

OVER THE WIRE BANDIT WARGAME

Level 0)

Establishing the connection to the OTW site with my kali VM

```
(kali㉿kali)-[~]
$ mkdir OTWbandit

(kali㉿kali)-[~]
$ cd OTWbandit

(kali㉿kali)-[~/OTWbandit]
$ ssh bandit0@bandit.labs.overthewire.org -p 2220
```



After logging into the bandit0 as the game said theres the password in the readme file so we first ls -l and then cat the readme file to get the PW, heading onto the next level

```
bandit0@bandit:~$ ls -l
total 4
-rw-r--r-- 1 bandit1 bandit0 438 Apr 10 14:22 readme
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNWOZ0Ta6ip5If
bandit0@bandit:~$
```

Level 1)

```
bandit1@bandit:~$ ls -l
total 4
-rw-r--r-- 1 bandit2 bandit1 33 Apr 10 14:23 -
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(kali㉿kali)-[~/OTWbandit]
$ echo 263JGJPfgU6LtdEvgfWU1XP5yac29mFx > 2

(kali㉿kali)-[~/OTWbandit]
$ ssh bandit2@bandit.labs.overthewire.org -p 2220
```

Here, after logging into the bandit1, it said the password for level 2 is in the - file, so we first use ls -l to list all the files in the directory, then we see the file with special character and to cat a special character file we use ./ before the file name to tell cat that it's a file in the pwd and not an option (cat treats "--" as options), therefore we use "cat ./-" to get the password

Level 2)

```
bandit2@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  2 root    root    4096 Apr 10 14:23 ./
4 drwxr-xr-x 70 root    root    4096 Apr 10 14:24 ../
4 -rw-r--r--  1 root    root     220 Mar 31 2024 .bash_logout
4 -rw-r--r--  1 root    root   3771 Mar 31 2024 .bashrc
4 -rw-r--r--  1 root    root     807 Mar 31 2024 .profile
4 -rw-r----- 1 bandit3 bandit2   33 Apr 10 14:23 spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
MNk8KNH3Usiio41PRUEoDFPqfxLPLSmx
bandit2@bandit:~$
```

Here, the level said the password is in a file called “spaces in this filename” so to cat this file we use “\” to escape each space so that when I used the cat command it would interpret each string as a filename and then it reveals the password.

Level 3)

```
bandit3@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root    root    4096 Apr 10 14:23 ./
4 drwxr-xr-x 70 root    root    4096 Apr 10 14:24 ../
4 -rw-r--r--  1 root    root     220 Mar 31 2024 .bash_logout
4 -rw-r--r--  1 root    root   3771 Mar 31 2024 .bashrc
4 drwxr-xr-x  2 root    root    4096 Apr 10 14:23 inhere/
4 -rw-r--r--  1 root    root     807 Mar 31 2024 .profile
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls -alps
total 12
4 drwxr-xr-x  2 root    root    4096 Apr 10 14:23 ./
4 drwxr-xr-x  3 root    root    4096 Apr 10 14:23 ../
4 -rw-r----- 1 bandit4 bandit3   33 Apr 10 14:23 ...Hiding-From-You
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(kali㉿kali)-[~/OTWbandit]
$ echo 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ > 4
```

Here, as the level said the password is in the “inhere” directory, so we use cd to change directory to inhere directory and there we use ls -alps again to list all the files, we see a “...Hiding-From-You” file, cat it so it reveals the password to our level 4

Level 4)

```
bandit4@bandit:~$ ls -alps
total 24
4 drwxr-xr-x 3 root root 4096 Apr 10 14:23 ./
4 drwxr-xr-x 70 root root 4096 Apr 10 14:24 ../
4 -rw-r--r-- 1 root root 220 Mar 31 2024 .bash_logout
4 -rw-r--r-- 1 root root 3771 Mar 31 2024 .bashrc
4 drwxr-xr-x 2 root root 4096 Apr 10 14:23 inheres/
4 -rw-r--r-- 1 root root 807 Mar 31 2024 .profile
bandit4@bandit:~$ cd inheres/
bandit4@bandit:~/inheres$ ls -alps
total 48
4 drwxr-xr-x 2 root root 4096 Apr 10 14:23 ./
4 drwxr-xr-x 3 root root 4096 Apr 10 14:23 ../
4 -rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file00
4 -rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file01
4 -rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file02
4 -rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file03
4 -rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file04
4 -rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file05
4 -rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file06
4 -rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file07
4 -rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file08
4 -rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file09
bandit4@bandit:~/inheres$ find . -type f | xargs file
./-file05: data
./-file03: data
./-file06: data
./-file02: data
./-file01: data
./-file09: data
./-file00: PGP Secret Sub-key -
./-file04: data
./-file08: data
./-file07: ASCII text
bandit4@bandit:~/inheres$ cat ./-file00
```

```
bandit4@bandit:~/inheres$ cat ./-file00
♦n0T♦♦♦S ♦pls]-EH♦♦:-♦Z♦
bandit4@bandit:~/inheres$
bandit4@bandit:~/inheres$ cat ./-file07
4oQYVPkxZ00E005pTW81FB8j8LxXGUQw
bandit4@bandit:~/inheres$ EXIT
EXIT: command not found
bandit4@bandit:~/inheres$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Here, level 4 said the password was in a human readable format file, so we cded our way to inheres/ then “ls -alps” to check all the files, it showed files from 00 through 09, now to check what type of a file each is, we use “find . -type f | xargs file” what this does is it finds all the regular files in the current directory and sub directories (if any) and then it also tells you which file is what type which helped us in differentiating the files containing password.

Level 5)

