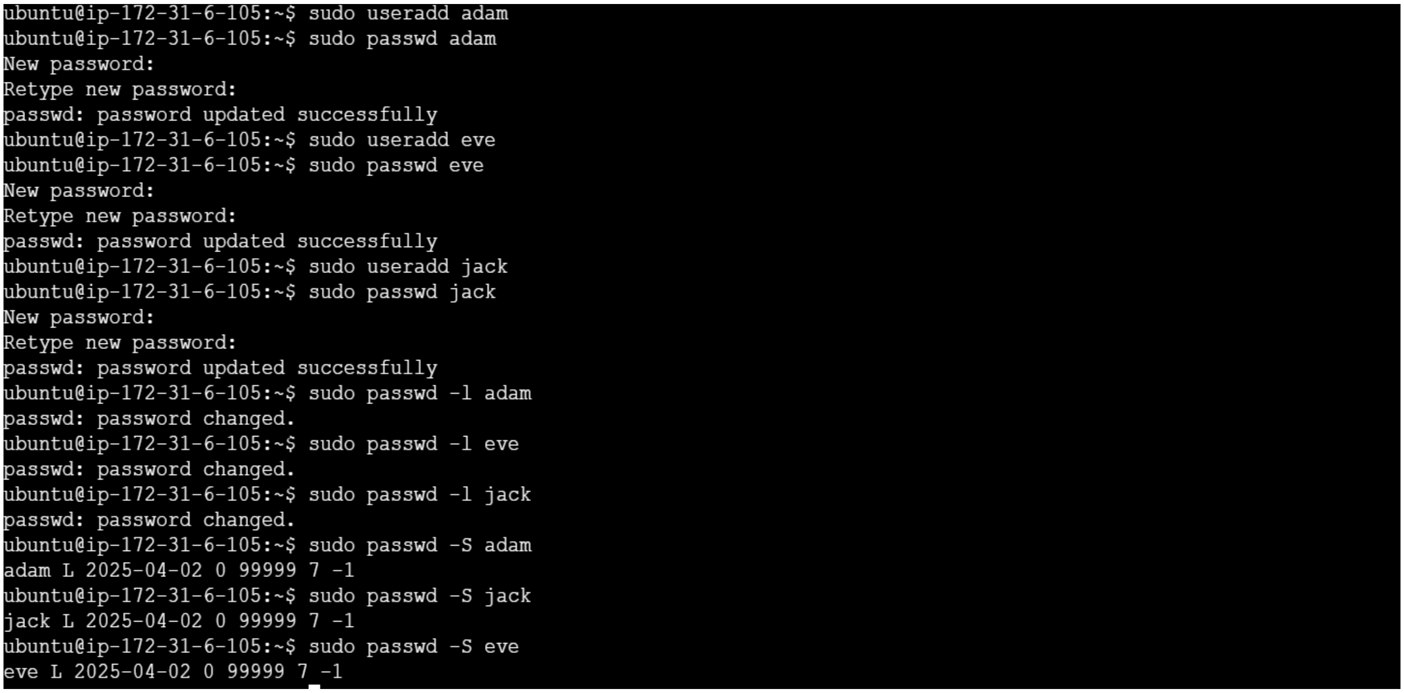
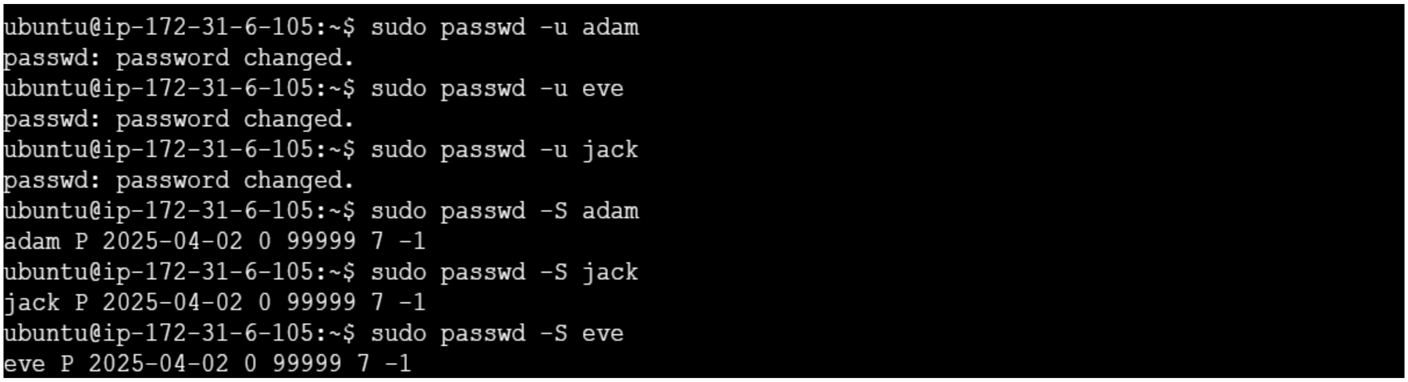
QUESTION 1 Due to a security incident, you need to take immediate action to lock down certain user accounts and enforce stricter password policies. Requirements: Lock User Accounts: Lock the accounts of users: Adam (adam), Eve (eve), and Jack (jack) to prevent them from logging in during the investigation. Enforce Strong Password Policies: Set a minimum password length of 12 characters for all users. Require all users to change their passwords immediately. Account Auditing: Generate a list of all user accounts and their password status.

