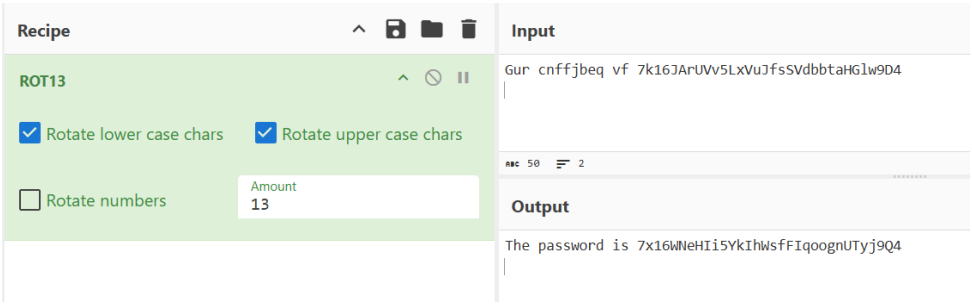
OVER THE WIRE BANDIT WARGAME

Level 10)

```
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==
bandit10@bandit:~$ base64 -d data.txt
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
```

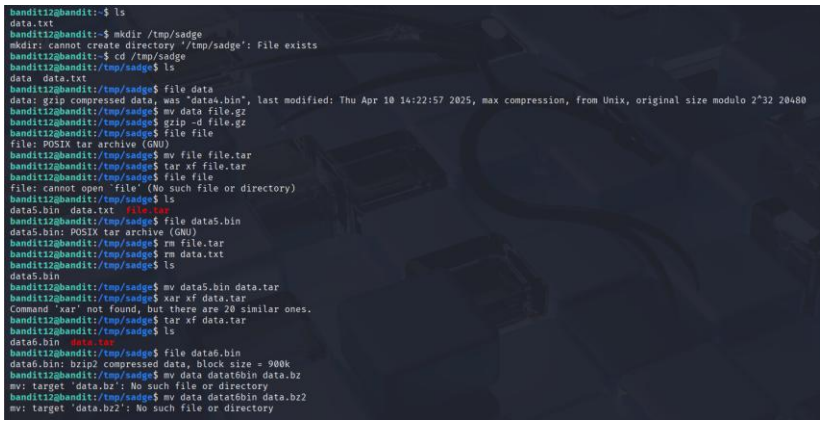
Here, the level told us that the password was encoded in base64 in data.txt so we used base64 to decode the file hence revealing the password

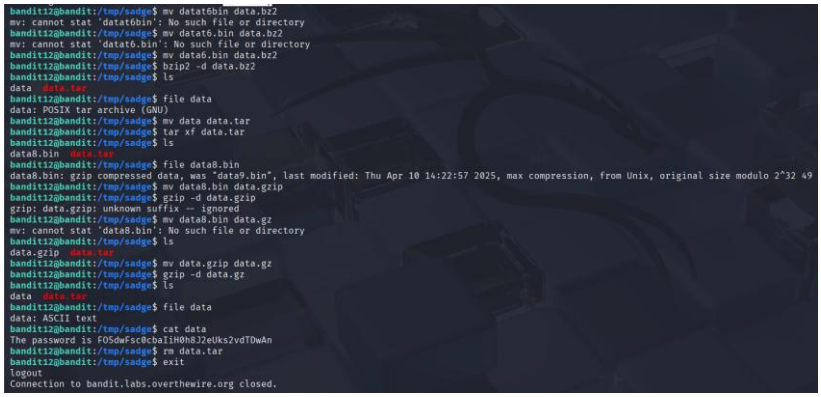
Level 11)



Here, the level said the password is stored in a file where all the lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions, so I used the cyberchef io to help me with the same and save time (snapshot), revealing the password, first I cat the data.txt to show the contents of the file and then put the same in “input” section of cyberchef io (search for rot13 for rotation 13)

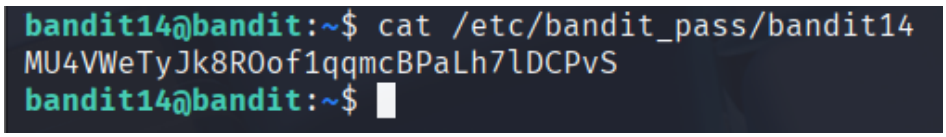
Level 12)





Okay starting off with, this level being soooo different from the previous ones, increase in difficulty is crazy too but the basic logic here was to repeatedly decompress the repeatedly compressed file until we get the file with the password (different format than any compressed format) we checked this by using the file command

Level 13)



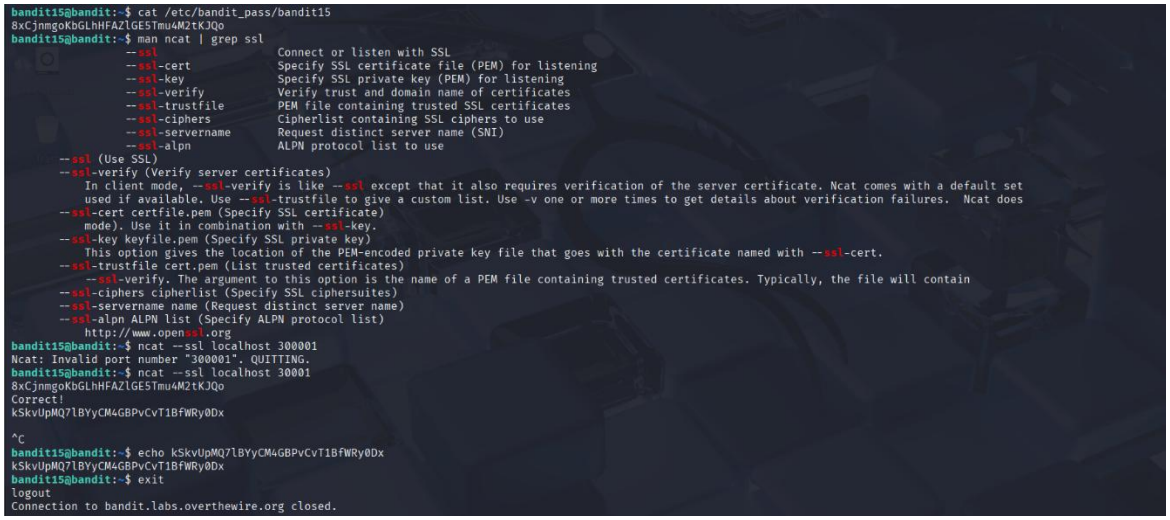
Here, first we use the ssh key to login to the next level and then as it was mentioned in the level we cat the content of the “/etc/bandit_pass/bandit14” file which gives us the password, why this happens?? Because it can only be read by the user bandit14 and we login as the user itself in as the first step

Level 14)

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
bandit14@bandit:~$ nc localhost 30000
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
```

Staying as the same user now to find the password for the next level we need to access the port 30000 of the localhost (the machine we are working on) therefore we use nc “netcat” to get the password for level 15, it asks us to give the password we had just discovered and then provides the password for the next level

Level 15)



Here, we were told the password is on the port 30001 and is saved using SSL/TLS encryption, so we used –ssl and connected tot hat port then we entered the password to get the password for the next level.

Level 16)

```
bandit16@bandit:~$ nmap localhost -p 31000-32000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-02 10:28 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00010s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
bandit16@bandit:~$ nc localhost 31046
^C
bandit16@bandit:~$ cat /etc/bandit_pass/bandit16
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
bandit16@bandit:~$ nc localhost 31046
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
^C
bandit16@bandit:~$ nc localhost 31518
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
bandit16@bandit:~$ nc localhost 31790
^C
bandit16@bandit:~$ ncat -ssl localhost 31046
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
^C
bandit16@bandit:~$ ncat -ssl localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Ncat: Could not resolve source address "sl": Temporary failure in name resolution. QUITTING.
bandit16@bandit:~$ kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx: command not found
bandit16@bandit:~$ ncat --ssl localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
```

Here we were told that the password for the next level is on the active ports ranging from 31000 to 32000, so we used nmap in this range to get to know the active ports and used ssl again to gain access to that particular port, enter our password and then get the password for the next level.

Level 17)

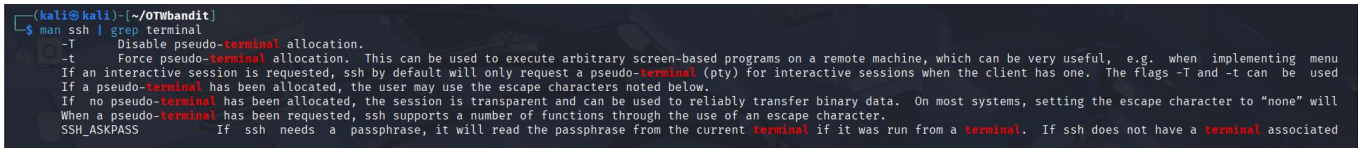
```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.new passwords.old
42c42
< x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
---
> C6XNBdYOkgt5ARXESMKWWOUwBeaIQZ0Y
bandit17@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

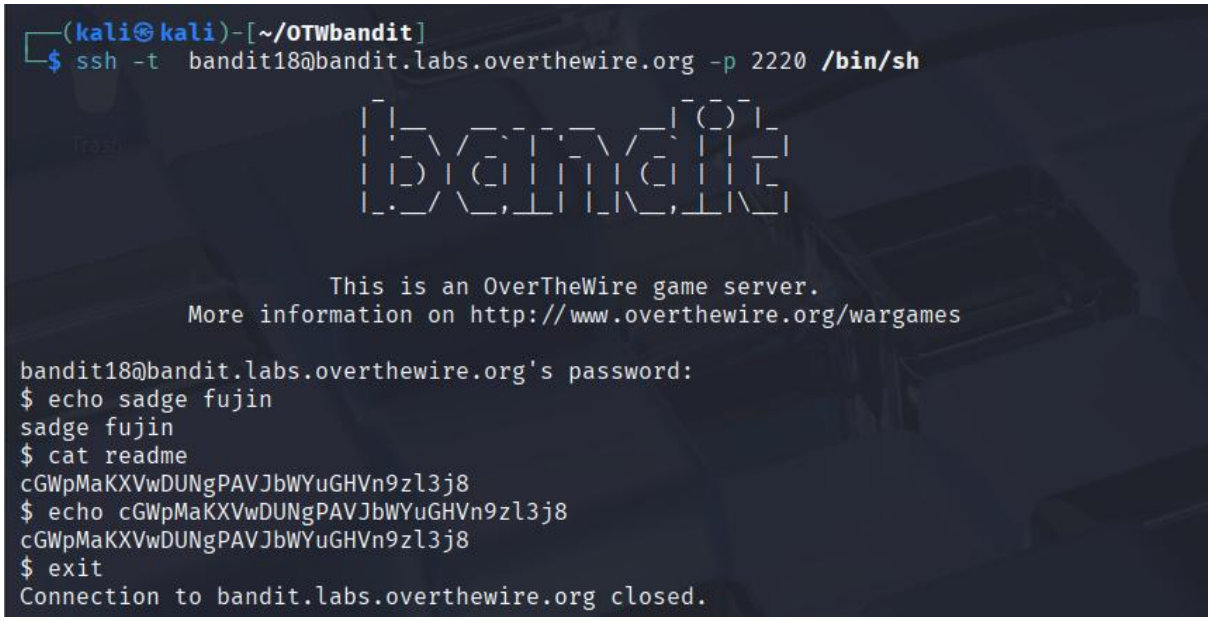
Here, this level we just had to use the diff command to differentiate between the old and new password file, which has the changed password.

```
Byebye !
Connection to bandit.labs.overthewire.org closed.
```

Here, to verify if the password is correct, we try to login to the next level, if it is correct then at the end of the default OTW message it'll say "byebye!" because someone has modified the .bashrc to reject our access whenever we try to login with SSH

Level 18)





Here, like we said the bashrc was modified to not let us gain access, so we used a different command to access the shell, the "-t" forces a pseudo terminal allocation which is necessary for interactive shell sessions. And WKT the default shell of the server (bashrc) has been modified so we need to use a different shell to login other than the bash shell, so in the end we specify which shell to use "/bin/sh" this is done to circumvent the problem of the bashrc file, now we enter the password we had obtained from the previous level and enter it, it shows that we are in the sh shell and from here on we can cat the readme file to get the password for the next level.
this was def a tricky ques lol took me some time, trial and error methods

Level 19)

Here, when we execute the executable it temporarily changes the user's effective uid (it is 20 in this case) makes bandit20 the owner of the file, meaning commands executed with bandit20-do will run the perms of bandit20, and now because bandit20 is the owner we use the cat command to reveal the password