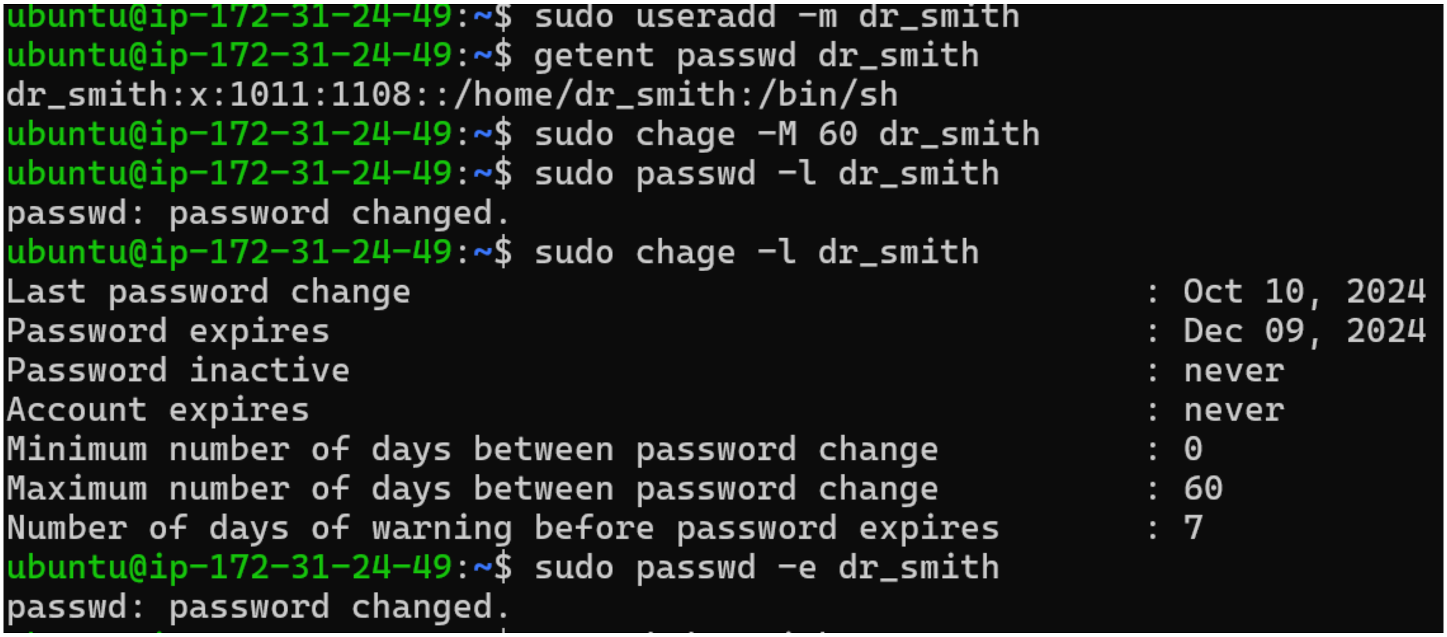
Assignment On User Management Commands

Scenario: You are managing a Linux server in a healthcare environment where data sensitivity is crucial.

