

# BANDIT

- Level 0 :

```
yasasri@yasasri:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
bandit0@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ Playing the games ]--
```

```
--[ Playing the games ]--

This machine might hold several wargames.
If you are playing "somegame", then:

* USERNAMES are somegame0, somegame1, ...
* Most LEVELS are stored in /somegame/.
* PASSWORDS for each level are stored in /etc/somegame_pass/.

Write-access to homedirectories is disabled. It is advised to create a
working directory with a hard-to-guess name in /tmp/. You can use the
command "mktemp -d" in order to generate a random and hard to guess
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice:

* don't leave orphan processes running
* don't leave exploit-files laying around
* don't annoy other players
* don't post passwords or spoilers
* again, DONT POST SPOILERS!
  This includes writeups of your solution on your blog or website!

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled
by default, although ASLR has been switched off. The following
compiler flags might be interesting:

-m32          compile for 32bit
-fno-stack-protector  disable ProPolice
-Wl,-z,norelro  disable relro
```

```
In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.

Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!
```

To ssh into a machine, I used a Linux Terminal.. I used a very basic command ssh for that.. After getting into it, it will ask us to give a password which is “bandit0” which is already given to us at the beginning.. After I enter the password, I got connected to bandit0.. And we need to go to overthewire and see the corresponding task and perform it to get the password to log into the next level..

- Level 0 to Level 1 :

```
bandit0@bandit:~$ ls
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: ZjLjTmM6FvvyRnrb2rfNW0Z0Ta6ip5If

bandit0@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.
```

The task is to get the password for the next level which is stored in the file called “readme”.. I used the command “ls” to see all the files present in the bandit0.. It gives the list of all the files and directories present in the home directory.. When I typed “ls”, we can see there’s only one file there.. and that’s the one we want to read.. So, to read what’s in that file, we use a command called “cat”.. So cat “filename” gives us what’s in that particular file.. So, we need to type “cat readme”.. After using that command, we got the password for the next level.. I copied that and logged out of bandit0 and then logged into bandit 1..


- Level 1 to Level 2 :

```
yasasri@Yasasri:~$ ssh bandit1@bandit.labs.overthewire.org -p 2220
```



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

```
bandit1@bandit.labs.overthewire.org's password:
```



```
www.ver he ire.org
```

```
Welcome to OverTheWire!
```

```
If you find any problems, please report them to the #wargames channel on  
discord or IRC.
```


```
--[ Playing the games ]--
```

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat < "-"
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.
```

I logged into level 1.. The task is to get the password which is stored in a file named `“-“`.. I used `“ls”` command to see the files present in there and there’s only one file present which is what we need.. So to read what’s in that file, I used `“cat”` command.. Since the filename consists of some special character it is recommended to use `<` symbol and the filename should be placed between quotes.. Generally cat command structure is `cat < “filename”`.. But if the filename consists of no special characters and no spaces we can just use `“cat filename”` as we did before.. When I used the cat command, I got the password for the next level.. I logged out of level 1 and logged into level 2..


- Level 2 to Level 3 :

```
yasasri@Yasasri:~$ ssh bandit2@bandit.labs.overthewire.org -p 2220
```



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

bandit2@bandit.labs.overthewire.org's password:



www. ver he " ire.org

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on discord or IRC.

--[ Playing the games ]--

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat "spaces in this filename"
MNk8KNH3Usiio41PRUEoDFPqfxLPtSmx
bandit2@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.
```

The password is stored in the file called "spaces in this filename".. I checked if there are any other files present but the only file present is what we need.. So, I used "cat" command to get what's stored in that file.. When I used it, I got the password.. I copied it and logged out of level 2 and logged into level 3..

