

COGNIZANCE

TASK – 5[LINUX GAMES]

1) Password 1: boJ9jbbUNNfktd7800psq0ltutMc3MY1

```
Activities Terminal Jun 25 08:47
siva@VirtualBox:~$ ssh -p 2220 bandit0@bandit.labs.overthewire.org
This is an OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit0@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
[REDACTED]
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!
```

```
Activities Terminal Jun 25 08:49
bandit0@bandit:~$ 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
boJ9jbbUNNfktd7800psq0ltutMc3MY1
bandit0@bandit:~$ ^C
bandit0@bandit:~$
```

2) Password 2: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

```
Activities Terminal Jun 25 08:59
bandit1@bandit: ~

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!

bandit1@bandit:~$ ls
bandit1@bandit:~$ ls -la
total 24
-rw-r----- 1 bandit2 bandit1 33 May  7 2020 -
drwxr-xr-x  2 root    root   4096 May  7 2020 .
drwxr-xr-x 41 root    root   4096 May  7 2020 ..
-rw-r----- 1 root    root   220 May 15 2017 .bash_logout
-rw-r----- 1 root    root   3526 May 15 2017 .bashrc
-rw-r----- 1 root    root   675 May 15 2017 .profile
bandit1@bandit:~$ cat < -
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$
```

3) Password 3: UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

```
Activities Terminal Jun 25 09:02
bandit2@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/
* 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!

bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat 'spaces in this filename'
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$
```

4) Password 4: pIwrPrtPN36QITSp3EQaw936yaFoFgAB

```
Activities Terminal Jun 25 09:04
bandit3@bandit: ~/Inhere
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!

bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -la
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 bandit3 bandit3   33 May  7  2020 .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$
```

5) Password 5: koReBOKuIDDepwhWk7jZC0RTdopnAYKh

```
Activities Terminal Jun 25 09:20
bandit4@bandit: ~/Inhere
For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Enjoy your stay!

bandit4@bandit:~$ ls
inhere
bandit4@bandit:~/inhere$ ls
-file00  -file02  -file04  -file06  -file08
-file01  -file03  -file05  -file07  -file09
bandit4@bandit:~/inhere$ cat < file00
-bash: file00: No such file or directory
bandit4@bandit:~/inhere$ cat < file00
bandit4@bandit:~/inhere$ clear
// 2fo%o!L-5egooo #####bandit4@bandit:~/inhere$ clear
// 2fo%o!L-5egooo #####bandit4@bandit:~/inhere$ clear
bandit4@bandit:~/inhere$ ls -la
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 bandit5 bandit4   33 May  7  2020 -file00
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file01
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file02
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file03
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file04
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file05
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file06
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file07
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file08
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file09
bandit4@bandit:~/inhere$ cat < -file00
// 2fo%o!L-5egooo #####bandit4@bandit:~/inhere$ cat < -file01
// 2fo%o!L-5egooo #####bandit4@bandit:~/inhere$ cat < -file02
// 2fo%o!L-5egooo #####bandit4@bandit:~/inhere$ cat < -file03
// 2fo%o!L-5egooo #####bandit4@bandit:~/inhere$ cat < -file04
?♦bandit4@bandit:~/inhere$ cat < -file05
?♦bandit4@bandit:~/inhere$ cat < -file06
?♦bandit4@bandit:~/inhere$ cat < -file07
?♦bandit4@bandit:~/inhere$ cat < -file08
?♦bandit4@bandit:~/inhere$ cat < -file09
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

6) Password 6: DXjZPULLxYr17uwoI01bNLQbtFemEgo7

```
Activities Terminal Jun 25 12:45
bandit5@bandit:~/inhere/maybehere07

Enjoy your stay!
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls -la
total 88
drwxr-x--- 22 root bandits 4096 May 7 2020 .
drwxr-xr-x  3 root root  4096 May 7 2020 ..
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere00
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere01
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere02
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere03
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere04
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere05
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere06
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere07
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere08
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere09
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere10
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere11
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere12
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere13
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere14
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere15
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere16
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere17
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere18
drwxr-x---  2 root bandits 4096 May 7 2020 maybehere19
bandit5@bandit:~/inhere$ find . -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cd maybehere07
bandit5@bandit:~/inhere/maybehere07$ cat .file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7

bandit5@bandit:~/inhere/maybehere07$
```

7) Password 7: HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

```
Activities Terminal Jun 25 13:05
bandit6@bandit:~$ ls
bandit6@bandit:~$ cd ..
bandit6@bandit:~/home$ cd ..
bandit6@bandit:~/$ ls
bin cgroup2 etc initrd.img lib lib64 lost+found mnt proc root sbin srv var vmlinuz vmlinuz.old
boot dev home initrd.img.old lib32 libx32 media opt README.txt run share sys usr vmlinuz
bandit6@bandit:~/$ find . -size 33c | find -group bandit6 | find -user bandit7
find: './root': Permission denied
find: './home/bandit28-git': Permission denied
find: './root': Permission denied
find: './home/bandit30-git' find: './home/bandit28-git': Permission denied
: Permission denied
find: './home/bandit30-git': Permission deniedfind: './home/bandit5/inhere': Permission denied
find: './home/bandit27-git': Permission denied
find: './home/bandit30-git': Permission denied
find: './home/bandit29-git': Permission denied
find: './home/bandit31-git': Permission denied
find: './root': Permission denied
find: './home/bandit28-git': Permission denied
find: './home/bandit5/inhere': Permission denied
find:
find: './home/bandit27-git': Permission denied
find: './home/bandit30-git': Permission denied
find: './home/bandit29-git': Permission denied
find: './home/bandit31-git': Permission denied
./home/bandit5/inhere': Permission denied
find: './home/bandit27-git': Permission denied
find: './home/bandit29-git': Permission denied
find: './lost+found': Permission denied
find: './etc/ssl/private': Permission denied
find: './etc/polkit-1/localauthority': Permission denied
find: './etc/vm/archive': Permission denied
find: './etc/vm/backup': Permission denied
find: './lost+found': Permission denied
./dev/pts/42
find: './lost+found': Permission denied
./etc/bandit_pass/bandit7
find: './etc/ssl/private': Permission denied
find: './etc/ssl/private': Permission denied
find: find: './etc/polkit-1/localauthority': Permission denied
find: './etc/polkit-1/localauthority': Permission denied
```

```
Activities Terminal Jun 25 13:10
bandit6@bandit: /  
  
find: './run/screen/S-bandit': 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-bandit8': Permission denied  
./run/screen/S-bandit  
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-bandit5': Permission denied  
find: './run/screen/S-bandit4': Permission denied  
find: './run/screen/S-bandit9': Permission denied  
find: './run/screen/S-bandit11': Permission denied  
find: './run/screen/S-bandit17': Permission denied  
find: './run/screen/S-bandit2': Permission denied  
find: './run/screen/S-bandit22': Permission denied  
find: './run/screen/S-bandit21': Permission denied  
find: './run/screen/S-bandit14': Permission denied  
find: './run/screen/S-bandit24': Permission denied  
find: './run/screen/S-bandit23': Permission denied  
find: './run/shm' Permission denied  
find: './run/lock/lvm': Permission denied  
find: './var/spool/bandit24': Permission denied  
find: './var/spool/cron/crontabs': Permission denied  
find: './var/spool/rsyslog': Permission denied  
find: './var/tmp': Permission denied  
find: './var/lib/apt/lists/partial': Permission denied  
find: './var/lib/polkit-1': Permission denied  
.var/lib/dpkg/info/bandit7.password  
find: './var/log': Permission denied  
find: './var/cache/apt/archives/partial': Permission denied  
find: './var/cache/ldconfig': Permission denied  
find: './boot/lost+found': Permission denied  
find: './tmp': Permission denied  
find: './run/lvm': Permission denied  
find: './run/screen/S-bandit5': Permission denied  
bandit6@bandit: $ cat ./var/lib/dpkg/info/bandit7.password  
HKBP7KQnIay4Fw76bEY8PVxKEDQRKTzS  
bandit6@bandit: $
```

8) Password 8: cvX2JJJa4CFALtqS87jk27qwqGhBM9plV

```
Activities Terminal Jun 25 13:30
bandit7@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 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://irc.overthewire.org #wargames.  
  
Enjoy your stay!  
bandit7@bandit: $ ls  
data.txt  
bandit7@bandit: $ grep -h 'millionth' data.txt  
millionth cvX2JJJa4CFALtqS87jk27qwqGhBM9plV  
bandit7@bandit: ~$
```

9) Password 9: UsVvYfSfZZWbi6wgC7dAFyFuR6jQQUhR

```
Activities Terminal Jun 25 14:22
bandit8@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/
* 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!
bandit8@bandit: $ ls
data.txt
bandit8@bandit: $ cat data.txt | sort | uniq -u
UsVvYfSfZZWbi6wgC7dAFyFuR6jQQUhR
bandit8@bandit: $
```

10) Password 10: truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

```
Activities Terminal Jun 25 14:35
bandit9@bandit: ~

-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/pwendbg/pwendbg) in /usr/local/pwendbg/
* 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!
bandit9@bandit: $ ls
data.txt
bandit9@bandit: $ strings data.txt | grep -E "===="
===== the*21^4
===== password
Z)=====
&===== is
&===== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
bandit9@bandit: $
```

11) Password 11: IFukwKGsFW8M0q3IRFqrxE1hxTNEbUPR

```
Activities Terminal Jun 25 14:42
bandit10@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/
* 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:~$ ls
data.txt
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8M0q3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$
```

12) Password 12: 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

```
Activities Terminal Jun 25 14:54
bandit11@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/
* 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!

bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5GrBL4qetPEsPk8htqjhRK8XSP6x2RHh
bandit11@bandit:~$ cat data.txt | tr 'a-zA-Z' 'n-za-mN-ZA-M'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
bandit11@bandit:~$
```

13) Password 13: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

```
Activities Terminal Jun 26 10:52
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ mkdir /tmp/MyFolder
bandit12@bandit:~$ cp data.txt /tmp/MyFolder
bandit12@bandit:~$ cd ..
bandit12@bandit:/home$ cd ..
bandit12@bandit:$ cd /tmp/MyFolder
bandit12@bandit:$ ls
data.txt
bandit12@bandit:/tmp/MyFolder$ mv data.txt dumpfile.txt
bandit12@bandit:/tmp/MyFolder$ ls
dumpfile.txt
bandit12@bandit:/tmp/MyFolder$ xxd -r dumpfile.txt dump.txt
bandit12@bandit:/tmp/MyFolder$ ls
dumpfile.txt dump.txt
bandit12@bandit:/tmp/MyFolder$ cat dump.txt
P^data2.bin=++BZh1aY8SY0++++@Vee?}++^ooooooooooooo;+0`0ooheF+Fee4LM
@eozeeoFM+eCehF+eC@+4@F+eo
4hh+=C%=>X,,keeee1eeGye+hPhoMh
@Je+=Ole+[RBp+Qix+YeZ!de+j+e@F#eAe#eAeFee8P+e+e`+\"3+
+deebX++zeo<eeA en}
S(3A+=
W@R+eeee6eXS{+
@@9?LePoyB+=+z@?+L@Nt+@7(qP@@%&@w9+qm4++ N3@6+@K+H@+!+!
bandit12@bandit:/tmp/MyFolder$ ls
dumpfile.txt
bandit12@bandit:/tmp/MyFolder$ xxd -r dumpfile.txt dump
bandit12@bandit:/tmp/MyFolder$ file dump
dump: gzip compressed data, was "data2.bin", last modified: Thu May 7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/MyFolder$ mv dump dump1
bandit12@bandit:/tmp/MyFolder$ ls
dump1 dumpfile.txt
bandit12@bandit:/tmp/MyFolder$ gzip -d dump1
gzip: dump1: unknown suffix -- ignored
bandit12@bandit:/tmp/MyFolder$ gzip -d dump1.gz
gzip: dump1.gz: no such file or directory
bandit12@bandit:/tmp/MyFolder$ tar -xvf dump1
tar: This does not look like a tar archive
tar: Skipping to next header
tar: Exiting with failure status due to previous errors
bandit12@bandit:/tmp/MyFolder$ rm dump.txt
```

```
Activities Terminal Jun 26 10:56
bandit12@bandit:~$ ls
dump1 dumpfile.txt
bandit12@bandit:/tmp/MyFolder$ mv dump1 dump1.gz
bandit12@bandit:/tmp/MyFolder$ gzip -d dump1.gz
bandit12@bandit:/tmp/MyFolder$ ls
dump1 dumpfile.txt
bandit12@bandit:/tmp/MyFolder$ file dump1
dump1: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/MyFolder$ mv dump1 dump1.bz2
bandit12@bandit:/tmp/MyFolder$ bzip2 -d dump1.bz2
bandit12@bandit:/tmp/MyFolder$ ls
dump1 dumpfile.txt
bandit12@bandit:/tmp/MyFolder$ file dump1
dump1: gzip compressed data, was "data4.bin", last modified: Thu May 7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/MyFolder$ mv dump1 dump1.gz
bandit12@bandit:/tmp/MyFolder$ gzip -d dump1.gz
bandit12@bandit:/tmp/MyFolder$ file dump1
dump1: POSIX tar archive (GNU)
bandit12@bandit:/tmp/MyFolder$ mv dump1 dump1.xvf
bandit12@bandit:/tmp/MyFolder$ mv dump1 dump1.tar
mv: cannot stat 'dump1': No such file or directory
bandit12@bandit:/tmp/MyFolder$ ls
dump1.xvf dumpfile.txt
bandit12@bandit:/tmp/MyFolder$ mv dump1client loop: send disconnect: Broken pipe
stiva@VirtualBox:~$ ssh -p 2220 bandit12@bandit.labs.overthewire.org
This is an 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

      /-' \ : / , /' . | / . /'- . / \ |
      / ; \ ; / ; / ; / ; / ; / ; / ; / \ |
      ; | ; | ; | ; | ; | ; | ; | ; | ; | ; / |
      ; | ; | ; | ; | ; | ; | ; | ; | ; | ; | ; / |
      ; | ; | ; | ; | ; | ; | ; | ; | ; | ; | ; / |
      ; | ; | ; | ; | ; | ; | ; | ; | ; | ; | ; / |
```

```

Activities Terminal Jun 26 10:56
bandit12@bandit:~/tmp/MyFolder
```

Enjoy your stay!

```

bandit12@bandit:~$ cd /tmp/MyFolder
bandit12@bandit:/tmp/MyFolder$ ls
dump1.xvf dumpfile.txt
bandit12@bandit:/tmp/MyFolder$ mv dump1.xvf dump1.tar
bandit12@bandit:/tmp/MyFolder$ tar -xvf dump1.tar
data5.bin
bandit12@bandit:/tmp/MyFolder$ cat data5.bin
data6.bin|000064400000000000000000000000003361365505000601247 0star rootrootBZh91AY&SY
+   *@@@Y@@@U@@@Zet!>@@@o
@@@A@@@Z<jA@@@j
@@@B@@@E@@@f@@@z@@@G@@@)+@@@P(f)@@@@@@@@Tj@@@P@@@E@@@T@@@o@@@=@@@S@@@*@@@A@@@Y@@@*@@@I@@@+@@@S@@@*@@@E@@@S@@@)+@@@B@@@0@@@,bandit12@bandit:/tmp/MyFolder$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/MyFolder$ mv data5.bin data5.tar
bandit12@bandit:/tmp/MyFolder$ tar -xvf data5.tar
data6.bin
bandit12@bandit:/tmp/MyFolder$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/MyFolder$ mv data6.bin data6.bz2
bandit12@bandit:/tmp/MyFolder$ bzip2 -d data6.bz2
bandit12@bandit:/tmp/MyFolder$ ls
data5.tar data6 dump1.tar dumpfile.txt
bandit12@bandit:/tmp/MyFolder$ file data6
data6: POSIX tar archive (GNU)
bandit12@bandit:/tmp/MyFolder$ mv data6 data6.tar
bandit12@bandit:/tmp/MyFolder$ tar -xvf data6.tar
data8.bin
bandit12@bandit:/tmp/MyFolder$ 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/MyFolder$ mv data8.bin data8.gz
bandit12@bandit:/tmp/MyFolder$ gzip -d data8.gz
bandit12@bandit:/tmp/MyFolder$ ls
data5.tar data6.tar data8 dump1.tar dumpfile.txt
bandit12@bandit:/tmp/MyFolder$ file data8
data8: ASCII text
bandit12@bandit:/tmp/MyFolder$ cat data8
The password is 8ZjyCr1BNFVneahHwxCv3wb2a10RpYL
bandit12@bandit:/tmp/MyFolder$
```

14) Password 14: 4wCYUJFw0k0XLShlDzztnTBHiqxU3b3e

