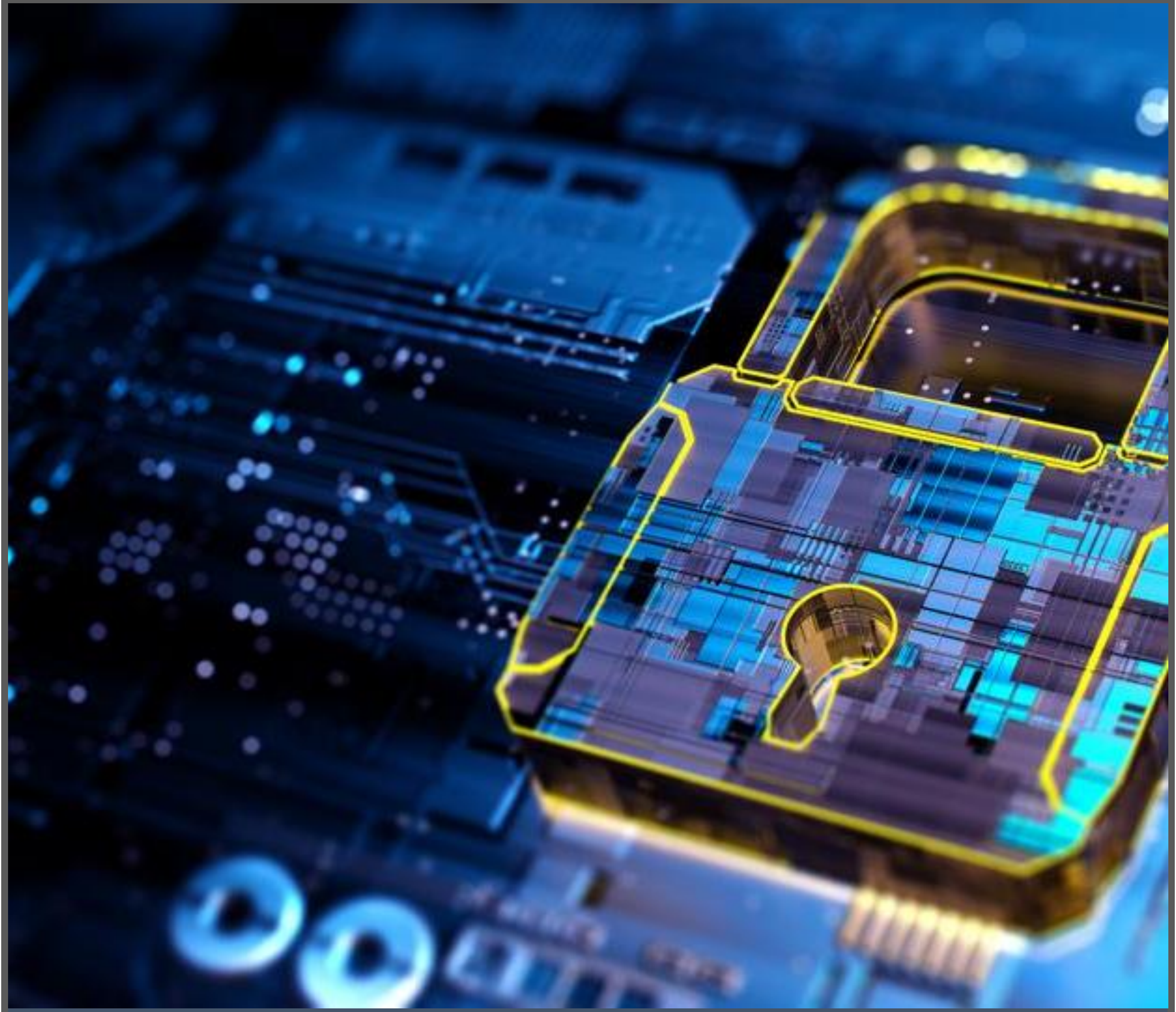


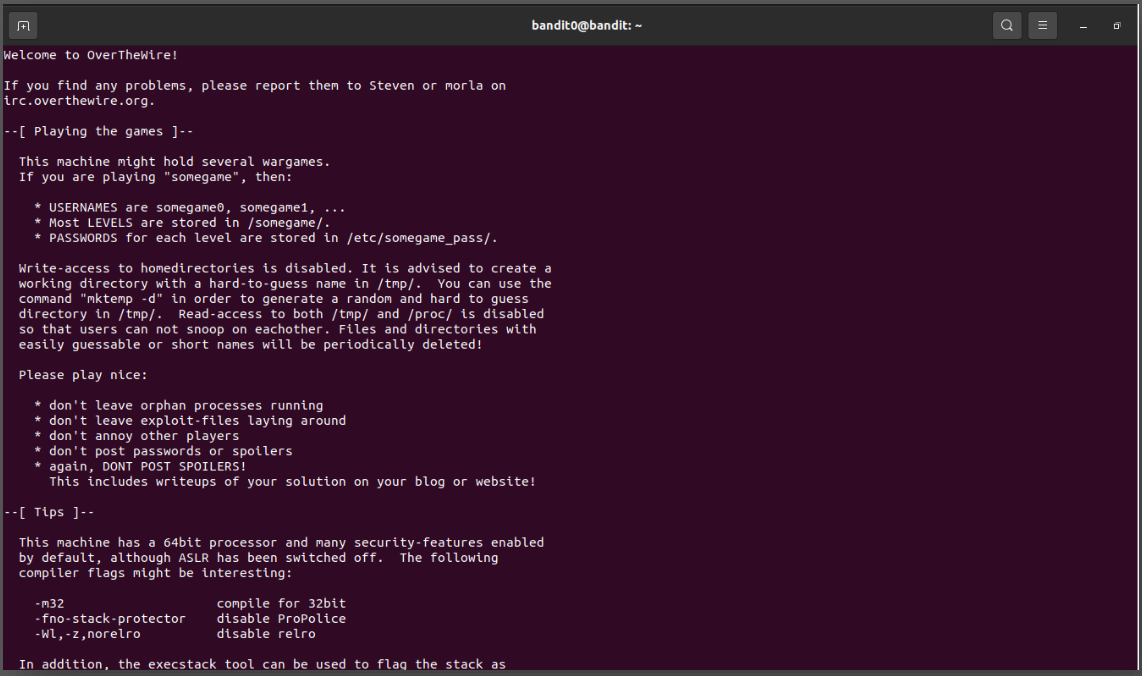
# TASK 7

## THE COGNIZANCE

OverTheWire 15 Levels Aparna S

## LEVEL 0

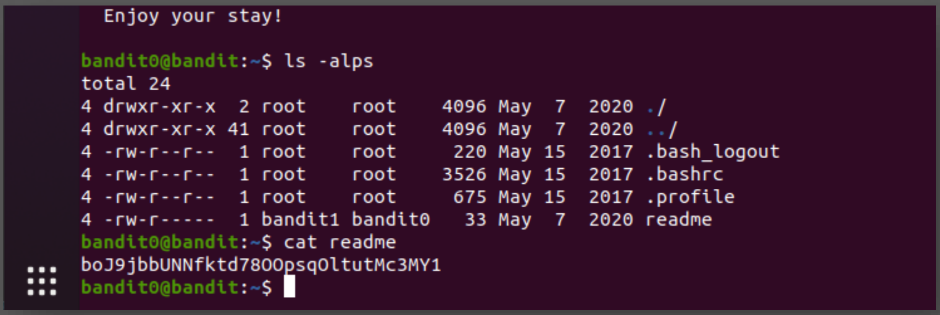
Password: bandit0



```
Welcome to OverTheWire!

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 "mktemp -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
    * again, DONT POST SPOILERS!
      This includes writeups of your solution on your blog or website!

--[ Tips ]--

  This machine has a 64bit processor and many security-features enabled
  by default, although ASLR has been switched off.  The following
  compiler flags might be interesting:

    -m32                    compile for 32bit
    -fno-stack-protector    disable ProPolice
    -Wl,-z,norelro          disable relro

  In addition, the execstack tool can be used to flag the stack as
```

## LEVEL 0-1

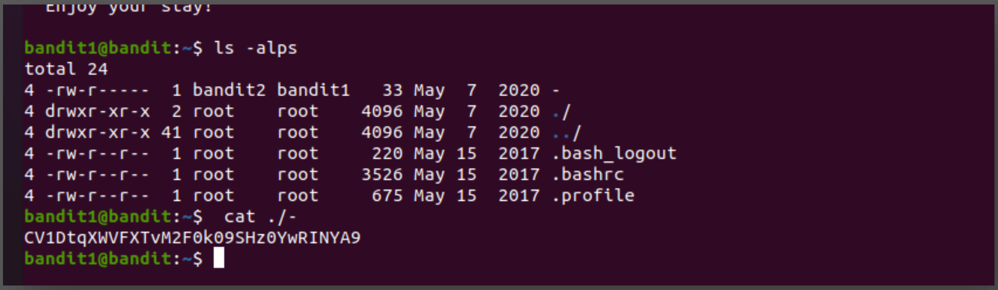
Password: boJ9jbbUNNfktd78OOpsqOltutMc3MY1



```
  Enjoy your stay!

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

## LEVEL 1-2

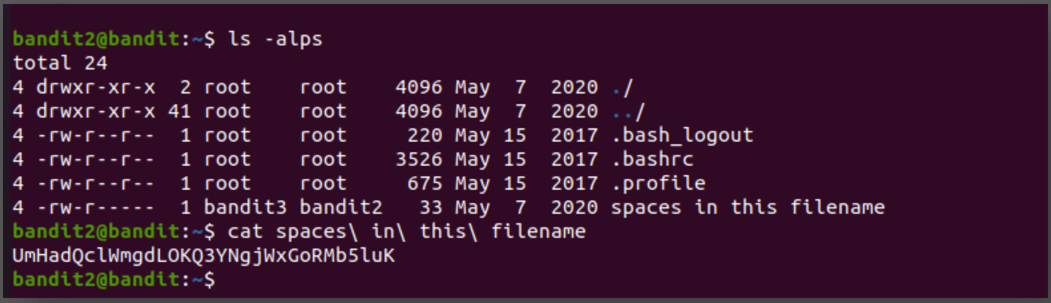
Password: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9



```
  Enjoy your stay!

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

LEVEL 2-3

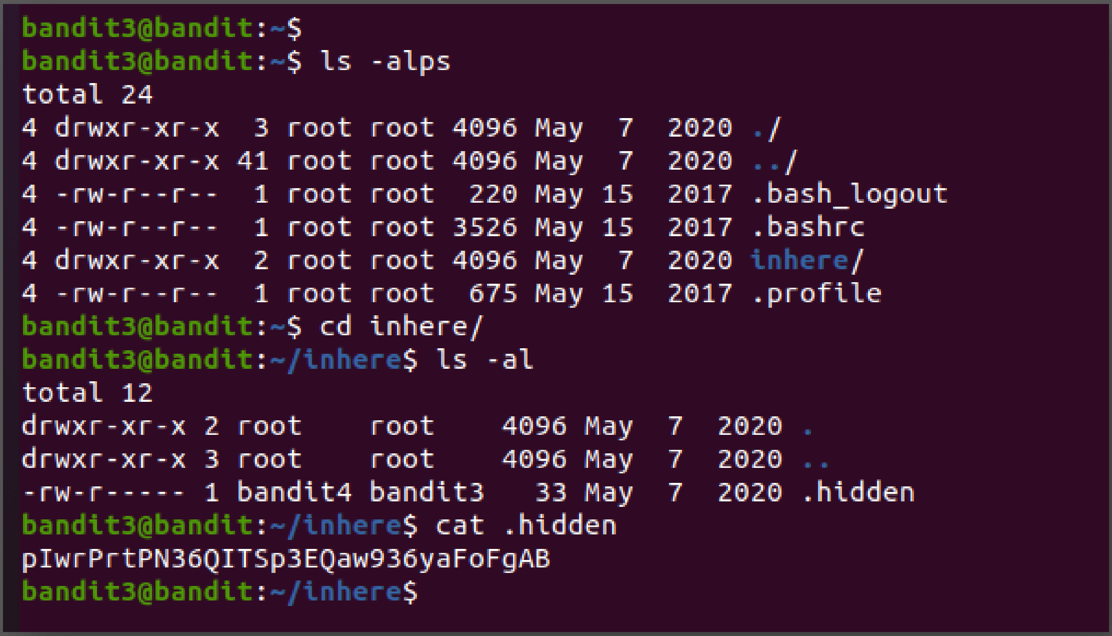
Password: UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK



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

LEVEL 3-4

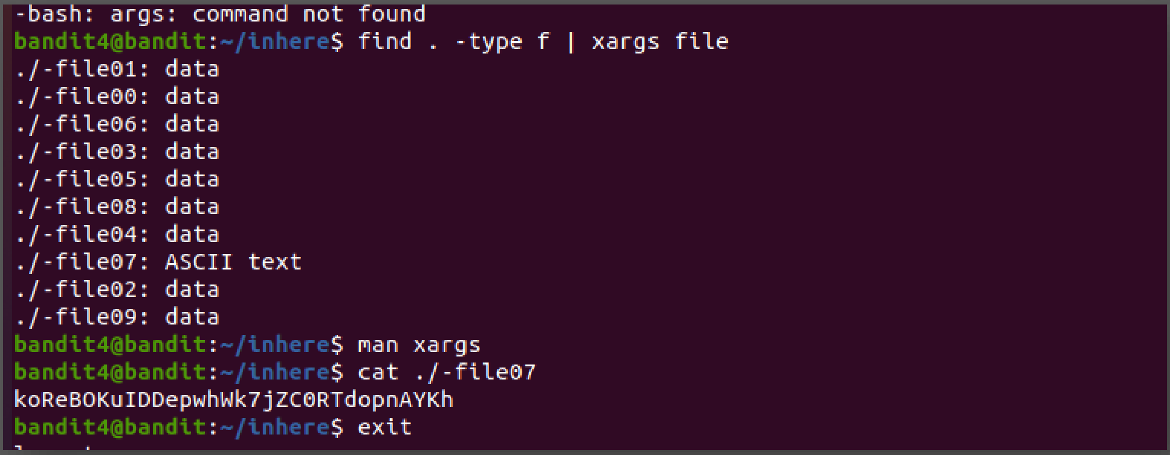
Password: pIwrPrtPN36QITSp3EQaw936yaFoFgAB



```
bandit3@bandit:~$
bandit3@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root root 4096 May  7  2020 ./
4 drwxr-xr-x 41 root root 4096 May  7  2020 ../
4 -rw-r--r--  1 root root  220 May 15  2017 .bash_logout
4 -rw-r--r--  1 root root 3526 May 15  2017 .bashrc
4 drwxr-xr-x  2 root root 4096 May  7  2020 inhere/
4 -rw-r--r--  1 root root  675 May 15  2017 .profile
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root    root    4096 May  7  2020 .
drwxr-xr-x 3 root    root    4096 May  7  2020 ..
-rw-r----- 1 bandit4 bandit3   33 May  7  2020 .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$
```

LEVEL 4-5

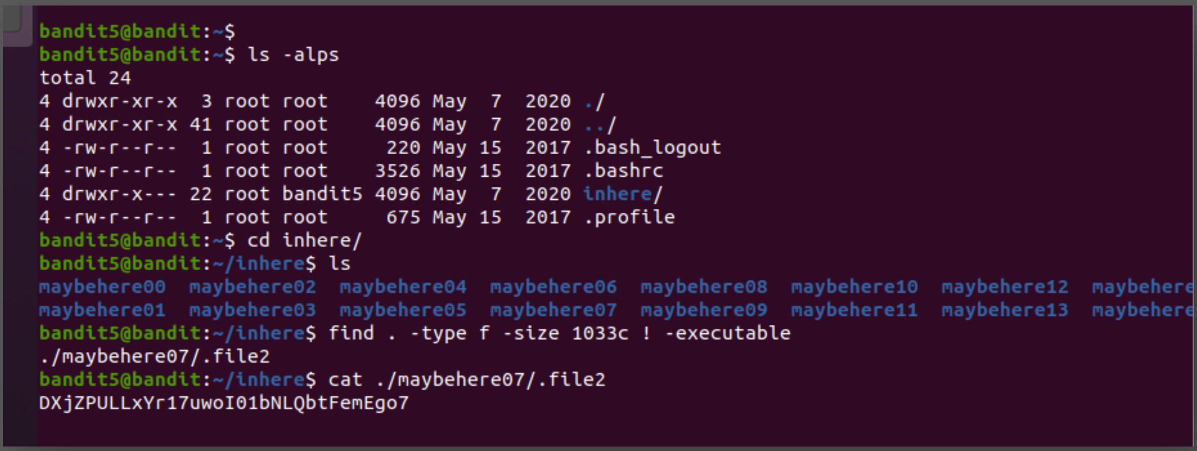
Password: koReBOKuIDDepwhWk7jZC0RTdopnAYKh



```
-bash: args: command not found
bandit4@bandit:~/inhere$ find . -type f | xargs file
./-file01: data
./-file00: data
./-file06: data
./-file03: data
./-file05: data
./-file08: data
./-file04: data
./-file07: ASCII text
./-file02: data
./-file09: data
bandit4@bandit:~/inhere$ man xargs
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$ exit
```

LEVEL 5-6

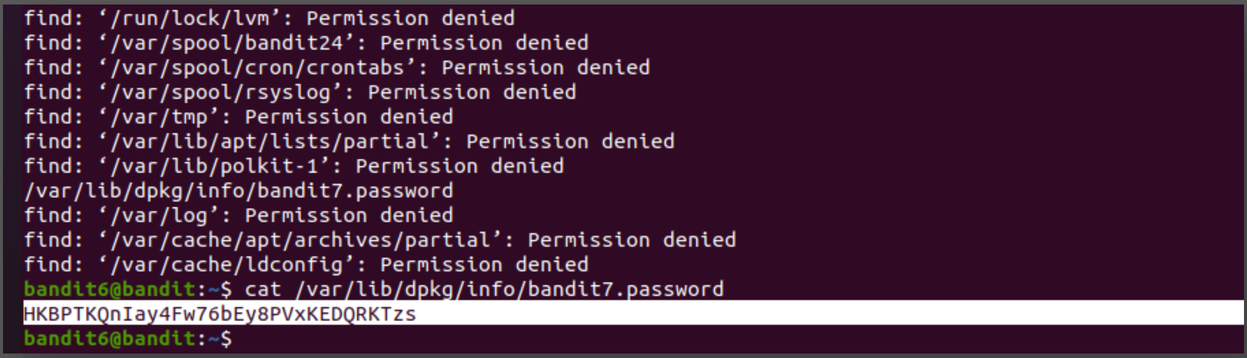
Password: DXjZPULLxYr17uwoI01bNLQbtFemEgo7



```
bandit5@bandit:~$
bandit5@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root root    4096 May  7  2020 ./
4 drwxr-xr-x 41 root root    4096 May  7  2020 ../
4 -rw-r--r--  1 root root     220 May 15  2017 .bash_logout
4 -rw-r--r--  1 root root    3526 May 15  2017 .bashrc
4 drwxr-x--- 22 root bandit5 4096 May  7  2020 inhere/
4 -rw-r--r--  1 root root     675 May 15  2017 .profile
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere02  maybehere04  maybehere06  maybehere08  maybehere10  maybehere12  maybehere
maybehere01  maybehere03  maybehere05  maybehere07  maybehere09  maybehere11  maybehere13  maybehere
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

LEVEL 6-7

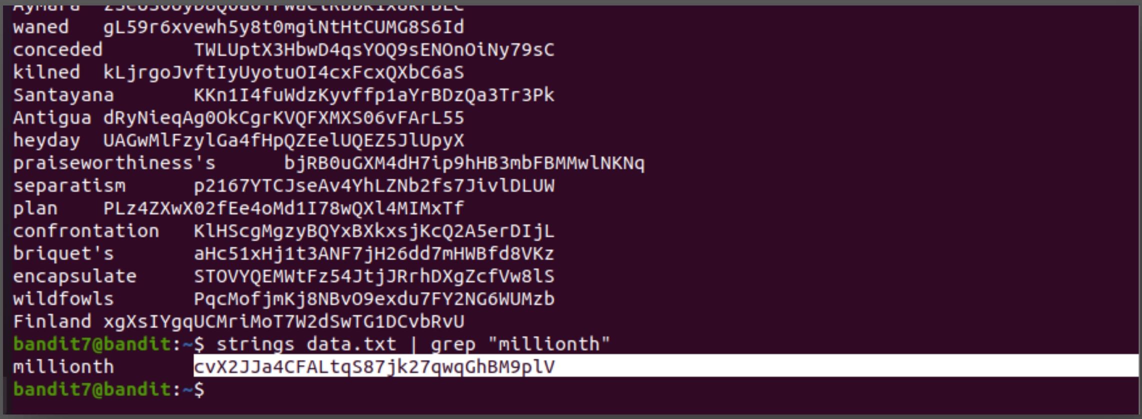
Password: HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs



```
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:~$
```

## LEVEL 7-8

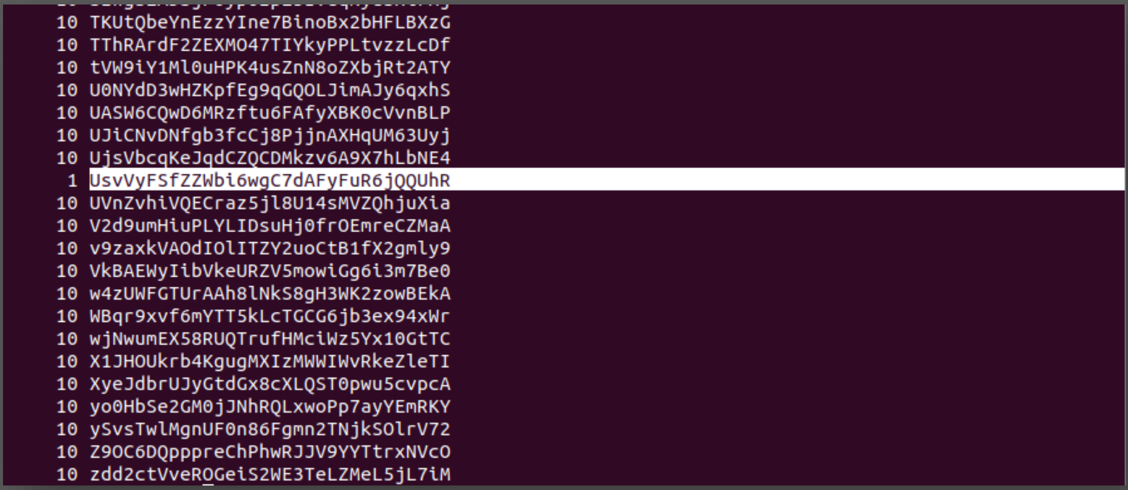
Password: cvX2JJa4CFALtqS87jk27qwqGhBM9plV



```
waned   gL59r6xvewh5y8t0mgiNtHtCUMG8S6Id
conceded        TWLUptX3HbwD4qsYOQ9sENOnOiNy79sC
kilned  kLjrgoJvftIyUyotuOI4cxFcxQXbC6aS
Santayana       KKn1I4fuWdzKyvffp1aYrBDzQa3Tr3Pk
Antigua dRyNieqAg0OkCgrKVQFXMXS06vFArL55
heyday  UAGwMlFzylGa4fHpQZEelUQEZ5JlUpyX
praiseworthiness's      bjRB0uGXM4dH7ip9hHB3mbFBMMwlNKNq
separatism      p2167YTCJseAv4YhLZNb2fs7JivlDLUW
plan    PLz4ZXwX02fEe4oMd1I78wQXl4MIMxTf
confrontation   KlHScgMgzyBQYxBXkxsjKcQ2A5erDIjL
briquet's       aHc51xHj1t3ANF7jH26dd7mHWBfd8VKz
encapsulate     STOVYQEMWtFz54JtjJRrhDXgZcfVw8lS
wildfowls       PqcMofjmKj8NBvO9exdu7FY2NG6WUMzb
Finland xgXsIYgqUCMriMoT7W2dSwTG1DCvbRvU
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth       cvX2JJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$
```

## LEVEL 8-9

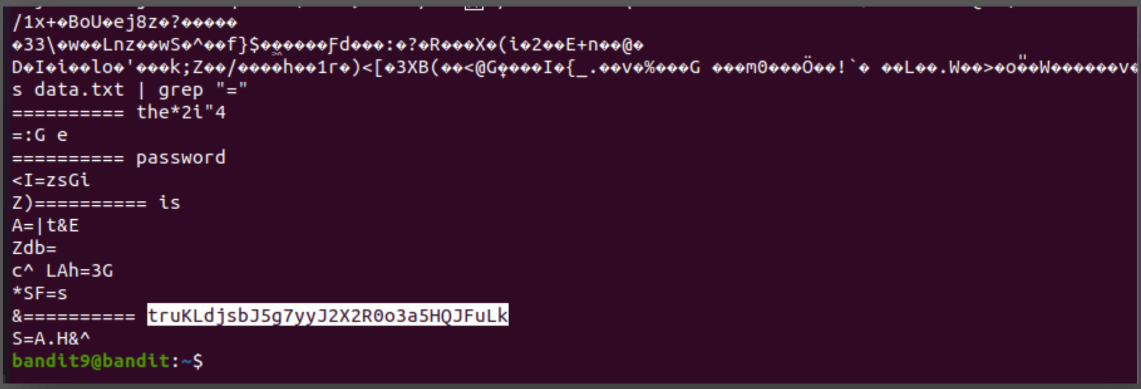
Password: UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR



```
     10 TKUtQbeYnEzzYIne7BinoBx2bHFLBXzG
     10 TThRArdF2ZEXMO47TIYkyPPLtvzzLcDf
     10 tVW9iY1Ml0uHPK4usZnN8oZXbjRt2ATY
     10 U0NYdD3wHZKpfEg9qGQOLJimAJy6qxhS
     10 UASW6CQwD6MRzftu6FAfyXBK0cVvnBLP
     10 UJiCNvDNfgb3fcCj8PjjnAXHqUM63Uyj
     10 UjsVbcqKeJqdCZQCDMkzv6A9X7hLbNE4
      1 UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
     10 UVnZvhiVQECraz5jl8U14sMVZQhjuXia
     10 V2d9umHiuPLYLIDsuHj0frOEmreCZMaA
     10 v9zaxkVAOdIOlITZY2uoCtB1fX2gmly9
     10 VkBAEWyIibVkeURZV5mowiGg6i3m7Be0
     10 w4zUWFGTUrAAh8lNkS8gH3WK2zowBEkA
     10 WBqr9xvf6mYTT5kLcTGCG6jb3ex94xWr
     10 wjNwumEX58RUQTrufHMciWz5Yx10GtTC
     10 X1JHOUkrb4KgugMXIzMWWIWvRkeZleTI
     10 XyeJdbrUJyGtdGx8cXLQST0pwu5cvpcA
     10 yo0HbSe2GM0jJNhRQLxwoPp7ayYEmRKY
     10 ySvsTwlMgnUF0n86Fgmn2TNjkSOlrV72
     10 Z9OC6DQpppreChPhwRJJV9YYTtrxNVcO
     10 zdd2ctVveROGeiS2WE3TeLZMeL5jL7iM
```

## LEVEL 9-10

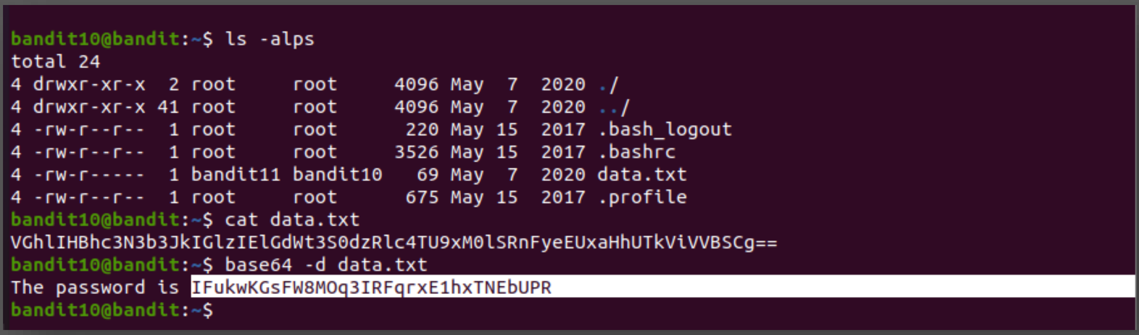
Password: truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk



```
/1x+�BoU�ej8z�?�����
�33\�w��Lnz��wS�^��f}$������Fd���:�?�R���X�(i�2��E+n��@�
D�I�i��lo�'���k;Z��/����h��1r�)<[�3XB(��<@G����I�{_.��v�%���G ���m0����Ö��!`� ��L��.W��>�oö�W�������v�
s data.txt | grep "="
========== the*2i"4
=:G e
========== password
<I=zsGi
Z)========== is
A=|t&E
Zdb=
c^ LAh=3G
*SF=s
&========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.H&^
bandit9@bandit:~$
```

## LEVEL 10-11

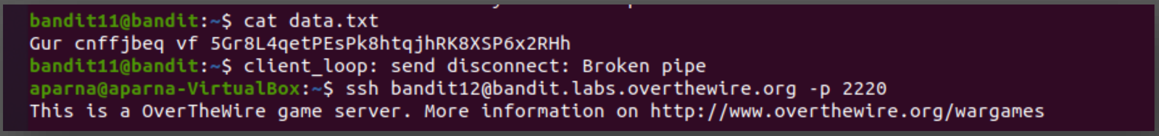
Password: IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR



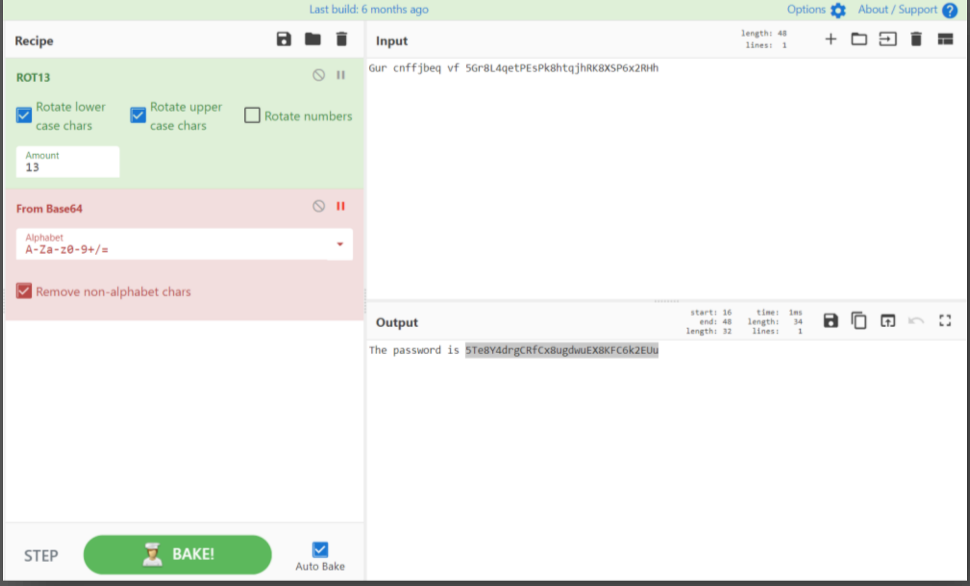
```
bandit10@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  2 root     root     4096 May  7  2020 ./
4 drwxr-xr-x 41 root     root     4096 May  7  2020 ../
4 -rw-r--r--  1 root     root      220 May 15  2017 .bash_logout
4 -rw-r--r--  1 root     root     3526 May 15  2017 .bashrc
4 -rw-r-----  1 bandit11 bandit10   69 May  7  2020 data.txt
4 -rw-r--r--  1 root     root      675 May 15  2017 .profile
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$
```

## LEVEL 11-12

Password: 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu



```
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh
bandit11@bandit:~$ client_loop: send disconnect: Broken pipe
aparna@aparna-VirtualBox:~$ ssh bandit12@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
```



ROT13

☑ Rotate lower case chars ☑ Rotate upper case chars □ Rotate numbers

Amount
13

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

Input length: 48 lines: 1

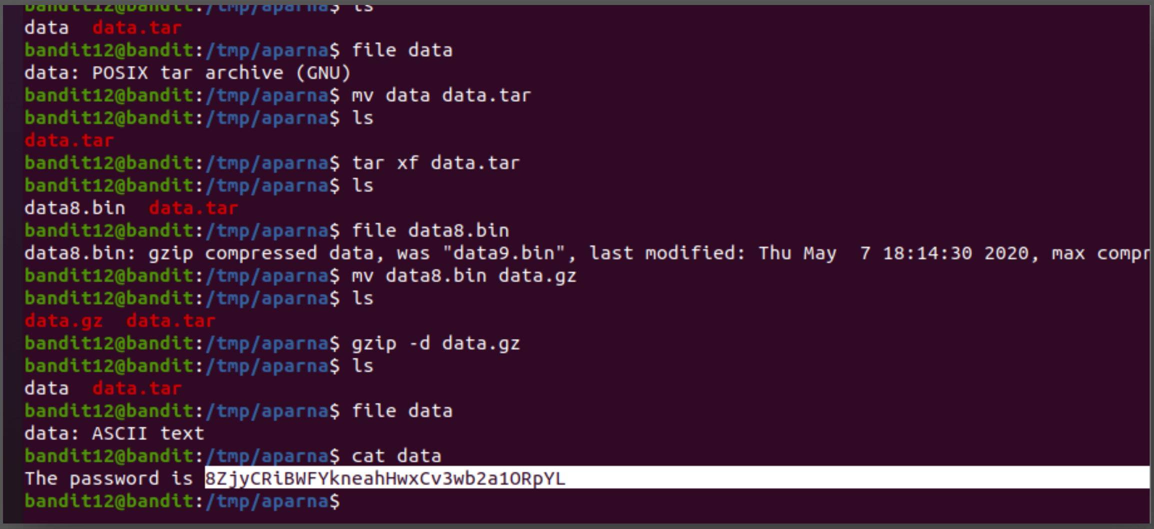
```
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh
```

Output start: 16 end: 48 length: 32 time: 1ms length: 34 lines: 1

```
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
```

LEVEL 12-13

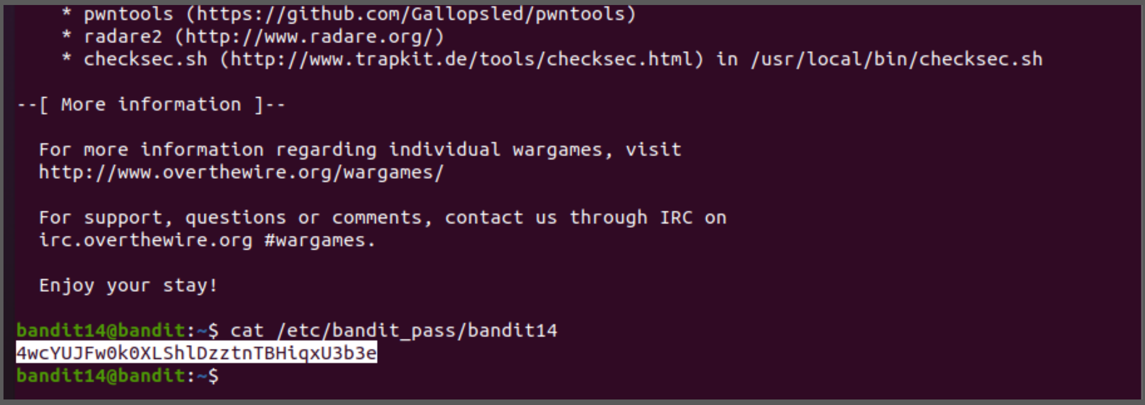
Password: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL



```
bandit12@bandit:/tmp/aparna$ ls
data  data.tar
bandit12@bandit:/tmp/aparna$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/aparna$ mv data data.tar
bandit12@bandit:/tmp/aparna$ ls
data.tar
bandit12@bandit:/tmp/aparna$ tar xf data.tar
bandit12@bandit:/tmp/aparna$ ls
data8.bin  data.tar
bandit12@bandit:/tmp/aparna$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu May  7 18:14:30 2020, max compr
bandit12@bandit:/tmp/aparna$ mv data8.bin data.gz
bandit12@bandit:/tmp/aparna$ ls
data.gz  data.tar
bandit12@bandit:/tmp/aparna$ gzip -d data.gz
bandit12@bandit:/tmp/aparna$ ls
data  data.tar
bandit12@bandit:/tmp/aparna$ file data
data: ASCII text
bandit12@bandit:/tmp/aparna$ cat data
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/aparna$
```

LEVEL 13-14

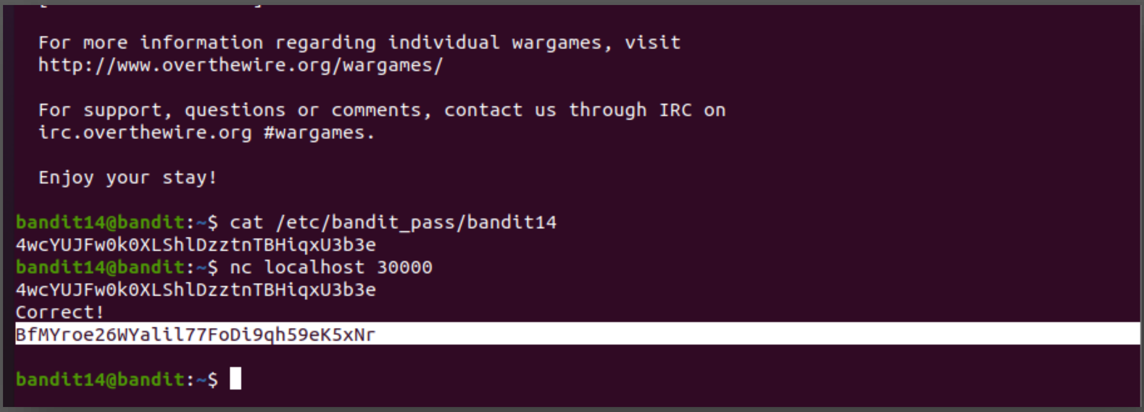
Password: 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e



```
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[ More information ]--

  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!

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

LEVEL 14-15

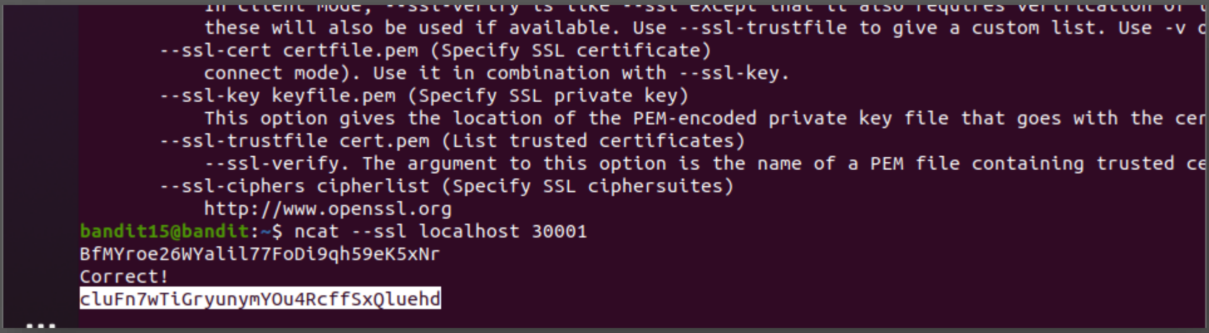
Password: BfMYroe26WYalil77FoDi9qh59eK5xNr



```
  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!

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

bandit14@bandit:~$
```

LEVEL 15-16

Password: cluFn7wTiGryunymYOu4RcffSxQluehd



```
           In client mode, --ssl-verify is like --ssl except that it also requires verification of t
           these will also be used if available. Use --ssl-trustfile to give a custom list. Use -v c
       --ssl-cert certfile.pem (Specify SSL certificate)
           connect mode). Use it in combination with --ssl-key.
       --ssl-key keyfile.pem (Specify SSL private key)
           This option gives the location of the PEM-encoded private key file that goes with the cer
       --ssl-trustfile cert.pem (List trusted certificates)
           --ssl-verify. The argument to this option is the name of a PEM file containing trusted ce
       --ssl-ciphers cipherlist (Specify SSL ciphersuites)
           http://www.openssl.org
bandit15@bandit:~$ ncat --ssl localhost 30001
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd
```