

COGNIZANCE TASKS

TASK 5 [LINUX GAMES]

OVERTHEWIRE WAR GAMES: BANDIT WARGAME

1. LEVEL 0

```
Activities Terminal Jun 24 21:07 • bandit0@bandit:~  
kritchka@kritchka-Laptop:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220 ([176.9.9.172]:2220) can't be established.  
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([176.9.9.172]:2220)' can't be established.  
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRKkLo2x30PhyPS85tB5RPbhczc.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[176.9.9.172]:2220' (ECDSA) to the list of known hosts.  
Connection to 176.9.9.172 port 2220 accepted.  
kritchka@kritchka-Laptop:~$ 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 bandit0.otw.local 5.4.8 x86_64 GNU/Linux  
  
Welcome to OverTheWire!  
If you find any problems, please report them to Steven or m0rla 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 snop 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  
* 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/  
* pwnutils (https://github.com/Gallopsled/pwnutils)  
* 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!  
bandit0@bandit:~$ ls  
readme  
bandit0@bandit:~$ cat readme  
b039jbbUNNFkttd7800psq0ltutMc3MY1  
bandit0@bandit:~$ █
```

```
Activities Terminal Jun 25 22:17 • bandit0@bandit:~  
  
* 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/  
* pwnutils (https://github.com/Gallopsled/pwnutils)  
* 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!  
bandit0@bandit:~$ ls  
readme  
bandit0@bandit:~$ cat readme  
b039jbbUNNFkttd7800psq0ltutMc3MY1  
bandit0@bandit:~$ █
```

PASSWORD FOR LEVEL 1: ***boJ9jbbUNNfktd78OOpsqOltutMc3MYI***

2. LEVEL 1

```
Activities Terminal Jun 24 21:32
kirthika@kirthika-Laptop:~$ 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:
Linux bandit.owt.local 5.4.8 x86_64 GNU/Linux

Welcome to OverTheWire!
If you find any problems, please report them to Steven or mrlor 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 directores 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
* 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 ]--

```

```
Activities Terminal Jun 24 21:36
bandit2@bandit:~

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 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!
bandit1@bandit:~$ ls
bandit1@bandit:~$ cat ./
CV1DtqXWVFTVM2F0k09SHz0YwRINYA9

```

PASSWORD FOR LEVEL 2: ***CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9***

3. LEVEL 2

```
Activities Terminal Jun 24 21:36 •
krithikagkrithika-Laptop:~$ ssh bandit2@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit2@bandit.labs.overthewire.org's password:
Linux bandit.labs.local 5.4.8 x86_64 GNU/Linux

Welcome to OverTheWire!
If you find any problems, please report them to Steven or m0rla 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
* 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 ]--
bandit2@bandit:~
```

```
Activities Terminal Jun 24 21:52 •
Jun 24 21:52 •
bandit2@bandit:~

* 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/
* pwnutils (https://github.com/Gallopsled/pwnutils)
* 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"
UmHadQclWmgdLOKQ3YN0jWxGoRMb5luK
bandit2@bandit:~$ [ ]
```

PASSWORD FOR LEVEL 3: *UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK*

4. LEVEL 3

```
Activities Terminal Jun 24 21:54 •
krithika@krithika-Laptop:~$ ssh bandit3@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit3@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

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 directorties 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
* 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 ]--
bandit3@bandit:~/Inhere
```

```
Activities Terminal Jun 24 21:54 •
bandit3@bandit:~/Inhere
-fno-stack-protector disable ProPolice
-Wl,-z,noexec 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!

bandit3@bandit:~$ ls
Inhere
bandit3@bandit:~$ ls -al
total 24
drwxr-xr-x 3 root root 4096 May  7  2020 .
drwxr-xr-x 41 root root 4096 May  7  2020 ..
-rw-r--r--  1 root root  220 May 15 2017 .bash_logout
-rw-r--r--  1 root root 3526 May 15 2017 .bashrc
drwxr-xr-x  2 root root 4096 May  7  2020 Inhere
-rw-r--r--  1 root root  675 May 15 2017 .profile
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
pIwPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/Inhere$ 
```

