

1

Level01

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

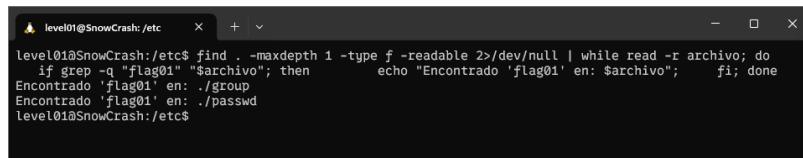
```
find . -maxdepth 1 -type f 2>/dev/null
```

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

Aquí 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.



```
level01@SnowCrash:/etc$ find . -maxdepth 1 -type f -readable 2>/dev/null | while read -r archivo; do
    if grep -q "flag01" "$archivo"; then
        echo "Encontrado 'flag01' en: $archivo"
    fi
done
Encontrado 'flag01' en: ./group
Encontrado 'flag01' en: ./passwd
level01@SnowCrash:/etc$
```

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

```
level14:x:2014:2014::/home/user/level14:/bin/bash
flag00:x:3000:3000::/home/flag/flag00:/bin/bash
flag01:42hDRfypTqqnw:3001:3001::/home/flag/flag01:/bin/bash
flag02:x:3002:3002::/home/flag/flag02:/bin/bash
flag03:x:3003:3003::/home/flag/flag03:/bin/bash
flag04:x:3004:3004::/home/flag/flag04:/bin/bash
flag05:x:3005:3005::/home/flag/flag05:/bin/bash
```

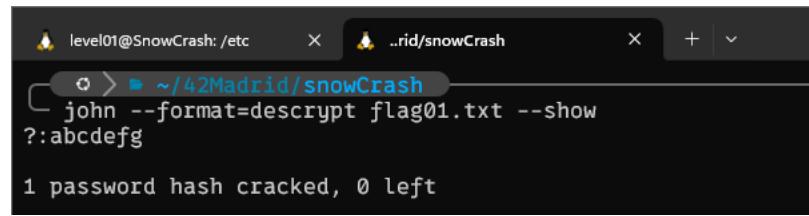
Efectivamente la tiene, ahora lo que tenemos que ver es que cifrado tiene esa contraseña.

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 fácilmente, para ello ejecutaremos `john` de la siguiente manera.

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

Y esto nos descifra la pass.



A screenshot of a terminal window titled "level01@snowCrash: /etc". The window contains two tabs: one for the user and another for the root user. The root tab is active and shows the command "john --format=descrypt flag01.txt --show" being run. The output of the command is displayed below, showing a single password hash cracked. The cracked password is highlighted in red.

```
john --format=descrypt flag01.txt --show
?:abcdefg
1 password hash cracked, 0 left
```

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