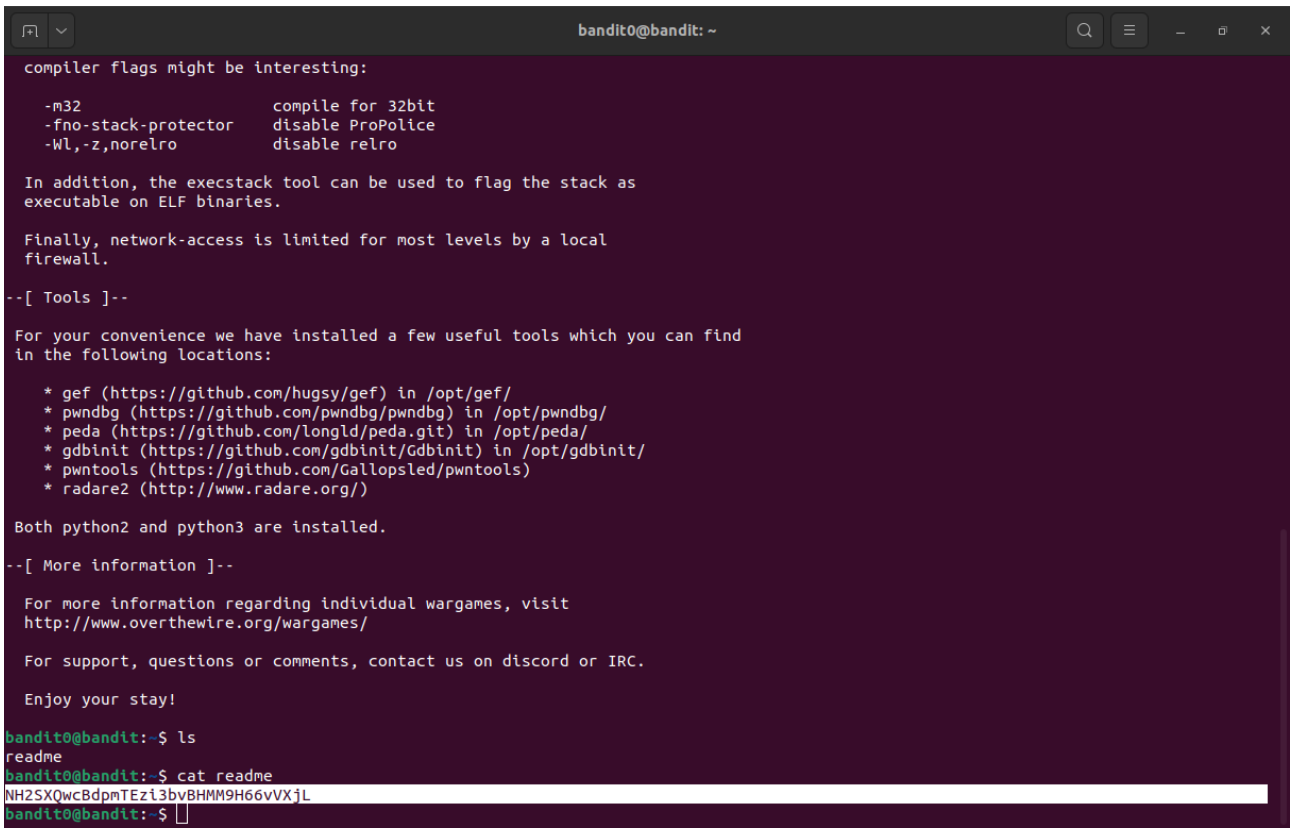


Bandit 0 => 1

1.Logged on using ssh

Hostname : bandit0

Password : bandit0

Port : 2220

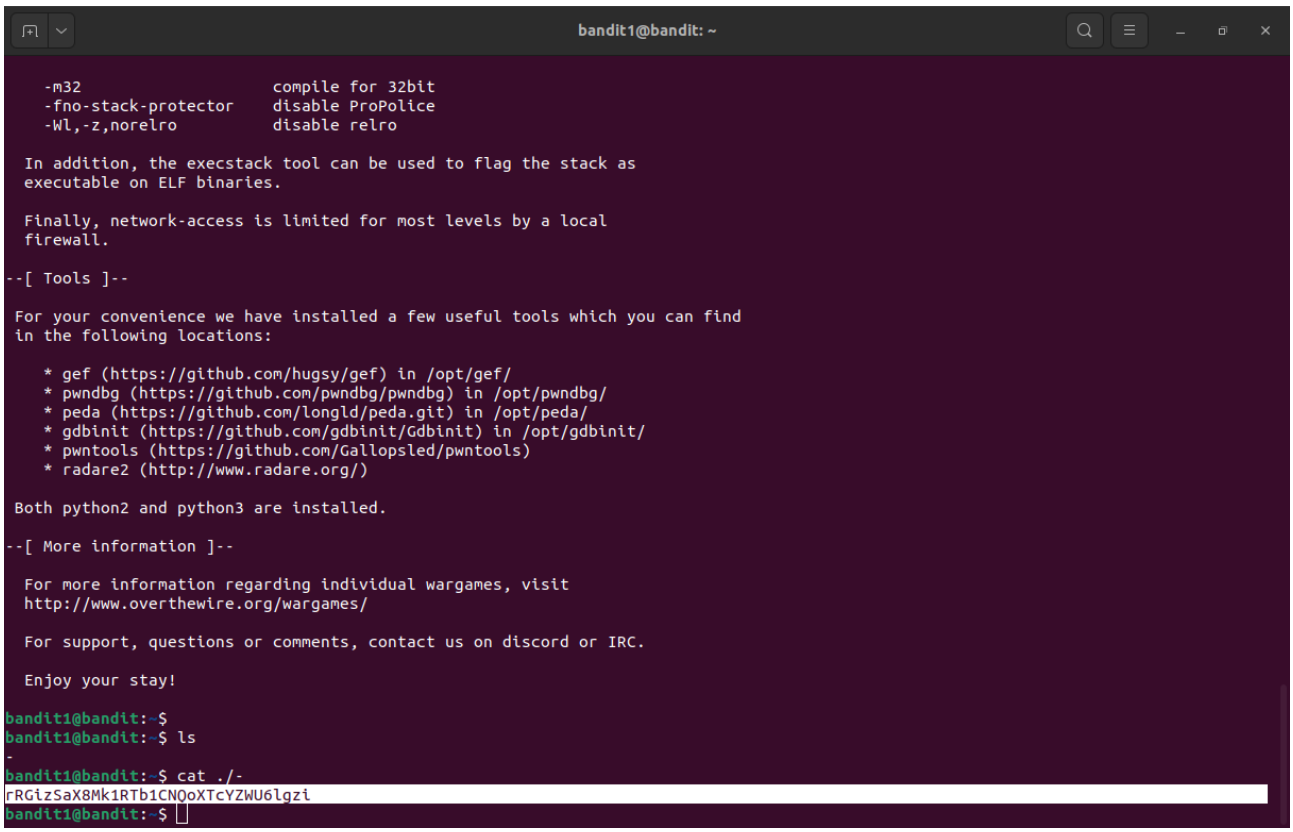
Host : bandit.labs.overthewire.org

2.Used ls command to look for files

3.Found a file named readme

4.Used cat command to read the file

5.Found the password to be NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL



Bandit 1=>2

1.Logged on using ssh

Hostname : bandit1

Password : **NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL**

Port : 2220

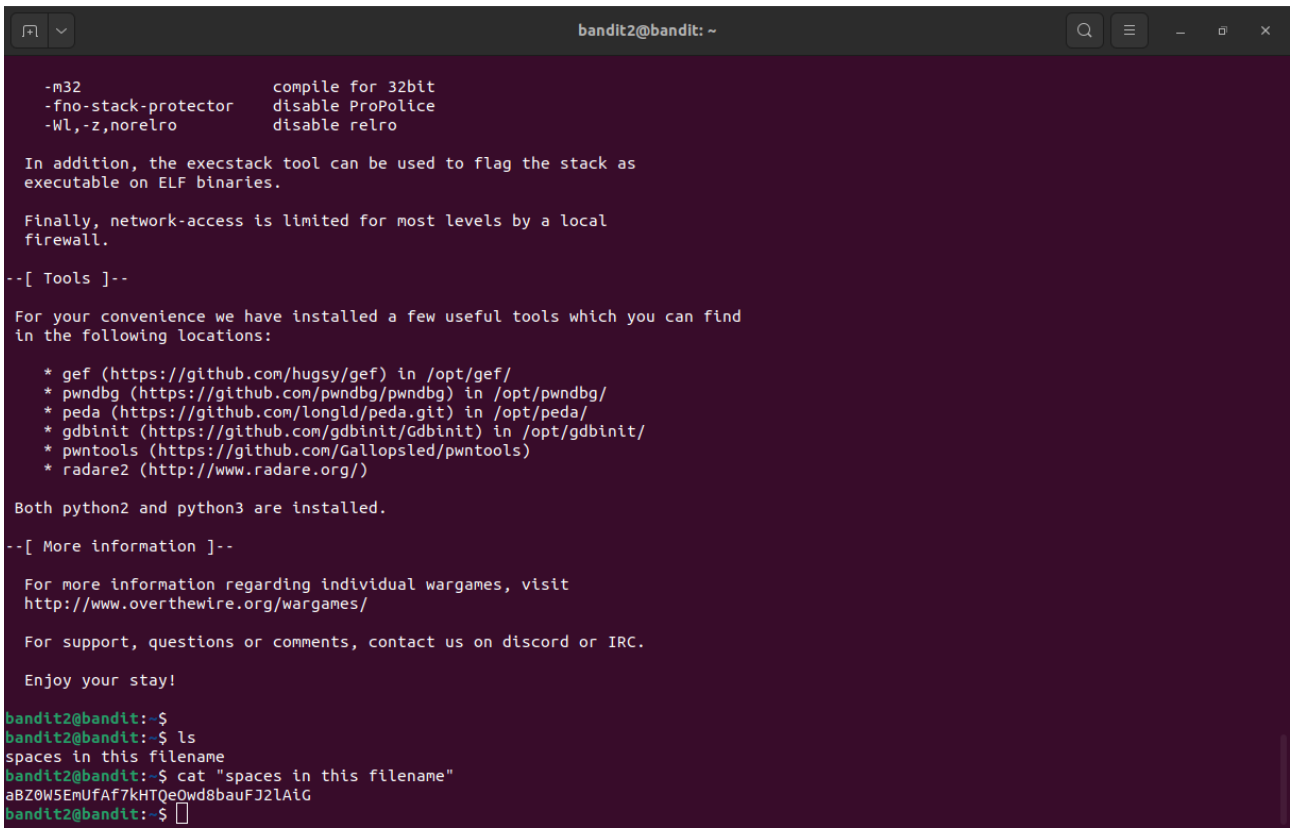
Host : bandit.labs.overthewire.org

2.Looked for files by using the ls command

3.Found a file named “-”

