SCENARIO BASED QUESTIONS

Name: Parth Galhotra

QUESTION 1

Due to a security incident, you need to take immediate action to lock down certain user accounts and enforce stricter password policies.
Requirements:
Lock User Accounts:
Lock the accounts of users: Adam (adam), Eve (eve), and Jack (jack) to prevent them from logging in during the investigation.
First we need to create the users Adam, Eve and Jack to lock their account.
This is done by using useradd command which is only run by super-user

```
ubuntu@ip-172-31-12-62:~$ sudo useradd Adam
ubuntu@ip-172-31-12-62:~$ sudo useradd Eve
ubuntu@ip-172-31-12-62:~$ sudo useradd Jack
```

```
nikhil:x:1009:1009::/nikhil:/bin/sh
Adam:x:1010:1010::/home/Adam:/bin/sh
Eve:x:1011:1011::/home/Eve:/bin/sh
Jack:x:1012:1012::/home/Jack:/bin/sh
```

To lock account we have two ways:
1. sudo passwd -l <username>
This will disable the user's account password. Since the password is disabled, the user won't be able to log in via password but can still login through other methods like SSH keys.
2. sudo usermod -L <username>
This will disable the account itself. The user won't be able to log in through any method until it is unlocked again.
We need to give a password to all the users first to lock them

```
ubuntu@ip-172-31-12-62:~$ sudo usermod -L Adam
ubuntu@ip-172-31-12-62:~$ su Adam
Password:
su: Authentication failure
```

Enforce Strong Password Policies:
Set a minimum password length of 12 characters for all users.
Require all users to change their passwords immediately.
To set the minimum password length of 12 characters for all users, We need to set a rule that the minimum password length is 12.
This is done by editing the password policy file named "/etc/security/pwquality.conf"
Linux enforces all the policies by PAM(Pluggable Authentication Module)
First we will need to download the PAM package by giving this command
sudo apt install libpam-pwquality -y
We will find/add this line:

minlen=12
This will set the minimum password length as 12 characters

```
ubuntu@ip-172-31-12-62:~$ sudo nano /etc/security/pwquality.conf
ubuntu@ip-172-31-12-62:~$ sudo passwd nikhil
New password:
BAD PASSWORD: The password is shorter than 12 characters
Retype new password:
passwd: password updated successfully
```

Then to force all the users to change their passwords we will put a command to expire all the users' passwords so that they have to set a new password upon login.
We will use the chage command with the -d flag to force new password from the system administrator

```
ubuntu@ip-172-31-12-62:~$ sudo chage -d 0 nikhil
ubuntu@ip-172-31-12-62:~$ su nikhil
Password:
You are required to change your password immediately (administrator enforced).
Changing password for nikhil.
Current password:
New password:
BAD PASSWORD: The password is the same as the old one
New password:
```

To verify it we will run the following command.
(Optional)
To ensure the changes take effect, we will restart the PAM service by giving this command
sudo systemctl restart sshd

Account Auditing:

Generate a list of all user accounts and their password status.

To generate a list of all user accounts we use
To see all the non system users status at once we use awk command to process the script

```
ubuntu@ip-172-31-12-62:~$ awk -F: '$3 >= 1000 { print $1 }' /etc/passwd
nobody
ubuntu
parth
shubham
nikhil
Adam
Eve
Jack
```

To see the password status of these users we use awk command again with the chage command to get the password status. We use xargs command to convert script to command

```
ubuntu@ip-172-31-12-62:~$ sudo awk -F: '$3 >= 1000 { print $1 }' /etc/passwd | xargs -I{} sudo chage -l {} 2>/dev/null
Last password change                                    : Mar 05, 2025
Password expires                                        : never
Password inactive                                       : never
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
Last password change                                    : Mar 28, 2025
Password expires                                        : never
Password inactive                                       : never
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
Last password change                                    : Mar 29, 2025
Password expires                                        : never
Password inactive                                       : never
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
Last password change                                    : Apr 01, 2025
Password expires                                        : never
Password inactive                                       : never
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
```

```
Last password change                                    : password must be changed
Password expires                                        : password must be changed
Password inactive                                       : password must be changed
Account expires                                         : May 02, 2025
Minimum number of days between password change          : 0
Maximum number of days between password change          : 9
Number of days of warning before password expires       : 2
Last password change                                    : Apr 02, 2025
Password expires                                        : never
Password inactive                                       : never
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
Last password change                                    : Apr 02, 2025
Password expires                                        : never
Password inactive                                       : never
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
Last password change                                    : Apr 02, 2025
Password expires                                        : never
Password inactive                                       : never
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
```

QUESTION 2

Scenario: You are the system administrator for a medium-sized company that uses a Linux-based server for its internal operations. Your company has recently undergone a reorganization, and there is a need to update the user groups to reflect the new structure.

The following changes are required:

1. Create New Groups:
• A new department called "Research" has been formed. You need to create a new group named research.
• Another new department called "Development" has also been established. Create a new group named development.
2. Modify Existing Groups:
• The existing group engineering needs to be renamed to tech.
• The existing group admin needs its group ID changed from 1001 to 2001.
3. Add Users to Groups:
• A new employee, Alice, is joining the Research department. Create a user account for Alice and add her to the research group.
• Another new employee, Bob, is joining the Development department. Create a user account for Bob and add him to the development group.
• Charlie, who is already a part of the engineering group, should now be part of the newly named tech group.
• Dave, an existing member of the admin group, should remain in the group after the group ID change.

Requirements:

1. Create the new groups research and development.

We have used groupadd command to add a group in the server which is done by using the superuser do to get the necessary permissions to add a group

To verify that a group has been created , we have used cat to view the /etc/group file which stores the information of groups

```
ubuntu@ip-172-31-12-62:~$ sudo groupadd research
ubuntu@ip-172-31-12-62:~$ sudo groupadd development
```

```
ubuntu@ip-172-31-12-62:~$ cat /etc/group
```

```
research:x:1013:
development:x:1014:
```

2. Rename the engineering group to tech.

We have used groupmod to modify the group and -n flag to rename it

```
ubuntu@ip-172-31-12-62:~$ sudo groupmod -n tech engineering
ubuntu@ip-172-31-12-62:~$ cat /etc/group
development:x:1014:
tech:x:1015:
```

3. Change the group ID of admin to 2001.

This is before the change. The GID is 110

```
admin:x:110:
```

We have used groupmod to change the group id to 2001

We have used getent command to get the group details of admin to verify the result

```
ubuntu@ip-172-31-12-62:~$ sudo groupmod -g 2001 admin
ubuntu@ip-172-31-12-62:~$ getent group admin
admin:x:2001:
```

4. Create new user accounts for Alice and Bob, and add them to the respective groups.

We will use usermod command to add the users in the group

-a flag is used to prevent the command from deleting all the groups the user is part of

-G flag is used to specify the new list of supplementary groups

```
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG research Alice
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG development Bob
ubuntu@ip-172-31-12-62:~$ getent group research
research:x:1013:Alice
ubuntu@ip-172-31-12-62:~$ getent group development
development:x:1014:Bob
```

5. Ensure Charlie is added to the tech group and confirm his membership.

```
ubuntu@ip-172-31-12-62:~$ sudo useradd charlie
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG tech charlie
ubuntu@ip-172-31-12-62:~$ getent group tech
tech:x:1015:charlie
```

6. Ensure Dave remains in the admin group after the group ID change.

```
ubuntu@ip-172-31-12-62:~$ getent group admin
admin:x:2001:
ubuntu@ip-172-31-12-62:~$ sudo useradd dave
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG admin dave
ubuntu@ip-172-31-12-62:~$ getent group admin
admin:x:2001:dave
ubuntu@ip-172-31-12-62:~$
```

QUESTION 3

You are a system administrator managing a shared directory /projects on a Linux server used by different teams in your organization. The directory contains subdirectories for different projects, and each project directory needs specific access permissions for different users and groups.

<u>Requirements:</u>

1. *Project Managers* (group proj_managers) should have read, write, and execute permissions on all project directories.
2. *Developers* (group developers) should have read and execute permissions on all project directories, but they should not be able to delete or modify any files.
3. *QA Engineers* (group qa_engineers) should have read-only access to the project_alpha directory but no access to other project directories.
4. User alice (a senior developer) should have read, write, and execute permissions on the project_beta directory only.
5. Ensure that default ACLs are set so that any new files or subdirectories created within /projects inherit the correct permissions.

Tasks:

Example Subdirectories in /projects:

/projects/project_alpha
/projects/project_beta
/projects/project_gamma

First we have to create /project directory with project_alpha, project_beta, project_gamma subdirectories in it by using -p and doing it in one command.

```
ubuntu@ip-172-31-12-62:~$ sudo mkdir -p /projects/project_alpha /projects/project_beta /projects/project_gamma
```

```
ubuntu@ip-172-31-12-62:~$ ls /projects
project_alpha  project_beta  project_gamma
```

Now we create the three groups asked

```
ubuntu@ip-172-31-12-62:~$ sudo groupadd proj_managers
```

```
ubuntu@ip-172-31-12-62:~$ sudo groupadd developers
ubuntu@ip-172-31-12-62:~$ sudo groupadd qa_engineers
```

Now we make sure that the /project directory is owned by root and no one else

```
ubuntu@ip-172-31-12-62:~$ ls -l /projects
total 12
drwxr-xr-x 2 root root 4096 Apr  2 21:17 project_alpha
drwxr-xr-x 2 root root 4096 Apr  2 21:17 project_beta
drwxr-xr-x 2 root root 4096 Apr  2 21:17 project_gamma
ubuntu@ip-172-31-12-62:~$
```

