OverTheWire – Bandit:

Level 0-10

Today, I will play a war-game called **Bandit**. It has 34 levels. In this write-up I will play level 0-10.

The main objective is to access password files which will help us login into the next levels.

Level 0

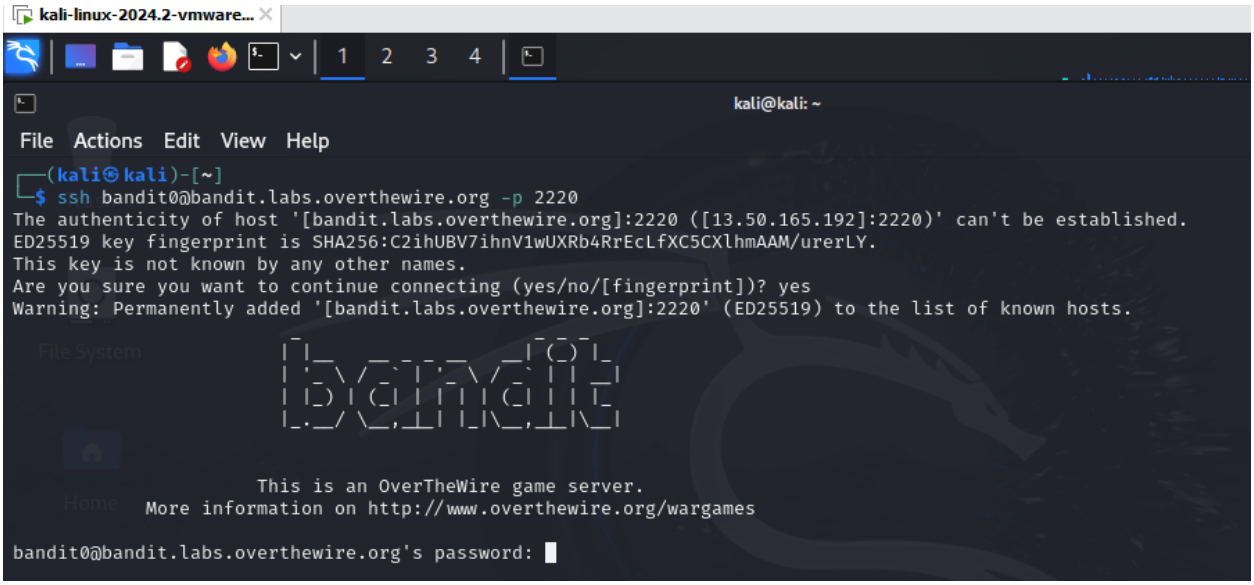
This is a pretty simple level. In this level we will connect to a host using ssh, so we will use the ssh command here. We have the following information on the instruction page of bandit.

