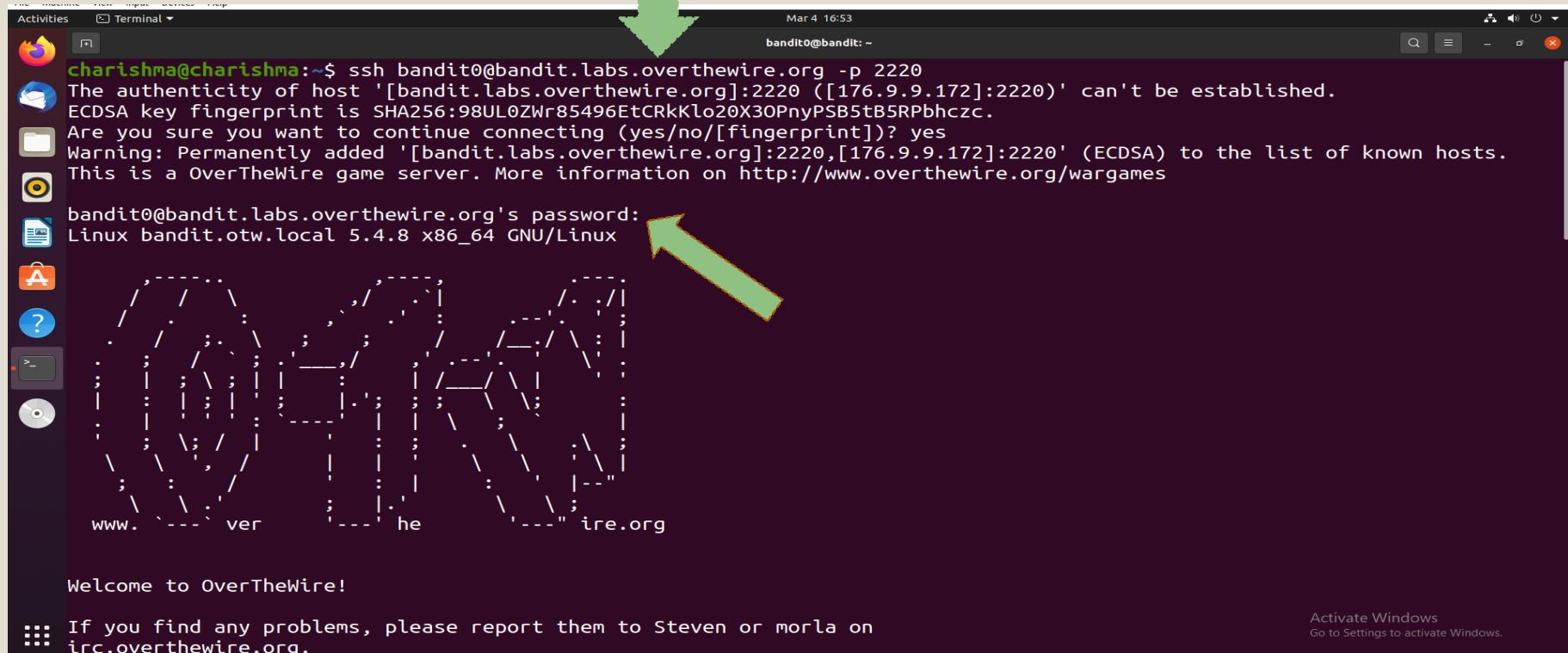


# TASK-7

**CHARISHMA LOTTI  
U4CYS21010**

# LEVEL - 0



```
charisma@charisma:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([176.9.9.172]:2220)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[176.9.9.172]:2220' (ECDSA) to the list of known hosts.
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

      ,-' . \ ; : , / . ' . ' / . / \ ; ;
     / . ; \ ; : , / . ' . ' / . / \ ; ;
    . ; \ ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
   ; : | ; | ; ; ; ; ; ; ; ; ; ; ; ; ;
  ; : \ ; / | ; ; ; ; ; ; ; ; ; ; ; ;
 / \ ; : / | ; ; ; ; ; ; ; ; ; ; ; ;
; \ ; : / | ; ; ; ; ; ; ; ; ; ; ; ;
 www. --- ver     ; --- he     ' --- ire.org

Welcome to OverTheWire!

If you find any problems, please report them to Steven or morla on
irc.overthewire.org.
```

