Bandit Level 0:

I was given a username and password for Bandit Level 0. I logged in using these credentials. After logging in, I ran the 'ls' command to see the files, and I found a file named "readme" with the password for Bandit Level 1 inside.

Bandit Level 1:

I logged in with the provided username and password. Using the 'ls' command, I checked the files and found the "readme" file. Inside it, I discovered the password for Bandit Level 1.

Bandit Level 2:

After logging in, I used the 'ls' command to see the files and noticed a file named "-". To read it, I used the 'cat <-' command and found the password for Bandit Level 2.

Bandit Level 3:

I found a file named "spaces in this filename" when I used the 'ls' command after logging in. To read this file, I used 'cat "spaces in this filename"' and found the password for Bandit Level 3.

Bandit Level 4:

The password was hidden in a file within the "inhere" directory. I used the 'ls' command to check the files and 'cd' to enter the "inhere" folder. Then, I ran 'ls -a' to see hidden files (which start with a dot). The hidden file was named ".hidden," and I used 'cat .hidden' to get the password for Bandit Level 4.

Bandit Level 5:

In the "inhere" folder, most files are binary, making them unreadable with 'cat.' To find the the only readable file i used xargs

```
find . -type f | xargs file
```

The readable file was "-file07." Using 'cat ./file07,' I found the password for Bandit Level 5.

Bandit Level 6:

The password was hidden in a file in the "inhere" folder with specific properties. I used the 'find' command:

```
find / -type f -size 1033c ! -executable
```

This command looked for a 33-byte file that wasn't executable and was owned by user bandit7 and group bandit6. It found the file '/var/lib/dpkg/info/bandit7.password,' and I used 'cat' to read it.\

Bandit Level 7:

The password was in a file on the server with specific properties. I used the 'find' command:

```
find / -user bandit7 -group bandit6 -size 33c
```

This command found the file '/var/lib/dpkg/info/bandit7.password.' I used 'cat' to read it.

Bandit Level 8:

The password was in 'data.txt' next to the word 'millionth.' I used 'cat data.txt | grep millionth' to find it.

Bandit Level 9:

The password was in 'data.txt,' and it was the only line that occurred only once. I used 'sort data.txt | uniq -u' to find it.

Bandit Level 10:

The password was in 'data.txt' in a string beginning with several '=' characters. I used 'cat data.txt | strings | grep ‘=' to find it.

Bandit Level 11:

The password was in 'data.txt,' which contained base64 encoded data. I used 'cat data.txt | base64 --decode' to decode and find the password.

Bandit Level 12:

I cated the file then I used an online tool codechef to decode it from rot13 to english

Bandit Level 12 – 13

The password for the next level was stored in 'data.txt,' which was a hexdump of a file that had undergone repeated compression. Following a specific series of commands, including 'xxd -r data.txt data1,' I extracted the password.

```
ls
```

```
cat data.txt
```

```
mkdir /tmp/coolmmoks
cp data.txt /tmp/coolmmoks
cd /tmp/coolmmoks
ls
file data.txt
xxd -r data.txt data1
file data1
mv data1 data2.gz
gzip -d data2.gz
```

```
file data2
mv data2 data3.bz2
bzip2 -d data3.bz2
file data3
mv data3 data4.gz
gzip -d data4.gz
file data4
tar -xvf data4
```

```
file data5.bin
tar -xvf data5.bin
file data6.bin
mv data6.bin data7.bz2
bzip2 -d data7.bz2
file data7
tar -xvf data7
```

```
file data8.bin
mv data8.bin data9.gz
gzip -d data9.gz
file data9
cat data9
ssh bandit13@localhost
```

Bandit Level 13 – 14

The password for the next level was kept in '/etc/bandit_pass/bandit14' and could only be accessed by user bandit14. I used an SSH key to access the next level, which was provided in a private SSH key file.

```
ls
```

```
ssh bandit14@localhost -i sshkey.private
```

Bandit Level 14 – 15

The password for the next level could be retrieved by sending the current level's password to port 30000 on localhost via telnet. After successfully entering the password, I obtained the next password.cat /etc/bandit_pass/bandit14

```
telnet localhost 30000
```

Paste the password in the escape characters, then you get the correct password

```
ssh bandit15@localhost
```

Bandit Level 15 – 16

The next level's password could be retrieved by sending the current level's password to port 30001 on localhost using SSL encryption through the 'openssl s_client' command.

```
openssl s_client -connect localhost:30001 -ign_eof
```

Now, paste the previous level password

```
ssh bandit16@localhost
```

Bandit Level 16 – 17

To find the credentials for the next level, I had to send the current level's password to a port in the range 31000 to 32000 on localhost. I used the 'nmap' command to discover which ports had a server listening, and then I used 'openssl s_client' to connect to the correct port. After providing the previous level's password, I received the next password.

```
nmap -A localhost -p 31000-32000
```

```
openssl s_client -connect localhost:31790
```

Now, enter the previous level password

Copy the RSA Private key

```
mkdir /tmp/coolmmoks_ssh
```

```
cd /tmp/coolmmoks_ssh
```

```
nano coolmmoks.private
```

ctrl +x and y

```
chmod 600 coolmmoks.coolmmoks
```

```
ssh bandit17@localhost -i coolmmoks.coolmmoks
```

Password: Not required

Bandit Level 17 – 18

In this level, there were two files in the home directory: "passwords.old" and "passwords.new." The password for the next level was in "passwords.new," and it was the only line that had changed between "passwords.old" and "passwords.new."

```
ls

diff passwords.old passwords.new

ssh bandit18@localhost
```

Bandit Level 18 – 19

To access the next level, I had to use the setuid binary in the home directory, which had the ability to read the password from the file "/etc/bandit_pass/bandit20." After running the setuid binary without arguments, I used it to retrieve the password.

```
ssh -T bandit18@localhost

ls

cat readme

ctrl + c

ssh bandit19@localhost
```

Bandit Level 19 – 20

A setuid binary in the home directory allowed me to make a connection to localhost on a specified port. This binary then compared a line of text from the connection to the password from the previous level (bandit20). If the comparison was successful, it transmitted the password for the next level (bandit21).ls

```
./bandit20-do
```

```
./bandit20-do cat /etc/bandit_pass/bandit20
```

```
ssh bandit20@localhost
```

Bandit Level 20 – 21

In this level, I was presented with a setuid binary that connected to localhost on a specified port and read text from the connection. It compared the text to the password from the previous level (bandit20) and, if correct, provided the password for bandit21. To solve this, I set up a listener on the specified port and used the binary to transmit the password.

```
ls
```

```
./suconnect
```

Now on the right terminal enter

```
nc -lvp 4444
```

```
./suconnect 4444
```

```
ssh bandit21@localhost
```

Bandit Level 21 – 22

An automated program was running at regular intervals from cron, a time-based job scheduler. I examined the configuration in "/etc/cron.d/" to see the command being executed and discovered a script that generated an MD5 hash from the text "I am user bandit23" and compared it to a provided hash.cd /etc/cron.d/

```
ls
```

```
cat cronjob_bandit22
```

Enter the below command

```
cat /usr/bin/cronjob_bandit22.sh
```

```
cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
```

```
ssh bandit22@localhost
```

PASSWORDS FOR ALL LEVELS IN ORDER

0- NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

1- rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

2- aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

3- 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

4- lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

5- P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

6- z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

7- TESKZC0XvTetK0S9xNwm25STk5iWrBvP

8- EN632PlfYiZbn3PhVK3XOGSINInNE00t

9- G7w8LIi6J3kTb8A7j9LgrywtEUIyyp6s

10- 6zPeziLdR2RKNdNYFNb6nVCKzphIXHBM

11- JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

12- wbWdIBxEir4CaE8LaPhauuOo6pwRmrDw

13- fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq

14- jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

15- JQttfApK4SeyHwDIl9SXGR50qcIOAil1

16- 16- -----BEGIN RSA PRIVATE KEY-----

MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWl/oTqexh+cAMTSMIOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AIbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd

```
HCctNi/FwjuIhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enClvGCSx+X3I5SiWg0A
R57hJgIezIiVjv3aGwHwvIZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUI+iU7rWkGAXFpMLFteQEsRr7PJ/IemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKIwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBApITfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
bIh9eIyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdIc1gvtGCWW+9Cq0b
dxviW8+TFVEBI1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

17- p6ggwdNHncnmCNxuAt0KtKVq185ZU7AW

18- awhqfNnAbc1naukrpqDYcF95h7HoMTrC

19-VxCazJaVykI6W36BkBU0mJTCM8rR95XT

20-NvEJF7oVjkddItPSrdKEFOIIh9V1IBcq

21-Yk7owGAcWjwMVQhjwTesJEwB7WVOwiLI