Host: bandit.labs.overthewire.org

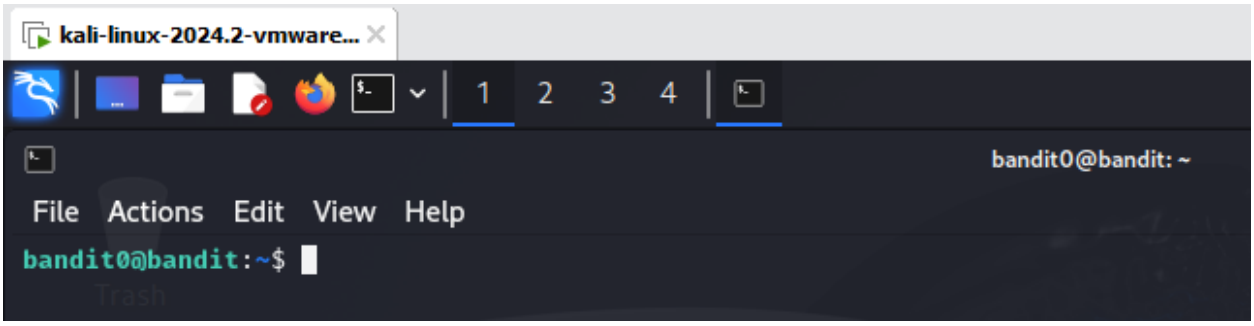
Port: 2220

Username: bandit0

Password: bandit0

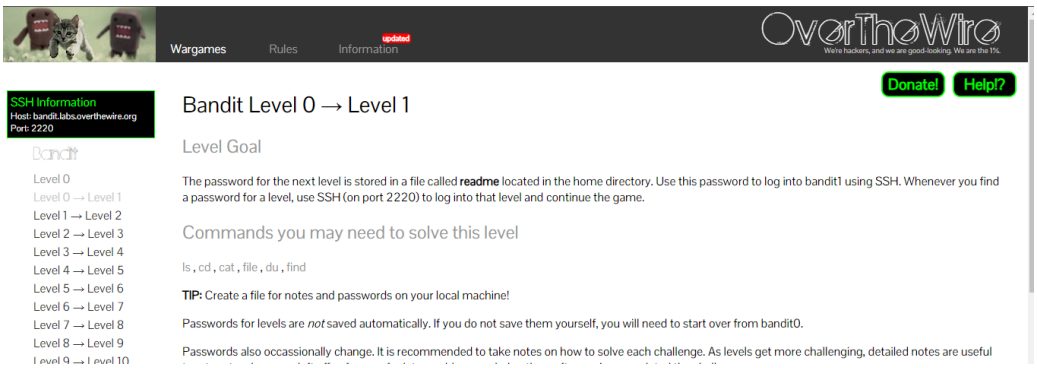


So here I entered the password and we are in bandit0 shell now:

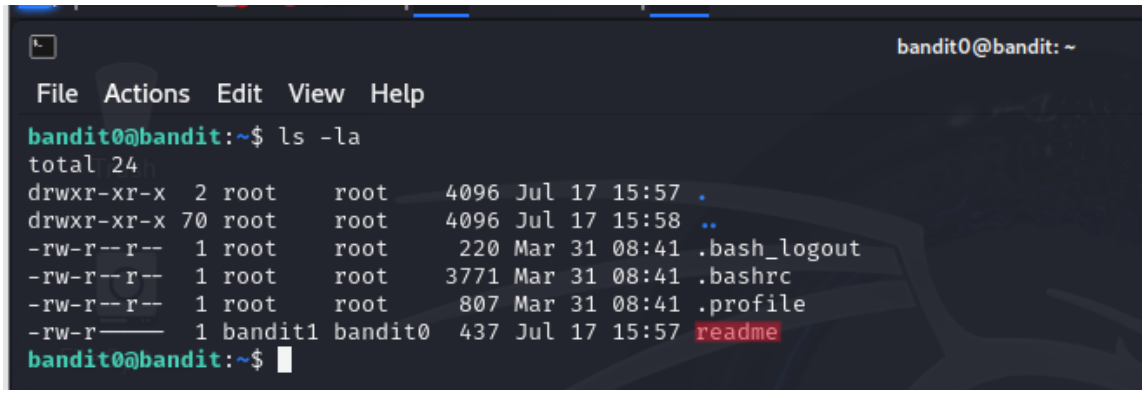


Level 0-1

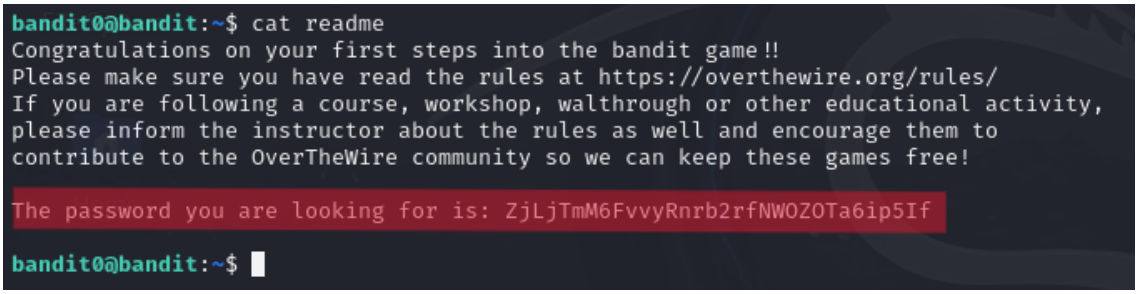
Now from bandit0 we have to find the password for bandit level 1. And for that I am going to list the files in the directory to find the readme file. And this was the hint given on the bandit webpage:



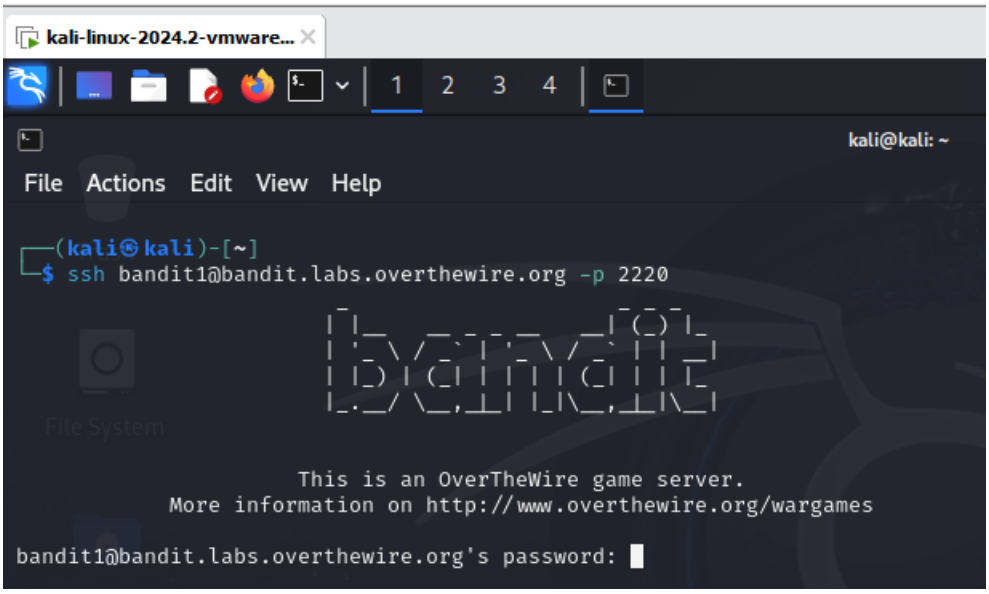
Now to list the files in the directory I am going to use the `ls` command:



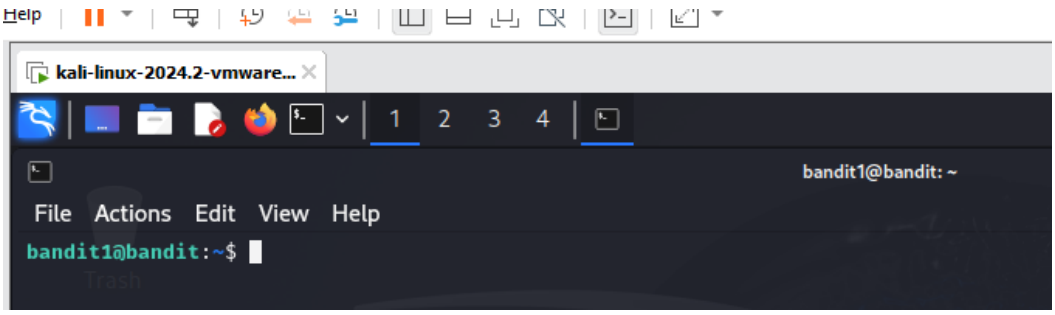
See here I got the readme file, now to read this file I am gonna use the `cat` command.



Now I am going to use this password for logging in to the next level using `ssh` command:

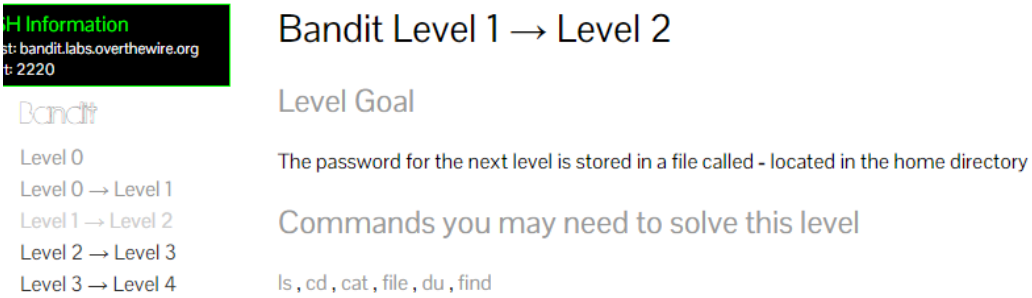


After entering the password here I am in bandit1 shell.

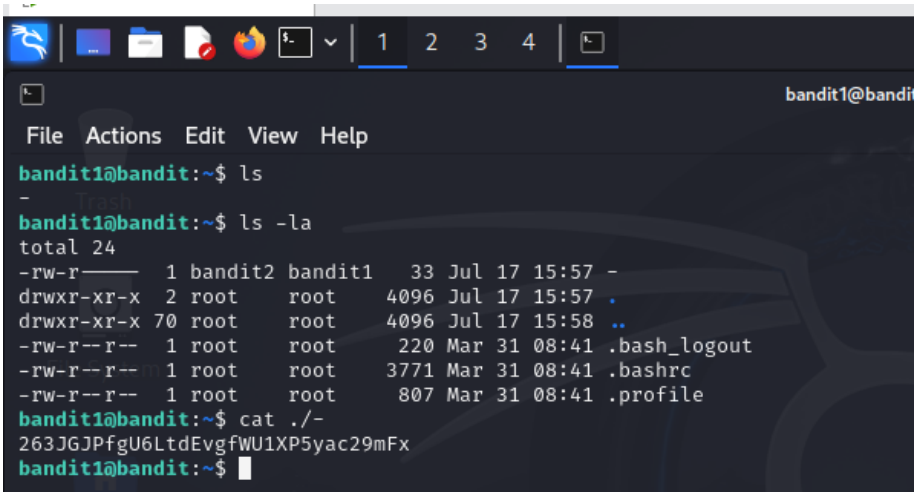


Level 1-2:

So here we can see that now the password is in –(file).



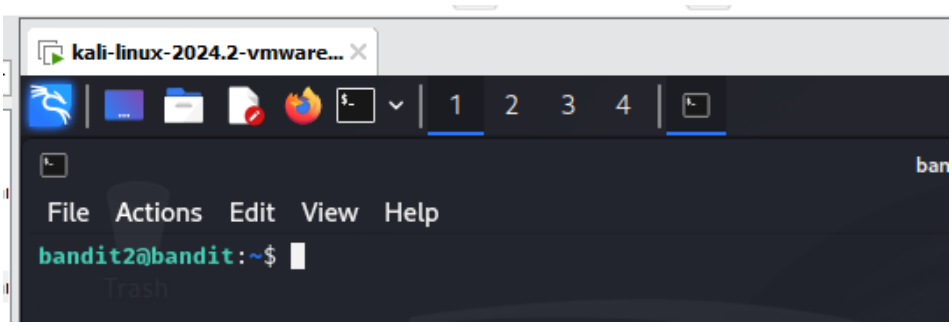
So to find the password I will use the `ls` command. As the file is named -(hyphen) we won't be able to read it simply by cat command. As cat command considers -(hyphen) as stdin/Stout. If we directly use cat command, it won't be able to understand that hyphen is a file name. So, we will prefix the command with the path ./



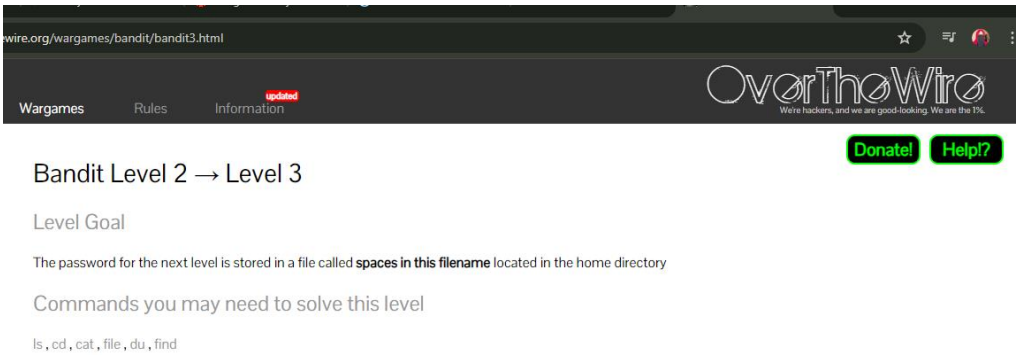
Now I am going to use this password for logging in to the next level using `ssh` command:

`ssh bandit2@bandit.labs.overthewire.org -p 2220`

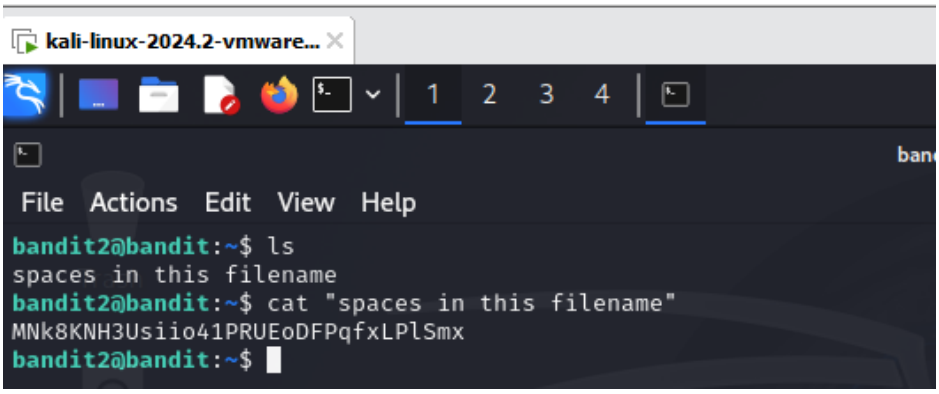
After entering the password here I am in bandit2 shell.



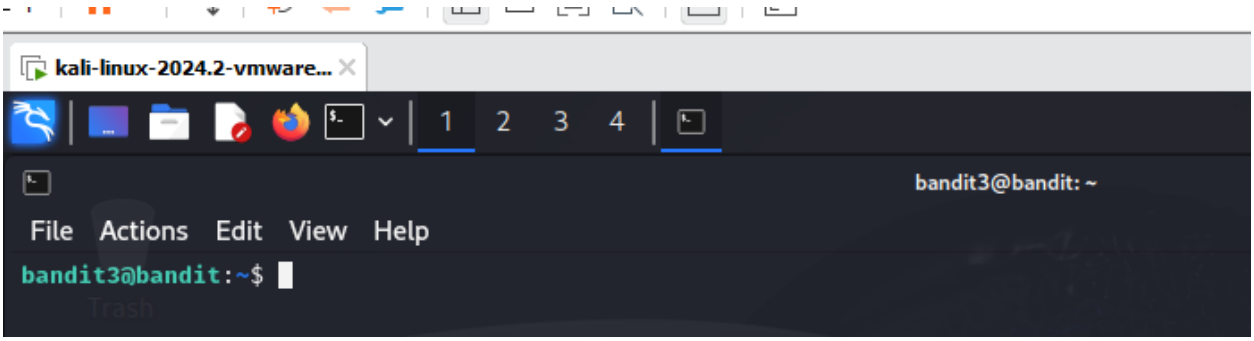
Level 2-3:



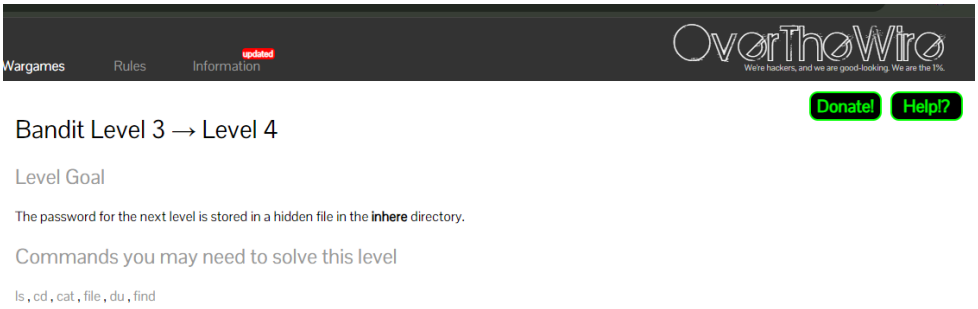
We can see that the password for the next level is stored inside a file named **spaces in this filename**. So, to find it we use the ls command. Now we have to read the file. As the file is named **spaces in this filename**, we won't be able to read it simply by cat command. So, we will write the name of the file in quotes.



After entering the password we are in the bandit3 shell:

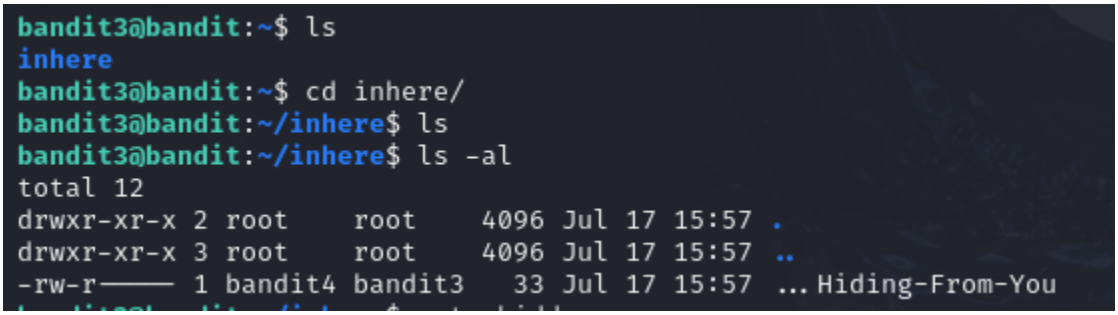


Level 3-4:



The password for the next level is stored inside a directory named **inhere**. So, we use the `ls` command.

It might be the case that the file is hidden. So, we run ls command with `-al` parameter. It lists all files including the hidden one. And we found the .Hiding-From-You file.



Now we would simply use the cat command to read the password stored in the file.

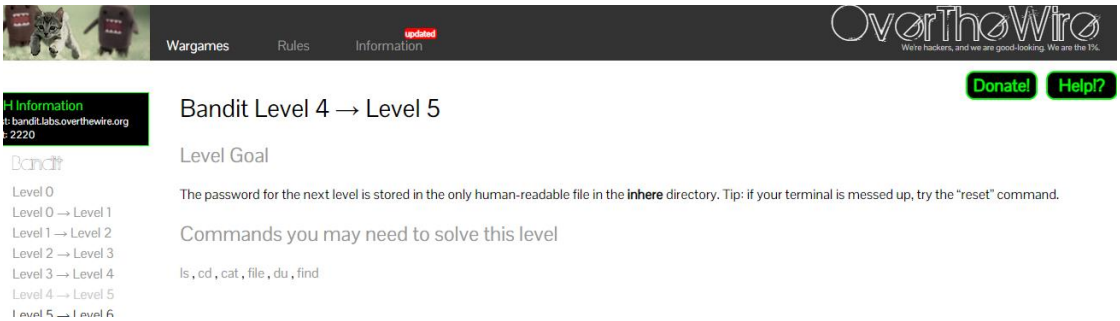
```
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
```

After entering the password we are in bandit4 shell:

```
  Enjoy your stay!

bandit4@bandit:~$
```

Level 4-5:



So, here the password is in the inhere directory which is a human-readable file, So after getting inside inhere directory we run ls command. Here we can see there are so many files given.

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$
```

We will use the file command to get the information about the files.

```
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$
```

Here I saw that the file07 contains **ASCII text**(readable text). So, let's read it using cat command.

