Thapar Institute of Engineering and Technology, Patiala

Computer Science and Engineering

Information Security Laboratory (UCT602) Assignment:5

Do the following:

Sr. No.	Query	Remarks
1	• Changing file ownership: ▪ chown- change owner/user, ▪ chgrp- change group ownership • Changing file permission command: • chmod	chown hexa:random hello.txt sudo chgrp groupnew hello.txt sudo chmod -rwx hello.txt
2	**Access Control Lists:** • View ACL permissions • Set ACL on file and directory • Delete ACL • Set recursive ACL **Others:** **i.** To add permission for user. **ii.** To add permissions for a group. **iii.** To allow all files or directories to inherit ACL entries from the directory it is within. ***iv.*** To remove a specific entry. **v.** To remove all entries.	getfacl filename setfacl -m u:isi:rwx hello.txt setfacl --remove-all hello.txt setfacl -R -m u:romi:rwx .

3	**Monitor user activity:** • View history of all logged users • View login history of a certain user • View all bad login attempts • Who is currently logged in (tty and pts) • View User command history • tcpdump = View Server incoming and outgoing traffic	last last hexa grep "Failed password" /var/log/auth.log who history sudo tcpdump
4	What is **SUID** (Set-UID) and **SGID** (Set-GID) in Linux? • Implement UID/GID policy • Use *chmod* to set/unset	chmod u+s hello.txt # SUID chmod g+s . # SGID chmod u-s hello.txt # Unset SUID chmod g-s . # Unset SGID

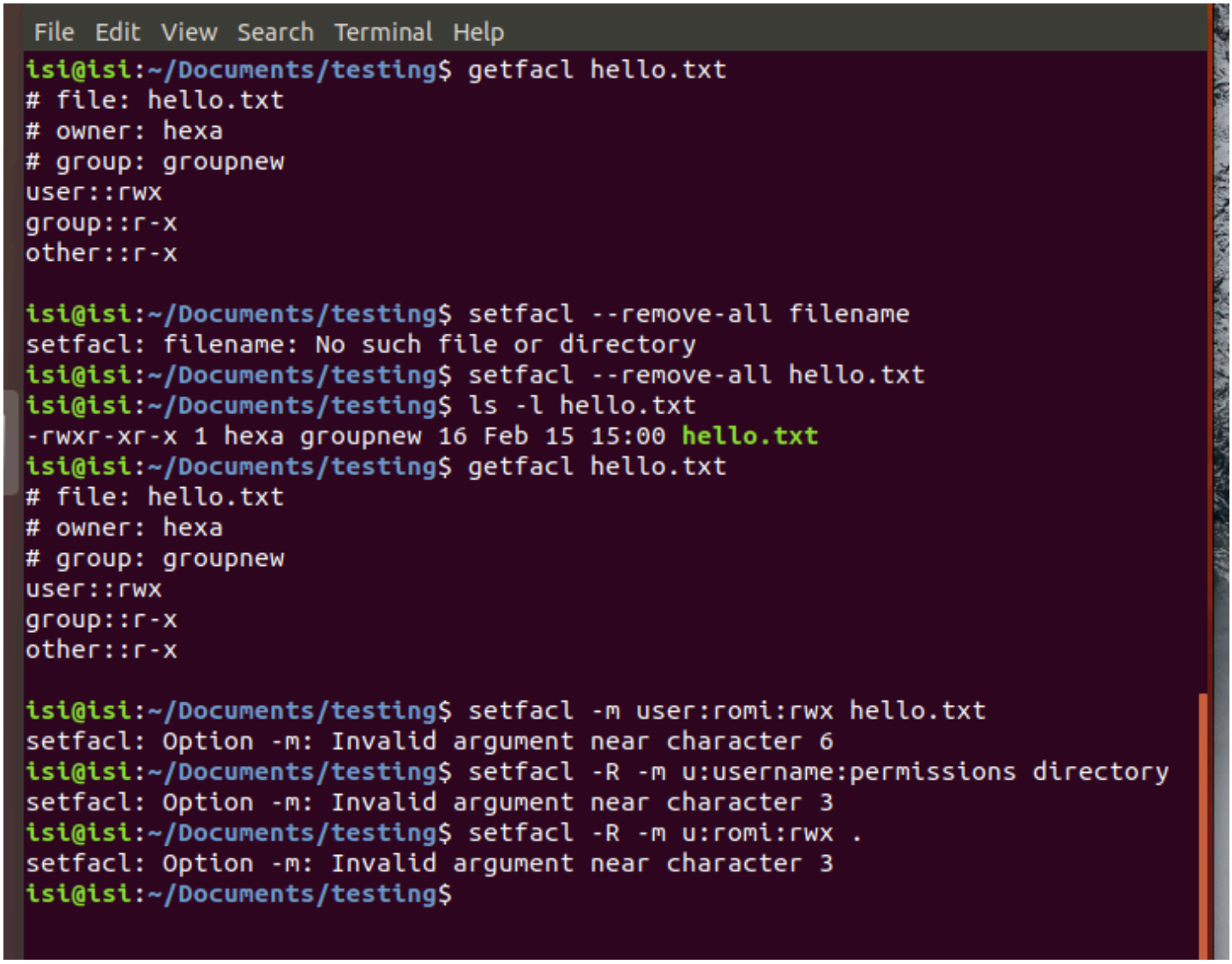
1.

```
File  Edit  View  Search  Terminal  Help
isi@isi:~/Documents/testing$ ls
hello.txt
isi@isi:~/Documents/testing$ ls -l hello.txt
-rw-r--r-- 1 root root 16 Feb 15 15:00 hello.txt
isi@isi:~/Documents/testing$ chown hexa:random hello.txt
chown: changing ownership of 'hello.txt': Operation not permitted
isi@isi:~/Documents/testing$ sudo chown hexa:random hello.txt
isi@isi:~/Documents/testing$ ls -l hello.txt
-rw-r--r-- 1 hexa random 16 Feb 15 15:00 hello.txt
isi@isi:~/Documents/testing$ sudo chgrp random  hello.txt
isi@isi:~/Documents/testing$ ls -l hello.txt
-rw-r--r-- 1 hexa random 16 Feb 15 15:00 hello.txt
isi@isi:~/Documents/testing$ sudo groupadd groupnew
isi@isi:~/Documents/testing$ sudo chgrp groupnew  hello.txt
isi@isi:~/Documents/testing$ ls -l hello.txt
-rw-r--r-- 1 hexa groupnew 16 Feb 15 15:00 hello.txt
isi@isi:~/Documents/testing$ chmod -rwx hello.txt
chmod: changing permissions of 'hello.txt': Operation not permitted
isi@isi:~/Documents/testing$ sudo chmod -rwx hello.txt
isi@isi:~/Documents/testing$ ls -l hello.txt
---------- 1 hexa groupnew 16 Feb 15 15:00 hello.txt
isi@isi:~/Documents/testing$
```

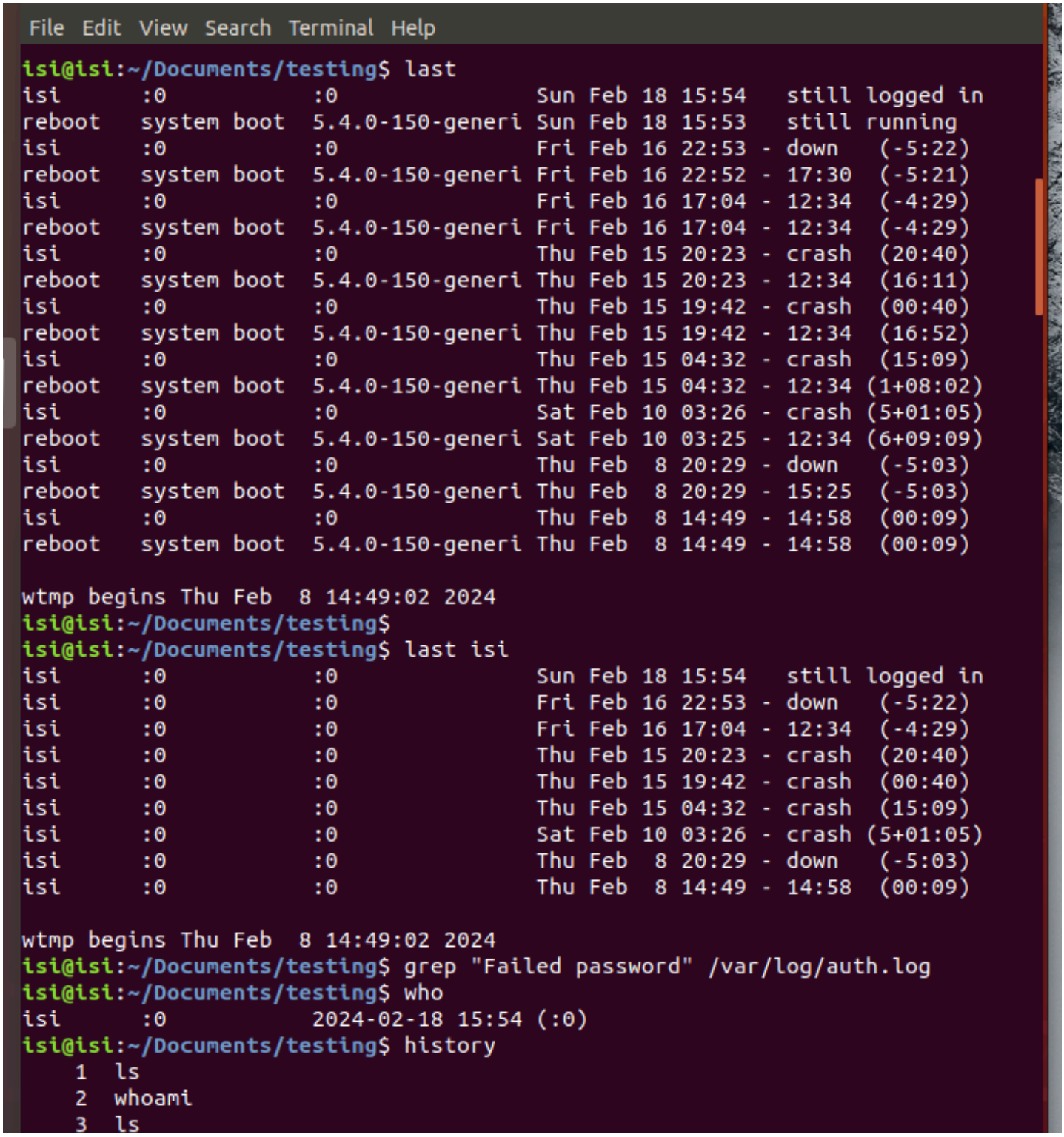
2.

```
File  Edit  View  Search  Terminal  Help
isi@isi:~/Documents/testing$ getfacl hello.txt
# file: hello.txt
# owner: hexa
# group: groupnew
user::rwx
group::r-x
other::r-x

isi@isi:~/Documents/testing$
```