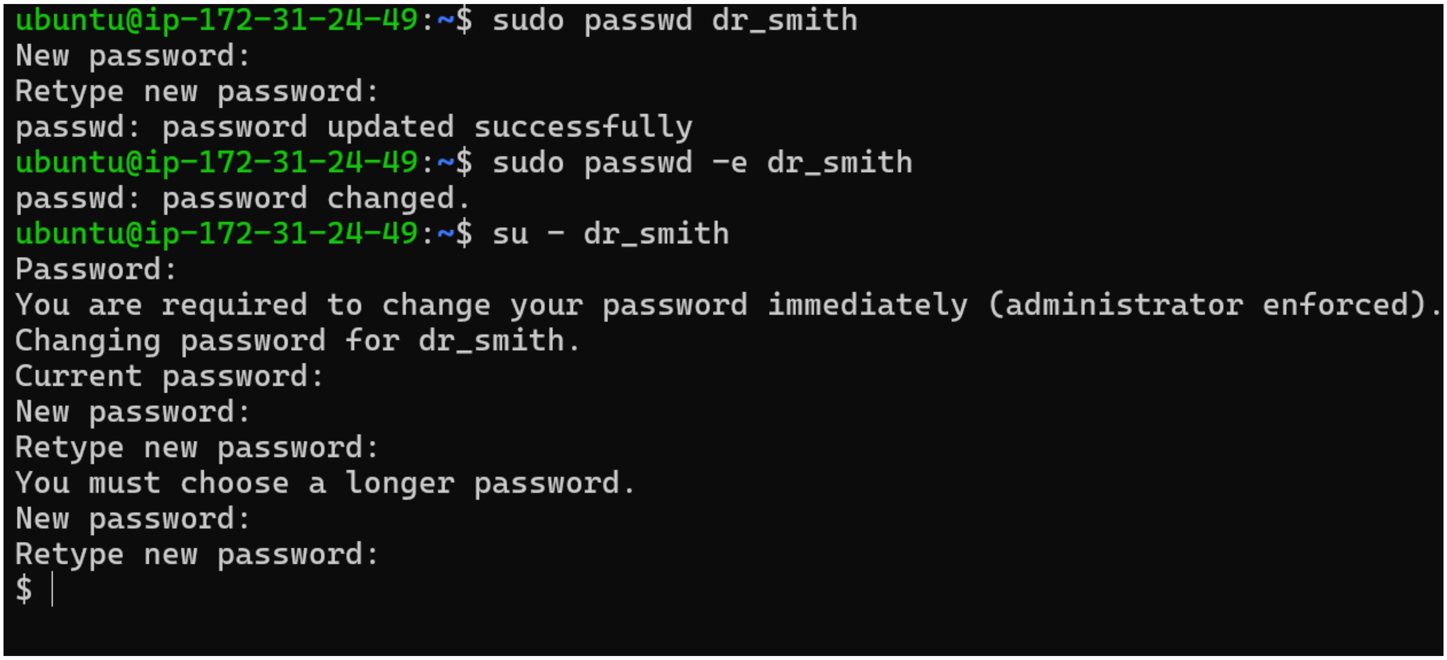
1. Enforce Password Policies:

* 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.



```
ubuntu@ip-172-31-24-49:~$ sudo useradd -m dr_smith
ubuntu@ip-172-31-24-49:~$ getent passwd dr_smith
dr_smith:x:1011:1108::/home/dr_smith:/bin/sh
ubuntu@ip-172-31-24-49:~$ sudo chage -M 60 dr_smith
ubuntu@ip-172-31-24-49:~$ sudo passwd -l dr_smith
passwd: password changed.
ubuntu@ip-172-31-24-49:~$ sudo chage -l dr_smith
Last password change                                    : Oct 10, 2024
Password expires                                        : Dec 09, 2024
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 60
Number of days of warning before password expires       : 7
ubuntu@ip-172-31-24-49:~$ sudo passwd -e dr_smith
passwd: password changed.
```

