

Sree Chandana.M

CH.EN.U4CSE20042

Commands: ssh

Level 0

Password: bandit0

```
sree@sree-VirtualBox:~/Desktop$ ssh bandit0@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

      _/\_ \_/\_ \_/\_ \_/\_ \_/\_ \_/\_ \_/\_ \_/\_ \_/\_ \_/\_ \_/\_ \_/\_ \_/\_ \_/\_
     /  \ /  \ /  \ /  \ /  \ /  \ /  \ /  \ /  \ /  \ /  \ /  \ /  \ /  \ /  \ /  \ /  \
    /  ; \ /  ; \ /  ; \ /  ; \ /  ; \ /  ; \ /  ; \ /  ; \ /  ; \ /  ; \ /  ; \ /  ;
   /  : \ /  : \ /  : \ /  : \ /  : \ /  : \ /  : \ /  : \ /  : \ /  : \ /  : \ /  :
  /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \
 /  ; \ \ /  ; \ \ /  ; \ \ /  ; \ \ /  ; \ \ /  ; \ \ /  ; \ \ /  ; \ \ /  ; \ \ /  ; \ \
\  : \ \ /  : \ \ /  : \ \ /  : \ \ /  : \ \ /  : \ \ /  : \ \ /  : \ \ /  : \ \ /  : \ \
\  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \ /  \ \
www.----ver----he----"ire.org

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 ]--

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,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 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!
```

Level 0 → Level 1

```
bandit0@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  2 root      root      4096 May  7  2020 .
4 drwxr-xr-x  41 root      root      4096 May  7  2020 ..
4 -rw-r--r--  1 root      root      220 May 15 2017 .bash_logout
4 -rw-r--r--  1 root      root     3526 May 15 2017 .bashrc
4 -rw-r--r--  1 root      root      675 May 15 2017 .profile
4 -rw-r----- 1 bandit1 bandit0   33 May  7  2020 readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd780OpsqOltutMc3MY1
bandit0@bandit:~$
```

```
bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
sree@Sree-VirtualBox:~/Desktop$ 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.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!

--[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 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 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/Gallopsled/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!

Password: boJ9jbbUNNfktd780OpsqOltutMc3MY1

Level 1 → Level 2

```
banditi@bandit:~$ ls -alps
total 24
4 -rw-r----- 1 bandit2 bandit1 33 May 7 2020 -
4 drwxr-xr-x 2 root root 4096 May 7 2020 ../
4 drwxr-xr-x 41 root root 4096 May 7 2020 ...
4 -rw-r--r-- 1 root root 220 May 15 2017 .bash_logout
4 -rw-r--r-- 1 root root 3526 May 15 2017 .bashrc
4 -rw-r--r-- 1 root root 675 May 15 2017 .profile
banditi@bandit:~$ cat ./
CV1DtqXWVFTvM2F0k09SHz0YwRINYA9
L...j...ch...d...t...c...
```

```
banditi@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
sree@sree-VirtualBox:~/Desktop$ 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.otw.local 5.4.8 x86_64 GNU/Linux

          _/\_      _/\_      _/\_      _/\_
         / \ \    / \ \    / \ \    / \ \
        ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
       ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
      ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
     ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
    \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ ;
   ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
  www. --- ver     --- he     \--- ire.org

Welcome to OverTheWire!

If you find any problems, please report them to Steven or morla on
irc.overthewire.org.

--[ Playing the games ]--

This machine might hold several wargames.
If you are playing "somegame", then:

 * USERNAMEs are somegame0, somegame1, ...
 * Most LEVELS are stored in /somegame/.
 * PASSWORDs for each level are stored in /etc/somegame_pass/.

Write-access to homedirectories is disabled. It is advised to create a
working directory with a hard-to-guess name in /tmp/. You can use the
command "mktemp -d" in order to generate a random and hard to guess
directory in /tmp/. Read-access to both /tmp/ and /proc/ is disabled
so that users can not snoop on eachother. Files and directories with
easily guessable or short names will be periodically deleted!

