

Over The Wire Bandit walkthrough

Now we are going to play a beginner level CTF called bandit which is hosted by [OverTheWire](https://overthewire.org/) organization. You can enter the war game through link provided. In this game you can learn basic Linux commands.

Table of content

- Level 0
- Level 0-1
- Level 1-2
- Level 2-3
- Level 3-4
- Level 4-5
- Level 5-6
- Level 6-7
- Level 7-8
- Level 8-9
- Level 9-10
- Level 10-11
- Level 11-12
- Level 12-13
- Level 13-14
- Level 14-15

Level 0

This is simple level. In this level you going to learn about **SSH** protocol to remote login. We need some required information to login.

Host - bandit.labs.overthewire.org

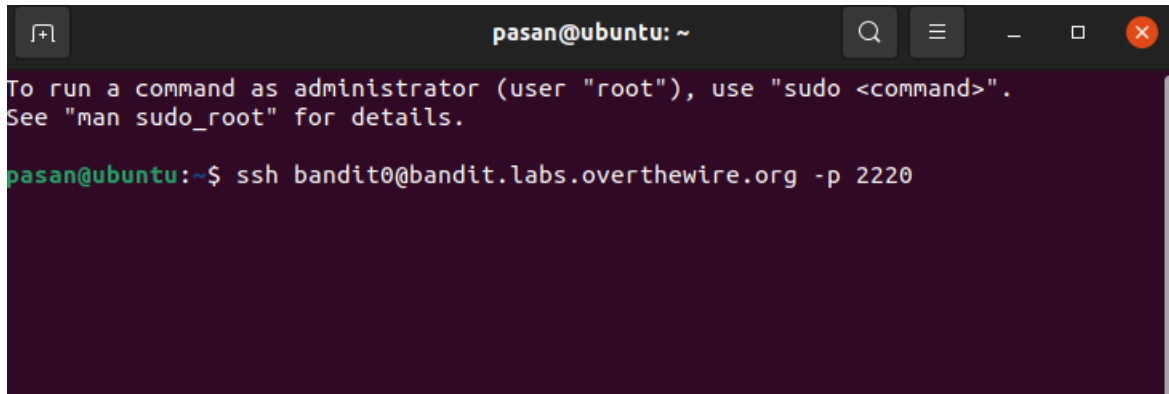
Port – 2220

Username - bandit0

Password - bandit0

We use the following command to login our machine as mentioned in figure 1.1.

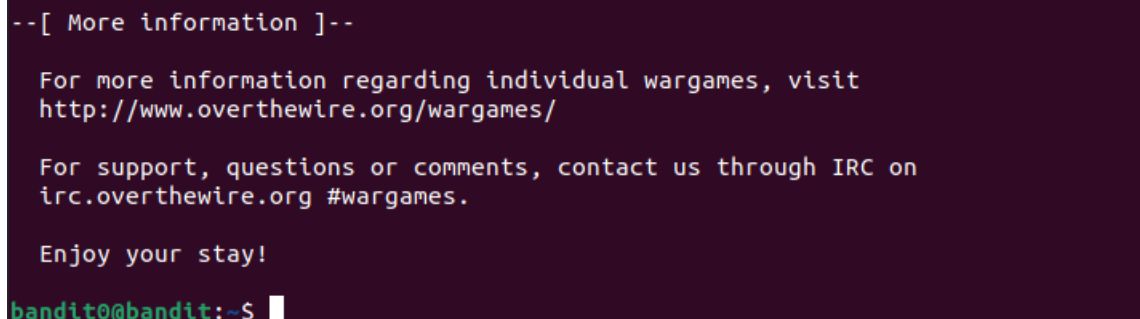
ssh bandit0@bandit.labs.overthewire.org -p 2220



```
pasan@ubuntu: ~  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
pasan@ubuntu:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
```

figure 1.1

When your ssh login successfully done, you will see the following in terminal. (figure1.2)



```
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us through IRC on  
#wargames.  
  
Enjoy your stay!  
  
bandit0@bandit:~$
```

figure 1.2

Level 0-1

Now we are at bandit0 shell, we must find the password to login the next level. Therefore, we need to know what the files are listed here. So, we type in our terminal command “**ls**” to list the files in the directory. Then we can see the file **readme**. Next, we type in our terminal command “**cat readme**”, which is concatenate the file and show the findings.