```

Activities Terminal Jun 26 16:16
bandit14@bandit:~/etc/bandit_pass
```

```

bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ cat sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEpaIBAAKCAQEAxk0E83W2c0T7IWfc9aPaaQM0DgzuXcv+ppZHa++buSkN+
gg0tcr7FWNLGq5+UzeC2rEq0Wnneeb13AIoYp0ZYETq46t+jk9puNwZwIt9xgB
ZufGTzEwBFlw/vLNwOxBe4WStcRwzgPpEe5vTb1jLz1BdGphTIK22amZ6g
ThMsImyJaFeWj/18PQ03ny591vUHeuOMaZoUId4K4NOMEZ3+xahyK0HJvg68KsV
ObefxG1vAv3CA29KxJaqRfgYnqzrWn7w3CHJN4Uc/23kp+n8L0SnxaNA+YyA7
jiPyTF0lsuzMLY0411Lzh/8MpvhCOf8r22dwIDQAABAoIBAQCC6dWBjhYoEzjeA
j3j/RwmmapM5zfTj/wb2bfidNpwbB8rsJ4sZTDZ07XuIh4lfyogaQS+bbw3RxVzf
pvJt3Smu8hIDuLscj1.1VnBV5pYBju8g8ar/3FyjyNaqx/TlfzLYf0u7i93jt67
xAh0tONG/18FB5I3LA12Vp60vtwdWeC4n0xCth1dpUKNLA8rMMVRTKQ+7T2VS
nXnwYckKUcUgozvSp1Nz50zDydpdy2+tRH3Mqa5kq11KjvF8RC47woOYcKtsD
o3FpgNFe91aa3Msy+DfQohKZFK1L3bJD0NtmrVvtYK40/yeu4aZ/HAD2Qzwhe
o1AfTeAoGBAOAnjosBkn7sb1k+n+41EpPx5s0mhpnTUDy5WGrpsCrXomsV1BuF
laL3Qlx3C1wtCnEu89DvNHzkupc/h6nTKU1YqlqxyLD8njjTrBrhgbC90rK+F
M1F2F5TxVgPtZDlMw4NR04xHA/fkbhbxXYMoHNTNHnbhb3McdURjaocBANKU
1hgfwnw7+axNcJ9bjysr1zbqoESNd8AfqwaKuGTVXNsUoNcmld0p+*Fak40H
PKNkJNdbG+ex0h9JNQsTK3x5PBMAS8xAoGrKeuKhA6erytVTqJofVcdp5+z9s
8DtVcxDuVsM+i4X8UqIG0tVcbtKEVokHPXPiQ/dAgAcHg5YX7WEehCgCYTzp0+
xysBSCM2G6xuZ3MqUAXwkhNGZvheosGy9t0dANzkw7mUUFVtaCMR/t54H
GC83s0s3D7nsMj8x3Ndo8xft7Dta245Tva0q7Kmnp5g/SCKCw43eiLava+J
3btvJeSIU-82Xg9XjPrpkUcgYA7z6l1Q0KxxNeXh3gHxnRokB5maJ5fNpDBy
idkyZ8ySF8GLcfksyBw6FwCqfG3zDroh193meSbh7SadkwzhevCs9t4vby
9/8x4j5OP8ibfCK54nBP+dT81kkqg5Z5MohxBORA7Wvx+Ac0h0dEkpr0+32xe0
qT1EvQKBgDKm6ws2ByvSu9vGjTilCaJ0evYzRpA6f+Gw/UVAPV4c+S0
kAlpXb5tbkkzb50eaLPTKqLzavXtQoTtkwrlpoLHKIHUz6Nu+n4abfAIRFub0dN
/+aLrQ0yBDRbdXMsZN/jv44eM+rLrdRVyMndPtp8belRi2E2aEza=
-----END RSA PRIVATE KEY-----
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
Could not create directory '/home/bandit13/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL02Wr85496EtCRKklo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
```

Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

```
Activities Terminal Jun 26 16:16
bandit14@bandit: /etc/bandit_pass

-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/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
* checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

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

Enjoy your stay!

bandit14@bandit:~$ cd /etc/bandit_pass/
bandit14@bandit:/etc/bandit_pass$ ls
bandit0 bandit10 bandit12 bandit14 bandit16 bandit18 bandit2 bandit21 bandit23 bandit25 bandit27 bandit29 bandit30 bandit32 bandit4 bandit6 bandit8
bandit1 bandit11 bandit13 bandit15 bandit17 bandit19 bandit20 bandit22 bandit24 bandit26 bandit28 bandit3 bandit31 bandit33 bandit5 bandit7 bandit9
bandit14@bandit:/etc/bandit_pass$ cat bandit14
4wcYUJFw0k0XLshIDzztnTBHiqxU3b3e
bandit14@bandit:/etc/bandit_pass$ ^C
bandit14@bandit:/etc/bandit_pass$
```

15) Password 15: BfMYroe26WYalil77FoDi9qh59eK5xNr

```
Activities Terminal Jun 26 16:20
bandit14@bandit: ~

-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/pwendbg/pwendbg) in /usr/local/pwendbg/
* 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:~$ telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^'.
4wcYUJFw0k0XLshIDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
Connection closed by foreign host.
bandit14@bandit:~$
```