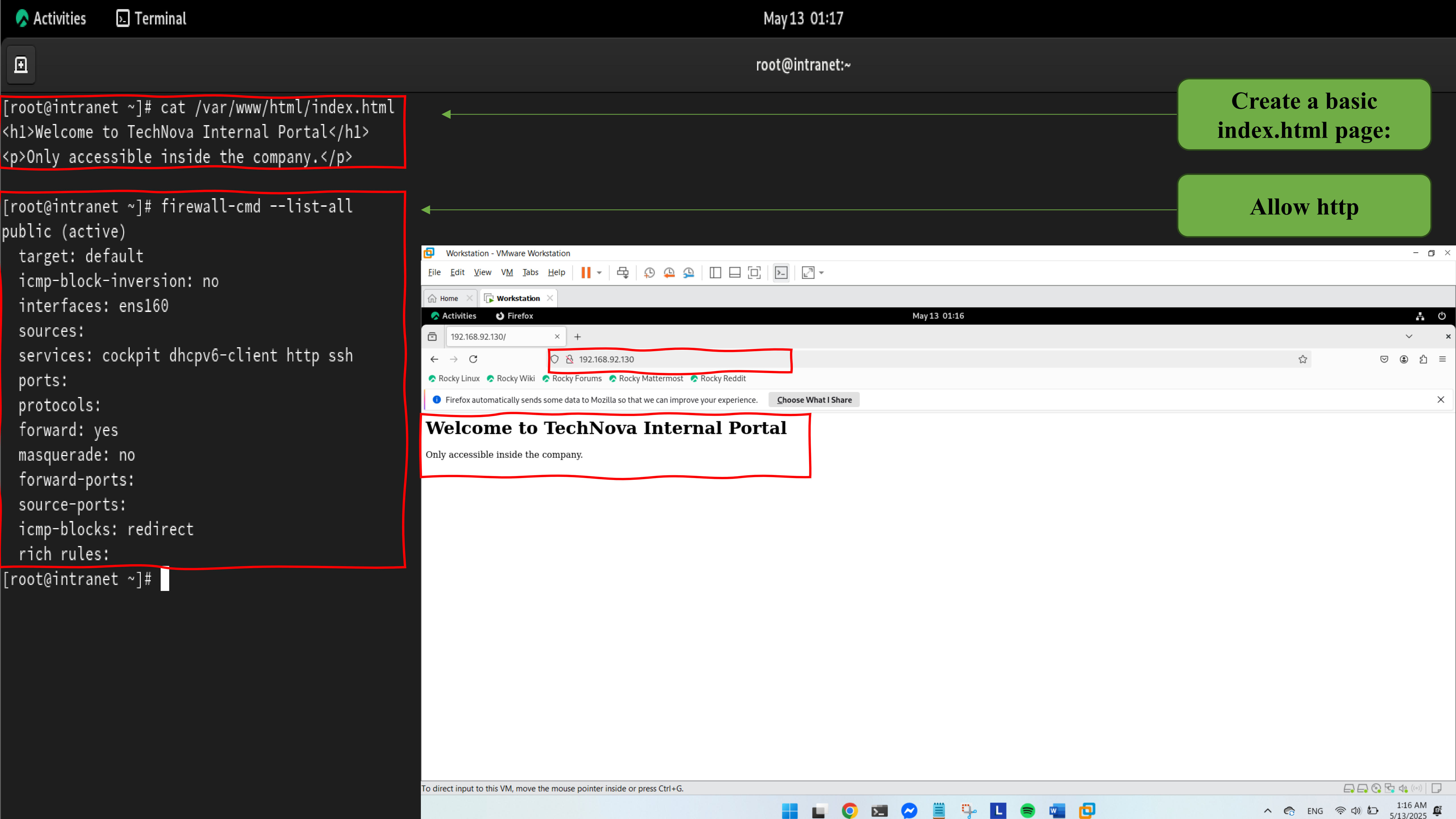
- **Objective:** Host a simple internal company web page.

