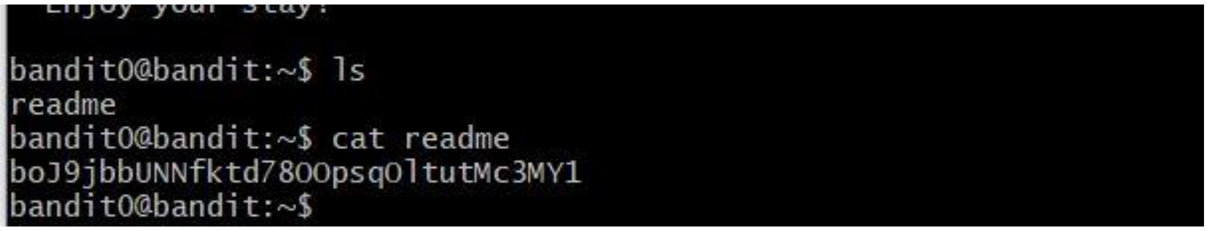
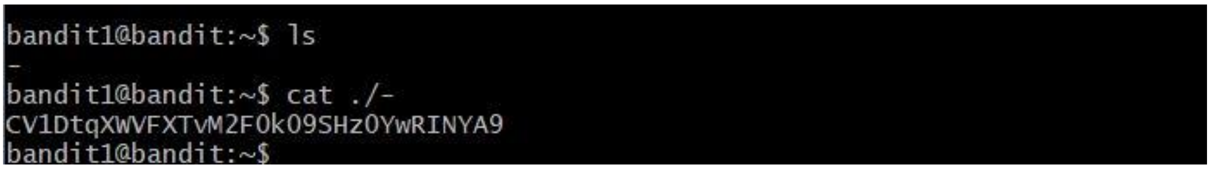
Hi,

For something awesome project I used Cygwin64 (https://www.cygwin.com/) to use Linux on windows, so I started with bandit on the website overthewire.org, I started with level 0 which was easy I just have to connect to ssh using the given username and password which was bandit0, for level 1 I just had to use the cat command of Linux to read the file readme and I got the password for level 1.



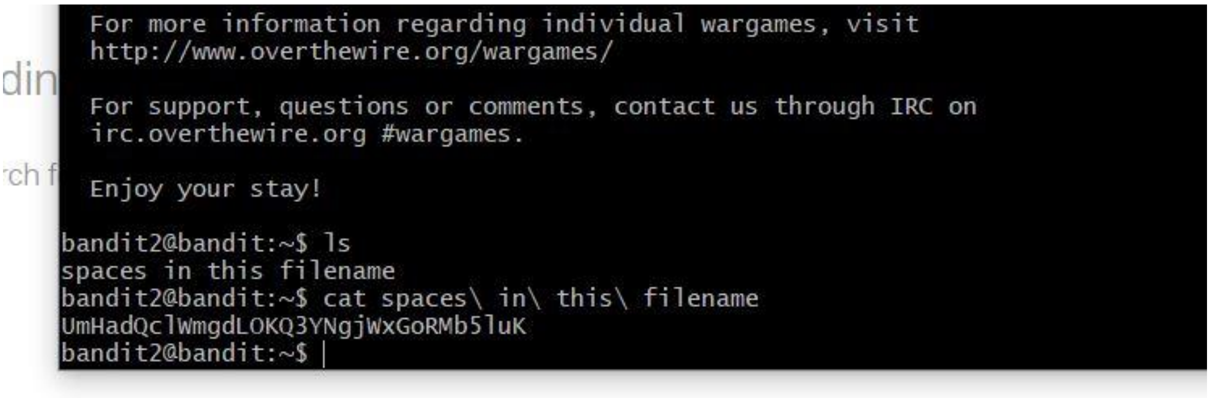
```
  Enjoy your stay!

bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
bandit0@bandit:~$
```

For Level 2 I just had to do cat from a special character by using cat ./- and I got the password for it.



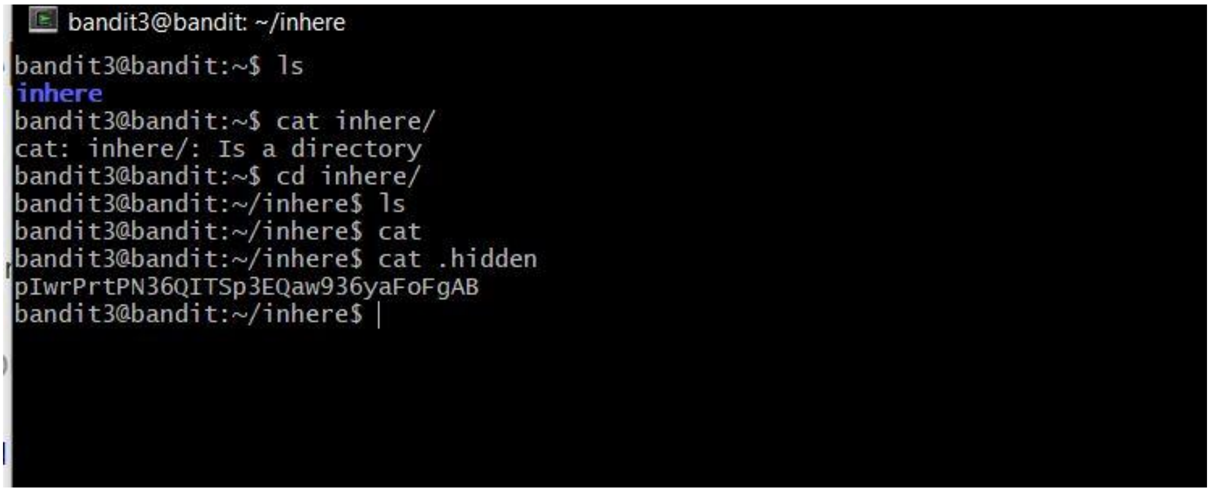
```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$
```

For Level 3 I had to read from file name which contain spaces in it so I just had to put "\" for every time it had a space.



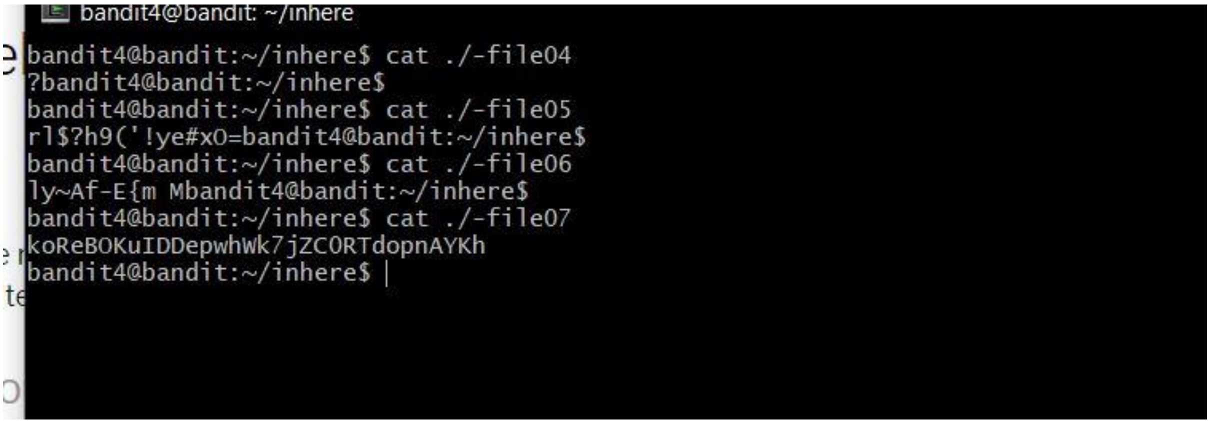
```
  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$ |
```

So for the Level 4 I had to switch directory using cd and the file was hidden so I just pressed "TAB" after cat and I got the file and read the password inside it.



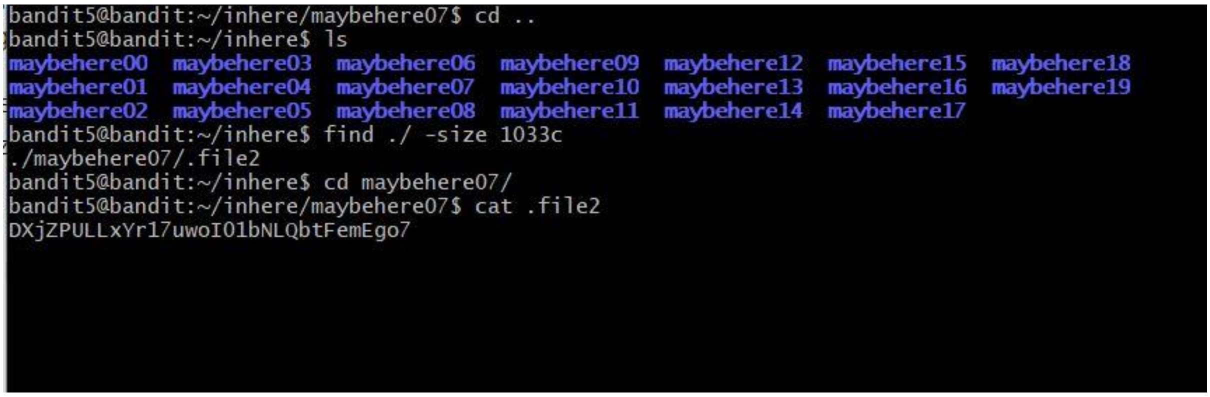
```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cat inhere/
cat: inhere/: Is a directory
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ cat
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$ |
```

So for Level 5 it was really similar to level 2 just had to use ./ to read the file.



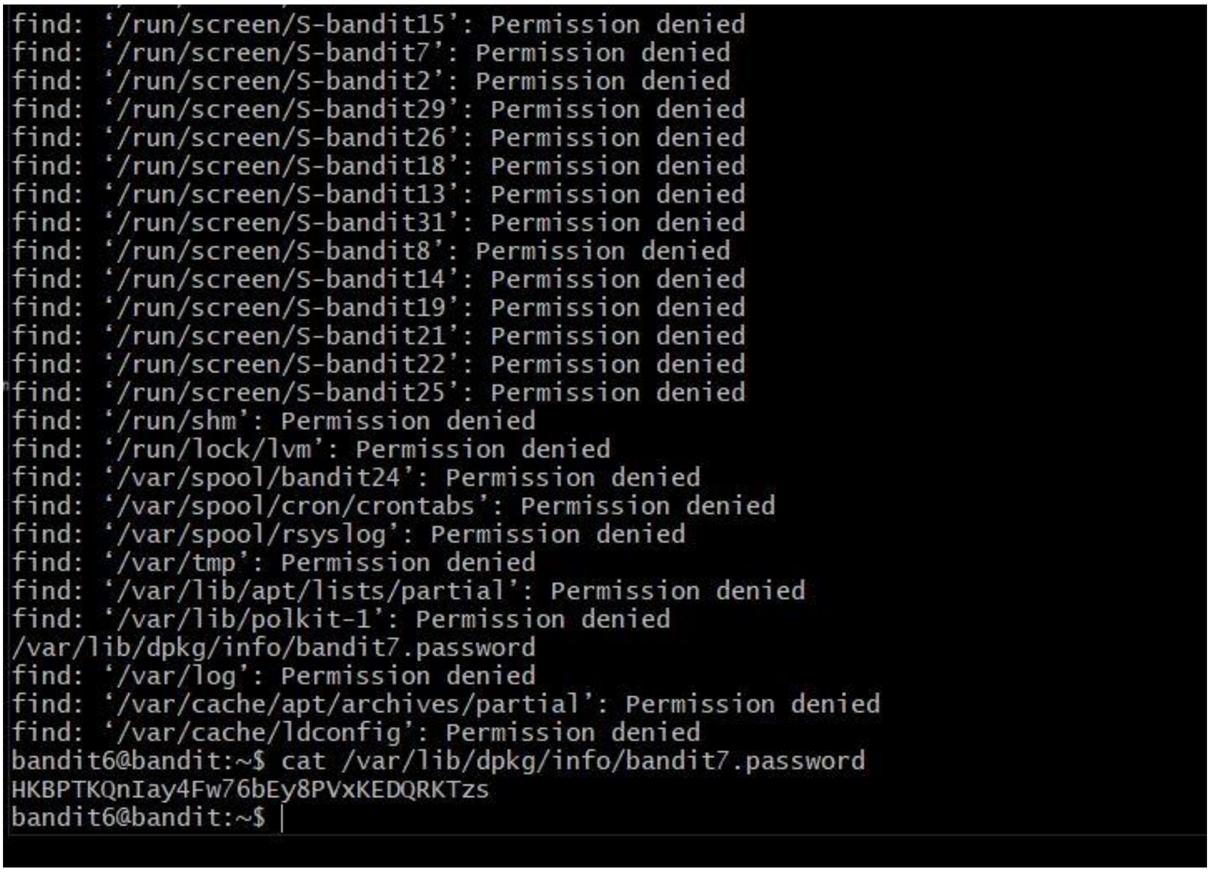
```
bandit4@bandit:~/inhere$ cat ./-file04
?bandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ cat ./-file05
rl$?h9('!ye#x0=bandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ cat ./-file06
ly~Af-E{m Mbandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$ |
```

For the Next level I had use the command find to search through the current directory to look for the file of size 1033 btyes so by running the command "find ./ (./ for the current directory) -size 1033c" I found the location of that file and read the password for the next level.



