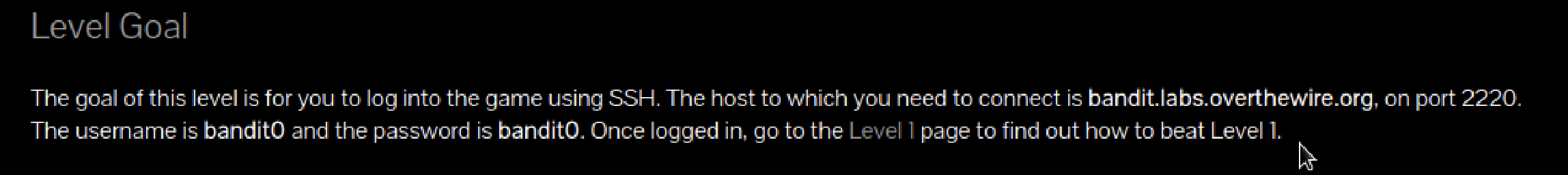
BANDIT WRITEUPS

**Level 0->1**

Question -

****

Solution –

Use the command – ssh [bandit0@bandit.labs.overthewire.org](mailto:bandit0@bandit.labs.overthewire.org) -p 2220

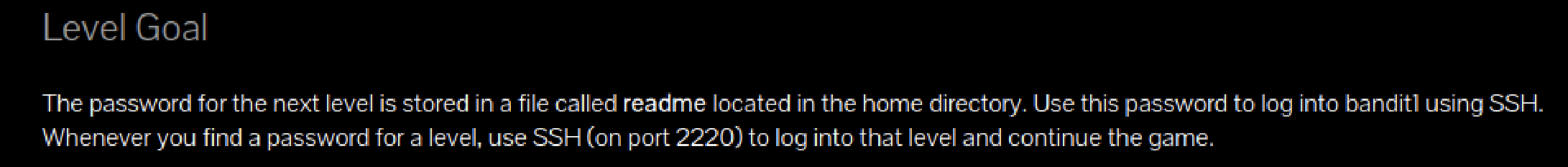
Then follow these steps

Text

Description automatically generated

**Level 1->2**

Question –

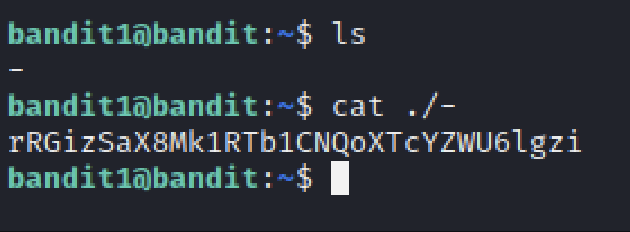


Solution –

Use the command- ssh [bandit1@bandit.labs.overthewire.org](mailto:bandit1@bandit.labs.overthewire.org) -p 2220

Use the password obtained in the previous level to login into this level

Then follow these steps -



**Level 2->3**

Question -

Text

Description automatically generated

Solution –

Use the command- ssh [bandit2@bandit.labs.overthewire.org](mailto:bandit2@bandit.labs.overthewire.org) -p 2220

Use the password obtained in the previous level to login into this level

Then follow these steps

Text

Description automatically generated

**Level 3->4**

Question –

Text

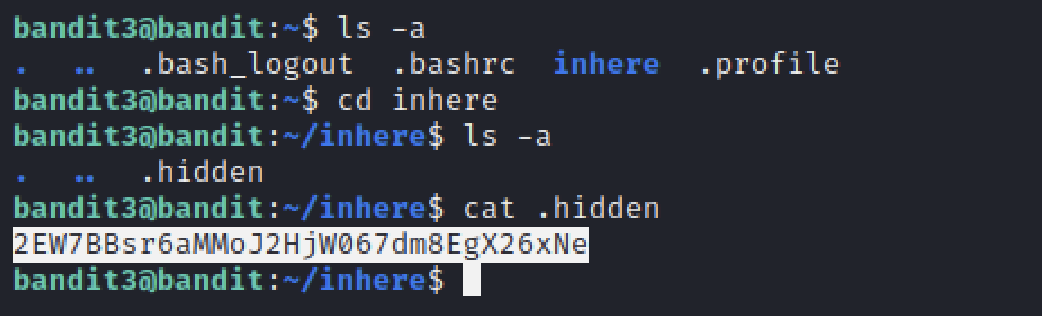
Description automatically generated

Solution –

Use the command- ssh [bandit3@bandit.labs.overthewire.org](mailto:bandit3@bandit.labs.overthewire.org) -p 2220

Use the password obtained in the previous level to login into this level

Then follow these steps



**Level 4->5**

Question –

A picture containing text

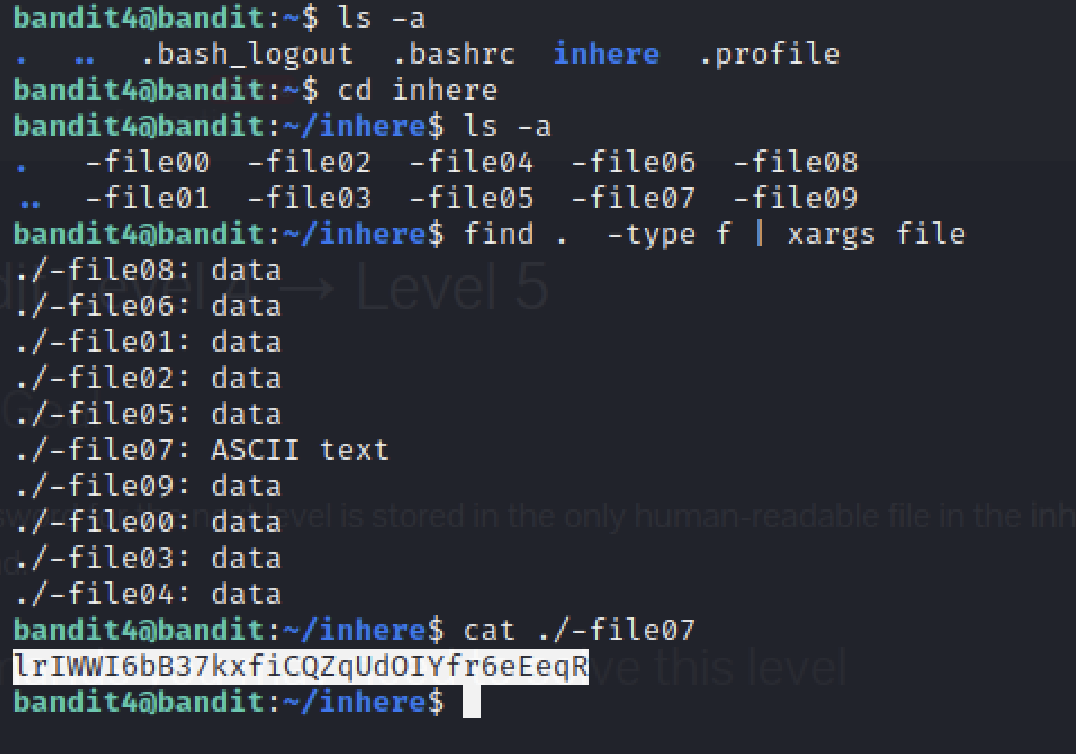
Description automatically generated

Solution –

Use the command- ssh [bandit4@bandit.labs.overthewire.org](mailto:bandit4@bandit.labs.overthewire.org) -p 2220

Use the password obtained in the previous level to login into this level

Then follow these steps



The find command is used to look for files. “xargs file” is passed as the file is mentioned to be human-readable.

