

TASK-7

COGNIZANCE-LINUX GAMES

S.V.SIVANANTH

21165

LEVEL 0-1

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd780OpsqOltutMc3MY1
bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Pass: boJ9jbbUNNfktd780OpsqOltutMc3MY1

LEVEL 1-2

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ ls -a
- . .. .bash_logout .bashrc .profile
bandit1@bandit:~$ cat -
^Z
[1]+  Stopped                  cat -
bandit1@bandit:~$ cat ~/*
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ exit
logout
There are stopped jobs.
```

Pass: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

LEVEL 2-3

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ ls -a
. .. .bash_logout .bashrc .profile spaces in this filename
bandit2@bandit:~$ cat ~/*
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Pass: UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

LEVEL 3-4

```
bandit3@bandit:~$ ls
inhere
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$ exit
```

Pass: pIwrPrtPN36QITSp3EQaw936yaFoFgAB

LEVEL 4-5

```
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$ cat -file00
cat: invalid option -- 'f'
Try 'cat --help' for more information.
bandit4@bandit:~/inhere$ find -file06
find: unknown predicate `-file06'
Try 'find --help' for more information.
bandit4@bandit:~/inhere$ grep -file09
grep: ile09: No such file or directory
bandit4@bandit:~/inhere$ ls -file02
ls: invalid option -- 'e'
Try 'ls --help' for more information.
bandit4@bandit:~/inhere$ cat -file07
cat: invalid option -- 'f'
Try 'cat --help' for more information.
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
```

Pass: koReBOKuIDDepwhWk7jZC0RTdopnAYKh

LEVEL 5-6

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

Pass: DXjZPULLxYr17uwoI01bNLQbtFemEgo7

LEVEL 6-7

```
bandit6@bandit:~$ ls -a
.  .. .bash_logout .bashrc .profile
bandit6@bandit:~$ cat ~/*
cat: '/home/bandit6/*': No such file or directory
bandit6@bandit:~$ ls -a
.  .. .bash_logout .bashrc .profile
bandit6@bandit:~$ cd .profile
-bash: cd: .profile: Not a directory
bandit6@bandit:~$ cat .profile
# ~/.profile: executed by the command interpreter for login shells.
# This file is not read by bash(1), if ~/.bash_profile or ~/.bash_login
# exists.
# see /usr/share/doc/bash/examples/startup-files for examples.
# the files are located in the bash-doc package.

# the default umask is set in /etc/profile; for setting the umask
# for ssh logins, install and configure the libpam-umask package.
#umask 022

# if running bash
if [ -n "$BASH_VERSION" ]; then
    # include .bashrc if it exists
    if [ -f "$HOME/.bashrc" ]; then
        . "$HOME/.bashrc"
    fi
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/bin" ] ; then
    PATH="$HOME/bin:$PATH"
fi
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/
backups/      crash      lib/       lock/       mail/       run/       tmp/
cache/        .info22.txt local/      log/        opt/        spool/
bandit6@bandit:~$ cat /var/
backups/      crash      lib/       lock/       mail/       run/       tmp/
cache/        .info22.txt local/      log/        opt/        spool/
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
```

Pass: HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

LEVEL 7-8

```
bandit7@bandit:~$ grep millionth
^Z
[1]+  Stopped                  grep millionth
bandit7@bandit:~$ cat data.txt|grep millionth
millionth      cvX2JJJa4CFALtqS87jk27qwqGhBM9pLV
```

Pass: cvX2JJJa4CFALtqS87jk27qwqGhBM9pLV

LEVEL 8-9

```
flyKxCbHB8uLTaIB5LXqNuJj3yj00eh
w4zUWFGTUraAh8lNkS8gH3WK2zowBEkA
bandit8@bandit:~$ sort data.txt|uniq-u
-bash: uniq-u: command not found
bandit8@bandit:~$ sort data.txt | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhr
bandit8@bandit:~$ exit
```

Pass: UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhr

LEVEL 9-10

```
P'up
\~A:
sCtY
Z/1x+
ej8z
P"'\XZ
1KOA
bandit9@bandit:~$ cat data.txt | strings | grep ^==
===== the*2i"4
===== password
bandit9@bandit:~$ cat data.txt | strings | grep ^=
===== the*2i"4
=:G e
===== password
bandit9@bandit:~$ cat ===== password
cat: '=====': No such file or directory
cat: password: No such file or directory
bandit9@bandit:~$ strings data.txt | grep "="
===== the*2i"4
=:G e
===== password
<I=zsGi
Z)===== is
A=|t8E
Zdb=
c^ LAh=3G
*SF=s
6===== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.H6^
```

Pass: truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

LEVEL 10-11

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhliHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==
bandit10@bandit:~$ base64 --decode
^Z
[1]+  Stopped                  base64 --decode
bandit10@bandit:~$ cat data.txt | base64 --decode
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
```

Pass: IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

LEVEL 11-12

```
bandit11@bandit:~$ ls -a
.  .. .bash_logout .bashrc data.txt .profile
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2Rhh
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z]' '[N-ZA-Mn-za-m]'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
```

Pass: 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

LEVEL 12-13

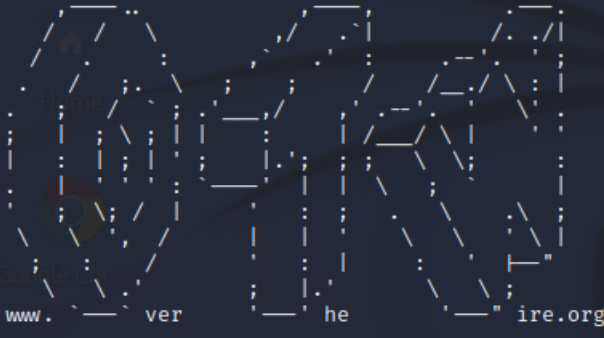
```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ mkdir /tmp/Sivaananth
bandit12@bandit:~$ cp data.txt /tmp/Sivaananth
bandit12@bandit:~$ cd /tmp/Sivaananth
bandit12@bandit:/tmp/Sivaananth$ ls
data.txt
bandit12@bandit:/tmp/Sivaananth$ file data.txt
data.txt: ASCII text
bandit12@bandit:/tmp/Sivaananth$ xxd -r data.txt > data_xxd_reverse
bandit12@bandit:/tmp/Sivaananth$ file data_xxd_reverse
data_xxd_reverse: gzip compressed data, was "data2.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/Sivaananth$ zcat data_xxd_reverse > data_zcat
bandit12@bandit:/tmp/Sivaananth$ file data_zcat
data_zcat: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/Sivaananth$ bzip2 -d data_zcat
bzip2: Can't guess original name for data_zcat -- using data_zcat.out
bandit12@bandit:/tmp/Sivaananth$ file data_zcat.out
data_zcat.out: gzip compressed data, was "data4.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/Sivaananth$ ls
data.txt data_xxd_reverse data_zcat.out
bandit12@bandit:/tmp/Sivaananth$ zcat data_zcat.out > data_zcat_2
bandit12@bandit:/tmp/Sivaananth$ file data_zcat_2
data_zcat_2: POSIX tar archive (GNU)
bandit12@bandit:/tmp/Sivaananth$ tar xvf data_zcat_2
data5.bin
bandit12@bandit:/tmp/Sivaananth$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/Sivaananth$ tar xvf data5.bin
data6.bin
bandit12@bandit:/tmp/Sivaananth$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/Sivaananth$ bzip2 -d data6.bin
bzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/Sivaananth$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/Sivaananth$ tar xvf data6.bin.out
data8.bin
bandit12@bandit:/tmp/Sivaananth$ 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/Sivaananth$ zcat data8.bin > data8_zcat
bandit12@bandit:/tmp/Sivaananth$ file data8_zcat
data8_zcat: ASCII text
bandit12@bandit:/tmp/Sivaananth$ cat data8_zcat
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/Sivaananth$
```

Pass: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

LEVEL 13-14

```
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 SHA256:98UL0ZWr85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
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

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



The logo for OverTheWire is displayed in a large, stylized font. The letters are composed of a grid of small squares, some of which are filled with different colors (red, green, blue, yellow). The logo is set against a dark background with a faint, stylized dragon or dragon-like creature in the background.

```
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:

    * don't leave orphan processes running
    * don't leave exploit-files laying around
```

```

* 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!

bandit14@bandit:~$ cd /etc/bandit_pass/
bandit14@bandit:/etc/bandit_pass$ ls
bandit0  bandit12  bandit16  bandit2  bandit23  bandit27  bandit30  bandit4  bandit8
bandit1  bandit13  bandit17  bandit20  bandit24  bandit28  bandit31  bandit5  bandit9
bandit10  bandit14  bandit18  bandit21  bandit25  bandit29  bandit32  bandit6
bandit11  bandit15  bandit19  bandit22  bandit26  bandit3  bandit33  bandit7
bandit14@bandit:/etc/bandit_pass$ cat bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

```

Pass: 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

LEVEL 14-15

```

bandit14@bandit:~$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr

```

Pass: BfMYroe26WYalil77FoDi9qh59eK5xNr