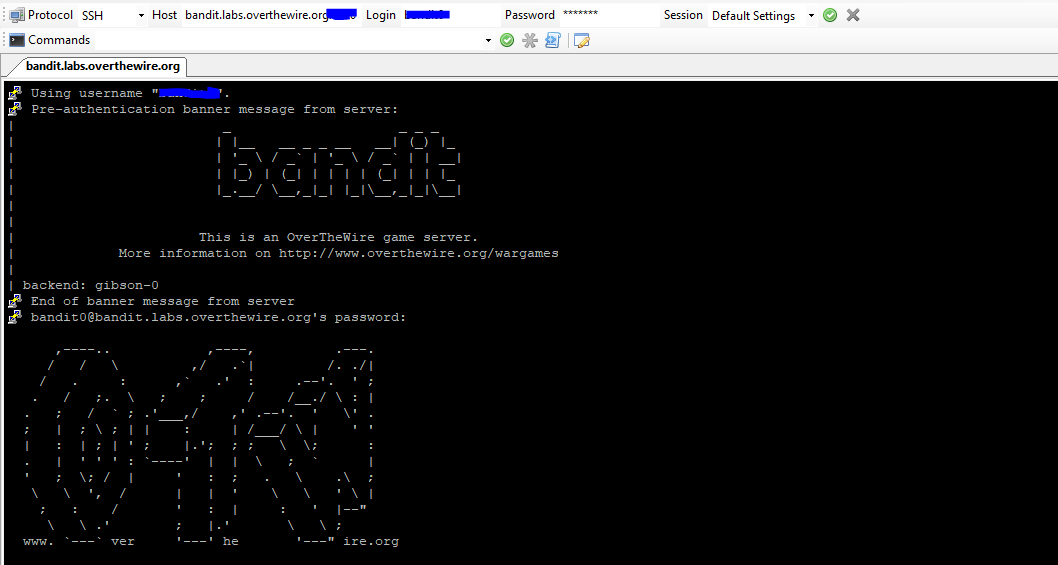
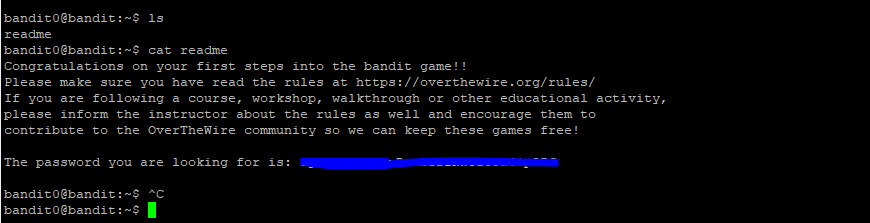
Level 0:-

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



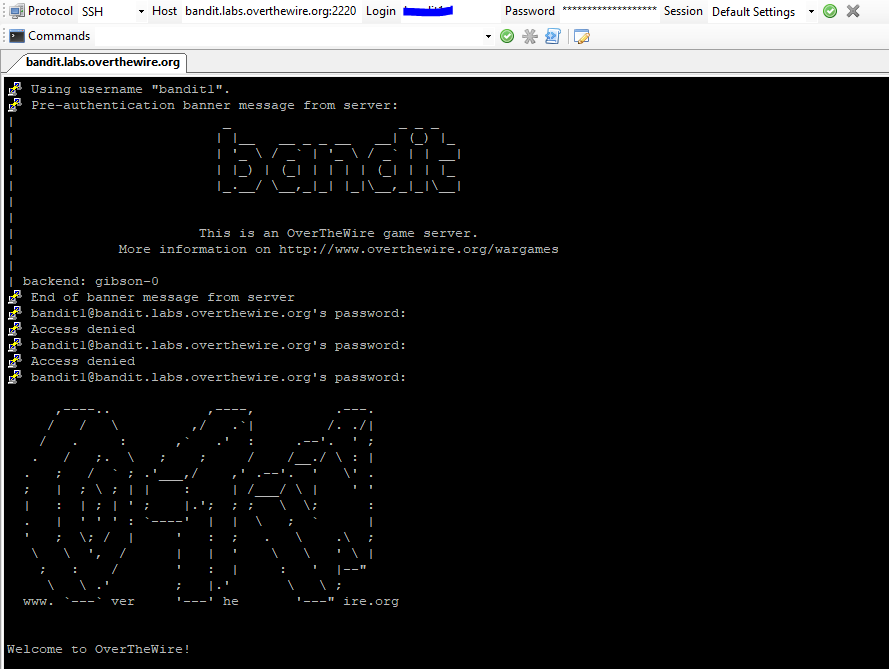
L0

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



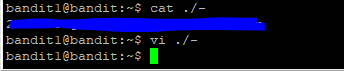
L0 -> Level 1:

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:-

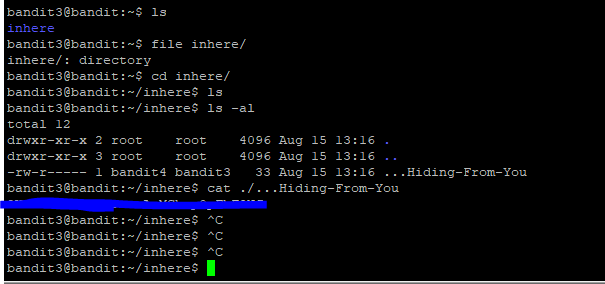
How do you open a file which has spaces between it?

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



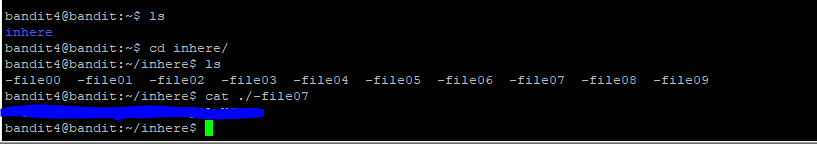
Level 3 -> Level 4:-

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.



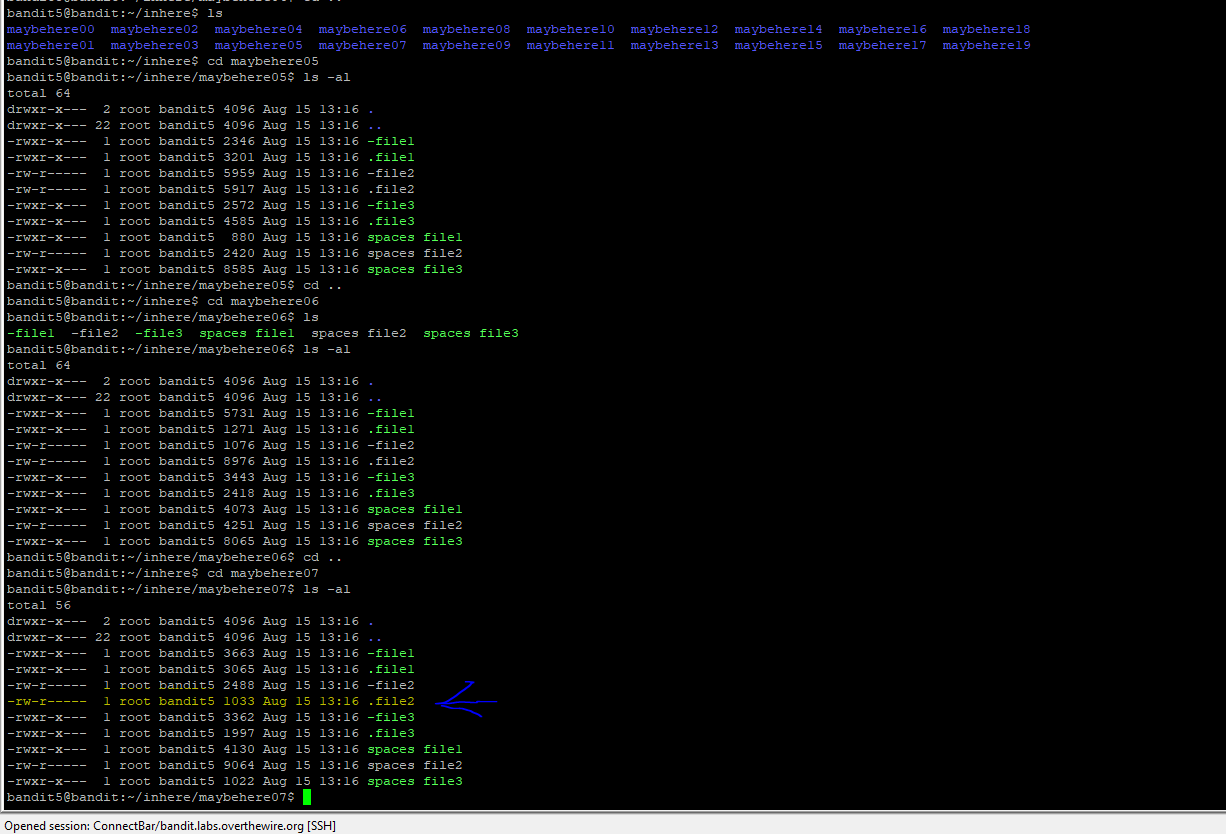
Level 4 -> Level 5:-

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

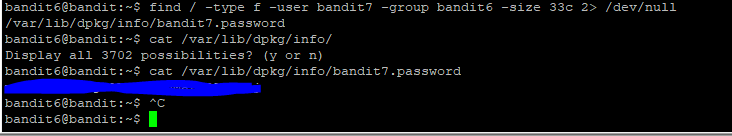
After a lot of effort I was able to find the correct file. I just looked at the size of the file I had to find out about.



Level 6 -> Level 7:-

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

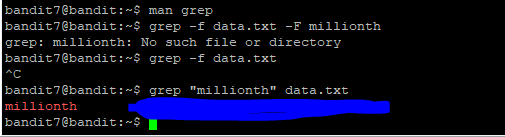
**find / type –f –user bandit7 –group bandit6 –size 33c 2> /dev/null**



Level 7 -> Level 8:

**Grep “millionth” data.txt**

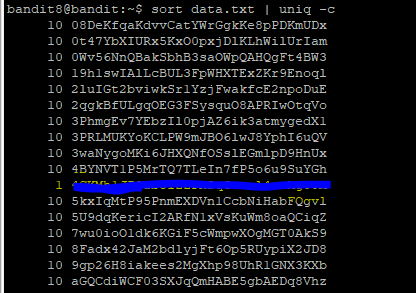
This was very easy as well.



Level 8 -> Level 9

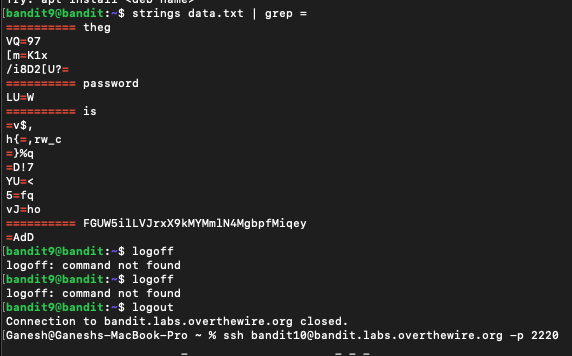
A simple sort cmd pipelined into a uniq command gives the only line with the password. This was pretty easy and simple

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



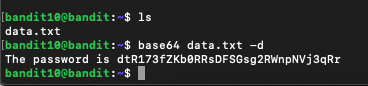
Level 9 -> Level 10

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.



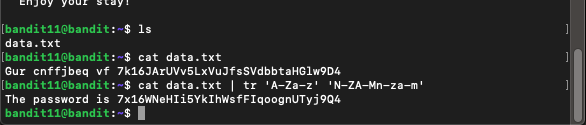
Level 10 -> Level 11

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.



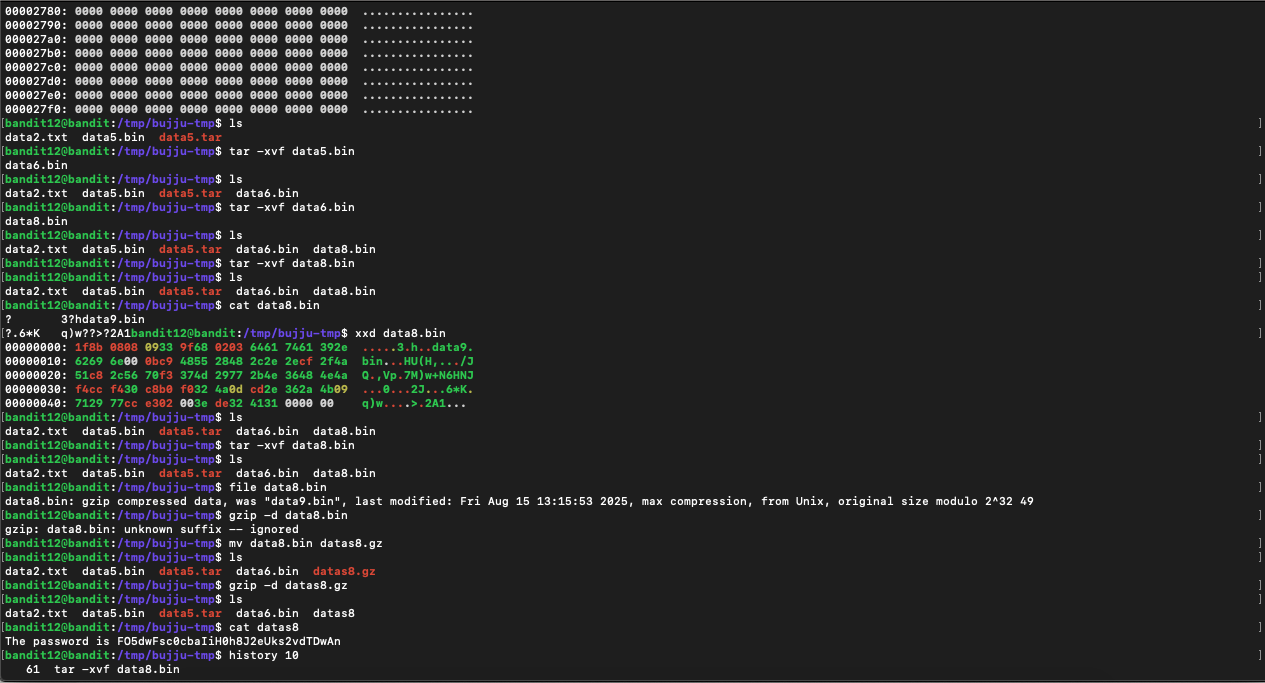
Level 11 -> Level 12

This particular challenge totally stumped me. I was in a doubt whether we have to use strings cmd or tr command. Eventually I looked up the solution on the internet and just copied it here to progress to another level.

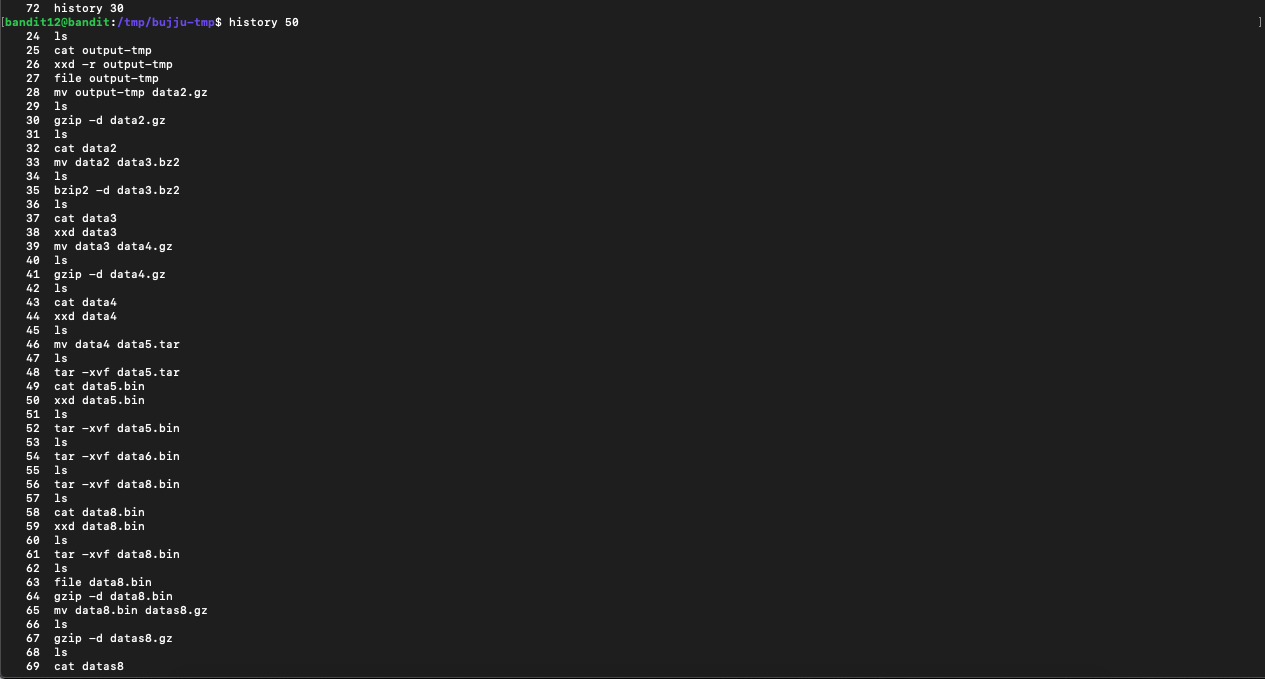


Level12 -> Level 13:-

This particular challenge was way beyond my knowledge. I did not have any working knowledge about signatures and how to use them in identifying the compression of a file. So I took help from google in removing all kinds of compression till I found my file containing the password. I found this to be a unique way of storing passwords. As it has so many layers of compression.

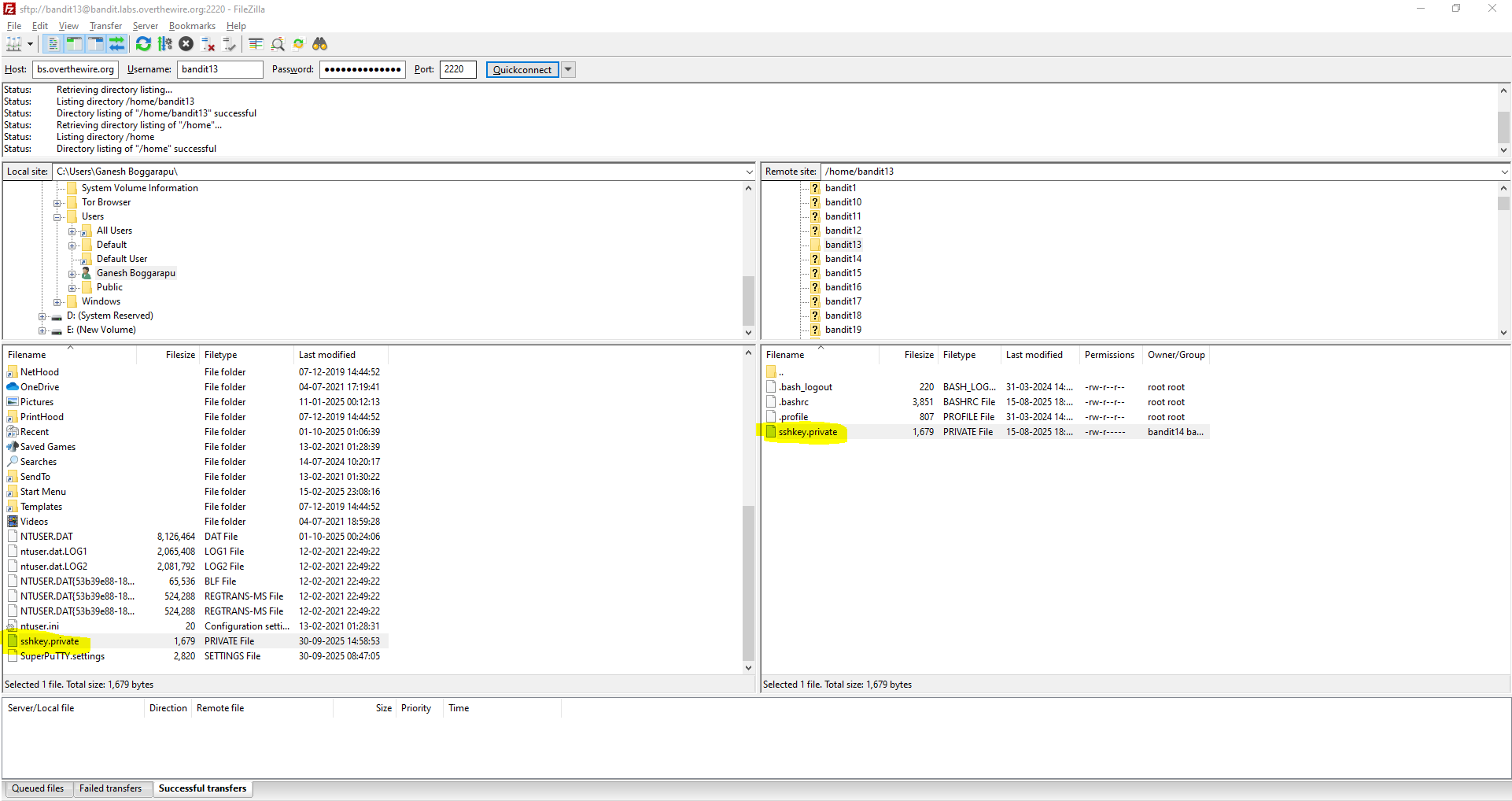


Below is the list of commands I used to reach to the final destination.

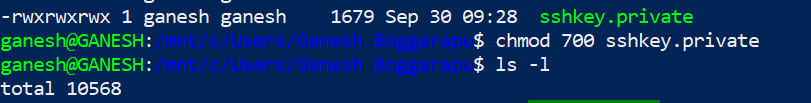


Level 13 -> level 14:

I first downloaded the sshkey.private from the Linux VM onto my windows desktop using FileZilla.



Then I modified the permissions on the file to ensure only I had full permissions to execute/manipulate the file.



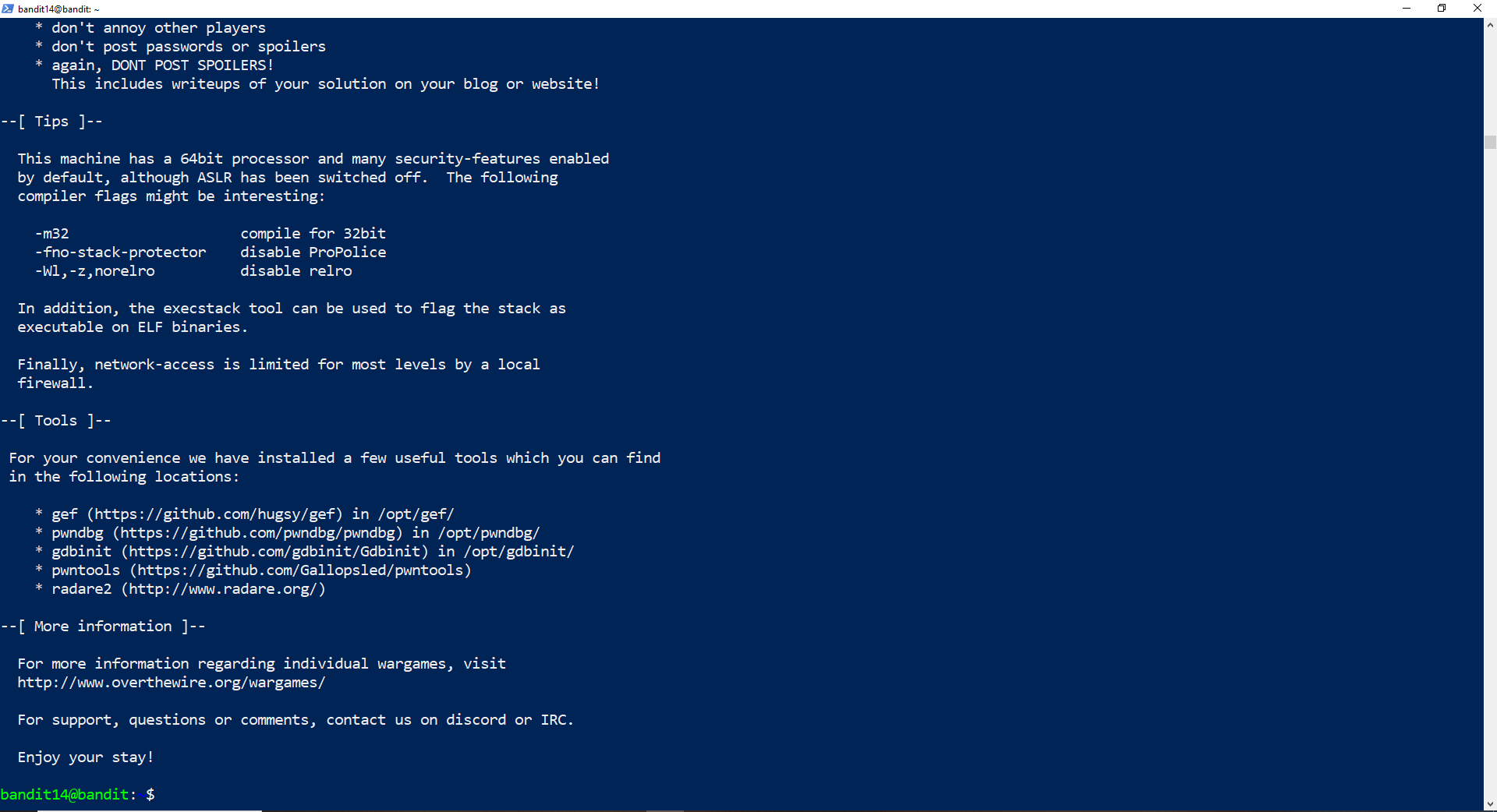
So the result now looks like this:



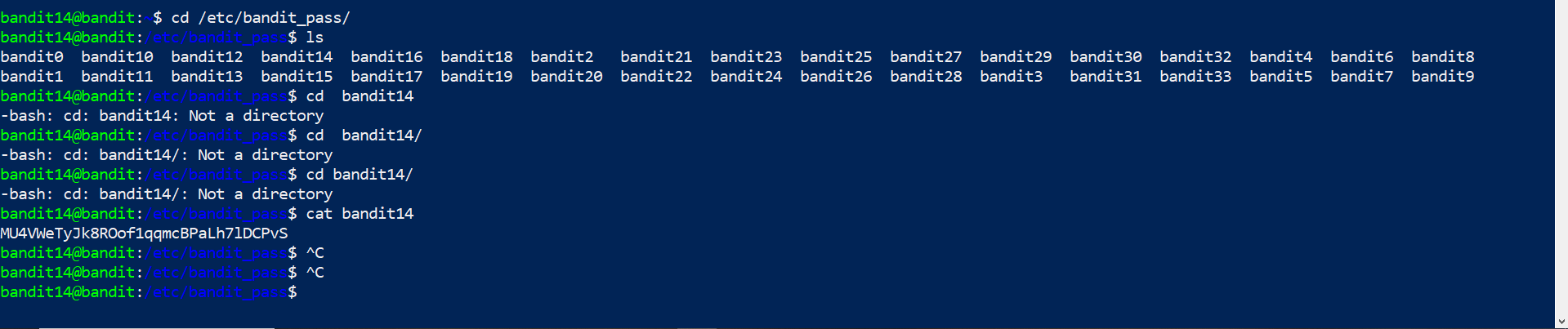
Then I used the private key to SSH into the VM as Bandit14 user. If we don’t have password to login to a server via SSh. We can also use a private key to SSH.

So below is the result of the ssh using a private key.





Now I just have to cat the file at the specified location.



This whole level 13 -> Level 14 has sent me down a rabbit hole which has really made me learn new things.

1. Initially I was not able download the sshprivate.key from the Linux Vm to a Windows machine. So I had to figure out the best way to do that via a CLI. I came across pscp which is thought would be useful but for some reason I found out that it did not allow me to establish an SSH connection directly.
2. So I eventually had to resort to using a GUI tool like FileZilla to make the file transfer.
3. Later I came across WSL in Windows Systems which will allow you to run a Linux Environment on your Windows machine that will allow you to use your Windows machine like a Linux System.

So I finally installed a Linux Distro(Ubuntu) on my Windows 10 and used it to finish the remaining tasks to complete this level.