BSc (Hons) in IT Specialized in CS Year 2 Semester 1,

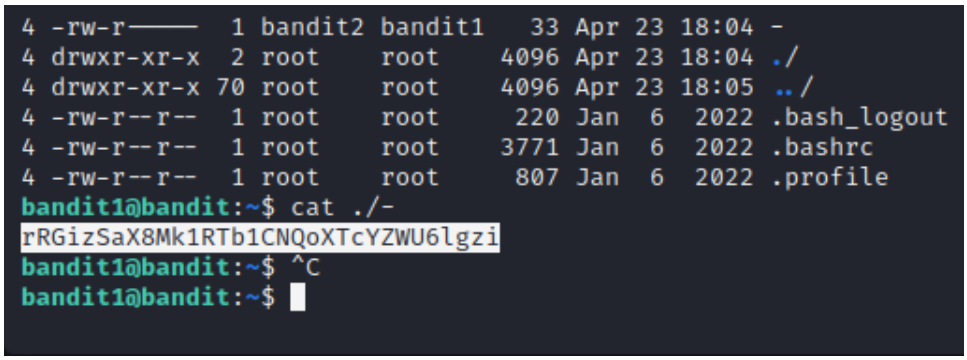
2023

SNP Work Sheet 01

IT22581402

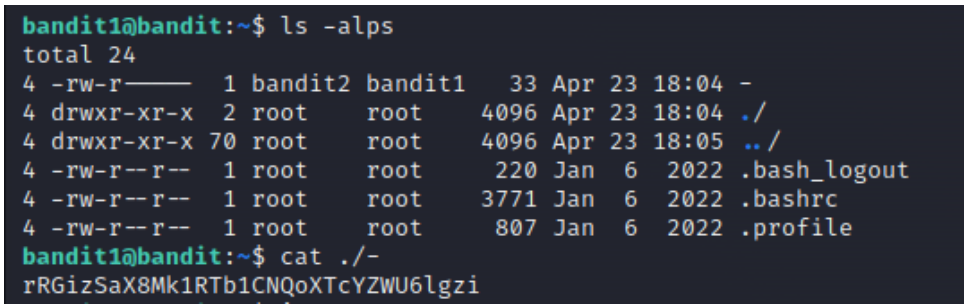
C.D.Aluthge

Level 0 -> Level 01



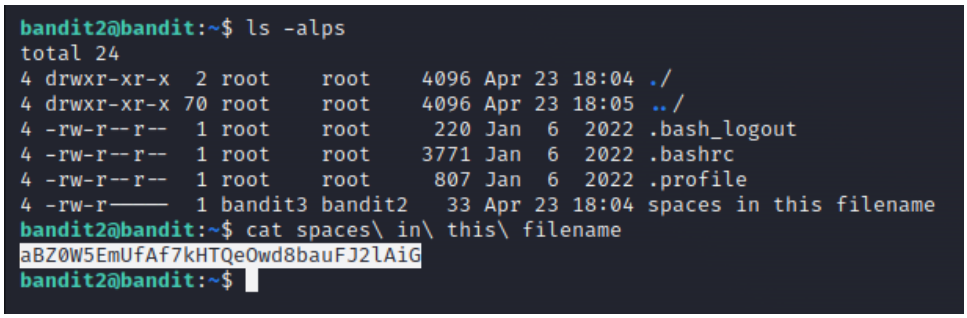
- First open the terminal type "**ssh** bandit0@bandit.labs.overthewire.org **-p 2220**" and press enter.
- Then give password as "**bandit0**"
- First open the terminal and press the then type "**ls**" command to show available files.
- after that type "**cat readme**" then you will display the password

Level 01 -> Level 02



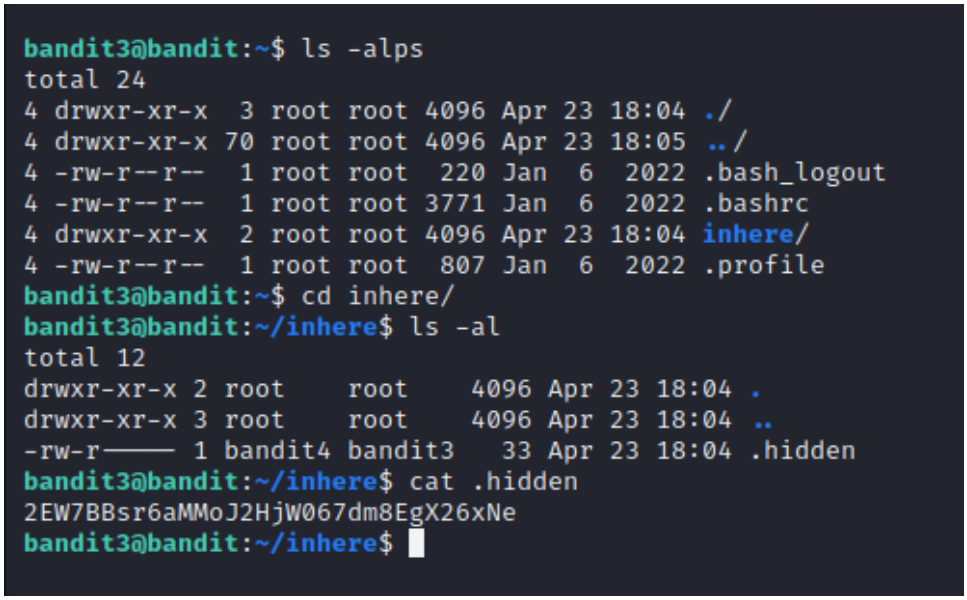
- Then type the "**ssh** bandit1@bandit.labs.overthewire.org **-p 2220**" on the terminal.
- Enter the password we found in level1 "**NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL**"
- Type the **ls** command and type **cat ./-** then you can see the password.

Level 02-> Level 03



- Then type the "**ssh bandit2@bandit.labs.overthewire.org -p 2220**" on the terminal.
- After that using ls command can see the file directory
- Then you can get the password using **"cat spaces\ in\ this\ filename"** command.

Level 03-> Level 04



- Then type the "**ssh bandit3@bandit.labs.overthewire.org -p 2220**" on the terminal.
- In this level password is stored in a hidden file in the **inhere** directory.
- First need to go inhere directory using "**cd inhere"** command.
- After that type **"cat. Hidden"** to viwe the password.

Level 04-> Level 05

```
bandit4@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root root 4096 Apr 23 18:04 ./
4 drwxr-xr-x 70 root root 4096 Apr 23 18:05 ../
4 -rw-r--r--  1 root root  220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root root 3771 Jan  6  2022 .bashrc
4 drwxr-xr-x  2 root root 4096 Apr 23 18:04 inhere/
4 -rw-r--r--  1 root root  807 Jan  6  2022 .profile
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ find . -type f | xargs file
./-file03: data
./-file06: data
./-file08: data
./-file07: ASCII text
./-file04: data
./-file00: data
./-file01: data
./-file02: data
./-file09: Non-ISO extended-ASCII text, with no line terminators
./-file05: data
bandit4@bandit:~/inhere$ man xargs
bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$
```

- Then type the "**ssh bandit4@bandit.labs.overthewire.org -p 2220**" on the terminal.
- In this level password is stored in the only human-readable file in the **inhere** directory.
- First need to go inhere directory using "**cd inhere"** command.
- Using **"ls"** command you can see the available files.
- After using **"file ./*"** you can see the type of files.one of the file type is deferent from others.
- Run the **"cat ./-file07"** command and will display the password.