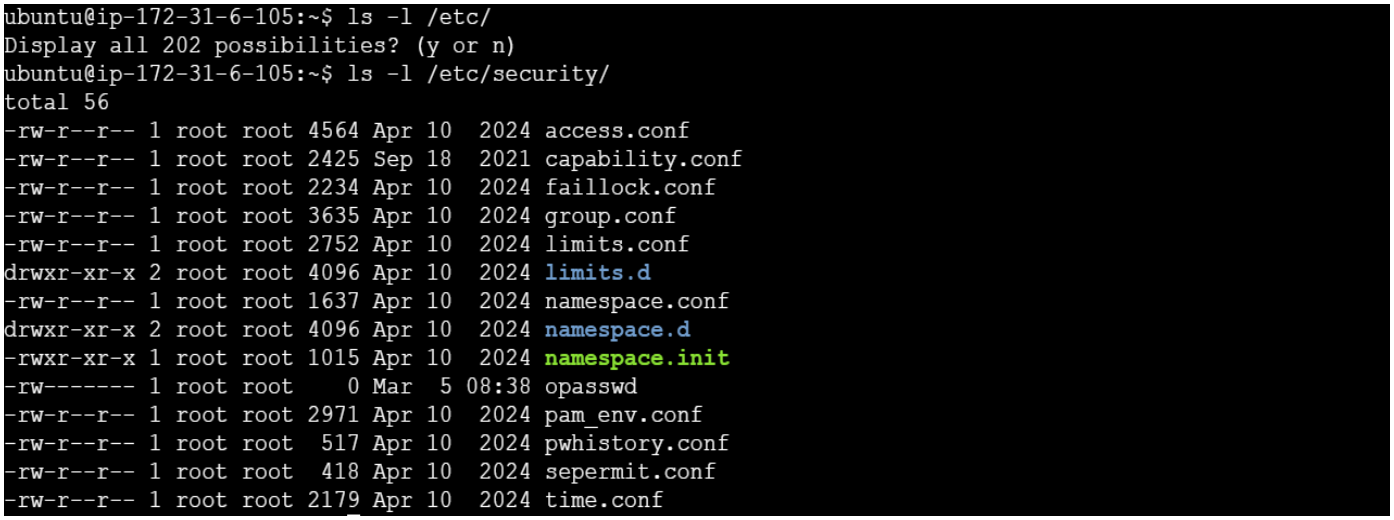
Solution:



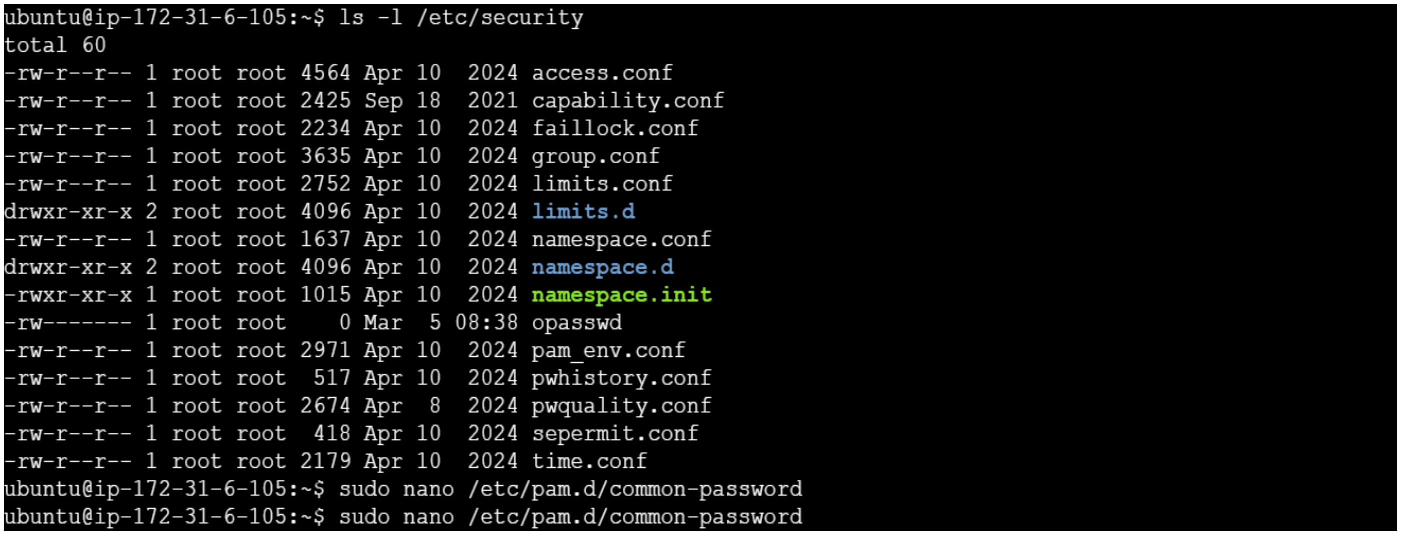
```
ubuntu@ip-172-31-6-105:~$ sudo useradd adam
ubuntu@ip-172-31-6-105:~$ sudo passwd adam
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-6-105:~$ sudo useradd eve
ubuntu@ip-172-31-6-105:~$ sudo passwd eve
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-6-105:~$ sudo useradd jack
ubuntu@ip-172-31-6-105:~$ sudo passwd jack
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-6-105:~$ sudo passwd -l adam
passwd: password changed.
ubuntu@ip-172-31-6-105:~$ sudo passwd -l eve
passwd: password changed.
ubuntu@ip-172-31-6-105:~$ sudo passwd -l jack
passwd: password changed.
ubuntu@ip-172-31-6-105:~$ sudo passwd -S adam
adam L 2025-04-02 0 99999 7 -1
ubuntu@ip-172-31-6-105:~$ sudo passwd -S jack
jack L 2025-04-02 0 99999 7 -1
ubuntu@ip-172-31-6-105:~$ sudo passwd -S eve
eve L 2025-04-02 0 99999 7 -1
```



