


TASK-7

Name: M.Aravind

Roll No: CH.EN.U4CYS21006

LEVEL – 0 to 1

```
bandit0@bandit:~  
File Mousepad Simple Text Editor Help  
  
$ ssh -o StrictHostKeyChecking=no bandit0@bandit.labs.overthewire.org  
The authenticity of host 'bandit0.labs.overthewire.org ([176.9.9.172]:2220)' can't be established.  
(ECDSA key fingerprint is SHA256:9eUkQZw8S49HETCRklOzXK3OmYpSdts5B8Phnczc.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'bandit.labs.overthewire.org' (ECDSA) to the list of known hosts.  
This is a OverWire game server. More information on http://www.overthewire.org/wargames  
  
bandit0@bandit.labs.overthewire.org's password:  
Linux bandit0.tgw.local 5.4.8 x86_64 GNU/Linux  
  
www ver he ire.org
```



```
Welcome to OverWire!  
  
If you find any problems, please report them to Steven or morla on  
irc.overthewire.org.  
  
--[ Playing the games ]--  
  
This machine might hold several wargames.  
If you are playing "somegame", then:  
  
• USERNAMES are somegame0, somegame1, ...  
• Most LEVELS are stored in /somegame/.  
• PASSWORDS for each level are stored in /etc/somegame_pass/.  
  
Write-access to homedirectories is disabled. It is advised to create a  
working directory with a hard-to-guess name in /tmp/. You can use the  
command "mkdir -d" in order to generate a random and hard to guess  
directory in /tmp/. Read-access to both /tmp/ and /proc/ is disabled  
so that users can not snoop on eachother. Files and directories with  
easily guessable or short names will be periodically deleted!
```

```
Please play nice:  
  
• don't leave orphan processes running  
• don't leave exploit-files laying around  
• don't annoy other players  
• don't post passwords or spoilers
```

LEVEL – 1 to 2

Username: bandit1

Password: boJ9jbbUNNfktD7800psqOl tutMc3MY1

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd7800psq0ltutMc3MY1
bandit0@bandit:~$
```

LEVEL – 2 to 3

Username: bandit2

Password: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

```
bandit1@bandit:~$ ls
_
bandit1@bandit:~$ cat < -
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$
```

LEVEL – 3 to 4

Username: bandit3

Password: UmHadQclWmgdLOKQ3YNggjWxGoRmb5luK

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat 'spaces in this filename'
UmHadQclWmgdLOKQ3YNggjWxGoRmb5luK
bandit2@bandit:~$
```

LEVEL – 4 to 5

Username: bandit4

Password: pIwrPrtPN36QITSp3EQaw936yaFoFgAB

```
bandit3@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  inhere  .profile
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$
```

LEVEL – 5 to 6

Username: bandit5

Password: koReBOKuIDDepwhWk7jZC0RTdopnAYKh

```
bandit4@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  inhere  .profile
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -a
.  -file00  -file02  -file04  -file06  -file08
.. -file01  -file03  -file05  -file07  -file09
bandit4@bandit:~/inhere$ file ./-file*
./-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$
```

LEVEL – 6 to 7

Username: bandit6

Password: DXjZPULLxYr17uwoI01bNLQbtFemEgo7

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybeh ere00 maybeh ere02 maybeh ere04 maybeh ere06 maybeh ere08 maybeh ere10 maybeh ere12 maybeh ere14 maybeh ere16 maybeh ere18
maybeh ere01 maybeh ere03 maybeh ere05 maybeh ere07 maybeh ere09 maybeh ere11 maybeh ere13 maybeh ere15 maybeh ere17 maybeh ere19
bandit5@bandit:~/inhere$ find -readable -size 1033c
./maybeh ere07/.file2
bandit5@bandit:~/inhere$ cat ./maybeh ere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

LEVEL – 7 to 8

Username: bandit7

Password: HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$
```

LEVEL – 8 to 9

Username: bandit8

Password: cvX2JJJa4CFALtqS87jk27qwqGhBM9plV

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ grep millionth data.txt
millionth cvX2JJJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$
```

LEVEL – 9 to 10

Username: bandit9

Password: UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhr

```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ sort data.txt | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhr
bandit8@bandit:~$
```

LEVEL – 10 to 11

Username: bandit10

Password: truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt | grep =====
===== the*2i"4
===== password
Z)===== is
5===== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
bandit9@bandit:~$
```

LEVEL – 11 to 12

Username: bandit11

Password: IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

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

LEVEL – 12 to 13

Username: bandit12

Password: 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
bandit11@bandit:~$
```

