

## Level 0

```
bandit0@bandit:~$
C:\Users\micha\ssh bandit0@bandit.labs.overthewire.org -p 2220

bandit
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password:
Permission denied, please try again.
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 ]--

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/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice!

* 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, DON'T POST SPOILERS!
This includes writeups of your solution on your blog or website!

--[ Tips ]--
```

## Level 1

```
bandit17@bandit:~$
C:\Users\micha\ssh -i Bandit17.Key.private bandit17@bandit.labs.overthewire.org -p 2220

bandit
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

Welcome to OverTheWire!

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

--[ 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/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice!

* 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, DON'T 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:
```



## Level 4

```
bandit14@bandit:~$
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 64 bit 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/)

--[ 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!

bandit14@bandit:~$ ls
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VweTyk8R0of1qqac8Pa1h7LDCpV5
bandit14@bandit:~$ nc localhost 30000
Wrong! Please enter the correct current password.
MU4VweTyk8R0of1qqac8Pa1h7LDCpV5
bandit14@bandit:~$ nc localhost 30000
MU4VweTyk8R0of1qqac8Pa1h7LDCpV5
Correct!
BxcJmgokbG1HF4Z1G5Tmu4R2tKJQo
```

## Level 5

```
bandit14@bandit:~$
* 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/)

--[ 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!

bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

C:\Users\micha>scp -P 2220 bandit13@bandit.labs.overthewire.org:sshkey.private .

bandit

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit13@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit13@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit13@bandit.labs.overthewire.org's password:
Permission denied (publickey,password).
bandit13@bandit.labs.overthewire.org:
C:\Users\micha>scp -P 2220 bandit13@bandit.labs.overthewire.org:sshkey.private .

bandit

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit13@bandit.labs.overthewire.org's password:
sshkey.private
C:\Users\micha>ssh -i sshkey.private bandit14@bandit.labs.overthewire.org -p 2220

bandit

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
```

## Level 6

```
Command Prompt - scp -P 2222 bandit1@bandit.labs.overthewire.org:shkey private.
bandit1@bandit:~$ cd /tmp; mv 6me7j6lrj5 15
compressed_data.tar data5.bin hexdump_data
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ tar -xf data5.bin
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ 15
compressed_data.tar data5.bin data6.bin hexdump_data
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ xxd data6.bin
00000000: 425e 8139 31a1 5926 3359 affc af1 0000 02091a059...
00000010: 8c7f efd6 6400 0e03 247f e126 5321 8a75  ....iB...[4x
00000020: 21fe 0000 0000 0000 0000 6602 0108 204c  [...]B...L
00000030: 0028 0001 0040 0020 d221 00d0 0010 0c46  ....L...P
00000040: 6519 000a 00f5 150a 0021 0403 000a 01a0  B.....P]B...
00000050: 8c40 c4c8 0008 0c20 071d 8da1 fc81 017c  @...h.P.....
00000060: e010 0072 0075 000a 0000 0000 c45f 0705  ..J...B...
00000070: 0707 0705 9158 00d4 09a1 30e1 020e f1f9  ..7]X...B....
00000080: 00d1 470b 4d38 0126 0c04 4aa0 cda5 afd3  .dPMBLJ...
00000090: c5f0 000e 2144 0a03 0550 0000 200e c0e5  ...D...B....
000000a0: 2c11 20a7 4e7b 5d19 90e7 d27a d800 9487  .+N[.....
000000b0: 0572 1f00 0046 8c2a 0a0b 300e b010 1fe1  .P...P...P..
000000c0: 0101 0102 072c 072b 0002 9a04 2009 beb1  .B...P...P..
000000d0: 0100 fe2e e48a 70a1 215f f95a c2  ....P...P..
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ 15
compressed_data.tar data5.bin data6.bin hexdump_data
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ bzip2 -d data6.bin
bzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ 15
compressed_data.tar data5.bin data6.bin.out hexdump_data
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ tar -xf data6.bin.out
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ 15
compressed_data.tar data5.bin data6.bin.out hexdump_data
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Wed Jul 17 15:57:00 2024, max compression, from Unix, original size modulo 2^32 49
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ 15
compressed_data.tar data5.bin data6.bin.out data8.bin hexdump_data
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ xxd data8.bin
00000000: 1f8b 0000 d1a5 970e 0003 0403 0000 0000  ....f..data9.
00000010: 6260 0000 00c9 4855 2848 2c2e 20cf 2f4a  bin...M(M...../
00000020: 5128 0000 7043 27ad 2002 2002 0000 0000  Q...P...W...M...
00000030: f4cc f410 c800 f012 4e0d c02e 362a 4009  ..8...T...6%..
00000040: 7120 77cc e302 0030 de12 0101 0000 00  qW.....2A1...
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ mv data8.bin
mv: missing destination file operand after 'data8.bin'
Try 'mv --help' for more information.
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ 15
compressed_data.tar data5.bin data6.bin.out data8.bin hexdump_data
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ mv data8.bin data8.bz
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ mv data8.bz data8.gz
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ 15
compressed_data.tar data5.bin data6.bin.out data8.gz hexdump_data
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ gzip -d data8.gz
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ 15
compressed_data.tar data5.bin data6.bin.out data8 hexdump_data
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ file data8
data8: ASCII text
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ cat data8
The password is F0SdWfsc0cbal10H0H8J20K5zvdTDNan
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ CLEAR
CLEAR: command not found
bandit1@bandit:/tmp/tmp.6me7j6lrj5$ exit
logout
```

## Level 7

```
bandit1@bandit:~$
* USERNAMES are somegame0, somegame1, ...
* Host 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 "mkdir -d" in order to generate a random and hard to guess
directory in /tmp/. Read access to both /tmp/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice:

* 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
-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:

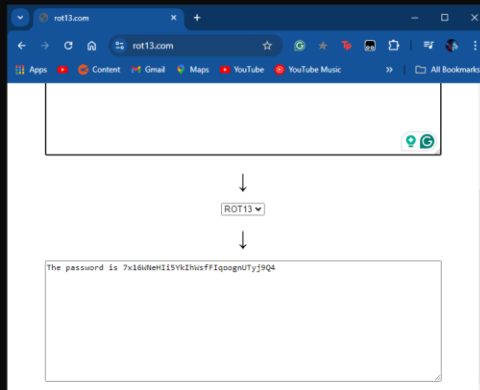
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/lionel/peda.git) in /opt/peda/
* g0blin (https://github.com/g0blin/g0blin) in /opt/g0blin/
* pwnTools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ 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!

bandit1@bandit:~$ 15
data.txt
bandit1@bandit:~$ cat data.txt
Gur cnffjbeq vf 7x16J0ArUVf5LXVJf5SVdbbtarHGlw004
bandit1@bandit:~$
```



## Level 8

```
Command Prompt
Directory is regularly wiped.
Please play nice!

* 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 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/l0ngd/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwn tools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ 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!

bandit@bandit:~$ ls
data.txt
bandit@bandit:~$ cat data.txt
VGH1Hbhc3N3b3JkIGl1IGR0b3R5IEp0Z2a5Zlwl1jREZTR3NhMl13bm80WmoczV3YgCg==
bandit@bandit:~$ base64 -d data.txt
The password is g1rl7fZb6tR5CfScgZRHqNvj3qR
bandit@bandit:~$ cls
Command 'cls' not found, but there are 20 similar ones.
bandit@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
C:\Users\micha\ssh bandit@bandit.labs.overthewire.org -p 2220
```

## Level 9

```
Command Prompt
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/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice!

* 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 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/l0ngd/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwn tools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ 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!

bandit@bandit:~$ ls
data.txt
bandit@bandit:~$ strings data.txt | grep ==
\al;===== the
===== password
===== irc
===== FGdMS1LVJ~>X3K4M7MlN4MgbpH1qey
bandit@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

## Level 10

```
bandit@bandit:~$ 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/lionel0/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/)

--[ 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!

bandit@bandit:~$ ls
data.txt
bandit@bandit:~$ sort data.txt | uniq -u
AC0h11918bUZZP0Qd4n4Lxv4g3M
bandit@bandit:~$
```

## Level 11

```
bandit@bandit:~$
* 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/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice:

* 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 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/lionel0/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/)

--[ 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!

bandit@bandit:~$ ls
data.txt
bandit@bandit:~$ cat data.txt | grep millionth
millionth      dfvzvzQ4mu4vfnbF0e9R0kssK0Lg7eEc
bandit@bandit:~$
```

## Level 12

```
bandit@bandit:~$ cat /etc/somegame_pass/

* 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/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice!

* 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 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/l0ngld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwn tools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ 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!

bandit@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
m0rb1tDk5W6j1lUcYw0QnAlN0lFvAa
bandit@bandit:~$
```

## Level 13

```
bandit@bandit:~/inhere/maybehere07$ cat /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/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice!

