OVER THE WIRE BANDIT

**SOLUTIONS**

**LEVELS UPTO 15**

****

CONTRIBUTED BY

## SIDHARTH KRISHNA

**INTRODUCTION**

Over The Wire is a platform to develop basics of security concepts using games as a medium. It has various wargames and their internal levels are designed in terms of increasing difficulty for each level to pass on.

Wargames include:

1. Bandit
2. Natas
3. Leviathan
4. Krypton
5. Narnia
6. Behemoth
7. Utumno
8. Maze
9. Vortex
10. Manpage

Each wargame specializes in teaching a particular security concept. We will solve each and every wargame including it’s internal levels and cover important concepts if necessary.

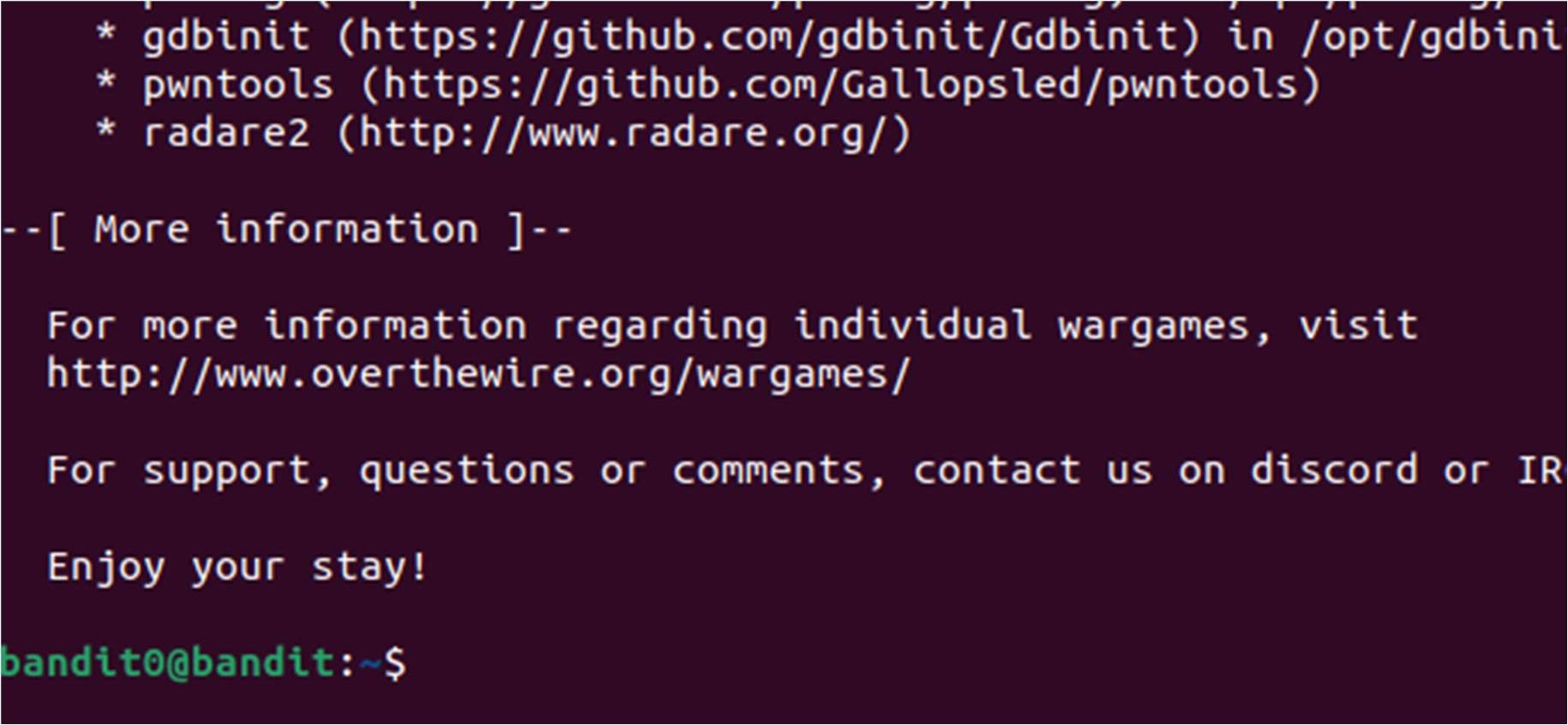
This document covers all the commands used to complete levels upto 15 and their respective explanations.

**BANDIT – LEVEL(1-15)**

# Level 0

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is **bandit.labs.overthewire.org**, on port 2220. The username is **bandit0** and the password is **bandit0**. Once logged in, go to the level 1 page to find out how to beat Level 1.