4.Found out that it starts with a special character and cant be directly opened with the cat command so added “./” after the command

5.Found the password to be **rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi**



Bandit 2=>3

1.Logged on using ssh

Hostname : bandit2

Password : **rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi**

Port : 2220

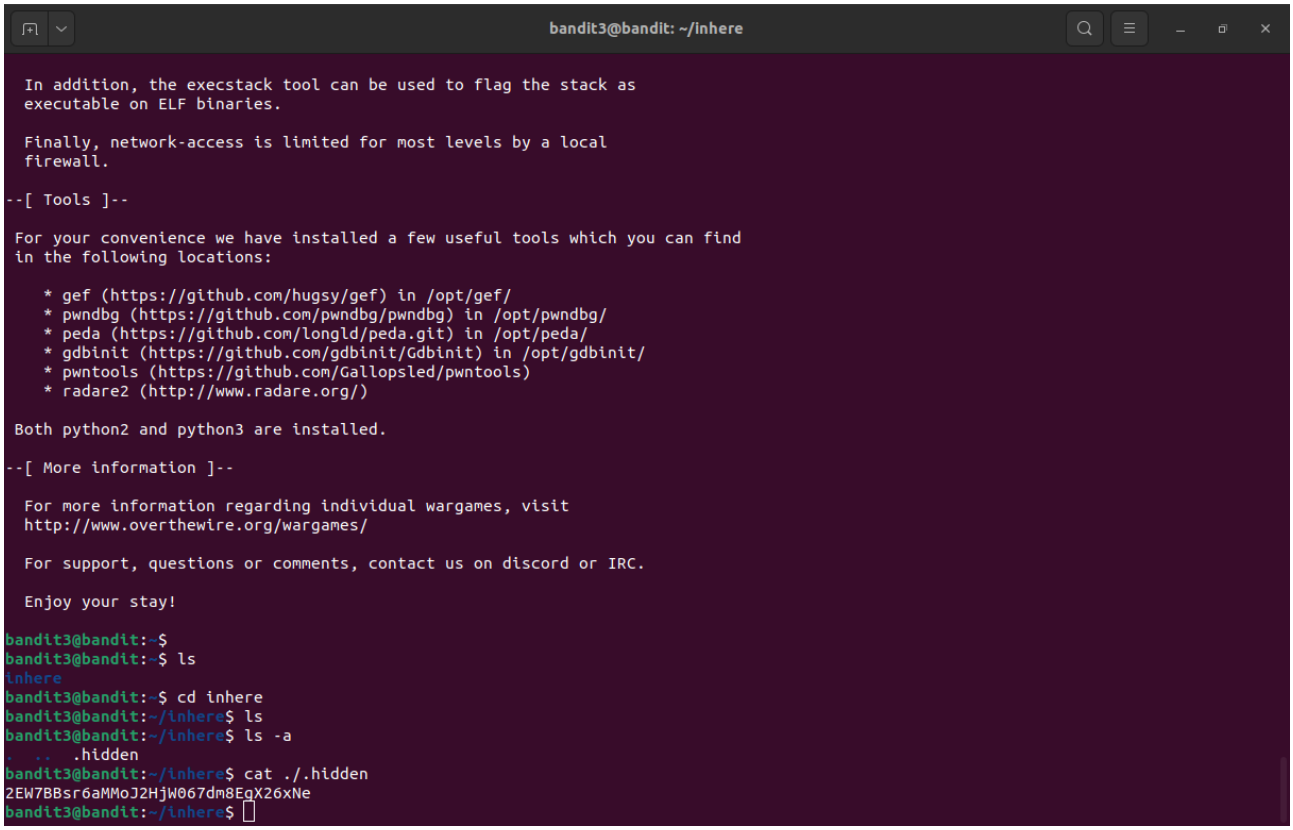
Host : bandit.labs.overthewire.org

2.Looked for files using the ls command

3.Found a file named “spaces in this filename”

4.Used the cat command on the file wrapped up in “”

5.Found the password to be **aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG**



Bandit 3=>4

1.Logged on using ssh

Hostname : bandit3

Password : **aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG**

Port : 2220

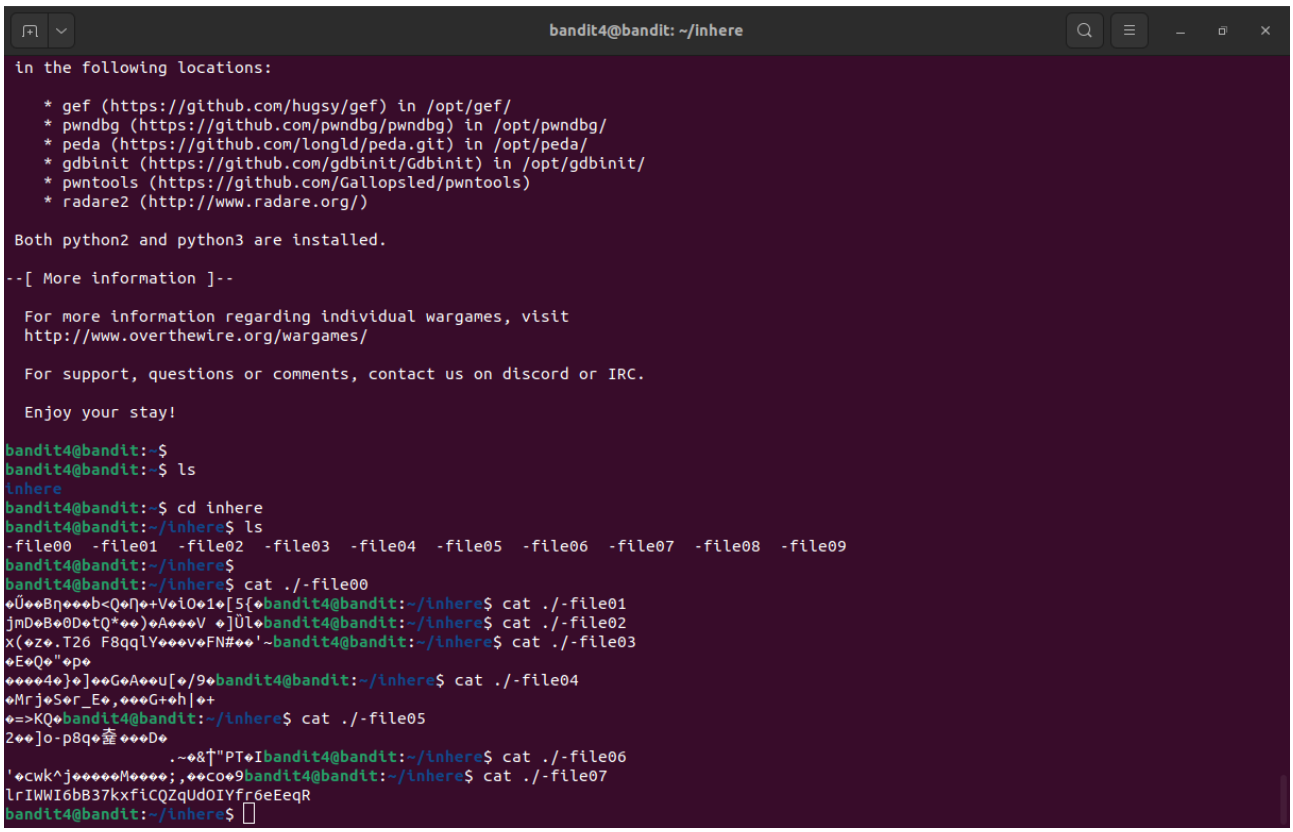
Host : bandit.labs.overthewire.org

2.Looked for files using the ls command but didnt find any

3.So used the ls -a command to look for any hidden files found a file named .hidden

4.Used cat ./ command since it started with a special character

5.Found the password to be **2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe**