- Level 3 to Level 4 :

```
yasasri@Yasasri:~$ ssh bandit3@bandit.labs.overthewire.org -p 2220

      |_____|
      |  O  |
      |_____|
      |  O  |
      |_____|
      |  O  |
      |_____|
      |  O  |
      |_____|
      |  O  |
      |_____|

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

bandit3@bandit.labs.overthewire.org's password:

      |_____|
      |  O  |
      |_____|
      |  O  |
      |_____|
      |  O  |
      |_____|
      |  O  |
      |_____|
      |  O  |
      |_____|

www. ver he ire.org

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ Playing the games ]--
```

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -a
. . . ...Hiding-From-You
bandit3@bandit:~/inhere$ cat "...Hiding-From-You"
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$ logout
Connection to bandit.labs.overthewire.org closed.
```

The password is stored in a hidden file in inhere directory.. When I used “ls” command, I can see “inhere” in blue colour which means it is a directory.. We need to read a file in inhere directory so we need to change our present location to inhere directory.. We use the command “cd” for it.. It is used to change the locations into different directories.. It can go back directories too.. When I used “cd inhere” we can see that the location we are in is inhere directory.. Then I used “ls -a” to list out all the files and directories present in the inhere directory.. I added “-a” to it because “ls” shows only normal files.. But when we use “ls -a” it will show all the files including the hidden ones.. When I used it, I saw a file “...Hiding-from-You”.. I used “cat” command and got the password.. I copied it, logged out of level 3 and logged into level 4..

- Level 4 to Level 5 :


```
yasasri@Yasasri:~$ ssh bandit4@bandit.labs.overthewire.org -p 2220
[bandit4@bandit4 ~]$
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit4@bandit.labs.overthewire.org's password:
[bandit4@bandit4 ~]$
Welcome to OverTheWire!
If you find any problems, please report them to the #wargames channel on
discord or IRC.
--[ Playing the games ]--
This machine might hold several wargames.
If you are playing "somegame", then:
* USERNAMES are somegame0, somegame1, ...
```

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ file ./-file07
./-file07: ASCII text
bandit4@bandit:~/inhere$ cat < "-file07"
4oQYVPkxZ00E005pTW81FB8j8lxXGUQw
bandit4@bandit:~/inhere$ logout
Connection to bandit.labs.overthewire.org closed.
```

The task is to find the password which is stored in a file which is the only human readable file in inhere directory.. Same story again.. I used ls to see the directories present there.. I used "cd" to direct the present location to inhere directory.. Then there are many files in inhere directory.. We need to find the file which is in human readable form.. I used the command "file ./-\*" which will show all the files present in that directory and also the datatype which they are in.. We can see the data types of those files.. There is only one file in which the data is in ascii text form which is nothing but human readable form.. The file is "-file07".. I used "cat" to read it and got the password.. I copied, logged out of level 4 and logged into level 5..


- Level 5 to Level 6 :

```
yasaari@Yasaari:~$ ssh bandit5@bandit.labs.overthewire.org -p 2220
```



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

bandit5@bandit.labs.overthewire.org's password:



www. ver he ire.org

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on discord or IRC.

--[ Playing the games ]--

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybeh ere00 maybeh ere02 maybeh ere04 maybeh ere06 maybeh ere08 maybeh ere10 maybeh ere12 maybeh ere14 maybeh ere16 maybeh ere18
maybeh ere01 maybeh ere03 maybeh ere05 maybeh ere07 maybeh ere09 maybeh ere11 maybeh ere13 maybeh ere15 maybeh ere17 maybeh ere19
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybeh ere07/.file2
bandit5@bandit:~/inhere$ cat ./maybeh ere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

bandit5@bandit:~/inhere$ logout
```

Connection to bandit.labs.overthewire.org closed.

The task is to find the password which is stored in a file which is of human readable form, 1033 bytes in size and non executable.. I used “ls” and “cd” to check and change the location to inhere directory.. I used “ls” again and saw there are many more directories in there.. I used “find” function to find the file with required properties.. The command is “find . -type f -size 1033c ! -executable” because the thing we are looking for is a file.. So “-type f”.. and the size is 1033 bytes.. So “-size 1033c” c stands for characters which is nothing but size.. “! -executable” because it is not executable.. “!” stands for not.. Then we saw that the required file is “.file2” in “maybehere07” directory.. I used “cat” and found the password.. I copied it, logged out of level 5 and logged into level 6..

- Level 6 to Level 7 :

