

Mini Project - Secure User Access Management in Linux

Problem Statement Document

Identity and Access Management (IAM) is a centralized and consistent way to manage user identities (that is, people, services, and servers), automate access controls, and meet compliance requirements across traditional and containerized environments.

User management includes everything from creating a user to deleting a user on your system.

User management can be done in three ways on a Linux system. Graphical tools are easy and suitable for new users, as they make sure you'll not run into any trouble.

LAB 1:

The CTO of the company, Mr. Penny Johnson, has recently discussed a new project with a potential client. He has sent you the file and asked you to —

noida.txt

save it on your Linux machine. Once saved, you are instructed to create a user account “pjohnson” and the project directory and place the file in the folder. Applying the concepts of ACL (Access Control List), you have to give access to Mr. Johnson. No one else should be able to access the file except Mr. Johnson. Make sure to remove any other user access to that file. As a part of the assignment, kindly log in as another user and try accessing the file.

Kindly compile and explain the process in a report (support with visual evidence).

Note: You are expected to demonstrate that Mr. Penny has access and that any other user cannot access the file.

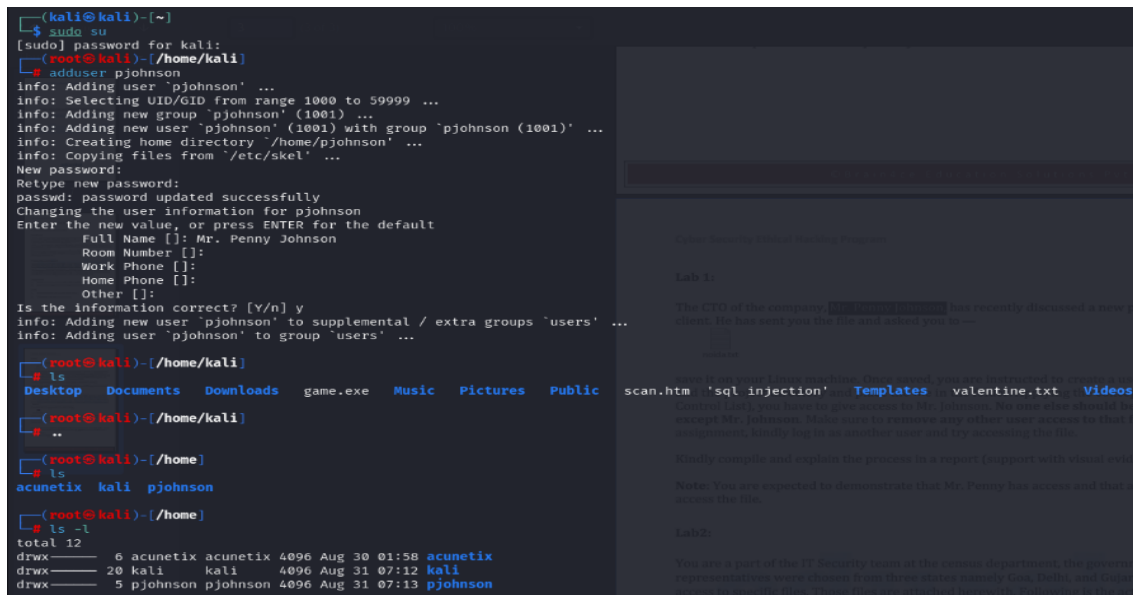
:-

1.I have added a new user with name pjohanson. Using command adduser.

Adduser:- Creates a new user account.

ls:- It is used to list files and directory

-l:- Is used to list the information about the file.



```
(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
└─$ adduser pjohanson
info: Adding user 'pjohanson' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'pjohanson' (1001) ...
info: Adding new user 'pjohanson' (1001) with group 'pjohanson (1001)' ...
info: Creating home directory '/home/pjohnson' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for pjohanson
Enter the new value, or press ENTER for the default
  Full Name []: Mr. Penny Johnson
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
info: Adding new user 'pjohanson' to supplemental / extra groups 'users' ...
info: Adding user 'pjohanson' to group 'users' ...

(root@kali)-[/home/kali]
└─$ ls
Desktop  Documents  Downloads  game.exe  Music  Pictures  Public

(root@kali)-[/home/kali]
└─$ ..

(root@kali)-[/home]
└─$ ls
acunetix  kali  pjohanson

(root@kali)-[/home]
└─$ ls -l
total 12
drwx--- 6 acunetix acunetix 4096 Aug 30 01:58 acunetix
drwx--- 20 kali      kali      4096 Aug 31 07:12 kali
drwx--- 5 pjohanson pjohanson 4096 Aug 31 07:13 pjohanson
```

2.Create a directory name ‘project’. Using command ‘mkdir’.