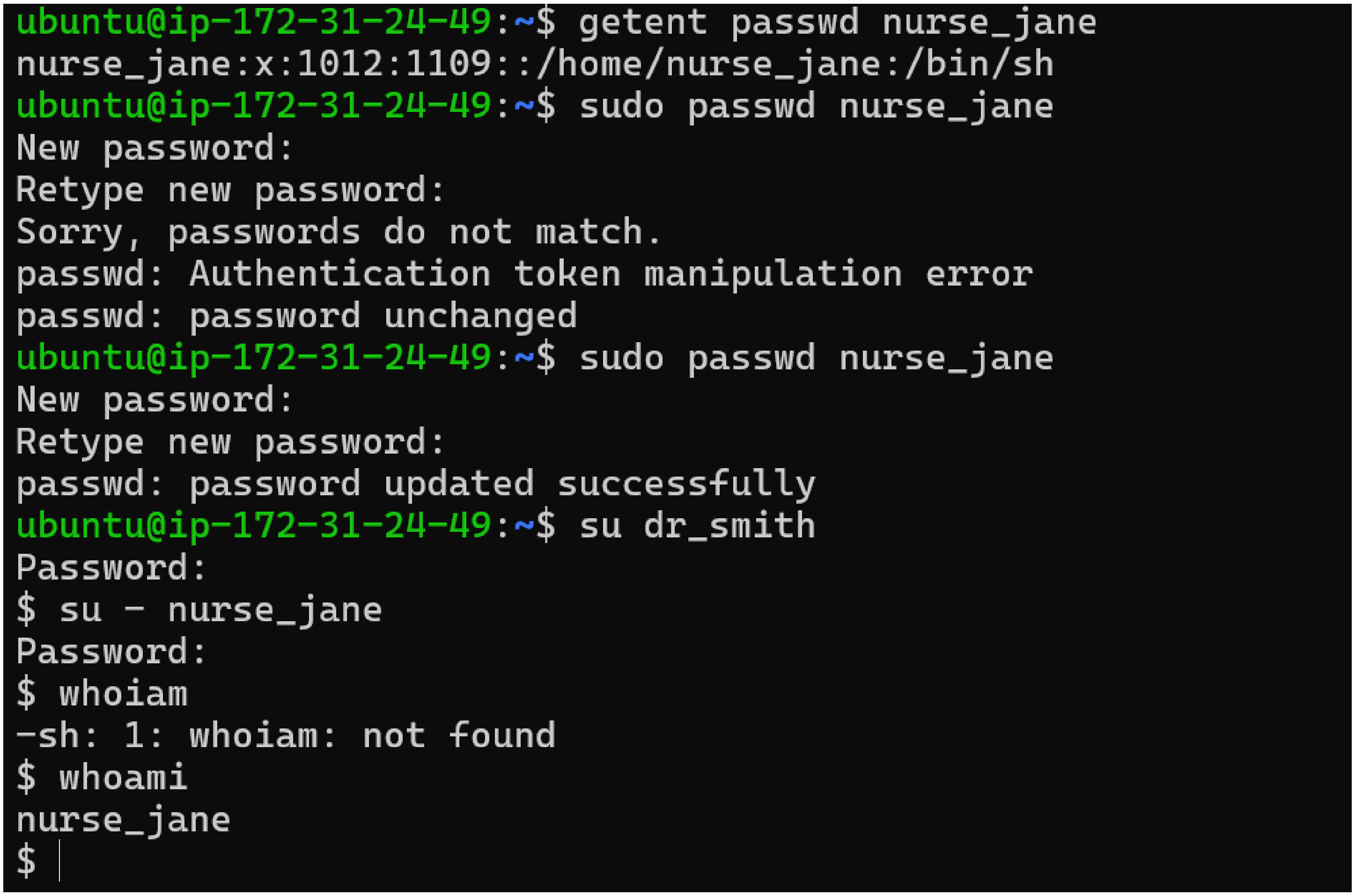
* Ensure that Dr. Smith is prompted to change the password the next time he logs in.



```
ubuntu@ip-172-31-24-49:~$ sudo passwd dr_smith
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-24-49:~$ sudo passwd -e dr_smith
passwd: password changed.
ubuntu@ip-172-31-24-49:~$ su - dr_smith
Password:
You are required to change your password immediately (administrator enforced).
Changing password for dr_smith.
Current password:
New password:
Retype new password:
You must choose a longer password.
New password:
Retype new password:
$ 
```

2. 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.

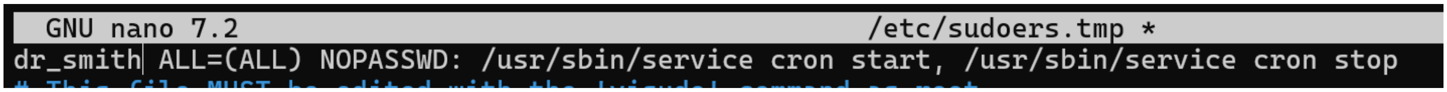


```
ubuntu@ip-172-31-24-49:~$ getent passwd nurse_jane
nurse_jane:x:1012:1109::/home/nurse_jane:/bin/sh
ubuntu@ip-172-31-24-49:~$ sudo passwd nurse_jane
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
ubuntu@ip-172-31-24-49:~$ sudo passwd nurse_jane
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-24-49:~$ su dr_smith
Password:
$ su - nurse_jane
Password:
$ whoiam
-sh: 1: whoiam: not found
$ whoami
nurse_jane
$ 
```

* Guide Dr. Smith on how to use su to switch to Nurse Jane’s account and emphasize the importance of logging out afterward.

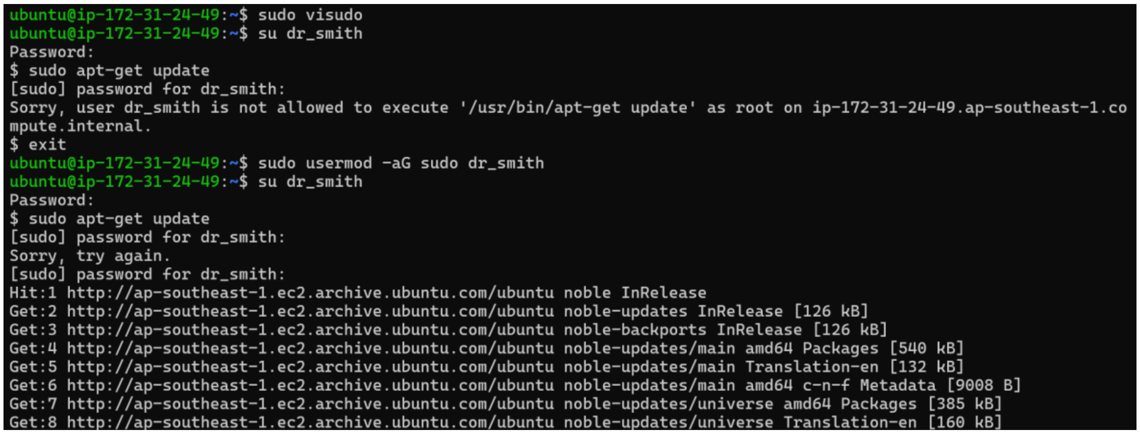
3. Granting Administrative Rights with sudo:

* 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.



```
  GNU nano 7.2                                      /etc/sudoers.tmp *
dr_smith ALL=(ALL) NOPASSWD: /usr/sbin/service cron start, /usr/sbin/service cron stop
# This file MUST be edited with the 'visudo' command as root
```

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

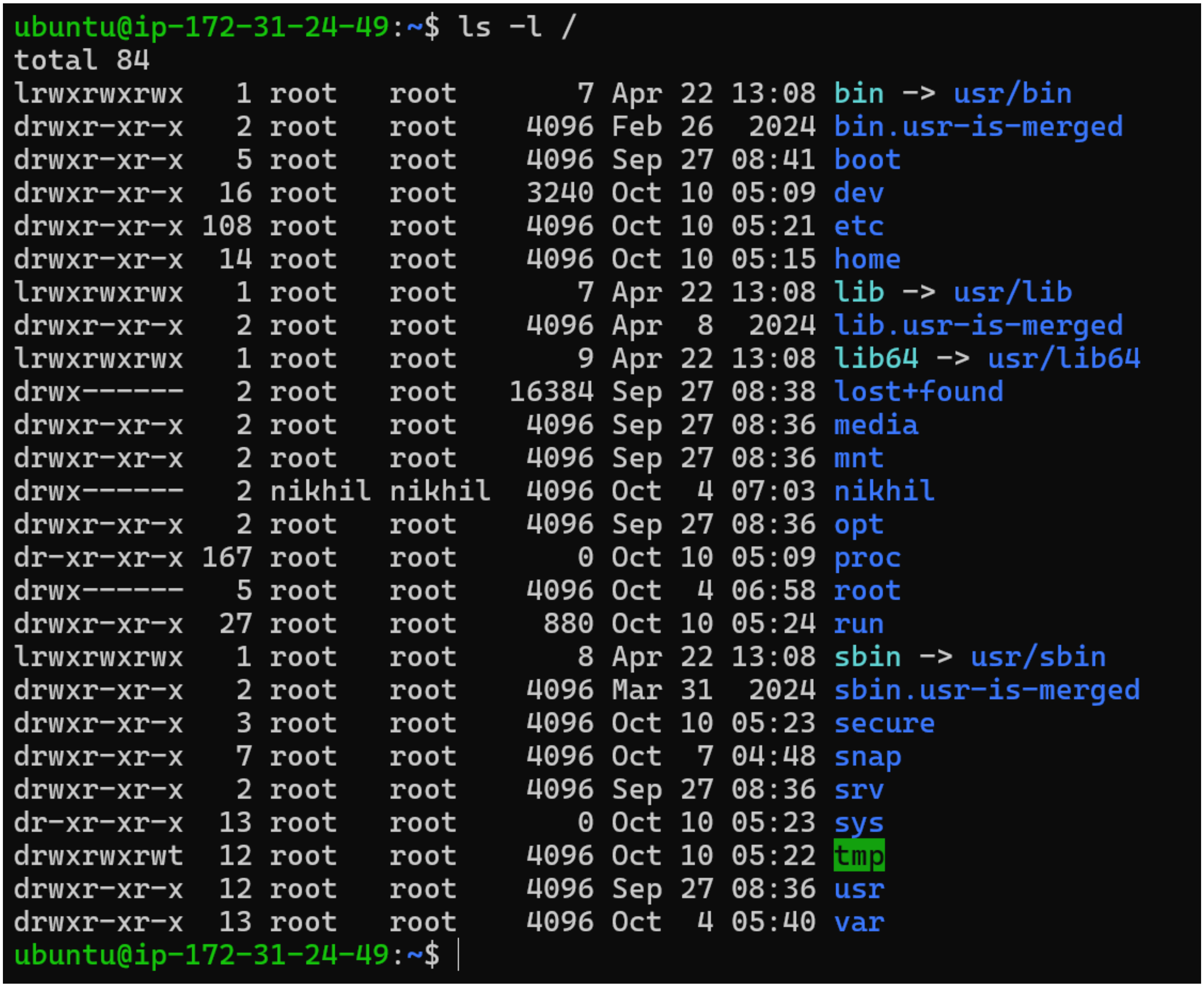


```
ubuntu@ip-172-31-24-49:~$ sudo visudo
ubuntu@ip-172-31-24-49:~$ su dr_smith
Password:
$ sudo apt-get update
[sudo] password for dr_smith:
Sorry, user dr_smith is not allowed to execute '/usr/bin/apt-get update' as root on ip-172-31-24-49.ap-southeast-1.co
mpute.internal.
$ exit
ubuntu@ip-172-31-24-49:~$ sudo usermod -aG sudo dr_smith
ubuntu@ip-172-31-24-49:~$ su dr_smith
Password:
$ sudo apt-get update
[sudo] password for dr_smith:
Sorry, try again.
[sudo] password for dr_smith:
Hit:1 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [540 kB]
Get:5 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [132 kB]
Get:6 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [9008 B]
Get:7 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [385 kB]
Get:8 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [160 kB]
```

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

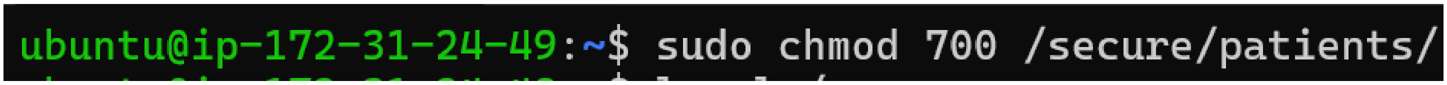
4. Setting Permissions on Sensitive Files:

