**LEVEL-0:**

I used the following command to connect the bandit

ssh bandit.labs.overthewire.org -l bandit0 -p 2220

The password to connect the bandit0 is “bandit0”.

When I connected to the bandit0 I found a readme file in home directory I used the “ls” command to see the files in the specific directory and “cat” filename to find the content in the file

As it is specified in the description that the password for the next level is stored in the readme file.

        The password for the next level is "boJ9jbbUNNfktd78OOpsqOltutMc3MY1".

**LEVEL-1:**

I logged into the bandit I used “ls” command to find any files stored in it then I found an dashed file I used “cat ./-filename” to see the content in the file and I found the password.

        The password for the next level is "CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9"

**LEVEL-2:**

In the description it is mentioned that the password is saved in the file named "spaces in this filename". So I used the command cat “file name” to display the file content if we are giving the space in this filename linux terminal identifies this as 4 different file so to understand the linux terminal that it is a single file name we have enclose it in double quotes.

        The password is displayed as "UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK"

**LEVEL-3:**

        In this level the "ls" command displays a directory named inhere. To open the file inhere I used the “cd filename”.

As mentioned in the question that password is hidden in a file So I used “ls -a” ls is used to display all the directories except some directories starting with “.” Which means that it is hidden by using -a it will not ignore such type of entries it will display every file present in the current folder. So as the password is stored in hidden file I used the mentioned command. Then I used the “cat .filename” to display the content in the hidden file

        The password  is "pIwrPrtPN36QITSp3EQaw936yaFoFgAB".

**LEVEL-4:**

        In this level there is a folder inhere in home directory which I found by using “ls” command. When I moved into the in here using “cd filename” command I found so many files there. In these only one file contains the password so I used the command “file ./\*” to find the file type of all the dashed file stored in that folder I found one of the file is ascii and all others are in the format  data so I used the command “cat ./-filename” to display the content in the ascii file then I found the password in it.

        The password for next level is "koReBOKuIDDepwhWk7jZC0RTdopnAYKh".

**LEVEL-5:**

        In the description it is mentioned that the password is stored in a file which is human readable;1033 bytes in size and not executable

In the terminal  I opened the inhere folder by command cd and type this command to find the file with specified "find -type f -size 1033c ! -executable". In this find is used to find any file or keyword from the whole system so I used ‘-size’ to specify size and ‘!=executable’ to specify file is not executable and “type -f” to specify it is a regular file and  found out the particular file and It contains password.

The Password for next level "DXjZPULLxYr17uwoI01bNLQbtFemEgo7".

**LEVEL-6:**

        In the description provided it is said that the file is somewhere in the server and has the following properties :

\*owned by user bandit7

\*owned by group bandit6

\*33 bytes in size

To find the file I used the linux command :

“find / -user bandit7 -group bandit6 -size 33c”.

 “find “ is used to search for the files in the directory ,  / is used to search the whole directory, “-user” is used to specify the name of the user who owns the file, “-group” is used to specify the group that owns the file , the the “-size” is used to specify the size of the file. After execution of the command we will get a lot of directories . We can find a directory with  the file bandit7.password.  Then I used “cat” to see the content in the file  and I found the password.

The Password for next level "HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs"

**LEVEL-7:**

In the description it is said  that the password is stored in a file named data.txt and it is stored near the name  ”millionth” , then I used the command "cat data.txt | grep millionth" to find the password. In it the “cat” command is used to see the content in the file and “grep“  is used to find the matching pattern specified. In it the word “millionth” is specified .So after running the command it extracted the text “millionth” from the text file which then shows the content .

The Password for the next level "cvX2JJa4CFALtqS87jk27qwqGhBM9plV".

**LEVEL-8:**

In the description it is mentioned that the password is stored in a file named data.txt  and is the only line of text that occurs only once . Then I used the command " cat data.txt|sort| uniq -c". In thi command “cat data.txt” is used to see the content of the file, “ sort “ sorts the file data in an alphabetic order, and “uniq –c “ will display the text in unique order and counts the number of times it  is repeated . In it only once a text is repeated so that is password as per the description provided.

The Password for next level "UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR".

**LEVEL-9:**

        As per the description , the password is stored in a data.txt file in one of the few human readable strings proceeded by several “=”characters. So I used the command "strings data.txt | grep =" In the  data.txt" file there are both human-readable and unreadable files  , To extract human readable file I used the command “strings filename” ,” grep” to match the pattern “=” . From this I found the password.

 The Password for next level "truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk"

**LEVEL-10:**

        As per the description, the password is stored  in a file data.txt which contains base64 encoded data. So I used the command "cat data.txt | base64 --decode" . In this the command “cat data.txt” will display the contents in the text file and “base64 --decode” will decode the displayed content and gives the output which is the password.

The Password for next level "IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR".