Task-7

How to login to ssh : use ssh command to connect to port 2220 and use hostname@bandit.labs.overthewire.org .
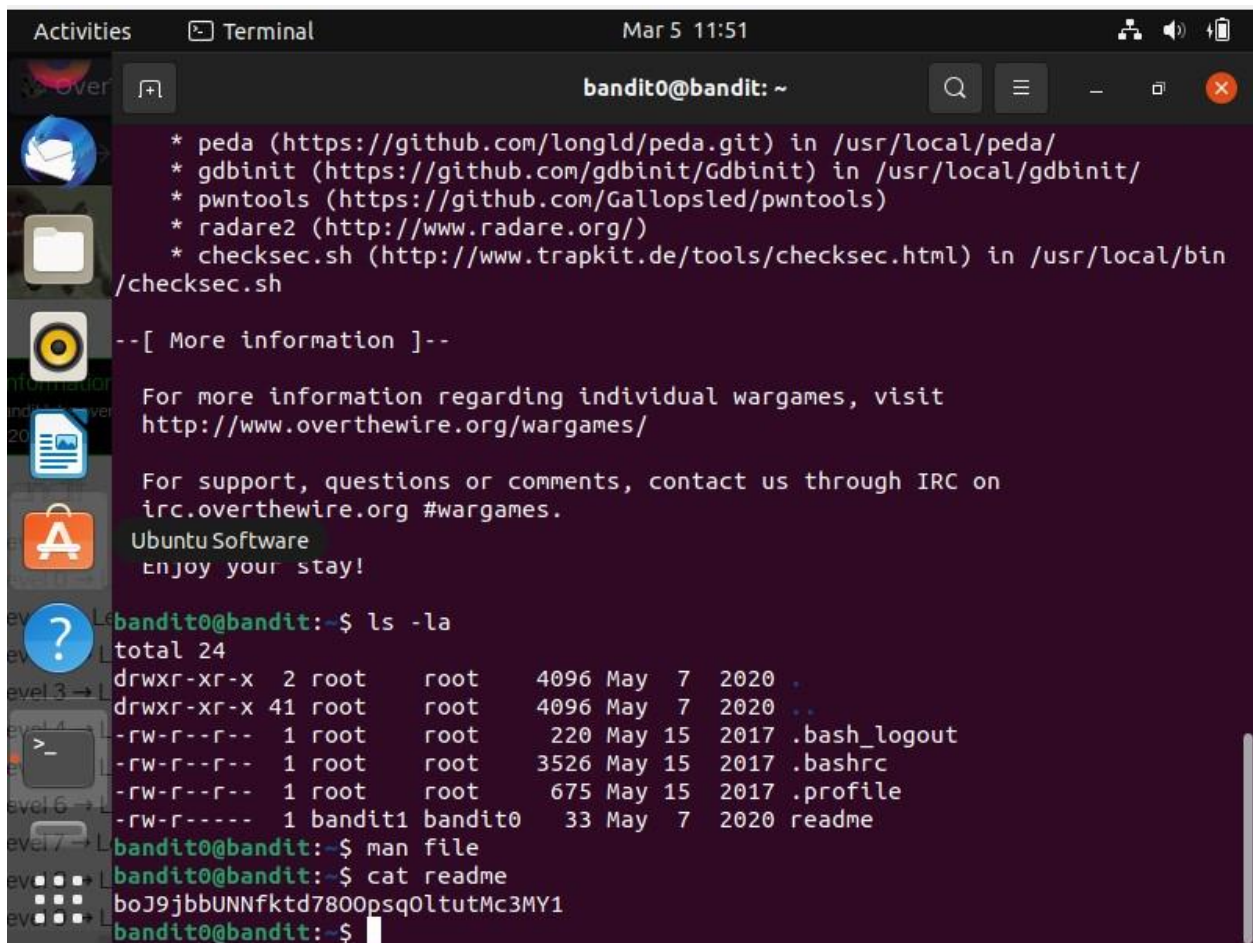
Level 0:

Hostname:bandit0

Password: bandit0

I connected to the bandit server by giving the username and password given in the overthewire.org website.

