

SOC (Security Operations Center)

Módulo 2



Linux – OverTheWire

Bandit - Ejercicios


Sheila Fernández Cisneros – 02/06/2024

Nivel 0 -> 1

Contraseña almacenada en un archivo de texto llamado “readme”. Buscar dicho archivo y mostrar el contenido. COMANDOS RECOMENDADOS: ls, cd, cat, find

Establecemos la conexión ssh y cuando acabemos el reto saldremos de la conexión con éxito (esto se hará para todos los niveles): `ssh bandit0@bandit.labs.overthewire.org -p 2220`

```
(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 e
stablished.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RRcELfXC5CXlhmAAM/ureryLY.
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 know
n hosts.
```



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

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

Introducimos la contraseña bandit0 y entramos al juego!.

Nos encontramos en un directorio que no conocemos, lo primero que suelo hacer en estos casos es usar el comando ``ls -la`` para que nos liste todos los archivos que haya.

El comando `ls -la` en Unix/Linux se utiliza para listar el contenido de un directorio con detalles adicionales. Aquí está la explicación concisa de cada componente:

- ls: Lista los archivos y directorios en el directorio actual.
- -l: Utiliza el formato de lista larga. Esto muestra detalles adicionales como permisos, número de enlaces, propietario, grupo, tamaño del archivo y fecha/hora de la última modificación.
- -a: Muestra todos los archivos, incluidos los ocultos (aquellos cuyo nombre empieza con un punto .).

Seguimos la pista del enunciado y mostramos el contenido del archivo ``readme`` con el comando ``cat`` y encontramos la flag!.

```
bandit0@bandit:~$ ls -la
total 24
drwxr-xr-x  2 root    root    4096 Oct  5  2023 .
drwxr-xr-x 70 root    root    4096 Oct  5  2023 ..
-rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
-rw-r--r--  1 root    root     807 Jan  6  2022 .profile
-rw-r-----  1 bandit1 bandit0   33 Oct  5  2023 readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
bandit0@bandit:~$
```

Contraseña: NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

Nivel 1 -> 2

Contraseña almacenada en un archivo de texto llamado “-”. Buscar dicho archivo y mostrar el contenido, teniendo en cuenta que “-” es un símbolo especial.

COMANDOS RECOMENDADOS: ls, cd, cat, find

Conexión ssh al nivel 1: ssh bandit1@bandit.labs.overthewire.org -p 2220

Este reto tiene una gran pista, nos dice que tenemos que mostrar el archivo `.` para encontrar la flag, esto se hace con el comando `cat ./-`.

- cat: Comando para mostrar el contenido de un archivo.
- ./: Indica que el archivo está en el directorio actual.
- -: Nombre del archivo.

```
bandit1@bandit:~$ ls -la
total 24
-rw-r-----  1 bandit2 bandit1   33 Oct  5  2023 -
drwxr-xr-x  2 root    root    4096 Oct  5  2023 .
drwxr-xr-x 70 root    root    4096 Oct  5  2023 ..
-rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
-rw-r--r--  1 root    root     807 Jan  6  2022 .profile
bandit1@bandit:~$ cat ./-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit1@bandit:~$
```

Contraseña: rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

Nivel 2 -> 3

Contraseña almacenada en un archivo de texto llamado “spaces in this filename”. Buscar dicho archivo y mostrar el contenido, teniendo en cuenta que el nombre del archivo contiene espacios (comprobar que pasa si se hace de manera normal).

COMANDOS RECOMENDADOS: ls, cd, cat, find

Conexión ssh al nivel 2: ssh bandit2@bandit.labs.overthewire.org -p 2220

Este ejercicio de nuevo tiene una pista que dice donde está la flag. Mostramos el contenido del archivo space in this filename, en este caso usamos comillas para indicar al comando cat que toda la frase forma parte del nombre del archivo, si no fuera así, los espacios no los interpretaría como parte del mismo.

```
bandit2@bandit:~$ ls -la
total 24
drwxr-xr-x  2 root    root    4096 Oct  5  2023 .
drwxr-xr-x 70 root    root    4096 Oct  5  2023 ..
-rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root    root   3771 Jan  6  2022 .bashrc
-rw-r--r--  1 root    root    807 Jan  6  2022 .profile
-rw-r-----  1 bandit3 bandit2   33 Oct  5  2023 spaces in this filename
bandit2@bandit:~$ cat "spaces in this filename"
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
bandit2@bandit:~$
```

Contraseña: aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

Nivel 3 -> 4

Contraseña almacenada en un archivo de texto oculto llamado en el directorio llamado “inhere”. Buscar dicho archivo y mostrar el contenido. Para buscar el nombre del archivo oculto se recomienda buscar en el manual (man) del comando “ls” la función de cada una de las flags, como “-a”, “-l”, etc.

COMANDOS RECOMENDADOS: ls, cd, cat, find

Conexión ssh al nivel 3: ssh bandit3@bandit.labs.overthewire.org -p 2220

Este ejercicio viene prácticamente resuelto también, volvemos a usar el comando `cat` para mostrar el contenido del archivo `.hidden`.

```

bandit3@bandit:~$ ls -la
total 24
drwxr-xr-x  3 root root 4096 Oct  5  2023 .
drwxr-xr-x 70 root root 4096 Oct  5  2023 ..
-rw-r--r--  1 root root  220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root root 3771 Jan  6  2022 .bashrc
drwxr-xr-x  2 root root 4096 Oct  5  2023 inhere
-rw-r--r--  1 root root  807 Jan  6  2022 .profile
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -la
total 12
drwxr-xr-x 2 root  root  4096 Oct  5  2023 .
drwxr-xr-x 3 root  root  4096 Oct  5  2023 ..
-rw-r----- 1 bandit4 bandit3  33 Oct  5  2023 .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$

```

Contraseña: 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

Nivel 4 -> 5

Contraseña almacenada en un archivo de texto en el directorio “inhere”. Ahora hay varios archivos, pero solamente uno es leíble por humanos (esto quiere decir que el formato es “ASCII text”). Además, los archivos de texto empiezan por el símbolo “-”, así que hay que operar como en el Nivel 1 -> 2.

COMANDOS RECOMENDADOS: ls, cd, cat, find, file

Conexión ssh al nivel 4: `ssh bandit4@bandit.labs.overthewire.org -p 2220`

En este caso he usado la fuerza bruta de prueba y error hasta que he encontrado el archivo que contenía la flag. Usamos de nuevo el comando ``cat./-filename``.


```

bandit4@bandit:~$ ls -la
total 24
drwxr-xr-x  3 root root 4096 Oct  5  2023 .
drwxr-xr-x 70 root root 4096 Oct  5  2023 ..
-rw-r--r--  1 root root  220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root root 3771 Jan  6  2022 .bashrc
drwxr-xr-x  2 root root 4096 Oct  5  2023 inhere
-rw-r--r--  1 root root  807 Jan  6  2022 .profile
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -la
total 48
drwxr-xr-x  2 root  root  4096 Oct  5  2023 .
drwxr-xr-x  3 root  root  4096 Oct  5  2023 ..
-rw-r-----  1 bandit5 bandit4  33 Oct  5  2023 -file00
-rw-r-----  1 bandit5 bandit4  33 Oct  5  2023 -file01
-rw-r-----  1 bandit5 bandit4  33 Oct  5  2023 -file02
-rw-r-----  1 bandit5 bandit4  33 Oct  5  2023 -file03
-rw-r-----  1 bandit5 bandit4  33 Oct  5  2023 -file04
-rw-r-----  1 bandit5 bandit4  33 Oct  5  2023 -file05
-rw-r-----  1 bandit5 bandit4  33 Oct  5  2023 -file06
-rw-r-----  1 bandit5 bandit4  33 Oct  5  2023 -file07
-rw-r-----  1 bandit5 bandit4  33 Oct  5  2023 -file08
-rw-r-----  1 bandit5 bandit4  33 Oct  5  2023 -file09
bandit4@bandit:~/inhere$ ls -a
.  .. -file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ cat ./-file00
QHRrtZ0i0
bandit4@bandit:~/inhere$ cat ./-file01
7L300Y* W0000E0Y0
bandit4@bandit:~/inhere$ cat ./-file02
000y000000`0\0-0Hx00200Kbandit4@bandit:~/inhere$ cat ./-file03
00i0x0#e0>0V000p{0
bandit4@bandit:~/inhere$ cat ./-file04
00gQ00eE}:0g000j800000<.0ebandit4@bandit:~/inhere$ cat ./-file05
00S000e 000000]70000000b0<0-bandit4@bandit:~/inhere$ cat ./-file06
G=10000000B:0"
bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEqR
bandit4@bandit:~/inhere$