Copy Noida.txt in project directory. Using ‘cp’ command.

Change the permission of noida.txt. Using command ‘chmod’.

chmod:- used to change access permission of files and directory.

```

root@kali:~# cd Project1
root@kali:~/Desktop/Project1# mkdir project
root@kali:~/Desktop/Project1# ls -l
total 4
drwxr-xr-x 2 root root 4096 Aug 31 07:24 project
root@kali:~/Desktop/Project1# cd project
root@kali:~/Desktop/Project1/project# cp /home/kali/Desktop/ie_cseh_additional_files_v1_cfc_pl6s60s\ \2\)/noida.txt .
root@kali:~/Desktop/Project1/project# ls
noida.txt
root@kali:~/Desktop/Project1/project# ls -l
total 4
-rw-r--r-- 1 root root 4 Aug 31 07:28 noida.txt
root@kali:~/Desktop/Project1/project# chmod 700 noida.txt
root@kali:~/Desktop/Project1/project# su thanos
(thanos@kali)~/Desktop/Project1/project# ls
noida.txt
(thanos@kali)~/Desktop/Project1/project# cat noida.txt
cat: noida.txt: Permission denied
(thanos@kali)~/Desktop/Project1/project#
::1 ff02::1 ff02::2 ip6-allnodes ip6-allrouters ip6-localhost ip6-loopback kali
(thanos@kali)~/Desktop/Project1/project#

```

3.Checked pjohnson can access noida.txt or not.

Using setfacl granted read, write, execute permissions to pjohnson.

Checked whether permission is assigned or not.

Now pjohnson can access noida.txt.

setfacl:-It sets, modify, or removes the access control list.it let you assign permission for each unique user or group.

-m used for modification, u used for user, g used for group, -r used for recursive.

```

File Actions Edit View Help
(pjohnson@kali)~/Desktop/Project1/project# ls
noida.txt
(pjohnson@kali)~/Desktop/Project1/project# cat noida.txt
cat: noida.txt: Permission denied
(pjohnson@kali)~/Desktop/Project1/project# exit
exit
(thanos@kali)~/Desktop/Project1/project# exit
exit
root@kali:~/Desktop/Project1/project# setfacl -m u:pjohnson:rwx noida.txt
root@kali:~/Desktop/Project1/project# su thanos
(thanos@kali)~/Desktop/Project1/project# ls
noida.txt
(thanos@kali)~/Desktop/Project1/project# cat noida.txt
cat: noida.txt: Permission denied
(thanos@kali)~/Desktop/Project1/project# su pjohnson
Password:
(pjohnson@kali)~/Desktop/Project1/project# ls
noida.txt
(pjohnson@kali)~/Desktop/Project1/project# cat noida.txt
Carl
(pjohnson@kali)~/Desktop/Project1/project#

```

Lab2:

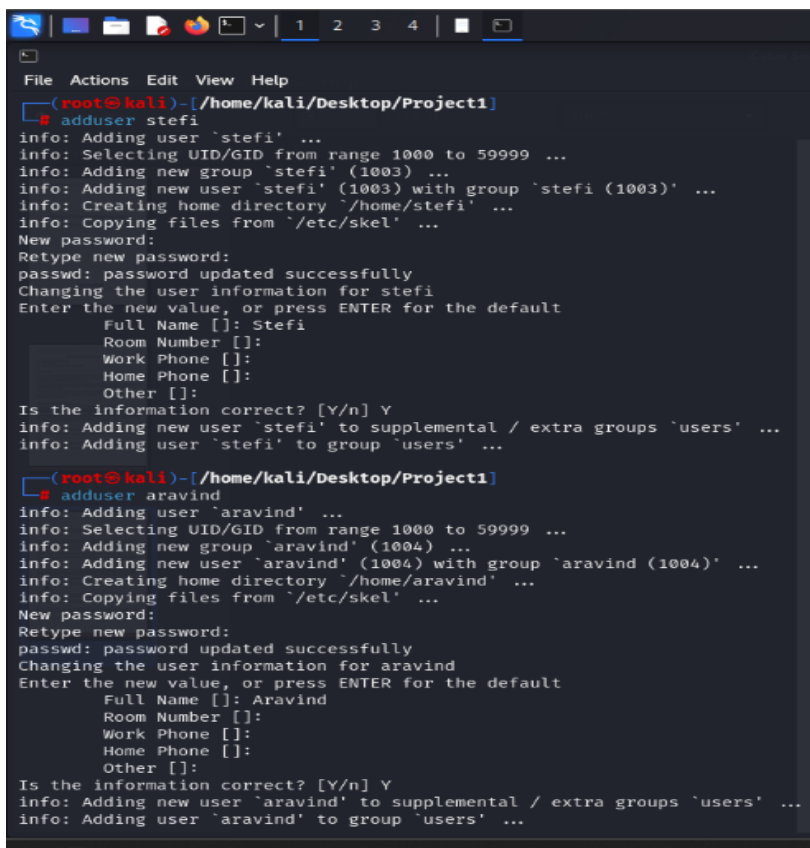
You are a part of the IT Security team at the census department, the government of India. Three representatives were chosen from three states namely Goa, Delhi, and Gujarat who need to have access to specific files. Those files are attached herewith. Following is the activity to be performed. Create users “stefi, aravind, and jignesh”. Keep the password as “india”. Create a new group called “citizen”. Download the following and extract it to the desktop:

