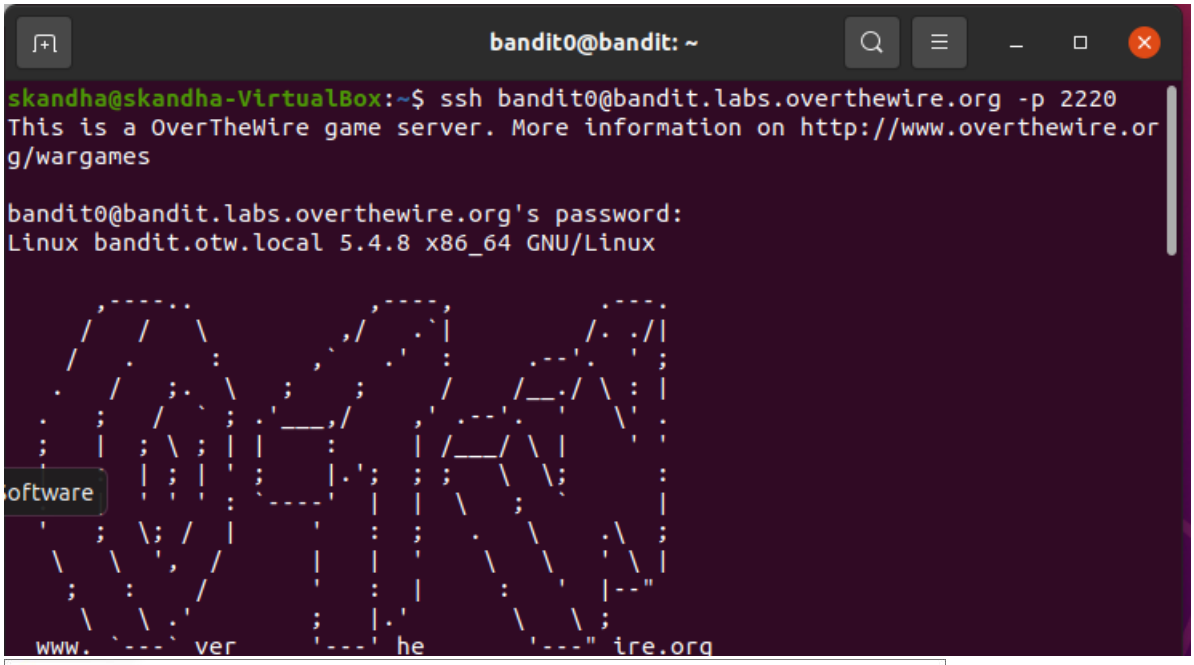
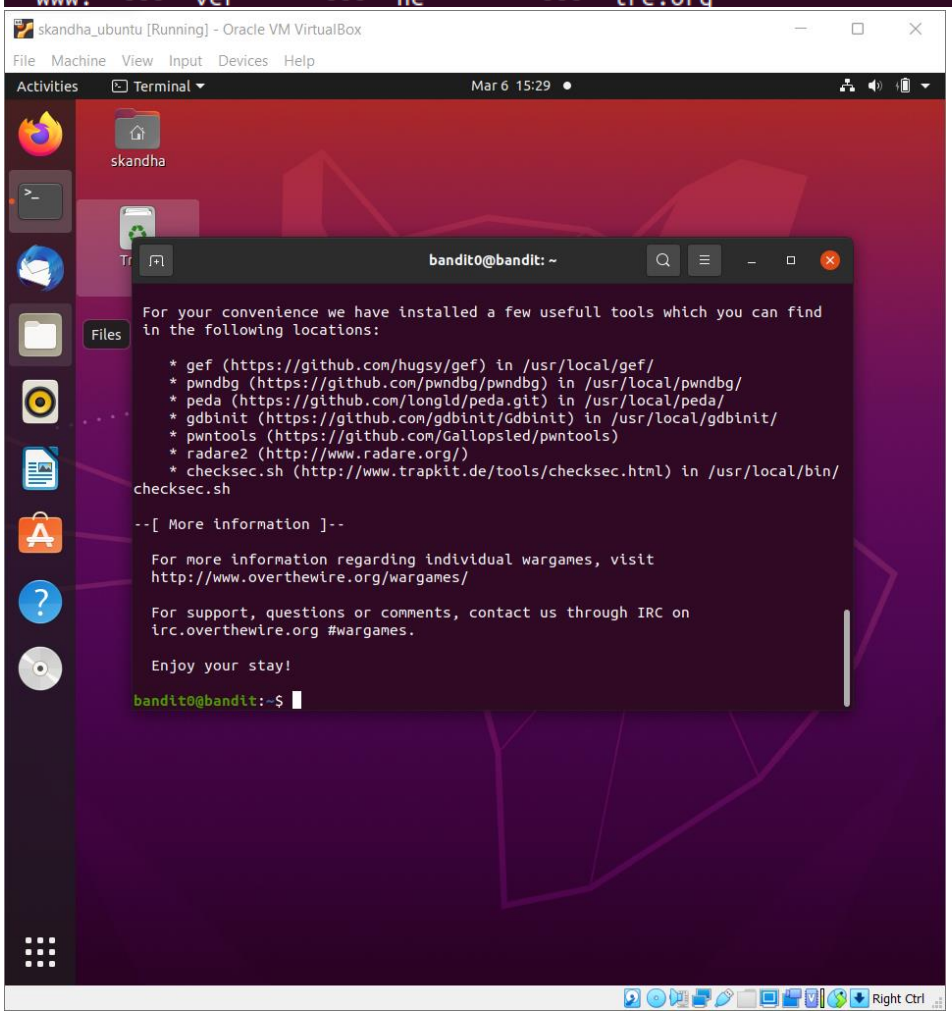
TASK-7 OVERTHEWIRE WAR GAME (TILL LEVEL 15) **VS SKANDHA**