File Edit View Search Terminal Help
isi@isi:~/Documents/testing$ getfacl hello.txt
file: hello.txt
owner: hexa
group: groupnew
user::rwx
group::r-x
other::r-x
isi@isi:~/Documents/testing$ setfacl --remove-all filename
setfacl: filename: No such file or directory
isi@isi:~/Documents/testing$ setfacl --remove-all hello.txt
isi@isi:~/Documents/testing$ ls -l hello.txt
-rwxr-xr-x 1 hexa groupnew 16 Feb 15 15:00 hello.txt
isi@isi:~/Documents/testing$ getfacl hello.txt
file: hello.txt
owner: hexa
group: groupnew
user::rwx
group::r-x
other::r-x
isi@isi:~/Documents/testing$ setfacl -m user:romi:rwx hello.txt
setfacl: Option -m: Invalid argument near character 6
isi@isi:~/Documents/testing$ setfacl -R -m u:username:permissions directory
setfacl: Option -m: Invalid argument near character 3
isi@isi:~/Documents/testing$ setfacl -R -m u:romi:rwx .
setfacl: Option -m: Invalid argument near character 3
isi@isi:~/Documents/testing$

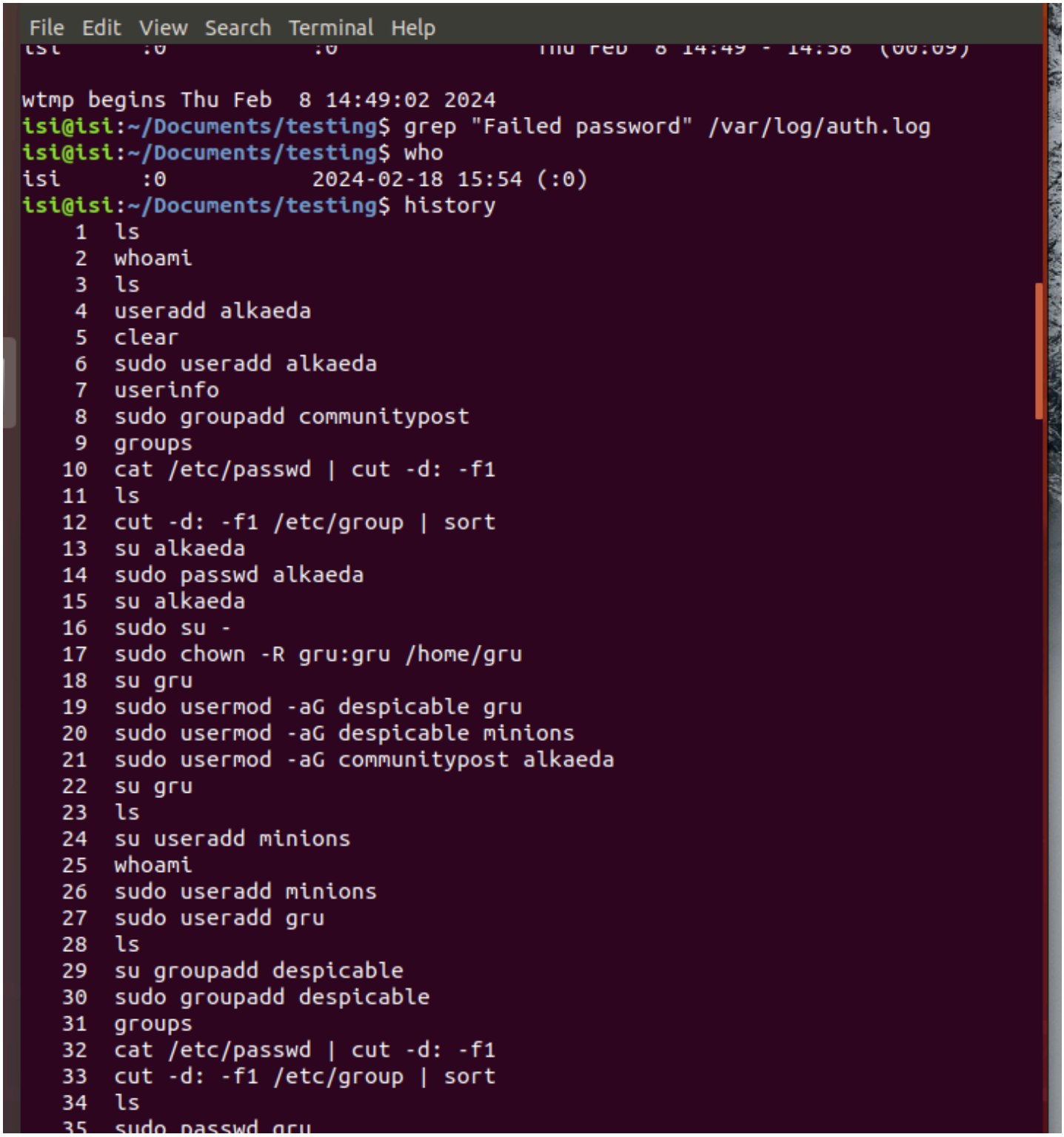
3.

