Sri Lanka Institute of Information Technology

BSc Honors in information Technology

Specializing in Cyber Security

IE2021 – System and Network Programming

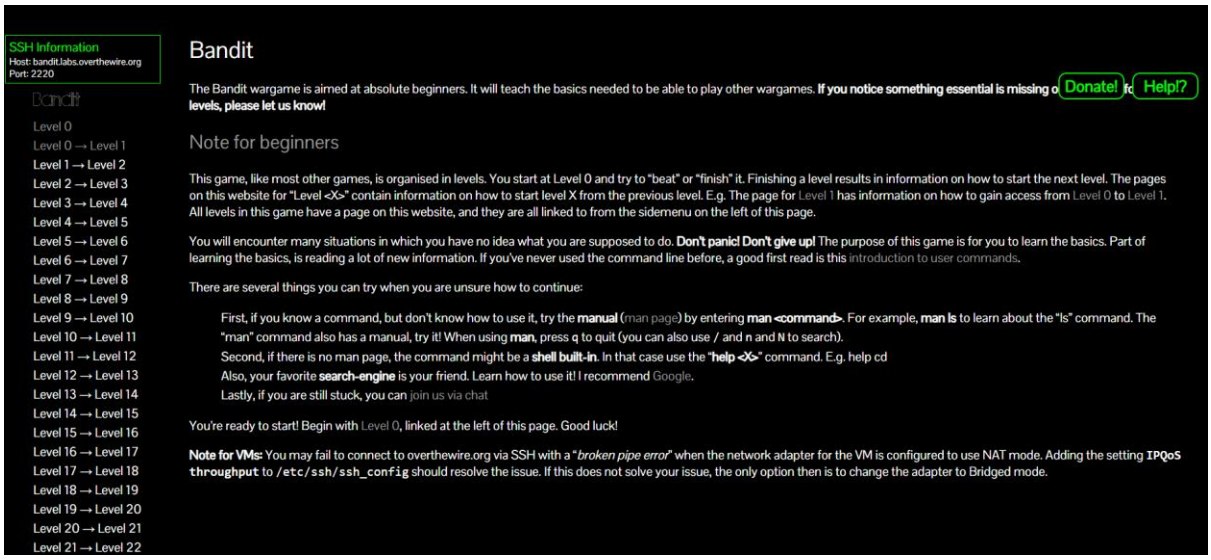
Bandit Overthewire (Level 0 – 20)

IT23238794

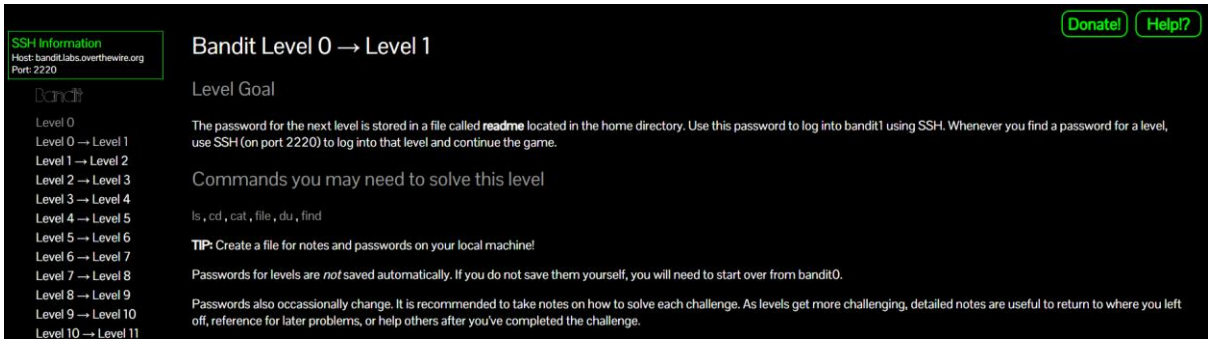
DISSANAYAKE Y.Y

Bandit 0

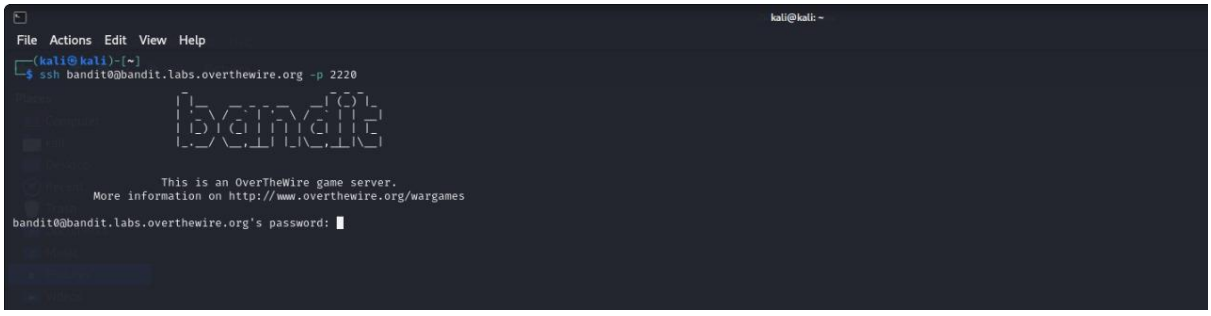
Before starting Bandit 0 we are given a brief introduction about Bandit and how the game progresses.



Here we can continue the Bandit game on Windows or Linux. Must log in via SSH to start. We have been given the username and password for Bandit 0.



Type, "ssh bandit.labs.overthewire.org -p 2220 -l bandit0" and use the given password log Bandit0.



Bandit0 -> Bandit1

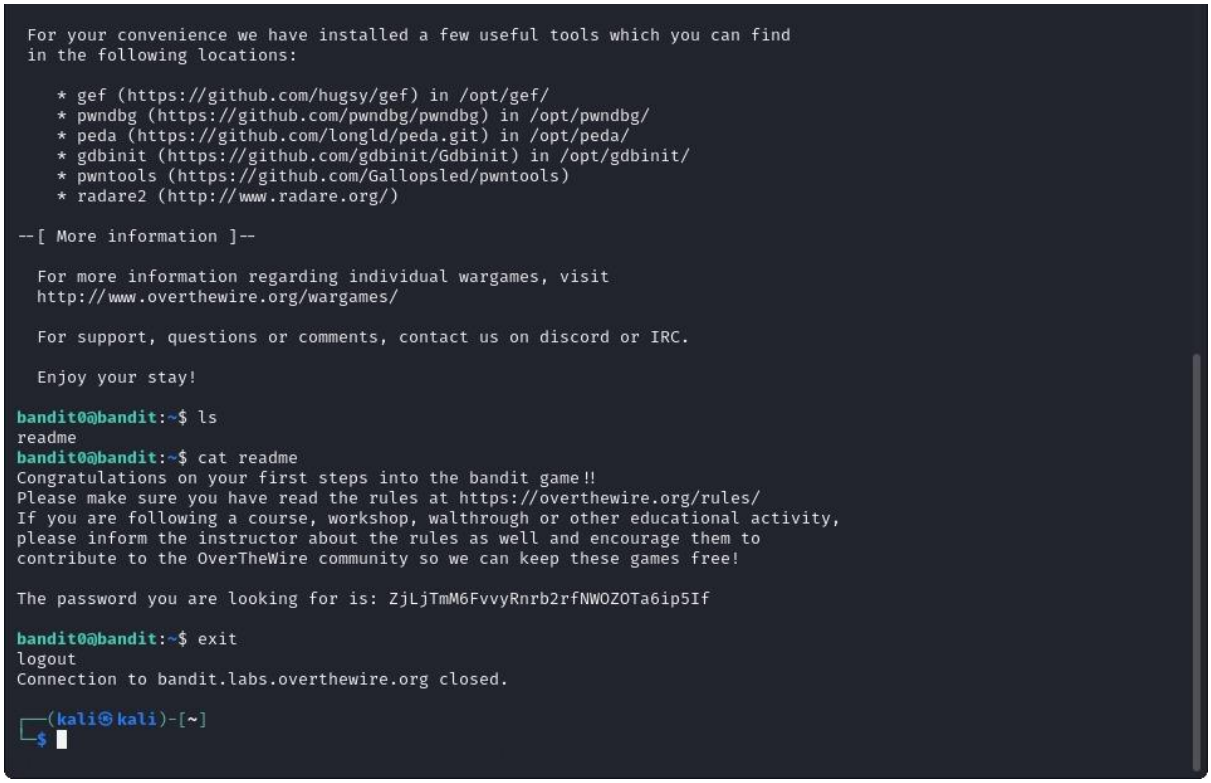
Once we log Bandit0 we need to find the password of Bandit 1. They give us a hint and some commands. Here are those commands.

- ls – list directory.
- cd – change the working directory.
- cat - print the content of a file onto the standard output stream.
- file – determine file type.
- du – measure the disk space occupied by files or directories.
- find - search for files in a directory hierarchy.

Use the “ls” command to see the file readme.

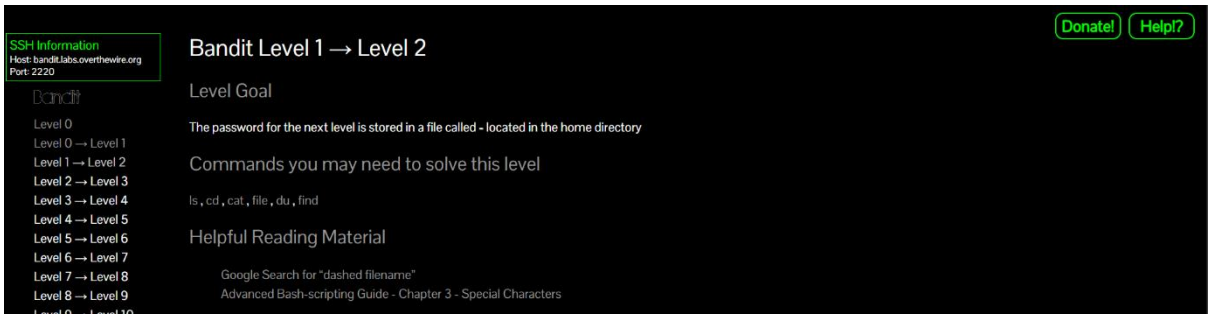
Run “cat readme” to see the contents of the readme and to get the password.

To logout, run “exit”.



Bandit1 -> Bandit2

Read the hint and try to get an idea.



Now log in to Bandit1, from the found password.

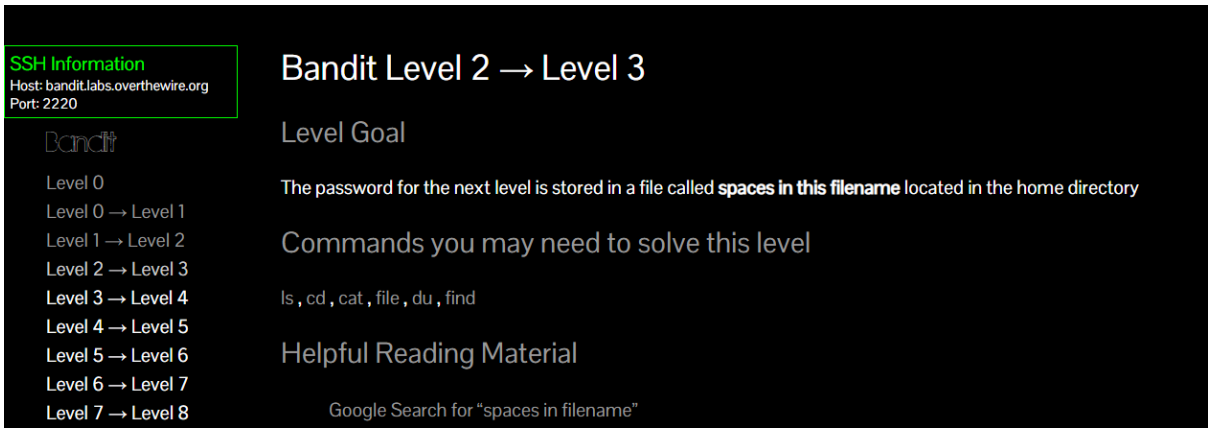
Run the “ls” command and find the “- “file

Use the “cat” command to find the Bandit2 password. But we cannot use the cat command and only “- “because the system thinks “- “is a command. So, we need to use the cat command within “. /- “these commands and get the password.

Log out using the “exit” command.

Bandit 2 -> Bandit 3

They tell us the next password is in a “spaces in this filename” file.



Log into Bandit2 using the username and the password.

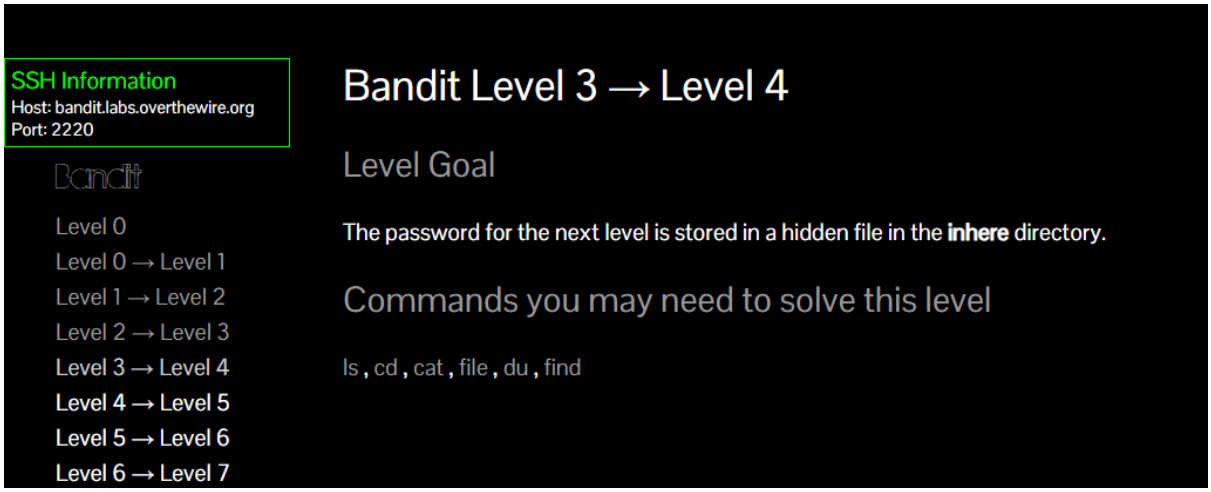
Using the “ls” command find the file name.