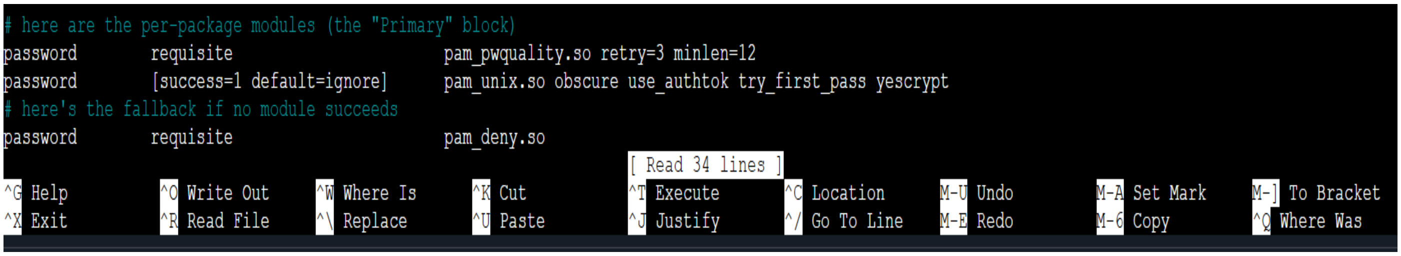
```
ubuntu@ip-172-31-6-105:~$ sudo passwd -u adam
passwd: password changed.
ubuntu@ip-172-31-6-105:~$ sudo passwd -u eve
passwd: password changed.
ubuntu@ip-172-31-6-105:~$ sudo passwd -u jack
passwd: password changed.
ubuntu@ip-172-31-6-105:~$ sudo passwd -S adam
adam P 2025-04-02 0 99999 7 -1
ubuntu@ip-172-31-6-105:~$ sudo passwd -S jack
jack P 2025-04-02 0 99999 7 -1
ubuntu@ip-172-31-6-105:~$ sudo passwd -S eve
eve P 2025-04-02 0 99999 7 -1
```



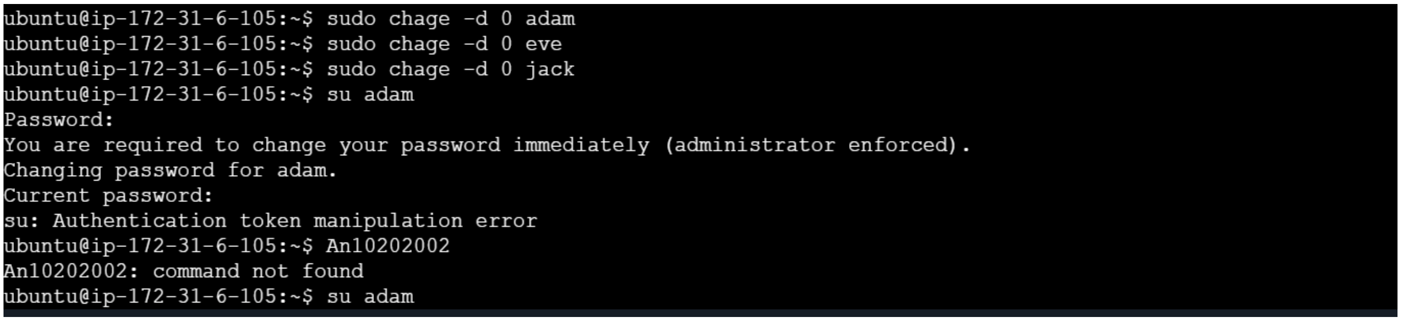
```
ubuntu@ip-172-31-6-105:~$ ls -l /etc/
Display all 202 possibilities? (y or n)
ubuntu@ip-172-31-6-105:~$ ls -l /etc/security/
total 56
-rw-r--r-- 1 root root 4564 Apr 10  2024 access.conf
-rw-r--r-- 1 root root 2425 Sep 18  2021 capability.conf
-rw-r--r-- 1 root root 2234 Apr 10  2024 faillock.conf
-rw-r--r-- 1 root root 3635 Apr 10  2024 group.conf
-rw-r--r-- 1 root root 2752 Apr 10  2024 limits.conf
drwxr-xr-x 2 root root 4096 Apr 10  2024 limits.d
-rw-r--r-- 1 root root 1637 Apr 10  2024 namespace.conf
drwxr-xr-x 2 root root 4096 Apr 10  2024 namespace.d
-rwxr-xr-x 1 root root 1015 Apr 10  2024 namespace.init
-rw------- 1 root root    0 Mar  5 08:38 opasswd
-rw-r--r-- 1 root root 2971 Apr 10  2024 pam_env.conf
-rw-r--r-- 1 root root  517 Apr 10  2024 pwhistory.conf
-rw-r--r-- 1 root root  418 Apr 10  2024 sepermit.conf
-rw-r--r-- 1 root root 2179 Apr 10  2024 time.conf
```