Bandit 4=>5

1.Logged on using ssh

Hostname : bandit4

Password : **2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe**

Port : 2220

Host : bandit.labs.overthewire.org

2.Looked for files using ls command

3.Found a file named inhere

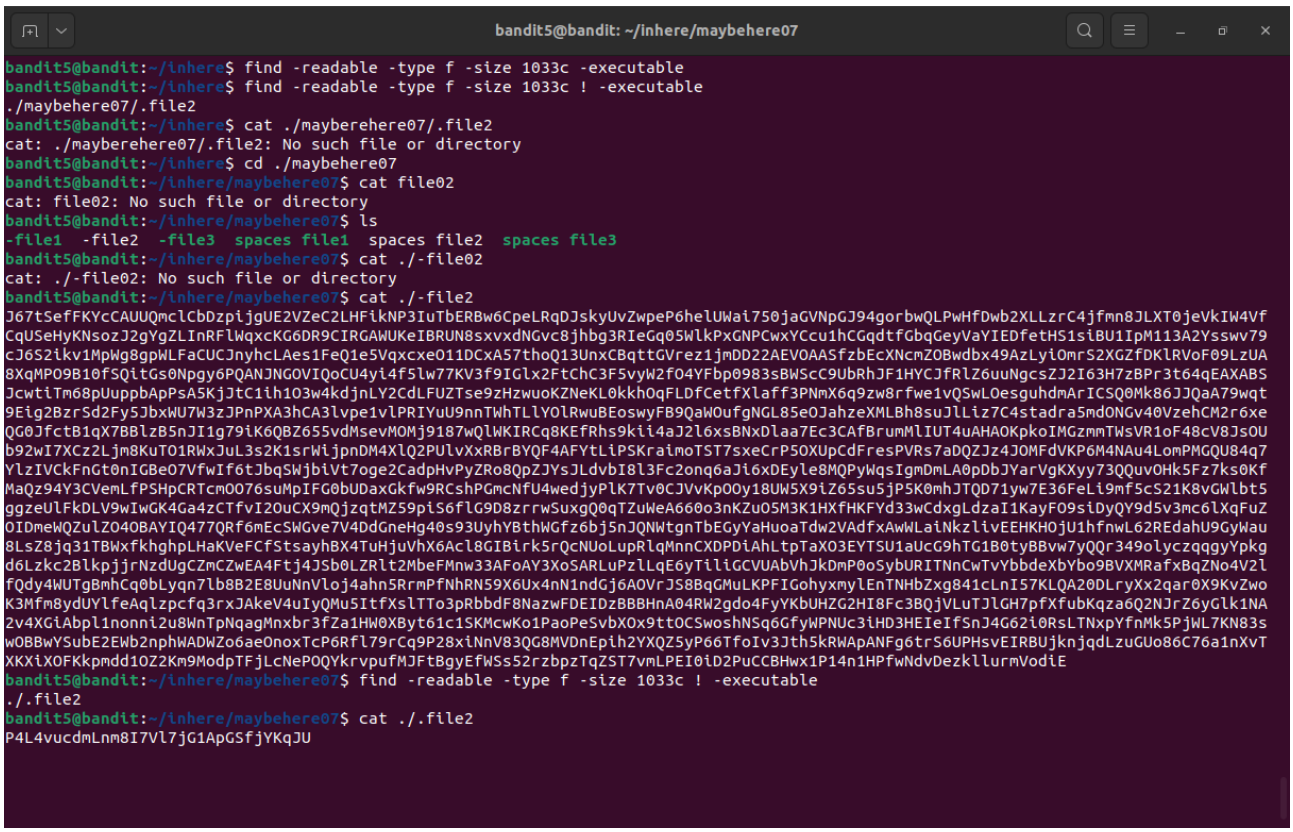
4.Set that as directory using the cd command

5.Looked for files using the ls command and found 10 files

6.Looked into each one of them using the cat command

7.Found the password in “-file07”

8.Pass = **lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR**



Bandit 5=>6

1.Logged on using ssh

Hostname : bandit5

Password : **lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR**

Port : 2220

Host : bandit.labs.overthewire.org

2.Looked for files using the ls command

3.Found a file named inhere and opened it

4.Found several files and thought they cant be checked one by one

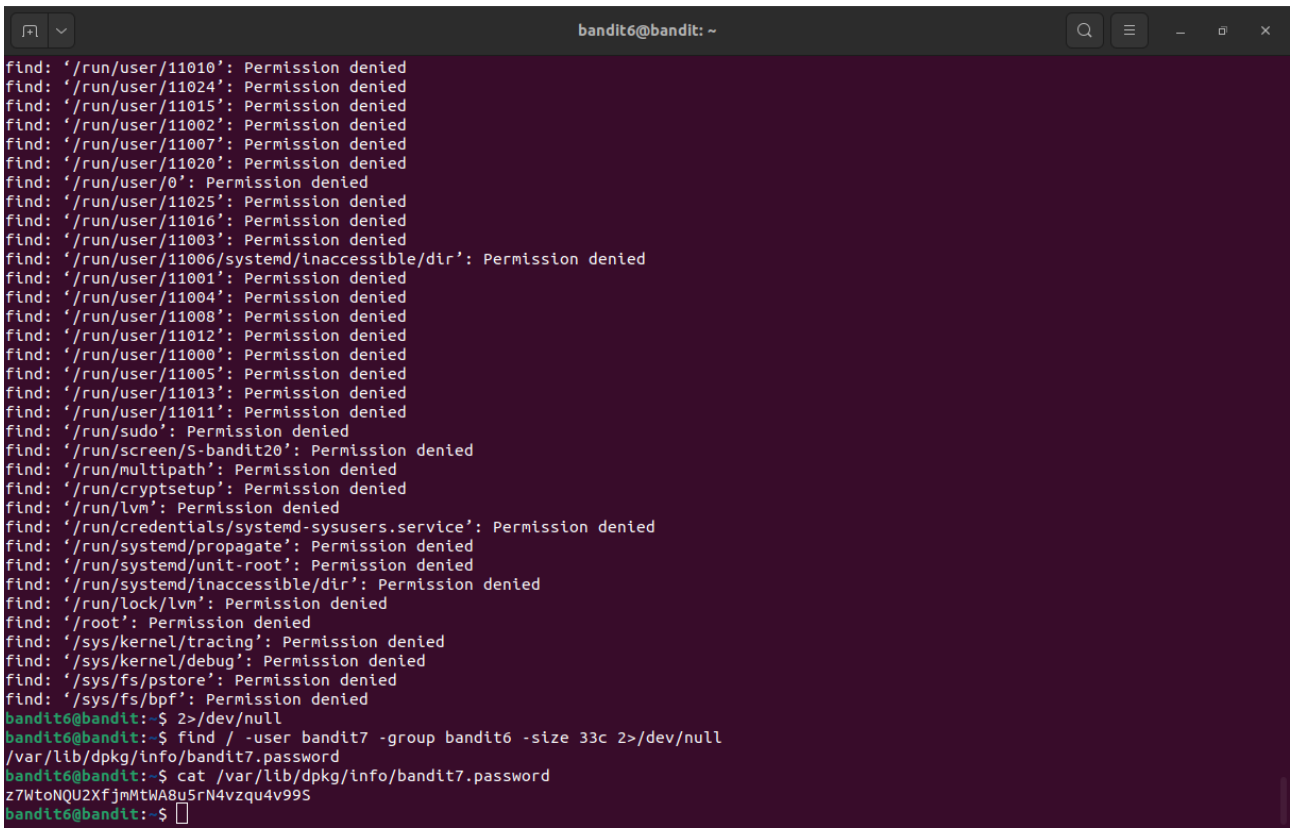
5.Used the find command to find a file related to the clues given in the website

6.Used find -readable -type f -size 1033c ! -executable

7.Found the file in .maybeinhere07/.file02

8.First opened a wrong file and then corrected it

9.Found the password to be **P4L4vucdmLnm8I7VI7jG1ApGSfjYKqJU**



Bandit 6=>7

1.Logged on using ssh

Hostname : bandit6

Password : **P4L4vucdmLnm8I7VI7jG1ApGSfjYKqJU**

Port : 2220

Host : bandit.labs.overthewire.org

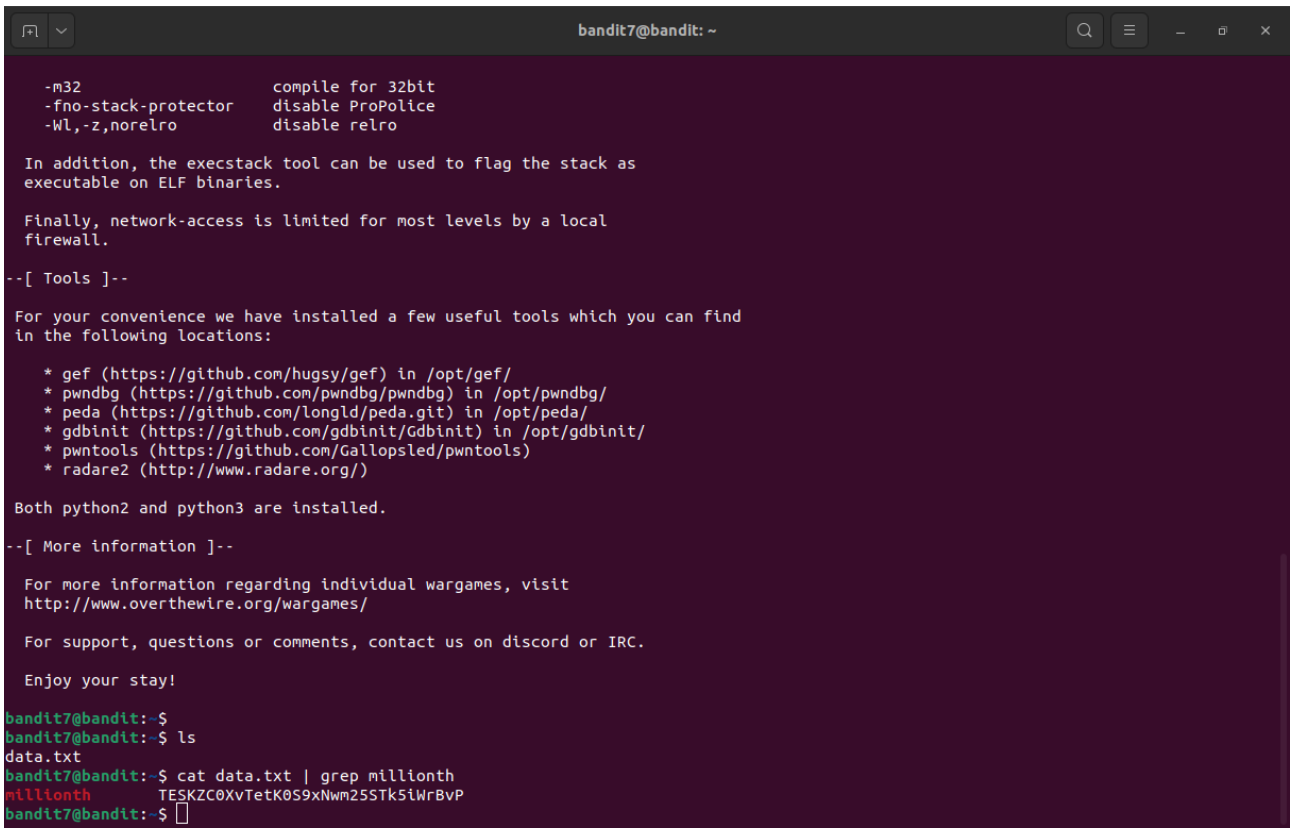
2.Looked for files using the ls command and found nothing

3.Used the find command “find / -user bandit7 -group bandit6 -size 33c 2>/dev/null”

4.Got a path to a file

5.Used cat on that path

6.Found out the password to be **z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S**



Bandit 7=>8

1.Logged on using ssh

Hostname : bandit7

Password : **z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S**

Port : 2220

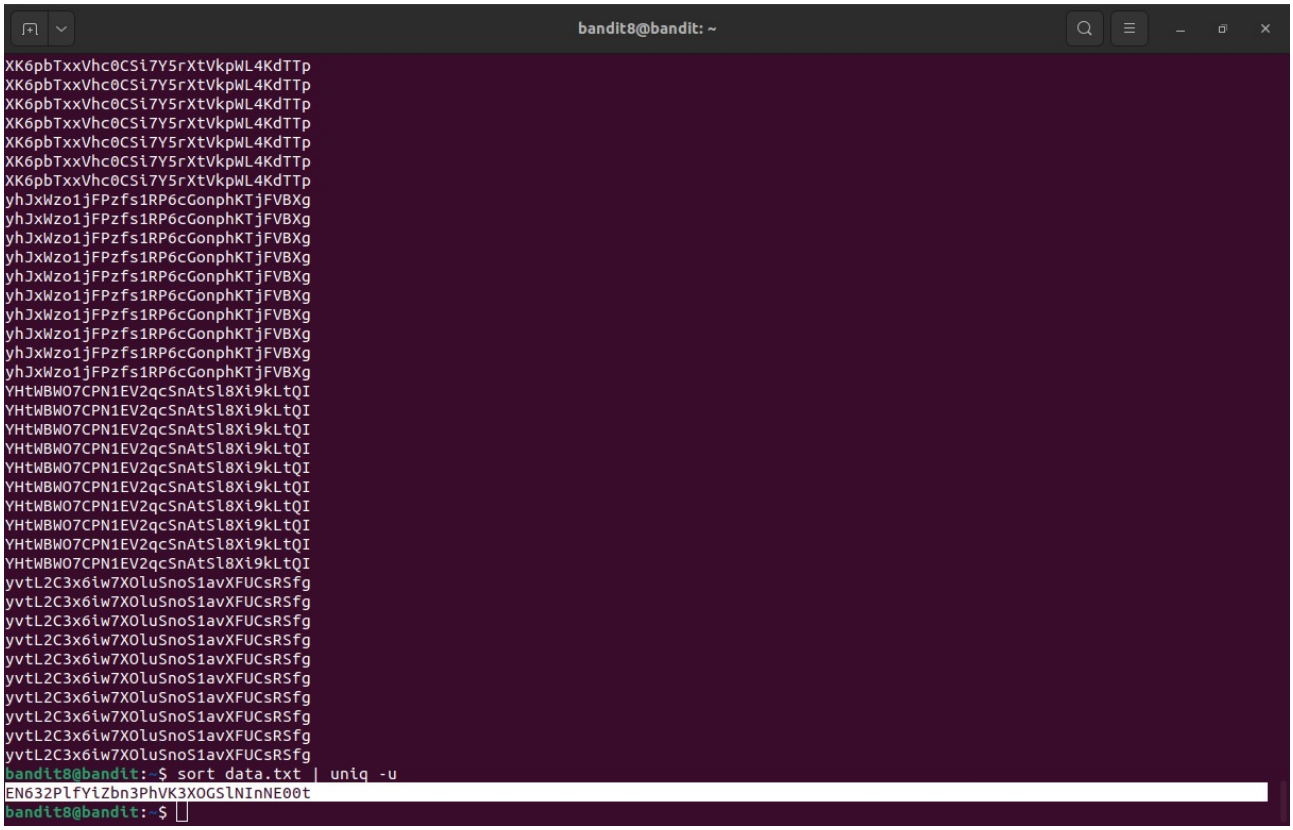
Host : bandit.labs.overthewire.org

2.Used the ls command to search for files and found data.txt

3.It is said that the password is next to the word millionth

4.So I used “cat data.txt | grep millionth

5.Found out the password to be **TESKZC0XvTetK0S9xNwm25STk5iWrBvP**



Bandit 8=>9

1.Logged on using ssh

Hostname : bandit8

Password : **TESKZC0XvTetK0S9xNwm25STk5iWrBvP**

Port : 2220

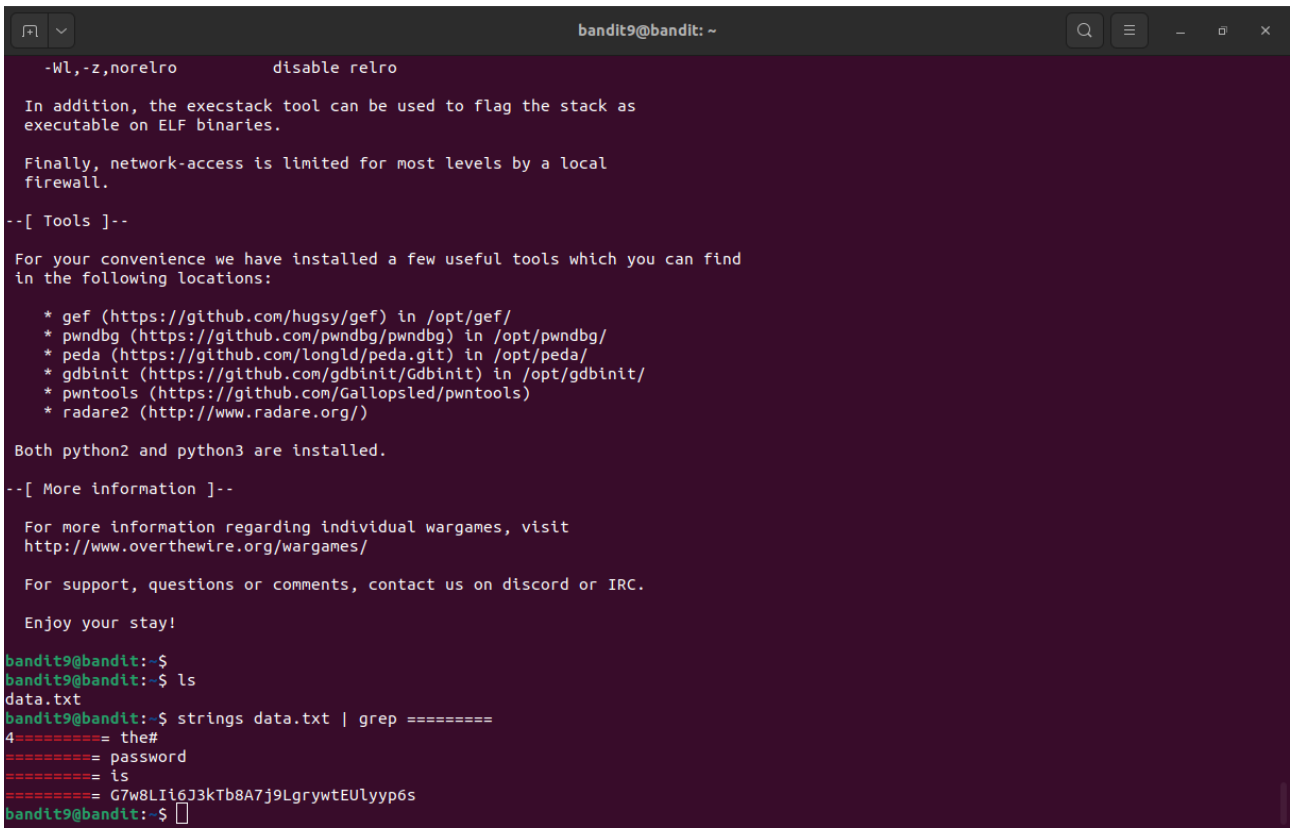
Host : bandit.labs.overthewire.org

2.Used ls to search for any document

3.Found data.txt

4.Used sort data.txt | uniq -u

5.Found the unique password to be **EN632PlfYiZbn3PhVK3XOGSlNInNE00t**



Bandit 9=>10

1.Logged on using ssh

Hostname : bandit9

Password : **EN632PlfYiZbn3PhVK3XOGSlNInNE00t**

Port : 2220

Host : bandit.labs.overthewire.org

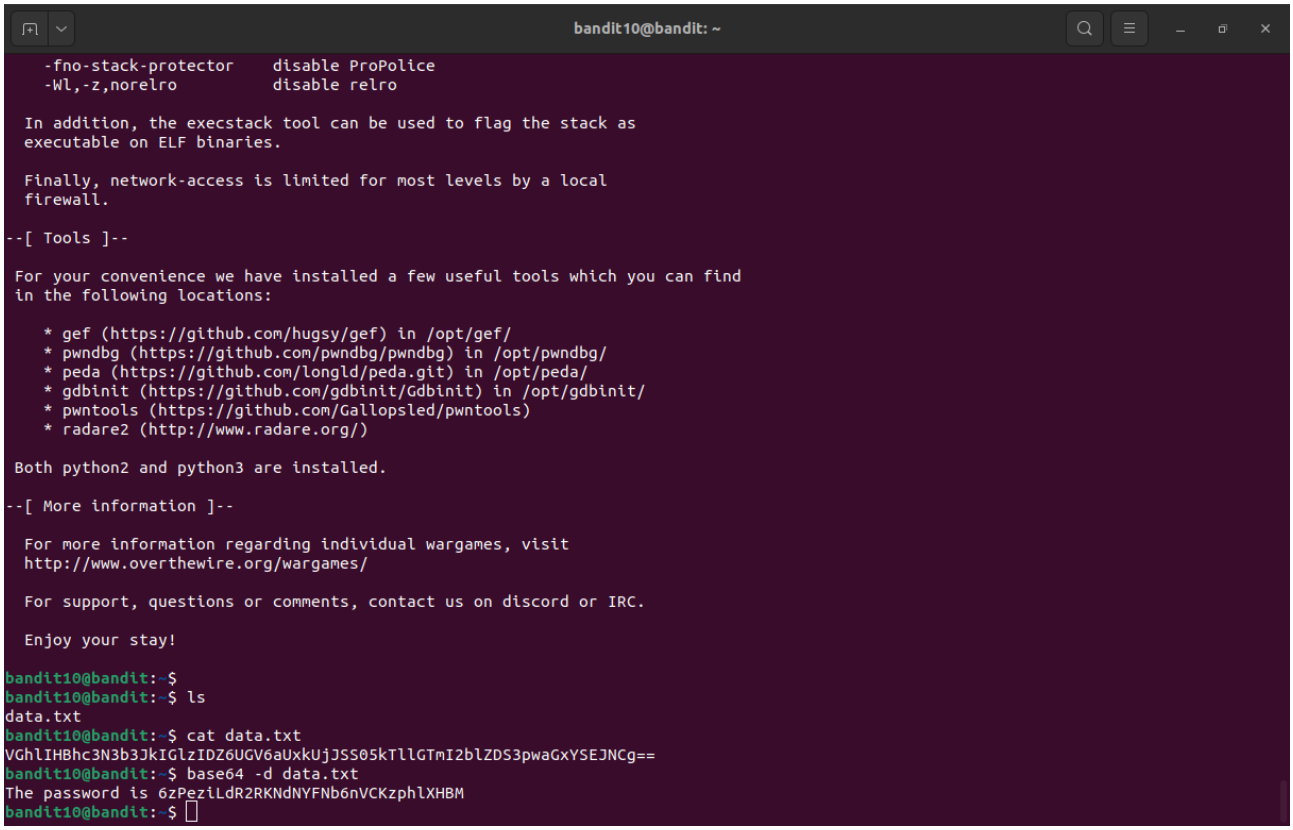
2.Used ls command to look for any files

3.Found data.txt

4.It is said that the password contains a series of = symbols

5.So used strings data.txt | grep ====

6.Found out the password to be **G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s**