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

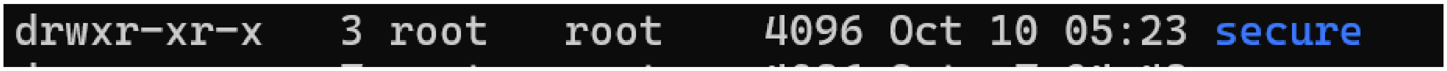


```
ubuntu@ip-172-31-24-49:~$ ls -l /
total 84
lrwxrwxrwx   1 root   root       7 Apr 22 13:08 bin -> usr/bin
drwxr-xr-x   2 root   root    4096 Feb 26  2024 bin.usr-is-merged
drwxr-xr-x   5 root   root    4096 Sep 27 08:41 boot
drwxr-xr-x  16 root   root    3240 Oct 10 05:09 dev
drwxr-xr-x 108 root   root    4096 Oct 10 05:21 etc
drwxr-xr-x  14 root   root    4096 Oct 10 05:15 home
lrwxrwxrwx   1 root   root       7 Apr 22 13:08 lib -> usr/lib
drwxr-xr-x   2 root   root    4096 Apr  8  2024 lib.usr-is-merged
lrwxrwxrwx   1 root   root       9 Apr 22 13:08 lib64 -> usr/lib64
drwx------   2 root   root   16384 Sep 27 08:38 lost+found
drwxr-xr-x   2 root   root    4096 Sep 27 08:36 media
drwxr-xr-x   2 root   root    4096 Sep 27 08:36 mnt
drwx------   2 nikhil nikhil  4096 Oct  4 07:03 nikhil
drwxr-xr-x   2 root   root    4096 Sep 27 08:36 opt
dr-xr-xr-x 167 root   root       0 Oct 10 05:09 proc
drwx------   5 root   root    4096 Oct  4 06:58 root
drwxr-xr-x  27 root   root     880 Oct 10 05:24 run
lrwxrwxrwx   1 root   root       8 Apr 22 13:08 sbin -> usr/sbin
drwxr-xr-x   2 root   root    4096 Mar 31  2024 sbin.usr-is-merged
drwxr-xr-x   3 root   root    4096 Oct 10 05:23 secure
drwxr-xr-x   7 root   root    4096 Oct  7 04:48 snap
drwxr-xr-x   2 root   root    4096 Sep 27 08:36 srv
dr-xr-xr-x  13 root   root       0 Oct 10 05:23 sys
drwxrwxrwt  12 root   root    4096 Oct 10 05:22 tmp
drwxr-xr-x  12 root   root    4096 Sep 27 08:36 usr
drwxr-xr-x  13 root   root    4096 Oct  4 05:40 var
ubuntu@ip-172-31-24-49:~$
```

  * 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.



```
ubuntu@ip-172-31-24-49:~$ sudo chmod 700 /secure/patients/
```

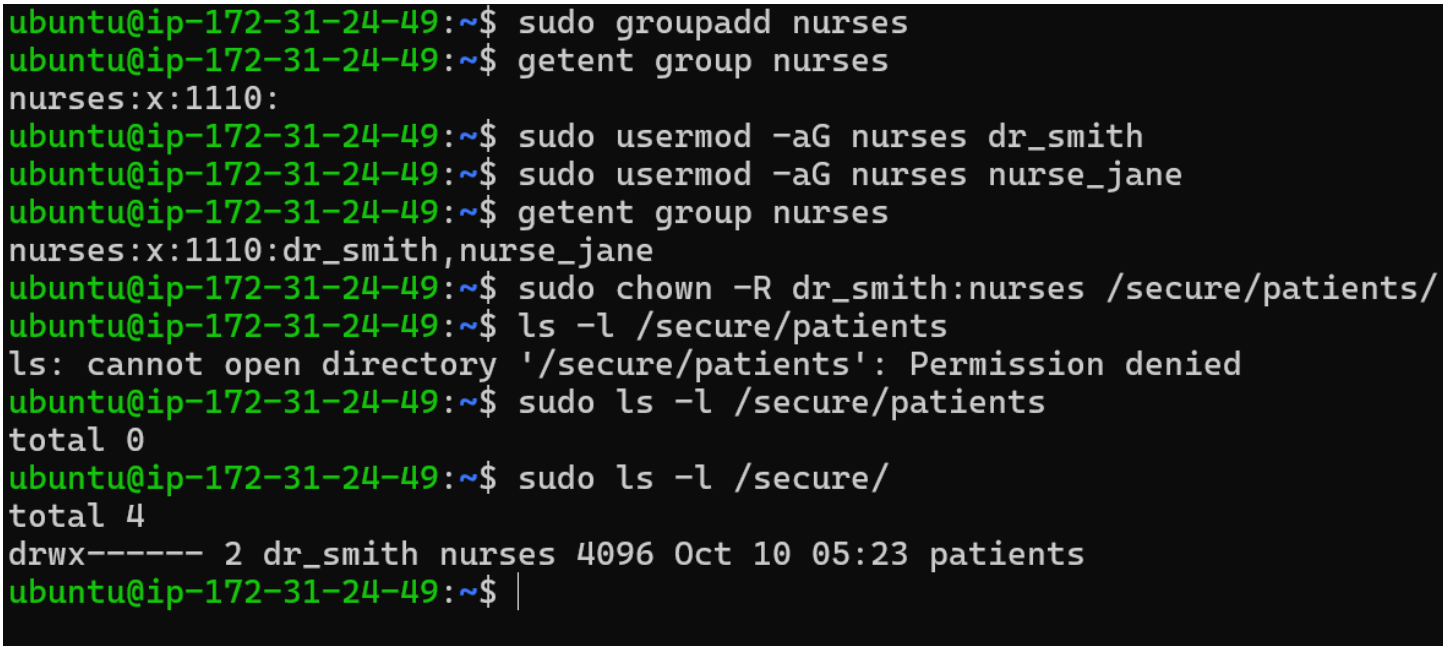


```
drwxr-xr-x   3 root   root    4096 Oct 10 05:23 secure
```

5. 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.

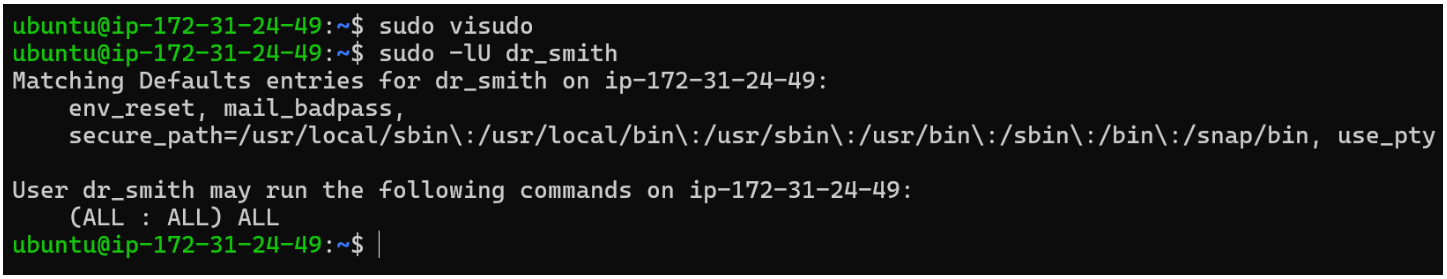


```
ubuntu@ip-172-31-24-49:~$ sudo groupadd nurses
ubuntu@ip-172-31-24-49:~$ getent group nurses
nurses:x:1110:
ubuntu@ip-172-31-24-49:~$ sudo usermod -aG nurses dr_smith
ubuntu@ip-172-31-24-49:~$ sudo usermod -aG nurses nurse_jane
ubuntu@ip-172-31-24-49:~$ getent group nurses
nurses:x:1110:dr_smith,nurse_jane
ubuntu@ip-172-31-24-49:~$ sudo chown -R dr_smith:nurses /secure/patients/
ubuntu@ip-172-31-24-49:~$ ls -l /secure/patients
ls: cannot open directory '/secure/patients': Permission denied
ubuntu@ip-172-31-24-49:~$ sudo ls -l /secure/patients
total 0
ubuntu@ip-172-31-24-49:~$ sudo ls -l /secure/
total 4
drwx------ 2 dr_smith nurses 4096 Oct 10 05:23 patients
ubuntu@ip-172-31-24-49:~$ 
```

6. 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.



```
ubuntu@ip-172-31-24-49:~$ sudo visudo
ubuntu@ip-172-31-24-49:~$ sudo -lU dr_smith
Matching Defaults entries for dr_smith on ip-172-31-24-49:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User dr_smith may run the following commands on ip-172-31-24-49:
    (ALL : ALL) ALL
ubuntu@ip-172-31-24-49:~$ 
```