Part A: User Creation and Management

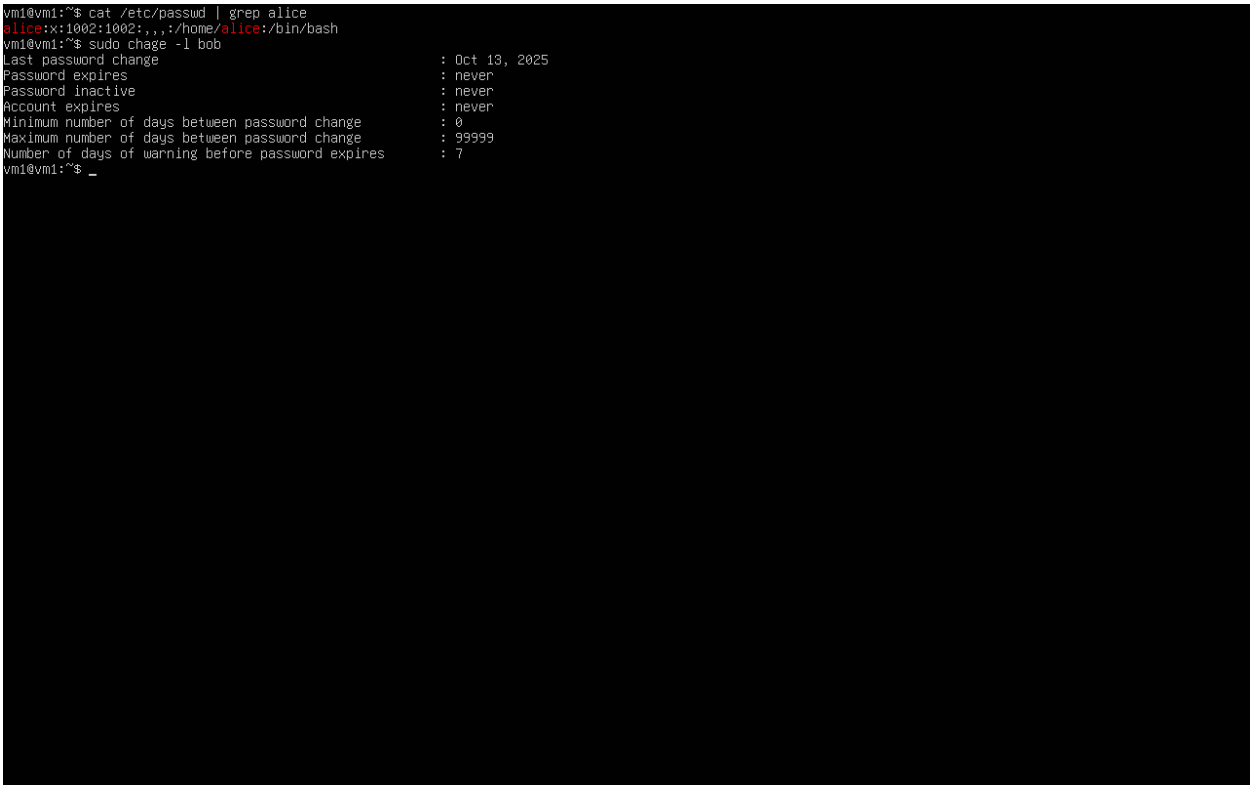
1. **Create three new users** using adduser command:
    - alice (interactive creation with full prompts)
    - bob (with custom home directory /opt/users/bob)
    - charlie (system user for services)
2. **Set passwords** for alice and bob:
    - Use passwd command
    - Force alice to change password at next login
3. **View user information**:
    - Display alice's entry from /etc/passwd
    - Show bob's password aging information using chage -l bob

```
vm1@vm1:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:992:992:systemd Resolver:/:/usr/sbin/nologin
pollinate:x:102:1::/var/cache/pollinate:/bin/false
polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin
syslog:x:103:104::/nonexistent:/usr/sbin/nologin
uuidd:x:104:105::/run/uuidd:/usr/sbin/nologin
tcpdump:x:105:107::/nonexistent:/usr/sbin/nologin
tss:x:106:108:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:107:109::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
vm1:x:1000:1000:Mina:/home/vm1:/bin/bash
lxd:x:999:101::/var/snap/lxd/common/lxd:/bin/false
alice:x:1002:1002:,,,:/home/alice:/bin/bash
bob:x:1003:1003::/opt/users/bob:/bin/sh
charlie:x:996:988::/home/charlie:/bin/sh
vm1@vm1:~$
```

```
vm1@vm1:~$ sudo adduser alice
info: Adding user `alice' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `alice' (1002) ...
info: Adding new user `alice' (1002) with group `alice (1002)' ...
warn: The home directory `/home/alice' already exists.  Not touching this directory.
New password:
Retype new password:
No password has been supplied.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for alice
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `alice' to supplemental / extra groups `users' ...
info: Adding user `alice' to group `users' ...
vm1@vm1:~$
```

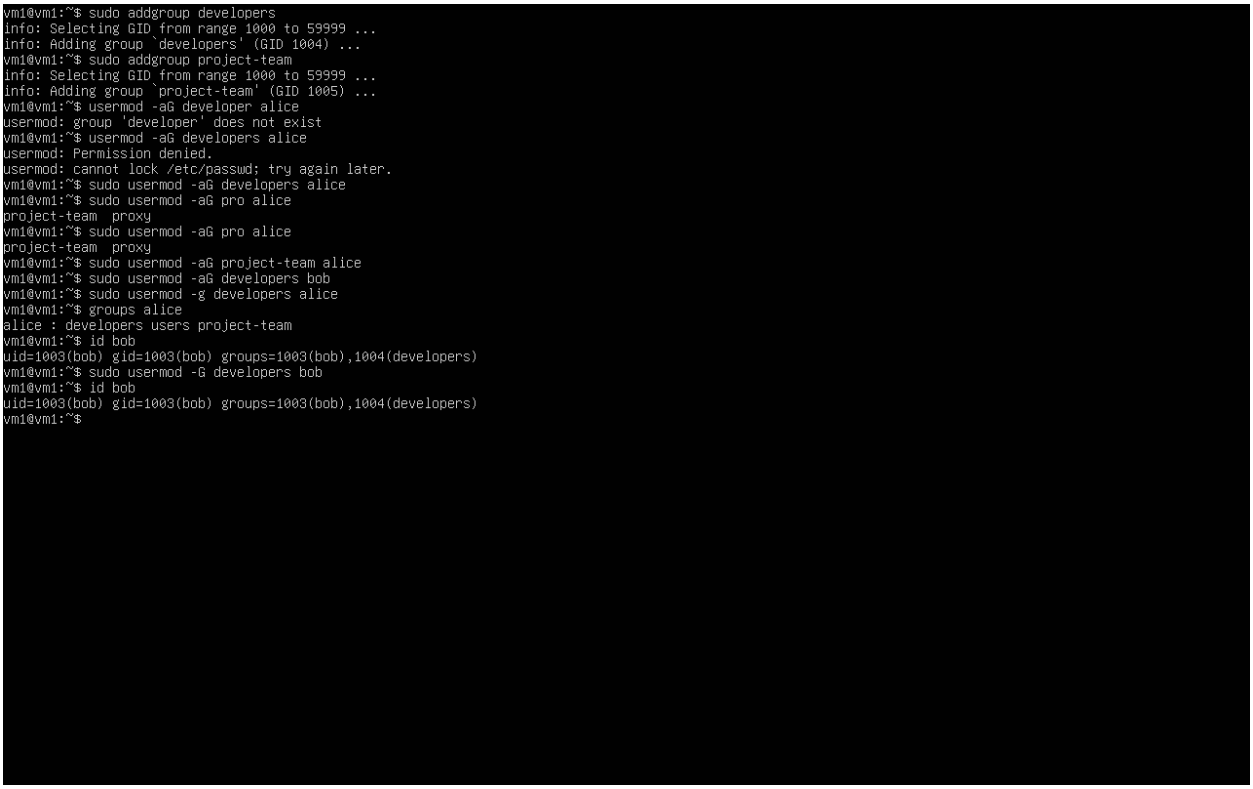
```
vm1@vm1:~$ sudo adduser alice
info: Adding user `alice' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `alice' (1002) ...
info: Adding new user `alice' (1002) with group `alice (1002)' ...
warn: The home directory `/home/alice' already exists.  Not touching this directory.
New password:
Retype new password:
No password has been supplied.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for alice
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `alice' to supplemental / extra groups `users' ...
info: Adding user `alice' to group `users' ...
vm1@vm1:~$ sudo useradd bob --home /opt/users/bob
vm1@vm1:~$ sudo useradd --system charlie
vm1@vm1:~$ _
```

```
vm1@vm1:~$ sudo passwd alice
New password:
Retype new password:
passwd: password updated successfully
vm1@vm1:~$ sudo passwd bob
New password:
Retype new password:
passwd: password updated successfully
vm1@vm1:~$ sudo passwd -e alice
passwd: password changed.
vm1@vm1:~$ su alice
Password:
You are required to change your password immediately (administrator enforced).
Changing password for alice.
Current password:
New password:
Retype new password:
The password has not been changed.
New password:
Retype new password:
You must choose a longer password.
New password:
Retype new password:
alice@vm1:/home/vm1$ _
```



Part B: Group Management

4. **Create two groups**:
    - developers (regular group)
    - project-team (using addgroup command)
5. **Add users to groups**:
    - Add alice to both developers and project-team
    - Add bob to developers only
    - Make developers alice's primary group
6. **Verify group memberships**:
    - Use groups command to show alice's groups
    - Use id command to display bob's UID and GID information



Part C: File Permissions and Ownership (25 points)

7. **Create test files and directories**:
    - Create directory /tmp/lab1_test
    - Create file /tmp/lab1_test/data.txt with some content
    - Create file /tmp/lab1_test/script.sh
8. **Set permissions using symbolic notation**:
    - Set data.txt permissions to rw-r--r-- (owner: read/write, group: read, others: read)
    - Set script.sh permissions to rwxr-xr-x (owner: full access, group/others: read/execute)
9. **Change ownership**:
    - Change owner of data.txt to alice and group to developers
    - Change owner of entire /tmp/lab1_test directory to bob and group to project-team (recursive)

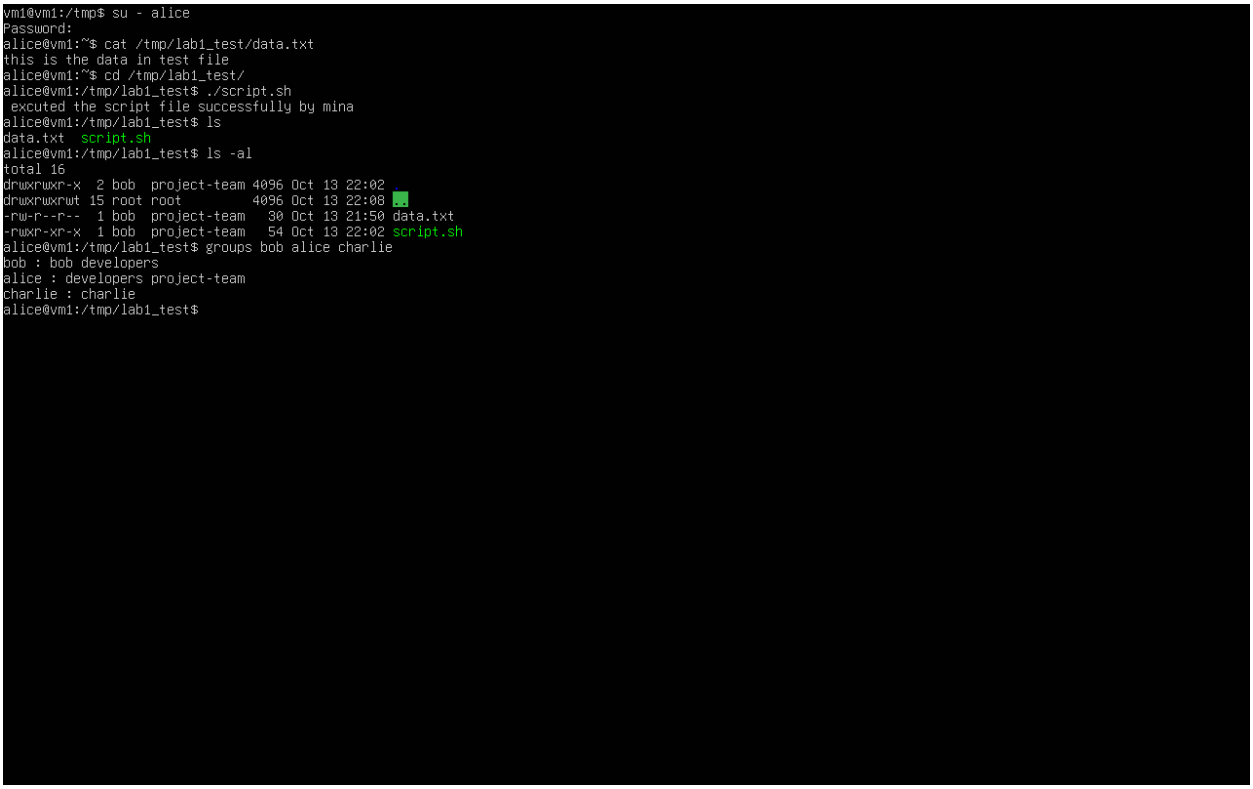
```
vm1@vm1:/tmp$ sudo chown -R bob:project-team lab1_test/
vm1@vm1:/tmp$ ls lab1_test/
data.txt  script.sh
vm1@vm1:/tmp$ ll lab1_test/
total 12
drwxrwxr-x  2 bob  project-team 4096 Oct 13 21:50 ./
drwxrwxrwt 15 root root         4096 Oct 13 21:57 ../
-rw-r--r--  1 bob  project-team   30 Oct 13 21:50 data.txt
-rwxr-xr-x  1 bob  project-team    0 Oct 13 21:50 script.sh*
vm1@vm1:/tmp$
```

```
vm1@vm1:~$ mkdir /tmp/lab1_test
vm1@vm1:~$ cat > /tmp/lab1_test/data.txt
this is the data in test file
end the file now ^C
vm1@vm1:~$ touch /tmp/lab1_test/script.sh
vm1@vm1:~$ cd /tmp/lab1_test/
vm1@vm1:/tmp/lab1_test$ ll
total 12
drwxrwxr-x  2 vm1  vm1  4096 Oct 13 21:50 ./
drwxrwxrwt 15 root root 4096 Oct 13 21:51 ../
-rw-rw-r--  1 vm1  vm1    30 Oct 13 21:50 data.txt
-rw-rw-r--  1 vm1  vm1     0 Oct 13 21:50 script.sh
vm1@vm1:/tmp/lab1_test$ chmod g-w
chmod: missing operand after 'g-w'
Try 'chmod --help' for more information.
vm1@vm1:/tmp/lab1_test$ chmod g-w data.txt script.sh
vm1@vm1:/tmp/lab1_test$ chmod +x script.sh
vm1@vm1:/tmp/lab1_test$ ll
total 12
drwxrwxr-x  2 vm1  vm1  4096 Oct 13 21:50 ./
drwxrwxrwt 15 root root 4096 Oct 13 21:53 ../
-rw-r--r--  1 vm1  vm1    30 Oct 13 21:50 data.txt
-rwxr-xr-x  1 vm1  vm1     0 Oct 13 21:50 script.sh*
vm1@vm1:/tmp/lab1_test$ _
```

```
vm1@vm1:~$ cat > /tmp/lab1_test/data.txt
this is the data in test file
end the file now ^C
vm1@vm1:~$ touch /tmp/lab1_test/script.sh
vm1@vm1:~$ cd /tmp/lab1_test/
vm1@vm1:/tmp/lab1_test$ ll
total 12
drwxrwxr-x  2 vm1  vm1  4096 Oct 13 21:50 ./
drwxrwxrwt 15 root root 4096 Oct 13 21:51 ../
-rw-rw-r--  1 vm1  vm1    30 Oct 13 21:50 data.txt
-rw-rw-r--  1 vm1  vm1     0 Oct 13 21:50 script.sh
vm1@vm1:/tmp/lab1_test$ chmod g-w
chmod: missing operand after ‘g-w’
Try 'chmod --help' for more information.
vm1@vm1:/tmp/lab1_test$ chmod g-w data.txt script.sh
vm1@vm1:/tmp/lab1_test$ chmod +x script.sh
vm1@vm1:/tmp/lab1_test$ ll
total 12
drwxrwxr-x  2 vm1  vm1  4096 Oct 13 21:50 ./
drwxrwxrwt 15 root root 4096 Oct 13 21:53 ../
-rw-r--r--  1 vm1  vm1    30 Oct 13 21:50 data.txt
-rwxr-xr-x  1 vm1  vm1     0 Oct 13 21:50 script.sh*
vm1@vm1:/tmp/lab1_test$ chown alice:developers data.txt
chown: changing ownership of 'data.txt': Operation not permitted
vm1@vm1:/tmp/lab1_test$ sudo chown alice:developers data.txt
vm1@vm1:/tmp/lab1_test$ cd ..
vm1@vm1:/tmp$ ll
total 60
drwxrwxrwt 15 root root 4096 Oct 13 21:55 ./
drwxr-xr-x 23 root root 4096 Oct  7 15:42 ../
drwxrwxrwt  2 root root 4096 Oct 13 19:30 .ICE-unix/
drwxrwxrwt  2 root root 4096 Oct 13 19:30 .X11-unix/
drwxrwxrwt  2 root root 4096 Oct 13 19:30 .XIM-unix/
drwxrwxrwt  2 root root 4096 Oct 13 19:30 .font-unix/
drwxrwxr-x  2 vm1  vm1  4096 Oct 13 21:50 lab1_test/
drwx------  8 root root 4096 Oct 13 19:31 snap-private-tmp/
drwx------  3 root root 4096 Oct 13 19:31 systemd-private-6974cc4ce0e843abb7d5cb7013b44a5b-ModemManager.service-drjMYD/
drwx------  3 root root 4096 Oct 13 20:26 systemd-private-6974cc4ce0e843abb7d5cb7013b44a5b-fwupd.service-bufSNi/
drwx------  3 root root 4096 Oct 13 19:31 systemd-private-6974cc4ce0e843abb7d5cb7013b44a5b-polkit.service-ie25H3/
drwx------  3 root root 4096 Oct 13 19:54 systemd-private-6974cc4ce0e843abb7d5cb7013b44a5b-systemd-logind.service-kULk5h/
drwx------  3 root root 4096 Oct 13 19:54 systemd-private-6974cc4ce0e843abb7d5cb7013b44a5b-systemd-resolved.service-rrHM57/
drwx------  3 root root 4096 Oct 13 19:54 systemd-private-6974cc4ce0e843abb7d5cb7013b44a5b-systemd-timesyncd.service-O3BA9R/
drwx------  3 root root 4096 Oct 13 20:26 systemd-private-6974cc4ce0e843abb7d5cb7013b44a5b-upower.service-oy59bu/
vm1@vm1:/tmp$ ls -al lab1_test/
total 12
drwxrwxr-x  2 vm1   vm1        4096 Oct 13 21:50 .
drwxrwxrwt 15 root  root       4096 Oct 13 21:56 ..
-rw-r--r--  1 alice developers   30 Oct 13 21:50 data.txt
-rwxr-xr-x  1 vm1   vm1           0 Oct 13 21:50 script.sh
vm1@vm1:/tmp$
```

Part D: Verification and Testing

10. **Test permissions**:
    - Switch to alice user (su - alice)
    - Try to read data.txt
    - Try to execute script.sh
    - Document what works and what doesn't
11. **Display final state**:
    - Use ls -la /tmp/lab1_test to show all permissions and ownership
    - Show group memberships for all created users



Expected Commands to Use

- adduser
- passwd
- chage
- addgroup
- usermod
- groups
- id
- chmod
- chown
- chgrp
- ls -l
- su

Deliverables

1. Screenshot or copy of terminal output for each completed task
2. Brief explanation of any permission errors encountered
3. Final ls -la output of the test directory

Tasks

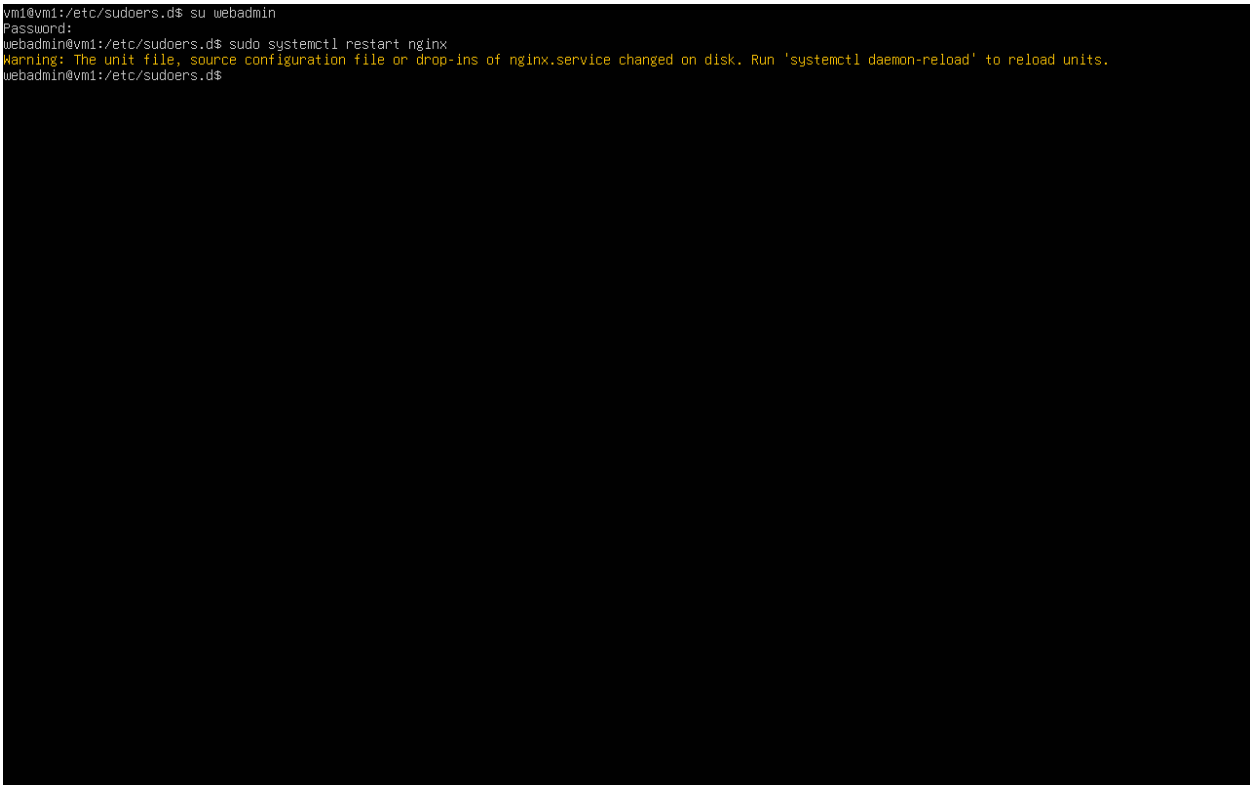
Part A: Basic Sudo Configuration (25 points)

1. **Set up sudo for web server management**:
    - Create user webadmin
    - Configure sudo to allow webadmin to restart nginx/apache without password
    - Test the configuration

```
vm1@vm1:/etc/sudoers.d$ sudo adduser webadmin
info: Adding user `webadmin' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `webadmin' (1008) ...
info: Adding new user `webadmin' (1008) with group `webadmin (1008)' ...
warn: The home directory `/home/webadmin' already exists.  Not touching this directory.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for webadmin
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `webadmin' to supplemental / extra groups `users' ...
info: Adding user `webadmin' to group `users' ...
vm1@vm1:/etc/sudoers.d$ ll
total 16
drwxr-xr-x   2 root root 4096 Oct 16 19:03 ./
drwxr-xr-x 115 root root 4096 Oct 16 19:03 ../
-r--r-----   1 root root 1068 Jan 29  2024 README
-rw-r-----   1 root root  122 Oct 15 18:26 mon
vm1@vm1:/etc/sudoers.d$ which systemctl
/usr/bin/systemctl
vm1@vm1:/etc/sudoers.d$ systemctl restart nginx
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'nginx.service'.
Multiple identities can be used for authentication:
 1.  Mina (vm1)
 2.  ,,, (mon)
Choose identity to authenticate as (1-2): 1
Password:
==== AUTHENTICATION COMPLETE ====
Warning: The unit file, source configuration file or drop-ins of nginx.service changed on disk. Run 'systemctl daemon-reload' to reload units.
vm1@vm1:/etc/sudoers.d$
```

```
Cmnd_Alias COMMAND = /usr/bin/systemctl restart nginx, /usr/bin/systemctl reload nginx ,/usr/bin/systemctl restart apache2 ,/usr/bin/systemctl reload apache2

webadmin ALL=(ALL) NOPASSWORD: COMMAND
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:wq_
```