Here we already have root as the owner otherwise we would have to sue chown command to change the owner of the directory to root

sudo chown root:root /projects

We would also have to give read, write , execute permissions to the directory
4 - read, 2 - write, 1 - execute

sudo chmod 755 /projects

Now we give the ownership of all the files in the /project directory to proj_manager group.
To do this we need to use the chown command and use the -R flag to include all the files in the directory in the new ownership command

```
ubuntu@ip-172-31-12-62:~$ ls -l /projects
total 12
drwxr-xr-x 2 root root 4096 Apr  2 21:17 project_alpha
drwxr-xr-x 2 root root 4096 Apr  2 21:17 project_beta
drwxr-xr-x 2 root root 4096 Apr  2 21:17 project_gamma
ubuntu@ip-172-31-12-62:~$ sudo chown -R :proj_managers /projects
ubuntu@ip-172-31-12-62:~$ ls -l /projects
total 12
drwxr-xr-x 2 root proj_managers 4096 Apr  2 21:17 project_alpha
drwxr-xr-x 2 root proj_managers 4096 Apr  2 21:17 project_beta
drwxr-xr-x 2 root proj_managers 4096 Apr  2 21:17 project_gamma
```

We also have to give permission of read,write and execute to owner and his/her group and no permission to anyone else

```
ubuntu@ip-172-31-12-62:~$ sudo chmod -R 770 /projects
ubuntu@ip-172-31-12-62:~$ ls -l /projects
ls: cannot open directory '/projects': Permission denied
```

Now we have to give the user and group special access to files.
To do this we need to set up an ACL(Access Control List) to give specific permissions to specific users and groups. We will use setfacl command to set up rules in the ACL about the access -R to set the ACL to all the files inside /projects, -m to modify the ACL ,-d to set it as default.

```
ubuntu@ip-172-31-12-62:~$ sudo setfacl -R -m g:developers:rx /projects
ubuntu@ip-172-31-12-62:~$ sudo setfacl -d -m g:developers:rx /projects
ubuntu@ip-172-31-12-62:~$ getfacl /projects
getfacl: Removing leading '/' from absolute path names
# file: projects
# owner: root
# group: proj_managers
user::rwx
group::rwx
group:developers:r-x
mask::rwx
other::---
default:user::rwx
default:group::rwx
default:group:developers:r-x
default:mask::rwx
default:other::---
```

Now we will do it for others also

```
ubuntu@ip-172-31-12-62:~$ sudo setfacl -R -m g:proj_managers:rwx /projects
ubuntu@ip-172-31-12-62:~$ sudo setfacl -d -m g:proj_managers:rwx /projects
ubuntu@ip-172-31-12-62:~$ sudo setfacl -R -m g:qa_engineers:r /projects/project_alpha
ubuntu@ip-172-31-12-62:~$ sudo setfacl -d -m g:qa_engineers:r /projects/project_alpha
ubuntu@ip-172-31-12-62:~$ getfacl /projects
getfacl: Removing leading '/' from absolute path names
# file: projects
# owner: root
# group: proj_managers
user::rwx
group::rwx
group:proj_managers:rwx
group:developers:r-x
mask::rwx
other::---
default:user::rwx
default:group::rwx
default:group:proj_managers:rwx
default:group:developers:r-x
default:mask::rwx
default:other::---
```

```
ubuntu@ip-172-31-12-62:~$ getfacl /projects/project_alpha
getfacl: /projects/project_alpha: Permission denied
ubuntu@ip-172-31-12-62:~$ sudo getfacl /projects/project_alpha
getfacl: Removing leading '/' from absolute path names
# file: projects/project_alpha
# owner: root
# group: proj_managers
user::rwx
group::rwx
group:proj_managers:rwx
group:developers:r-x
group:qa_engineers:r--
mask::rwx
other::---
default:user::rwx
default:group::rwx
default:group:qa_engineers:r--
default:mask::rwx
default:other::---

ubuntu@ip-172-31-12-62:~$
```

QUESTION 4

Your company has a new project starting, and a temporary project team needs to be set up on the server.
This involves creating user accounts, modifying permissions, and ensuring account security.
Requirements:

Create New User Accounts:
Create user accounts for new team members: Alice (username alice), Bob (username bob), and Charlie
(username charlie), and set initial passwords for each.
Set the shell for all new users to /bin/bash.
chsh command is used to change shell for the current user but when we use sudo and use -s flag we can change the default shell for other users also

```
ubuntu@ip-172-31-12-62:~$ sudo chsh -s /bin/bash Bob
ubuntu@ip-172-31-12-62:~$ sudo chsh -s /bin/bash charlie
ubuntu@ip-172-31-12-62:~$ sudo chsh -s /bin/bash Alice
ubuntu@ip-172-31-12-62:~$ cat /etc/passwd
```

```
Alice:x:1013:2002::/home/Alice:/bin/bash
Bob:x:1014:2003::/home/Bob:/bin/bash
charlie:x:1015:2004::/home/charlie:/bin/bash
```

Modify User Permissions:
Alice needs to be added to the developers group.

```
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG developers Alice
```

Bob and Charlie need to be added to the testers group.

```
ubuntu@ip-172-31-12-62:~$ getent group testers
testers:x:2008:
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG testers Bob
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG testers charlie
ubuntu@ip-172-31-12-62:~$ getent group testers
testers:x:2008:Bob,charlie
ubuntu@ip-172-31-12-62:~$
```

