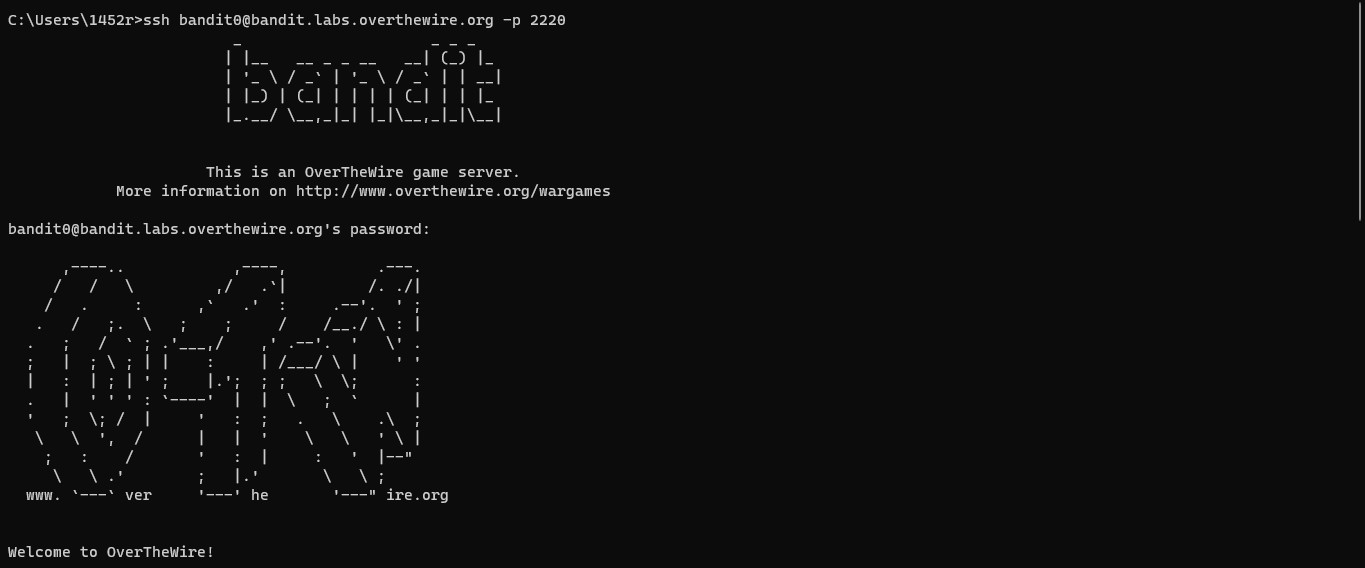
BANDIT OTW

Write-Up

# Level 0 –

**By rishabh sharma**

The 0 level was about learning what is ssh and a quick wikipedia page reading and how to use usernames and determine ports with ssh command was well enough to solve this level

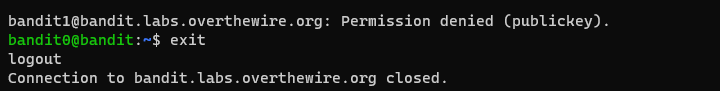


## Level 0 to 1 **–**

This level was about on how to navigate files through ls command and how to read a normal file using cat command I used a quick google search on examples of these commands and also some brute attempt at running them.

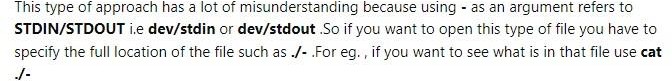
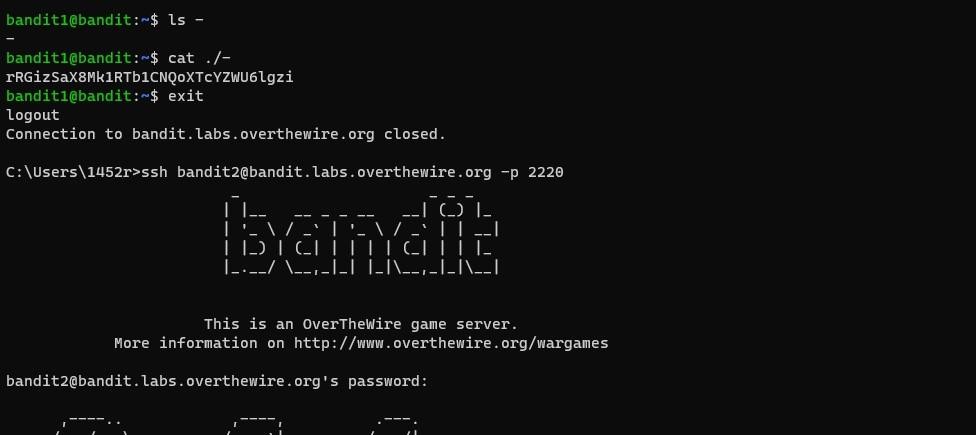


I was trying to log into new level without signing out of server, so I found out that I had to logout to sign onto different user



