CÁTEDRA DE CIBERSEGURIDAD CIBERUGR, INCIBE-UGR

Nombre	History Rewind
Categoría	Forense
Dificultad	Fácil
Puntos	200

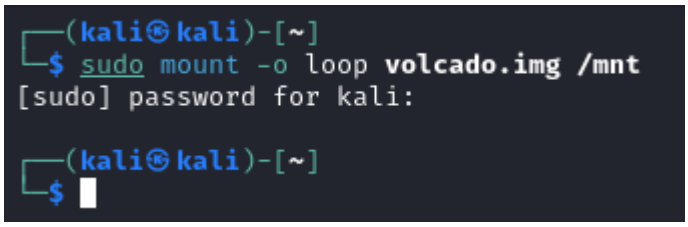
DESCRIPCIÓN DEL RETO

Algunas huellas del pasado pueden dejar más que recuerdos. Revisa con cuidado lo que ha quedado atrás, a menudo, las acciones del pasado revelan mucho más de lo que se muestra a simple vista. ¿Serás capaz de encontrar lo que otros intentaron ocultar?

WRITEUP

1. Monta la imagen de disco:

```
sudo mount -o loop volcado.img /mnt
```

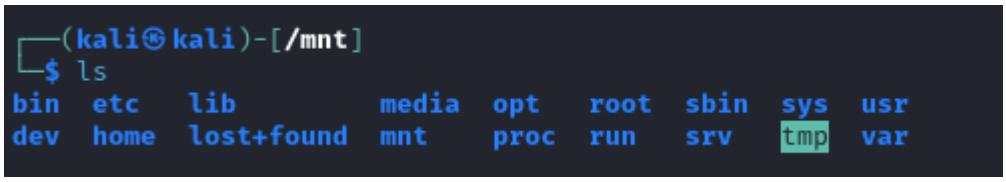


Nota: Si el comando anterior falla, utilizar estos dos:

```
sudo losetup /dev/loop0 volcado.img

sudo mount /dev/loop0 /mnt
```

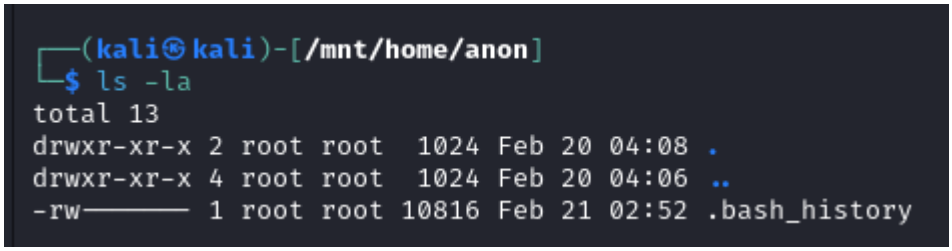
2. Accede al directorio donde se ha montado la imagen:

```
cd /mnt

ls
```



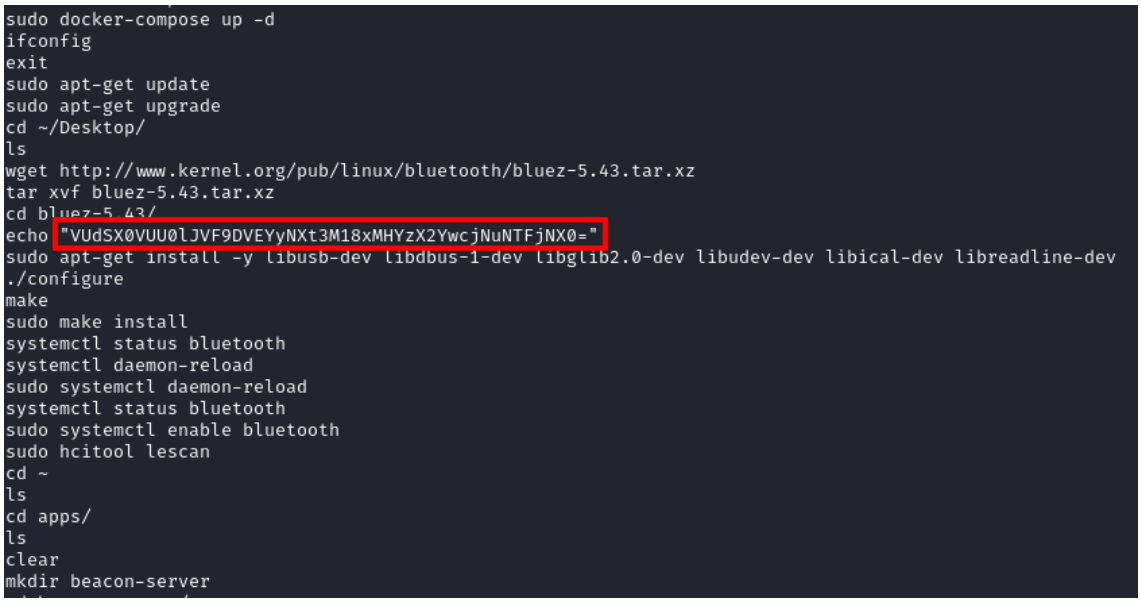
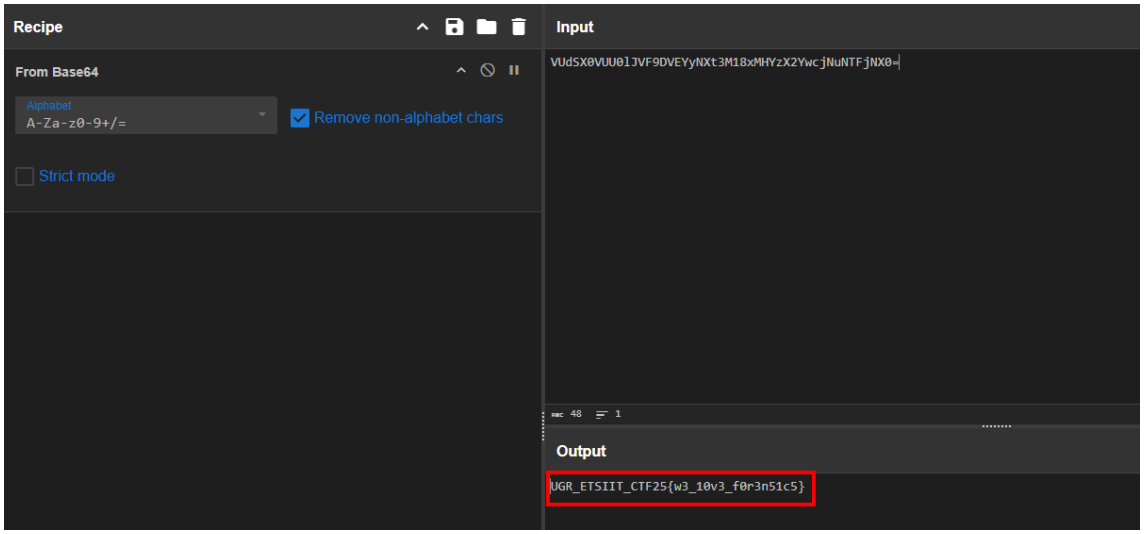
3. Accede al home del usuario “anon” y lista todos los archivos, incluyendo los ocultos:

```
cd /mnt/home/anon

ls -la
```



4. Inspecciona el contenido del archivo .bash_history y en una de las líneas se verá un echo con una cadena en base 64:

```
sudo cat .bash_history
```



5. Ve a cyberchef (https://gchq.github.io/CyberChef/) y decodifica la cadena: