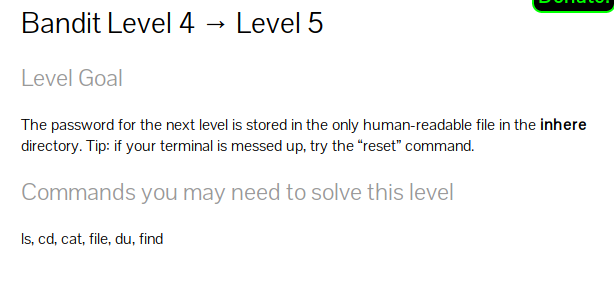
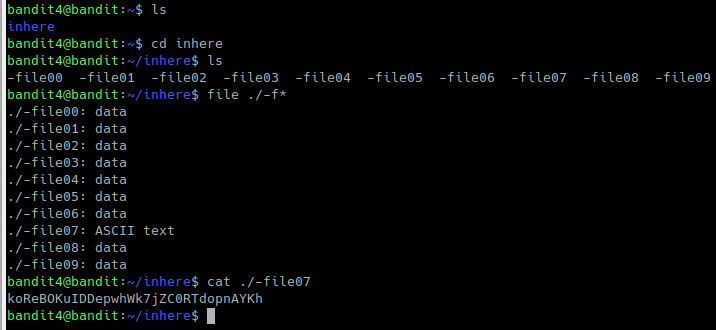


ls -a : a stands for all shows entries that starts with ‘.’ which are generally hidden