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`.



Create a basic index.html page:

```
[root@intranet ~]# cat /var/www/html/index.html
<h1>Welcome to TechNova Internal Portal</h1>
<p>Only accessible inside the company.</p>
```

Allow http

```
[root@intranet ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client http ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks: redirect
  rich rules:
[root@intranet ~]#
```

Firefox automatically sends some data to Mozilla so that we can improve your experience.

Welcome to TechNova Internal Portal

Only accessible inside the company.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

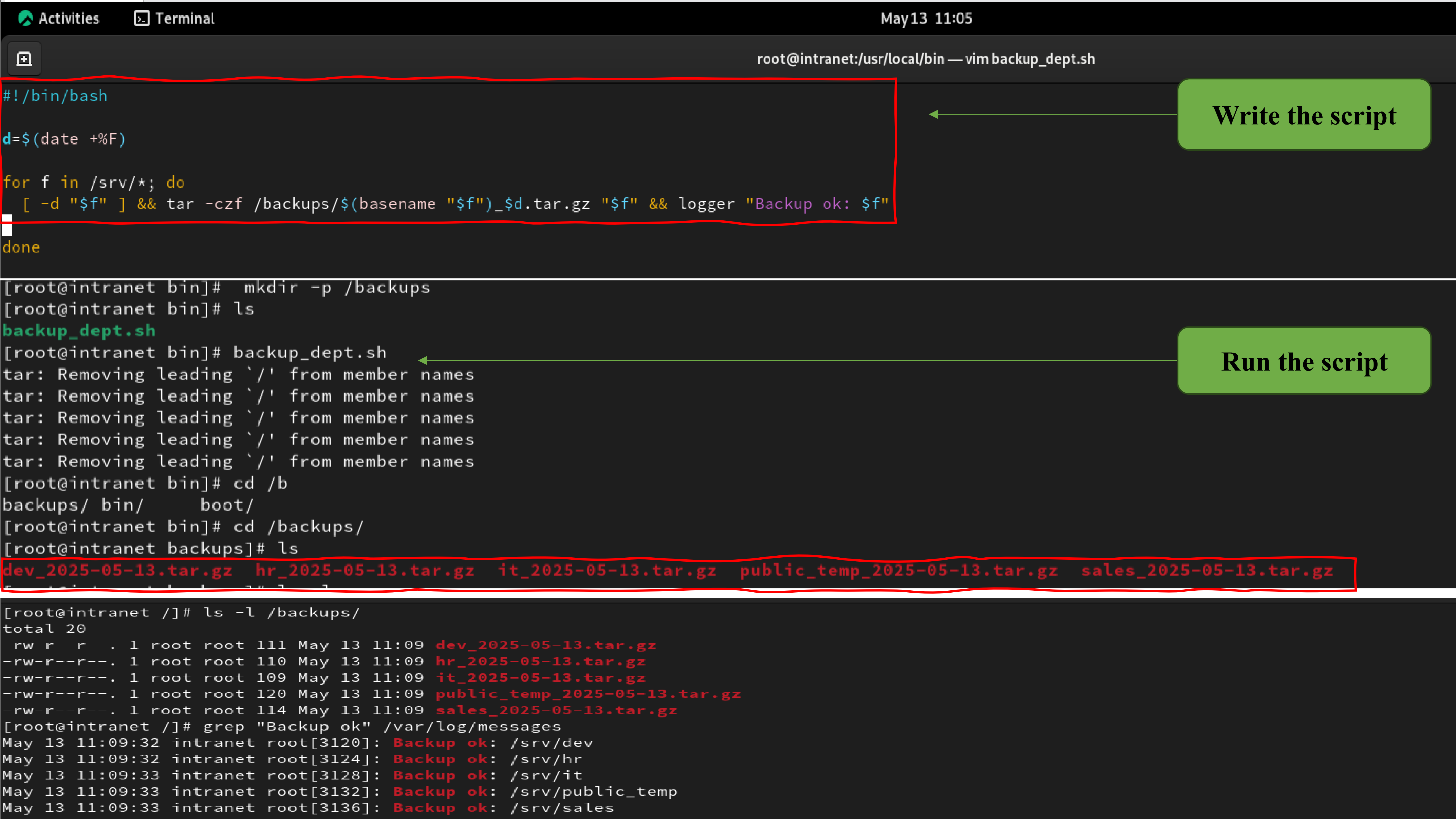
Phase 6: Automation & Scripting

- **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!"



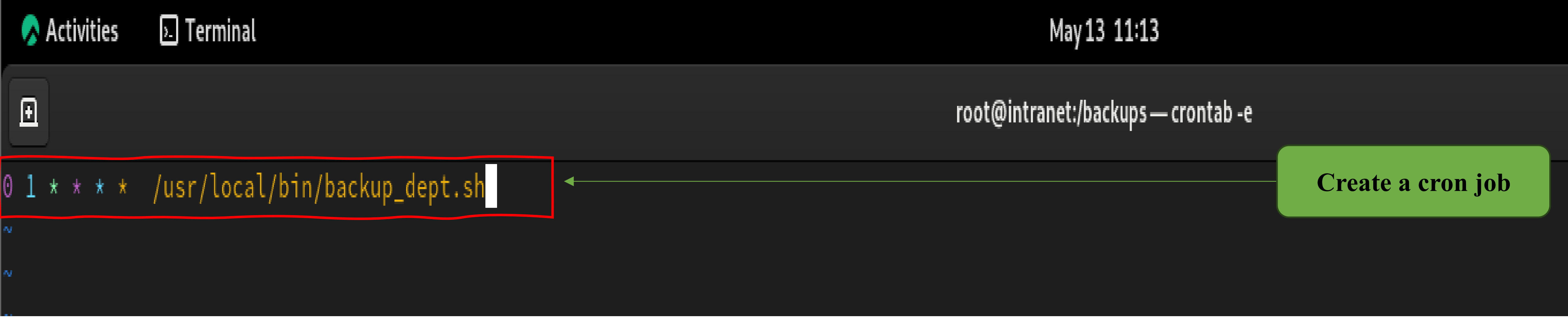
Write the script

```
#!/bin/bash

d=$(date +%F)

for f in /srv/*; do
  [ -d "$f" ] && tar -czf /backups/$(basename "$f")_$d.tar.gz "$f" && logger "Backup ok: $f"

done
```

Run the script

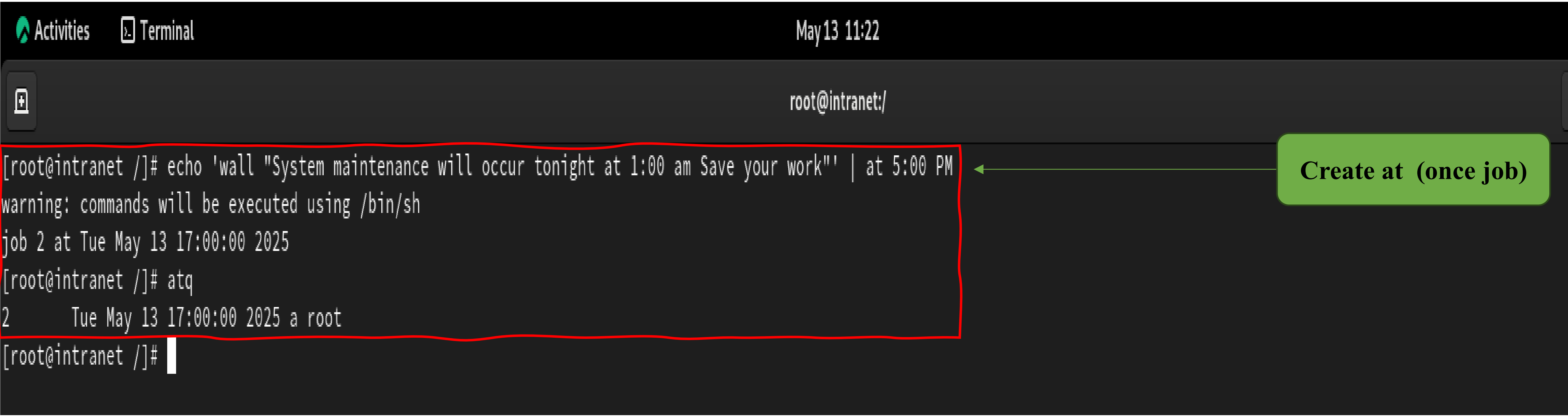
```
[root@intranet bin]#  mkdir -p /backups
[root@intranet bin]# ls
backup_dept.sh
[root@intranet bin]# backup_dept.sh
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
[root@intranet bin]# cd /b
backups/ bin/     boot/
[root@intranet bin]# cd /backups/
[root@intranet backups]# ls
dev_2025-05-13.tar.gz  hr_2025-05-13.tar.gz  it_2025-05-13.tar.gz  public_temp_2025-05-13.tar.gz  sales_2025-05-13.tar.gz
```

```
[root@intranet /]# ls -l /backups/
total 20
-rw-r--r--. 1 root root 111 May 13 11:09 dev_2025-05-13.tar.gz
-rw-r--r--. 1 root root 110 May 13 11:09 hr_2025-05-13.tar.gz
-rw-r--r--. 1 root root 109 May 13 11:09 it_2025-05-13.tar.gz
-rw-r--r--. 1 root root 120 May 13 11:09 public_temp_2025-05-13.tar.gz
-rw-r--r--. 1 root root 114 May 13 11:09 sales_2025-05-13.tar.gz
[root@intranet /]# grep "Backup ok" /var/log/messages
May 13 11:09:32 intranet root[3120]: Backup ok: /srv/dev
May 13 11:09:32 intranet root[3124]: Backup ok: /srv/hr
May 13 11:09:33 intranet root[3128]: Backup ok: /srv/it
May 13 11:09:33 intranet root[3132]: Backup ok: /srv/public_temp
May 13 11:09:33 intranet root[3136]: Backup ok: /srv/sales
```



```
0 1 * * * *  /usr/local/bin/backup_dept.sh
~
~
```

Create a cron job



```
[root@intranet /]# echo 'wall "System maintenance will occur tonight at 1:00 am Save your work"' | at 5:00 PM
warning: commands will be executed using /bin/sh
job 2 at Tue May 13 17:00:00 2025
[root@intranet /]# atq
2       Tue May 13 17:00:00 2025 a root
[root@intranet /]# 
```

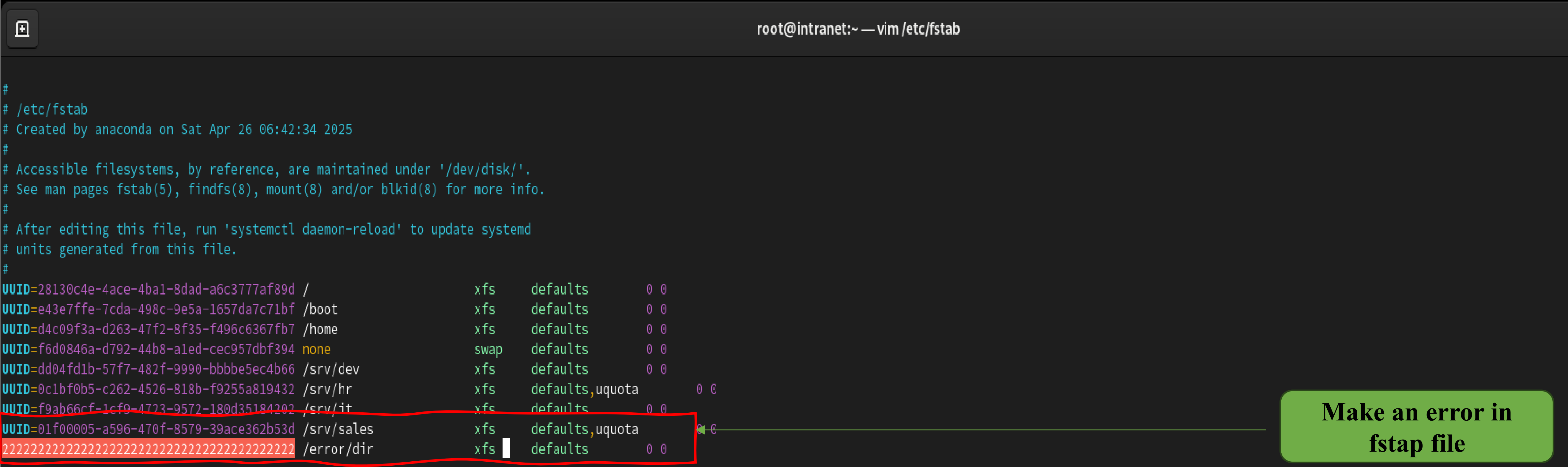
Create at (once job)

Phase 7: Troubleshooting & Logs

- **Objective:** Practice system recovery and log monitoring.

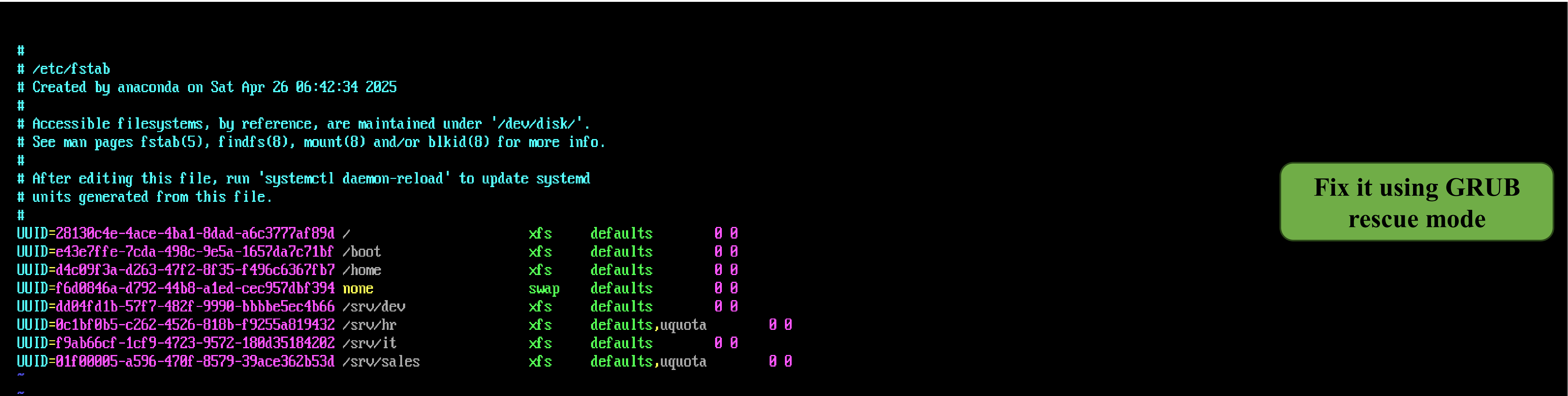
Tasks:

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.



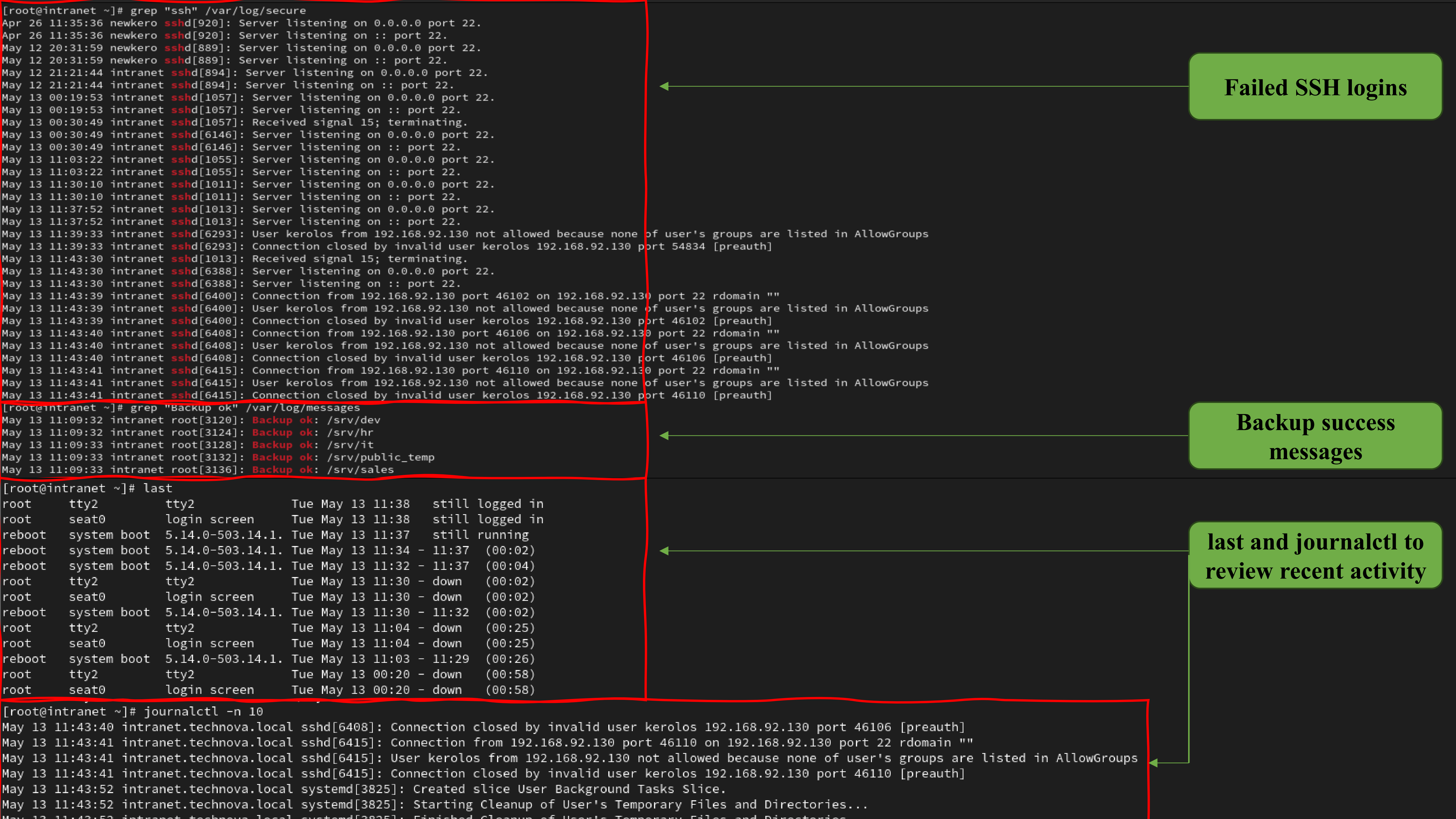
```
#
# /etc/fstab
# Created by anaconda on Sat Apr 26 06:42:34 2025
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
UUID=28130c4e-4ace-4ba1-8dad-a6c3777af89d /                       xfs     defaults        0 0
UUID=e43e7ffe-7cda-498c-9e5a-1657da7c71bf /boot                   xfs     defaults        0 0
UUID=d4c09f3a-d263-47f2-8f35-f496c6367fb7 /home                   xfs     defaults        0 0
UUID=f6d0846a-d792-44b8-a1ed-cec957dbf394 none                    swap    defaults        0 0
UUID=dd04fd1b-57f7-482f-9990-bbbbe5ec4b66 /srv/dev                xfs     defaults        0 0
UUID=0c1bf0b5-c262-4526-818b-f9255a819432 /srv/hr                 xfs     defaults,uquota        0 0
UUID=f9ab66cf-1cf9-4723-9572-180d35184202 /srv/it                 xfs     defaults        0 0
UUID=01f00005-a596-470f-8579-39ace362b53d /srv/sales              xfs     defaults,uquota        0 0
22222222222222222222222222222222222222222 /error/dir              xfs     defaults        0 0
```

