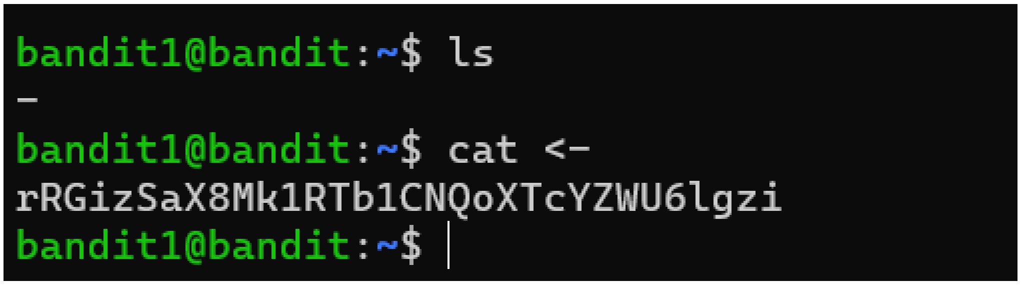
Bandit (Over the Wire)
Report

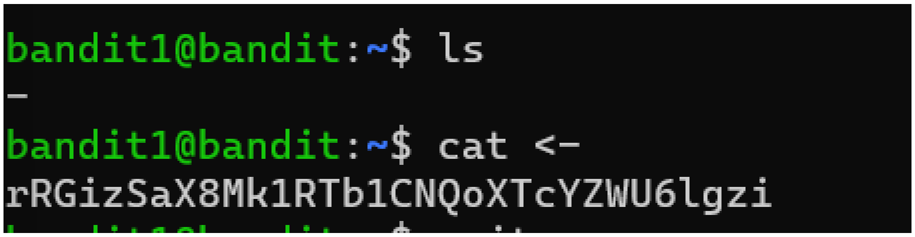
Start
Command used – ssh -p 2220 bandit0@bandit.labs.overthewire.org
Password - bandit0 (given)

Level 0
Command used – cat readme
Password - NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL



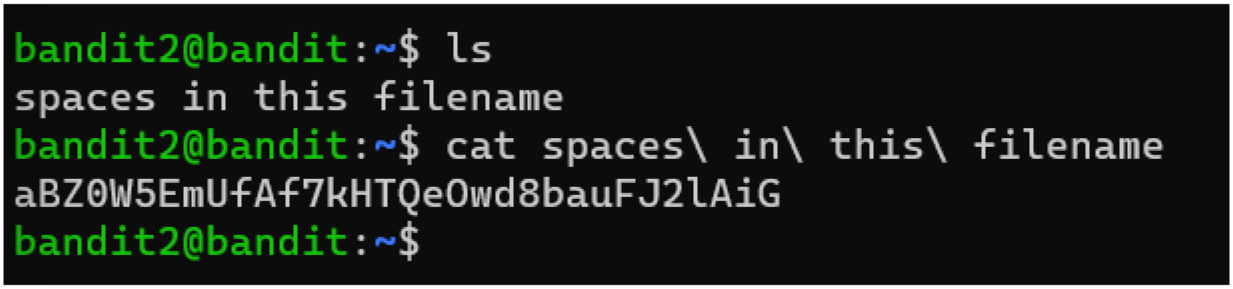
```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat <-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit1@bandit:~$
```

Level 1
Command used – cat <-
Password – rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
If the file name starts with -, we use < before the name to read the file.



```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat <-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
```

Level2
Command used – cat spaces\ in\ this\ filename
Password – aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
If the file name has spaces in between we use \ before every space.



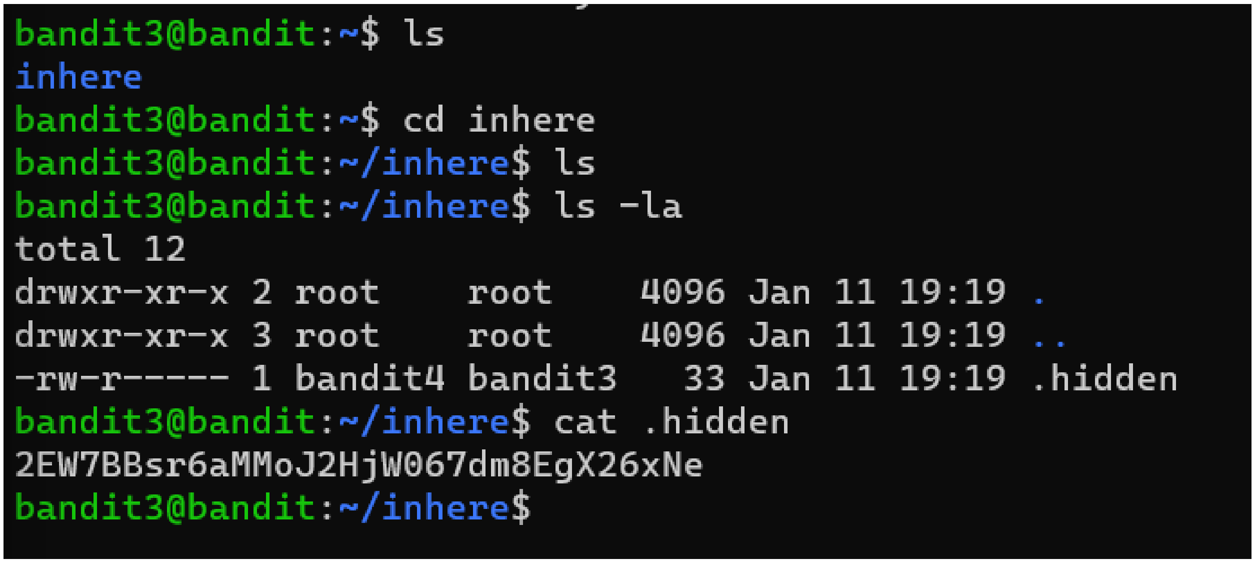
```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
bandit2@bandit:~$
```

Level3

Command used – cat .hidden

Password – 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

Ls -la displays all the files in the directory along with their properties (including hidden files).



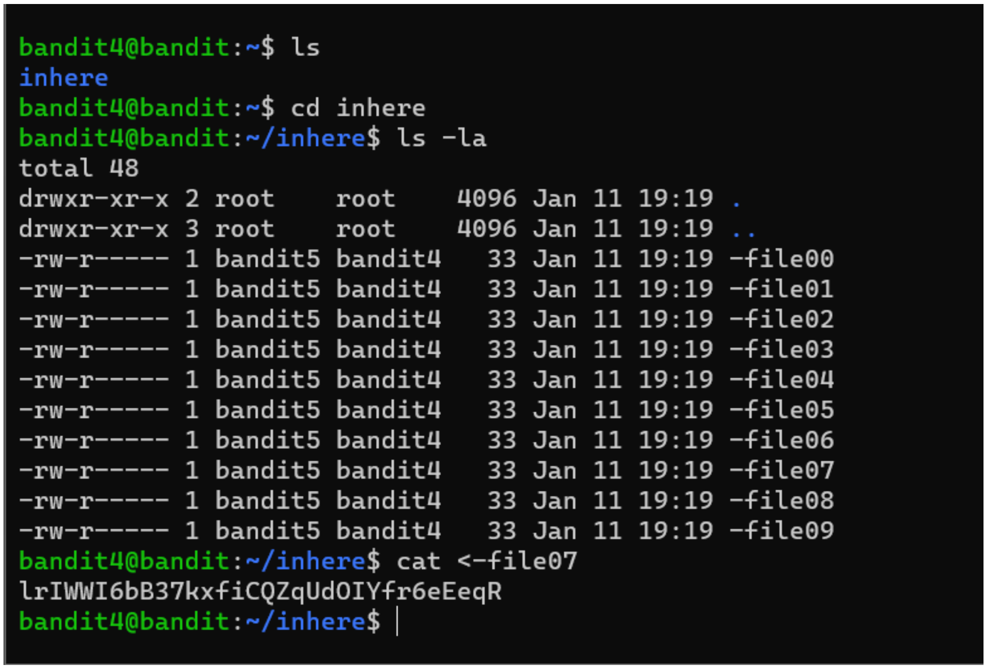
```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -la
total 12
drwxr-xr-x 2 root    root    4096 Jan 11 19:19 .
drwxr-xr-x 3 root    root    4096 Jan 11 19:19 ..
-rw-r----- 1 bandit4 bandit3   33 Jan 11 19:19 .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$
```

Level4

Command used – cat <-file07

Password – lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

In this question, we read different files present in the directory to find the file with human-readable content.