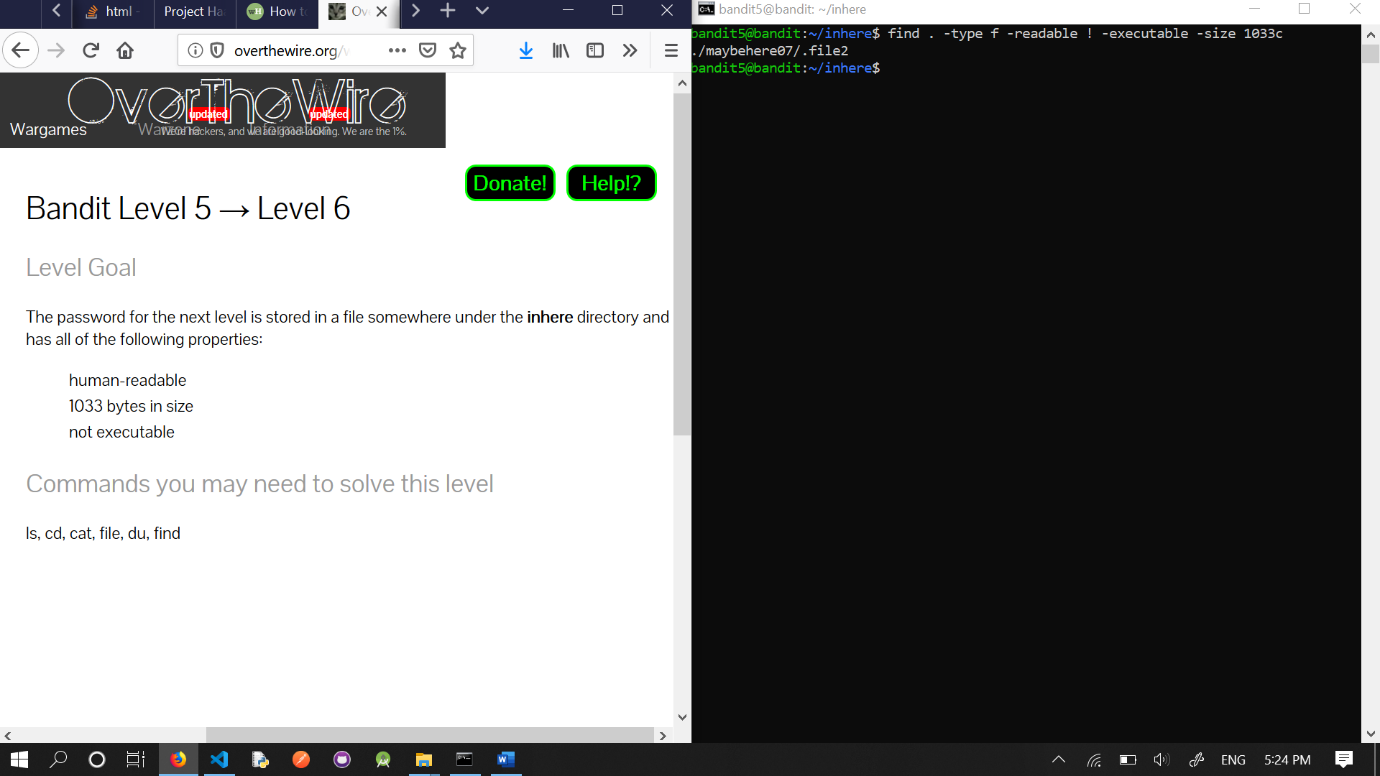




file \* lists the data types of all the files but since the file name starts with ‘-f’ \* will give ‘ ile00 ‘ instead of ‘ -file00 ‘ and so on therfore giving the wrong output.

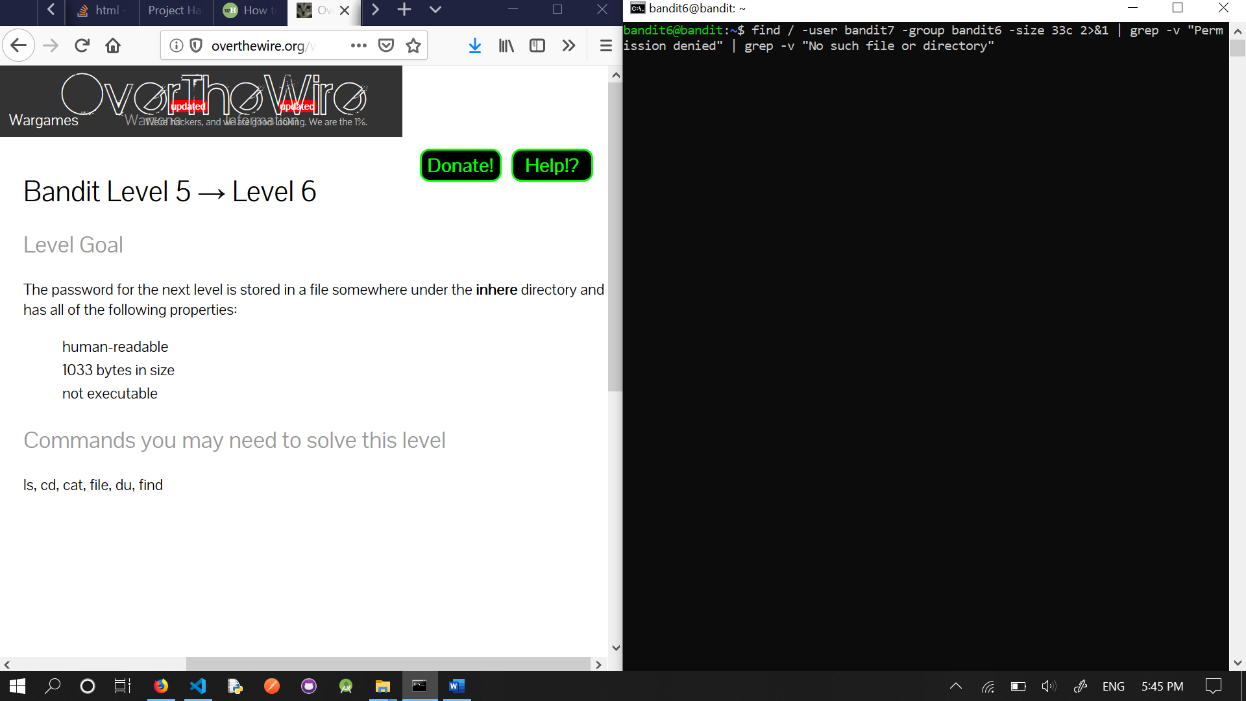
To overcome this we use ./-f\*

Level 5  Level 6



* -readable flag indicates file is “human readable” form
* ! executable because the file should not be executable :p
* -size 1033c indicating file size specified by the problem statement.

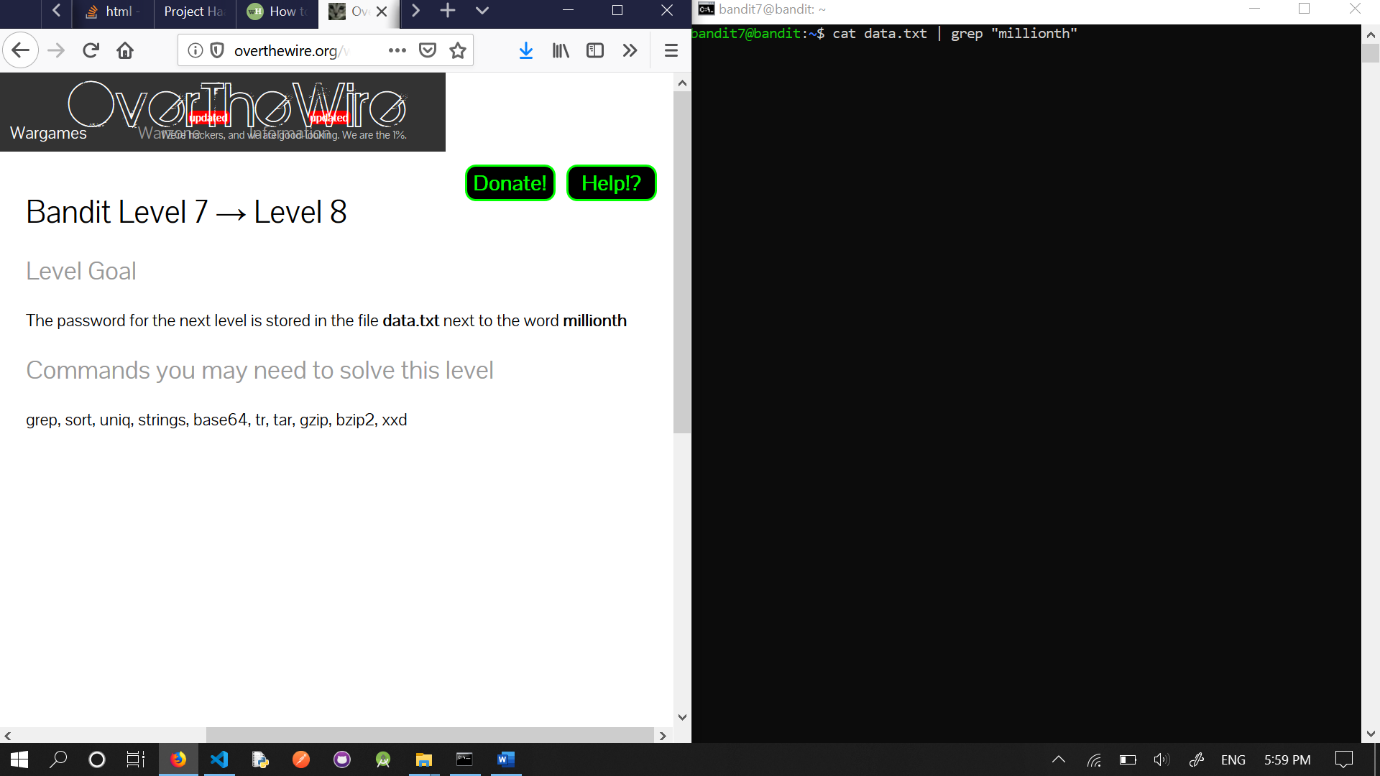
Level 6  Level 7

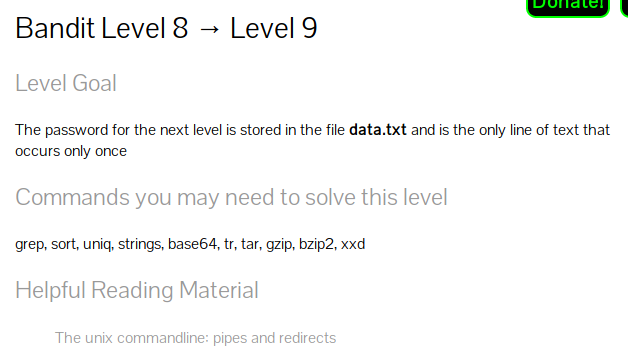


* -user, -group, -size to search for the specified user, group and file size.
* 2>&1 : basically redirect any stdout message which is an error message of type “Permission denied” or “No such file or directory” to stderr.
* The file containing password is the only file without the above mentioned errors.