government.zip

Change the permissions for Gujarat so that jignesh has full permissions and aravind has only read and execute permissions. Log in as aravind. Is he able to edit Gujarat\ahmedabad.txt? Edit the permissions for Delhi recursively in such a way that stefi has no access. Log in as stefi and check if he is unable to access the content of Delhi. Grant full rights to the citizen of Goa. Edit the rights for goa\anjuna.txt so that only stefi can write and aravind to read, and for goa\candolim.txt so that only jignesh can write and stefi to read. Considerations: You have root privileges

:-

1. Add user stefi, aravind, Jignesh with password :india. Using command ‘adduser’



```
(root@kali)-[/home/kali/Desktop/Project1]
# adduser stefi
info: Adding user 'stefi' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'stefi' (1003) ...
info: Adding new user 'stefi' (1003) with group 'stefi (1003)' ...
info: Creating home directory '/home/stefi' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for stefi
Enter the new value, or press ENTER for the default
  Full Name []: Stef
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] Y
info: Adding new user 'stefi' to supplemental / extra groups 'users' ...
info: Adding user 'stefi' to group 'users' ...

(root@kali)-[/home/kali/Desktop/Project1]
# adduser aravind
info: Adding user 'aravind' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'aravind' (1004) ...
info: Adding new user 'aravind' (1004) with group 'aravind (1004)' ...
info: Creating home directory '/home/aravind' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for aravind
Enter the new value, or press ENTER for the default
  Full Name []: Aravind
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] Y
info: Adding new user 'aravind' to supplemental / extra groups 'users' ...
info: Adding user 'aravind' to group 'users' ...
```

2. Check whether they are added or not. Using command 'cat /etc/passwd'

```
File Actions Edit View Help
Other []:
Is the information correct? [Y/n] Y
info: Adding new user 'aravind' to supplemental / extra groups 'users' ...
info: Adding user 'aravind' to group 'users' ...

(root@kali)~/Desktop/Project1
# adduser jignesh
info: Adding user 'jignesh' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'jignesh' (1006) ...
info: Adding new user 'jignesh' (1006) with group 'jignesh (1006)' ...
info: Creating home directory '/home/jignesh' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for jignesh
Enter the new value, or press ENTER for the default
Full Name []: jignesh
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] Y
info: Adding new user 'jignesh' to supplemental / extra groups 'users' ...
info: Adding user 'jignesh' to group 'users' ...

(root@kali)~/Desktop/Project1
# cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
usbmux:x:105:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:106:108:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:107:29:Speech Dispatcher,,:/run/speech-dispatcher:/bin/false
pulse:x:108:110:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin
lightdm:x:109:112:Light Display Manager:/var/lib/lightdm:/bin/false
saned:x:110:114::/var/lib/saned:/usr/sbin/nologin
polkitd:x:991:991:User for polkitd:/usr/sbin/nologin
rtkit:x:111:115:RealtimeKit,,:/proc:/usr/sbin/nologin
colord:x:112:116:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:x:113:117:NetworkManager OpenVPN,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:114:118:NetworkManager OpenConnect plugin,,:/var/lib/NetworkManager:/usr/sbin/nologin
_galera:x:115:65534:/:nonexistent:/usr/sbin/nologin
mysql:x:116:120:MySQL Server,,:/nonexistent:/bin/false
stunnel4:x:990:990:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
_rpc:x:117:65534:/:run/rpcbind:/usr/sbin/nologin
geoclue:x:118:122:/:var/lib/geoclue:/usr/sbin/nologin
Debian-snmpp:x:119:123:/:var/lib/snmpp:/bin/false
sshd:x:120:124:/:nonexistent:/usr/sbin/nologin
ntpsvc:x:121:127:/:nonexistent:/usr/sbin/nologin
redsocks:x:122:128:/:var/run/redsocks:/usr/sbin/nologin
rwhod:x:123:65534:/:var/spool/rwhod:/usr/sbin/nologin
_gophish:x:124:130:/:var/lib/gophish:/usr/sbin/nologin
Iodine:x:125:65534:/:run/iodine:/usr/sbin/nologin
miredo:x:126:65534:/:var/run/miredo:/usr/sbin/nologin
statd:x:127:65534:/:var/lib/nfs:/usr/sbin/nologin
redis:x:128:131:/:var/lib/redis:/usr/sbin/nologin
postgres:x:129:132:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
mosquitto:x:130:133:/:var/lib/mosquitto:/usr/sbin/nologin
inetsim:x:131:134:/:var/lib/inetsim:/usr/sbin/nologin
_gvm:x:132:135:/:var/lib/openvas:/usr/sbin/nologin
kali:x:1000:1000:,,:/home/kali:/usr/bin/zsh
debian-tor:x:133:138:/:var/lib/tor:/bin/false
Debian-exim:x:134:139:/:var/spool/exim4:/usr/sbin/nologin
acunetix:x:997:1005:/:home/acunetix:/bin/sh
pjohnson:x:1001:1001:Mr. Penny Johnson,,:/home/pjohnson:/bin/bash
thanos:x:1002:1002:Thanos,,:/home/thanos:/bin/bash
stefi:x:1003:1003:Stefi,,:/home/stefi:/bin/bash
aravind:x:1004:1004:Aravind,,:/home/aravind:/bin/bash
jignesh:x:1006:1006:Jignesh,,:/home/jignesh:/bin/bash

(root@kali)~/Desktop/Project1
#
```

