

OverTheWire Bandit All Levels Walkthrough

 medium.com/@tugba.arslan9744/overthewire-bandit-all-levels-walkthrough-5b81cd41b1e1

Tuğba Arslan

June 28, 2024



Tuğba Arslan

Bandit Level 0

<https://overthewire.org/wargames/bandit/bandit0.html>

Level Goal

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is **bandit.labs.overthewire.org**, on port 2220. The username is **bandit0** and the password is **bandit0**. Once logged in, go to the [Level 1](#) page to find out how to beat Level 1.

Password: bandit0

Host: bandit.labs.overthewire.org

Port: 2220

Here is the Bandit0's password: *bandit0*

Bandit Level 0 → Level 1

<https://overthewire.org/wargames/bandit/bandit1.html>

Level Goal

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.

Password: bandit0

Host: bandit.labs.overthewire.org

Port: 2220



```
(tugbaarslan㉿kali)-[~]
$ ssh bandit0@bandit.labs.overthewire.org -p 2220
```

The terminal shows a file system tree with a root folder containing .bash_logout, .bashrc, .profile, and a file named readme. The file system icon is visible at the top.

| Firstly, use this command and then write bandit0's password:

```
$ ssh -p 2220
```

bandit0

```
bandit0@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  2 root      root      4096 Jun 20 04:06 .
4 drwxr-xr-x 70 root      root      4096 Jun 20 04:08 ..
4 -rw-r--r--  1 root      root      220 Mar 31 08:41 .bash_logout
4 -rw-r--r--  1 root      root     3771 Mar 31 08:41 .bashrc
4 -rw-r--r--  1 root      root      807 Mar 31 08:41 .profile
4 -rw-r----- 1 bandit1 bandit0  437 Jun 20 04:06 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
```

| Write these commands.

```
$ ls -alps
```

```
$ cat readme
```

Here is the Bandit1's password: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

Bandit Level 1 → Level 2

<https://overthewire.org/wargames/bandit/bandit2.html>

Level Goal

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

Password: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

Host: bandit.labs.overthewire.org

Port: 2220

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



| Firstly, use this command and then write bandit1's password:

```
$ ssh -p 2220
```

ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5lf

```
bandit1@bandit:~$ ls -alps
total 24
4 -rw-r----- 1 bandit2 bandit1   33 Jun 20 04:07 -
4 drwxr-xr-x  2 root      root    4096 Jun 20 04:07 ./
4 drwxr-xr-x 70 root      root    4096 Jun 20 04:08 ../
4 -rw-r--r--  1 root      root     220 Mar 31 08:41 .bash_logout
4 -rw-r--r--  1 root      root    3771 Mar 31 08:41 .bashrc
4 -rw-r--r--  1 root      root     807 Mar 31 08:41 .profile
bandit1@bandit:~$ cat ./
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
```

| Write these commands.

```
$ ls -alps
```

```
$ cat ./
```

Here is the Bandit2's password: 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

Bandit Level 2 → Level 3

<https://overthewire.org/wargames/bandit/bandit3.html>

Level Goal

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

Password: 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

Host: bandit.labs.overthewire.org

Port: 2220

```
(tugbaarslan㉿kali)-[~]
$ ssh bandit2@bandit.labs.overthewire.org -p 2220
```



| Firstly, use this command and then write bandit2's password:

```
$ ssh -p 2220
```

```
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
```

```
bandit2@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  2 root      root      4096 Jun 20  04:07 .
4 drwxr-xr-x 70 root      root      4096 Jun 20  04:08 ..
4 -rw-r--r--  1 root      root      220 Mar 31 08:41 .bash_logout
4 -rw-r--r--  1 root      root     3771 Mar 31 08:41 .bashrc
4 -rw-r--r--  1 root      root      807 Mar 31 08:41 .profile
4 -rw-r--r--  1 bandit3 bandit2   33 Jun 20  04:07 spaces in this filename
bandit2@bandit:~$ cat 'spaces in this filename'
MNk8KNH3Usii041PRUEoDFPqfxLPISmx
```

| Write these commands.

```
$ ls -alps
```

```
$ cat 'spaces in this filename'
```

Here is the Bandit3's password: MNk8KNH3Usii041PRUEoDFPqfxLPISmx

Bandit Level 3 → Level 4

<https://overthewire.org/wargames/bandit/bandit4.html>

Level Goal

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

Password: MNk8KNH3Usii041PRUEoDFPqfxLPISmx

Host: bandit.labs.overthewire.org

Port: 2220

```
(tugbaarslan㉿kali)-[~]
$ ssh bandit3@bandit.labs.overthewire.org -p 2220
```



| Firstly, use this command and then write bandit3's password:

```
$ ssh -p 2220
```

MNk8KNH3Usio41PRUEoDFPqfxLPISmx

```
bandit3@bandit:~$ ls -alps
total 24
4 drwxr-xr-x 3 root root 4096 Jun 20 04:07 .
4 drwxr-xr-x 70 root root 4096 Jun 20 04:08 ..
4 -rw-r--r-- 1 root root 220 Mar 31 08:41 .bash_logout
4 -rw-r--r-- 1 root root 3771 Mar 31 08:41 .bashrc
4 drwxr-xr-x 2 root root 4096 Jun 20 04:07 inhere/
4 -rw-r--r-- 1 root root 807 Mar 31 08:41 .profile
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root      root      4096 Jun 20 04:07 .
drwxr-xr-x 3 root      root      4096 Jun 20 04:07 ..
-rw-r----- 1 bandit4  bandit3    33 Jun 20 04:07 ... Hiding-From-You
bandit3@bandit:~/inhere$ cat ... Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
```

| Write these commands.

```
$ ls -alps
```

```
$ cd inhere
```

```
$ ls -al
```

```
$ cat ...Hiding-From-You
```

Here is the Bandit4's password: 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

Bandit Level 4 → Level 5

<https://overthewire.org/wargames/bandit/bandit5.html>

Level Goal

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.

Password: 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

Host: bandit.labs.overthewire.org

Port: 2220

```
(tugbaarslan㉿kali)-[~]
$ ssh bandit4@bandit.labs.overthewire.org -p 2220
```

Firstly, use this command and then write bandit4's password:

```
$ ssh -p 2220
```

2WmrDFRmJlq3IPxneAaMGhap0pFhF3NJ

```
bandit4@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root root 4096 Jun 20 04:07 .
4 drwxr-xr-x 70 root root 4096 Jun 20 04:08 ..
4 -rw-r--r--  1 root root  220 Mar 31 08:41 .bash_logout
4 -rw-r--r--  1 root root 3771 Mar 31 08:41 .bashrc
4 drwxr-xr-x  2 root root 4096 Jun 20 04:07 inhere/
4 -rw-r--r--  1 root root  807 Mar 31 08:41 .profile
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ find . -type f | xargs file
./-file08: data
./-file06: data
./-file09: data
./-file01: data
./-file03: data
./-file04: data
./-file00: data
./-file07: ASCII text
./-file05: data
./-file02: data
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZOOE005pTW81FB8j8lxXGUQw
```

Write these commands.

```
$ ls -alps
```

```
$ cd inhere
```

§ /s

```
$ find . -type f | xargs file
```

```
$ cat ./-file07
```

Here is the Bandit5's password: 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

Bandit Level 5 → Level 6

<https://overthewire.org/wargames/bandit/bandit6.html>

Level Goal

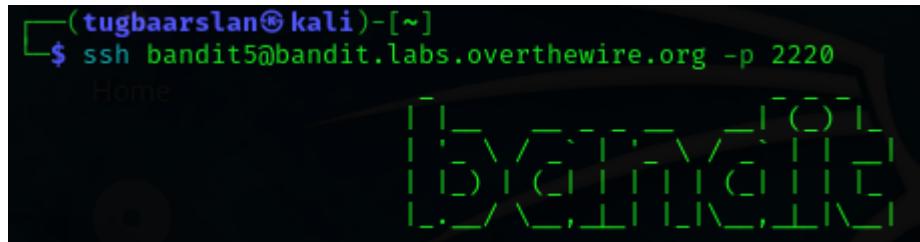
The password for the next level is stored in a file somewhere under the `inhere` directory and has all of the following properties:

- human-readable
- 1033 bytes in size
- not executable

Password: 4oQYVPkxZOOE0O5pTW81FB8j8lxXGUQw

Host: bandit.labs.overthewire.org

Port: 2220



```
(tugbaarslan㉿kali)-[~]
$ ssh bandit5@bandit.labs.overthewire.org -p 2220
```

| *Firstly, use this command and then write bandit5's password:*

```
$ ssh -p 2220
```

4oQYVPkxZOOE0O5pTW81FB8j8lxXGUQw

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

| *Write these commands.*

```
$ ls
```

```
$ cd inhere
```

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

```
$ cat ./maybehere07/.file2
```

Here is the Bandit6's password: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

Bandit Level 6 → Level 7

<https://overthewire.org/wargames/bandit/bandit7.html>

Level Goal

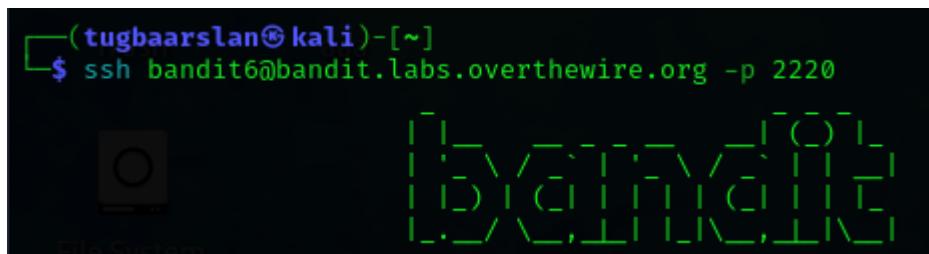
The password for the next level is stored **somewhere on the server** and has all of the following properties:

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

Password: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

Host: bandit.labs.overthewire.org

Port: 2220



```
(tugbaarslan㉿kali)-[~]
$ ssh bandit6@bandit.labs.overthewire.org -p 2220
```

| *Firstly, use this command and then write bandit6's password:*

```
$ ssh -p 2220
```

HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

```
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIIUc0ymOdMaLnOlFVAaj
```

| *Write these commands.*

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

```
$ cat /var/lib/dpkg/info/bandit7.password
```

Here is the Bandit7's password: `morbNTDkSW6jIIUc0ymOdMaLnOlFVAaj`

Bandit Level 7 → Level 8

<https://overthewire.org/wargames/bandit/bandit8.html>

Level Goal

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

Password: morbNTDkSW6jIIUc0ymOdMaLnOlFVAaj

Host: bandit.labs.overthewire.org

Port: 2220



```
(tugbaarslan㉿kali)-[~]
$ ssh bandit7@bandit.labs.overthewire.org -p 2220
```

| Firstly, use this command and then write bandit7's password:

```
$ ssh -p 2220
```

morbNTDkSW6jIIUc0ymOdMaLnOIFVAaj

```
bandit7@bandit:~$ ls -alps
total 4108
 4 drwxr-xr-x  2 root      root        4096 Jun 20 04:07 .
 4 drwxr-xr-x 70 root      root        4096 Jun 20 04:08 ..
 4 -rw-r--r--  1 root      root       220 Mar 31 08:41 .bash_logout
 4 -rw-r--r--  1 root      root      3771 Mar 31 08:41 .bashrc
4088 -rw-r----- 1 bandit8 bandit7 4184396 Jun 20 04:07 data.txt
 4 -rw-r--r--  1 root      root       807 Mar 31 08:41 .profile
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth      dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
```

| Write these commands.

```
$ ls -alps
```

```
$ strings data.txt | grep "millionth"
```

Here is the Bandit8's password: *dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc*

Bandit Level 8 → Level 9

<https://overthewire.org/wargames/bandit/bandit9.html>

Level Goal

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

Password: dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

Host: bandit.labs.overthewire.org

Port: 2220

```
(tugbaarslan㉿kali)-[~]
$ ssh bandit8@bandit.labs.overthewire.org -p 2220
```



| Firstly, use this command and then write bandit8's password:

```
$ ssh -p 2220
```

dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

| Write this command.

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

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

Here is the Bandit9's password: 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

Bandit Level 9 → Level 10

<https://overthewire.org/wargames/bandit/bandit10.html>

Level Goal

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.

Password: 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

Host: bandit.labs.overthewire.org

Port: 2220

```
(tugbaarslan㉿kali)-[~]
$ ssh bandit9@bandit.labs.overthewire.org -p 2220
```



| Firstly, use this command and then write bandit9's password:

```
$ ssh -p 2220
```

4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

```
bandit9@bandit:~$ strings data.txt | grep "="
[===== the
EJ}@k=
T%===== passwordG
\ ====== f7
}===== ist"
WL[L=S
)|P=Vz
=Y`W^
=9|
s7.=;$
g=6E
|=?y=
===== FGUW5illVJrxX9kMYMmlN4MgbpfMiqey
=n/iZ
:'=F
```

Write this command.

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

Here is the Bandit10's password: FGUW5iLVJrxX9kMYMmlN4MqbpfMiqey

Bandit Level 10 → Level 11

<https://overthewire.org/wargames/bandit/bandit11.html>

Level Goal

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

Password: FGUW5ilLVJrxX9kMYMmIN4MgbpfMiqey

Host: bandit.labs.overthewire.org

Port: 2220

```
[tugbaarslan㉿kali)-[~]
$ ssh bandit10@bandit.labs.overthewire.org -p 2220
```

| Firstly, use this command and then write bandit10's password:

```
$ ssh -p 2220
```

FGUW5iLVJrxX9kMYMmIN4MqbpfMiqey

```
bandit10@bandit:~$ cat data.txt  
VGhlIHBlc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnB0VmozcVJyCg=  
bandit10@bandit:~$ base64 -d data.txt  
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
```

| Write these commands.

```
$ cat data.txt
```

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

Here is the Bandit11's password: dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

Bandit Level 11 → Level 12

<https://overthewire.org/wargames/bandit/bandit12.html>

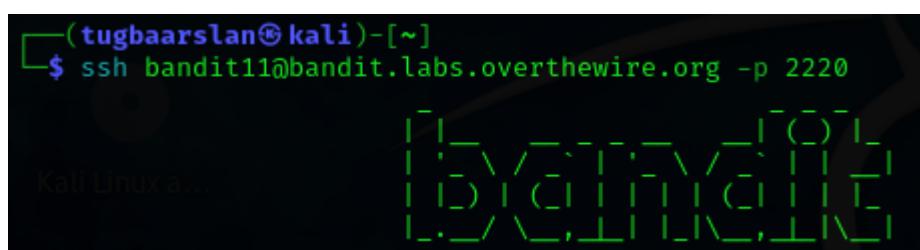
Level Goal

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

Password: dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

Host: bandit.labs.overthewire.org

Port: 2220



| Firstly, use this command and then write bandit11's password:

```
$ ssh -p 2220
```

dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

```
bandit11@bandit:~$ cat data.txt  
Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtahGlw9D4
```

| Write this command.

```
$ cat data.txt
```

| Use CyberChef, decrypt encrypted text with rot13.

Here is the Bandit12's password: 7x16WNeHli5YklhWsfFlqoognUTyj9Q4

Bandit Level 12 → Level 13

<https://overthewire.org/wargames/bandit/bandit13.html>

Level Goal

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!)

>Password: 7x16WNeHli5YklhWsfFlqoognUTyj9Q4

Host: *bandit.labs.overthewire.org*

Port: 2220

| Firstly, use this command and then write bandit12's password:

\$ ssh -p 2220

7x16WNeHli5YklhWsfFlqoognUTyj9Q4

```
bandit12@bandit:~$ mkdir /tmp/matryoshka
bandit12@bandit:~$ cp data.txt /tmp/matryoshka
bandit12@bandit:~$ cd /tmp/matryoshka
bandit12@bandit:/tmp/matryoshka$ ls
data.txt
bandit12@bandit:/tmp/matryoshka$ xxd -r data.txt > data
bandit12@bandit:/tmp/matryoshka$ ls
data data.txt
bandit12@bandit:/tmp/matryoshka$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu Jun 20 04:06:52 2024, max compression, from Unix, original size modulo 2^32 577
bandit12@bandit:/tmp/matryoshka$ mv data file.gz
bandit12@bandit:/tmp/matryoshka$ gzip -d file.gz
bandit12@bandit:/tmp/matryoshka$ ls
data.txt file
bandit12@bandit:/tmp/matryoshka$ file file
file: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/matryoshka$ mv file file.bz2
bandit12@bandit:/tmp/matryoshka$ bzip2 -d file.bz2
bandit12@bandit:/tmp/matryoshka$ ls
data.txt file
bandit12@bandit:/tmp/matryoshka$ file file
file: gzip compressed data, was "data4.bin", last modified: Thu Jun 20 04:06:52 2024, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/matryoshka$ mv file file.gz
bandit12@bandit:/tmp/matryoshka$ gzip -d file.gz
bandit12@bandit:/tmp/matryoshka$ ls
data.txt file
bandit12@bandit:/tmp/matryoshka$ file file
file: POSIX tar archive (GNU)
bandit12@bandit:/tmp/matryoshka$ mv file file.tar
bandit12@bandit:/tmp/matryoshka$ tar xf file.tar
bandit12@bandit:/tmp/matryoshka$ ls
data5.bin data.txt file.tar
bandit12@bandit:/tmp/matryoshka$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/matryoshka$ mv data5.bin data.tar
bandit12@bandit:/tmp/matryoshka$ tar xf data.tar
bandit12@bandit:/tmp/matryoshka$ ls
data6.bin data.tar data.txt file.tar
bandit12@bandit:/tmp/matryoshka$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/matryoshka$ mv data6.bin data.bz2
bandit12@bandit:/tmp/matryoshka$ bzip2 -d data.bz2
bandit12@bandit:/tmp/matryoshka$ ls
data data.tar data.txt file.tar
```

| Write these commands.

