BANDIT OVERTHEWIRE

REDTEAM HACKING ACADEMY
CERTIFIED IT INFRASTRUCTURE AND CYBER SOC ANALYST

Submitted by
Manikandan.M

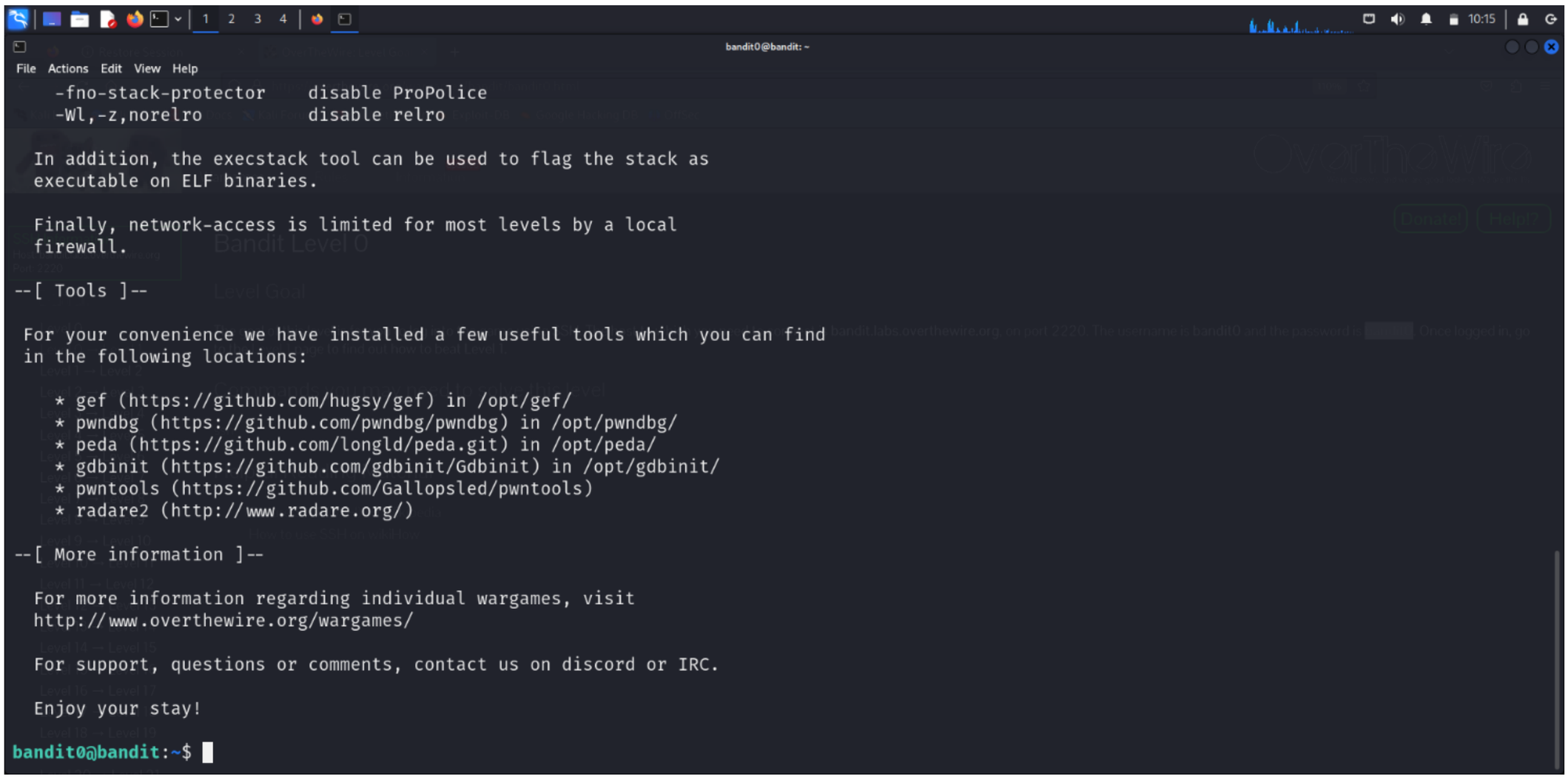
OverTheWire

BANDIT

LEVEL 0

Goal: SSH Login

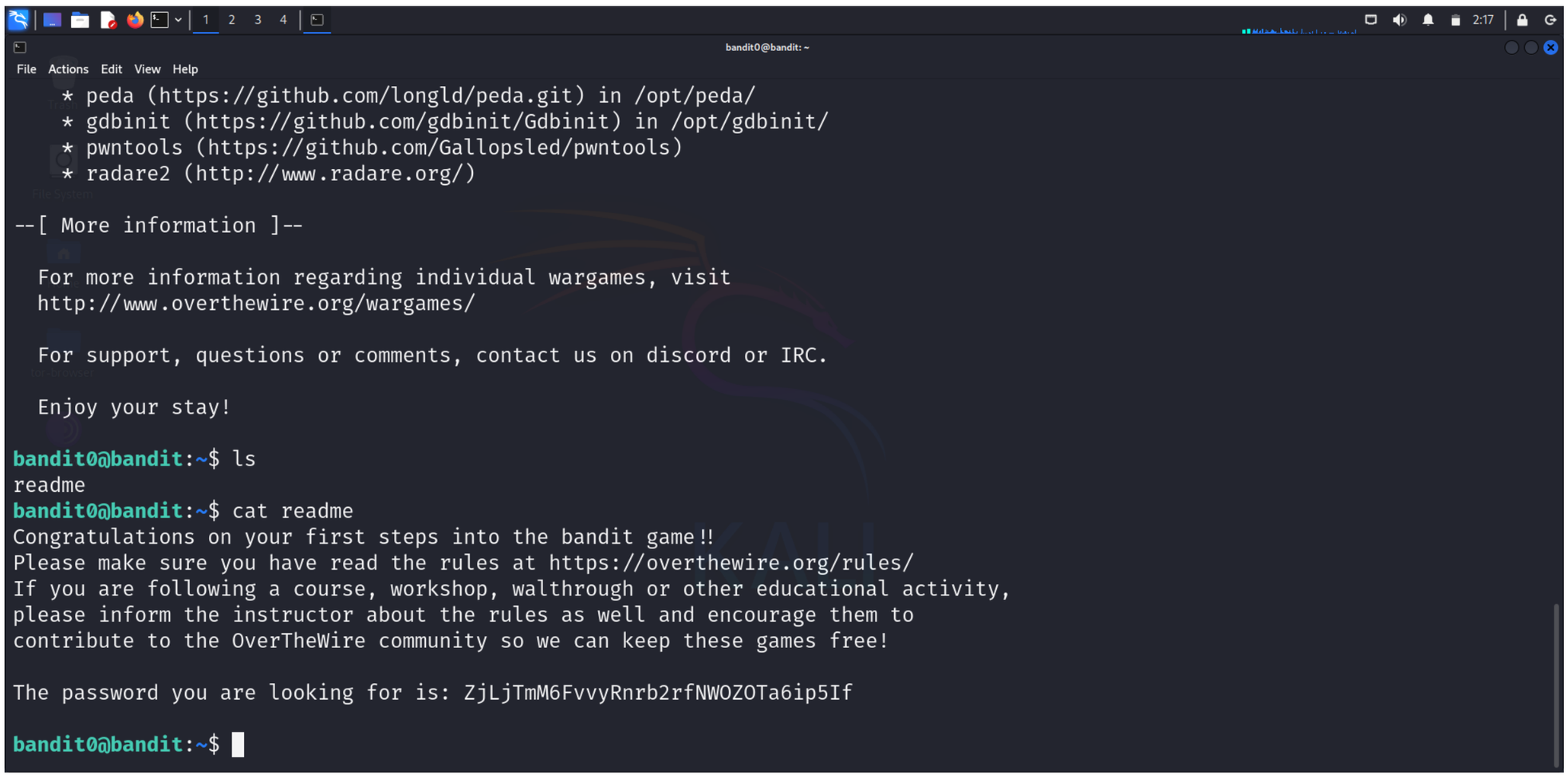
- The goal of this level is for you to log into the game using SSH.
- The ssh command provides a secure encrypted connection between two hosts over an insecure network
- The host to which you need to connect is **bandit.labs.overthewire.org**, on port 2220.
- The username is **bandit0** and the password is **bandit0.then the result is,**
- **Command** **ssh bandit0@bandit.labs.overthewire.org -p 2220**



LEVEL 0 → LEVEL 1

Goal: Read a File.

- The password for the next level is stored in a file called **readme** located in the home directory.
- To use the cat command.
- After viewing passwords save it for next level,
- After viewing the password for level 1 need to exit from user bandit0.

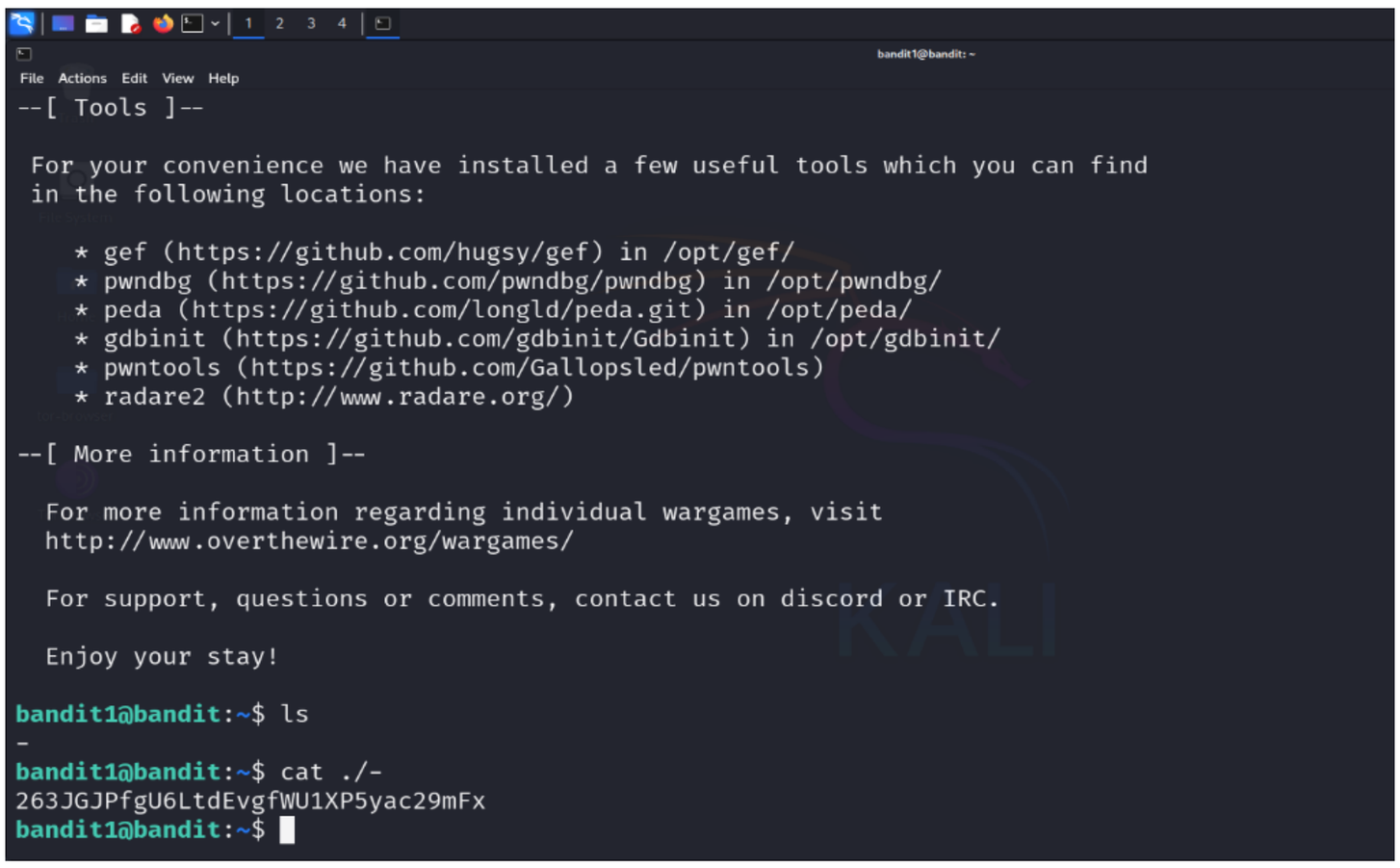


LEVEL 1 → LEVEL 2

Goal: Unusually named Files.

- After finding the password for level 1, we to need change the username as bandit1 with the same host and port to level1.
- Connect with ssh bandit1@bandit.labs.overthewire.org -p 2220.
- The password for the next level is stored in a file called **-** located in the home directory.
- ls (list all the files and directories under a specified directory).

- This type of approach has a lot of misunderstanding because using - as an argument refers to STDIN/STDOUT i.e dev/stdin or dev/stdout .So if you want to open this type of file you have to specify the full location of the file such as ./- .For eg. , if you want to see what is in that file use cat ./-



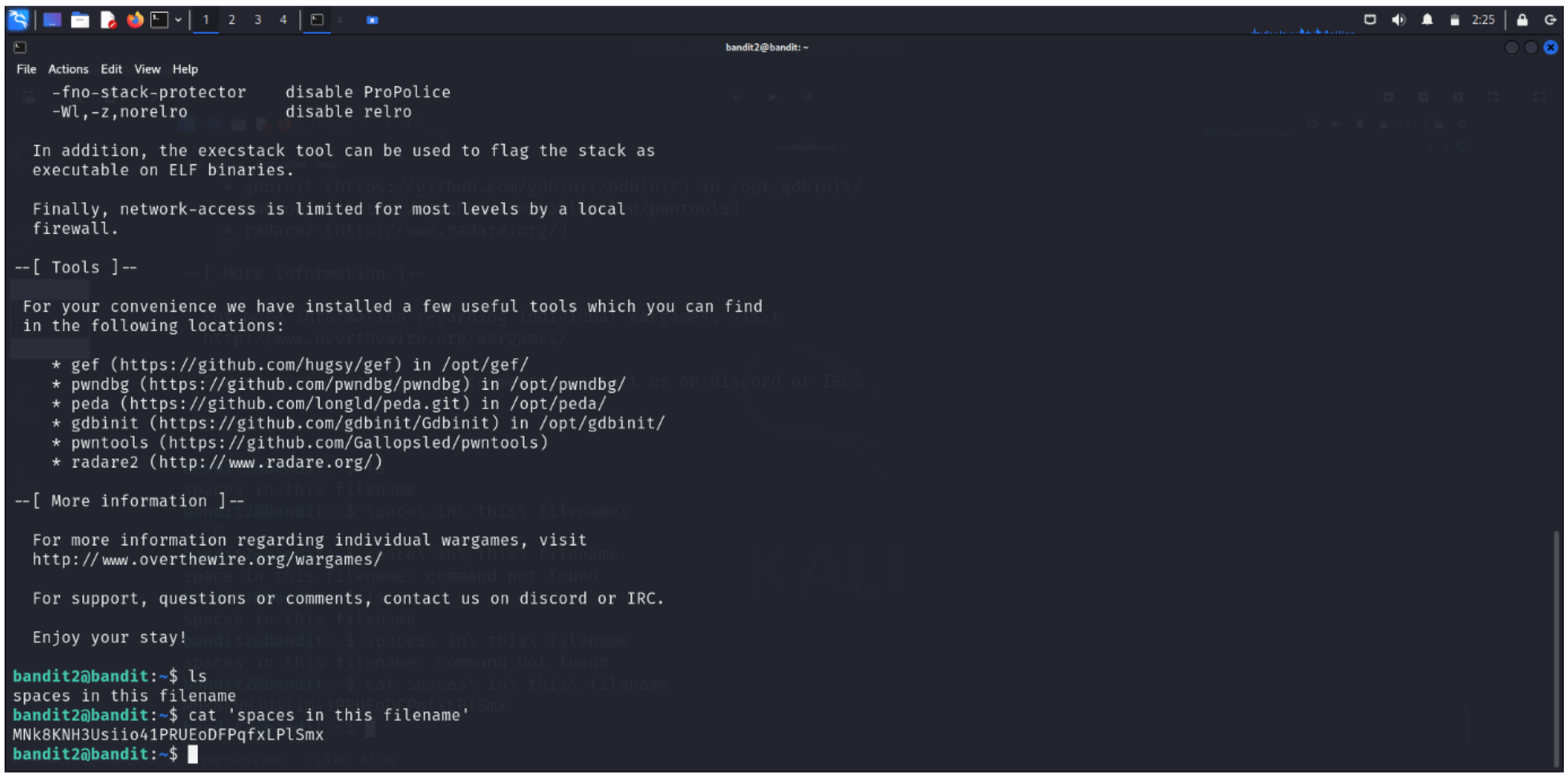
LEVEL 2 → LEVEL 3

Goal: Spaces in a filename.

- After switch the username 2
- After ls(list) you can see the file called space in this filename.
- If we directly use cat command, it won't be able to find the file.
- As the file is named spaces in this filename, we won't be able to read it simply by cat

command. As cat command reads files name only until space as it considers space as null ‘/0’.

- Command cat ‘spaces in this filename’.



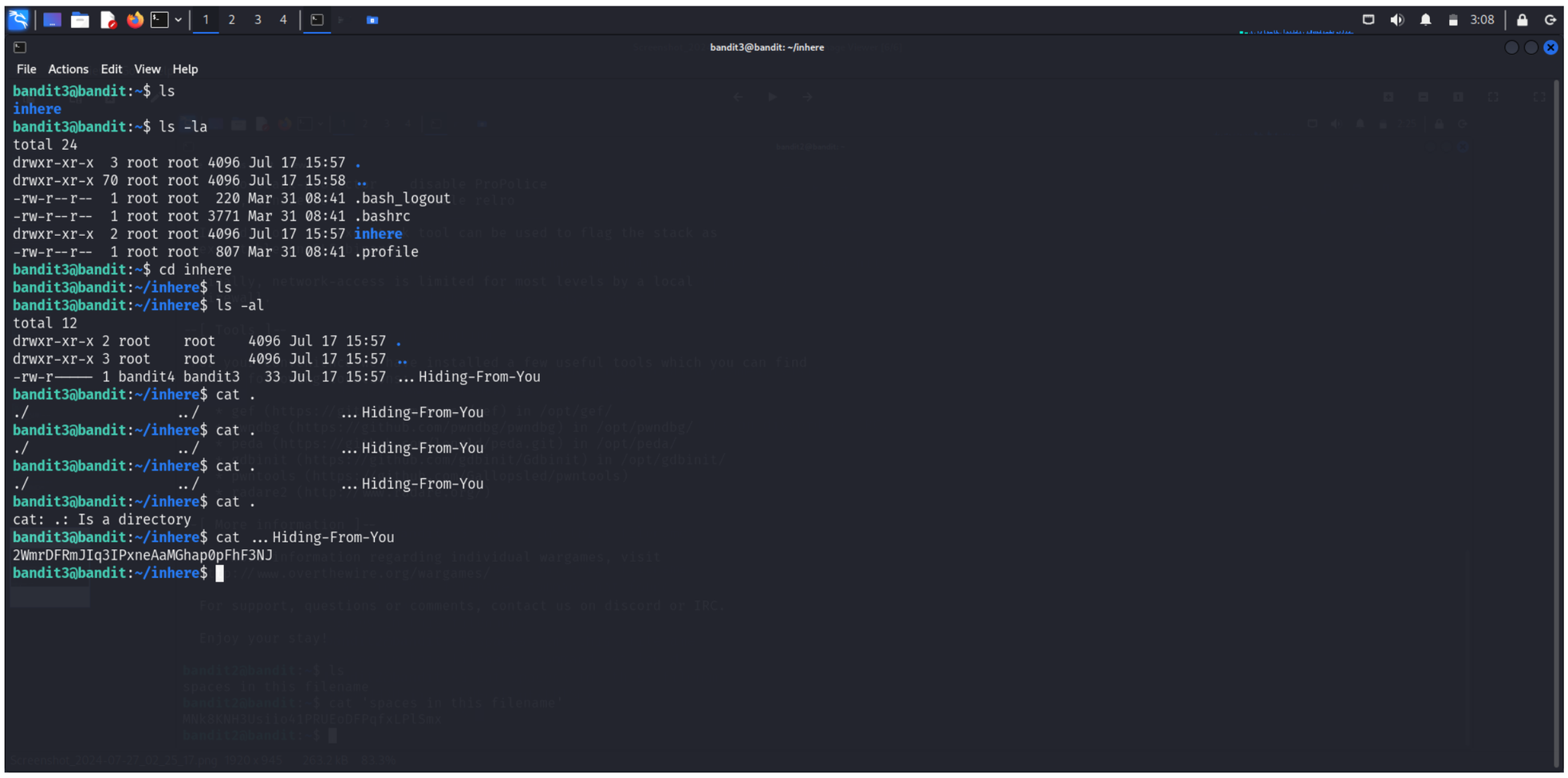
LEVEL 3 → LEVEL 4

Goal: Hidden Files.

- After Finding password for level 3, switch the username.
- The password for the next level is stored in a hidden file in the **inhere** directory
- After ls(list) you can see the directory called inhere

cd to change the directory inhere.

- ls -la (lists the contents and hidden file of your current working directory)
- After ls -la you can see a hidden file called ...hiding-from-you
- You can cat ...hiding-from-you

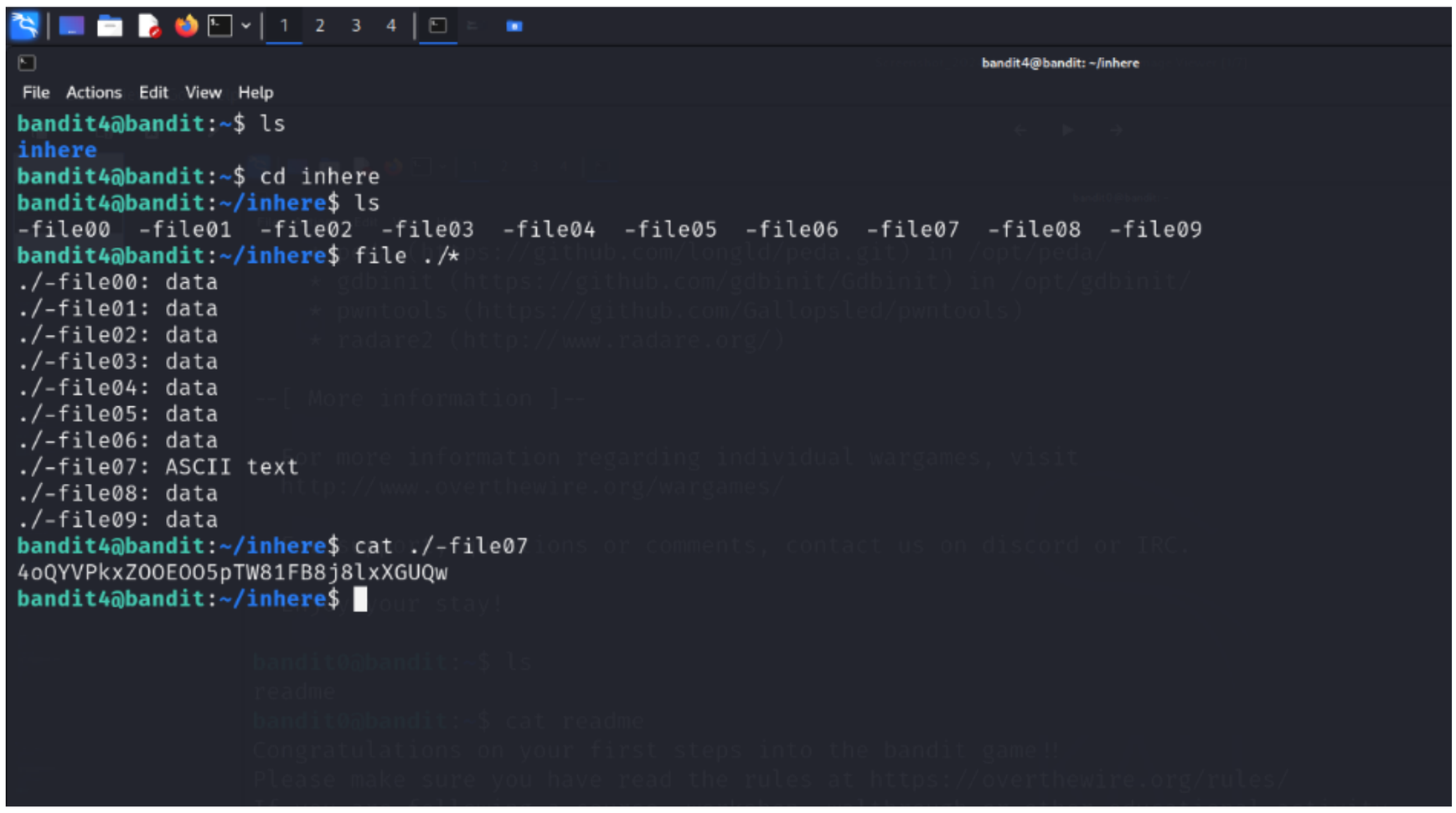


LEVEL 4 → LEVEL 5

Goal: File types, specifically human-readable files.

- After Finding password for level 4, switch the username.
- The password for the next level is stored in the only human-readable file in the **inhere** directory.

- file is a command used to find the type of file. . / is use consider -file00 as a file. * is used to list the type of files in the current working directory.
- Use this command file ./-file*
- Then its displays -file07 in ASCII text.ASCII text is human readable file.
- So cat ./-file07 after get the password 5.

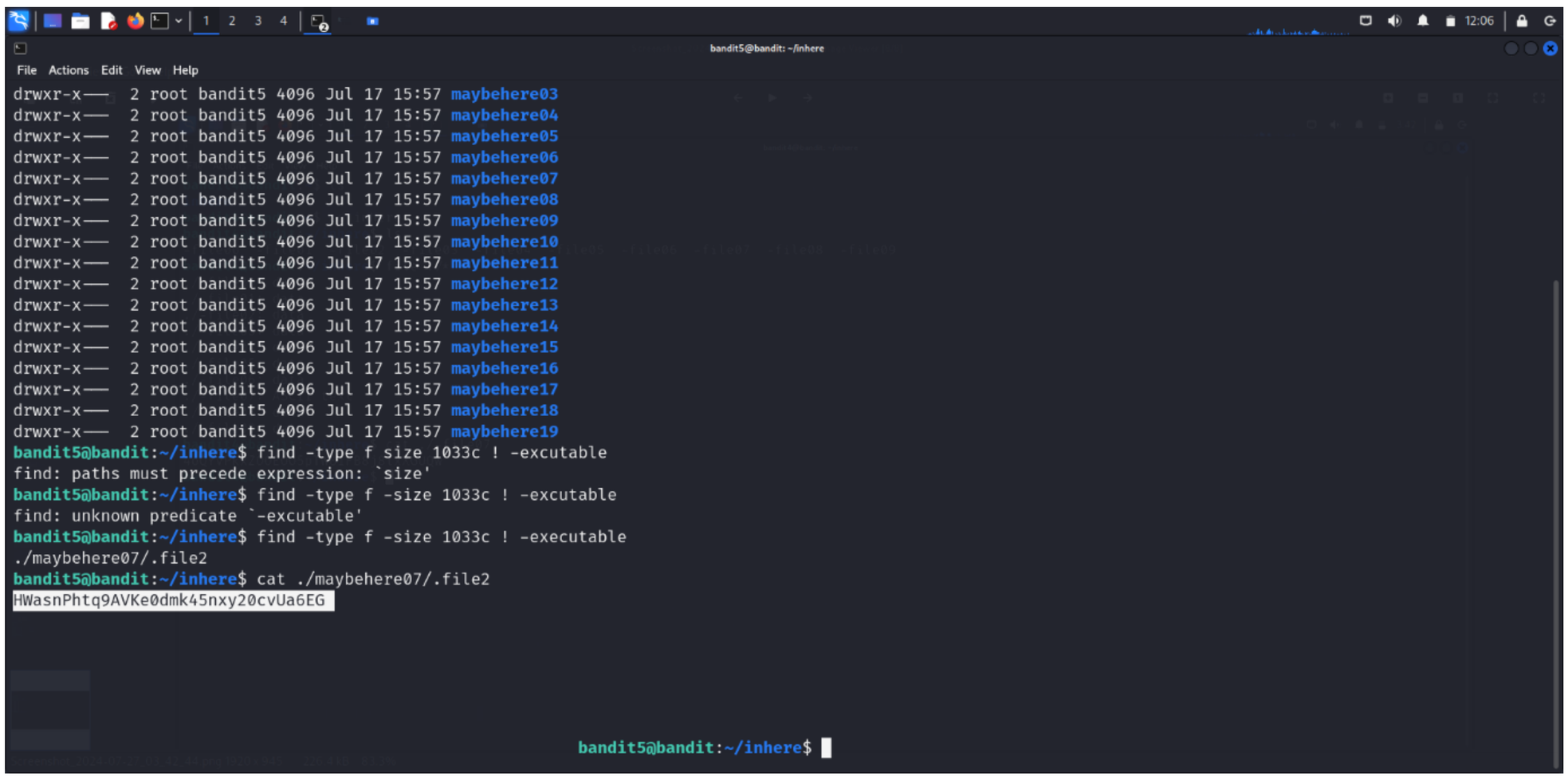


LEVEL 5 → LEVEL 6

Goal: Human-readable files, file sizes and non-executable files.

- After Finding password for level 5, switch the username.

- 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
- After ls(list) you can see the directory called inhere
- cd to change the directory inhere
- You can see multiple directory with multiple files and directory in the inhere directory.
- Command find -type f -size 1033c ! executable
    - find command is used to find the specific directory or file
    - To mention human-readable command is -type f. (f-file).
    - .To mention size command is -size 1033c . we have to use ‘c’ for depicting size in bytes.
    - To mention not executable command is ! executable.
    - After using this command cat . /maybehere07/.file2



LEVEL 6 → LEVEL 7

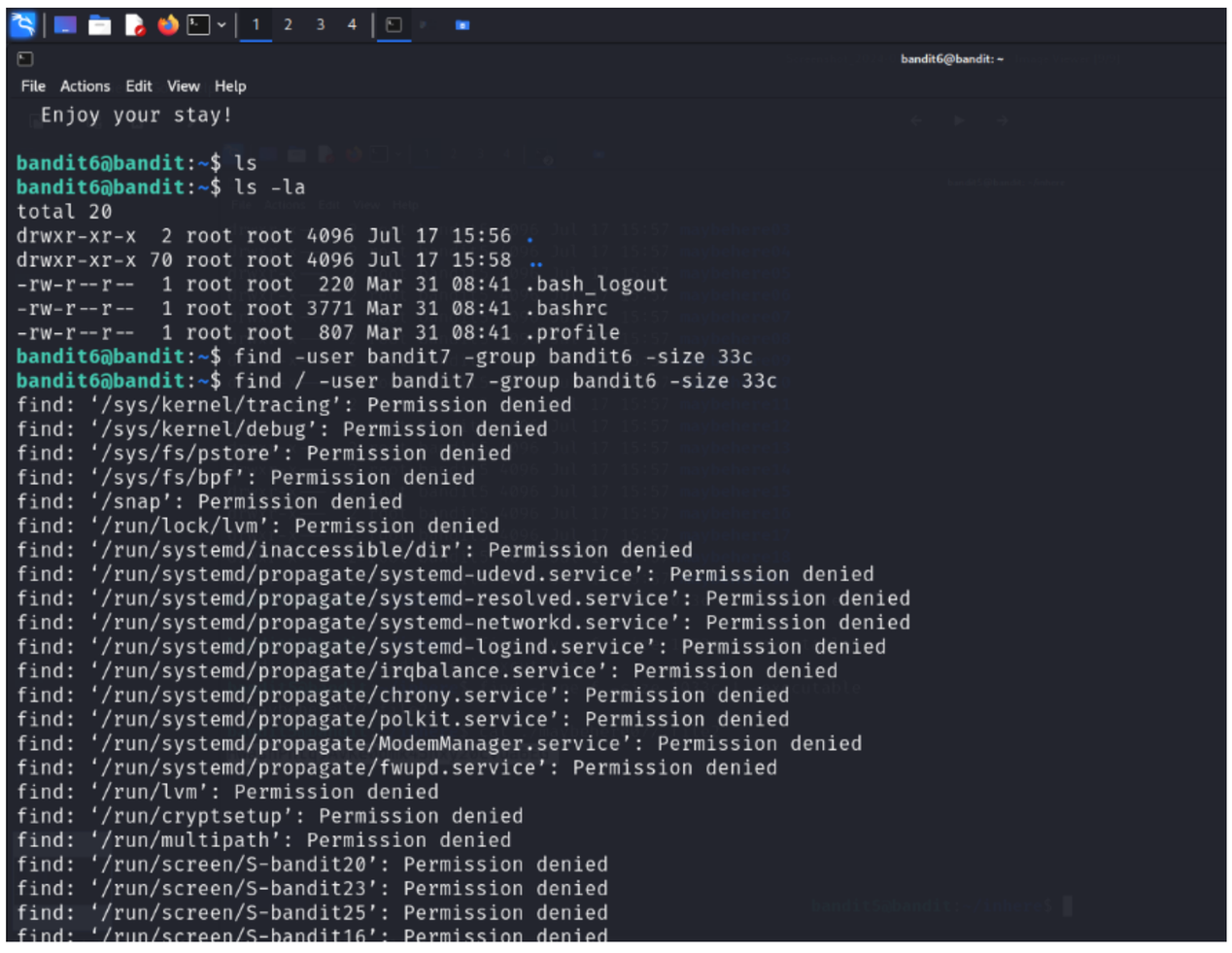
Goal: Find a file with specific user and group ownership.