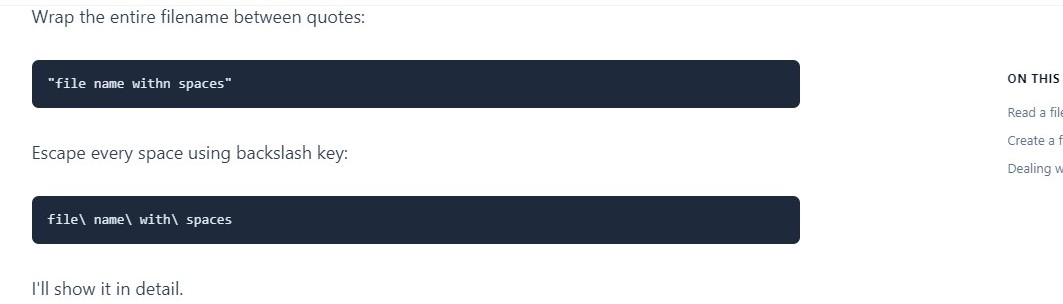
## Level 1 –

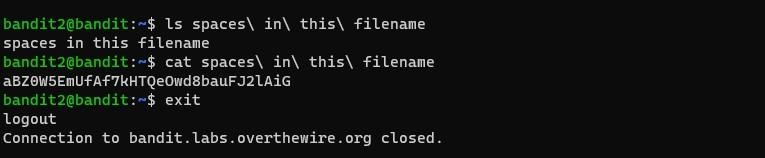
This level was about handling different file names which Linux may consider as part of the command a google search and a visit to stack overflow about how to do it solved the problem.



## level 2 –

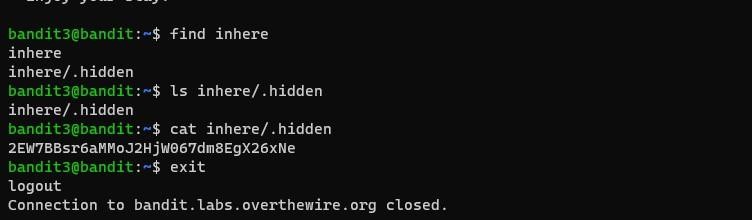
this level was about on how to specify and navigate through files with spaces in the names Linux gets confused that there is a space in the file name, and we must specify the space used so I found out how to handle spaces on google and got through the level quick





## Level 3 –

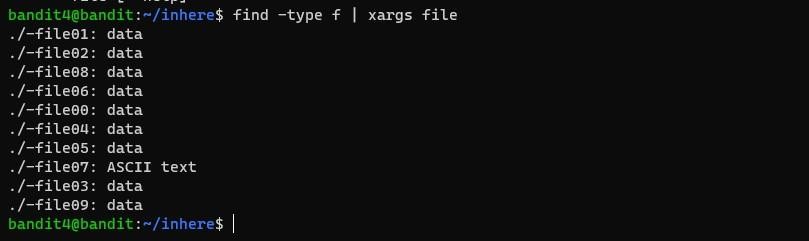
This level was about navigating hidden files in linux and how to handle them in while specifying their path in commands just trying random commands and I figured it out by the output that was given.



## Level 4 –

This level was about discovering the file command and how to use it I looked through the help of find command and tried but was wrong about how to use the command then I looked through stackoverflow and found some helpful information and it solved the level



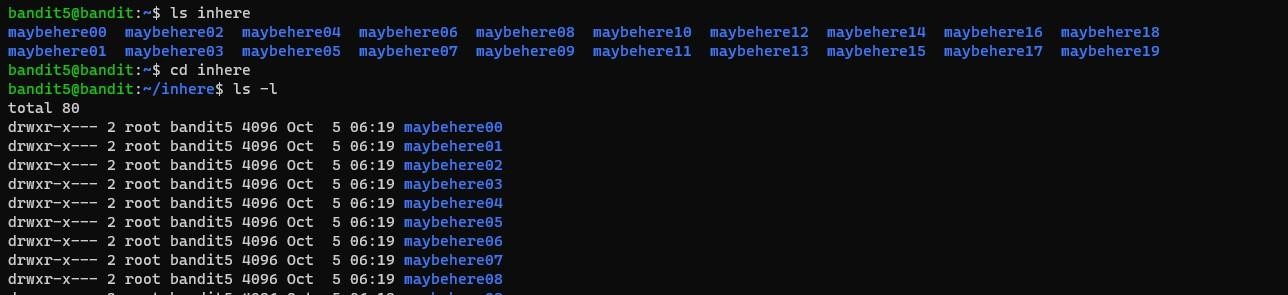


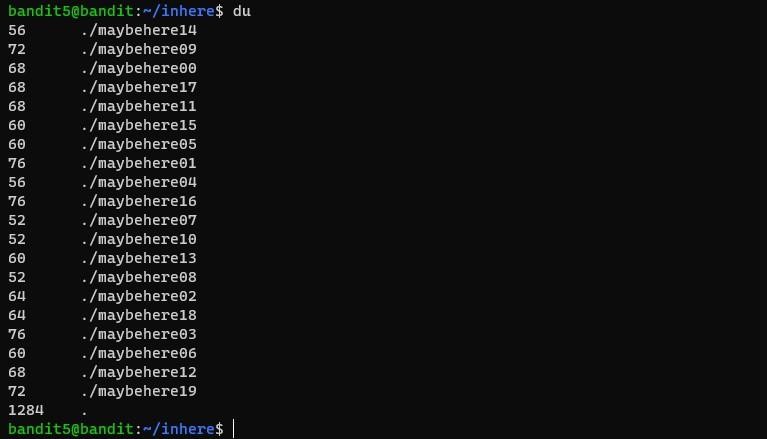


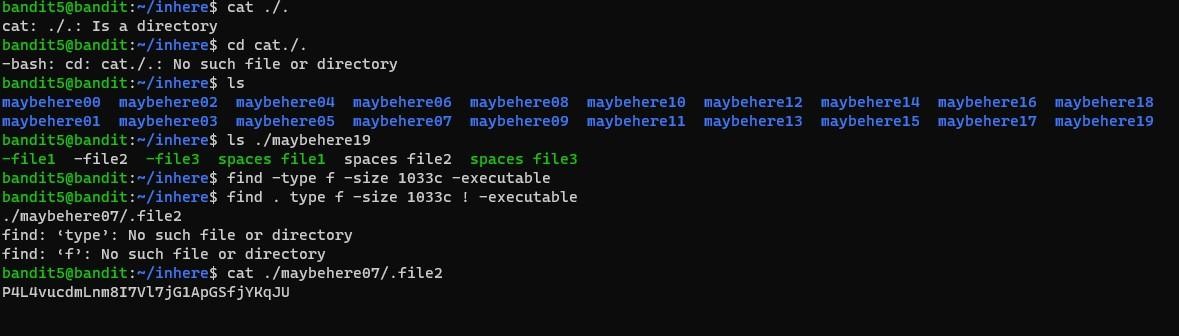
# Level 5 –

This level was about how to use find command with file sizes and specifying executable or not a google search about it and I had done this level

Here is what it looked like-

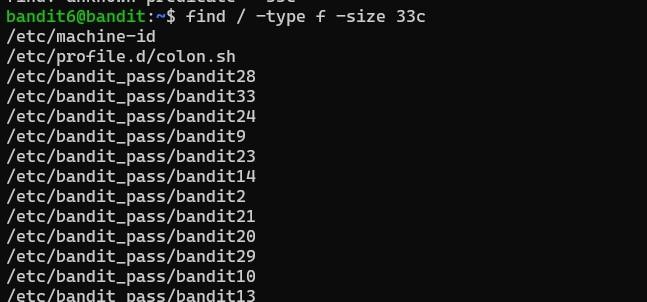


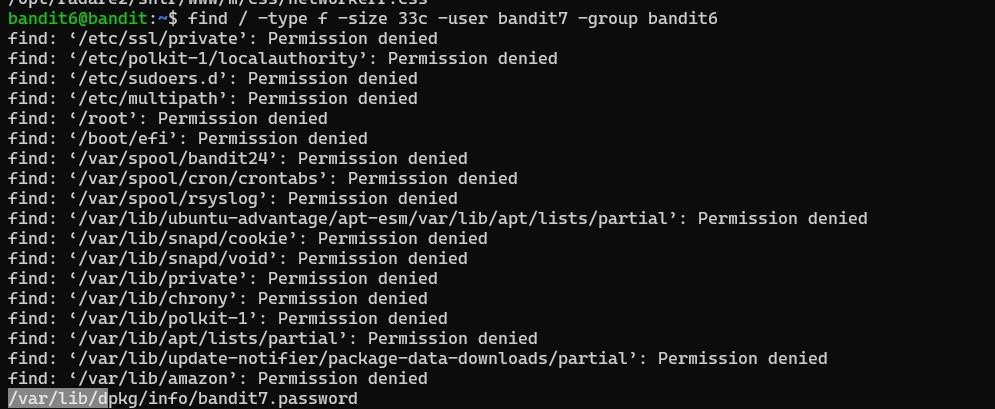
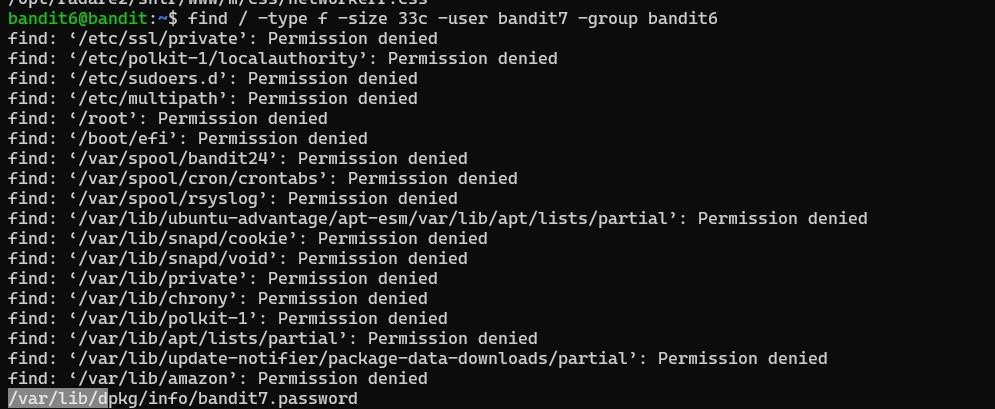




# Level 6-

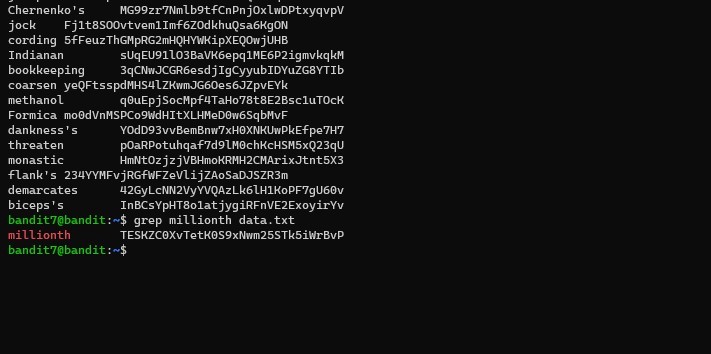
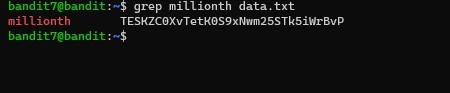
This level further extended into how you would use the find command with additional parameters such as user and group and was able to find the answer after looking at it enough but to find a more efficient way to do it I learned about specifying user and group and search by file size.





# Level 7 –

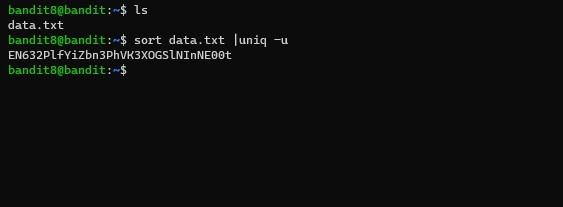
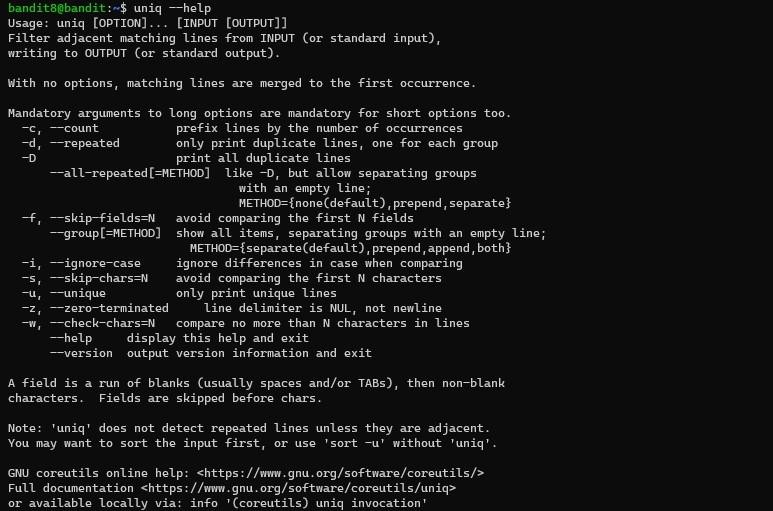
taking hint from commands listed below I searched about grep and found out it can be used in this situation to sort this



# Level 8 –

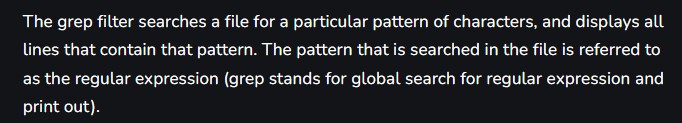
For this level I found about uniq command under the commands you may use section and tried to open help for it and it listed how it works -u was for just showing the unique string in the whole file but I could not use it standalone as the output was just same as cat I had to use it

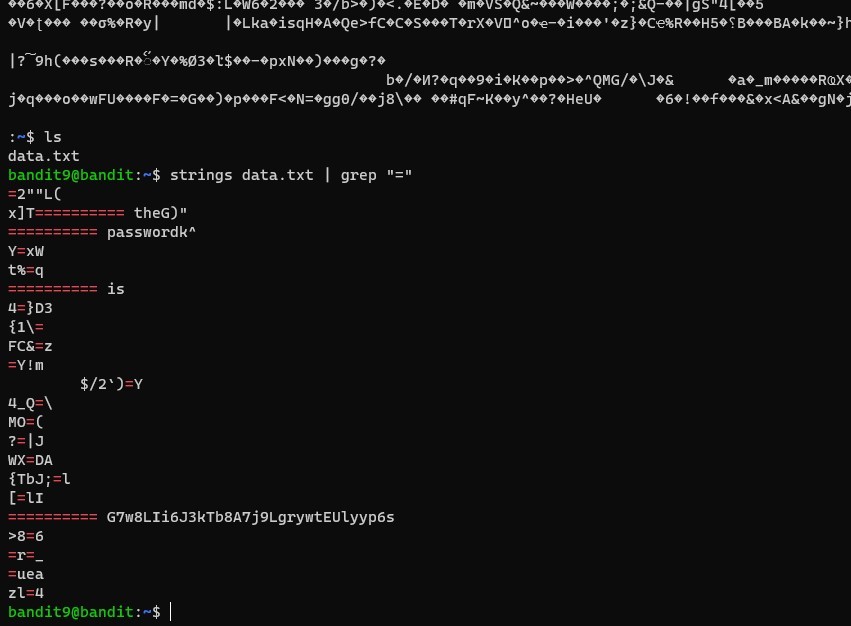
with sort command I found that in a online forum .