```
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
```

This gave me the password for the next level. We will use it to get an SSH connection as bandit5.

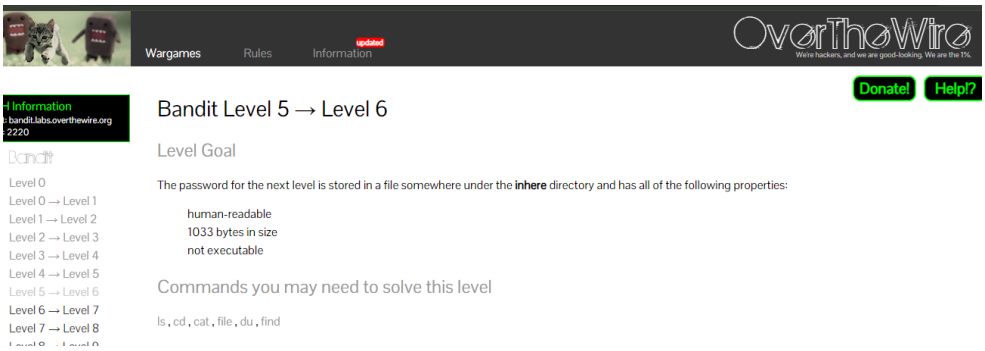
Harrum Fatima

Here we are in bandit shell5:

```
Enjoy your stay!

bandit5@bandit:~$
```

Level 5-6:



After getting inside inhere directory we run ls command. Here we can see there are so many files given.

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere02  maybehere04  maybehere06  maybehere08  maybehere10  maybehere12  maybehere14  maybehere16  maybehere18
maybehere01  maybehere03  maybehere05  maybehere07  maybehere09  maybehere11  maybehere13  maybehere15  maybehere17  maybehere19
bandit5@bandit:~/inhere$
```

Again there are so many files given, so according to the hint given (file size = 1033 bytes). We can use the find size command to see which file is of 1033 bytes:

```
bandit5@bandit:~/inhere$ find . -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$
```

Now we can see that the file size matches this file, so lets see the cat command:

```
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

bandit5@bandit:~/inhere$
```

So got the password for bandit 6. After using the credentials we are in bandit shell 6:

```
Enjoy your stay!

bandit6@bandit:~$
```

Level 6-7:

Wargames Rules Information updated OverTheWire We're hackers, and we are good-looking. We are the 1%.

Donate! Help!?

Bandit Level 6 → Level 7

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

Commands you may need to solve this level

ls , cd , cat , file , du , find , grep

So here according to the hints given password is somewhere on the server, but finding the password in this way is difficult so we can use the other hints using the find command, As the user is bandit7 and the group is bandit6 and size is 33 bytes:

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c
find: '/sys/kernel/tracing': Permission denied
```

So here we got the password file:

```
find: '/root': Permission denied
find: '/tmp': Permission denied
find: '/lost+found': Permission denied
find: '/dev/shm': Permission denied
find: '/dev/mqueue': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/lib/udisks2': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/lib/snapd/void': Permission denied
find: '/var/lib/snapd/cookie': Permission denied
find: '/var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/private': Permission denied
find: '/var/lib/update-notifier/package-data-downloads/partial': Permission denied
```

Now by using simply the cat command we can access bandit7:

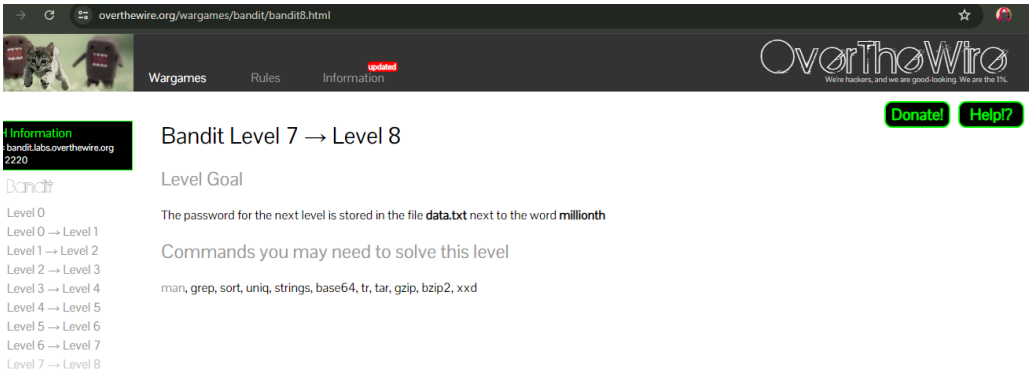
```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:~$
```

After entering the password we are in bandit7 shell:

