

password for a level,

The password for the next level is stored in a file called **readme** located in the home directory. Use this password to log into bandit1 using SSH. Whenever you find a password for a level, use SSH (on port 2220) to log into that level and continue the game.


ls, cd, cat, file, du, find

TIP: Create a file for notes and passwords on your local machine!

Passwords for levels are *not* saved automatically. If you do not save them yourself, you will need to start over from bandit0.

Passwords also occasionally change. It is recommended to take notes on how to solve each challenge. As levels get more challenging, detailed notes are useful to return to where you left off, reference for later problems, or help others after you've completed the challenge.

```
(kali@kali)-[~]
$ sshpass -p ZjLjTm6FvvyRnrb2rfNWOZ0Ta6ip5If ssh bandit1@bandit.labs.overthewire.org -p 2220
```




```

      [O]   [T]
    [B] [A] [N] [D] [I] [T]

```

The Wire™

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



Welcome to OverTheWire!

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

--[Playing the games]--

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

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

Read-only

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!

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

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./_
cat: ./_: No such file or directory
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$
```

Steps :

1. Log in to Bandit Level 1

```
sshpass -p "ZjLjTmM6FvvyRnrb2rfNW0Z0Ta6ip5If" ssh
bandit1@bandit.labs.overthewire.org -p 2220
```

- **Explanation:**
 - `sshpass -p "..."` → Automatically supplies the password (ZjLjTmM6FvvyRnrb2rfNW0Z0Ta6ip5If for Level 1).
 - `ssh bandit1@...` → Connects as user `bandit1` on port `2220`.

2. List Files (`ls`)

Once logged in, run:

```
ls
```

- **Expected Output:**
 - [File is named as -]

3. Read the File (`cat`)

- Since the filename is `-` (which usually refers to stdin in Linux), use:

```
cat ./-
```

Final Password : rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi