

# OverTheWire – Bandit Walkthrough (1-10)

**Wasiq Abbasi-24109122**

## Level 0

This is a simple level. It teaches us to connect to a host using SSH. This is going to teach players the usage of SSH command.

We got the required information from reading the instruction page.

**Host:** bandit.labs.overthewire.org

**Port:** 2220

**Username:** bandit0

**Password:** bandit0

We used the above information to login using ssh as shown in the given image.

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

This level doesn't require anything else other than logging in. Time to move in on the next level.

## Level 0-1

Now, from the bandit0 shell, we need to find the password for logging as the next user. To find that password, we are going to list files in the directory. Our target is to find a file named readme. After finding that file, we need to read the password stored inside that file.

We use the ls command to list the files in the current directory. We found the readme file. Now to read the password we will use the cat command. After that, we are going to use the password to login into next level using SSH

```
ls -la
cat readme
ssh bandit1@localhost
```

# OverTheWire – Bandit Walkthrough (1-10)

**Wasiq Abbasi-24109122**

```
root@kali:~# ssh bandit0@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password:
Linux bandit 4.18.12 x86_64 GNU/Linux
```

```
www. ver he ire.org
```

```
Welcome to OverTheWire!
```

## Level 1-2

We are informed that the password for the next level is stored inside a file named `-(hyphen)`. So, to find it we use the `ls` command. Now comes the part where we have to read the file. 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 `./`, This will help us to read the password stored as shown in the given figure. Since we found the password for the user `bandit2`. We will use it to get an SSH connection as `bandit2`.

```
ls
cat ./-
ssh bandit2@localhost
```

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
CV1DtqXwVFXTvM2F0k09SHZ0YwRINYA9
bandit1@bandit:~$ ssh bandit2@localhost
Could not create directory '/home/bandit1/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit1/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit2@localhost's password:
Linux bandit 4.18.12 x86_64 GNU/Linux
```

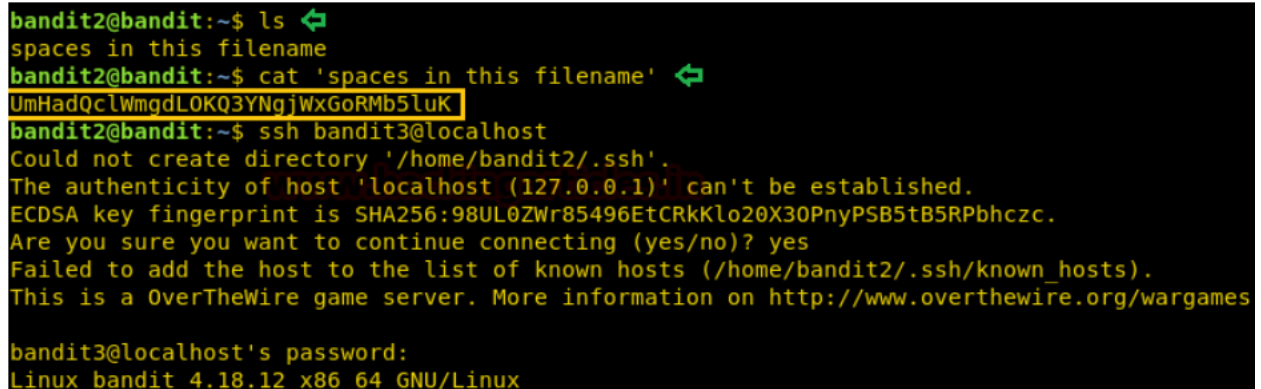
# OverTheWire – Bandit Walkthrough (1-10)

**Wasiq Abbasi-24109122**

## Level 2-3

We are informed 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 comes the part where 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. As cat command reads files name only until space as it considers space as null '/0'. If we directly use cat command, it won't be able to find the file. So, we will write the name of the file in quotes, this will help us to read the password stored as shown in the given figure. Since we found the password for the user bandit3. We will use it to get an SSH connection as bandit3.

```
ls  
  
cat 'spaces in this filename'  
  
ssh bandit3@localhost
```



A terminal window showing the following commands and output:

```
bandit2@bandit:~$ ls  
spaces in this filename  
bandit2@bandit:~$ cat 'spaces in this filename'  
UmHadQclWmgdLOKQ3YNgjWxGoRmb5lUK  
bandit2@bandit:~$ ssh bandit3@localhost  
Could not create directory '/home/bandit2/.ssh'.  
The authenticity of host 'localhost (127.0.0.1)' can't be established.  
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.  
Are you sure you want to continue connecting (yes/no)? yes  
Failed to add the host to the list of known hosts (/home/bandit2/.ssh/known_hosts).  
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames  
  