**COMMAND USED : ssh bandit0@bandit.labs.overthewire.org -p 2220**

Using the given information , logged into the game using SSH

**HOST : bandit.labs.overthewire.org**

**PORT : 2220**

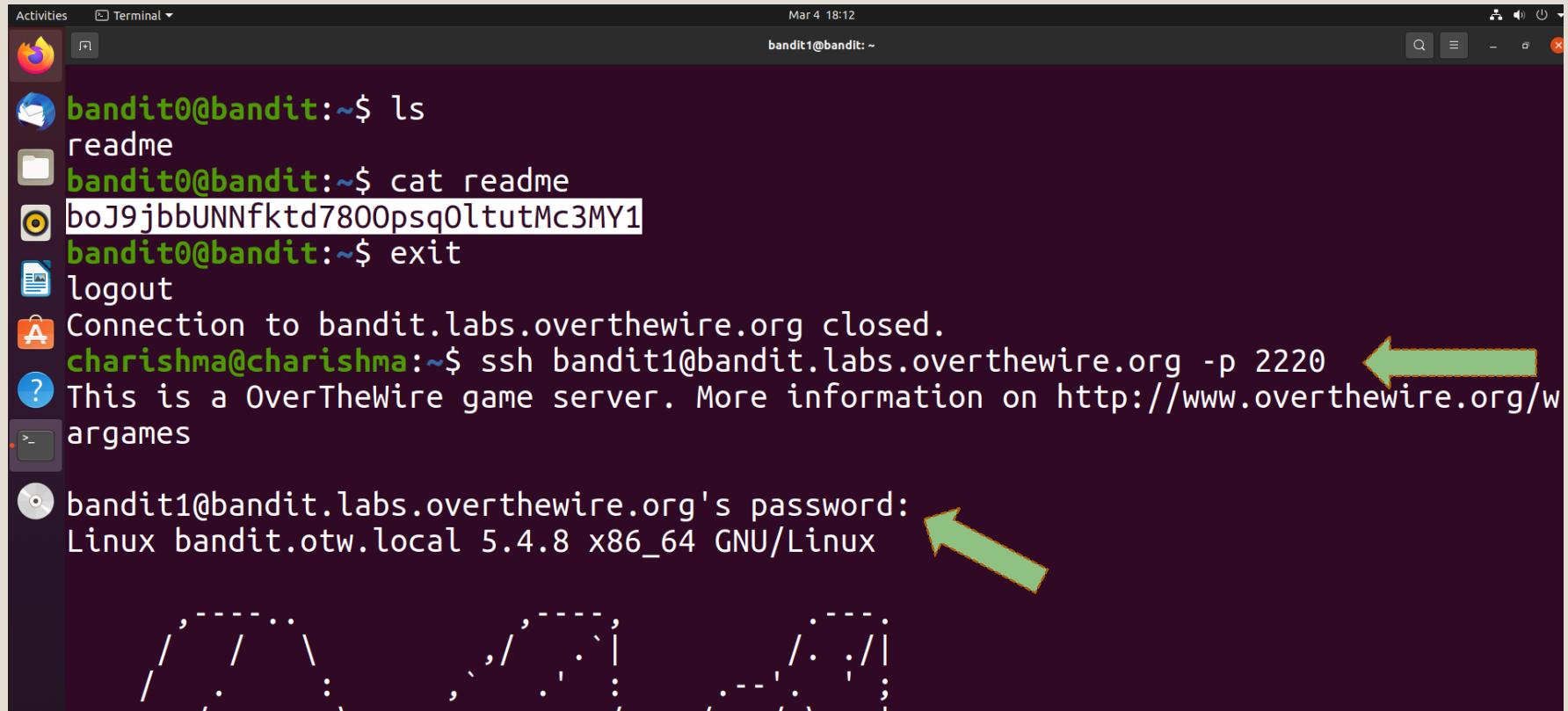
**USERNAME : bandit0**

**PASSWORD : bandit0**

# LEVEL - 0 → LEVEL-1

```
Activities Terminal Mar 4 18:12
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd780Opsq0ltutMc3MY1
bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
charishma@charishma:~$ ssh bandit1@bandit.labs.overthewire.org -p 2220
? This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit1@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
/ ,---.. \ . : , / ' .` | . . / : . / ;
```