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

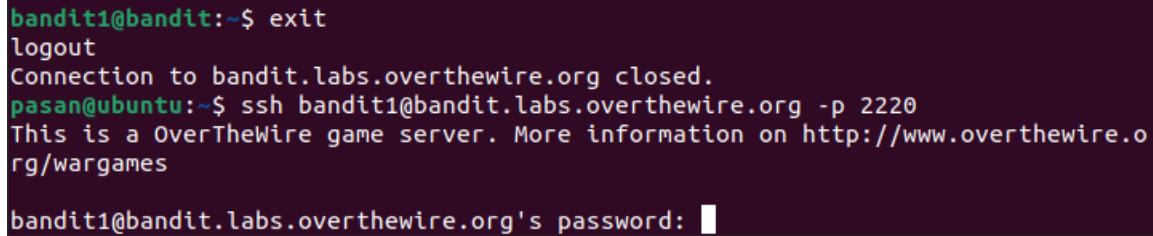
figure 1.3

Then exit from the current login by typing command “**exit**” on terminal.

Level 1-2

Now we know that the password to level 1. Typing the following command, you can login to the bandit level 1. We can provide the readme file's content as the password for the level 1 login.

ssh [bandit1@bandit.labs.overthewire.org](https://bandit1.bandit.labs.overthewire.org) -p 2220

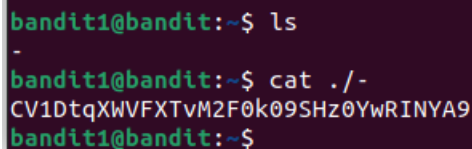


```
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
pasan@ubuntu:~$ ssh bandit1@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit1@bandit.labs.overthewire.org's password: █
```

figure 1.4

By typing following commands we can extract the password hidden in the file called "-"(hyphen).

First, we type usually as "ls" command to view files and there are shown a file called "-". The problem is, we cannot cat the file as usual like "cat -", there will be show an error message. We can use here the command "cat ./-" to read the file called "-".



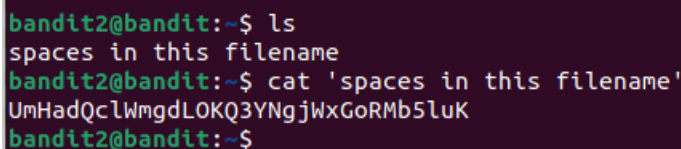
```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$
```

figure 1.5

Level 2-3

Now we can login to level 2 by using the password provided in level 1. In the description they mentioned the password is stored in the file called **spaces in this file name** and it's located in the home directory. As usually we type the command **ls** command to display the files. There are spaces in the file name, therefore we cannot use the cat command as usual. So, we use the cat command by following to read the file which are contains spaces in the file name.

ssh [bandit2@bandit.labs.overthewire.org](https://bandit2.bandit.labs.overthewire.org) -p 2220



```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat 'spaces in this filename'
UmHadQclWmgdLOKQ3YNgjWxGoRMB5LuK
bandit2@bandit:~$
```

figure 1.6

Now copy the given password in the terminal to login level 3. Remember to type **exit** and closed the connection with current level.

Level 3-4

Now move on to level 3 by typing the password we are extract from the level 2 and type **ls** command to display the files or directories in the server.

ssh [bandit3@bandit.labs.overthewire.org](https://bandit3.bandit.labs.overthewire.org) -p 2220

```
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:~$
```

figure 1.7

In the description they mentioned the file is in directory called inhere. There is a new command you are going to learn **cd**, which is used to move through the directories in Linux. Command **cd** is stands for change directory. As first step we type the command **ls** to view directories and then we can see there a directory called inhere. So, we use the command mentioned **cd inhere** to move the directory inhere. Then we type the command **ls** but there is nothing to display by the server. May be there are some hidden files. Then we can use command **ls -al** to see the hidden files in directory. Now we can see there are some data files and a file called **".hidden"**. So, we try to cat the file and read the content. Now we can cat the file using **cat .hidden** command.

```
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
bandit3@bandit:~/inhere$
```

figure 1.8

Level 4-5

Game is getting change from this level. We are not supposed to just type the ls and cd commands, we have to learn new things and go ahead. In this level they mentioned the file is stored in the file which is human readable file in the inhere directory. We need to know what the directories in the server are to start the sniffing. So, we type the ls command and there is directory called inhere and by using cd command we moved to the inhere directory. Again we typing the ls command we see some files which are shown like data files so we want to know what are the ASCII file to extract the password. Now we have to use following command to see the files data types. The command **file ./*** is help us to see data type of files. After the command execution we can see the ./-file07 is the ASCII text file which is human readable file. As usually next we cat the file and extract the password using cat ./-file07 command.