```
  Enjoy your stay!

bandit7@bandit:~$
```

Level 7-8:



Here we are given the hint that password is in the file named **data.txt** and is written next to the word **millionth**. So it means we have to find the word **millionth**, for this purpose we will use the `grep` command.

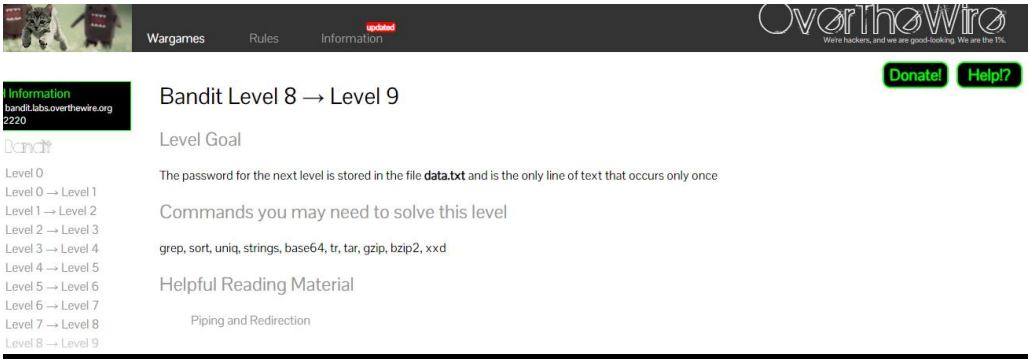
```
bandit7@bandit:~$ cat data.txt | grep millionth
millionth       dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$
```

And yes!! Here is the password for bandit 8. Now after entering the password using ssh command we are in bandit8 shell:

```
  Enjoy your stay!

bandit8@bandit:~$
```

Level 8-9:



Here we are hinted that the password is in file named **data.txt** but the solid hint is that the file contains many repetitive statements and the password is only unique statement which does not repeat, so we will use `sort` and `uniqu` command to sort out the password.

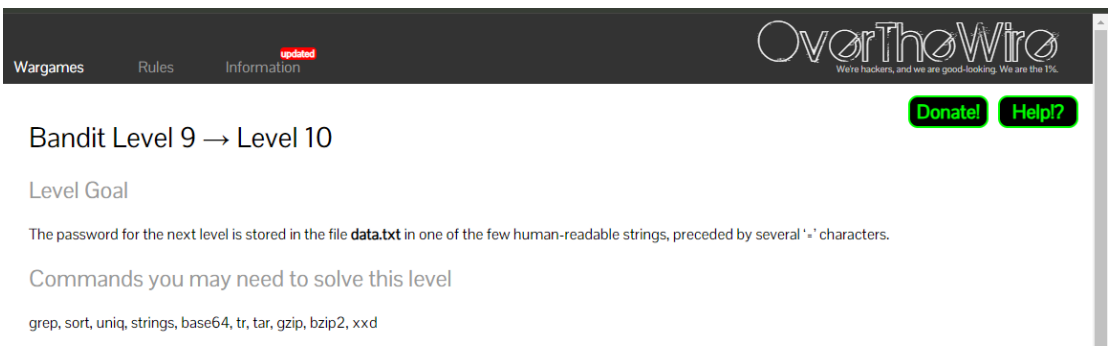
```
bandit8@bandit:~$ cat data.txt | sort | uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:~$
```

And yes here is the password for bandit9, so we can now access the bandit9 shell:

```
  Enjoy your stay!

bandit9@bandit:~$
```

Level 9-10:



So here we again the password is in **data.txt** but this time we are given the hint that password is preceded by several = characters.

So again I am using the **grep** command here:

```
bandit9@bandit:~$ strings data.txt | grep =
=aA"f
\a!;========== the
PWAF=1
         M),\}=
2Y6=
G';?e=
========== passwordf
========== isc
*=N6
m=</
E=Bty
=sw
"M1=
========== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
!&=u&4$
*XA=
bandit9@bandit:~$
```

Harrum Fatima

Now we have the password so we can login to level 10 using ssh:

```
  Enjoy your stay!

bandit10@bandit:~$
```

And yes!!!! Here we are in bandit10 shell.