\$ mkdir /tmp/matryoshka

\$ cp data.txt /tmp/matryoshka

\$ cd /tmp/matryoshka

\$ ls

\$ xxd -r data.txt > data

\$ ls

\$ file data

\$ mv data file.gz

\$ gzip -d file.gz

\$ ls

\$ file file

```
$ mv file file.bz2
```

```
$ bzip2 -d file.bz2
```

```
$ ls
```

```
$ file file
```

```
$ mv file file.gz
```

```
$ gzip -d file.gz
```

```
$ ls
```

```
$ file file
```

```
$ mv file file.tar
```

```
$ tar xf file.tar
```

```
$ ls
```

```
$ file data5.bin
```

```
$ mv data5.bin data.tar
```

```
$ tar xf data.tar
```

```
$ ls
```

```
$ file data6.bin
```

```
$ mv data6.bin data.bz2
```

```
$ bzip2 -d data.bz2
```

```
$ ls
```

```
bandit12@bandit:/tmp/matyoshka$ mv data data.tar
bandit12@bandit:/tmp/matyoshka$ tar xf data.tar
bandit12@bandit:/tmp/matyoshka$ ls
data8.bin  data.tar  data.txt  file.tar
bandit12@bandit:/tmp/matyoshka$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Jun 20 04:06:52 2024, max compression, from Unix,
original size modulo 2^32 49
bandit12@bandit:/tmp/matyoshka$ mv data8.bin data.gz
bandit12@bandit:/tmp/matyoshka$ gzip -d data.gz
bandit12@bandit:/tmp/matyoshka$ ls
data  data.tar  data.txt  file.tar
bandit12@bandit:/tmp/matyoshka$ file data
data: ASCII text
bandit12@bandit:/tmp/matyoshka$ cat data
The password is F05dwFsc0cbaiiH0h8J2eUks2vdTDwAn
```

| Write these commands.

```
$ mv data data.tar
```

```
$ tar xf data.tar
```

```
$ ls  
$ file data8.bin  
$ mv data8.bin data.gz  
$ gzip -d data.gz
```

```
$ ls
```

```
$ file data  
$ cat data
```

Here is the Bandit13's password: FO5dwFsc0cbaliH0h8J2eUks2vdTDwAn

Bandit Level 13 → Level 14

<https://overthewire.org/wargames/bandit/bandit14.html>

Level Goal

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

Password: FO5dwFsc0cbaliH0h8J2eUks2vdTDwAn

Host: bandit.labs.overthewire.org

Port: 2220



```
(tugbaarslan㉿kali)-[~]$ ssh bandit13@bandit.labs.overthewire.org -p 2220
```

| Firstly, use this command and then write bandit13's password:

```
$ ssh -p 2220
```

FO5dwFsc0cbaliH0h8J2eUks2vdTDwAn

```
bandit13@bandit:~$ ls  
sshkey.private  
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220  
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.  
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfxC5CXlhmAAM/urerLY.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Could not create directory '/home/bandit13/.ssh' (Permission denied).  
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).
```

| Write these commands.

```
$ ls
```

```
$ ssh -i sshkey.private bandit14@localhost -p 2220
```

| You are now in bandit14.

Bandit Level 14 → Level 15

<https://overthewire.org/wargames/bandit/bandit15.html>

Level Goal

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

Password: MU4VWeTyJk8ROof1qqmcBPaLh7IDCPvS

Host: bandit.labs.overthewire.org

Port: 2220

```
└─(tugbaarslan㉿kali)-[~]  
└─$ ssh bandit14@bandit.labs.overthewire.org -p 2220
```

| Firstly, use this command and then write bandit14's password:

```
$ ssh -p 2220
```

MU4VWeTyJk8ROof1qqmcBPaLh7IDCPvS

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8R0of1qqmcBPaLh7lDCPvS
bandit14@bandit:~$ nc localhost 30000
MU4VWeTyJk8R0of1qqmcBPaLh7lDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

exit
bandit14@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

[tugbaarslan@kali)-[~]
$ ssh bandit15@bandit.labs.overthewire.org -p 2220
```

| Then, write and enter this command:

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

| After use the nc command with bandit14's password:

```
$ nc localhost 30000MU4VWeTyJk8R0of1qqmcBPaLh7lDCPvS
```

Here is the Bandit15's password: 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

Bandit Level 15 → Level 16

<https://overthewire.org/wargames/bandit/bandit16.html>

Level Goal

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

Helpful note: Getting “HEARTBEATING” and “Read R BLOCK”? Use `-ign_eof` and read the “CONNECTED COMMANDS” section in the manpage. Next to ‘R’ and ‘Q’, the ‘B’ command also works in this version of that command...

Password: 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

Host: `bandit.labs.overthewire.org`

Port: 2220

```
[tugbaarslan@kali)-[~]
$ ssh bandit15@bandit.labs.overthewire.org -p 2220
```



```
██████
██  ██
██   ██
██     ██
██   ██
██  ██
██████
```

| Firstly, use this command and then write bandit15's password:

```
$ ssh -p 2220
```

```
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
```

```
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
bandit15@bandit:~$ nc -ssl localhost 30001
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
Correct!
kSkvUpMQ7IBYyCM4GBPvCvT1BfWRy0Dx

^C
bandit15@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

└─(tugbaarslan㉿kali)-[~]
$ ssh bandit16bandit.labs.overthewire.org -p 2220
```

| Then, write and enter this command:

```
$ cat /etc/bandit_pass/bandit15
```

| After use the nc command with bandit14's password:

```
$ nc -ssl localhost 300018xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
```

Here is the Bandit16's password: kSkvUpMQ7IBYyCM4GBPvCvT1BfWRy0Dx

Bandit Level 16 → Level 17

<https://overthewire.org/wargames/bandit/bandit17.html>

Level Goal

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 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.

Password: kSkvUpMQ7IBYyCM4GBPvCvT1BfWRy0Dx

Host: bandit.labs.overthewire.org

Port: 2220

```
(tugbaarslan㉿kali)-[~]
$ ssh bandit16@bandit.labs.overthewire.org -p 2220
```

| Firstly, use this command and then write bandit16's password:

```
$ ssh -p 2220
```

```
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
```

```
bandit16@bandit:~$ cat /etc/bandit_pass/bandit16
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
bandit16@bandit:~$ nmap localhost -p 31000-32000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-15 00:11 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00018s 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 0.08 seconds
```

| Then, write and enter this command:

```
$ cat /etc/bandit_pass/bandit16
```

| After this, nmap scan should be done:

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

```

bandit16@bandit:~$ ncat --ssl localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPI0jon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSml0Jf7+BrJ0bArnx9Y7YT2bRPQ
Ja6Lzb558YW3Fzl870Ri0+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkr2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfku1jHS+9EbVNj+D1XF0JuaQIDAQABAOIBABagpxpM1aoLwfVd
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RllwD1NhPx3iBl
J9nOM80J0VToum43UOS8YxF8WwhXriYGnc1sskbwpX0UDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52y0Q9q0kwFTEQpjF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXycUp1DGL51s0mama
+TOWwgECgYEAE8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur850Efc9TncnCY2crpoqsgifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNTMSkCgYEAYpHd
HCctNi/FwjuhhttFx/rHYKhLidZDFYeie/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFau0EcgYAbjo46T4hyP5tJi93V5HDi
Ttie7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEG0iu
L8ktHMPvodBwNsSBULpG0QKBgBApLTfc1HOnWiMGOU3KPwYwt006CdTkmJ0mL8Ni
blh9elyz9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
Y0djHdSOoKvDQNwu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviw8+TFVEBL104f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9G0tt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40f0oZyfAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

^C
bandit16@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

└─(tugbaarslan㉿kali)-[~]
└─$ vim key

```

| Now, use `ncat` command with `bandit16`'s password. I used 31790 TCP port:

```
$ ncat — ssl localhost 31790 kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
```

| When the private key is shown to us, exit that area with `CTRL+C` and enter the personal area by typing the `exit` command.

```
^C
```

```
$ exit
```

| Then write the `vim` command.

```
$ vim key
```

Then paste the text we found into it. After paste it, write this command.

```
[tugbaarslan㉿kali)-[~]
$ chmod 400 key

[tugbaarslan㉿kali)-[~]
$ ssh -i key bandit17@bandit.labs.overthewire.org -p 2220
```

Type the `chmod` command, because we need to give read permission.

```
$ chmod 400 key
```

| Finally, you can login with key:

Here is the login path: ssh -i key bandit.labs.overthewire.org -p 2220

Bandit Level 17 → Level 18

<https://overthewire.org/wargames/bandit/bandit18.html>

Level Goal

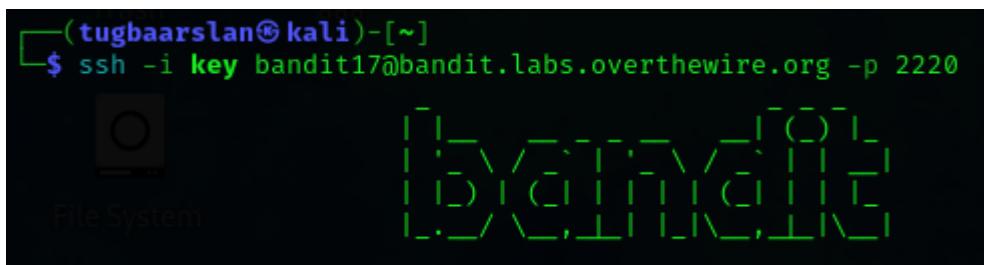
There are 2 files in the homedirectory: `passwords.old` and `passwords.new`. The password for the next level is in `passwords.new` and is the only line that has been changed between `passwords.old` and `passwords.new`

NOTE: if you have solved this level and see ‘Byebye!’ when trying to log into bandit18, this is related to the next level, bandit19

Login path: ssh -i key -p 2220

Host: bandit.labs.overthewire.org

Port: 2220



```
(tugbaarslan㉿kali)-[~]
$ ssh -i key bandit17@bandit.labs.overthewire.org -p 2220
```

| Firstly, login with key:

```
$ ssh -i key -p 2220
```

```
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< 7l8XDIVIk4Xtl7jMkwSKw6wYEedt6lcp
> x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlo
bandit17@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(tugbaarslan㉿kali)-[~]
$ ssh bandit18@bandit.labs.overthewire.org -p 2220
```

| Then, use the `diff` command and exit that area. Since one of the two options is a password, you should try entering both results as a password.

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

Here is the Bandit18's password: x2gLTtjFwMOhQ8oWNbMN362QKxfRqGIO

Bandit Level 18 → Level 19

<https://overthewire.org/wargames/bandit/bandit19.html>

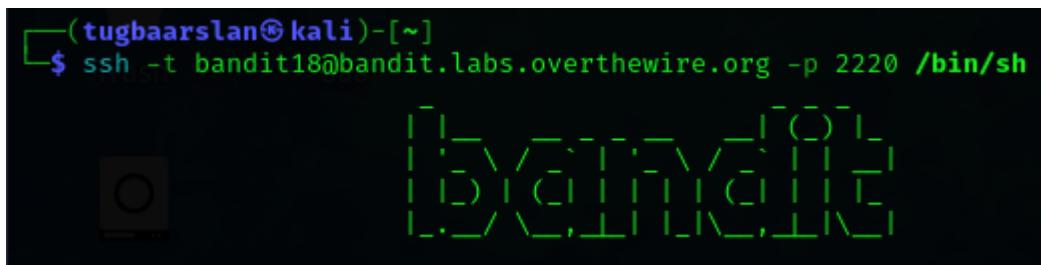
Level Goal

The password for the next level is stored in a file `readme` in the homedirectory.
Unfortunately, someone has modified `.bashrc` to log you out when you log in with SSH.

Password: x2gLTtjFwMOhQ8oWNbMN362QKxfRqGIO

Host: `bandit.labs.overthewire.org`

Port: 2220

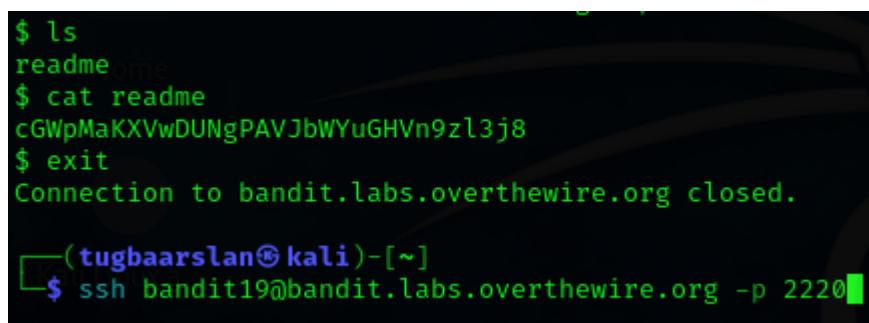


```
(tugbaarslan㉿kali)-[~]
$ ssh -t bandit18@bandit.labs.overthewire.org -p 2220 /bin/sh
```

Firstly, when logging in use `-t` parameter and `/bin/sh` bash scripts. Then type bandit18's password:

```
$ ssh -t bandit18@bandit.labs.overthewire.org -p 2220 /bin/sh
```

x2gLTtjFwMOhQ8oWNbMN362QKxfRqGIO



```
$ ls
readme
$ cat readme
cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
$ exit
Connection to bandit.labs.overthewire.org closed.

(tugbaarslan㉿kali)-[~]
$ ssh bandit19@bandit.labs.overthewire.org -p 2220
```

Execute `ls` command, you will find `readme` file. Read the file you found with the `cat` command and exit.

```
$ ls
```

```
$ cat readme
```

```
$ exit
```

Here is the Bandit19's password: cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8

Bandit Level 19 → Level 20

<https://overthewire.org/wargames/bandit/bandit20.html>

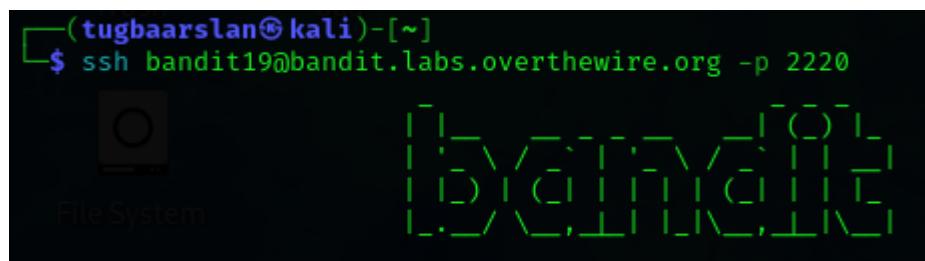
Level Goal

To gain access to the next level, you should use the setuid binary in the homedirectory. Execute it without arguments to find out how to use it. The password for this level can be found in the usual place (/etc/bandit_pass), after you have used the setuid binary.

Password: cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8

Host: bandit.labs.overthewire.org

Port: 2220

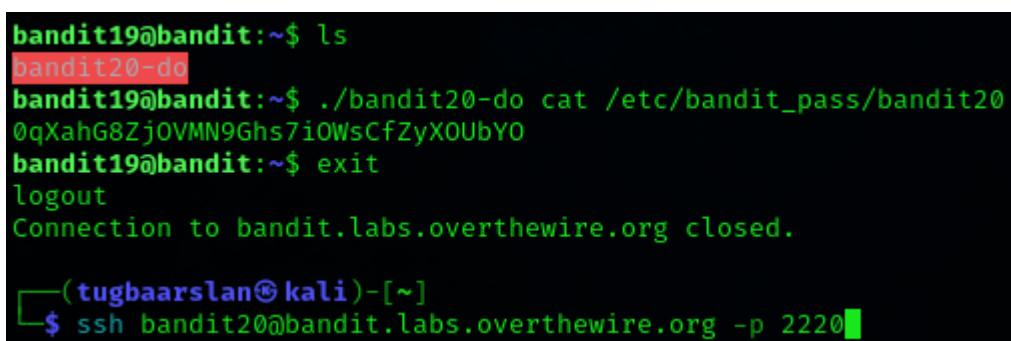


```
(tugbaarslan㉿kali)-[~]
$ ssh bandit19@bandit.labs.overthewire.org -p 2220
```

| Firstly, use this command and then write bandit19's password:

```
$ ssh -p 2220
```

cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8



```
bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8Zj0VMN9Ghs7iOWsCfZyXOUbYO
bandit19@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(tugbaarslan㉿kali)-[~]
$ ssh bandit20@bandit.labs.overthewire.org -p 2220
```

| Then, write the ls command and we see the target directory.

```
$ ls
```

| We use this command to display the data in:

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

Here is the Bandit20's password: 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO

Bandit Level 20 → Level 21

<https://overthewire.org/wargames/bandit/bandit21.html>

Level Goal

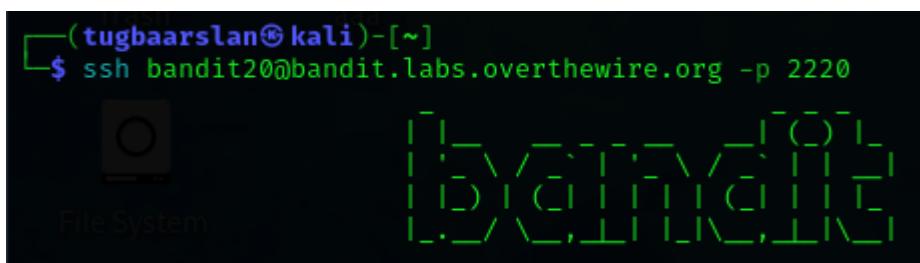
There is a setuid binary in the homedirectory that does the following: it makes a connection to localhost on the port you specify as a commandline argument. It then reads a line of text from the connection and compares it to the password in the previous level (bandit20). If the password is correct, it will transmit the password for the next level (bandit21).

NOTE: Try connecting to your own network daemon to see if it works as you think

Password: 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO

Host: bandit.labs.overthewire.org

Port: 2220



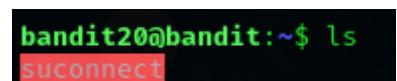
```
(tugbaarslan㉿kali)-[~]
$ ssh bandit20@bandit.labs.overthewire.org -p 2220
[File System]
```

Firstly, use this command and then write bandit20's password:

```
$ ssh -p 2220
```

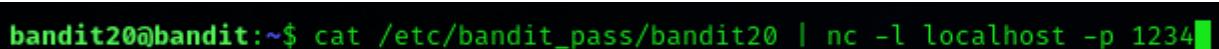
0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO

Then, write the ls command and we see the target directory.



```
bandit20@bandit:~$ ls
suconnect
```

```
$ ls
```



```
bandit20@bandit:~$ cat /etc/bandit_pass/bandit20 | nc -l localhost -p 1234
```

Press CTRL+T and write this command on the new screen and run it.

```
$ cat /etc/bandit_pass/bandit20 | nc -l localhost -p 1234
```

or

```
$ cat /etc/bandit_pass/bandit20 | nc -l -p 1234
```

| Go back to the previous screen and
run this command.

```
$ ./suconnect 1234
```

```
bandit20@bandit:~$ ./suconnect 1234
Read: 0qXahG8Zj0VMN9Ghs7iOWsCfZyX0UbYO
Password matches, sending next password
```

```
bandit20@bandit:~$ cat /etc/bandit_pass/bandit20 | nc -l -p 1234
EeoULMCra2q0dSkYj561DX7s1CpBuOBt
```

| Go back to the new page and the new password is here.

Here is the Bandit21's password: EeoULMCra2q0dSkYj561DX7s1CpBuOBt

Bandit Level 21 → Level 22

<https://overthewire.org/wargames/bandit/bandit22.html>

Level Goal

A program is running automatically at regular intervals from **cron**, the time-based job scheduler. Look in **/etc/cron.d/** for the configuration and see what command is being executed.

Password: EeoULMCra2q0dSkYj561DX7s1CpBuOBt

Host: bandit.labs.overthewire.org

Port: 2220

```
└─(tugbaarslan㉿kali)-[~]
$ ssh bandit21@bandit.labs.overthewire.org -p 2220
[██████████]
```

| Firstly, use this command and then write bandit21's password:

```
$ ssh -p 2220
```

EeoULMCra2q0dSkYj561DX7s1CpBuOBt

```
bandit21@bandit:~$ ls /etc/cron.d/
cronjob_bandit22 cronjob_bandit23 cronjob_bandit24 e2scrub_all otw-tmp-dir sysstat
bandit21@bandit:~$ cat /etc/cron.d/cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh >> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh >> /dev/null
bandit21@bandit:~$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:~$ cat /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q
bandit21@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

| Then, run these commands one by one.

```
$ ls /etc/cron.d/
$ cat /etc/cron.d/cronjob_bandit22
$ cat /usr/bin/cronjob_bandit22.sh
$ cat /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
```

Here is the Bandit22's password: tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q

Bandit Level 22 → Level 23

<https://overthewire.org/wargames/bandit/bandit23.html>

Level Goal

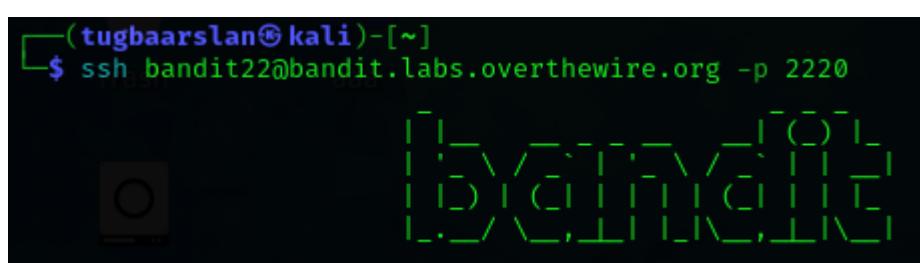
A program is running automatically at regular intervals from **cron**, the time-based job scheduler. Look in **/etc/cron.d/** for the configuration and see what command is being executed.

