OverTheWire Bandit Level 0-20 Guide

Level 0: Initial Access

1. Open your terminal
2. Connect using SSH:

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

3. Enter password:

Level 0 → 1

1. Look for readme file:

```
ls
```

2. Read the file:

```
cat readme
```

3. Save the password shown

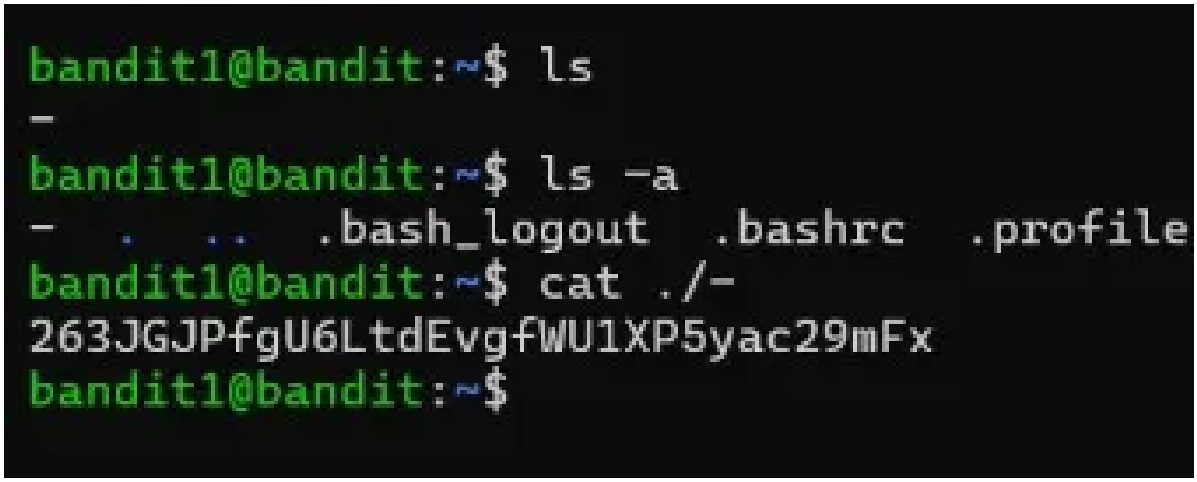
```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor 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
```