3. Add group name 'citizen'. Using addgroup.
4. Check whether group is added or not using command 'cat /etc/group | grep "citizen" '.
5. Add Stefi, Aravind ,and Jignesh in group citizen. Using command usermod.
usermod:-to modify user account details.
-a means to append, -G means Group

```

File Actions Edit View Help
jignesh:x:1006:1006:Jignesh,,,:/home/jignesh:/bin/bash

(root@kali)-[/home/kali/Desktop/Project1]
# addgroup citizen
info: Selecting GID from range 1000 to 59999 ...
info: Adding group 'citizen' (GID 1007) ...

(root@kali)-[/home/kali/Desktop/Project1]
# cat /etc/group | grep "citizen"
citizen:x:1007:

(root@kali)-[/home/kali/Desktop/Project1]
# usermod -a -G citizen stefi

(root@kali)-[/home/kali/Desktop/Project1]
# usermod -a -G citizen aravind

(root@kali)-[/home/kali/Desktop/Project1]
# usermod -a -G citizen jignesh

(root@kali)-[/home/kali/Desktop/Project1]
# cat /etc/group | grep "citizen"
citizen:x:1007:stefi,aravind,jignesh

(root@kali)-[/home/kali/Desktop/Project1]
# ls
project

(root@kali)-[/home/kali/Desktop/Project1]
# cp -r /home/kali/Desktop/ie_cseh_additional_files_v1_cfc_pl6s60s\ \2\government
cp: missing destination file operand after '/home/kali/Desktop/ie_cseh_additional_files_v1_cfc_pl6s60s (2)/government'
Try 'cp --help' for more information.

(root@kali)-[/home/kali/Desktop/Project1]
# cp -r /home/kali/Desktop/ie_cseh_additional_files_v1_cfc_pl6s60s\ \2\government .

(root@kali)-[/home/kali/Desktop/Project1]
# ls
government project

(root@kali)-[/home/kali/Desktop/Project1]
# cd government

