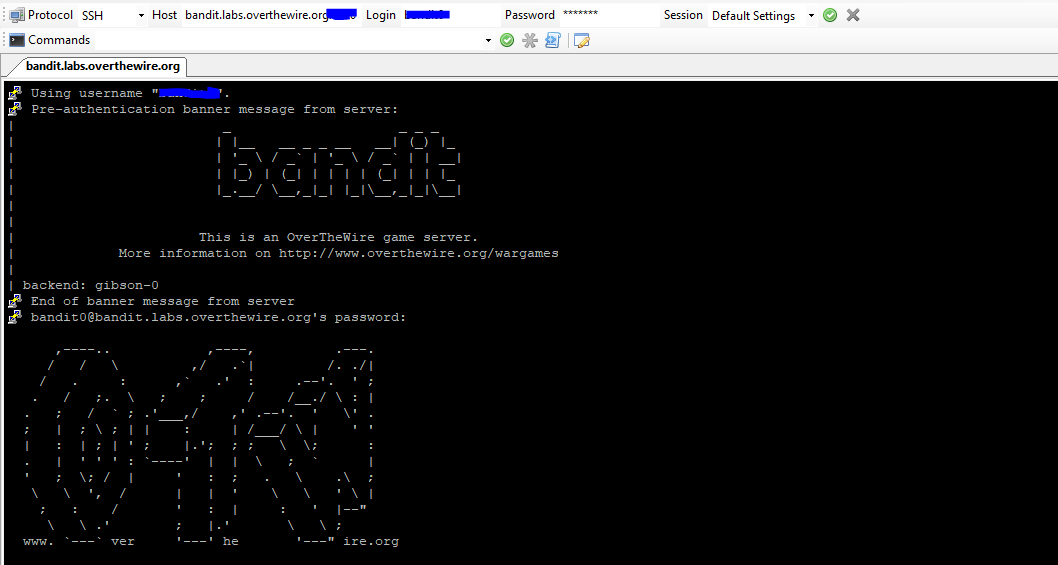
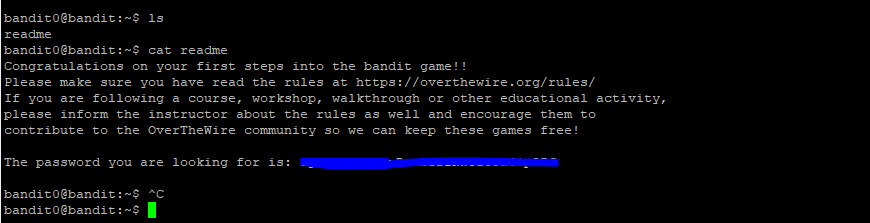
Level 0:-

Just SSH into overthebandit server with username, password domain name and port



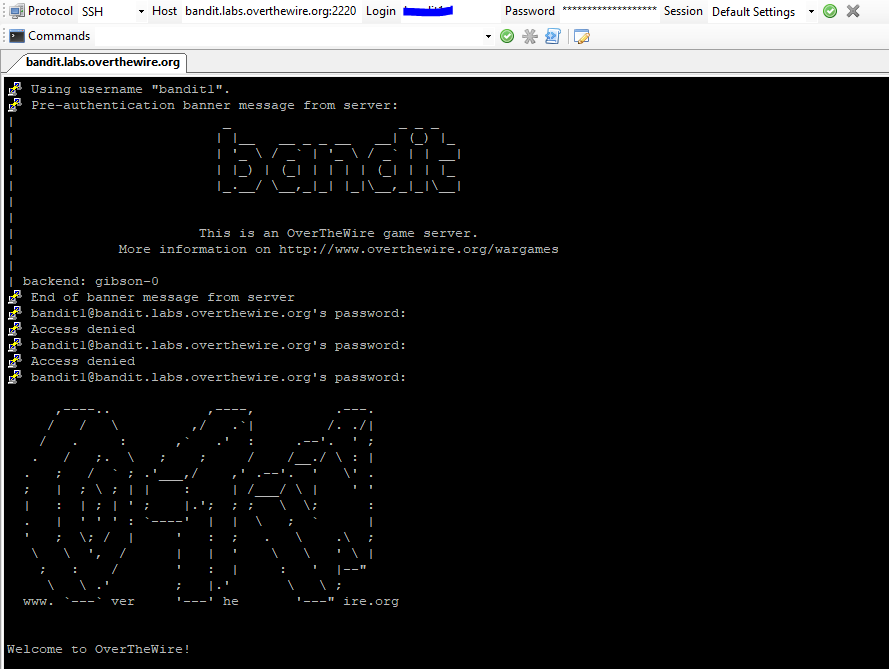
L0

Open the readme file and copy the password to a secure location on your local machine.



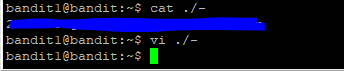
L0 -> Level 1:

Login to a new session with the password from the old session you got from the readme file.



Level 1 -> L2 :-

This level is about a unique file name which starts with a special character “-“ i.e hyphen. So how do you open this? This is a dashed filename.



Level 2 -> Level 3:-

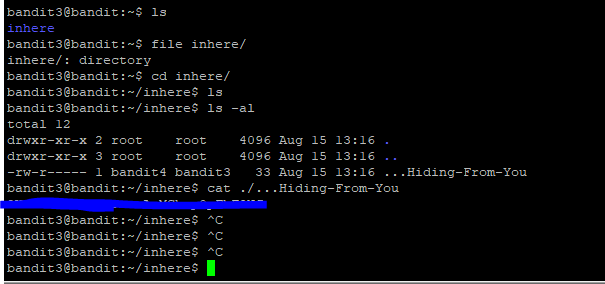
How do you open a file which has spaces between it?

You type/copy the filename till the first space and press tab till you have reached your target file.



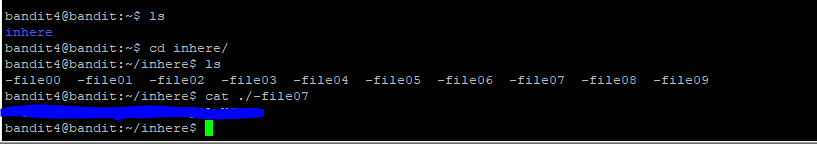
Level 3 -> Level 4:-

The file is a hidden file inside a directory so you open the directory. When you do a simple **ls** you do not see anything because all the files are hidden. So you use **ls –al** which will show you all the files.



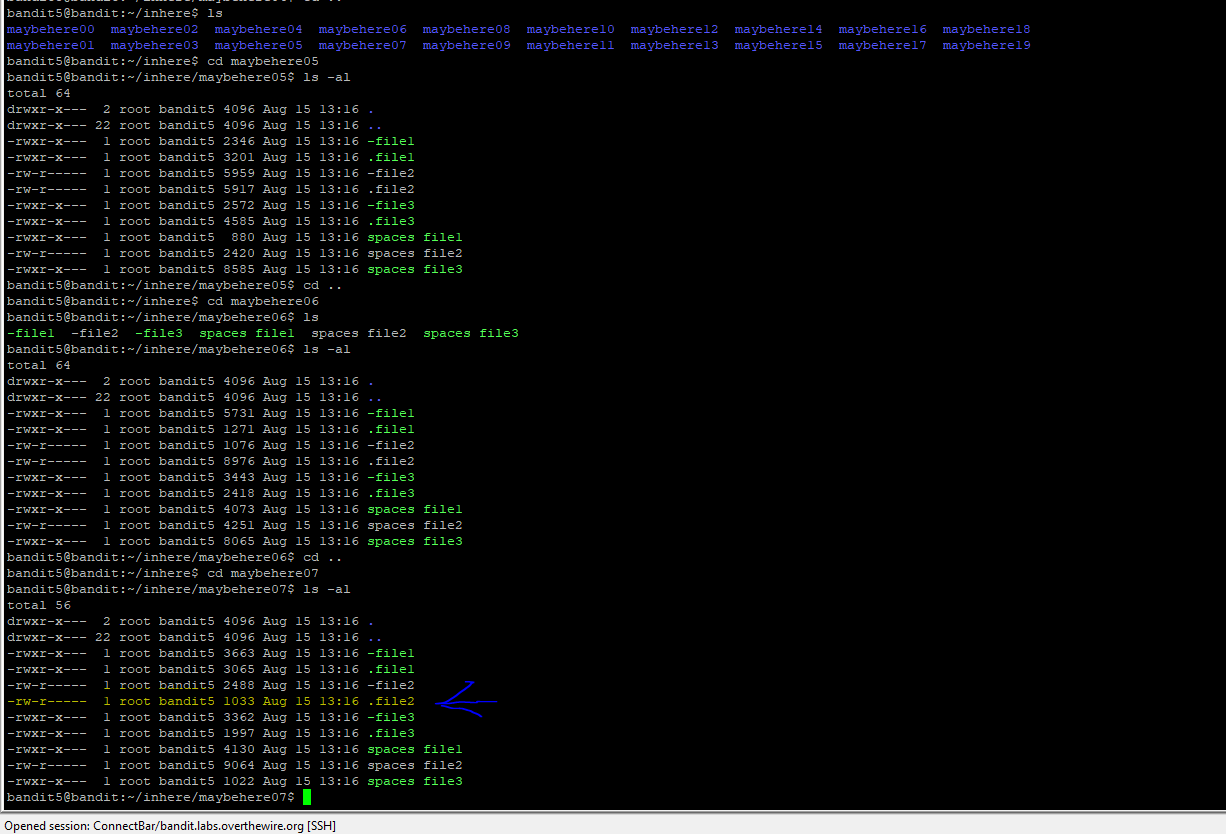
Level 4 -> Level 5:-

The file 07 is the only file which is in ASCII readable format so it has the password for the next level.



Level 5 -> level 6

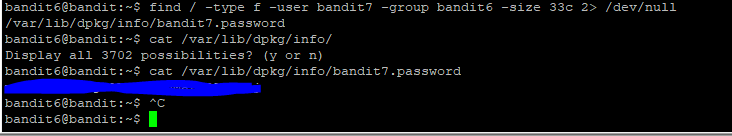
After a lot of effort I was able to find the correct file. I just looked at the size of the file I had to find out about.



Level 6 -> Level 7:-

This took some significant time. But a simple google search showed me how to get the solution.

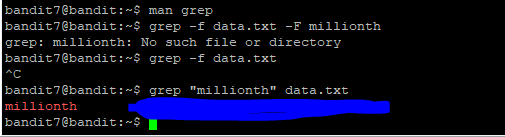
**find / type –f –user bandit7 –group bandit6 –size 33c 2> /dev/null**



Level 7 -> Level 8:

**Grep “millionth” data.txt**

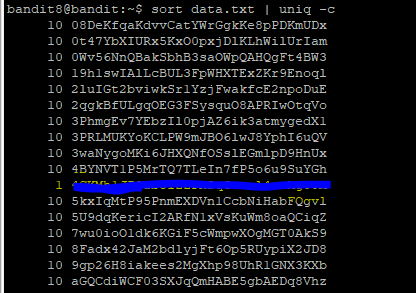
This was very easy as well.



Level 8 -> Level 9

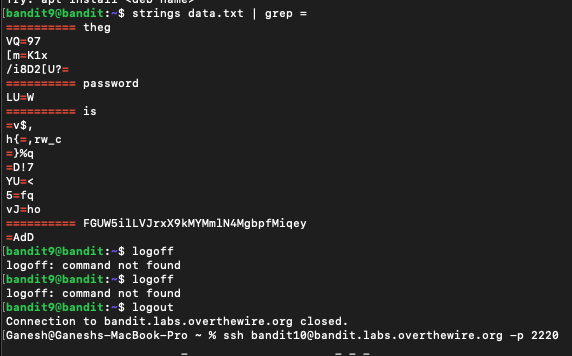
A simple sort cmd pipelined into a uniq command gives the only line with the password. This was pretty easy and simple

**Sort data.txt | uniq -c**



Level 9 -> Level 10

This was a bit tricky as I initially tried using base 64. Eventually after I tried using strings cmd I was able to decode the script and get the correct password which has many appending “=”. We basically have two sets of strings which come close to the password. I have to try out both and see which one is the correct password.



Level 10 -> Level 11

This was pretty easy and simple again. I just had to run the base64 command and decode it, that gave me the password for the next level.

