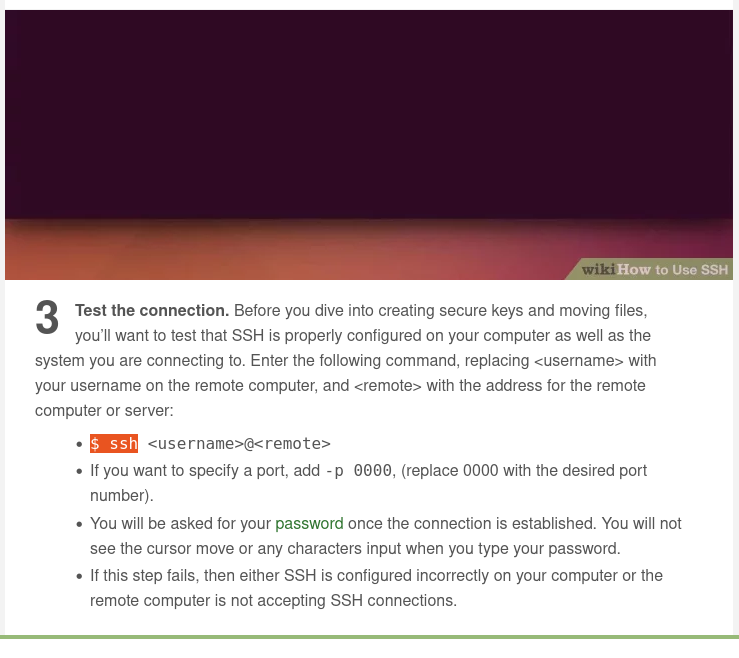
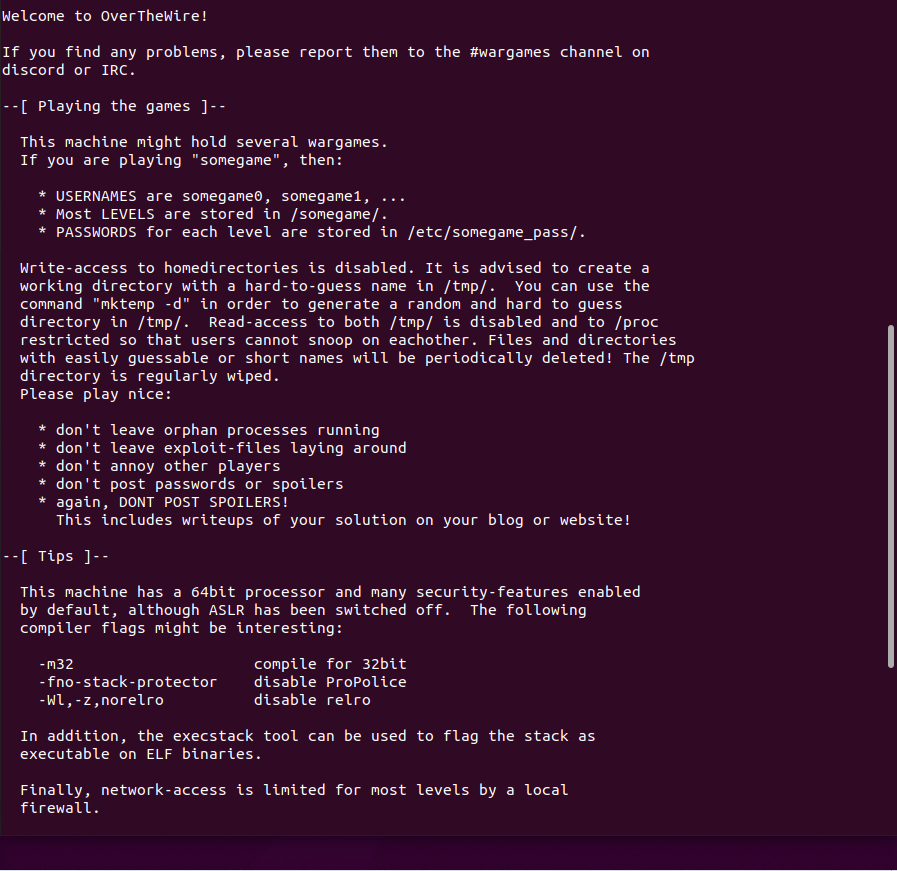
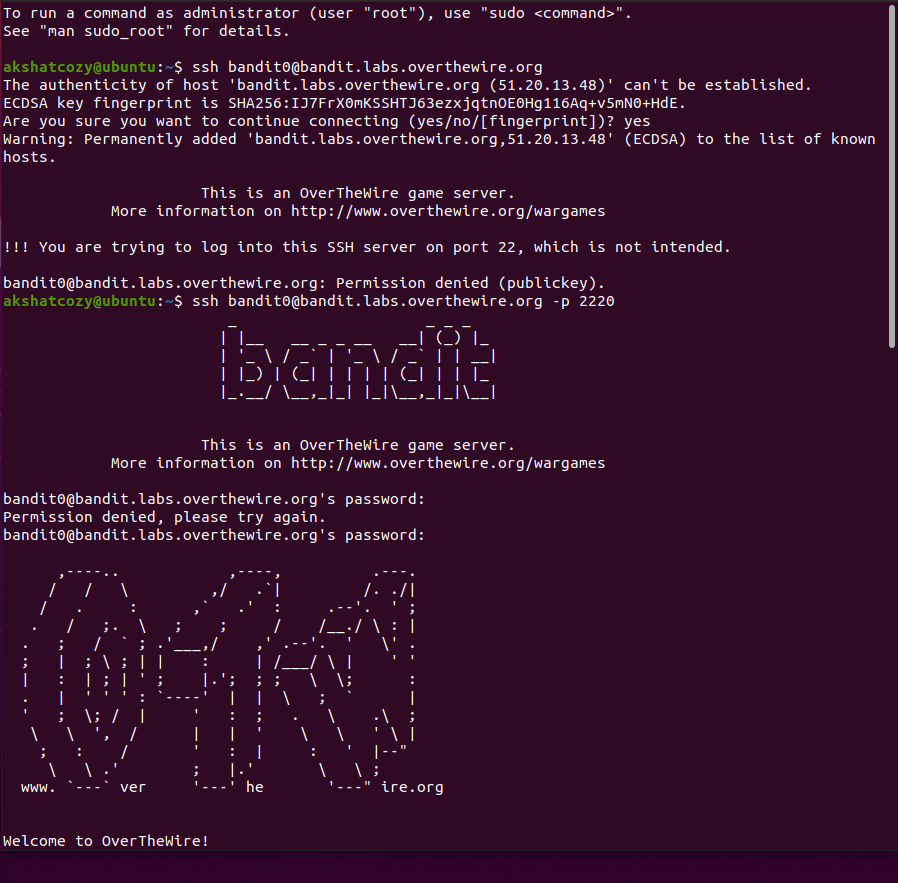
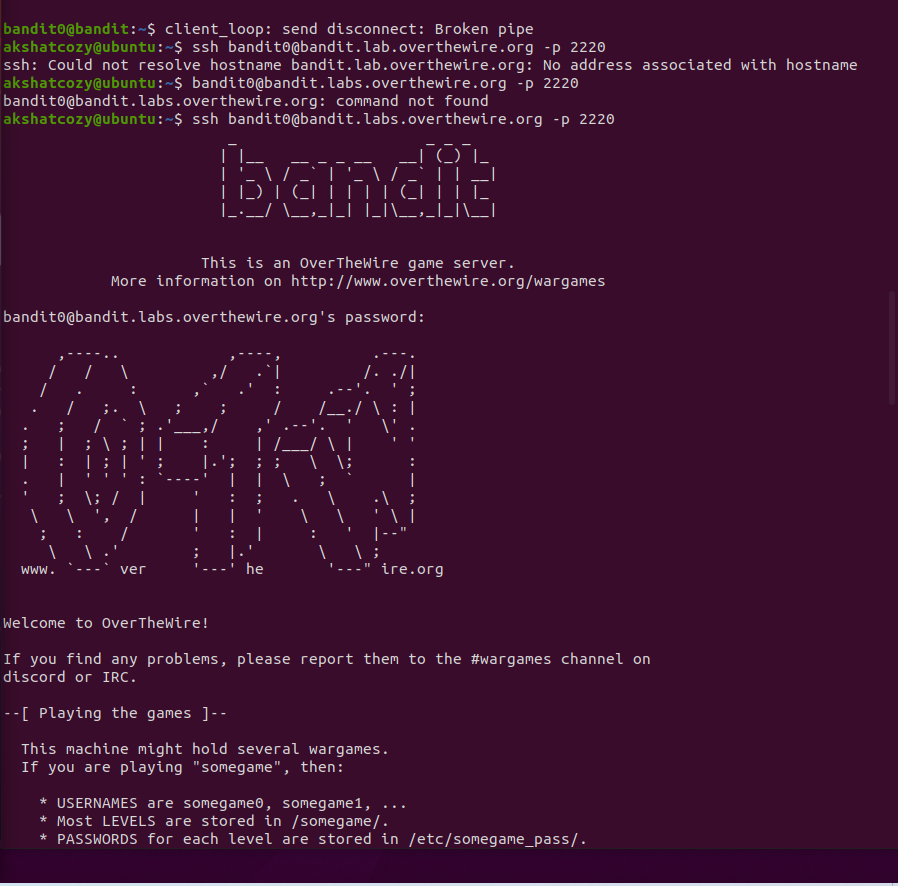
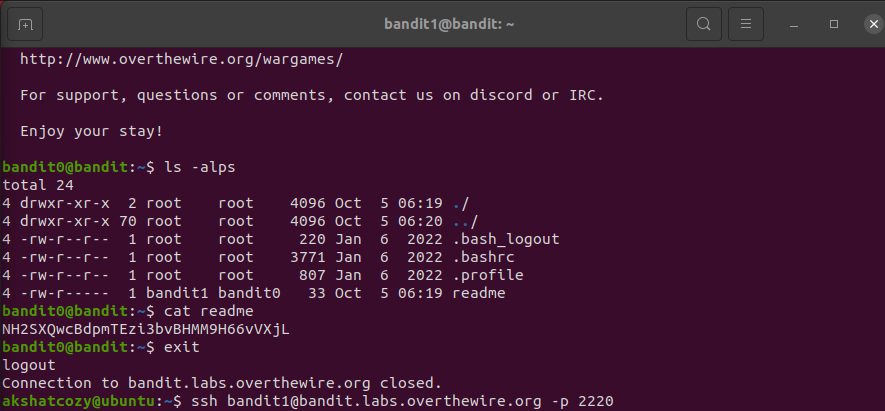
Writeup For BANDIT Wargame - Akshat Kumar – 230957098

LEVEL 0

1. Reading the materials on SSH and trying to understand how everything works.  
   
2. I did not understand how to set up a port and what it meant at first but I got it after that on my second attempt. I also failed to input the password correctly the first time as I was not aware the password is not visible while typing.



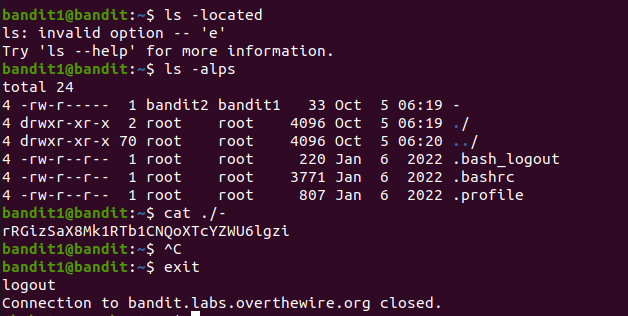
LEVEL 1

1. Disconnected and got broken pipe error. Reconnected to Level 0 after that.  
   
2. Learnt about all the mentioned commands such as ls , cat , cd , file , du and find to solve level one and got the password as follows.  
   ls -alps  
   cat readme  
   exit



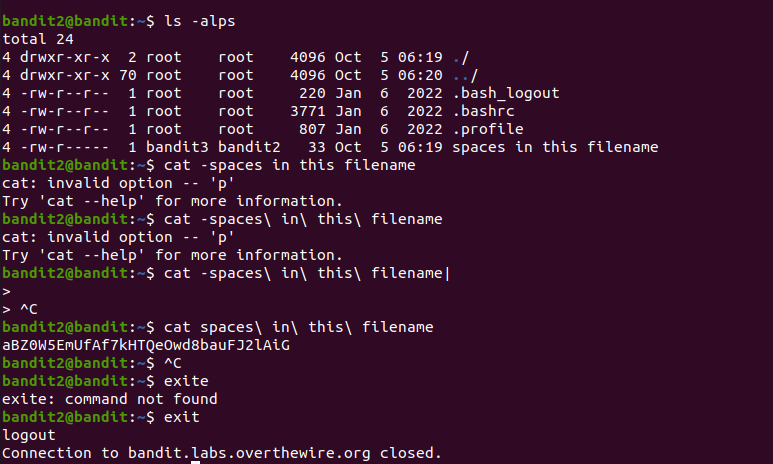
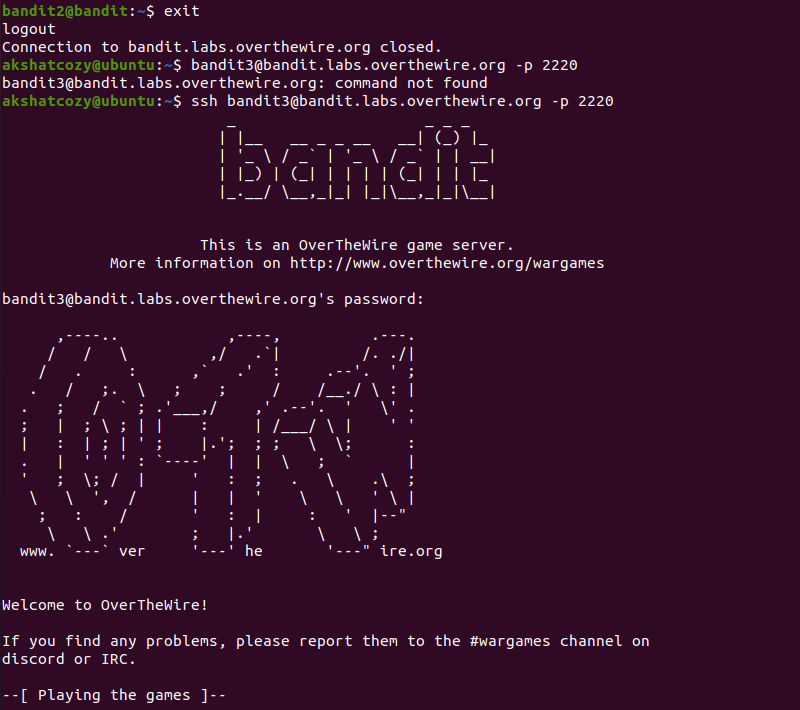
LEVEL 2

1. After level 1 I got confused as to what I have to search for. To which I thought I have to locate ‘ - located ‘ and did not realize that I was looking for ‘-‘ in the directory. After which I was able to log into level 2.