* 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 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/l0ngld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwn tools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ 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!

bandit@bandit:~$ find . -type f -size 1033c ! -executable -exec file {} \; | grep "ASCII text"
./inhere/maybehere07/.file2: ASCII text, with very long lines (1000)
bandit@bandit:~$ cd inhere/maybehere07
bandit@bandit:~/inhere/maybehere07$ cat ./file2
H4asnPhqtQAWkeedwK45ny28cvia6G

bandit@bandit:~/inhere/maybehere07$
```

## Level 14

```
bandit@bandit:~/inhere$ ls -la
total 48
drwxr-xr-x 2 root root 4096 Jul 17 15:57 .
drwxr-xr-x 3 root root 4096 Jul 17 15:57 ..
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file00
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file01
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file02
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file03
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file04
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file05
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file06
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file07
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file08
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file09
bandit@bandit:~/inhere$ file -/*
./file00: data
./file01: data
./file02: data
./file03: data
./file04: data
./file05: data
./file06: data
./file07: ASCII text
./file08: data
./file09: data
bandit@bandit:~/inhere$ cat ./-file07
4QYV9kZ0G005Thd1z8$1kx0jQw
bandit@bandit:~/inhere$
```

## Level 15

```
bandit@bandit:~/inhere
* 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 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/lionel/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/)

--[ 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!

bandit@bandit:~$ ls
inhere
bandit@bandit:~$ cd inhere
bandit@bandit:~/inhere$ ls
Command 'ls' not found, did you mean:
  command 'lsd' from snap lsd (0.16.0)
  command 'lsx' from deb suckless-tools (47-1)
  command 'xx' from deb lrsx (0.12.21-10)
  command 'lsim' from deb lsm (1.0.4-2)
  command 'lsc' from deb lvescript (1.8.1vdfsg-3)
  command 'lsd' from deb lsd (0.23.1-3)
  command 'lsh' from deb lsh-client (2.1-14)
  command 'lex' from deb flex (2.6.4-8.2)
  command 'qts' from deb qtscsp (1.5.2-1ubuntu2)
  command 'lyx' from deb lyx (2.3.7-1)
  command 'ls' from deb cowpall (9.4-ubuntu2)
See 'snap info csnapmcs' for additional versions.
bandit@bandit:~/inhere$ ls
... ..Hiding-From-You
bandit@bandit:~/inhere$ ls -a
... ..Hiding-From-You
bandit@bandit:~/inhere$ cat ./...Hiding-From-You
2lweOfRz1q3Pmea8n0h0p9pRf3M3
bandit@bandit:~/inhere$
```



## Level 16

```
bandit@bandit:~$ cat /etc/somegame_pass/

* 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/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice:

* 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 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/)

--[ 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!

bandit@bandit:~$ ls
spaces in this filename
MUKBKNH5Uio41PMUo0OPqFwP15mX
bandit@bandit:~$
```

## Level 17

```
bandit@bandit:~$ cat /etc/somegame_pass/

* 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/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice:

* 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 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/)

--[ 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!

bandit@bandit:~$ ls -a
. . . .bash_logout .bashrc .profile
bandit@bandit:~$ cat ./
263XQZPg6u4KxfvgrM1X9yxc29mfX
bandit@bandit:~$
```

## Level 18

```
bandit@bandit:~$ cat /etc/passwd | grep bandit
bandit:x:1000:1000::/home/bandit:/bin/bash

restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice!

* 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, DON'T 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 useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* nundbg (https://github.com/pwndbg/nundbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* puntools (https://github.com/calloppled/puntools)
* radare2 (http://www.radare.org/)

--[ 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!

bandit@bandit:~$ ls
readme
bandit@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTm6FvvyRnb2rFmQZ0Ta6lp5lf

bandit@bandit:~$ ^C
bandit@bandit:~$ ^C
bandit@bandit:~$
```

## Level 19

```
bandit@bandit:~$ cat /etc/passwd | grep bandit
bandit:x:1000:1000::/home/bandit:/bin/bash

restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice!

* 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, DON'T 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 useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* nundbg (https://github.com/pwndbg/nundbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* puntools (https://github.com/calloppled/puntools)
* radare2 (http://www.radare.org/)

--[ 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!

bandit@bandit:~$ ls
passwords.new  passwords.old
bandit@bandit:~$ diff passwords.old passwords.new
42c42
< b5raCv3vB5xRQ25Gv55n@vc3xgyp
...
> x2gLTtJfWQHQB0aMhB362QKxRq5l0
bandit@bandit:~$
```

**Question 1: Do you think people would leave passwords on a server? Why or why not?**

I think people wouldn't leave passwords on a server as it could lead to a potential breach especially if not secured properly. Whenever passwords are stored on a pc if that pc is hacked then it may lead to a password leak. It is very important not to leave passwords on servers as that could allow for a bad actor to scan the network and exploit your system in that way.

**Question 2: Which level did you find the most challenging? Why?**

I found the level in which I had to decompress a file many times. It was more tedious but after I got the hang of it became very easy. I think during the level it frustrated me but after I got the hang of it and I can say I enjoyed it.

I also found the last level with the private key difficult. I was able to scan the network and find the open ports although, once I did, I struggled in actually getting the file. I had to resort to copying and pasting each line onto a file on my computer to get it to work.

I overall really enjoyed this assignment.