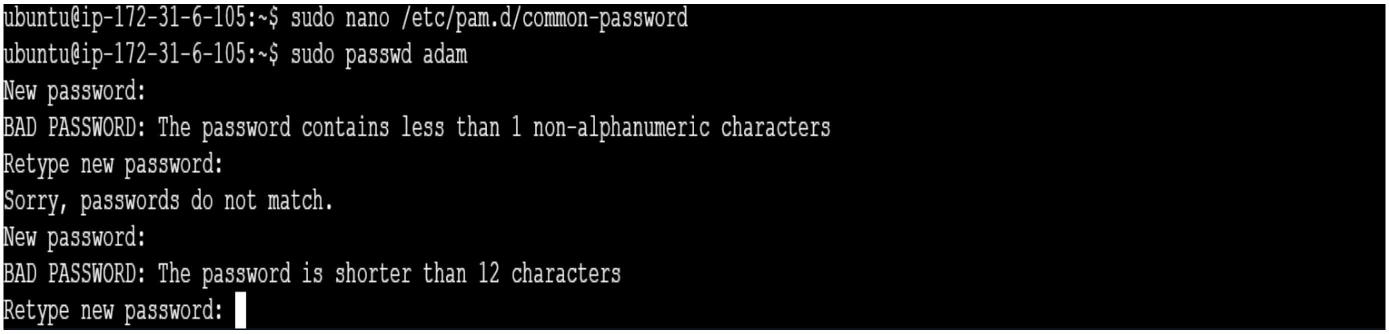
```
ubuntu@ip-172-31-6-105:~$ ls -l /etc/security
total 60
-rw-r--r-- 1 root root 4564 Apr 10  2024 access.conf
-rw-r--r-- 1 root root 2425 Sep 18  2021 capability.conf
-rw-r--r-- 1 root root 2234 Apr 10  2024 faillock.conf
-rw-r--r-- 1 root root 3635 Apr 10  2024 group.conf
-rw-r--r-- 1 root root 2752 Apr 10  2024 limits.conf
drwxr-xr-x 2 root root 4096 Apr 10  2024 limits.d
-rw-r--r-- 1 root root 1637 Apr 10  2024 namespace.conf
drwxr-xr-x 2 root root 4096 Apr 10  2024 namespace.d
-rwxr-xr-x 1 root root 1015 Apr 10  2024 namespace.init
-rw------- 1 root root    0 Mar  5 08:38 opasswd
-rw-r--r-- 1 root root 2971 Apr 10  2024 pam_env.conf
-rw-r--r-- 1 root root  517 Apr 10  2024 pwhistory.conf
-rw-r--r-- 1 root root 2674 Apr  8  2024 pwquality.conf
-rw-r--r-- 1 root root  418 Apr 10  2024 sepermit.conf
-rw-r--r-- 1 root root 2179 Apr 10  2024 time.conf
ubuntu@ip-172-31-6-105:~$ sudo nano /etc/pam.d/common-password
ubuntu@ip-172-31-6-105:~$ sudo nano /etc/pam.d/common-password
```



```
# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so retry=3 minlen=12
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yescrypt
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
                                          [ Read 34 lines ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark   M-] To Bracket
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy       ^Q Where Was
```



```
ubuntu@ip-172-31-6-105:~$ sudo chage -d 0 adam
ubuntu@ip-172-31-6-105:~$ sudo chage -d 0 eve
ubuntu@ip-172-31-6-105:~$ sudo chage -d 0 jack
ubuntu@ip-172-31-6-105:~$ su adam
Password:
You are required to change your password immediately (administrator enforced).
Changing password for adam.
Current password:
su: Authentication token manipulation error
ubuntu@ip-172-31-6-105:~$ An10202002
An10202002: command not found
ubuntu@ip-172-31-6-105:~$ su adam
```



```
ubuntu@ip-172-31-6-105:~$ sudo nano /etc/pam.d/common-password
ubuntu@ip-172-31-6-105:~$ sudo passwd adam
New password:
BAD PASSWORD: The password contains less than 1 non-alphanumeric characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password is shorter than 12 characters
Retype new password:
```

If the file /etc/security/pwquality.conf is missing or not working, you may need to install libpam-pwquality.

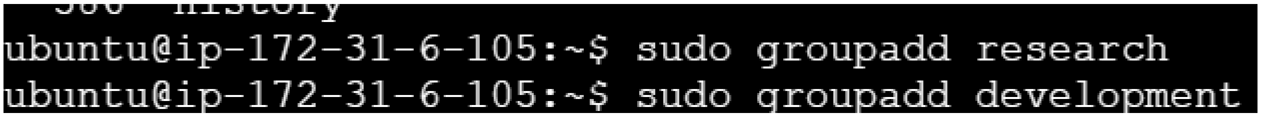
Go to pwquality.conf file and update minlen policy and enforce for root.

Use chage –d 0 to make user immediately change the password.