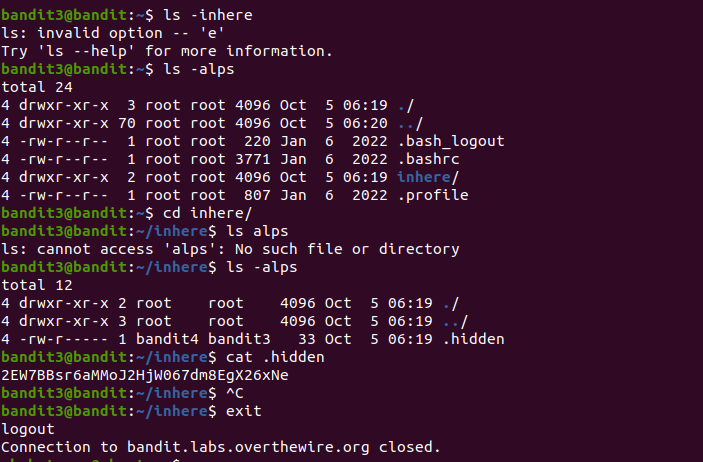
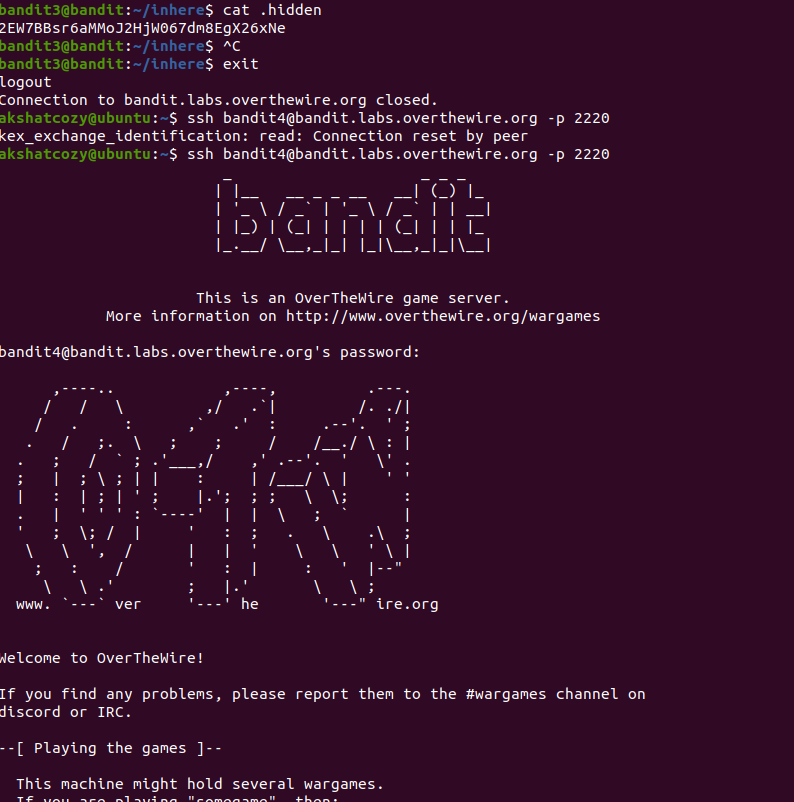




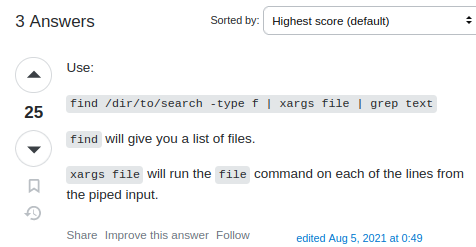
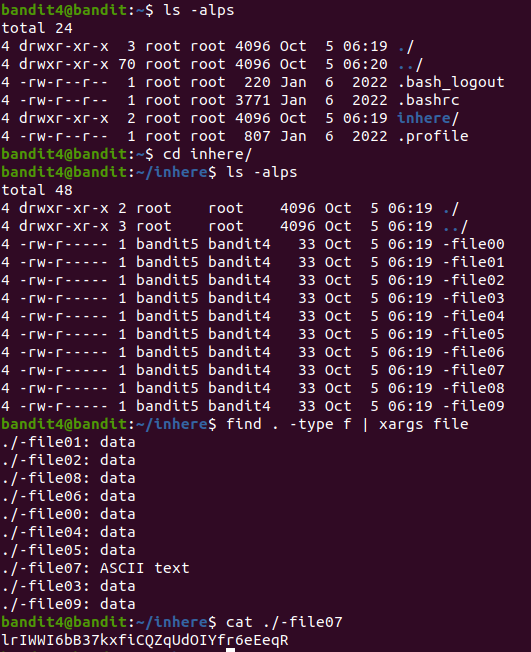
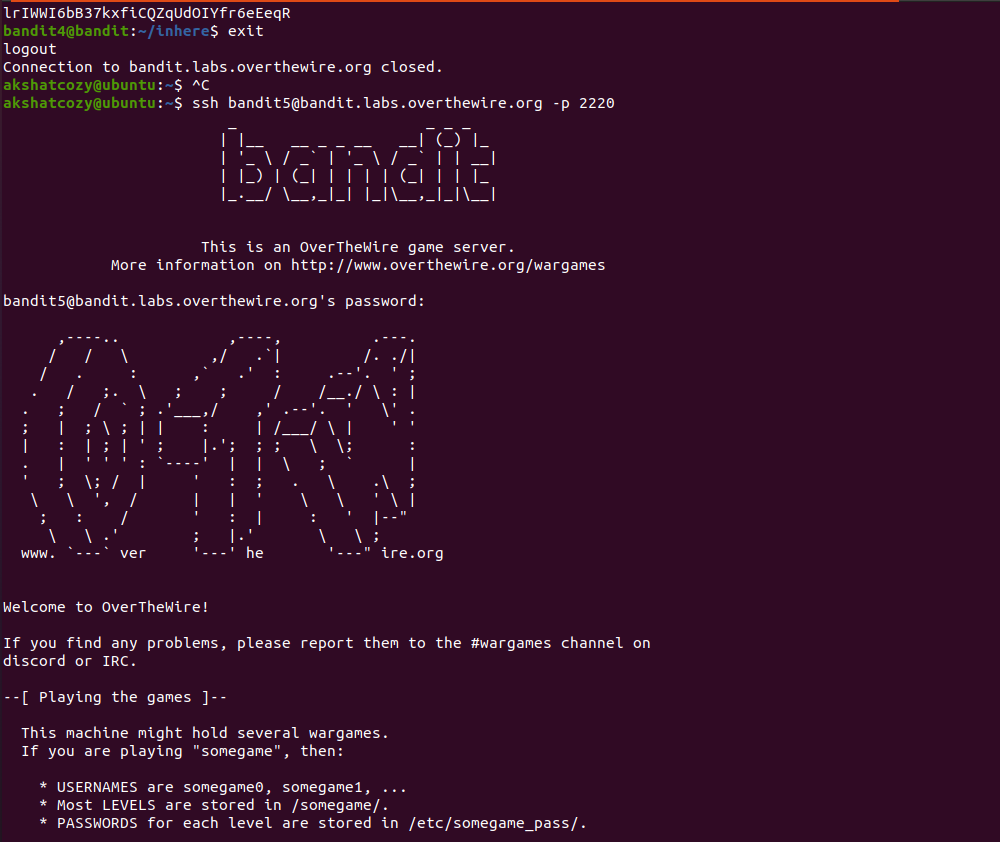
LEVEL 3

1. Tried a few methods of inputting an element which contained of spaces in the filename we were looking for in the directory.  
   