Make an error in fstap file



```
#
# /etc/fstab
# Created by anaconda on Sat Apr 26 06:42:34 2025
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
UUID=28130c4e-4ace-4ba1-8dad-a6c3777af89d /                       xfs     defaults        0 0
UUID=e43e7ffe-7cda-498c-9e5a-1657da7c71bf /boot                   xfs     defaults        0 0
UUID=d4c09f3a-d263-47f2-8f35-f496c6367fb7 /home                   xfs     defaults        0 0
UUID=f6d0846a-d792-44b8-a1ed-cec957dbf394 none                    swap    defaults        0 0
UUID=dd04fd1b-57f7-482f-9990-bbbbe5ec4b66 /srv/dev                xfs     defaults        0 0
UUID=0c1bf0b5-c262-4526-818b-f9255a819432 /srv/hr                 xfs     defaults,uquota        0 0
UUID=f9ab66cf-1cf9-4723-9572-180d35184202 /srv/it                 xfs     defaults        0 0
UUID=01f00005-a596-470f-8579-39ace362b53d /srv/sales              xfs     defaults,uquota        0 0
~
~
```

Fix it using GRUB rescue mode



Failed SSH logins

```
[root@intranet ~]# grep "ssh" /var/log/secure
Apr 26 11:35:36 newkero sshd[920]: Server listening on 0.0.0.0 port 22.
Apr 26 11:35:36 newkero sshd[920]: Server listening on :: port 22.
May 12 20:31:59 newkero sshd[889]: Server listening on 0.0.0.0 port 22.
May 12 20:31:59 newkero sshd[889]: Server listening on :: port 22.
May 12 21:21:44 intranet sshd[894]: Server listening on 0.0.0.0 port 22.
May 12 21:21:44 intranet sshd[894]: Server listening on :: port 22.
May 13 00:19:53 intranet sshd[1057]: Server listening on 0.0.0.0 port 22.
May 13 00:19:53 intranet sshd[1057]: Server listening on :: port 22.
May 13 00:30:49 intranet sshd[1057]: Received signal 15; terminating.
May 13 00:30:49 intranet sshd[6146]: Server listening on 0.0.0.0 port 22.
May 13 00:30:49 intranet sshd[6146]: Server listening on :: port 22.
May 13 11:03:22 intranet sshd[1055]: Server listening on 0.0.0.0 port 22.
May 13 11:03:22 intranet sshd[1055]: Server listening on :: port 22.
May 13 11:30:10 intranet sshd[1011]: Server listening on 0.0.0.0 port 22.
May 13 11:30:10 intranet sshd[1011]: Server listening on :: port 22.
May 13 11:37:52 intranet sshd[1013]: Server listening on 0.0.0.0 port 22.
May 13 11:37:52 intranet sshd[1013]: Server listening on :: port 22.
May 13 11:39:33 intranet sshd[6293]: User kerolos from 192.168.92.130 not allowed because none of user's groups are listed in AllowGroups
May 13 11:39:33 intranet sshd[6293]: Connection closed by invalid user kerolos 192.168.92.130 port 54834 [preauth]
May 13 11:43:30 intranet sshd[1013]: Received signal 15; terminating.
May 13 11:43:30 intranet sshd[6388]: Server listening on 0.0.0.0 port 22.
May 13 11:43:30 intranet sshd[6388]: Server listening on :: port 22.
May 13 11:43:39 intranet sshd[6400]: Connection from 192.168.92.130 port 46102 on 192.168.92.130 port 22 rdomain ""
May 13 11:43:39 intranet sshd[6400]: User kerolos from 192.168.92.130 not allowed because none of user's groups are listed in AllowGroups
May 13 11:43:39 intranet sshd[6400]: Connection closed by invalid user kerolos 192.168.92.130 port 46102 [preauth]
May 13 11:43:40 intranet sshd[6408]: Connection from 192.168.92.130 port 46106 on 192.168.92.130 port 22 rdomain ""
May 13 11:43:40 intranet sshd[6408]: User kerolos from 192.168.92.130 not allowed because none of user's groups are listed in AllowGroups
May 13 11:43:40 intranet sshd[6408]: Connection closed by invalid user kerolos 192.168.92.130 port 46106 [preauth]
May 13 11:43:41 intranet sshd[6415]: Connection from 192.168.92.130 port 46110 on 192.168.92.130 port 22 rdomain ""
May 13 11:43:41 intranet sshd[6415]: User kerolos from 192.168.92.130 not allowed because none of user's groups are listed in AllowGroups
May 13 11:43:41 intranet sshd[6415]: Connection closed by invalid user kerolos 192.168.92.130 port 46110 [preauth]
```