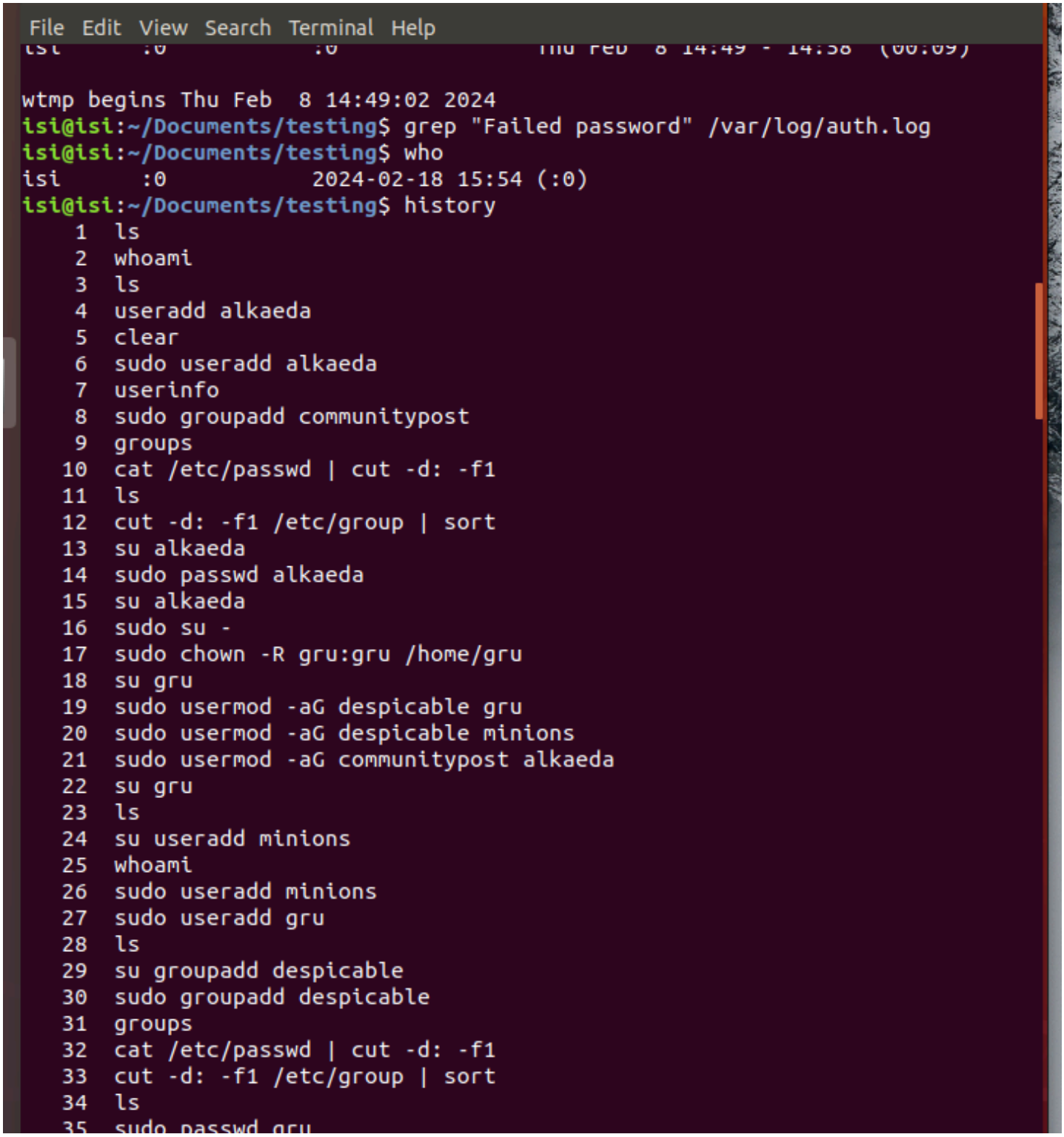


```
File  Edit  View  Search  Terminal  Help
isi@isi:~/Documents/testing$ last
isi      :0           :0               Sun Feb 18 15:54   still logged in
reboot   system boot  5.4.0-150-generi Sun Feb 18 15:53   still running
isi      :0           :0               Fri Feb 16 22:53 - down   (-5:22)
reboot   system boot  5.4.0-150-generi Fri Feb 16 22:52 - 17:30  (-5:21)
isi      :0           :0               Fri Feb 16 17:04 - 12:34  (-4:29)
reboot   system boot  5.4.0-150-generi Fri Feb 16 17:04 - 12:34  (-4:29)
isi      :0           :0               Thu Feb 15 20:23 - crash  (20:40)
reboot   system boot  5.4.0-150-generi Thu Feb 15 20:23 - 12:34  (16:11)
isi      :0           :0               Thu Feb 15 19:42 - crash  (00:40)
reboot   system boot  5.4.0-150-generi Thu Feb 15 19:42 - 12:34  (16:52)
isi      :0           :0               Thu Feb 15 04:32 - crash  (15:09)
reboot   system boot  5.4.0-150-generi Thu Feb 15 04:32 - 12:34 (1+08:02)
isi      :0           :0               Sat Feb 10 03:26 - crash (5+01:05)
reboot   system boot  5.4.0-150-generi Sat Feb 10 03:25 - 12:34 (6+09:09)
isi      :0           :0               Thu Feb  8 20:29 - down   (-5:03)
reboot   system boot  5.4.0-150-generi Thu Feb  8 20:29 - 15:25  (-5:03)
isi      :0           :0               Thu Feb  8 14:49 - 14:58  (00:09)
reboot   system boot  5.4.0-150-generi Thu Feb  8 14:49 - 14:58  (00:09)

wtmp begins Thu Feb  8 14:49:02 2024
isi@isi:~/Documents/testing$
isi@isi:~/Documents/testing$ last isi
isi      :0           :0               Sun Feb 18 15:54   still logged in
isi      :0           :0               Fri Feb 16 22:53 - down   (-5:22)
isi      :0           :0               Fri Feb 16 17:04 - 12:34  (-4:29)
isi      :0           :0               Thu Feb 15 20:23 - crash  (20:40)
isi      :0           :0               Thu Feb 15 19:42 - crash  (00:40)
isi      :0           :0               Thu Feb 15 04:32 - crash  (15:09)
isi      :0           :0               Sat Feb 10 03:26 - crash (5+01:05)
isi      :0           :0               Thu Feb  8 20:29 - down   (-5:03)
isi      :0           :0               Thu Feb  8 14:49 - 14:58  (00:09)

wtmp begins Thu Feb  8 14:49:02 2024
isi@isi:~/Documents/testing$ grep "Failed password" /var/log/auth.log
isi@isi:~/Documents/testing$ who
isi      :0           2024-02-18 15:54 (:0)
isi@isi:~/Documents/testing$ history
    1  ls
    2  whoami
    3  ls
```