- After Finding password for level 6, switch the username.
- The password for the next level is stored **somewhere on the server** and has all of the following properties:

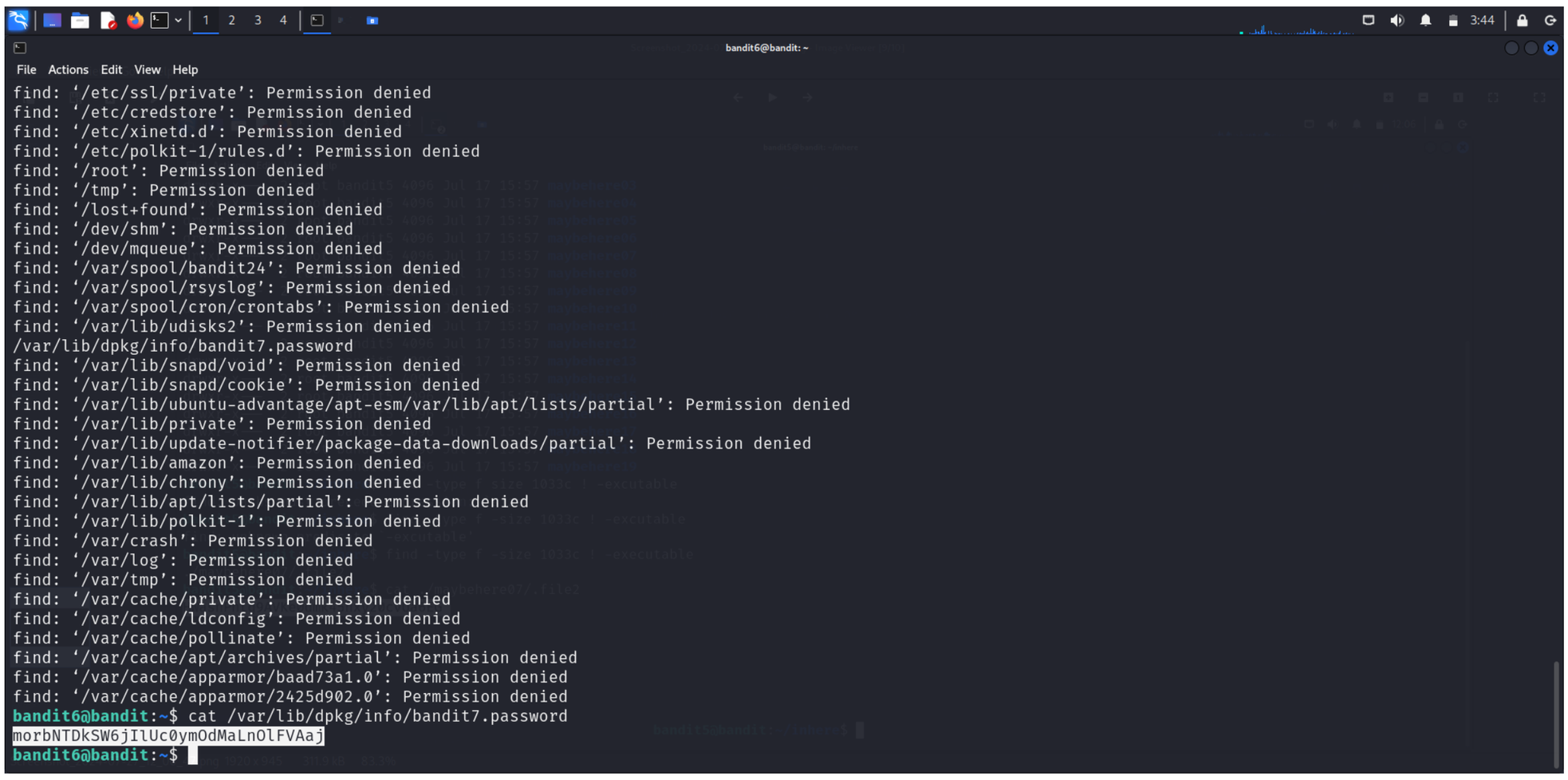
- owned by user bandit7
- owned by group bandit6

- 33 bytes in size
    - Command find / -user bandit7 -group bandit6 -size 33c.

        - find command is used to find the specific directory . / is used for run the folder to mention user the command is -user bandit7. To mention group the command is -group bandit6.To mention size command is -size 33c . we have to use ‘c’ for depicting size in bytes.



- Permission denied for all directory except /var/lib/dpkg/info/bandit7.password.
- Cat /var/lib/dpkg/info/bandit7.password.
- **Then the result is**



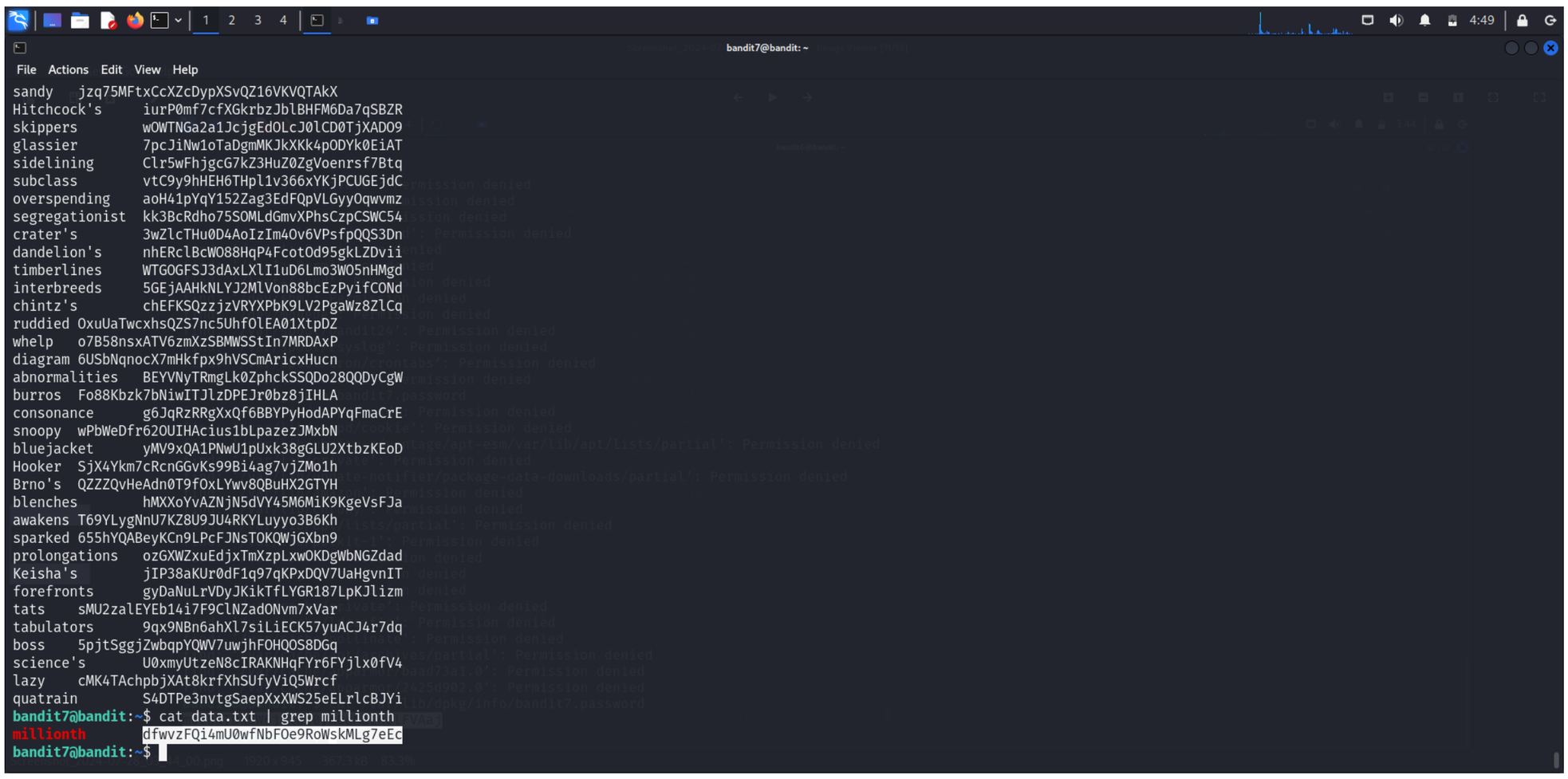
LEVEL 7 → LEVEL 8

Goal: grep and piping

- After Finding password for level 7, switch the username.
- The password for the next level is stored in the file **data.txt** next to the word **millionth**
- Learning grep and piping

- Is there is a file called data.txt

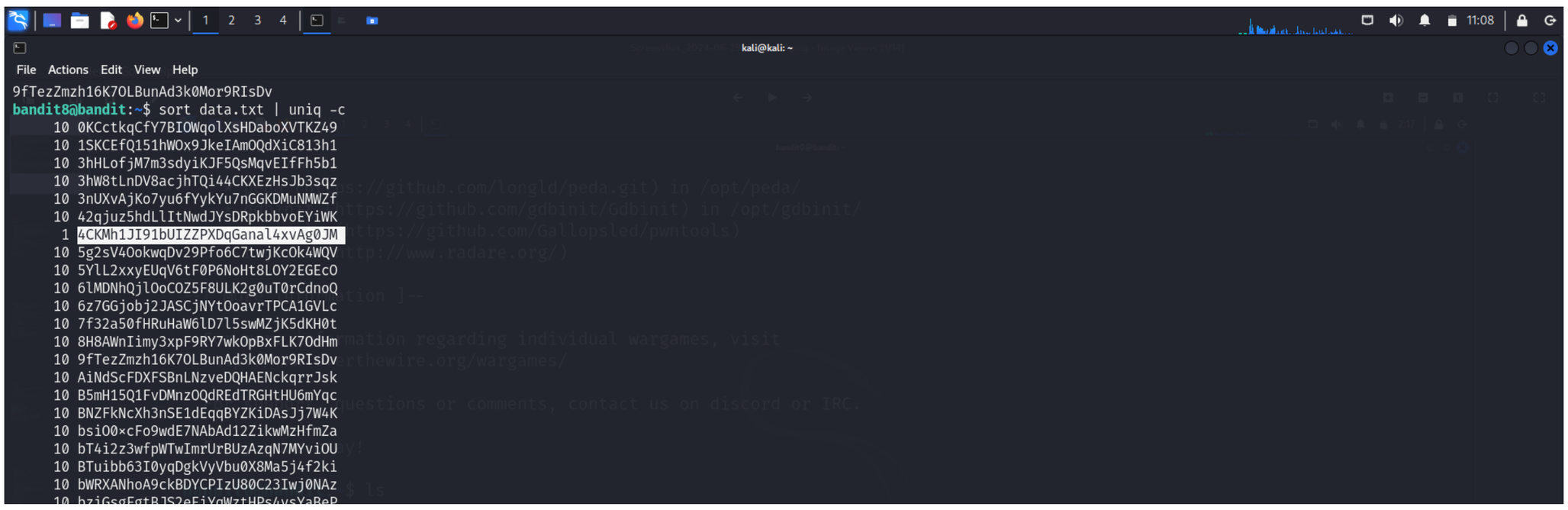
- cat data.txt we can see multiple texts.
- the next level password is stored in the file data.txt next to millionth.
- We are going to use the grep command for finding millionth. Here we using the (|) Unix pipe. The Pipe connects the standard output from the first command and feeds it as standard input to the second command. In our case, first cat command reads the file and then the data inside the file is sent to grep command to work on.
- **Command** **cat data.txt | grep millionth**



LEVEL 8 → LEVEL 9

Goal: uniq and sort, to find lines only appearing once.

- After Finding password for level 8, switch the username.
- The password for the next level is stored in the file **data.txt** and is the only line of text that occurs only once
- grep, sort, uniq
- command sort data.txt | uniq -c
- ls there is a file called data.txt, use cat data.txt after can see multiple lines of words
- sort is the command used to arrange the group of word in ascending order. uniq is the command used to find the unique word or number -c is to specify the count
- Displayed by unique line count of 1



LEVEL 9 → LEVEL 10

Goal: Find human-readable strings in a file.

- After Finding password for level 9, switch the username.
- 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.
- Is there is a file called data.txt, use cat data.txt after can see multiple lines of words.
    - Command string data.txt | grep =
    - string is the command used to convert string characters into files.
    - **Then the result is**

LEVEL 10 → LEVEL 11

Goal: Base64.

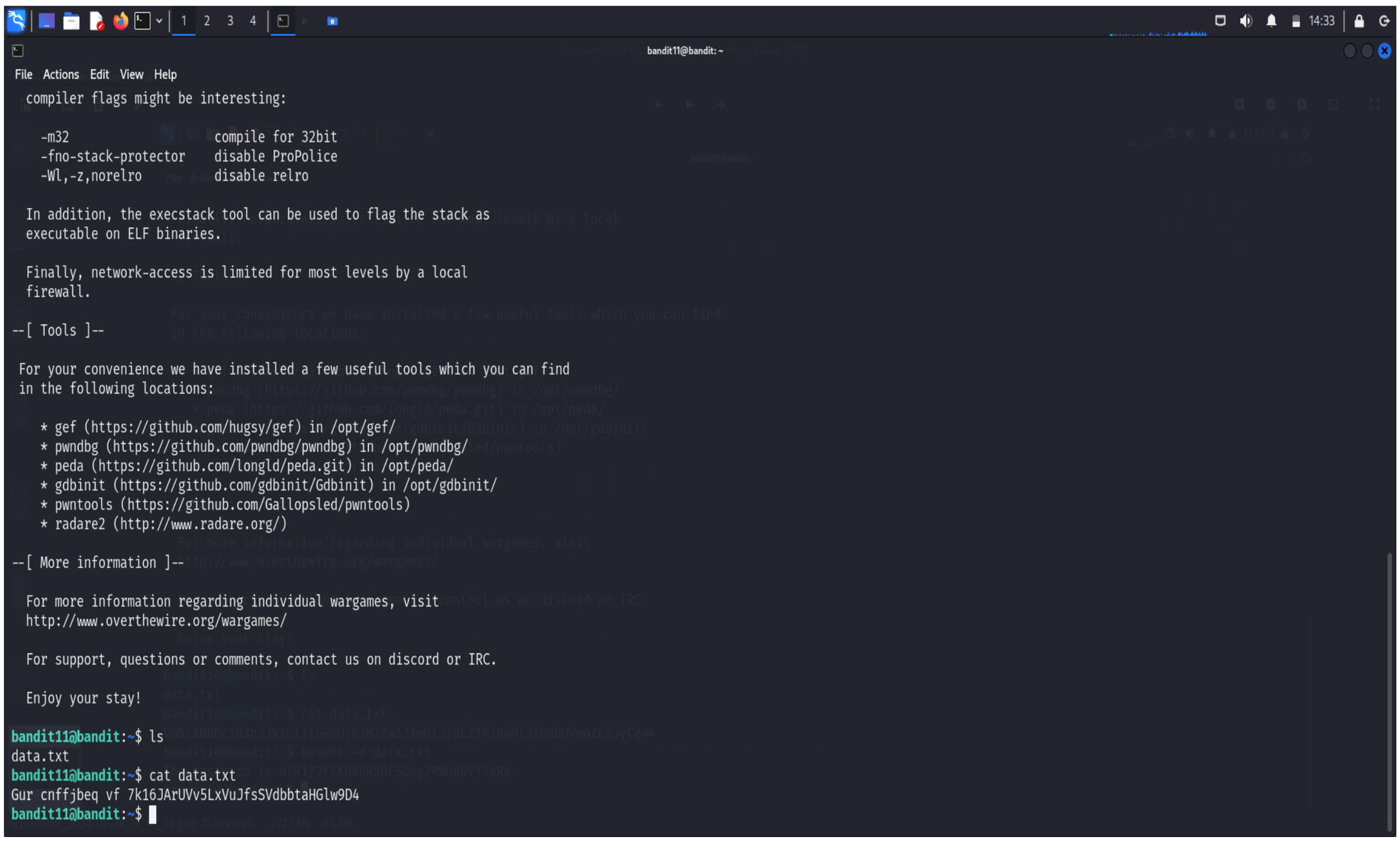
- After Finding password for level 10, switch the username.
- The password for the next level is stored in the file **data.txt**, which contains base64 encoded data
- Use ls command get data.txt, use cat data.txt after can see encoded data.
- **echo** - display a line of text
- base64 -d command is a powerful tool for encoding and decoding data, making it safe for transmission, -d is refers to decode.
- Command echo "VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg=" | base64 -d

```
    * 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!

bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==
bandit10@bandit:~$ echo 'VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==' | base64 -d
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit:~$
```

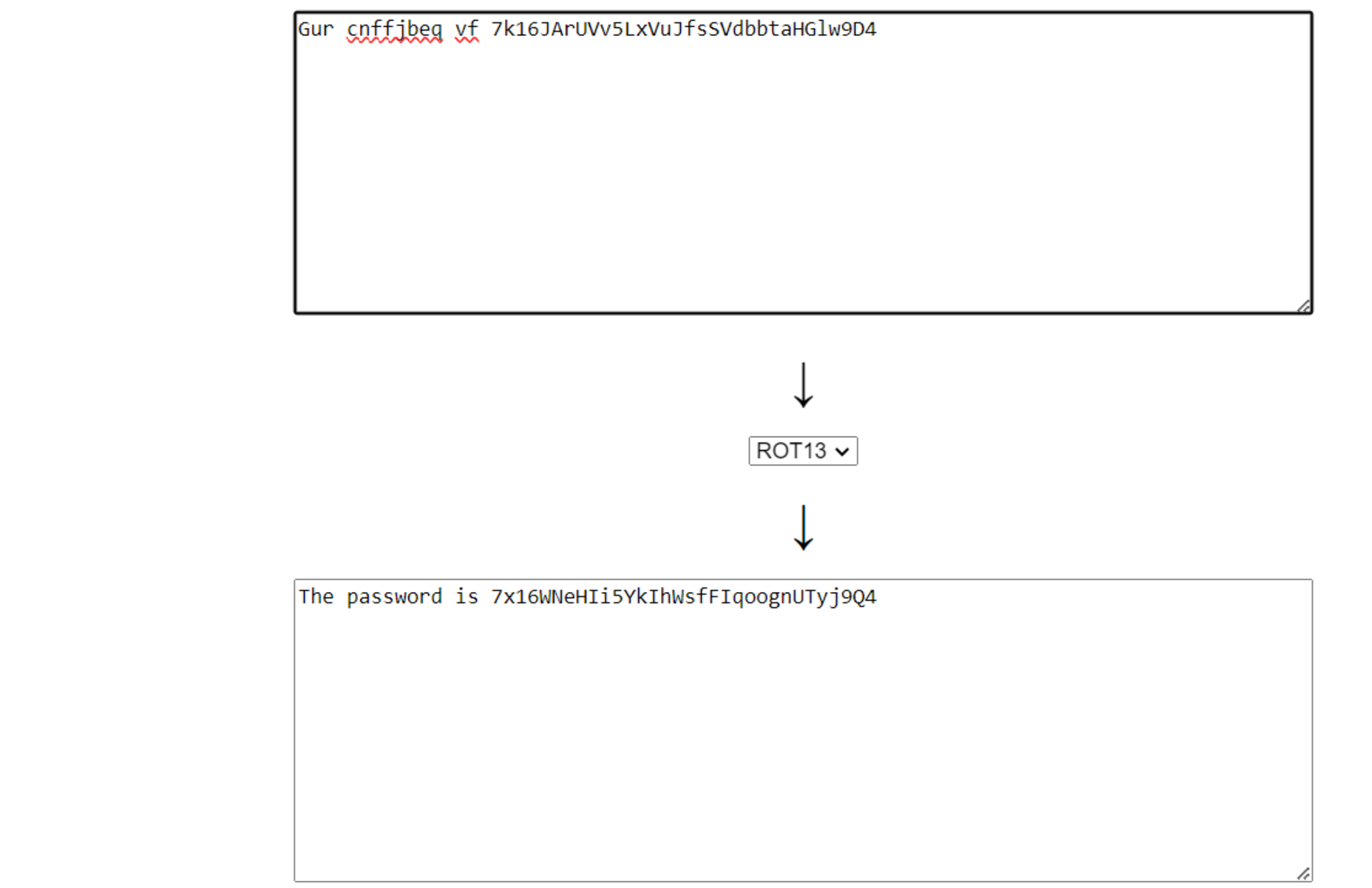
LEVEL 11 → LEVEL 12

Goal: lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions Rot13

- After Finding password for level 11, switch the username.
- 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
- cat data.txt



- There is website called rot13.com, copy the code and paste in that website. we found the password for level 12.

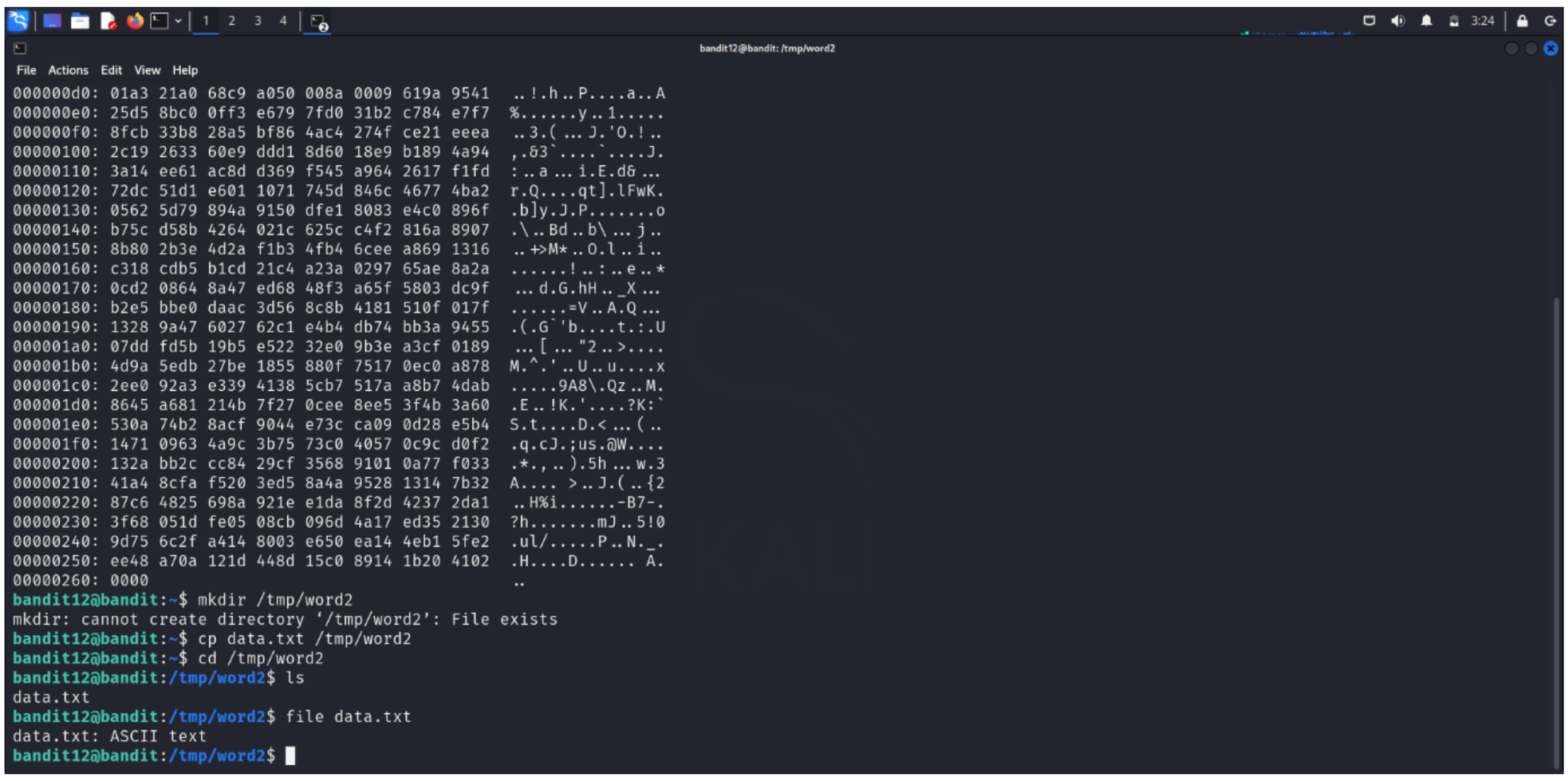


LEVEL 12 → LEVEL 13

Goal: Hexdumps and compression

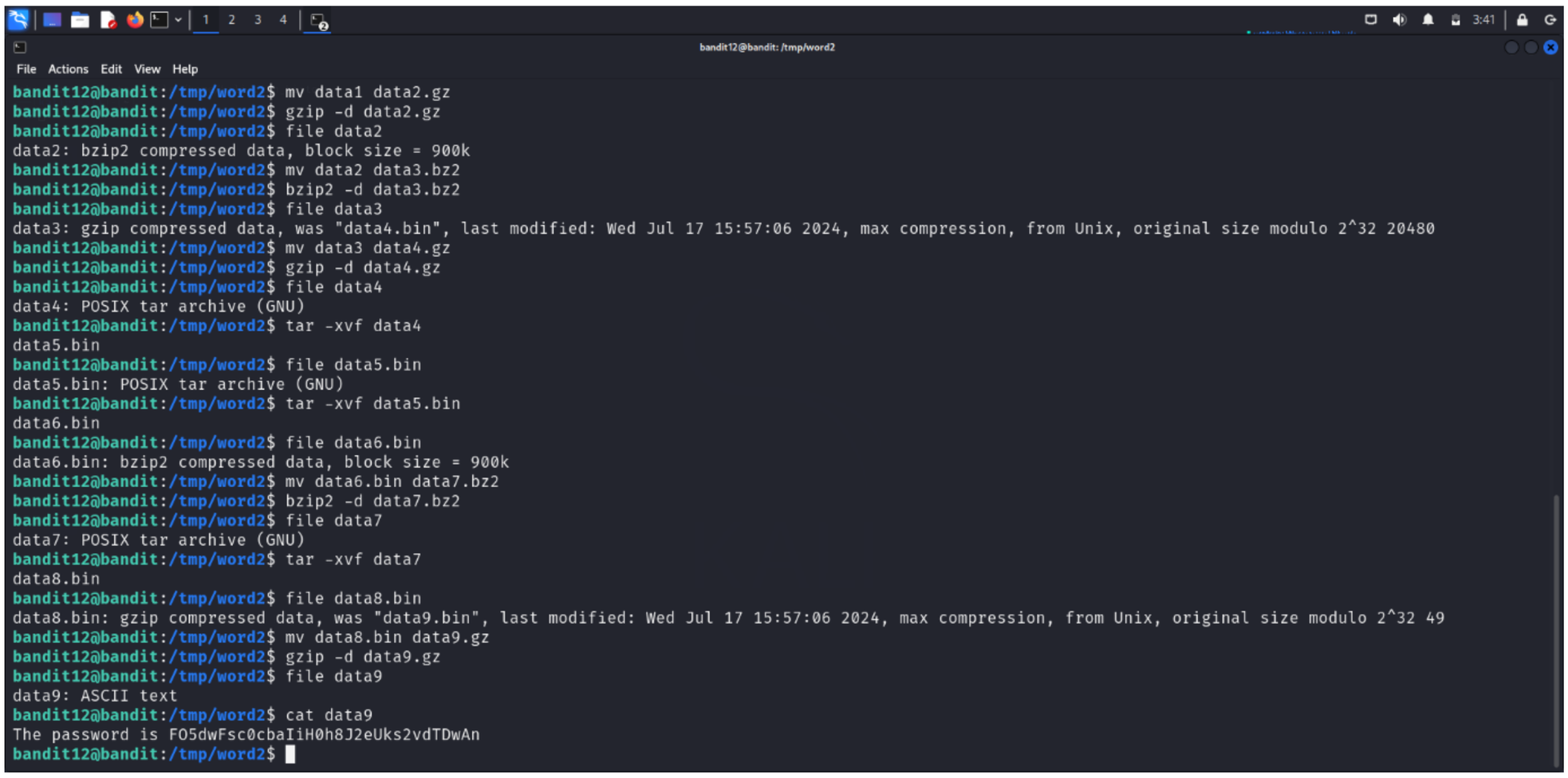
- After Finding the password for level 12, switch the username.
- The password for the next level is stored in the file **data.txt**, which is a hexdump of a file that has been repeatedly compressed. For this level it may be useful to create a directory under /tmp in which you can work. Use mkdir with 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!)
- A file named data.txt could be found in the home directory.
- For this level it may be useful to create a directory under /tmp in which you can work.
    - Since the file require multiple modification, create new directory mkdir command in Linux is a command-line utility that allows users to create new directories.
    - the command is mkdir/tmp/name of the file

- I give the name to the directory /tmp/word2
- cp command in linux copying files from one location to another.
- To copy the **data.txt file to /tmp/word2**
- Afer accessing the /tmp directory, use the ls command to check if the files exists.
- The command file data.txt displays ASCII text, which is not readable.



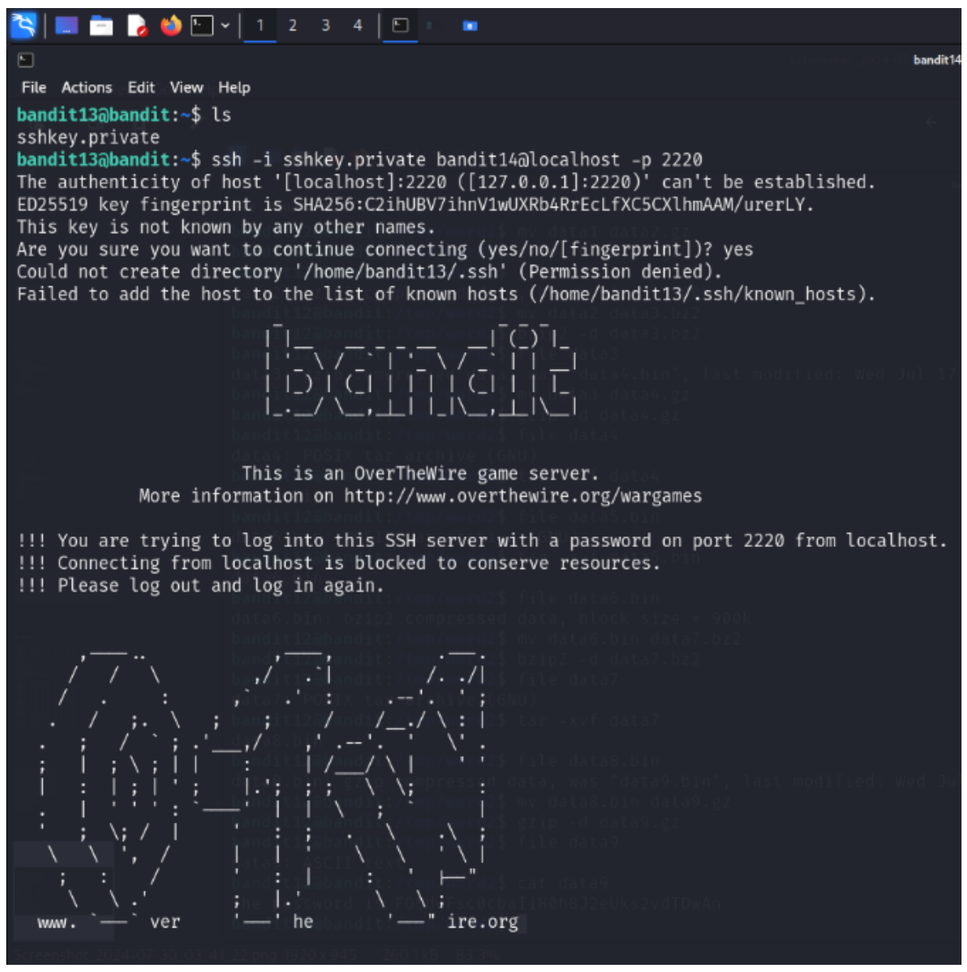
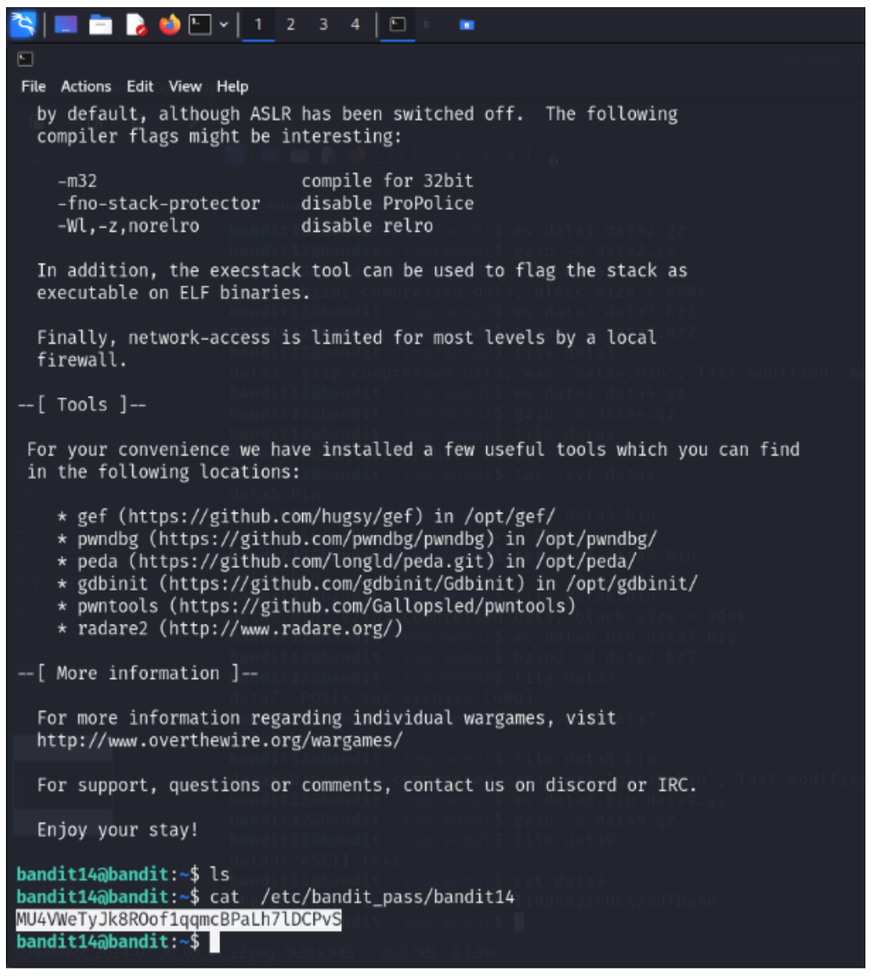
- To retrieve data, use the command xxd -r data.txt data1. The xxd command creates a hexdump of a file.

- while the -r parameter reverts the process. I named the file "data 1".
- We used the file command to verify that the file was retrieved, and it shows that it is a gzip compressed file.
- To decompress data2.gz, use the command gzip -d.
- Check the retrieved file using the file command "data2," which displays a compressed file.
- Once more, the command bzip2 -d data3.bz2 must be used to decompress that.
- Until you obtain an ASCII text file, the same procedure of altering the file name and repeatedly decomposing the file will be carried out.
- After receiving the ASCII text file, you must use the cat command to read it in order to find your password.
- Finally received the password.



LEVEL 13 → LEVEL 14

Goal:SSH Login with key and transferring files from a remote host.

- After finding the password for level 13, change the username.
- 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.
- They have already stated that we must utilize the private SSH key and use localhost as our hostname in order to go to level 14.

- Thus, to inspect the file, use ls. You will be able to see the sshkey.private using this when we move on to the next phase.
- Here, the command is: private bandit14@localhost -p2220 ssh -I sshkey.
- Finally received the password.