

1. Level 0

username	bandit0
password	bandit0
command	ssh bandit0@bandit.labs.overthewire.org -p 2220

 bandit0@bandit: ~

```
[03/03/25]seed@VM:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
```

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

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

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```

This machine might hold several wargames.

If you are playing "somegame", then:

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

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

 bandit0@bandit: ~

Please play nice:

- \* don't leave orphan processes running
- \* don't leave exploit-files laying around
- \* don't annoy other players
- \* don't post passwords or spoilers
- \* again, DONT POST SPOILERS!  
This includes writeups of your solution on your blog or website!

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

|                      |                   |
|----------------------|-------------------|
| -m32                 | compile for 32bit |
| -fno-stack-protector | disable ProPolice |
| -Wl,-z,norelro       | disable relro     |

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find in the following locations:

- \* gef (<https://github.com/hugsy/gef>) in /opt/gef/
- \* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* radare2 (<http://www.radare.org/>)

--[ More information ]--

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

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvYRnrb2rfNWOZOTa6ip5If

bandit0@bandit:~$ █
```

```
bandit0@bandit:~$ ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface] [-b bind_address]
          [-c cipher_spec] [-D [bind_address:]port] [-E log_file]
          [-e escape_char] [-F configfile] [-I pkcs11] [-i identity_file]
          [-J destination] [-L address] [-l login_name] [-m mac_spec]
          [-O ctl_cmd] [-o option] [-P tag] [-p port] [-R address]
          [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
          destination [command [argument ...]]
ssh [-Q query_option]
```

## 2. Level 0 → Level 1

|          |                                                 |
|----------|-------------------------------------------------|
| username | bandit1                                         |
| password | ZjLjTmM6FvvYRnrb2rfNWOZOTa6ip5If                |
| command  | ssh bandit1@bandit.labs.overthewire.org -p 2220 |

Note:

- need to **log out from bandit0** and connect again **from your own machine**.
- The password for the next level is stored in a file called **readme** located in the home directory

 bandit1@bandit: ~

```
bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
[03/03/25]seed@VM:~$ ssh bandit1@bandit.labs.overthewire.org -p 2220
```

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

bandit1@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```

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

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

Write-access to homedirectories is disabled. It is advised to create a working directory with a hard-to-guess name in /tmp/. You can use the command "mktemp -d" in order to generate a random and hard to guess

```
bandit1@bandit: ~  
  
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc  
restricted so that users cannot snoop on eachother. Files and directories  
with easily guessable or short names will be periodically deleted! The /tmp  
directory is regularly wiped.  
Please play nice:  
  
* don't leave orphan processes running  
* don't leave exploit-files laying around  
* don't annoy other players  
* don't post passwords or spoilers  
* again, DONT POST SPOILERS!  
  This includes writeups of your solution on your blog or website!  
  
--[ Tips ]--  
  
This machine has a 64bit processor and many security-features enabled  
by default, although ASLR has been switched off. The following  
compiler flags might be interesting:  
  
-m32                compile for 32bit  
-fno-stack-protector  disable ProPolice  
-Wl,-z,norelro        disable relro  
  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
  
Finally, network-access is limited for most levels by a local  
firewall.  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!
```

### 3. Level 1 → Level 2

username	bandit2
----------	---------

password	263JGJPfgU6LtdEvgfWU1XP5yac29mFx
command	ssh bandit2@bandit.labs.overthewire.org -p 2220

Note:

- The password for the next level is stored in a file called - located in the home directory

Dashed filename

```
bandit1@bandit:~$ ls
-
```

```
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$ cat < -
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
```

```
bandit1@bandit:~$ file -
Buiphuongthanh
/dev/stdin: ASCII text
```

du	Shows disk usage of the current directory and its subdirectories.
----	---

```
bandit1@bandit:~$ du
20  .
bandit1@bandit:~$ find
.
./ .profile
./ .bashrc
./ .bash_logout
./ -
```

 bandit2@bandit: ~

```
bandit1@bandit:~$ exit
```

[logout](#)

```
Connection to bandit.labs.overthewire.org closed.
```

```
[03/03/25]seed@VM:~$ ssh bandit2@bandit.labs.overthewire.org -p 2220
```

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

bandit2@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```


This machine might hold several wargames.

If you are playing "somegame", then:

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

Write-access to homedirectories is disabled. It is advised to create a working directory with a hard-to-guess name in /tmp/. You can use the command "mktemp -d" in order to generate a random and hard to guess



 bandit2@bandit: ~

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

Please play nice:

- \* don't leave orphan processes running
  - \* don't leave exploit-files laying around
  - \* don't annoy other players
  - \* don't post passwords or spoilers
  - \* again, DONT POST SPOILERS!
- This includes writeups of your solution on your blog or website!

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

|                      |                   |
|----------------------|-------------------|
| -m32                 | compile for 32bit |
| -fno-stack-protector | disable ProPolice |
| -Wl,-z,norelro       | disable relro     |

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find in the following locations:

- \* gef (<https://github.com/hugsy/gef>) in /opt/gef/
- \* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* radare2 (<http://www.radare.org/>)

--[ More information ]--

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

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

#### 4. Level 2 → Level 3

|          |                                                 |
|----------|-------------------------------------------------|
| username | bandit3                                         |
| password | MNk8KNH3Usiio41PRUEoDFPqfxLP1Smx                |
| command  | ssh bandit3@bandit.labs.overthewire.org -p 2220 |

Note:

- The password for the next level is stored in a file called **spaces in this filename** located in the home directory

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

```
bandit2@bandit:~$ cat "spaces in this filename"  
MNk8KNH3Usiio41PRUEoDFPqfxLP1Smx  
bandit2@bandit:~$ cat 'spaces in this filename'  
MNk8KNH3Usiio41PRUEoDFPqfxLP1Smx
```

Escape every space with backslash but it is more work and more confusing than the previous method

```
bandit2@bandit:~$ cat spaces\ in\ this\ filename  
MNk8KNH3Usiio41PRUEoDFPqfxLP1Smx
```

 bandit3@bandit: ~

```
bandit2@bandit:~$ exit
```

[logout](#)

```
Connection to bandit.labs.overthewire.org closed.
```

```
[03/09/25]seed@VM:~$ ssh bandit3@bandit.labs.overthewire.org -p 2220
```

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32  
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32  
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32  
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

This is an OverTheWire game server.

More information on <http://www.overthewire.org/wargames>

```
bandit3@bandit.labs.overthewire.org's password:
```

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```

This machine might hold several wargames.

If you are playing "somegame", then:

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

Write-access to homedirectories is disabled. It is advised to create a working directory with a hard-to-guess name in /tmp/. You can use the command "mktemp -d" in order to generate a random and hard to guess

```
bandit3@bandit: ~  
  
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc  
restricted so that users cannot snoop on eachother. Files and directories  
with easily guessable or short names will be periodically deleted! The /tmp  
directory is regularly wiped.  
Please play nice:  
  
* don't leave orphan processes running  
* don't leave exploit-files laying around  
* don't annoy other players  
* don't post passwords or spoilers  
* again, DONT POST SPOILERS!  
  This includes writeups of your solution on your blog or website!  
  