**PASSWORD : boJ9jbbUNNfktd780Opsq0ltutMc3MY1**

Found the password in “readme” file . Now logged into bandit1 using the password found

## LEVEL – 1 → LEVEL-2

The screenshot shows a terminal window titled "Terminal" with the command "ls" run by user "bandit1". It lists a file named "-". The contents of this file are displayed using the command "cat ./-", revealing the password: "CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9". The user then exits the session with "exit". The terminal then connects to another host, "charishma@charishma", via SSH. The password for this connection is also "CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9". The terminal interface includes a dock with various icons like Firefox, Mail, and Files, and a status bar at the bottom right indicating "Activate Windows Go to Settings to activate Windows".

```
Activities Terminal Mar 4 18:22
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
charishma@charishma:~$ ssh bandit2@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/w
argames
bandit2@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

. / , - - - .. \ , , / ' . ' | , , , / : . / |
. / . ; . \ ; ; ; , . ' | , , / . - - . / \ ; ; ;
; ; ; \ ; ; ; i - - : , , / _ _ / \ | ; ; ;
```

**PASSWORD : CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9**

**The password is in the file “ – ” . Logged into bandit2 using the password found.**

## LEVEL – 2 → LEVEL-3

The screenshot shows a terminal window with the following session:

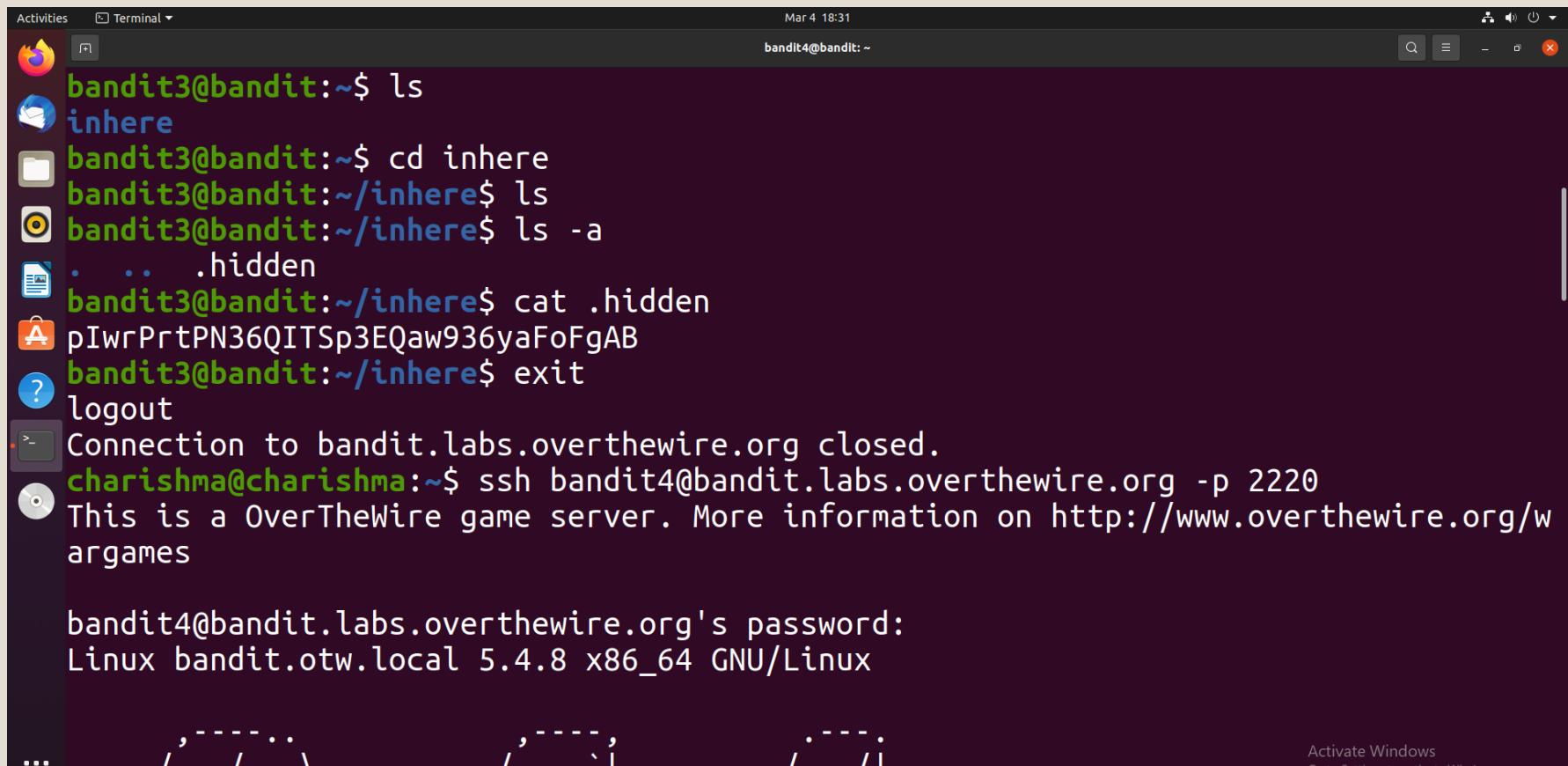
```
Activities Terminal Mar 4 18:26
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
charishma@charishma:~$ ssh bandit3@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/w
argames
bandit3@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

Below the terminal window, there is a decorative ASCII art of a tree made of punctuation marks (/, ., ;, :). On the right side of the terminal window, there is a message: "Activate Windows Go to Settings to activate Windows".

**PASSWORD : UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK**

Found the password in the file “ spaces in the file name ” . We use ‘\’ when there are spaces in filename . Logged into bandit3 using the password found .

## LEVEL – 3 → LEVEL-4



Activities Terminal Mar 4 18:31 bandit4@bandit: ~

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
. . . .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
charishma@charishma:~$ ssh bandit4@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit4@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

Activate Windows  
Go to Settings to activate Windows

**PASSWORD : pIwrPrtPN36QITSp3EQaw936yaFoFgAB**

**Password is in the hidden file [.]hidden] located in the directory : “inhere”**

# LEVEL – 4 → LEVEL-5