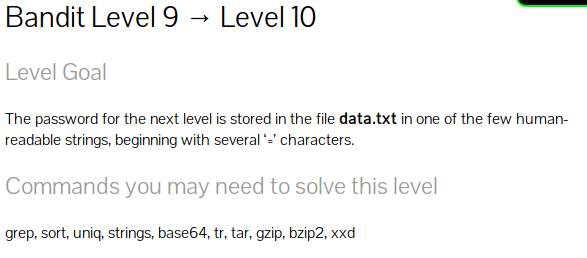
Level 7  Level 8

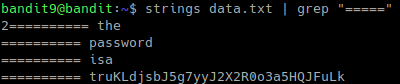
grep is a command line utility to filter text with the help of regular expressions

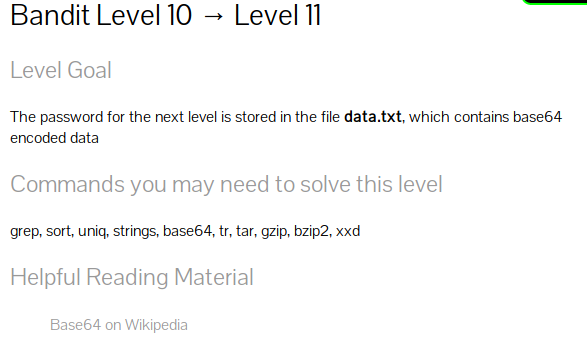


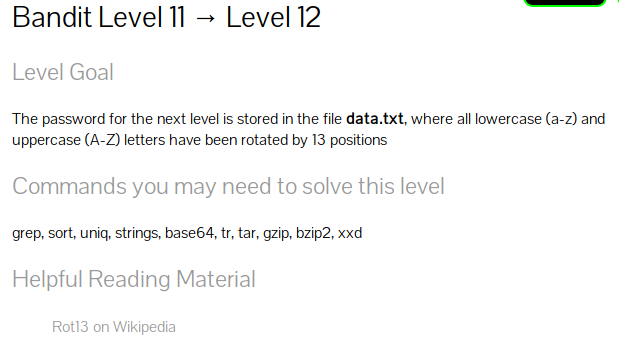








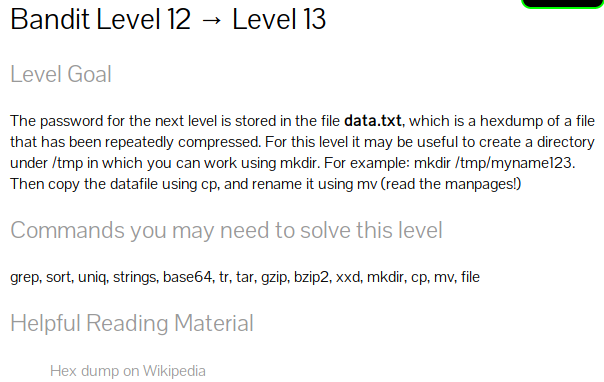


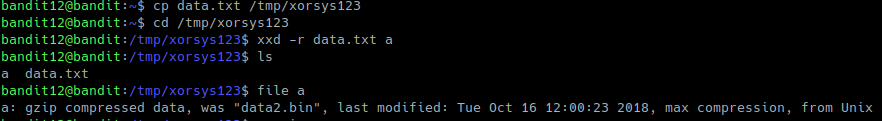


tr converts elements from one set to another

[a-zA-Z] makes a set of lowercase+uppercase in normal order

[n-za-mN-ZA-M] makes a set shifted by 13 digits