2. **Create command aliases in sudoers**:
    - Create a WEB_CMDS alias for web server commands
    - Allow webadmin to use these commands
    - Use visudo safely to edit configuration

```
vm1@vm1:~$
vm1@vm1:~$ cd /etc/sudoers.d/
vm1@vm1:/etc/sudoers.d$ ll
total 24
drwxr-xr-x   2 root root 4096 Oct 16 21:24 ./
drwxr-xr-x 115 root root 4096 Oct 16 21:28 ../
-r--r-----   1 root root 1068 Jan 29  2024 README
-rw-r-----   1 root root  122 Oct 15 18:26 mon
-rw-r-----   1 root root  221 Oct 16 21:24 web_cmds
-rw-r-----   1 root root  196 Oct 16 20:03 webadmin
vm1@vm1:/etc/sudoers.d$ vim web_cmds
vm1@vm1:/etc/sudoers.d$ sudo visudo web_cmds
vm1@vm1:/etc/sudoers.d$ sudo visudo webadmin
visudo: webadmin.tmp unchanged
vm1@vm1:/etc/sudoers.d$ sudo visudo web_cmds
vm1@vm1:/etc/sudoers.d$ systemctl start nginx
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to start 'nginx.service'.
Authenticating as: Mina (vm1)
Password:
```

```
==== AUTHENTICATION COMPLETE ====
Warning: The unit file, source configuration file or drop-ins of nginx.service
changed on disk. Run 'systemctl daemon-reload' to reload units.
vm1@vm1:/etc/sudoers.d$ sudo systemctl start nginx
Warning: The unit file, source configuration file or drop-ins of nginx.service
changed on disk. Run 'systemctl daemon-reload' to reload units.
vm1@vm1:/etc/sudoers.d$ su - webadmin
Password:
webadmin@vm1:~$ sudo systemctl start nginx
Warning: The unit file, source configuration file or drop-ins of nginx.service
changed on disk. Run 'systemctl daemon-reload' to reload units.
webadmin@vm1:~$
```

Part B: Group-Based Sudo Permissions

3. **Configure sudo for developers group**:
    - Create group devops
    - Add alice and bob to devops group
    - Allow devops group to run docker and systemctl commands
    - Require password for these operations
4. **Test group permissions**:
    - Switch to alice and test docker commands
    - Switch to bob and test systemctl commands
    - Verify password prompts work correctly

```
 vm1@vm1:~$ sudo addgroup devops
info: Selecting GID from range 1000 to 59999 ...
info: Adding group `devops' (GID 1006) ...
vm1@vm1:~$ sudo usermod -aG devops alice
vm1@vm1:~$ sudo usermod -aG devops bob
vm1@vm1:~$ sudo visudo /etc/sudoers.d/
README    mon       web_cmds  webadmin
vm1@vm1:~$ sudo visudo /etc/sudoers.d/web_cmds
[sudo] password for vm1:

[1]+  Stopped                 sudo visudo /etc/sudoers.d/web_cmds
vm1@vm1:~$ which docker
/usr/bin/docker
vm1@vm1:~$ fg
sudo visudo /etc/sudoers.d/web_cmds
vm1@vm1:~$ sudo visudo /etc/sudoers.d/web_cmds
vm1@vm1:~$
```

```
vm1@vm1:~$
vm1@vm1:~$ su - alice
Password:
su: Authentication failure
vm1@vm1:~$ su - alice
Password:
su: Authentication failure
vm1@vm1:~$ su - bob
Password:
su: warning: cannot change directory to /opt/users/bob: No such file or directo
$
$
$ exit
vm1@vm1:~$ su - alice
Password:
 welcome mina
alice@vm1:~$ docker start
docker: 'docker start' requires at least 1 argument

Usage:  docker start [OPTIONS] CONTAINER [CONTAINER...]

See 'docker start --help' for more information
alice@vm1:~$ docker --help
alice@vm1:~$ docker ps
permission denied while trying to connect to the Docker daemon socket at
unix:/var%2Frun%2Fdocker.sock/v1.50/containers/json": dial unix /var/run/docker.sock:
alice@vm1:~$
alice@vm1:~$ docker ps
permission denied while trying to connect to the Docker daemon socket at
unix:/var%2Frun%2Fdocker.sock/v1.50/containers/json": dial unix /var/run/docker.sock:
alice@vm1:~$ su - bob
Password:
su: warning: cannot change directory to /opt/users/bob: No such file or directo
$ systemctl start docker
-sh: 1: systemct: not found
$ systemctl start docker
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to start 'docker.service'.
Authenticating as: Mina (vm1)
Password:
==== AUTHENTICATION COMPLETE ====
Warning: The unit file, source configuration file or drop-ins of docker.servicen-
reload' to reload units.
$ su - alice
Password:
 welcome mina
alice@vm1:~$ systemctl start docker
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to start 'docker.service'.
Authenticating as: Mina (vm1)
Password:
==== AUTHENTICATION COMPLETE ====
Warning: The unit file, source configuration file or drop-ins of docker.servicen-
reload' to reload units.
alice@vm1:~$
```

Part C: User Account Management

5. **Practice user locking and unlocking**:
    - Lock charlie's account using usermod -L
    - Test that charlie cannot login
    - Unlock the account and verify access is restored

```
vm1@vm1:~$ sudo usermod -L charlie
vm1@vm1:~$ su charlie
Password:
su: Authentication failure
vm1@vm1:~$ usermod --help
vm1@vm1:~$ sudo usermod -U charlie
vm1@vm1:~$ su charlie
Password:
charlie@vm1:/home/vm1$
charlie@vm1:/home/vm1$
```

6. **Set password policies**:
    - Set password expiration for bob (30 days)
    - Set minimum password age for alice (7 days)
    - Force alice to change password at next login
7. **Account expiration**:
    - Set charlie's account to expire in 30 days
    - Verify the setting using chage -l Charlie

```
vm1@vm1:~$ sudo usermod -E 2025-11-13
usermod: invalid option -- 'E'
Usage: usermod [options] LOGIN

Options:
  ------------------------------------------------

vm1@vm1:~$ sudo usermod -e 2025-11-16 charlie
vm1@vm1:~$ chage -l charlie
chage: Permission denied.
vm1@vm1:~$
vm1@vm1:~$ sudo chage -l charlie
Last password change                                    : Oct 16, 2025
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : Nov 16, 2025
```

```
Minimum number of days between password change          : -1
Maximum number of days between password change          : -1
Number of days of warning before password expires       : -1
```

Part D: Complete System Administration Scenario

8. **Create a database administrator setup**:
    - Create user dbadmin
    - Create group database-team
    - Configure sudo permissions for:
        - Starting/stopping MySQL/PostgreSQL services
        - Running database backup scripts (create a dummy script)
        - Managing database user accounts (MySQL commands)
9. **Test the complete setup**:
    - Create a test backup script in /opt/scripts/backup.sh
    - Configure sudo to allow dbadmin to run it
    - Test all permissions work correctly
    - Document any security considerations
10. **Clean up and security review**:
    - List all users and their sudo permissions using sudo -l
    - Remove any test users that shouldn't have sudo access
    - Verify sudoers file syntax using visudo -c

Expected Commands to Use

- visudo (to safely edit sudoers)
- sudo -l (to list permissions)
- usermod (for locking/unlocking accounts)
- chage (for password aging)
- passwd (for password management)
- adduser / addgroup

- su (for user switching and testing)
- systemctl (for service management testing)

Key Concepts to Demonstrate

- Safe sudoers editing with visudo
- Command aliases in sudoers
- Group-based permissions
- NOPASSWD vs password-required operations
- User account locking/unlocking
- Password aging and expiration
- Account expiration dates
- Security considerations for privilege escalation

Files to Work With

- /etc/sudoers
- /etc/sudoers.d/ (separate configuration files)
- /etc/passwd (user information)
- /etc/shadow (password information)