Accessing Level 0

We use ssh command to access level 0





Level 0 to Level 1

We use cat command to open the readme file

```
bandit0@bandit: ~

--[ 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!

bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cd readme
-bash: cd: readme: Not a directory
bandit0@bandit:~$ gedit readme
-bash: gedit: command not found
bandit0@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  .profile  readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
```

The password for the next level is boJ9jbbUNNfktd78OOpsqOltutMc3MY1

Level 1 to Level 2

We again use cat command but since the filename has a dash at the beginning, we use cat <-

```
bandit1@bandit: ~

    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * 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!

bandit1@bandit:~$ ls
-
bandit1@bandit:~$ ./-
-bash: ./-: Permission denied
bandit1@bandit:~$ cat < -
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$
```

The password for the next level is CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

Level 2 to Level 3

We again use cat command but we use single quotes to open the file since it has spaces in its name

```
bandit2@bandit: ~
    * gef (https://github.com/hugsy/gef) in /usr/local/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * 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!

bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat 'spaces in this filename'
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
```

The password for the next level is UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

Level 3 to Level 4

We use ls -a to find hidden files of a directory after that we use the cat command to find the file.

```
bandit3@bandit: ~/inhere
    * 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!

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

The password for the next level is pIwrPrtPN36QITSp3EQaw936yaFoFgAB

Level 4 to Level 5

We can open each file one by one to find the password or use the find command to find the file with ASCII text and then open the required file.

```
bandit4@bandit: ~/inhere
file: Cannot open `ile00' (No such file or directory).
bandit4@bandit:~/inhere$ cat <-file01
◆◆p,k◆;◆◆r*◆◆   ◆.!◆◆C◆◆J       ◆dx,◆bandit4@bandit:~/inhere$ cat <-file02
e◆)◆#◆◆5◆◆
          ◆◆p◆◆V◆_◆◆◆◆◆mmbandit4@bandit:~/inhere$ cat <-file03
◆◆◆◆◆◆h!TQO◆`◆4"aP◆7phT◆◆,◆Abandit4@bandit:~/inhere$ cat <-file04
?◆bandit4@bandit:~/inhere$ cat <-file05
◆r◆l$◆?h◆9('◆◆◆!y◆e◆#◆x◆O◆◆=◆◆bandit4@bandit:~/inhere$ cat <-file06
ly◆◆◆~◆◆A◆f◆◆◆◆-E◆{◆◆◆m◆◆◆◆◆◆Mbandit4@bandit:~/inhere$ cat <-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
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
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

The password for the next level is koReBOKuIDDepwhWk7jZC0RTdopnAYKh

Level 5 to Level 6

Here if we use the find command with the size parameter, we can narrow down the needed file. After that we can use the cd and cat command consecutively to find the password

```
bandit5@bandit: ~/inhere/maybehere07
maybehere18: directory
maybehere19: directory
bandit5@bandit:~/inhere$ find -size 1033.c
find: Invalid argument `1033.c' to -size
bandit5@bandit:~/inhere$ find -size 1033c
./maybehere07/.file2
ox dit5@bandit:~/inhere$ file ./maybehere07/.file2
./maybehere07/.file2: ASCII text, with very long lines
bandit5@bandit:~/inhere$ cd maybehere07
bandit5@bandit:~/inhere/maybehere07$ cat .file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
bandit5@bandit:~/inhere/maybehere07$
```

The password for the next level is DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Level 6 to Level 7

We use find command with user, size and group parameters and enter the needed parameters

In the list we can find the file ./var/lib/dpkg/info/bandit7.password and then use the cat command to find the password

```
bandit6@bandit: /
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-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:/$ ^C
bandit6@bandit:/$ cat <./var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:/$
```

The password for the next level is HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Level 7 to Level 8

Here we use the grep command and find the line in the file with the password as given in the question

```
bandit7@bandit: ~
knotting        vh268WJXw1OSnszed9MVaHD4rTP69lZr
hymnals 7MqsN32lfDbPigtAX6cwFbMZcPAMUoae
Fremont tCy02wC8xdpFqjlZ8xdBQYAHFZPHk7ls
punter's        zAfzaA1IOuBSamCR6eMmRoc9oNXPQ16a
junking 6Tlr5K8YZ1d2Xsdku3TTFYXWB6WOMXyT
Aymara  zSeUS0UyD8Q6a6YPwaClRBbk1x8kFBEc
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:~$ cat data.txt|grep millionth
millionth       cvX2JJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$ ^C
bandit7@bandit:~$
```

The password for the next level is cvX2JJa4CFALtqS87jk27qwqGhBM9plV

Level 8 to Level 9

Here in this level, we pipe the sort and uniq with -u parameter to get the only line which is the password for the next level

```
bandit8@bandit: ~
TKUtQbeYnEzzYIne7BinoBx2bHFLBXzG
TThRArdF2ZEXMO47TIYkyPPLtvzzLcDf
tVW9iY1Ml0uHPK4usZnN8oZXbjRt2ATY
U0NYdD3wHZKpfEg9qGQOLJimAJy6qxhS
UASW6CQwD6MRzftu6FAfyXBK0cVvnBLP
UJiCNvDNfgb3fcCj8PjjnAXHqUM63Uyj
UjsVbcqKeJqdCZQCDMkzv6A9X7hLbNE4
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
UVnZvhiVQECraz5jl8U14sMVZQhjuXia
V2d9umHiuPLYLIDsuHj0frOEmreCZMaA
v9zaxkVAOdIOlITZY2uoCtB1fX2gmly9
VkBAEWyIibVkeURZV5mowiGg6i3m7Be0
w4zUWFGTUrAAh8lNkS8gH3WK2zowBEkA
WBqr9xvf6mYTT5kLcTGCG6jb3ex94xWr
wjNwumEX58RUQTrufHMciWz5Yx10GtTC
X1JHOUkrb4KgugMXIzMWWIWvRkeZleTI
XyeJdbrUJyGtdGx8cXLQST0pwu5cvpcA
yo0HbSe2GM0jJNhRQLxwoPp7ayYEmRKY
ySvsTwlMgnUF0n86Fgmn2TNjkSOlrV72
Z9OC6DQpppreChPhwRJJV9YYTtrxNVcO
zdd2ctVveROGeiS2WE3TeLZMeL5jL7iM
bandit8@bandit:~$ sort data.txt |uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
bandit8@bandit:~$
```

The password for the next level is UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Level 9 to Level 10

Here we use strings command for the readable text and grep with = and pipe them together

We can then find the password for next Level

```
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&^
```

The password for the next level is truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Level 10 to Level 11

Here we use the base64 with -d to decrypt the encoded data and find the password for the next Level

```
bandit10@bandit: ~
in/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!

bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ data.txt
-bash: data.txt: command not found
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==
bandit10@bandit:~$ base64 data.txt
VkdobElIQmhjM04zYjNKa0lHbHpJRWxHZFd0M1MwZHpSbGM0VFU5eE0wbFNSbkZ5ZUVVeGFIaFVU
a1ZpVlZCU0NnPT0K
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$
```

The password for the next level is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Level 11 to Level 12

We use the tr command and use the encoding pattern of ROT13 and then translate the file to find the next password

```
bandit11@bandit: ~
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/b
in/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!

bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ tr 'A-Za-z' 'N-ZA-Mn-za-m' data.txt
tr: extra operand ‘data.txt’
Try 'tr --help' for more information.
bandit11@bandit:~$ man tr
bandit11@bandit:~$ tr 'A-Za-z' 'N-ZA-Mn-za-m'< data.txt
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
bandit11@bandit:~$
```

The password for the next level is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Level 12 to Level 13

In this Level we use the temporary directory and create a directory there and then copy the data.txt file to this the directory we have created and then use xxd -r on the data.txt file and direct it to file (here named test). Here the test file will be of gz (using file command).So rename it with .gz extension.

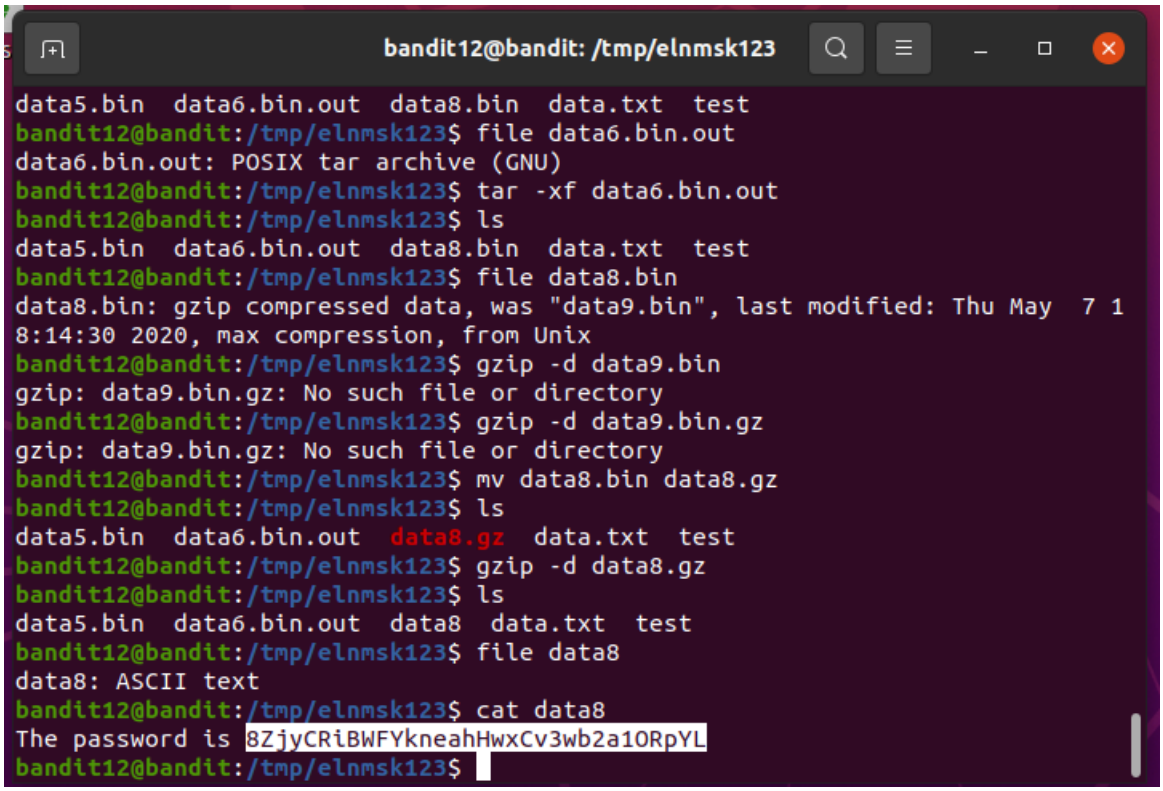
After this use gzip -d to decompress the file.

Since there are many consecutive steps, I have mentioned the types of files and how to decompress it.

- Bzip2: We use bzip2 -d to decompress the file
- Tar: We use tar -xf to decompress the file

Note: Some of the file names will be not right and the type may not be right, so by using the file command we can find the right name and type of the file and then decompress the correct way.

Finally, we get an ASCII text file where the password can be retrieved.



The password for the next level is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Level 13 to Level 14

We use ssh -i ./sshkey.private bandit14@localhost to access the Level 14 via a private key present in Level 13. After that we open the file path given in the question to find the actual password of this Level.

```
bandit14@bandit: ~
    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/b
in/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:~$ ls
bandit14@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  .profile  .ssh
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$ ^C
bandit14@bandit:~$
```

The password for the next level is 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

Level 14 to Level 15

Now here we use the netcat command via localhost to the given port in the question and the enter the password of this level and then we get the password for Level 15

```
bandit14@bandit: ~

--[ 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!
ice Writer
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

bandit14@bandit:~$
```

The password for the next level is BfMYroe26WYalil77FoDi9qh59eK5xNr.

Accessed Level 15

```
bandit15@bandit: ~

 For your convenience we have installed a few usefull tools which you can fin
d
 in the following locations:

    * gef (https://github.com/hugsy/gef) in /usr/local/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/b
in/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!

bandit15@bandit:~$
```