Then as per the instructions I used cat command on readme file to get the password.
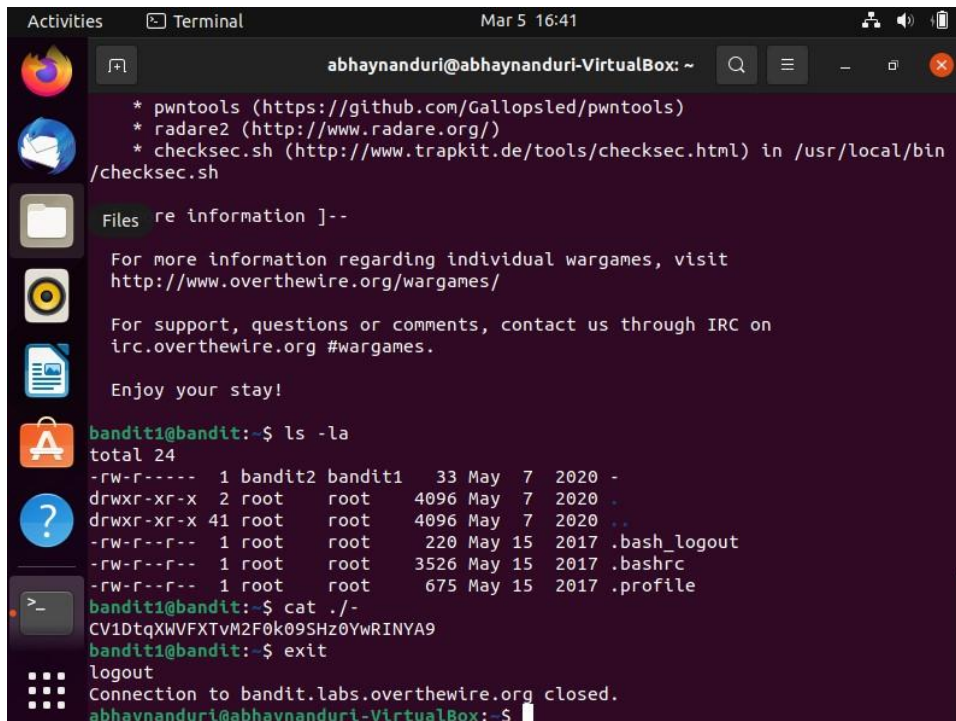
Level 1

Hostname: bandit1

Password: boJ9jbbUNNfktd78OOpsqOltutMc3MY1

Logic:

Opening a file named '–' using cat command normally isn't possible as cat expects us to give an option. So, we write the whole path to open the file. Since the file exists in the current file, we use "cat ./-". Here "." means "current directory".

Level 2

Hostname: bandit2

Password: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

Logic:

The file here contains spaces so the linux system is going to confuse it with concatenating multiple files. So we enclose it in single quotes.
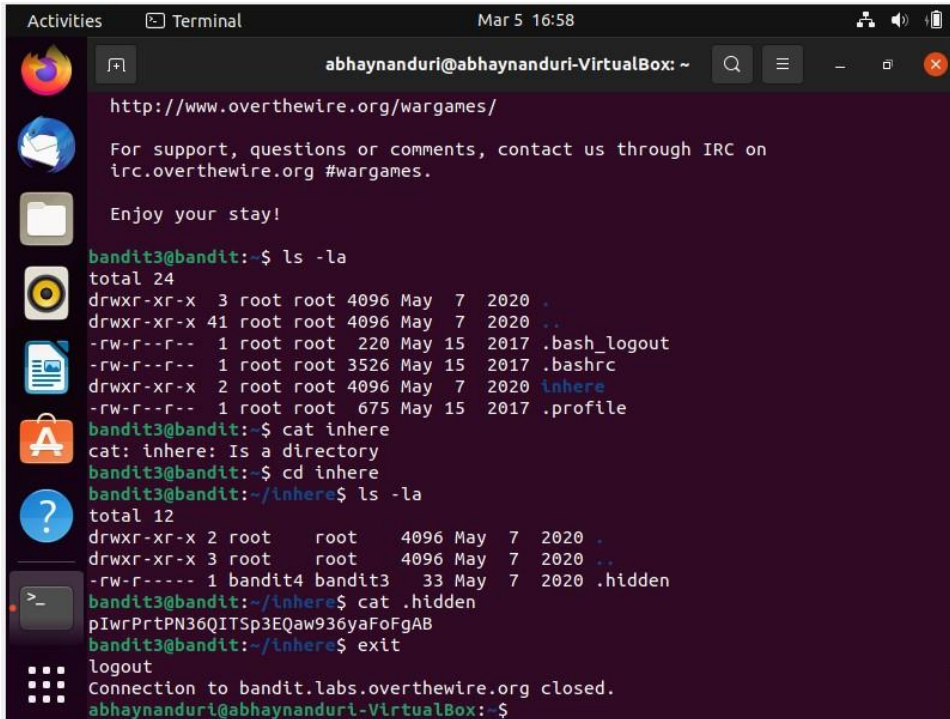
Or we can use "\" instead of spaces.