NOTE: Looking at shell scripts written by other people is a very useful skill. The script for this level is intentionally made easy to read. If you are having problems understanding what it does, try executing it to see the debug information it prints.

Password: tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q

Host: *bandit.labs.overthewire.org*

Port: 2220



| Firstly, use this command and then write bandit22's password:

```
$ ssh -p 2220
```

tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q

```
bandit22@bandit:~$ ls /etc/cron.d/
cronjob_bandit22 cronjob_bandit23 cronjob_bandit24 e2scrub_all otw-tmp-dir sysstat
bandit22@bandit:~$ cat /etc/cron.d/cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
bandit22@bandit:~$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget
bandit22@bandit:~$ echo "I am user bandit23" | md5sum | cut -d ' ' -f 1
8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:~$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
0Zf11ioIjMVN551jX3CmStKLYqjk54Ga
bandit22@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

| Then, run these commands one by one.

```
$ ls /etc/cron.d/
```

```
$ cat /etc/cron.d/cronjob_bandit23
```

```
$ cat /usr/bin/cronjob_bandit23.sh
```

```
$ echo "I am user bandit23" | md5sum | cut -d ' ' -f 1
```

```
$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
```

Here is the Bandit23's password: 0Zf11ioIjMVN551jX3CmStKLYqjk54Ga

Bandit Level 23 → Level 24

<https://overthewire.org/wargames/bandit/bandit24.html>

Level Goal

A program is running automatically at regular intervals from **cron**, the time-based job scheduler. Look in **/etc/cron.d/** for the configuration and see what command is being executed.

NOTE: This level requires you to create your own first shell-script. This is a very big step and you should be proud of yourself when you beat this level!

NOTE 2: Keep in mind that your shell script is removed once executed, so you may want to keep a copy around...

Password: 0Zf11ioljMVN551jX3CmStKLYqjk54Ga

Host: bandit.labs.overthewire.org

Port: 2220

```
(tugbaarslan㉿kali)-[~]
$ ssh bandit23@bandit.labs.overthewire.org -p 2220
```

| Firstly, use this command and then write bandit23's password:

```
$ ssh -p 2220
```

0Zf11ioljMVN551jX3CmStKLYqjk54Ga

```
bandit23@bandit:~$ cd /tmp
bandit23@bandit:/tmp$ mkdir /tmp/newdirectory
bandit23@bandit:/tmp$ chmod 777 /tmp/newdirectory
bandit23@bandit:/tmp$ echo '#!/bin/bash cat /etc/bandit_pass/bandit24 > /tmp/newdirectory/password.txt' > /tmp/newdirectory/myscript.sh
bandit23@bandit:/tmp$ chmod +x /tmp/newdirectory/myscript.sh
bandit23@bandit:/tmp$ mkdir -p /var/spool/bandit24/foo
bandit23@bandit:/tmp$ cp /tmp/newdirectory/myscript.sh /var/spool/bandit24/foo/myscript.sh
bandit23@bandit:/tmp$ cat /tmp/newdirectory/password.txt
```

| Then, run these commands one by one.

```
$ cd /tmp
```

```
$ mkdir /tmp/newdirectory
```

```
$ chmod 777 /tmp/newdirectory
```

```
$ echo '#!/bin/bash cat /etc/bandit_pass/bandit24 > /tmp/newdirectory/password.txt' > /tmp/newdirectory/myscript.sh
```

```
$ chmod +x /tmp/newdirectory/myscript.sh
```

```
$ mkdir -p /var/spool/bandit24/foo
```

```
$ cp /tmp/newdirectory/myscript.sh /var/spool/bandit24/foo/myscript.sh
```

```
$ cat /tmp/newdirectory/password.txt
```

```
gb8KRRCCsshuZXI0tUuR6yp0FjiZbf3G8
bandit23@bandit:/tmp$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Here is the Bandit24's password: `gb8KRRCCsshuZXI0tUuR6ypOFjiZbf3G8`

Bandit Level 24 → Level 25

<https://overthewire.org/wargames/bandit/bandit25.html>

Level Goal

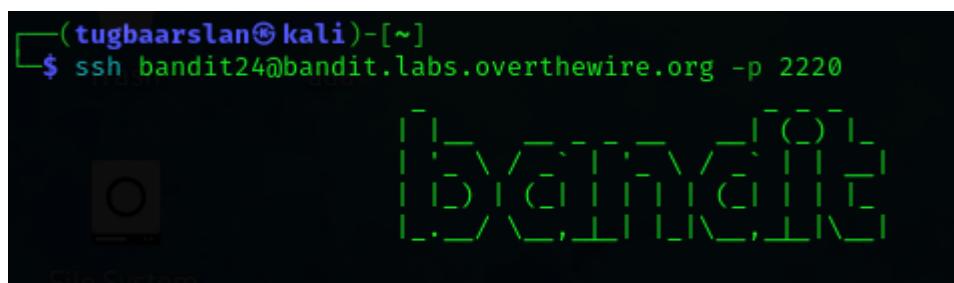
A daemon is listening on port 30002 and will give you the password for bandit25 if given the password for bandit24 and a secret numeric 4-digit pincode. There is no way to retrieve the pincode except by going through all of the 10000 combinations, called brute-forcing.

You do not need to create new connections each time

Password: `gb8KRRCCsshuZXI0tUuR6ypOFjiZbf3G8`

Host: `bandit.labs.overthewire.org`

Port: 2220

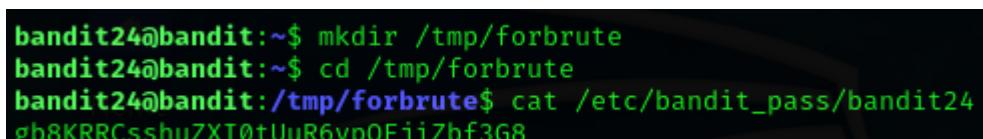


```
(tugbaarslan㉿kali)-[~]
$ ssh bandit24@bandit.labs.overthewire.org -p 2220
```

| Firstly, use this command and then write bandit24's password:

```
$ ssh -p 2220
```

gb8KRRCCsshuZXI0tUuR6ypOFjiZbf3G8



```
bandit24@bandit:~$ mkdir /tmp/forbrute
bandit24@bandit:~$ cd /tmp/forbrute
bandit24@bandit:/tmp/forbrute$ cat /etc/bandit_pass/bandit24
gb8KRRCCsshuZXI0tUuR6ypOFjiZbf3G8
```

| Then, run these commands.

```
$ mkdir /tmp/forbrute
```

```
$ cd /tmp/forbrute
```

```
$ cat /etc/bandit_pass/bandit24
```

| Then, create a file.

```
bandit24@bandit:/tmp/forbrute$ vim brute.sh
```

```
$ vim brute.sh
```

| Write this script inside.

```
#!/bin/bash
```

```
#!/bin/bash
bandit24=gb8KRRCCsshuZXI0tUuR6ypOFjiZbf3G8

for pin in {0000..9999}; do
    echo "$bandit24 $pin"
done | nc localhost 30002
```

bandit24=gb8KRRCCsshuZXI0tUuR6ypOFjiZbf3G8

for pin in {0000..9999}; do echo "\$bandit24 \$pin" done | nc localhost 30002

```
bandit24@bandit:/tmp/forbrute$ chmod 777 brute.sh
```

```
bandit24@bandit:/tmp/forbrute$ chmod +x ./brute.sh
```

| You can use one of these commands.

\$ chmod 777 brute.sh

| or

\$ chmod +x ./brute.sh

```
bandit24@bandit:/tmp/forbrute$ ./brute.sh
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret pincode on a
line, separated by a space.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
```

| Then, write this command.

\$./brute.sh

| Brute Force attack has begun.

```
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Correct!
The password of user bandit25 is iCi86ttT4KSNe1armKiwbQNmB3YJP3q4
```

| Password found.

Here is the Bandit25's password: *iCi86ttT4KSNe1armKiwbQNmB3YJP3q4*

Bandit Level 25 → Level 26

<https://overthewire.org/wargames/bandit/bandit26.html>

Level Goal

Logging in to bandit26 from bandit25 should be fairly easy... The shell for user bandit26 is not **/bin/bash**, but something else. Find out what it is, how it works and how to break out of it.