File Edit View Search Terminal Help
wtmp begins Thu Feb 8 14:49:02 2024
isi@isi:~/Documents/testing$ grep "Failed password" /var/log/auth.log
isi@isi:~/Documents/testing$ who
isi :0 2024-02-18 15:54 (:0)
isi@isi:~/Documents/testing$ history
1 ls
2 whoami
3 ls
4 useradd alkaeda
5 clear
6 sudo useradd alkaeda
7 userinfo
8 sudo groupadd communitypost
9 groups
10 cat /etc/passwd | cut -d: -f1
11 ls
12 cut -d: -f1 /etc/group | sort
13 su alkaeda
14 sudo passwd alkaeda
15 su alkaeda
16 sudo su -
17 sudo chown -R gru:gru /home/gru
18 su gru
19 sudo usermod -aG despicable gru
20 sudo usermod -aG despicable minions
21 sudo usermod -aG communitypost alkaeda
22 su gru
23 ls
24 su useradd minions
25 whoami
26 sudo useradd minions
27 sudo useradd gru
28 ls
29 su groupadd despicable
30 sudo groupadd despicable
31 groups
32 cat /etc/passwd | cut -d: -f1
33 cut -d: -f1 /etc/group | sort
34 ls


File Edit View Search Terminal Help
wtmp begins Thu Feb 8 14:49:02 2024
isi@isi:~/Documents/testing$ grep "Failed password" /var/log/auth.log
isi@isi:~/Documents/testing$ who
isi :0 2024-02-18 15:54 (:0)
isi@isi:~/Documents/testing$ history
1 ls
2 whoami
3 ls
4 useradd alkaeda
5 clear
6 sudo useradd alkaeda
7 userinfo
8 sudo groupadd communitypost
9 groups
10 cat /etc/passwd | cut -d: -f1
11 ls
12 cut -d: -f1 /etc/group | sort
13 su alkaeda
14 sudo passwd alkaeda
15 su alkaeda
16 sudo su -
17 sudo chown -R gru:gru /home/gru
18 su gru
19 sudo usermod -aG despicable gru
20 sudo usermod -aG despicable minions
21 sudo usermod -aG communitypost alkaeda
22 su gru
23 ls
24 su useradd minions
25 whoami
26 sudo useradd minions
27 sudo useradd gru
28 ls
29 su groupadd despicable
30 sudo groupadd despicable
31 groups
32 cat /etc/passwd | cut -d: -f1
33 cut -d: -f1 /etc/group | sort
34 ls