Run the “cat” command with the file name. You can get the Bandit3 password.

Log out using the “exit” command.

Bandit3 -> Bandit4

Log Bandit 3 to use the password.



The next level password is hidden in the inhere file. Using the “ls” command find the “inhere” file name.

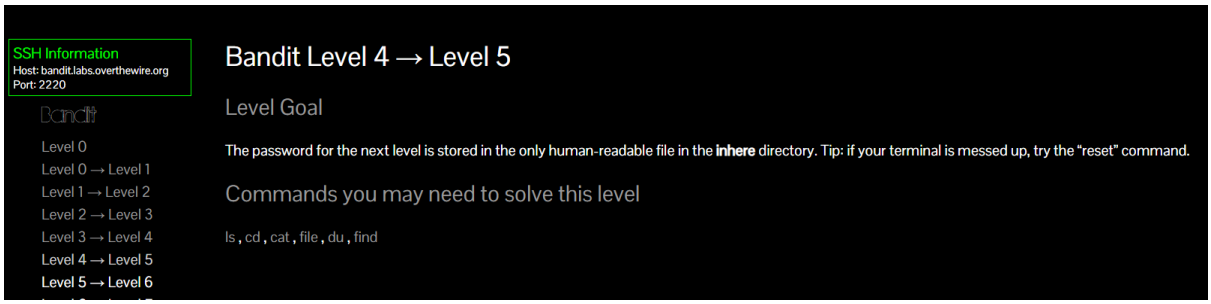
Using the “cd” command change the directory. Only non-hidden files are displayed by the “ls” command. With the “-a” flag, however, it displays all files, including hidden files.

We can read the contents of the file because it is named “. hidden” and includes the password

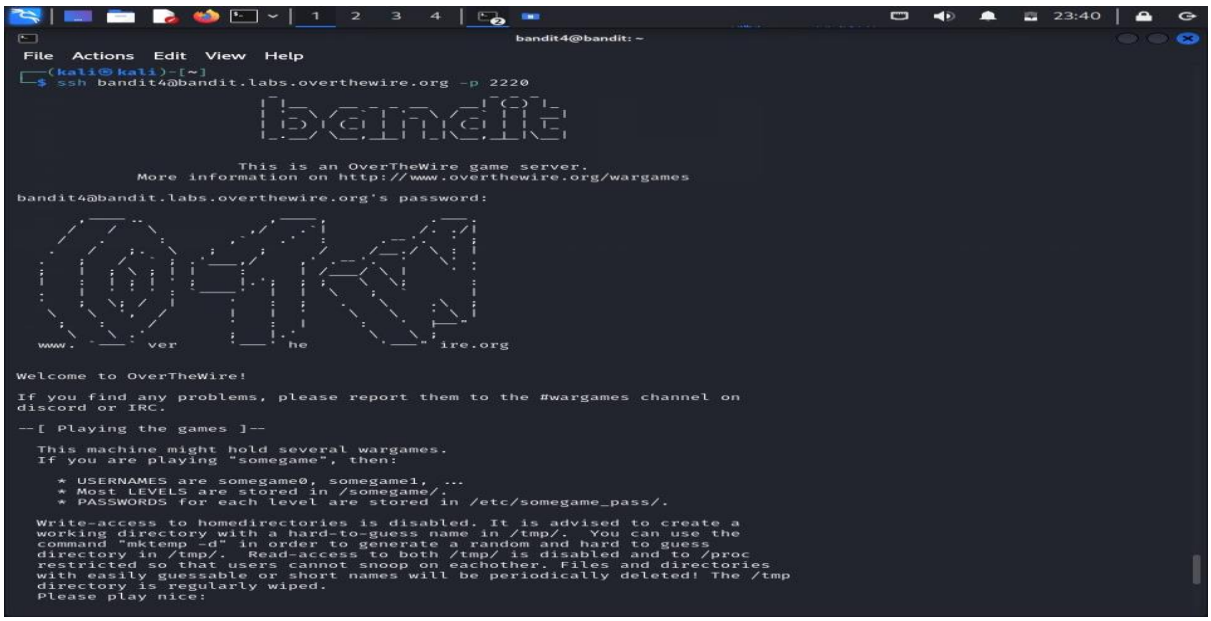
Log out using the “exit” command.

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

  Enjoy your stay!

bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -a
.  ..  ...Hiding-From-You
bandit3@bandit:~/inhere$ cat  ...Hiding-From-Yo
cat:  ...Hiding-From-Yo: No such file or directory
bandit3@bandit:~/inhere$ cat  ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.