```
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ ls -alps
total 88
4 drwxr-x— 22 root bandit5 4096 Apr 10 14:23 ./
4 drwxr-xr-x 3 root root 4096 Apr 10 14:23 ../
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere00/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere01/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere02/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere03/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere04/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere05/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere06/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere07/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere08/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere09/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere10/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere11/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere12/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere13/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere14/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere15/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere16/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere17/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere18/
4 drwxr-x— 2 root bandit5 4096 Apr 10 14:23 maybehere19/
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

Here, in level 5 we were asked to do the same thing so we cded to inhere and found 20 maybehere files, again used the command “find . type f -size 1033c ! executable” meaning finding the particular file which is human readable, is of 1033 bytes of size (1033c) and is not executable (! Executable) hence giving us the password.

Level 6)

```
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
find: '/root': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/885568/task/885568/fdinfo/6': No such file or directory
find: '/proc/885568/task/885568/fdinfo/5': No such file or directory
find: '/proc/885568/task/885568/fdinfo/4': No such file or directory
find: '/var/lib/polkit-1': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/chrony': Permission denied
find: '/var/lib/amazon': Permission denied
find: '/var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/snapd/cookie': Permission denied
find: '/var/lib/snapd/void': Permission denied
find: '/var/lib/private': Permission denied
find: '/drifter/drifter14_src/axTLS': Permission denied
find: '/tmp': Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIUc0ymOdMaLn0LFVAaj
bandit6@bandit:~$
```

Here, the level told us that the PW is stored somewhere on the server and is owned by user bandit7 owned by group bandit6 33 bytes in size, so we used -user bandit7 for file to be of bandit7, used -group bandit 6 for the file to be of bandit6 group and 33c for the file to be of 33 bytes, hence getting the password (highlighted part)

Level 7)

```
bandit7@bandit:~$ ls -alps
total 4108
4 drwxr-xr-x 2 root root 4096 Apr 10 14:23 ./
4 drwxr-xr-x 70 root root 4096 Apr 10 14:24 ../
4 -rw-r--r-- 1 root root 220 Mar 31 2024 .bash_logout
4 -rw-r--r-- 1 root root 3771 Mar 31 2024 .bashrc
4088 -rw-r----- 1 bandit8 bandit7 4184396 Apr 10 14:23 data.txt
4 -rw-r--r-- 1 root root 807 Mar 31 2024 .profile
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth dfwvzFQ14mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Here, the level told us that the password was next to the word “millionth”, so we use “strings data.txt | grep “millionth” this extracts all the readable text strings from the data.txt file which then piped as an input to grep “millionth”, grep efficiently searches throughout the file for the millionth word and when it finds it, prints the whole containing the password next to it aswell, if it isn’t matched then grep just discards it.

Level 8)

```
bandit8@bandit:~$ sort data.txt | uniq -c
10 0LLAU8Hx0a5E8URNEITfTie9sy6tcpeE
10 0oTVZsmZ20mngEgPis8LloSSnuBmm7t9
10 11RbnkUhGZG3V5XHw9YBKPWcdZTQrYSQ
10 3M5U6xE6bEuGjktQvDD4eyHnW3bwvCkj
10 3WrYuQdo7JuGsvyB8hRss8A1uKcda2q4
1 4CKMh1JI91bUIZZPXQdGana14xvAg0JM
10 4rrSr6IONT8TbtjY0fBa6G5SxLu76X4U
10 5EL94fXpDzA3o08q2IFwAQ7Wwd0BnUz2
10 5H1aeINYBEB5D2SFLQqdbuzFmORwBo95
```

Here, the level said that the password is a line which only occurs once so we use “sort data.txt | uniq -c” this sorts the data.txt file and then pipes that as input to the “uniq -c” which mean count thus prefixing the lines by the no. of their occurrences, hence giving the answer

Another way of doing this is using grep which then shortens the output to showing just that one line occurs once, the “^” matches the beginning of the line.

```
bandit8@bandit:~$ sort data.txt | uniq -c | grep "^ *1 "
1 4CKMh1JI91bUIZZPXQdGana14xvAg0JM
bandit8@bandit:~$
```

Level 9)

```
bandit9@bandit:~$ strings data.txt | grep "="
,k=?
@k*=
===== the
#e=in
g+=ypF
ea+=
K>=*<
===== password{k
===== is
1R=j/
e=<2g%
+G/YD=
=wDk
=3?lOt
===== FGUW5iLLVJrxX9kMYMmLN4MgbpfMiqey
=D!f
H =sS
```

Here, the level told us that the password was preceded with many "=" so we used "strings data.txt | grep "=", the former part before the pipe extracts all the readable strings from the data.txt and sends as input to the latter part which is "grep "=", what this does is it searches for all the signs containing = and then prints the whole line hence printing the password too