Bandit Level 0

SSH Information

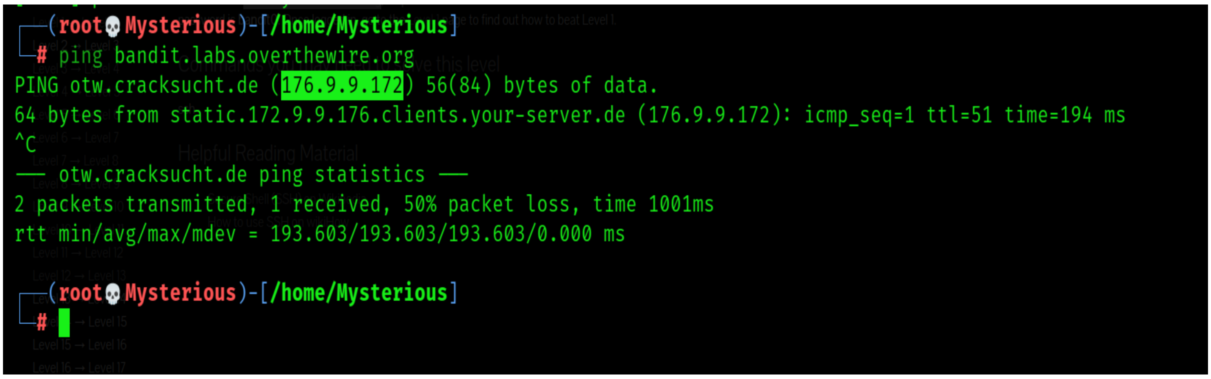
Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

Port: 2220

Username: bandit0

Password: bandit0



```
┌──(root💀Mysterious)-[/home/Mysterious]
└─# ping bandit.labs.overthewire.org
PING otw.cracksucht.de (176.9.9.172) 56(84) bytes of data.
64 bytes from static.172.9.9.176.clients.your-server.de (176.9.9.172): icmp_seq=1 ttl=51 time=194 ms
^C
── otw.cracksucht.de ping statistics ──
2 packets transmitted, 1 received, 50% packet loss, time 1001ms
rtt min/avg/max/mdev = 193.603/193.603/193.603/0.000 ms

┌──(root💀Mysterious)-[/home/Mysterious]
└─# █
```

```
ping bandit.labs.overthewire.org
```

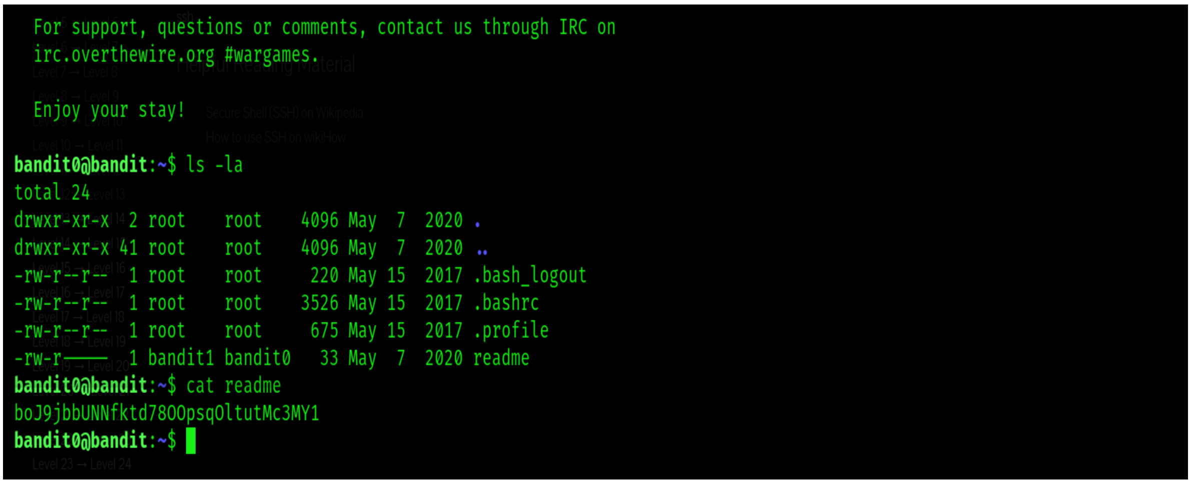
[Note: This step is optional. I have used it to check whether the site is responding back or not and also find the ipv4 address of the host website.]

Using the given details, connect to the server via ssh

```
ssh bandit0@176.9.9.172 -p2220
```

or

ssh bandit0@ bandit.labs.overthewire.org -p2220



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

   Enjoy your stay!

bandit0@bandit:~$ ls -la
total 24
drwxr-xr-x  2 root    root    4096 May  7  2020 .
drwxr-xr-x 41 root    root    4096 May  7  2020 ..
-rw-r--r--  1 root    root     220 May 15  2017 .bash_logout
-rw-r--r--  1 root    root    3526 May 15  2017 .bashrc
-rw-r--r--  1 root    root     675 May 15  2017 .profile
-rw-r-----  1 bandit1 bandit0   33 May  7  2020 readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
bandit0@bandit:~$ █
```

Use ls -la to list all the files and directories. We'll get a readme file which contains the password of the next level.

Using cat command we can print the content in the terminal.

Bandit Level 1

SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

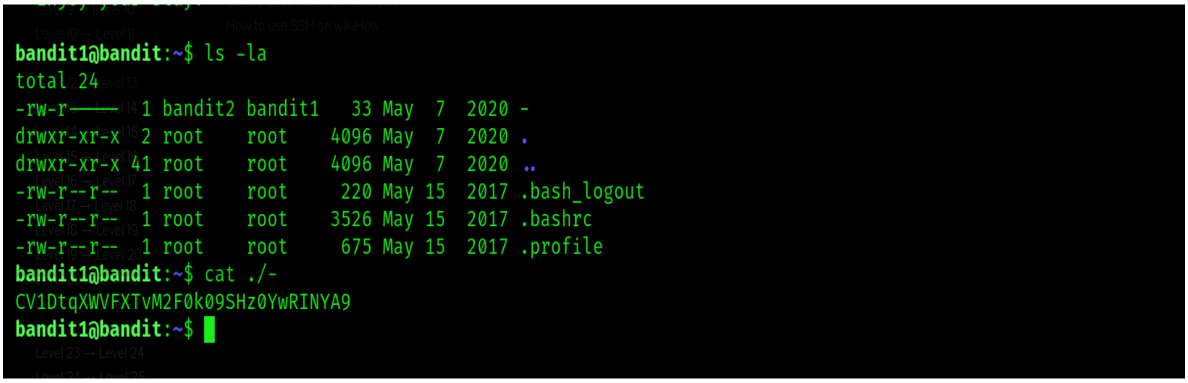
Port: 2220

Username: bandit1

Password:
boJ9jbbUNNfktd78OOpsqOltutMc3MY1

Using the given details, connect to the server via ssh

```
ssh bandit1@176.9.9.172 -p2220
```



```
bandit1@bandit:~$ ls -la
total 24
-rw-r-----  1 bandit2 bandit1   33 May  7  2020 -
drwxr-xr-x  2 root    root    4096 May  7  2020 .
drwxr-xr-x 41 root    root    4096 May  7  2020 ..
-rw-r--r--  1 root    root     220 May 15  2017 .bash_logout
-rw-r--r--  1 root    root    3526 May 15  2017 .bashrc
-rw-r--r--  1 root    root     675 May 15  2017 .profile
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ 
```

After listing all the content of the file, we found a file ‘-‘. Using `cat ./-` command, we get the password of next level.

[Note: As the file name is ‘-‘, so we can’t use cat -. We have to use the full path `cat /home/bandit1/-` or `cat ./-`]

Bandit Level 2

SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

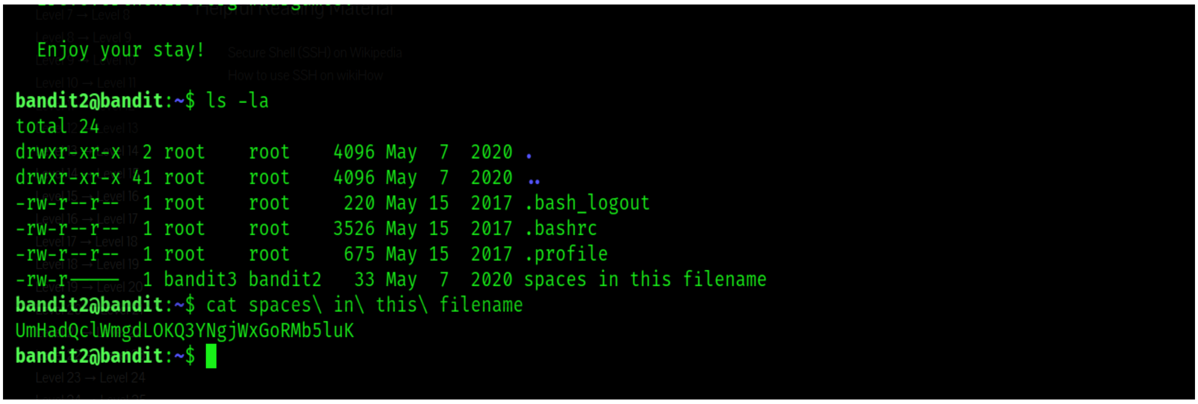
Port: 2220

Username: bandit2

Password:
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

Using the given details, connect to the server via ssh

ssh bandit2@176.9.9.172 -p2220



```
  Enjoy your stay!

bandit2@bandit:~$ ls -la
total 24
drwxr-xr-x  2 root    root    4096 May  7  2020 .
drwxr-xr-x 41 root    root    4096 May  7  2020 ..
-rw-r--r--  1 root    root     220 May 15  2017 .bash_logout
-rw-r--r--  1 root    root    3526 May 15  2017 .bashrc
-rw-r--r--  1 root    root     675 May 15  2017 .profile
-rw-r-----  1 bandit3 bandit2   33 May  7  2020 spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$ 
```

After listing all the content of the file, we found a file ‘space in this filename ‘.

Using cat spaces\ in\ this\ filename command, we get the password of next level.

Bandit Level 3

SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

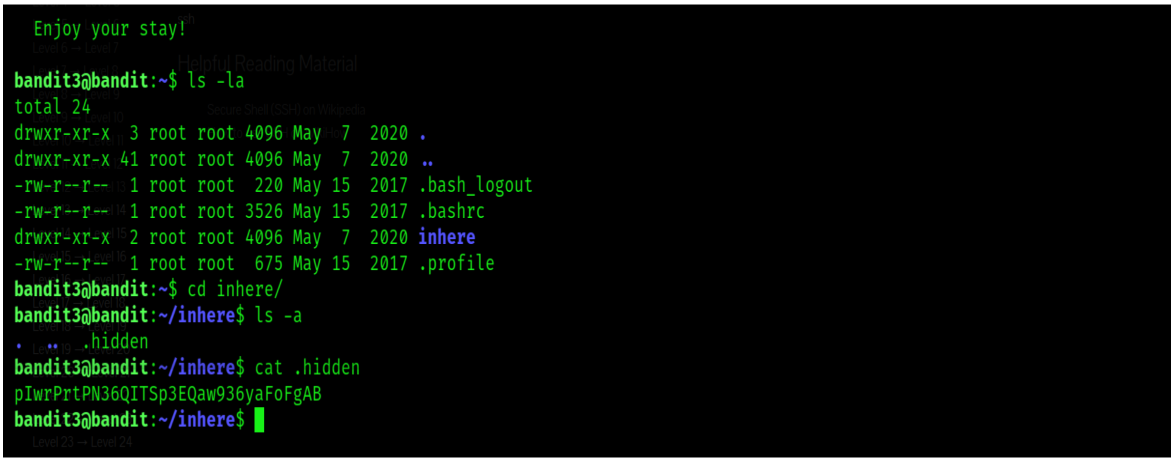
Port: 2220

Username: bandit3

Password: UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

Using the given details, connect to the server via ssh

```
ssh bandit3@176.9.9.172 -p2220
```



```
  Enjoy your stay!

bandit3@bandit:~$ ls -la
total 24
drwxr-xr-x  3 root root 4096 May  7  2020 .
drwxr-xr-x 41 root root 4096 May  7  2020 ..
-rw-r--r--  1 root root  220 May 15  2017 .bash_logout
-rw-r--r--  1 root root 3526 May 15  2017 .bashrc
drwxr-xr-x  2 root root 4096 May  7  2020 inhere
-rw-r--r--  1 root root  675 May 15  2017 .profile
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$ 
```

We found a sub-dir “inhere” in the current dir. Using cd inhere we entered the inhere dir. After that we got a hidden file called “.hidden” inside the inhere dir which contains the password of the next level.

Bandit Level 4

SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

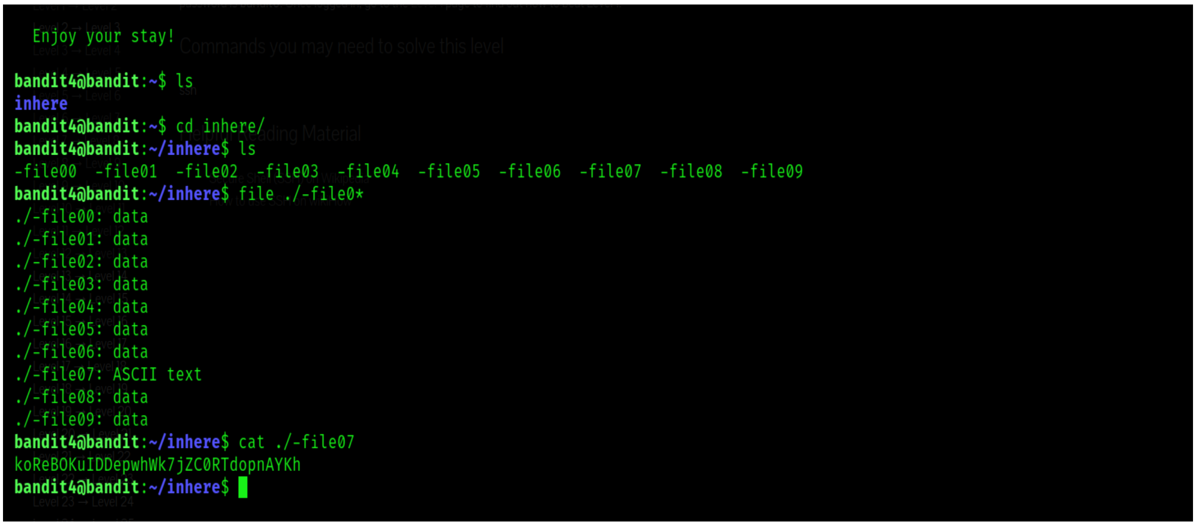
Port: 2220

Username: bandit4

Password:
pIwrPrtPN36QITSp3EQaw936yaFoFgAB

Using the given details, connect to the server via ssh

```
ssh bandit4@176.9.9.172 -p2220
```



```
  Enjoy your stay!

bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ file ./-file0*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$ 
```

We got 10 files inside the inhere dir. We can find the exact human readable file using the command file ./-file0*

Bandit Level 5

SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

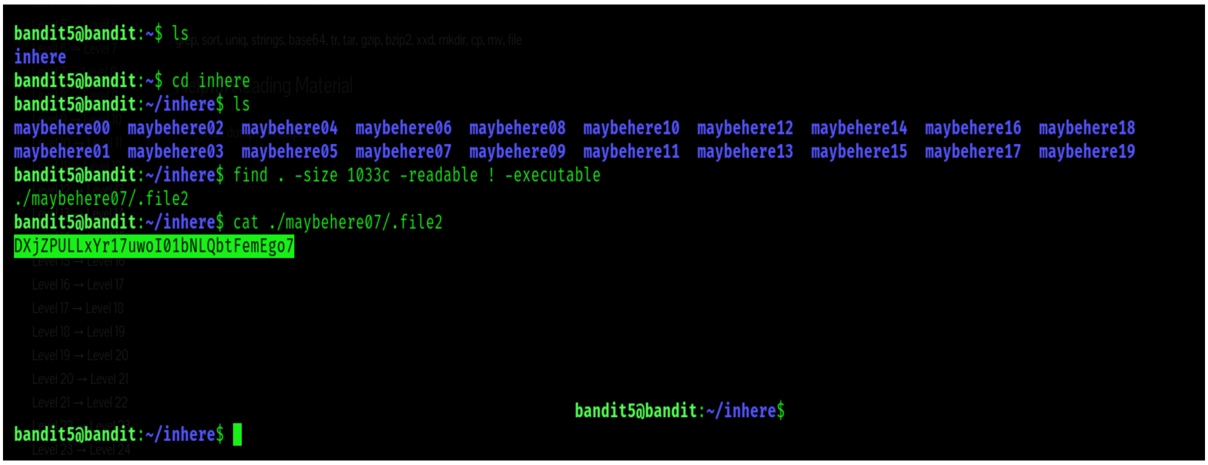
Port: 2220

Username: bandit5

Password:
koReBOKuIDDepwhWk7jZC0RTdopnAYKh

Using the given details, connect to the server via ssh

```
ssh bandit5@176.9.9.172 -p2220
```



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






                                                                  bandit5@bandit:~/inhere$
bandit5@bandit:~/inhere$ 
```

We got 20 dir inside the inhere dir. We can find the exact file having 1033 bytes size using the command find . -size 1033c -readable ! -executable

Bandit Level 6

SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

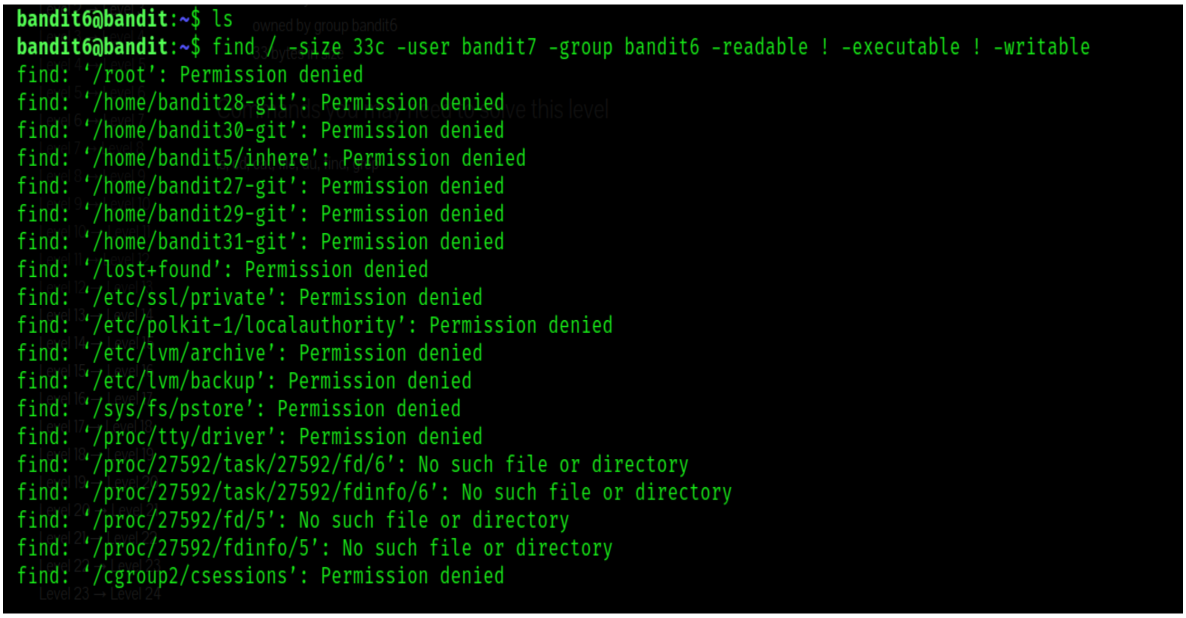
Port: 2220

Username: bandit6

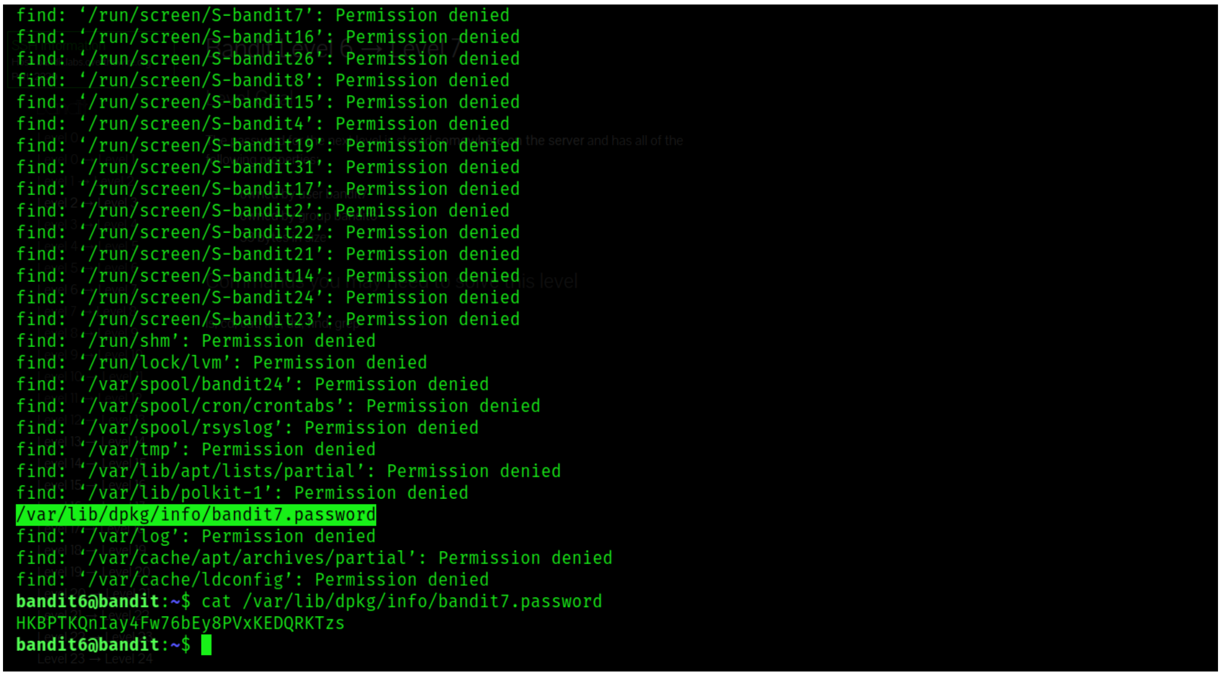
Password:
DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Using the given details, connect to the server via ssh

ssh bandit6@176.9.9.172 -p2220



```
bandit6@bandit:~$ ls
bandit6@bandit:~$ find / -size 33c -user bandit7 -group bandit6 -readable ! -executable ! -writable
find: '/root': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/home/bandit29-git': Permission denied
find: '/home/bandit31-git': Permission denied
find: '/lost+found': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/lvm/archive': Permission denied
find: '/etc/lvm/backup': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/27592/task/27592/fd/6': No such file or directory
find: '/proc/27592/task/27592/fdinfo/6': No such file or directory
find: '/proc/27592/fd/5': No such file or directory
find: '/proc/27592/fdinfo/5': No such file or directory
find: '/cgroup2/csessions': Permission denied
```



```
find: ‘/run/screen/S-bandit7’: Permission denied
find: ‘/run/screen/S-bandit16’: Permission denied
find: ‘/run/screen/S-bandit26’: Permission denied
find: ‘/run/screen/S-bandit8’: Permission denied
find: ‘/run/screen/S-bandit15’: Permission denied
find: ‘/run/screen/S-bandit4’: Permission denied
find: ‘/run/screen/S-bandit19’: Permission denied
find: ‘/run/screen/S-bandit31’: Permission denied
find: ‘/run/screen/S-bandit17’: Permission denied
find: ‘/run/screen/S-bandit2’: Permission denied
find: ‘/run/screen/S-bandit22’: Permission denied
find: ‘/run/screen/S-bandit21’: Permission denied
find: ‘/run/screen/S-bandit14’: Permission denied
find: ‘/run/screen/S-bandit24’: Permission denied
find: ‘/run/screen/S-bandit23’: 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:~$ 
```

Using the command find / -size 33c -user bandit7 -group bandit6 -readable ! -executable ! -writable, we found a bunch of files but among them there is only one file named “/var/lib/dpkg/info/bandit7.password” which we have permissions. Therefore, we got our password file.

Bandit Level 7

SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

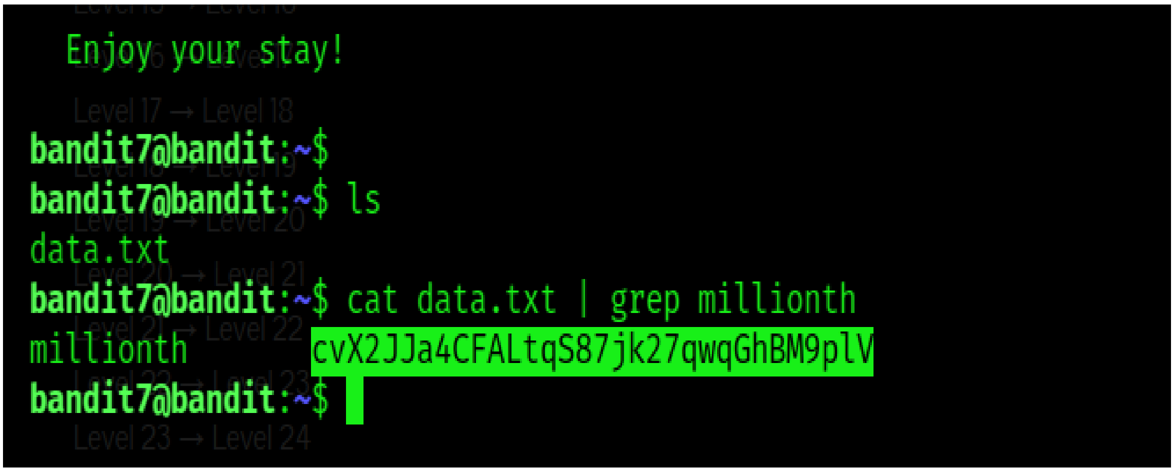
Port: 2220

Username: bandit7

Password:
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Using the given details, connect to the server via ssh

```
ssh bandit7@176.9.9.172 -p2220
```



```
  Enjoy your stay!

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

Using the command `cat data.txt | grep millionth` we can find the password which is located next to the word “millionth” inside the file data.txt

Bandit Level 8

SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

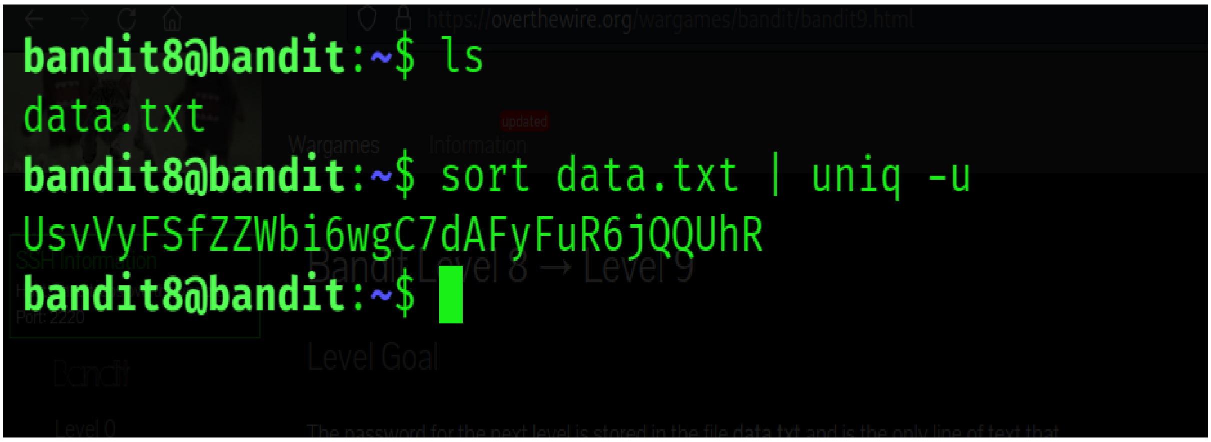
Port: 2220

Username: bandit8

Password:
cvX2JJa4CFALtqS87jk27qwqGhBM9plV

Using the given details, connect to the server via ssh

ssh bandit8@176.9.9.172 -p2220



```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ sort data.txt | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
bandit8@bandit:~$ 
```

Using the command sort data.txt | uniq -u, we found the unique line, i.e., password inside the file.

Bandit Level 9

SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

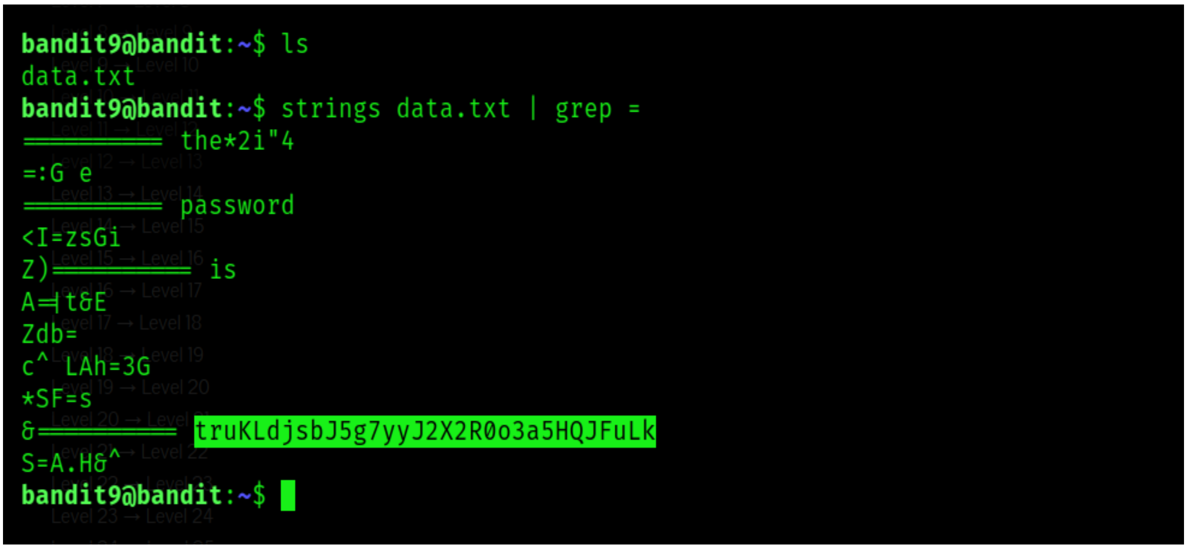
Port: 2220

Username: bandit9

Password: UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Using the given details, connect to the server via ssh

```
ssh bandit9@176.9.9.172 -p2220
```



```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt | grep =
========== the*2i"4
=:G e
========== password
<I=zsGi
Z)========== is
A=|t&E
Zdb=
c^ LAh=3G
*SF=s
&========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.H&^
bandit9@bandit:~$ 
```

Using strings command, we can print only the human readable part. So, we can use strings data.txt | grep = command to search the password.

Bandit Level 10

SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

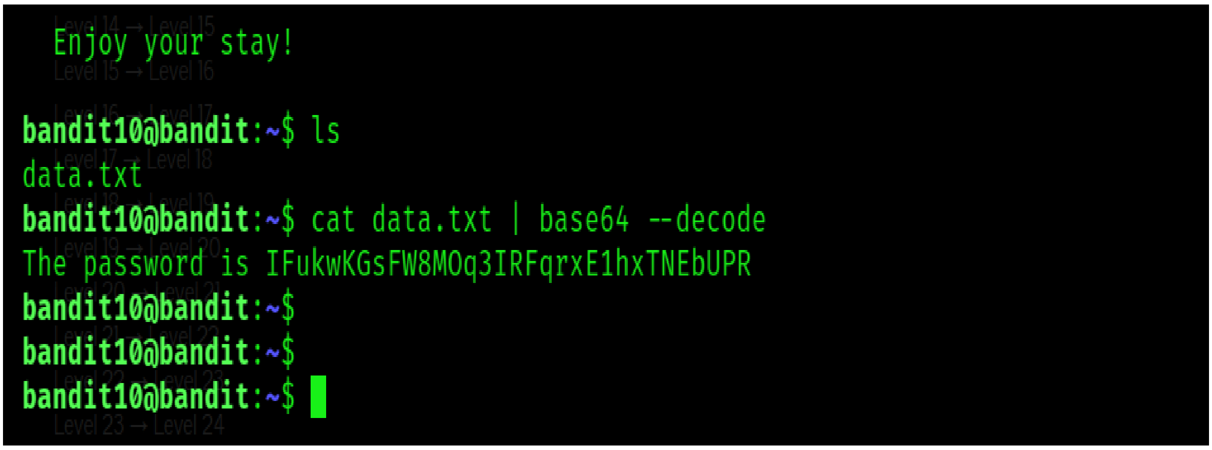
Port: 2220

Username: bandit10

Password:
truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Using the given details, connect to the server via ssh

ssh bandit10@176.9.9.172 -p2220



```
  Enjoy your stay!

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

Since the file “data.txt” is a base64 encrypted file, therefore to decode it we can use cat data.txt | base64 –decode.

Bandit Level 11

SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

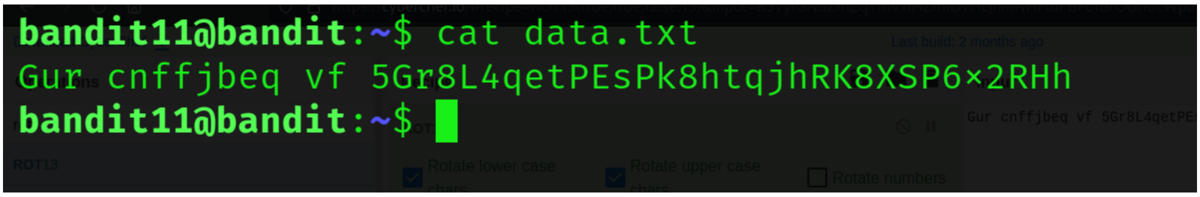
Port: 2220

Username: bandit11

Password: IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

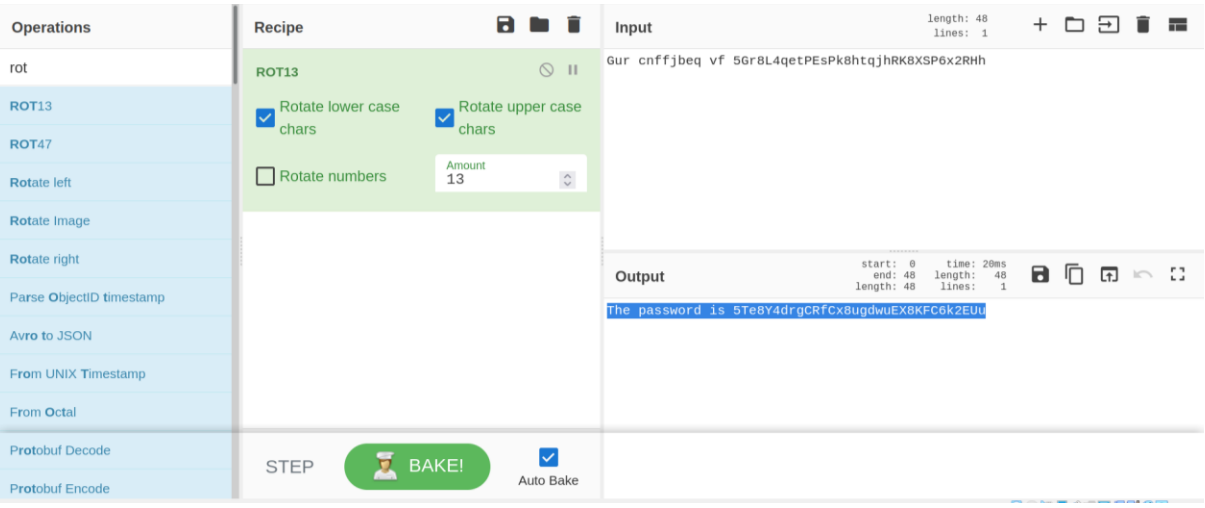
Using the given details, connect to the server via ssh

```
ssh bandit11@176.9.9.172 -p2220
```



```
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh
bandit11@bandit:~$ 
```

Here ”data.txt” is encrypted with rot13. So, we can use cyberchef.io to decrypt it.



ROT13

☑ Rotate lower case chars

☑ Rotate upper case chars

□ Rotate numbers

Amount: 13

Input

```
length: 48
 lines:  1
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh
```

Output

```
 start:  0    time: 20ms
   end: 48  length:   48
length: 48   lines:    1
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
```

Bandit Level 12

SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

Port: 2220

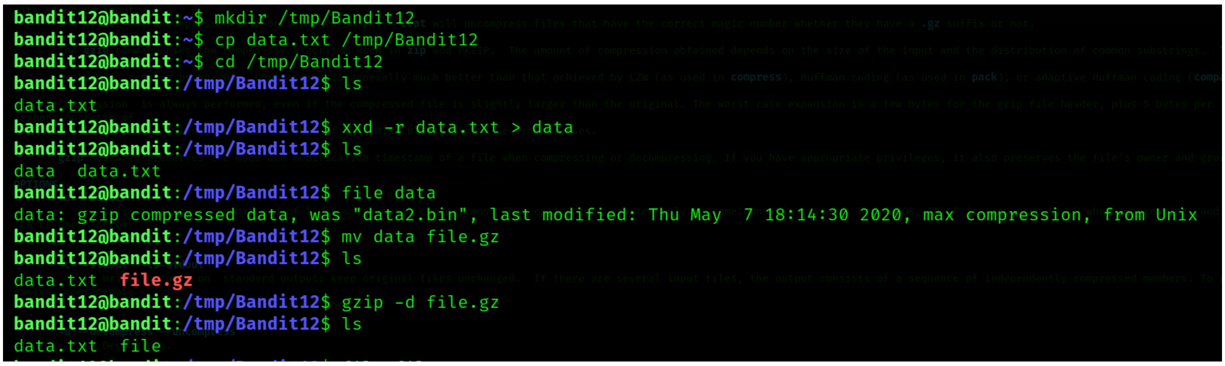
Username: bandit12

Password:
5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Using the given details, connect to the server via ssh

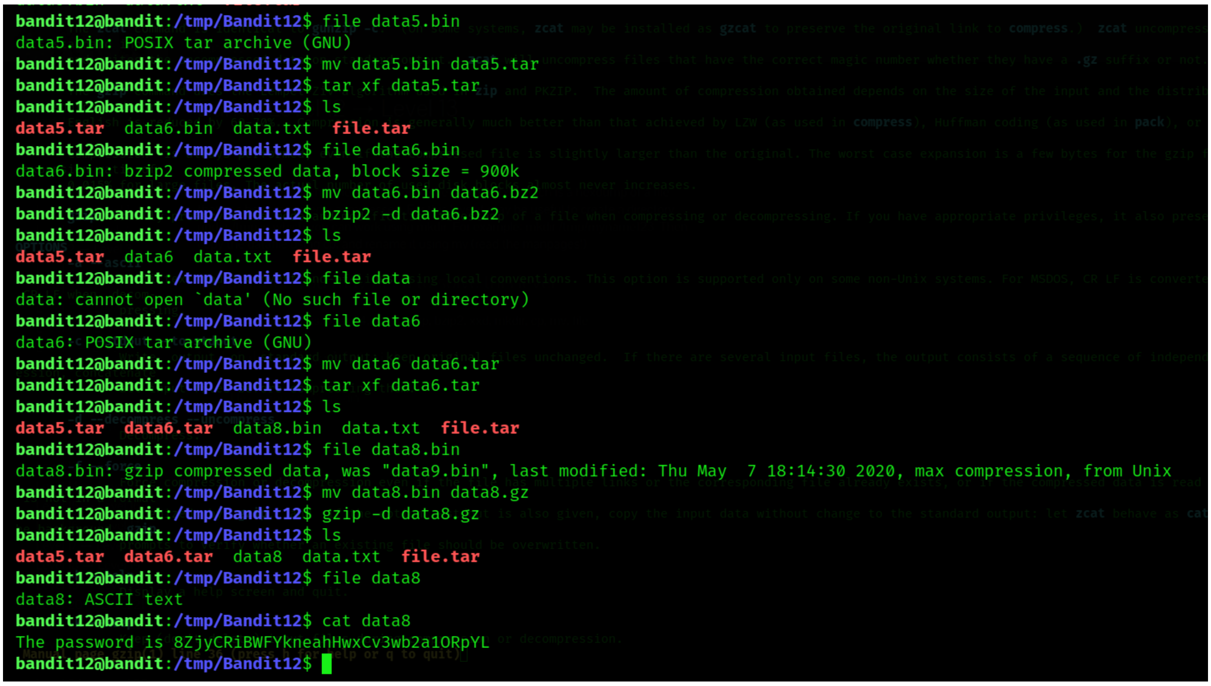
ssh bandit12@176.9.9.172 -p2220

As we have less permissions in home directory so we can create a new directory inside the /tmp directory for full access. Copy the “data.txt file” into the new dir. Reverse the hexdump file and copy it inside a new file. Now check the file type of the new file.



```
bandit12@bandit:~$ mkdir /tmp/Bandit12
bandit12@bandit:~$ cp data.txt /tmp/Bandit12
bandit12@bandit:~$ cd /tmp/Bandit12
bandit12@bandit:/tmp/Bandit12$ ls
data.txt
bandit12@bandit:/tmp/Bandit12$ xxd -r data.txt > data
bandit12@bandit:/tmp/Bandit12$ ls
data  data.txt
bandit12@bandit:/tmp/Bandit12$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/Bandit12$ mv data file.gz
bandit12@bandit:/tmp/Bandit12$ ls
data.txt  file.gz
bandit12@bandit:/tmp/Bandit12$ gzip -d file.gz
bandit12@bandit:/tmp/Bandit12$ ls
data.txt  file
```

Change the extension of the file accordingly and use gzip -d file_name.gz, bzip2 -d file_name.bz2, tar xf file_name.tar according to the compressed file type. After decompressing many times, we will get a human readable file called “data8” which contains the password.



```
bandit12@bandit:/tmp/Bandit12$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/Bandit12$ mv data5.bin data5.tar
bandit12@bandit:/tmp/Bandit12$ tar xf data5.tar
bandit12@bandit:/tmp/Bandit12$ ls
data5.tar  data6.bin  data.txt  file.tar
bandit12@bandit:/tmp/Bandit12$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/Bandit12$ mv data6.bin data6.bz2
bandit12@bandit:/tmp/Bandit12$ bzip2 -d data6.bz2
bandit12@bandit:/tmp/Bandit12$ ls
data5.tar  data6  data.txt  file.tar
bandit12@bandit:/tmp/Bandit12$ file data
data: cannot open `data' (No such file or directory)
bandit12@bandit:/tmp/Bandit12$ file data6
data6: POSIX tar archive (GNU)
bandit12@bandit:/tmp/Bandit12$ mv data6 data6.tar
bandit12@bandit:/tmp/Bandit12$ tar xf data6.tar
bandit12@bandit:/tmp/Bandit12$ ls
data5.tar  data6.tar  data8.bin  data.txt  file.tar
bandit12@bandit:/tmp/Bandit12$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/Bandit12$ mv data8.bin data8.gz
bandit12@bandit:/tmp/Bandit12$ gzip -d data8.gz
bandit12@bandit:/tmp/Bandit12$ ls
data5.tar  data6.tar  data8  data.txt  file.tar
bandit12@bandit:/tmp/Bandit12$ file data8
data8: ASCII text
bandit12@bandit:/tmp/Bandit12$ cat data8
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/Bandit12$
```

Bandit Level 13

SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

Port: 2220

Username: bandit13

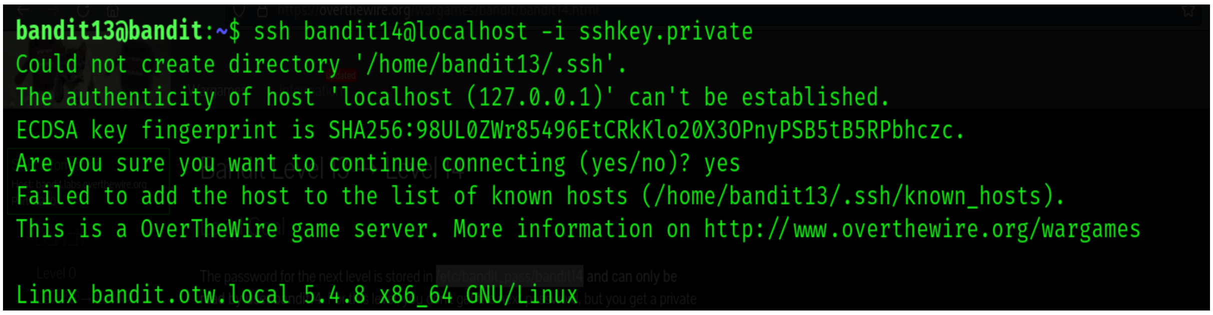
Password:
8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Using the given details, connect to the server via ssh

```
ssh bandit13@176.9.9.172 -p2220
```

After login to bandit13 we get a ssh private key for accessing bandit14.

Using the command `ssh bandit14@localhost -i sshkey.private`, we can login to bandit14 without any password.



```
bandit13@bandit:~$ ssh bandit14@localhost -i sshkey.private
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
```

Bandit Level 14

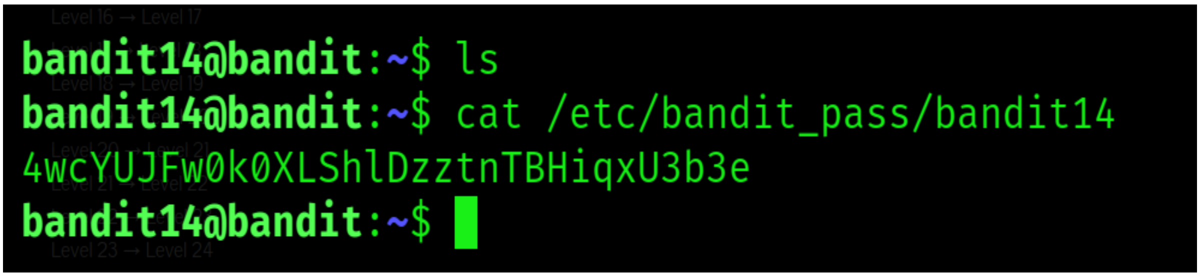
SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

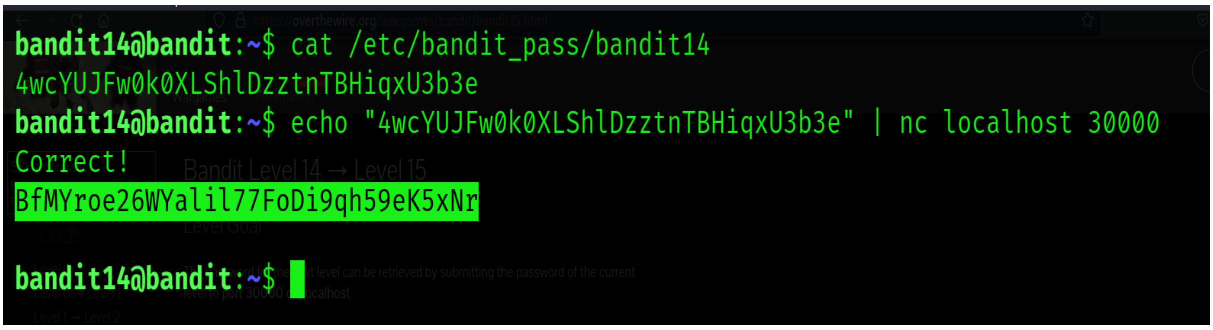
Port: 2220

Username: bandit14



```
bandit14@bandit:~$ ls
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$ 
```

Since the file name was given is the previous level, so we can directly print the content of the "/etc/bandit_pass/bandit14" file. Now copy the content and submit it to the localhost at port 30000.



```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$ echo "4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e" | nc localhost 30000
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr

bandit14@bandit:~$ 
```

After submitting, you will get the original password of the next level.

Bandit Level 15

SSH Information

Host URL: bandit.labs.overthewire.org

Host IP: 176.9.9.172

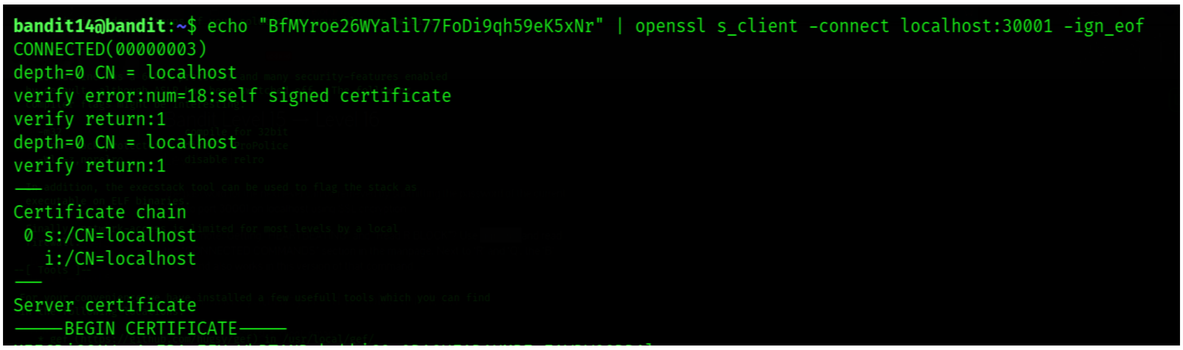
Port: 2220

Username: bandit15

Password: BfMYroe26WYalil77FoDi9qh59eK5xNr

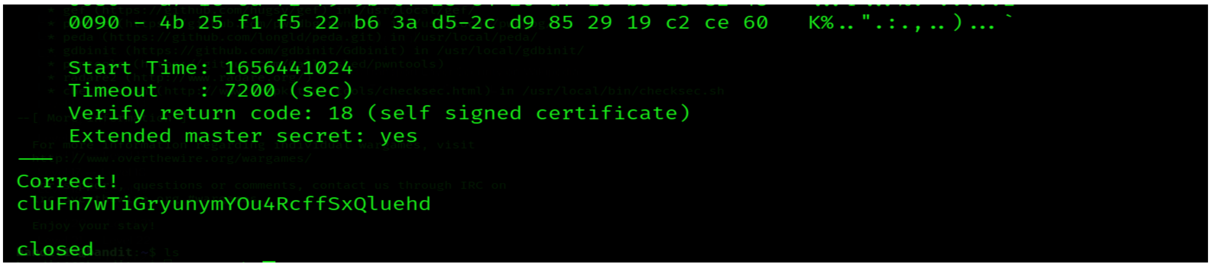
Using the given details, connect to the server via ssh

ssh bandit15@176.9.9.172 -p2220



```
bandit14@bandit:~$ echo "BfMYroe26WYalil77FoDi9qh59eK5xNr" | openssl s_client -connect localhost:30001 -ign_eof
CONNECTED(00000003)
depth=0 CN = localhost
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = localhost
verify return:1
---
Certificate chain
 0 s:/CN=localhost
   i:/CN=localhost
---
Server certificate
-----BEGIN CERTIFICATE-----
```

Using the command echo "BfMYroe26WYalil77FoDi9qh59eK5xNr" | openssl s_client -connect localhost:30001 -ign_eof, we will get our password for next level.



```
    0090 - 4b 25 f1 f5 22 b6 3a d5-2c d9 85 29 19 c2 ce 60   K%..".:.,..)...`

    Start Time: 1656441024
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
    Extended master secret: yes
---
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd

closed
```