```

Contraseña: lrIWWI6bB37kxfiCQZqUdOIYfr6eEqR

Nivel 5 -> 6

Contraseña almacenada en un archivo de texto en alguno de los directorios que hay en “inhere”. Las propiedades que se indican del archivo de texto que buscamos son las siguientes: leíble por humanos (formato “ASCII text”), tamaño de 1033 Bytes y no ejecutable. Se recomienda usar pipes (“|”) y la ayuda de “find”.

COMANDOS RECOMENDADOS: ls, cd, cat, find, file, du, grep

Conexión ssh al nivel 5: ssh bandit5@bandit.labs.overthewire.org -p 2220

```

bandit5@bandit:~$ ls -la
total 24
drwxr-xr-x  3 root root   4096 Oct  5 2023 .
drwxr-xr-x 70 root root   4096 Oct  5 2023 ..
-rw-r--r--  1 root root    220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root root   3771 Jan  6 2022 .bashrc
drwxr-x--- 22 root bandit5 4096 Oct  5 2023 inhere
-rw-r--r--  1 root root    807 Jan  6 2022 .profile
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls -la
total 88
drwxr-x--- 22 root bandit5 4096 Oct  5 2023 .
drwxr-xr-x  3 root root   4096 Oct  5 2023 ..
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere00
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere01
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere02
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere03
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere04
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere05
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere06
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere07
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere08
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere09
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere10
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere11
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere12
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere13
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere14
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere15
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere16
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere17
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere18
drwxr-x---  2 root bandit5 4096 Oct  5 2023 maybehere19
bandit5@bandit:~/inhere$

```

En este caso como necesitamos encontrar un archivo conociendo su tamaño, usamos el comando `find` para encontrar el archivo de 1033 bytes:

find . -size 1033c

- `find`: Comando para buscar archivos y directorios.
- `.`: Directorio actual.
- `-size 1033c`: Busca archivos de tamaño exactamente 1033 bytes (c significa bytes).

```

bandit5@bandit:~/inhere$ find . -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

```

Contraseña: P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

Nivel 6 -> 7

Contraseña almacenada en algún archivo de texto ubicado en cualquier directorio del servidor (esto obliga a buscar desde el directorio raíz (/)). Las propiedades de este archivo son las siguientes: usuario propietario “bandit7”, grupo propietario “bandit6” y tamaño del archivo de 33 Bytes. Redireccionar errores al “/dev/null”.

COMANDOS RECOMENDADOS: ls, cd, cat, find, file, du, grep

Conexión ssh al nivel 6: ssh bandit6@bandit.labs.overthewire.org -p 2220

Utilizamos el comando **find** para buscar archivos que cumplan con los criterios que nos indica el enunciado:

find / -user bandit7 -group bandit6 -size 33c 2>/dev/null

- / indica que la búsqueda debe realizarse en todo el sistema.
- -user bandit7 busca archivos propiedad del usuario bandit7.
- -group bandit6 busca archivos pertenecientes al grupo bandit6.
- -size 33c busca archivos de 33 bytes de tamaño.
- 2>/dev/null redirige los mensajes de error a /dev/null para que no se muestren en la terminal.


```

bandit6@bandit:~$ ls -la
total 20
drwxr-xr-x  2 root root 4096 Oct  5 2023 .
drwxr-xr-x 70 root root 4096 Oct  5 2023 ..
-rw-r--r--  1 root root  220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root root 3771 Jan  6 2022 .bashrc
-rw-r--r--  1 root root  807 Jan  6 2022 .profile
bandit6@bandit:~$ cd
bandit6@bandit:~$ cd ..
bandit6@bandit:/home$ cd ..
bandit6@bandit:/$ ls -la
total 10476
drwxr-xr-x  22 root root    4096 Jun  2 18:02 .
drwxr-xr-x  22 root root    4096 Jun  2 18:02 ..
lrwxrwxrwx   1 root root      7 Sep 19 2023 bin -> usr/bin
drwxr-xr-x   4 root root    4096 Sep 19 2023 boot
drwxr-xr-x  14 root root   3260 Jun  2 18:02 dev
drwxr-xr-x   7 root root    4096 Oct  5 2023 drifter
drwxr-xr-x 106 root root  12288 Oct  5 2023 etc
drwxr-xr-x   3 root root    4096 Oct  5 2023 formulaone
drwxr-xr-x  70 root root    4096 Oct  5 2023 home
drwxr-xr-x   8 root root    4096 Oct  5 2023 krypton
lrwxrwxrwx   1 root root      7 Sep 19 2023 lib -> usr/lib
lrwxrwxrwx   1 root root      9 Sep 19 2023 lib32 -> usr/lib32
lrwxrwxrwx   1 root root      9 Sep 19 2023 lib64 -> usr/lib64
lrwxrwxrwx   1 root root     10 Sep 19 2023 libx32 -> usr/libx32
drwx-----  2 root root   16384 Sep 19 2023 lost+found
drwxr-xr-x   2 root root    4096 Sep 19 2023 media
drwxr-xr-x   2 root root    4096 Sep 19 2023 mnt
drwxr-xr-x   7 root root    4096 Oct  5 2023 opt
dr-xr-xr-x 567 root root      0 Jun  2 18:01 proc
drwx-----  9 root root    4096 May  6 20:43 root
drwxr-xr-x  26 root root    1000 Jun  2 18:02 run
lrwxrwxrwx   1 root root      8 Sep 19 2023 sbin -> usr/sbin
drwx-----  8 root root    4096 Sep 19 2023 snap
drwxr-xr-x   2 root root    4096 Sep 19 2023 srv
dr-xr-xr-x  13 root root      0 Jun  2 18:01 sys
drwxrwx-wt  91 root root 10633216 Jun  2 19:48 tmp
drwxr-xr-x  14 root root    4096 Oct  5 2023 usr
drwxr-xr-x  13 root root    4096 Oct  5 2023 var
bandit6@bandit:/$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:/$ cat /var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
bandit6@bandit:/$

```

Contraseña: z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

Nivel 7 -> 8

Contraseña almacenada en archivo llamado “data.txt”, cerca de la palabra “millionth”.

COMANDOS RECOMENDADOS: ls, cd, cat, find, file, du, grep

Conexión ssh al nivel 7: ssh bandit7@bandit.labs.overthewire.org -p 2220

Para este reto, usamos el comando `grep` que se utiliza para buscar patrones dentro de archivos.

grep [opciones] patrón [archivo]

```
bandit7@bandit:~$ ls -la
total 4108
drwxr-xr-x  2 root    root      4096 Oct  5  2023 .
drwxr-xr-x 70 root    root      4096 Oct  5  2023 ..
-rw-r--r--  1 root    root        220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root    root      3771 Jan  6  2022 .bashrc
-rw-r-----  1 bandit8 bandit7 4184396 Oct  5  2023 data.txt
-rw-r--r--  1 root    root        807 Jan  6  2022 .profile
bandit7@bandit:~$ grep "millionth" data.txt
millionth      TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@bandit:~$
```

Contraseña: TESKZC0XvTetK0S9xNwm25STk5iWrBvP

Nivel 8 -> 9

Contraseña almacenada en el archivo de texto llamado “data.txt”. La contraseña que buscamos es la única que se muestra una única vez en el archivo. Para ello se recomienda mostrar de manera ordenada el archivo y filtrar por aquella línea que aparezca solamente una vez.