Level 3

Hostname: bandit3

Password: UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

Logic:

The file containing password is hidden so we use ls –la to reaveal it and open it.

Level 4

Hostname: bandit4

Password: IwrPrtPN36QITSp3EQaW936yaFoFgAB

Logic:

We need to check for the type of data we are reading in the directory. It is achieved by using file command and to see the type of all the given files we use "file ./*". "*" is for all files in the directory.
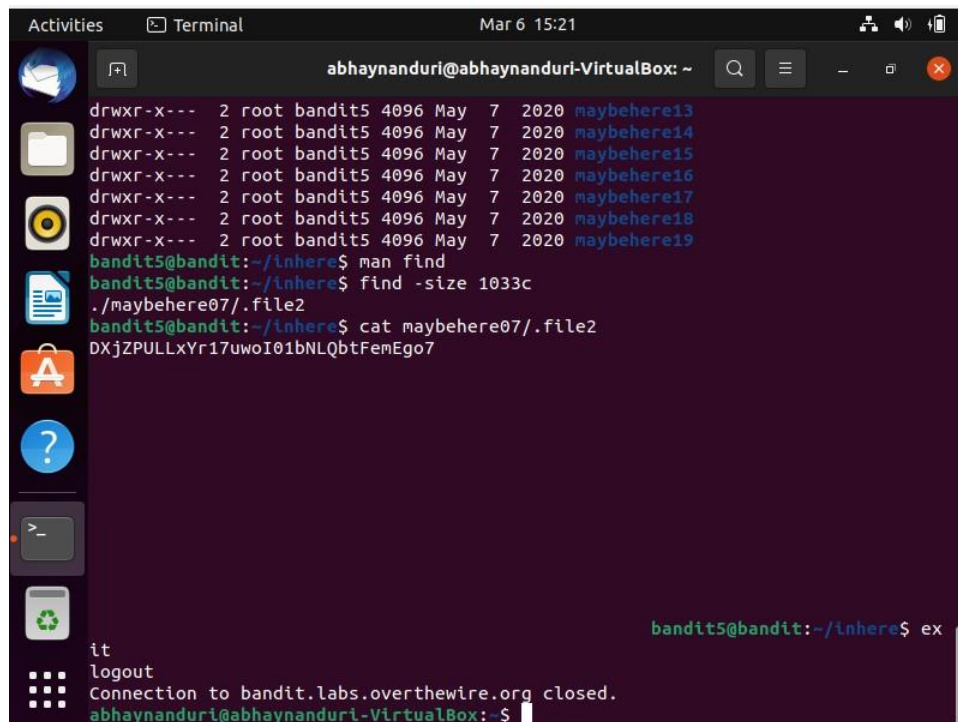
Level 5

Hostname: bandit5

Password: koReBOKuIDDepwhWk7jZC0RTdopnAYKh

Logic:

Use find command with given parameters to acquire the file. Then open it.

```
drwxr-x---  2 root bandit5 4096 May  7  2020 maybehere13
drwxr-x---  2 root bandit5 4096 May  7  2020 maybehere14
drwxr-x---  2 root bandit5 4096 May  7  2020 maybehere15
drwxr-x---  2 root bandit5 4096 May  7  2020 maybehere16
drwxr-x---  2 root bandit5 4096 May  7  2020 maybehere17
drwxr-x---  2 root bandit5 4096 May  7  2020 maybehere18
drwxr-x---  2 root bandit5 4096 May  7  2020 maybehere19
bandit5@bandit:~/inhere$ man find
bandit5@bandit:~/inhere$ find -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
                                        bandit5@bandit:~/inhere$ ex
it
logout
Connection to bandit.labs.overthewire.org closed.
abhaynanduri@abhaynanduri-VirtualBox:~$
```
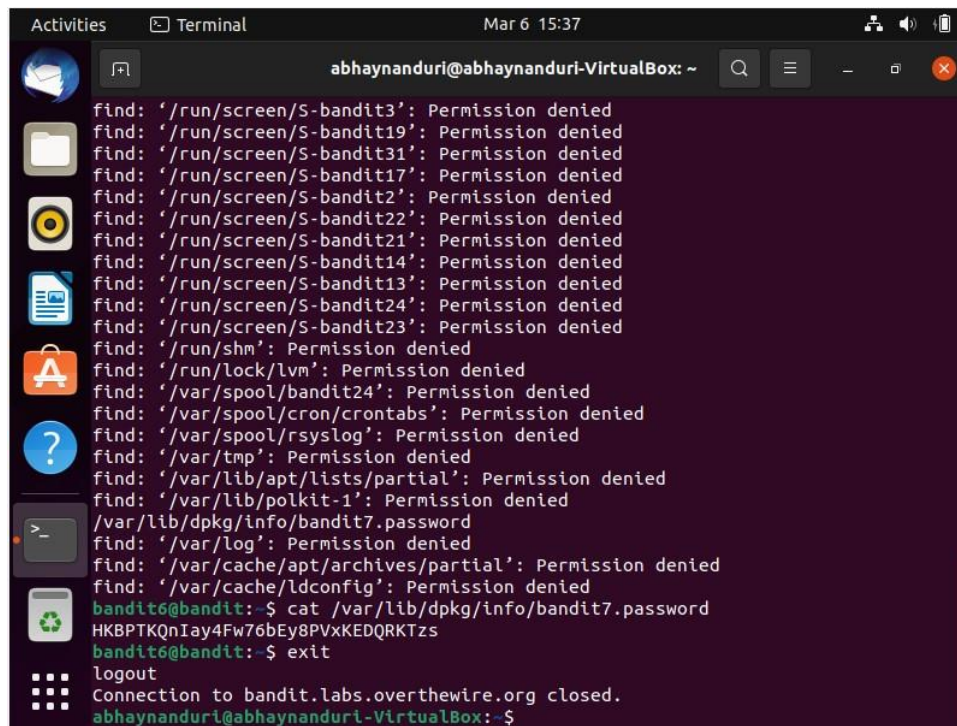
Level 6

Hostname: bandit6

Password: DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Logic:

Using ls (even ls –la) will show that the directory is empty. So, we use the find command to find any hidden paths with the given parameters.

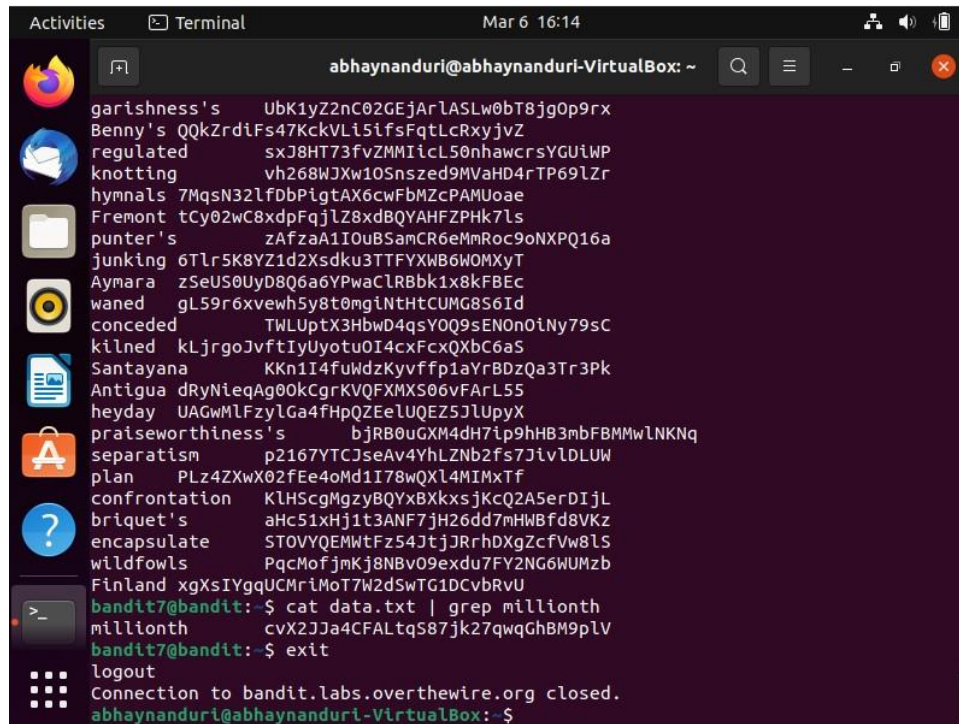And You will see that there is only one file for which we have access so we open that and we get the password

Level 7

Hostname: bandit7

Password HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Logic:

The password is said to be in file data.txt and associated with word millionth so we pipeline cat with grep command to get the line with string millionth in it.
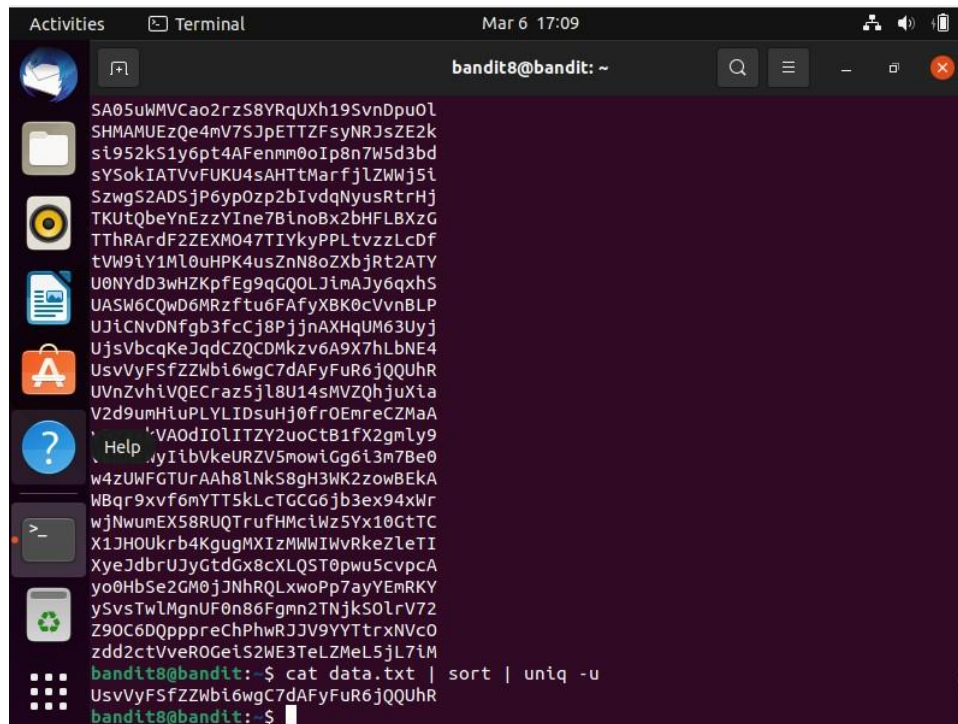
Level 8

Hostname: bandit8

Password cvX2JJa4CFALtqS87jk27qwqGhBM9plv

Logic:

By pipelining cat and sort command we get to know that many lines repeat so we pipeline an extra command uniq to find the password

Level 9

Hostname: bandit9

Password: UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Logic:

Strings command gives printable strings in file. So, we use grep to find strings with "=" in it.

Level 10

Hostname: bandit10

Password: truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Logic:

Use base64 to decode the encryption in data.txt

Level 11

Hostname: bandit11

Password: IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Logic: This is a special type of cipher used by Julius Ceasar. All lower-case letters and upper-case letters are rotated by 13 letters each.

Input	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
Output	NOPQRSTUVWXYZABCDEFGHIJKLMnopqrstuvwxyzabcdefghijklm

Level 12

Hostname: bandit12

Password: 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Logic: we decrypt the hexdump using xxd command and make a temporary directory as specified. Now we repeatedly unzip the files.

Level 13

Hostname: bandit13

Password: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Logic:

We use ssh command using hostname@localhost and -i option as shown below. The password for level 14 is in level 14 itself so we get the level 14 password in the specified path of the Level 13 problem statement.

Level 14

Hostname: bandit14

Password: 4wcYUFw0k0XLShlDzztnTBHiqxU3b3e

Logic: We connect to telnet interface by using given port on localhost and password of level 14. And we get the password of level 15

Level 15

Hostname: bandit15

Password: BfMYroe26WYalil77FoDi9qh59eK5xNr