IT20028046

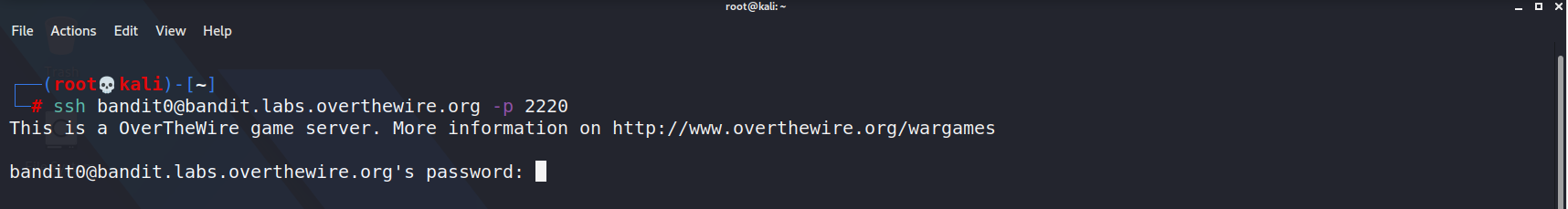
Gunathilaka S.B.M.B.S.A

Video presentation link

https://drive.google.com/file/d/1\_AW1FbejAAygK4fCsUlvFiXx3ka4tjoW/view?usp=sharing

Level 0

This is a very simple level. We need to connect a specific host to play the bandit war game. So first we should connect to the host using the given URL and port number. After that using the ls command, we can find the files and view the content then we have the password. At this level, we need to read the content of the readme file using the cat command.





Level 1

The password for level 1 is stored in a file but the filename is - (dash) so we need to read this file using given commands. - as an argument refers to STDIN and STOUT. If you want to open this file, we have to specify the full location of the file like this.



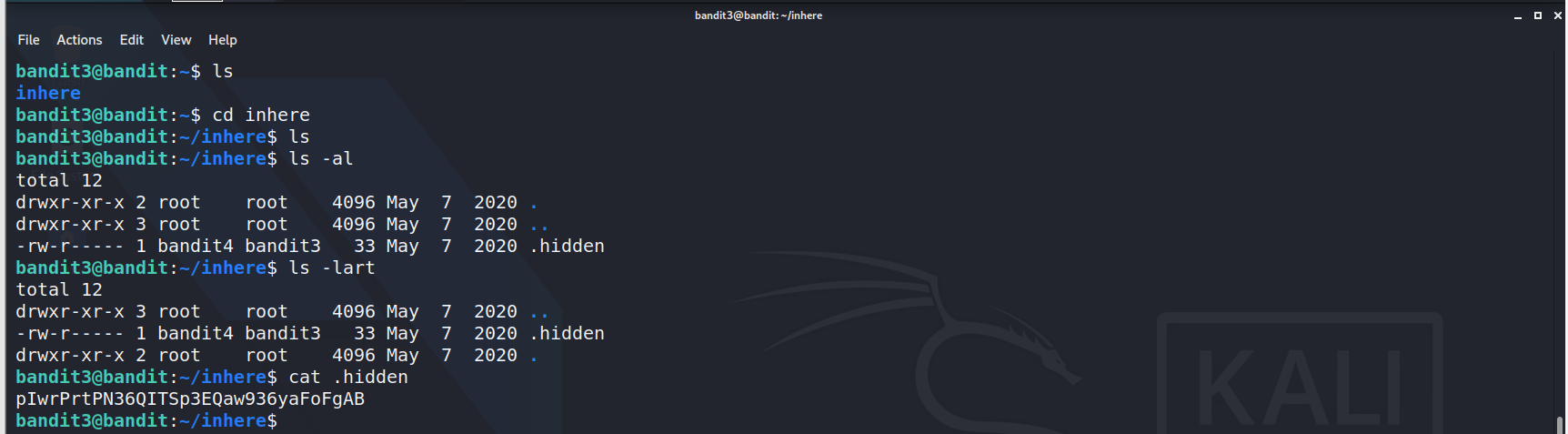
Level 2

First, we need to list files in this directory. Then we can see the file named spaces in this filename. The cat command reads the file's name only until space is met. Consider space as null Then stop reading so we can't directly use the cat command. We can escape spaces using backslash or single and double-quotes.