Password: iCi86ttT4KSNe1armKiwbQNmB3YJP3q4

Host: bandit.labs.overthewire.org

Port: 2220

```
[tugbaarslan@kali) ~]$ ssh bandit25@bandit.labs.overthewire.org -p 2220
```

Firstly, use this command and then write bandit25's password:

```
$ ssh -p 2220
```

jCj86ttT4KSNe1armKjwbQNmB3YJP3q4

```
bandit25@bandit:~$ cat /etc/passwd | grep bandit26
bandit26:x:11026:11026:bandit level 26:/home/bandit26:/usr/bin/showtext
bandit25@bandit:~$ cat /usr/bin/showtext
#!/bin/sh

export TERM=linux

KaliLinux a
exec more ~/text.txt
exit 0
```

Then run these commands

```
$ cat /etc/passwd | grep bandit26
```

```
$ cat /usr/bin/showtext
```

```
bandit25@bandit:~$ ssh -i bandit26.sshkey -p 2220 bandit26@bandit.labs.overthewire.org
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnv1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit25/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit25/.ssh/known_hosts).
```

Send a connection request with the ssh command. Don't forget to make the terminal a very small window before running this command.

```
$ ssh -i bandit26.sshkey -p 2220 bandit26@bandit.labs.overthewire.org
```

| Switch to vi mode by pressing the letter 'v'.

| Write this command.

```
:e /etc/bandit_pass/bandit26
```



A screenshot of a terminal window. The command ':e /etc/bandit_pass/bandit26' is typed at the bottom. The screen shows the file contents in vi mode, with the cursor at the end of the line.

```
s0773xxkk0MXfdqOfPRVr9L3jJBUOgCZ
~/Trash/aaa
"/etc/bandit_pass/bandit26" [readonly] 1L, 33B
```

Here is the Bandit26's password: 0773xxkk0MXfdqOfPRVr9L3jJBUOgCZ

Bandit Level 26 → Level 27

<https://overthewire.org/wargames/bandit/bandit27.html>

Level Goal

Good job getting a shell! Now hurry and grab the password for bandit27!

>Password: 0773xxkk0MXfdqOfPRVr9L3jJBUOgCZ

Host: *bandit.labs.overthewire.org*

Port: 2220



A screenshot of a terminal window. The command ':set shell=/bin/bash' is typed at the bottom. The screen shows the file contents in vi mode, with the cursor at the end of the line.

| Write this command when you in the vi mode.

```
:set shell=/bin/bash
```



A screenshot of a terminal window. The command ':shell' is typed at the bottom. The screen shows the file contents in vi mode, with the cursor at the end of the line.

| Press Enter and then add this command.

```
:shell
```

| View the contents of the directory.

```
$ ls
```

```
bandit26@bandit:~$ ls  
bandit27-do  text.txt
```

```
bandit26@bandit:~$ ./bandit27-do cat /etc/bandit_pass/bandit27  
upsNCc7vzaRDx6oZC6GiR6ERwe1MowGB  
bandit26@bandit:~$
```

| Write this command and find the password.

```
./bandit27-do cat /etc/bandit_pass/bandit27
```

Here is the Bandit27's password: upsNCc7vzaRDx6oZC6GiR6ERwe1MowGB

Bandit Level 27 → Level 28

<https://overthewire.org/wargames/bandit/bandit28.html>

Level Goal

There is a git repository at `ssh://bandit27-git@localhost/home/bandit27-git/repo` via the port `2220`. The password for the user `bandit27-git` is the same as for the user `bandit27`.

Clone the repository and find the password for the next level.

Password: `upsNCc7vzaRDx6oZC6GiR6ERwe1MowGB`

Host: `bandit.labs.overthewire.org`

Port: `2220`

```
(tugbaarslan㉿kali)-[~]  
$ ssh bandit27@bandit.labs.overthewire.org -p 2220
```

| Firstly, use this command and then write bandit27's password:

```
$ ssh -p 2220
```

`upsNCc7vzaRDx6oZC6GiR6ERwe1MowGB`

```
bandit27@bandit:~$ cat /etc/bandit_pass/bandit27  
upsNCc7vzaRDx6oZC6GiR6ERwe1MowGB  
bandit27@bandit:~$ mkdir /tmp/forclone  
bandit27@bandit:~$ cd /tmp/forclone
```

| Write these commands.

```
$ cat /etc/bandit_pass/bandit27
```

```
$ mkdir /tmp/forclone
```

```
$ cd /tmp/forclone
```

```
bandit27@bandit:/tmp/forclone$ GIT_SSH_COMMAND='ssh -p 2220' git clone ssh://bandit27-git@localhost/home/bandit27-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit27/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit27/.ssh/known_hosts).

[REDACTED]
Home

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

bandit27-git@localhost's password:
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3) done.
```

| Type the command required to clone git and enter the password bandit27.

```
$ GIT_SSH_COMMAND='ssh -p 2220' git clone ssh://bandit27-
git@localhost/home/bandit27-git/repo
```

upsNCc7vzaRDx6oZC6GiR6ERwe1MowGB

```
bandit27@bandit:/tmp/forclone$ ls -al
total 280
drwxrwxr-x  3 bandit27 bandit27  4096 Jun 27 20:48 .
drwxrwxr-x 7068 root    root     274432 Jun 27 20:49 [REDACTED]
drwxrwxr-x  3 bandit27 bandit27  4096 Jun 27 20:48 repo
bandit27@bandit:/tmp/forclone$ cd repo/
bandit27@bandit:/tmp/forclone/repo$ ls -al
total 16
drwxrwxr-x  3 bandit27 bandit27  4096 Jun 27 20:48 .
drwxrwxr-x  3 bandit27 bandit27  4096 Jun 27 20:48 ..
drwxrwxr-x  8 bandit27 bandit27  4096 Jun 27 20:48 .git
-rw-rw-r--  1 bandit27 bandit27   68 Jun 27 20:48 README
bandit27@bandit:/tmp/forclone/repo$ cat README
The password to the next level is: Yz9IpL0sBcCeug7m9uQFt8ZNpS4HZRcN
bandit27@bandit:/tmp/forclone/repo$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

| Write these commands and find the password.

```
$ ls -al
```

```
$ cd repo/
```

```
$ ls -al
```

```
$ cat README
```

Here is the Bandit28's password: Yz9IpL0sBcCeuG7m9uQFt8ZNpS4HZRcN

Bandit Level 28 → Level 29

<https://overthewire.org/wargames/bandit/bandit29.html>

Level Goal

There is a git repository at `ssh://bandit28-git@localhost/home/bandit28-git/repo` via the port `2220`. The password for the user `bandit28-git` is the same as for the user `bandit28`.

Clone the repository and find the password for the next level.

Password: Yz9IpL0sBcCeuG7m9uQFt8ZNpS4HZRcN

Host: bandit.labs.overthewire.org

Port: 2220



```
(tugbaarslan㉿kali)-[~]
$ ssh bandit28@bandit.labs.overthewire.org -p 2220
```

| Firstly, use this command and then write bandit28's password:

\$ ssh -p 2220

Yz9IpL0sBcCeuG7m9uQFt8ZNpS4HZRcN

```
bandit28@bandit:~$ pass=Yz9IpL0sBcCeuG7m9uQFt8ZNpS4HZRcN
```

| Write this command.

\$ pass=Yz9IpL0sBcCeuG7m9uQFt8ZNpS4HZRcN

| Type these commands too.

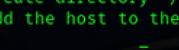
\$ mkdir /tmp/othergitclone

```
bandit28@bandit:~$ mkdir /tmp/othergitclone
bandit28@bandit:~$ cd /tmp/othergitclone
```

\$ cd /tmp/othergitclone

```
bandit28@bandit:~/tmp/othergitclone$ GIT_SSH_COMMAND='ssh -p 2220' git clone ssh://bandit28-git@localhost/home/bandit28-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfxC5XLhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit28/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit28/.ssh/known_hosts).

Home
```



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

```
bandit28-git@localhost's password:
```

```
remote: Enumerating objects: 9, done.
remote: Counting objects: 100% (9/9), done.
remote: Compressing objects: 100% (6/6), done.
```

Type the command required to clone git and enter the password bandit28.

```
$ GIT_SSH_COMMAND='ssh -p 2220' git clone ssh://bandit28-git@localhost/home/bandit28-git/repo
```

Yz9lpL0sBcCeuG7m9uQFt8ZNpS4HZRcN

```
bandit28@bandit:/tmp/othergitclone$ ls -al
total 280
drwxrwxr-x    3 bandit28 bandit28  4096 Jun 27 22:01 .
drwxrwxrwt 7117 root      root     274432 Jun 27 22:02 ..
drwxrwxr-x    3 bandit28 bandit28  4096 Jun 27 22:01 repo
bandit28@bandit:/tmp/othergitclone$ cd repo/
bandit28@bandit:/tmp/othergitclone/repo$ ls -al
total 16
drwxrwxr-x  3 bandit28 bandit28 4096 Jun 27 22:01 .
drwxrwxr-x  3 bandit28 bandit28 4096 Jun 27 22:01 ..
drwxrwxr-x  8 bandit28 bandit28 4096 Jun 27 22:01 .git
-rw-rw-r--  1 bandit28 bandit28  111 Jun 27 22:01 README.md
bandit28@bandit:/tmp/othergitclone/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: xxxxxxxxxxxx
```

Write these commands

§ 18-a

```
$ cd repo/
```

§ 18-a(1)

```
$ cat README.md
```

```
bandit28@bandit:/tmp/othergitclone/repo$ git log
commit ad9a337071c5e3d4509559d36128b38a0e5571f1 (HEAD → master, origin/master, origin/HEAD)
Author: Morla Porla <morla@overthewire.org>
Date: Thu Jun 20 04:07:12 2024 +0000

    fix info leak

commit 229f6001e1ff407bb935b82a94c6749e41a0693e
Author: Morla Porla <morla@overthewire.org>
Date: Thu Jun 20 04:07:12 2024 +0000

    add missing data

commit ea882192c25642e69627b13179f9fb98f409ed5d
Author: Ben Dover <noone@overthewire.org>
Date: Thu Jun 20 04:07:12 2024 +0000

    initial commit of README.md
bandit28@bandit:/tmp/othergitclone/repo$ git branch
* master
bandit28@bandit:/tmp/othergitclone/repo$ git checkout 229f6001e1ff407bb935b82a94c6749e41a0693e
Note: switching to '229f6001e1ff407bb935b82a94c6749e41a0693e'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.
```

Since we cannot view the password, type these commands. Then add the data in one of them to the ‘checkout’ command.