Please play nice!
```

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

Password: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

Level 2 → Level 3

```
bandit2@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  2 root      root      4096 May  7  2020 .
4 drwxr-xr-x 41 root      root      4096 May  7  2020 ..
4 -rw-r--r--  1 root      root       220 May 15 2017 .bash_logout
4 -rw-r--r--  1 root      root      3526 May 15 2017 .bashrc
4 -rw-r--r--  1 root      root       675 May 15 2017 .profile
4 -rw-r----- 1 bandit3  bandit2    33 May  7  2020 spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
```

```
bandit2@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
sree@sree-VirtualBox:~/Desktop$ 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.owt.local 5.4.8 x86_64 GNU/Linux

          _/\_ \_/\_ \_/\_ \_/\_ \_/\_ \_/\_ \_/\_ \_/\_
         / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ 
        / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ 
       / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ 
      / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ 
     / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ 
    / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ 
   / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ 
  / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ 
 / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ / \ \ 
www.--- ver     --- he     ---" ire.org

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 ]--

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 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!
```

Password: UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

Level 3 → Level 4

```
bandit3@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root root 4096 May  7  2020 .
4 drwxr-xr-x 41 root root 4096 May  7  2020 ..
4 -rw-r--r--  1 root root  220 May 15 2017 .bash_logout
4 -rw-r--r--  1 root root 3526 May 15 2017 .bashrc
4 drwxr-xr-x  2 root root 4096 May  7  2020 inhere/
4 -rw-r--r--  1 root root  675 May 15 2017 .profile
bandit3@bandit:~$ cat inhere/
cat: inhere/: Is a directory
bandit3@bandit:~$ cd inhere/
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
pIwrPrtpN36QITSp3EQaw936yaFoFgAB
```

```
* 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!
```

Password: plwrPrtPN36QITSp3EQaw936yaFoFgAB

Level 4 → Level 5

```
bandit4@bandit:~$ ls -alps
total 24
4 drwxr-xr-x 3 root root 4096 May  7 2020 ./
4 drwxr-xr-x 41 root root 4096 May  7 2020 ../
4 -rw-r--r-- 1 root root 220 May 15 2017 .bash_logout
4 -rw-r--r-- 1 root root 3526 May 15 2017 .bashrc
4 drwxr-xr-x 2 root root 4096 May  7 2020 inhere/
4 -rw-r--r-- 1 root root 675 May 15 2017 .profile
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ find . -type f | xargs file
./file01: data
./file00: data
./file06: data
./file03: data
./file05: data
./file08: data
./file04: data
./file07: ASCII text
./file02: data
./file09: data
bandit4@bandit:~/inhere$ man xarg
No manual entry for xarg
bandit4@bandit:~/inhere$ man xargs
bandit4@bandit:~/inhere$ cat ./file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

