

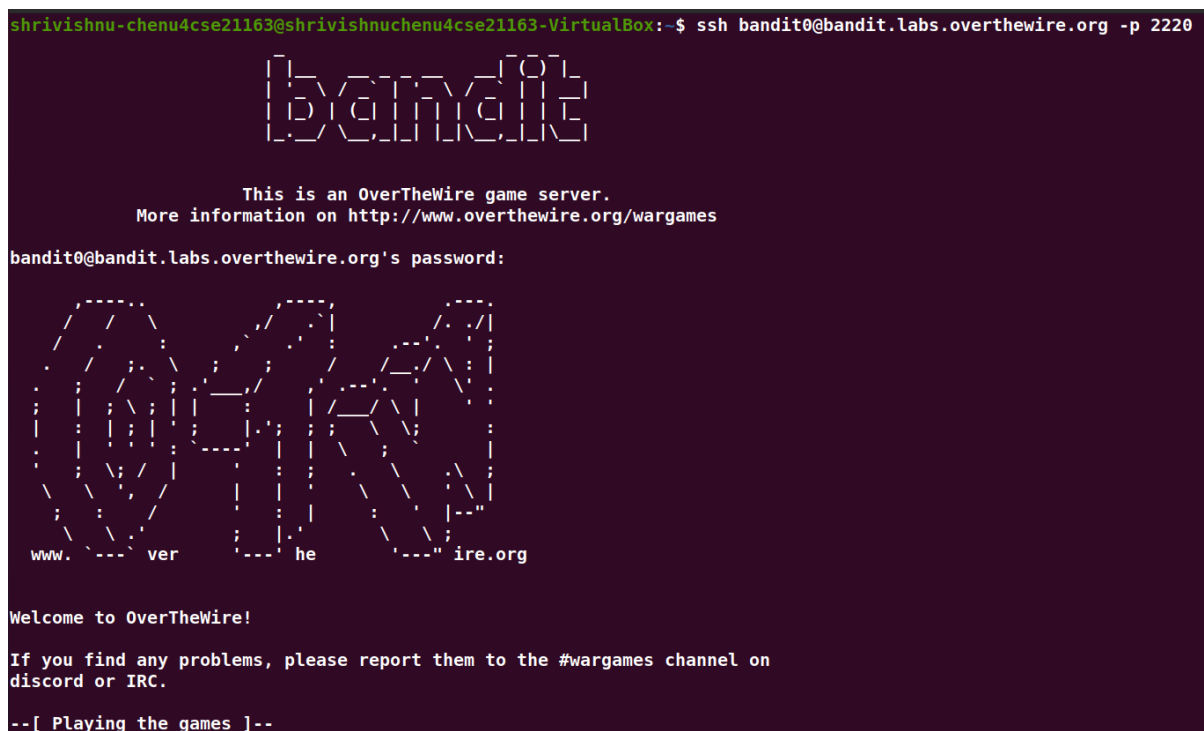
TASK 2 [LINUX GAMES]

Rohan R
CSE –B
CH.EN.U4CSE21155

Accessing Level 0

We use ssh command to access level 0.

```
shrivishnu-chenu4cse21163@shrivishnuchenu4cse21163-VirtualBox:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
```



```
bandit0@bandit.labs.overthewire.org's password:
```

```
Welcome to OverTheWire!
```

```
If you find any problems, please report them to the #wargames channel on discord or IRC.
```

```
--[ Playing the games ]--
```

```
-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 executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

--[Tools]--

For your convenience we have installed a few useful tools which you can find in the following locations:

- * gef (<https://github.com/hugsy/gef>) in /opt/gef/
- * pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
- * peda (<https://github.com/longld/peda.git>) in /opt/peda/
- * gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
- * pwntools (<https://github.com/Gallopsled/pwntools>)
- * radare2 (<http://www.radare.org/>)

Both python2 and python3 are installed.

--[More information]--

For more information regarding individual wargames, visit <http://www.overthewire.org/wargames/>

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit0@bandit:~\$ █

Level 0 to Level 1

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cd readme
-bash: cd: readme: Not a directory
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
```

The password for the next level is

NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

Level 1 to Level 2

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

The password for the next level is `rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi`

Level 2 to Level 3

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat 'spaces in this filename'
aBZ0W5EmUfAf7kHTQe0wd8bauFJ2lAiG
bandit2@bandit:~$
```

The password for the next level is `aBZ0W5EmUfAf7kHTQe0wd8bauFJ2lAiG`

Level 3 to Level 4

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$
```

The password for the next level is `2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe`

Level 4 to Level 5

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ file ./-file0*
./-file00: OpenPGP Public Key
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$
```

The password for the next level is `lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR`

Level 5 to Level 6

```
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere04  maybehere08  maybehere12  maybehere16
maybehere01  maybehere05  maybehere09  maybehere13  maybehere17
maybehere02  maybehere06  maybehere10  maybehere14  maybehere18
maybehere03  maybehere07  maybehere11  maybehere15  maybehere19
bandit5@bandit:~/inhere$ find -type f -size 1033c ! -executable
./maybehere07/.file2
./maybehere07/.file2
-bash: ./maybehere07/.file2: Permission denied
bandit5@bandit:~/inhere$ cd maybehere07
bandit5@bandit:~/inhere/maybehere07$ ls
-file1 -file2 -file3 spaces file1 spaces file2 spaces file3
bandit5@bandit:~/inhere/maybehere07$ cat .file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

The password for the next level is **P4L4vucdmLnm8I7VI7jG1ApGSfjYKqJU**

Level 6 to Level 7

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>&1 | grep -F  
-v Permission | grep -F -v directory  
/var/lib/dpkg/info/bandit7.password  
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password  
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S  
bandit6@bandit:~$
```

The password for the next level is **z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S**

Level 7 to Level 8

```
scabies's      4LIUlwG5IxHDvPmZiqlKLWib1Wluolqp  
barber 0UJ8SYbjoIASJ4vwfX3TpbTuL1rERwMT  
certitude     4HJYxK0TZuswyxHzYoDgfISThys2emPm  
punt's  ETr7K4q09Zq4IiiCTRUzUePcH236s6FT  
portrayed     K6H2o7EbY5N7NI8ccfPXtM0zNAC5BYxC  
governorship  rijZYefUnjZWhppZVhnPMLEltdXJ92BD  
Arab  UxymMbHC4razqjrFCzQujqWs6M15Smcd  
bluffest      ZhXPrBHFzxV12ISYbgMX2w6rlnLU4ep8  
steam's WxyX3phGx3cPU9TOGUvtmnFmFEQtqMf9  
works  tbzupEMQ13eaqzaYnpddzawMXvakbKAL  
tenser  DhAcJssgc1C3CtgytSytkcptwuRx40lZ  
compatible    hZpBYqoiHWwyy6q57in4CtXISP2a5Q4S  
Freon  2dhr2KY9Dk08nkgQBqmypb41YHA6pDbX  
sociables     yxJS10Kyz2fU7sKtP2gR9YNIKTKf9754  
trophy's      4B6orPD7mbqYvRI4xjm5Dke9EJ4fuPlm  
removes pwix1fbzX1f7tNNrfqwMZqx9IiM891Rj  
critically    GQaWLRneBYoEpishazb4T455svysfwar  
legerdemain's QGgM6Kbg1XFYdrwIsHtZQW0KgMThyhyk  
rebuilds      BC2HELCHXjQFHY3Q7ri204EeYC7bvXrK  
haywire's     HyRSR10U7LTRaUqfdESisLx1QvlpAC3q  
acrobatic     KqtL4NhJ0NUssPohSALoawSsmxDfr9dQ  
bandit7@bandit:~$ cat data.txt | grep millionth  
millionth      TESKZC0XvTetK0S9xNwm25STk5iWrBvP  
bandit7@bandit:~$
```

The password for the next level is **TESKZC0XvTetK0S9xNwm25STk5iWrBvP**

Level 8 to Level 9

```
mzCnXrbqm8QdgjRP1A12isJwyCZ0uTJn
i6t6LYg1JArHP57SS8532uSDt6HRA9Ln
Z8ncb64yvxMpYu6kyuRadwjouYpkMLPN
f0hFsyegU2D3zLrex0WI90sw2DlNYIlj
ryM64LqAra2XBhstdzbLWfUS26Xa9o6C
wN85lAbx5wkDs0IfVpbIldSUSgY16QmL
6hXvdZamDJFnfKX808UZPVjZpjeqeq6M
DHMhiE3MDZYEnc0WimJaGxkVfAejqL1c
AyLowHutWTI3WLR37pvKFBdxrk0GDuux
jBN1cLA8VHLIWyD7rsg1WULYyDvnMoyA
vCV4xQA9BY6D78vlljAq3SEFY7mGeLJd
tnh0GCM27V5Ao0MfLWhsZM1EFc8DZe3x
QrMLTTEu3KGuydS2w9FLTTLzuRldf6f6
oUHk3VaGVlNeB52K6cV03vEPAjMDshRR
UPmZTd6oJGLWmYM1dRXgWEKEX4GEs10M
7HNLPWyymsBFNjZJVPRro4zPh2p1imsN
68qUzJZLu0Iw5a6iPi2CVsxlP6l0wgaS
TuYdzYVx3Z5ue4jRa0qX301qf8Y1M97I
Rp0wfRgvra5Z0obMMG0FzLaJLN0Uq8IS
HqxUEnCqSABq86q6oEXA0cTCRkdXaRGB
XCAk2n2alytIxQABvtUUjqAL4I4Cchdm
bandit8@bandit:~$ cat data.txt | sort | uniq -c -u
1 EN632PlfYiZbn3PhVK3XOGSlnInNE00t
bandit8@bandit:~$
```

The password for the next level is **EN632PlfYiZbn3PhVK3XOGSlnInNE00t**

Level 9 to Level 10

```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt | grep ====
===== the
bu===== password
4iu===== is
===== G7w8LIi6J3kTb8A7j9LgrywtEulyyp6s
bandit9@bandit:~$
```

The password for the next level is `G7w8Lli6J3kTb8A7j9LgrywtEUlyyp6s`

Level 10 to Level 11

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTl1GTmI2b1ZDS3pwaGxYSEJNCg==
bandit10@bandit:~$ cat data.txt | base64 --decode
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$
```

The password for the next level is `6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM`

Level 11 to Level 12

```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIA00SFzMjXXBC0KoSKBbJ8puQm5lIEi
bandit11@bandit:~$ cat data.txt | tr a-zA-Z n-za-mN-ZA-M
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
bandit11@bandit:~$
```

The password for the next level is `JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv`

Level 12 to Level 13

```
00000200: 829b 0182 07ef fbee dff1 40da 6f5a c7fb .....@.oZ..
00000210: 5412 78a9 43dd 2198 d456 3c1f e161 2b1f T.x.C!..V<..a+.
00000220: 6e82 f066 70e2 67b8 ec48 d418 3e6a 0ee7 n..fp.g..H..>j..
00000230: 868a 1dcc e7b0 11ee 8b2a 8c53 0009 37f9 .....*.S..7.
00000240: 1017 0d29 485a ec30 cb90 45b8 93ff 1772 ...)HZ.0..E....r
00000250: 4538 5090 5ded 11a8 e965 cb22 3f02 0000 E8P.]....e."?...

bandit12@bandit:~$ mkdir /tmp/vishnu
bandit12@bandit:~$ xxd -r data.txt > /tmp/vishnu/file.bin
bandit12@bandit:~$ cd /tmp/vishnu
-bash: cd: /tmp/vishnu: No such file or directory
bandit12@bandit:~$ cd /tmp/vishnu
bandit12@bandit:~$ cd /tmp/vishnu$ ls -la
.  file.bin
bandit12@bandit:~$ cd /tmp/vishnu$ file file.bin
file.bin: gzip compressed data, was "data2.bin", last modified: Thu Sep 1 06:30:09 2022, max compression, from Unix, original size modulo 2^32 575
bandit12@bandit:~$ cd /tmp/vishnu$ zcat file.bin | file -
/dev/stdin: bzip2 compressed data, block size = 900k
bandit12@bandit:~$ cd /tmp/vishnu$ zcat file.bin | bzipcat | file -
/dev/stdin: gzip compressed data, was "data4.bin", last modified: Thu Sep 1 06:30:09 2022, max compression, from Unix
bandit12@bandit:~$ cd /tmp/vishnu$ zcat file.bin | bzipcat | zcat | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:~$ cd /tmp/vishnu$ zcat file.bin | bzipcat | zcat | tar x0 | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:~$ cd /tmp/vishnu$ zcat file.bin | bzipcat | zcat | tar x0 | tar x0 | file -
/dev/stdin: bzip2 compressed data, block size = 900k
bandit12@bandit:~$ cd /tmp/vishnu$ zcat file.bin | bzipcat | zcat | tar x0 | tar x0 | bzipcat | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:~$ cd /tmp/vishnu$ zcat file.bin | bzipcat | zcat | tar x0 | tar x0 | bzipcat | tar x0 | file -
/dev/stdin: gzip compressed data, was "data9.bin", last modified: Thu Sep 1 06:30:09 2022, max compression, from Unix
bandit12@bandit:~$ cd /tmp/vishnu$ zcat file.bin | bzipcat | zcat | tar x0 | tar x0 | bzipcat | tar x0 | zcat | file -
/dev/stdin: ASCII text
bandit12@bandit:~$ cd /tmp/vishnu$ zcat file.bin | bzipcat | zcat | tar x0 | tar x0 | bzipcat | tar x0 | zcat
The password is wbWdLBxEir4CaE8LaPhauuOo6pwRmrDw
bandit12@bandit:~$ cd /tmp/vishnu$
```

The password for the next level is **wbWdLBxEir4CaE8LaPhauuOo6pwRmrDw**

Level 13 to Level 14

```
bandit14@bandit:~$ ls -la
.  ..  .bash_logout  .bashrc  .profile  .ssh
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShLDzztnTBHiqxU3b3e
```

The password for the next level is **4wcYUJFw0k0XLShLDzztnTBHiqxU3b3e**

Level 14 to Level 15

```
bandit14@bandit:~$ nc localhost 3000 4wcYUJFw0k0XLShLDzztnTBHiqxU3b3e
bandit14@bandit:~$ nc localhos 3000
localhos: forward host lookup failed: No address associated with name
bandit14@bandit:~$ nc localhost 3000 4wcYUJFw0k0XLShLDzztnTBHiqxU3b3e
bandit14@bandit:~$ nc localhost 30000 4wcYUJFw0k0XLShLDzztnTBHiqxU3b3e

Wrong! Please enter the correct current password
bandit14@bandit:~$ nc localhost 30000 4wcYUJFw0k0XLShLDzztnTBHiqxU3b3e
4wcYUJFw0k0XLShLDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
```

The password for the next level is **BfMYroe26WYalil77FoDi9qh59eK5xNr**