Level 05-> Level 06

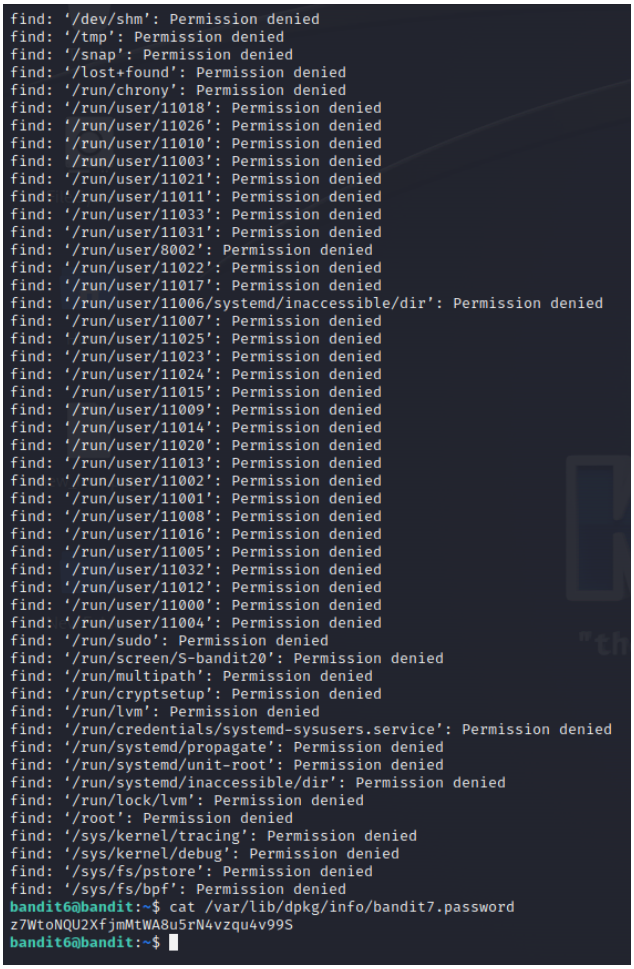
```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
                                                    bandit5@bandit:~/inhere$ ^C
bandit5@bandit:~/inhere$
```

- Then type the "**ssh bandit5@bandit.labs.overthewire.org -p 2220**" on the terminal.
- In this level password is tored in a file somewhere under the **inhere** directory and has all of the following properties:

1) human-readable
2) 1033 bytes in size
3) not executable

- First need to go inhere directory using "**cd inhere"** command.
- Then find the all bandit5 directories using "ls -al" command.
- Then find the password location using **"find . -readable -size 1033c ! -executable"** and will display **"./maybehere07/.file2".**
- Using cat command can easily retrieve the password.

Level 06-> Level 07



Exit from the bandot5using "exit" command.

Then type the "**ssh bandit6@bandit.labs.overthewire.org -p 2220**" on the terminal.

In this level password is stored **somewhere on the server** and has all of the following properties:

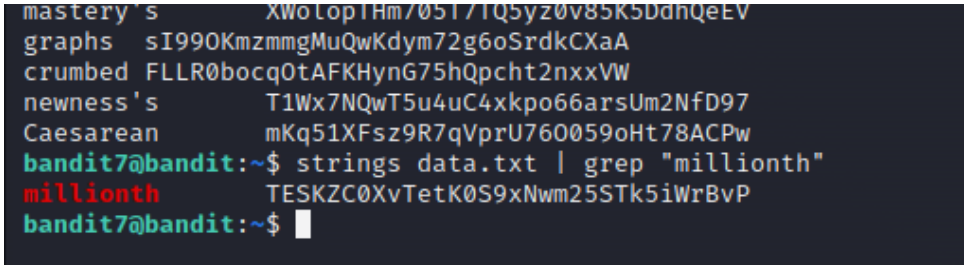
1. owned by user bandit7
2. owned by group bandit6
3. 33 bytes in size

Type the **“find / -user bandit7 -group bandit6 -size 33c”** command in the terminal then will display the lot of files.

There can see the password location as the **“/var/lib/dpkg/info/bandit7.password”.**

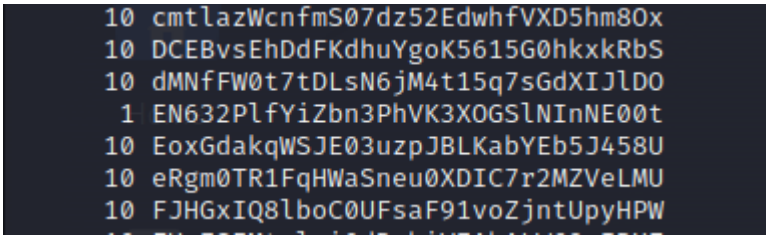
Can display the password using “cat /var/lib/dpkg/info/bandit7.password” command.

Level 07-> Level 08



- Exit from the bandot6using “exit” command.
- Then type the “**ssh bandit6@bandit.labs.overthewire.org -p 2220**” on the terminal.
- In this level password is stored in the file **data.txt** next to the word **millionth.**
- Using **“cat data.txt”** command can display all the data in data.txt.
- Run the **“grep millionth data.txt”** command and retrieve the password.

Level 08-> Level 09



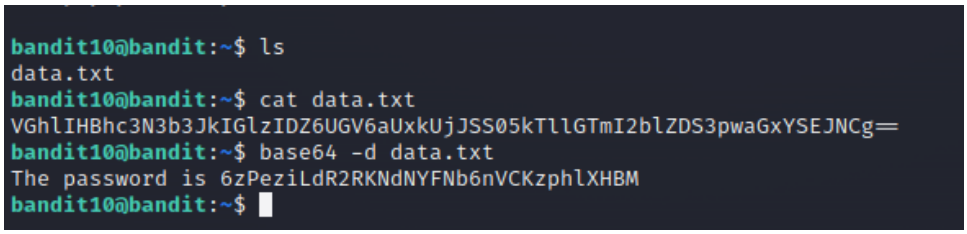
- Exit from the bandot7using “**exit**” command.
- Then type the “**ssh bandit8@bandit.labs.overthewire.org -p 2220**” on the terminal.
- In this level password is stored in the file **data.txt** and is the only line of text that occurs only once
- Using **“cat data.txt”** command can display all the data in data.txt.

- Run the **“sort data.txt | uniq -u”** command and retrieve the password.

Level 09-> Level 10

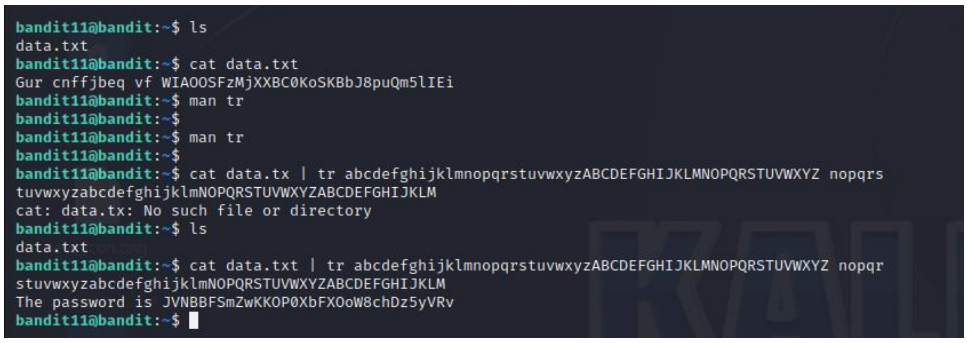
- Exit from the bandot8using “**exit**” command.
- Then type the “**ssh** bandit9@bandit.labs.overthewire.org **-p 2220**” on the terminal.
- In this level password is stored in the file **data.txt** in one of the few human-readable strings, preceded by several ‘=’ characters.
- Open the terminal and run the **“strings data.txt | grep "==""”**
- Then display the password as the below picture.

Level 10-> Level 11



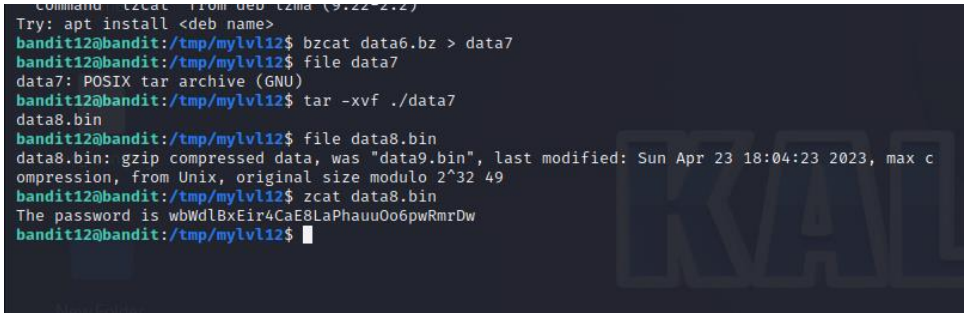
- Exit from the bandot9using “**exit**” command.
- Then type the “**ssh** bandit10@bandit.labs.overthewire.org **-p 2220**” on the terminal.
- In this level password is encoded with the 64base encoded data.
- Encoded data is display in the below picture. Need to decode the data using this command “**base64 -d data.txt**”.
- Then will display the password.

Level 11-> Level 12



- Exit from the bandot10using "**exit**" command.
- Then type the "**ssh bandit11@bandit.labs.overthewire.org -p 2220**" on the terminal.
- In this level password is stored in data.txt file and the password is rotated by 13 position.
- First retrieve the data from the data.txt file using "cat **data.txt**".
- After that copy data retrieve from the data.txt file.
- Then search the cyberchef and search and select rot13 function
- Then paste copy data to the input section after that will display the correct format of the password at the output section.

Level 12-> Level 13

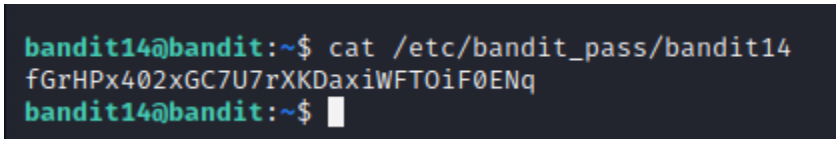


- Then type the "**ssh bandit12@bandit.labs.overthewire.org -p 2220**" on the terminal.
- There the data available in hexa and compressed level.
- As the bandit instruction first need to create new directory and copy data.txt file to the that directory.
- Create new directory –mkdir /tmp/lev12
- Copy data.txt file to the new directory –cp data.txt /tmp/lev12
- Change directory – cd /tmp/lev12
- After that file is in as the bzip compressdata.check the file type using"**file.datad**" command.
- We need to decompress again first need to change file extention to bzip.it can do using this command "**mv datad datad1.bz2**"

- Decompress the file using "**bzip2 -d datad1.bz2".**
- After the decompress file is again in as the gz compress file.

- Then do hexadump and copy data to new file using this command "**xxd -r data.txt > data**".
- Then need to change file format to decomress the data.it can do using this command" **mv data datad.gz".**
- Then decompress the gz file using **"gzip -d datad.gz".**
- After that we can see the file is available in tar file format.
- Then change the file format to the tar "**mv datad1 datad1.tar"**.
- Then extract the file "**tar xf datad1.tar**".Password fill is compressed lot of time then we need to do decompress again and again as the previously done

Level 13-> Level 14



- Then type the "**ssh bandit13@bandit.labs.overthewire.org -p 2220**" on the terminal.
- In this level password can get only bandit 14 user the need to connect bandit 14.
- Can use tho command to log bandit14 using ssh Privert key" s**sh -i sshkey.private bandit14@localhost -p 2220**".
- Then using cat command can get the password **"cat /etc/bandit_pass/bandit14"**