Password Policies:
Set an expiry date for all user passwords to ensure they are changed in 30 days.
We have used chage to set the age of the password which is 30 days.
-M signifies Maximum days in which the password is valid
After 30 days the passwor dwill be invalid and the user will need ot change the password again

```
ubuntu@ip-172-31-12-62:~$ sudo chage -M 30 Alice
ubuntu@ip-172-31-12-62:~$ sudo chage -M 30 Bob
ubuntu@ip-172-31-12-62:~$ sudo chage -M 30 charlie
```

To verify it We have to check every user separately

```
ubuntu@ip-172-31-12-62:~$ sudo chage -l Alice
Last password change                                    : Apr 02, 2025
Password expires                                        : May 02, 2025
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 30
Number of days of warning before password expires       : 7
ubuntu@ip-172-31-12-62:~$ sudo chage -l Bob
Last password change                                    : Apr 02, 2025
Password expires                                        : May 02, 2025
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 30
Number of days of warning before password expires       : 7
ubuntu@ip-172-31-12-62:~$ sudo chage -l charlie
Last password change                                    : Apr 02, 2025
Password expires                                        : May 02, 2025
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 30
Number of days of warning before password expires       : 7
ubuntu@ip-172-31-12-62:~$
```

==========

QUESTION 5

You have recently been hired as a System Administrator at a mid-sized company. The company is restructuring its IT department, and you have been tasked with managing user accounts and groups on one
of the company's Linux servers. Your tasks are as follows:

• Create a New User:

• A new employee, Alice Johnson, has joined the IT department as a Network Engineer.

• Create a user account for Alice with the username alicej.

We will create a new user alicej using sudo useradd command

• Ensure Alice's home directory is located at /home/alicej, and set the default shell to /bin/bash.

To set the home directory as /home/alicej we will need to use the command usermod -d (flag to change the home directory)

```
ubuntu@ip-172-31-12-62:~$ sudo useradd alicej
ubuntu@ip-172-31-12-62:~$ sudo usermod -d /home/alicej alice j
```

```
dave:x:1016:1016::/home/dave:/bin/sh
alicej:x:1017:1017::/home/alicej:/bin/sh
```

To set the default shell to /bin/bash we need to use the command chsh -s <path_to_directory>

```
ubuntu@ip-172-31-12-62:~$ sudo chsh -s /bin/bash alicej
ubuntu@ip-172-31-12-62:~$ cat /etc/passwd
```

```
alicej:x:1017:1017::/home/alicej:/bin/bash
ubuntu@ip-172-31-12-62:~$
```

• Create a Group:

• The IT department has a special group for network engineers called neteng.

• Create this group on the system.

We will create the group by groupadd groupname command and verify it using getent command which will show the users in the group

```
ubuntu@ip-172-31-12-62:~$ sudo groupadd neteng
```

```
ubuntu@ip-172-31-12-62:~$ getent group neteng
neteng:x:2009:
ubuntu@ip-172-31-12-62:~$
```

• Add the User to the Group:

• Add Alice to the neteng group.

To add Alice to the neteng group we need to use sudo usermod -aG group Username command

```
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG neteng alicej
ubuntu@ip-172-31-12-62:~$ getent group neteng
neteng:x:2009:alicej
ubuntu@ip-172-31-12-62:~$
```

• Ensure that she is also part of the users group, which grants basic permissions.

Users group is already created by default, which has the basic permissions

```
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG users alicej
ubuntu@ip-172-31-12-62:~$ getent group users
users:x:100:alicej
```

• Modify User Account:

• After a security review, it's been decided that all Network Engineers must use /bin/zsh as their default shell.

• Modify Alice's account to use /bin/zsh as the default shell.

To change the default shell we need to use chsh -s command again

```
ubuntu@ip-172-31-12-62:~$ sudo chsh -s /bin/zsh alicej
ubuntu@ip-172-31-12-62:~$ cat /etc/passwd
alicej:x:1017:1017::/home/alicej:/bin/zsh
```

• Delete a User Account:

• Another employee, Bob Smith, has left the company. His username was bobsmith.

First we add the user bobsmith to the server and check if he is in the server

```
ubuntu@ip-172-31-12-62:~$ sudo useradd bobsmith
ubuntu@ip-172-31-12-62:~$ cat /etc/passwd
bobsmith:x:1018:1018::/home/bobsmith:/bin/sh
```

• Delete Bob's user account along with his home directory and any associated files.

We use userdel command to delete bobsmith from the server which include its homie directory also

We can check if he is still in the server by using any command with username in it like id

```
ubuntu@ip-172-31-12-62:~$ sudo userdel bobsmith
ubuntu@ip-172-31-12-62:~$ id bobsmith
id: 'bobsmith': no such user
ubuntu@ip-172-31-12-62:~$
```

• Additional Group Requirement:

• There is another group, admins, that needs to be created for users with administrative privileges.

