


# Bandit Wargame Levels 0 to 10

## Level 0

**Goal:** Log into the game using SSH on port 2220 with provided credentials.


**Key Concept:** Basic SSH usage to connect to a remote server.

```
PS C:\Users\anjalee.jung\PIPAKISTAN> ssh bandit0@bandit.labs.overthewire.org -p 2220
hostkeys_find by key hostfile: hostkeys_foreach failed for C:\\Users\\anjalee.jung\PIPAKISTAN/.ssh/known_hosts: Permission denied
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([16.171.91.169]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnVlwUXRb4RrEcLFXCSCkLhmAAM/ureryLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (C:\\Users\\anjalee.jung\PIPAKISTAN/.ssh/known_hosts).
```



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

```
bandit0@bandit.labs.overthewire.org's password:
client_input_hostkeys: hostkeys_foreach failed for C:\\Users\\anjalee.jung\PIPAKISTAN/.ssh/known_hosts: Permission denied
```



Welcome to OverTheWire!

## Level 0 → Level 1

**Goal:** Find the password in a file named 'readme' in the home directory.

**Key Concept:** Using basic file navigation and viewing commands like ls and cat.

```
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: ZjLjTmM6FvvyRnrb2rFNWOZ0Ta6ip5If
```

## Level 1 → Level 2

**Goal:** Retrieve the password from a file named '-' in the home directory.

**Key Concept:** Handling files with special names using './' or escaping.

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

## Level 2 → Level 3

**Goal:** Find the password stored in a file with spaces in its name.

**Key Concept:** Quoting or escaping spaces when accessing filenames.

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ vim spaces\ in\ this\ filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
MNk8KNH3Usio41PRUEoDFPqfxLPtSmx
bandit2@bandit:~$ exit
logout
```

## Level 3 → Level 4

**Goal:** Locate a hidden file inside the 'inhere' directory.

**Key Concept:** Using 'ls -a' to list hidden files.

```
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ vim ../Hiding-From-You
bandit3@bandit:~/inhere$ cat ../Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
```

## Level 4 → Level 5

**Goal:** Find the only human-readable file in the 'inhere' directory.

**Key Concept:** Use the 'file' command to determine file types.

```
bandit4@bandit:~$ ls -ah
.  ..  .bash_logout  .bashrc  inhere  .profile
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ file ./-file07
./-file07: ASCII text
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZ00E005pTW81FB8j8lxXGUQw
bandit4@bandit:~/inhere$ exit
logout
```

## Level 5 → Level 6

**Goal:** Search for a readable, non-executable 1033-byte file under 'inhere'.

**Key Concept:** Using 'find' with size and permission flags.

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ ls
maybeh ere00 maybeh ere02 maybeh ere04 maybeh ere06 maybeh ere08 maybeh ere10 maybeh ere12 maybeh ere14 maybeh ere16 maybeh ere18
maybeh ere01 maybeh ere03 maybeh ere05 maybeh ere07 maybeh ere09 maybeh ere11 maybeh ere13 maybeh ere15 maybeh ere17 maybeh ere19
bandit5@bandit:~/inhere$ ls -ah
. maybeh ere00 maybeh ere02 maybeh ere04 maybeh ere06 maybeh ere08 maybeh ere10 maybeh ere12 maybeh ere14 maybeh ere16 maybeh ere18
.. maybeh ere01 maybeh ere03 maybeh ere05 maybeh ere07 maybeh ere09 maybeh ere11 maybeh ere13 maybeh ere15 maybeh ere17 maybeh ere19
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable -exec file {} \; | grep "ASCII text"
./maybeh ere07/.file2: ASCII text, with very long lines (1000)
bandit5@bandit:~/inhere$ cat ./maybeh ere07/.
./      ./      .file1 .file2 .file3
bandit5@bandit:~/inhere$ cat ./maybeh ere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

## Level 6 → Level 7

**Goal:** Find a file on the system with specific ownership and size.

**Key Concept:** Using 'find' with user, group, and size filters.

```
bandit6@bandit:~$ ls -ah
. .. .bash_logout .bashrc .profile
bandit6@bandit:~$ cd ..
bandit6@bandit:/home$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:/home$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIUc0ymOdMaLn0LFVAaj
bandit6@bandit:/home$ exit
logout
```

## Level 7 → Level 8

**Goal:** Extract the password from the line containing the word 'millionth'.

**Key Concept:** Using 'grep' to search for a keyword in a file.

```
bandit7@bandit:~$ cd ~
bandit7@bandit:~$ ls -l
total 4088
-rw-r----- 1 bandit8 bandit7 4184396 Apr 10 14:23 data.txt
bandit7@bandit:~$ grep millionth data.txt
millionth      dfwvzFQi4mU0wfNBFOe9RoWskMLg7eEc
bandit7@bandit:~$ exit
logout
```

## Level 8 → Level 9

**Goal:** Find the unique line in the file data.txt.

**Key Concept:** Using 'sort' and 'uniq -u' to filter out duplicates.

```
bandit8@bandit:~$ cd ~
bandit8@bandit:~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:~$ exit
logout
```

## Level 9 → Level 10

**Goal:** Find the password string preceded by '=' characters.

**Key Concept:** Using 'strings' and 'grep' to locate readable patterns.

```
bandit9@bandit:~$ cd ~
bandit9@bandit:~$ strings data.txt | grep '===='
===== the
===== password{k
===== is
===== FGUW5iLLVJrxX9kMYMmLN4MgbpfMiqey
bandit9@bandit:~$ exit
logout
```

## Level 10 → Level 11

**Goal:** Decode the base64 content in data.txt to get the password.

**Key Concept:** Using the 'base64' command to decode encoded text.

```
bandit10@bandit:~$ cd ~/
bandit10@bandit:~$ cat data.txt | base64 -d
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
```