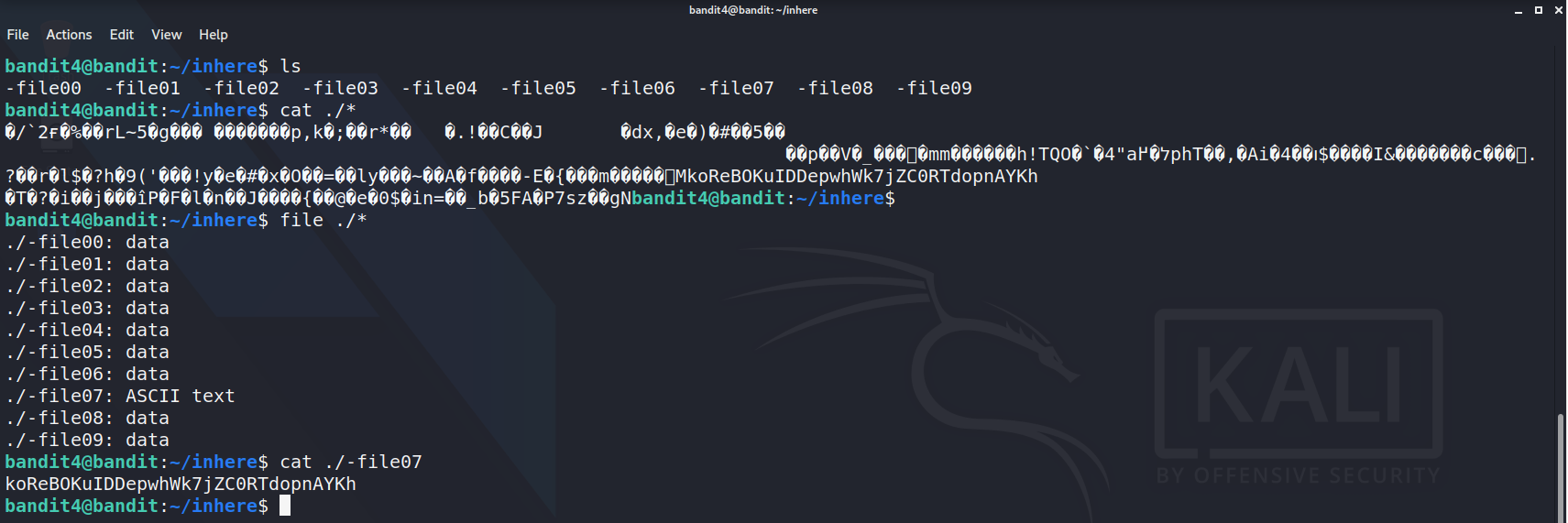
Level 3

The password for level 4 is inside the inhere directory. So, we can use the ls command for list files inside the inhere directory. But ls command does not give any output.it Might be the case that there are some files hi hidden. Then we can use the ls command with -al parameter to obtain the hidden file.



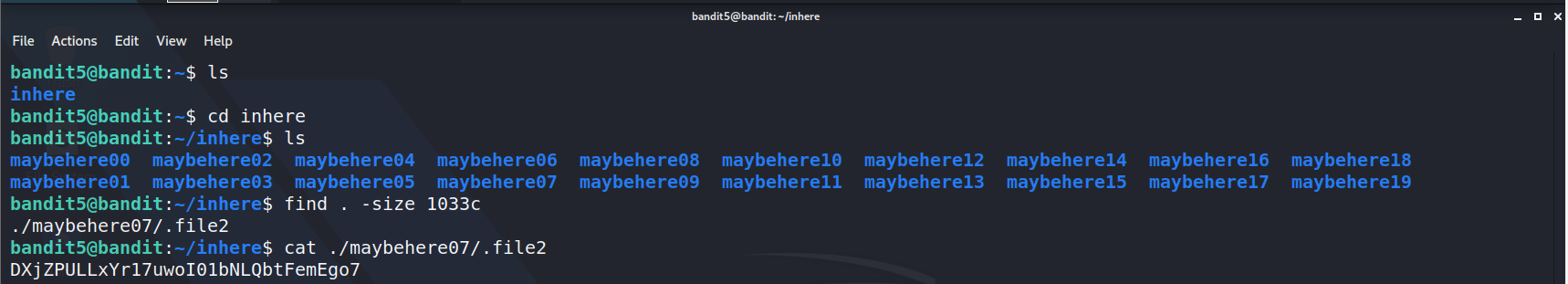
Level 4

First, we can list files in the inhere directory using the ls command. Then we have Few files. The password is stored inside a human-readable file among these files. We can use the cat ./\* command to show every file contains at the same time. We have another way to do this activity using the file command. The file command can show information about the files. From the file command, we can see there is a file named file07 that contains ASCII text. It is mostly human-readable text. Now we can guess that the password is inside the file07.



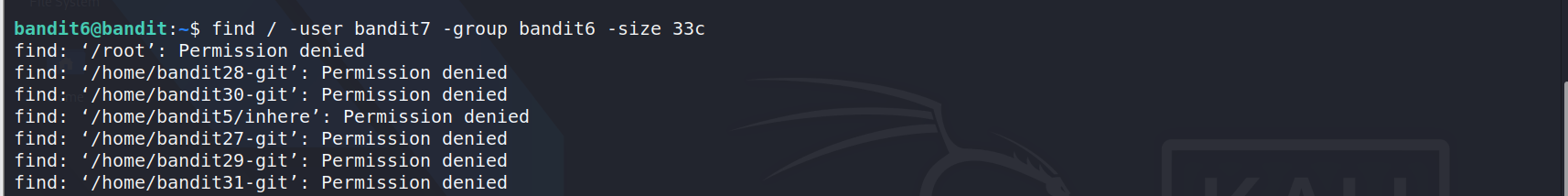
Level 5

The password file is somewhere inside a directory named inhere. First, we should use the ls command to lock inside the Inhere directory. Then we can filter the file using the given data. Sofi can filter using file size. Find command has a parameter off size and we have to use "c" for depicting size in bytes.



Level 6

At this level the password is stored somewhere on the server .so, finding the password file over the server. we have to use the ls command but a more advanced way. let's filter the password file with the given detail. now we know that the user of the file is bandit7 and the file is a part of group bandit6.then we will try to widen find command scope.