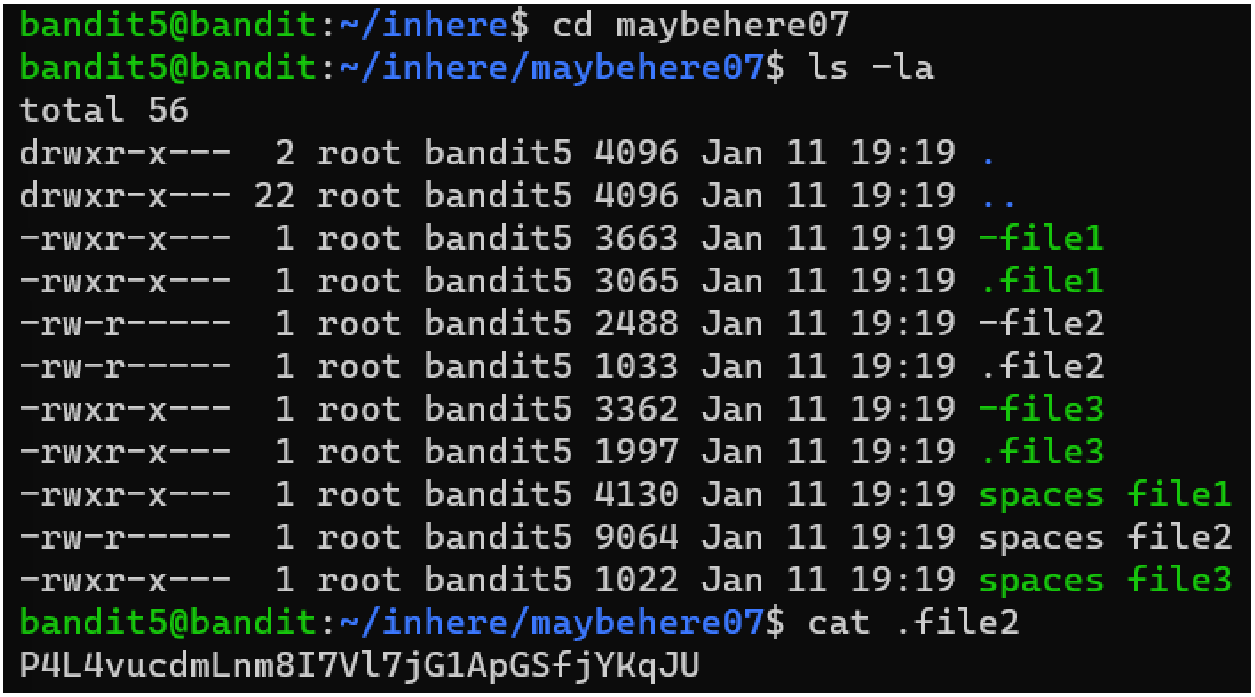


```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -la
total 48
drwxr-xr-x 2 root    root    4096 Jan 11 19:19 .
drwxr-xr-x 3 root    root    4096 Jan 11 19:19 ..
-rw-r----- 1 bandit5 bandit4   33 Jan 11 19:19 -file00
-rw-r----- 1 bandit5 bandit4   33 Jan 11 19:19 -file01
-rw-r----- 1 bandit5 bandit4   33 Jan 11 19:19 -file02
-rw-r----- 1 bandit5 bandit4   33 Jan 11 19:19 -file03
-rw-r----- 1 bandit5 bandit4   33 Jan 11 19:19 -file04
-rw-r----- 1 bandit5 bandit4   33 Jan 11 19:19 -file05
-rw-r----- 1 bandit5 bandit4   33 Jan 11 19:19 -file06
-rw-r----- 1 bandit5 bandit4   33 Jan 11 19:19 -file07
-rw-r----- 1 bandit5 bandit4   33 Jan 11 19:19 -file08
-rw-r----- 1 bandit5 bandit4   33 Jan 11 19:19 -file09
bandit4@bandit:~/inhere$ cat <-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$ |
```

Level5

Password – P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

Like level5, we check different directories to find the file with desirable properties.



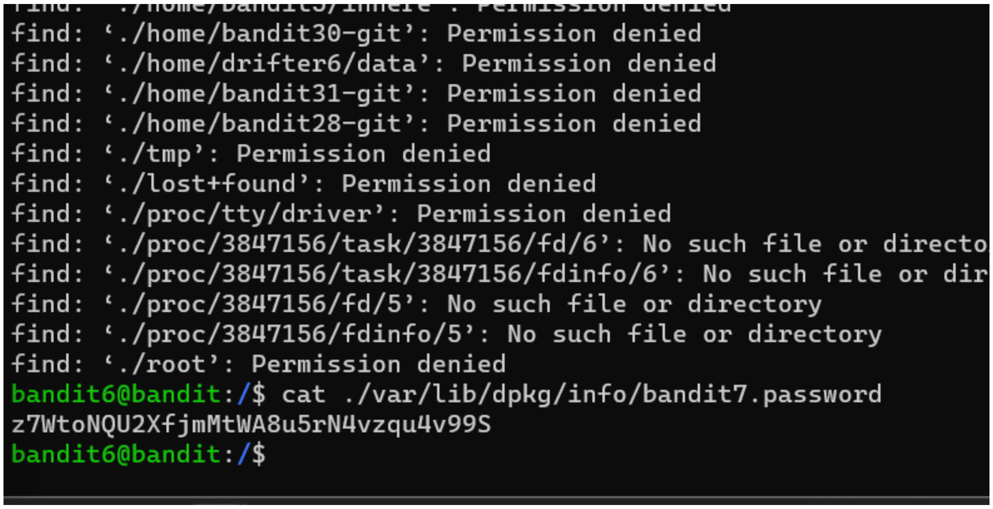
```
bandit5@bandit:~/inhere$ cd maybehere07
bandit5@bandit:~/inhere/maybehere07$ ls -la
total 56
drwxr-x---  2 root bandit5 4096 Jan 11 19:19 .
drwxr-x--- 22 root bandit5 4096 Jan 11 19:19 ..
-rwxr-x---  1 root bandit5 3663 Jan 11 19:19 -file1
-rwxr-x---  1 root bandit5 3065 Jan 11 19:19 .file1
-rw-r-----  1 root bandit5 2488 Jan 11 19:19 -file2
-rw-r-----  1 root bandit5 1033 Jan 11 19:19 .file2
-rwxr-x---  1 root bandit5 3362 Jan 11 19:19 -file3
-rwxr-x---  1 root bandit5 1997 Jan 11 19:19 .file3
-rwxr-x---  1 root bandit5 4130 Jan 11 19:19 spaces file1
-rw-r-----  1 root bandit5 9064 Jan 11 19:19 spaces file2
-rwxr-x---  1 root bandit5 1022 Jan 11 19:19 spaces file3
bandit5@bandit:~/inhere/maybehere07$ cat .file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

Level6

Command – find ./ -user bandit7 -size 33c -group bandit6

Password – z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

First, I did some hit and trial and soon realised it won't work and used the find command with the given specifications. The non-Permission denied directory had the output.

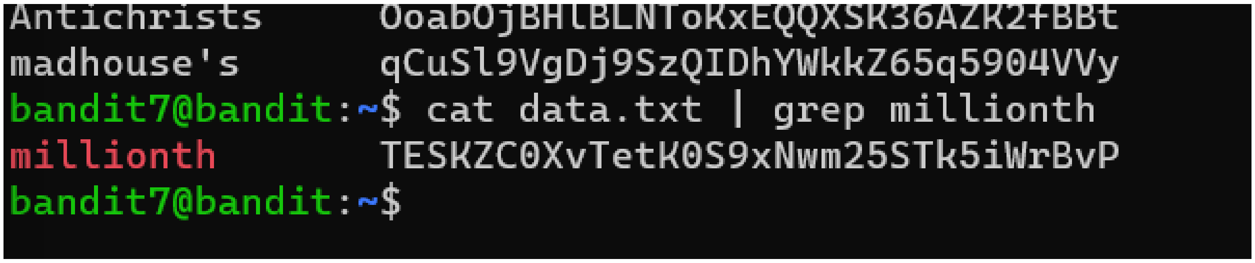


```
find: './home/bandit5/inhere': Permission denied
find: './home/bandit30-git': Permission denied
find: './home/drifter6/data': Permission denied
find: './home/bandit31-git': Permission denied
find: './home/bandit28-git': Permission denied
find: './tmp': Permission denied
find: './lost+found': Permission denied
find: './proc/tty/driver': Permission denied
find: './proc/3847156/task/3847156/fd/6': No such file or directo
find: './proc/3847156/task/3847156/fdinfo/6': No such file or dir
find: './proc/3847156/fd/5': No such file or directory
find: './proc/3847156/fdinfo/5': No such file or directory
find: './root': Permission denied
bandit6@bandit:/$ cat ./var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
bandit6@bandit:/$
```

Level7

Command – cat data.txt | grep millionth

Password – TESKZC0XvTetK0S9xNwm25STk5iWrBvP



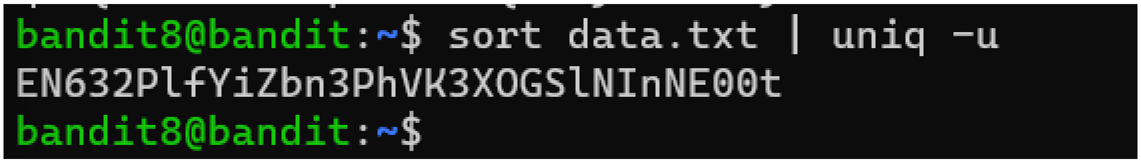
```
Antichrists     OoabOjBHlBLNToKxEQQXSK36AZK2+BBt
madhouse's      qCuSl9VgDj9SzQIDhYWkkZ65q5904VVy
bandit7@bandit:~$ cat data.txt | grep millionth
millionth       TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@bandit:~$
```

Level8

Command – sort data.txt | uniq -u

Password – EN632PlfYiZbn3PhVK3XOGSlNInNE00t

uniq removes sequentially same lines, so we first sort the data in the file and then -u flag[1] displays unique file.



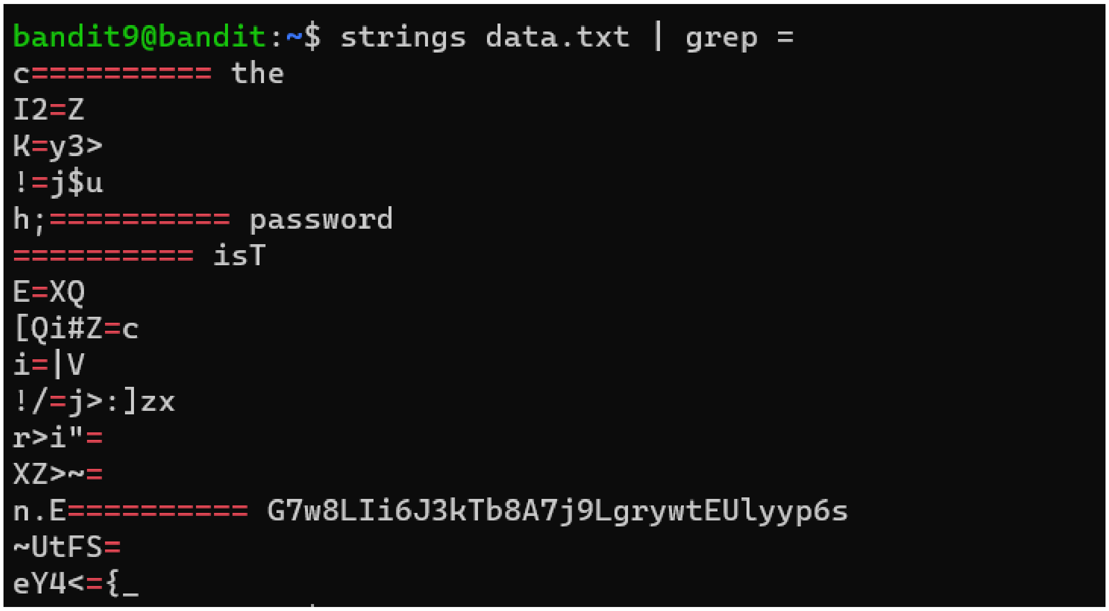
```
bandit8@bandit:~$ sort data.txt | uniq -u
EN632PlfYiZbn3PhVK3XOGSlNInNE00t
bandit8@bandit:~$
```

Level9

Command – strings data.txt | grep =

Password – G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

Search for strings in the file and look for = sign.