Backup success messages

```
[root@intranet ~]# grep "Backup ok" /var/log/messages
May 13 11:09:32 intranet root[3120]: Backup ok: /srv/dev
May 13 11:09:32 intranet root[3124]: Backup ok: /srv/hr
May 13 11:09:33 intranet root[3128]: Backup ok: /srv/it
May 13 11:09:33 intranet root[3132]: Backup ok: /srv/public_temp
May 13 11:09:33 intranet root[3136]: Backup ok: /srv/sales
```

last and journalctl to review recent activity

```
[root@intranet ~]# last
root     tty2         tty2             Tue May 13 11:38   still logged in
root     seat0        login screen     Tue May 13 11:38   still logged in
reboot   system boot  5.14.0-503.14.1. Tue May 13 11:37   still running
reboot   system boot  5.14.0-503.14.1. Tue May 13 11:34 - 11:37  (00:02)
reboot   system boot  5.14.0-503.14.1. Tue May 13 11:32 - 11:37  (00:04)
root     tty2         tty2             Tue May 13 11:30 - down   (00:02)
root     seat0        login screen     Tue May 13 11:30 - down   (00:02)
reboot   system boot  5.14.0-503.14.1. Tue May 13 11:30 - 11:32  (00:02)
root     tty2         tty2             Tue May 13 11:04 - down   (00:25)
root     seat0        login screen     Tue May 13 11:04 - down   (00:25)
reboot   system boot  5.14.0-503.14.1. Tue May 13 11:03 - 11:29  (00:26)
root     tty2         tty2             Tue May 13 00:20 - down   (00:58)
root     seat0        login screen     Tue May 13 00:20 - down   (00:58)
```

```
[root@intranet ~]# journalctl -n 10
May 13 11:43:40 intranet.technova.local sshd[6408]: Connection closed by invalid user kerolos 192.168.92.130 port 46106 [preauth]
May 13 11:43:41 intranet.technova.local sshd[6415]: Connection from 192.168.92.130 port 46110 on 192.168.92.130 port 22 rdomain ""
May 13 11:43:41 intranet.technova.local sshd[6415]: User kerolos from 192.168.92.130 not allowed because none of user's groups are listed in AllowGroups
May 13 11:43:41 intranet.technova.local sshd[6415]: Connection closed by invalid user kerolos 192.168.92.130 port 46110 [preauth]
May 13 11:43:52 intranet.technova.local systemd[3825]: Created slice User Background Tasks Slice.
May 13 11:43:52 intranet.technova.local systemd[3825]: Starting Cleanup of User's Temporary Files and Directories...
May 13 11:43:52 intranet.technova.local systemd[3825]: Finished Cleanup of User's Temporary Files and Directories.
```

Thank you for reviewing this project.