```

6. Using setfacl changed the permission of Jignesh and Aravind for the file gujarat.

```

File Actions Edit View Help

(root@kali)-[/home/kali/Desktop/Project1]
# cd government

(root@kali)-[/home/kali/Desktop/Project1/government]
# ls
delhi goa gujarat

(root@kali)-[/home/kali/Desktop/Project1/government]
# setfacl -R -m u:jignesh:rwX gujarat

(root@kali)-[/home/kali/Desktop/Project1/government]
# setfacl -R -m u:aravind:rx gujarat

(root@kali)-[/home/kali/Desktop/Project1/government]
# su aravind
(aravind@kali)-[/home/kali/Desktop/Project1/government]
$ ls
delhi goa gujarat

(aravind@kali)-[/home/kali/Desktop/Project1/government]
$ cd gujarat

(aravind@kali)-[/home/kali/Desktop/Project1/government/gujarat]
$ ls
ahmedabad.txt chandkheda.txt

(aravind@kali)-[/home/kali/Desktop/Project1/government/gujarat]
$ cat ahmedabad
cat: ahmedabad: No such file or directory

(aravind@kali)-[/home/kali/Desktop/Project1/government/gujarat]
$ cat ahmedabad.txt
Judy

(aravind@kali)-[/home/kali/Desktop/Project1/government/gujarat]
$ echo "Aravind" > ahmedabad.txt
bash: ahmedabad.txt: Permission denied

(aravind@kali)-[/home/kali/Desktop/Project1/government/gujarat]
$ exit
exit

```


7. Checked if the permission is changed or not.
8. Changed the permission of stefi for the text file delhi.
9. Checked if the permission is changed or not.

```

File Actions Edit View Help
exit

(root@kali)-[/home/kali/Desktop/Project1/government]
# su jignesh
(jignesh@kali)-[/home/kali/Desktop/Project1/government]
$ ls
delhi goa gujarat

(jignesh@kali)-[/home/kali/Desktop/Project1/government]
$ cd gujarat

(jignesh@kali)-[/home/kali/Desktop/Project1/government/gujarat]
$ cat ahmedabad.txt
Judy

(jignesh@kali)-[/home/kali/Desktop/Project1/government/gujarat]
$ echo "Jignesh" > ahmedabad.txt

(jignesh@kali)-[/home/kali/Desktop/Project1/government/gujarat]
$ exit
exit

(root@kali)-[/home/kali/Desktop/Project1/government]
# setfacl -R -m u:stefi:— delhi

(root@kali)-[/home/kali/Desktop/Project1/government]
# su stefi
(stefi@kali)-[/home/kali/Desktop/Project1/government]
$ cd delhi/
bash: cd: delhi/: Permission denied

(stefi@kali)-[/home/kali/Desktop/Project1/government]
$ cd goa

(stefi@kali)-[/home/kali/Desktop/Project1/government/goa]
$ ../
bash: ../: Is a directory

```

10. Changed the permission of group 'citizen' for file goa.
11. Changed the permission of stefi and Aravind dor anjuna.txt and checked.

```

(root@kali)-[/home/kali/Desktop/Project1/government]
# setfacl -R -m g:citizen:rwx goa

(root@kali)-[/home/kali/Desktop/Project1/government]
# cd goa

(root@kali)-[/home/.../Desktop/Project1/government/goa]
# ls
anjuna.txt candolim.txt corlim.txt

(root@kali)-[/home/.../Desktop/Project1/government/goa]
# setfacl -m u:stefi:w anjuna.txt
setfacl: anjuna.txt: No such file or directory

(root@kali)-[/home/.../Desktop/Project1/government/goa]
# setfacl -m u:stefi:w anjuna.txt

(root@kali)-[/home/.../Desktop/Project1/government/goa]
# setfacl -m u:aravind:r anjuna.txt

(root@kali)-[/home/.../Desktop/Project1/government/goa]
# su stefi
(stefi@kali)-[/home/kali/Desktop/Project1/government/goa]
$ cat anjuna.txt
cat: anjuna.txt: Permission denied

(stefi@kali)-[/home/kali/Desktop/Project1/government/goa]
$ exit
exit

(root@kali)-[/home/.../Desktop/Project1/government/goa]
# setfacl -m u:stefi:r candolim.txt

(root@kali)-[/home/.../Desktop/Project1/government/goa]
# setfacl -m u:aravind:w candolim.txt

(root@kali)-[/home/.../Desktop/Project1/government/goa]
# su aravind
(aravind@kali)-[/home/kali/Desktop/Project1/government/goa]
$ cat candolim.txt
cat: candolim.txt: Permission denied

```

12. Now , changed the permission of stefi and Aravind for candolim.txt .
13. Checked if the permission is changed or not.

```
(root@kali)-[/home/.../Desktop/Project1/government/goa]
# su aravind
(aravind@kali)-[/home/kali/Desktop/Project1/government/goa]
$ cat candolim.txt
cat: candolim.txt: Permission denied

(aravind@kali)-[/home/kali/Desktop/Project1/government/goa]
$ su stefi
Password:
(stefi@kali)-[/home/kali/Desktop/Project1/government/goa]
$ cat candolim.txt
Tulip
(stefi@kali)-[/home/kali/Desktop/Project1/government/goa]
$
```

a