# Level 9-

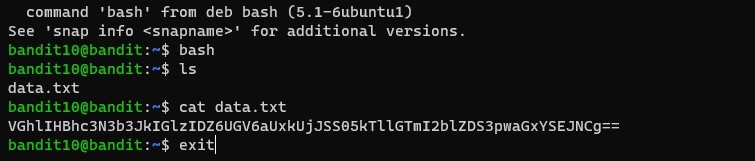
This level was about how to use grep and whay can grep do I found about it’s features on geeks for geeks and used it to solve this level on how to search for a particular character in an file

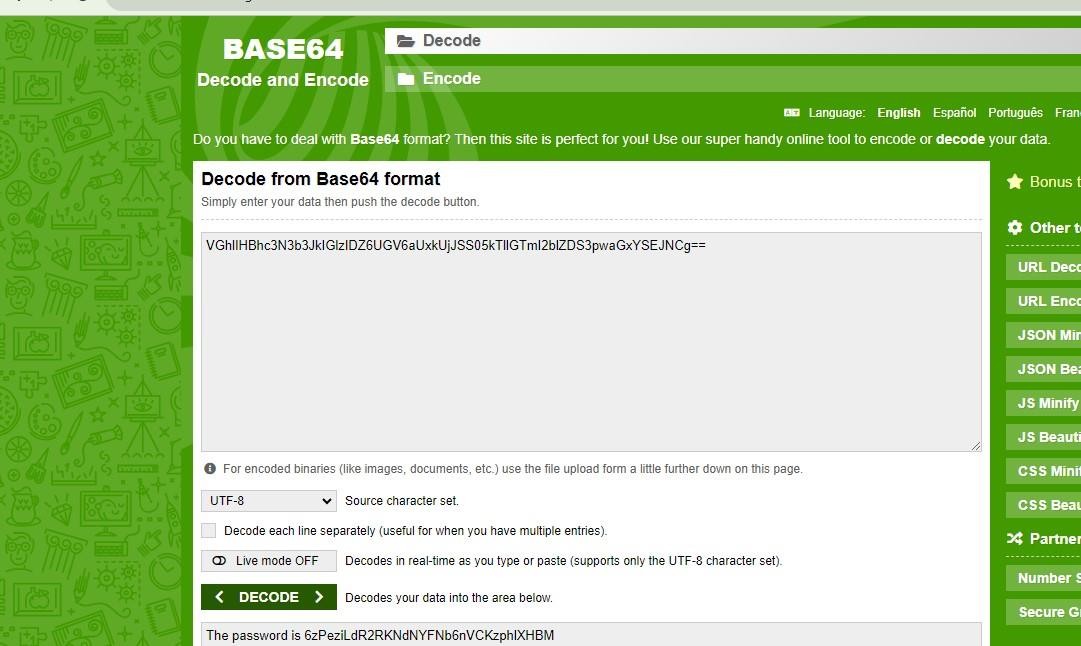




# Level 10 –

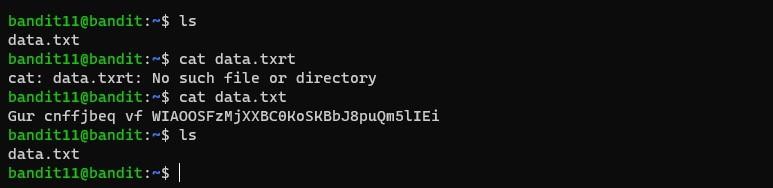
This level was about base64 and how the characters that we were given were encoded in base64 and we had to decode it I looked online for a base64 decoder and found the password and was able to find the text to decode by simply using the cat command