• Create the admins group and add yourself (yourusername) to it.

We will create the group admin and add ourselves into it by putting the value of user by putting $ at the start

Then we verify the user in the group by using the getent command

```
ubuntu@ip-172-31-12-62:~$ sudo groupadd admins
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG admins $USER
ubuntu@ip-172-31-12-62:~$ getent group admins
admins:x:2010:ubuntu
ubuntu@ip-172-31-12-62:~$
```

QUESTION 6

File Permissions and User Management for a Development Server

Scenario: You are managing a Linux development server used by multiple developers with different access needs.

• Password Reset for a Developer:
• A developer, john_r, has forgotten his password. Reset his password

First we have created the user john_r and have verified it by using the id command to get the id of john_r. If there was no john_r user in the server then it would have given an error

```
ubuntu@ip-172-31-12-62:~$ sudo useradd john_r
ubuntu@ip-172-31-12-62:~$ id john_r
uid=1018(john_r) gid=1018(john_r) groups=1018(john_r)
```

• Set a temporary password and require him to change it upon his next login.
We will create a password for a user and then we will set the command chage such that his password is invalid. So he will have to set a new password on his next login

```
ubuntu@ip-172-31-12-62:~$ sudo passwd john_r
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
```

```
ubuntu@ip-172-31-12-62:~$ sudo chage -d 0 john_r
ubuntu@ip-172-31-12-62:~$ sudo chage -l john_r
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
```

• Switch User for Testing:
• John needs to test a configuration under the testuser account without logging out of his current session.
• Show John how to use the su command to switch to testuser and run a test, then return to his own Account.

To do this first we need to create a testuser account and then we need to use su(switch-user) to change the user and run a test and then exit the shell to come back to the previous account

```
ubuntu@ip-172-31-12-62:~$ sudo useradd testuser
```

```
ubuntu@ip-172-31-12-62:~$ sudo passwd testuser
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: password updated successfully
```

```
$ echo "Hello"
Hello
$ exit
ubuntu@ip-172-31-12-62:~$
```

• Grant sudo Privileges for Software Installation:

• John needs to install development tools but should not have full administrative rights.
• Add John to the sudo group with permissions limited to installing software packages using apt-get.
We need to add the user john's privilege in the sudoers file to give limited privileges.
If we needed to give all the permission to john then we would just have to add the john user to the sudo group but for limited privileges we need to edit the sudoers file.

```
ubuntu@ip-172-31-12-62:~$ sudo visudo
```

```
john_r ALL=(ALL) NOPASSWD: /usr/bin/apt-get, /usr/bin/apt
```

• Provide an example command for John to install the git package using sudo.

```
ubuntu@ip-172-31-12-62:~$ sudo apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.43.0-1ubuntu7.2).
git set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 26 not upgraded.
```

• Set Directory Permissions for Shared Projects:
• John is working on a shared project in the /projects/shared/ directory.

```
ubuntu@ip-172-31-12-62:~$ sudo mkdir /projects/shared
ubuntu@ip-172-31-12-62:~$ sudo ls /projects
project_alpha  project_beta  project_gamma  shared
```

• Use chmod to set the directory permissions so that John and his group (devteam) can read, write, and execute files, but no other users can access the directory.

```
ubuntu@ip-172-31-12-62:~$ sudo chown -R john_r:devteam /projects/shared
ubuntu@ip-172-31-12-62:~$ sudo chmod -R 770 /projects/shared
ubuntu@ip-172-31-12-62:~$ sudo ls -l /projects/shared
total 16
drwxrwx---+ 2 john_r devteam 4096 Apr  3 06:10 file1
drwxrwx---+ 2 john_r devteam 4096 Apr  3 06:10 file2
ubuntu@ip-172-31-12-62:~$ sudo ls -ld /projects/shared
drwxrwx---+ 4 john_r devteam 4096 Apr  3 06:10 /projects/shared
ubuntu@ip-172-31-12-62:~$
```

• Change Ownership for File Maintenance:

• John needs to take ownership of some files within the /projects/shared/ directory that were created by another user.

• Use chown to change the ownership of these files to John, ensuring that he has full control over Them.

We can use chown to get the ownership of the directory to john_r then we can verify it using ls -ld command

```
ubuntu@ip-172-31-12-62:~$ sudo chown -R john_r:john_r /projects/shared
ubuntu@ip-172-31-12-62:~$ sudo ls -l /projects/shared
total 16
drwxrwx---+ 2 john_r john_r 4096 Apr  3 06:10 file1
drwxrwx---+ 2 john_r john_r 4096 Apr  3 06:10 file2
ubuntu@ip-172-31-12-62:~$
```

• Revoke Temporary sudo Access:

• After the tools are installed, remove John's sudo access to maintain security.

We can delete user john_r directly from the sudo file to revoke admin access if we have previously added the user directly to sudo group

We can also edit the sudoers file to delete the user from there manually

• Document the process to verify that his sudo privileges have been removed.