┌──(kali㉿kali)-[~]
└─$
```

Bandit4 -> Bandit5



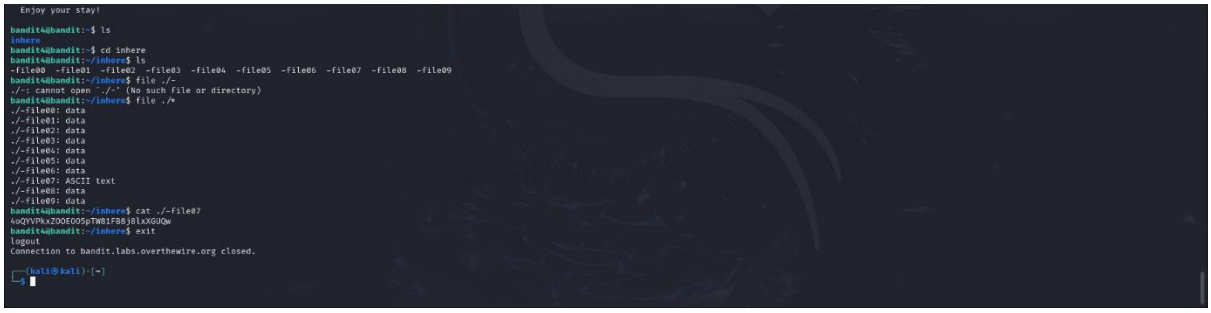
Log into the Bandit4 using the password. Use the “ls” command and find the file.



Using the “cd” command change the directory. And use the “ls” command.

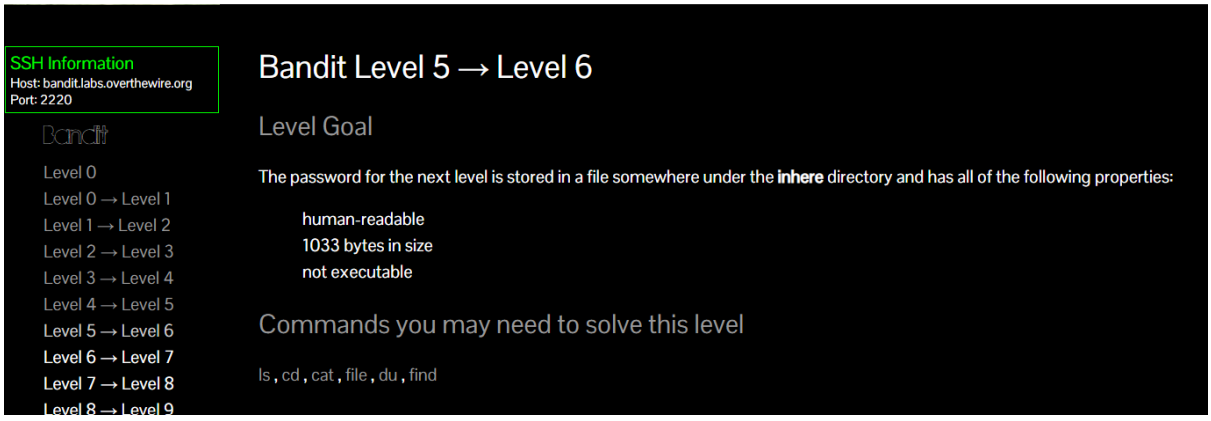
Type “./-file*” to get a list of all the files in the directory along with their data types.

The “-file07” has ASCII text. Type “cat ./-file07” to get the password of Bandit5.



Bandit5 -> Bandit6

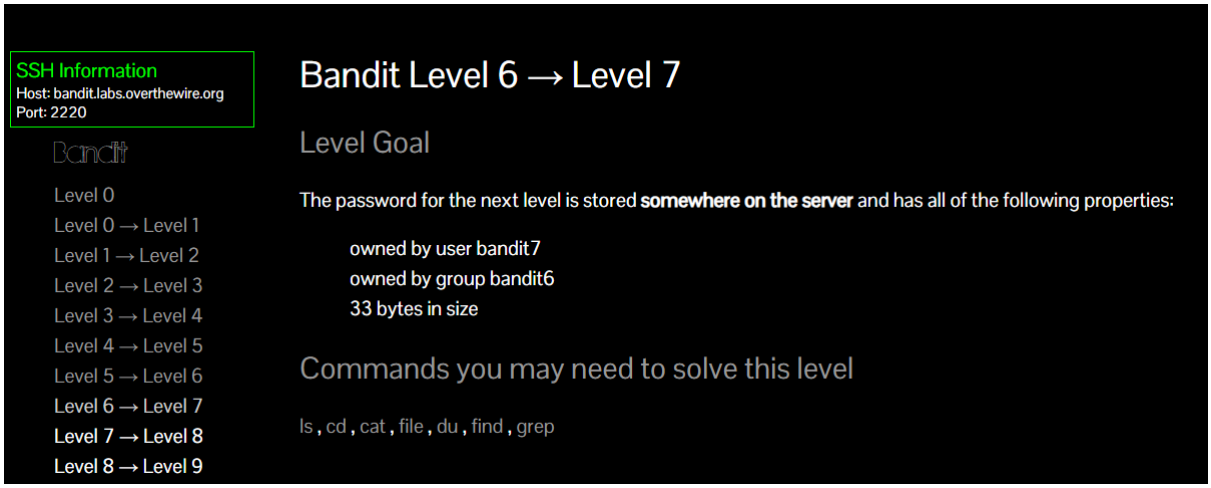
Log in to Bandit05 using the password.



Type the “ls” to find the file name. Next type the “cd inheres” to change the directory. Again, type the “ls” to list directory.

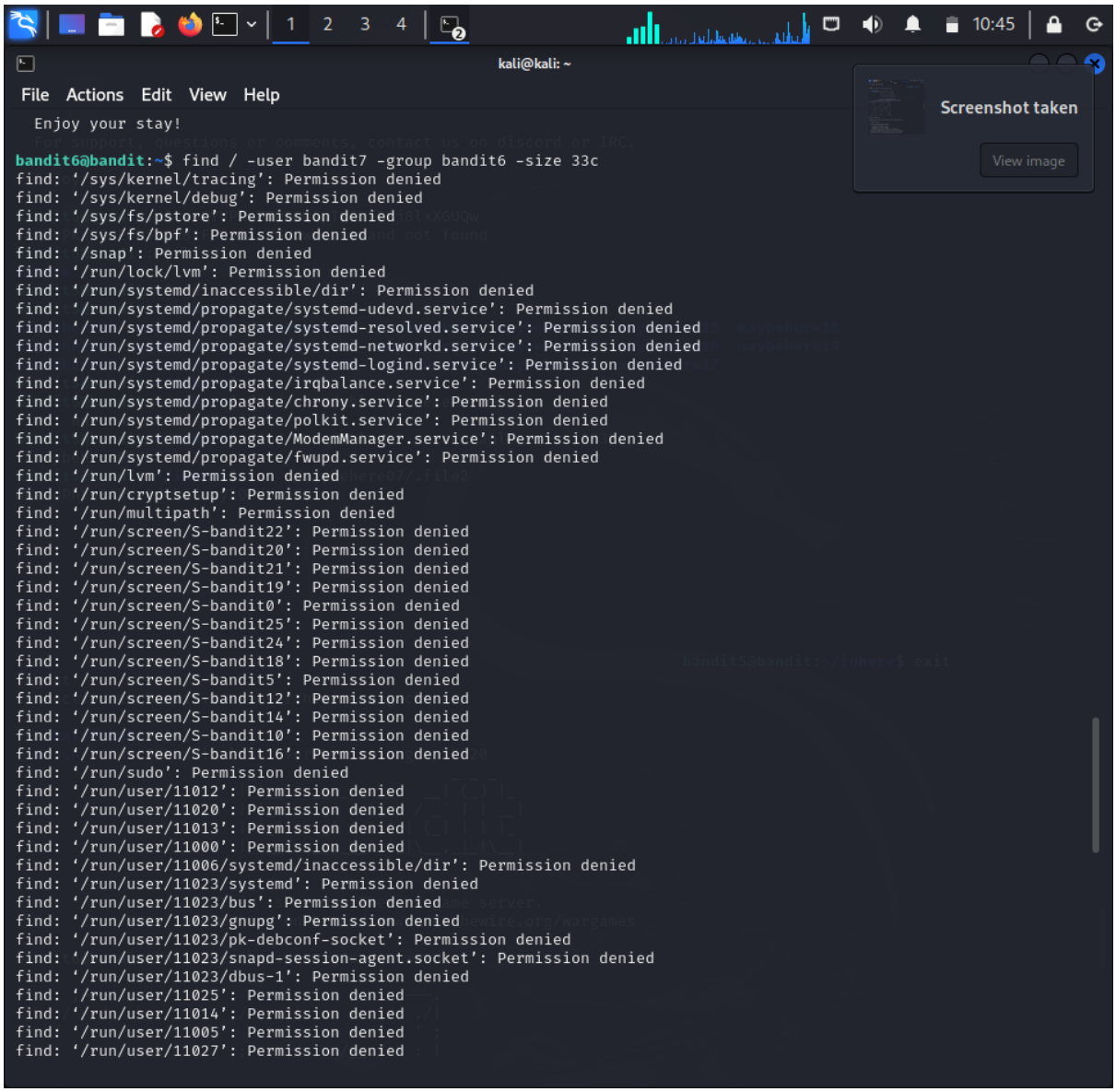
Type the “find -size 1033c” to find files that are readable with a size of 1033c. Forget the password, type “cat. maybehere07/. file2”.

Bandit6 -> Bandit7

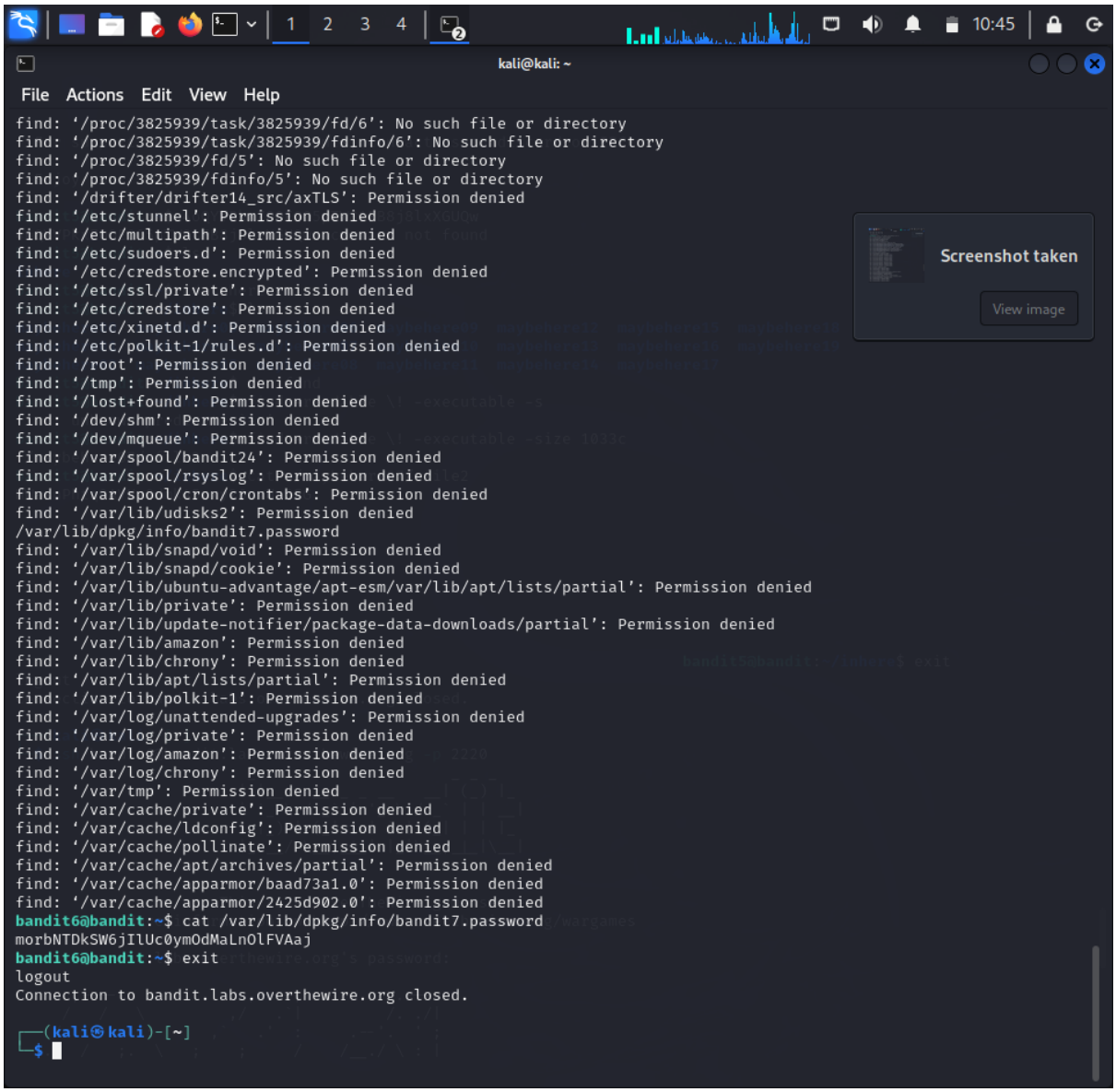


Log into the Bandit6 using the password. Use the root directory command to search the system.

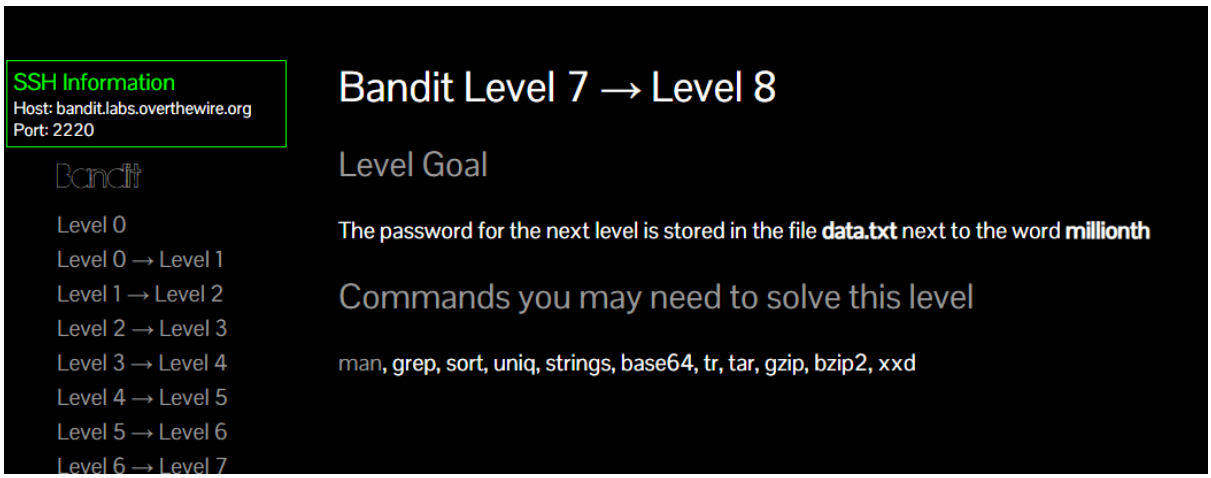
Type this command “cat /var/lib/dpkg/info/bandit7.password” and find the password.



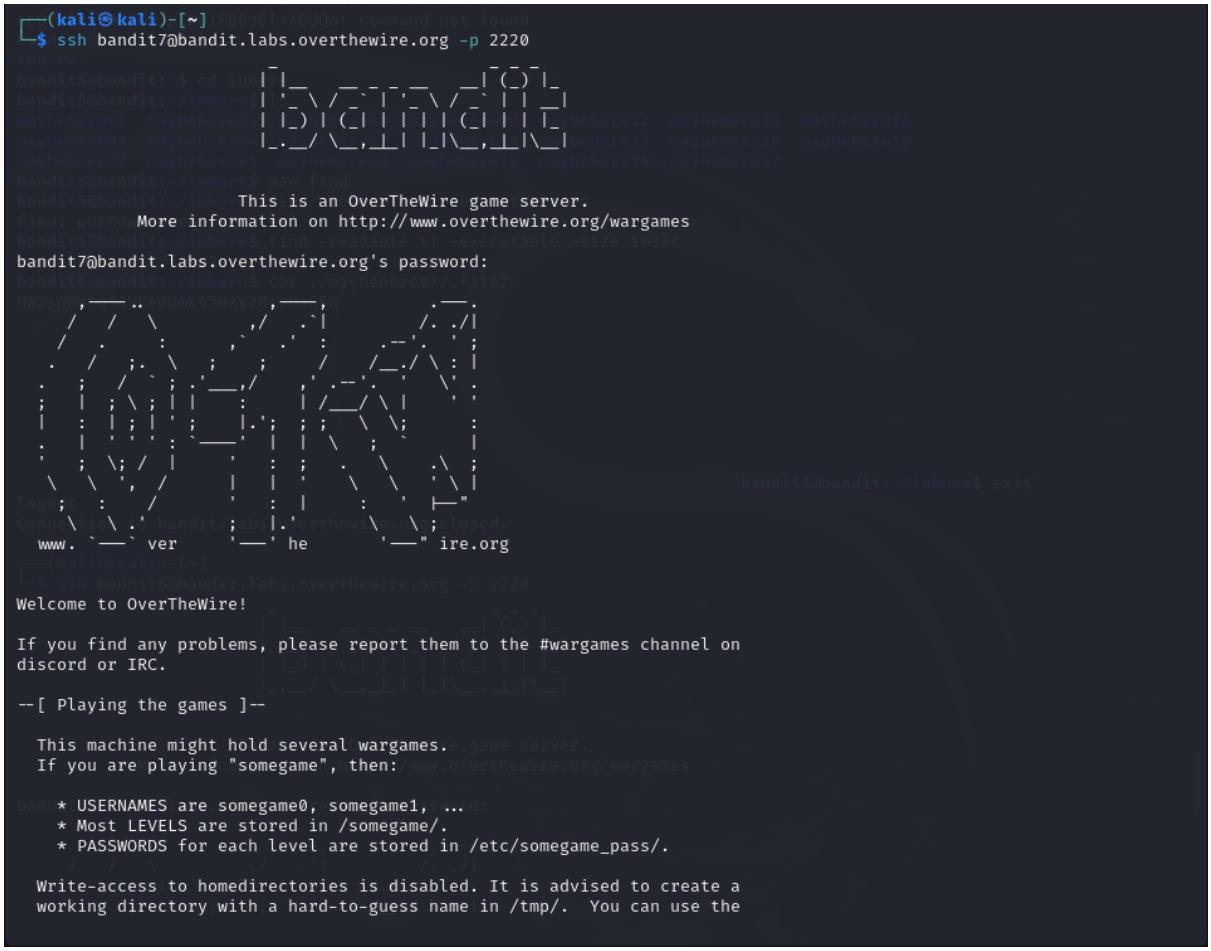
Log out using the “exit” command.



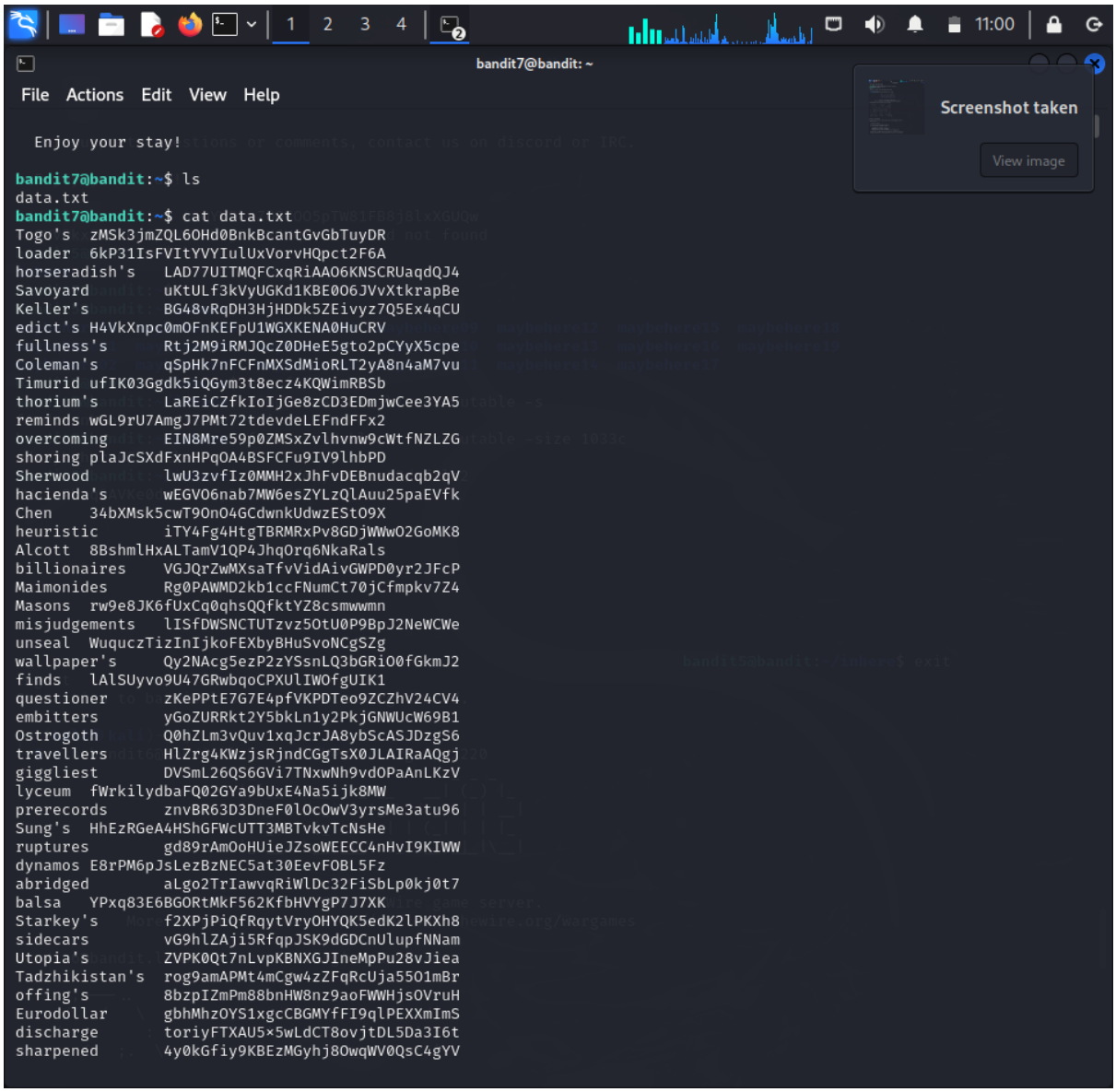
Bandit7 -> Bandit8



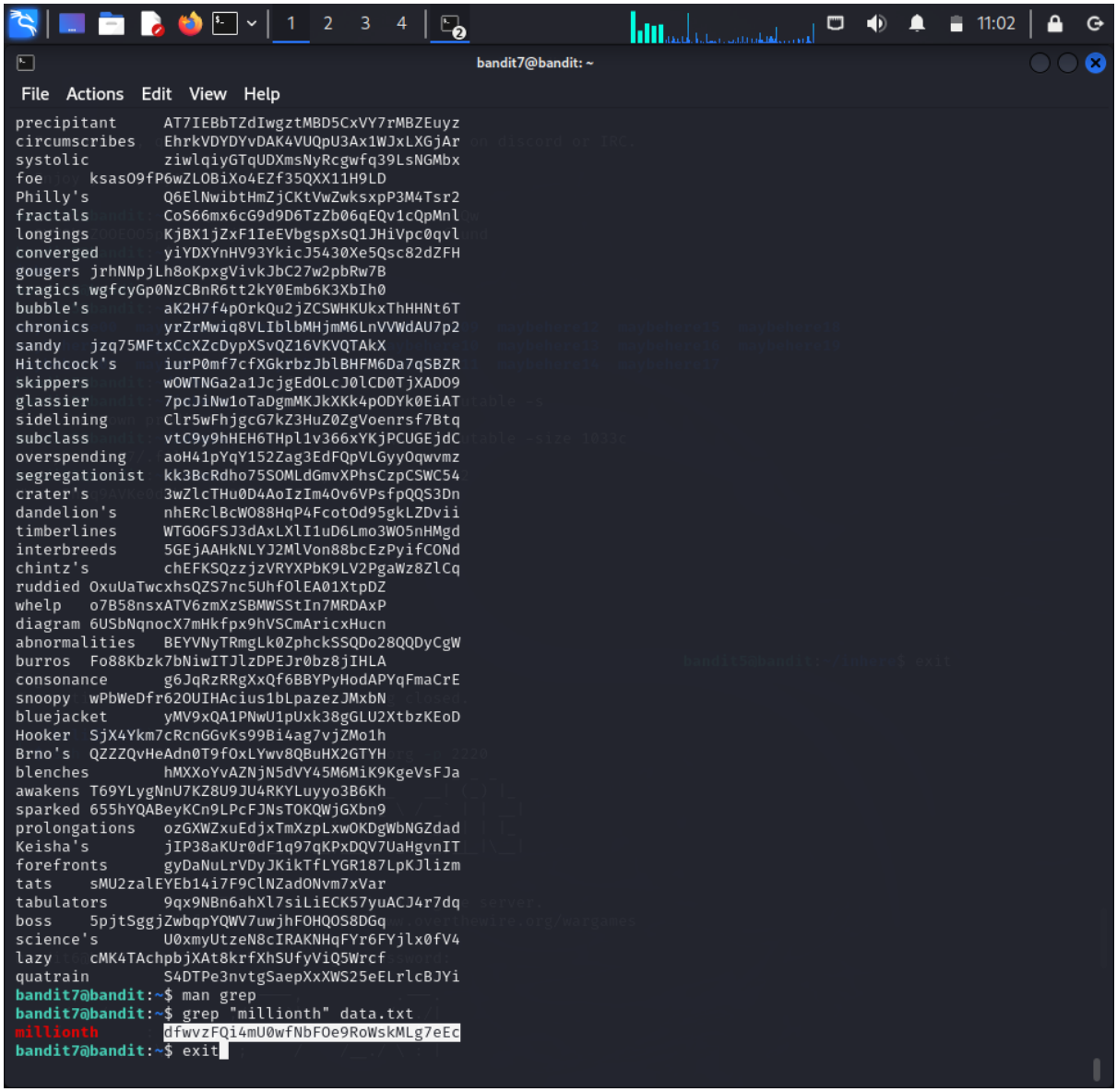
Log into Bandit7 using the password.



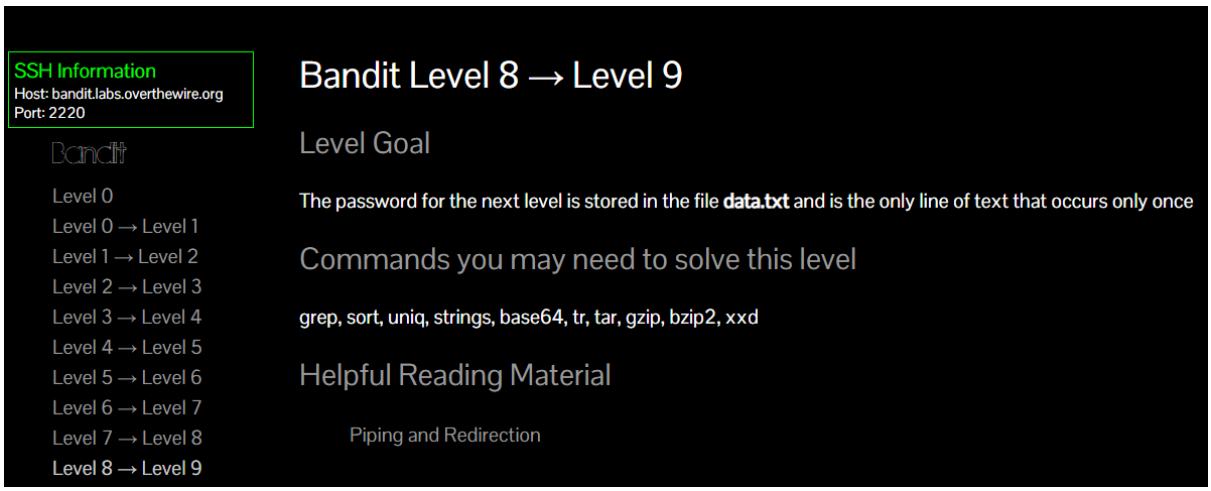
first check the size of the “data.txt” file.



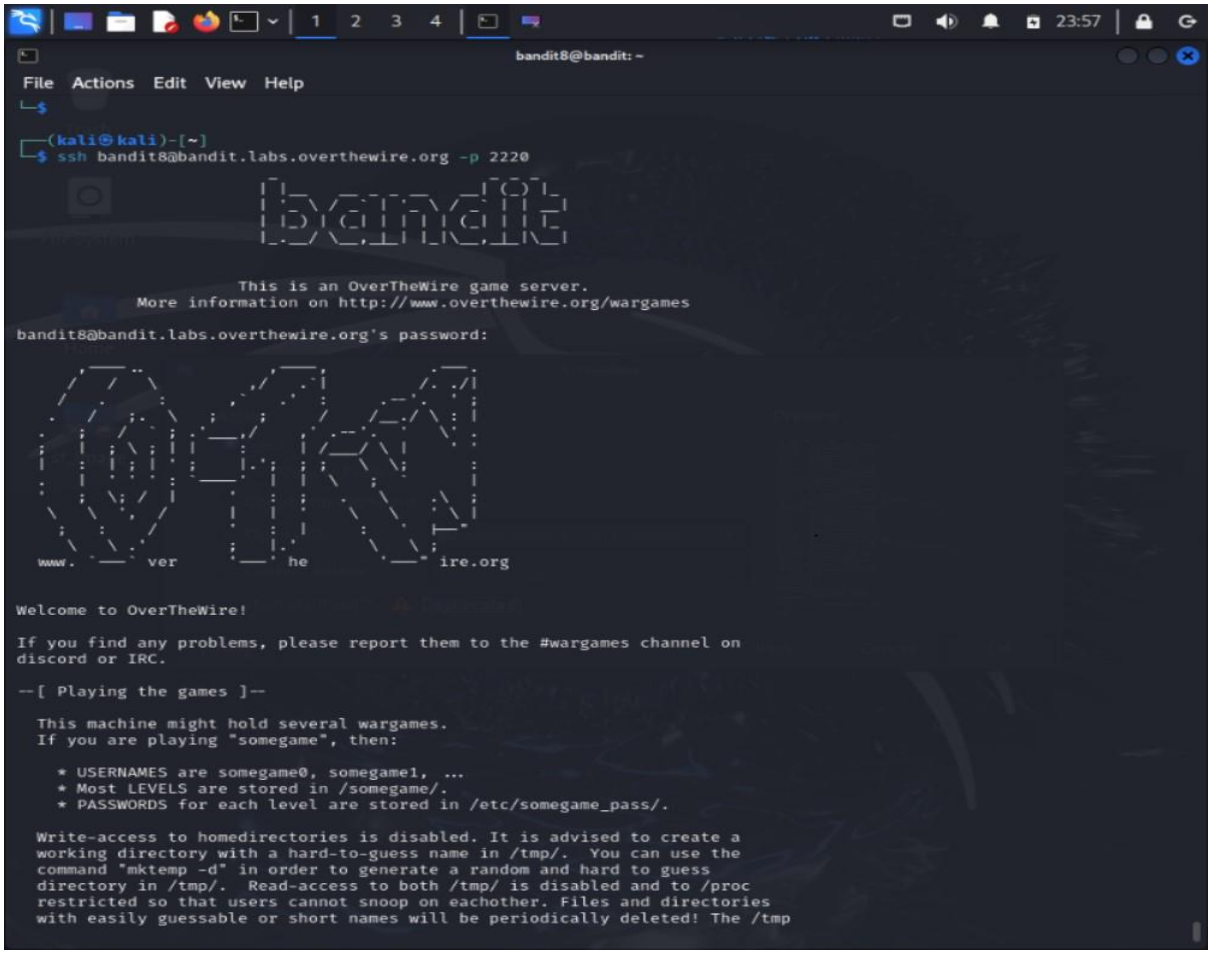
Now we need to use the “grep” command. grep command can be used to search lines that follow a particular pattern. Using the “grep” command and the pipe “|” we can find the password.



Bandit8 -> Bandit9



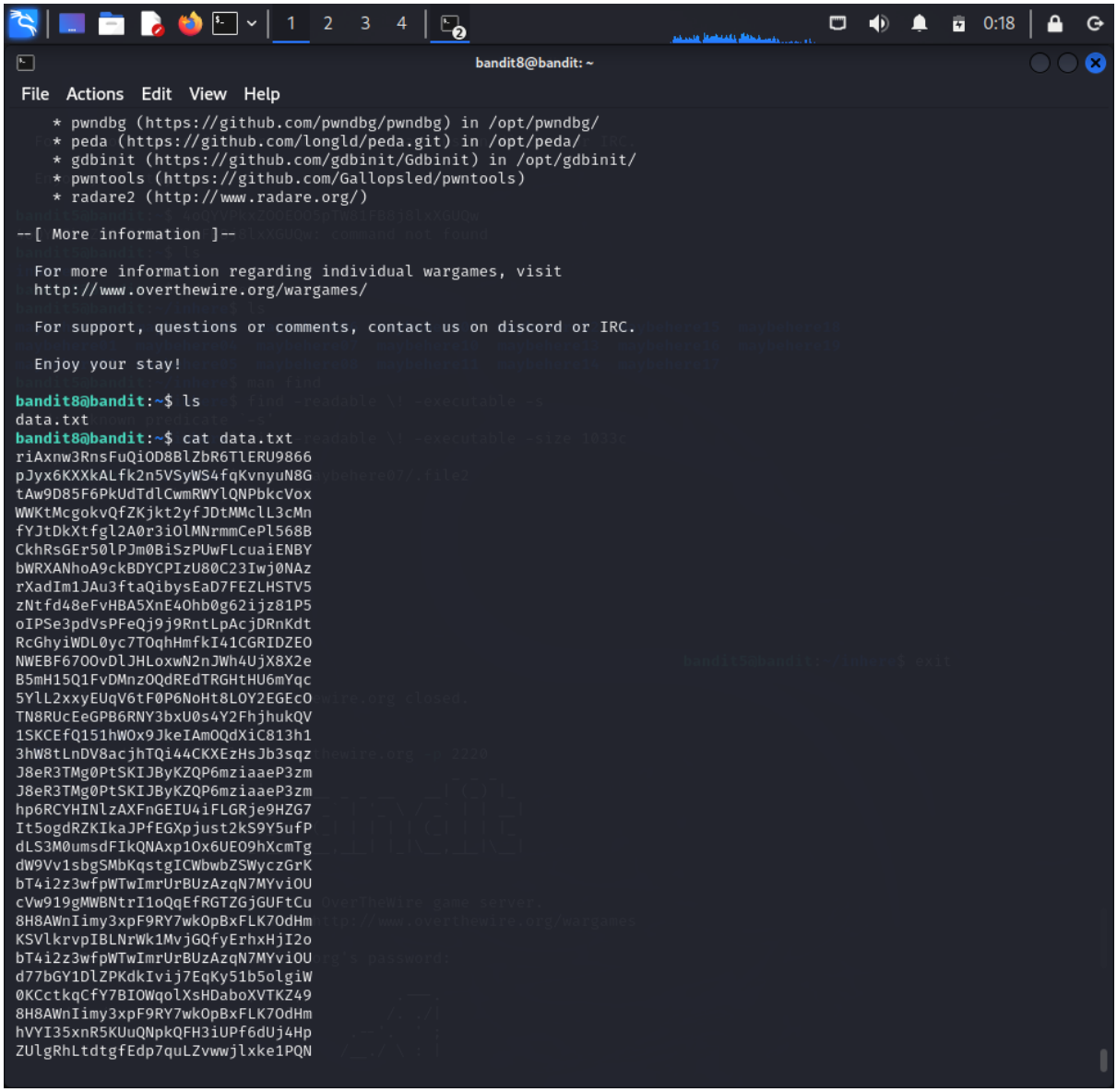
Log into Bandit8 using the password.



Sort – sorts the lines of a text file

Uniq – filters input and writers to the output

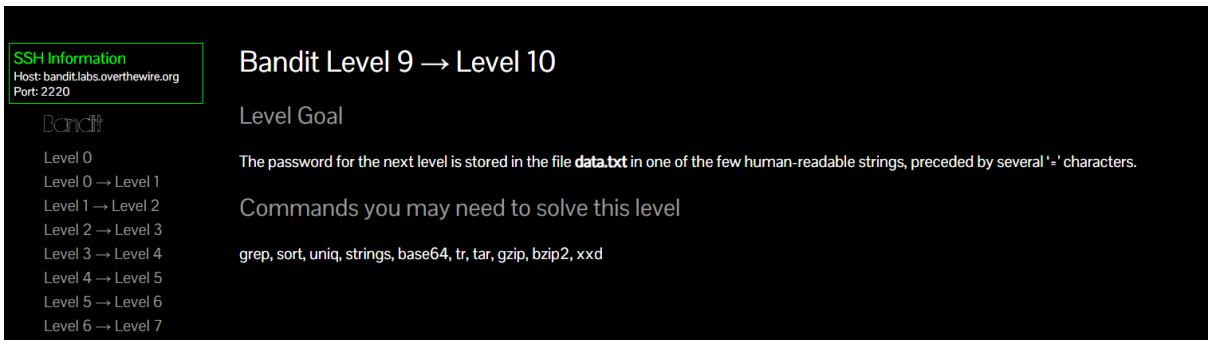
So, using “sort data.txt | uniq -u” we can get the password.



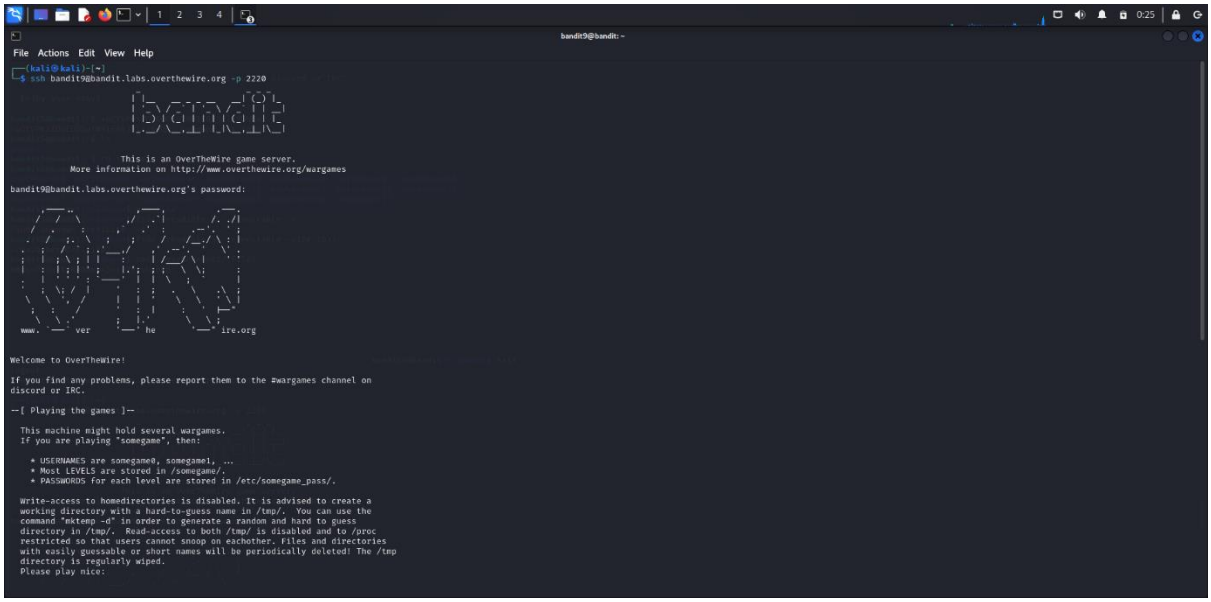
```
KSVlkrvpIBLNrWk1MvjGQfyErhxHjI2o
os7VWoGgtKC0MunbVdmG3P9ZYMPFFYyq
YdTp9FRR5ZxFPtRXHmLb8D3yMIs24jEc
9fTezZmzh16K7OLBunAd3k0Mor9RIsDv
bandit8@bandit:~$ man sort
bandit8@bandit:~$ man uniq
bandit8@bandit:~$ cat data.txt | sort | uniq
0KCctkqCfY7BIOWqolXsHDaboXVTKZ49
1SKCEfQ151hWOx9JkeIAmOQdXiC813h1
3hHLofjM7m3sdyiKJF5QsMqvEIfFh5b1
3hW8tLnDV8acjhTQi44CKXEzHsJb3sqz
3nUXvAjKo7yu6fYykYu7nGGKDMuNMWZf
42qjuz5hdLlItNwdJYsDRpkbbvoEYiWK
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
5g2sV4OokwqDv29Pfo6C7twjKcOk4WQV
5YlL2xxyEUqV6tF0P6NoHt8LOY2EGEcO
6lMDNhQjlOoCOZ5F8ULK2g0uT0rCdnoQ
6z7GGjobj2JASCjNYtOoavrTPCA1GVLc
7f32a50fHRuHaW6lD7l5swMZjK5dKH0t
```

```
bandit8@bandit:~$ cat data.txt | sort | uniq -c
     10 0KCctkqCfY7BIOWqolXsHDaboXVTKZ49
     10 1SKCEfQ151hWOx9JkeIAmOQdXiC813h1
     10 3hHLofjM7m3sdyiKJF5QsMqvEIfFh5b1
     10 3hW8tLnDV8acjhTQi44CKXEzHsJb3sqz
     10 3nUXvAjKo7yu6fYykYu7nGGKDMuNMWZf
     10 42qjuz5hdLlItNwdJYsDRpkbbvoEYiWK
      1 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
     10 5g2sV4OokwqDv29Pfo6C7twjKcOk4WQV
     10 5YlL2xxyEUqV6tF0P6NoHt8LOY2EGEcO
     10 6lMDNhQjlOoCOZ5F8ULK2g0uT0rCdnoQ
     10 6z7GGjobj2JASCjNYtOoavrTPCA1GVLc
     10 7f32a50fHRuHaW6lD7l5swMZjK5dKH0t
     10 8H8AWnIimy3xpF9RY7wkOpBxFLK7OdHm
     10 9fTezZmzh16K7OLBunAd3k0Mor9RIsDv
     10 AiNdScFDXFSBnLNzveDQHAENckqrrJsk
     10 B5mH15Q1FvDMnzOQdREdTRGHtHU6mYqc
     10 BNZFkNcXh3nSE1dEqqBYZKiDAsJj7W4K
     10 bsiO0×cFo9wdE7NAbAd12ZikwMzHfmZa
     10 bT4i2z3wfpWTwImrUrBUzAzqN7MYviOU
     10 BTuibb63I0yqDgkVyVbu0X8Ma5j4f2ki
     10 bWRXANhoA9ckBDYCPIzU80C23Iwj0NAz
     10 bziGsgFgtBJS2eEiYqWztHPs4ysYaBeP