COMANDOS RECOMENDADOS: `ls`, `cd`, `cat`, `find`, `sort`, `uniq`, `strings`, `grep`

Conexión ssh al nivel 8: `ssh bandit8@bandit.labs.overthewire.org -p 2220`

Para este reto usamos el comando `sort` y el comando `uniq`, el primero ordena los datos y `uniq` selecciona datos únicos.

- `sort data.txt`: Ordena el contenido del archivo data.txt.
- `|`: Pasa la salida del comando `sort` al comando `uniq`.
- `uniq -u`: Filtra y muestra solo las líneas que son únicas en el archivo ordenado.

He usado una redirección `<` para mandar el contenido de data.txt al comando `sort` pero se podría también hacer `sort data.txt`.

```
bandit8@bandit:~$ ls -la
total 56
drwxr-xr-x  2 root    root    4096 Oct  5  2023 .
drwxr-xr-x 70 root    root    4096 Oct  5  2023 ..
-rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
-rw-r-----  1 bandit9 bandit8 33033 Oct  5  2023 data.txt
-rw-r--r--  1 root    root     807 Jan  6  2022 .profile
bandit8@bandit:~$ <data.txt sort | uniq -u
EN632PlfYiZbn3PhVK3XOGSINInNE00t
bandit8@bandit:~$
```

Contraseña: EN632PlfYiZbn3PhVK3XOGSINInNE00t

Nivel 9 -> 10

Contraseña almacenada en el archivo de texto llamado “data.txt”. El archivo es casi entero no leible por humanos, y la contraseña está en una de los pocos strings que sí lo son. Además, está precedido de varios caracteres “=”.

COMANDOS RECOMENDADOS: ls, cd, cat, find, sort, uniq, strings, grep

Conexión ssh al nivel 9: ssh bandit9@bandit.labs.overthewire.org -p 2220

Este reto ha sido mas desafiante, en este caso usamos los comandos `strings` y `grep`.

- strings data.txt: Encuentra cadenas legibles en data.txt.
- |: Pasa la salida de strings data.txt como entrada al siguiente comando.
- grep "=====": Filtra la salida para mostrar solo las líneas que contienen "=====".

```
bandit9@bandit:~$ ls -la
total 40
drwxr-xr-x  2 root    root    4096 Oct  5  2023 .
drwxr-xr-x 70 root    root    4096 Oct  5  2023 ..
-rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
-rw-r-----  1 bandit10 bandit9 19379 Oct  5  2023 data.txt
-rw-r--r--  1 root    root     807 Jan  6  2022 .profile
bandit9@bandit:~$ strings data.txt | grep "====="
x]T===== theG)"
===== passwordk^
===== is
===== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
bandit9@bandit:~$
```

Contraseña: G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

Nivel 10 -> 11

Contraseña almacenada en el archivo de texto llamado “data.txt”. Se indica que el archivo está codificado en Base64, por lo que, aunque al mostrar el contenido de manera normal pueda parecer una contraseña, hay que decodificar este archivo para encontrar la contraseña que se busca. Se recomienda ver el manual (man) del comando “base64”.

COMANDOS RECOMENDADOS: ls, cd, cat, find, sort, uniq, strings, grep, base64

El comando base64 tiene una flag -d para decodificar. En este caso se redirecciona el contenido de data.txt al comando y nos muestra la flag.

- base64: El comando que maneja la codificación y decodificación en base64.
- -d o --decode: La opción que especifica que la operación es decodificar los datos de entrada.

También se podría usar: base64 -d data.txt.

```
bandit10@bandit:~$ man base64
bandit10@bandit:~$ ls -la
total 24
drwxr-xr-x  2 root    root    4096 Oct  5  2023 .
drwxr-xr-x 70 root    root    4096 Oct  5  2023 ..
-rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
-rw-r-----  1 bandit11 bandit10  69 Oct  5  2023 data.txt
-rw-r--r--  1 root    root     807 Jan  6  2022 .profile
bandit10@bandit:~$ <data.txt base64 -d
The password is 6zPezILdR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$
```

Contraseña: 6zPezILdR2RKNdNYFNb6nVCKzphlXHBM

This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>
bandit11@bandit.labs.overthewire.org's password:

13