

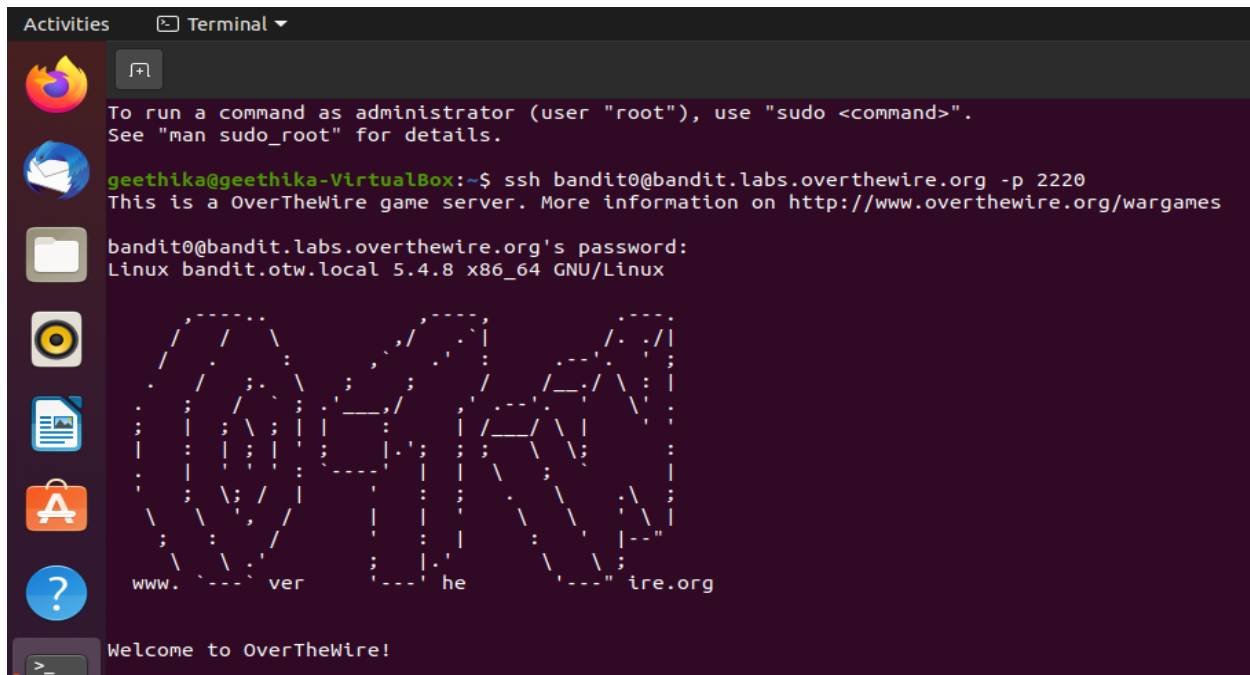
TASK-7

OVERTHEWIRE-BANDIT WAR GAME

Name:-Geethika

Section:-CSE AIE A

Level 0



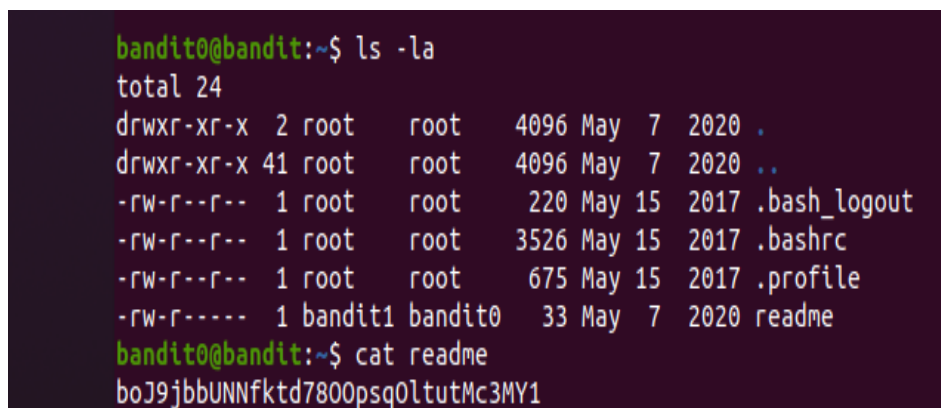
```
Activities Terminal
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
geethika@geethika-VirtualBox:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit0@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

www. ver he ire.org

Welcome to OverTheWire!
```