```
$ git log
```

```
$ git branch
```

```
$ git checkout 229f6001e1ff407bb935b82a94c6749e41a0693e
```

```
bandit28@bandit:/tmp/othergitclone/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: 4pT1t5DENaYuqnqvadYs1oE4QLCdjJ7
```

Write this command and find the password.

```
$ cat README.md
```

Here is the Bandit29’s password: 4pT1t5DENaYuqnqvadYs1oE4QLCdjJ7

Bandit Level 29 → Level 30

<https://overthewire.org/wargames/bandit/bandit30.html>

Level Goal

There is a git repository at `ssh://bandit29-git@localhost/home/bandit29-git/repo` via the port `2220`. The password for the user `bandit29-git` is the same as for the user `bandit29`.

Clone the repository and find the password for the next level.

>Password: 4pT1t5DENaYuqnqvadYs1oE4QLCdjJ7

Host: bandit.labs.overthewire.org

Port: 2220

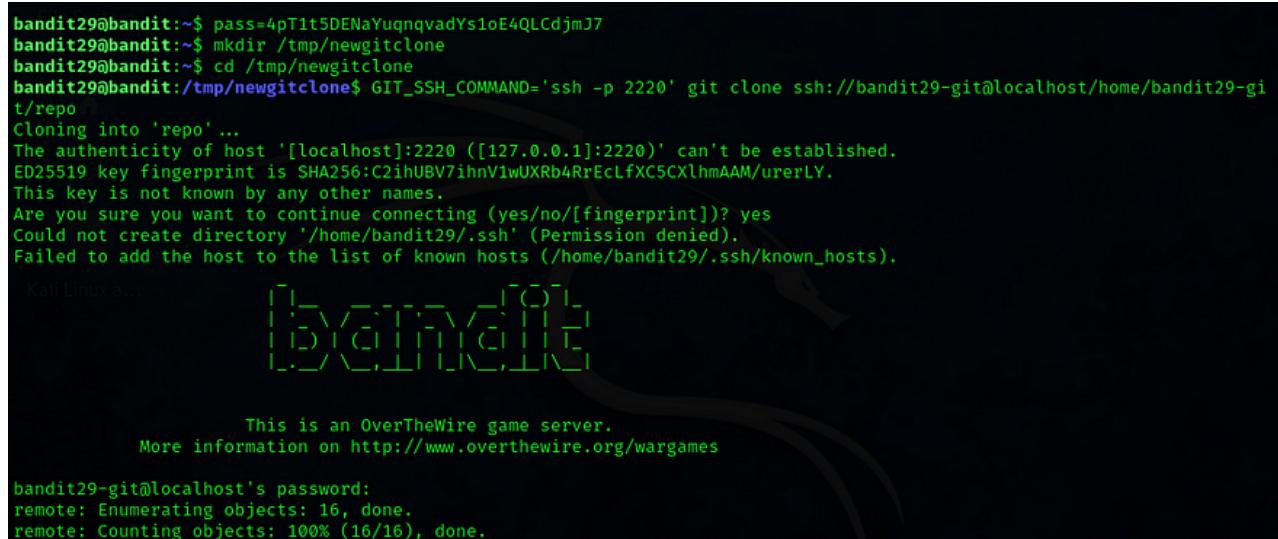


```
(tugbaarslan㉿kali)-[~]
$ ssh bandit29@bandit.labs.overthewire.org -p 2220
```

| Firstly, use this command and then write bandit29's password:

```
$ ssh -p 2220
```

4pT1t5DENaYuqnqvadYs1oE4QLCdjJ7



```
bandit29@bandit:~$ pass=4pT1t5DENaYuqnqvadYs1oE4QLCdjJ7
bandit29@bandit:~$ mkdir /tmp/newgitclone
bandit29@bandit:~$ cd /tmp/newgitclone
bandit29@bandit:/tmp/newgitclone$ GIT_SSH_COMMAND='ssh -p 2220' git clone ssh://bandit29-git@localhost/home/bandit29-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnViwUXRb4RrEcLfxC5CxLhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit29/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit29/.ssh/known_hosts).

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

bandit29-git@localhost's password:
remote: Enumerating objects: 16, done.
remote: Counting objects: 100% (16/16), done.
remote: Compressing objects: 100% (11/11), done.
```

| Write these commands. Then, enter the password of Bandit29.

```
$ pass=4pT1t5DENaYuqnqvadYs1oE4QLCdjJ7
```

```
$ mkdir /tmp/newgitclone
```

```
$ cd /tmp/newgitclone
```

```
$ GIT_SSH_COMMAND='ssh -p 2220' git clone ssh://bandit29-
git@localhost/home/bandit29-git/repo
```

4pT1t5DENaYuqnqvadYs1oE4QLCdjJ7

```
bandit29@bandit:/tmp/newgitclone$ ls -al
total 280
drwxrwxr-x    3 bandit29 bandit29   4096 Jun 27 22:20 .
drwxrwx-wt 7136 root      root     274432 Jun 27 22:22 ..
drwxrwxr-x    3 bandit29 bandit29   4096 Jun 27 22:20 repo
bandit29@bandit:/tmp/newgitclone$ cd repo
bandit29@bandit:/tmp/newgitclone/repo$ ls
README.md
bandit29@bandit:/tmp/newgitclone/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: <no passwords in production!>
```

| Write these commands.

```
$ ls -al
```

```
$ cd repo
```

```
$ ls
```

```
$ cat README.md
```

```
bandit29@bandit:/tmp/newgitclone/repo$ git branch -r
origin/HEAD → origin/master
origin/dev
origin/master
origin/sploits-dev
```

| Type these commands to view the password.

```
$ git branch -r
```

```
bandit29@bandit:/tmp/newgitclone/repo$ git checkout dev
branch 'dev' set up to track 'origin/dev'.
Switched to a new branch 'dev'
```

| Add this command as well.

```
$ git checkout dev
```

```
bandit29@bandit:/tmp/newgitclone/repo$ git log
commit 196330cb19cb783552d999864c06a9b81a4e60e8 (HEAD → dev, origin/dev)
Author: Morla Porla <morla@overthewire.org>
Date: Thu Jun 20 04:07:14 2024 +0000

    add data needed for development
    File System

commit 1f3fff853b240c291986d0a6b8c885a90e56322a
Author: Ben Dover <noone@overthewire.org>
Date: Thu Jun 20 04:07:14 2024 +0000

    add gif2ascii
    Home

commit a442ed81c95fac132590fdd218bd7b831db81fe4 (origin/master, origin/HEAD, master)
Author: Ben Dover <noone@overthewire.org>
Date: Thu Jun 20 04:07:14 2024 +0000

    fix username
    Kalilinux

commit 046a4d27b46af8f02879c890972d7f125f3ab824
Author: Ben Dover <noone@overthewire.org>
Date: Thu Jun 20 04:07:14 2024 +0000

    initial commit of README.md
bandit29@bandit:/tmp/newgitclone/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: qp30ex3VLz5MDG1n91YowTv4Q8l7CDZL
```

| You will get the password when you review and try again.

\$ git log

\$ cat README.md

Here is the Bandit30's password: qp30ex3VLz5MDG1n91YowTv4Q8l7CDZL

Bandit Level 30 → Level 31

<https://overthewire.org/wargames/bandit/bandit31.html>

Level Goal

There is a git repository at `ssh://bandit30-git@localhost/home/bandit30-git/repo` via the port `2220`. The password for the user `bandit30-git` is the same as for the user `bandit30`.

Clone the repository and find the password for the next level.

Password: qp30ex3VLz5MDG1n91YowTv4Q8l7CDZL

Host: bandit.labs.overthewire.org

Port: 2220

```
(tugbaarslan㉿kali)-[~]
$ ssh bandit30@bandit.labs.overthewire.org -p 2220
File System
```

| Firstly, use this command and then write bandit30's password:

```
$ ssh -p 2220
```

qp30ex3VLz5MDG1n91YowTv4Q8l7CDZL

```
bandit30@bandit:~$ shell=qp30ex3VLz5MDG1n91YowTv4Q8l7CDZL
bandit30@bandit:~$ mkdir /tmp/othernew
bandit30@bandit:~$ cd /tmp/othernew
bandit30@bandit:/tmp/othernew$ GIT_SSH_COMMAND='ssh -p 2220' git clone ssh://bandit30-git@localhost/home/bandit30-git/repo
Cloning into 'repo' ...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit30/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit30/.ssh/known_hosts).

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

bandit30-git@localhost's password:
```

| Write these commands. Then, enter the password of Bandit30.

```
$ shell=qp30ex3VLz5MDG1n91YowTv4Q8l7CDZL
```

```
$ mkdir /tmp/othernew
```

```
$ cd /tmp/othernew
```

```
$ GIT_SSH_COMMAND='ssh -p 2220' git clone ssh://bandit30-git@localhost/home/bandit30-git/repo
```

qp30ex3VLz5MDG1n91YowTv4Q8l7CDZL

```
bandit30@bandit:/tmp/othernew$ cd repo
bandit30@bandit:/tmp/othernew/repo$ ls -al
total 16
drwxrwxr-x 3 bandit30 bandit30 4096 Jun 27 22:48 .
drwxrwxr-x 3 bandit30 bandit30 4096 Jun 27 22:48 ..
drwxrwxr-x 8 bandit30 bandit30 4096 Jun 27 22:48 .git
-rw-rw-r-- 1 bandit30 bandit30 30 Jun 27 22:48 README.md
bandit30@bandit:/tmp/othernew/repo$ cat README.md
just an empty file ... muahaha
```

| Write these commands.