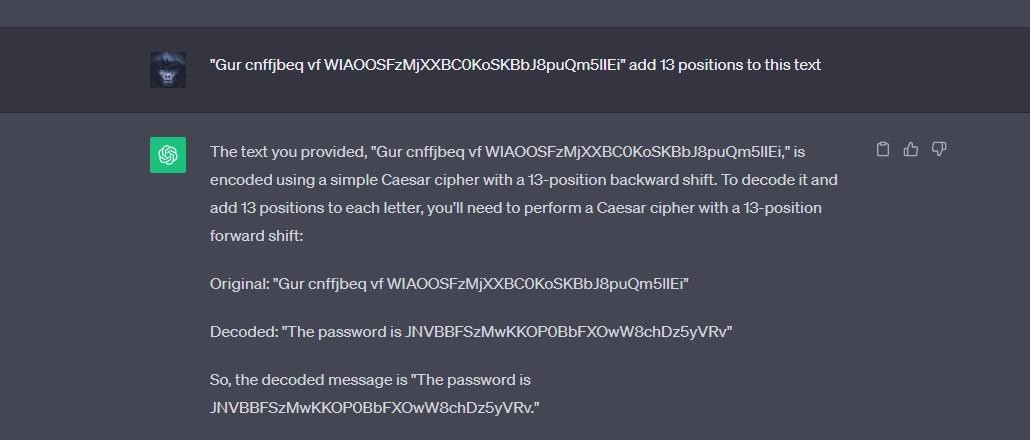


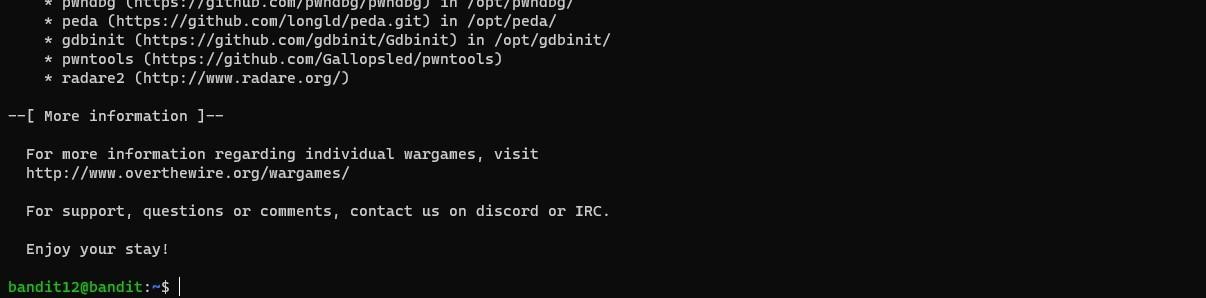


# Level 11-

This level was about finding automated ways to decode a code this level could be solved using various approaches asking chat gpt to rotate 13 characters or writing a C program to do it for you or use online tools like CyberChef also will get you the results (had to go through tons of reddit to find this one)

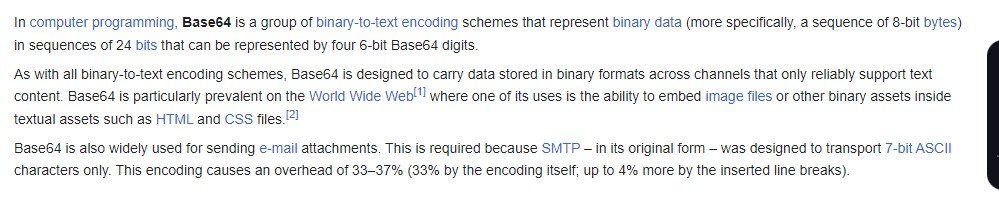




As you can see I was able to login

Level 12 –

This level was about he concept of base 64 and how we use xxd command to decode it and also multiple types of compression systems and how to decode them in here the manual page and online searches helped solve this level



A screenshot of a computer

Description automatically generated

A screen shot of a computer program

Description automatically generated



A black screen with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

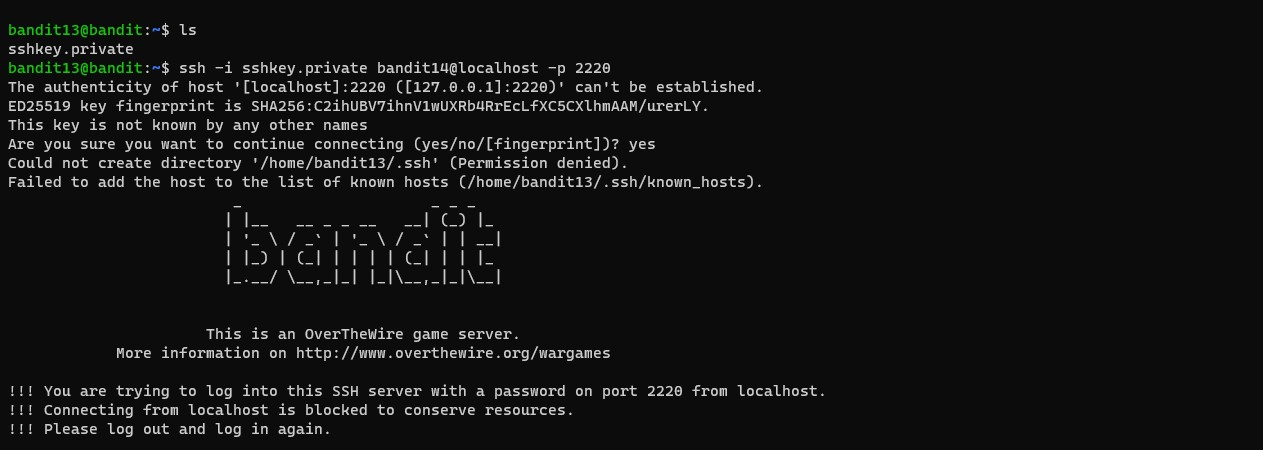
A black screen with a black background

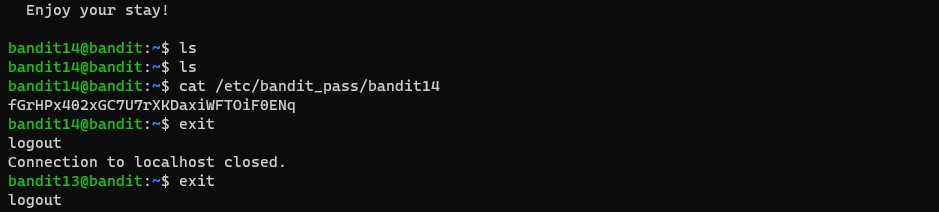
Description automatically generated

Level 13-

In this level we had to use a private ssh key instead of a password to login in into a local host on the server which had access to the password of the next level

Solved this problem by looking how to login with a private ssh key on an online forum and following the steps and retrieving the key from the specified location.