```
yasasri@Yasasri:~$ ssh bandit6@bandit.labs.overthewire.org -p 2220
```



```
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
bandit6@bandit.labs.overthewire.org's password:  
  
www.verheire.org
```

```
Welcome to OverTheWire!
```

```
If you find any problems, please report them to the #wargames channel on  
discord or IRC.
```

```
--[ Playing the games ]--
```

```
bandit6@bandit:~$ find . / -type f -user bandit7 -group bandit6 -size  
/var/lib/dpkg/info/bandit7.password  
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password  
morbNTDkSW6jILucOymOdMaLn0LFVAaj  
bandit6@bandit:~$ logout  
Connection to bandit.labs.overthewire.org closed.
```

The task is to get the password which is stored somewhere on the server and owned by user bandit7, owned by group bandit6 and 33 bytes in size.. So, we need to find the file with the above properties.. Hence we use the command “find . / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null”.. ‘-type f’ because the thing we are looking for is a file.. “-user bandit7” because it is owned by the user bandit7.. “-group bandit6” because it is owned by the group bandit6.. “-size 33c” cause it’s size is 33 bytes.. If by chance, the required file is not anywhere on the server, it will be showing some error.. To avoid that, we use “2>/dev/null” command.. If there is no such file exists, it won’t be showing any error now.. But since there is a file with the required properties, we go that file.. Using “cat” command, we got the password.. I copied, logged out of level 6 and logged into level 7..



- Level 7 to Level 8 :

```
yasasri@Yasasri:~$ ssh bandit7@bandit.labs.overthewire.org -p 2220
```

[ \_ \_ \_ \_ \_ ]  
[ B | C | I | N | D | I | T ]  
[ . \_ / \ \_ , \_ | | | \_ | | | ]

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

bandit7@bandit.labs.overthewire.org's password:

O v e r  
w w w . t h e w i r e . o r g

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on discord or IRC.

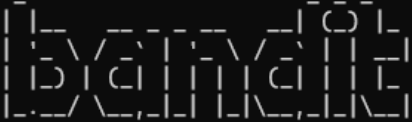
--[ Playing the games ]--

```
bandit7@bandit:~$ cat data.txt | grep millionth
millionth      dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.
```


The task to get the password which is stored in the file 'data.txt' and next to the word 'millionth'.. I used cat command to read the data in data.txt but since I don't need the total data and I know where my password is, I will just get to the line in which my password lies which is next to the word millionth.. I used "grep" command in combination to cat data.txt to get the line in which the word 'millionth' is present.. And we got the password.. 'grep' is used to search for a pattern we give next to it.. If it find any text which matched with the pattern, it prints the each line which matches the pattern.. Since we used "grep millionth", it printed the line where millionth is, and since the next word to millionth is our password, we got the password.. I copied it, logged out of level 7 and logged into level 8..

- Level 8 to Level 9 :

```
yasasri@Yasasri:~$ ssh bandit8@bandit.labs.overthewire.org -p 2220
```



```
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
bandit8@bandit.labs.overthewire.org's password:
```



```
Welcome to OverTheWire!  
  
If you find any problems, please report them to the #wargames channel on  
discord or IRC.
```

```
--[ Playing the games ]--
```

```
bandit8@bandit:~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXQdGana74xvAg0JM
bandit8@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.
```

The task is to get the password which is stored in the file data.txt and the only line of text that occurs only once.. I used the “sort” command to order the list of items in data.txt.. Then I used “uniq -u” command to remove all the duplicates which are now side by side because we sorted them.. and the reason we removed the duplicates is that we need a line which occurs only once.. When we removed all the duplicates, we are left with the line which occurs only once which is our password.. I used it to log into level 9..

- Level 9 to Level 10 :

```
yasasri@Yasasri:~$ ssh bandit9@bandit.labs.overthewire.org -p 2220
```

OverTheWire

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

bandit9@bandit.labs.overthewire.org's password:

**OVERTHEWIRE**

www. over he ire.org

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on discord or IRC.

--[ Playing the games ]--

```
bandit9@bandit:~$ strings data.txt | grep ==
\!;===== the
===== passwordf
===== isc
===== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
bandit9@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.
```

The task is to get the password which is stored in the file data.txt in hr string form and preceded by several "=" characters.. Since we need a string, we don't the total data present in the file data.txt.. So other than using "cat" command, we can use "strings" command.. Which will print the strings present in that file.. Other thing is, it is preceded by many "=" characters.. Here comes the use of grep command.. In combination to strings data.txt we use grep === because the password we are looking for is after those "===" characters.. We can see the password.. I copied it and used it to log into level 10..

- ```
yasasri@Yasasri:~$ ssh bandit10@bandit.labs.overthewire.org -p 2220
```
- OverTheWire
- This is an OverTheWire game server.  
More information on <http://www.overthewire.org/wargames>
- bandit10@bandit.labs.overthewire.org's password:
- OvErThEWiRe**  
[www.verheijere.org](http://www.verheijere.org)
- Welcome to OverTheWire!
- If you find any problems, please report them to the #wargames channel on discord or IRC.
- [ Playing the games ]--

```
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmозcVJyCg==
bandit10@bandit:~$ base64 -d data.txt
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.
```

The task is to get the password stored in the file data.txt which contains base64 encoded data.. First I used cat command to see how the data is.. It is in encoded form.. Now we need to decode it.. So I used the command “base64 -d” and type the filename in order to decode it as it is in encoded form.. “-d” is because we need to decrypt it.. The default for base64 command is to encode the data.. So it is necessary to use “-d” in order to decode it.. After decoding, we got the password.. I copied it and used it to log into level 11..

- ```
yasasri@Yasasri:~$ ssh bandit11@bandit.labs.overthewire.org -p 2220
```
- ```

      _-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_
      |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_| | | | | | | |
      |||||\\|||\\|||\\|||\\|||\\|||\\|||
      |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|

```
- ```

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

bandit11@bandit.labs.overthewire.org's password:
```
- ```

      _-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_
      |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_| | | | | | | |
      |||||\\|||\\|||\\|||\\|||\\|||\\|||
      |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|

```
- ```

www. ver he " ire.org

```
- ```
Welcome to OverTheWire!
```
- ```
If you find any problems, please report them to the #wargames channel on discord or IRC.
```
- ```
--[ Playing the games ]--
```

```
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
bandit11@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.
```

The task is to get the password which is stored in the file data.txt and which is rotated by 13 positions.. I used cat command to read what's in that file but that's not what we need.. If we again rotate the data by 13 positions, it gets back to it's original form.. So in addition to cat command, I used 'tr' command which means translate.. " tr 'A-Za-z' 'N-ZA-Mn-za-m'" command is used.. The first 13 letters of alphabets A-M or a-m are translated to N-Z or n-z.. The next 13 letters of alphabets N-Z or n-z are recycled and translated to A-M or a-m.. And hence the data in the file is rotated again and it came back to it's original form and we got the password.. I copied it and logged into level 12..

- Level 12 to Level 13 :

```
yasarri@Yasarri:~$ ssh bandit12@bandit.labs.overthewire.org -p 2220
```

bandit12

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

bandit12@bandit.labs.overthewire.org's password:

OverTheWire

www. ver he " ire.org

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on discord or IRC.

--[ Playing the games ]--