Bandit 10=>11

1.Logged on using ssh

Hostname : bandit10

Password : **G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s**

Port : 2220

Host : bandit.labs.overthewire.org

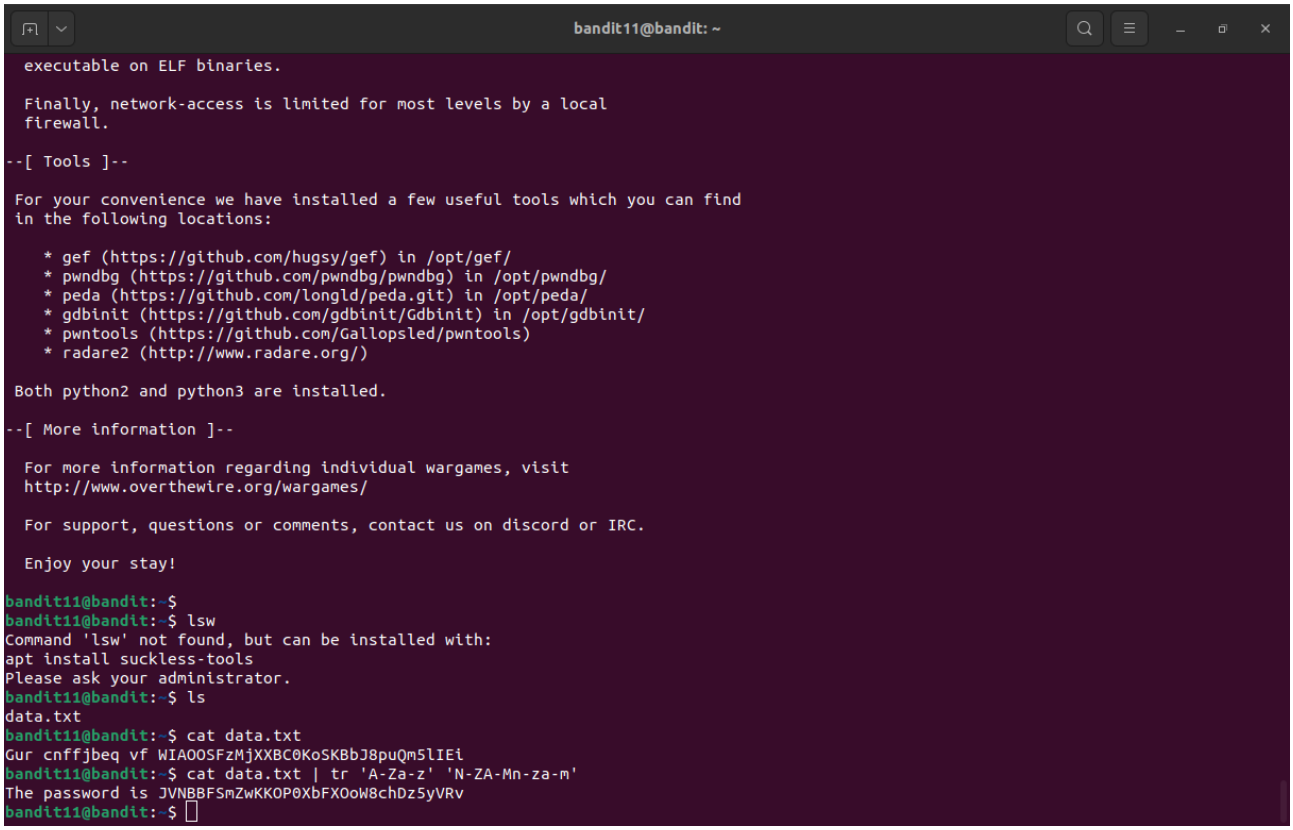
2.Used ls command to look for any files and found out data.txt

3.Opened the file using cat command

4.Looked at the two == symbols at the end and found out that it might be base 64 encoded string

5.Decoded it using base64 -d data.txt command

6.Found out the password to be **6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM**



Bandit 11=>12

1.Logged on using ssh

Hostname : bandit11

Password : **6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM**

Port : 2220

Host : bandit.labs.overthewire.org

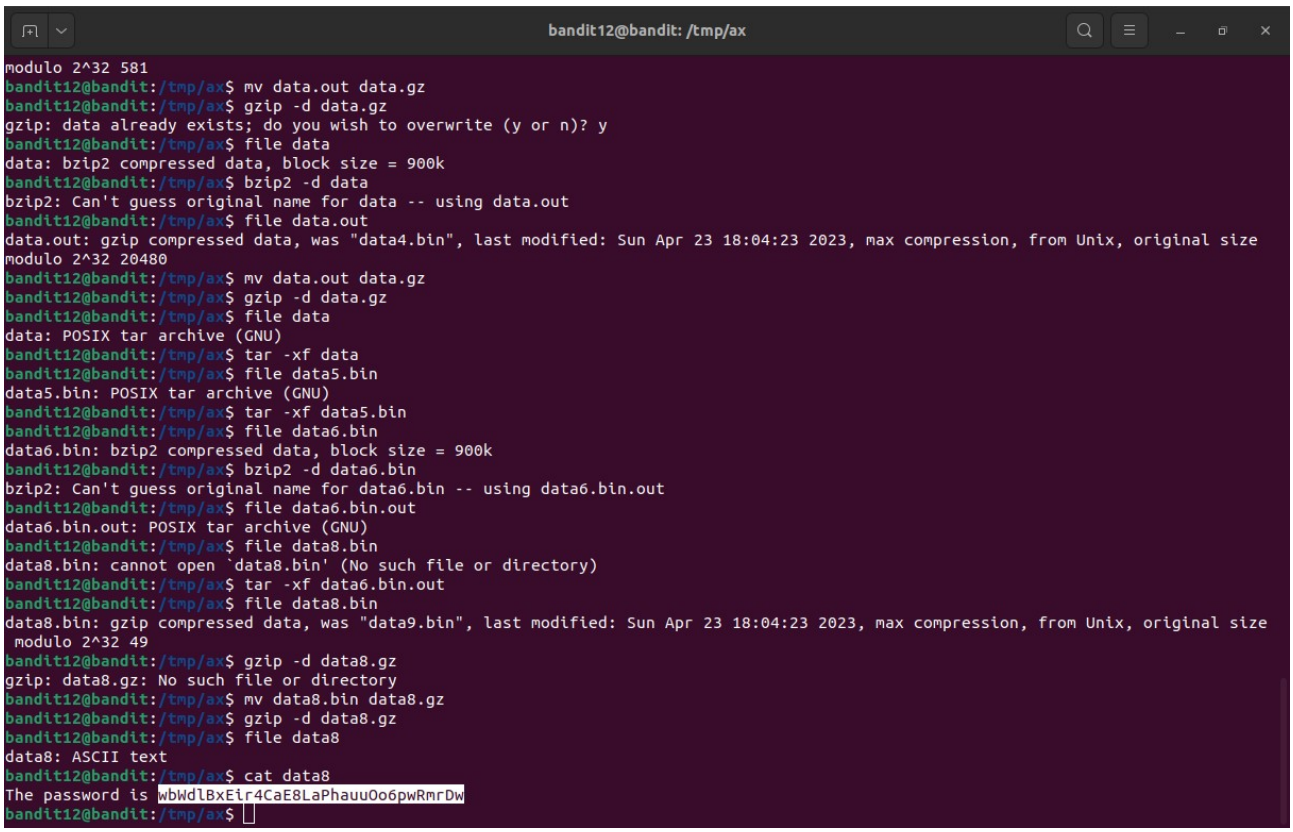
2.Used ls command to look for any files and found out data.txt

3.Opened the file using cat command and got a weird set of characters

4.Googled it for some clues and found it to be a rot 13 encoded string

5.Used the cat data.txt | tr ‘A-Za-z’ ‘N-ZA-Mn-za-m’

6.Found out the password to be **JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv**



Bandit 12=>13

1.Logged on using ssh

Hostname : bandit12

Password : **JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv**

Port : 2220

Host : bandit.labs.overthewire.org

2.Created a working folder using the mkdir command in *tmp*/ax/

3.Converted hex to binary using the xxd -x data.txt data.out

4.Checked the file type of data.out using the file command

5.It was in the gzip compressed format

6.Renamed data.out to data.gz using the mv command

7.So decompressed using the gzip -d data.gz command

8.Again used the file command and found out that data is in bzip2 compressed file

9.So decompressed it using the bzip2 -d data

10.It gave a prompt that the file name has been changed to data.out

11.Checked the file type and found out that it is again gzip compressed format

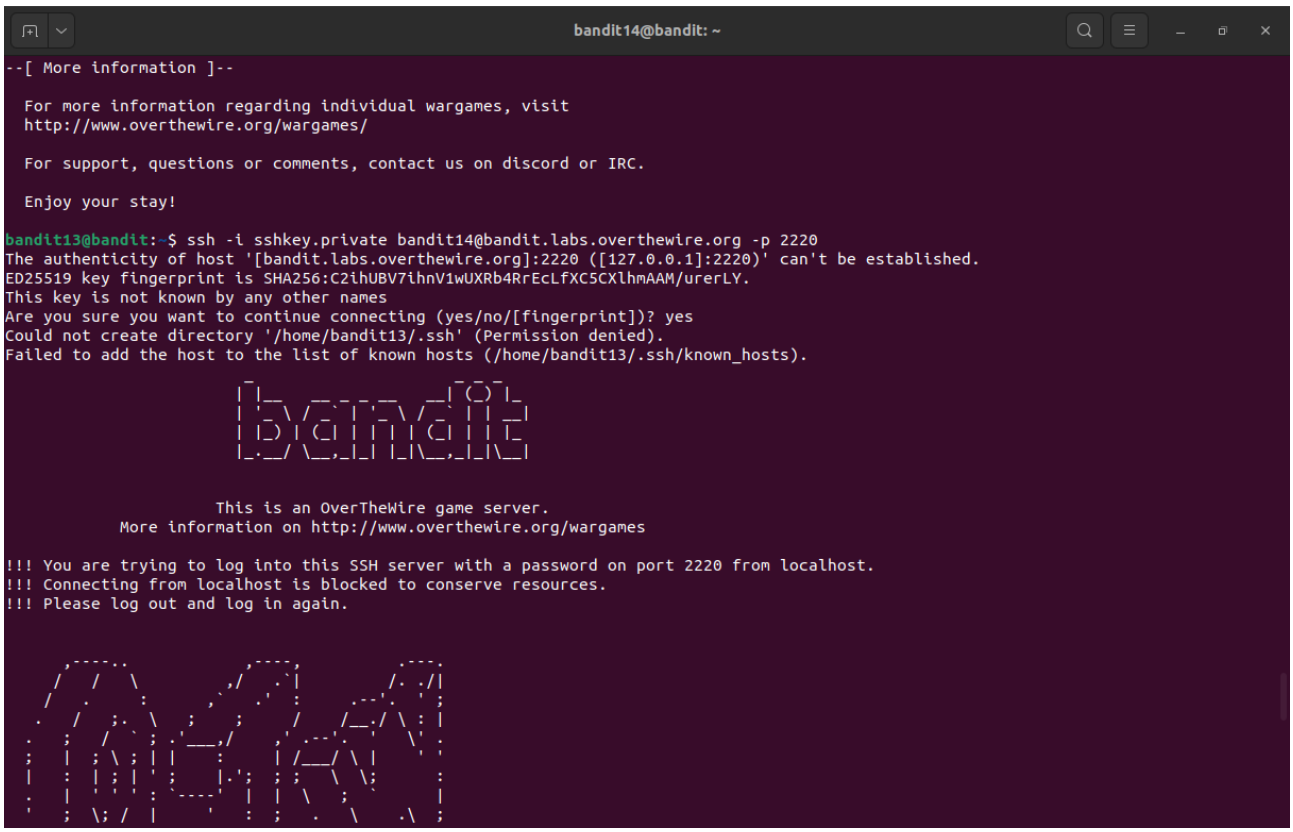
12.Changed its name to data.gz and decompressed it again

13.Now the file type is in POSIX tar archive

14.So I used the tar command to decompress and repeated this until the file is in the ASCII text format

15 Used cat command on the file after it is converted to ASCII file

16.Found the password to be **wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw**



Bandit 13=>14

1.Logged on using ssh

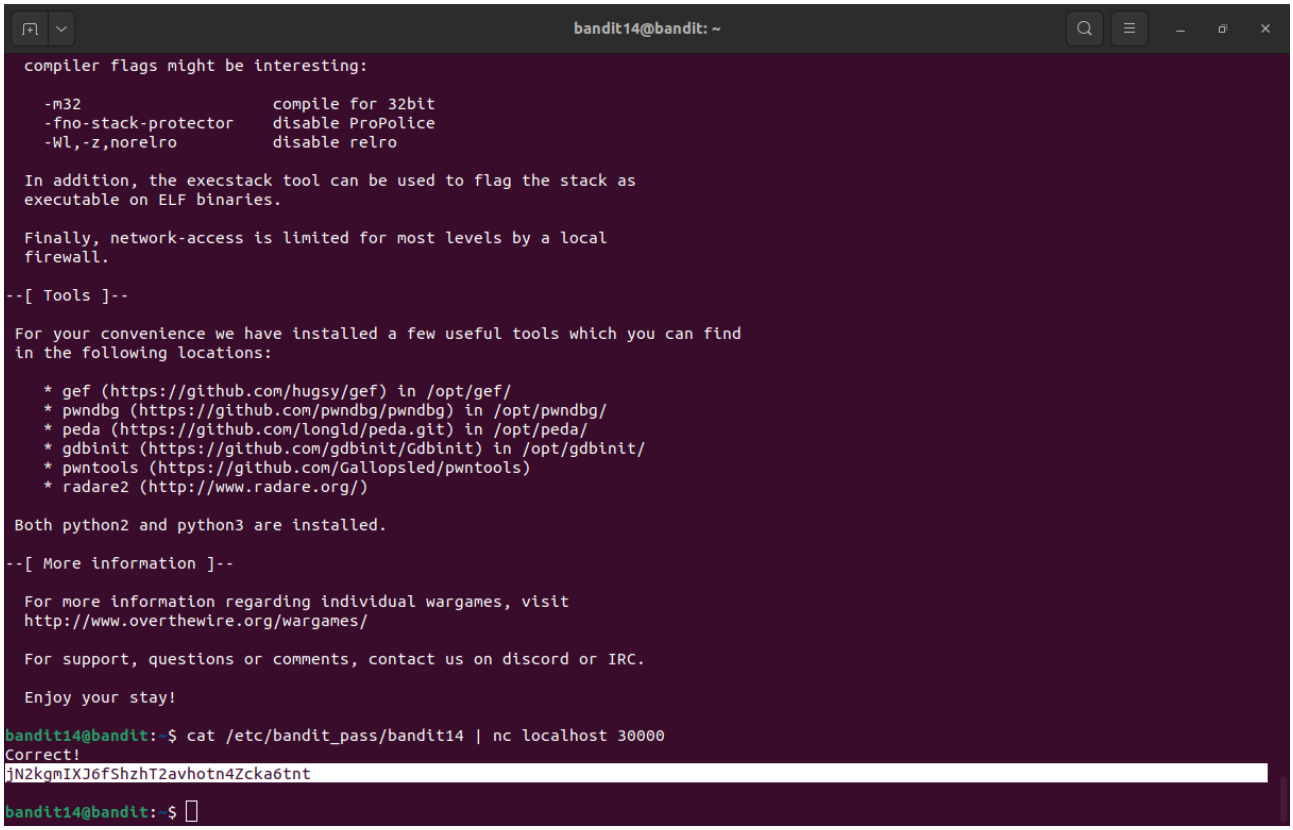
Hostname : bandit13

Password : **wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw**

Port : 2220

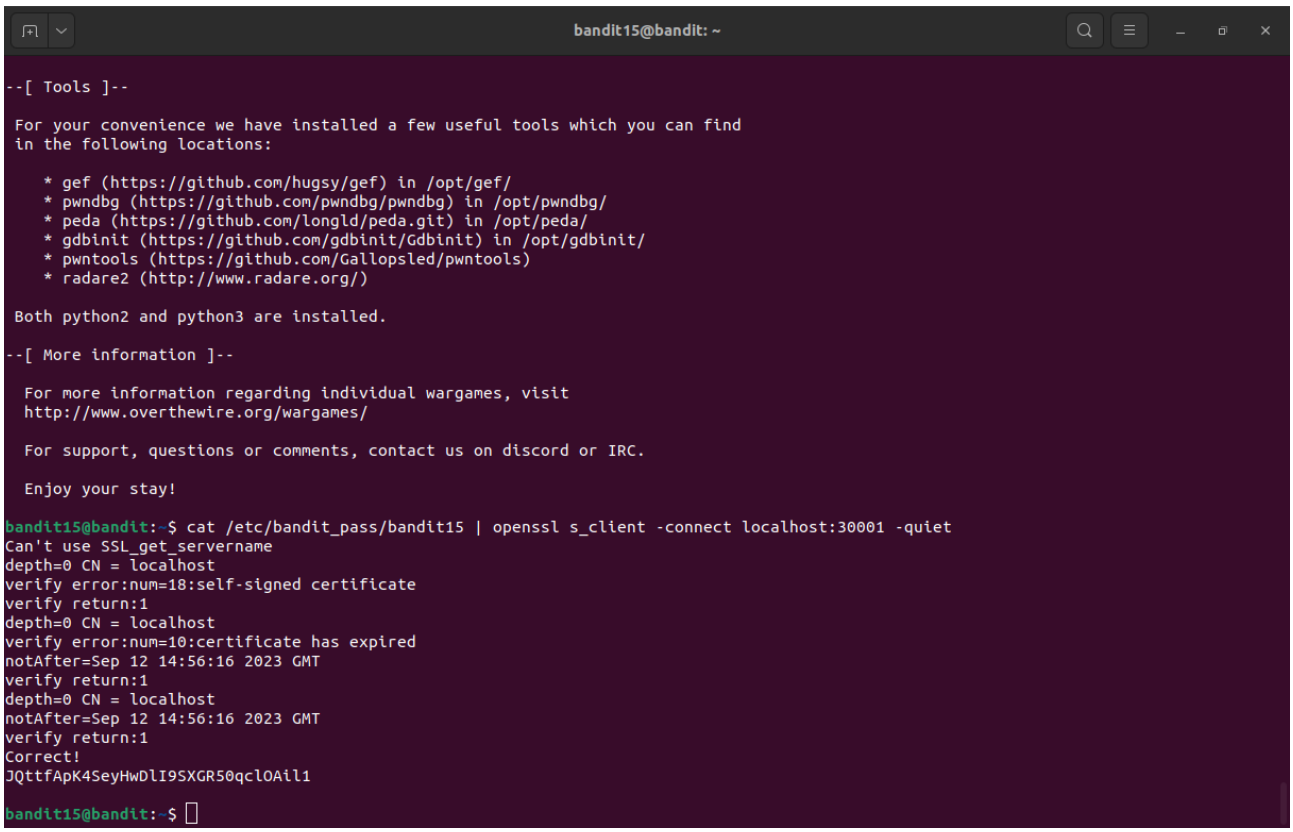
Host : bandit.labs.overthewire.org

2.The password for the next level is in sshkey.private which we can use to directly login to level 14



Bandit 14=>15

1.Logged in directly from level 13 using the sshkey.private
2.The passwrod must be submitted to the port 30000
3.The password is in the *etc/*bandit_pass/bandit14
4.The pass can be submitted directly using cat *etc/*bandit_pass/bandit14
5.Got the password **jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt**



Bandit 15=>16

1.Logged on using ssh

Hostname : bandit15

Password : **jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt**

Port : 2220

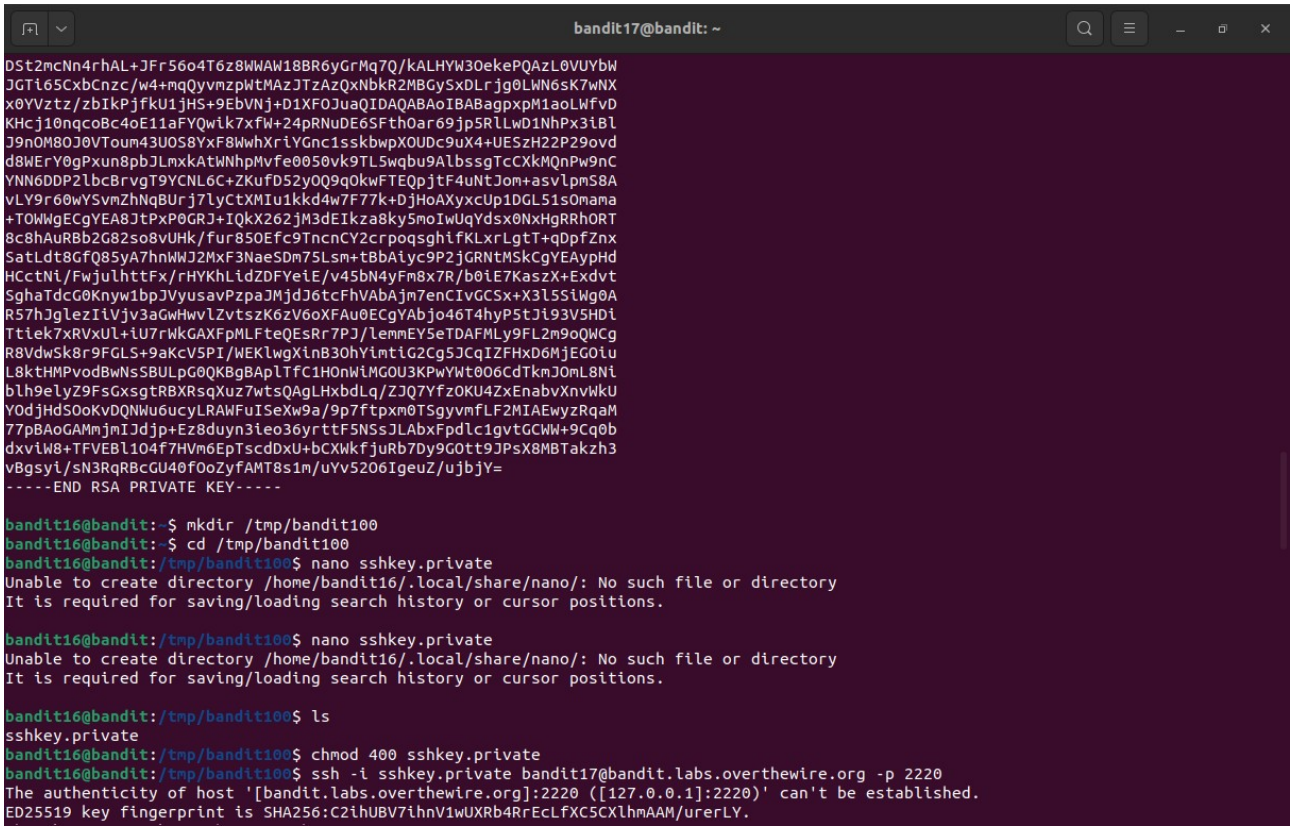
Host : bandit.labs.overthewire.org

2.The password for the next level can be retrieved by submitting the password of the current level to **port 30001 on localhost** using SSL encryption.

3.The pass is in *etc*bandit_pass/bandit15

4.The pass can be submitted using the command cat */etc/*bandit_pass/bandit15 | openssl s_client -connect localhost:>30001 -quiet

5.Now we get the pass for the next level **JqttfApK4SeyHwDlI9SXGR50qclOAil1**



Bandit 16=>17

1.Logged on using ssh

Hostname : bandit16

Password : **JqttfApK4SeyHwDlI9SXGR50qclOAil1**

Port : 2220

Host : bandit.labs.overthewire.org

2.Search for open ports in between 31000 and 32000 which have server listening on them and must speak ssl

3.So I used “for i in {31000..32000} ; do”

```
>   SERVER="localhost"
>   PORT=$i
>   (echo  > /dev/tcp/$SERVER/$PORT) >& /dev/null &&
>    echo "Port $PORT open"
```

4. This gave me 5 ports out of which only two have echo and one have ssl listening to it

5.So the password has been sent to the port 31790 using the command “cat /etc/bandit_pass/bandit16 | openssl s_client -connect localhost:31790 -quiet”

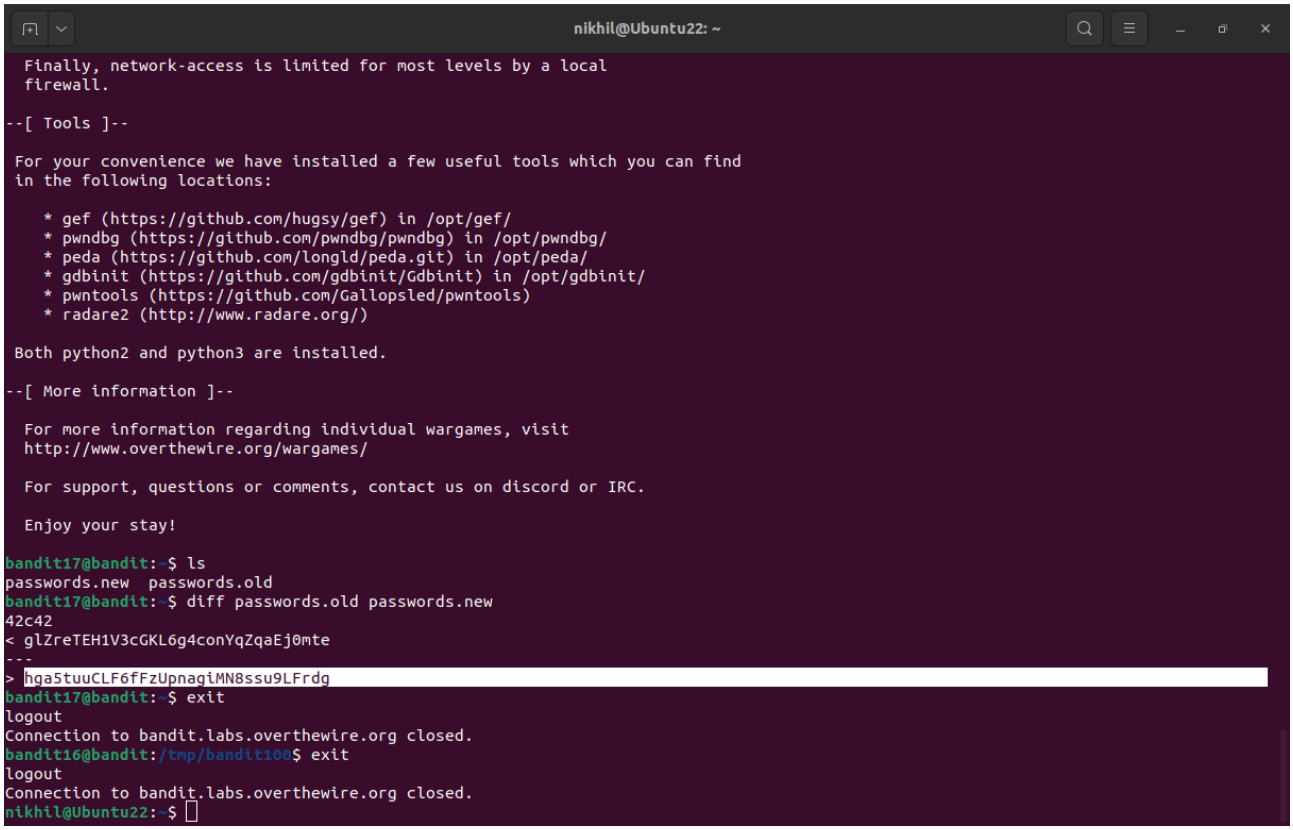
5.Sending the pass gave me a private rsa key

6.Now I created a directory using the mkdir command

7.Used the nano command to save the private key and named it to be sshkey.private

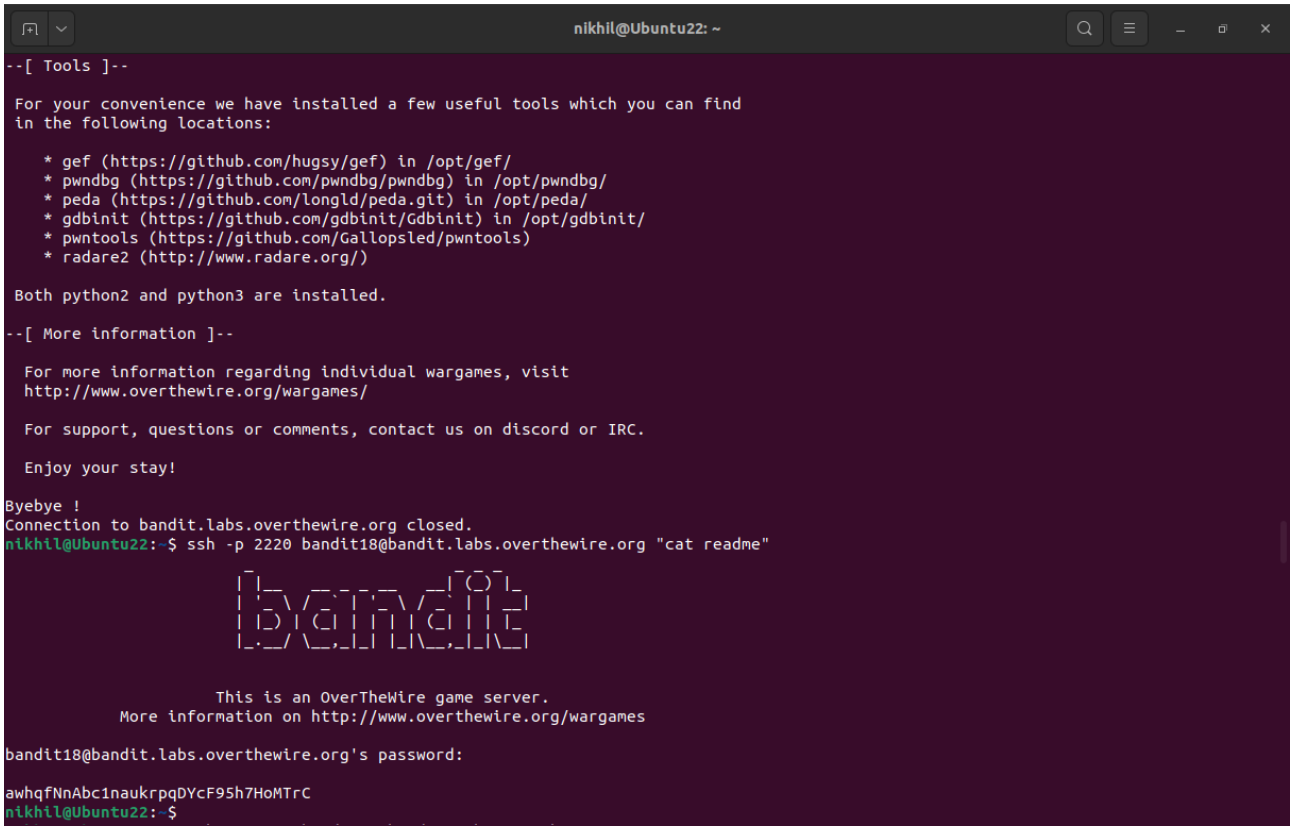
8.Now used chmod 400 sshkey.private to change the permission of the key to only admin

9.Now I used this key to directly access level 17



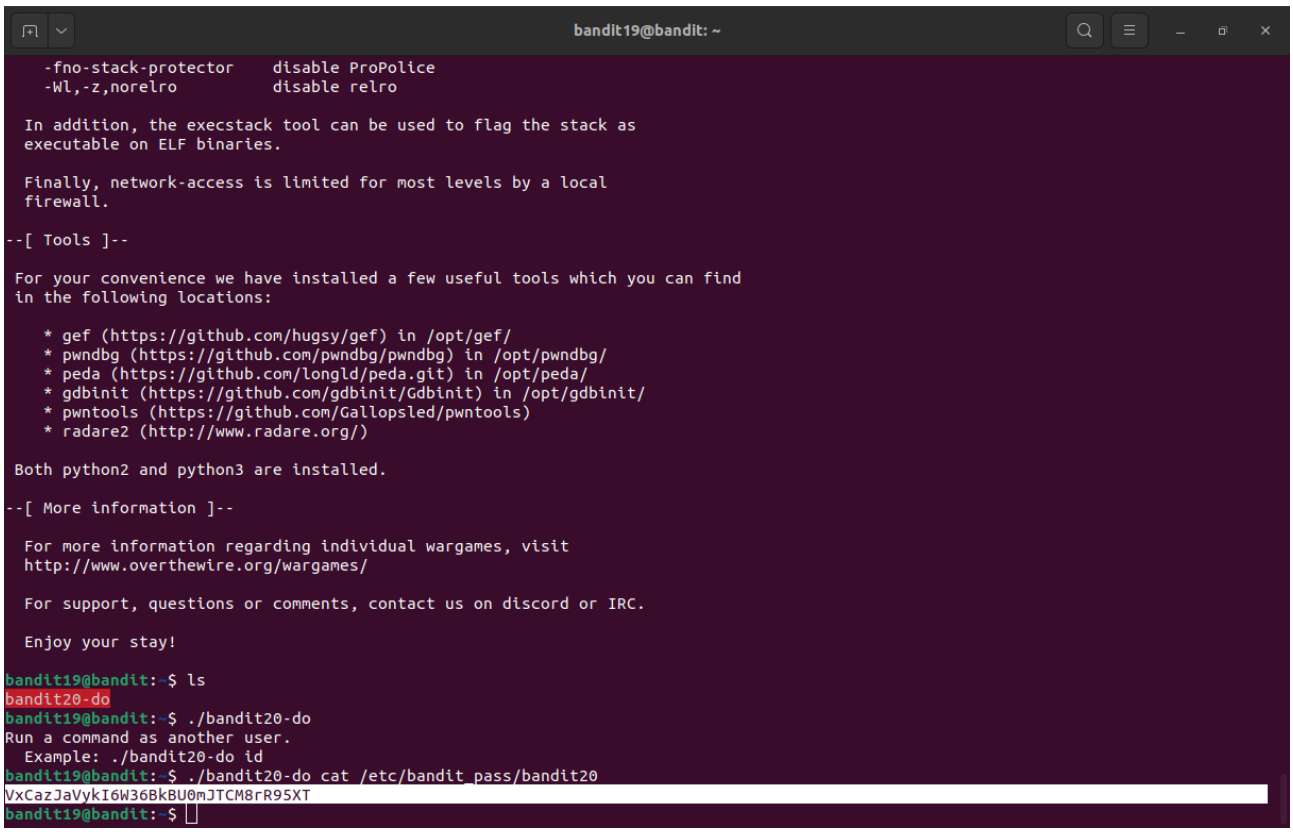
Bandit 17=>18

1.Logged in directly from level 16 using the private key given previously
2.Ran the ls command to look for the password files
3.Used diff command to compare the two files line by line
4.Used the first line of password and my permission to level 18 got denied
5.Now used the second line of password and got “ByeBye” at the end
6.Second line is **hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg**



Bandit 18=>19

1.Gets logged out if we try to login like the other levels
2.The password for the next level is in the readme file
3.So we can directly enter the command cat readme wrapped with “”
4.Then after entering the password we get the key for next levl to be
awhqfNnAbc1naukrpqDYcF95h7HoMTrC



Bandit 19=>20

1.Logged on using ssh

Hostname : bandit19

Password : **awhqfNnAbc1naukrpqDYcF95h7HoMTrC**

Port : 2220

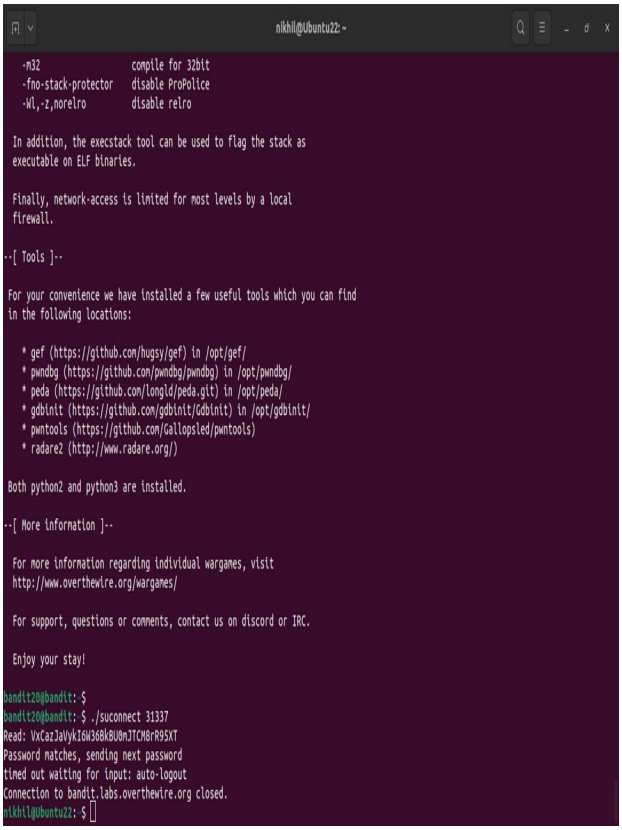
Host : bandit.labs.overthewire.org

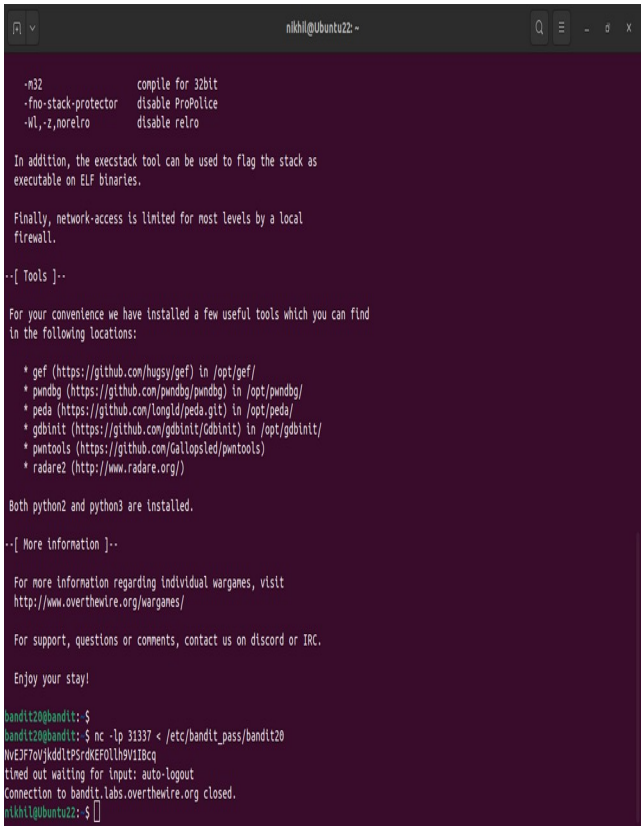
2.Used ls command to check for files

3.The password must be accessed as another user bandit20-do

4.So I used the command ./bandit20-do cat “/etc/bandit_pass/bandit20”

5.Found out the password to be **VxCazJaVykI6W36BkBU0mJTCM8rR95XT**





Bandit 20=>21

1.Logged on using ssh

Hostname : bandit20

Password : **VxCazJaVykI6W36BkBU0mJTCM8rR95XT**

Port : 2220

Host : bandit.labs.overthewire.org

2.Established a connection with ./suconnect 31337 command

3.Sent the password through another terminal using nc command

4.Then got the password **NvEJF7oVjkddltPSrdKEFOllh9V1IBcq**