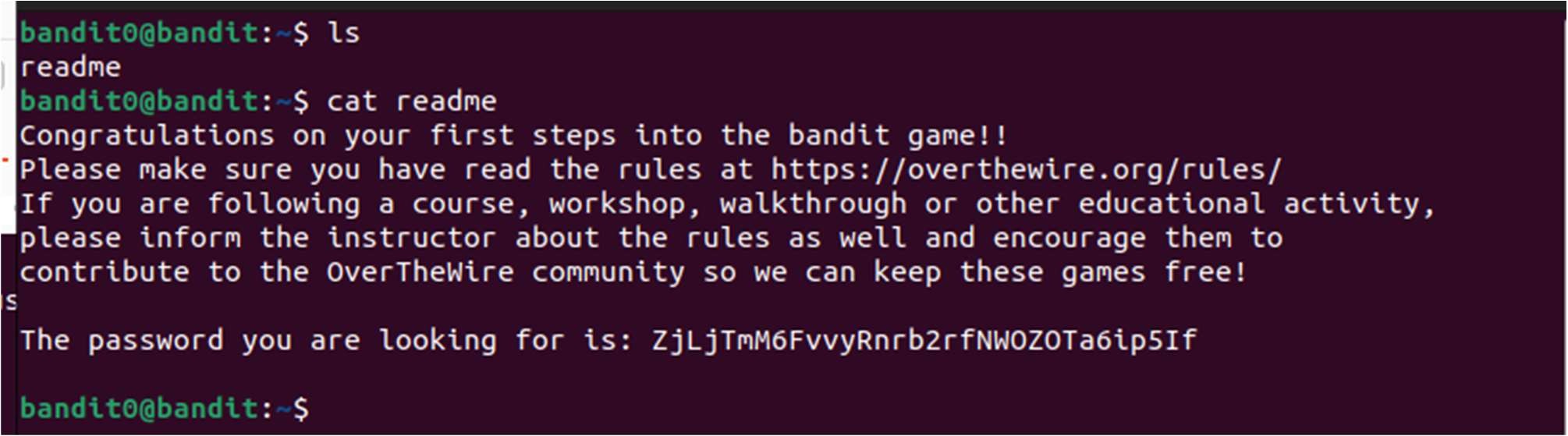




**Password:** bandit0

# Level 0 – Level 1

The password for the next level is stored in a file called **readme** located in the home directory. Use this password to log into bandit1 using SSH. Whenever you find a password for a level, use SSH (on port 2220) to log into that level and continue the game.



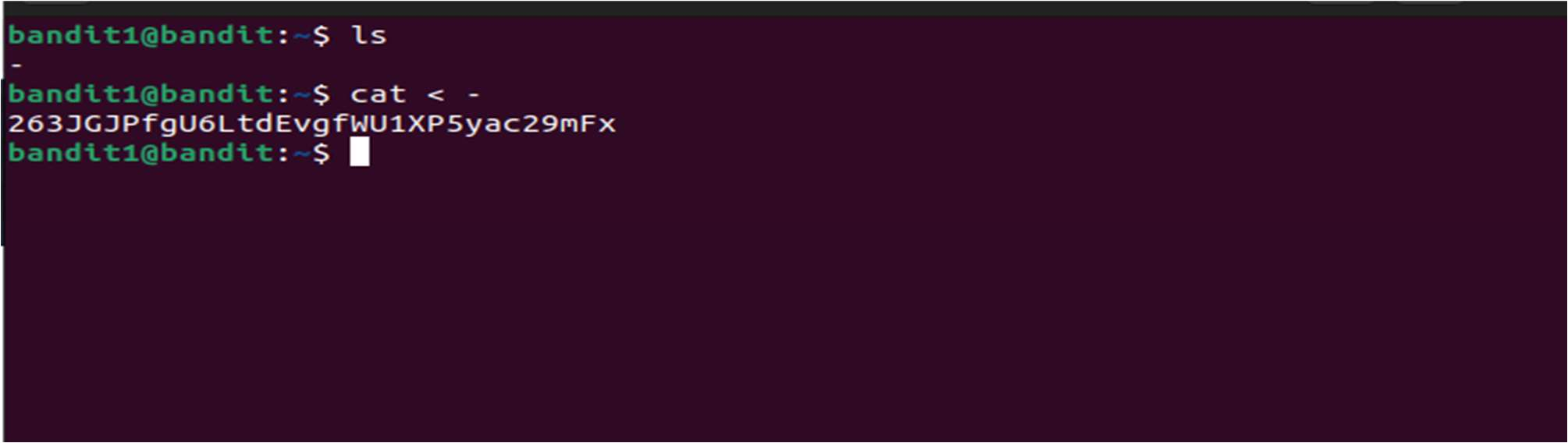
**Password:** ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

**Command:** cat readme

**Explanation:** cat displays the contents of the file, readme revealing the password.

# Level 1 – Level 2

The password for the next level is stored in a file called **-** located in the home directory



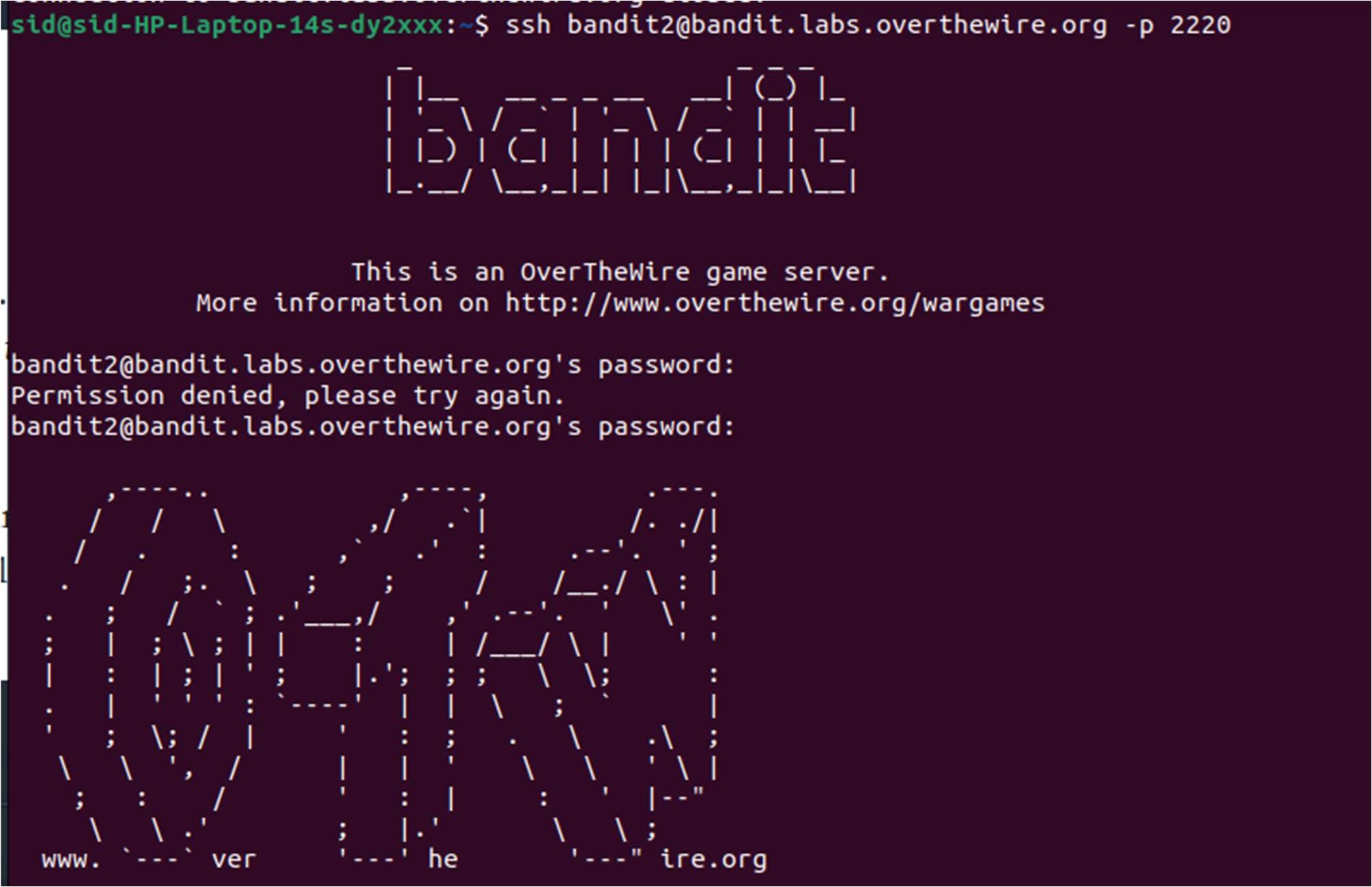
**Password:** 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

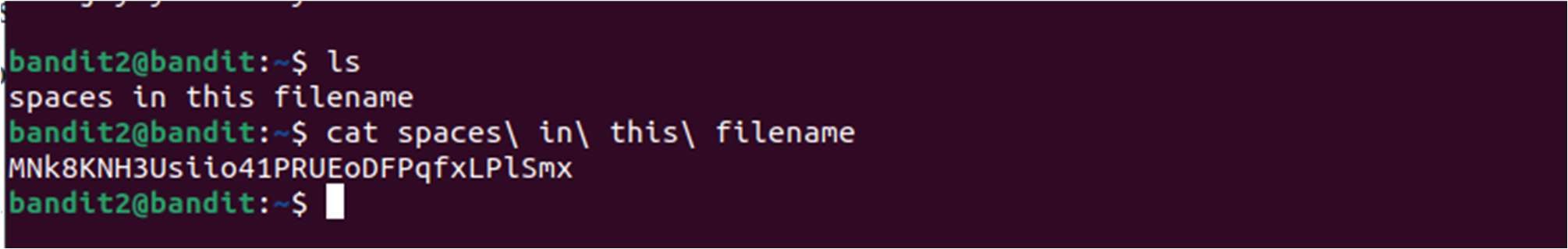
**Command:** cat ./-

**Explanation:** The ./ specifies the current directory and helps interpret - as a file, not an option for cat.

# Level 2 – Level 3

The password for the next level is stored in a file called **spaces in this filename** located in the home directory





**Password:** MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx

**Command:** cat "spaces in this filename"

**Explanation:** Quotes handle filenames with spaces.

# Level 3 – Level 4

The password for the next level is stored in a hidden file in the **inhere** directory.



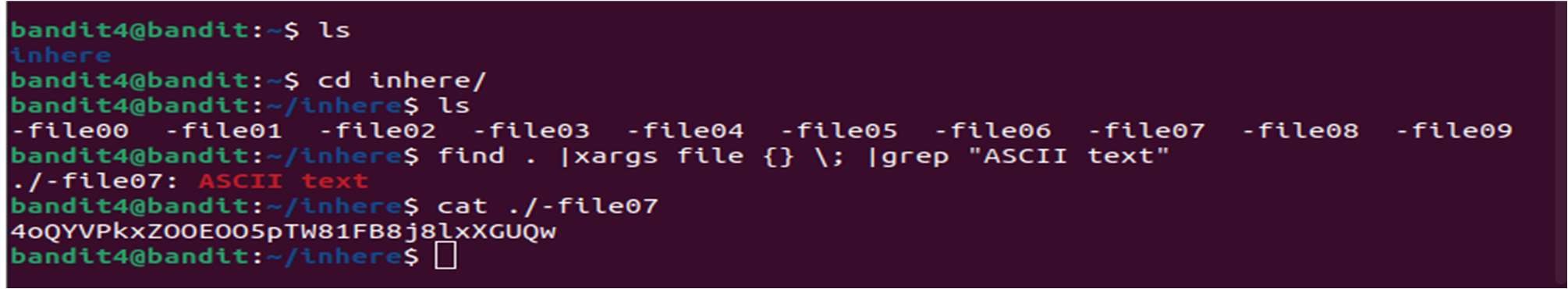
**Password:** 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

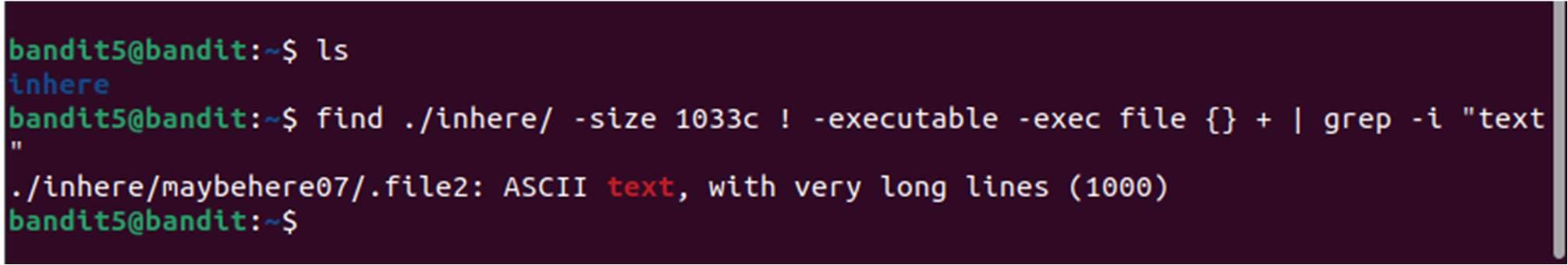
**Command:** ls -a cat .hidden

**Explanation:** ls -a lists all files, including hidden ones. cat displays the contents of .hidden.

# Level 4 – Level 5

The password for the next level is stored in the only human-readable file in the **inhere** directory. Tip: if your terminal is messed up, try the “reset” command.