--[ Tips ]--  
  
This machine has a 64bit processor and many security-features enabled  
by default, although ASLR has been switched off. The following  
compiler flags might be interesting:  
  
-m32                compile for 32bit  
-fno-stack-protector  disable ProPolice  
-Wl,-z,norelro        disable relro  
  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
  
Finally, network-access is limited for most levels by a local  
firewall.  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!
```

5. Level 3 → Level 4

username	bandit4
----------	---------

password	2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
command	ssh bandit4@bandit.labs.overthewire.org -p 2220

Note:

- The password for the next level is stored in a hidden file in the **inhere** directory.

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root    root    4096 Sep 19 07:08 .
drwxr-xr-x 3 root    root    4096 Sep 19 07:08 ..
-rw-r----- 1 bandit4 bandit3   33 Sep 19 07:08 ...Hiding-From-You
bandit3@bandit:~/inhere$ ls -a
.  ..  ...Hiding-From-You
bandit3@bandit:~/inhere$ ^C
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
```

**...Hiding-From-You:** reference hidden files in Linux

```
bandit3@bandit:~/inhere$ cd ..
bandit3@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
[03/09/25]seed@VM:~$ ssh bandit4@bandit.labs.overthewire.org -p 2220
```

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85															

```
bandit4@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit4@bandit.labs.overthewire.org's password:
```

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

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/.
```

bandit4@bandit: ~

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

Please play nice:

- \* don't leave orphan processes running
  - \* don't leave exploit-files laying around
  - \* don't annoy other players
  - \* don't post passwords or spoilers
  - \* again, DONT POST SPOILERS!
- This includes writeups of your solution on your blog or website!

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

|                      |                   |
|----------------------|-------------------|
| -m32                 | compile for 32bit |
| -fno-stack-protector | disable ProPolice |
| -Wl,-z,norelro       | disable relro     |

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find in the following locations:

- \* gef (<https://github.com/hugsy/gef>) in /opt/gef/
- \* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* radare2 (<http://www.radare.org/>)

--[ More information ]--

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

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit4@bandit:~\$

6. Level 4 → Level 5

|          |         |
|----------|---------|
| username | bandit5 |
|----------|---------|

|          |                                                 |
|----------|-------------------------------------------------|
| password | 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw                |
| command  | ssh bandit5@bandit.labs.overthewire.org -p 2220 |

Note:

- The password for the next level is stored in the only human-readable file in the **inhere** directory. Tip: if your terminal is messed up, try the “reset” command.
- **file ./-\*** : In case filenames start with ‘-’

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -al
total 48
drwxr-xr-x 2 root    root    4096 Sep 19 07:08 .
drwxr-xr-x 3 root    root    4096 Sep 19 07:08 ..
-rw-r----- 1 bandit5 bandit4   33 Sep 19 07:08 -file00
-rw-r----- 1 bandit5 bandit4   33 Sep 19 07:08 -file01
-rw-r----- 1 bandit5 bandit4   33 Sep 19 07:08 -file02
-rw-r----- 1 bandit5 bandit4   33 Sep 19 07:08 -file03
-rw-r----- 1 bandit5 bandit4   33 Sep 19 07:08 -file04
-rw-r----- 1 bandit5 bandit4   33 Sep 19 07:08 -file05
-rw-r----- 1 bandit5 bandit4   33 Sep 19 07:08 -file06
-rw-r----- 1 bandit5 bandit4   33 Sep 19 07:08 -file07
-rw-r----- 1 bandit5 bandit4   33 Sep 19 07:08 -file08
-rw-r----- 1 bandit5 bandit4   33 Sep 19 07:08 -file09
```



```
bandit4@bandit:~/inhere$ file ./-*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat -file07
cat: invalid option -- 'f'
Try 'cat --help' for more information.
bandit4@bandit:~/inhere$ cat -- -file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
```

 bandit5@bandit: ~

```
bandit4@bandit:~/inhere$ exit
```

[logout](#)

```
Connection to bandit.labs.overthewire.org closed.
```

```
[03/09/25]seed@VM:~$ ssh bandit5@bandit.labs.overthewire.org -p 2220
```

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

bandit5@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```

This machine might hold several wargames.

If you are playing "somegame", then:

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

Write-access to homedirectories is disabled. It is advised to create a working directory with a hard-to-guess name in /tmp/. You can use the command "mktemp -d" in order to generate a random and hard to guess directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc

bandit5@bandit: ~

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

Please play nice:

- \* don't leave orphan processes running
  - \* don't leave exploit-files laying around
  - \* don't annoy other players
  - \* don't post passwords or spoilers
  - \* again, DONT POST SPOILERS!
- This includes writeups of your solution on your blog or website!

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

-m32	compile for 32bit
-fno-stack-protector	disable ProPolice
-Wl,-z,norelro	disable relro

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find in the following locations:

- \* gef (<https://github.com/hugsy/gef>) in /opt/gef/
- \* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* radare2 (<http://www.radare.org/>)

--[ More information ]--

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

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit5@bandit:~\$

7. Level 5 → Level 6

username	bandit6
----------	---------

password	HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
command	ssh bandit6@bandit.labs.overthewire.org -p 2220

Note:

- The password for the next level is stored in a file somewhere under the **inhere** directory and has all of the following properties:
  - human-readable
  - 1033 bytes in size
  - not executable

find command to locate the **human-readable file**:

**find . -type f -size 1033c ! -executable**


**find .** → Search in the current (**inhere**) directory.

**-type f** → Look for **files** (not directories).

**-size 1033c** → Find a file that is **exactly 1033 bytes** (**c** stands for bytes).

**! -executable** → Ensure the file is **not executable**.

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls -al
total 88
drwxr-x--- 22 root bandit5 4096 Sep 19 07:08 .
drwxr-xr-x  3 root root    4096 Sep 19 07:08 ..
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere00
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere01
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere02
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere03
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere04
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere05
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere06
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere07
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere08
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere09
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere10
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere11
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere12
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere13
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere14
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere15
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere16
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere17
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere18
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere19
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ file^C
bandit5@bandit:~/inhere$ file ./maybehere07/.file2
./maybehere07/.file2: ASCII text, with very long lines (1000)
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

bandit5@bandit:~/inhere\$ 

 bandit6@bandit: ~

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

[logout](#)

```
Connection to bandit.labs.overthewire.org closed.
```

```
[03/09/25]seed@VM:~$ ssh bandit6@bandit.labs.overthewire.org -p 2220
```

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

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

```
bandit6@bandit.labs.overthewire.org's password:
```

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```

This machine might hold several wargames.

If you are playing "somegame", then:

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

Write-access to homedirectories is disabled. It is advised to create a working directory with a hard-to-guess name in /tmp/. You can use the command "mktemp -d" in order to generate a random and hard to guess directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc



bandit6@bandit: ~

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

Please play nice:

- \* don't leave orphan processes running
  - \* don't leave exploit-files laying around
  - \* don't annoy other players
  - \* don't post passwords or spoilers
  - \* again, DONT POST SPOILERS!
- This includes writeups of your solution on your blog or website!

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

|                      |                   |
|----------------------|-------------------|
| -m32                 | compile for 32bit |
| -fno-stack-protector | disable ProPolice |
| -Wl,-z,norelro       | disable relro     |

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find in the following locations:

- \* gef (<https://github.com/hugsy/gef>) in /opt/gef/
- \* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* radare2 (<http://www.radare.org/>)

--[ More information ]--

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

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit6@bandit:~\$ █

8. Level 6 → Level 7

|          |                                                 |
|----------|-------------------------------------------------|
| username | bandit7                                         |
| password | morbNTDkSW6jIlUc0ymOdMaLnOIFVAaj                |
| command  | ssh bandit7@bandit.labs.overthewire.org -p 2220 |

Note:

- The password for the next level is stored **somewhere on the server** and has all of the following properties:
  - owned by user bandit7
  - owned by group bandit6
  - 33 bytes in size

file is anywhere on the system, we search from the root (/):  
`find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null`

`/` → Search from the **root directory** (entire system).  
`-type f` → Look for **files** only.  
`-user bandit7` → The file must be **owned by user bandit7**.  
`-group bandit6` → The file must be **owned by group bandit6**.  
`-size 33c` → The file must be **exactly 33 bytes** (`c` stands for bytes).  
`2>/dev/null` → Hides **permission denied** errors.

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

```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
```



 bandit7@bandit: ~

```
bandit6@bandit:~$ exit
```

[logout](#)

```
Connection to bandit.labs.overthewire.org closed.
```

```
[03/09/25]seed@VM:~$ ssh bandit7@bandit.labs.overthewire.org -p 2220
```

[illegible]

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

```
bandit7@bandit.labs.overthewire.org's password:
```

Permission denied, please try again.

```
bandit7@bandit.labs.overthewire.org's password:
```

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```

This machine might hold several wargames.