```
bandit9@bandit:~$ strings data.txt | grep =
c========== the
I2=Z
K=y3>
!=j$u
h;========== password
========== isT
E=XQ
[Qi#Z=c
i=|V
!/=j>:]zx
r>i"=
XZ>~=
n.E========== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
~UtFS=
eY4<={_
```

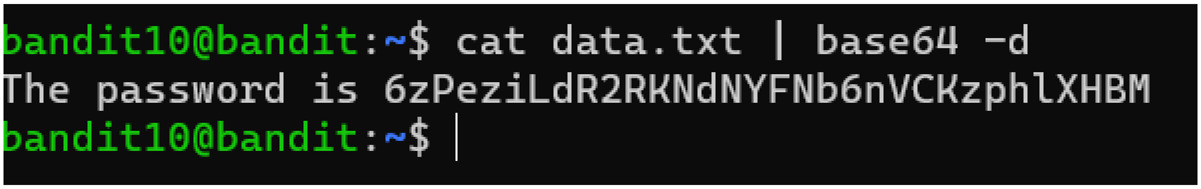
[1] https://www.ibm.com/docs/en/aix/7.2?topic=u-uniq-command

Level10

Command – cat data.txt | base64 -d

Password – 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

Read file and then decode base64 using -d flag.



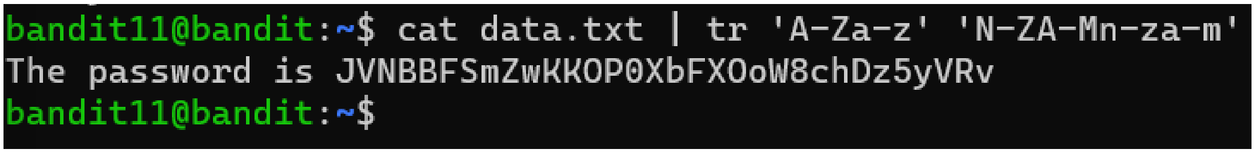
```
bandit10@bandit:~$ cat data.txt | base64 -d
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$ |
```

Level11

Command – cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'

Password – JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

As said on the wikipedia page, tr shifts the characters as mentioned, in this case ‘A-Za-z’ gets shifted by 13 characters to become 'N-ZA-Mn-za-m'. Since it is rot by 13, it is pretty simple to break it as twice the rotation gives the original output.



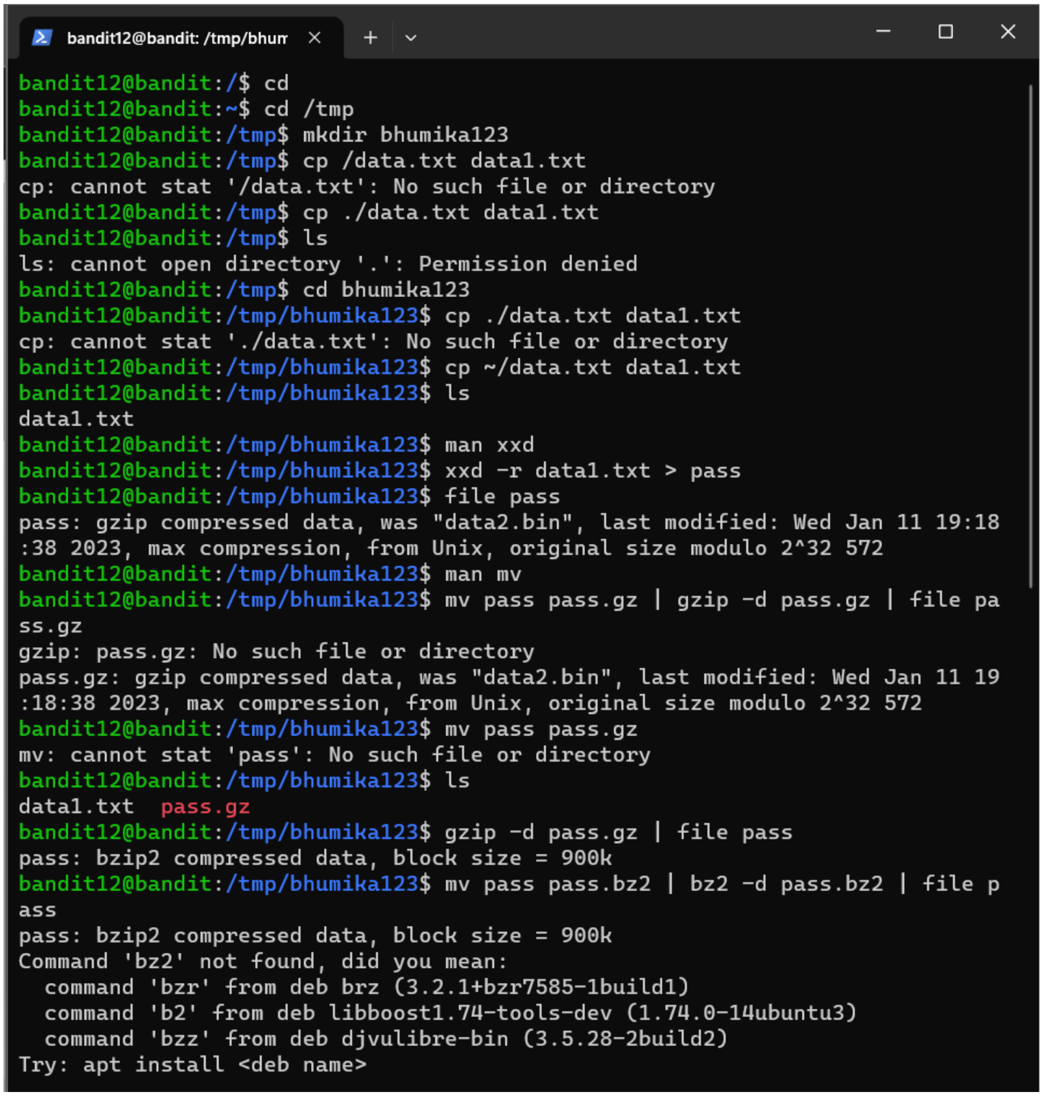
```
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
bandit11@bandit:~$
```

Level12

Password – wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

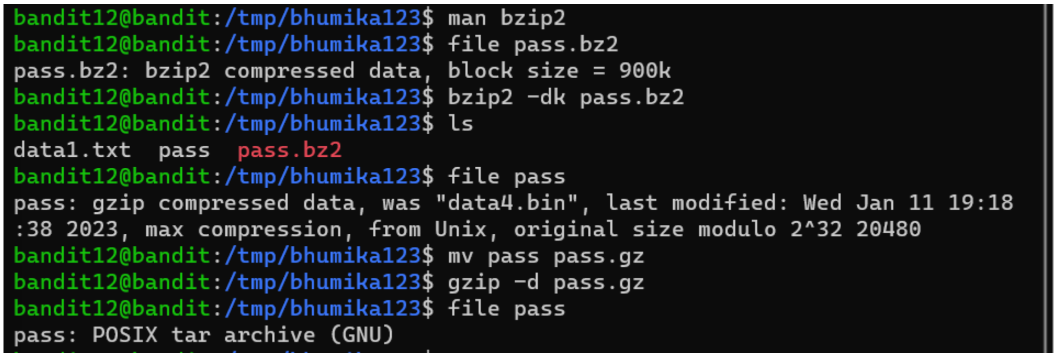
As mentioned in the question, I created a directory in tmp where I copied data.txt as data1.txt and then tried decoding hex dump using xxd and save it as pass. I then checked the file type using file pass cmd which told me the file is gzip type. Rename the file as pass.gz and check its details again using file cmd. This time the file is of bzip2 type whose extension is bz2.

Post which I ran into some errors due to typo and wasn’t able to decode the same. So I started the process again by removing the current pass file.



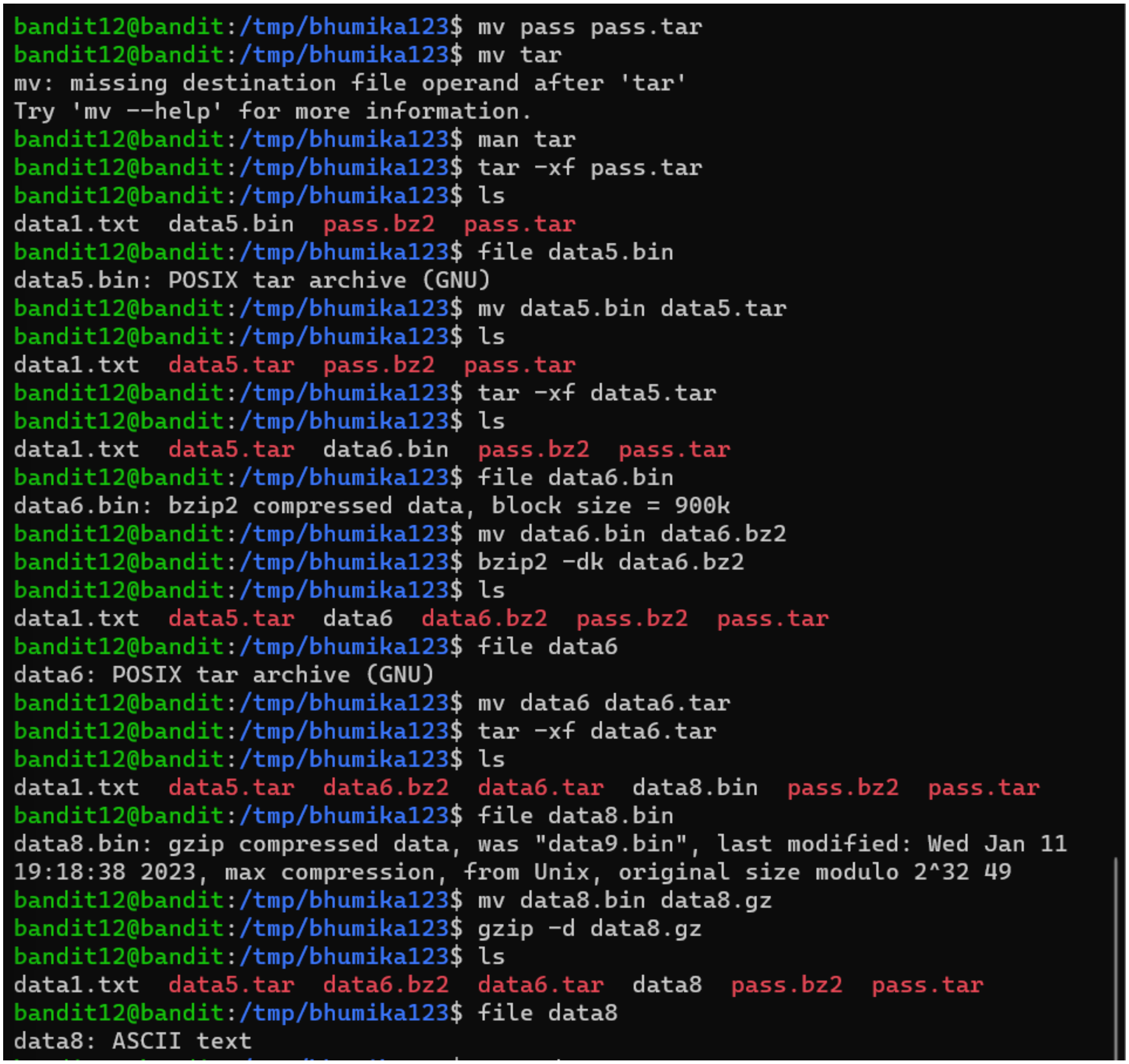
```
bandit12@bandit:/$ cd
bandit12@bandit:~$ cd /tmp
bandit12@bandit:/tmp$ mkdir bhumika123
bandit12@bandit:/tmp$ cp /data.txt data1.txt
cp: cannot stat '/data.txt': No such file or directory
bandit12@bandit:/tmp$ cp ./data.txt data1.txt
bandit12@bandit:/tmp$ ls
ls: cannot open directory '.': Permission denied
bandit12@bandit:/tmp$ cd bhumika123
bandit12@bandit:/tmp/bhumika123$ cp ./data.txt data1.txt
cp: cannot stat './data.txt': No such file or directory
bandit12@bandit:/tmp/bhumika123$ cp ~/data.txt data1.txt
bandit12@bandit:/tmp/bhumika123$ ls
data1.txt
bandit12@bandit:/tmp/bhumika123$ man xxd
bandit12@bandit:/tmp/bhumika123$ xxd -r data1.txt > pass
bandit12@bandit:/tmp/bhumika123$ file pass
pass: gzip compressed data, was "data2.bin", last modified: Wed Jan 11 19:18
:38 2023, max compression, from Unix, original size modulo 2^32 572
bandit12@bandit:/tmp/bhumika123$ man mv
bandit12@bandit:/tmp/bhumika123$ mv pass pass.gz | gzip -d pass.gz | file pa
ss.gz
gzip: pass.gz: No such file or directory
pass.gz: gzip compressed data, was "data2.bin", last modified: Wed Jan 11 19
:18:38 2023, max compression, from Unix, original size modulo 2^32 572
bandit12@bandit:/tmp/bhumika123$ mv pass pass.gz
mv: cannot stat 'pass': No such file or directory
bandit12@bandit:/tmp/bhumika123$ ls
data1.txt  pass.gz
bandit12@bandit:/tmp/bhumika123$ gzip -d pass.gz | file pass
pass: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/bhumika123$ mv pass pass.bz2 | bz2 -d pass.bz2 | file p
ass
pass: bzip2 compressed data, block size = 900k
Command 'bz2' not found, did you mean:
  command 'bzr' from deb brz (3.2.1+bzr7585-1build1)
  command 'b2' from deb libboost1.74-tools-dev (1.74.0-14ubuntu3)
  command 'bzz' from deb djvulibre-bin (3.5.28-2build2)
Try: apt install <deb name>
```

After repeating the previous steps and reaching till bz2 file, I read through the documentation of bzip2 and used the following commands to get the POSIX tar compressed file.



```
bandit12@bandit:/tmp/bhumika123$ man bzip2
bandit12@bandit:/tmp/bhumika123$ file pass.bz2
pass.bz2: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/bhumika123$ bzip2 -dk pass.bz2
bandit12@bandit:/tmp/bhumika123$ ls
data1.txt  pass  pass.bz2
bandit12@bandit:/tmp/bhumika123$ file pass
pass: gzip compressed data, was "data4.bin", last modified: Wed Jan 11 19:18
:38 2023, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/bhumika123$ mv pass pass.gz
bandit12@bandit:/tmp/bhumika123$ gzip -d pass.gz
bandit12@bandit:/tmp/bhumika123$ file pass
pass: POSIX tar archive (GNU)
```

Next, the tar file is unzipped and pass file is extracted from it using tar -xf which gives a file called data5.bin. Which is again a POSIX file and is decompressed to data6.bin which is a bzip2. Continuing this decompression process we finally reach ASCII file and get the password.

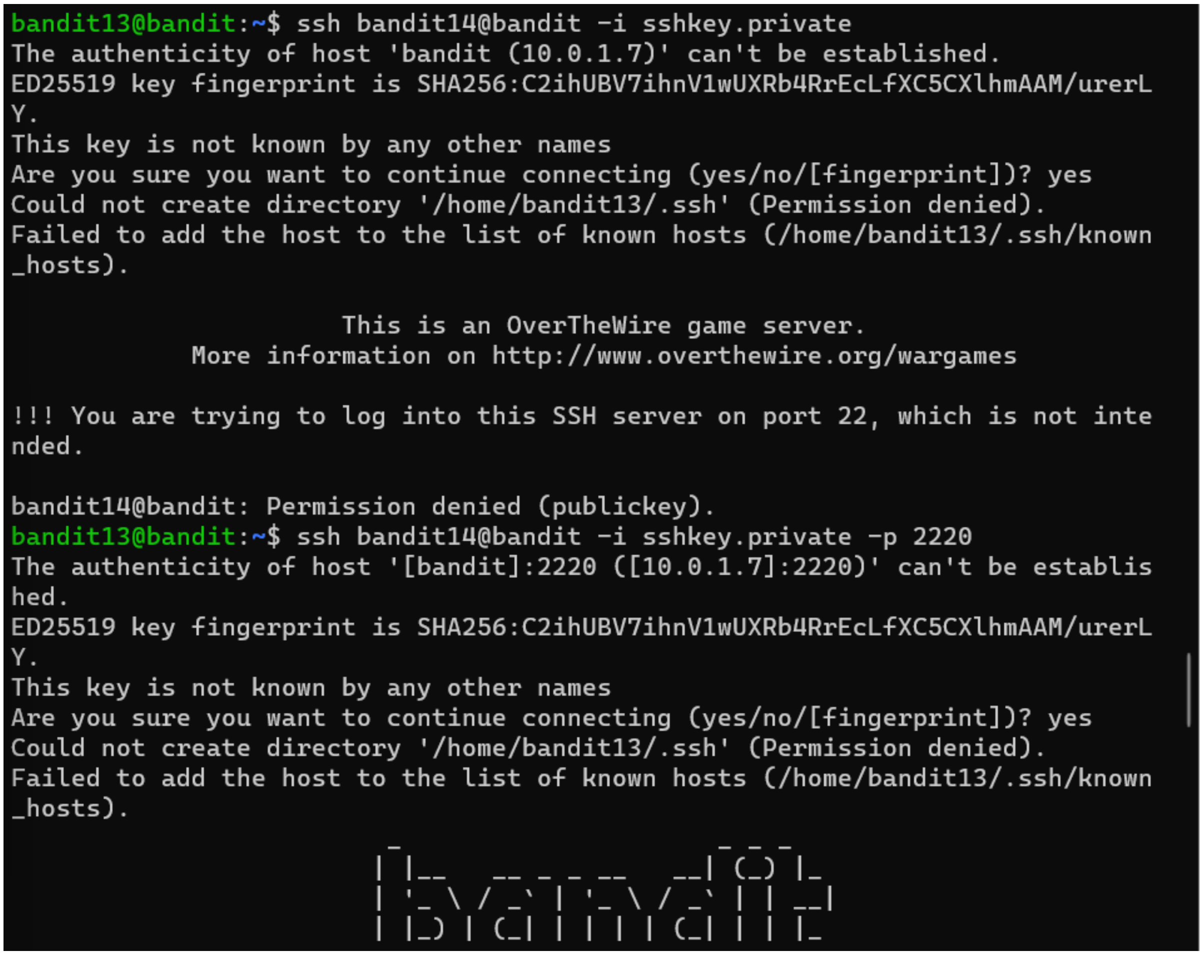


```
bandit12@bandit:/tmp/bhumika123$ mv pass pass.tar
bandit12@bandit:/tmp/bhumika123$ mv tar
mv: missing destination file operand after 'tar'
Try 'mv --help' for more information.
bandit12@bandit:/tmp/bhumika123$ man tar
bandit12@bandit:/tmp/bhumika123$ tar -xf pass.tar
bandit12@bandit:/tmp/bhumika123$ ls
data1.txt  data5.bin  pass.bz2  pass.tar
bandit12@bandit:/tmp/bhumika123$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/bhumika123$ mv data5.bin data5.tar
bandit12@bandit:/tmp/bhumika123$ ls
data1.txt  data5.tar  pass.bz2  pass.tar
bandit12@bandit:/tmp/bhumika123$ tar -xf data5.tar
bandit12@bandit:/tmp/bhumika123$ ls
data1.txt  data5.tar  data6.bin  pass.bz2  pass.tar
bandit12@bandit:/tmp/bhumika123$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/bhumika123$ mv data6.bin data6.bz2
bandit12@bandit:/tmp/bhumika123$ bzip2 -dk data6.bz2
bandit12@bandit:/tmp/bhumika123$ ls
data1.txt  data5.tar  data6  data6.bz2  pass.bz2  pass.tar
bandit12@bandit:/tmp/bhumika123$ file data6
data6: POSIX tar archive (GNU)
bandit12@bandit:/tmp/bhumika123$ mv data6 data6.tar
bandit12@bandit:/tmp/bhumika123$ tar -xf data6.tar
bandit12@bandit:/tmp/bhumika123$ ls
data1.txt  data5.tar  data6.bz2  data6.tar  data8.bin  pass.bz2  pass.tar
bandit12@bandit:/tmp/bhumika123$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Wed Jan 11
19:18:38 2023, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/bhumika123$ mv data8.bin data8.gz
bandit12@bandit:/tmp/bhumika123$ gzip -d data8.gz
bandit12@bandit:/tmp/bhumika123$ ls
data1.txt  data5.tar  data6.bz2  data6.tar  data8  pass.bz2  pass.tar
bandit12@bandit:/tmp/bhumika123$ file data8
data8: ASCII text
```

Level13

Password – fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
ls to see the file name and then use the following command –
ssh bandit14@bandit -i sshkey.private -p 2220

-i is used to identify the file sshkey.private and read the key from it. Earlier I was getting the error about the port which was resolved by adding -p 2220

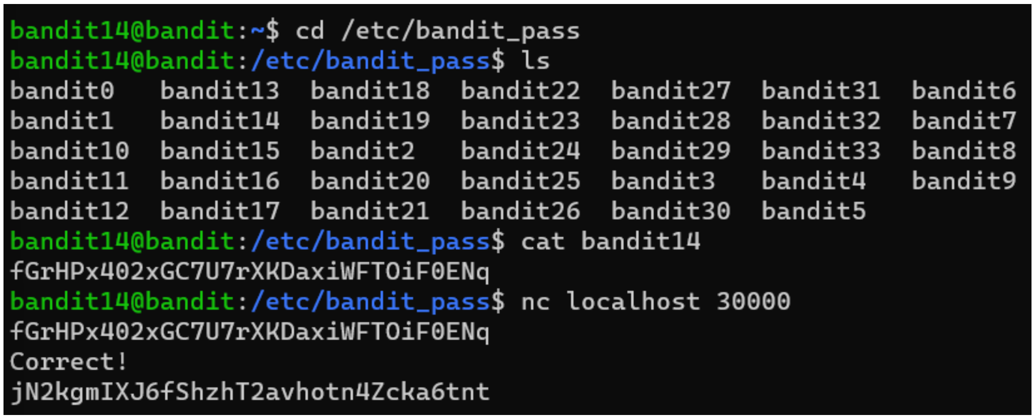


```
bandit13@bandit:~$ ssh bandit14@bandit -i sshkey.private
The authenticity of host 'bandit (10.0.1.7)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerL
Y.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit13/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known
_hosts).

                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

!!! You are trying to log into this SSH server on port 22, which is not inte
nded.

bandit14@bandit: Permission denied (publickey).
bandit13@bandit:~$ ssh bandit14@bandit -i sshkey.private -p 2220
The authenticity of host '[bandit]:2220 ([10.0.1.7]:2220)' can't be establis
hed.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerL
Y.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit13/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known
_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
```

Level14

Password – jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

First, get the password for level 14 as mentioned in lvl 13 and then we can use the following command : nc localhost 30000 to get the password for nect level.

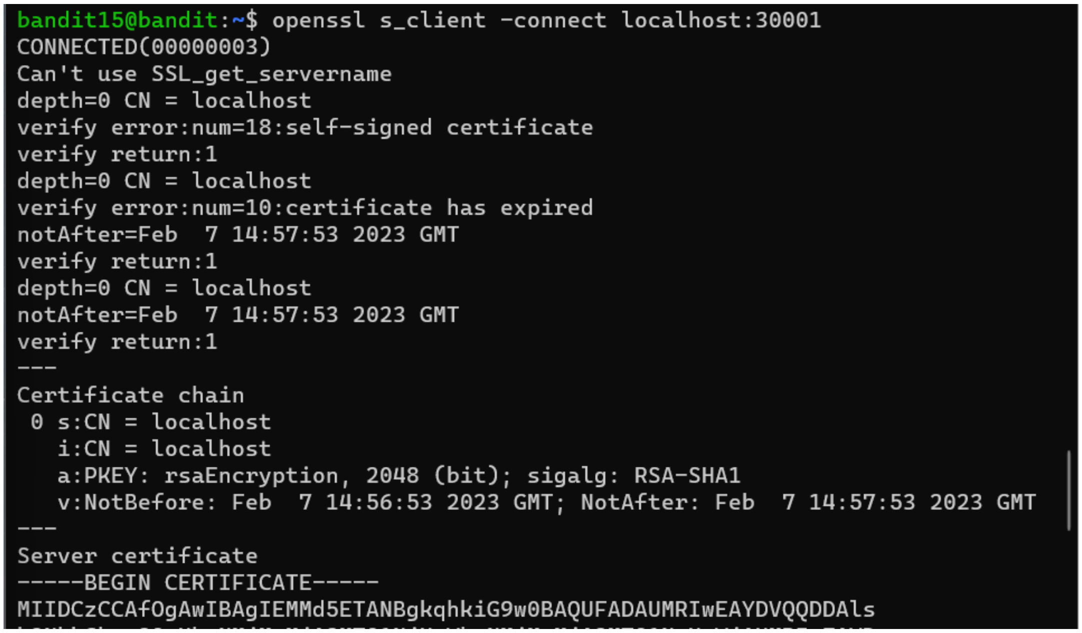


```
bandit14@bandit:~$ cd /etc/bandit_pass
bandit14@bandit:/etc/bandit_pass$ ls
bandit0   bandit13  bandit18  bandit22  bandit27  bandit31  bandit6
bandit1   bandit14  bandit19  bandit23  bandit28  bandit32  bandit7
bandit10  bandit15  bandit2   bandit24  bandit29  bandit33  bandit8
bandit11  bandit16  bandit20  bandit25  bandit3   bandit4   bandit9
bandit12  bandit17  bandit21  bandit26  bandit30  bandit5
bandit14@bandit:/etc/bandit_pass$ cat bandit14
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
bandit14@bandit:/etc/bandit_pass$ nc localhost 30000
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
```

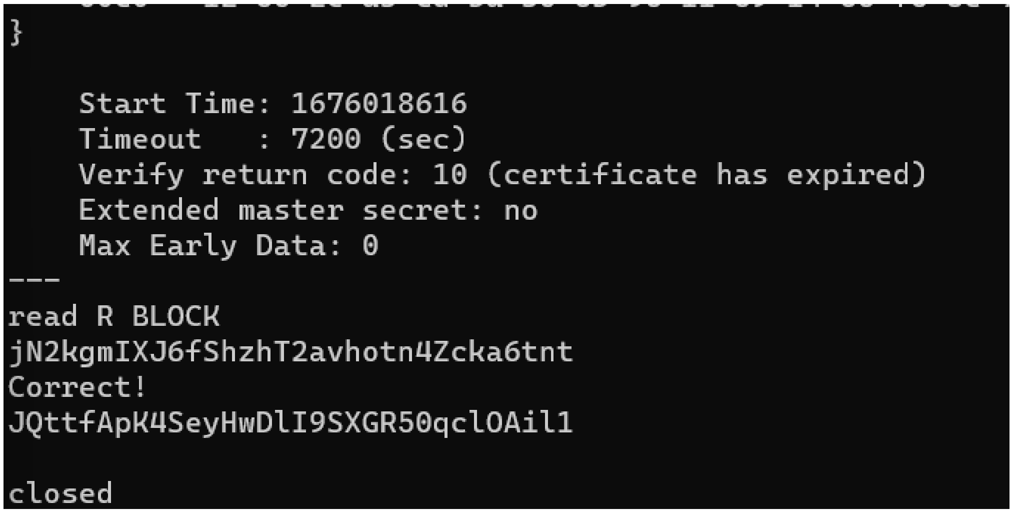
Level15

Password – JQttfApK4SeyHwDlI9SXGR50qclOAil1

I tried connecting to the server using the command[2]: openssl s_client -connect localhost:30001 which gave the following output and then entering the password of the previous level gave the new password.



```
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Feb  7 14:57:53 2023 GMT
verify return:1
depth=0 CN = localhost
notAfter=Feb  7 14:57:53 2023 GMT
verify return:1
---
Certificate chain
 0 s:CN = localhost
   i:CN = localhost
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA1
   v:NotBefore: Feb  7 14:56:53 2023 GMT; NotAfter: Feb  7 14:57:53 2023 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDCzCCAfOgAwIBAgIEMMd5ETANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDDAls
```



```
}

    Start Time: 1676018616
    Timeout   : 7200 (sec)
    Verify return code: 10 (certificate has expired)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
Correct!
JQttfApK4SeyHwDlI9SXGR50qclOAil1

closed
```

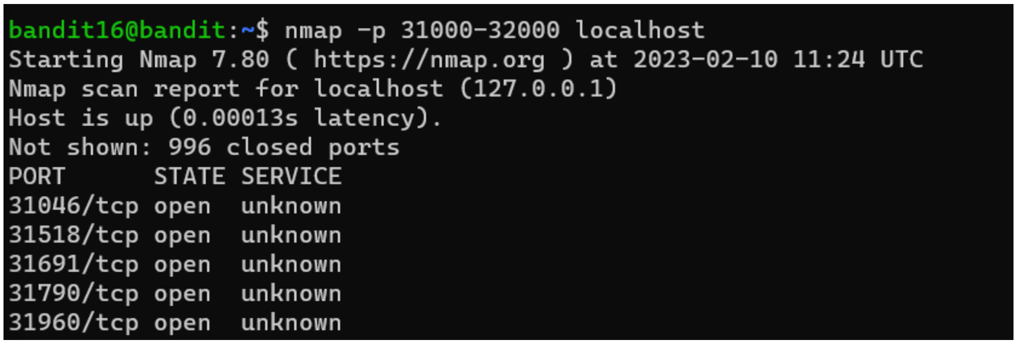
Level16

Password – VwOSWtCA7lRKkTfbr2IDh6awj9RNZM5e

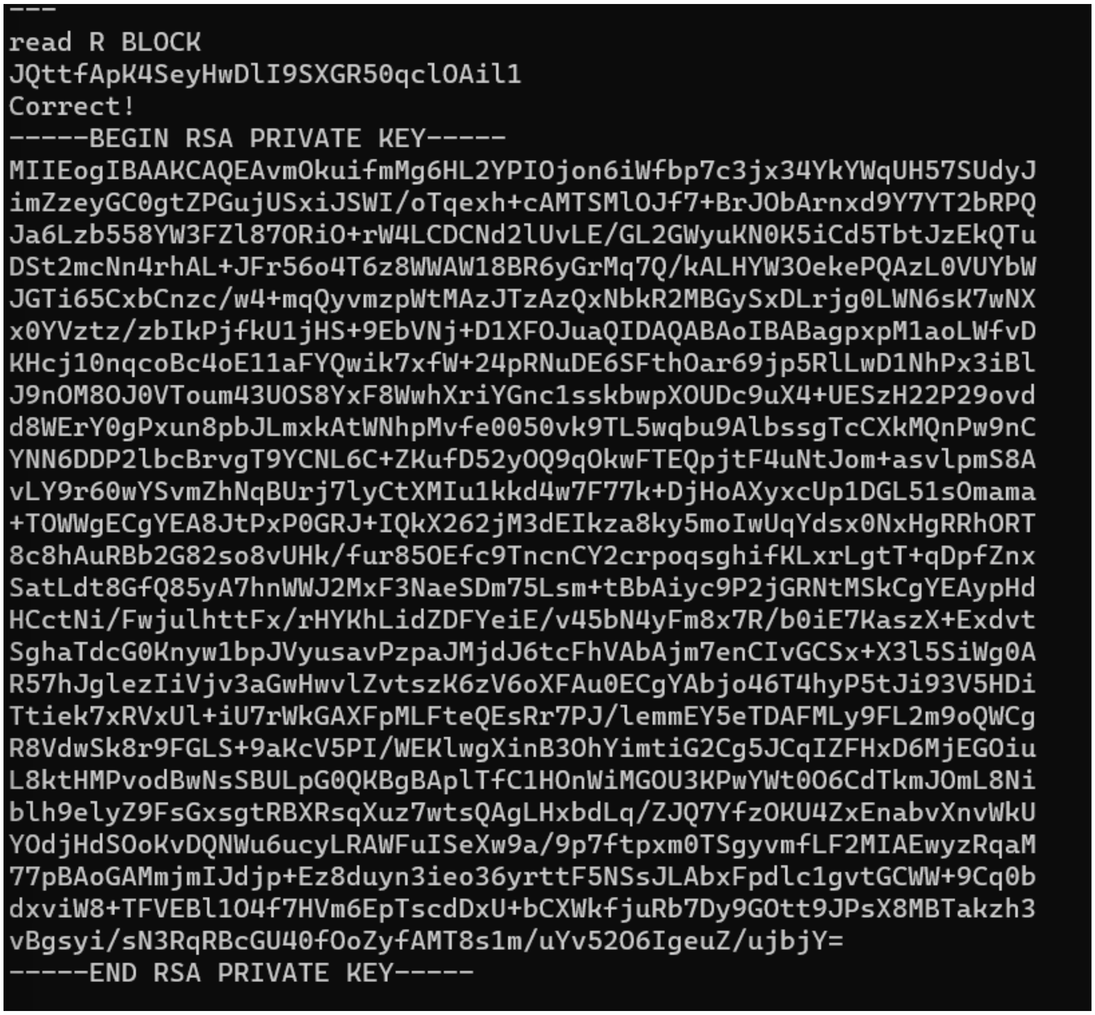
Use the command nmap -p 31000-32000 localhost to find that only 5 ports are open, rest 996 are closed. I tried using various flags to find the ssl port but none worked. Hit and trial gave the required port as 31790 which gave the required RSA private key.

We then save this in a file called pass.key

[2] https://www.openssl.org/docs/man1.0.2/man1/openssl-s_client.html



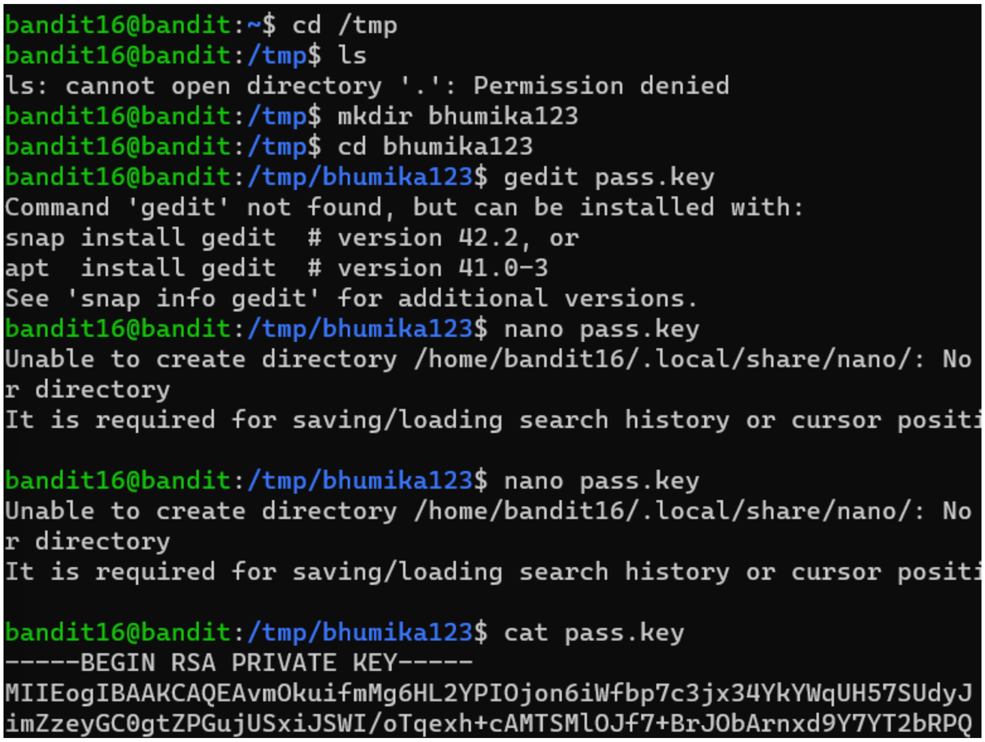
```
bandit16@bandit:~$ nmap -p 31000-32000 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-10 11:24 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown
```



```
---
read R BLOCK
JQttfApK4SeyHwDlI9SXGR50qclOAil1
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/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

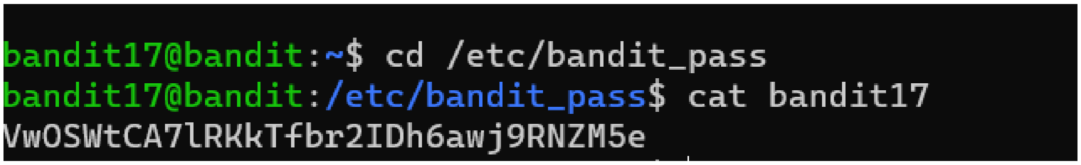
Imp — It is important to change the file permissions to make the pass.key a private file. Otherwise it will not accepted and throw the following error –

> Permissions 0664 for 'pass.key' are too open.
> It is required that your private key files are NOT accessible by others.
> This private key will be ignored.



```
bandit16@bandit:~$ cd /tmp
bandit16@bandit:/tmp$ ls
ls: cannot open directory '.': Permission denied
bandit16@bandit:/tmp$ mkdir bhumika123
bandit16@bandit:/tmp$ cd bhumika123
bandit16@bandit:/tmp/bhumika123$ gedit pass.key
Command 'gedit' not found, but can be installed with:
snap install gedit  # version 42.2, or
apt  install gedit  # version 41.0-3
See 'snap info gedit' for additional versions.
bandit16@bandit:/tmp/bhumika123$ nano pass.key
Unable to create directory /home/bandit16/.local/share/nano/: No
r directory
It is required for saving/loading search history or cursor positi

bandit16@bandit:/tmp/bhumika123$ nano pass.key
Unable to create directory /home/bandit16/.local/share/nano/: No
r directory
It is required for saving/loading search history or cursor positi

bandit16@bandit:/tmp/bhumika123$ cat pass.key
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
```

Then login using ssh to bandit17 and like the one of the previous level, locate the password file.

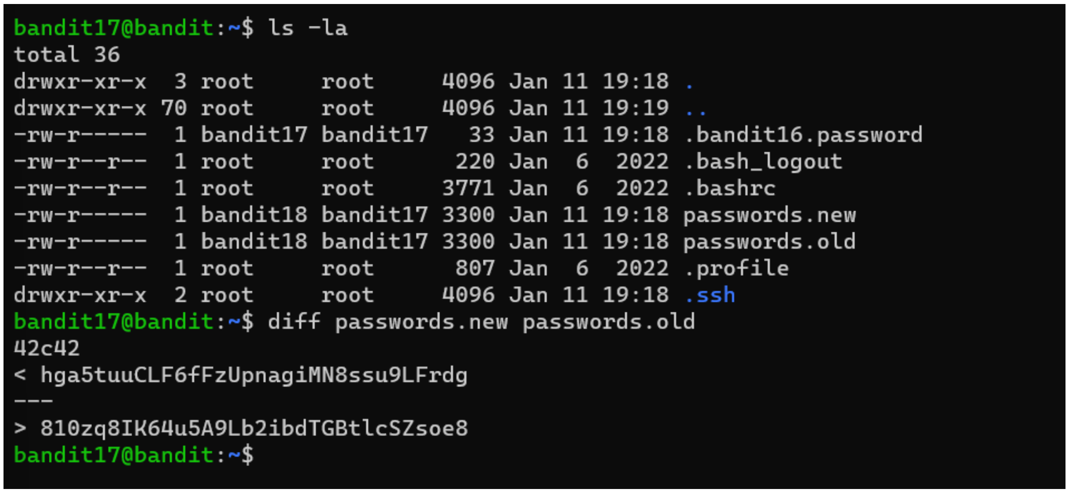


```
bandit17@bandit:~$ cd /etc/bandit_pass
bandit17@bandit:/etc/bandit_pass$ cat bandit17
VwOSWtCA7lRKkTfbr2IDh6awj9RNZM5e
```

Level17

Password – hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg

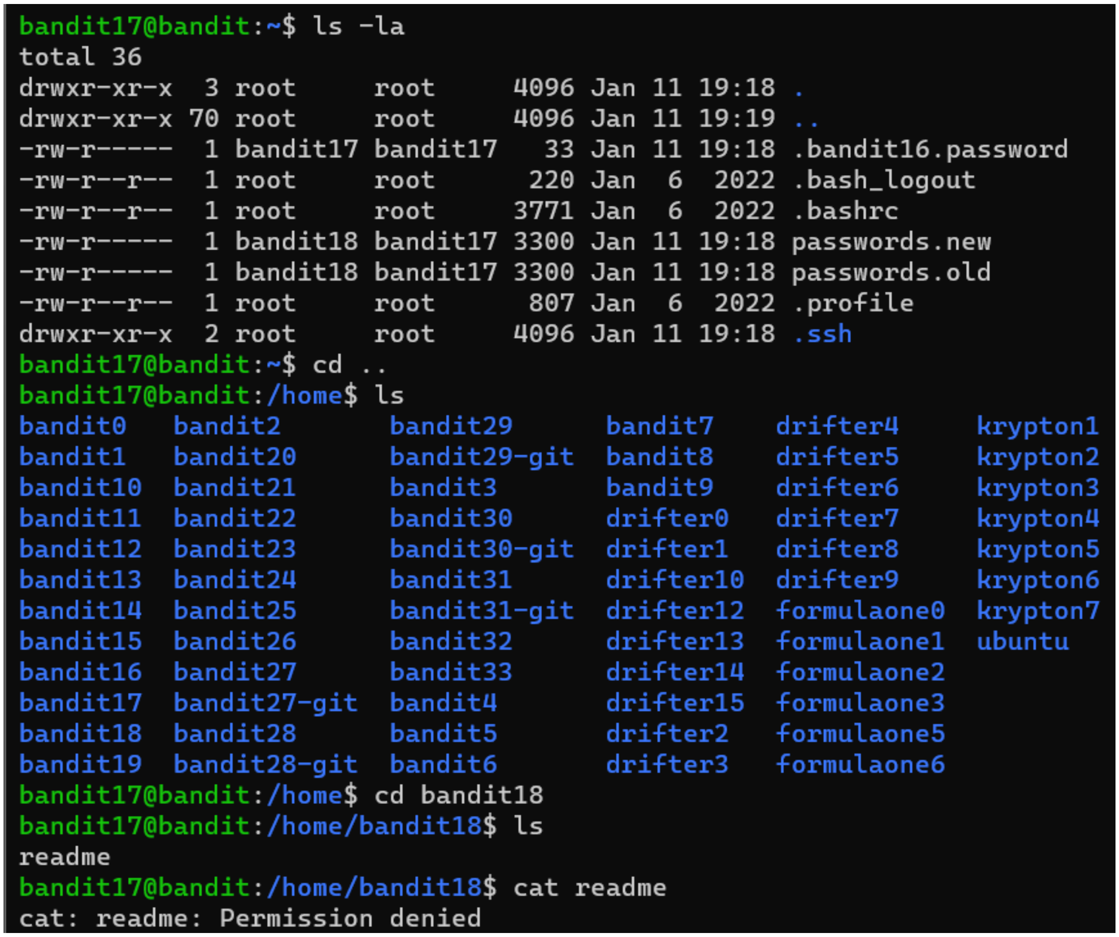
Using the command *diff passwords.new passwords.old*, we get the following two strings. I then tried both to login to bandit19 but only one of them worked and gave as hinted "Byebye !" but the connection closed as well.



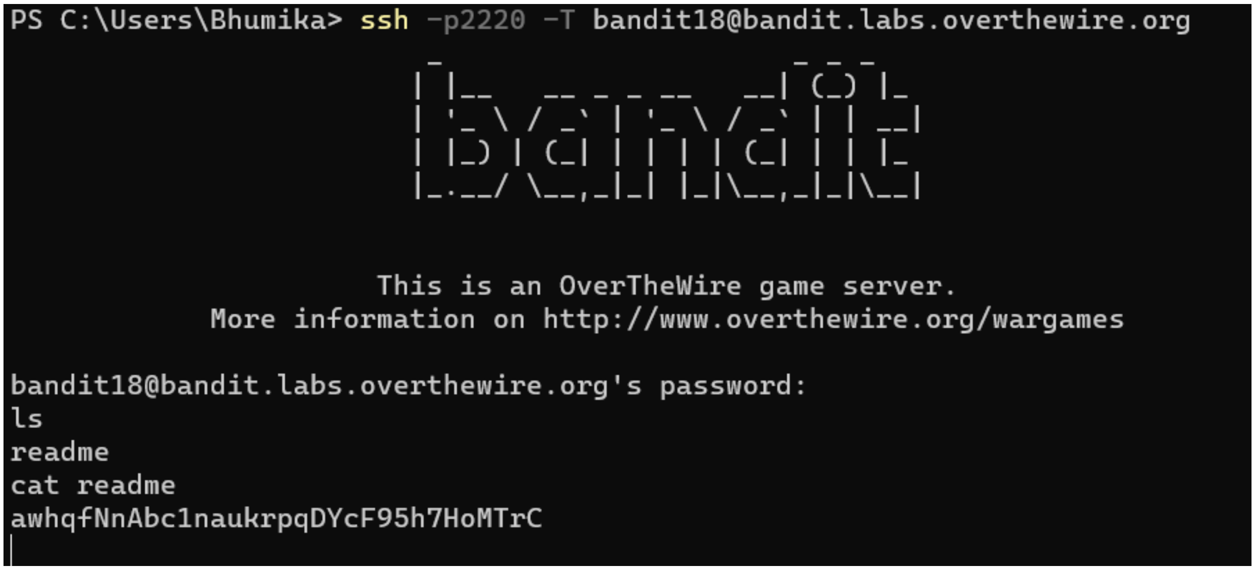
```
bandit17@bandit:~$ ls -la
total 36
drwxr-xr-x  3 root     root     4096 Jan 11 19:18 .
drwxr-xr-x 70 root     root     4096 Jan 11 19:19 ..
-rw-r-----  1 bandit17 bandit17   33 Jan 11 19:18 .bandit16.password
-rw-r--r--  1 root     root      220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root     root     3771 Jan  6  2022 .bashrc
-rw-r-----  1 bandit18 bandit17 3300 Jan 11 19:18 passwords.new
-rw-r-----  1 bandit18 bandit17 3300 Jan 11 19:18 passwords.old
-rw-r--r--  1 root     root      807 Jan  6  2022 .profile
drwxr-xr-x  2 root     root     4096 Jan 11 19:18 .ssh
bandit17@bandit:~$ diff passwords.new passwords.old
42c42
< hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
---
> 810zq8IK64u5A9Lb2ibdTGBtlcSZsoe8
bandit17@bandit:~$
```

Level18
Password – awhqfNnAbc1naukrpqDYcF95h7HoMTrC

I went to bandit18 from bandit17 and tried reading the file and modifying .bashrc file but I don’t have permission to do either. After making various such attempts to get access to either of these files, I looked up for other ways to login and tried ftp but in vain.
I tried ssh again with -t flag and it gave the error that rsa key is too public so I copied it, changed the file permissions and tried again using -i. But it didn’t work either. The error it gave was the issue with localhost login so I logged out and tried ssh-ing again using tunnel flag and VOILA, it worked. After entering the password, there was a blank screen, to which I thought wither it’s slow or might time out. After trying again, I randomly entered ls and it showed readme file, which gave the above password.



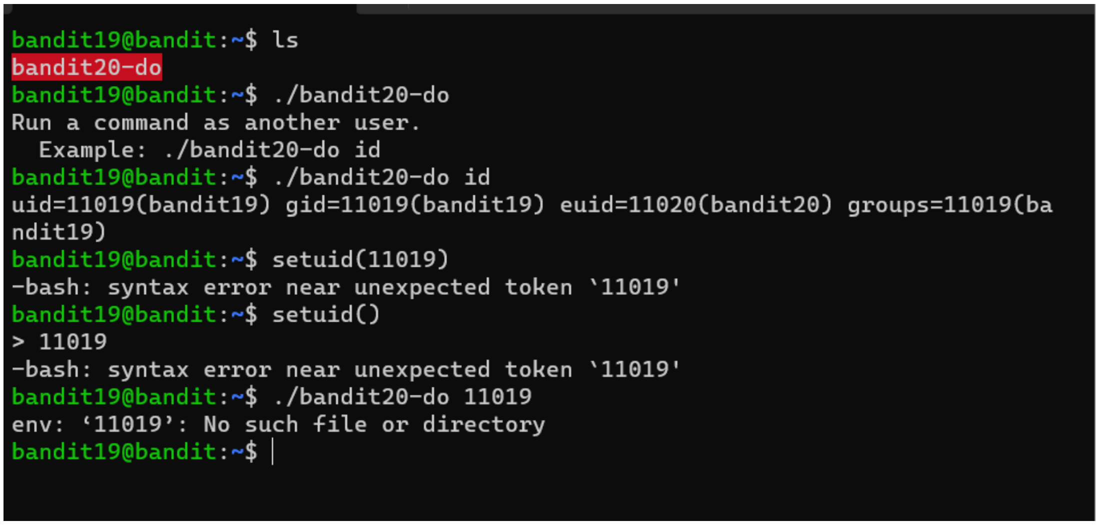
```
bandit17@bandit:~$ ls -la
total 36
drwxr-xr-x  3 root     root     4096 Jan 11 19:18 .
drwxr-xr-x 70 root     root     4096 Jan 11 19:19 ..
-rw-r-----  1 bandit17 bandit17   33 Jan 11 19:18 .bandit16.password
-rw-r--r--  1 root     root      220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root     root     3771 Jan  6  2022 .bashrc
-rw-r-----  1 bandit18 bandit17 3300 Jan 11 19:18 passwords.new
-rw-r-----  1 bandit18 bandit17 3300 Jan 11 19:18 passwords.old
-rw-r--r--  1 root     root      807 Jan  6  2022 .profile
drwxr-xr-x  2 root     root     4096 Jan 11 19:18 .ssh
bandit17@bandit:~$ cd ..
bandit17@bandit:/home$ ls
bandit0   bandit2       bandit29      bandit7    drifter4     krypton1
bandit1   bandit20      bandit29-git  bandit8    drifter5     krypton2
bandit10  bandit21      bandit3       bandit9    drifter6     krypton3
bandit11  bandit22      bandit30      drifter0   drifter7     krypton4
bandit12  bandit23      bandit30-git  drifter1   drifter8     krypton5
bandit13  bandit24      bandit31      drifter10  drifter9     krypton6
bandit14  bandit25      bandit31-git  drifter12  formulaone0  krypton7
bandit15  bandit26      bandit32      drifter13  formulaone1  ubuntu
bandit16  bandit27      bandit33      drifter14  formulaone2
bandit17  bandit27-git  bandit4       drifter15  formulaone3
bandit18  bandit28      bandit5       drifter2   formulaone5
bandit19  bandit28-git  bandit6       drifter3   formulaone6
bandit17@bandit:/home$ cd bandit18
bandit17@bandit:/home/bandit18$ ls
readme
bandit17@bandit:/home/bandit18$ cat readme
cat: readme: Permission denied
```



```
PS C:\Users\Bhumika> ssh -p2220 -T bandit18@bandit.labs.overthewire.org
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:
ls
readme
cat readme
awhqfNnAbc1naukrpqDYcF95h7HoMTrC
```

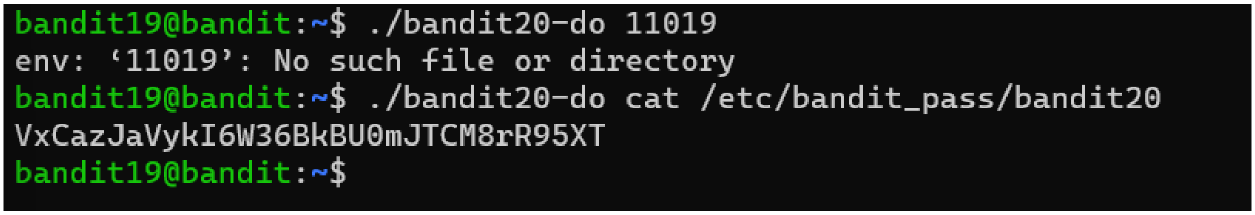
Level19
Password – VxCazJaVykI6W36BkBU0mJTCM8rR95XT

As mentioned in the hint, I ran setuid and also tried man setuid to understand it better. Then ls in the directory, which showed an executable. The executable said run a command as another user and following the instruction gave the following:



```
bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
  Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(ba
ndit19)
bandit19@bandit:~$ setuid(11019)
-bash: syntax error near unexpected token `11019'
bandit19@bandit:~$ setuid()
> 11019
-bash: syntax error near unexpected token `11019'
bandit19@bandit:~$ ./bandit20-do 11019
env: ‘11019’: No such file or directory
bandit19@bandit:~$ |
```

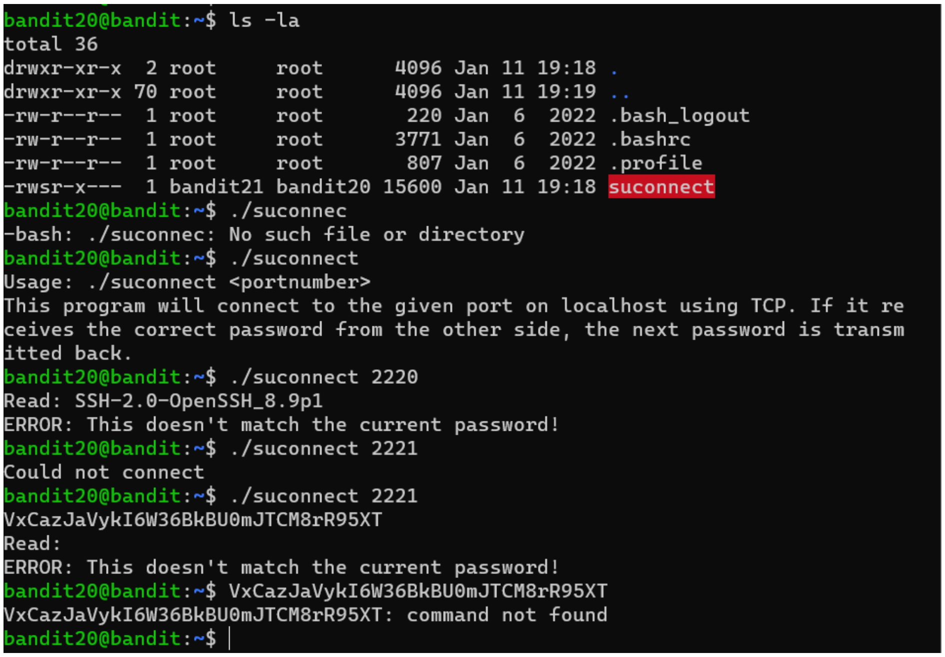
After, a few failed attempts, I tried the following command, which worked and gave the password.



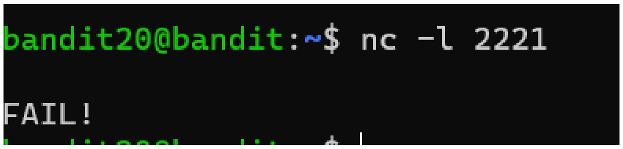
```
bandit19@bandit:~$ ./bandit20-do 11019
env: ‘11019’: No such file or directory
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVykI6W36BkBU0mJTCM8rR95XT
bandit19@bandit:~$
```

Level20
Password – NvEJF7oVjkddltPSrdKEFOllh9V1IBcq

We need two windows for this, one to send signal, other to receive. I tried the following basic commands to get the password, but it failed.

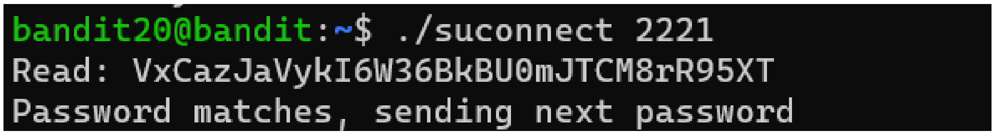


```
bandit20@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root     root      4096 Jan 11 19:18 .
drwxr-xr-x 70 root     root      4096 Jan 11 19:19 ..
-rw-r--r--  1 root     root       220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root     root      3771 Jan  6  2022 .bashrc
-rw-r--r--  1 root     root       807 Jan  6  2022 .profile
-rwsr-x---  1 bandit21 bandit20 15600 Jan 11 19:18 suconnect
bandit20@bandit:~$ ./suconnec
-bash: ./suconnec: No such file or directory
bandit20@bandit:~$ ./suconnect
Usage: ./suconnect <portnumber>
This program will connect to the given port on localhost using TCP. If it re
ceives the correct password from the other side, the next password is transm
itted back.
bandit20@bandit:~$ ./suconnect 2220
Read: SSH-2.0-OpenSSH_8.9p1
ERROR: This doesn't match the current password!
bandit20@bandit:~$ ./suconnect 2221
Could not connect
bandit20@bandit:~$ ./suconnect 2221
VxCazJaVykI6W36BkBU0mJTCM8rR95XT
Read:
ERROR: This doesn't match the current password!
bandit20@bandit:~$ VxCazJaVykI6W36BkBU0mJTCM8rR95XT
VxCazJaVykI6W36BkBU0mJTCM8rR95XT: command not found
bandit20@bandit:~$ |
```

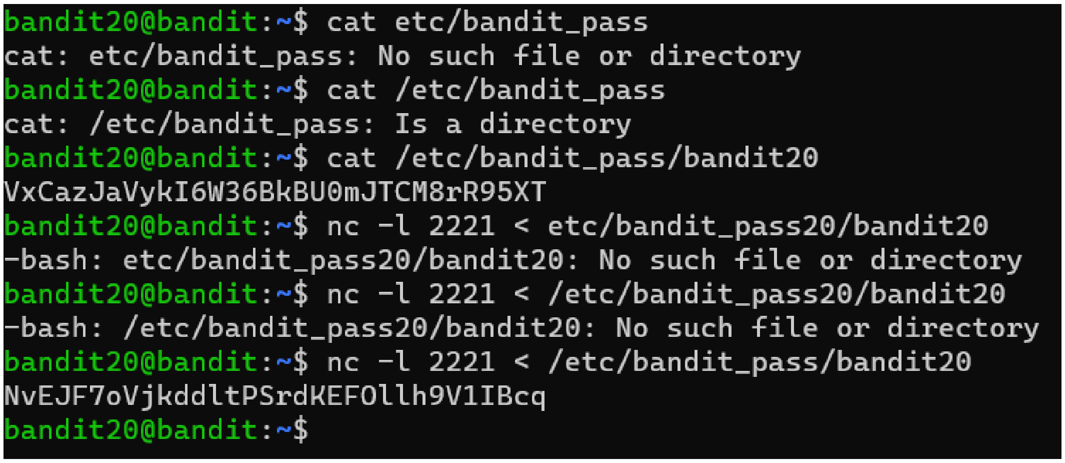


```
bandit20@bandit:~$ nc -l 2221

FAIL!
```

I then realised that nc -l 2221 also needs to have the same password, so connected it with the password path and tried the same thing again and it worked.



```
bandit20@bandit:~$ ./suconnect 2221
Read: VxCazJaVykI6W36BkBU0mJTCM8rR95XT
Password matches, sending next password
```



```
bandit20@bandit:~$ cat etc/bandit_pass
cat: etc/bandit_pass: No such file or directory
bandit20@bandit:~$ cat /etc/bandit_pass
cat: /etc/bandit_pass: Is a directory
bandit20@bandit:~$ cat /etc/bandit_pass/bandit20
VxCazJaVykI6W36BkBU0mJTCM8rR95XT
bandit20@bandit:~$ nc -l 2221 < etc/bandit_pass20/bandit20
-bash: etc/bandit_pass20/bandit20: No such file or directory
bandit20@bandit:~$ nc -l 2221 < /etc/bandit_pass20/bandit20
-bash: /etc/bandit_pass20/bandit20: No such file or directory
bandit20@bandit:~$ nc -l 2221 < /etc/bandit_pass/bandit20
NvEJF7oVjkddltPSrdKEFOllh9V1IBcq
bandit20@bandit:~$
```