```
bandit12@bandit:~$ cd /tmp
bandit12@bandit:/tmp$ mktemp -d
/tmp/tmp.Q9q5pRoVBa
bandit12@bandit:/tmp$ cd /tmp/tmp.Q9q5pRoVBa
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ cp ~/data.txt .
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ ls
data.txt
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ cat data.txt
00000000: 1f8b 0808 d2e9 9766 0203 6461 7461 322e .....f..data2.
00000010: 6269 6e00 0141 02be fd42 5a68 3931 4159 bin..A...BZh91AY
00000020: 2653 59ea 2468 ae00 0017 7fff dadb b7fb &SY.$h.....
00000030: dbff 5ffb f3fb d776 3d6f fffb dba fdbd .....v=o.....
00000040: 85db edfc ffa9 7def faaf efd f b001 386c .....}.....8l
00000050: 1001 a0d0 6d40 01a0 1a00 0006 8006 8000 ....m@.....
00000060: 0000 d034 01a1 a34d 0034 3d43 40d0 0d34 ...4...M.4=C@..4
00000070: d034 34da 9ea1 b49e a7a8 f29e 5106 4326 .44.....Q.C&
00000080: 9a19 1934 d1a0 341a 6234 d018 d468 6834 ...4..4.b4...hh4
00000090: 00c9 a308 6434 0000 0308 d068 0680 1900 ....d4....h....
000000a0: 0034 d068 1a34 d068 c3a7 a41a 0c9a 0d34 .4.h.4.h.....4
000000b0: 641a 0646 8346 4003 4d34 1a68 6806 9a06 d..F.F@.M4.hh...
000000c0: 9a64 d064 001a 0681 a343 10d0 d00d 1840 .d.d....C.....@
000000d0: 01a3 21a0 68c9 a050 008a 0009 619a 9541 ..!.h..P....a..A
000000e0: 25d5 8bc0 0ff3 e679 7fd0 31b2 c784 e7f7 %.....y..1.....
000000f0: 8fcb 33b8 28a5 bf86 4ac4 274f ce21 eeea ..3.(...J.'O.!...
00000100: 2c19 2633 60e9 ddd1 8d60 18e9 b189 4a94 ,.&3'....'....J.
00000110: 3a14 ee61 ac8d d369 f545 a964 2617 f1fd :.a....i.E.d&...
00000120: 72dc 51d1 e601 1071 745d 846c 4677 4ba2 r.Q....qt].lFwK.
00000130: 0562 5d79 894a 9150 dfe1 8083 e4c0 896f .b]y.J.P.....o
00000140: b75c d58b 4264 021c 625c c4f2 816a 8907 .\..Bd..b\...j..
00000150: 8b80 2b3e 4d2a f1b3 4fb4 6cee a869 1316 ..>M*..O.l..i..
00000160: c318 cdb5 b1cd 21c4 a23a 0297 65ae 8a2a .....!.....e..*
00000170: 0cd2 0864 8a47 ed68 48f3 a65f 5803 dc9f ...d.G.hH...X...
00000180: b2e5 bbe0 daac 3d56 8c8b 4181 510f 017f .....=V..A.Q...
00000190: 1328 9a47 6027 62c1 e4b4 db74 bb3a 9455 .(G`'b....t...U
000001a0: 07dd fd5b 19b5 e522 32e0 9b3e a3cf 0189 ...[..."2..>....
```





```

00000200: 4a95 2813 147b 3287 c648 2569 8a92 1ee1 J(..{2..H%i....
00000210: da8f 2d42 372d a13f 6805 1dfe 0508 cb09 ..-B7-.?h.....
00000220: 6d4a 17ed 3521 309d 756c 2fa4 1480 03e6 mJ..5!0.ul/.....
00000230: 50ea 144e b15f e2ee 48a7 0a12 1d44 8d15 P..N...H....D..
00000240: c0 .
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ mv compressed_data compressed_data.bz2
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ ls
compressed_data.bz2 hexdump_data
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ bzip2 -d compressed_data.bz2
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ ls
compressed_data hexdump_data
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ xxd compressed_data
00000000: 1f8b 0808 d2e9 9766 0203 6461 7461 342e .....f..data4.
00000010: 6269 6e00 edd1 4f28 a471 18c0 f1df 1466 bin...O(.q.....f
00000020: 6468 af93 36bf 37e5 30b6 e97d c73b ef4b dh..6.7.0..}.;K
00000030: 691b 928d 9072 61c5 36d3 b48d 3f2d 8d19 i....ra.6...?-..
00000040: 076b db71 22b1 2d39 b8f8 339b 7050 766b .k.q".-9..3.pPvk
00000050: 8f48 9b2d 972d d61e 5639 1829 c596 a44d .H.-.-.V9.)...M
00000060: 5ac9 70a4 764f 58f5 fd5c 9ea7 9ee7 f60d Z.p.vOX..\.....
00000070: f8c2 3e8f cdbf f44a dc1e 35c1 d0f5 ab99 ..>....J..5.....
00000080: 706d baf5 cb5d d30d dd63 1aba e976 0b55 pm...]...c...v.U
00000090: d3dc 8626 a42a ee40 a423 ec0b 4929 426d ...&.*.@.#..I)Bm
000000a0: 6de1 bffd fdeb fe40 0512 fd8d 7bed afaa m.....@.....{...
000000b0: 7979 9e9b fd4d fadf 85e2 e7c1 02ad a82e yy...M.....
000000c0: a7a6 6efe 6cde 27c4 c0db c3ad 66e1 5d7e ..n.l.'.....f.]~
000000d0: 7312 97f5 d9d1 8872 1e15 3611 f50a f172 s.....r..6....r
000000e0: d862 9315 3629 46d2 cb26 e586 32b9 1674 .b..6)F..&..2..t
000000f0: d84b 2b1d 2983 b3bf 33ab 9b94 297f 20b0 .K+.)...3....).
00000100: 3e3d e05d 5915 41bb 341f 0fc6 ce7a 2cdd >=.]Y.A.4....z,..
00000110: db8f 6487 3fe2 dd77 3a47 832b 25d6 c519 ..d.?.w:G.+%...
00000120: ab59 3f54 dbf7 6333 961f ff90 7174 1a5d .Y?T..c3....qt.]
00000130: 7f96 5699 6fc9 694d 2a9f fe56 3e75 fcf5 ..V.o.iM*..V>u..
00000140: 4fe3 8252 d2bf 91dc f0ae c535 b7fa eb89 0..R.....5....
00000150: k6b ad7a dde0 18db fbde f5f3 fd48 6f72 .k.z.....Hor
00000160: 286b 6db6 d4ee dc3f 789a f1b1 3a2b de33 (km....?x...:+3

```

```

bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ mv compressed_data compressed_data.gz
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ ls
compressed_data.gz hexdump_data
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ gzip -d compressed_data.gz
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ ls
compressed_data hexdump_data

```

```

bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ xxd compressed_data | head
00000000: 6461 7461 352e 6269 6e00 0000 0000 0000 data5.bin.....
00000010: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000020: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000030: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000040: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000050: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000060: 0000 0000 3030 3030 3634 3400 3030 3030 ....0000644.0000
00000070: 3030 3000 3030 3030 3030 3000 3030 3030 000.0000000.0000
00000080: 3030 3234 3030 3000 3134 3634 3537 3634 0024000.14645764
00000090: 3732 3200 3031 3132 3631 0020 3000 0000 722.011261.0...
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ mv compressed_data compressed_data.tar
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ ls
compressed_data.tar hexdump_data
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ tar -xvf compressed_data.tar
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ ls
compressed_data.tar data5.bin hexdump_data
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ xxd data5.bin | head
00000000: 6461 7461 362e 6269 6e00 0000 0000 0000 data6.bin.....
00000010: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000020: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000030: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000040: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000050: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000060: 0000 0000 3030 3030 3634 3400 3030 3030 ....0000644.0000
00000070: 3030 3000 3030 3030 3030 3000 3030 3030 000.0000000.0000
00000080: 3030 3030 3333 3500 3134 3634 3537 3634 0000335.14645764
00000090: 3732 3200 3031 3132 3637 0020 3000 0000 722.011267.0...
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ tar -xvf data5.bin
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ ls
compressed_data.tar data5.bin data6.bin hexdump_data
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ xxd data6.bin | head
00000000: 425a 6839 3141 5926 5359 affc af61 0000 BZh91AY&SY...a..
00000010: 8c7f efdc 6a00 40c0 7df7 e120 5b23 8075 ....j.@.}... [#.u
00000020: 21fe 8000 0800 8040 0000 6692 0108 204c !.....@..f... L

```



```

bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ bzip2 -d data6.bin
bzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ ls
compressed_data.tar data5.bin data6.bin.out hexdump_data
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ xxd data6.bin.out | head
00000000: 6461 7461 382e 6269 6e00 0000 0000 0000  data8.bin.....
00000010: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000030: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000040: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000050: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000060: 0000 0000 3030 3030 3634 3400 3030 3030  ....0000644.0000
00000070: 3030 3000 3030 3030 3030 3000 3030 3030  000.0000000.0000
00000080: 3030 3030 3131 3700 3134 3634 3537 3634  0000117.14645764
00000090: 3732 3200 3031 3132 3637 0020 3000 0000  722.011267. 0...

bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ tar -xf data6.bin
tar: data6.bin: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ tar -xf data6.bin.out
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ ls
compressed_data.tar data5.bin data6.bin.out data8.bin hexdump_data
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ xxd data8.bin | head
00000000: 1f8b 0808 d2e9 9766 0203 6461 7461 392e  ....f..data9.
00000010: 6269 6e00 0bc9 4855 2848 2c2e 2ecf 2f4a  bin...HU(H,.../J
00000020: 51c8 2c56 70f3 374d 2977 2b4e 3648 4e4a  Q.,Vp.7M)w+N6HNJ
00000030: f4cc f430 c8b0 f032 4a0d cd2e 362a 4b09  ...0...2J...6*K.
00000040: 7129 77cc e302 003e de32 4131 0000 00    q)w....>.2A1...

bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ mv data8.bin data8.gz
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ ls
compressed_data.tar data5.bin data6.bin.out data8.gz hexdump_data
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ gzip -d data8.gz
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ ls
compressed_data.tar data5.bin data6.bin.out data8 hexdump_data
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ xxd data8 | head
00000000: 5468 6520 7061 7373 776f 7264 2069 7320  The password is
00000010: 464f 3564 7746 7363 3063 6261 4969 4830  F05dwFsc0cbaIiH0
00000020: 6838 4a32 6555 6b73 3276 6454 4477 416e  h8J2eUks2vdTDwAn
00000030: 0a
bandit12@bandit:/tmp/tmp.Q9q5pRoVBa$ cat data8
The password is F05dwFsc0cbaIiH0h8J2eUks2vdTDwAn

```

The task is to get the password which is stored in the file data.txt, which is the hexdump of a file that has been repeatedly compressed.. First I created a directory under /tmp using “cd” command.. Then used the command “mktemp -d” to create a temporary for us to work in.. Then I copied data.txt using “cp” command to this directory.. Then used “mv” command to rename it into hexdump\_data which kinda makes sense.. I used “cat” command along with

head to read what's in the file.. When we use 'head' command we can see the first 10 lines in default which is enough to see whether the data is compressed or not.. This data is hexdump of a file which has been compressed many times.. Then I used the command "xxd -r" to revert the hexdump and stored that in another file "compressed\_data".. I tried "ls" and saw that there are two files.. One is reverted file another isn't.. Then I tried "cat" on compressed\_data to see that the data is so compressed.. If we decompress that, we are done with the thing.. We will get the password.. Again I used "cat" command on hexdump\_data which is the same as before to show the difference between reverted files and non reverted ones.. In order to decompress, we use many commands.. I first used "gzip" command.. A gzip file usually ends with '.gz'.. So I renamed the 'compressed\_data' as 'compressed\_data.gz' .. Then used 'ls' to check the files present there.. Then used the command 'gzip -d' to decompress the data in it.. After decompressing the data, the file becomes a normal file.. We can check it by 'ls' command.. Then I used "xxd" command to print the hexadecimal representation of the data in compressed\_data.. We can see that it is still compressed.. Now we can use "bzip2" command.. In order to use that, we should rename the file as 'compressed\_data.bz2'.. Then I used the command "bzip2 -d" to decompress the file.. After decompressing, the file becomes a normal file again.. Using "xxd" , we can still see that it is compressed.. I decompressed it again with gzip and saw that it is still compressed.. But I can see a file called "data5.bin".. It must be an archive file.. In order to unarchive it, we use the "tar" command for which the filename must end with ".tar".. So I renamed it as required.. Using "xxd" for data5.bin, I can see there's another file in it.. So using tar on data5.bin, we found another file 'data6.bin'..Using "xxd" on data6.bin, we can see it is compressed.. So I decompressed it using bzip2.. It gave us a new file 'data6.bin.out'.. Using "tar" on it, we can see there's another file named "data8.bin".. Using "xxd" we can see it is compressed.. I decompressed it again by using gzip.. Then we finally got a file named "data8".. Using "cat" on it, I got the password.. I copied it and logged into next level..

- Level 13 to Level 14 :

```

yasarri@Yasarri:~$ ssh bandit13@bandit.labs.overthewire.org -p 2220

      [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _
      [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _
      [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _

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

bandit13@bandit.labs.overthewire.org's password:

      [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _
      [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _
      [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _

      www. _ _ _ _ _ ver _ _ _ _ _ he _ _ _ _ _ ire.org

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ Playing the games ]--

```

```

bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ scp -p 2220 bandit13@bandit.labs.overthewire.org:sshkey.private .
cp: cannot stat '2220': No such file or directory
The authenticity of host 'bandit.labs.overthewire.org (127.0.0.1)' 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
Could not create directory '/home/bandit13/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).

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

!!! You are trying to log into this SSH server on port 22, which is not intended.

bandit13@bandit.labs.overthewire.org: Permission denied (publickey).
scp: Connection closed
bandit13@bandit:~$ ssh -i sshkey.private bandit14@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([127.0.0.1]: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
Could not create directory '/home/bandit13/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).

      [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _
      [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _
      [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _ [~]_ _ _ _ _

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

```

The task is to log into the next level using a private ssh key.. I used 'ls' to see the files and found "sshkey.private".. Then I used scp to connect to the remote machine and get the ssh key.. Now we have the private sshkey, we can log into the level 14.. I used the command "ssh -i sshkey.private" command along with the command to enter the level 14 as to read the file in which private key for public key authentication is read.. Then I typed yes and directly got directed to level 14.

- Level 14 to Level 15 :

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

!! You are trying to log into this SSH server with a password on port 2220 from localhost.
!! Connecting from localhost is blocked to conserve resources.
!! Please log out and log in again.

OverTheWire
www. ver he " ire.org

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
Discord or IRC.

--[ Playing the games ]--
```

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8R0of1qqmcBPALh7LDCPvS
bandit14@bandit:~$ nc localhost 30000
MU4VWeTyJk8R0of1qqmcBPALh7LDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
```

The task is to get the password by submitting the password of the current level to port 30000 on local host.. To find the password of the current level, we use the command “cat /etc/bandit\_pass/banditlevelnumber”.. By using this, I got the password of the current level.. To submit this password to port 30000 on localhost, I used the command “nc localhost 30000” to connect to the localhost port 30000 and pasted the password.. And we got the password for the next level..