     10 CJDmZTjXG6TosJ6YFPQ3BhefqBOzzPCq
     10 cJDU7Zp88KXORADTXYgR6sQOKceHRxYn
```

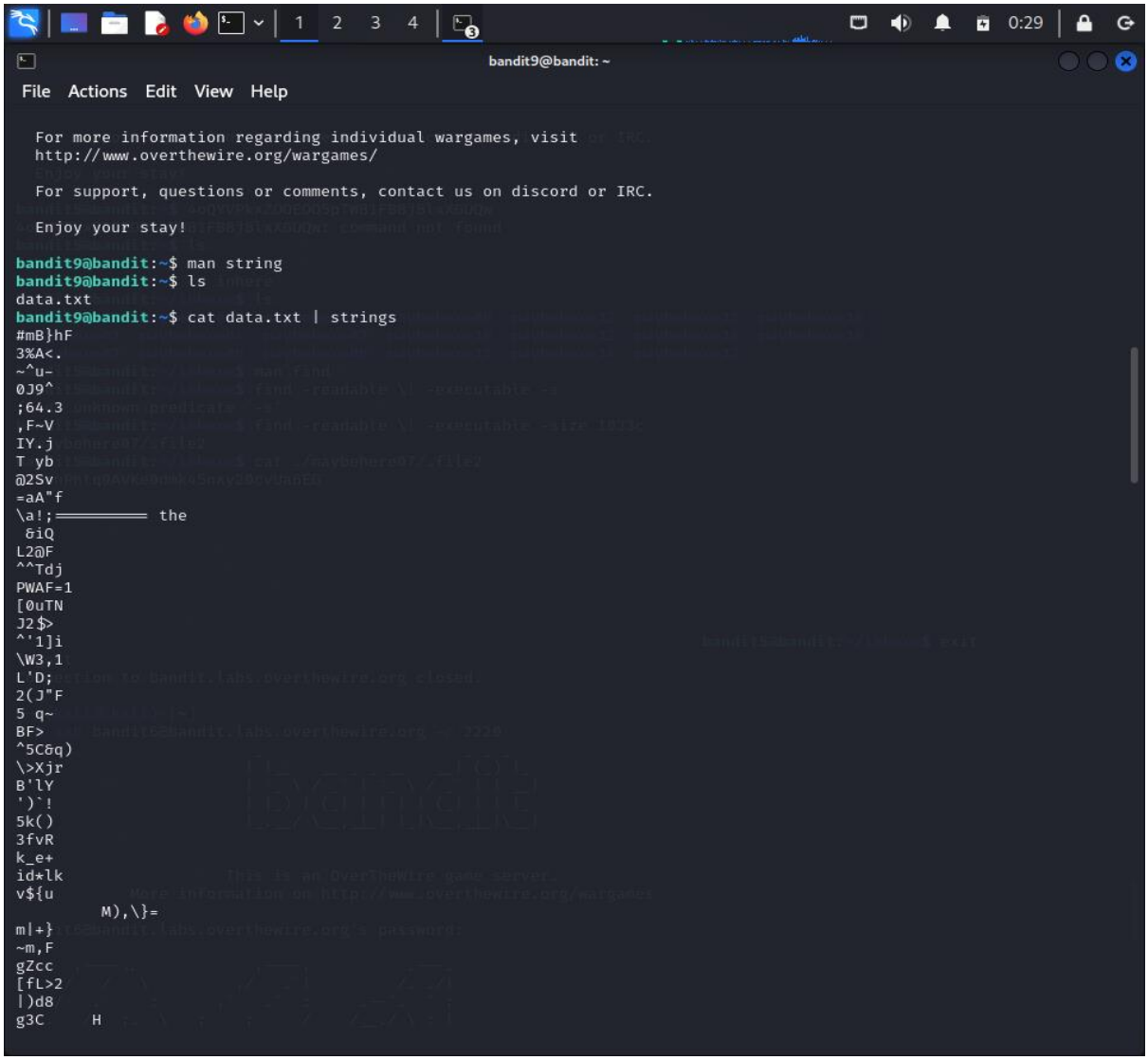
Bandit9 -> Bandit10



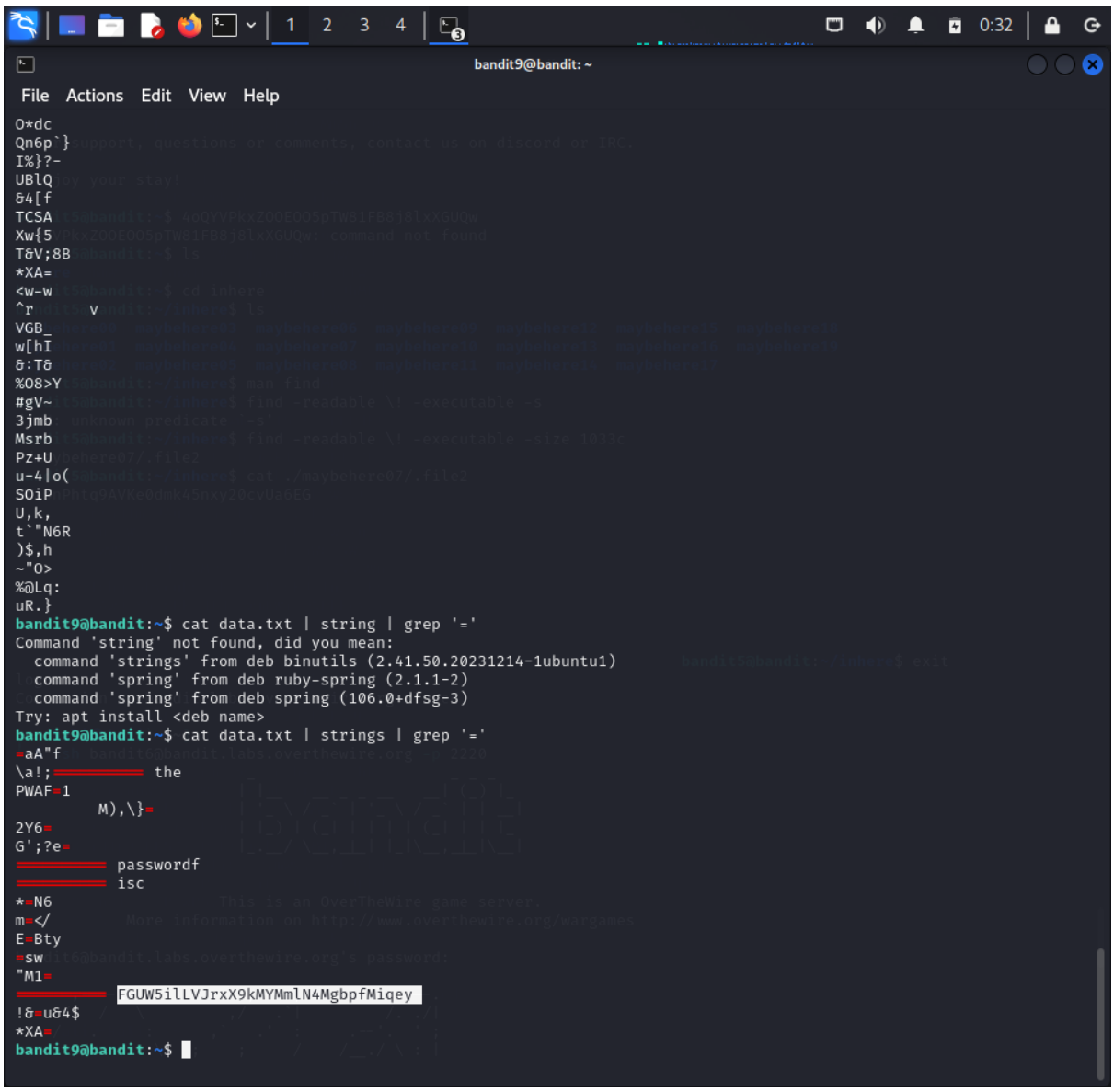
Log into Bandit8 using the password.



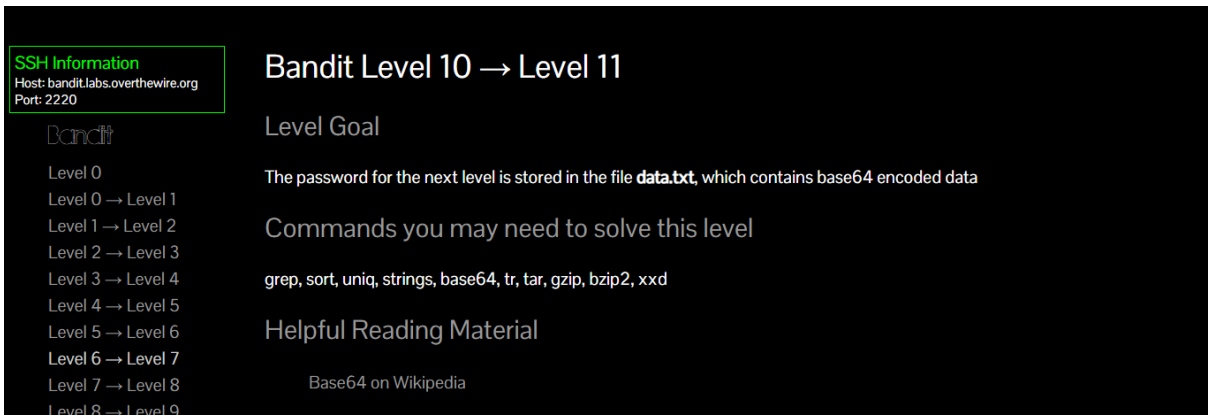
Using the “ls” command find the “data.txt” file.



We need to use the “string” command to separate human-readable strings in “data.txt”. And use “grep” within the equal sign “=”.

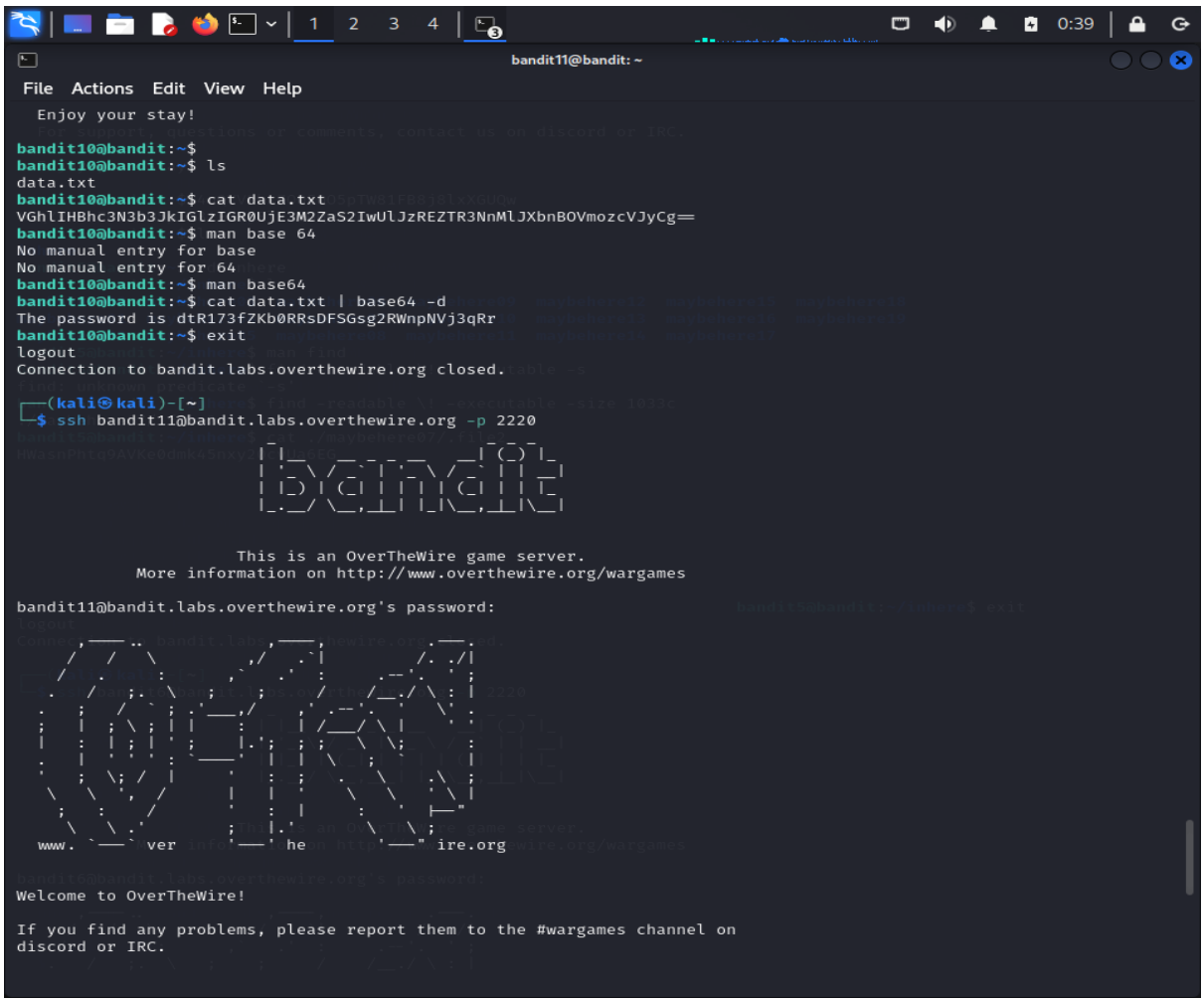


Bandit10 -> Bandit11

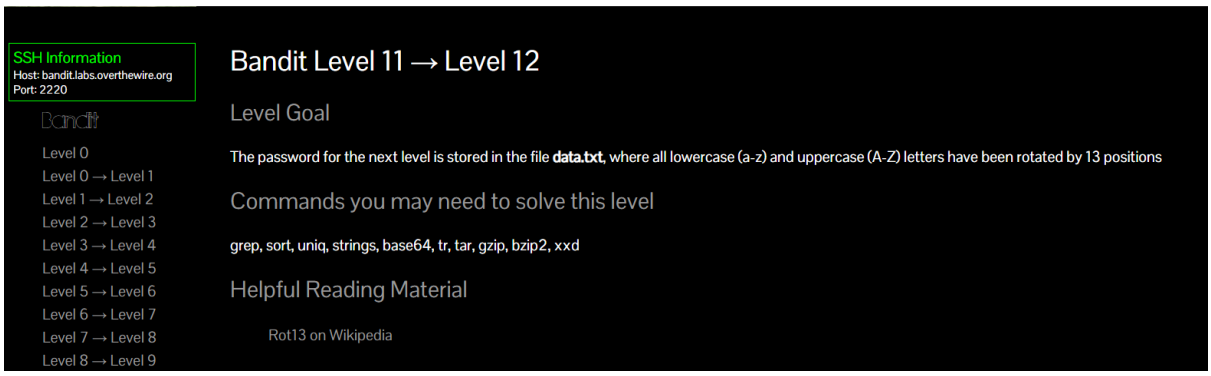


First, log into Bandit10. Run the “cat” command with the file name.

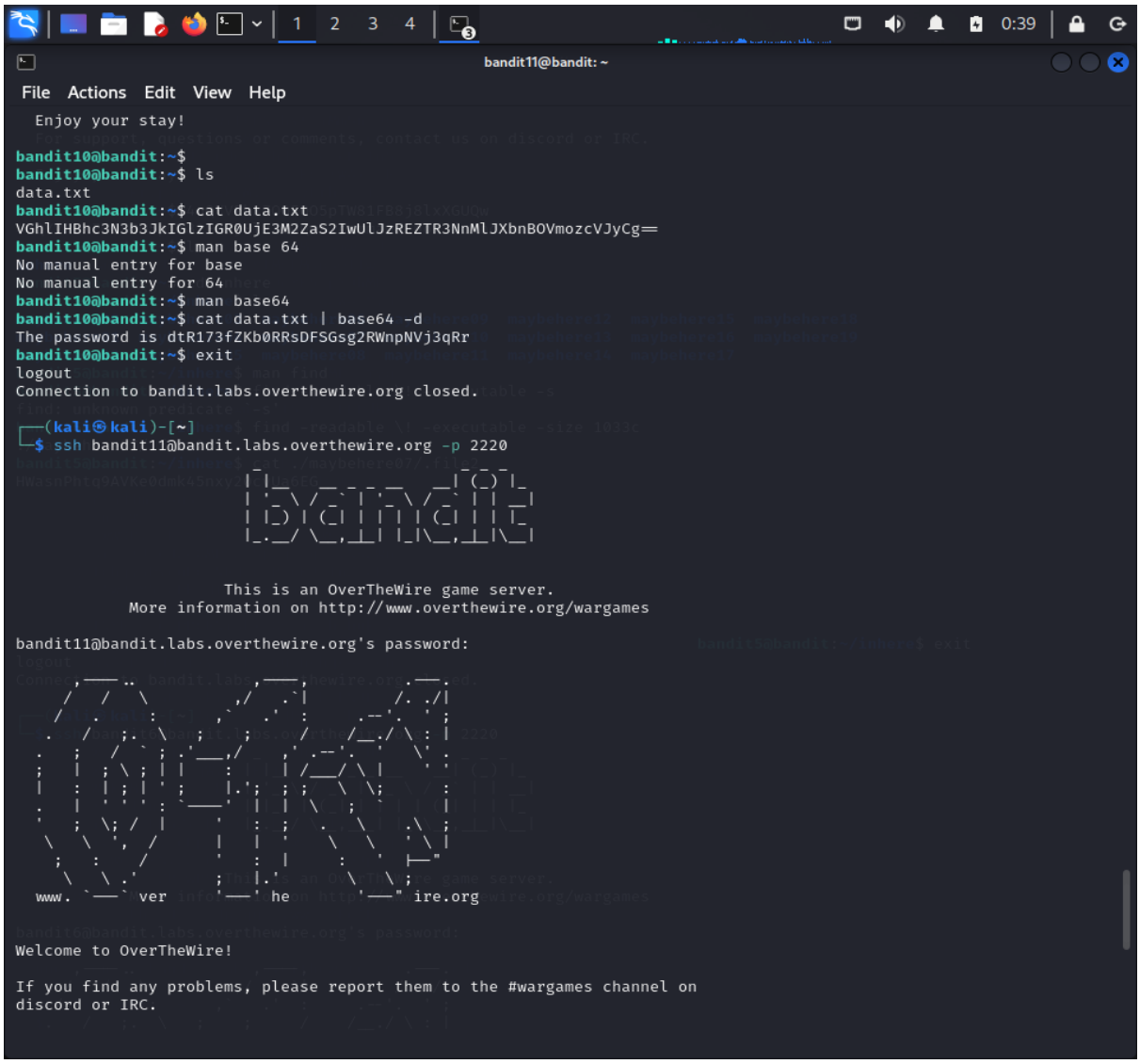
Use the “base64 -d data.txt” command for decoding to the password.



Bandit11 -> Bandit12



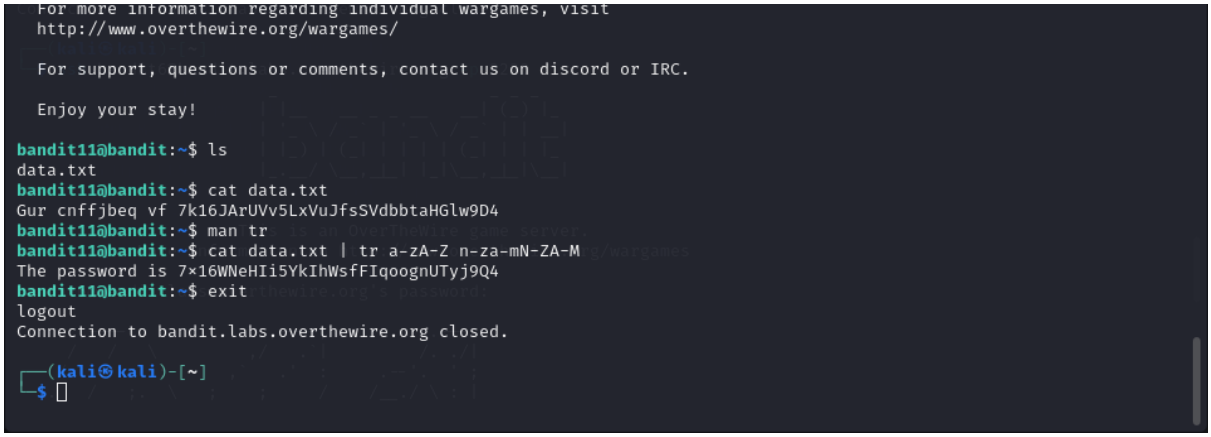
Log into Bandit11 with the password.



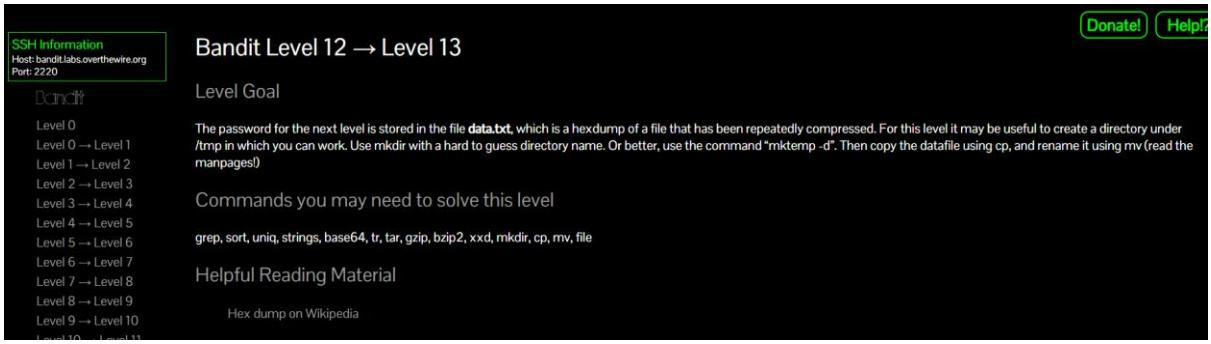
Use the “ls” command.

Use the “cat” command to get the password.