We can verify the privileges john has by sudo -l -U john command

```
ubuntu@ip-172-31-12-62:~$ sudo visudo
ubuntu@ip-172-31-12-62:~$ sudo -l -U john_r
User john_r is not allowed to run sudo on ip-172-31-12-62.
```

QUESTION 7

You are managing a Linux server in a healthcare environment where data sensitivity is crucial.
• Enforce Password Policies:
• The security policy requires all users to have passwords that expire every 60 days. Set this policy for the user dr_smith using the passwd command.
• Ensure that Dr. Smith is prompted to change the password the next time he logs in.
First we will create a user dr_smith and set a password
Then we will set the policy that dr_smith password will become invalid in 60 days.
And we will expire its password with a command

```
ubuntu@ip-172-31-12-62:~$ sudo useradd dr_smith
ubuntu@ip-172-31-12-62:~$ sudo passwd dr_smith
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-12-62:~$ sudo chage -M 60 dr_smith
ubuntu@ip-172-31-12-62:~$ sudo chage -d 0 dr_smith
```

• Use of su for Secure Access:
• Dr. Smith needs to access another user's account, nurse_jane, to review patient data. However, it is critical to ensure that this is done securely and logged.
• Guide Dr. Smith on how to use su to switch to Nurse Jane's account and emphasize the importance of logging out afterward.
We use sudo passwd to set the user password and use su to switch the user from dr_smith to nurse_jane and run the command whoami to know which user is currently logged in and we exit to return to the previous user to showcase the logging out

```
ubuntu@ip-172-31-12-62:~$ sudo useradd nurse_jane
ubuntu@ip-172-31-12-62:~$ sudo passwd
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-12-62:~$ su dr_smith
Password:
You are required to change your password immediately (administrator enforced).
Changing password for dr_smith.
Current password:
New password:
BAD PASSWORD: The password is shorter than 8 characters
New password:
BAD PASSWORD: The password is shorter than 8 characters
New password:
Retype new password:
$ echo "hello
> "
hello

$ exit
ubuntu@ip-172-31-12-62:~$
```

• Granting Administrative Rights with sudo:

• The IT department needs to perform system maintenance, but you want to ensure that Dr. Smith can only perform specific administrative tasks, such as restarting a service.

We add dr_smith to the group sudo to give him full sudo privileges

```
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG sudo dr_smith
ubuntu@ip-172-31-12-62:~$ sudo visudo
```

• Add Dr. Smith to the sudo group with permissions limited to restarting the apache2 service.

For limited privileges we have to edit the sudoers file to give permission to only restart apache2 service

```
dr_smith ALL=(ALL) NOPASSWD: /bin/systemctl restart apache2, /bin/systemctl start apache2, /bin/systemctl stop apache2
```

• Provide an example command Dr. Smith would use to restart the service with sudo.

We switch user to dr_smith to see if he has the permission to restart apache2

```
ubuntu@ip-172-31-12-62:~$ su dr_smith
Password:
$ sudo /bin/systemctl restart apache2
```

• Setting Permissions on Sensitive Files:

• Dr. Smith has created a directory for storing patient data, located at /secure/patients/.

• Use chmod to ensure that only Dr. Smith can access this directory and its files, with no read, write, or execute permissions for anyone else.

First we need to create the directory and subdirectories

Then we need to make dr_smith the owner of the directory and give permission of only the owner being able to read,write and execute on the directory.

```
ubuntu@ip-172-31-12-62:~$ sudo mkdir -p /secure/patients
ubuntu@ip-172-31-12-62:~$ sudo chown dr_smith /secure/patients
ubuntu@ip-172-31-12-62:~$ sudo chmod 700 /secure/patients
```

• Change Ownership for Secure Collaboration:

• The patient data needs to be shared with Nurse Jane, but no one else should have access.

• Use chown to change the group ownership of the /secure/patients/ directory to nurses, allowing only members of the nurses group to access it.

We create the group nurses and add dr_smith and nurse_jane to it

Then we make dr_smith the owner of the directory and share the directory with the whole group

```
ubuntu@ip-172-31-12-62:~$ sudo groupadd nurses
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG nurses dr_smith
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG nurses nurse_jane
```

```
ubuntu@ip-172-31-12-62:~$ sudo chown -R dr_smith:nurses /secure/patients
ubuntu@ip-172-31-12-62:~$ sudo chmod -R 700 /secure/patients
```

• Audit and Remove Unnecessary Privileges:

• After maintenance is complete, review and remove Dr. Smith's sudo privileges, ensuring no unnecessary access remains.

• Document how to check for any remaining sudo permissions and confirm their removal.

To delete sudo privileges for dr_smith we need to go to sudoers file and remove the access privileges and also remove the user from the sudo group that we added him into before

```
ubuntu@ip-172-31-12-62:~$ sudo visudo
ubuntu@ip-172-31-12-62:~$ sudo su dr_smith
$ whoami
dr_smith
$ sudo /bin/systemctl restart apache2
[sudo] password for dr_smith:
$ exit
ubuntu@ip-172-31-12-62:~$ sudo deluser dr_smith sudo
```

QUESTION 8

Scenario: A company is working on two major projects, Project Alpha and Project Beta. Specific users need access to these projects, and security is critical.

• Create Project Groups:

• Create two groups: alpha and beta for Project Alpha and Project Beta.

• Create User Accounts for Project Members:

• david_a and lisa_b are working on Project Alpha. Create their user accounts with usernames davida and lisab, respectively.

• nina_c and tom_d are working on Project Beta. Create their user accounts with usernames ninac and tomd.

• Assign each user to the appropriate project group (davida and lisab to alpha, ninac and tomd to beta).

```
ubuntu@ip-172-31-12-62:~$ sudo groupadd alpha
ubuntu@ip-172-31-12-62:~$ sudo groupadd beta
ubuntu@ip-172-31-12-62:~$ sudo useradd davida
ubuntu@ip-172-31-12-62:~$ sudo useradd lisab
ubuntu@ip-172-31-12-62:~$ sudo useradd ninac
ubuntu@ip-172-31-12-62:~$ sudo useradd tomd
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG alpha davida
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG alpha lisab
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG beta ninac
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG beta tomd
ubuntu@ip-172-31-12-62:~$ getent group alpha
alpha:x:2013:davida,lisab
ubuntu@ip-172-31-12-62:~$ getent group beta
beta:x:2014:ninac,tomd
ubuntu@ip-172-31-12-62:~$
```

• Cross-Project Access:

• David needs temporary access to Project Beta as well. Add him to the beta group.

```
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG beta davida
ubuntu@ip-172-31-12-62:~$ getent group beta
beta:x:2014:ninac,tomd,davida
```

• Security Update:

• Due to security policies, the default shell for all alpha project users must be changed to /bin/zsh.

• Apply this change to all users in the alpha group.

We use chsh command to set the change the shell and -s flag to set the default shell the user

But to change the default shell of another user we need to use sudo

```
ubuntu@ip-172-31-12-62:~$ sudo chsh -s /bin/zsh davida
ubuntu@ip-172-31-12-62:~$ sudo chsh -s /bin/zsh lisab
```

• Account Removal:

• Tom has completed his work on Project Beta and left the team. Remove his user account and all associated files.

To remove tom from the server we need to use userdel to remove this user from the server

```
ubuntu@ip-172-31-12-62:~$ sudo userdel -R tomd
userdel: invalid chroot path 'tomd', only absolute paths are supported.
ubuntu@ip-172-31-12-62:~$ sudo userdel -r tomd
userdel: tomd mail spool (/var/mail/tomd) not found
userdel: tomd home directory (/home/tomd) not found
ubuntu@ip-172-31-12-62:~$ sudo userdel tomd
userdel: user 'tomd' does not exist
ubuntu@ip-172-31-12-62:~$ getent group beta
beta:x:2014:ninac,davida
ubuntu@ip-172-31-12-62:~$
```

• Create a Shared Admin Group:

• Both projects need an admin group for managing project-specific permissions. Create an admin_alpha and admin_beta group.

```
ubuntu@ip-172-31-12-62:~$ sudo groupadd admin_alpha
ubuntu@ip-172-31-12-62:~$ sudo groupadd admin_beta
```

• Add yourself to both groups for administrative purposes.

To add multiple groups to a single user we can just do it in one command by adding them side by side

```
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG admin_alpha,admin_beta ubuntu
ubuntu@ip-172-31-12-62:~$ groups ubuntu
ubuntu : ubuntu shared admins admin_alpha admin_beta
ubuntu@ip-172-31-12-62:~$
```

QUESTION 9

You are a System Administrator responsible for maintaining a secure environment on a shared Linux server used by various teams.

• Set User Password:

• A new user, emma_w, has just joined the team. After creating her account, she needs to set a strong password.

• Guide her to set her password using the passwd command. Ensure the password meets the company's security policies.

```
ubuntu@ip-172-31-12-62:~$ sudo useradd emma_w
ubuntu@ip-172-31-12-62:~$ sudo passwd emma_w
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
```

• Temporary Root Access:

• For a critical system update, Emma needs temporary root access to perform administrative tasks.

• As a security measure, instead of sharing the root password, provide her with sudo privileges.

• Document the steps she would take to gain root access using the sudo command and how to perform a secure task, such as updating the system.

```
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG sudo emma_w
ubuntu@ip-172-31-12-62:~$ su emma_w
Password:
$ sudo apt update
[sudo] password for emma_w:
Hit:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [980 kB]
```

• Switch User Role:

• After finishing her work, Emma needs to switch to another user's account, john_d, to verify some configurations.

• Explain how Emma can use the su command to switch to John's account, and specify the importance of logging out after the task.

```
ubuntu@ip-172-31-12-62:~$ su emma_w
Password:
$ su john_d
Password:
$ whoami
john_d
$ exit
$ whoami
emma_w
$ exit
```

• Modify File Permissions:

• Emma notices that a script she needs to execute does not have the proper permissions. The script is located at /home/emma_w/scripts/update.sh.

• Change the permissions of the script to make it executable only by Emma using the chmod Command.

```
ubuntu@ip-172-31-12-62:~$ su emma_w
Password:
$ mkdir -p /home/emma_w/scripts/update.sh
mkdir: cannot create directory '/home/emma_w': Permission denied
$ sudo mkdir -p /home/emma_w/scripts/update.sh
$ sudo chmod 700 /home/emma_w/scripts/update.sh
```

• Change File Ownership:

• The script Emma worked on is now ready to be shared with the entire team. To ensure proper access, the ownership of the script should be transferred to the team group.

• Use the chown command to change the group ownership of the script to team, while keeping Emma as the file owner.

```
ubuntu@ip-172-31-12-62:~$ sudo groupadd team
ubuntu@ip-172-31-12-62:~$ sudo usermod -aG team emma_w
ubuntu@ip-172-31-12-62:~$ sudo chown -R emma_w:team /home/emma_w/scripts/update.sh
ubuntu@ip-172-31-12-62:~$ sudo ls -ld /home/emma_w/scripts/update.sh
drwx------ 2 emma_w team 4096 Apr  3 10:40 /home/emma_w/scripts/update.sh
```

• Remove Temporary Privileges:

• After the system update is complete, revoke Emma's sudo privileges to maintain security. Document the process to ensure the removal is verified.

```
ubuntu@ip-172-31-12-62:~$ sudo deluser emma_w sudo
info: Removing user `emma_w' from group `sudo' ...
```

QUESTION 10

Scenario: You are managing a Linux server that hosts files for various projects. Each project has specific access requirements.

• Set Password Expiry:

• The company's security policy requires users to change their passwords every 90 days. Set this policy for the user mike_b using the passwd command.

```
ubuntu@ip-172-31-12-62:~$ sudo useradd mike_b
ubuntu@ip-172-31-12-62:~$ sudo passwd mike_b
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-12-62:~$ sudo chage -M 90 mike-b
```

```
ubuntu@ip-172-31-12-62:~$ sudo chage -l mike_b
Last password change                                    : Apr 03, 2025
Password expires                                        : Jul 02, 2025
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 7
```

• Project File Permissions:

• Mike_b is working on a confidential project. The project files are stored in /projects/alpha/.

• Set permissions on this directory so that only Mike can read, write, and execute files within it. Use chmod to restrict access for all other users.

```
ubuntu@ip-172-31-12-62:~$ sudo chown mike_b /projects/alpha
ubuntu@ip-172-31-12-62:~$ sudo chmod 700 /projects/alpha
```

```
ubuntu@ip-172-31-12-62:~$ sudo ls -ld /projects/alpha
drwx------+ 2 mike_b root 4096 Apr  3 11:01 /projects/alpha
ubuntu@ip-172-31-12-62:~$
```

• Switch User Context:

• Mike needs to temporarily assume the identity of another user, sara_c, to check some configurations. Explain how he can switch to Sara's account using the su command.

```
ubuntu@ip-172-31-12-62:~$ sudo useradd sara_c
ubuntu@ip-172-31-12-62:~$ sudo passwd sara_c
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-12-62:~$ su mike_b
Password:
$ su sara_c
Password:
$ whoami
sara_c
$ exit
$ whoami
mike_b
$ exit
ubuntu@ip-172-31-12-62:~$
```

• Grant Limited Administrative Access:

• Mike needs to install some software but should not have full root access. Add him to the sudo group with limited privileges to install software packages only.

```
mike_b ALL=(ALL) NOPASSWD: /usr/bin/apt, /usr/bin/apt-get
```

• Provide an example of how Mike would install a package using sudo.

```
ubuntu@ip-172-31-12-62:~$ sudo visudo
ubuntu@ip-172-31-12-62:~$ su mike_b
Password:
$ sudo apt update
Hit:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
25 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

• Ownership Transfer for Collaboration:

• The project is now in a collaborative phase, and the files need to be accessible by the devteam group.

• Use the chown command to change the ownership of the files in /projects/alpha/ to the devteam group while retaining Mike as the file owner.

```
ubuntu@ip-172-31-12-62:~$ sudo chown -R mike_b:devteam /projects/alpha
ubuntu@ip-172-31-12-62:~$ sudo ls -ld /projects/aplha
ls: cannot access '/projects/aplha': No such file or directory
ubuntu@ip-172-31-12-62:~$ sudo ls -ld /projects/alpha
drwx------+ 2 mike_b devteam 4096 Apr  3 11:01 /projects/alpha
```

• Revoke User Access:

• Mike is transferring to a different project. Remove his access to the /projects/alpha/ directory and ensure he can no longer use sudo on the system. Document the steps to verify these changes.

```
ubuntu@ip-172-31-12-62:~$ sudo visudo
ubuntu@ip-172-31-12-62:~$ su mike_b
Password:
$ sudo apt update
[sudo] password for mike_b:
mike_b is not in the sudoers file.
$ exit
ubuntu@ip-172-31-12-62:~$
```