bandit3@localhost's password:  
Linux bandit 4.18.12 x86_64 GNU/Linux
```

## Level 3-4

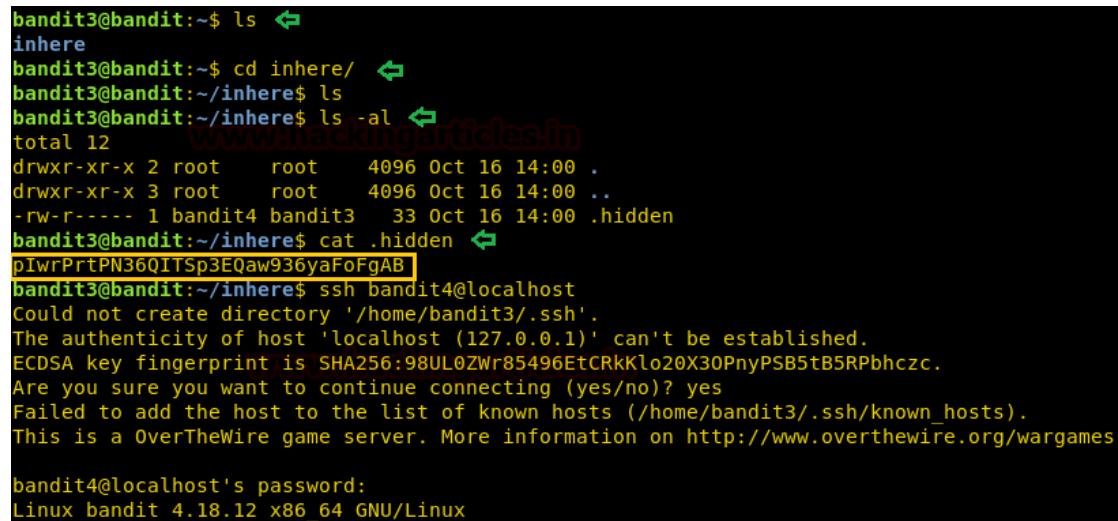
We are informed that the password for the next level is stored inside a directory named inhere. So, to find it we use the ls command. Now, after traversing inside inhere directory we run ls command again. Now it might be the case that the file is hidden. So, we run ls command with -al parameter. It lists all files including the hidden one. And we found the .hidden file. In Linux, the file with a dot(.) in front of the name of the file makes it hidden. Now we would simply use the cat command to read the password stored in the file. Since we found the password for the user bandit4. We will use it to get an SSH connection as bandit4.

```
ls  
  
cd inhere/
```

# OverTheWire – Bandit Walkthrough (1-10)

**Wasiq Abbasi-24109122**

```
ls
ls -al
cat .hidden
ssh bandit4@localhost
```

A terminal window showing the progression from bandit3 to bandit4. The user runs 'ls' in the '~' directory, then 'cd inhere/' to move into the 'inhere' directory. They run 'ls' and 'ls -al' to list files, revealing a file named '.hidden'. They use 'cat .hidden' to view the password 'pIwrPrTpN36QITSp3EQaw936yaFoFgAB'. Finally, they attempt an SSH connection to 'bandit4@localhost', which fails due to an authenticity issue, but they proceed by entering the password.

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root root 4096 Oct 16 14:00 .
drwxr-xr-x 3 root root 4096 Oct 16 14:00 ..
-rw-r----- 1 bandit4 bandit3 33 Oct 16 14:00 .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrTpN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$ ssh bandit4@localhost
Could not create directory '/home/bandit3/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit3/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit4@localhost's password:
Linux bandit 4.18.12 x86_64 GNU/Linux
```

## Level 4-5

We are informed that the password for the next level is stored inside a human-readable file. So, to find it we use the `ls` command. Now, after traversing inside `inhere` directory we run `ls` command again. This gives us a bunch of files as shown in the image. We will use the `file` command to get the information about the files. From `file` command, we now know that the `file07` contains ASCII text. It is mostly readable text. So, let's read it using `cat` command. This gives us the password for the next level. We will use it to get an SSH connection as `bandit5`.

```
ls -la
cd inhere/
ls
file ./*
cat ./-file07
ssh bandit5@localhost
```

# OverTheWire – Bandit Walkthrough (1-10)

Wasiq Abbasi-24109122

```
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$ file ./-file07
./-file07: ASCII text
bandit4@bandit:~/inhere$ cat ./-file07
koReB0KuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$ ssh bandit5@localhost
Could not create directory '/home/bandit4/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit4/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit5@localhost's password:
Linux bandit 4.18.12 x86_64 GNU/Linux
```

## Level 5-6

We are informed that the password for the next level is stored inside a directory named inhere. So, to find it we use the ls command. Now, after traversing inside inhere directory we run ls command again. This gives us a bunch of files as shown in the image. We will use the file size to find the file. Find command has the parameter of size in which we have to use 'c' for depicting size in bytes. From find command, we now know that the file2 contains the password. So, let's read it using cat command. This gives us the password for the next level. We will use it to get an SSH connection as bandit6.

```
ls
cd inhere/
ls
find . -size 1033c
cat ./maybehere07/.file2
ssh bandit6@localhost
```