PASSWORD FOR LEVEL 4: ***pIwrPrtPN36QITSp3EQaw936yaFoFgAB***

5. LEVEL 4

```
Activities Terminal Jun 24 22:11 •
krithika@krithika-Laptop:~$ ssh bandit4@bandit.labs.overthewire.org -p 2220
bandits@bandit:~/inhere/maybehere07
Jun 24 22:11 •
krithika@krithika-Laptop:~$ ssh bandit4@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit4@bandit.labs.overthewire.org's password:
Linux bandit.tow.local 5.4.0 x86_64 GNU/Linux

Welcome to OverTheWire!
If you find any problems, please report them to Steven or m0rla 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 ports open while 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 ]-
bandits@bandit:~/inhere/maybehere07
```

```
Activities Terminal Jun 24 22:11 •
bandits@bandit:~/inhere/maybehere07
Jun 24 22:11 •
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/
* pwnools (https://github.com/Gallopsled/pwnools)
* 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!

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$ ls -al
total 48
drwxr-xr-x 2 root root 4096 May 7 2020 .
drwxr-xr-x 3 root root 4096 May 7 2020 ..
-rw-r---- 1 bandits bandit4 33 May 7 2020 -file00
-rw-r---- 1 bandits bandit4 33 May 7 2020 -file01
-rw-r---- 1 bandits bandit4 33 May 7 2020 -file02
-rw-r---- 1 bandits bandit4 33 May 7 2020 -file03
-rw-r---- 1 bandits bandit4 33 May 7 2020 -file04
-rw-r---- 1 bandits bandit4 33 May 7 2020 -file05
-rw-r---- 1 bandits bandit4 33 May 7 2020 -file06
-rw-r---- 1 bandits bandit4 33 May 7 2020 -file07
-rw-r---- 1 bandits bandit4 33 May 7 2020 -file08
-rw-r---- 1 bandits bandit4 33 May 7 2020 -file09
bandit4@bandit:~/inhere$ file ./-file0*
./-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$
```

PASSWORD FOR LEVEL 5: *koReBOKuIDDepwhWk7jZC0RTdopnAYKh*

6. LEVEL 5

```
Activities Terminal Jun 24 22:11 •
bandit5@bandit: ~/Inhere/maybehere07

krithika@krithika-Laptop:~$ ssh bandit5@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit5@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

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 directorties 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
* 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 ]--

```

```
Activities Terminal Jun 24 22:15 •
bandit5@bandit: ~/Inhere/maybehere07

-m32          compile for 32bit
-fno-stack-protector  disable ProPolice
-Wl,-z,norelo  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/
* pwnools (https://github.com/Gallopsled/pwnools)
* 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!

bandit5@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  inhere  .profile
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls -a
.  maybehere00  maybehere02  maybehere04  maybehere06  maybehere08  maybehere10  maybehere12  maybehere14  maybehere16  maybehere18
..  maybehere01  maybehere03  maybehere05  maybehere07  maybehere09  maybehere11  maybehere13  maybehere15  maybehere17  maybehere19
bandit5@bandit:~/inhere$ find . -size 1033c
./maybehere07/file2
bandit5@bandit:~/inhere$ cd ./maybehere07
bandit5@bandit:~/inhere/maybehere07$ ls
-file1 -file2 -file3  spaces file1  spaces file2  spaces file3
bandit5@bandit:~/inhere/maybehere07$ cat .file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

PASSWORD FOR LEVEL 6: ***DXjZPULLxYr17uwoI01bNLQbtFemEgo7***

7. LEVEL 6

```
Activities Terminal Jun 24 22:21
krithika@krithika-Laptop:~$ ssh bandit6@bandit.labs.overthewire.org -p 2220
bandit6@bandit:~$ This is an OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit6@bandit.labs.overthewire.org's password:
Linux bandit.labs.local 5.4.8 x86_64 GNU/Linux

Welcome to OverTheWire!
If you find any problems, please report them to Steven or m0rta 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
* don't annoy other players
* don't post passwords or spoilers
* again, DONT POST SPOILERS!
  This includes writings of your solution on your blog or website!
bandit6@bandit:~$
```

```
Activities Terminal Jun 24 22:22
bandit6@bandit:~$ -m32      compile for 32bit
bandit6@bandit:~$ -fno-stack-protector  disable ProPolice
bandit6@bandit:~$ -Wl,-z,noexec  disable retro

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 /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.

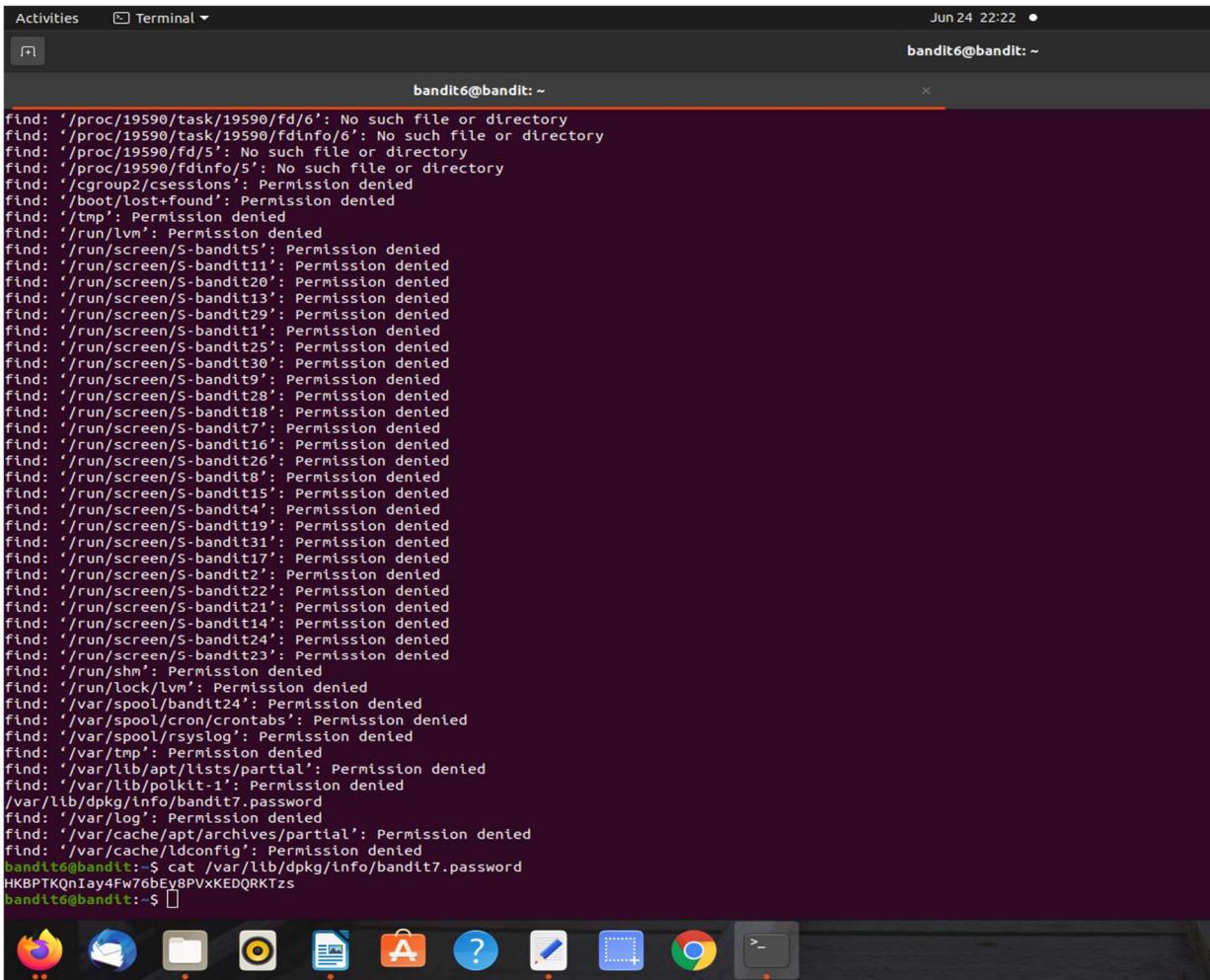
Enjoy your stay!

bandit6@bandit:~$ ls
bandit6@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  .profile
bandit6@bandit:~$ find / -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/lhere': 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: '/svs/fs/pstore': Permission denied
bandit6@bandit:~$
```

Activities Terminal Jun 24 22:22

bandit6@bandit: ~

```
find: '/proc/19590/task/19590/fd/6': No such file or directory
find: '/proc/19590/task/19590/fdinfo/6': No such file or directory
find: '/proc/19590/fd/5': No such file or directory
find: '/proc/19590/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-bandits': 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/syslog': 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: $
```



PASSWORD FOR LEVEL 7: **HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs**

8. LEVEL 7

Activities Terminal Jun 24 22:25

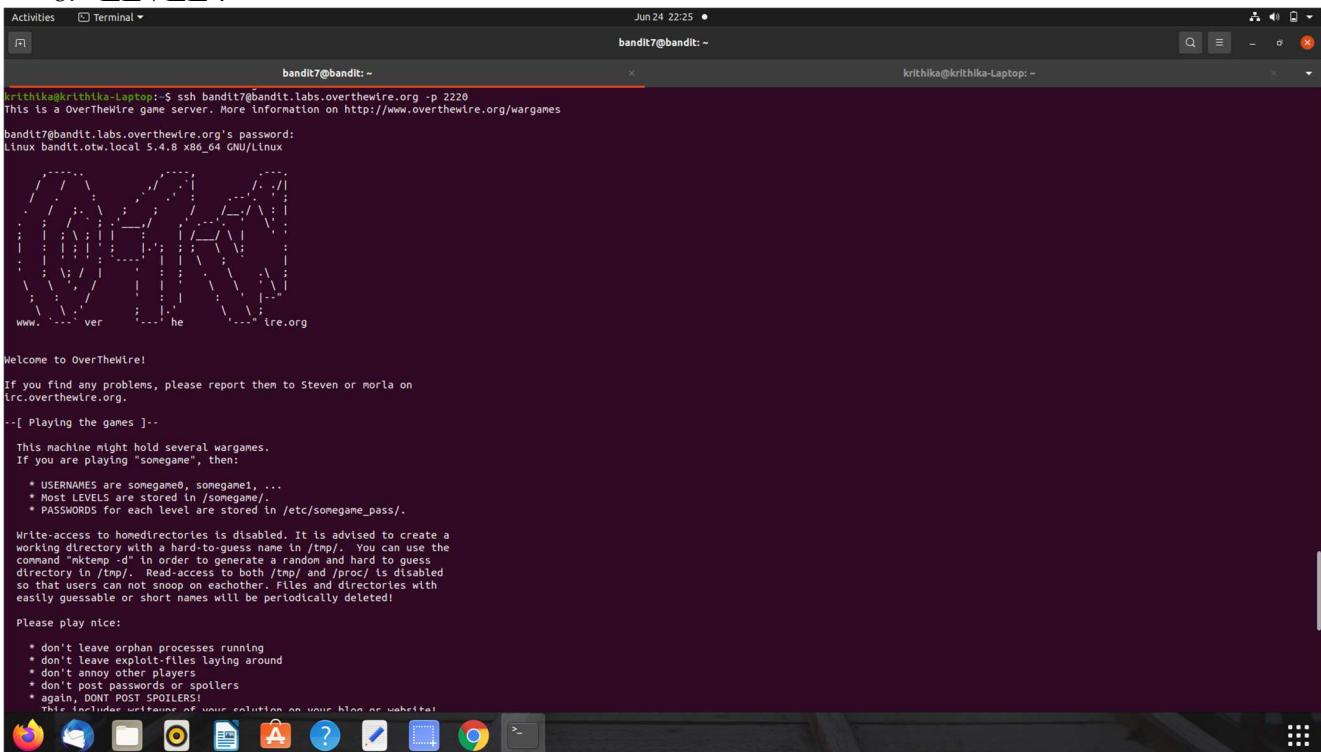
bandit7@bandit: ~

```
krithika@krithika-Laptop: $ ssh bandit7@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit7@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

Welcome to OverTheWire!
If you find any problems, please report them to Steven or m0rta 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
  * don't annoy other players
  * don't post passwords or spoilers
  * again, DONT POST SPOILERS!
  This includes writing of your solution on your blog or website!
```



Activities Terminal Jun 24 22:25 ● bandit7@bandit: ~

```
bandit7@bandit: ~
* 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,noexecro      disable retro

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 /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/
* pwnools (https://github.com/Gallopsled/pwnools)
* 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!
```

bandit7@bandit:~\$ ls
data.txt
bandit7@bandit:~\$ grep "millionth" data.txt
millionth cvX2JJa4CFALTqS87jk27qwqGhBM9plV
bandit7@bandit:~\$

PASSWORD FOR LEVEL 8: *cvX2JJa4CFALTqS87jk27qwqGhBM9plV*

9. LEVEL 8

Activities Terminal Jun 24 22:37 ● bandit8@bandit: ~ krithika@krithika-Laptop: ~/Downloads

```
bandit8@bandit: ~
krithika@krithika-Laptop:~$ ssh bandit8@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit8@bandit.labs.overthewire.org's password:
Linux bandit.owt.local 5.4.8 x86_64 GNU/Linux

Welcome to OverTheWire!
If you find any problems, please report them to Steven or m0rla 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
  * 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!
```

```

Activities Terminal Jun 24 22:37 •
bandit8@bandit: ~

* 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,nowrelro      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/
* pwnutils (https://github.com/Gallopsled/pwnutils)
* 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!

bandit8@bandit:~$ cat data.txt | sort |uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
bandit8@bandit:~$ 
```



PASSWORD FOR LEVEL 9: **UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR**

10. LEVEL 9

```

Activities Terminal Jun 24 22:46 •
bandit9@bandit: ~

krithika@krithika-Laptop:~$ ssh bandit9@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit9@bandit.labs.overthewire.org's password:
Linux bandit.owt.local 5.4.8 x86_64 GNU/Linux

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
* don't annoy other players
* don't post passwords or spoilers
* again, DONT POST SPOILERS!
This forbids writing of your solution on your blog or website!
```



```
Activities Terminal Jun 24 22:46 •
bandit9@bandit: ~
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!

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&^
bandit9@bandit:~$ 
```

PASSWORD FOR LEVEL 10: *truKLDjsbJ5g7yyJ2X2R0o3a5HQJFuLk*

11. LEVEL 10

```
Activities Terminal Jun 24 22:49 •
bandit10@bandit: ~
krithika@krithika-Laptop:~$ ssh bandit10@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit10@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux


```

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
- * 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!

```

Activities Terminal Jun 24 22:49 ●
bandit10@bandit: ~
bandit10@bandit: ~
* 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,noexecro      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/
* pwnools (https://github.com/Gallopsled/pwnools)
* 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!

bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$ 
```



PASSWORD FOR LEVEL 11: ***IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR***

12. LEVEL 11

```

Activities Terminal Jun 24 22:54 ●
bandit11@bandit: ~
bandit11@bandit: ~
krithika@krithika-Laptop:~$ ssh bandit11@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit11@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux



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
* 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!
```



```
Activities Terminal Jun 24 22:54 ●
bandit11@bandit: ~
bandit11@bandit: ~
* 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!