XARGS(1)	General Commands Manual	XARGS(1)
NAME	xargs - build and execute command lines from standard input	
SYNOPSIS	xargs [-0ptrx] [-E eof-str] [-e[eof-str]] [--eof[=eof-str]] [--null] [-d delimiter] [--delimiter delimiter] [-I replace-str] [-i[replace-str]] [--replace[-replace-str]] [-l[max-lines]] [-L max-lines] [-max-lines=max-lines] [-n max-args] [--max-args=max-args] [-s max-chars] [--max-chars=max-chars] [-P max-procs] [--max-procs=max-procs] [--process-slot-var=name] [--interactive] [--verbose] [--exit] [--no-run-if-empty] [--arg-file=file] [--show-limits] [--verston] [--help] [command [initial-arguments]]	
DESCRIPTION	This manual page documents the GNU version of xargs. xargs reads items from the standard input, delimited by blanks (which can be protected with double or single quotes or a backslash) or newlines, and executes the command (default is /bin/echo) one or more times with any initial-arguments followed by items read from standard input. Blank lines on the standard input are ignored.	
	The command line for command is built up until it reaches a system-defined limit (unless the -n and -L options are used). The specified command will be invoked as many times as necessary to use up the list of input items. In general, there will be many fewer invocations of command than there were items in the input. This will normally have significant performance benefits. Some commands can usefully be executed in parallel too; see the -P option.	
	Because Unix filenames can contain blanks and newlines, this default behaviour is often problematic; filenames containing blanks and/or newlines are incorrectly processed by xargs. In these situations it is better to use the -0 option, which prevents such problems. When using this option you will need to ensure that the program which produces the input for xargs also uses a null character as a separator. If that program is GNU find for example, the -print0 option does this for you.	
	If any invocation of the command exits with a status of 255, xargs will stop immediately without reading any further input. An error message is issued on stderr when this happens.	
OPTIONS		
-0, --null	Input items are terminated by a null character instead of by whitespace, and the quotes and backslash are not special (every character is taken literally). Disables the end of file string, which is treated like any other argument. Useful when input items might contain white space, quote marks, or backslashes. The GNU find -print0 option produces input suitable for this mode.	
-a file, --arg-file=file	Read items from file instead of standard input. If you use this option, stdin remains unchanged when commands are run. Otherwise, stdin is redirected from /dev/null.	
--delimiter=delim, -d delim	Input items are terminated by the specified character. The specified delimiter may be a single character, a C-style character escape such as \n, or an octal or hexadecimal escape code. Octal and hexadecimal escape codes are understood as for the printf command. Multibyte characters are not supported. When processing the input, quotes and backslash are not special; every character in the input is taken literally. The -d option disables any end-of-file string, which is treated like any other argument. You can use	
Manual page xargs(1) line 1 (press h for help or q to quit)		

```
bandit4@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
sree@ree-VirtualBox:~/Desktop$ ssh bandit5@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit5@bandit.labs.overthewire.org's password:
Linux bandit.owt.local 5.4.8 x86_64 GNU/Linux

[...]
www. .... ver     ... he     ... ire.org

Welcome to OverTheWire!

If you find any problems, please report them to Steven or morla on
irc.overthewire.org.

--[ Playing the games ]--

This machine might hold several wargames.
If you are playing "somegame", then:

* USERNAMEs are somegame0, somegame1, ...
* Most LEVELS are stored in /somegame/
* PASSWORDs for each level are stored in /etc/somegame_pass/.

Write-access to homedirectories is disabled. It is advised to create a
working directory with a hard-to-guess name in /tmp/. You can use the
command "mktemp -d" in order to generate a random and hard to guess
directory in /tmp/. Read-access to both /tmp/ and /proc/ is disabled
so that users can not snoop on eachother. Files and directories with
easily guessable or short names will be periodically deleted!

Please also note:
* 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!
```

Password: koReBOKuIDDepwhWk7jZCORTdopnAYKh

Level 5 → Level 6

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! executable
find: paths must precede expression: executable
Try 'find --help' for more information.
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

```
bandit5@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
sree@sree-VirtualBox:~/Desktop$
```

```
sree@sree-VirtualBox:~/Desktop$ ssh bandit6@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit6@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!

--[ 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!
```

Password: DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Level 6 → Level 7

```
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
find: '/root': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/home/bandit29-git': Permission denied
find: '/home/bandit31-git': Permission denied
find: '/lostfound': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/lvm/archive': Permission denied
find: '/etc/lvm/backup': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/6854/task/6854/fdinfo/6': No such file or directory
find: '/proc/6854/fdinfo/5': No such file or directory
find: '/proc/6857/fdinfo/9': 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-bandit11': Permission denied
find: '/run/screen/S-bandit25': Permission denied
find: '/run/screen/S-bandit30': Permission denied
find: '/run/screen/S-bandit9': Permission denied
find: '/run/screen/S-bandit28': Permission denied
find: '/run/screen/S-bandit18': Permission denied
find: '/run/screen/S-bandit7': Permission denied
find: '/run/screen/S-bandit16': Permission denied
find: '/run/screen/S-bandit26': Permission denied
find: '/run/screen/S-bandit8': Permission denied
find: '/run/screen/S-bandit15': Permission denied
find: '/run/screen/S-bandit4': Permission denied
find: '/run/screen/S-bandit19': Permission denied
find: '/run/screen/S-bandit31': Permission denied
find: '/run/screen/S-bandit17': Permission denied
find: '/run/screen/S-bandit2': Permission denied
find: '/run/screen/S-bandit22': Permission denied
find: '/run/screen/S-bandit21': Permission denied
find: '/run/screen/S-bandit14': Permission denied
find: '/run/screen/S-bandit24': Permission denied
find: '/run/screen/S-bandit23': Permission denied
find: '/run/shm': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/tmp': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/polkit-1': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/log': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/ldconfig': Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$
```

Password: HKBPTKQnlay4Fw76bEy8PVxKEDQRKTzs

Level 7 → Level 8

wrongheadedness's gjfU53a1Bf0itkMov3rlgbRHq6M1hiq
scrutinizes Z76LPyF18BhQhuJow1qW4MoDcoCdfOB9
refresher's dtfQgdVtYR1Ufx4D5YE01krnKndcu
earthlings IfhUcS0r0auQ8G45MVWSPUzDkTr6wnJ
Hera's gACryahuox36Ac01jgQ4p4ulwvkv3D
ferment's DTtIALtV7wmDWYDQ04Sm97jkCnNkw2P
Anouilh MKKDDk16xVFcZsBxhNeMsfeAoMoJa
overabundance E59eqyfnnhuB03XqT0AR7EKGgyCQ1Ifk
complement's MCmY3Mx3eNeqCkZGS4Sp59y036l2F5fJ
grape g00pwTz0tluZ6s3p1jpo7207LahPxu
Blaine k61r0i4u0d2PMExLD2RxDQWEbtAcyst
canonization's 7ITRzVfVsziJhLvh14qUgW19qUcN
reserve AH03PdguR05acaQVGFQr02RsByh
Zanuck 30KRL0qJnc5jDqyNpHaPHd6TzCbjVt1f
baritone XsodKcc2a05ckklp4auKwJrJVaCzKcpq
lineman's GhBHTLmkNmxxJxFzD4fzhu1pRv8xejb6yw
swaddled snDrp6ve7nuHPsB0tLrmpl0yondhVzAH
garishness's Ubk1y2z2C02GeJarlSlaLwb0tjhg0p9rx
Benny's QkQzRdfIs47KckVL15fsfTqlRcxryjvz
regulated sxJ8HT73fvwMMIcL50nhawacsYGuLWP
knotting vh268JXw10NsnsdzedwMaHd4rTP69Lzr
hymnals 7MqsN3zl2PdflgtAxt6cfwBzCpAMauo
Fremont vUBzXw8CxdpJglkZzdBpYAHfZPKh7Ls
punter's ZaFza110z0C6reMmRo9onXNPQ16a
junking 6tLr5K8Y21d2xsdku3T3TFXWb6WOMXty
Aymara zSeUs0uyB06a6YpwaLBBk1x8KFBC
waned gl59r6xvwih5y8t0mgJNtHwUMG856id
conceded TWLuPtX3hwBd4yQs095En0n0iNy79sC
kilned kLjrgojVftiyUotoU14cxFqCxb6C6as
Santayana KKn1i4fwuMkZhvfppfaYrBzdQa3Tr3Pk
Antigua qBzCgkAg00kCgrkVQFXXM0s6FvArL5s
heyday UAGwmlfzylGa4fPhQZeeUQEzZJlUpyx
praiseworthiness's bJrB8QwC4mh71p9hB3mbFBMMwlnKq
separatism p2167YTC3eAv4yhLznB2f73JvldLUw
plan PLz4Xw0zE0Fe40d117w8QXLMIMXft
confrontation AhC5c1H13Antf7H26d7tmBWhfd8Vkz
briquet's aHc5c1H13Antf7H26d7tmBWhfd8Vkz
encapsulate STOVQEMWtfz4zJrJhRdcgZcfvwbls
wildfowls PqcmofjnjkNBv09exud7Fv2XG6WUMzb
Finland xgxSiYggUCMrI莫T7w2sTwG1cdcvbRvU
bandit/bandit:::
bandit@bandit::: \$ strings data.txt | grep "millionth"
millionth cvx2Jja4CFALtz587jk27wqghBM9plv
bandit@bandit::: \$ █

```
bandit7@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

```
sree@sree-VirtualBox:~/Desktop$ ssh bandit8@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
```

```
bandit8@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

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 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 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 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!
```

Password: cvX2JJa4CFALtqS87jk27qwqGhBM9pIV

Level 8 → Level 9

```
bandit8@bandit:~$ cat data.txt
VkBBAEWyIibVkeURZV5mowiGg6i3m7Be0
zdd2ctVveROGeiS2WE3TeLZMeL5jL7iM
sYSokIAITvFUKU4sAHTtMarfjlZWWj5i
ySvsTwlMgnUF0n86Fgmn2TNjks0lrv72
NLWvtQvl7EaqBNx2x4eznRlQONULLCYZ
LfrBHfAh0pP9bgGAZP4QrVku3pysAYC
U0NYdD3wHZKpfEg9qgQ0LJimAjy6qxhs
flyKxCbHB8uLTaIB5LxqQNuJ3yj0eH
TThRARdF2ZEXM047TIYkyPPLtvzzLcDf
cIPbot7oYveUPNxDMhv1hiri50CqpkTG
kJTBMD8k90HyXwZ2aJMqkV23u0gyuoIO
J6Lzp6ZqTjs0uJRTXcvhwKfM0KK3xtbl
NLWvtQvl7EaqBNx2x4eznRlQONULLCYZ
0N65ZPpNGkUJePzfxcTcRZRvxvCbUGfm
SHMAMUEzQe4mV7SJpETTZFsYNRJsZE2k
I3fc578Vla7m0Q1t9zArPP0PY7aDVbcJ
8jtZmvqp9PTi8tp1oybBM663NQH3fhII
1ETSSkqjfQj1cJeFzXLJWzKzza3iWcJa
bRnkTwNdxFy2RPZIshXJikswwEzJGvJ9
0Xe6DLvK5i_zRqEtBA7sW2SPm1Ai_xlWvS9
```

```
bandit8@bandit:~$ sort data.txt | uniq -c
```

Count	User ID
10	UjsVbcqKeJqdCZQCDMkzv6A9X7hLbNE4
1	UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
10	UVNzVhiLVQEcrAz5jl8U14sMVZQhjuXia

```
bandit8@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

```
* 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,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 [#wargames](irc://irc.overthewire.org).

Enjoy your stay!

Password: UsVvYFSfZZWbi6wgC7dAFyFuR6jQQUhR

Level 9 → Level 10

```
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:~$
```

--[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 [#wargames](irc://irc.overthewire.org).

Enjoy your stay!

```
bandit9@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
sree@sree-VirtualBox:~/Desktop$ ssh bandit0@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password:
Linux bandit.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!

Password: truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Level 10 → Level 11

```
bandit10@bandit:~$ cat data.txt  
VGhlIHBhc3N3b3JkIGlZIElgDwts0dzRlc4TU9xM0lsRnFyeUxaHhUTkViVVBSG==  
bandit10@bandit:~$ base  
-bash: base: command not found  
bandit10@bandit:~$ base64 -d data.txt  
The password is IFukwKGsFW8M0q3IRFqrxE1hxTNEbUPR  
bandit10@bandit:~$
```

```
bandit10@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
sree@sree-VirtualBox:~/Desktop$ 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, ...
- * **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 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!
```

Password: IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Level 11 → Level 12

```
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh
bandit11@bandit:~$
```

The screenshot shows the CyberChef interface. On the left, a sidebar lists various operations like rot1, ROT13, and Favourites. The main area has tabs for 'Operations' (selected), 'Recipe', and 'Input'. Under 'Operations', 'ROT13' is selected. In the 'Input' tab, the text 'Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh' is pasted. The 'Output' tab shows the decrypted result: 'The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu'. Below the input and output fields are status bars showing character ranges and lengths. At the bottom, there's a 'STEP' button, a 'BAKE!' button with a chef icon, and an 'Auto Bake' checkbox.

```
bandit11@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
sree@sree-VirtualBox:~/Desktop$ 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!

--[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!
```

```
bandit12@bandit:~$
```

Password: 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Level 12 → Level 13

```
bandit12@bandit:~$ cat data.txt
00000000: 1f8b 0808 0650 b45e 0203 6461 7461 322e ....P.^..data2.
00000010: 6269 6e00 013d 02c2 fd42 5a68 3931 4159 bin..-=.BZh91AY
00000020: 2653 598e 4f1c c800 001e 7fff fbf9 7fda &SY.O.....
00000030: 9e7f 4f76 9fcf fe7d 3fff f67d abde 5e9f ..ov...?...)^.-
00000040: f3fe 9fbf f6f1 feee bfdf a3ff b001 3b1b .....).
00000050: 5481 a1a8 1ea0 1a34 d0d0 001a 68d3 4683 T.....4...h.F.
00000060: 4680 0680 0034 1918 4c4d 1904 4000 0001 F....4..LM..@...
00000070: a000 c87a 81a3 464d a8d3 43c5 1068 0346 ...z..FM..C..h.F.
00000080: 8343 49d9 3400 0340 66a6 8968 0cd4 f500 .C@.4..gf..h...
00000090: 69ea 6800 0f59 68f2 4d00 680d 06ca 0190 i.h..Ph..M..h....
000000a0: 0000 69a1 a1a0 1ea0 194d 340d 1eaf b280 ..i.....M4....
000000b0: f500 3406 2340 034d 3400 0000 3403 4400 ..4.#0.M4...4...
000000c0: 1a07 a832 3400 f51a 0003 43d1 0068 0d34 ..24.....C..h.4
000000d0: 6868 f51a 3d43 2580 3e58 061a 2c89 6bf3 hh..=C%>X..k.
000000e0: 0163 08ab dc31 91cd 1747 599b e401 0b06 ..c....1..GV....
000000f0: a8b1 7255 a3b2 9cf9 75cc f106 941b 347a ..rU....u....4z
00000100: d616 55c4 2ef2 9d46 e7d1 3050 b5fb 76eb ..U....F..OP..V.
00000110: 0178 60c1 2201 33f0 0de0 4aa6 ec8c 914f ..".3...J....0
00000120: cf8a aed5 7b52 4270 8d51 6978 c159 b85a ...{RbP.Qlx.Y.Z
00000130: 2164 fb1f c26a 8d28 b414 e690 bfdd b3e1 ld...j.(-.....
00000140: f414 2f9f d4e1 c523 b641 ac08 0c0b 06f5 ..}..A.#.A....
00000150: dd64 b862 1158 3f9e 897a 8cae 32b0 1fb7 ..d.b.X?..z..2...
00000160: 3c82 af41 20fd 6e7d 0a35 2833 41bd de0c <.A..n).5(3A...
00000170: 774f ae52 a1ac 0fb2 8c36 ef58 537b f30a w0.R.....6.XS{...
00000180: 1510 cab5 cb51 4231 95a4 d045 b95c ea09 ....0B1...E.\..
00000190: 9fa0 4d33 ba43 22c9 b5be d0ea eb7 ecb5 ..M3.".....
000001a0: 59fc 8bf1 97a0 87a5 0df0 7acd d555 fc11 Y.....z..U..
000001b0: 223f fdc6 2be3 e809 c974 271a 920e acbc "?.+....t'.....
000001c0: 0de1 f1a6 393f 4cf5 50eb 7942 86c3 3d7a ...97L.P..yB..-z
000001d0: feed 173f a84c bb4e 742a fc37 b771 508a .m.?..L.Nt*.7(qP.
000001e0: a2cc 9cf1 2522 8a77 39f2 716d 34f9 8620 ....%"..w..qM4..
000001f0: 4e33 ca36 eec0 cd4b b3e8 48e4 8b91 5bea N3..6...K..H..I[.
00000200: 01bf 7d21 0b64 82c0 3341 3424 e98b 4d7e ..}..d..3AA$...M-
00000210: c95c 1b1f cac9 a04a 1988 43b2 6b55 c6a6 \.....J..C.kU..
00000220: 075c 1eb4 8ecf 5cf0 4653 064a 84da 263d \.....\..F.S..&-
00000230: b15b bce1 7109 5c29 c524 3afe d715 4894 ..{..q.\}.S....H.
00000240: 7426 072f fc28 ab05 9603 b3f2 5dc9 14e1 t8./.({....]...
00000250: 4242 393c 7320 98f7 681d 3d02 0000 BB9<s ..h.=...
bandit12@bandit:~$ mkdir /tmp/f
bandit12@bandit:~$ cp data.txt /tmp/f
bandit12@bandit:~$ cd /tmp/f
bandit12@bandit:/tmp/f$ ls
data.txt
bandit12@bandit:/tmp/f$ xxd -r data.txt > data
```

```
bandit12@bandit:/tmp/f$ ls
data data.txt
bandit12@bandit:/tmp/f$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/f$ mv data file.gz
bandit12@bandit:/tmp/f$ gzip -d file.gz
bandit12@bandit:/tmp/f$ ls
data.txt file
bandit12@bandit:/tmp/f$ file file
file: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/f$ mv file file.bz2
bandit12@bandit:/tmp/f$ bzip2 -d file.bz2
bandit12@bandit:/tmp/f$ ls
data.txt file
bandit12@bandit:/tmp/f$ file file
file: gzip compressed data, was "data4.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/f$ mv file file.gz
bandit12@bandit:/tmp/f$ gzip -d file.gz
bandit12@bandit:/tmp/f$ ls
data.txt file
bandit12@bandit:/tmp/f$ file file
file: POSIX tar archive (GNU)
bandit12@bandit:/tmp/f$ mv file file.tar
bandit12@bandit:/tmp/f$ tar xf file.tar
bandit12@bandit:/tmp/f$ ls
data5.bin data.txt file.tar
bandit12@bandit:/tmp/f$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/f$ rm file.tar
bandit12@bandit:/tmp/f$ rm data.txt
bandit12@bandit:/tmp/f$ ls
data5.bin
bandit12@bandit:/tmp/f$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/f$ mv data5.bin data.tar
bandit12@bandit:/tmp/f$ tar xf data.tar
bandit12@bandit:/tmp/f$ ls
data6.bin data.tar
bandit12@bandit:/tmp/f$ file data6.bin
data6.bin: bztp compressed data, block size = 900k
bandit12@bandit:/tmp/f$ mv data6.bin data.bz2
bandit12@bandit:/tmp/f$ ls
data.bzz data.tar
bandit12@bandit:/tmp/f$ bzip2 -d data.bz2
bandit12@bandit:/tmp/f$ ls
data.tar
bandit12@bandit:/tmp/f$ mv data data.tar
bandit12@bandit:/tmp/f$ ls
bandit12@bandit:/tmp/f$ ls
data.tar
bandit12@bandit:/tmp/f$ file data
data: ASCII text
bandit12@bandit:/tmp/f$ cat data
The password is 8ZjyCrBWFYkeahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/f$
```

```
bandit12@bandit:/tmp/f$ exit
logout
Connection to bandit.labs.overthewire.org closed.
sree@sree-VirtualBox:~/Desktop$ 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

          _/\_      _/\_      _/\_
         / \ \    / \ \    / \ \
        ;   ; \  ;   ; \  ;   ; \
       ;   ; \  ;   ; \  ;   ; \
      ;   ; \  ;   ; \  ;   ; \
     ;   ; \  ;   ; \  ;   ; \
    ;   ; \  ;   ; \  ;   ; \
   ;   ; \  ;   ; \  ;   ; \
  ;   ; \  ;   ; \  ;   ; \
 www.----ver----he----"ire.org

Welcome to OverTheWire!

If you find any problems, please report them to Steven or morla on
irc.overthewire.org.

--[ Playing the games ]--

This machine might hold several wargames.
If you are playing "somegame", then:

* USERNAMES are somegame0, somegame1, ...
* Most LEVELS are stored in /somegame/.
* PASSWORDS for each level are stored in /etc/somegame_pass/.

Write-access to homedirectories is disabled. It is advised to create a
working directory with a hard-to-guess name in /tmp/. You can use the
command "mktemp -d" in order to generate a random and hard to guess
directory in /tmp/. Read-access to both /tmp/ and /proc/ is disabled
so that users can not snoop on eachother. Files and directories with
easily guessable or short names will be periodically deleted!

Please play nice:

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

Password: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Level 13 → Level 14

```
bandit13@bandit:~$ ls
sshkey.private
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 SHA256:98UL0ZWr85496EtcRK Klo20X30PnyPSB5tB5RPbhczc.
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

          _/\_      / \_/\_      / \_/\_      / \_/\_
         / \ \_/\_ / \ \_/\_ / \ \_/\_ / \ \_/\_
        / \ \_/\_ / \ \_/\_ / \ \_/\_ / \ \_/\_
       / \ \_/\_ / \ \_/\_ / \ \_/\_ / \ \_/\_
      / \ \_/\_ / \ \_/\_ / \ \_/\_ / \ \_/\_
     / \ \_/\_ / \ \_/\_ / \ \_/\_ / \ \_/\_
    / \ \_/\_ / \ \_/\_ / \ \_/\_ / \ \_/\_
   / \ \_/\_ / \ \_/\_ / \ \_/\_ / \ \_/\_
  / \ \_/\_ / \ \_/\_ / \ \_/\_ / \ \_/\_
 / \ \_/\_ / \ \_/\_ / \ \_/\_ / \ \_/\_
www. '---' ver      '---' he      '---" ire.org

Welcome to OverTheWire!

If you find any problems, please report them to Steven or morla on
irc.overthewire.org.

--[ Playing the games ]--

This machine might hold several wargames.
If you are playing "somegame", then:

 * USERNAMES are somegame0, somegame1, ...
 * Most LEVELS are stored in /somegame/.
 * PASSWORDS for each level are stored in /etc/somegame_pass/.

Write-access to homedirectories is disabled. It is advised to create a
working directory with a hard-to-guess name in /tmp/. You can use the
command `mktemp -d` in order to generate a random and hard to guess
directory in /tmp/. Read-access to both /tmp/ and /proc/ is disabled
so that users can not snoop on eachother. Files and directories with
easily guessable or short names will be periodically deleted!

Please play nice:
```

```
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,noexecstack  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
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$
```

Password: 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

Level 14 → Level 15

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr

bandit14@bandit:~$
```

```
bandit14@bandit:~$ exit
logout
Connection to localhost closed.
bandit13@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

```
sree@sree-VirtualBox:~/Desktop$ 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 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 ]--
```

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 /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!

Password: BfMYroe26WYalil77FoDi9qh59eK5xNr

Level 15 → Level 16

```
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
BFMyroe26WYalll77FoD19qh59eK5xNn
bandit15@bandit:~$ man nc | grep ssl
bandit15@bandit:~$ man ncat
bandit15@bandit:~$ man ncat | grep ssl
  --ssl          Connect or listen with SSL
  --ssl-cert     Specify SSL certificate file (PEM) for listening
  --ssl-key      Specify SSL private key (PEM) for listening
  --ssl-verify   Verify trust and domain name of certificates
  --ssl-trustfile PEM file containing trusted SSL certificates
  --ssl-ciphers  Cipherlist containing SSL ciphers to use
--ssl (Use SSL)
--ssl-verify (Verify server certificates)
  In client mode, --ssl-verify is like --ssl except that it also requires verification of the server certificate. Ncat comes with a default set of trusted certificates in the file ca-bundle.crt. Some operating systems provide a default list of trusted certificates; these will also be used if available. Use --ssl-trustfile to give a custom list. Use -v
--ssl-cert cert.pem (Specify SSL certificate)
  --ssl-key
--ssl-key keyfile.pem (Specify SSL private key)
  This option gives the location of the PEM-encoded private key file that goes with the certificate named with --ssl-cert.
--ssl-trustfile cert.pem (List trusted certificates)
  This option sets a list of certificates that are trusted for purposes of certificate verification. It has no effect unless combined with --ssl-verify. The argument to this
--ssl-ciphers cipherlist (Specify SSL ciphersuites)
  http://www.openssl.org
bandit15@bandit:~$ ncat --ssl localhost 30001
BFMyroe26WYalll77FoD19qh59eK5xNn
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd
^C
bandit15@bandit:~$
```

Password: cluFn7wTiGryunymYOu4RcffSxQlueh