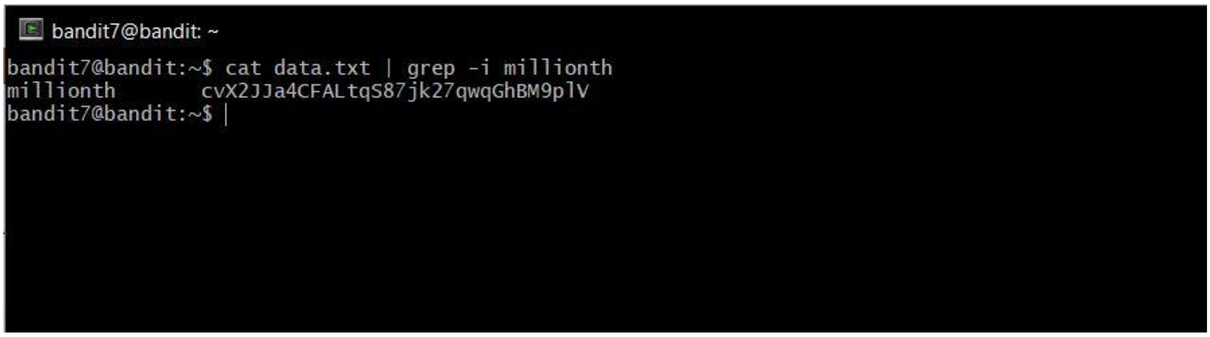
```
bandit5@bandit:~/inhere/maybehere07$ cd ..
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere03  maybehere06  maybehere09  maybehere12  maybehere15  maybehere18
maybehere01  maybehere04  maybehere07  maybehere10  maybehere13  maybehere16  maybehere19
maybehere02  maybehere05  maybehere08  maybehere11  maybehere14  maybehere17
bandit5@bandit:~/inhere$ find ./ -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cd maybehere07/
bandit5@bandit:~/inhere/maybehere07$ cat .file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

For Level 7 I used the same command from the pervious level "find" but this time I had to state the -user section and -group section which was owned by bandit 7 and bandit 6 respectivitly and I got bunch of permission denied but I got one directory which had the password for bandit7.



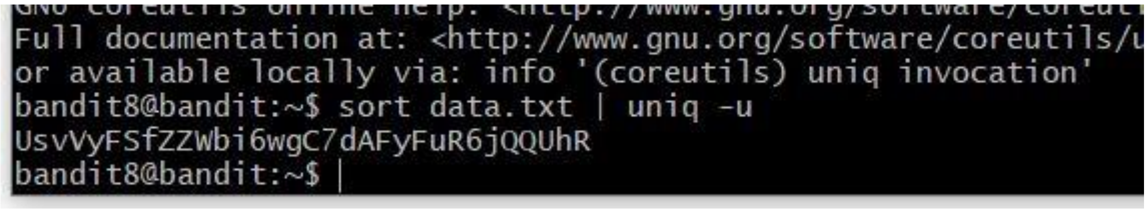
```
find: ‘/run/screen/S-bandit15’: Permission denied
find: ‘/run/screen/S-bandit7’: Permission denied
find: ‘/run/screen/S-bandit2’: Permission denied
find: ‘/run/screen/S-bandit29’: Permission denied
find: ‘/run/screen/S-bandit26’: Permission denied
find: ‘/run/screen/S-bandit18’: Permission denied
find: ‘/run/screen/S-bandit13’: Permission denied
find: ‘/run/screen/S-bandit31’: Permission denied
find: ‘/run/screen/S-bandit8’: Permission denied
find: ‘/run/screen/S-bandit14’: Permission denied
find: ‘/run/screen/S-bandit19’: Permission denied
find: ‘/run/screen/S-bandit21’: Permission denied
find: ‘/run/screen/S-bandit22’: Permission denied
find: ‘/run/screen/S-bandit25’: Permission denied
find: ‘/run/shm’: Permission denied
find: ‘/run/lock/lvm’: Permission denied
find: ‘/var/spool/bandit24’: Permission denied
find: ‘/var/spool/cron/crontabs’: Permission denied
find: ‘/var/spool/rsyslog’: Permission denied
find: ‘/var/tmp’: Permission denied
find: ‘/var/lib/apt/lists/partial’: Permission denied
find: ‘/var/lib/polkit-1’: Permission denied
/var/lib/dpkg/info/bandit7.password
find: ‘/var/log’: Permission denied
find: ‘/var/cache/apt/archives/partial’: Permission denied
find: ‘/var/cache/ldconfig’: Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$ |
```

For Level 8 I was given a file called data.txt which had hell lots of strings in it and the hint said the password is next to the word "millionth", so for this I use a command called grep which work as a regular expression and search for a word in a particular file by running the command cat data.txt with "grep -i millionth" gave me the line which had password.



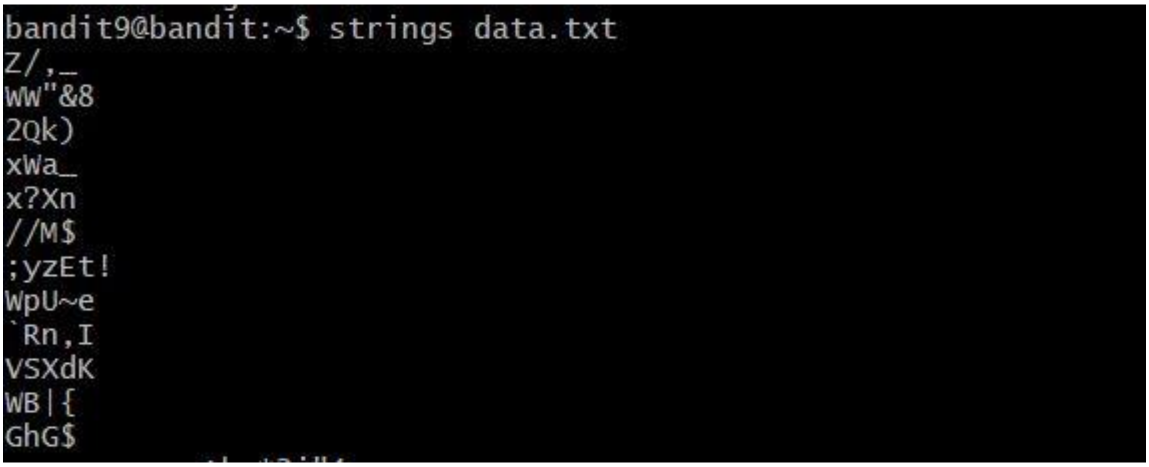
```
bandit7@bandit:~$ cat data.txt | grep -i millionth
millionth       cvX2JJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$ |
```

For this level, the file data.txt contain lots of multiple multiple string and the password only occur once so first I used sort command to sort the string in the data.txt and then run with uniq -u which only gives the unique string from a file and that's how I got the password.

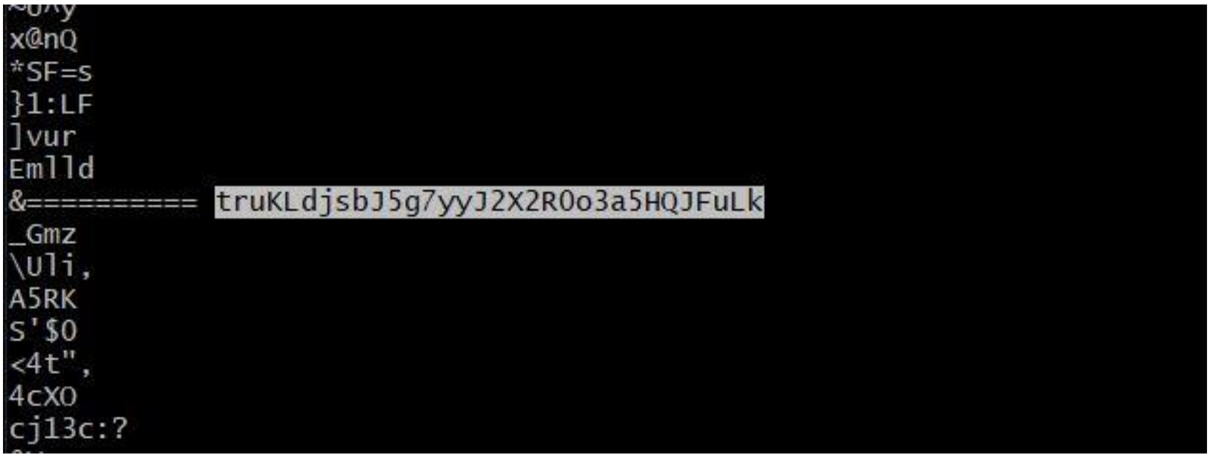


```
GNU coreutils online help: <http://www.gnu.org/software/coreut
Full documentation at: <http://www.gnu.org/software/coreutils/u
or available locally via: info '(coreutils) uniq invocation'
bandit8@bandit:~$ sort data.txt | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
bandit8@bandit:~$ |
```

For Level 10 the file data.txt contain lots of non printable character in the file so I used the command strings <filename> which dumped all the printable character from the file and by scrolling through the output I found the password.

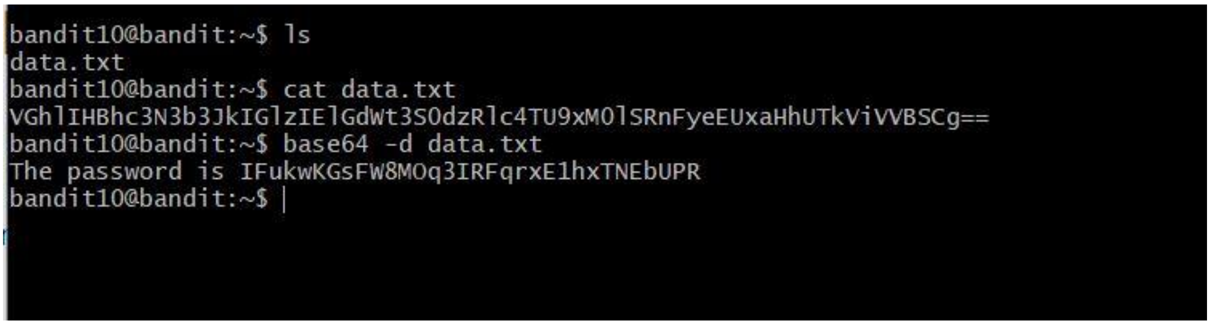


```
bandit9@bandit:~$ strings data.txt
Z/,_
WW"&8
2Qk)
xWa_
x?Xn
//M$
;yzEt!
WpU~e
`Rn,I
VSXdK
WB|{
GhG$
```



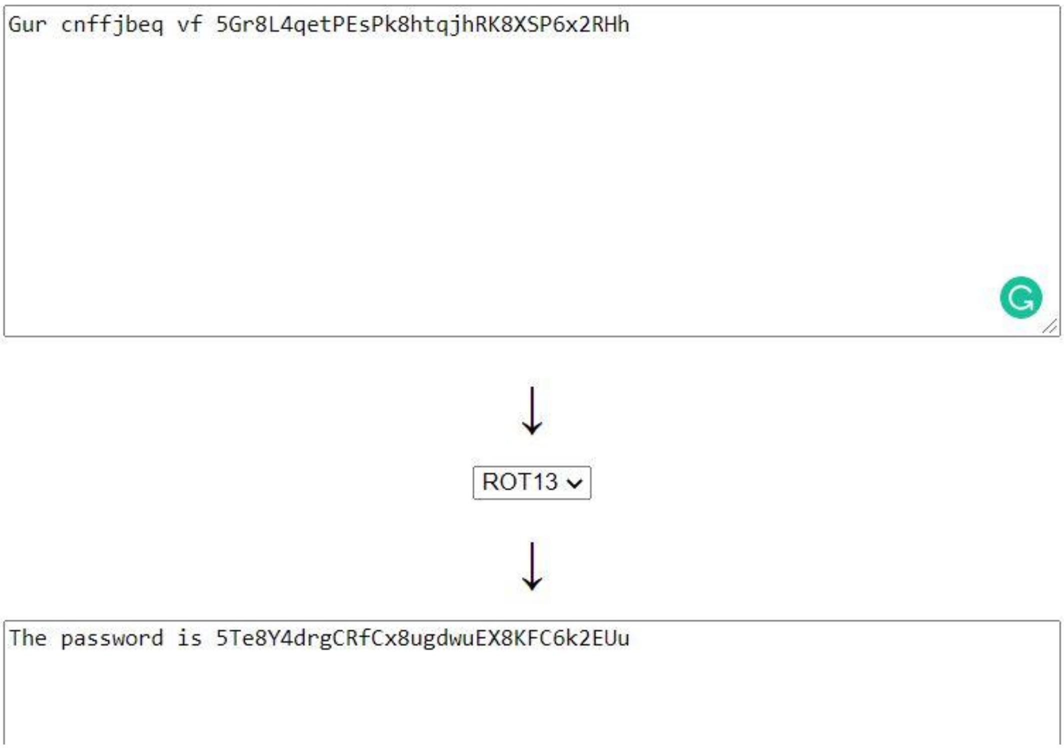
```
~UXy
x@nQ
*SF=s
}1:LF
]vur
Emlld
&========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
_Gmz
\Uli,
A5RK
S'$0
<4t",
4cXO
cj13c:?
```

For Level 11 it had given a file data.txt which was been encrypted with base64 has the question clearly tells that so for this part I had to use the command "base64 -d data.txt" to get the decryption.



```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$ |
```

For the next Level the file data.txt had been encrypt using a method called rot13 so this was not too difficult as I just copied the encode value and used a online rot13 decryptor to get the password.

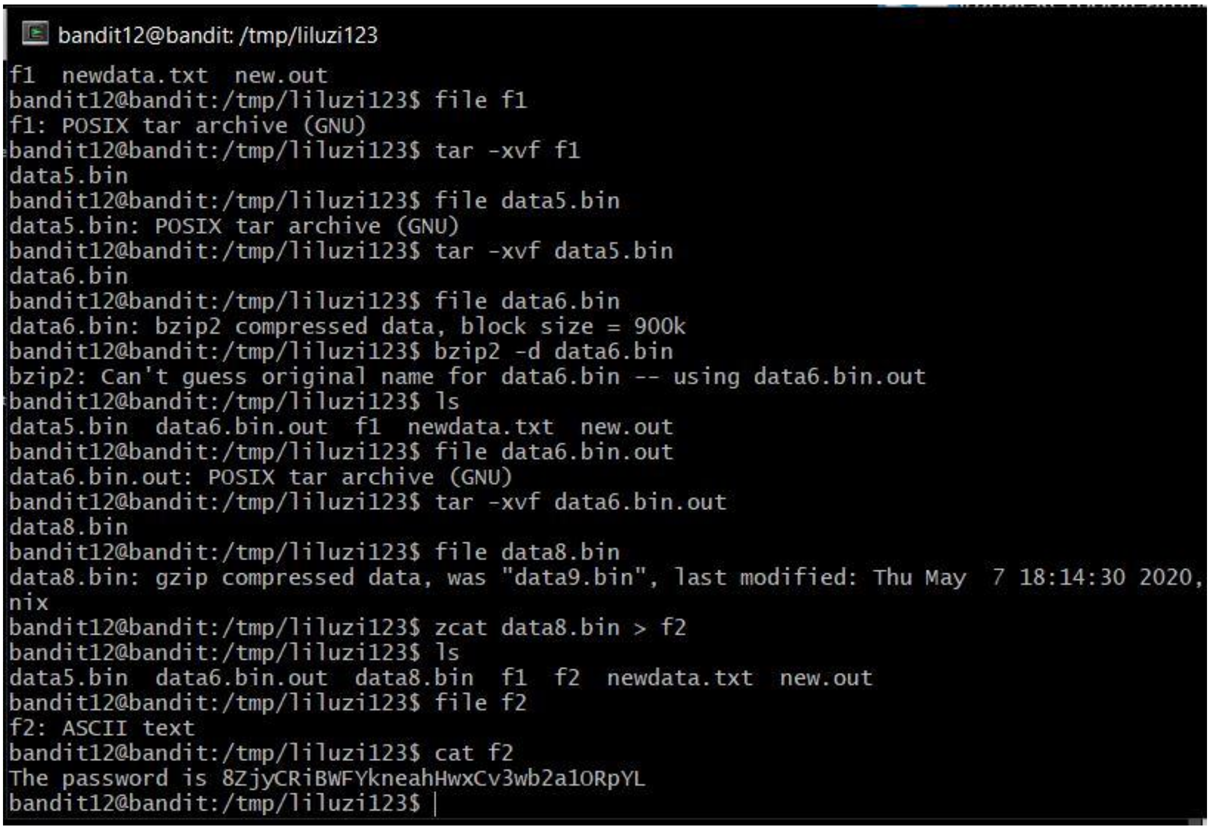


```
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh
```

ROT13

```
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
```

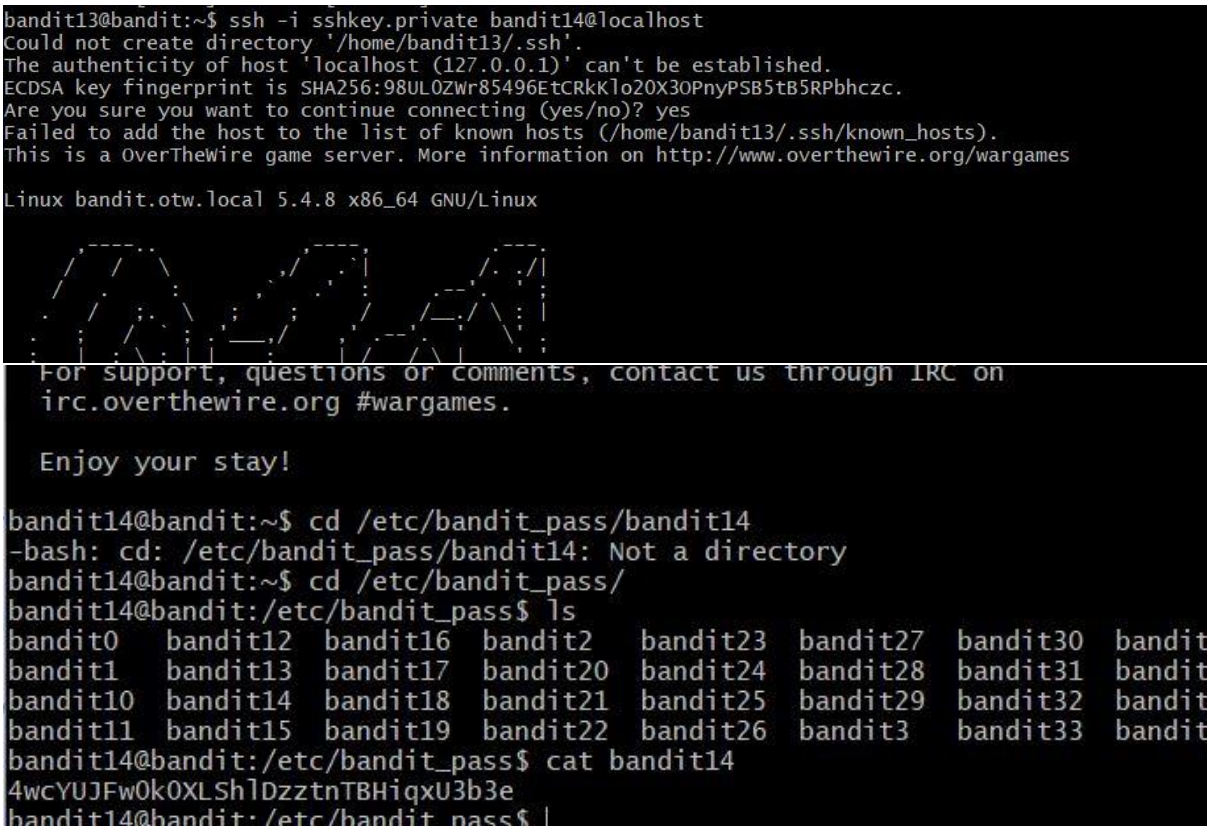
For the next Level, the file data.txt was compressed multiple times this took me a long time to do, first I used the command "xxd -r" to reverse the hexdump, and then after reversing the hex dump using the file command I check the file type of newfile which was Gzip compressed data so I had to decompress the file using the command "zcat -d <filename> > newfile" and then checking the file type again this time is showed a bzip2 compressed data so I had to use the command "bzip2 -d filename" to decompress it, as I read the file was compressed multiple times I had to keep on check the file type and after a while I got the file type as ASCII text and got the password.



bandit12@bandit: /tmp/liluzi123

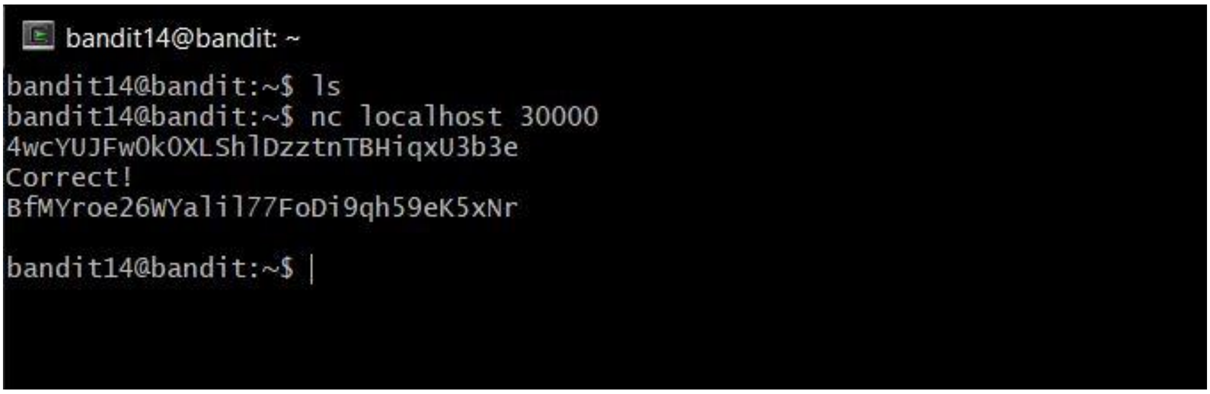
```
f1  newdata.txt  new.out
bandit12@bandit:/tmp/liluzi123$ file f1
f1: POSIX tar archive (GNU)
bandit12@bandit:/tmp/liluzi123$ tar -xvf f1
data5.bin
bandit12@bandit:/tmp/liluzi123$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/liluzi123$ tar -xvf data5.bin
data6.bin
bandit12@bandit:/tmp/liluzi123$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/liluzi123$ bzip2 -d data6.bin
bzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/liluzi123$ ls
data5.bin  data6.bin.out  f1  newdata.txt  new.out
bandit12@bandit:/tmp/liluzi123$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/liluzi123$ tar -xvf data6.bin.out
data8.bin
bandit12@bandit:/tmp/liluzi123$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu May  7 18:14:30 2020,
nix
bandit12@bandit:/tmp/liluzi123$ zcat data8.bin > f2
bandit12@bandit:/tmp/liluzi123$ ls
data5.bin  data6.bin.out  data8.bin  f1  f2  newdata.txt  new.out
bandit12@bandit:/tmp/liluzi123$ file f2
f2: ASCII text
bandit12@bandit:/tmp/liluzi123$ cat f2
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/liluzi123$ |
```

For Level 14, I was given a ssh private key for bandit 14 for this I used the commend "ssh -i sshkey.private bandit14@localhost" to access the bandit14 using the private key and once I was in bandit14 I knew password was store in a particular directory so I read the pass from that dir.



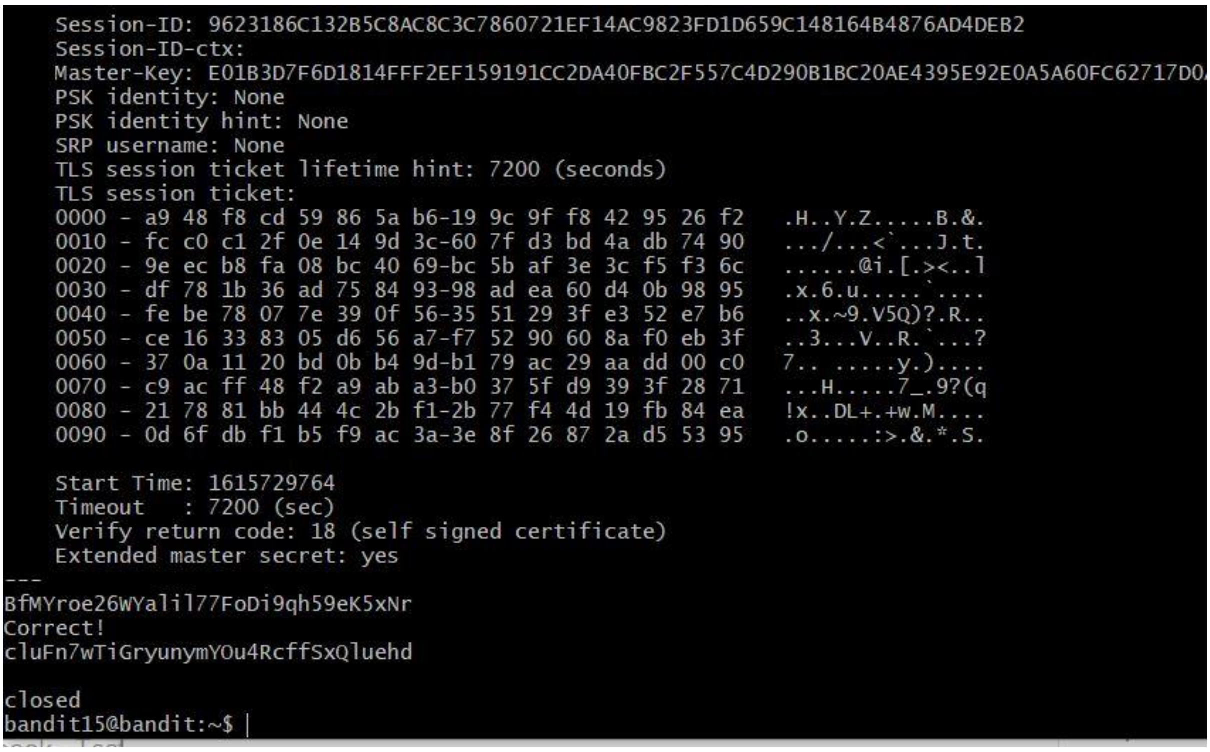
```
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
Could not create directory '/home/bandit13/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRkKlo20X3OPnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

     ,----..            ,----,          .---.
    /   /   \         ,/   .`|         /. ./|
   /   .     :      ,`   .'  :     .--'.  ' ;
  .   /   ;.  \   ;    ;     /    /__./ \ : |
 .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit14@bandit:~$ cd /etc/bandit_pass/bandit14
-bash: cd: /etc/bandit_pass/bandit14: Not a directory
bandit14@bandit:~$ cd /etc/bandit_pass/
bandit14@bandit:/etc/bandit_pass$ ls
bandit0   bandit12  bandit16  bandit2   bandit23  bandit27  bandit30  bandit
bandit1   bandit13  bandit17  bandit20  bandit24  bandit28  bandit31  bandit
bandit10  bandit14  bandit18  bandit21  bandit25  bandit29  bandit32  bandit
bandit11  bandit15  bandit19  bandit22  bandit26  bandit3   bandit33  bandit
bandit14@bandit:/etc/bandit_pass$ cat bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:/etc/bandit_pass$ |
```

For Level 15, It said that I need to connect to the port 30000 in localhost and use the password of bandit 14 to get the next password, so I used the commend nc for this to make a connection with the localhost on port 30000 and after sending the password of bandit 14 I got the pass for next level 15.



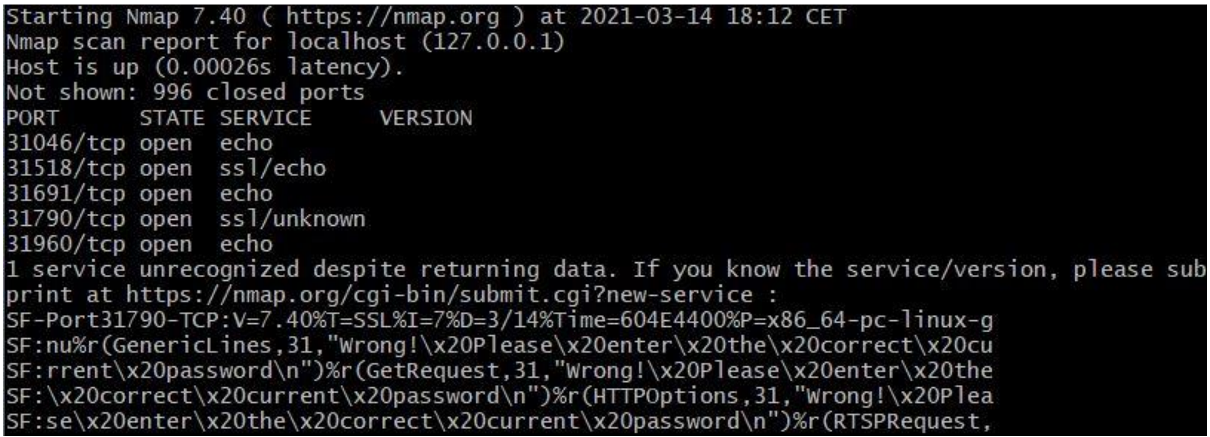
```
bandit14@bandit:~$ ls
bandit14@bandit:~$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr

bandit14@bandit:~$ |
```

For Level 16, I had to submit the current password to the port 31000 on localhost using SSL encryption, for this I had to use the command "openssl s_client -connect localhost:31000 -ign" to connect to the localhost on port 31000 using SSL encryption and then after submitting my current password I got the pass for Level 16.

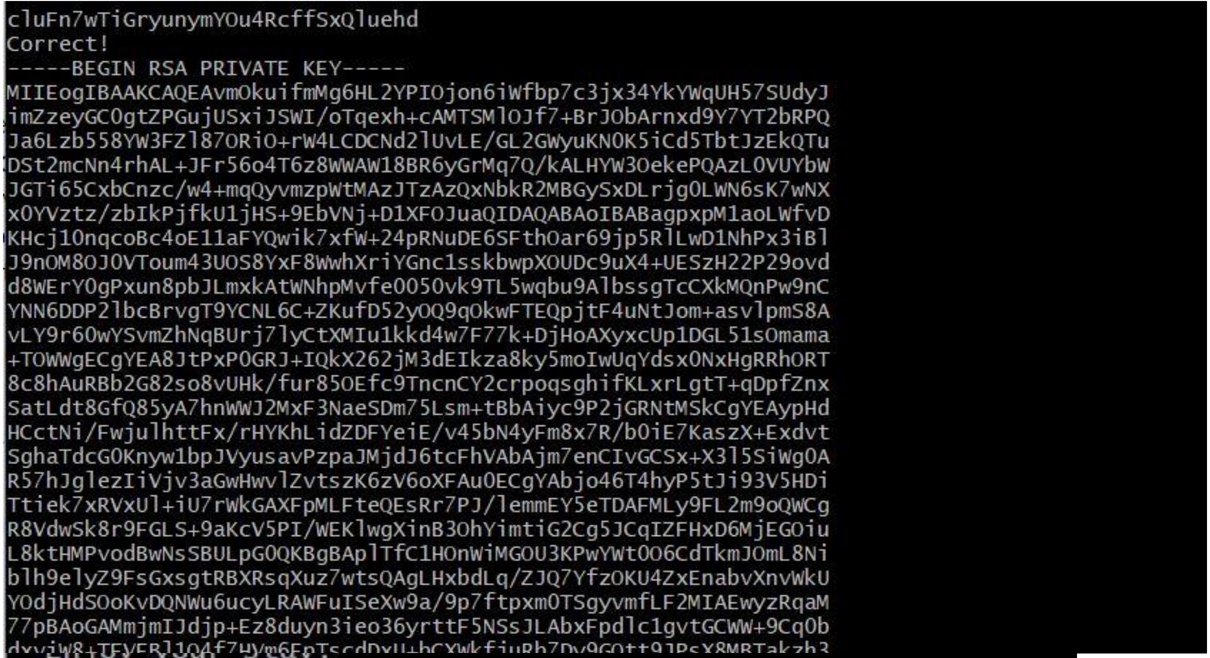


```
    Session-ID: 9623186C132B5C8AC8C3C7860721EF14AC9823FD1D659C148164B4876AD4DEB2
    Session-ID-ctx:
    Master-Key: E01B3D7F6D1814FFF2EF159191CC2DA40FBC2F557C4D290B1BC20AE4395E92E0A5A60FC62717D0
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - a9 48 f8 cd 59 86 5a b6-19 9c 9f f8 42 95 26 f2   .H..Y.Z.....B.&.
    0010 - fc c0 c1 2f 0e 14 9d 3c-60 7f d3 bd 4a db 74 90   .../...<`...J.t.
    0020 - 9e ec b8 fa 08 bc 40 69-bc 5b af 3e 3c f5 f3 6c   ......@i.[.><..l
    0030 - df 78 1b 36 ad 75 84 93-98 ad ea 60 d4 0b 98 95   .x.6.u.....`....
    0040 - fe be 78 07 7e 39 0f 56-35 51 29 3f e3 52 e7 b6   ..x.~9.V5Q)?.R..
    0050 - ce 16 33 83 05 d6 56 a7-f7 52 90 60 8a f0 eb 3f   ..3...V..R.`...?
    0060 - 37 0a 11 20 bd 0b b4 9d-b1 79 ac 29 aa dd 00 c0   7.. .....y.)....
    0070 - c9 ac ff 48 f2 a9 ab a3-b0 37 5f d9 39 3f 28 71   ...H.....7_.9?(q
    0080 - 21 78 81 bb 44 4c 2b f1-2b 77 f4 4d 19 fb 84 ea   !x..DL+.+w.M....
    0090 - 0d 6f db f1 b5 f9 ac 3a-3e 8f 26 87 2a d5 53 95   .o.....:>.&.*.S.

    Start Time: 1615729764
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
    Extended master secret: yes
---
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd

closed
bandit15@bandit:~$ |
```

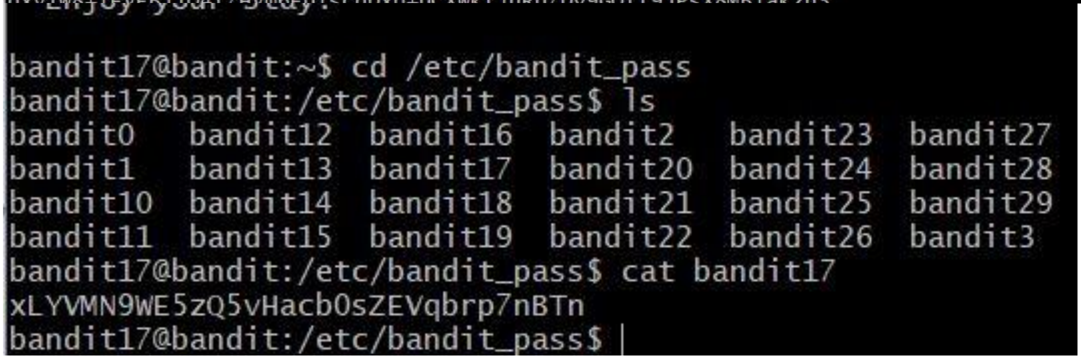
For the Level 17, this level took a lot of time for me, I was given a range of port from 31000 to 32000 and I had to find a open port which also had SSL in it. so for this level I used nmap to scan the port the command I used is "nmap -sV localhost -p 31000-32000" which gave me some info about the open ports and one of the port had ssl/unknow and the other one was ssl/echo which was just gonna reply me with the same message I send so I made a connection with that port using the command "openssl s_client -connect localhost:port" and once the connection was made I enter the current password and I saw a private key instead of a password but from the pervious level I knew I had to use this key to get the access of bandit 17 and I saved the key in a file and used the command "ssh -i <key> bandit17@localhost" and I got the access of bandit 17 and I followed the pervious method of get the password for level 17.



```
Starting Nmap 7.40 ( https://nmap.org ) at 2021-03-14 18:12 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00026s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE     VERSION
31046/tcp open  echo
31518/tcp open  ssl/echo
31691/tcp open  echo
31790/tcp open  ssl/unknown
31960/tcp open  echo
1 service unrecognized despite returning data. If you know the service/version, please sub
print at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port31790-TCP:V=7.40%T=SSL%I=7%D=3/14%Time=604E4400%P=x86_64-pc-linux-g
SF:nu%r(GenericLines,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20cu
SF:rrent\x20password\n")%r(GetRequest,31,"Wrong!\x20Please\x20enter\x20the
SF:\x20correct\x20current\x20password\n")%r(HTTPOptions,31,"Wrong!\x20Plea
SF:se\x20enter\x20the\x20correct\x20current\x20password\n")%r(RTSPRequest,
```



```
cluFn7wTiGryunymYOu4RcffSxQluehd
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxmOTSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVFBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dv9GOtt9JPsX8MBTakzh3
```



```
bandit17@bandit:~$ cd /etc/bandit_pass
bandit17@bandit:/etc/bandit_pass$ ls
bandit0   bandit12  bandit16  bandit2   bandit23  bandit27
bandit1   bandit13  bandit17  bandit20  bandit24  bandit28
bandit10  bandit14  bandit18  bandit21  bandit25  bandit29
bandit11  bandit15  bandit19  bandit22  bandit26  bandit3
bandit17@bandit:/etc/bandit_pass$ cat bandit17
xLYVMN9WE5zQ5vHacb0sZEVqbrp7nBTn
bandit17@bandit:/etc/bandit_pass$ |
```