Level 1 → 2

1. The file is named "-", which requires special handling
2. Read the file using:

   ```
   cat ./-
   ```

3. Save the password shown

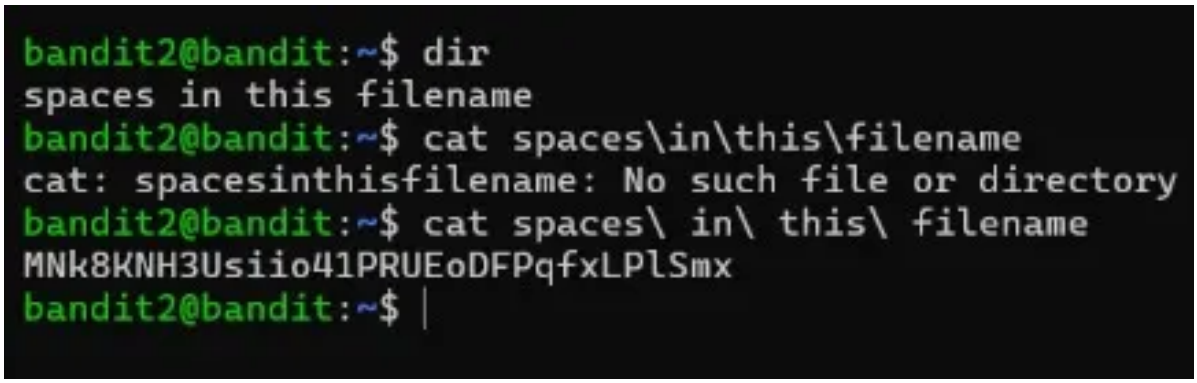


Level 2 → 3

1. The filename contains spaces
2. Read using quotes:

   ```
   cat "spaces in this filename"
   ```

3. Save the password shown



Level 3 → 4

1. Change to inhere directory:

   ```
   cd inhere
   ```

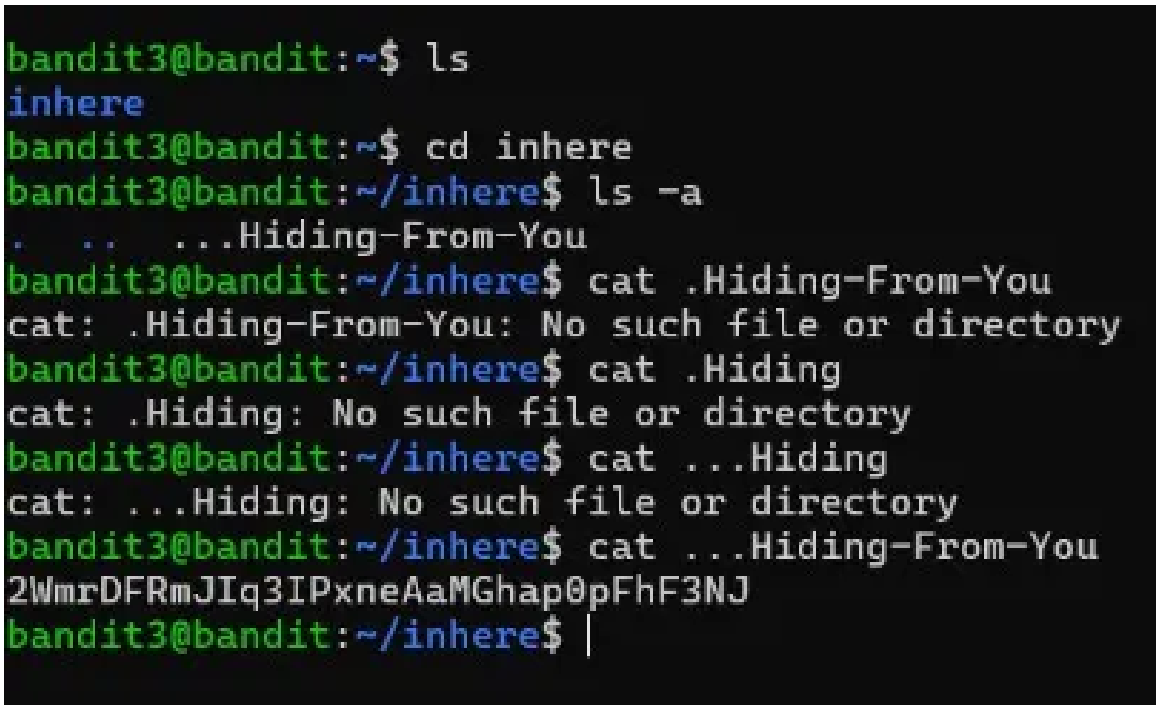
2. List all files including hidden:

   ```
   ls -la
   ```

3. Read the hidden file:

   ```
   cat .hidden
   ```

4. Save the password shown



Level 4 → 5

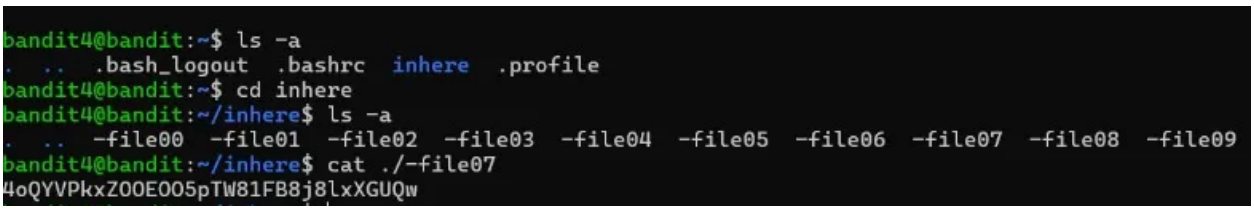
1. Change to inhere directory
2. Check file types:

   ```
   file ./*
   ```

3. Find and read the human-readable file:

   ```
   cat ./-file07
   ```

4. Save the password shown



Level 5 → 6

1. Navigate to inhere directory
2. Find file with specific properties:

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

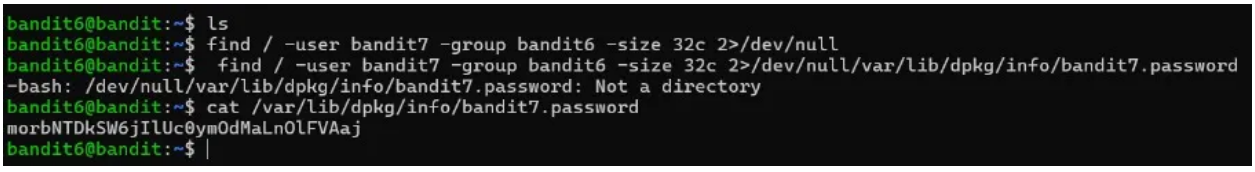
3. save the password shown

Level 6 → 7

1. Search entire system with specific criteria:

```
find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
```

2. save the password shown



Level 7 → 8

1. Search for "millionth" in data.txt:

```
cat data.txt | grep millionth
```

2. Save the password shown

```
bandit7@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit7@bandit:~$ awk '/^millionth/ {print $2;}' data.txt
dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$
```

Level 8 → 9

1. Find unique line:

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

2. Save the password shown

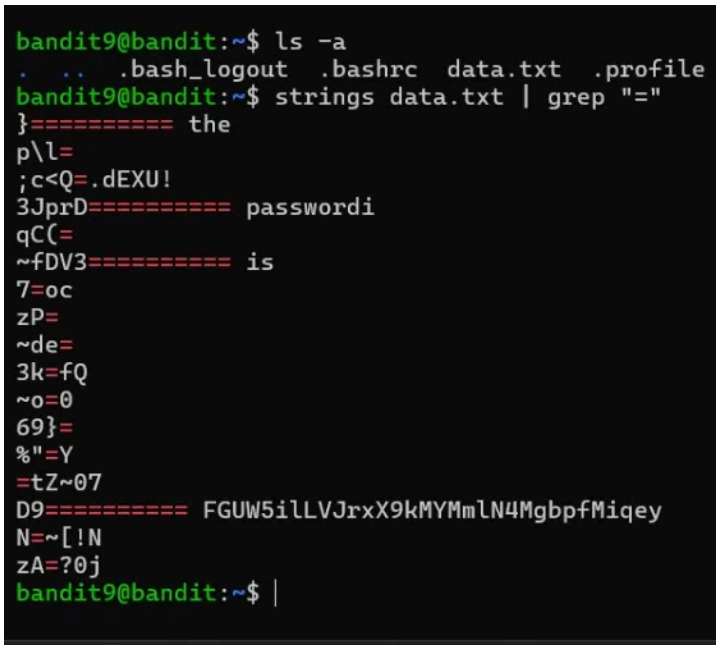
```
bandit8@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit8@bandit:~$ cat data.txt | sort |uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:~$
```

Level 9 → 10

1. Search for human-readable strings with "=":

   ```
   strings data.txt | grep "="
   ```

2. Save the password shown

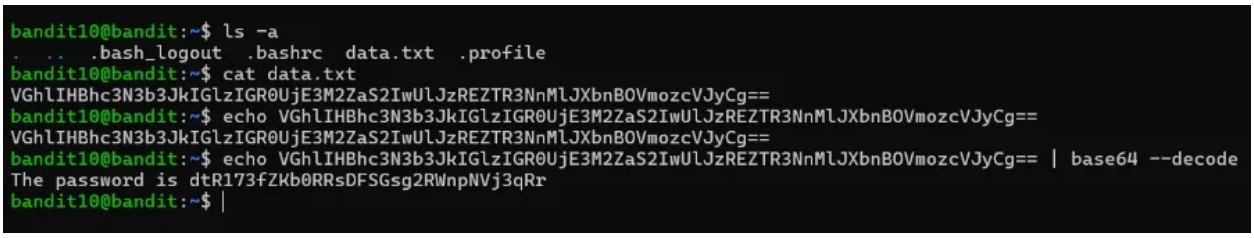


Level 10 → 11

1. Decode base64 content:

   ```
   base64 -d data.txt
   ```

2. Save the password shown



Level 11 → 12

1. Decode ROT13:

   ```
   cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
   ```

2. Save the password shown

```
bandit11@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4
bandit11@bandit:~$ echo Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4 | tr [a-zA-Z] [n-za-mN-ZA-M]
The password is 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
bandit11@bandit:~$
```

Level 12 → 13

1. Create temporary directory:

   ```
   mkdir /tmp/myname123
   ```

2. Copy and navigate:

   ```
   cp data.txt /tmp/myname123
   cd /tmp/myname123
   ```

3. Convert hex dump:

   ```
   xxd -r data.txt > data
   ```

4. Save the password shown

```
bandit12@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit12@bandit:~$ cd /tmp/jhalon
bandit12@bandit:/tmp/jhalon$ ls -a
.  ..  file.bin
bandit12@bandit:/tmp/jhalon$ file file.bin
file.bin: 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/jhalon$ zcat file.bin | file -
/dev/stdin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | file -
/dev/stdin: gzip compressed data, was "data4.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | zcat | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | zcat | tar xO | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | zcat | tar xO | tar xO | file -
/dev/stdin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | zcat | tar xO | tar xO | bzcat | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | zcat | tar xO | tar xO | bzcat | tar xO | file -
/dev/stdin: gzip compressed data, was "data9.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | zcat | tar xO | tar xO | bzcat | tar xO | zcat | file -
/dev/stdin: ASCII text
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | zcat | tar xO | tar xO | bzcat | tar xO | zcat
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
```

Level 13 → 14

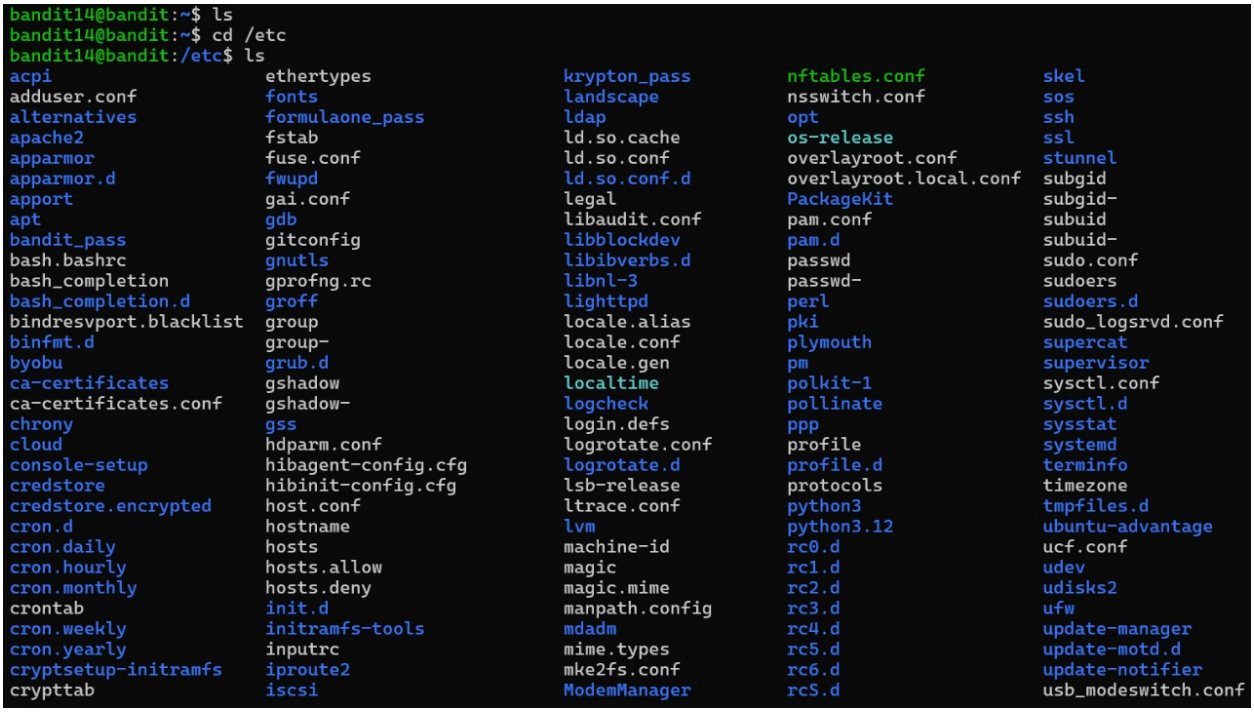
1. Use private key to login:

```
ssh -i sshkey.private bandit14@localhost
```