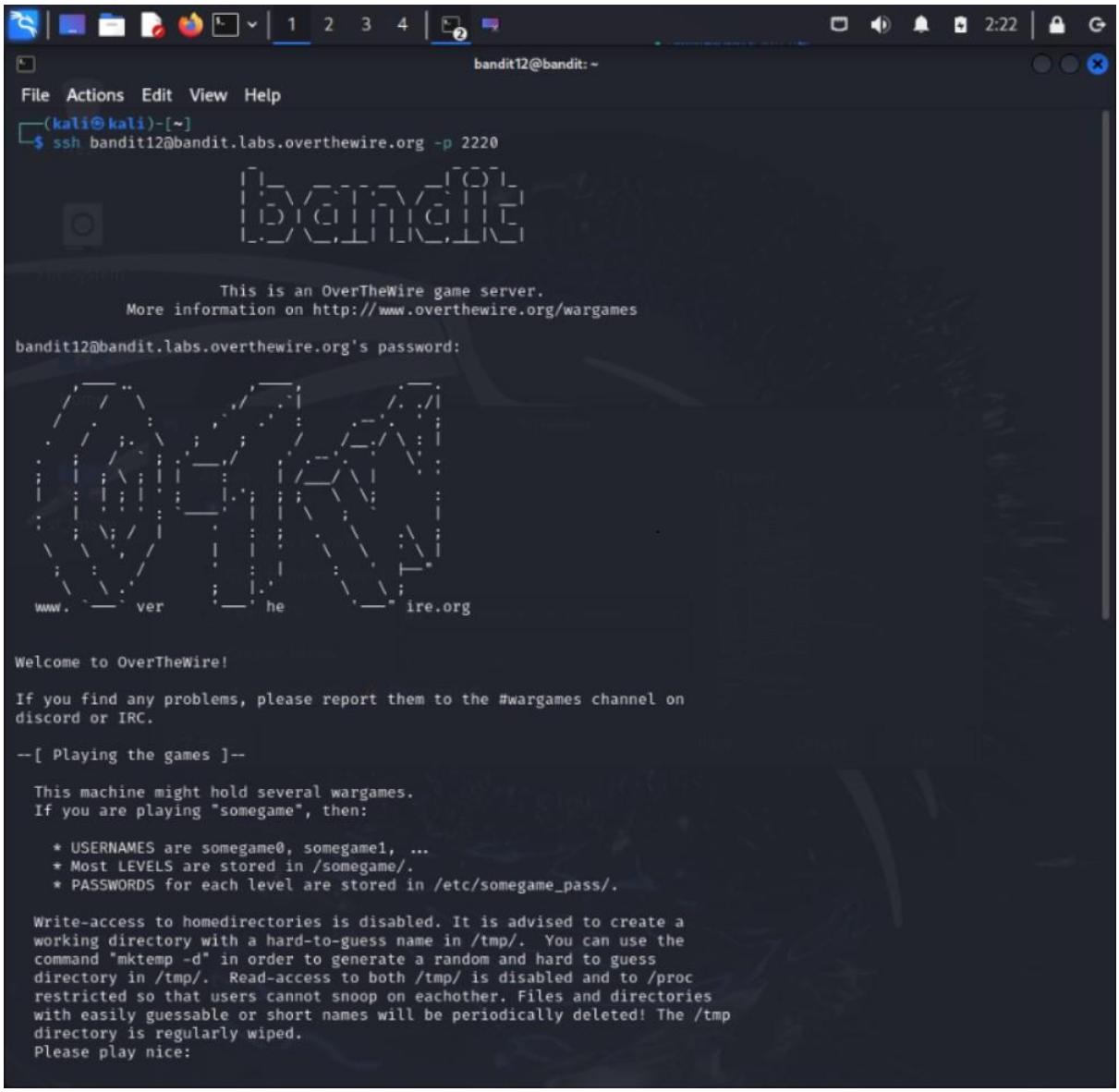
Now use the “tr” command for translation, allowing replacing the characters with others. And “A ->N, ..., Z ->M” to get the password.



Bandit12 -> Bandit13

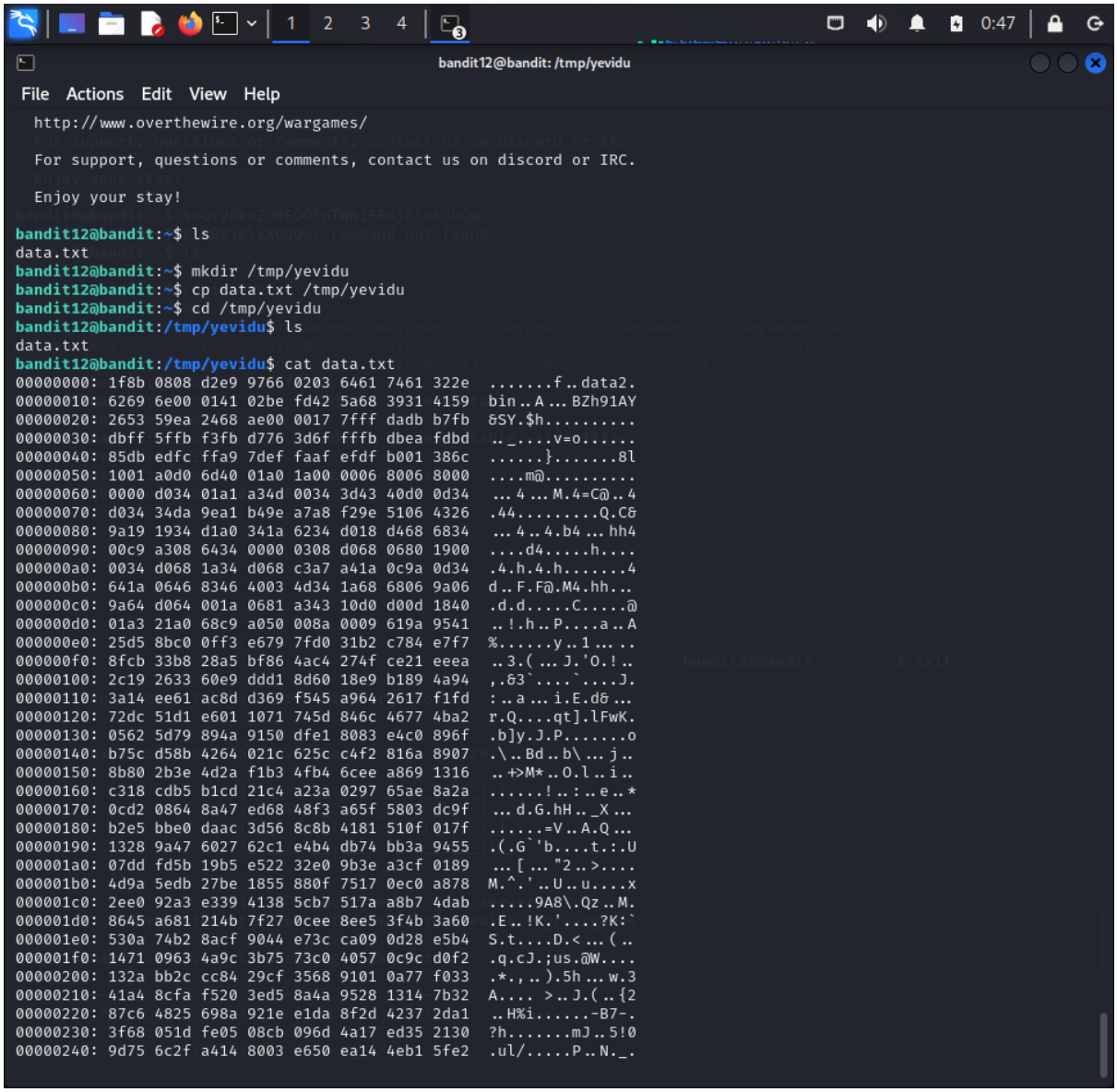


Log into Bandit12 using the password.



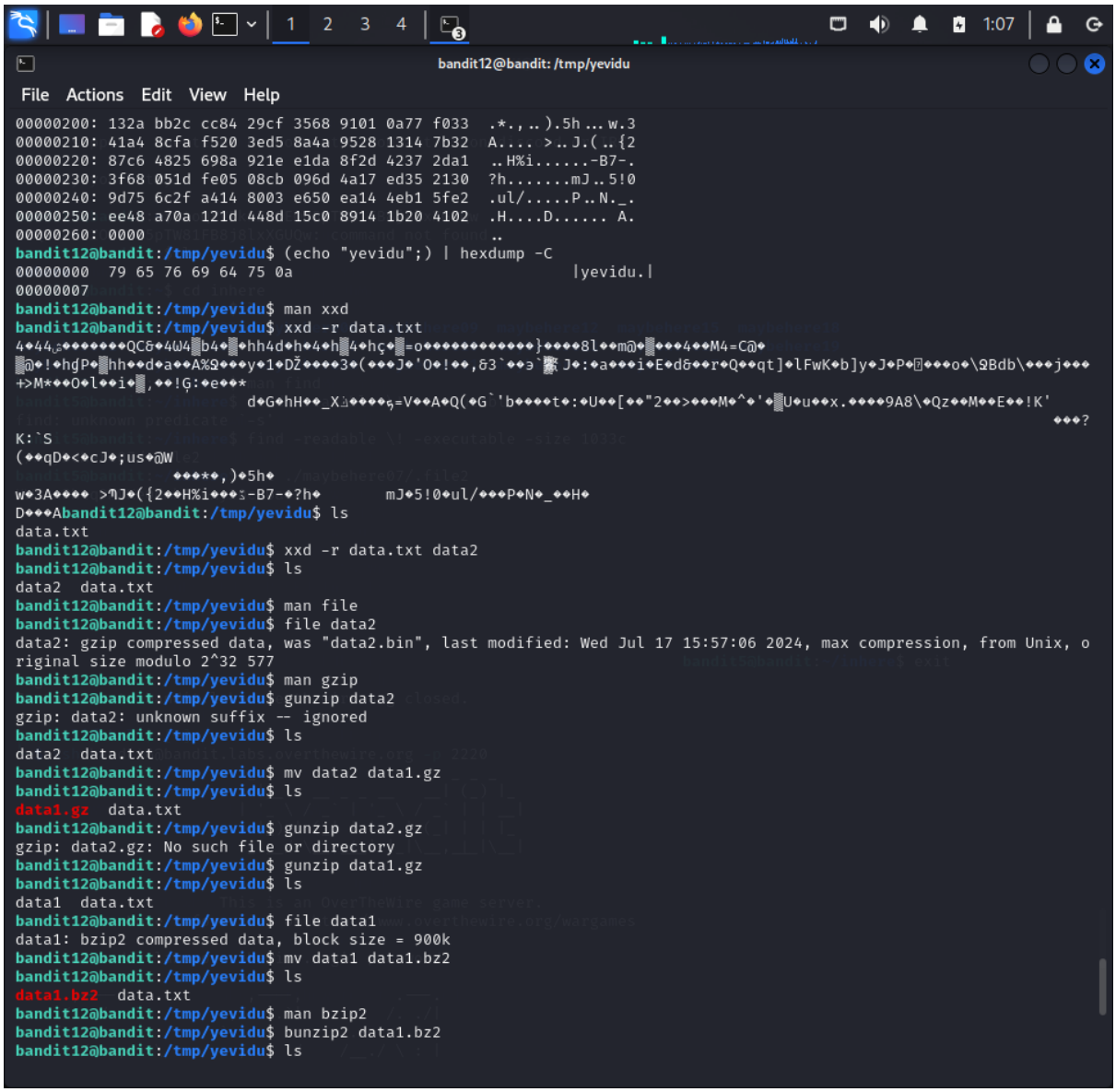
Type “ls” and find the list. Use the “data.txt” and find the file to know what the password is.

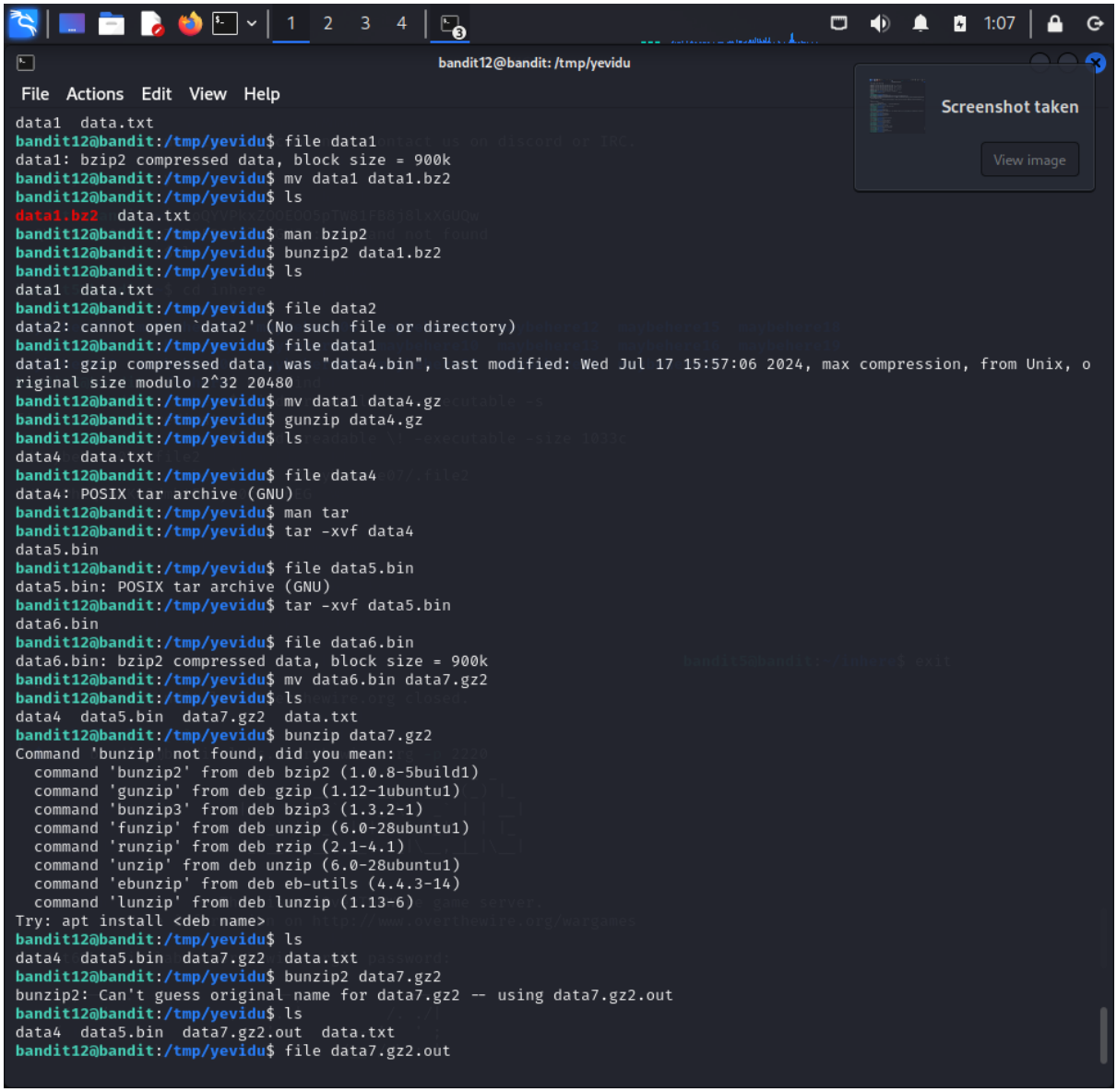
Run the “cat data.txt”.



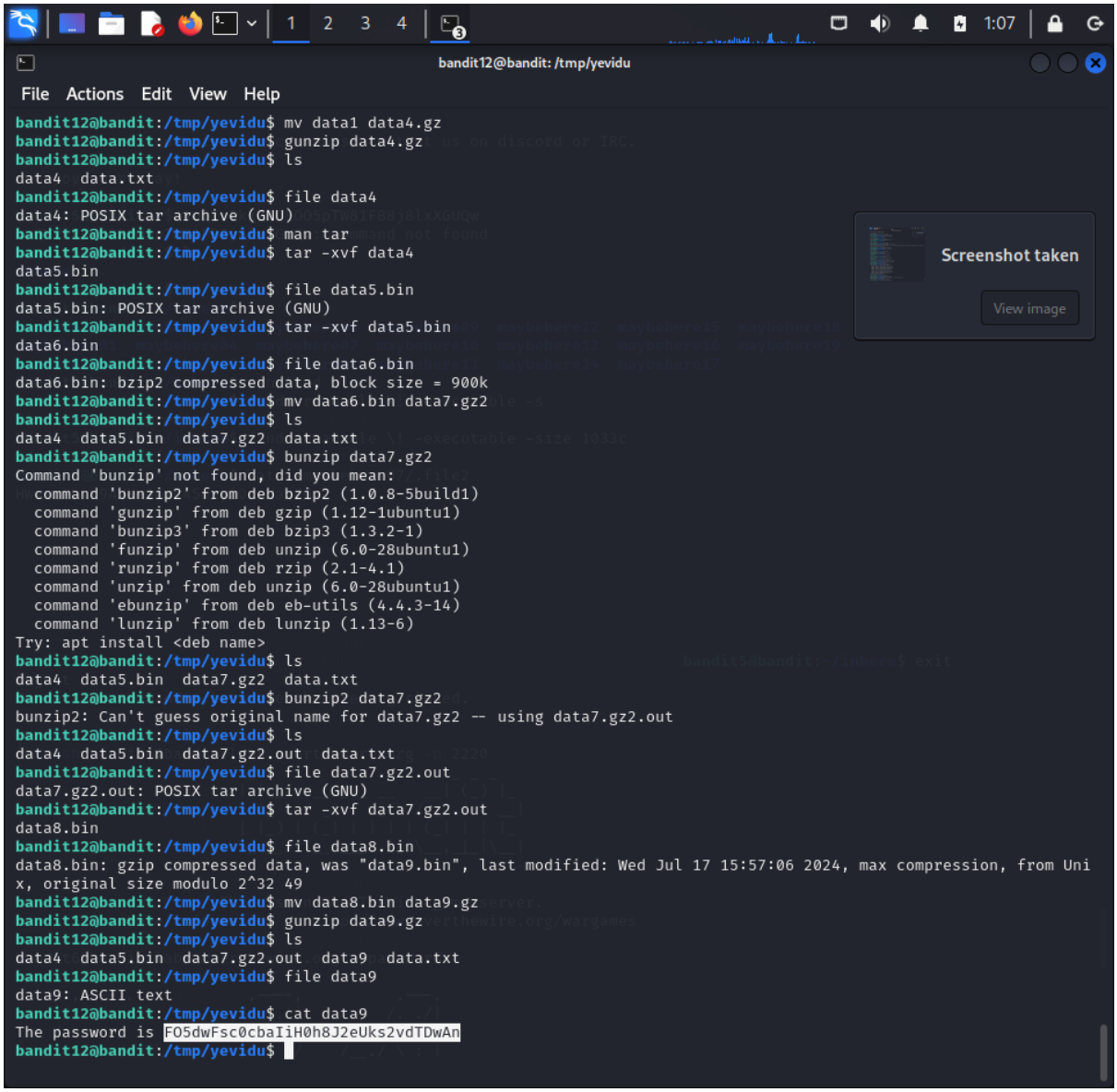
Run “xxd -r data.txt >data1.bin” and next run the “ls” to find all the files.

A command called “zcat” is included with “gzip” and is used to decompress “gzip” compressed files. Using the file command on myfile2, we can find bzip2 compressed data. Use that command to all 9 files and use the “tar” for archiving files and options. Finally, we can find the password.



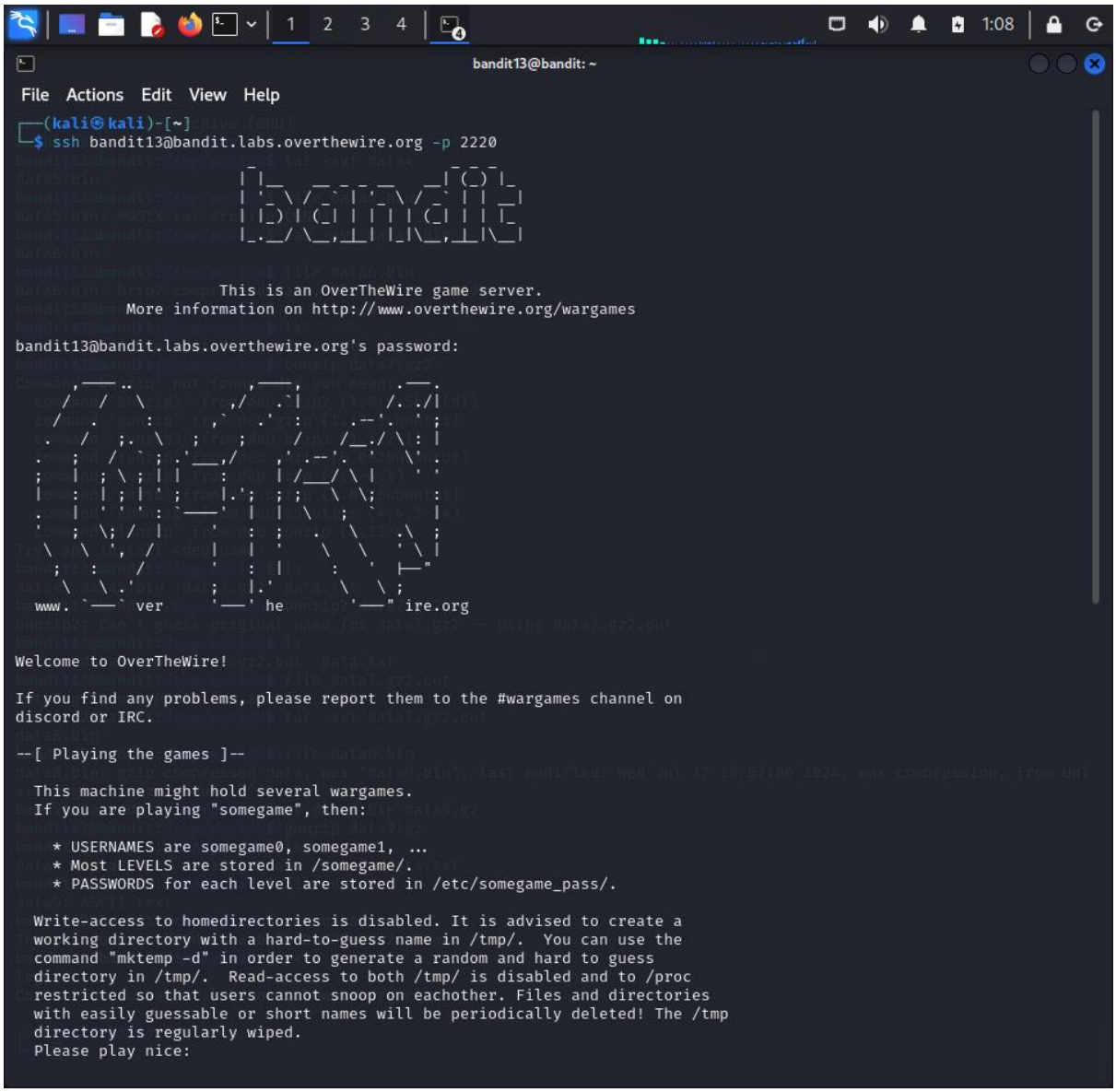



```
data1  data.txt
bandit12@bandit:/tmp/yevidu$ file data1
data1: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/yevidu$ mv data1 data1.bz2
bandit12@bandit:/tmp/yevidu$ ls
data1.bz2  data.txt
bandit12@bandit:/tmp/yevidu$ man bzip2
bandit12@bandit:/tmp/yevidu$ bunzip2 data1.bz2
bandit12@bandit:/tmp/yevidu$ ls
data1  data.txt
bandit12@bandit:/tmp/yevidu$ file data2
data2: cannot open `data2' (No such file or directory)
bandit12@bandit:/tmp/yevidu$ file data1
data1: gzip compressed data, was "data4.bin", last modified: Wed Jul 17 15:57:06 2024, max compression, from Unix, o
riginal size modulo 2^32 20480
bandit12@bandit:/tmp/yevidu$ mv data1 data4.gz
bandit12@bandit:/tmp/yevidu$ gunzip data4.gz
bandit12@bandit:/tmp/yevidu$ ls
data4  data.txt
bandit12@bandit:/tmp/yevidu$ file data4
data4: POSIX tar archive (GNU)
bandit12@bandit:/tmp/yevidu$ man tar
bandit12@bandit:/tmp/yevidu$ tar -xvf data4
data5.bin
bandit12@bandit:/tmp/yevidu$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/yevidu$ tar -xvf data5.bin
data6.bin
bandit12@bandit:/tmp/yevidu$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/yevidu$ mv data6.bin data7.gz2
bandit12@bandit:/tmp/yevidu$ ls
data4  data5.bin  data7.gz2  data.txt
bandit12@bandit:/tmp/yevidu$ bunzip data7.gz2
Command 'bunzip' not found, did you mean:
  command 'bunzip2' from deb bzip2 (1.0.8-5build1)
  command 'gunzip' from deb gzip (1.12-1ubuntu1)
  command 'bunzip3' from deb bzip3 (1.3.2-1)
  command 'funzip' from deb unzip (6.0-28ubuntu1)
  command 'runzip' from deb rzip (2.1-4.1)
  command 'unzip' from deb unzip (6.0-28ubuntu1)
  command 'ebunzip' from deb eb-utils (4.4.3-14)
  command 'lunzip' from deb lunzip (1.13-6)
Try: apt install <deb name>
bandit12@bandit:/tmp/yevidu$ ls
data4  data5.bin  data7.gz2  data.txt
bandit12@bandit:/tmp/yevidu$ bunzip2 data7.gz2
bunzip2: Can't guess original name for data7.gz2 -- using data7.gz2.out
bandit12@bandit:/tmp/yevidu$ ls
data4  data5.bin  data7.gz2.out  data.txt
bandit12@bandit:/tmp/yevidu$ file data7.gz2.out
```



Bandit 13 -> Bandit14

Log into Bandit13 using the password.



Use the “ls” command to find the file.

For remote machine access and command execution, use the “ssh” command.

The “sshkey. private” file and the option “-i” are used to choose the identified file for RSA or DSA authentication.