If you are playing "somegame", then:

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

Write-access to homedirectories is disabled. It is advised to create a working directory with a hard-to-guess name in /tmp/. You can use the

```
bandit7@bandit: ~  
restricted so that users cannot snoop on eachother. Files and directories  
with easily guessable or short names will be periodically deleted! The /tmp  
directory is regularly wiped.  
Please play nice:  
  
* don't leave orphan processes running  
* don't leave exploit-files laying around  
* don't annoy other players  
* don't post passwords or spoilers  
* again, DONT POST SPOILERS!  
  This includes writeups of your solution on your blog or website!  
  
--[ Tips ]--  
  
This machine has a 64bit processor and many security-features enabled  
by default, although ASLR has been switched off. The following  
compiler flags might be interesting:  
  
-m32                compile for 32bit  
-fno-stack-protector  disable ProPolice  
-Wl,-z,norelro        disable relro  
  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
  
Finally, network-access is limited for most levels by a local  
firewall.  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit7@bandit:~$
```

9. Level 7 → Level 8

username	bandit8
----------	---------

password	dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
command	ssh bandit8@bandit.labs.overthewire.org -p 2220

Note:

- The password for the next level is stored in the file **data.txt** next to the word **millionth**

Use the **grep** command to find the line that contains "millionth":  
grep "millionth" data.txt

return the line containing **"millionth" and the password** next to it

```
bandit7@bandit:~$ ls -la
total 4108
drwxr-xr-x  2 root    root      4096 Sep 19 07:08 .
drwxr-xr-x 70 root    root      4096 Sep 19 07:09 ..
-rw-r--r--  1 root    root        220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root    root      3771 Mar 31  2024 .bashrc
-rw-r-----  1 bandit8 bandit7 4184396 Sep 19 07:08 data.txt
-rw-r--r--  1 root    root        807 Mar 31  2024 .profile
bandit7@bandit:~$ grep "millionth" data.txt
millionth      dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$
```



bandit8@bandit: ~

```
bandit7@bandit:~$ exit
```

```
logout
```

```
Connection to bandit.labs.overthewire.org closed.
```

```
[03/09/25]seed@VM:~$ ssh bandit8@bandit.labs.overthewire.org -p 2220
```

```

  _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

```

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



--[ Tips ]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

-m32	compile for 32bit
-fno-stack-protector	disable ProPolice
-Wl,-z,norelro	disable relro

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find in the following locations:

- \* gef (<https://github.com/hugsy/gef>) in /opt/gef/
- \* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* radare2 (<http://www.radare.org/>)

--[ More information ]--

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

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit8@bandit:~\$ █

10. Level 8 → Level 9

username	bandit9
password	4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
command	ssh bandit9@bandit.labs.overthewire.org -p 2220

Note:

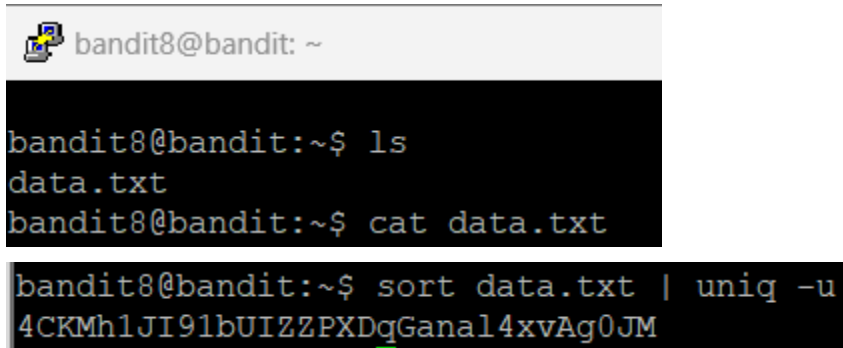
- The password for the next level is stored in the file **data.txt** and is the only line of text that occurs only once

find the **line that appears only once**, you can use **uniq** in combination with **sort**

**sort data.txt | uniq -u**

`sort data.txt` → Sort the lines in the file.

`uniq -u` → Show only lines that appear exactly once.



```
bandit8@bandit: ~  
  
bandit8@bandit:~$ ls  
data.txt  
bandit8@bandit:~$ cat data.txt  
  
bandit8@bandit:~$ sort data.txt | uniq -u  
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
```

 bandit9@bandit: ~

Host key verification failed.

```
bandit8@bandit:~$ exit
```

[logout](#)

```
Connection to bandit.labs.overthewire.org closed.
```

```
[03/09/25]seed@VM:~$ ssh bandit9@bandit.labs.overthewire.org -p 2220
```

```
This is an OverTheWire game server.
```

More information on <http://www.overthewire.org/wargames>

```
bandit9@bandit.labs.overthewire.org's password:
```

Permission denied, please try again.

```
bandit9@bandit.labs.overthewire.org's password:
```

Permission denied, please try again.

bandit9@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```

This machine might hold several wargames.

If you are playing "somegame", then:

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





bandit9@bandit: ~

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

Please play nice:

- \* don't leave orphan processes running
  - \* don't leave exploit-files laying around
  - \* don't annoy other players
  - \* don't post passwords or spoilers
  - \* again, DONT POST SPOILERS!
- This includes writeups of your solution on your blog or website!

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

|                      |                   |
|----------------------|-------------------|
| -m32                 | compile for 32bit |
| -fno-stack-protector | disable ProPolice |
| -Wl,-z,norelro       | disable relro     |

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find in the following locations:

- \* gef (<https://github.com/hugsy/gef>) in /opt/gef/
- \* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* radare2 (<http://www.radare.org/>)

--[ More information ]--

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

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit9@bandit:~\$ █

11. Level 9 → Level 10

|          |                                                  |
|----------|--------------------------------------------------|
| username | bandit10                                         |
| password | FGUW5iILVJrxX9kMYMmIN4MgbpfMiqey                 |
| command  | ssh bandit10@bandit.labs.overthewire.org -p 2220 |

Note:

- The password for the next level is stored in the file **data.txt** in one of the few human-readable strings, preceded by several '=' characters.

bandit9@bandit: ~

bandit9@bandit:~\$ cat data.txt

```
%P_A#C_LMS6v_pL_dM
s:ey_wj) LB=h\ J
7Z_R\ . b$-yO`N; pg_X(n_eLg_Y_VQu_z_S_JiqP.q.\ w_h!]v_y O_3*bm
~BF_|j#r>)l_v

)
j_T, o_D'M') dyaE?E^
>n_$J_u! I&_w U_S_i<2+$_z_i YX^ FEz_F#X[ 7$'0'T_B" w' o; W_9^0

]T?; Ec_O+^ {~S_t_u_ZY ^^K_W &Y5} | 9g_$k|^Q_u_i u_vU} # 5R!SL4
^J

C% ^h#%EG8)
U V F> V*_k_x {L} s_b_w o6a_D_dL; t_R8=0
<KQ_> f_w )X_K(L`^_) JJ
j q/ pQR/OZ[4'7-Z_eL 2_qG:E
A_W_T[ <tumi_0_oOd^' D#?P_X4 r_o z<V
D_]
h#! Q_J_s_v_z17 POLY] H_a^ UvTo_d |@T ^N_8?g ) b )?
Q#_g_mlx )----- the A+ i_d_w ^ F1 > fSK_3_PZ t &xs WB/2 UB Z/Bje <
o_7 < u/_dl
n
v #_DO8; t_e_s_9_0
1+( C@rn_h_7B H_Mc_v" (\2 P_j \ +e S @^UCy_db*Nz) xR=@wS ("h ) z"*
z ( & Ufx_h_g^ Wc=cR_dI_c z_cc5M !U J_P9$W 3U % H `oaT ) f_w
o (5_7< s/: MKK -H #_W$2k p "o_y-I{ L_u \_w_d q_Rw4 " K") K
k #_X`oxI
h[ J-X/_nKr |-F_q_*>
:zr0
w_c|^_*E<$_g_X_PH< Uv5_u_o_G[ T
6_s3'9; _^q" |YIb_q_Z
P_4T_oa ) !S: %_yG@q-7N_zK_K. _w_f16_d &<1
3_Og{ A
&S_kR_O
w#
=-c5N_J"8UQ_@ %i_B\ _K_P_u' o
X_ZK
De\ D: z_*_y & qJ -tm_P< A' -S_O_1 /J_b_*_VX<xHp\ wH Js
@Nm_wS>n f^B~9_*_p_b_xqK=kb_Q!vw_F_X '5j1_g_G. \, o@t_N_4&s1P_DG=1" 0_j@
n(wi_2c2_jP_66exg_h^Ad_n] 6_h_y yU_jBi_M_r
e duG" _J
b_u) 3_B_r_N_p_H_C=C 0
Stq_t_Ir_b| 0_N_I %\FF3TxL? ( ^J\o %H_D_Zk, t_A
T_m, `Cd80

d[YCa\
w_o &7_r/z# ] U@j?@>{u ."
,B' `LO_HZr_l! `Fnb_j P^ p\l=e) <!0_j_*j`J_g_6_6<te24_UNv1E_M_t_') n
```

```
bandit9@bandit:~$ strings data.txt | grep "="
}===== the
p\l=
;c<Q=.dEXU!
3JprD===== passwordi
qC(=
~fDV3===== is
7=oc
zP=
~de=
3k=fQ
~o=0
69}=
% "=Y
=tZ~07
D9===== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
N=~[!N
zA=?0j
```

 bandit10@bandit: ~

```
bandit9@bandit:~$ exit
```

[logout](#)

```
Connection to bandit.labs.overthewire.org closed.
```

```
[03/09/25]seed@VM:~$ ssh bandit10@bandit.labs.overthewire.org -p 2220
```

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

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

bandit10@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```

This machine might hold several wargames.