```
Activities Terminal Mar 4 19:16
bandit4@bandit:~/inhere
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00  -file02  -file04  -file06  -file08
-file01  -file03  -file05  -file07  -file09
bandit4@bandit:~/inhere$ find . -type f | xargs file
A ./-file01: data
? ./-file00: data
./-file06: data
./-file03: data
./-file05: data
./-file08: data
./-file04: data
./-file07: ASCII text
./-file02: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

Activate Windows  
Go to Settings to activate Windows.

**PASSWORD : koReBOKuIDDepwhWk7jZC0RTdopnAYKh**

Using the hint : human readable file : -file07 has ASCII text . So we can directly open -file07 . No need to search all the files .

Activities Terminal Mar 4 19:20 bandit5@bandit: ~

```
charisma@charisma:~$ ssh bandit5@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/w
argames

bandit5@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux


```

Activate Windows  
Go to Settings to activate Windows

Logged into bandit5 using the password found in -file07

## LEVEL – 5 → LEVEL - 6

The screenshot shows a terminal window titled "Terminal" with the command line "bandit5@bandit:~\$". The user is in a directory named "inhere". They run "ls" to see files: maybehere00, maybehere04, maybehere08, maybehere12, maybehere16, maybehere01, maybehere05, maybehere09, maybehere13, maybehere17, maybehere02, maybehere06, maybehere10, maybehere14, maybehere18, maybehere03, maybehere07, maybehere11, maybehere15, maybehere19. Then they run "find . -type f -size 1033c ! -executable ./maybehere07/.file2". Finally, they run "cat ./maybehere07/.file2" which outputs the password: DXjZPULLxYr17uwoI01bNLQbtFemEgo7.

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere04  maybehere08  maybehere12  maybehere16
maybehere01  maybehere05  maybehere09  maybehere13  maybehere17
maybehere02  maybehere06  maybehere10  maybehere14  maybehere18
maybehere03  maybehere07  maybehere11  maybehere15  maybehere19
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

PASSWORD : **DXjZPULLxYr17uwoI01bNLQbtFemEgo7**

Using the given data and “find” command , got the directory maybehere07 and found password in it

Activities Terminal ▾

Mar 4 19:28

☰ 🔍 ⌂ ⌂ X

bandit6@bandit: ~

```
charishma@charishma:~$ ssh bandit6@bandit.labs.overthewire.org -p 2220
```

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

```
bandit6@bandit.labs.overthewire.org's password:  
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

```
,---.. ,---, .-. /|  
/ \ ; : ,` .': ; / \ ; |  
. / ; \ ; ; ; / \ ; |  
; / ; \ ; ; ; / \ ; |  
; / ; \ ; ; ; / \ ; |  
; / ; \ ; ; ; / \ ; |  
; / ; \ ; ; ; / \ ; |  
; / ; \ ; ; ; / \ ; |
```

Logged into bandit6 using the password found

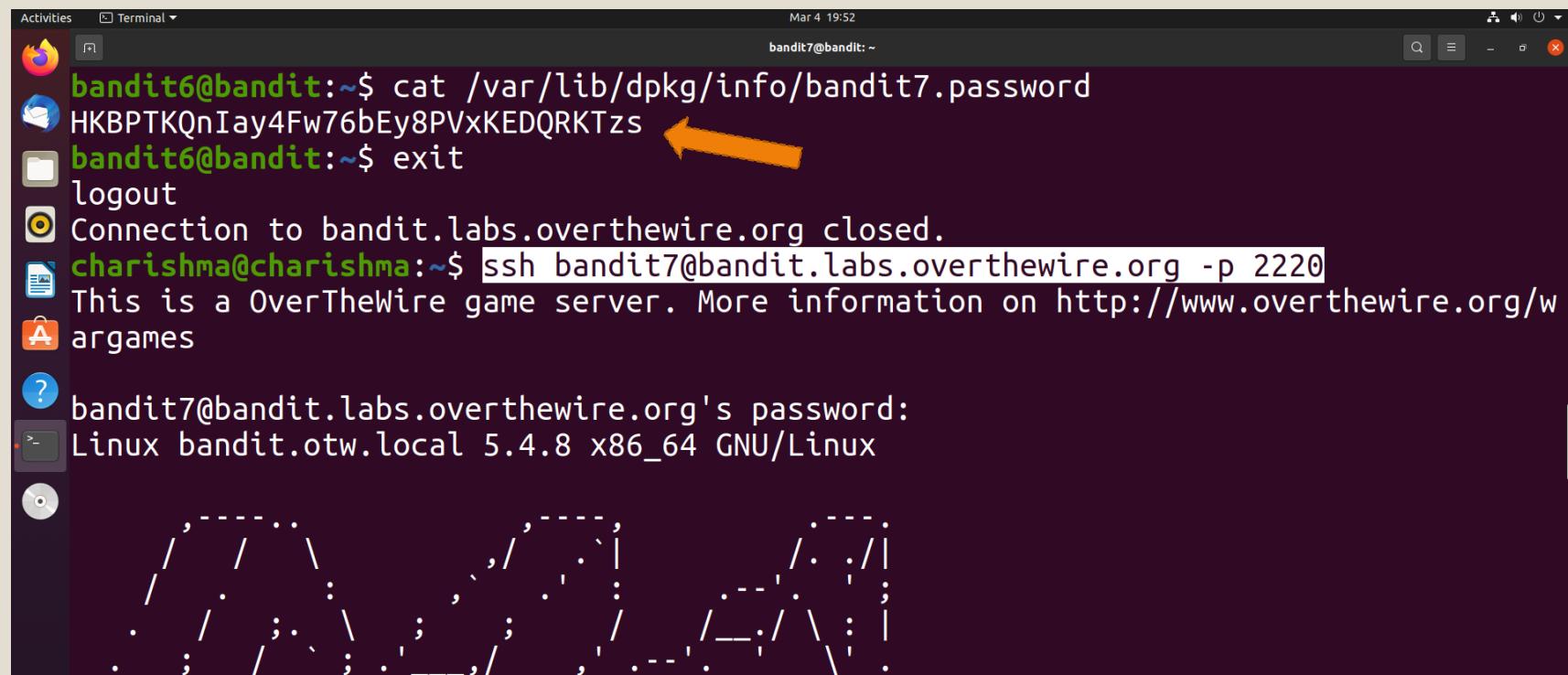
# LEVEL – 6 → LEVEL-7

```
Activities Terminal Mar 4 19:48
bandit6@bandit:~$ ls
bandit6@bandit:~$ find / -type f -size 33c -user bandit7 -group bandit6
find: '/root': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/home/bandit29-git': Permission denied
find: '/home/bandit31-git': Permission denied
find: '/lost+found': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/lvm/archive': Permission denied
find: '/etc/lvm/backup': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/14595/task/14595/fdinfo/6': No such file or directory
find: '/proc/14595/fdinfo/5': No such file or directory
find: '/cgroup2/csessions': Permission denied
find: '/boot/lost+found': Permission denied
find: '/tmp': Permission denied
```

Owned by user bandit7  
Owned by group bandit6  
33 bytes in size

} Using the given details found the file containing password

```
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/polkit-1': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/log': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/ldconfig': Permission denied
bandit6@bandit:~$
```



A screenshot of a Linux desktop environment showing a terminal window. The terminal window title is "Activities Terminal" and the status bar shows "Mar 4 19:52". The terminal content is as follows:

```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
charishma@charishma:~$ ssh bandit7@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/w
argames
? bandit7@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

An orange arrow points from the terminal window to the password "HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs" which is displayed in a dashed box at the bottom of the terminal window.

PASSWORD : HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

## LEVEL – 7 → LEVEL-8

The screenshot shows a terminal window with the following session:

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ cat data.txt | grep millionth
millionth      cvX2JJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
charishma@charishma:~$ ssh bandit8@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/w
argames

bandit8@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

[REDACTED]
```

At the bottom right of the terminal window, there is a watermark that says "Activate Windows" and "Go to Settings to activate Windows".

**PASSWORD : cvX2JJa4CFALtqS87jk27qwqGhBM9plV**

Given : password is beside the word “millionth” . Found the password using “grep” command

## LEVEL – 8 → LEVEL-9

```
Activities Terminal Mar 4 20:38
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ sort data.txt | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
bandit8@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
charishma@charishma:~$ ssh bandit9@bandit.labs.overthewire.org -p 2220
kex_exchange_identification: Connection closed by remote host
charishma@charishma:~$ ssh bandit9@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/w
argames

bandit9@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

. / ,---.. \ , / .-' | / . . / |
. / ;. \ ; ; / /_. / \ : |
```

Activate Windows  
Go to Settings to activate Windows.

**PASSWORD : UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR**

The line containing password occurs only once : sort and uniq commands are used to find the password

# LEVEL – 9 → LEVEL-10

The screenshot shows a terminal window with the following session:

```
Activities Terminal Mar 4 21:20
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt | grep "="
===== the*2i"4
=:G e
===== password
<I=zsGi
Z)===== is
A=|t&E
Zdb=
?
c^ LAh=3G
*SF=s
&===== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.H&^
bandit9@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
charishma@charishma:~$ ssh bandit10@bandit.labs.overthewire.org -p 2220
kex_exchange_identification: Connection closed by remote host
charishma@charishma:~$ ssh bandit10@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit10@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

In the terminal, the user is on bandit9 and runs `ls` to find `data.txt`. They then use the `strings` command to extract all strings from the file, specifically filtering for the character '='. This reveals several strings, including a password entry. The password is highlighted in a dashed box.

Activate Windows  
Go to Settings to activate Windows.

**PASSWORD : truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk**

GIVEN : line containing password has many “=” symbols . Using “grep” command found the lines containing “=” and found the password

# LEVEL – 10 → LEVEL-11

The screenshot shows a terminal window on a Linux desktop environment. The terminal history is as follows:

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSG==
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
charishma@charishma:~$ ssh bandit11@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit11@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit11@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

Below the terminal window, there is a decorative ASCII art logo consisting of various punctuation marks like slashes, dots, and colons arranged in a grid-like pattern.

Activate Windows  
Go to Settings to activate Windows.

**PASSWORD : IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR**

The file has base64 encoded data . Found the password by decoding it .

## LEVEL - 11 → LEVEL-12

The terminal window shows the following session:

```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh
bandit11@bandit:~$ cat data.txt | tr 'N-ZA-Mn-za-m' 'A-Za-z'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
bandit11@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
charishma@charishma:~$ ssh bandit12@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit12@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

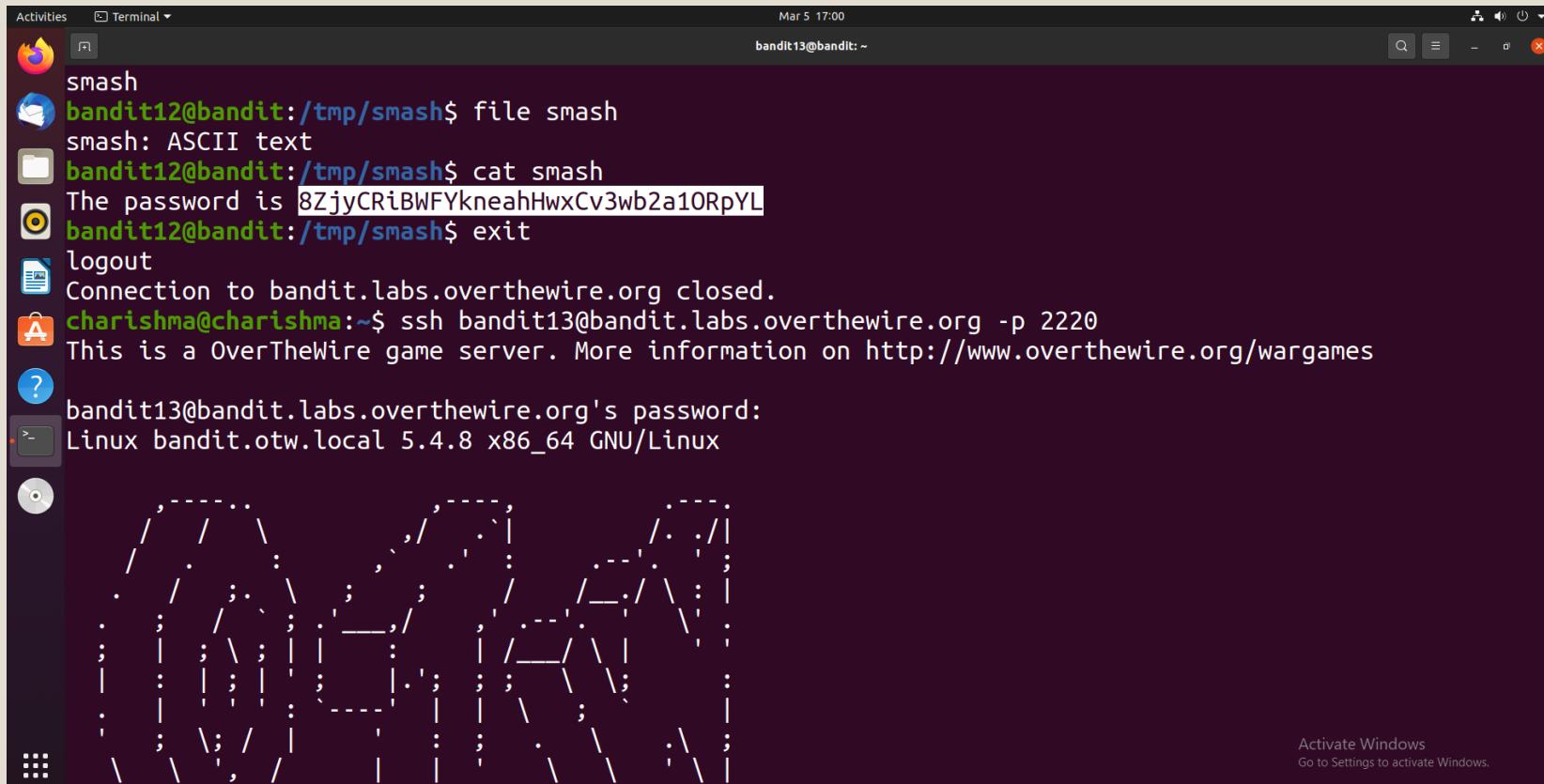
Below the terminal window, there is a decorative ASCII art logo consisting of various punctuation marks (., ;, /, \, |) arranged in a grid-like pattern.

Activate Windows  
Go to Settings to activate Windows.

PASSWORD : **5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu**

Here the letters have been rotated by 13 positions . So decrypted the msg and found the password

# LEVEL – 12 → LEVEL-13



The screenshot shows a terminal window on a Linux desktop environment. The terminal window title is "Terminal" and the status bar indicates it's Mar 5 17:00 and the user is "bandit13@bandit: ~". The terminal content is as follows:

```
Activities Terminal ▾ Mar 5 17:00
bandit12@bandit:/tmp/smash$ file smash
smash: ASCII text
bandit12@bandit:/tmp/smash$ cat smash
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/smash$ exit
logout
Connection to bandit.labs.overthewire.org closed.
charishma@charishma:~$ ssh bandit13@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit13@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

[REDACTED]
```

The password "8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL" is highlighted in red and enclosed in a dashed border.

The file is repeatedly compressed .

**Procedure :** Identifying the file type using “file” command and proceeding with the suitable command .

# LEVEL – 13 → LEVEL-14

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window has a dark background and light-colored text. It displays the following session:

```
Activities Terminal Mar 5 19:08
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
Could not create directory '/home/bandit13/.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/bandit13/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

Below the terminal window, there is a decorative ASCII art representation of a person's head and shoulders, composed of various punctuation marks like commas, periods, and colons.

On the right side of the terminal window, there is a watermark-like message: "Activate Windows Go to Settings to activate Windows."

Logged into bandit14 using the private SSH key

# LEVEL – 14 → LEVEL-15

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Terminal". The date and time at the top right are "Mar 5 19:26". The user is currently logged in as "bandit14" at the prompt "bandit14@bandit:~". The terminal displays the following session:

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr

bandit14@bandit:~$ ssh bandit15@localhost
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/bandit14/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit15@localhost's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

[REDACTED]
```

In the bottom right corner of the terminal window, there is a watermark that says "Activate Windows Go to Settings to activate Windows."

PASSWORD : BfMYroe26WYalil77FoDi9qh59eK5xNr

Submitted the password of current level to PORT 30000 on localhost. Logged into bandit15 Using the password found .

# LEVEL - 15 → LEVEL-16

```
Activities Terminal Mar 5 19:55
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
depth=0 CN = localhost
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = localhost
verify return:1
---
Certificate chain
  0 s:/CN=localhost
    i:/CN=localhost
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICBjCCAw+gAwIBAgIEZOzuVDANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDDA1s
b2NhbGhvc3QwHhcNMjEwOTMwMDQ0NTU0WhcNMjIwOTMwMDQ0NTU0WjAUMRIwEAYD
VQQDDA1sb2NhbGhvc3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJaoGBAM9En7CC
uPr6cVPATLAvhWMU1hggyFIJEp5sZN9RPUbK0zKBv802yD540bHYmIge6lqqkgX0z
2AuI4UFCG4iMb0UYUCA/wISwNQuQrjcja0OnqzCTRscXzzoIsHbC8LGfzMDRz3Jw
8nBD6/2jvFt1rnBtz4ghibNn5rFHRi5EC+k/AgMBAAGjZTBjMBQGA1UdEQQNMAuC
CWxvY2FsaG9zdDBLBglhgkBhvhCAQ0EPHY8QXV0b21hdGljYWxseSBnZW5lcmF0
ZWQgYnkgtmNhdc4gU2VLIGH0dHBz0i8vb1hcC5vcmcvbmNhdc8uMA0GCSqGSIb3
DQEBBQUAA4GBAD7/moj14DUi6/D6imJ8pQ1Ay/8lzlrbryRnqpzjWaATShDYr7k3
umdg+36McINFAglE7nGYZroTSDCm650D81+797owSXLPAdp1Q6JfQH5LOni2kbw
-----END CERTIFICATE-----
```

```
Start Time: 1646490294
Timeout   : 7200 (sec)
Verify return code: 18 (self signed certificate)
Extended master secret: yes
---
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd

closed
bandit15@bandit:~$
```

PASSWORD : cluFn7wTiGryunymYOu4RcffSxQluehd

Submitted the current level password to PORT 30001 . Found the password  
For next level