**Level 5->6**

Question

Text

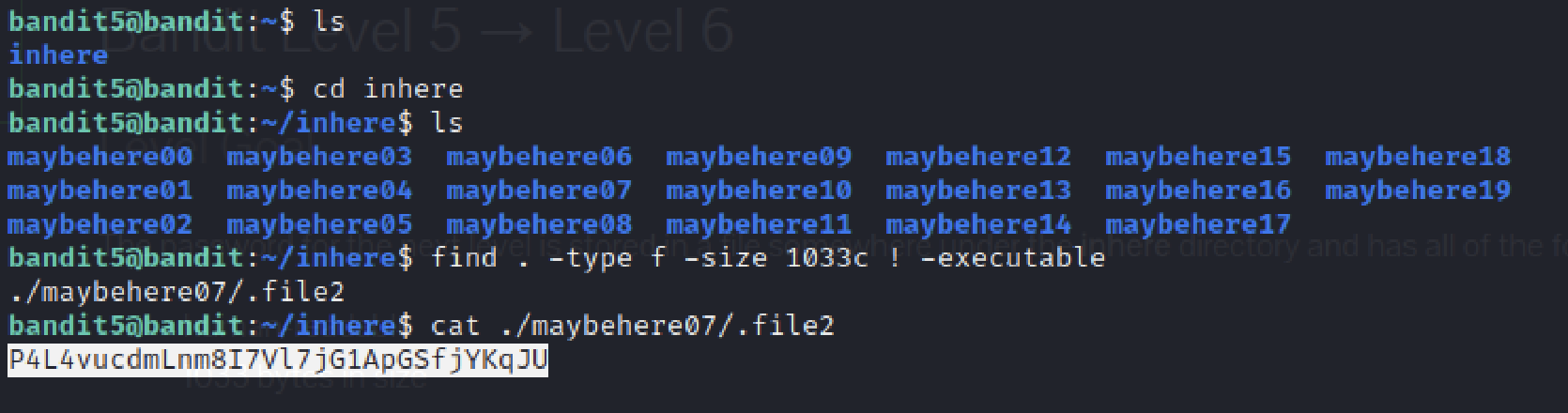
Description automatically generated

Solution –

Use the command- ssh [bandit5@bandit.labs.overthewire.org](mailto:bandit5@bandit.labs.overthewire.org) -p 2220

Use the password obtained in the previous level to login into this level

Then follow these steps



The arguments to the find command are the size of the file and it is mentioned to be not executable.

**Level 6->7**

Question

Text

Description automatically generated

Solution –

Use the command- ssh [bandit6@bandit.labs.overthewire.org](mailto:bandit6@bandit.labs.overthewire.org) -p 2220

Use the password obtained in the previous level to login into this level

Then follow these steps

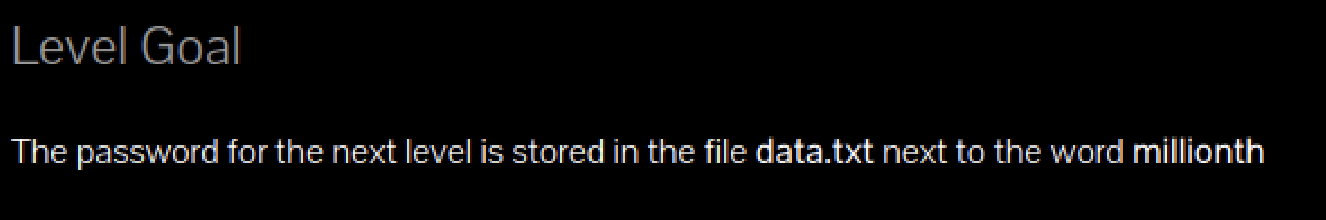
Text

Description automatically generated

The find command now has user, group and size as the arguments. The “2>/dev/null” is used to filter the files which deny permission.

**Level 7->8**

Question

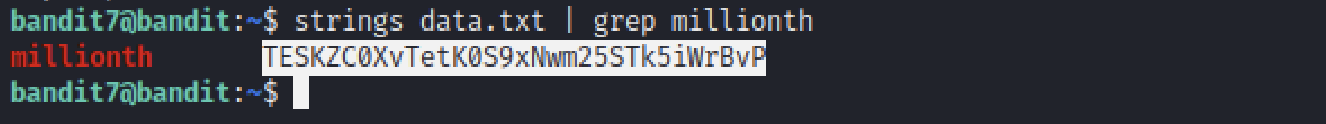


Solution –

Use the command- ssh [bandit7@bandit.labs.overthewire.org](mailto:bandit7@bandit.labs.overthewire.org) -p 2220

Use the password obtained in the previous level to login into this level

Then follow these steps



The grep command is used to find the strings in a given file

**Level 8->9**

Question

Text

Description automatically generated

Solution –

Use the command- ssh [bandit8@bandit.labs.overthewire.org](mailto:bandit8@bandit.labs.overthewire.org) -p 2220

Use the password obtained in the previous level to login into this level

Then follow these steps

Graphical user interface, text

Description automatically generated

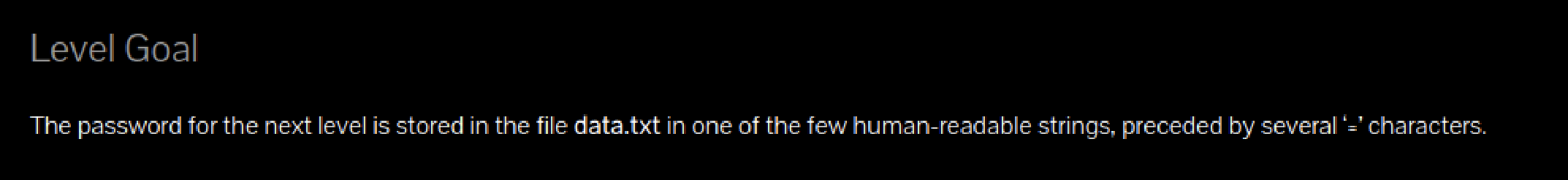
The uniq -c command gives all the unique strings with the number of repetitions. Out of all the strings, only one string appears once. Which is the password for the next level.