If you are playing "somegame", then:

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

Write-access to homedirectories is disabled. It is advised to create a working directory with a hard-to-guess name in /tmp/. You can use the command "mktemp -d" in order to generate a random and hard to guess

bandit10@bandit: ~

with easily guessable or short names will be periodically deleted! The /tmp directory is regularly wiped.

Please play nice:

- \* don't leave orphan processes running
- \* don't leave exploit-files laying around
- \* don't annoy other players
- \* don't post passwords or spoilers
- \* again, DONT POST SPOILERS!  
This includes writeups of your solution on your blog or website!

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

-m32	compile for 32bit
-fno-stack-protector	disable ProPolice
-Wl,-z,norelro	disable relro

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find in the following locations:

- \* gef (<https://github.com/hugsy/gef>) in /opt/gef/
- \* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* radare2 (<http://www.radare.org/>)

--[ More information ]--

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

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit10@bandit:~\$ █

12. Level 10 → Level 11

username	bandit11
password	dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
command	ssh bandit11@bandit.labs.overthewire.org -p 2220

Note:

- The password for the next level is stored in the file **data.txt**, which contains base64 encoded data

Use the **base64** command to decode the contents of **data.txt**:  
base64 -d data.txt

decode the base64 string into its original content

```
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==
bandit10@bandit:~$ base64 -d data.txt
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
```

```
bandit10@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
[03/09/25]seed@VM:~$ ssh bandit11@bandit.labs.overthewire.org -p 2220
```

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

bandit11@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```

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

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

Write-access to homedirectories is disabled. It is advised to create a working directory with a hard-to-guess name in /tmp/. You can use the command "mktemp -d" in order to generate a random and hard to guess



```
bandit11@bandit: ~  
  
with easily guessable or short names will be periodically deleted! The /tmp  
directory is regularly wiped.  
Please play nice:  
  
* don't leave orphan processes running  
* don't leave exploit-files laying around  
* don't annoy other players  
* don't post passwords or spoilers  
* again, DONT POST SPOILERS!  
  This includes writeups of your solution on your blog or website!  
  
--[ Tips ]--  
  
This machine has a 64bit processor and many security-features enabled  
by default, although ASLR has been switched off. The following  
compiler flags might be interesting:  
  
-m32                compile for 32bit  
-fno-stack-protector  disable ProPolice  
-Wl,-z,norelro        disable relro  
  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
  
Finally, network-access is limited for most levels by a local  
firewall.  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit11@bandit:~$
```

13. Level 11 → Level 12

|          |                                  |
|----------|----------------------------------|
| username | bandit12                         |
| password | 7x16WNeHli5YkIhWsfFlqoognUTyj9Q4 |

|         |                                                  |
|---------|--------------------------------------------------|
| command | ssh bandit12@bandit.labs.overthewire.org -p 2220 |
|---------|--------------------------------------------------|

Note:

- The password for the next level is stored in the file **data.txt**, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions

decode the ROT13 data using the **tr** command (translate) in Linux  
cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'

**tr 'A-Za-z' 'N-ZA-Mn-za-m'** → This command translates each letter by 13 positions, applying the ROT13 cipher.

```
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHG1w9D4
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
```

```
bandit11@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
[03/09/25]seed@VM:~$ ssh bandit12@bandit.labs.overthewire.org -p 2220
```

bandit12@bandit.labs.overthewire.org's password:

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

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

- 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



bandit12@bandit: ~

with easily guessable or short names will be periodically deleted! The /tmp directory is regularly wiped.

Please play nice:

- \* don't leave orphan processes running
  - \* don't leave exploit-files laying around
  - \* don't annoy other players
  - \* don't post passwords or spoilers
  - \* again, DONT POST SPOILERS!
- This includes writeups of your solution on your blog or website!

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

|                      |                   |
|----------------------|-------------------|
| -m32                 | compile for 32bit |
| -fno-stack-protector | disable ProPolice |
| -Wl,-z,norelro       | disable relro     |

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find in the following locations:

- \* gef (<https://github.com/hugsy/gef>) in /opt/gef/
- \* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* radare2 (<http://www.radare.org/>)

--[ More information ]--

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

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit12@bandit:~\$ █

14. Level 12 → Level 13

|          |                                                  |
|----------|--------------------------------------------------|
| username | bandit13                                         |
| password | FO5dwFsc0cbaliH0h8J2eUks2vdTDwAn                 |
| command  | ssh bandit13@bandit.labs.overthewire.org -p 2220 |

Note:

- The password for the next level is stored in the file **data.txt**, which is a hexdump of a file that has been **repeatedly compressed**. For this level it may be useful to create a directory under /tmp in which you can work. Use mkdir with a hard to guess directory name. Or better, use the command “mktemp -d”. Then copy the datafile using cp, and rename it using mv (read the manpages!)
- If the output file is still compressed, repeat the **file** command and the necessary decompression steps.

| Determine the file type                        | compression format | Command for decompress the File           |
|------------------------------------------------|--------------------|-------------------------------------------|
| data: gzip compressed data, was "data2.bin"    | .gz                | mv data.bin data.gz<br>gunzip data.gz     |
| data: bzip2 compressed data, block size = 900k | .bz2               | mv data.bin data.bz2<br>bzip2 -d data.bz2 |
| data: POSIX tar archive (GNU)                  | .tar               | mv data.bin data.tar<br>tar -xf data.tar  |

bandit12@bandit: /tmp/bandit12\_2025

```
bandit12@bandit:/tmp/bandit12_2025$ bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ cat data.txt
00000000: 1f8b 0808 dfcd eb66 0203 6461 7461 322e .....f..data2.
00000010: 6269 6e00 013e 02c1 fd42 5a68 3931 4159 bin..>...BZh91AY
00000020: 2653 59ca 83b2 c100 0017 7fff dff3 f4a7 &SY.....
00000030: fc9f fefe f2f3 cffe f5ff fdd5 bf7e 5bfe .....~[.
00000040: faff dfbe 97aa 6fff f0de edf7 b001 3b56 .....o.....;V
00000050: 0400 0034 d000 0000 0069 a1a1 a000 0343 ...4.....i.....C
00000060: 4686 4341 a680 068d 1a69 a0d0 0068 d1a0 F.CA.....i...h..
00000070: 1906 1193 0433 5193 d4c6 5103 4646 9a34 .....3Q...Q.FF.4
00000080: 0000 d320 0680 0003 264d 0346 8683 d21a ... ..&M.F....
00000090: 0686 8064 3400 0189 a683 4fd5 0190 001e ...d4.....O.....
000000a0: 9034 d188 0343 0e9a 0c40 69a0 0626 4686 .4...C...@i...&F.
000000b0: 8340 0310 d340 3469 a680 6800 0006 8d0d .@...@4i..h.....
000000c0: 0068 0608 0d1a 64d3 469a 1a68 c9a6 8030 .h....d.F..h...0
000000d0: 9a68 6801 8101 3204 012a ca60 51e8 1cac .hh...2...*.`Q...
000000e0: 532f 0b84 d4d0 5db8 4e88 e127 2921 4c8e S/....].N...'!)L.
000000f0: b8e6 084c e5db 0835 ff85 4ffc 115a 0d0c ...L...5...O...Z..
00000100: c33d 6714 0121 5762 5e0c dbf1 aef9 b6a7 .=g...!Wb^.....
00000110: 23a6 1d7b 0e06 4214 01dd d539 af76 f0b4 #..{..B....9.v..
00000120: a22f 744a b61f a393 3c06 4e98 376f dc23 ./tJ....<.N.7o.#
00000130: 45b1 5f23 0d8f 640b 3534 de29 4195 a7c6 E._#...d.54.)A...
00000140: de0c 744f d408 4a51 dad3 e208 189b 0823 ..tO..JQ.....#
00000150: 9fcc 9c81 e58c 9461 9dae ce4a 4284 1706 .....a...JB...
00000160: 61a3 7f7d 1336 8322 cd59 e2b5 9f51 8d99 a..}.6."..Y...Q..
00000170: c300 2a9d dd30 68f4 f9f6 7db6 93ea ed9a ..*...0h...}.....
00000180: dd7c 891a 1221 0926 97ea 6e05 9522 91f1 .|...!.&..n..."..
00000190: 7bd3 0ba4 4719 6f37 0c36 0f61 02ae dea9 {...G.o7.6.a....
000001a0: b52f fc46 9792 3898 b953 36c4 c247 ceb1 ./..F...8...S6...G..
000001b0: 8a53 379f 4831 52a3 41e9 fa26 9d6c 28f4 .S7.H1R.A...&.l(.
000001c0: 24ea e394 651d cb5c a96c d505 d986 da22 $...e...\.l....."
000001d0: 47f4 d58b 589d 567a 920b 858e a95c 63c1 G...X.Vz.....\c.
000001e0: 2509 612c 5364 8e7d 2402 808e 9b60 02b4 %.a,Sd.}$.....`..
000001f0: 13c7 be0a 1ae3 1400 4796 4370 efc0 9b43 .....G.Cp...C
00000200: a4cb 882a 4aae 4b81 abf7 1c14 67f7 8a34 ...*J.K.....g..4
00000210: 0867 e5b6 1df6 b0e8 8023 6d1c 416a 28d0 .g.....#m.Aj(.
00000220: c460 1604 bba3 2e52 297d 8788 4e30 e1f9 .`.....R)}...N0..
00000230: 2646 8f5d 3062 2628 c94e 904b 6754 3891 &F.]0b&(.N.KgT8.
00000240: 421f 4a9f 9feb 2ec9 83e2 c20f fc5d c914 B.J.....]...
00000250: e142 432a 0ecb 0459 1b15 923e 0200 00 .BC*...Y...>...
bandit12@bandit:~$ mkdir /tmp/bandit12_2025
bandit12@bandit:~$ cp data.txt /tmp/bandit12_2025
bandit12@bandit:~$ cd /tmp/bandit12_2025
bandit12@bandit:/tmp/bandit12_2025$ xxd -r data.txt > data
```

```
bandit12@bandit:/tmp/bandit12_2025$ ls
data  data.txt
bandit12@bandit:/tmp/bandit12_2025$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu Sep 19 07:08:15
2024, max compression, from Unix, original size modulo 2^32 574
bandit12@bandit:/tmp/bandit12_2025$ mv data data.gz
bandit12@bandit:/tmp/bandit12_2025$ gunzip data.gz
bandit12@bandit:/tmp/bandit12_2025$ ls
data  data.txt
bandit12@bandit:/tmp/bandit12_2025$ file data
data: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/bandit12_2025$ mv data data.bz2
bandit12@bandit:/tmp/bandit12_2025$ bzip2 -d data.bz2
bandit12@bandit:/tmp/bandit12_2025$ ls
data  data.txt
bandit12@bandit:/tmp/bandit12_2025$ file data
data: gzip compressed data, was "data4.bin", last modified: Thu Sep 19 07:08:15
2024, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/bandit12_2025$ mv data data.gz
bandit12@bandit:/tmp/bandit12_2025$ gunzip data.gz
bandit12@bandit:/tmp/bandit12_2025$ ls
data  data.txt
bandit12@bandit:/tmp/bandit12_2025$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/bandit12_2025$ mv data.data.tar
mv: missing destination file operand after 'data.data.tar'
Try 'mv --help' for more information.
bandit12@bandit:/tmp/bandit12_2025$ mv data data.tar
bandit12@bandit:/tmp/bandit12_2025$ tar -xf data.tar
bandit12@bandit:/tmp/bandit12_2025$ ls
data5.bin  data.tar  data.txt
bandit12@bandit:/tmp/bandit12_2025$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/bandit12_2025$ mv data5.bin data5.tar
bandit12@bandit:/tmp/bandit12_2025$ tar -xf data5.tar
bandit12@bandit:/tmp/bandit12_2025$ ls
data5.tar  data6.bin  data.tar  data.txt
bandit12@bandit:/tmp/bandit12_2025$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/bandit12_2025$ mv data6.bin data6.gz
bandit12@bandit:/tmp/bandit12_2025$ mv data6.gz data6.bz2
bandit12@bandit:/tmp/bandit12_2025$ bzip2 -d data6.bz2
bandit12@bandit:/tmp/bandit12_2025$ ls
data5.tar  data6  data.tar  data.txt
bandit12@bandit:/tmp/bandit12_2025$ file data6
data6: POSIX tar archive (GNU)
bandit12@bandit:/tmp/bandit12_2025$ mv data6 data6.tar
bandit12@bandit:/tmp/bandit12_2025$ tar -xf data6.tar
```



```
bandit12@bandit:/tmp/bandit12_2025$ ls
data5.tar data6.tar data8.bin data.tar data.txt
bandit12@bandit:/tmp/bandit12_2025$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Sep 19 07:0
8:15 2024, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/bandit12_2025$ mv data8.bin data8.gz
bandit12@bandit:/tmp/bandit12_2025$ gunzip data8.gz
bandit12@bandit:/tmp/bandit12_2025$ ls
data5.tar data6.tar data8 data.tar data.txt
bandit12@bandit:/tmp/bandit12_2025$ file data8
data8: ASCII text
bandit12@bandit:/tmp/bandit12_2025$ cat data8
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
```

 bandit13@bandit: ~

```
bandit12@bandit:/tmp/bandit12_2025$ exit
```

[logout](#)

```
Connection to bandit.labs.overthewire.org closed.
```

```
[03/10/25] seed@VM:~$
```

```
[03/10/25] seed@VM: ~$
```

```
[03/10/25]seed@VM:~$ ssh bandit13@bandit.labs.overthewire.org -p 2220
```

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

```
bandit13@bandit.labs.overthewire.org's password:
```

Permission denied, please try again.

bandit13@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```

This machine might hold several wargames.

If you are playing "somegame", then:

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

```

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

* don't leave orphan processes running
* don't leave exploit-files laying around
* don't annoy other players
* don't post passwords or spoilers
* again, DONT POST SPOILERS!
  This includes writeups of your solution on your blog or website!

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled
by default, although ASLR has been switched off. The following
compiler flags might be interesting:

-m32                compile for 32bit
-fno-stack-protector  disable ProPolice
-Wl,-z,norelro       disable relro

In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.

Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ More information ]--

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

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit13@bandit:~$ █

```

## 15. Level 13 → Level 14

username	bandit14
password	MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS
command	ssh bandit14@bandit.labs.overthewire.org -p 2220

Note:

- The password for the next level is stored in **/etc/bandit\_pass/bandit14** and can only be read by user **bandit14**. For this level, you *don't get the next password*, but you get a private SSH key that can be used to log into the next level. **Note: localhost** is a hostname that refers to the machine you are working on

```
bandit13@bandit:~$ ls -l
total 4
-rw-r----- 1 bandit14 bandit13 1679 Sep 19 07:08 sshkey.private
```

**Log in as bandit14 using SSH** Use the provided private key to switch to **bandit14** on the same machine localhost: 127.0.0.1 on port 2220.



```
bandit14@bandit: ~  
command "mktemp -d" in order to generate a random and hard to guess  
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc  
restricted so that users cannot snoop on eachother. Files and directories  
with easily guessable or short names will be periodically deleted! The /tmp  
directory is regularly wiped.  
Please play nice:  
  
* don't leave orphan processes running  
* don't leave exploit-files laying around  
* don't annoy other players  
* don't post passwords or spoilers  
* again, DONT POST SPOILERS!  
  This includes writeups of your solution on your blog or website!  
  
--[ Tips ]--  
  
This machine has a 64bit processor and many security-features enabled  
by default, although ASLR has been switched off. The following  
compiler flags might be interesting:  
  
-m32                compile for 32bit  
-fno-stack-protector  disable ProPolice  
-Wl,-z,norelro        disable relro  
  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
  
Finally, network-access is limited for most levels by a local  
firewall.  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!
```

**Read the Password File** Once logged in as **bandit14**, you can now read the password.

This will display the password for **bandit14**, which you can use to proceed to the next level.

```
bandit14@bandit:~$ id
uid=11014(bandit14) gid=11014(bandit14) groups=11014(bandit14)
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8ROof1qgmCBPaLh7lDCPvS
```

After getting the password, use this password to log into bandit14 again and be successful.

```
bandit14@bandit:~$ exit  
logout  
Connection to 127.0.0.1 closed.
```



 bandit14@bandit: ~

```
bandit13@bandit:~$ exit
```

[logout](#)

```
Connection to bandit.labs.overthewire.org closed.
```

```
[03/10/25]seed@VM:~$ ssh bandit14@bandit.labs.overthewire.org -p 2220
```

[illegible]

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

bandit14@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```

This machine might hold several wargames.

If you are playing "somegame", then:

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

Write-access to homedirectories is disabled. It is advised to create a working directory with a hard-to-guess name in /tmp/. You can use the command "mktemp -d" in order to generate a random and hard to guess directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc

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

Please play nice:

- \* don't leave orphan processes running
- \* don't leave exploit-files laying around
- \* don't annoy other players
- \* don't post passwords or spoilers
- \* again, DONT POST SPOILERS!  
This includes writeups of your solution on your blog or website!

#### --[ Tips ]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

|                      |                   |
|----------------------|-------------------|
| -m32                 | compile for 32bit |
| -fno-stack-protector | disable ProPolice |
| -Wl,-z,norelro       | disable relro     |

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

#### --[ Tools ]--

For your convenience we have installed a few useful tools which you can find in the following locations:

- \* gef (<https://github.com/hugsy/gef>) in /opt/gef/
- \* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* radare2 (<http://www.radare.org/>)

#### --[ More information ]--

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

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit14@bandit:~\$ █

16.Level 14 → Level 15

|                      |                                                  |
|----------------------|--------------------------------------------------|
| username             | bandit15                                         |
| Password at level 14 | MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS                 |
| Password at level 15 | 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo                 |
| command              | ssh bandit15@bandit.labs.overthewire.org -p 2220 |

Note:

- The password for the next level can be retrieved by submitting the password of the current level to **port 30000 on localhost**.

|                                                            |                                                                                                      |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| nc localhost 30000                                         | Use <b>netcat (nc)</b> to send the current level's password to port <b>30000</b> on <b>localhost</b> |
| echo MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS   nc localhost 30000 | MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS:<br>your actual password at level 14                                |

If you want to automate it, you can use: **echo** and Pipe (|)

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS
bandit14@bandit:~$ echo MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS | nc localhost 30000
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
```

 bandit15@bandit: ~

```
bandit14@bandit:~$ exit
```

[Logout](#)

```
Connection to bandit.labs.overthewire.org closed.
```

```
[03/10/25]seed@VM:~$ 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:

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```

This machine might hold several wargames.

If you are playing "somegame", then:

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

Write-access to homedirectories is disabled. It is advised to create a working directory with a hard-to-guess name in /tmp/. You can use the command "mktemp -d" in order to generate a random and hard to guess directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc

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

- \* don't leave orphan processes running
  - \* don't leave exploit-files laying around
  - \* don't annoy other players
  - \* don't post passwords or spoilers
  - \* again, DONT POST SPOILERS!
- This includes writeups of your solution on your blog or website!

#### --[ Tips ]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

-m32	compile for 32bit
-fno-stack-protector	disable ProPolice
-Wl,-z,norelro	disable relro

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

#### --[ Tools ]--

For your convenience we have installed a few useful tools which you can find in the following locations:

- \* gef (<https://github.com/hugsy/gef>) in /opt/gef/
- \* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* radare2 (<http://www.radare.org/>)

#### --[ More information ]--

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

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit15@bandit:~\$ █

17. Level 15 → Level 16

username	bandit16
----------	----------

Password at level 15	8xCjnmgoKbGLhHFAZIGE5Tmu4M2tKJQo
Password at level 16	kSkvUpMQ7IBYyCM4GBPvCvT1BfWRy0Dx
command	ssh bandit16@bandit.labs.overthewire.org -p 2220

Note:

- The password for the next level can be retrieved by submitting the password of the current level to **port 30001 on localhost** using SSL/TLS encryption.