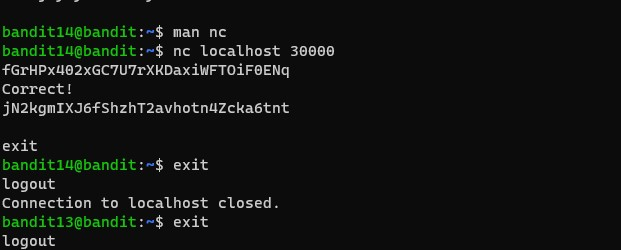




Level 14 –

In this level we had to submit the key obtained from the above level to a localhost port 30000

The nc command was used to do it and some reading of online forums and man pages helped in solving the level.



Level 15 –

In this level we had to submit key obtained to a local host port 30001 using ssl protocol.

I tried using the nc command but couldn’t specify the use of ssl also tried other command like Nmap thinking I could brute some commands and it would work (reading the manual pages and searching the internet.) found out we can use ncat command and also specify the ssl pages.

Man pages for ncat showing we can specify ssl-

A screen shot of a computer

Description automatically generated



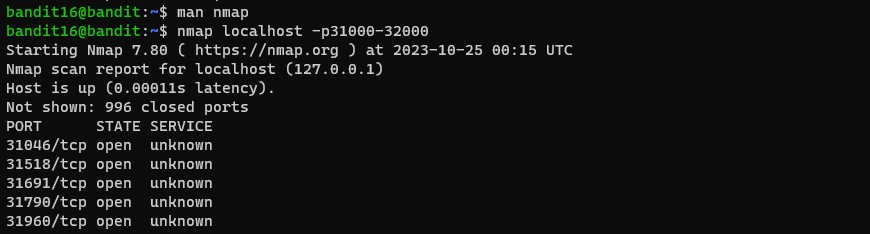
A computer screen shot

Description automatically generated

Level 16 –

This level was about scanning for active ports and finding out which one of them used ssl and returned us with a private key when we gave it a password.

This level became hard because certain commands did not work due to root access issues in WSL tried solving with 3 different approaches but did not work so eventually had to switch to checking the 5 ports 1 by 1 for the return of a private key.





While going through the man pages found this and tried running it -



A black screen with white text

Description automatically generated

But could not due to root issues. now left with no other choice manually check all 5 ports for ssl-

A screenshot of a computer screen

Description automatically generated

Found the key!