ssh bandit4@bandit.labs.overthewire.org -p 2220

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
-bash: cd: inhere: No such file or directory
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00 -file02 -file04 -file06 -file08
-file01 -file03 -file05 -file07 -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
bandit4@bandit:~/inhere$
```

figure 1.8

Level 5-6

We are informed that the next level password is stored in inhere directory, and it has some properties such as human readable, 1033 bytes and not executable. We can use find command to execute this task. We use find -readable \! -executable -size 1033c command to find the relevant file. After the executing the command, the server gives us a file according to the filters we use. Now we can concatenate the file to see the password.

ssh bandit5@bandit.labs.overthewire.org -p 2220

```

bandit5@bandit:~$ ls
inhere
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 -readable \! -executable -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7

```

figure 1.9

Level 6-7

Now we know the password is stored somewhere in the sever, and it has some properties. Over the wire gave us some hint about the file. So, we have to widen our scope to search the password file in this step. After the find command, we can see lot of files are found by the command but most of them are permission denied ones. If you scroll your cursor carefully there is an only one file called bandit7.password, isn't a permission denied one. Therefore, we can concatenate that file for password.

ssh bandit6@bandit.labs.overthewire.org -p 2220

```

bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c

```

figure 2.0

```

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
bandit6@bandit:~$

```

figure 2.1

Level 7-8

In this level they are mentioned the password for the next level is stored in the file data.txt next to the word millionth. Here we are using cat and grep commands to perform this task. Also, we are using the Unix pipe method. The pipe method helps us to connect the output from the first method and feed it to the second command. Lets see how it done.

ssh bandit7@bandit.labs.overthewire.org -p 2220

```
bandit7@bandit:~$  
bandit7@bandit:~$ cat data.txt | grep "millionth" data.txt  
millionth      cvX2JJJa4CFALtqS87jk27qwqGhBM9pLV  
bandit7@bandit:~$
```

figure 2.2

Level 8-9

They mentioned us that the next level password is stored on the file called data.txt and it is an unique content. Here we can use sort command to sort the text but there will be contains repeating lines, so we also using uniq command to filter the repeating lines.

ssh bandit8@bandit.labs.overthewire.org -p 2220

```
bandit8@bandit:~$ ls  
data.txt  
bandit8@bandit:~$ cat data.txt | sort | uniq -c  
10 07KC3ukwX7kswl8Le9ebh3H3s0oNTsP2
```

figure 2.3

But there's a problem still we can't see the exact result what we expect to see. So we can use the flag -c to get a count about the repeated times.

```

10 SHMAMUEzQe4mV7SJpETTzFsyNRJsZE2k
10 si952kS1y6pt4AFenmm0oIp8n7W5d3bd
10 sYSokIATVvFUKU4sAHTtMarfjLZWwj5i
10 SzwgS2ADSjP6yp0zp2bIvdqNyusRtrHj
10 TKUtQbeYnEzzYIne7BinoBx2bHFLBXzG
10 TThRArdF2ZEXM047TIYkyPPLtvzzLcDf
10 tVW9iY1Ml0uHPK4usZnN8oZXbjRt2ATY
10 U0NYdD3wHZKpfEg9qGQOLJiMAJy6qxhS
10 UASW6CQwD6MRzftu6FAfyXBK0cVvnBLP
10 UJiCNvDNfGb3fcCj8PjjnAXHqUM63Uyj
10 UjsVbcqKeJqdCZQCDMkzv6A9X7hLbNE4
10 UsvVyFSfZZWbi6wgC7dAFyFuR6jQUuHr
10 UVnZvhiVQECraz5jl8U14sMVZQhjuXia
10 V2d9umHiuPLYLIDsuHj0froEmreCZMaA
10 v9zaxkVA0dIOLITZY2uoCtB1fX2gmly9
10 VkBAEWyIibVkeURZV5mowiGg6i3m7Be0
10 w4zUWFGTURAAh8lNkS8gH3WK2zowBEkA
10 WBqr9xvf6mYTT5kLcTGCG6jb3ex94xWr
10 wjNwumEX58RUQTrufHMcIWz5Yx10GtTC
10 X1JHOUkrb4KgugMXIzMWWIWVRkeZleTI
10 XyeJdbrUJyGtdGx8cXLQST0pWu5cvpcA
10 xyeJdbrUJyGtdGx8cXLQST0pWu5cvpcA

```

figure 2.4

Level 9-10

Now they hinted for the password for the next level is stored inside a file named data.txt. Also that the password is preceded by several "=" characters. If we are just cat the file, the terminal fill with unreadable content. So, we have to use some filtering methods make this process clear.

ssh [bandit9@bandit.labs.overthewire.org](https://bandit.labs.overthewire.org) -p 2220

```

bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ cat data.txt | strings
Z/,_
WW"&8
2Qk)
xWa_
x?Xn
//M$
;yzEt!
WpU~e
`Rn,I
VSXdk
WB|{
GhGS

```

figure 2.5

There are many unreadable things, so we use grep command and make the result clearer.

```
bandit9@bandit:~$ cat data.txt | strings | 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:~$
```

figure 2.6

Level 10-11

In this level password hint is little bit change, so there is an encoded password to find and decode it to make usable. It is stored in data.txt. Base64 is common encoded method for many systems.

ssh bandit10@bandit.labs.overthewire.org -p 2220

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSKg==
bandit10@bandit:~$ cat data.txt | base64 -d
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$
```

figure 2.6

Level 11-12

This level password hint is bit difficult because it is encoded by rot13 encoding method. First we concatenate the data.txt file and pipe it into tr method to decrypt.

ssh bandit11@bandit.labs.overthewire.org -p 2220

```
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:~$
```

figure 2.7

Level 12-13

Bandit hinted us the password for the next level is stored in the file data.txt. Also a hex dump file, which is repeatedly compressed. And they advised us to create a directory under /tmp using mkdir method. Then copy it to that the folder you created.

ssh bandit12@bandit.labs.overthewire.org -p 2220

First we make the hex dump file using tool xxd, that helps us to make hex dump file or decode a hex dump file. We cannot make changes in hex dump file, so we have to convert it to ASCII file.

```
bandit12@bandit:~$ mkdir /tmp/usr
bandit12@bandit:~$ cp data.txt /tmp/usr
bandit12@bandit:~$ cd /tmp/usr
bandit12@bandit:/tmp/usr$ ls
data.txt
```

figure 2.7

Here we create a file called data1 hex dump file. compressed many times.

```
bandit12@bandit:/tmp/usr$ ls
data.txt
bandit12@bandit:/tmp/usr$ xxd -r data.txt data1
bandit12@bandit:/tmp/usr$ ls
data1 data.txt
bandit12@bandit:/tmp/usr$
```

figure 2.8

We can check the file type by using file command as mentioned below.

```
bandit12@bandit:/tmp/usr$ file data1
data1: gzip compressed data, was "data2.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
```

figure 2.9

Now we unzip the gzip compressed file using the gunzip command.

```
bandit12@bandit:/tmp/usr$ mv data1 data2.gz
bandit12@bandit:/tmp/usr$ ls
data2.gz data.txt
bandit12@bandit:/tmp/usr$ gunzip data2.gz
bandit12@bandit:/tmp/usr$ ls
data2 data.txt
bandit12@bandit:/tmp/usr$ file data2
data2: bzip2 compressed data, block size = 900k
```

figure 3.1

Then extract the data2.gz file.

```
bandit12@bandit:/tmp/usr$ gunzip data2.gz
bandit12@bandit:/tmp/usr$ ls
data2 data.txt
bandit12@bandit:/tmp/usr$ file data2
data2: bzip2 compressed data, block size = 900k
```

figure 3.2

Before unzip the bzip2 file we have to rename the file.

```
bandit12@bandit:/tmp/usr$ mv data2 data2.bz2
bandit12@bandit:/tmp/usr$ ls
data2.bz2  data.txt
```

figure 3.3

Now it's possible to unzip using bunzip2 command.

```
bandit12@bandit:/tmp/usr$ bunzip2 data2.bz2
bandit12@bandit:/tmp/usr$ ls
data2  data.txt
bandit12@bandit:/tmp/usr$ file data2
data2: gzip compressed data, was "data4.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
```

figure 3.4

When executing the file command it's shown as gzip file, therefore we can use gunzip command to unzip.

```
bandit12@bandit:/tmp/usr$ mv data2 data4.gz
bandit12@bandit:/tmp/usr$ gunzip data4.gz
bandit12@bandit:/tmp/usr$ ls
data4  data.txt
bandit12@bandit:/tmp/usr$ file data4
data4: POSIX tar archive (GNU)
```

figure 3.5

File type has changed. So, we can now use tar command to compress or decompress file. We are using some flags such as -x for extract -v for verbose -f for filename.

```
bandit12@bandit:/tmp/usr$ tar -xvf data4
data5.bin
bandit12@bandit:/tmp/usr$ file data5.bin
data5.bin: POSIX tar archive (GNU)
```

figure 3.6

data4.bin file compressed again to tar archive format, therefore we can use the same command to extract it.

```
bandit12@bandit:/tmp/usr$ tar -xvf data5.bin
data6.bin
bandit12@bandit:/tmp/usr$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
```

figure 3.7

Now the file compressed the bzip2 format. We can use bunzip2 method to unzip this. Before that don't forget to rename the file.

```
bandit12@bandit:/tmp/usr$ mv data6.bin data7.gz2
bandit12@bandit:/tmp/usr$ ls
data4  data5.bin  data7.gz2  data.txt
```

figure 3.8

Follow these steps to unzip the file. Don't worry about the error.

```
bandit12@bandit:/tmp/usr$ bunzip2 data7.gz2
bunzip2: Can't guess original name for data7.gz2 -- using data7.gz2.out
bandit12@bandit:/tmp/usr$ ls
data4 data5.bin data7.gz2.out data.txt
bandit12@bandit:/tmp/usr$ file data7.gz2.out
data7.gz2.out: POSIX tar archive (GNU)
```

figure 3.9

Again, the file extract to the tar archive, so we can use the previous method to unzip the file.

```
bandit12@bandit:/tmp/usr$ tar -xvf data7.gz2.out
data8.bin
bandit12@bandit:/tmp/usr$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
```

figure 4.0

Again, file compressed as gzip compression method. We can follow the previous steps as we did.

```
bandit12@bandit:/tmp/usr$ mv data8.bin data9.gz
bandit12@bandit:/tmp/usr$ gunzip data9.gz
bandit12@bandit:/tmp/usr$ ls
data4 data5.bin data7.gz2.out data9 data.txt
bandit12@bandit:/tmp/usr$ file data9
data9: ASCII text
```

figure 4.1

data9 file is an ASCII text, so we can easily cat this file and extract the password.

```
bandit12@bandit:/tmp/usr$ cat data9
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a10RpYL
bandit12@bandit:/tmp/usr$ client_loop: send disconnect: Broken pipe
pasan@ubuntu:~$
```

figure 4.2

Level 13-14

They hinted us, in this level we haven't got any password for next level but we get a private ssh key, that can be used to log into next level, and the file path is also given. Ssh key is more secure than the password. We can give the command as ssh -i for attach the file and the username finally the host name. Full command is ssh -i sshkey.private bandit14@localhost. After the executing command server asked that if you want to continue the connection, type yes and the key is displayed below.

```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
Could not create directory '/home/bandit13/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
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

Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

figure 4.3

Then you automatically login to the next level bandit level 14.

```
For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Enjoy your stay!

bandit14@bandit:~$
```

figure 4.4

Level 14-15

First, we retrieve the password for the current level. Use the following cat command to retrieve the password.

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHlqxU3b3e
```

figure 4.5

Then connect to the localhost port 30000 using netcat command.

```
bandit14@bandit:~$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHlqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
```

figure 4.6

By submitting the password you got from the level 14, you can successfully login to bandit level 15 as following.

```
bandit14@bandit:~$ exit
logout
Connection to localhost closed.
bandit13@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
pasan@ubuntu:~$ ssh bandit15@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit15@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

figure 4.7

```
For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Enjoy your stay!

bandit15@bandit:~$
```

figure 4.8