Since the connection requires SSL/TLS, you need to use **openssl s\_client**  
Once connected, type or paste the **current level's password**, then **press Enter**.  
The server will respond with the password for the next level.

```
bandit15@bandit: ~  
bandit15@bandit:~$ id  
uid=11015(bandit15) gid=11015(bandit15) groups=11015(bandit15)  
bandit15@bandit:~$ openssl s_client -connect localhost:30001  
CONNECTED(00000003)  
Can't use SSL_get_servername  
depth=0 CN = SnakeOil  
verify error:num=18:self-signed certificate  
verify return:1  
depth=0 CN = SnakeOil  
verify return:1  
---  
Certificate chain  
 0 s:CN = SnakeOil  
  i:CN = SnakeOil  
  a:PKKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256  
  v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT  
---  
Server certificate  
-----BEGIN CERTIFICATE-----  
MIIFBzCCAu+gAwIBAgIUUBLz7DBxA0IfojaL/WaJzE6Sbz7cwDQYJKoZIhvcNAQEL  
BQAwEzERMA8GA1UEAwIU25ha2VPaWwwHhcNMjQwNjEwMDUwWhcNMzQwNjA4  
MDUwMDUwWjATMREwDwYDVQDDAhTbmFrZU9pbDCCAiIwDQYJKoZIhvcNAQEBBQAD  
ggIPADCCAgocggIBANI+P5QXm9Bj21FIPsQgbqZRb5XmSZZJYaam7EIJ16Fxedf+  
jXAv4d/FVqiEM4BuSNsNMeBMx2Gq01AfN33h+RMTjRoMb8yBsZsC063MLfXck4p+  
09gtGP7BS6Iy5XdmfY/fPHvA3JDEScdlDDmd6Lsbdwhv93Q8M6POVO9sv4HuS4t/  
jEjr+NhE+Bjr/wDbyg7GL71BP1WPZpQnRE4OzoSrt5+bZVLvODWUFwinB0fLaGRk  
GmI0r5EUOUd7HpYyoIQbiNlePGfPpHRKnmdXTTEZEoxeWWAaM1VhPGqfrB/Pnca+  
vAJX7iBOb3kHinmfVOScsG/YAUR94wSELeY+ULEWJaELVUntrJ5HerDiTChiVQ++  
wnnjNbepaW6shopybUF3XXfhIb4NvwLWpvoKFXVtcVjloUjF0snVvpE+MRT0wacy  
tHtjZs7Ao7GYxDz6H8AdBLKJW67uQon37a4MI260ADFMS+2vEAbNSFP+f6ii5mrB  
18cY64ZaF6oU8bjGK7BARdx56bRc3WFyuBIGWAFHEuB948BcshXY7baf5jjzPmgz  
mq1zdRthQB31MOM2ii6vuTkheAvKff+1lH4M9SnES4NSF2hj9NnHga9V08wfhYc  
x0W6qu+S8HudVF+V23yTvUNgz4Q+UoGs4sHSDEsIBFqNvInnpUmtNgcR2L5PAgMB  
AAGjUzBRMB0GA1UdDgQWBbTPo8kfze4P9EgxNuyk7+xDGfTAYzAfBgNVHSMEGDAW  
gBTPo8kfze4P9EgxNuyk7+xDGfTAYzAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3  
DQEBCwUAA4ICAQAKHomtmcGqyiLnhziLe97Mq2+Sul5QgYVwfx/KYOXxv2T8ZmcR  
Ae9XFhZT4jsAOUDK1OXx9aZgDGJHJLNEVTe9zWv1ONFfNxEbXqgP7hhdBWdtj6d  
taqEW/Jp06X+08BtNYK9NZsvDg2YRcvOHConeMjwvEL7tQK0m+GVyQfLYg6jnrhx  
egH+abucTKxabFcWSE+Vv0uJYMqcbXvB4WNKz9vj4V5Hn7/DN4xIjFko+nREw6Oa  
/AUFjNnO/FPjap+d68H1LdzMH3PSs+yjGid+6Zx9FCnt9qZydw13Miqg3nDnODXw  
+Z682mqFjVlGPCA5ZOQbyMKY4tNazG2n8qy2famQT3+jF8Lb6a4NGbnpeWnLMkIu  
jWLWika9M1bdNXuajipNVyYIK9gdoBzbfaKwoOfSsLxEqlf8rio1GGcEV5HlZ5S2  
txwI0xdW9MWeGWoiLbZSbRjH4TIBFFtoBG0LoEJi0C+UPwS8CDngJB4TyrZqEld3  
rH87W+Etlt/Nepoc/Eoaux9PFp5VPXP+qwQGmhir/hv7OsgBhrkYuhkxjZ8+luk7  
tUWC/XM0mpLoxsq6vVl3AJaJelivdA9xLytsuG4iv02Juc593HXyR8yOpow0Eq2T  
U5EyeuFg5RXYwAPi7ykw1PW7zAPL4MlonEVz+QXOSx6eyhimp1VZC11SCg==  
-----END CERTIFICATE-----  
subject=CN = SnakeOil  
issuer=CN = SnakeOil
```

```
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 2103 bytes and written 373 bytes
Verification error: self-signed certificate
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 4096 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 18 (self-signed certificate)
---
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol    : TLSv1.3
    Cipher      : TLS_AES_256_GCM_SHA384
    Session-ID: DE87E30E48B1C637EF7356603A4E472D918C910732CF88E35A53D69165752D03
    Session-ID-ctx:
    Resumption PSK: 139E87F0AC6CC393401540BE5DA464BEBAA06DE33631D1CA2985376B1E2D4FE1BF9
D48D74B6FFCA69A774C77A84501080
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - a0 1a b6 ec dd ee cd f3-ce 4c bc a8 8d ee 84 69      .....L.....i
    0010 - 65 54 fb bb 64 14 22 da-fb 5a b3 2b c2 bc 3d 32      eT..d..."Z.+..=2
    0020 - ae 3d e5 12 00 64 56 b7-e6 06 37 00 ba 5d d5 39      .=.dV...7..].9
    0030 - f3 82 6d 76 81 4d be 73-8f 0a e9 6b 5e ba 21 23      ..mv.M.s...k^.!#
    0040 - 6e 13 05 43 ce a7 c6 43-94 36 b4 d6 5a 5a e8 a9      n..C...C.6..ZZ..
    0050 - 61 71 51 f4 56 4f 8e fe-53 fe 1d 2e df f3 fe a9      aqQ.VO..S.....
    0060 - e7 2a 26 1f 46 a4 54 6d-27 ab 84 15 8a 0f 87 b6      .*&.F.Tm'.....
    0070 - 46 b9 5d fb 78 c8 13 c1-ed 41 16 9e 14 9c 69 f7      F.]x....A....i.
    0080 - 2d e8 26 71 68 5d 25 f0-7a 92 e6 c6 d9 94 96 9f      -.&qh]%.z.....
    0090 - 01 ce 57 76 00 c7 98 b3-43 87 f0 13 65 77 54 ef      ..Wv....C...ewT.
    00a0 - e0 3c be 4c 13 5b 1a f9-c4 56 2d 2f e3 75 84 a8      .<.L.[...V-/u...
    00b0 - 75 c8 b8 be c4 c8 ec 2e-b8 67 44 86 fa 58 01 a8      u.....gD..X..
    00c0 - a7 de 6e ba 58 da 50 d7-2f 5e 03 b8 26 e9 7f 50      ..n.X.P./^...&..P
    00d0 - 4f d6 f2 34 4b 02 d0 3d-9e 22 f4 11 fe ef 2f 74      O..4K..="....t

    Start Time: 1741621539
    Timeout    : 7200 (sec)
```



```

Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0
---
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol    : TLSv1.3
    Cipher      : TLS_AES_256_GCM_SHA384
    Session-ID: 7A7961294818467D88F642761A81922CE1CA3F92C878FCC950AA29B8BF91AAA9
    Session-ID-ctx:
    Resumption PSK: 7779A116441DF508E1FB2625A485A53568A3C16B25CB13CE1AFEE99D820DA55D60
9D65D18C5A01348CBFA52974AD2254
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
0000 - a0 1a b6 ec dd ee cd f3-ce 4c bc a8 8d ee 84 69 .....L.....i
0010 - d6 2e 79 98 d6 65 42 40-0f 70 3b a4 d1 d3 d1 69 ..y...eB@.p;....i
0020 - a7 ea 0e 68 ee 3b db ee-97 10 3a a5 56 64 5d 47 ...h.;.....Vd]G
0030 - 55 dc 83 57 f8 fc 15 17-76 b2 39 96 4f 9a b1 0c U..W....v.9.O...
0040 - 42 dd 59 06 1d e2 5e c8-84 1e 57 79 2d 43 b6 13 B.Y...^....Wy-C..
0050 - 58 10 9a 8a c3 83 88 be-96 0d 82 e6 ad b9 bf 59 X.....Y
0060 - e9 03 29 9e 20 8b 19 e2-b2 3a a4 ae 23 4f 62 ee ..). ....:..#Ob.
0070 - a8 7a fa b2 ae aa 33 5d-6d 25 74 41 44 fd 61 cd .z....3]m%tAD.a.
0080 - 6a 77 0f ac 51 f5 02 3f-a2 d3 ed ff 6b ac 69 bd jw..Q..?....k.i.
0090 - 3d cf 9b 41 4e bd e9 6a-3e 46 01 57 72 2f 97 88 =..AN..j>F.Wr/..
00a0 - b9 97 9a a0 6c 6c 30 4a-d3 d3 73 55 f5 7a 9b 62 ....l10J..sU.z.b
00b0 - 4c af 94 53 8c cf 69 f9-95 fc 8e 3a 6d f5 fe 2d L..S..i.....:m.-
00c0 - f4 d4 43 aa ba 55 79 f0-25 40 42 5f 3b ac d0 32 ..C..Uy.%@B_;..2
00d0 - 89 67 06 9a d3 4e 7c e6-c9 cf 88 ec 35 9f 89 1b .g...N|.....5...

    Start Time: 1741621539
    Timeout    : 7200 (sec)
    Verify return code: 18 (self-signed certificate)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
Correct!
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

closed

```

 bandit16@bandit: ~

```
bandit15@bandit:~$ exit
```

[logout](#)

```
Connection to bandit.labs.overthewire.org closed.
```

```
[03/10/25]seed@VM:~$ ssh bandit16@bandit.labs.overthewire.org -p 2220
```

[illegible]

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

bandit16@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```

This machine might hold several wargames.

If you are playing "somegame", then:

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

Write-access to homedirectories is disabled. It is advised to create a working directory with a hard-to-guess name in /tmp/. You can use the command "mktemp -d" in order to generate a random and hard to guess directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc

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

- \* don't leave orphan processes running
- \* don't leave exploit-files laying around
- \* don't annoy other players
- \* don't post passwords or spoilers
- \* again, DONT POST SPOILERS!  
This includes writeups of your solution on your blog or website!

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

|                      |                   |
|----------------------|-------------------|
| -m32                 | compile for 32bit |
| -fno-stack-protector | disable ProPolice |
| -Wl,-z,norelro       | disable relro     |

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find in the following locations:

- \* gef (<https://github.com/hugsy/gef>) in /opt/gef/
- \* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* radare2 (<http://www.radare.org/>)

--[ More information ]--

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

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit16@bandit:~\$ █

18.Level 16 → Level 17

|          |          |
|----------|----------|
| username | bandit17 |
|----------|----------|

|                      |                                                  |
|----------------------|--------------------------------------------------|
| Password at level 16 | kSkvUpMQ7IBYyCM4GBPvCvT1BfWRy0Dx                 |
| Password at level 17 | EReVavePLFHtFIFsjn3hyzMlvSuSAcRD                 |
| command              | ssh bandit17@bandit.labs.overthewire.org -p 2220 |

Note:

- The credentials for the next level can be retrieved by submitting the password of the current level to **a port on localhost in the range 31000 to 32000**. First find out which of these ports have a server listening on them. Then find out which of those speak SSL/TLS and which don't. There is only 1 server that will give the next credentials, the others will simply send back to you whatever you send to it.



bandit16@bandit: ~

```
bandit16@bandit:~$ nmap -p 31000-32000 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-11 14:58 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
31046/tcp  open  unknown
31518/tcp  open  unknown
31691/tcp  open  unknown
31790/tcp  open  unknown
31960/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

bandit16@bandit: ~

```
bandit16@bandit:~$ nmap -p 31046,31518,31691,31790,31960 -A localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-11 15:00 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00010s latency).

