

# CTF 01 – Reto de comandos Linux

Autor: Jesús Díaz

Bootcamp Cyberskills Read Team 2025

Fecha: 22/05/2025

⚠ Este reto se realizó en un laboratorio virtual controlado con fines educativos. Todos los usuarios y contraseñas son ficticios y no representan sistemas reales.

## 1. Resumen Ejecutivo

Este reto básico de tipo CTF (Capture The Flag) fue diseñado para aprender y reforzar el uso de comandos de Linux en un entorno educativo. El objetivo principal fue moverse entre distintos usuarios del sistema, comprender permisos de archivos, descifrar ficheros protegidos y obtener el acceso final al usuario objetivo.

## 2. Objetivos del Reto

- Familiarizarse con la estructura de archivos y comandos básicos en Linux.
- Practicar el cambio de usuarios mediante credenciales encontradas en el sistema.
- Analizar permisos de archivos y grupos de usuarios.
- Descifrar archivos protegidos con ccrypt/decrypt.
- Ejecutar scripts en Bash con claves de descifrado.
- Acceder al usuario final (user5) y leer el flag exito.txt.

## 3. Entorno de Pruebas

- Sistema operativo: Ubuntu (máquina virtual de laboratorio)
- Herramientas: terminal Bash, ccrypt/decrypt, cat, su, ls -la
- Todos los datos son ficticios.

## 4. Desarrollo Paso a Paso

1. Acceso inicial con usuario user1 y revisión de archivos en el directorio home con el comando: ll (ls -la)

```
user1@ubuntu:~$ ll
total 40
drwxr-xr-x 4 user1 user1 4096 Mar 14 2024 .
drwxr-xr-x 8 root  root 4096 Sep 18 2020 ..
-rw----- 1 user1 user1 48 Mar 14 2024 .bash_history
-rw-r--r-- 1 user1 user1 220 Sep 18 2020 .bash_logout
-rw-r--r-- 1 user1 user1 3771 Sep 18 2020 .bashrc
drwx----- 2 user1 user1 4096 Feb  2 2023 .cache/
-rw-rw-r-- 1 user1 user1 426 Mar 14 2024 instrucciones.txt
-rwsr-sr-t 1 root   root  12 Sep 18 2020 keyboard.sh*
drwxrwxr-x 3 user1 user1 4096 Sep 18 2020 .local/
-rw-r--r-- 1 user1 user1 807 Sep 18 2020 .profile
```

2. Identificación de instrucciones en instrucciones.txt.

```
user1@ubuntu:~$ cat instrucciones.txt
¿Serás capaz de conseguir el usuario user5?

[REDACTED]
```

Cambiamos a directorio user2 y listamos su contenido, donde encontramos el archivo contraseña\_user2.txt en texto plano, el cual aloja la contraseña de user2.

```
user1@ubuntu:~$ cd ../user2
user1@ubuntu:/home/user2$ ll
total 32
drwxr-xr-x 3 user2 user2 4096 Jul 21 2022 ./
drwxr-xr-x 8 root root 4096 Sep 18 2020 ../
-rw----- 1 user2 user2 13 Jul 21 2022 .bash_history
-rw-r--r-- 1 user2 user2 220 Sep 18 2020 .bash_logout
-rw-r--r-- 1 user2 user2 3771 Sep 18 2020 .bashrc
-rw-rw-r-- 1 user2 user2 11 Sep 18 2020 contraseña_user2.txt
drwxrwxr-x 3 user2 user2 4096 Sep 18 2020 .local/
-rw-r--r-- 1 user2 user2 807 Sep 18 2020 .profile
```

```
user1@ubuntu:/home/user2$ cat contraseña_user2.txt
Alakazam65
```

3. Cambio a user2 mediante credenciales encontradas: su user2. Revisión de directorio de user3 y obtención de nueva contraseña desde el archivo oculto .historial.

```
user1@ubuntu:/home/user2$ su user2
Password:
user2@ubuntu:~$ cd ../user3
user2@ubuntu:/home/user3$ ll
total 40
drwxr-xr-x 3 user3 user3 4096 Jul 21 2022 ./
drwxr-xr-x 8 root root 4096 Sep 18 2020 ../
-rw----- 1 user3 user3 13 Jul 21 2022 .bash_history
-rw-r--r-- 1 user3 user3 220 Sep 18 2020 .bash_logout
-rw-r--r-- 1 user3 user3 3771 Sep 18 2020 .bashrc
-rw-r----- 1 user3 bulbasaur 28 Sep 18 2020 .historial
-rw-rw-r-- 1 user3 user3 677 Sep 18 2020 info.txt
drwxrwxr-x 3 user3 user3 4096 Sep 18 2020 .local/
-rw-r--r-- 1 user3 user3 807 Sep 18 2020 .profile
-rw----- 1 user3 user3 532 Sep 18 2020 .viminfo
user2@ubuntu:/home/user3$ cat .historial
La contraseña es Psyduck54
```

4. Cambio a user3: su user3. Localización de archivo cifrado contraseña.txt.cpt en el directorio de user4

```
user2@ubuntu:/home/user3$ su user3
Password:

user3@ubuntu:~$ cd ../user4
user3@ubuntu:/home/user4$ ll
total 52
drwxr-xr-x 5 user4 user4 4096 May 11 2023 ./
drwxr-xr-x 8 root root 4096 Sep 18 2020 ../
-rw----- 1 user4 user4 13 Jul 21 2022 .bash_history
-rw-r--r-- 1 user4 user4 220 Sep 18 2020 .bash_logout
-rw-r--r-- 1 user4 user4 3771 Sep 18 2020 .bashrc
drwxrwxr-x 2 user4 user4 4096 May 11 2023 .cache/
-rw-r----- 1 user4 user3 61 Feb 2 2023 contraseña.txt.cpt
-rwxrwxr-- 1 user4 user3 88 Sep 18 2020 dame_pass.sh*
drwxr----- 3 user4 user4 4096 Sep 18 2020 .gnupg/
-rw-rw-r-- 1 user4 user4 177 Sep 18 2020 instrucciones.txt
drwxrwxr-x 3 user4 user4 4096 Sep 18 2020 .local/
-rw-r--r-- 1 user4 user4 807 Sep 18 2020 .profile
-rw-r--r-- 1 user4 user4 0 Sep 18 2020 .sudo_as_admin_successful
-rw-rw---- 1 user4 pokemon 12 Sep 18 2020 token.txt
```

5. Identificación de token.txt protegido por permisos de grupo y lectura del archivo instrucciones.txt.

```

user3@ubuntu:/home/user4$ cat instrucciones.txt
El fichero de la contraseña está cifrado con ccencrypt.
Para descifrarlo necesitas la clave que está en token.txt.

Una vez tengas la clave, ejecuta el programa dame_pass.sh

user3@ubuntu:/home/user4$ cat token.txt
cat: token.txt: Permission denied

user3@ubuntu:/home/user4$ groups user2
user2 : user2 pokemon bulbasaur

```

6. Al pertenecer el archivo token.txt al grupo pokemon, cambiamos a user2, que pertenece a dicho grupo, para leerlo:

```

user3@ubuntu:/home/user4$ su user2
Password:

user2@ubuntu:/home/user4$ cat token.txt
qwerty67890

```

7. Ahora, se ejecuta el script dame\_pass.sh que en su código incluye:

```

echo "Introduce clave de cifrado:"
read key
ccdecrypt -d contraseña.txt.cpt -K $key

```

De esta forma, nos pide la clave obtenida de token.txt y desencripta el archivo contraseña.txt.cpt en un nuevo archivo contraseña.txt para el user3 tiene permisos de lectura, obteniendo la contraseña de user4.

```

user3@ubuntu:/home/user4$ ./dame_pass.sh
Introduce la clave de cifrado:
qwerty67890

user3@ubuntu:/home/user4$ cat contraseña.txt
La contraseña es Slowpoke79

```

8. Cambio a user4: su user4 y acceso final al directorio de user5 y lectura del archivo exito.txt con permisos sudo.

```

user4@ubuntu:~$ cat contraseña.txt
La contraseña es Slowpoke79

user4@ubuntu:~$ cd .. /user5
user4@ubuntu:/home/user5$ ll
total 32
drwxr-xr-x 3 user5 user5 4096 Jul 21 2022 .
drwxr-xr-x 8 root root 4096 Sep 18 2020 ..
-rw----- 1 user5 user5 18 Jul 21 2022 .bash_history
-rw-r--r-- 1 user5 user5 220 Sep 18 2020 .bash_logout
-rw-r--r-- 1 user5 user5 3771 Sep 18 2020 .bashrc
-rw-r--r-- 1 user5 user5 85 Sep 18 2020 exito.txt
drwxrwxr-x 3 user5 user5 4096 Sep 18 2020 .local/
-rw-r--r-- 1 user5 user5 807 Sep 18 2020 .profile

user4@ubuntu:/home/user5$ groups user4
user4 : user4 sudo pokemon
user4@ubuntu:/home/user5$ sudo cat exito.txt
[sudo] password for user4:

Conseguido!!
Escribe la palabra CALEIDOSCOPIO en el chat de slack para confirmarlo!

```

## **5. Resultados**

Se logró acceder exitosamente al usuario final (user5) y se pudo leer el archivo `exito.txt`, confirmando el éxito del reto. El proceso implicó el uso de comandos básicos de Linux y comprensión de permisos de archivos y grupos.

## **6. Aviso Legal**

Este informe corresponde a un ejercicio realizado exclusivamente en un entorno educativo y controlado. No contiene información ni vulnerabilidades de sistemas reales.