**Password:** 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

**Command:** ls -l inhere/ cat inhere/<filename>

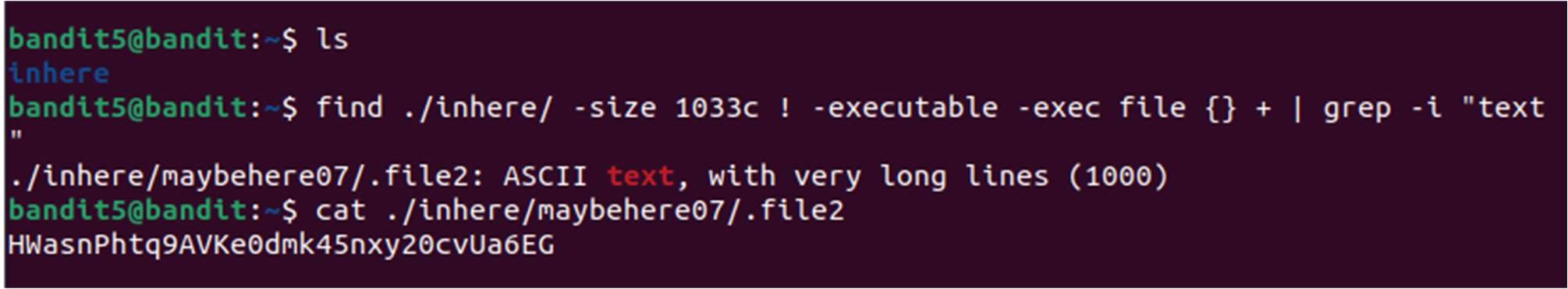
**Explanation:** ls -l lists file permissions. Identify the readable file and use cat to read it.

# Level 5 – Level 6

The password for the next level is stored in a file somewhere under the **inhere** directory and has all of the following properties:

* + human-readable
  + 1033 bytes in size
  + not executable





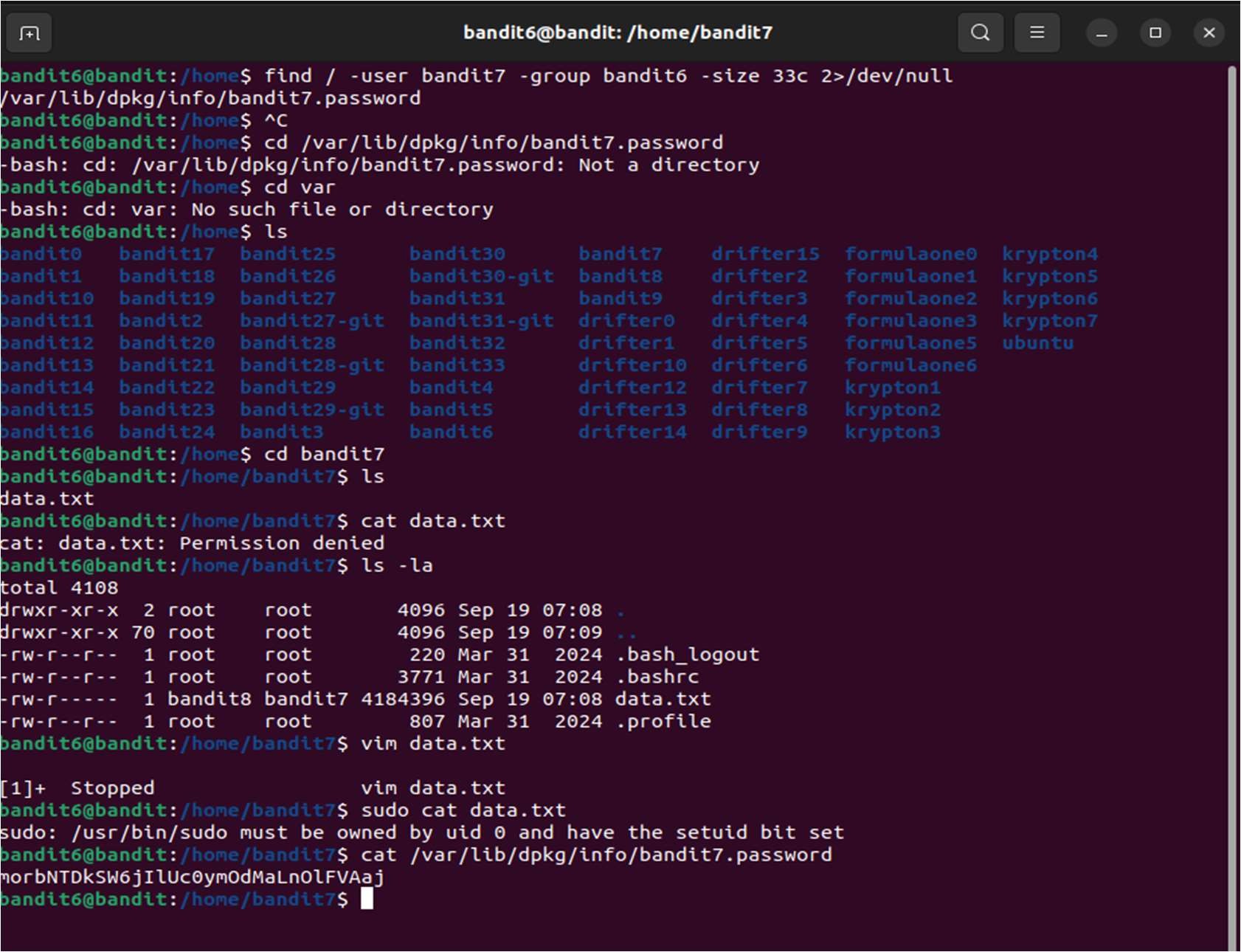
**Password:** HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

**Command:** find ./inhere/ -size 1033c ! -executable -exec file {} + | grep -i “text” cat ./inhere/maybehere07/.file2

**Explanation:** find locates the file by size and readability. cat displays its content. The c in 1033 is used to represent bytes. ! -executable means non executable file.

# Level 6 – Level 7

The password for the next level is stored **somewhere on the server** and has all of the following properties:



* + owned by user bandit7
  + owned by group bandit6
  + 33 bytes in size

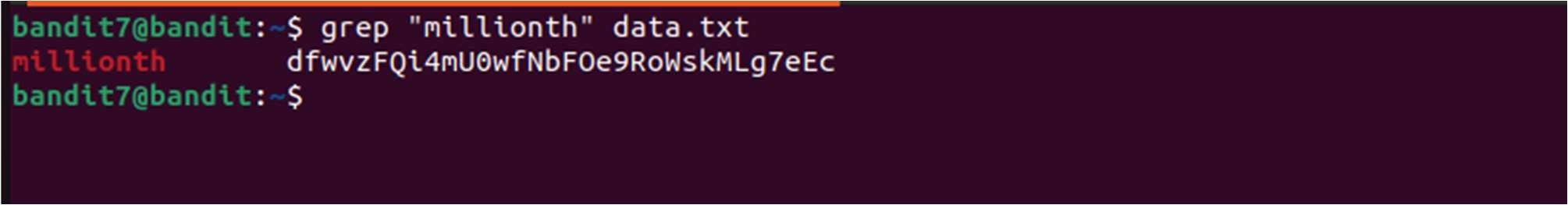
**Password:** morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj

**Command:** find / -user bandit7 -group bandit6 -size33c 2>/dev/null

**Explanation:** find searches files by user and size. 2>/dev/null suppresses errors.

# Level 7 -Level 8

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

****

**Password:** dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

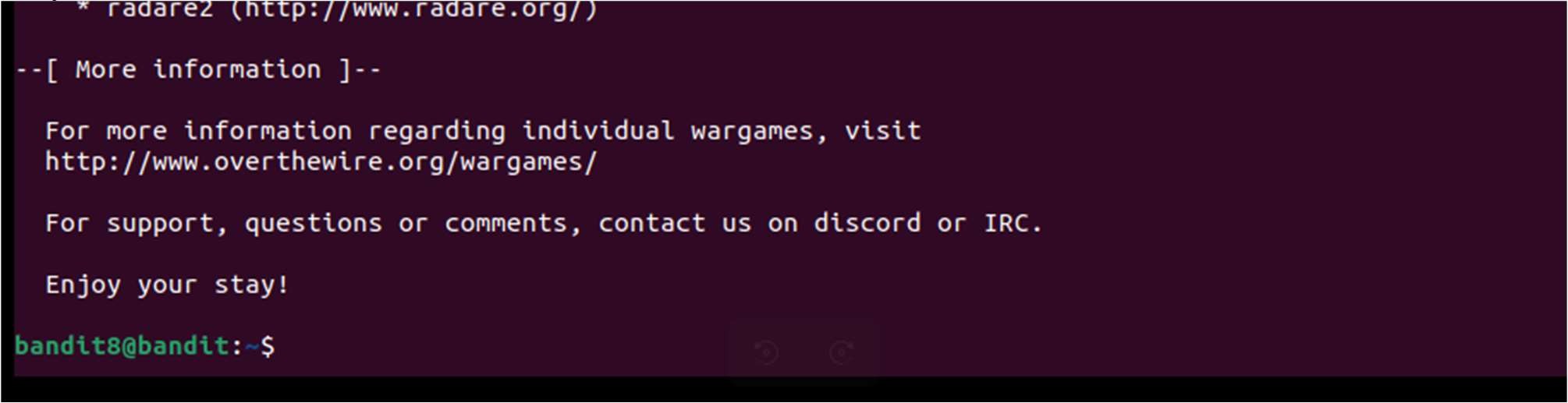
**Command:** grep "millionth" data.txt

**Explanation:** grep searches for the string millionth in data.txt.

Grep – global regular expression print. Used to search for patterns in a file.

# Level 8 – Level 9

The password for the next level is stored in the file **data.txt** and is the only line of text that occurs only once





**Password:** 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

**Command:** sort data.txt | uniq -u

**Explanation:** sort organizes lines, and uniq -u identifies unique lines. Uniq alone just removes the consecutive duplicate lines. The -u flag removes all the duplicate lines in the file.

# Level 9 – Level 10

The password for the next level is stored in the file **data.txt** in one of the few human-readable strings, preceded by several ‘=’ characters.



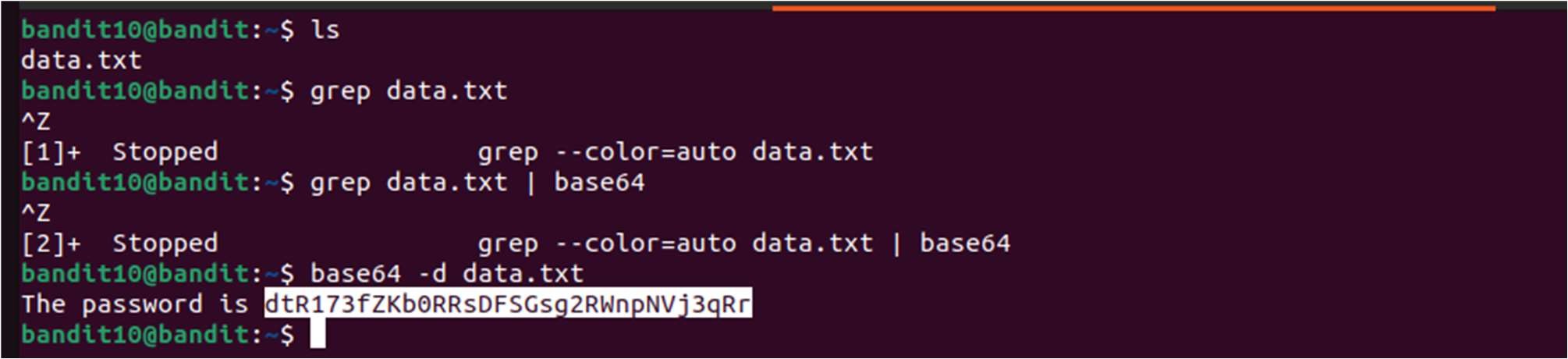
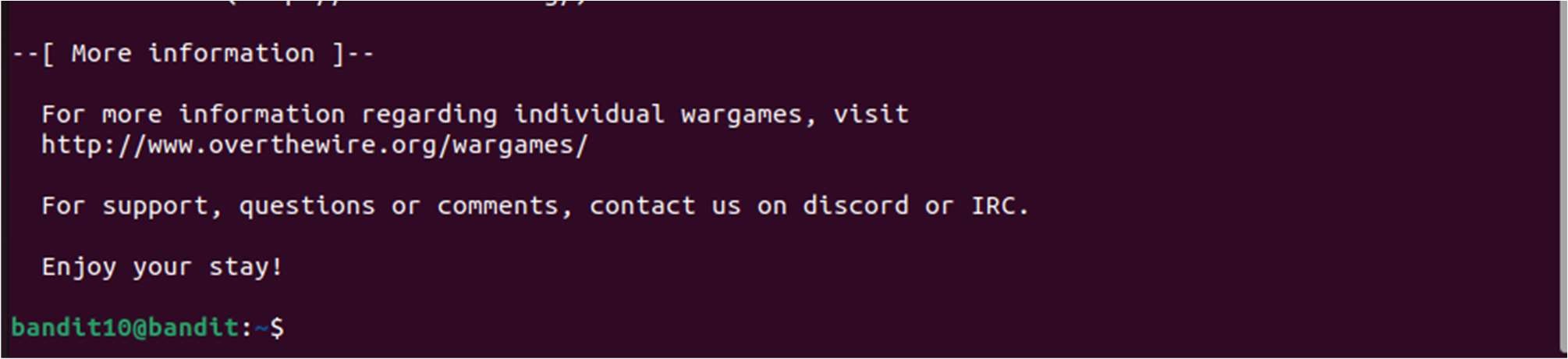
**Password:** FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

**Command:** strings data.txt | grep "=="

**Explanation:** strings extracts readable text from binary files. grep filters lines with ==.

# Level 10 - Level 11

The password for the next level is stored in the file **data.txt**, which contains base64 encoded data



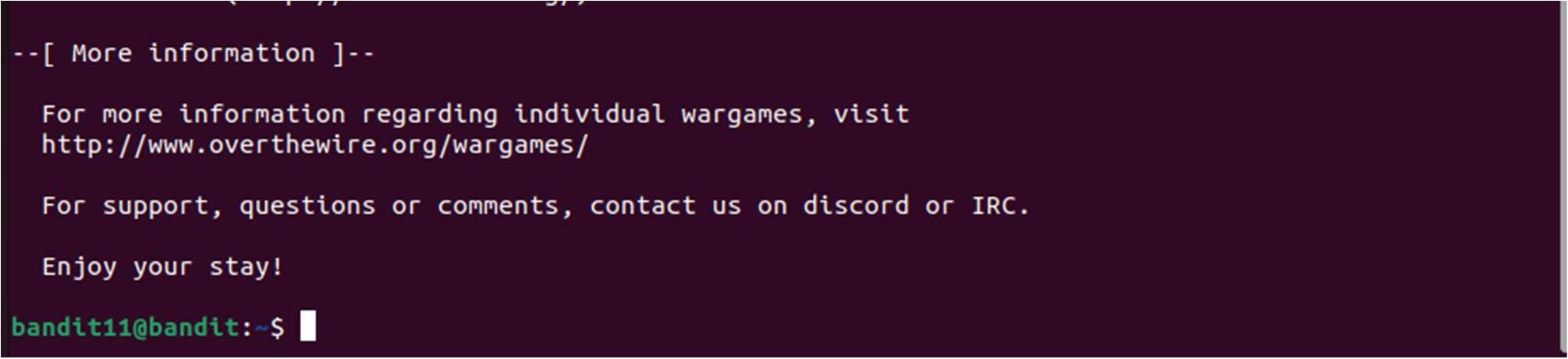
**Password:** dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

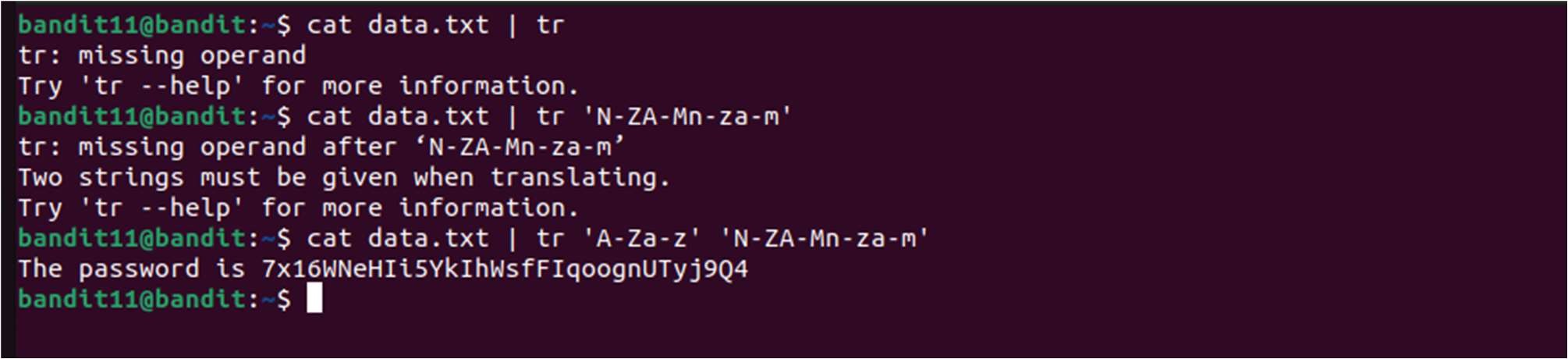
**Command:** base64 -d data.txt

**Explanation:** base64 -d decodes the contents of data.txt. The -d signifies decoding

# Level 11 – Level 12

The password for the next level is stored in the file **data.txt**, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions





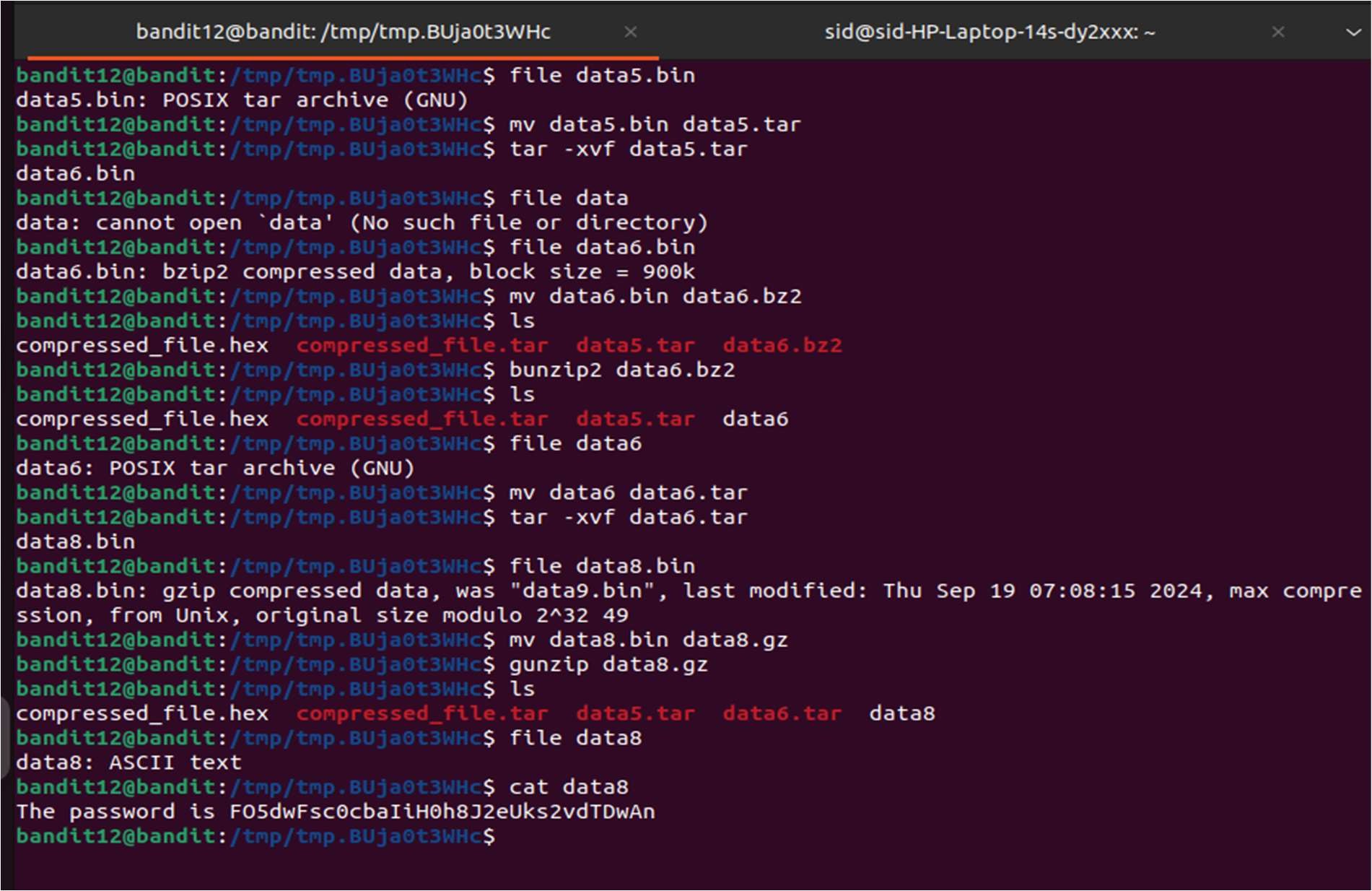
**Password:** 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4

**Command:** cat data.txt | tr ‘A-Za-z’ ‘N-ZA-Mn-za-m’

**Explanation:** the tr (translate) command decode the ROT13 passwd back to normal. This command is used to both encode and decode in ROT13 cipher.

# Level 12 – Level 13

The password for the next level is stored in the file **data.txt**, which is a hexdump of a file that has been repeatedly compressed. For this level it may be useful to create a directory under /tmp in which you can work. Use mkdir with a hard to guess directory name. Or better, use the command “mktemp -d”. Then copy the datafile using cp, and rename it using mv (read the manpages!)



Password: FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn Command: mkdir /tmp/mydir