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
bandit11@bandit:~$ 
```



PASSWORD FOR LEVEL 12: **5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu**

13. LEVEL 12

```
Activities Terminal Jun 25 20:58 ●
krithika@krithika-Laptop: ~
krithika@krithika-Laptop: ~
krithika@krithika-Laptop:~$ ssh bandit12@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit12@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

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
* 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!
```



Activities Terminal Jun 25 20:57 krithika@krithika-Laptop: ~

```
 Enjoy your stay!
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ mkdir /tmp/lvl12
bandit12@bandit:~$ cp data.txt /tmp/lvl12
bandit12@bandit:~$ cd /tmp/lvl12
bandit12@bandit:/tmp/lvl12$ ls
data.txt
bandit12@bandit:/tmp/lvl12$ file data.txt
data.txt: ASCII text
bandit12@bandit:/tmp/lvl12$ xxd -r data.txt data1
bandit12@bandit:/tmp/lvl12$ file data1
data1: gzip compressed data, was "data2.bin", last modified: Thu May 7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/lvl12$ mv data1 data2.gz
bandit12@bandit:/tmp/lvl12$ gzip -d data2.gz
bandit12@bandit:/tmp/lvl12$ file data2
data2: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/lvl12$ mv data2 data3.b2z
bandit12@bandit:/tmp/lvl12$ bzip2 -d data3.b2z
bandit12@bandit:/tmp/lvl12$ file data3
data3: gzip compressed data, was "data4.bin", last modified: Thu May 7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/lvl12$ mv data3 data4.gz
bandit12@bandit:/tmp/lvl12$ gzip -d data4.gz
bandit12@bandit:/tmp/lvl12$ file data4
data4: POSIX tar archive (GNU)
bandit12@bandit:/tmp/lvl12$ tar -xvf data4
data5.bin
bandit12@bandit:/tmp/lvl12$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/lvl12$ tar -xvf data5.bin
data6.bin
bandit12@bandit:/tmp/lvl12$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/lvl12$ mv data6.bin data7.b2z
bandit12@bandit:/tmp/lvl12$ bzip2 -d data7.b2z
bandit12@bandit:/tmp/lvl12$ file data7
data7: POSIX tar archive (GNU)
bandit12@bandit:/tmp/lvl12$ tar -xvf data7
data8.bin
bandit12@bandit:/tmp/lvl12$ 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/lvl12$ mv data8.bin data9.gz
bandit12@bandit:/tmp/lvl12$ gzip -d data9.gz
bandit12@bandit:/tmp/lvl12$ file data9
data9: ASCII text
bandit12@bandit:/tmp/lvl12$ cat data9
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
```

PASSWORD FOR LEVEL 13: **8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL**

14. LEVEL 13

Activities Terminal Jun 25 21:21 bandit14@bandit: /etc/bandit_pass

```
krithika@krithika-Laptop:~$ ssh bandit13@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit13@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

Welcome to OverTheWire!
If you find any problems, please report them to Steven or morla on
trc.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 shop on eachother. Files and directores 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
 * don't annoy other players
 * don't post passwords or spoilers
 * again, DONT POST SPOILERS!
 This includes writings of your solution on your blog or website!
```

Activities Terminal Jun 25 21:21

bandit14@bandit: /etc/bandit_pass krithika@krithika-Laptop: ~

```
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/golang/peda.git) in /usr/local/peda/
* gdbinit (https://github.com/overthewire/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!
```

bandit13@bandit:~\$ ls
sshkey.private
bandit13@bandit:~\$ ssh -L 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 SHA256:98UL0z4c85496EtCRKkloz0X30PnyPS8tB5RPbhcz.
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.ottw.local 5.4.8 x86_64 GNU/Linux



Welcome to OverTheWire!
If you find any problems, please report them to Steven or m0rbi on

Activities Terminal Jun 25 21:21

bandit14@bandit: /etc/bandit_pass

```
* 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/golang/peda.git) in /usr/local/peda/
* gdbinit (https://github.com/overthewire/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:~\$ ls -a
. .. .bash_logout .bashrc .profile .ssh
bandit14@bandit:~\$ cd /etc/bandit_pass/
bandit14@bandit:/etc/bandit_pass\$ cat bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:/etc/bandit_pass\$

PASSWORD FOR LEVEL 14: **4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e**

15. LEVEL 14

```
Activities Terminal ▾ Jun 25 21:47 •
R bandit14@bandit: ~
krithika@krithika-Laptop: $ ssh bandit14@bandit.labs.overthewire.org -p 2220
Jun 25 21:47 •
bandit14@bandit.labs.overthewire.org's password:
krithika@krithika-Laptop: ~
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
Linux bandit.owt.local 5.4.8 x86_64 GNU/Linux

Welcome to OverTheWire!
If you find any problems, please report them to Steven or m0rla 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
* don't annoy other players
* don't post passwords or spoilers
* again, DONT POST SPOILERS!
  This includes writing up your solution on your blog or website!
```

```
Activities Terminal ▾ Jun 25 21:47 •
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 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:~\$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDztnTBHiqxU3b3e
bandit14@bandit:~\$ telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^'.
4wcYUJFw0k0XLShlDztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
Connection closed by foreign host.

bandit14@bandit:~\$

PASSWORD FOR LEVEL 15: BfMYroe26WYalil77FoDi9qh59eK5xNr

16. LEVEL 15

```
Activities Terminal Jun 25 22:08
bandit15@bandit: ~
krithika@krithika-Laptop: $ ssh bandit15@bandit.labs.overthewire.org -p 2220
This is an 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

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
* don't annoy other players
* don't post passwords or spoilers
* again, DONT POST SPOILERS!
  This includes writing of your solution on your blog or website!


```

```
Activities Terminal Jun 25 22:09
bandit15@bandit: ~
bandit15@bandit: ~
--[ https ]--

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,relro      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 /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!

bandit15@bandit: $ openssl s_client -connect localhost:30001 -ign_eof
CONNECTED(0x000000)
depth=0 CN = localhost
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = localhost
verify return:1
...
Certificate chain
0 s:/CN=localhost
i:/CN=localhost

```

Activities Terminal ▾ Jun 25 22:09 •

bandit15@bandit: ~

```
subject=/CN=localhost
issuer=/CN=localhost
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 1019 bytes and written 269 bytes
Verification error: self signed certificate
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher   : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 2FAABE3760AB23396527E151C4996CC52BC63FBFB91B3958BD65D6E9E069E0B6
    Session-ID-ctx:
    Master-Key: FAC3952B49A8F9B976803E63C0C2AF8032E03C61B3F386E49272BD3F6BEF65859DD1B910D5329662B752A2D3F23BE85B
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
0000 - d3 53 01 d9 4c 2e 82 50-ef 16 38 c5 d8 1b dd f2 .S..L..P..8.....
0010 - a6 dd 2f 8e 44 91 f8 0a-c8 da 12 4d a6 e4 78 60 .../D.....M..x`...
0020 - 29 db 3d 4f aa 6a 34 49-70 c9 2d 4c e9 bd 1a f4 ).=0.j4Ip..L....
0030 - 34 aa 4e 85 67 99 d9 9e-b7 46 10 42 2c 4b 2f ae 4.N.g....F.B,K/..
0040 - 78 1c 27 66 d5 68 e6 cc-e6 65 e5 92 4b 34 85 1f x.'f.h....e..K4..
0050 - b1 2a 20 1f 65 28 65 a4-d0 cf 13 18 e5 4f 32 28 .* .e(e.....02(
0060 - bf df e2 34 89 6b fc 5e-3a ed c7 0e 21 a9 33 0f ...4.k.^:....!..3.
0070 - c9 87 6e f2 84 97 73 db-a8 85 56 ae 8a 73 ad b5 ...n....s....V...s..
0080 - db e5 8a 58 ca 57 e1 21-fd 1e 92 db 9f 7b e5 a3 ...X.W.!.....{..
0090 - 82 2f 74 9d 23 64 1a d8-db 62 68 2e 3a ca e7 c7 ./t.#d...bh.:.....
Start Time: 1656174926
Timeout   : 7200 (sec)
Verify return code: 18 (self signed certificate)
Extended master secret: yes
---
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd
closed
bandit15@bandit:~$
```



PASSWORD FOR LEVEL 16: **cluFn7wTiGryunymYOu4RcffSxQluehd**