

Tanusha G  
20125

Name: Tanusha Gudise

Roll. No: CH.EN.U4CSE20125

Discord Server: Tanusha Tanu#0880

## TASK 5 [LINUX GAMES]

#OverTheWire Wargames

### TASK

Read the instructions given in the OverTheWire website properly and then find whatever is needed to proceed to next levels. You have to complete upto **level 15**. Submit us a **PROPER PDF** document of the passwords you found along with the screenshots of the passwords.

### SCREENSHOTS OF THE PASSWORDS:

LEVEL 0

Command: ssh [bandit0@bandit.labs.overthewire.org](http://bandit0@bandit.labs.overthewire.org) -p 2220

Password: bandit0

```
tanusha@tanusha-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

  OoT  Wg  M
www.   ver   he   ire.org

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:
```

Tanusha G  
20125

```
* 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
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 usefull tools which you can find
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/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!
```

LEVEL 0 → 1

Command: ssh [bandit0@bandit.labs.overthewire.org](mailto:bandit0@bandit.labs.overthewire.org) -p 2220

Password: boJ9jbbUNNfktd78OOpsqOltutMc3MY1

```
Enjoy your stay!

bandit0@bandit:~$ ls -a
.  ..  .bash_logout .bashrc .profile readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
bandit0@bandit:~$
```

LEVEL 1 → 2

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

Password: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

```
Enjoy your stay!

bandit1@bandit:~$ ls -a
-  .  ..  .bash_logout .bashrc .profile
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$
```

Tanusha G  
20125

LEVEL 2 → 3

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

Password: UmHadQcIWmgdLOKQ3YNgjWxGoRMb5luK

```
Enjoy your stay!

bandit2@bandit:~$ ls -a
.  ..  .bash_logout .bashrc .profile spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQcIWmgdLOKQ3YNgjWxGoRMb5luK
```

LEVEL 3 → 4

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

Password: pIwrPrtPN36QITSp3EQaw936yaFoFgAB

```
Enjoy your stay!

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

LEVEL 4 → 5

Command: ssh [bandit4@bandit.labs.overthewire.org](https://bandit4@bandit.labs.overthewire.org) -p 2220

Password: koReBOKuIDDepwhWk7jZC0RTdopnAYKh

```
Enjoy your stay!

bandit4@bandit:~$ ls -a
.  ..  .bash_logout .bashrc  inhere .profile
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls -a
.  ..  -file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
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$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

Tanusha G  
20125

LEVEL 5 → 6

Command: ssh [bandit5@bandit.labs.overthewire.org](mailto:bandit5@bandit.labs.overthewire.org) -p 2220

Password: DXjZPULLxYr17uwoI01bNLQbtFemEgo7

```
Enjoy your stay!
bandit5@bandit:~$ ls -la
.  .. .bash_logout .bashrc  inhere  .profile
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ ls -la
.  .. maybehere00 maybehere02 maybehere04 maybehere06 maybehere08 maybehere10 maybehere12 maybehere14 maybehere16 maybehere18
.. maybehere01 maybehere03 maybehere05 maybehere07 maybehere09 maybehere11 maybehere13 maybehere15 maybehere17 maybehere19
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

LEVEL 6 → 7

Command: ssh [bandit6@bandit.labs.overthewire.org](mailto:bandit6@bandit.labs.overthewire.org) -p 2220

Password: HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

```
Enjoy your stay!
bandit6@bandit:~$ find / -type f -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/32727/task/32727/fdinfo/6': No such file or directory
find: '/proc/32727/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-bandit5': Permission denied
find: '/run/screen/S-bandit11': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/screen/S-bandit13': Permission denied
find: '/run/screen/S-bandit29': Permission denied
find: '/run/screen/S-bandit1': 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-bandit7': Permission denied
find: '/run/screen/S-bandit16': Permission denied
find: '/run/screen/S-bandit26': Permission denied
find: '/run/screen/S-bandit8': Permission denied
find: '/run/screen/S-bandit15': Permission denied
find: '/run/screen/S-bandit4': Permission denied
find: '/run/screen/S-bandit19': Permission denied
find: '/run/screen/S-bandit31': Permission denied
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-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:~$
```

Tanusha G  
20125

LEVEL 7 → 8

Command: ssh [bandit7@bandit.labs.overthewire.org](mailto:bandit7@bandit.labs.overthewire.org) -p 2220

Password: cvX2JJJa4CFALtqS87jk27qwqGhBM9pIV

```
Enjoy your stay!

bandit7@bandit:~$ ls -a
.  .. .bash_logout .bashrc data.txt .profile
bandit7@bandit:~$ cat data.txt | grep "millionth"
millionth      cvX2JJJa4CFALtqS87jk27qwqGhBM9pIV
bandit7@bandit:~$
```

LEVEL 8 → 9

Command: ssh [bandit8@bandit.labs.overthewire.org](mailto:bandit8@bandit.labs.overthewire.org) -p 2220

Password: UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUHR

```
Enjoy your stay!

bandit8@bandit:~$ ls -a
.  .. .bash_logout .bashrc data.txt .profile
bandit8@bandit:~$ sort data.txt | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUHR
bandit8@bandit:~$
```

LEVEL 9 → 10

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

Password: truKLDjsbJ5g7yyJ2X2R0o3a5HqJFuLk

```
Enjoy your stay!

bandit9@bandit:~$ ls -a
.  .. .bash_logout .bashrc data.txt .profile
bandit9@bandit:~$ strings data.txt | grep -E "=+"
===== the*2i"4
=:G e
===== password
<I=zsGi
Z)====== is
A=|t&E
Zdb=
c^ LAh=3G
*$F=s
&===== truKLDjsbJ5g7yyJ2X2R0o3a5HqJFuLk
S=A.H&^
bandit9@bandit:~$
```

LEVEL 10 → 11

Command: ssh [bandit10@bandit.labs.overthewire.org](mailto:bandit10@bandit.labs.overthewire.org) -p 2220

Password: IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

```
Enjoy your stay!

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



Tanusha G  
20125

LEVEL 11 → 12

Command: ssh [bandit11@bandit.labs.overthewire.org](mailto:bandit11@bandit.labs.overthewire.org) -p 2220

Password: 5Te8Y4drgCRfCx8ugdWuEX8KFC6k2EUu

```
Enjoy your stay!

bandit11@bandit:~$ ls -la
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit11@bandit:~$ cat data.txt | tr 'n-Za-mN-ZA-M' 'a-zA-Z'
The password is 5Te8Y4drgCRfCx8ugdWuEX8KFC6k2EUu
bandit11@bandit:~$
```

LEVEL 12 → 13

Command: ssh [bandit12@bandit.labs.overthewire.org](mailto:bandit12@bandit.labs.overthewire.org) -p 2220

Password: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

```
bandit12@bandit:/tmp/tanusha$ ls
file.gz
bandit12@bandit:/tmp/tanusha$ mv data.txt myfile.txt
mv: cannot stat 'data.txt': No such file or directory
bandit12@bandit:/tmp/tanusha$ mv file.gz myfile.txt
bandit12@bandit:/tmp/tanusha$ ls
myfile.txt
bandit12@bandit:/tmp/tanusha$ file myfile.txt
myfile.txt: empty
bandit12@bandit:/tmp/tanusha$ cat myfile.txt
bandit12@bandit:/tmp/tanusha$ xxd -r myfile.txt > myfile1.bin
bandit12@bandit:/tmp/tanusha$ ls
myfile1.bin  myfile.txt
bandit12@bandit:/tmp/tanusha$ file myfile1.bin
myfile1.bin: empty
bandit12@bandit:/tmp/tanusha$ zcat myfile1.bin > myfile2

gzip: myfile1.bin: unexpected end of file
bandit12@bandit:/tmp/tanusha$ ls
myfile1.bin  myfile2  myfile.txt
bandit12@bandit:/tmp/tanusha$ file myfile2
myfile2: empty
bandit12@bandit:/tmp/tanusha$ bzcat myfile2 > myfile3

bzcat: Compressed file ends unexpectedly;
       perhaps it is corrupted? *Possible* reason follows.
bzcat: Success
       Input file = myfile2, output file = (stdout)

It is possible that the compressed file(s) have become corrupted.
You can use the -tvv option to test integrity of such files.

You can use the 'bzip2recover' program to attempt to recover
data from undamaged sections of corrupted files.

bandit12@bandit:/tmp/tanusha$ ls
myfile1.bin  myfile2  myfile3  myfile.txt
bandit12@bandit:/tmp/tanusha$ file myfile3
myfile3: empty
bandit12@bandit:/tmp/tanusha$ zcat myfile3 > myfile4

gzip: myfile3: unexpected end of file
bandit12@bandit:/tmp/tanusha$ ls
myfile1.bin  myfile2  myfile3  myfile4  myfile.txt
bandit12@bandit:/tmp/tanusha$ cat file9
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
```

Tanusha G  
20125

LEVEL 13 → 14

Command: ssh [bandit14@bandit.labs.overthewire.org](https://bandit14@bandit.labs.overthewire.org) -p 2220

Password: 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

```
Enjoy your stay!
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$
```

LEVEL 14 → 15

Command: ssh [bandit14@bandit.labs.overthewire.org](https://bandit14@bandit.labs.overthewire.org) -p 2220

Password: BfMYroe26WYalil77FoDi9qh59eK5xNr

```
Enjoy your stay!
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$ echo 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e | nc localhost 30000
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
bandit14@bandit:~$
```

LEVEL 15 → 16

Command: ssh [bandit15@bandit.labs.overthewire.org](https://bandit15@bandit.labs.overthewire.org) -p 2220

Password: cluFn7wTiGryunymYOu4RcfftSxQluehd

```
Start Time: 1656129081
Timeout : 7200 (sec)
Verify return code: 18 (self signed certificate)
Extended master secret: yes
...
Correct!
cluFn7wTiGryunymYOu4RcfftSxQluehd
closed
bandit15@bandit:~$
```