cp data.txt /tmp/mydir

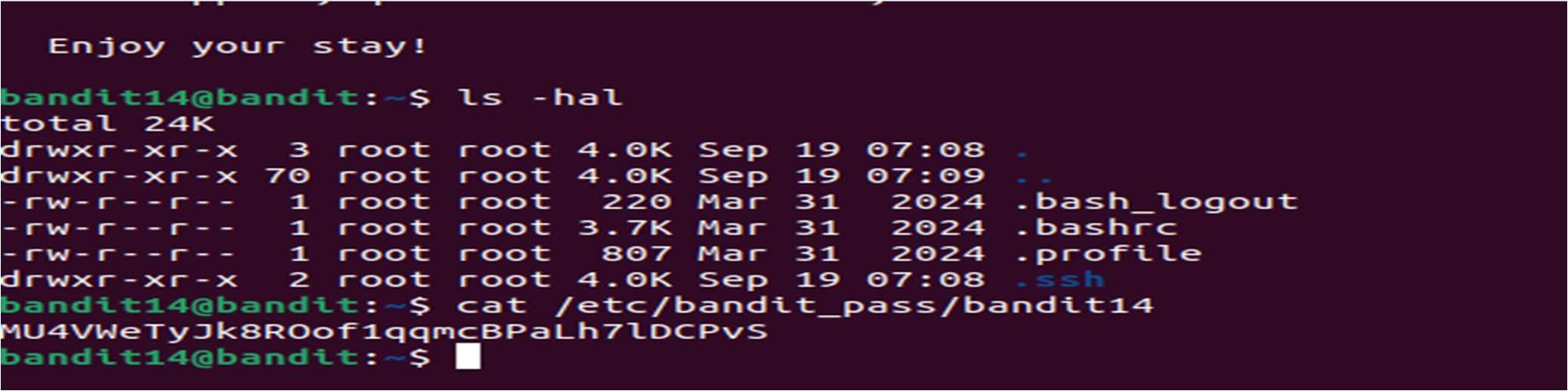
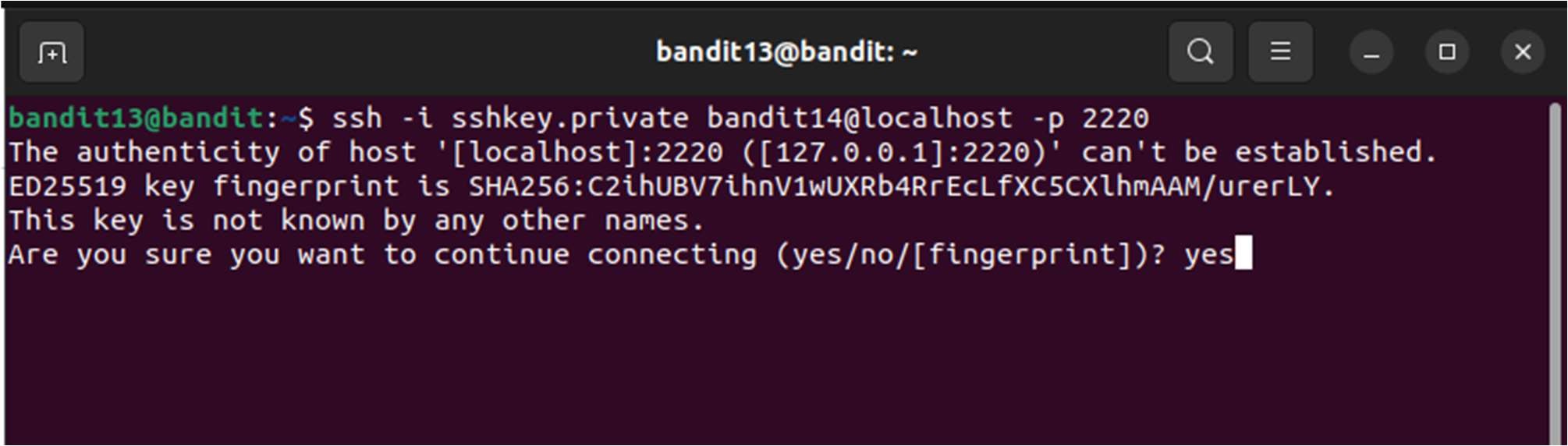
cd /tmp/mydir file data.txt # Use the file type to decide decompression commands: xxd -r data.txt # For hex

gzip -d file.gz tar -xf file.tar bzip2 -d file.bz

**Explanation:** Create a temporary file in /tmp and store the contents in it. Then decompress it based on its relative compressed modes and obtain the psswd from data8 file. Properties of a file can be obtained from file command.

# Level 13 – Level 14

The password for the next level is stored in **/etc/bandit\_pass/bandit14 and can only be read by user bandit14**. For this level, you don’t get the next password, but you get a private SSH key that can be used to log into the next level. **Note: localhost** is a hostname that refers to the machine you are working on



**Password:** MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS

**Command:** ssh -i sshkey.private bandit14@localhost cat /etc/bandit\_pass/bandit14

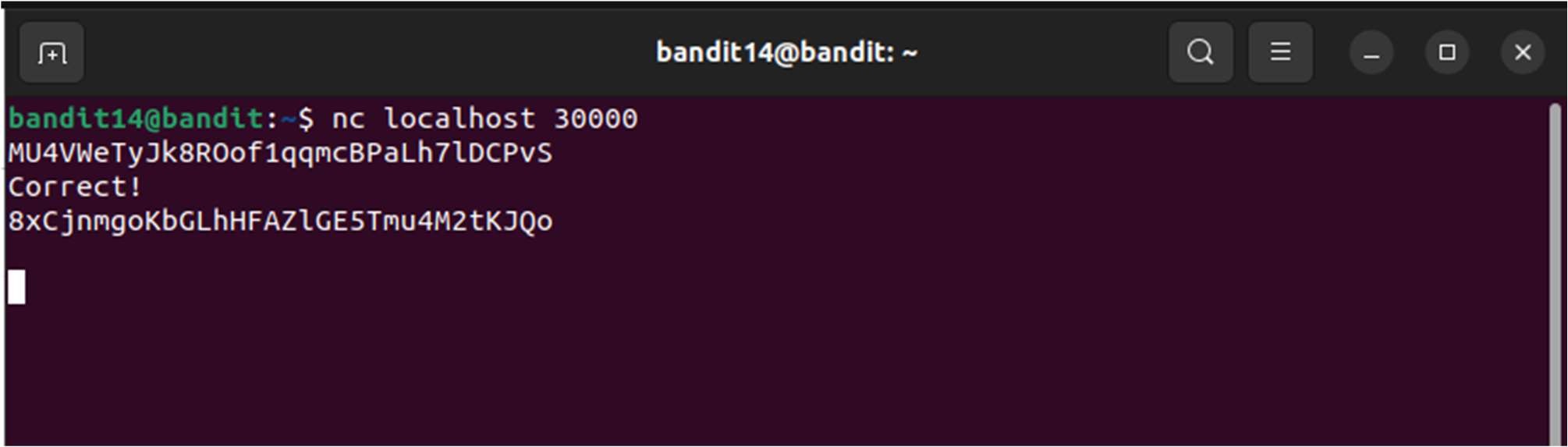
**Explanation:** ssh is used to access bandit14 locally and then obtain the psswd from the file cat

/etc/bandit\_pass/bandit14 stored in bandit 14.

1. **Level 14 – Level 15**

The password for the next level can be retrieved by submitting the password of the current level to

## port 30000 on localhost.



**Password:** 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

**Command:** nc localhost 30000

**Explanation:** The command nc localhost 30000 is used to connect to a server running on your local machine (localhost) at port 30000. Then enter your current psswd to obtain the next level’s psswd.