Level 17 –

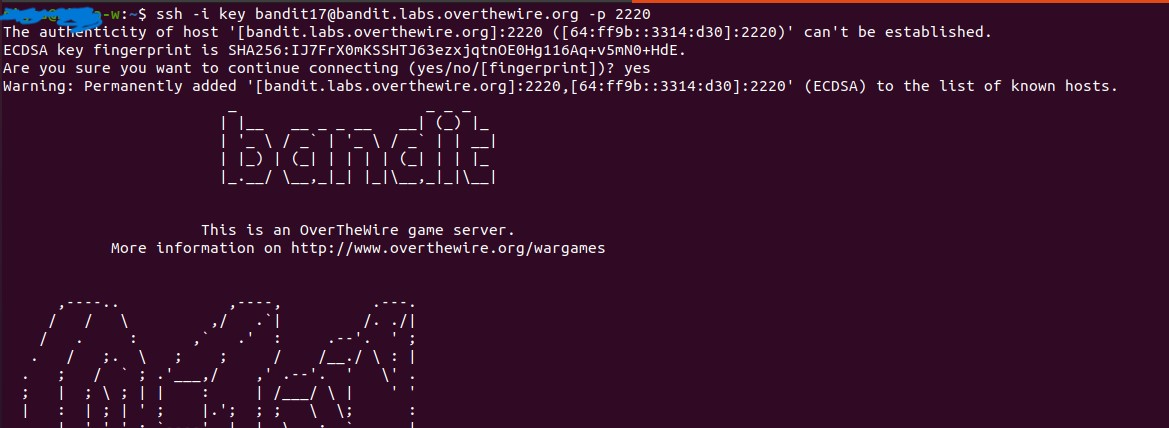
The problem

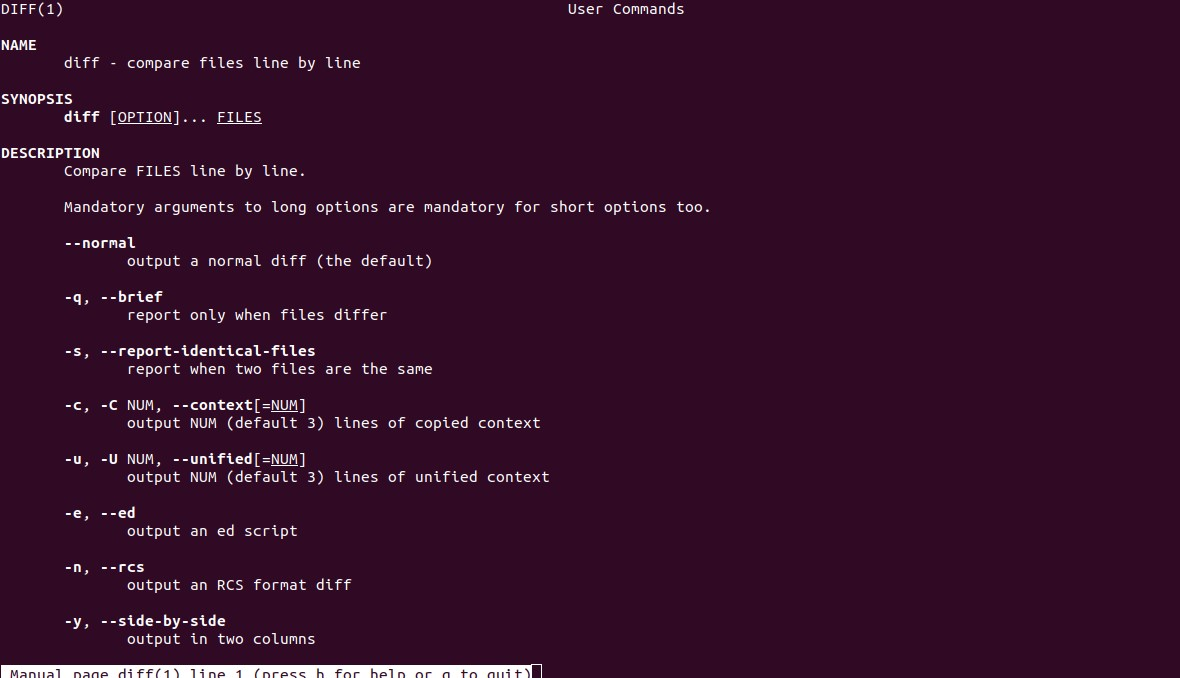
This level was about storing the private key given in the earlier level and using it to login.

By using the vim tool and then checking for single different line of code between 2 different files

Using diff command

My approach-   
I could not complete this problem on wsl as the server determined that the private key was not secure enough due to permission issues even after running chmod to give appropriate permissions (windows file system magic on the subsystem) so had to switch to ubuntu install vim using terminal and creating a new private key to login and giving appropriate permissions using chmod (400 or 600) then logging into the level and using diff command to obtain the key.





A screenshot of a computer

Description automatically generated

Level 18 –

In this level we were constantly being logged out by a modified bashrc file and had to login in the server bypassing the bashrc file here we can solve this problem by forcing a pseudo terminal using -t or directly using the cat command with terminal



Level acquired pass - hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg

Level 19 –

This level revolved around setuid and how to use it the approach I took was to read man pages and try but the wsl was giving root problems and had to switch approach so I tried to use ./ and it gave me indicators and then I used stack overflow in which someone had asked a similar question and was able to figure it out from there

A screenshot of a computer program

Description automatically generated

Level acquired pass- VxCazJaVykI6W36BkBU0mJTCM8rR95XT

Level 20 –

This level was about setting up a listener in one terminal and using a random port which should not be in use and then connecting to the same port and inputting the level 20 password and then it would send the next level’s password to the listener we setup earlier.



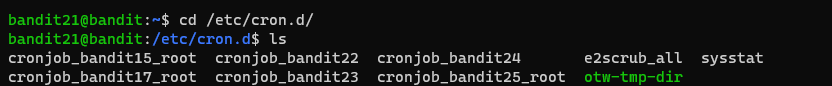
A black background with white text

Description automatically generated

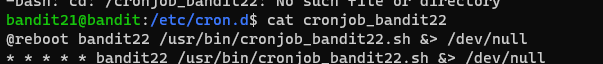
Level acquired password - NvEJF7oVjkddltPSrdKEFOllh9V1IBcq

Level 21

Using the hint given I cd to the specified folder and do an ls



I find out there are multiple files and assume that cronjob\_bandit22 is the targeted file as we need to find password for next level, and I cat to it.



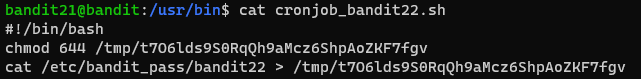
I see it is performing some task in /usr/bin/cronjob\_bandit22.sh so now I cd to /usr/bin/ and then ls just to check

A black screen with green text

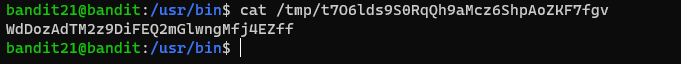
Description automatically generated



Now I cat the cronjob\_bandit22.sh and find it is using the below file



Now I cat the file in tmp folder and sure enough our password is in it!



Level acquired pass - WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff