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.

Sudo useradd adam
Sudo useradd Eve
Sudo useradd jack
Sudo /etc/passwd

```
Adam:x:1001:1001::/home/Adam:/bin/sh
Eve:x:1002:1002::/home/Eve:/bin/sh
Jack:x:1003:1003::/home/Jack:/bin/sh
ubuntu@ip-172-31-26-179:/$
```

Usermod -L adam
Usermmd -L Eve
Usermod -L jack
Sudo passwd -S jack

```
ubuntu@ip-172-31-26-179:/$ sudo passwd -S Jack
Jack L 2024-10-01 0 99999 7 -1
ubuntu@ip-172-31-26-179:/$
```

Suod grep Jack /etc/shadow

Enforce Strong Password Policies:
Set a minimum password length of 12 characters for all users.
Require all users to change their passwords immediately.

sudo passwd Adam
Sudo passwd Eve
Sudo passwd jack
Cat /etc/shadow

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

Cat /etc/shadow

```
Adam:$y$j9T$MhS.wwIgMEhoZ1G5lPMDT.$k7ISj4r15bFIbhc0tNdeSkJvx1HuVF/sMsQuwx8Yh.9:19997:0:99999
Eve:$y$j9T$y/DA3m6niWAMMpFSTs228/$ysSSWpKQpQNyzk.whxwlT1UQ8oZJpomoX7TOiA6LcSD:19997:0:99999:
Jack:$y$j9T$O4QAAihqoTcNzwL51hLUL/$nm3xxzpELeCRTPt0GesVIWIIUaQicdWItlm50QUMmI5:19997:0:99999
```

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.

Ans- groupadd Research
groupadd development

```
research:x:1004:
development:x:1005:
ubuntu@ip-172-31-26-179:/$
```

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.

Ans- sudo groupmod -n tech engineering
Sudo groupmod -g 2001 tech

```
tech:x:2002:
ubuntu@ip-172-31-26-179:/$
```

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 existingmember of the admin group, should remain in the group after the group ID change. Requirements:

Ans- usermod -aG research alice
Usermod -aG development bob
Usermod -aG tech charlie

```
research:x:1004:Alice
development:x:1005:Bob
tech:x:2002:Charlie
```

Getent group admin

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

Sudo groupmod -g 2000 admi

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

Ans- groups charlie

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

Ans- getent group admin

```
admin:x:2000:Dave
```

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 projectdirectory needs specific access permissions for different users and groups.

1. *Project Managers* (group proj_managers) should have read, write, and execute permissions on all
project directories.

Ans- sudo setfacl -m g:proj_manager:rwx /home/ubuntu/project

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.

Ans- sudo setfacl -m g:developers:rx /home/ubuntu/projects

3. *QA Engineers* (group qa_engineers) should have read-only access to the project_alpha directory but no access to other project directories.

Ans- sudo setfacl -m g:qa_engineers:r /home/ubuntu/projects

```
group:proj_manager:rwx
group:developers:r-x
group:qa_engineers:r--
```

4. User alice (a senior developer) should have read, write, and execute permissions on the project_beta
directory only.

sudo setfacl -m u:alice:rwx /projects/project_beta

```
user:alice:rwx
```

4. Ensure that default ACLs are set so that any new files or subdirectories created within /projects inherit the correct permissions.

sudo setfacl -m u:ubuntu:rwx /projects/project_beta

sudo setfacl -d -m u:ubuntu:rwx /projects/project_beta

```
default:user::rwx
default:user:ubuntu:rwx
default:group::rwx
default:group:ubuntu:rwx
```

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.

Ans- sudo useraadd alice

Sudo useradd bob

Sudo useradd charlie

Sudo passwd alice

Sudo passwd bob

Sudo passwd charlie

Sudo usermod -S /bin/bash alice

Sudo usermod -S /bin/bash bob

Sudo usermod -S /bin/bash charlie

```
Alice:x:1004:2003::/home/Alice:/bin/bash
Bob:x:1005:2004::/home/Bob:/bin/bash
Charlie:x:1006:1006::/home/Charlie:/bin/bash
```

Modify User Permissions:

Alice needs to be added to the developers group.

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

Ans- sudo usermod -aG developers Alice

```
developers:x:2006:Alice
```

Sudo usermod -aG testers bob

Sudo usermod -aG testers charlie

```
testers:x:2008:Bob,Charlie
```

Password Policies:

Set an expiry date for all user passwords to ensure they are changed in 30 days.

Ans- sudo chage -M 30 alice
Sudo chage -M 30 bob
Sudo chage -M 30 charlie

```
ubuntu@ip-172-31-26-179:~$ sudo chage -l Alice
Last password change                                    : Oct 01, 2024
Password expires                                        : Oct 31, 2024
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
```

==========

Your company is migrating to a new server. As part of this migration, you need to ensure that all user accounts are recreated on the new server with the same settings and passwords.

