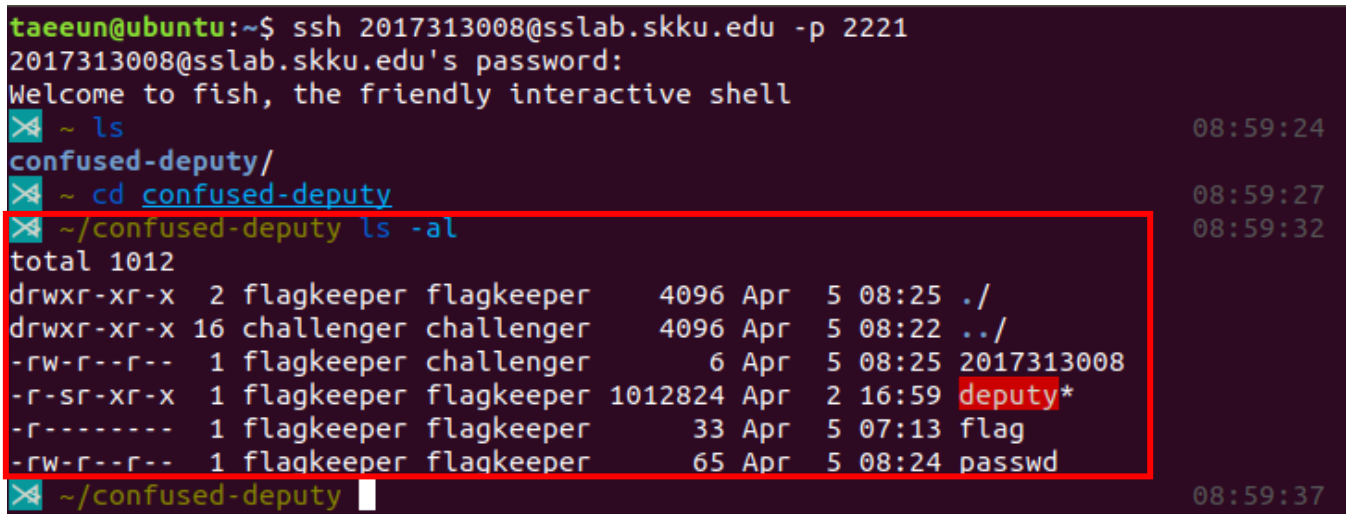
Lab1 (confused-deputy) Report

2017313008 Kim Tae Eun

How to solve:



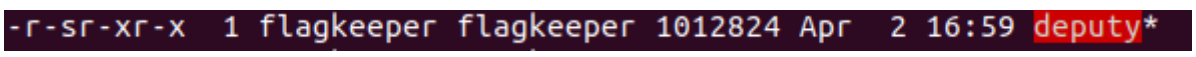
Enter ls -al command in the confused-deputy directory to see a list of all files in that directory. You can also see file permissions, owner, and group here.

The file permissions of the flag file(target) are only readable by the owner(flagkeeper), so challenger(me) cannot read the flag file.

Also, the passwd file can only be written by the flagkeeper (“written” means it can be changed).

And if you read the passwd file through the ‘cat passwd’ command, you can see that SHA256 hash value is stored. (it can not be decoded)

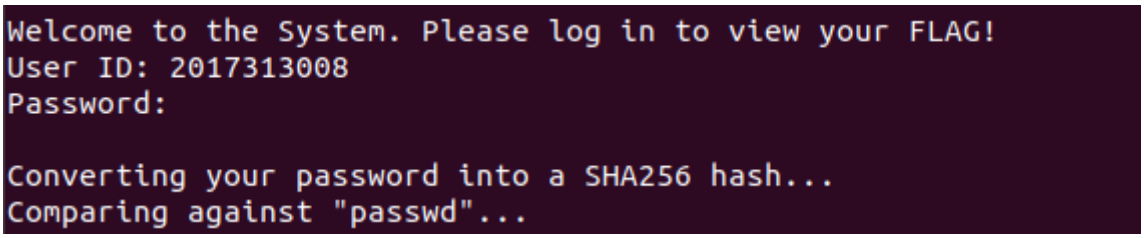
However, what should be noted here is that SetUID is set in the file permission of the deputy executable file.



When executing a file with SetUID, it can be temporarily executed with the permission of the owner(flagkeeper).

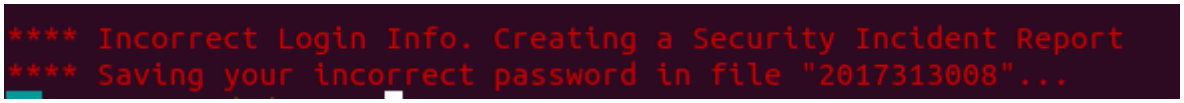
Therefore, we can expect to get a solution to the problem by executing deputy. (confused-deputy is the subject of this lab)

First, let's see how deputy works.

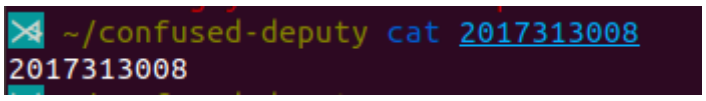


If you execute deputy, you can see that you are prompted to enter your ID and password as shown in the picture above.

Then, deputy changes the password we enter to SHA256 hash to determine whether it matches or not compared with the "passwd" file.



And if we fail to log in, we can see that deputy saves the password we entered in a file with the ID name(2017313008).



As above, the password (2017313008) I entered was stored in a file named “2017313008” (ID).

Then we can realize one thing here.

If you enter "passwd" in the ID, you have the permissions of the flagkeeper while executing the disputy, so you can overwrite the original passwd file. (confused-deputy)

So, after entering “passwd” in the ID and entering the value changed to SHA256 hash of any word I know (MANGO) into the password, you can see that the contents of the passwd file have changed as shown below.

```
~/confused-deputy cat passwd
9997ec87851aa725648de72d56a608a20c80f1dc4eb12dc2829bf91708db82de
```

The above is the SHA256 hash value of “MANGO”.

Therefore, we can enter the ID (2017313008) again in the deputy program and enter “MANGO” in the password to successfully log in and read the flag.

During deputy execution, the flag can be read with the flagkeeper's authority. (confused-deputy)

```
Login Succesful!!!
Good Job!!! Here's your flag:

kzz9YmM6VRUh24NVfvL7mNM2p0Ho6jfh
```