Bandit game level 0

Get in level 0 by using
ssh bandit0@bandit.labs.overthewire.org -p 2220

```
bandit0@bandit: ~

 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/
    * 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!

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: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

bandit0@bandit:~$
```

Command “ls” was used to see if there are any files, then use “cat” to read the file and we found the password ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

Level 1

ssh bandit1@bandit.labs.overthewire.org -p 2220

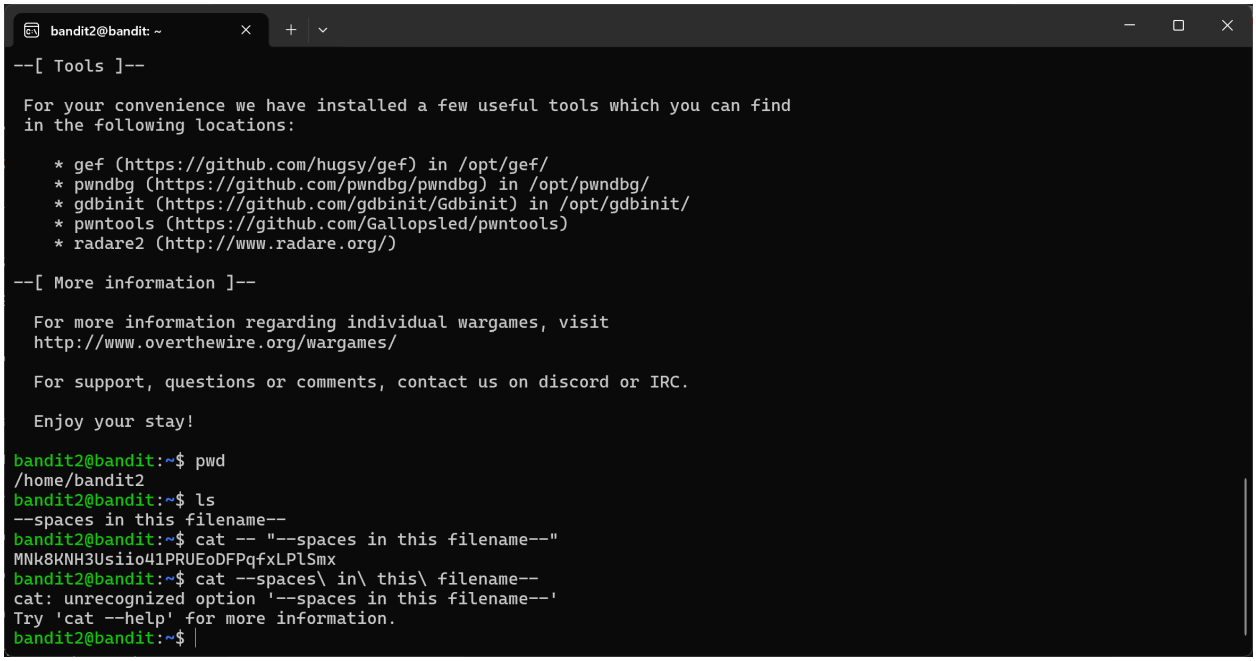
```
bandit1@bandit: ~

bandit1@bandit:~$ ls
-
bandit1@bandit:~$ pwd
/home/bandit1
bandit1@bandit:~$ cat -
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$
```

“ls” to check and there seems to be a file named “-“. cat – alone doesn’t work because – is special so we need to tell terminal that it is in our current directory by doing ./- so cat ./- gave the password for level 2

263JGJPfgU6LtdEvgfWU1XP5yac29mFx

Level 2

ssh bandit2@bandit.labs.overthewire.org -p 2220




“ls” and found a file called “—spaces in this filename—” so if we do literally cat –spaces in this filename—the “cat” will take options because of – so we have to do cat – “—spaces in this filename—”

--can bypass option

MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx

Level 3

ssh bandit3@bandit.labs.overthewire.org -p 2220

```
bandit3@bandit: ~/inhere

    * gef (https://github.com/hugsy/gef) in /opt/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
    * 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!

bandit3@bandit:~$ pwd
/home/bandit3
bandit3@bandit:~$ ls -l
total 4
drwxr-xr-x 2 root root 4096 Aug 15 13:16 inhere
bandit3@bandit:~$ cat inhere
cat: inhere: Is a directory
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -l
total 0
bandit3@bandit:~/inhere$ ls -a
.  ..  ...Hiding-From-You
bandit3@bandit:~/inhere$ cat "...Hiding-From-You"
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$
```

“ls” and found “inhere” then cd into it. “ls-a” and found a file name “…Hiding-From-You” then cat “…Hiding-From-You”

2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

Level 4

ssh bandit4@bandit.labs.overthewire.org -p 2220

```
bandit4@bandit: ~/inhere
            [--mime-type] [-e <testname>] [-F <separator>]  [-f <namefile>]
            [-m <magicfiles>] [-P <parameter=value>] [--exclude-quiet]
            <file> ...
       file -C [-m <magicfiles>]
       file [--help]
bandit4@bandit:~/inhere$ file -- -file0*
-file00: Non-ISO extended-ASCII text, with no line terminators, with overstriking
-file01: data
-file02: data
-file03: data
-file04: data
-file05: data
-file06: data
-file07: ASCII text
-file08: data
-file09: data
bandit4@bandit:~/inhere$ file ./*
./-file00: Non-ISO extended-ASCII text, with no line terminators, with overstriking
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat -- -file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
bandit4@bandit:~/inhere$
```

First I cd into “inhere” and check “ls” and found 10 files but we were tasked to read file that is a human readable so I have to use “file -- -file*” or “file ./*” works too. File number 7 is our target so “cat -- -file07”

4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

Level 5

ssh bandit5@bandit.labs.overthewire.org -p 2220

```
Select bandit5@bandit: ~/inhere/maybehere07
bandit5@bandit:~$ pwd
/home/bandit5
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere03  maybehere06  maybehere09  maybehere12  maybehere15  maybehere18
maybehere01  maybehere04  maybehere07  maybehere10  maybehere13  maybehere16  maybehere19
maybehere02  maybehere05  maybehere08  maybehere11  maybehere14  maybehere17
bandit5@bandit:~/inhere$ find -type f -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ".file2"
cat: .file2: No such file or directory
bandit5@bandit:~/inhere$ cd maybehere07
bandit5@bandit:~/inhere/maybehere07$ cat ".file2"
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

bandit5@bandit:~/inhere/maybehere07$
```

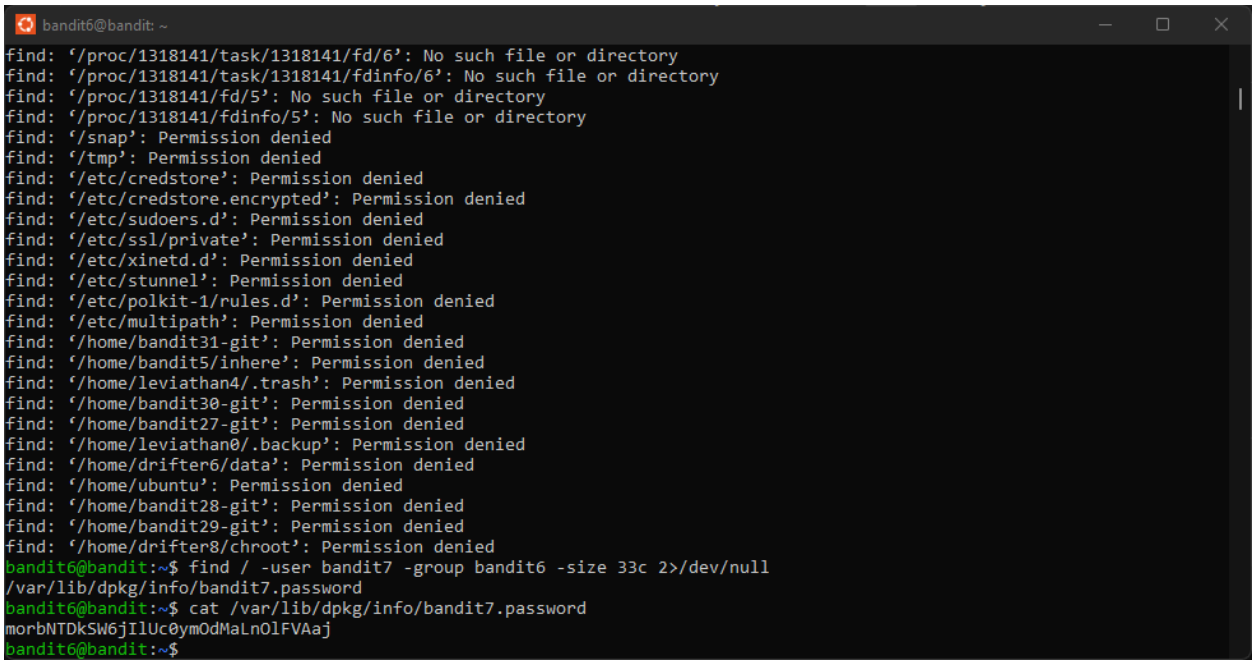
Cd into “inhere” and “ls” found a lot of directories. We were tasked to find human readable files, 1033 bytes in size and not executable so I tried “find -type f -size 1033c” and it shows “./maybehere07/.file2” so the answer must be in “.file2” so I cd into “maybehere07” and “cat “.file2”.

Alternative: I just searched more about the bitmask method so this one works too “find -type f -size 1033c ! -perm 111”

HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

Level 6

ssh bandit6@bandit.labs.overthewire.org -p 2220



```
bandit6@bandit: ~
find: ‘/proc/1318141/task/1318141/fd/6’: No such file or directory
find: ‘/proc/1318141/task/1318141/fdinfo/6’: No such file or directory
find: ‘/proc/1318141/fd/5’: No such file or directory
find: ‘/proc/1318141/fdinfo/5’: No such file or directory
find: ‘/snap’: Permission denied
find: ‘/tmp’: Permission denied
find: ‘/etc/credstore’: Permission denied
find: ‘/etc/credstore.encrypted’: Permission denied
find: ‘/etc/sudoers.d’: Permission denied
find: ‘/etc/ssl/private’: Permission denied
find: ‘/etc/xinetd.d’: Permission denied
find: ‘/etc/stunnel’: Permission denied
find: ‘/etc/polkit-1/rules.d’: Permission denied
find: ‘/etc/multipath’: Permission denied
find: ‘/home/bandit31-git’: Permission denied
find: ‘/home/bandit5/inhere’: Permission denied
find: ‘/home/leviathan4/.trash’: Permission denied
find: ‘/home/bandit30-git’: Permission denied
find: ‘/home/bandit27-git’: Permission denied
find: ‘/home/leviathan0/.backup’: Permission denied
find: ‘/home/drifter6/data’: Permission denied
find: ‘/home/ubuntu’: Permission denied
find: ‘/home/bandit28-git’: Permission denied
find: ‘/home/bandit29-git’: Permission denied
find: ‘/home/drifter8/chroot’: Permission denied
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
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:~$
```

Conditions are owned by user bandit7, owned by group bandit6, and 33 bytes in size. First I tried “find / -user bandit7 -group bandit6 -size 33c” but there were a lot of permission denied stuffs so I tried more then the good command would be “find / -user bandit7 -group bandit6 -size 33c 2>/dev/null” Somehow “2>/dev/null” works like magic where it will automatically filter out those permission denied stuffs and then the targeted file is now located so I just type “cat /var/lib/dpkg/info/bandit7.password”

morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj

Level 7

ssh bandit7@bandit.labs.overthewire.org -p 2220

```
bandit7@bandit: ~
--[ 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/
    * 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!

bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ grep "millionth"
d
sss
bandit7@bandit:~$ grep data.txt "millionth"
grep: millionth: No such file or directory
bandit7@bandit:~$ grep "millionth" data.txt
millionth       dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$
```

The password for the next level is stored in the file **data.txt** next to the word **millionth**

I tried cat it and it shows so many things so I tried grep

‘Grep “millionth” data.txt’

dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

Level 8
ssh bandit8@bandit.labs.overthewire.org -p 2220

I tried cat it and found so many arbitrary random thing so i tried “sort data.txt” looks more organise but i need to find a password which is a line that only occurred once so I have to use uniq to count and grep number 1. Uniq is cutting duplicated lines -c is count

‘sort data.txt | uniq -c | grep “ 1 “‘

4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

```
bandit8@bandit: ~
     10 Tx2u6Y2xu4EC0NkI1gWsIlDf6Xw2HB75
     10 U1SwcmbW4KtKfbSfwFbMLrglLIt2wAHC
     10 u3u2A89W6wrNLaArSfEE0H79g3gImwne
     10 UDHTxlRyU0bBKtjUUhJG2VRoT1MJyk8b
     10 uG6s7CFzkh4lqmcJtwLIxa4sU1v8gkhU
     10 ukWEPonuKwvEKvX0eNw6NNbChvzltM5M
     10 v6gHt2LZHqAVeQuOyc41wu1pSU47Z1kH
     10 VAJMrSbPZg5Yftj43U1fGc8w88s5PhBE
     10 WfgyTavpK4WAaGEeD0lLP069oebJFnin
     10 wGkPzkDSLDmsfycqfhPLrnX5AnT2U5ei
     10 WkcJmDs54n2OynP1oYNjZ64kXa4KjVJY
     10 wWBMq60soClrdCxvoUioXvdqOUrOafOV
     10 WzbOaR7zpAoOT49J8Id5MBmhy9ucfJTD
     10 XDUhleli7YNGHFPqMARmOZvnekNLGbVB
     10 XLIyGDiAhBDFA9bxwymTQ8Dqm5YibqnK
     10 XLtOPYSExyUGQWWjCS0nBkTqXvn2lD3H
     10 XX9oUvVIq06yj5BzH4rwFGTDzxavfsSX
     10 Y8fwKYAyzkZ1H4TVJYjw2R9xPgrHpapw
     10 yauCrBTowLdc0tmfZsZgnAKIVdIHRdac
     10 yPp4j25oBTCzQdXC6fpsn4fJMJG037ld
     10 YXLjy2VZD7aGc0TnvNTEQQAA0xQp2W1B
     10 ZGl3TAlcKjZUfIeu6Kr8cyO8AGavta9l
     10 zGPz6R7fFM2cQ7T2D8BhJnSAnBRKCryS
     10 zRgElIOsTXVPZuVWVkp7fOShIqHOCX4O
     10 ZzQDv5Imr9y5XSYGD3r61uP1fjXAhuod
bandit8@bandit:~$ sort data.txt | uniq -c | grep " 1 "
      1 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:~$ sort data.txt | uniq -c | grep " 1 "
      1 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:~$
```

Level 9

ssh bandit9@bandit.labs.overthewire.org -p 2220

```
bandit9@bandit: ~
%1p75(~
G,]kl
FT^I
igar[
&b0R
&x,[g
O5W^%
bandit9@bandit:~$ strings data.txt | grep =
========== theg
VQ=97
[m=K1x
/i8D2[U?=
========== password
LU=W
========== is
=v$,
h{=,rw_c
=}%q
=D!7
YU=<
5=fq
vJ=ho
========== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
=AdD
bandit9@bandit:~$ strings data.txt | grep ===
========== theg
========== password
========== is
========== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
bandit9@bandit:~$
```

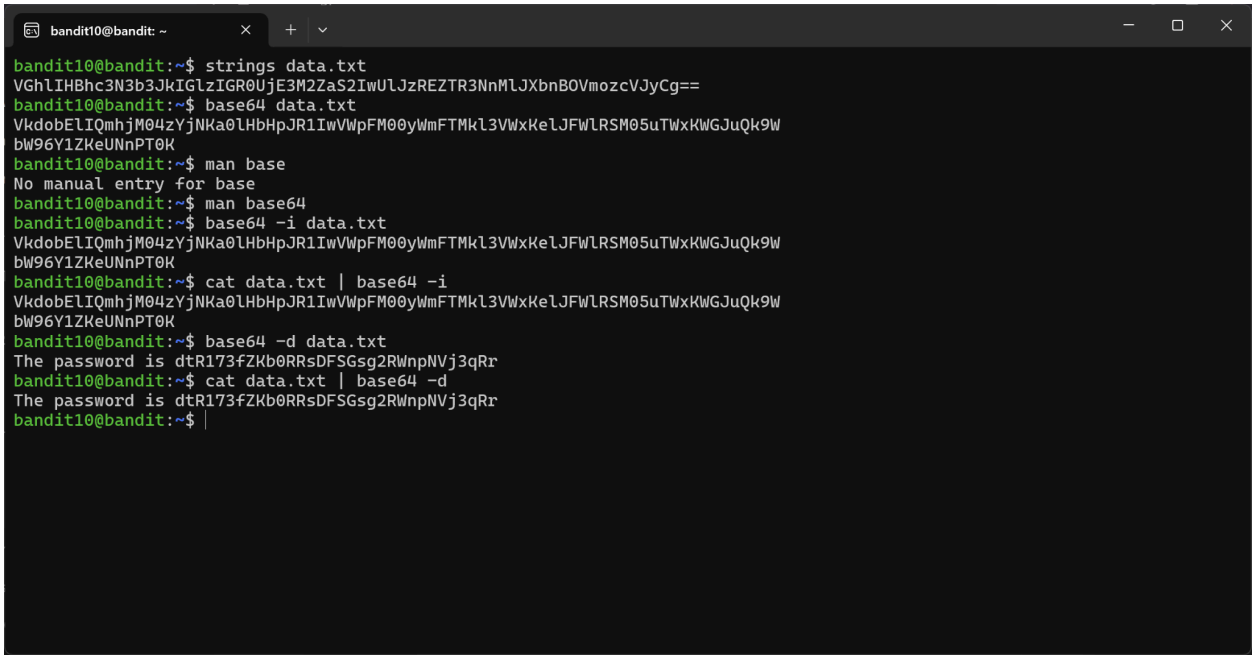
I tried catting it and found so many weird emoji so I tried using command “strings” which will pull out only human readable line from the file and then I grep “=” from it and found the password

‘strings data.txt | grep “===”’

FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

Level 10

ssh bandit10@bandit.labs.overthewire.org -p 2220

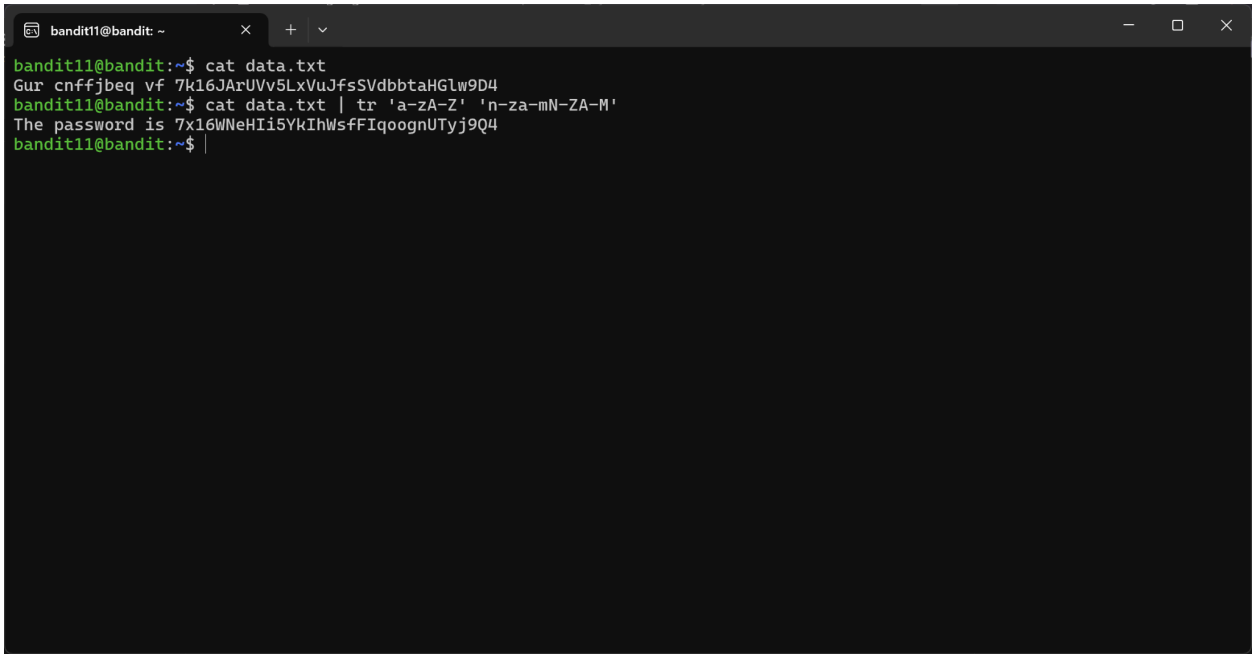



This is something very new “contains base64 encoded data”. At first I tried “base64 data.txt” but this is just keep encoding the encoded data but the correct command is “base64 -d data.txt”

dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

Level 11

ssh bandit11@bandit.labs.overthewire.org -p 2220




“all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions”. By far the most confusing leveling. Those letters were shifted 13 positions so we have to use command “tr”. tr translate one character set to another character set for example “echo hello | tr ‘el’ ‘ip’” the answer will be hippo

Cat data.txt | tr ‘a-zA-Z’ ‘n-za-mN-ZA-M’

We shift english alphabets by 13 positions

7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4

Level 12

ssh bandit12@bandit.labs.overthewire.org -p 2220

```
bandit12@bandit: /tmp/tmp.\
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ mktemp -d
/tmp/tmp.W1MZJW90bQ
bandit12@bandit:~$ cd /tmp/tmp.W1MZJW90bQ
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ ls
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ cp /home/bandit12/data.txt ./data.hex
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ ls -l
total 4
-rw-r----- 1 bandit12 bandit12 2645 Sep 20 13:50 data.hex
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ xxd -r data.hex > data.bin
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ ls
data.bin  data.hex
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ file data.hex
data.hex: ASCII text
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ file data.bin
data.bin: gzip compressed data, was "data2.bin", last modified: Fri Aug 15 13:15:53 2025, max compression, from Unix, or
iginal size modulo 2^32 584
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ gunzip data.bin
gzip: data.bin: unknown suffix -- ignored
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ ls
data.bin  data.hex
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ ls
data.bin  data.hex
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ mv data.bin data.gz
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ ls
data.gz  data.hex
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$
```

```
bandit12@bandit: /tmp/tmp.\
  command 'runzip' from deb rzip (2.1-4.1)
  command 'gunzip' from deb gzip (1.12-1ubuntu1)
Try: apt install <deb name>
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ bunzip2 data6.bin
bunzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ ls
data2  data5.bin  data6.bin.out  data.hex
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ tar -xf data6.bin.out
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ ls
data2  data5.bin  data6.bin.out  data8.bin  data.hex
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Fri Aug 15 13:15:53 2025, max compression, from Unix, o
riginal size modulo 2^32 49
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ ls
data2  data5.bin  data6.bin.out  data8.bin  data.hex
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ gunzip data8.bin
gzip: data8.bin: unknown suffix -- ignored
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ mv data8.bin data8.gz
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ ls
data2  data5.bin  data6.bin.out  data8.gz  data.hex
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ gunzip data8.gz
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ ls
data2  data5.bin  data6.bin.out  data8  data.hex
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ file data8
data8: ASCII text
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ cat data8
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
bandit12@bandit:/tmp/tmp.W1MZJW90bQ$
```

I went through a lot of things and I thought I got played.

Banditgames recommended me to create a temporary directory so I did

“mktemp -d” This will generate a temporary dir for you then we cd into it “ cd /tmp/tmp.W1MZJW90bQ”

After creating a temp dir we just need to copy the data text to our new space “cp /home/bandit12/data.txt ./data.hex” in this case I named it data.hex “./data.hex” is the current directory.

To decompress the file, right now it is hexdump file so we need to convert it into binary file so we use this command “xxd -r data.hex > data.bin”. Now we have to check the data.bin file by “file data.bin”

“data.bin: gzip compressed data, was "data2.bin",”

This mean we can decompress the file now using the gzip type by using “gunzip data.bin” but I won’t work yete because we need to rename it into “.gz” file so “mv data.bin data.gz” then “gunzip data.gz”. Now we will get the decompressed data now is called “data”. We have to check its file type so “file data”

“data: bzip2 compressed data, block size = 900k”

This means we need to use “bunzip2” command to unzip it again. Another type is “data2: POSIX tar archive (GNU)”. This type need “tar -xf” type decompression for example “tar -xf data8”

We keep repeating the process until we check the file and it shows “data8: ASCII text”

bandit12@bandit:/tmp/tmp.W1MZJW90bQ$ cat data8

The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn

FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn

Level 13

ssh bandit13@bandit.labs.overthewire.org -p 2220

```
bandit14@bandit: ~

 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/
    * 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!

bandit14@bandit:~$ ls
bandit14@bandit:~$ ls -la
total 24
drwxr-xr-x   3 root root 4096 Aug 15 13:15 .
drwxr-xr-x 150 root root 4096 Aug 15 13:18 ..
-rw-r--r--   1 root root  220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root root 3851 Aug 15 13:09 .bashrc
-rw-r--r--   1 root root  807 Mar 31  2024 .profile
drwxr-xr-x   2 root root 4096 Aug 15 13:15 .ssh
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
bandit14@bandit:~$
```

We have to connect to bandit14 user so we have to use that private ssh key to enter it by this command

“ssh -i sshkey.private -p 2220 bandit14@localhost”

Ssh stands for Secure shell. I’ve been using this command since level zero using this port -p 2220

“-i sshkey.private” will identify the private key

bandit14@localhost means we are telling shell that we are logging in as bandit14 on the machine called ‘localhost’

The hint is “The password for the next level is stored in **/etc/bandit_pass/bandit14”**

So we can just cat the password

“cat /etc/bandit_pass/bandit14”

MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS

Chaiyanun Sakulsaowapakkul 6681299