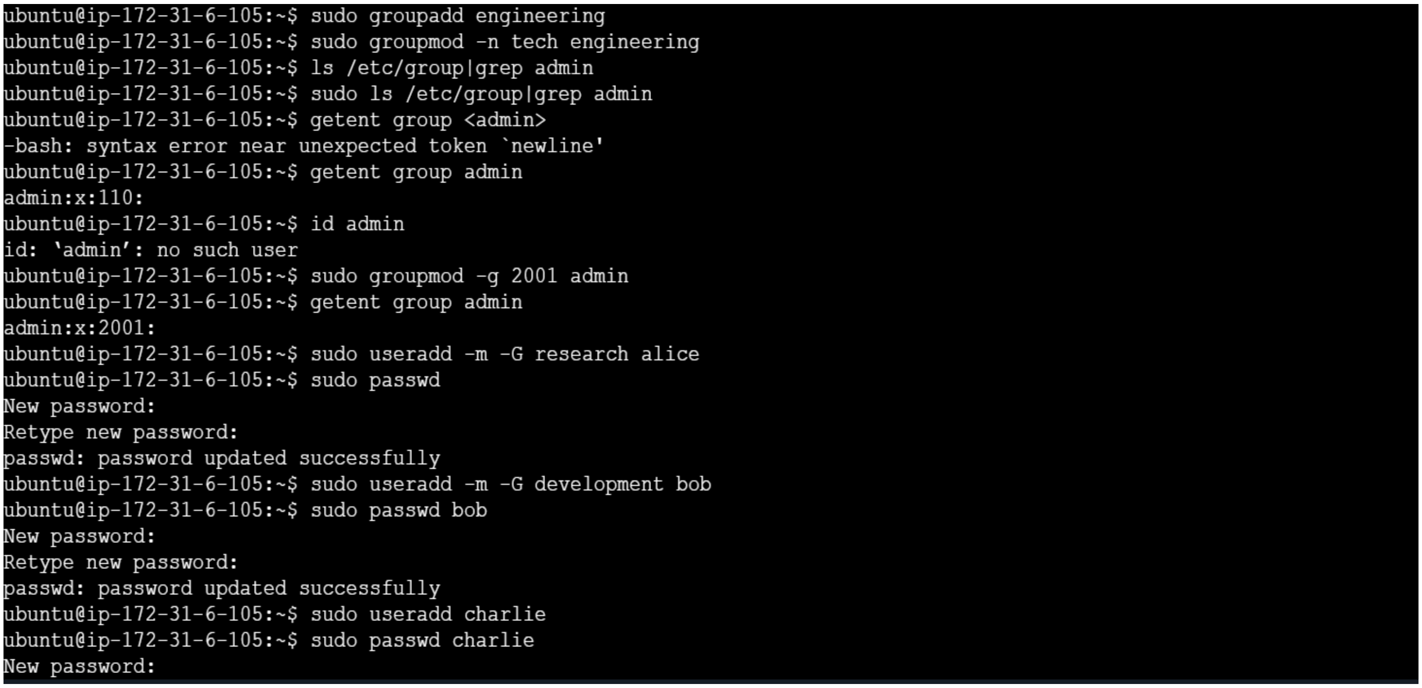
Using cut command to show the username and password. The ! Mark after name indicates that the user is locked.

Further the users can be unlocked by using chage –u username after the investigation.

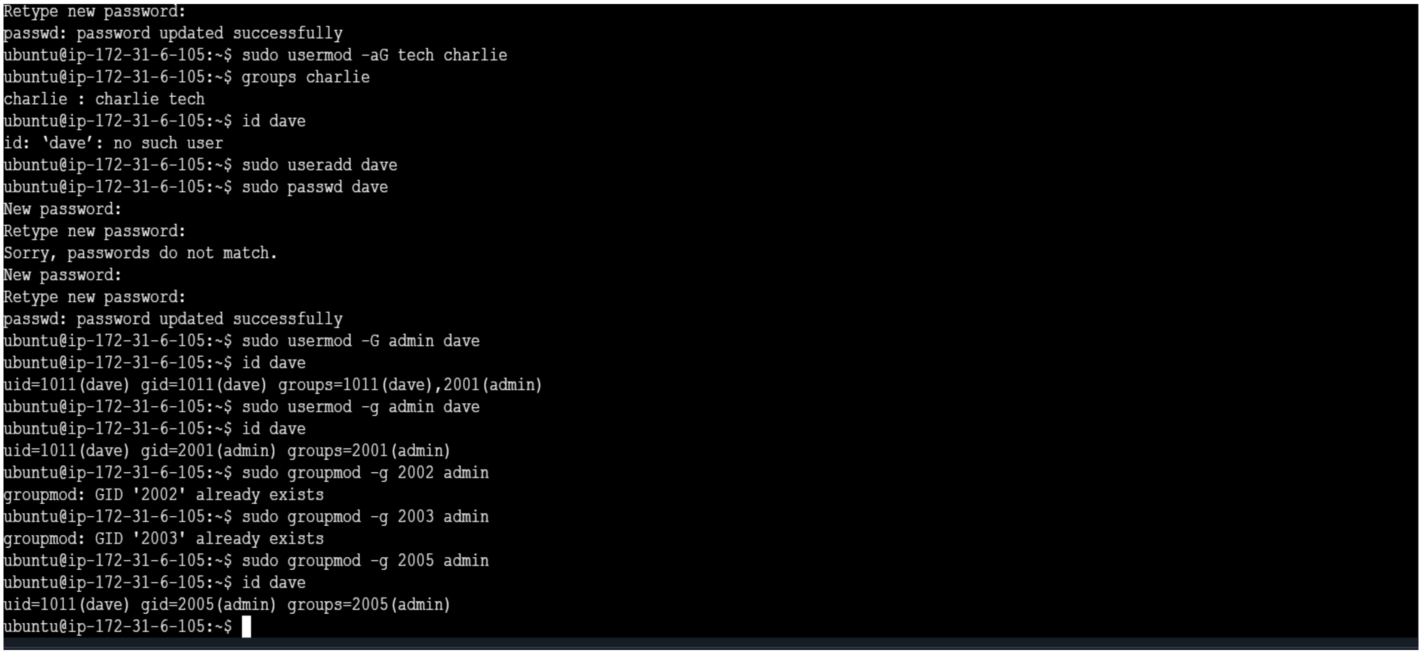
QUESTION 2 Scenario: You are the system administrator for a medium-sized company that uses a Linux-based server for its internal operations. Your company has recently undergone a reorganization, and there is a need to update the user groups to reflect the new structure. The following changes are required: 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. 2. Rename the engineering group to tech. 3. Change the group ID of admin to 2001. 4. Create new user accounts for Alice and Bob, and add them to the respective groups. 5. Ensure Charlie is added to the tech group and confirm his membership. 6. Ensure Dave remains in the admin group after the group ID change.



```
  308  history
ubuntu@ip-172-31-6-105:~$ sudo groupadd research
ubuntu@ip-172-31-6-105:~$ sudo groupadd development
```



```
ubuntu@ip-172-31-6-105:~$ sudo groupadd engineering
ubuntu@ip-172-31-6-105:~$ sudo groupmod -n tech engineering
ubuntu@ip-172-31-6-105:~$ ls /etc/group|grep admin
ubuntu@ip-172-31-6-105:~$ sudo ls /etc/group|grep admin
ubuntu@ip-172-31-6-105:~$ getent group <admin>
-bash: syntax error near unexpected token `newline'
ubuntu@ip-172-31-6-105:~$ getent group admin
admin:x:110:
ubuntu@ip-172-31-6-105:~$ id admin
id: ‘admin’: no such user
ubuntu@ip-172-31-6-105:~$ sudo groupmod -g 2001 admin
ubuntu@ip-172-31-6-105:~$ getent group admin
admin:x:2001:
ubuntu@ip-172-31-6-105:~$ sudo useradd -m -G research alice
ubuntu@ip-172-31-6-105:~$ sudo passwd
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-6-105:~$ sudo useradd -m -G development bob
ubuntu@ip-172-31-6-105:~$ sudo passwd bob
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-6-105:~$ sudo useradd charlie
ubuntu@ip-172-31-6-105:~$ sudo passwd charlie
New password:
```

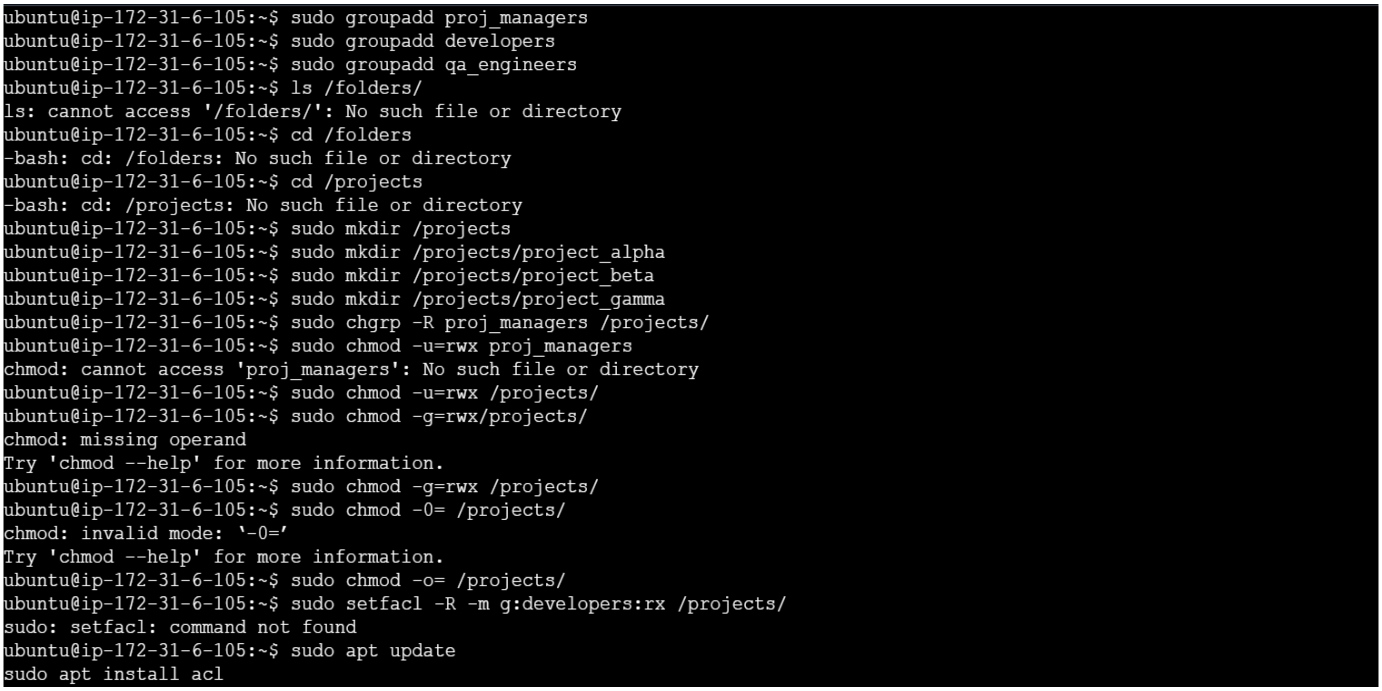


```
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-6-105:~$ sudo usermod -aG tech charlie
ubuntu@ip-172-31-6-105:~$ groups charlie
charlie : charlie tech
ubuntu@ip-172-31-6-105:~$ id dave
id: ‘dave’: no such user
ubuntu@ip-172-31-6-105:~$ sudo useradd dave
ubuntu@ip-172-31-6-105:~$ sudo passwd dave
New password:
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-6-105:~$ sudo usermod -G admin dave
ubuntu@ip-172-31-6-105:~$ id dave
uid=1011(dave) gid=1011(dave) groups=1011(dave),2001(admin)
ubuntu@ip-172-31-6-105:~$ sudo usermod -g admin dave
ubuntu@ip-172-31-6-105:~$ id dave
uid=1011(dave) gid=2001(admin) groups=2001(admin)
ubuntu@ip-172-31-6-105:~$ sudo groupmod -g 2002 admin
groupmod: GID '2002' already exists
ubuntu@ip-172-31-6-105:~$ sudo groupmod -g 2003 admin
groupmod: GID '2003' already exists
ubuntu@ip-172-31-6-105:~$ sudo groupmod -g 2005 admin
ubuntu@ip-172-31-6-105:~$ id dave
uid=1011(dave) gid=2005(admin) groups=2005(admin)
ubuntu@ip-172-31-6-105:~$ █
```

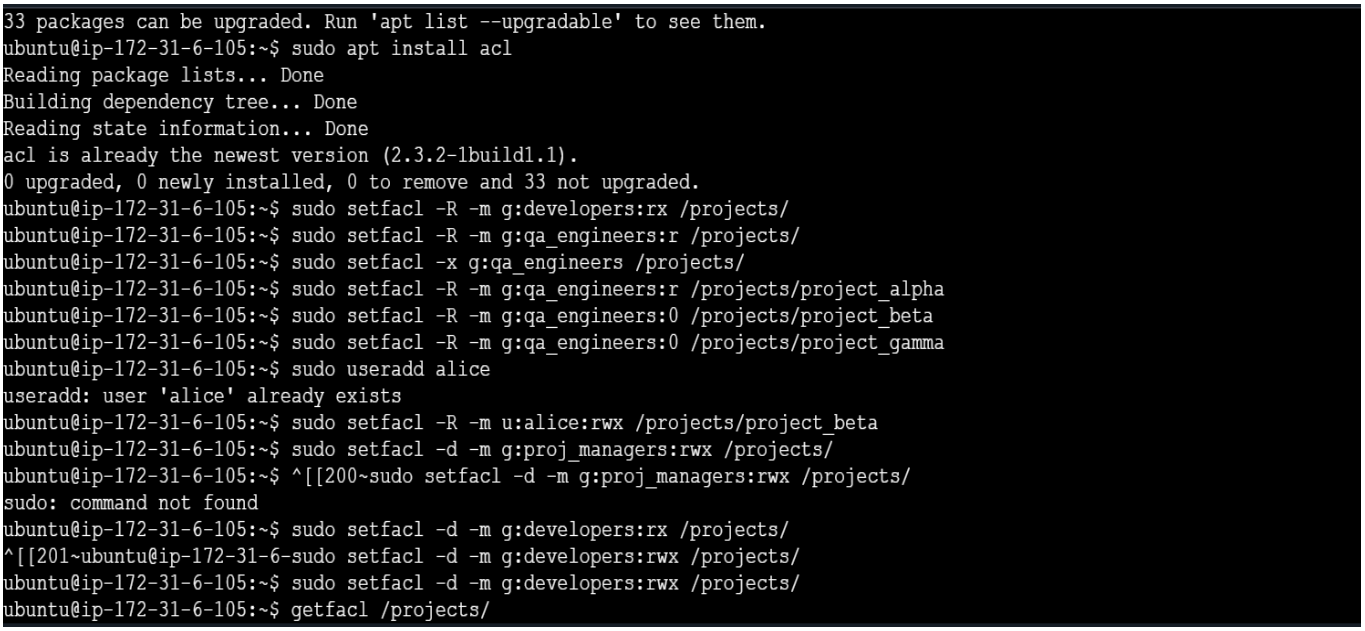
1. Create the groups research, development, engineering, and tech.
2. Check if the admin group exists and change its group ID to 2001.
3. Create the users alice, bob, charlie, and dave.
4. Add alice to the research group and bob to the development group.
5. Add charlie to the tech group.
6. Set passwords for all the users.
7. Add dave to the admin group as a secondary group, then make it his primary group.

8. Attempt changing the admin group’s ID multiple times due to conflicts and finally set it to 2005.
9. Verify user and group details using id and groups commands.

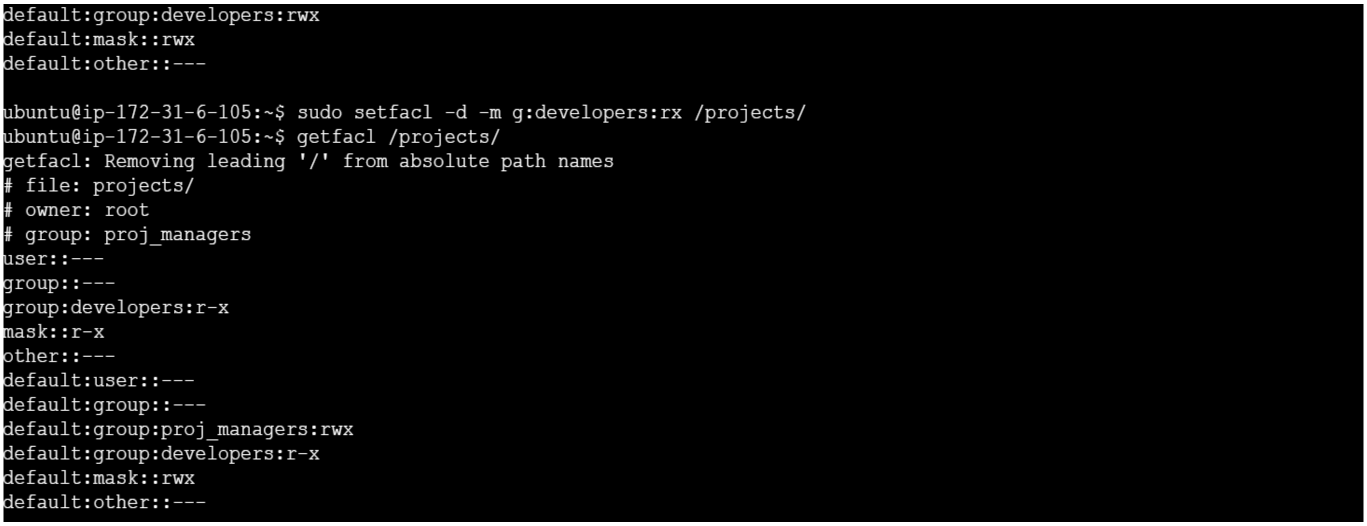
QUESTION 3 You are a system administrator managing a shared directory /projects on a Linux server used by different teams in your organization. The directory contains subdirectories for different projects, and each project directory needs specific access permissions for different users and groups. *Requirements:* 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



```
ubuntu@ip-172-31-6-105:~$ sudo groupadd proj_managers
ubuntu@ip-172-31-6-105:~$ sudo groupadd developers
ubuntu@ip-172-31-6-105:~$ sudo groupadd qa_engineers
ubuntu@ip-172-31-6-105:~$ ls /folders/
ls: cannot access '/folders/': No such file or directory
ubuntu@ip-172-31-6-105:~$ cd /folders
-bash: cd: /folders: No such file or directory
ubuntu@ip-172-31-6-105:~$ cd /projects
-bash: cd: /projects: No such file or directory
ubuntu@ip-172-31-6-105:~$ sudo mkdir /projects
ubuntu@ip-172-31-6-105:~$ sudo mkdir /projects/project_alpha
ubuntu@ip-172-31-6-105:~$ sudo mkdir /projects/project_beta
ubuntu@ip-172-31-6-105:~$ sudo mkdir /projects/project_gamma
ubuntu@ip-172-31-6-105:~$ sudo chgrp -R proj_managers /projects/
ubuntu@ip-172-31-6-105:~$ sudo chmod -u=rwx proj_managers
chmod: cannot access 'proj_managers': No such file or directory
ubuntu@ip-172-31-6-105:~$ sudo chmod -u=rwx /projects/
ubuntu@ip-172-31-6-105:~$ sudo chmod -g=rwx/projects/
chmod: missing operand
Try 'chmod --help' for more information.
ubuntu@ip-172-31-6-105:~$ sudo chmod -g=rwx /projects/
ubuntu@ip-172-31-6-105:~$ sudo chmod -0= /projects/
chmod: invalid mode: ‘-0=’
Try 'chmod --help' for more information.
ubuntu@ip-172-31-6-105:~$ sudo chmod -o= /projects/
ubuntu@ip-172-31-6-105:~$ sudo setfacl -R -m g:developers:rx /projects/
sudo: setfacl: command not found
ubuntu@ip-172-31-6-105:~$ sudo apt update
sudo apt install acl
```



```
33 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-172-31-6-105:~$ sudo apt install acl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
acl is already the newest version (2.3.2-1build1.1).
0 upgraded, 0 newly installed, 0 to remove and 33 not upgraded.
ubuntu@ip-172-31-6-105:~$ sudo setfacl -R -m g:developers:rx /projects/
ubuntu@ip-172-31-6-105:~$ sudo setfacl -R -m g:qa_engineers:r /projects/
ubuntu@ip-172-31-6-105:~$ sudo setfacl -x g:qa_engineers /projects/
ubuntu@ip-172-31-6-105:~$ sudo setfacl -R -m g:qa_engineers:r /projects/project_alpha
ubuntu@ip-172-31-6-105:~$ sudo setfacl -R -m g:qa_engineers:0 /projects/project_beta
ubuntu@ip-172-31-6-105:~$ sudo setfacl -R -m g:qa_engineers:0 /projects/project_gamma
ubuntu@ip-172-31-6-105:~$ sudo useradd alice
useradd: user 'alice' already exists
ubuntu@ip-172-31-6-105:~$ sudo setfacl -R -m u:alice:rwx /projects/project_beta
ubuntu@ip-172-31-6-105:~$ sudo setfacl -d -m g:proj_managers:rwx /projects/
ubuntu@ip-172-31-6-105:~$ ^[[200~sudo setfacl -d -m g:proj_managers:rwx /projects/
sudo: command not found
ubuntu@ip-172-31-6-105:~$ sudo setfacl -d -m g:developers:rx /projects/
^[[201~ubuntu@ip-172-31-6-sudo setfacl -d -m g:developers:rwx /projects/
ubuntu@ip-172-31-6-105:~$ sudo setfacl -d -m g:developers:rwx /projects/
ubuntu@ip-172-31-6-105:~$ getfacl /projects/
```



```
default:group:developers:rwx
default:mask::rwx
default:other::---

ubuntu@ip-172-31-6-105:~$ sudo setfacl -d -m g:developers:rx /projects/
ubuntu@ip-172-31-6-105:~$ getfacl /projects/
getfacl: Removing leading '/' from absolute path names
# file: projects/
# owner: root
# group: proj_managers
user::---
group::---
group:developers:r-x
mask::r-x
other::---
default:user::---
default:group::---
default:group:proj_managers:rwx
default:group:developers:r-x
default:mask::rwx
default:other::---
```

1. Create the groups proj_managers, developers, and qa_engineers.
2. Create the projects directory along with subdirectories project_alpha, project_beta, and project_gamma.
3. Change the group ownership of the projects directory to proj_managers.
4. Attempt to change permissions using chmod, with some corrections due to errors.
5. Install the acl package to manage advanced permissions.
6. Set read and execute permissions for the developers group on the projects directory.
7. Set read-only access for the qa_engineers group on the projects directory and project_alpha, and remove access from project_beta and project_gamma.
8. Assign full access to alice on the project_beta directory.
9. Grant full access to the proj_managers group on the projects directory.
10. Set default ACLs so that new files and folders under projects inherit group permissions.
11. Use getfacl to verify that the ACL settings are correctly applied.