Requirements:

Extract User Information:

Extract user information (username, home directory, shell) from the old server's /etc/passwd file.

Extract password information from the old server's /etc/shadow file.

Ans- awk -F: '$3 >= 1000 {print $1 ":" $6 ":" $7}' /etc/passwd > users_info.txt
awk -F: '$3 >= 1000 {print $1 ":" $2}' /etc/shadow > passwords_info.txt

Recreate User Accounts:

Recreate the user accounts on the new server with the same settings.

Ans- while IFS=: read -r username home_dir shell; do
sudo useradd -m -d "$home_dir" -s "$shell" "$username"
done < users_info.txt

Preserve Passwords:

Ans- while IFS=: read -r username password; do
echo "$username:$password" | sudo chpasswd -e

done < passwords_info.txt

Ensure that the passwords are preserved during the migration.

Verify Migration:

Ans- cat /etc/passwd | grep username

Verify that the user accounts and passwords have been correctly migrated.

Ans- su - username

Ans- sudo rm -f users_info.txt passwords_info.txt

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.

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

Ans- sudo useradd -m alicej -s /bin/bash

```
ubuntu@ip-172-31-26-179:/home$ ls
alicej  ubuntu
alicej:x:1009:1009::/home/alicej:/bin/bash
```

• Create a Group:

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

• Create this group on the system.

• Add the User to the Group:

• Add Alice to the neteng group.

Ans - sudo groupadd neteng

Sudo usermod -aG neteng alice

```
neteng:x:2009:alicej
```

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

• Modify User Account:

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

Ans- sudo usermod -s /bin/zsh alicej

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

Ans- sudo usermod -d -s /bin/zsh alicej

• Delete a User Account:

Ans- sudo userdel alice

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

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

```
ubuntu@ip-172-31-26-179:/home$ ls
alicej  bobsmith  ubuntu
```

Ans- sudo userdel -r bobsmith

```
ubuntu@ip-172-31-26-179:/home$ ls
ubuntu
```

• 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.

Ans- sudo groupadd admins

Sudo usermod -aG admins bob

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

Ans- sudo passwd john_r

• Set a temporary password and require him to change it upon his next login.

Ans- sudo chage -d 0 john_r

```
ubuntu@ip-172-31-26-179:/home$ sudo chage -d 0 john_r
ubuntu@ip-172-31-26-179:/home$ 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.

Ans- sudo useradd testuser
sudo su testuser
exit

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

```
ubuntu@ip-172-31-26-179:/home$ sudo cat /etc/group | grep sudo
sudo:x:27:ubuntu,john_r
```

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

Ans- sudo setfacl -m u:john_r:rwx ./projects

```
user:john_r:rwx
```

Ans- sudo setfacl -m g:devteam:rwx ./projects

```
group:devteam:rwx
```

• 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.

Ans- chown john_r /projects/shared/
Ans- setfacl -m u:john_r:rwx ./projects/shared

```
ubuntu@ip-172-31-26-179:~$ getfacl ./projects/shared/
# file: projects/shared/
# owner: john_r
# group: ubuntu
```

• Revoke Temporary sudo Access:
• After the tools are installed, remove John's sudo access to maintain security.
• Document the process to verify that his sudo privileges have been removed.

Ans- sudo deluser john_r sudo

Sudo cat /etc/group | grep sudo

```
ubuntu@ip-172-31-26-179:~$ sudo cat /etc/group | grep sudo
sudo:x:27:ubuntu
```

Sudo groups john_r

```
ubuntu@ip-172-31-26-179:~$ groups john_r
john_r : john_r
```

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.

Ans- sudo sueradd dr_smith

Sudo passwd dr_smith

Sudo chage -M 60 dr_smith

```
ubuntu@ip-172-31-26-179:~$ sudo chage -l dr_smith
Last password change                                    : Oct 02, 2024
Password expires                                        : Dec 01, 2024
Password inactive                                       : never
```

• Ensure that Dr. Smith is prompted to change the password the next time he logs in.

Ans- sudo chage -d 0 dr_smith

```
ubuntu@ip-172-31-26-179:~$ sudo chage -l dr_smith
Last password change                                    : password must be changed
Password expires                                        : password must be changed
Password inactive                                       : password must be changed
Account expires                                         : never
```

• 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.

Ans- sudo su nurse_jane

```
ubuntu@ip-172-31-26-179:~$ sudo su nurse_jane
$ whoami
nurse_jane
```

• 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.

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

Ans - usermod -aG sudo dr_smith

```
ubuntu@ip-172-31-26-179:~$ sudo su nurse_jane
$ whoami
nurse_jane
```

• Provide an example command Dr. Smith would use to restart the service with sudo.
• 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.
Ans- sudo chmod 100 ./secure/patients

Ans- sudo setfacl -m u:dr_smith:x ./secure/patients

```
user:dr_smith:--x
```

• 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.

Ans- chown dr_smith ./secure/patients
Ans- chown :nurse_john ./secure/patinets
Ans- chown dr_smith:nurse_john ./secure/patients

```
ubuntu@ip-172-31-26-179:~$ sudo getfacl ./secure/patients/
# file: secure/patients/
# owner: dr_smith
# group: nurse_jane
```

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

Ans- sudo deluser sudo dr_smith

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

Ans- sudo cat /etc/group | grep sudo

```
ubuntu@ip-172-31-26-179:~$ sudo cat /etc/group | grep sudo
sudo:x:27:ubuntu
```

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).

Ans- sudo useradd davida

Sudo useradd lisab

Sudo useradd nina

Sudo useradd tom

Sudo groupadd alpha

Sudo groupadd beta

Sudo usermod -aG beta nina

Sudo usermod -aG beta tom

Sudo usermod -aG alpha davida

Sudo usermod -aG alpha lisabcd

```
alpha:x:2011:davida,lisab
beta:x:2012:nina,tom
```

• Cross-Project Access:

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

Ans- sudo usermod -aG beta davida

```
beta:x:2012:nina,tom,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.

Ans- sudo usermod -s /bin/zsh davida

Ans- sudo usermod -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.

Ans- sudo gpasswd -d tom beta

Groups tom

```
ubuntu@ip-172-31-26-179:/$ groups tom
tom : tom
```

• Create a Shared Admin Group:

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

Ans- sudo groupadd admin_alpha

Sudo groupadd admin_beta

• Add yourself to both groups for administrative purposes.

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.

Ans- sudo useradd -m emma_w

Sudo passwd emm_w

• 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.

Ans- sudo gpasswd -a emma_w sudo

```
ubuntu@ip-172-31-26-179:/home$ sudo cat /etc/group | grep sudo
sudo:x:27:ubuntu,emma_w
```

• 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.

• 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.

Ans- sudo useradd john_d

Sudo passwd john_d

Sudo su john_d

• 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.

Ans- sudo chown emma_w /home/emma_w/scripts

Sudo chmod 700 /home/emma_w/scripts

• 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.

Ans- sudo chown :emma_w /home/emma_w/sctipts

```
emma_w@ip-172-31-26-179:~$ getfacl /home/emma_w/scripts/
getfacl: Removing leading '/' from absolute path names
# file: home/emma_w/scripts/
# owner: emma_w
# group: emma_w
user::rwx
group::---
other::---
```

• Remove Temporary Privileges:

• After the system update is complete, revoke Emma's sudo privileges to maintain security.

Ans- sudo gpasswd -d emma_w sudo

Document the process to ensure the removal is verified.

Ans- sudo cat /etc/group | grep sudo

```
emma_w@ip-172-31-26-179:~$ sudo cat /etc/group | grep sudo
sudo:x:27:ubuntu
```

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.

Ans- sudo sueradd mike_b

Sudo passwd mike_b

Sudo chage -M 90 mike_b

```
ubuntu@ip-172-31-26-179:/$ sudo chage -l mike_b
Last password change                                    : Oct 02, 2024
Password expires                                        : Dec 31, 2024
```

• 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.

Ans- mkdir -p /projects/alpha

Sudo chown mike_b ./projetcs/alpha

Sudo chmod 700 ./projetcs/alpha

```
ubuntu@ip-172-31-26-179:~$ getfacl ./projects/alpha/
# file: projects/alpha/
# owner: mike_b
# group: ubuntu
user::rwx
```

• 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.

Ans- sudo useradd sara_c

Sudo passwd sara_c

Sudo su sara_c

• Grant Limited Administrative Access:

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

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

Ans- sudo usermod -aG sudo mike_b

```
ubuntu@ip-172-31-26-179:~$ sudo cat /etc/group | grep sudo
sudo:x:27:ubuntu,mike_b
```

• 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.

Ans- suod chown :devteam ./projects/alpha

```
ubuntu@ip-172-31-26-179:~$ getfacl ./projects/alpha/
# file: projects/alpha/
# owner: mike_b
# group: devteam
```

• 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.

Ans- sudo gpasswd -d mike_b sudo

Document the steps to verify these changes.
Ans- sudo cat /etc/passwd | grep sudo

```
ubuntu@ip-172-31-26-179:~$ sudo cat /etc/group | grep sudo
sudo:x:27:ubuntu
```