# OverTheWire – Bandit Walkthrough (1-10)

Wasiq Abbasi-24109122

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ ls
maybehere00 maybehere02 maybehere04 maybehere06 maybehere08 maybehere10 maybehere12
maybehere01 maybehere03 maybehere05 maybehere07 maybehere09 maybehere11 maybehere13
bandit5@bandit:~/inhere$ find . -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
bandit5@bandit:~/inhere$ ssh bandit6@localhost
Could not create directory '/home/bandit5/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit5/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit6@localhost's password:
Linux bandit 4.18.12 x86_64 GNU/Linux
```

## Level 6-7

We are informed that the password for the next level is stored somewhere on the server. So, finding the file over the server would be a lot trickier if we are using ls. So, we will try to widen our scope of search using the find command. We are hinted that the user of the file is bandit7 and it is a part of group bandit 6. We will add this information as parameters in the find command. We are given the size too. Let's add that too. Now as we can see in the given image, we successfully located the password file hidden over the server.

```
find / -user bandit7 -group bandit6 -size 33c
```

# OverTheWire – Bandit Walkthrough (1-10)

Wasiq Abbasi-24109122

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c
find: '/run/lvm': Permission denied
find: '/run/screen/S-bandit31': Permission denied
find: '/run/screen/S-bandit30': Permission denied
find: '/run/screen/S-bandit25': Permission denied
find: '/run/screen/S-bandit0': Permission denied
find: '/run/screen/S-bandit14': Permission denied
find: '/run/screen/S-bandit4': Permission denied
find: '/run/screen/S-bandit2': Permission denied
find: '/run/screen/S-bandit24': Permission denied
find: '/run/screen/S-bandit23': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/shm': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/log': Permission denied
find: '/var/tmp': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/polkit-1': Permission denied
find: '/cgroup2/csessions': Permission denied
find: '/home/bandit28-git': Permission denied
```

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

```
ssh bandit7@localhost
```

From find command, we now know that the bandit7.password contains the credentials. So, let's read it using cat command. This gives us the password for the next level. We will use it to get an SSH connection as bandit7.

```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$ ssh bandit7@localhost
Could not create directory '/home/bandit6/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit6/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit7@localhost's password:
Linux bandit 4.18.12 x86_64 GNU/Linux
```

# OverTheWire – Bandit Walkthrough (1-10)

**Wasiq Abbasi-24109122**

## Level 7-8

We are informed that the password for the next level is stored inside a file named data.txt. So, to find it we use the ls command. Now we are hinted that the password is written next to the word millionth in the data.txt file. This means if we find the millionth word, we find the password. We are going to use the grep command for finding millionth. Here we use the (|) Unix pipe. The Pipe connects the standard output from the first command and feeds it as standard input to the second command. In our case, first cat command reads the file and then the data inside the file is sent to grep command to work on. This gives us the password for the next level. We will use it to get an SSH connection as bandit8.

```
ls

cat data.txt | grep millionth

ssh bandit8@localhost
```

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ cat data.txt | grep millionth ↩
millionth      cvX2JJJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$ ssh bandit8@localhost
Could not create directory '/home/bandit7/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit7/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit8@localhost's password:
Linux bandit 4.18.12 x86_64 GNU/Linux
```

## Level 8-9

We are informed that the password for the next level is stored inside a file named data.txt. It is hinted that the password is the only line of text that occurs only once. Here we are going to use sort command to sort the text inside the data.txt file. But still, the file contains a lot of repeating statements so we will use the uniq command to print the not repeating statement. We are using multiple pipes here to get a filtered result. This gives us the password for the next level. We will use it to get an SSH connection as bandit9.

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



# OverTheWire – Bandit Walkthrough (1-10)

## Wasiq Abbasi-24109122

```
ssh bandit9@localhost
```

```
bandit8@bandit:~$ cat data.txt | sort | uniq -u ↵
UsvVyFSfZZWb16wgC7dAFyFuR6jQQUhR
bandit8@bandit:~$ ssh bandit9@localhost
Could not create directory '/home/bandit8/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit8/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit9@localhost's password:
Linux bandit 4.18.12 x86_64 GNU/Linux
```

## Level 9-10

We are informed that the password for the next level is stored inside a file named data.txt. We are hinted that the password is followed by several '=' characters. Now if we are to use the cat command our screen would be filled with unreadable mesh. So, to get a more refined approach we are going to use strings command which prints character sequences that are at least 4 characters long. And to get to the exact location of the password, we are going to use grep. This gives us the password for the next level. We will use it to get an SSH connection as bandit10.

```
ls

strings data.txt | grep =

ssh bandit10@localhost
```

# OverTheWire – Bandit Walkthrough (1-10)

Wasiq Abbasi-24109122

```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt | grep =
2===== the
===== password
>t=
rV~dHm=
===== isa
=FQ?P\U
=      F[
pb=x
J;m=
=)$=
===== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
iv8!=
bandit9@bandit:~$ ssh bandit10@localhost
Could not create directory '/home/bandit9/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit9/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit10@localhost's password:
Linux bandit 4.18.12 x86_64 GNU/Linux
```