Graphical user interface, application, Teams

Description automatically generated

**Level 9->10**

Question



Solution –

Use the command- ssh [bandit9@bandit.labs.overthewire.org](mailto:bandit9@bandit.labs.overthewire.org) -p 2220

Use the password obtained in the previous level to login into this level

Then follow these steps

Text

Description automatically generated

**Level 10->11**

Question

Text

Description automatically generated

Solution –

Use the command- ssh [bandit10@bandit.labs.overthewire.org](mailto:bandit10@bandit.labs.overthewire.org) -p 2220

Use the password obtained in the previous level to login into this level

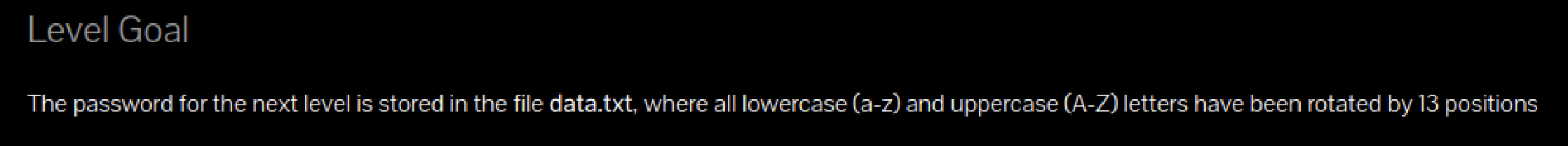
Then follow these steps –

Text

Description automatically generated

Level 11->12

Question

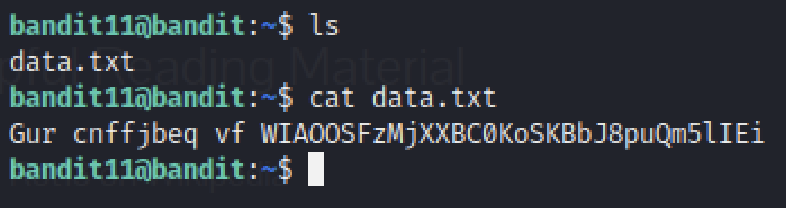


Solution –

Use the command- ssh [bandit11@bandit.labs.overthewire.org](mailto:bandit11@bandit.labs.overthewire.org) -p 2220

Use the password obtained in the previous level to login into this level

Then follow these steps –



As mentioned in the question, the letters are rotated by 13 positions. So, this is a rot 13 cypher text. Hence, I used an online tool to decode the cipher.

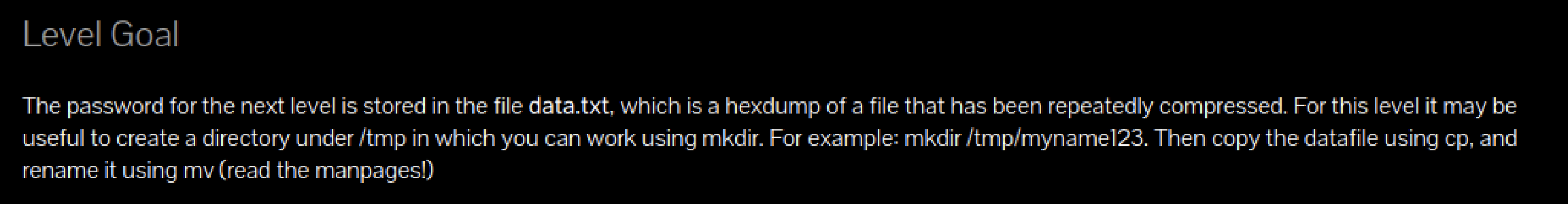
Graphical user interface, text, application

Description automatically generated

This password can now be used to log in to the next level.

**Level 12->13**

Question

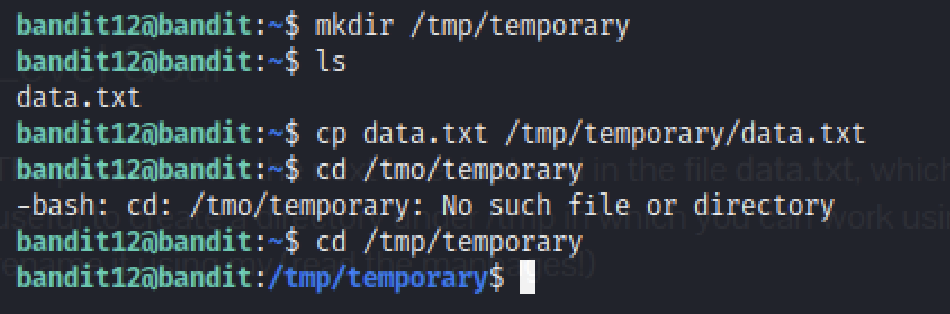


Solution –

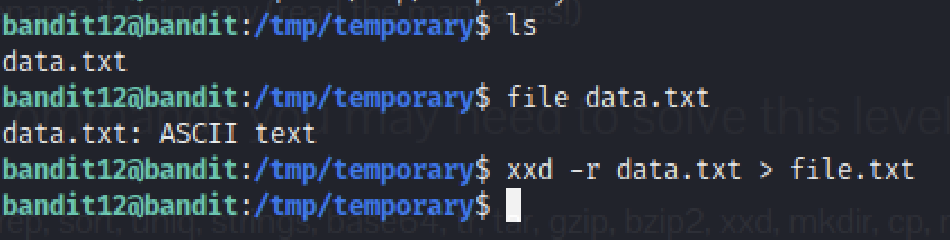
Use the command- ssh [bandit12@bandit.labs.overthewire.org](mailto:bandit12@bandit.labs.overthewire.org) -p 2220

Use the password obtained in the previous level to login into this level

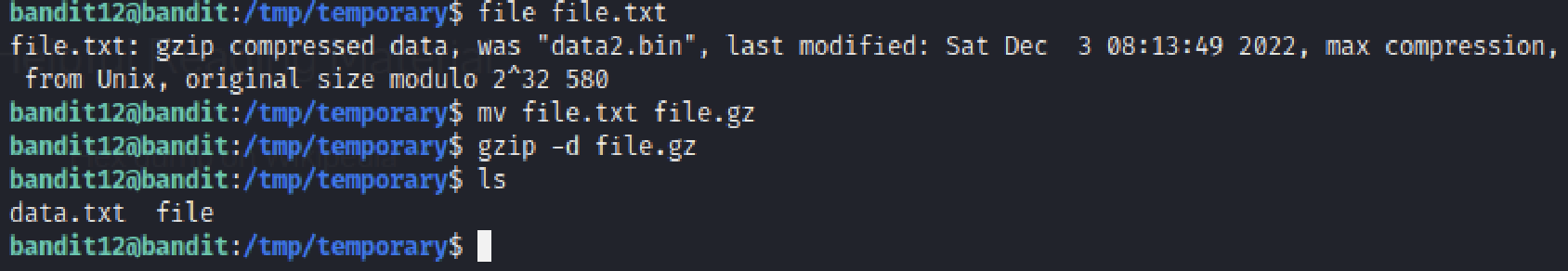
Then follow these steps –



Using the mkdir command, a new directory is created and the file data.txt is copied to that directory.



The file command is used to know the kind of file given. This file is a hexdump as mentioned. So The xxd -r command reverses the hexdump and the output of that is now stored in a file called file.txt

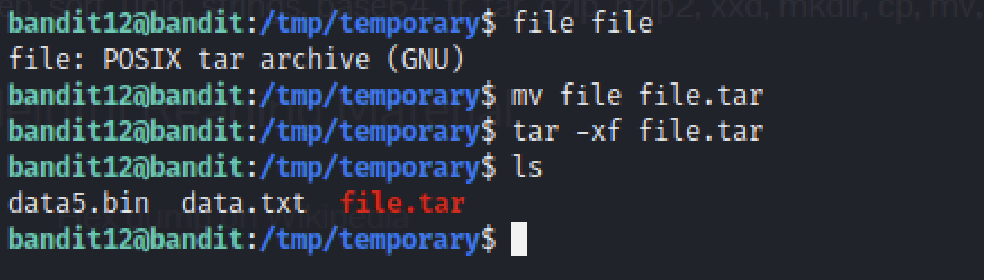


The file is now gzip compressed. So, the file has to be given a suitable extension which is done using the mv command. Then “gzip -d” decompresses the file.

Text

Description automatically generated

This file is now bzip2 compressed. Which is then given a suitable extension and decompressed using “bzip2 -d” command.



In a few such iterations, we come across a tar archive. Again, the file extension must be changed and the “tar -xf” command is used to extract the file.

Text

Description automatically generated After several iterations of decompressions, we come across a file of ASCII text containing our password for the next level.