2. Read password from:

```
cat /etc/bandit_pass/bandit14
```

3. Save the password shown



Level 14 → 15

1. Connect to port 30000:

```
nc localhost 30000
```

2. Save the password shown

```
bandit14@bandit:~$  telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

Connection closed by foreign host.
```

Level 15 → 16

1. Connect using SSL:

   ```
   openssl s_client -connect localhost:30001
   ```

2. save the password shown

```
bandit15@bandit:~$ openssl s_client -ign_eof -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:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
   v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT
---
```

Level 16 → 17

1. Scan ports:

   ```
   nmap -p 31000-32000 localhost
   ```

2. Connect to correct SSL port:

```
openssl s_client -connect localhost:31790
```

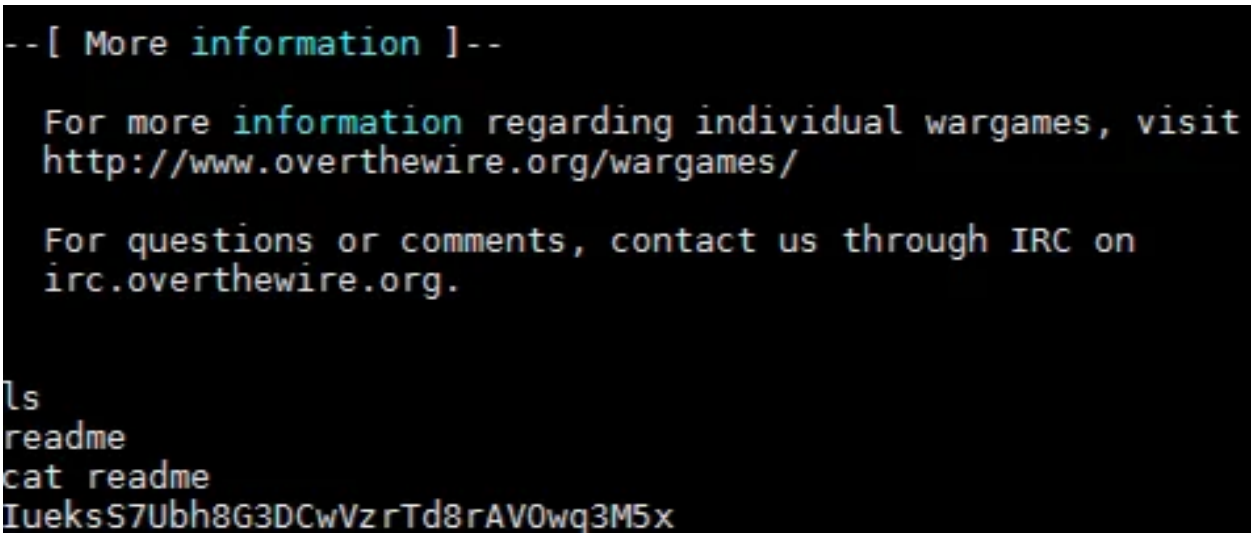
3. save the password shown

Level 17 → 18

1. Compare password files:

```
diff passwords.old passwords.new
```

2. save the password shown



Level 18 → 19

1. Execute command directly via SSH:

```
ssh bandit18@localhost "cat readme"
```

2. save the password shown

Level 19 → 20

1. Use setuid binary:

```
./bandit20-do cat /etc/bandit_pass/bandit20
```

```
./bandit20-do cat /etc/bandit_pass/bandit20
```

2. save the password shown