



---

# HACKING ÉTICO

---

Unidad 1. Actividad 4/Bonus



11 DE OCTUBRE DE 2023  
CARLOS DÍAZ MONTES  
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Nivel 0. ....2

Nivel 2. ....3

Nivel 3 .....4

Nivel 4 .....4

Nivel 5 .....4

Nivel 6 .....4

Nivel 7 .....5

Nivel 8 .....5

Nivel 9 .....5


Nivel 10 .....5

Nivel 11 .....5

Nivel 0.


Me conecto mediante ssh:

```
(kali㉿kali)-[~]
$ ssh bandit0@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([51.20.13.48]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLFXC5CXlhmAAM/urerLY
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? Yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220' (ED25519) to
the list of known hosts.
```



```
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
```

```
bandit0@bandit.labs.overthewire.org's password:
```



Miramos el contenido del directorio readme:



## Nivel 3

```
spaces in this filename
bandit2@bandit:~$ ls -la
total 24
drwxr-xr-x 2 root root 4096 Oct 5 06:19 .
drwxr-xr-x 70 root root 4096 Oct 5 06:20 ..
-rw-r--r-- 1 root root 220 Jan 6 2022 .bash_lo
-rw-r--r-- 1 root root 3771 Jan 6 2022 .bashrc
-rw-r--r-- 1 root root 807 Jan 6 2022 .profile
-rw-r--r-- 1 bandit3 bandit2 33 Oct 5 06:19 spaces
bandit2@bandit:~$ cat spaces\ in\ this\ filename
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
bandit2@bandit:~$
```

## Nivel 4

```
bandit3@bandit:~$
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Oct 5 06:19 .
drwxr-xr-x 3 root root 4096 Oct 5 06:19 ..
-rw-r--r-- 1 bandit4 bandit3 33 Oct 5 06:19 .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$
```

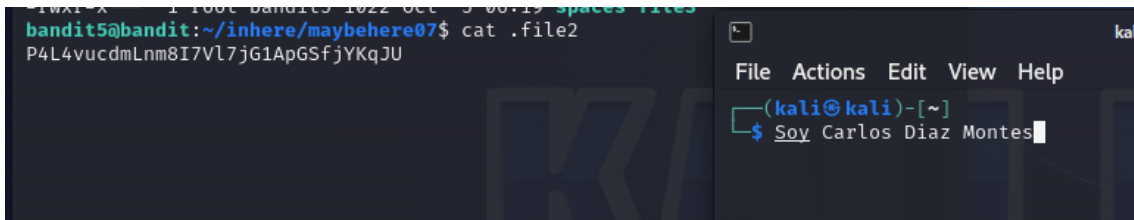
## Nivel 5

```
bandit4@bandit:~/inhere$ ls -la
total 48
drwxr-xr-x 2 root root 4096 Oct 5 06:19 .
drwxr-xr-x 3 root root 4096 Oct 5 06:19 ..
-rw-r--r-- 1 bandit5 bandit4 33 Oct 5 06:19 -file00
-rw-r--r-- 1 bandit5 bandit4 33 Oct 5 06:19 -file01
-rw-r--r-- 1 bandit5 bandit4 33 Oct 5 06:19 -file02
-rw-r--r-- 1 bandit5 bandit4 33 Oct 5 06:19 -file03
-rw-r--r-- 1 bandit5 bandit4 33 Oct 5 06:19 -file04
-rw-r--r-- 1 bandit5 bandit4 33 Oct 5 06:19 -file05
-rw-r--r-- 1 bandit5 bandit4 33 Oct 5 06:19 -file06
-rw-r--r-- 1 bandit5 bandit4 33 Oct 5 06:19 -file07
-rw-r--r-- 1 bandit5 bandit4 33 Oct 5 06:19 -file08
-rw-r--r-- 1 bandit5 bandit4 33 Oct 5 06:19 -file09
bandit4@bandit:~/inhere$ cat ←file00
QRrtZi
bandit4@bandit:~/inhere$ cat ←file01
7L3Y W E V h F
bandit4@bandit:~/inhere$ cat ←file02
y O \ - H x 2 K
bandit4@bandit:~/inhere$ cat ←file03
i x # e > V O p {
bandit4@bandit:~/inhere$ cat ←file04
g Q e E } : g j s < . e
bandit4@bandit:~/inhere$ cat ←file05
S e 0 [ 7 ] b < -
bandit4@bandit:~/inhere$ cat ←file06
G=1 B :
bandit4@bandit:~/inhere$ cat ←file07
lrIWWI6bB37kxfiCQZqUd0IYfr6eEqR
bandit4@bandit:~/inhere$
```

## Nivel 6

He estado mirando archivo a archivo, preguntar en clase si hay alguna forma más rápida de encontrarlo.

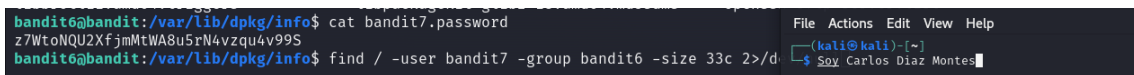
```
bandit5@bandit:~/inhere/maybehere07$ cat .file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```



## Nivel 7

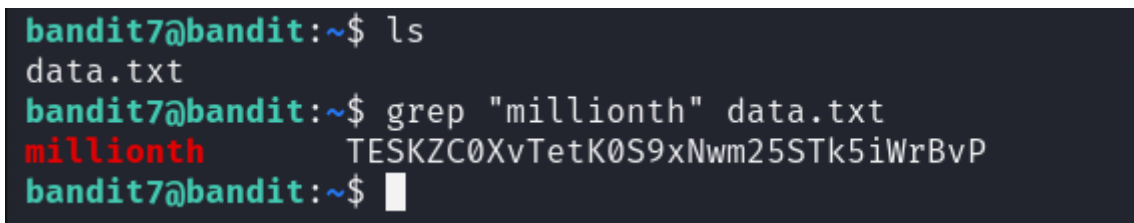
El comando de abajo es el que he usado para encontrar la ubicación del archivo.

```
bandit6@bandit:/var/lib/dpkg/info$ cat bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
bandit6@bandit:/var/lib/dpkg/info$ find / -user bandit7 -group bandit6 -size 33c 2>/d
```



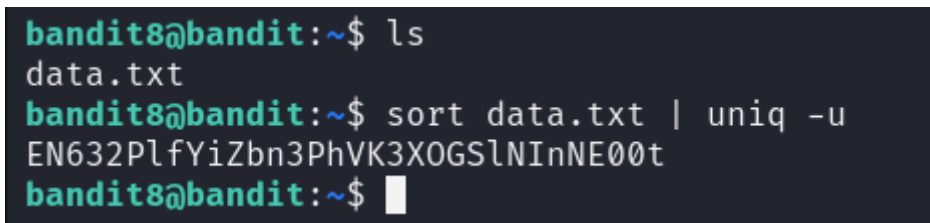
## Nivel 8

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ grep "millionth" data.txt
millionth      TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@bandit:~$
```



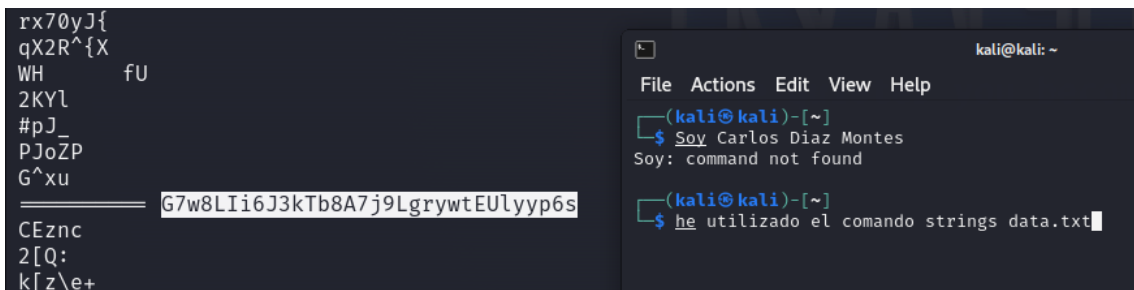
## Nivel 9

```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ sort data.txt | uniq -u
EN632PlfYiZbn3PhVK3XOGSlnInNE00t
bandit8@bandit:~$
```



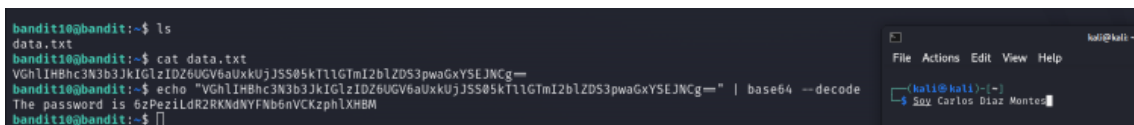
## Nivel 10

```
rx70yJ{
qX2R^{X
WH      fU
2KYl
#pJ_
PJoZP
G^xu
===== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
CEznc
2[Q:
k[z\e+
```



## Nivel 11

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHh3N3B3bkIzIDZ6UGV6aUxkUjJSOj5kT1lGTmI2b1ZDS3pwaGxYSEJNCg==
bandit10@bandit:~$ echo "VGhlIHh3N3B3bkIzIDZ6UGV6aUxkUjJSOj5kT1lGTmI2b1ZDS3pwaGxYSEJNCg==" | base64 --decode
The password is 6zPezILD2RKNdNYFNb6nVCKzphlXhBM
bandit10@bandit:~$
```



Por último, muestro que la contraseña que me da me deja conectarme a bandit11:

```
For support, questions or comments, contact us on discord or IRC.  
Enjoy your stay!  
bandit11@bandit:~$
```

File Actions Edit View Help

(kali@kali)-[~]  
\$ Soy Carlos Diaz Montes