LEVEL – 13 to 14

Username: bandit13

Password: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

```
bandit12@bandit:~$ mkdir /tmp/beastAM
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ cp data.txt /tmp/beastAM
bandit12@bandit:~$ cd /tmp/beastAM
bandit12@bandit:/tmp/beastAM$ ls
data.txt
bandit12@bandit:/tmp/beastAM$ mv data.txt AMD.txt
bandit12@bandit:/tmp/beastAM$ xxd -r AMD.txt > AM.txt
bandit12@bandit:/tmp/beastAM$ file AM.txt
AM.txt: gzip compressed data, was "data2.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/beastAM$ mv AM.txt AM.gz
bandit12@bandit:/tmp/beastAM$ gunzip AM.gz
bandit12@bandit:/tmp/beastAM$ ls
AM  AMD.txt
bandit12@bandit:/tmp/beastAM$ file AM
AM: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/beastAM$ bzip2 -d AM
bzip2: Can't guess original name for AM -- using AM.out
bandit12@bandit:/tmp/beastAM$ file AM.out
AM.out: gzip compressed data, was "data4.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/beastAM$ mv AM.out AM.gz
bandit12@bandit:/tmp/beastAM$ gunzip AM.gz
bandit12@bandit:/tmp/beastAM$ ls
AM  AMD.txt
bandit12@bandit:/tmp/beastAM$ file AM
AM: POSIX tar archive (GNU)
bandit12@bandit:/tmp/beastAM$ tar xvf AM
data5.bin
bandit12@bandit:/tmp/beastAM$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/beastAM$ tar xvf data5.bin
data6.bin
bandit12@bandit:/tmp/beastAM$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/beastAM$ bzip2 -d data6.bin
bzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/beastAM$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/beastAM$ tar xvf data6.bin.out
data8.bin
bandit12@bandit:/tmp/beastAM$ file data8.bin
data8.bin: cannot open `data8.bin' (No such file or directory)
bandit12@bandit:/tmp/beastAM$ file data8
data8: ASCII text
bandit12@bandit:/tmp/beastAM$ cat data8
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
```

```
bandit12@bandit:/tmp/beastAM$ file data8
data8: ASCII text
bandit12@bandit:/tmp/beastAM$ mv data8 data8.gz
bandit12@bandit:/tmp/beastAM$ sunzip data8.gz
-bash: sunzip: command not found
bandit12@bandit:/tmp/beastAM$ gunzip data8.gz
bandit12@bandit:/tmp/beastAM$ ls
AM  AMD.txt  data5.bin  data6.bin.out  data8
bandit12@bandit:/tmp/beastAM$ file data8
data8: ASCII text
bandit12@bandit:/tmp/beastAM$ cat data8
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
```

LEVEL – 14 to 15

Username: bandit14

Password: Private key in bandit13

Username: bandit15

Password: BfMYroe26WYalil77FoDi9qh59eK5xNr

```
bandit13@bandit:~$ clear
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ file sshkey.private
sshkey.private: PEM RSA private key
bandit13@bandit:~$ head sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxkkOE83W2cOT7IWfFc9aPaaQmQDgzuxCv+ppZHa++buSkN+
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AioYp0MZYETq46t+jk9puNwZwIt9XgB
ZufGtZEwWbFWw/vVLNwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb
ThMsiMnyJafEwJ/T8PQO3myS91vUHEuo0MAzoUID4kN0MEZ3+XahyK0HJVq68KsV
ObefXG1vvA3GAJ29kxJaqrFgYnqZryWN7w3CHjNU4c/2Jkp+n8L0SnxANA+WYA7
jiPyTF0is8uzMLYQ4l1Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dWBjhyE0zjeA
J3j/RWmap9M5zfJ/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfyoAQSS+bBw3RXvzE
pvJt3SmU8hIDuLsCjL1VnBY5pY7Bju8g8aR/3FyjjNAqx/TLfzLLYfOu7i9Jet67
xAh0tONG/u8FB5I3LAI2Vp60viwvdWeC4nOxCthldpuPKNLA8rmMMVRTKQ+7T2VS
bandit13@bandit:~$ chmod 600 sshkey.private
chmod: changing permissions of 'sshkey.private': Operation not permitted
bandit13@bandit:~$ ssh bandit14@localhost -i sshkey.private
```

```
bandit14@bandit:~$ echo "4wcYUJFw0k0XLShLDzztnTBHiqxU3b3e" | nc localhost 30000
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
```

LEVEL – 15 to 16

Username: bandit16

Password: cluFn7wTiGryunymYOu4RcfftSxQluehd

```
bandit15@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
---
```

```
Start Time: 1646413843
Timeout    : 7200 (sec)
Verify return code: 18 (self signed certificate)
Extended master secret: yes
---
Correct!
cluFn7wTiGryunymYOu4RcfftSxQluehd
closed
```