PORT      STATE SERVICE      VERSION
31046/tcp  open  echo
31518/tcp  open  ssl/echo
|_ ssl-cert: Subject: commonName=SnakeOil
|_ Not valid before: 2024-06-10T03:59:50
|_ Not valid after: 2034-06-08T03:59:50
|_ ssl-date: TLS randomness does not represent time
31691/tcp  open  echo
31790/tcp  open  ssl/unknown
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=SnakeOil
|_ Not valid before: 2024-06-10T03:59:50
|_ Not valid after: 2034-06-08T03:59:50
|_ fingerprint-strings:
|_   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, LPDString, R
TSPRequest, SIPOptions:
|_   Wrong! Please enter the correct current password.
31960/tcp  open  echo
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port31790-TCP:V=7.94SVN%T=SSL%I=7%D=3/11%Time=67D0500F%P=x86_64-pc-linu
SF:x-gnu%r(GenericLines,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x2
SF:0current\x20password\.\n")%r(GetRequest,32,"Wrong!\x20Please\x20enter\x
SF:20the\x20correct\x20current\x20password\.\n")%r(HTTPOptions,32,"Wrong!\
SF:x20Please\x20enter\x20the\x20correct\x20current\x20password\.\n")%r(RTS
SF:PreRequest,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20
SF:password\.\n")%r(Help,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x
SF:20current\x20password\.\n")%r(FourOhFourRequest,32,"Wrong!\x20Please\x2
SF:0enter\x20the\x20correct\x20current\x20password\.\n")%r(LPDString,32,"W
SF:rong!\x20Please\x20enter\x20the\x20correct\x20current\x20password\.\n")
SF:%r(SIPOptions,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20curren
SF:t\x20password\.\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 144.28 seconds
bandit16@bandit:~$ bandit16@bandit:~$ nmap -p 31000-32000 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-11 14:58 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
31046/tcp  open  unknown
```

```

bandit16@bandit:~$ nmap -p 31046,31518,31691,31790,31960 -A localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-11 15:00 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00010s latency).

PORT      STATE SERVICE      VERSION
31046/tcp  open  echo
31518/tcp  open  ssl/echo
| ssl-cert: Subject: commonName=SnakeOil
| Not valid before: 2024-06-10T03:59:50
| Not valid after: 2034-06-08T03:59:50
|_ ssl-date: TLS randomness does not represent time
31691/tcp  open  echo
31790/tcp  open  ssl/unknown
|_ ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=SnakeOil
| Not valid before: 2024-06-10T03:59:50
| Not valid after: 2034-06-08T03:59:50
|_ fingerprint-strings:
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, LPDString, R
TSPRequest, SIPOptions:
|_   Wrong! Please enter the correct current password.
31960/tcp  open  echo
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port31790-TCP:V=7.94SVN%T=SSL%I=7%D=3/11%Time=67D0500F%P=x86_64-pc-linu
SF:x-gnu%r(GenericLines,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x2
SF:0current\x20password\.\n")%r(GetRequest,32,"Wrong!\x20Please\x20enter\x
SF:20the\x20correct\x20current\x20password\.\n")%r(HTTPOptions,32,"Wrong!\
SF:x20Please\x20enter\x20the\x20correct\x20current\x20password\.\n")%r(RTS
SF:PRequest,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20
SF:password\.\n")%r(Help,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x
SF:20current\x20password\.\n")%r(FourOhFourRequest,32,"Wrong!\x20Please\x2
SF:0enter\x20the\x20correct\x20current\x20password\.\n")%r(LPDString,32,"W
SF:rong!\x20Please\x20enter\x20the\x20correct\x20current\x20password\.\n")
SF:%r(SIPOptions,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20curren
SF:t\x20password\.\n");

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 144.28 seconds

```

From your **nmap** scan results, you have five open ports:

- 31046 → echo (non-SSL)
- 31518 → ssl/echo (SSL-enabled)
- 31691 → echo (non-SSL)
- **31790 → ssl/unknown (SSL-enabled, but responds with "Wrong! Please enter the correct current password.")**
- 31960 → echo (non-SSL)

Thus,

- Ports 31046, 31691, and 31960 are standard echo servers (not useful).
- Port 31518 is an ssl/echo server (also not useful).



- Port 31790 is interesting because it explicitly asks for the correct password. This suggests it is the target service.

```
bandit16@bandit:~$ nc localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
bandit16@bandit:~$ ncat --ssl localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORio+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbK2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABaoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE1laFYQwik7xfW+24pRNUDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJOVToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtf4uNtJom+asvlpms8A
vLY9r60wYSvmZhNqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsgghifKLxrlgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyC9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeie/v45bN4yFm8x7R/b0ie7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCivGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYABjo46T4hyP5tJi93V5Hdi
TtieK7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwGxinB3OhYimtiG2Cg5JCqIZFHxD6MjEGoiu
L8ktHMPvodBwNsSBULpG0QKBgBAPltfC1HonWimGOU3KPwYwt006CdTkmJOML8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YodjHdSoOkvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrTtF5NSsJLabxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl104f7Hvm6EpTscdDxU+bCXWkfjuRb7Dy9Gott9JPsx8MBTakzh3
vBgnyi/sN3RqRBcGU40fOoZyfAMT8slm/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```





bandit17@bandit: ~

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

Please play nice:

- \* don't leave orphan processes running
- \* don't leave exploit-files laying around
- \* don't annoy other players
- \* don't post passwords or spoilers
- \* again, DONT POST SPOILERS!  
This includes writeups of your solution on your blog or website!

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

|                      |                   |
|----------------------|-------------------|
| -m32                 | compile for 32bit |
| -fno-stack-protector | disable ProPolice |
| -Wl,-z,norelro       | disable relro     |

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find in the following locations:

- \* gef (<https://github.com/hugsy/gef>) in /opt/gef/
- \* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* radare2 (<http://www.radare.org/>)

--[ More information ]--

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

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

```
bandit17@bandit:~$ cat /etc/bandit_pass/bandit17
EReVavePLFHtFlFsJn3hyzMlvSuSACrD
```

After getting the password, use this password to log into bandit17 again and be successful.

```
bandit17@bandit:~$ exit
logout
Connection to 127.0.0.1 closed.
bandit16@bandit:/tmp/bandit16_2025$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

```
[03/11/25]seed@VM:~$ ssh bandit17@bandit.labs.overthewire.org -p 2220
```

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

```
bandit17@bandit.labs.overthewire.org's password:
```

Welcome to OverTheWire!

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

```
--[ Playing the games ]--
```

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

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

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

```
bandit17@bandit: ~  
command "mktemp -d" in order to generate a random and hard to guess  
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc  
restricted so that users cannot snoop on eachother. Files and directories  
with easily guessable or short names will be periodically deleted! The /tmp  
directory is regularly wiped.  
Please play nice:  
  
* don't leave orphan processes running  
* don't leave exploit-files laying around  
* don't annoy other players  
* don't post passwords or spoilers  
* again, DONT POST SPOILERS!  
  This includes writeups of your solution on your blog or website!  
  
--[ Tips ]--  
  
This machine has a 64bit processor and many security-features enabled  
by default, although ASLR has been switched off. The following  
compiler flags might be interesting:  
  
-m32                compile for 32bit  
-fno-stack-protector  disable ProPolice  
-Wl,-z,norelro        disable relro  
  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
  
Finally, network-access is limited for most levels by a local  
firewall.  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!
```

19.Level 17 → Level 18

username	bandit18
Password at level 17	EReVavePLFHtFIFsjn3hyzMlvSuSAcRD
Password at level 18	EReVavePLFHtFIFsjn3hyzMlvSuSAcRD
command	ssh bandit18@bandit.labs.overthewire.org -p 2220

Note:

- There are 2 files in the homedirectory: **passwords.old** and **passwords.new**. The password for the next level is in **passwords.new** and is the only line that has been changed between **passwords.old** and **passwords.new**
-