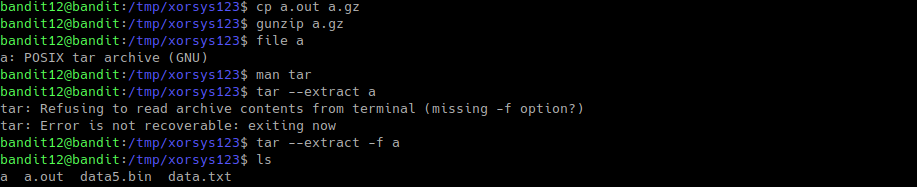
for this question we have to reverse engineer our file by finding out the type at each step and extracting them

to extract using gunzip you need to rename to the proper extension

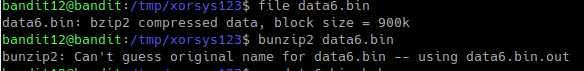






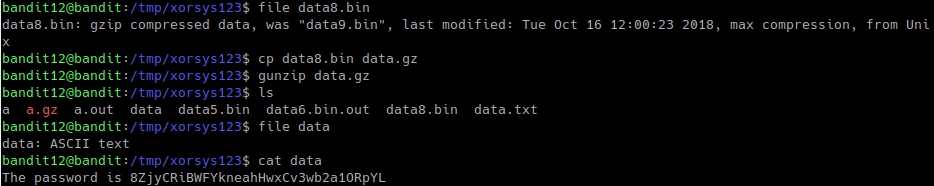


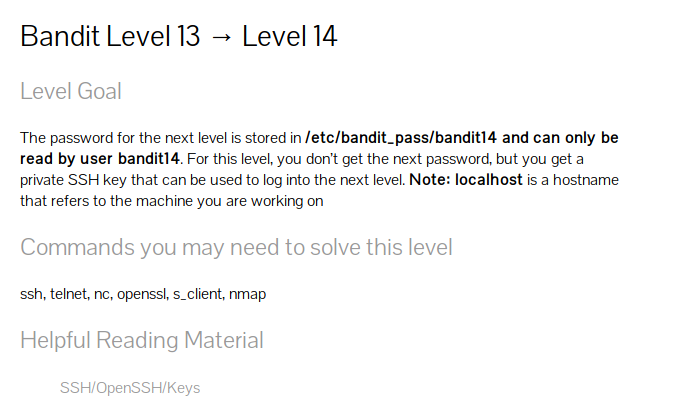








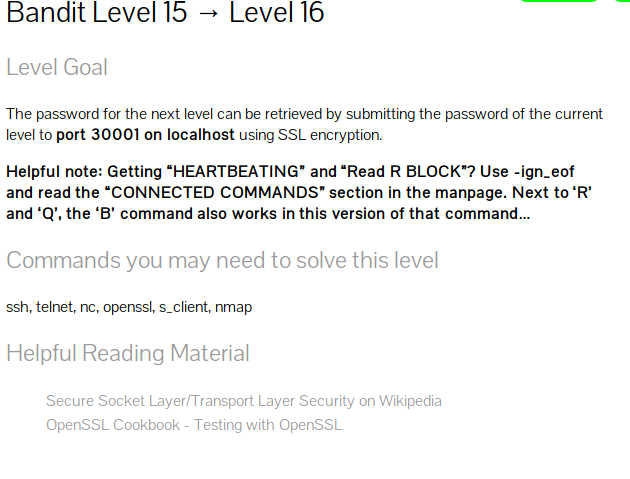
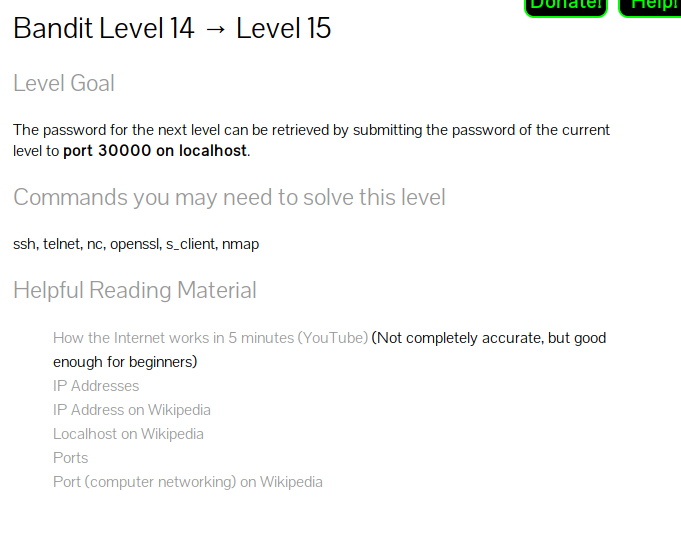
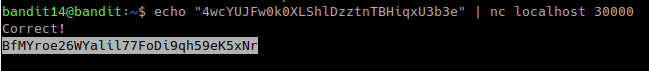






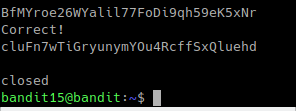


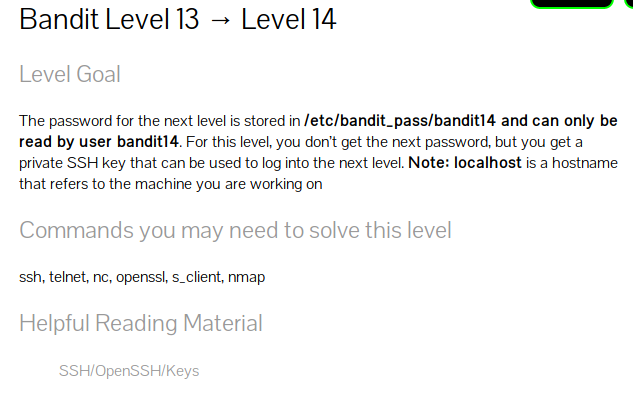
the password is only accessible by the bandit14 user therefor we need to use the bandit14 account which can be done by connecting to it using the private key.





After connecting, input password of the previous problem.





Use command

nmap -p 31000-32000 localhost

to find out the open ports

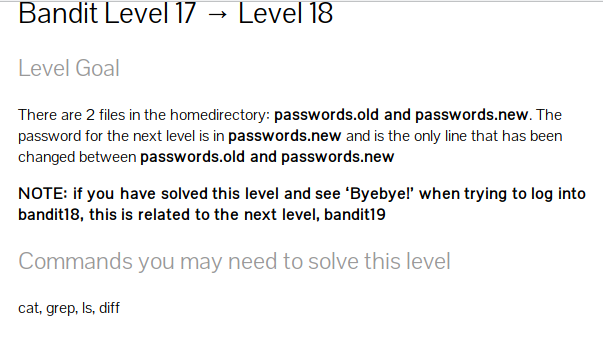
use openssl to connect to the port and put in the current password like we did in an earlier problem

you will get a rsa key. Copy and paste that rsa key onto your pc and use

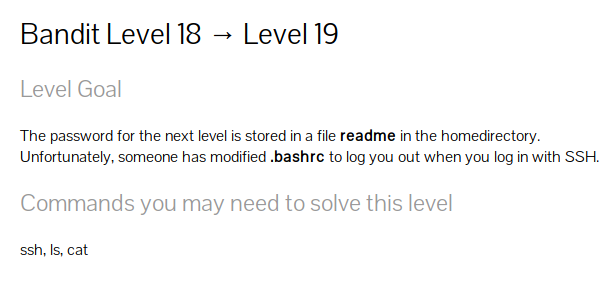
chmod 400 rsa\_key //to change permissions

ssh -i rsa\_key bandit17@bandit.labs.overthewire.org -p 2220

cat /etc/bandit\_pass/bandit17 // to get the flag

  
diff -q passwords.old passwords.new

the second string is the flag as it is in passwords.new

you will be logged out too quickly to do anything in bandit18

so to overcome this, we need to send a command as soon as the computer logs us in

we use echo to pipe our command to the server

echo "cat readme" | ssh  bandit18@bandit.labs.overthewire.org -p 2220