2. Got into Level 3  
   

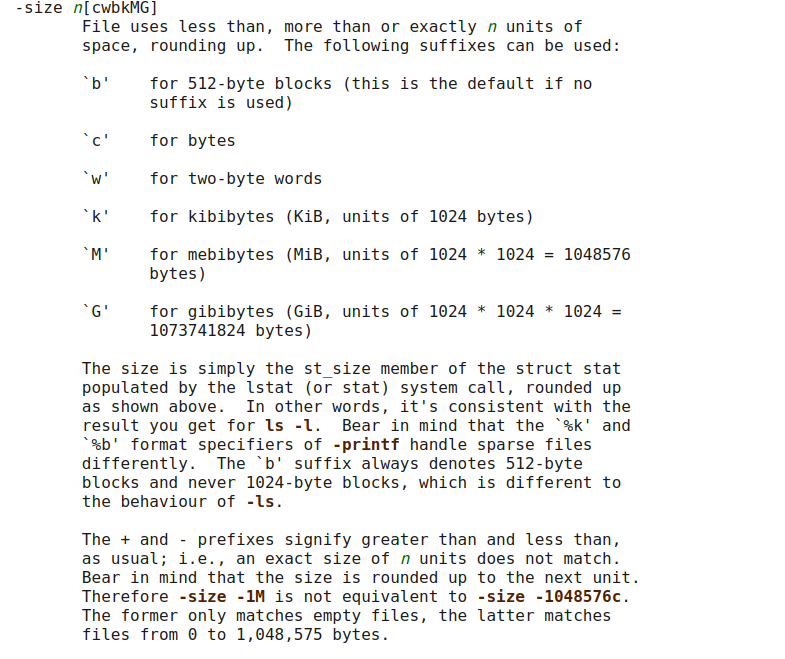
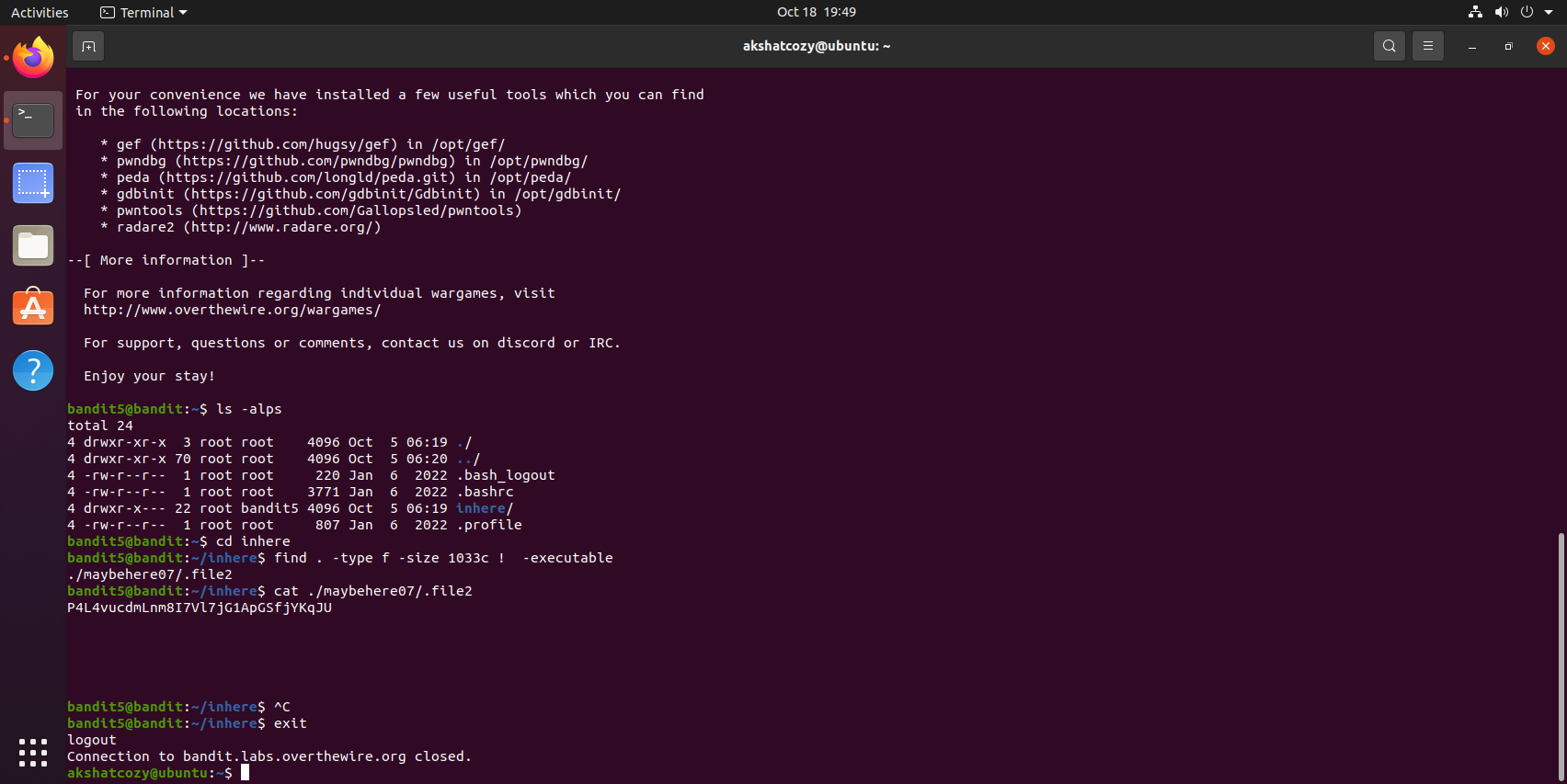
LEVEL 4

1. Learnt how to access directories that are inside other directories using cd and got the password.  
   
2. Got into Level 4  
   

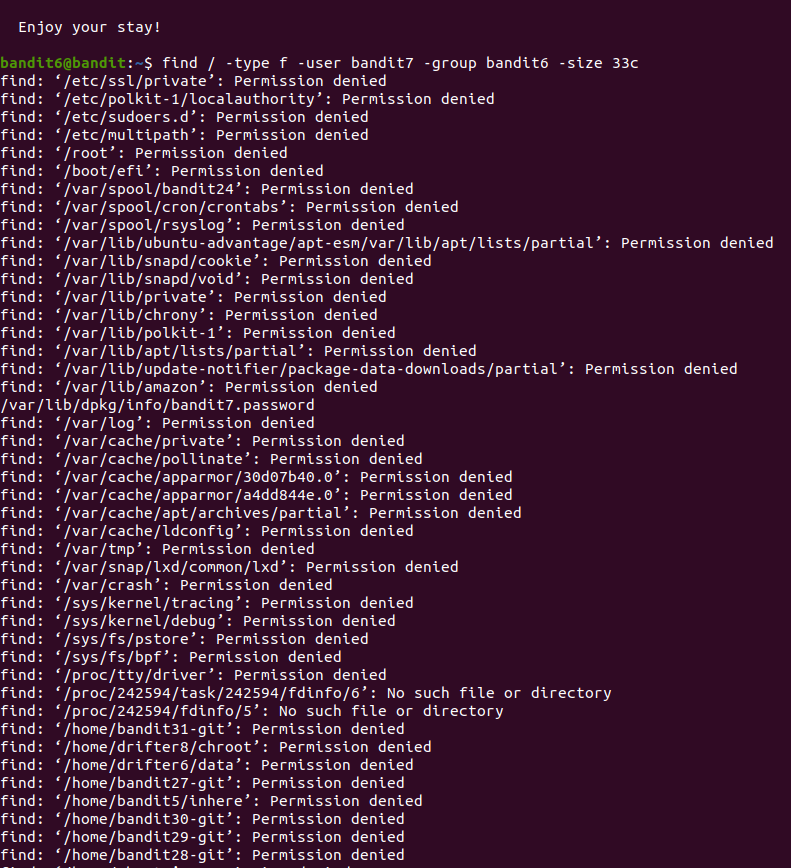
LEVEL 5

1. Tried reset command.
2. Looked online to find out how to see if a file is human readible or not.  
   
3. Used the data to cat file 7 as it was human readable in ascii text format.  
   
4. Got into level 5.  
   

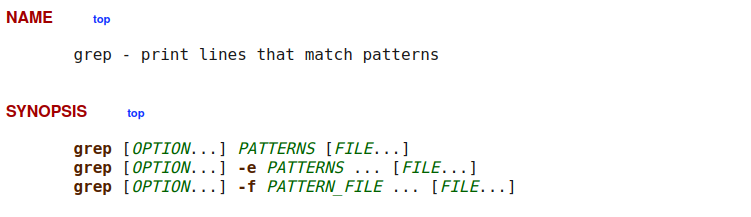
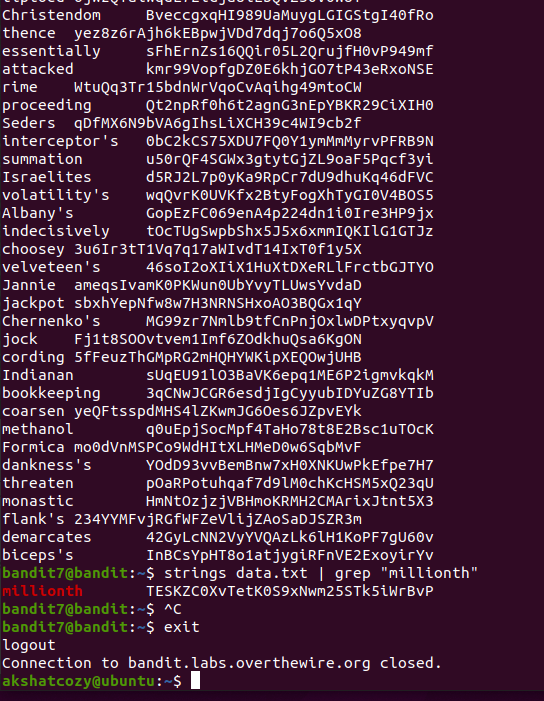
LEVEL 6

1. In Level 6 we have to sort using size of files in bytes…,  
   
2. , if it is not executable and that it is human readable. Using these two suffixes.  
   
3. Using the two commands I was able to shortlist down to only one file which would be my answer.  
   

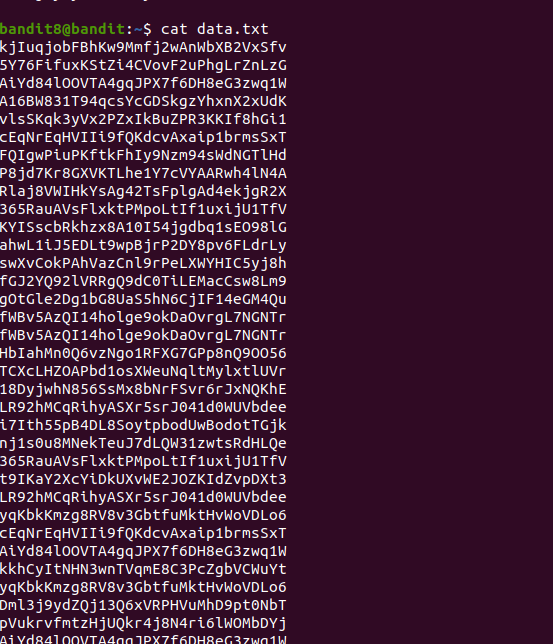
LEVEL 7

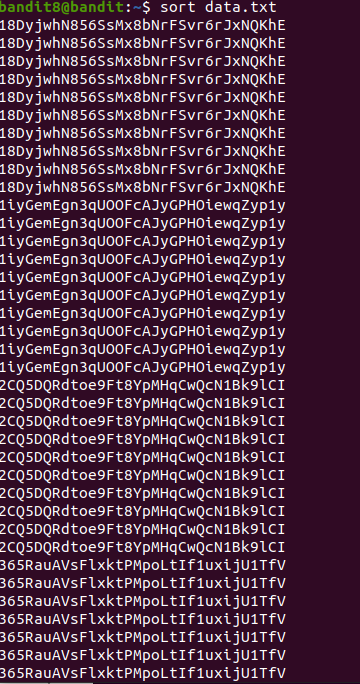
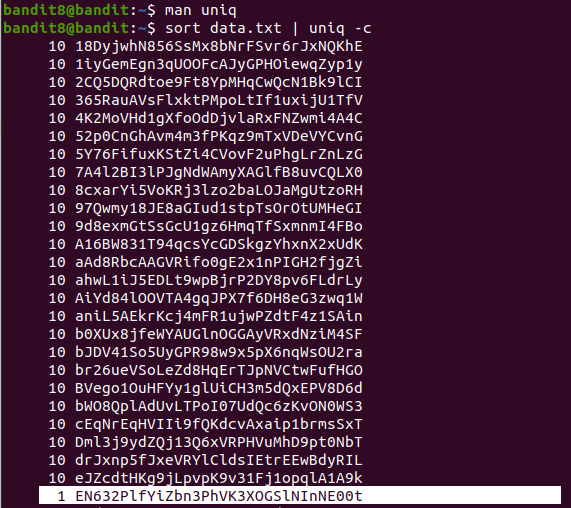
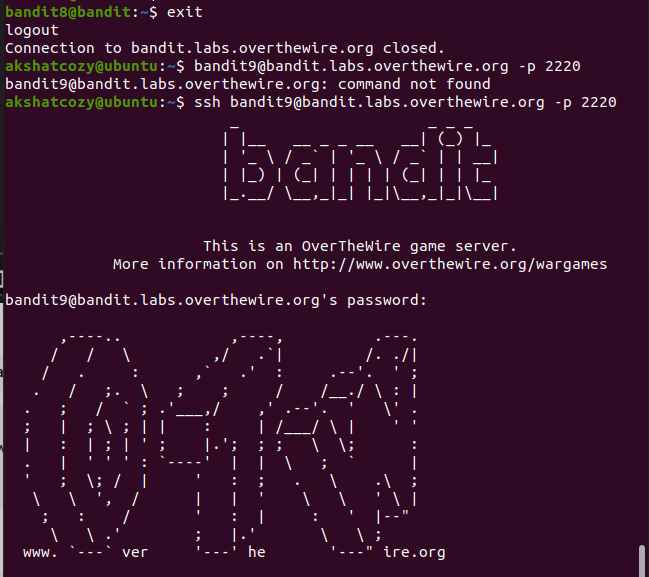
1. Using what I have learnt up until now I was able to find the password file.  
   
2. 😉😉😉  
   
3. NICEE LEVEL inside level 7.  
   

LEVEL 8

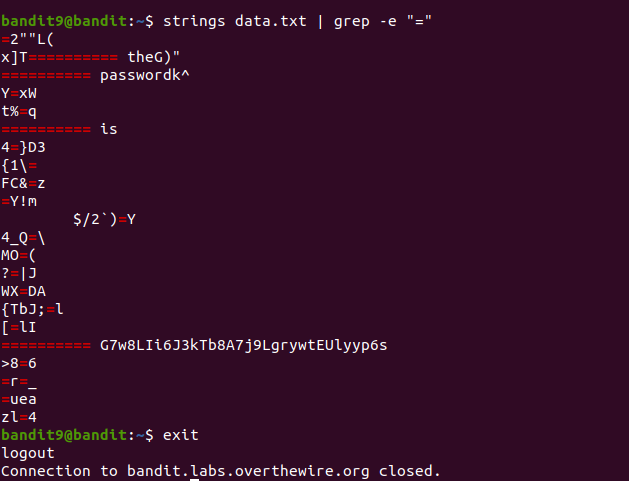
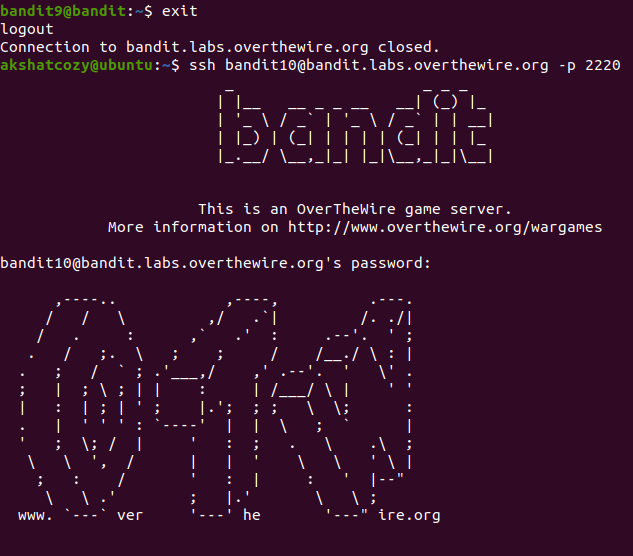
1. Learnt about grep command for this level.  
   
2. Found password for Level 8.  
   
3. Logged into Level 8.  
   

LEVEL 9

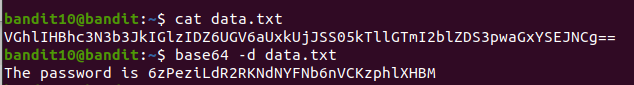
1. Searching the entire car data to interpret the question better.  
   

1. Sorting all the data in the given list.  
   
2. Using uniq condition for count condition to find the single right option.  
   
3. LEVEL 9 unlocked.  
   

LEVEL 10

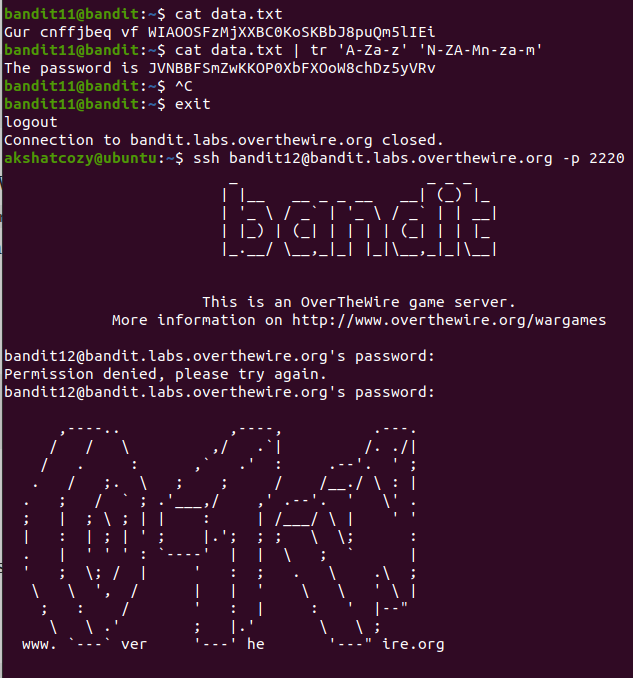
1. Learnt usage of grep (Use PATTERNS as the patterns. If this option is used multiple times or is combined with the -f (--file) option, search for all patterns given. This option can be used to protect a pattern beginning with “-”.  
   
2. Got into LEVEL 10 😊  
   

LEVEL 11

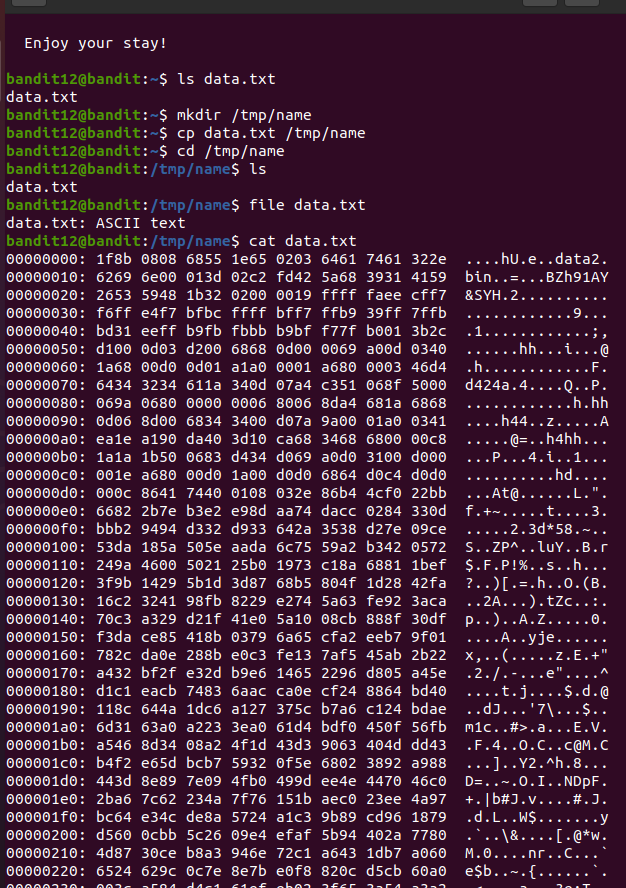
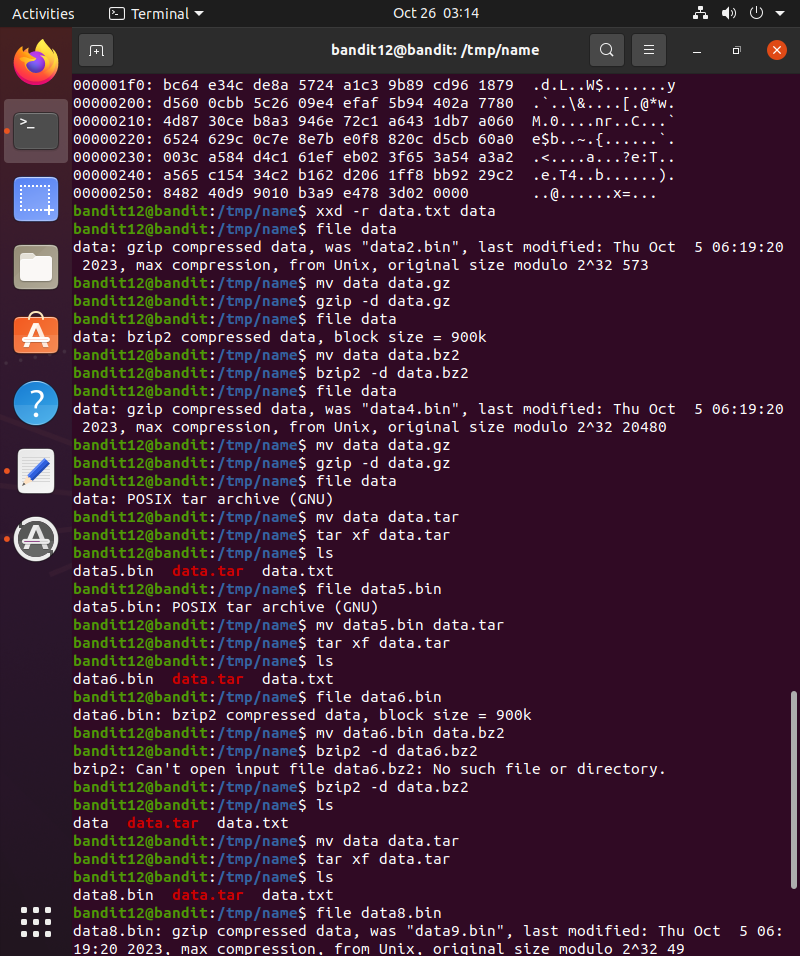
1. Decoded base64 encoded data to obtain the password.
2. Got into bandit LEVEL 11.

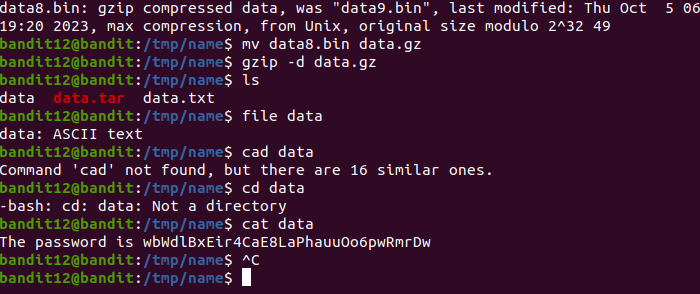


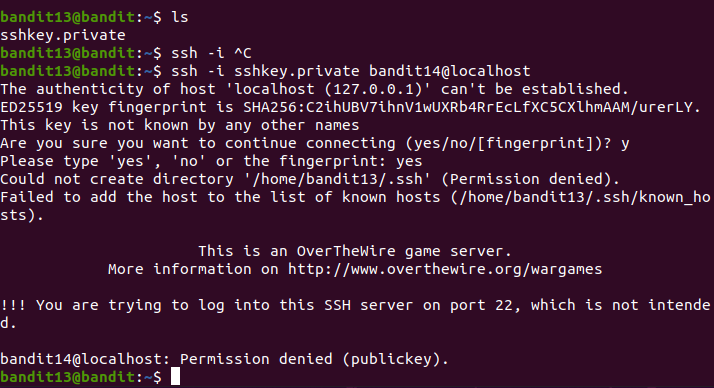
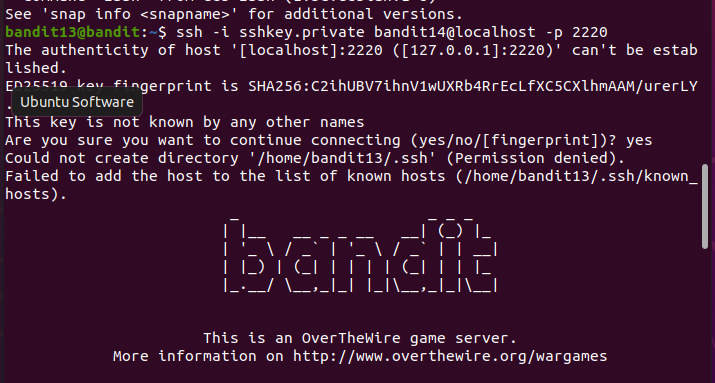
LEVEL 12

1. After translating the letters according to the given conditions I got the desired password for LEVEL 12 :P  
   

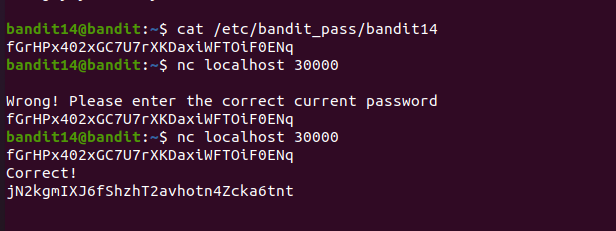
LEVEL 13

1. Made a temporary directory to see the txt in the given hexdump and using xxd afterward to change from .txt to a file.  
   
2. After a series of decodes and extract files from tar gzip and bzip2 formats I reached the ascii text hence the password.  
   

