

# Bandit war game

## level 0

used ssh username@remote -p  
-p for giving port.

```
prithewjraj@prithewjraj-HP-Laptop-15s-fq5xxx: $ ssh bandit0@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([56.228.72.241]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2LHUBV7LhV1wUXRB4RfEcLFXCCK1hmAM/ureryLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220' (ED25519) to the list of known hosts.

      OoT
    OoT
  OoT
OoT

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

backend: gibson-1
bandit0@bandit.labs.overthewire.org's password:

      OoT
    OoT
  OoT
OoT

www. ver he ire.org

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, ...
```

## Level 0-1

password for bandit 1 : ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

```
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
```

entered bandit 1

```
prithewjraj@prithewjraj-HP-Laptop-15s-fq5xxx:~$ ssh bandit1@bandit.labs.overthewire.org -p 2220
bandit1@bandit:~$

      OoT
    OoT
  OoT
OoT

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

backend: gibson-1
bandit1@bandit.labs.overthewire.org's password:

      OoT
    OoT
  OoT
OoT

www. ver he ire.org

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:
```

## Level 1-2

If a file has a name that begins with a dash (-), we must prefix it with “./” to read it.

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

password for bandit2 : 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

## Level 2-3

```
bandit2@bandit:~$ cat " ./--spaces in this filename--"
MNk8KNH3Usiio41PRUEoDFPqfxLPISmx
bandit2@bandit:~$
```

password for bandit3 : MNk8KNH3Usiio41PRUEoDFPqfxLPISmx

## Level 3-4

Used command “ls -la” to find hidden files from directory ‘inhere’.

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cat inhere
cat: inhere: Is a directory
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -la
total 12
drwxr-xr-x 2 root    root    4096 Aug 15 13:16 .
drwxr-xr-x 3 root    root    4096 Aug 15 13:16 ..
-rw-r----- 1 bandit4 bandit3   33 Aug 15 13:16 ...Hiding-From-You
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$
```

Password for bandit4 : 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

## Level 4-5

```
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: ./file07: No such file or directory
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZOOE005pTW81FB8j8lxXGUQw
bandit4@bandit:~/inhere$
```

password for bandit5 : 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

### Level 5-6

“find . -readable -size 1033c ! -executable” used this command to find the file.

```
bandit5@bandit:~/inhere$ find . -readable -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

Password for bandit6 : HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

### Level 6-7

```
bandit6@bandit:~$ find / -size 33c -user bandit7 -group bandit6 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:~$
```

Password for bandit7 : morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj

### Level 7-8

used “grep millionth data.txt” to find the word millionth from that file.

```
traumatizing      TQQ84B6uHNAAnU829DYHKnROYHMOVUSVwu
surrender         9iYksKyjhX383seDdx88X90kYbqPKW5C
baptists          JfA8mhlCTmxsqo5bFJyDlkQCRjMmtrX9
bandit7@bandit:~$ grep millionth data.txt
millionth         dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$
```

password for bandit8 : dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

### Level 8-9

used sort command to make it in order, ie, same together. Used “cat data.txt | sort | uniq -q” to get the unique password .

```
zRgELiOsTXVPZuVWVkp7f0ShIqH0CX40
zRgELiOsTXVPZuVWVkp7f0ShIqH0CX40
ZzQDv5Imr9y5XSYGD3r61uP1fjXAhud
ZzQDv5Imr9y5XSYGD3r61uP1fjXAhud
ZzQDv5Imr9y5XSYGD3r61uP1fjXAhud
ZzQDv5Imr9y5XSYGD3r61uP1fjXAhud
ZzQDv5Imr9y5XSYGD3r61uP1fjXAhud
ZzQDv5Imr9y5XSYGD3r61uP1fjXAhud
ZzQDv5Imr9y5XSYGD3r61uP1fjXAhud
ZzQDv5Imr9y5XSYGD3r61uP1fjXAhud
ZzQDv5Imr9y5XSYGD3r61uP1fjXAhud
ZzQDv5Imr9y5XSYGD3r61uP1fjXAhud
ZzQDv5Imr9y5XSYGD3r61uP1fjXAhud
ZzQDv5Imr9y5XSYGD3r61uP1fjXAhud
bandit8@bandit:~$ cat data.txt | sort | uniq -u
4CKMh1JI91bUIZZPXQqGanal4xvAg0JM
bandit8@bandit:~$
```

Password for bandit9 : 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

### Level 9-10

“strings” is used to extract only printable character sequences , commonly to identify human readable text. grep “==” is used to print lines containing “==”.

command used “ strings data.txt | grep “==” “

```
&x,[g
05W^%
bandit9@bandit:~$ strings data.txt | grep"=="
grep==: command not found
bandit9@bandit:~$ strings data.txt | grep "=="
===== theg
===== password
===== is
===== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
bandit9@bandit:~$
```

password for bandit10 : FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

### Level 10-11

Decoded the Base64 text using a website to obtain the password.

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ wc -l data.txt
1 data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnB0VmozcVJyCg==
```

password for bandit11 : dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

### Level 11-12

Decoded the ciphertext to obtain the password.

```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ wc -l data.txt
1 data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4
```

Password for bandit12 : 7x16WNeHli5YkIhWsfFIqoognUTyj9Q4

### Level 12-13

This level was quite challenging – I had to repeatedly extract gzip , bzip , and tar files to finally get the password .



```

bandit12@bandit:/tmp/light$ ls
candy5.tar candy6.tar candy7 data.txt
bandit12@bandit:/tmp/light$ file candy7
candy7: POSIX tar archive (GNU)
bandit12@bandit:/tmp/light$ mv candy7 candy8.tar
bandit12@bandit:/tmp/light$ ls
candy5.tar candy6.tar candy8.tar data.txt
bandit12@bandit:/tmp/light$ tar -xf candy8.tar
bandit12@bandit:/tmp/light$ ls
candy5.tar candy6.tar candy8.tar data8.bin data.txt
bandit12@bandit:/tmp/light$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Fri Aug 15 13:1
5:53 2025, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/light$ mv data8.bin candy9.gz
bandit12@bandit:/tmp/light$ ls
candy5.tar candy6.tar candy8.tar candy9.gz data.txt
bandit12@bandit:/tmp/light$ gzip -d candy9.gz
bandit12@bandit:/tmp/light$ ls
candy5.tar candy6.tar candy8.tar candy9 data.txt
bandit12@bandit:/tmp/light$ file candy9
candy9: ASCII text
bandit12@bandit:/tmp/light$ cat candy9
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
bandit12@bandit:/tmp/light$

```

password for bandit13 : FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn

### Level 13-14

```

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8ROof1qqmcBPALh7lDCPvS
bandit14@bandit:~$

```

password for bandit14: MU4VWeTyJk8ROof1qqmcBPALh7lDCPvS

### Level 14-15

I used the command “telnet localhost 30000” to connect to the localhost through port 30000.

```

bandit14@bandit:~$ ssh bandit14@localhost -p 30000
Connection closed by 127.0.0.1 port 30000
bandit14@bandit:~$ telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
MU4VWeTyJk8ROof1qqmcBPALh7lDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

Connection closed by foreign host.
bandit14@bandit:~$

```

Password for bandit15: 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

## Level 15-16

Used ncat to open a ssl encrypted connection to a service that's on port 30001.  
command used "ncat 127.0.0.1 30001 --ssl"

```
bandit15@bandit:~$ ncat 127.0.0.1 30001 --ssl
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
Correct!
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
```

Password for bandit 16 : kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

## Level 16-17

first used "nmap 127.0.0.1 -p 31000-32000" to find which port have server listening to them.

Then used "ncat localhost port" and tried the ports

Got a private RSA key,saved it in a file by using "nano /tmp/bandit17.key"

```
Ncat: Input/output error.
bandit16@bandit:~$ ncat localhost --ssl 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvm0kuiFmMg6HL2YPI0jon6iWfbp7c3jx34YkYwUH57SUdyJ
imZzeyGC0gtZPGuJUSxiJSWI/oTqexh+cAMTSMLOJf7+BrJ0bArnxd9Y7YT2bRPQ
Ja6Lzb5S8YW3FZl870RiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAl+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpwTMAZJTzAzQxNbK2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQABAoIBABagpxpM1aoLWfVd
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUDE6SFth0ar69jp5RLLwD1NhPx3iBl
J9n0M8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpX0UDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmXkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPW9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52y0Q9q0kwFTEQpjtF4uNtJom+asvlpMS8A
vLY9r60wYSvmZhNqBurl7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHK/fur850Efc9TncnCY2crpoqsgHfKLxrLgt+qDpfZnx
SatLdt8GfQ85yA7hnWJ2MxF3NaeSDm75Lsm+tBbAiyC9P2jGRNtMSKcGyEAYpHd
HCctNi/FwjuLhtFf/rHYKhLidZDFYeIE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJYusavPzpaJMjdJ6tcFhVAbAjm7enCivGCsX+X3L5SiWg0A
R57hJglezIiVjv3aGwHwVZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93VSHDi
TtieK7xRVxUL+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFmly9FL2m9oQWcG
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB30hYimtiG2Cg5JCqIZFHxD6MjEG0iu
L8ktHMPvodBwNsSBULPcG0QKBgBAPlTfC1H0nWiMGOU3KPwYwt006CdTkMJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
Y0djHdS0oKvDQNWu6ucyLRAWFuISeXw9a/9p7fpxm0TSgyvmfLF2MIAEwyzRqAM
77pBAoGAMmjmIjdjp+Ez8duyn3ieo36yrTtF5NSsJLABxPpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl104f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9G0tt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40f0oZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

^C
bandit16@bandit:~$ ^C
bandit16@bandit:~$ ^C
bandit16@bandit:~$ mkdir /tmp/bandit17.key
mkdir: cannot create directory '/tmp/bandit17.key': File exists
bandit16@bandit:~$ mkdir /tmp / bandit17.key
mkdir: cannot create directory '/tmp': File exists
mkdir: cannot create directory '/': File exists
mkdir: cannot create directory 'bandit17.key': Permission denied
bandit16@bandit:~$ nano /tmp/bandit17.key
```

Then entered bandit 17.



```
bandit19@bandit:~$ ls
```

```
bandit20-do
```

```
bandit19@bandit:~$ ls -la
```

```
total 36
```

```
drwxr-xr-x  2 root    root      4096 Aug 15 13:16 .
```

```
drwxr-xr-x 150 root    root      4096 Aug 15 13:18 ..
```

```
-rwsr-x---  1 bandit20 bandit19 14884 Aug 15 13:16 bandit20-do
```

```
-rw-r--r--  1 root    root        220 Mar 31  2024 .bash_logout
```

```
-rw-r--r--  1 root    root      3851 Aug 15 13:09 .bashrc
```

```
-rw-r--r--  1 root    root        807 Mar 31  2024 .profile
```

```
bandit19@bandit:~$ ./bandit20-do cat/etc/bandit_pass/bandit20
```

```
env: 'cat/etc/bandit_pass/bandit20': No such file or directory
```

```
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
```

```
0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbY0
```

```
bandit19@bandit:~$
```