Password:- bandit0

Level 0→1:-



```
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
boJ9jbbUNNfktd780OpsqOltutMc3MY1
```

Password → boJ9jbbUNNfktd780OpsqOltutMc3MY1

Level 1→2

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

Password:- CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

Level 2→3

```
= bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat 'spaces in this filename'
UmHadQclWmgdLOKQ3YNgjWxGoRMB5luK
```

Password:- UmHadQclWmgdLOKQ3YNgjWxGoRMB5luK

Level 3→4

```
? bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
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
```

Password:- plwrPrtPN36QITSp3EQaw936yaFoFgAB

Level 4→5

```
bandit4@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
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ 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
koReB0KuIDDepwhWk7jZC0RTdopnAYKh
```

Password:- koReBOKuIDDepwhWk7jZC0RTdopnAYKh

Level 5→6

```
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 . -size 1033c
./maybeh ere07/.file2
bandit5@bandit:~/inhere$ cat ./maybeh ere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

Password:- DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Level 6→7

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c
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/758/task/758/fd/6': No such file or directory
find: '/proc/758/task/758/fdinfo/6': No such file or directory
find: '/proc/758/fd/5': No such file or directory
find: '/proc/758/fdinfo/5': No such file or directory
find: '/cgroup2/csessions': Permission denied
find: '/boot/lost+found': Permission denied
find: '/tmp': Permission denied
find: '/run/lvm': Permission denied
find: '/run/screen/S-bandit10': Permission denied
find: '/run/screen/S-bandit29': Permission denied
find: '/run/screen/S-bandit25': Permission denied
find: '/run/screen/S-bandit30': Permission denied
find: '/run/screen/S-bandit9': Permission denied
find: '/run/screen/S-bandit28': Permission denied
find: '/run/screen/S-bandit18': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/screen/S-bandit12': Permission denied
find: '/run/screen/S-bandit5': Permission denied
```

```
find: '/run/screen/S-bandit14': Permission denied
find: '/run/screen/S-bandit13': 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
```

Password:- HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Level 7→8

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

Password:- cvX2JJJa4CFALtqS87jk27qwqGhBM9plV

Level 8→9

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

Password:- UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Level 9→10

```
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&^
```

Password:- truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Level 10→11

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

Password:- IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Level 11→12

```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt | tr a-zA-Z n-za-mN-ZA-M
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
```

Password:- 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Level 12→13

```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ cat data.txt
00000000: 1f8b 0808 0650 b45e 0203 6461 7461 322e .....P.^..data2.
00000010: 6269 6e00 013d 02c2 fd42 5a68 3931 4159 bin...BZh91AY
00000020: 2653 598e 4f1c c800 001e 7fff fb9f 7fda &SY.O.....
00000030: 9e7f 4f76 9fcf fe7d 3fff f67d abde 5e9f ..Ov...}?...^.
00000040: f3fe 9fbf f6f1 feee bdfd a3ff b001 3b1b .....;.;
00000050: 5481 a1a0 1ea0 1a34 d0d0 001a 68d3 4683 T.....4....h.F.
00000060: 4680 0680 0034 1918 4c4d 190c 4000 0001 F....4..LM..@...
00000070: a000 c87a 81a3 464d a8d3 43c5 1068 0346 ...z..FM..C..h.F
00000080: 8343 40d0 3400 0340 66a6 8068 0cd4 f500 .C@.4..@f..h....
00000090: 69ea 6800 0f50 68f2 4d00 680d 06ca 0190 i.h..Ph.M.h....
000000a0: 0000 69a1 a1a0 1ea0 194d 340d 1ea1 b280 ..i.....M4.....
000000b0: f500 3406 2340 034d 3400 0000 3403 d400 ..4.#@.M4...4...
000000c0: 1a07 a832 3400 f51a 0003 43d4 0068 0d34 ...24.....C..h.4
000000d0: 6868 f51a 3d43 2580 3e58 061a 2c89 6bf3 hh...=C%.>X...k.
000000e0: 0163 08ab dc31 91cd 1747 599b e401 0b06 .c...1...GY.....
000000f0: a8b1 7255 a3b2 9cf9 75cc f106 941b 347a ..rU....u.....4z
00000100: d616 55cc 2ef2 9d46 e7d1 3050 b5fb 76eb ..U....F..0P..v.
00000110: 01f8 60c1 2201 33f0 0de0 4aa6 ec8c 914f ..'."3...J....0
00000120: cf8a aed5 7b52 4270 8d51 6978 c159 8b5a ....{RBp.Qix.Y.Z
00000130: 2164 fb1f c26a 8d28 b414 e690 bfdd b3e1 !d...j.(.....
00000140: f414 2f9e d041 c523 b641 ac08 0c0b 06f5 ../.A.#.A.....
00000150: dd64 b862 1158 3f9e 897a 8cae 32b0 1fb7 .d.b.X?...z...2...
00000160: 3c82 af41 20fd 6e7d 0a35 2833 41bd de0c <..A .n}.5(3A...
00000170: 774f ae52 a1ac 0fb2 8c36 ef58 537b f30a w0.R.....6.XS{..
00000180: 1510 cab5 cb51 4231 95a4 d045 b95c ea09 .....QB1...E.\..
00000190: 9fa0 4d33 ba43 22c9 b5be d0ea eeb7 ec85 ..M3.C".....
000001a0: 59fc 8bf1 97a0 87a5 0df0 7acd d555 fc11 Y.....Z..U..
000001b0: 223f fdc6 2be3 e809 c974 271a 920e acbc "?...+...t'.....
000001c0: 0de1 f1a6 393f 4cf5 50eb 7942 86c3 3d7a ....9?L.P.yB..=z
000001d0: fe6d 173f a84c bb4e 742a fc37 7b71 508a .m.?..L.Nt*.7{qP.
000001e0: a2cc 9cf1 2522 8a77 39f2 716d 34f9 8620 ....%"..w9.qm4..
000001f0: 4e33 ca36 eec0 cd4b b3e8 48e4 8b91 5bea N3.6...K..H...[.
00000200: 01bf 7d21 0b64 82c0 3341 342a e98b 4d7e ..}!.d...3A4$.M~
00000210: c95c 1b1f cac9 a04a 1988 43b2 6b55 c6a6 .\.....J..C.kU..
00000220: 075c 1eb4 8ecf 5cdf 4653 064e 84da 263d .\....\..FS.N..&=
```



```

00000130: 2164 fb1f c26a 8d28 b414 e690 bfdd b3e1 1d...j.(.....
00000140: f414 2f9e d041 c523 b641 ac08 0c0b 06f5 ../.A.#.A.....
00000150: dd64 b862 1158 3f9e 897a 8cae 32b0 1fb7 .d.b.X?...z..2...
00000160: 3c02 af41 20fd 6e7d 0a35 2833 41bd de0c <..A .n).5(3A...
00000170: 774f ae52 a1ac 0fb2 8c36 ef58 537b f30a wO.R.....6.XS{..
00000180: 1510 cab5 cb51 4231 95a4 d045 b95c ea09 .....QB1...E.\..
00000190: 9fa0 4d33 ba43 22c9 b5be d0ea eeb7 ec85 ..M3.C".....
000001a0: 59fc 8bf1 97a0 87a5 0df0 7acd d555 fc11 Y.....Z...U..
000001b0: 223f fdc6 2be3 e809 c974 271a 920e acbc "?.+...t'.....
000001c0: 0de1 f1a6 393f 4cf5 50eb 7942 86c3 3d7a ....9?L.P.yB...=z
000001d0: fe6d 173f a84c bb4e 742a fc37 7b71 508a .m.?.L.Nt*.7{qP.
000001e0: a2cc 9cf1 2522 8a77 39f2 716d 34f9 8620 ....%".w9.qm4..
000001f0: 4e33 ca36 eec0 cd4b b3e8 48e4 8b91 5bea N3.6...K..H...[.
00000200: 01bf 7d21 0b64 82c0 3341 3424 e98b 4d7e ..}!..d..3A4$..M~
00000210: c95c 1b1f cac9 a04a 1988 43b2 6b55 c6a6 .\.....J..C.kU..
00000220: 075c 1eb4 8ecf 5cdf 4653 064e 84da 263d .\....\FS.N..&=
00000230: b15b bcea 7109 5c29 c524 3afc d715 4894 .[...q.\).$.:...H.
00000240: 7426 072f fc28 ab05 9603 b3fc 5dc9 14e1 t8./.(.....)]...
00000250: 4242 393c 7320 98f7 681d 3d02 0000 BB9<s ..h=...

bandit12@bandit:~$ mkdir /tmp/geethika
bandit12@bandit:~$ cp data.txt /tmp/geethika
bandit12@bandit:~$ cd /tmp/geethika
bandit12@bandit:/tmp/geethika$ ls
data.txt
bandit12@bandit:/tmp/geethika$ file data.txt
data.txt: ASCII text
bandit12@bandit:/tmp/geethika$ xxd -r data.txt data1
bandit12@bandit:/tmp/geethika$ file data1
data1: gzip compressed data, was "data2.bin", last modified: Thu May 7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/geethika$ mv data1 data2.gz
bandit12@bandit:/tmp/geethika$ gzip -d data2.gz
bandit12@bandit:/tmp/geethika$ file data2
data2: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/geethika$ mv data2 data3.bz2
bandit12@bandit:/tmp/geethika$ bzip2 -d data3.bz2
-bash: bzip2: command not found
bandit12@bandit:/tmp/geethika$ bzip2 -d data3.bz2
bandit12@bandit:/tmp/geethika$ file data3
data3: gzip compressed data, was "data4.bin", last modified: Thu May 7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/geethika$ mv data3 data4.gz
bandit12@bandit:/tmp/geethika$ gzip -d data4.gz
bandit12@bandit:/tmp/geethika$ file data4
data4: POSIX tar archive (GNU)
bandit12@bandit:/tmp/geethika$ tar -xvf data4
data5.bin
bandit12@bandit:/tmp/geethika$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/geethika$ tar -xvf data5.bin
data6.bin
bandit12@bandit:/tmp/geethika$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/geethika$ mv data6.bin data7.bz2
bandit12@bandit:/tmp/geethika$ bzip2 -d data7.bz2
bandit12@bandit:/tmp/geethika$ file data7
data7: POSIX tar archive (GNU)
bandit12@bandit:/tmp/geethika$ tar -xvf data7

```

```

bandit12@bandit:/tmp/geethika$ mv data6.bin data7.bz2
bandit12@bandit:/tmp/geethika$ bzip2 -d data7.bz2
bandit12@bandit:/tmp/geethika$ file data7
data7: POSIX tar archive (GNU)
bandit12@bandit:/tmp/geethika$ tar -xvf data7
data8.bin
bandit12@bandit:/tmp/geethika$ 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/geethika$ mv data8.bin data9.gz
bandit12@bandit:/tmp/geethika$ gzip -d data9.gz
bandit12@bandit:/tmp/geethika$ file data9
data9: ASCII text
bandit12@bandit:/tmp/geethika$ cat data9
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/geethika$ ssh bandit13@localhost

```

Password:- 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Level 13→14

```

bandit13@bandit:~$ ls
sshkey.private
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 SHA256:98UL0ZWr85496EtCRkKLo20X30PnyPSB5tB5RPbhczc.
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

```

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHixuU3b3e
```

Password:- 4wcYUJFw0k0XLShlDzztnTBHixuU3b3e

Level 14→15

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHixuU3b3e
bandit14@bandit:~$ telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
4wcYUJFw0k0XLShlDzztnTBHixuU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
```

```
Connection closed by foreign host.
```

Password:- BfMYroe26WYalil77FoDi9qh59eK5xNr

Level 15→16

```
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
BfMYroe26WYalil77FoDi9qh59eK5xNr
bandit15@bandit:~$ man nc | grep ssl
bandit15@bandit:~$ man nc
bandit15@bandit:~$ man ncat
bandit15@bandit:~$ man ncat | grep ssl
--ssl                Connect or listen with SSL
--ssl-cert            Specify SSL certificate file (PEM) for listening
--ssl-key             Specify SSL private key (PEM) for listening
--ssl-verify          Verify trust and domain name of certificates
--ssl-trustfile       PEM file containing trusted SSL certificates
--ssl-ciphers         Cipherlist containing SSL ciphers to use
--ssl (Use SSL)
--ssl-verify (Verify server certificates)
    In client mode, --ssl-verify is like --ssl except that it also requires verification of the server certificate. Ncat comes with a default set of trusted certificates used if available. Use --ssl-trustfile to give a custom list. Use -v one or more times to get details about verification failures. Ncat does not support --ssl-verify in server mode.
--ssl-cert certfile.pem (Specify SSL certificate)
    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 certificate named with --ssl-cert.
--ssl-trustfile cert.pem (List trusted certificates)
--ssl-verify. The argument to this option is the name of a PEM file containing trusted certificates. Typically, the file will contain a list of trusted certificates.
--ssl-ciphers cipherlist (Specify SSL ciphersuites)
    http://www.openssl.org
bandit15@bandit:~$ ncat --ssl localhost 30001
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcfftSxQluehd
```

Password:- cluFn7wTiGryunymYOu4RcfftSxQluehd