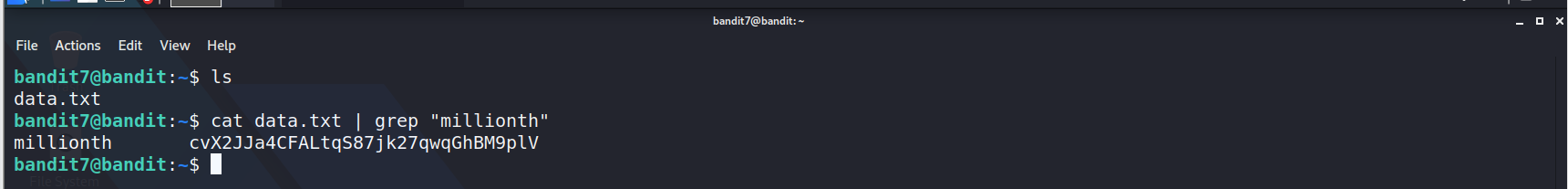






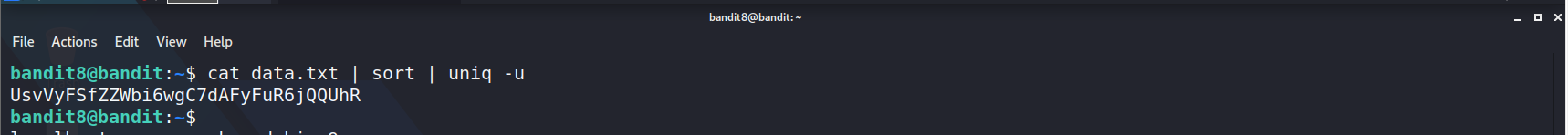
Level 07

Now we have to find the password file with the word millionth. The password is written next to the word millionth.so if we can find the word millionth, we can get the password as well. for that, we can use the grep command. also, we have to use the Unix pipe (|). Unix pipe referred to as a filter. the grep command searches files for lines that have a looking pattern.



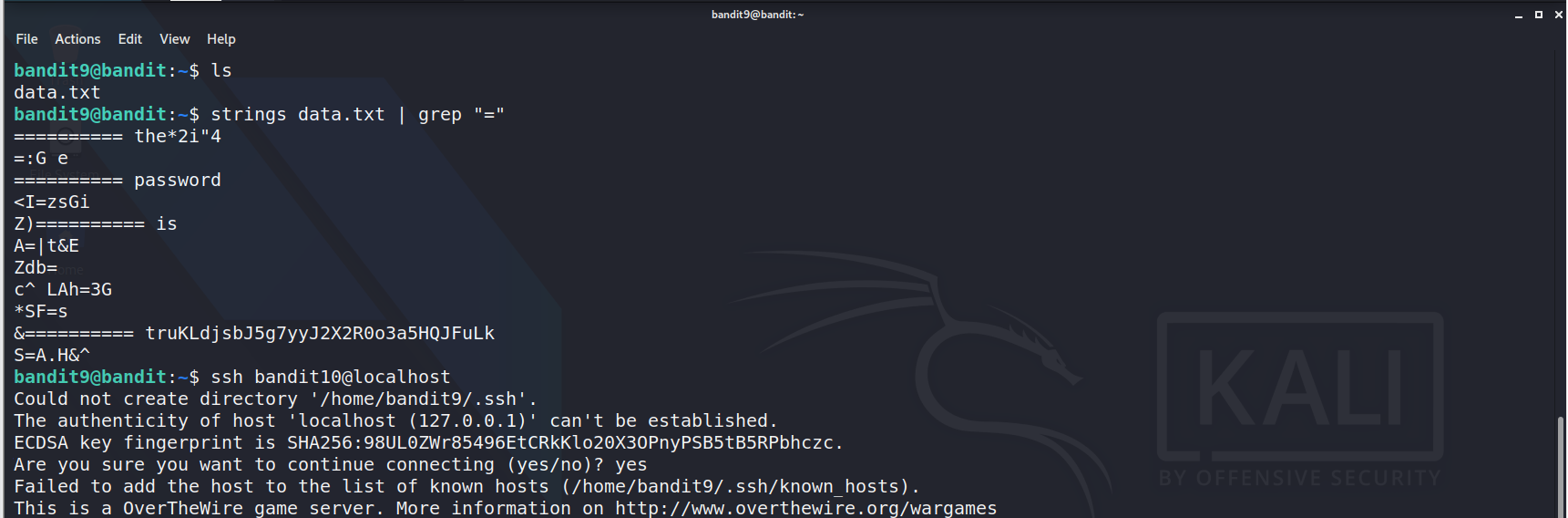
Level 8

The password is stored inside the data.txt file and it is the only line that occurs only once. So, we have to use the sort command to sort the text.to prevent a lot of repeating statements we can use multiple pipes to filter the password.



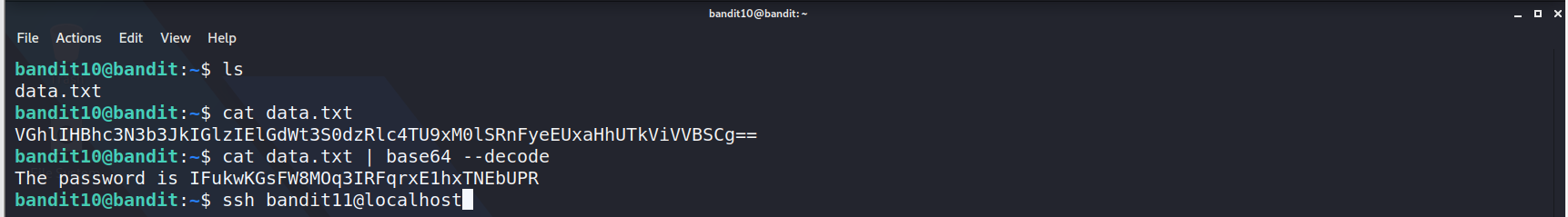
Level 9

At this level our password is stored in data.txt. but there are some equal symbols in front of the password. in this situation, if we use the cat command the result is unreadable strings. so, we have to use a string command to print character sequences that are at least 4 characters long.



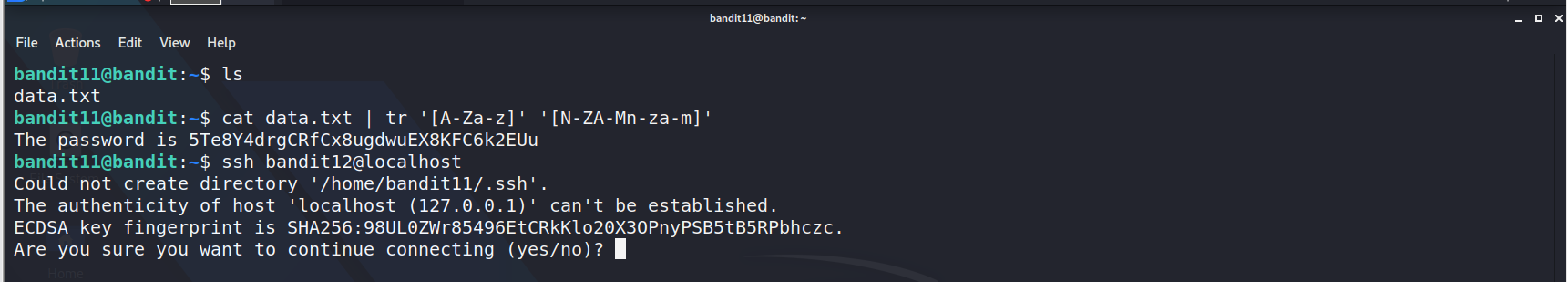
Level 10

First, we use the ls command to get a list of files .now we are hinted that the password is encoded in base64. we can use Unix pipe with cat command and bas64 command. we can use d parameter with base64 command. then it will be read and decode the text.



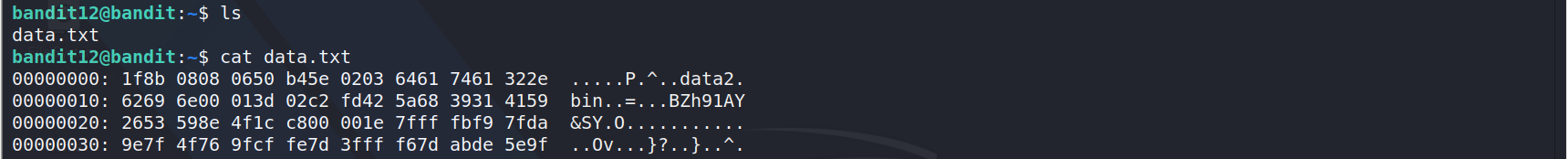
Level 11

At this level, the password has changed the format of letters. The lowercase and uppercase letters have been rotated by 13 positions. We have to convert the text to the correct position. So, we can use the tr command to do that. The tr Command will translate characters depending on the given parameters. TR will not continue to translate after the letter z. So, we have to use a-m and n-z.

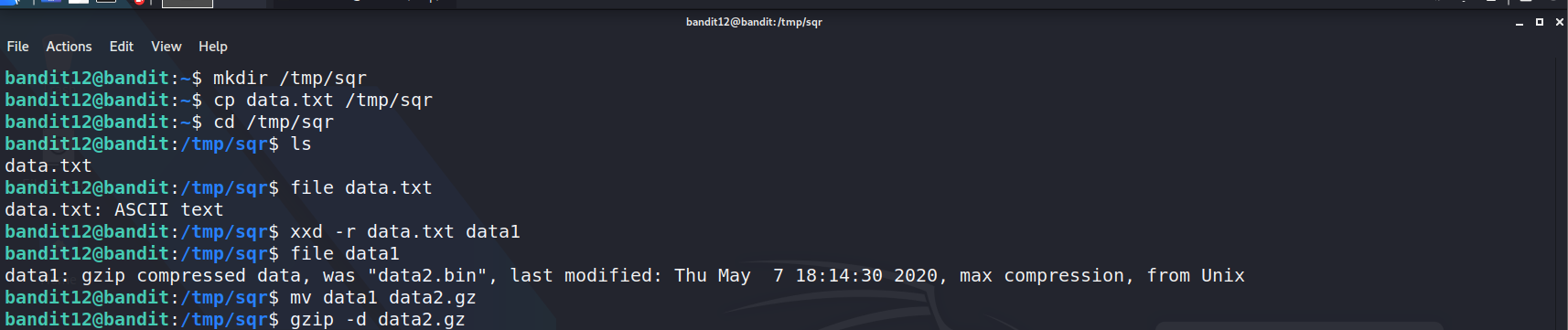


Level 12

We can use the LS command and get the data.txt file. Using the cat command, we can view the file contains. But the contains is in the form of a hex dump and the password file is repeatedly compressed. To decompress it we need a directory with the necessary permissions.

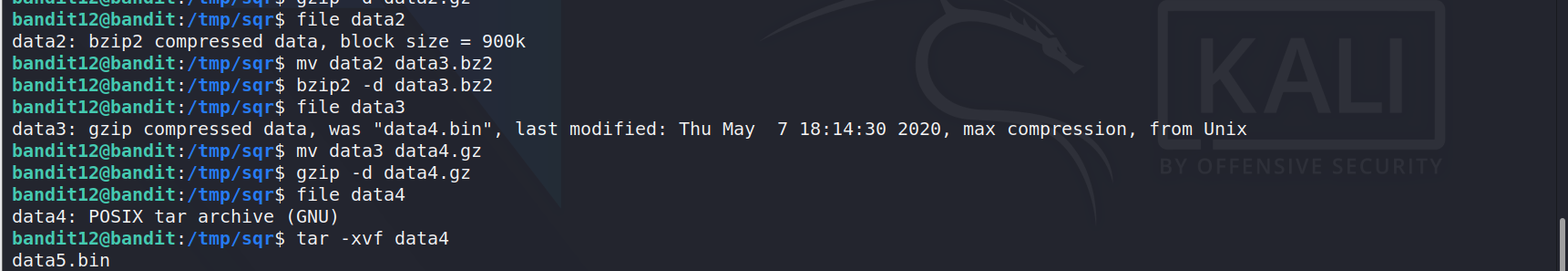


So, let's create a directory inside the TMP directory. I name it XYZ. Now for the rest of the operations let's copy to the file we have created directory now. Now let's look inside the file using the CD command. To get the details about the file we can use the file command. The File is ASCII text but not readable. The "xxd" command can make a hex dump file and it used to reverse this process as well. So, we can use it to retrieve the original file. With the "xxd" command with the " r " parameter. It can reverse the process and give a file name to that output. We will name it data2. Now, we can check the output file using the file command. Then it shows that it is a gzip compressed file. Using the move command, we can rename and give a gzip file extension. Now we can decompress the file.



Now we can check the output file. To find the compressed status we have to use the file command again. Using the move command, we can give it a proper name and bzip file extension. Using the bzip command and - d parameter we Can decompress the file. Now check the file using the file command. Now it's a gzip compressed file.

Before decompress we need to rename and the gzip extension. We can do that using the move command(data5.gz). Now we can decompress. Again, check the output file using the file command. Now it's a tar achieve file. When we can extract this file using the tar command with xvf parameters. It output data5.bin.



Now check the output file using the file command. It's a tar achieve file now. Now extract this file using tar command with xvf parameter. Then we have the file named data6.bin

Check the output file using the file command. Now it's a bzip compressed file.

Before decompress we need to rename the file name and change the file extension to bzip format. The renamed file name is data7.bz2. Now we Can decompress the file. Now check the file using the file command. It shows that it is a tar achieve file. Next, we can extract the file using the tar command with xvf parameters.

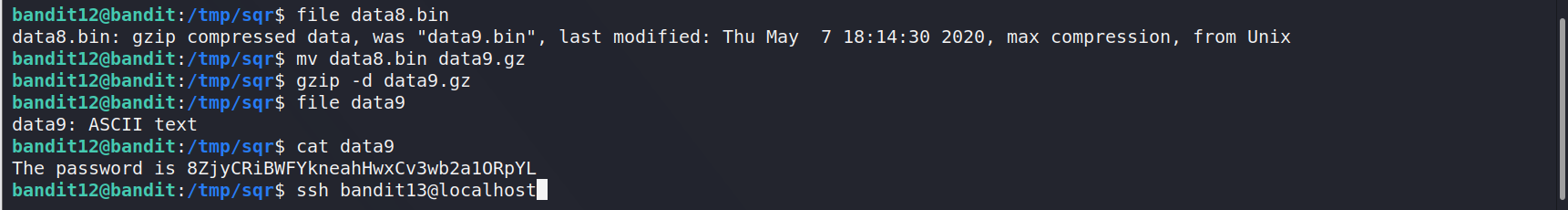
It gives another file data8.bin.



Now we can check the output file. So, we have to use the file command. It shows that this is a gzip compressed file. Before decompress we need to rename and give a proper file format. So, we need again the move command.

after Rename the file as data9.gz. Now We can decompress the file.

Using the file command, we can have the file type. We can see it is ASCII text. This might be readable. Using the cat command, we can read it now.



Level 13

We have to get the password for the next level. We're given an ssh private key. So, we have to use the private key to find the password. Let's use the LS command and we have the private key. We can use it to build a connection as bandit14.



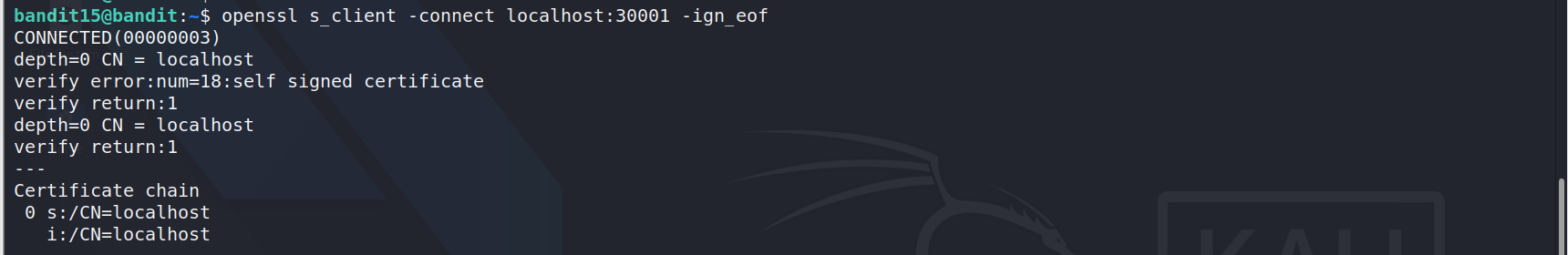
Level 14

At this level, we have to submit the current level password to port 30000 localhosts to get the next level password. We can use the cat command to print the current level password. We have to use telnet to connect port 30000. After connecting to the port, we can enter the current password. Now we can see the next level on the screen.

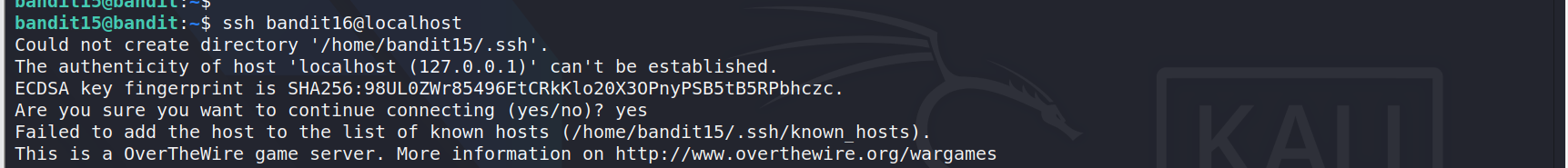


Level 15

We have to submit the current level password to port 30001 only localhost with SSL encryption to get the next level password. To connect port 30001 as localhost we have to use the openssl command with s\_client parameter. We use - ign\_eof to close the connection. When the end of the file is reached in the input.



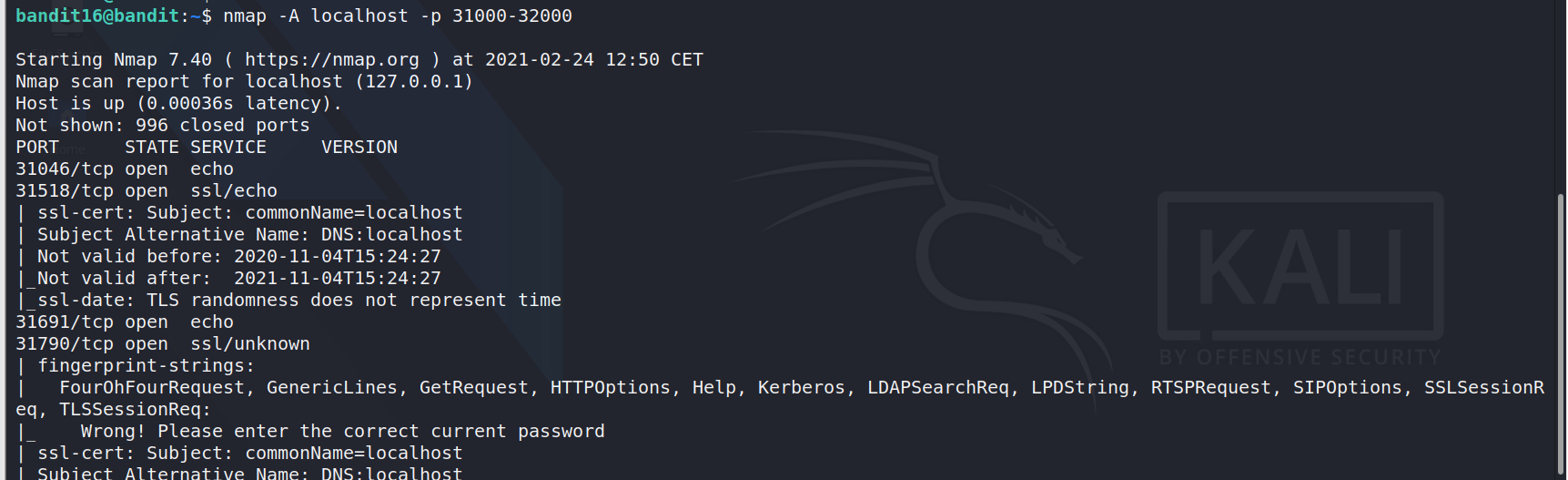
After the connection is successful now, we can provide the password for the current level password. After checking the password, it output the password next level. We can use this password to create ssh connection as bandit16.





Level 16

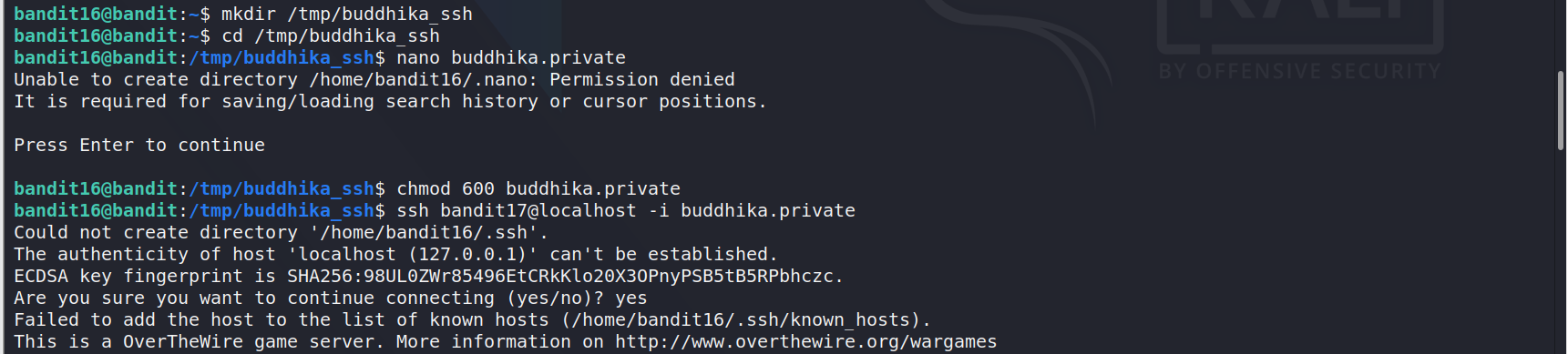
At this level, we have to submit the current level password to a port on localhost in the range 31000 to 32000. First, we have to find which ports have a server listening to them. We can use Nmap to scan the ports and filter what is the exact port. Nmap scan shows that on port 31790. There is a message regarding the password.



Using openssl we can connect to this port as a localhost

After connecting the port now, we can enter the password of bandit16. After verifying it we can see an RSA key.

We need a private key to use this RSA key. First, we must go to a directory with the necessary permissions. We can create a directory using the mkdir command. Then we can create a private key inside that directory.

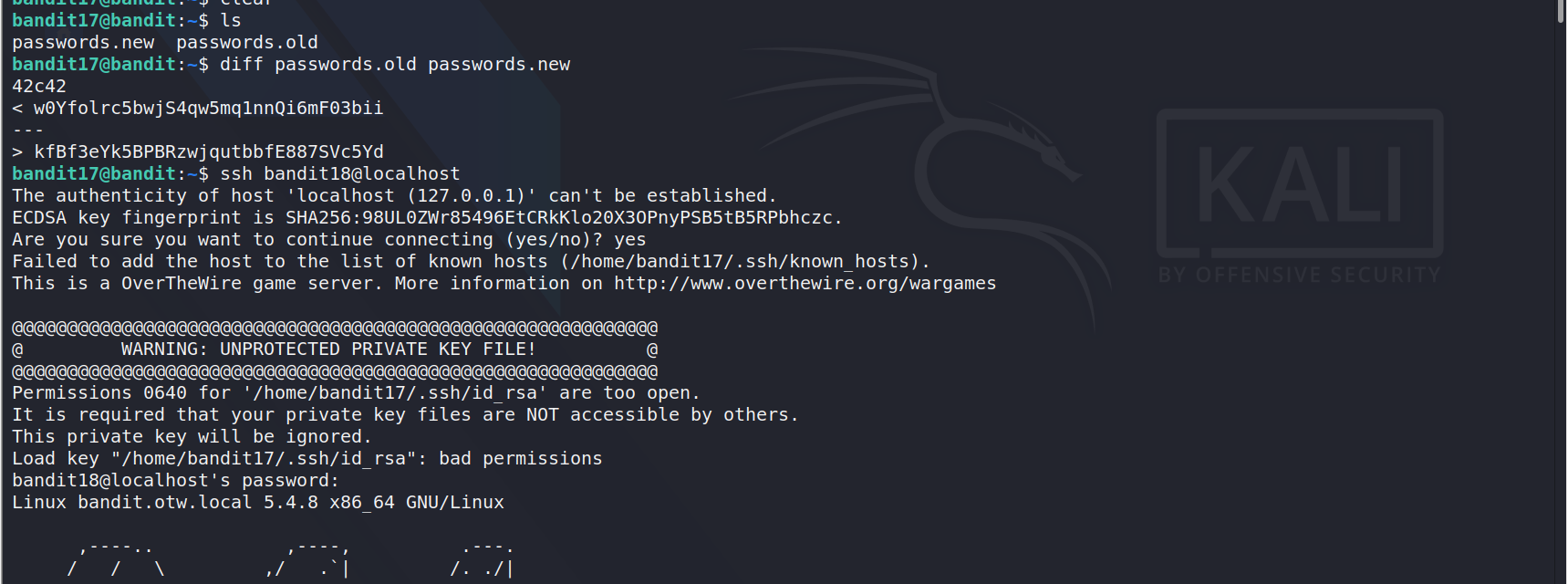


After the Nano command is executed. The animal we can paste here the RSA key we found earlier. We can exit using the ctrl+x key combination. Prompt asking us to save the updates at this moment. So, we will press "y".

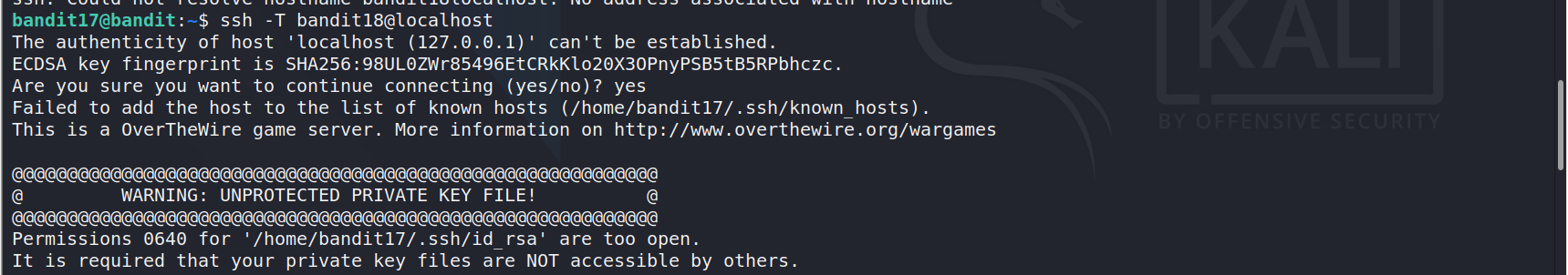
We can use the chmod command to apply necessary permissions equivalent to 600. It means the owner can read and write the fi file. We can use the private key to build an ssh connection as bandit17.

Level 17/18

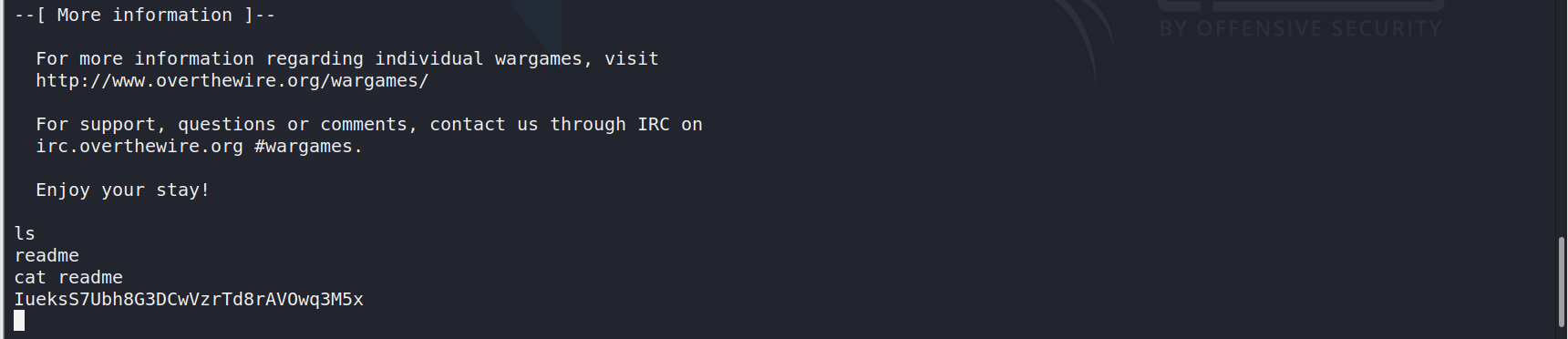
After login in as Bandit17, we can Run the LS command to get lists files. We can see two password files. The password for the next level. The only line that has been changed between two password files. We can use the diff command to find that Bandit18 password.



After providing the password the connection was closed. We can use the - t parameter to disable pseudo - tty allocation



Now using the LS command, we can see the files in the directory. Our password is inside the readme file now.



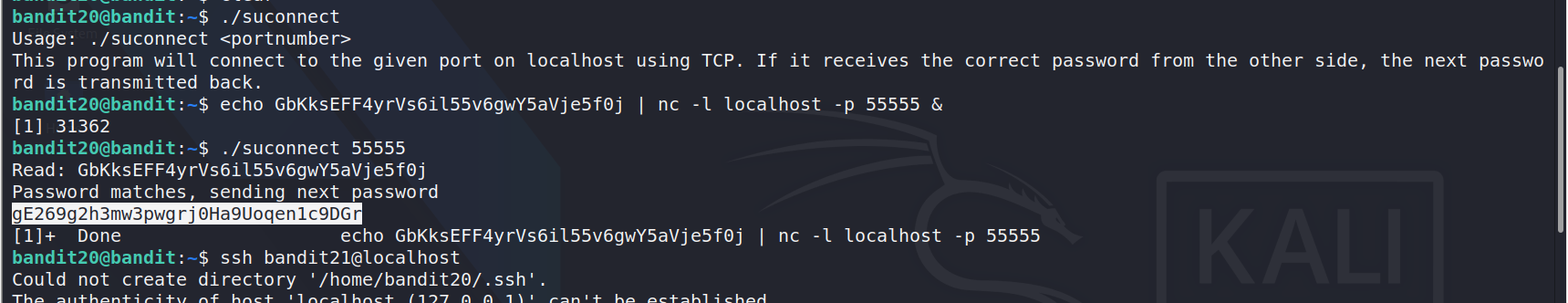
Level 19

First, we can use the ls command and see what we got this time. We can see a text. It seems like a script. Let's check the script is working. Now we can see the script runs a command as another user. We got the actual password location now. Let use the cat command and try to retrieve the password.



Level 20

First, we use the LS command to get a list of files. Now we have a script suconnect. The suconnect command needs a port number to execute. But here we run the suconnect command without parameter and create other instances of the same shell. Then We have to use Netcat to grab a session. Now we can enter the password that is used to enter bandit20. Password is read by suconnect and once the password is verified the password to the next level is sent to the listener.



Now, we get the password for the next level now we can move to the first instance and used the password to login as bandit21.