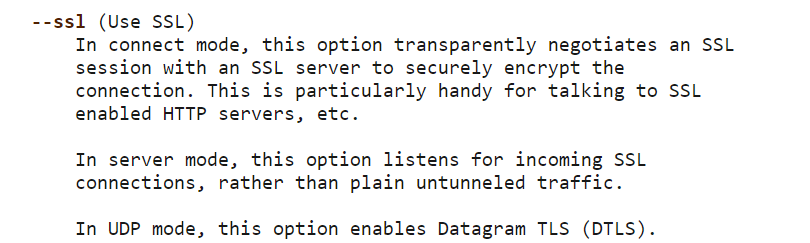
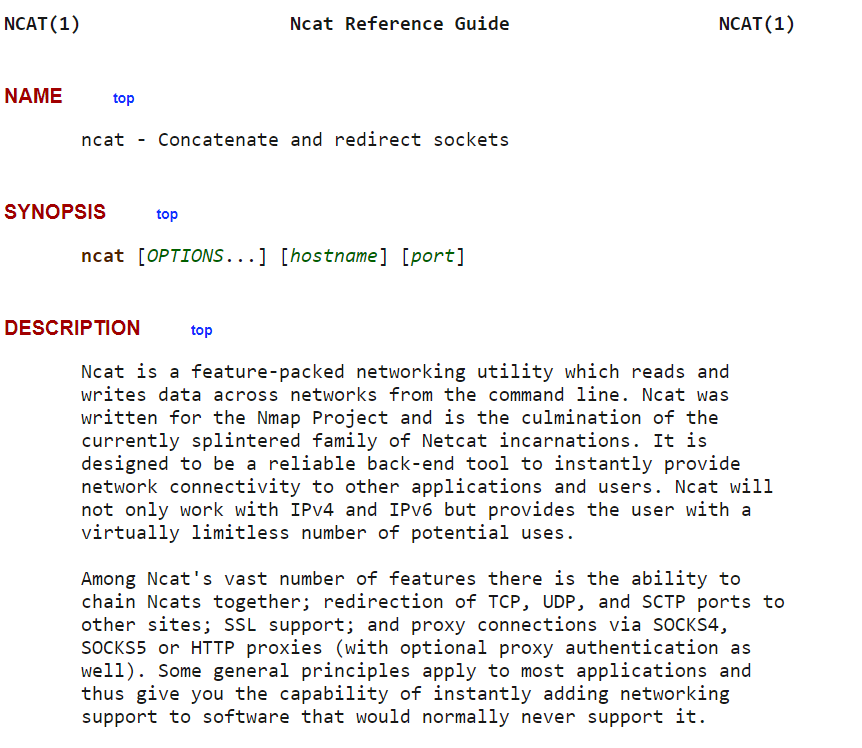
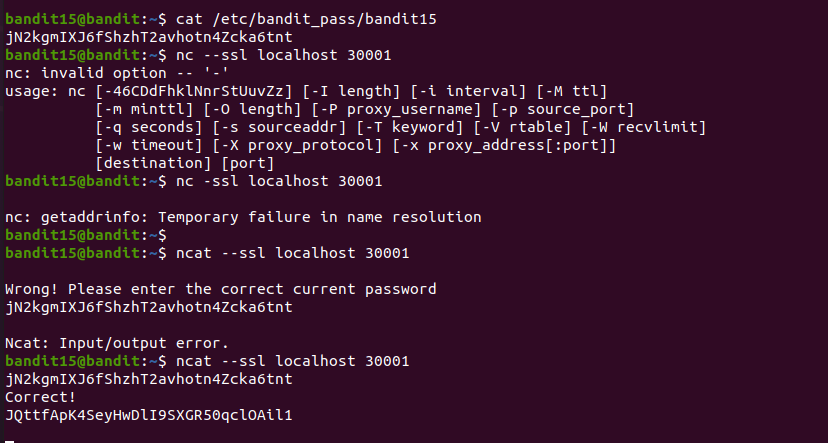
  
  
  
  
  
LEVEL 14

1. I was confused why the SSH command was not working and showing error even after inputting all the value correctly.   
   
2. It was a port issue which I fixed and got into level 14.  
   

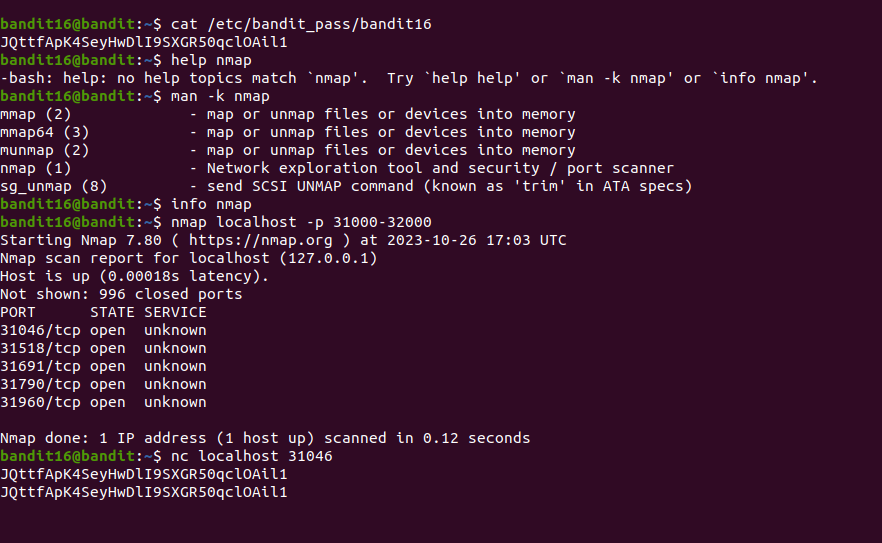
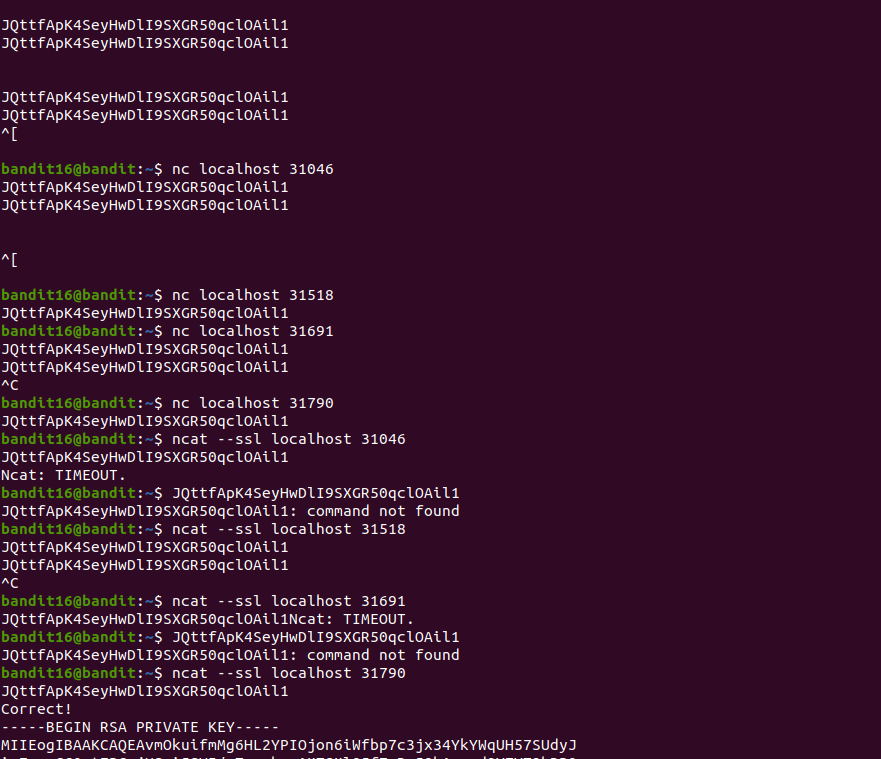
LEVEL 15

1. Learning netcat commands and using it to get password to level 15.  
   

LEVEL 16

1. Using Ncat with SSL server option.  
   
2. Using level password for current level as the key I was able to get the new password.  
   

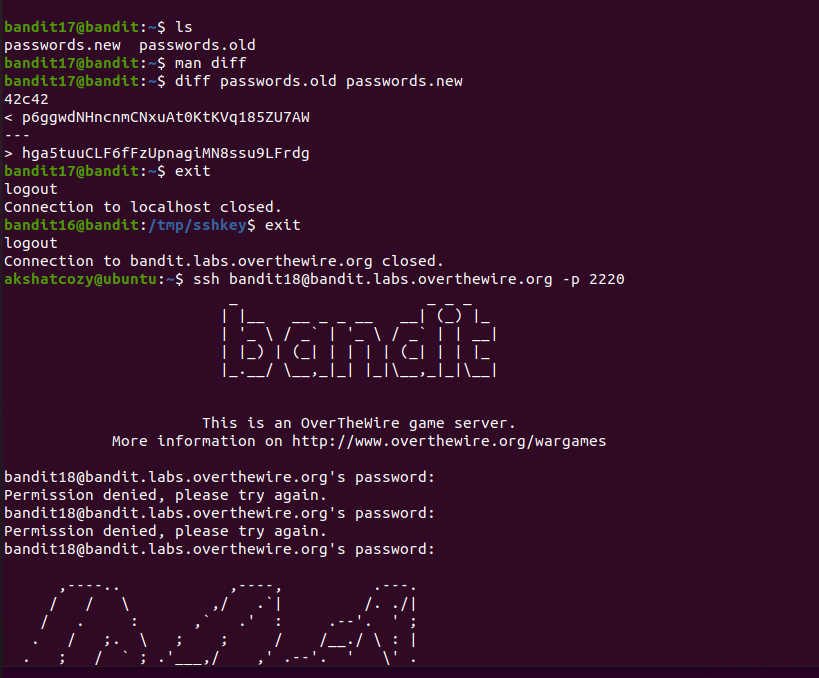
LEVEL 17

1. Mapped all possible files using NMAP and then proceeded to use Netcat for the RSA private key.  
     
   

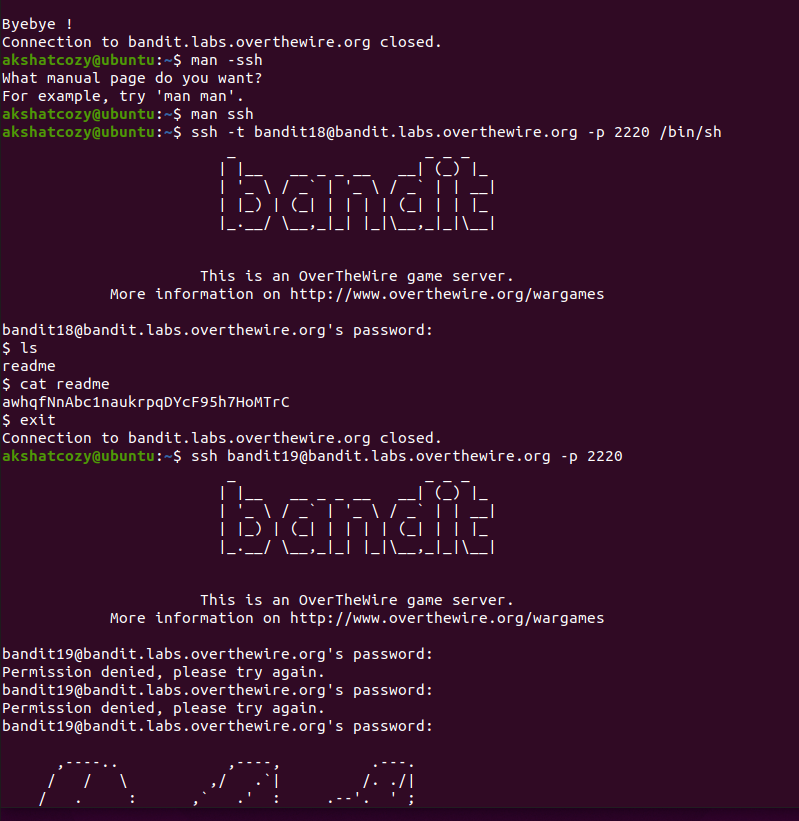
1. Used MKDIR, touch, vim, chmod to set conditions to use the key and then logged in to level 17.



LEVEL 18

1. Used the diff operator to find the difference between 2 passwords in the directory.  
   

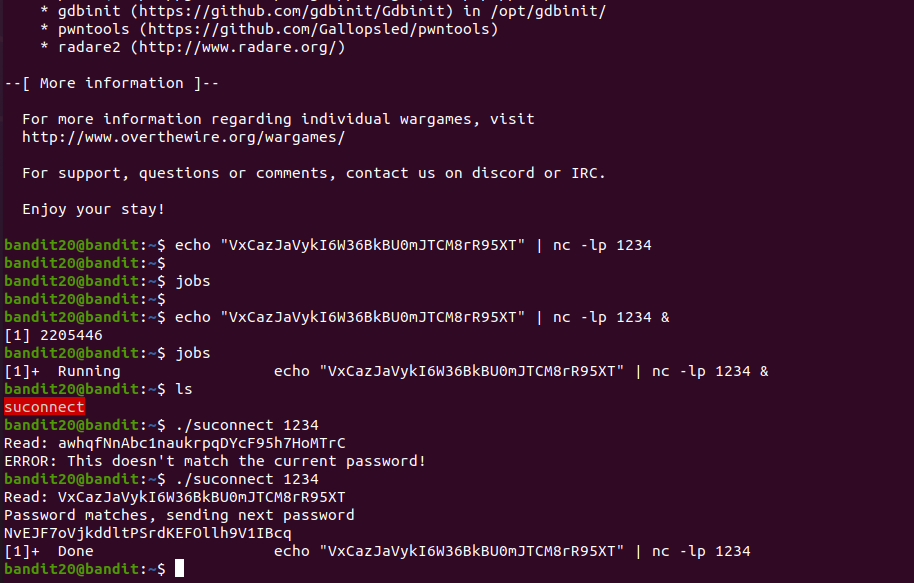
LEVEL 19

1. Used SSH to get password from level by getting remote login as directly logging in just kicks us out of the server.  
   

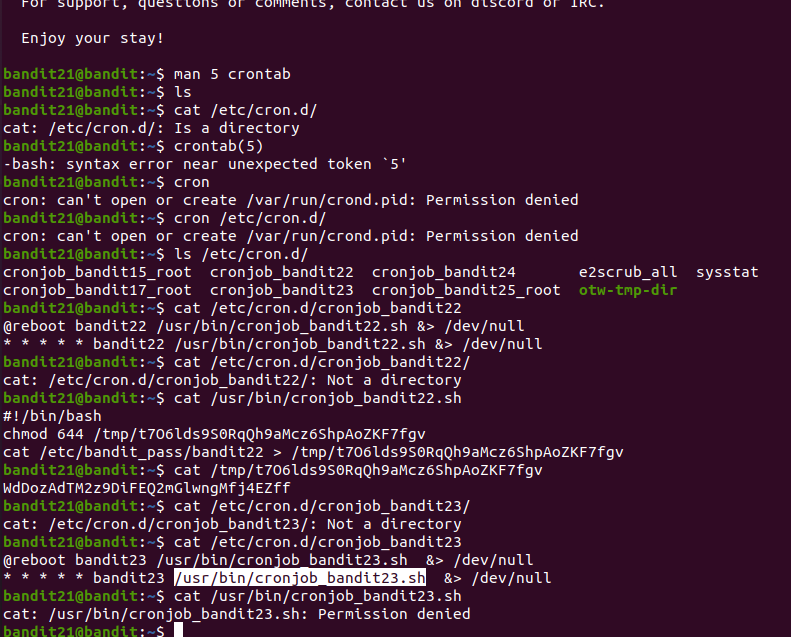
LEVEL 20

1. Navigating euid bandit 20 for getting the password.  
   

LEVEL 21

1. Used echo and a user id to return the password to the user id hence unlocking the next level.  
     
   

LEVEL 22

1. Learning cron commands and navigating through cron.d for password.  
   

LEVEL 23

1. First using cron subtype we get to echo “copying password file…. “ . Which I use as a base format to input the required parameters like $myname. Which resulted in the password for the level 23.  
   