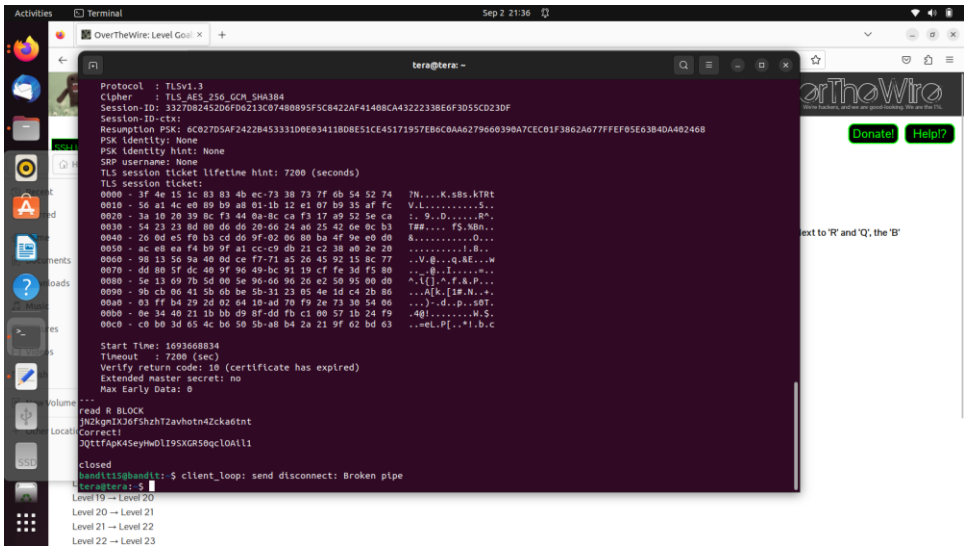
Level 14-> Level 15

```
bandit14@bandit:~$ cat /ect/bandit_pass/bandit14
cat: /ect/bandit_pass/bandit14: No such file or directory
bandit14@bandit:~$ cat /etc/bandit_passbandit14
cat: /etc/bandit_passbandit14: No such file or directory
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
bandit14@bandit:~$ man nc
bandit14@bandit:~$ nc localhost 30000
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

bandit14@bandit:~$
```

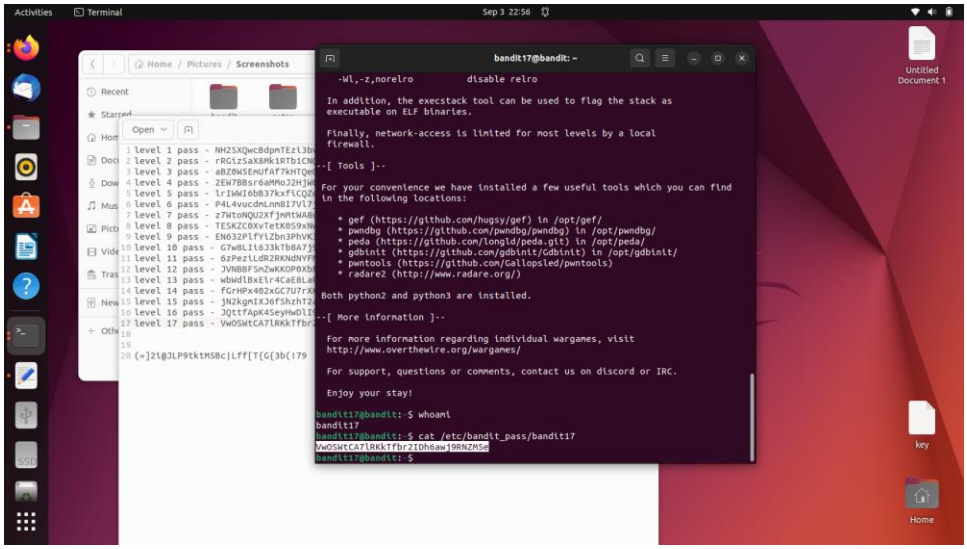
- Without exit from the bandit 14(previously logged) connect throw the port 30000 using "**nc localhost 30000**"
- After that enter the bandit14 password and press enter. Then will display the password

Level 15-> Level 16



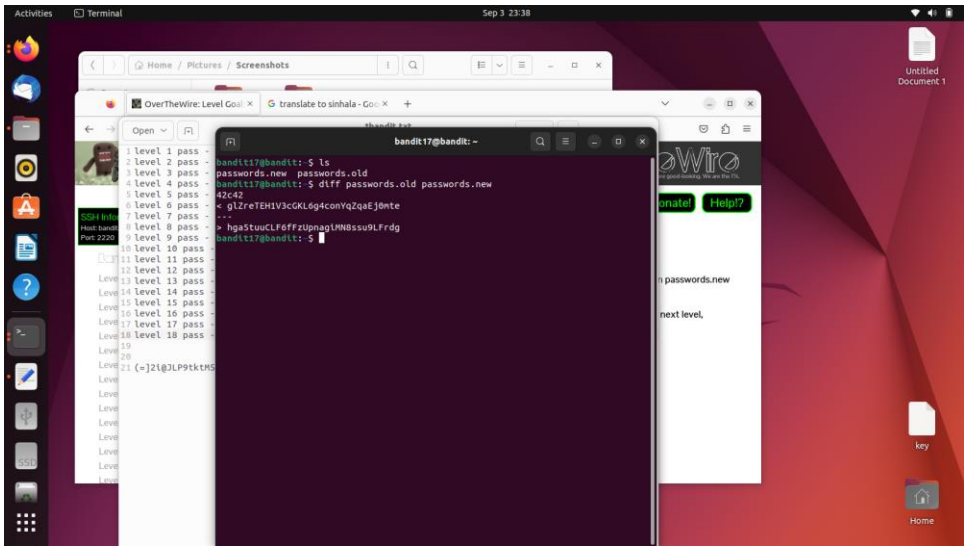
- Then type the "**ssh** bandit15@bandit.labs.overthewire.org **-p 2220**" on the terminal and enter the password **"jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt".**
- Connected to the localhost server using open ssl.
- Run "**openssl s_client -connect localhost:30001"**
- After that enter the level 15 password the will display the level16 password.

Level 16-> Level 17



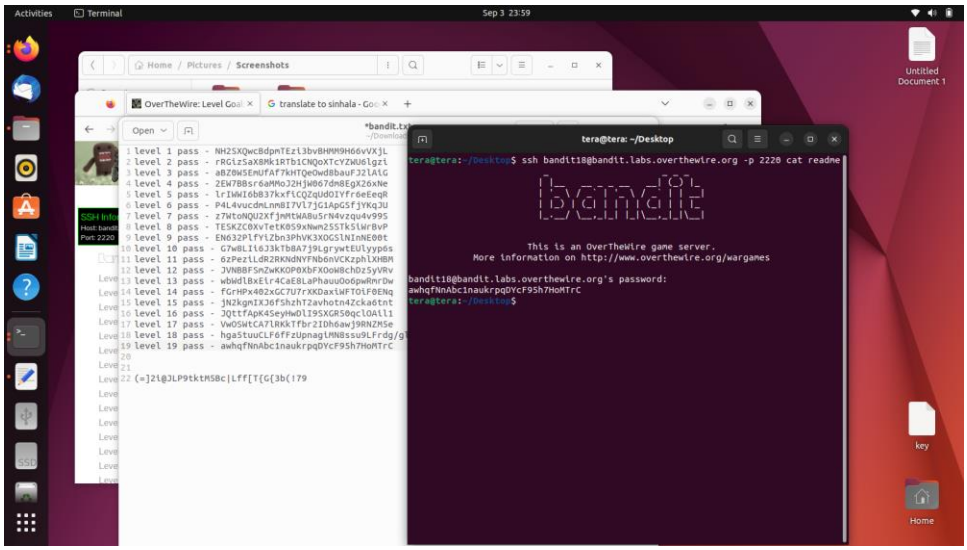
- Then type the "**ssh bandit16@bandit.labs.overthewire.org -p 2220**" on the terminal and enter.
- Find the open ports in given range.
- Then type "**nc localhost 31790**" in terminal .
- Then enter the bandit password.
- Then connect to the server using "**ncat --ssl localhost 31790**".and enter the password
- After that will display the private key.
- Open nano editor and save the private key.**"nano key"**
- Then change key file to mod bits "**chmod 400 key**".
- Then connect to the bandit17 using key file." **ssh -i key bandit17@bandit.labs.overthewire.org -p 2220**"
- Then using "**cat /etc/bandit_pass/bandit17**" can display the password.

Level 17-> Level 18



- Then type the "**ssh bandit16@bandit.labs.overthewire.org -p 2220**" on the terminal and enter.
- Using ls command can see the password files.
- Then find the defferent between password new and password old" **diff passwords.old passwords.new".**
- Here we can get the password as the password new.

Level 18-> Level 19



- In this level cannot connect directly for the server using ssh.
- It need to run another command when the connect to the server.

- Using "**ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme**" commmand can display password in the file.

Level 19-> Level 20