```
$ cd repo  
$ ls -al  
$ cat README.md
```

```
bandit30@bandit:/tmp/othernew/repo$ git tag  
secret  
bandit30@bandit:/tmp/othernew/repo$ git show secret  
fb5S2xb7bRyFmAvQYQGEqsbhVJqhnDy
```

| Type these commands and find the password.

```
$ git tag  
$ git show secret
```

Here is the Bandit31's password: fb5S2xb7bRyFmAvQYQGEqsbhVJqhnDy

Bandit Level 31 → Level 32

<https://overthewire.org/wargames/bandit/bandit32.html>

Level Goal

There is a git repository at `ssh://bandit31-git@localhost/home/bandit31-git/repo` via the port `2220`. The password for the user `bandit31-git` is the same as for the user `bandit31`.

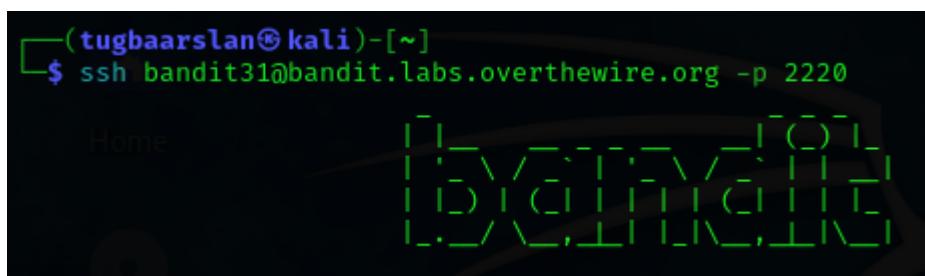
Clone the repository and find the password for the next level.

Password: fb5S2xb7bRyFmAvQYQGEqsbhVJqhnDy

Host: bandit.labs.overthewire.org

Port: 2220

```
└─(tugbaarslan㉿kali)-[~]  
$ ssh bandit31@bandit.labs.overthewire.org -p 2220
```



| Firstly, use this command and then write bandit31's password:

```
$ ssh -p 2220  
fb5S2xb7bRyFmAvQYQGEqsbhVJqhnDy
```

```
bandit31@bandit:~$ shell=fb552xb7bRyFmAvQYQGEqsbhVJqhnDy
bandit31@bandit:~$ mkdir /tmp/otheroneclone
bandit31@bandit:~$ cd /tmp/otheroneclone
bandit31@bandit:/tmp/otheroneclone$ GIT_SSH_COMMAND='ssh -p 2220' git clone ssh://bandit31-git@localhost/home/bandit31-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit31/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).

[|]_ \_\_--\_\_/\_\_ [|-]_-_
[|]_ | \_ | | | | | | | |
[|]_ | \_ | | | | | | | |
[|]_ | \_ | | | | | | | |

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

bandit31-git@localhost's password:
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
```

Write these commands. Then, enter the password of Bandit31.

`$ shell=fb5S2xb7bRyFmAvQYQGEqsbhVyJqhnDy`

```
$ mkdir /tmp/otheroneclone
```

```
$ cd /tmp/otheroneclone
```

```
$ GIT_SSH_COMMAND='ssh -p 2220' git clone ssh://bandit31-git@localhost/home/bandit31-git/repo
```

fb5S2xb7bRyFmAvQYQGEqsbhVyJghnDy

```

bandit31@bandit:/tmp/otheroneclone$ ls -al
total 284
drwxrwxr-x 3 bandit31 bandit31 4096 Jun 27 23:10 .
drwxrwxrwt 7167 root root 278528 Jun 27 23:11 ..
drwxrwxr-x 3 bandit31 bandit31 4096 Jun 27 23:11 repo
bandit31@bandit:/tmp/otheroneclone$ cd repo
bandit31@bandit:/tmp/otheroneclone/repo$ ls -al
total 20
drwxrwxr-x 3 bandit31 bandit31 4096 Jun 27 23:11 .
drwxrwxr-x 3 bandit31 bandit31 4096 Jun 27 23:10 ..
drwxrwxr-x 8 bandit31 bandit31 4096 Jun 27 23:11 .git
-rw-rw-r-- 1 bandit31 bandit31 6 Jun 27 23:11 .gitignore
-rw-rw-r-- 1 bandit31 bandit31 147 Jun 27 23:11 README.md
bandit31@bandit:/tmp/otheroneclone/repo$ cat .gitignore
*.txt
bandit31@bandit:/tmp/otheroneclone/repo$ cat README.md
This time your task is to push a file to the remote repository.

```

Details:

File name: key.txt
Content: 'May I come in?'
Branch: master

```

bandit31@bandit:/tmp/otheroneclone/repo$ git branch
* master
bandit31@bandit:/tmp/otheroneclone/repo$ ls -al
total 20
drwxrwxr-x 3 bandit31 bandit31 4096 Jun 27 23:11 .
drwxrwxr-x 3 bandit31 bandit31 4096 Jun 27 23:10 ..
drwxrwxr-x 8 bandit31 bandit31 4096 Jun 27 23:11 .git
-rw-rw-r-- 1 bandit31 bandit31 6 Jun 27 23:11 .gitignore
-rw-rw-r-- 1 bandit31 bandit31 147 Jun 27 23:11 README.md
bandit31@bandit:/tmp/otheroneclone/repo$ rm .gitignore
bandit31@bandit:/tmp/otheroneclone/repo$ echo "May I come in?" > key.txt
bandit31@bandit:/tmp/otheroneclone/repo$ cat key.txt
May I come in?
bandit31@bandit:/tmp/otheroneclone/repo$ git add key.txt
bandit31@bandit:/tmp/otheroneclone/repo$ git commit -m "Added key.txt"
[master e6c66ac] Added key.txt
 1 file changed, 1 insertion(+)
 create mode 100644 key.txt

```

Write these commands.

```

$ ls -al
$ cd repo
$ ls -al
$ cat .gitignore
$ cat README.md
$ git branch
$ ls -al
$ rm .gitignore

```

```
$ echo "May I come in?" > key.txt
```

```
$ cat key.txt
```

```
$ git add key.txt
```

```
$ git commit -m "Added key.txt"
```

```
bandit31@bandit:/tmp/otheroneclone/repo$ GIT_SSH_COMMAND='ssh -p 2220' git push
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit31/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).
```

Home



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

```
Kali Linux a...  
bandit31-git@localhost's password:  
Enumerating objects: 4, done.  
Counting objects: 100% (4/4), done.  
Delta compression using up to 2 threads  
Compressing objects: 100% (2/2), done.  
Writing objects: 100% (3/3), 325 bytes | 108.00 KiB/s, done.  
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0  
remote: ### Attempting to validate files ... ####  
remote:  
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.  
remote:  
remote: Well done! Here is the password for the next level:  
remote: 3O9RfhqyAlVBEZpVb6LYStshZoqoSx5K  
remote:  
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.  
remote:  
To ssh://localhost/home/bandit31-git/repo  
 ! [remote rejected] master → master (pre-receive hook declined)  
error: failed to push some refs to 'ssh://localhost/home/bandit31-git/repo'
```

Type the command needed to run `git push` and enter the password `bandit31`. So you can find the new password.

```
$ GIT_SSH_COMMAND='ssh -p 2220' git push
```

```
fb5S2xb7bRyFmAvQYQGEqsbhVyJqhnDy
```

Here is the Bandit32's password: 3O9RfhqyAlVBEZpVb6LYStshZoqoSx5K

Bandit Level 32 → Level 33

<https://overthewire.org/wargames/bandit/bandit33.html>

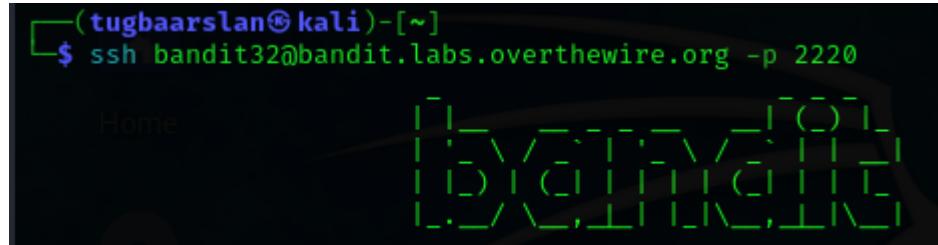
Level Goal

After all this `git` stuff, it's time for another escape. Good luck!

Password: 3O9RfhqyAlVBEZpVb6LYStshZoqoSx5K

Host: bandit.labs.overthewire.org

Port: 2220



```
(tugbaarslan㉿kali)-[~]
$ ssh bandit32@bandit.labs.overthewire.org -p 2220
```

| *Firstly, use this command and then write bandit32's password:*

```
$ ssh -p 2220
```

3O9RfhqyAlVBEZpVb6LYStshZoqoSx5K

| *Type these commands and find the password.*

```
>> $0
```

```
WELCOME TO THE UPPERCASE SHELL
>> $0
$ cat /etc/bandit_pass/bandit33
tQdtbs5D5i2vJwkO8mEyYEyTL8izoeJ0
```

```
$ cat /etc/bandit_pass/bandit33
```

Here is the Bandit33's password: tQdtbs5D5i2vJwkO8mEyYEyTL8izoeJ0

Congratulations, everything is done! Thanks for reading my work.

My LinkedIn account: <https://www.linkedin.com/in/tugba--arslan/>