1️⃣ Level01

En este nivel como tampoco tenemos nada en nuestro usuario tendremos que volver a la raiz, aquí volveremos a buscar archivos a los que podamos acceder, en este caso haremos un find pero de archivos exclusivamente.

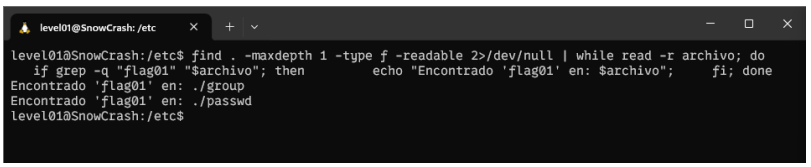
```
find . -maxdepth 1 -type f 2>/dev/null
```

Como en la raiz no encontramos nada con maxdepth 1, se me ocurrió mirar en `etc` que es donde se almacenan muchos archivos importantes.

Aqui tenemos acceso a muchos archivos y con ayuda de un script busqué en cada archivo a ver si alguno tenía la palabra `flag01`.

```
find . -maxdepth 1 -type f -readable 2>/dev/null | while read -r archivo; do
    # Buscar la palabra "flag01" dentro del archivo
    if grep -q "flag01" "$archivo"; then
        echo "Encontrado 'flag01' en: $archivo"
    fi
done
```

Ejecutando el script anterior podemos buscar la palabra flag01 dentro de los archivos y esto nos da el siguiente resultado.



Vamos a mirar dentro de passwd a ver si tiene alguna contraseña.

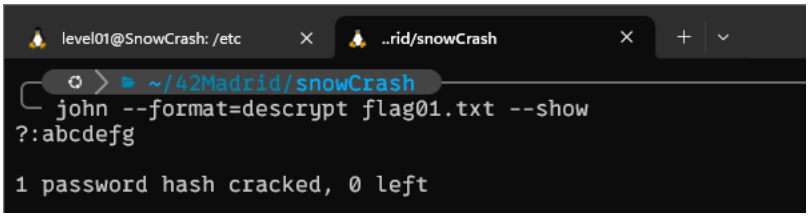
Efectivamente la tiene, ahora lo que tenemos que ver es que cifrado tiene esa contraseña.

Investigando un poco vemos que antiguamente las contraseñas en /etc/passwd se almacenaban con cifrado DES por lo que ya sabemos que tenemos que descifrar este tipo de cifrado.

Por suerte este cifrado es muy antiguo y usando john podemos descifrarlo facilmente, para ello ejecutaremos john de la siguiente manera.

```
john --format=descrypt flag01.txt --show
```

Y esto nos descifra la pass.



Ya sabemos que la contraseña de acceso a la flag01 es `abcdefg`.