

OVER THE WIRE

BANDIT

SOLUTIONS

LEVELS UPTO 15



CONTRIBUTED BY
SIDHARTH KRISHNA

INTRODUCTION

Over The Wire is a platform to develop basics of security concepts using games as a medium. It has various wargames and their internal levels are designed in terms of increasing difficulty for each level to pass on.

Wargames include:

1. Bandit
2. Natas
3. Leviathan
4. Krypton
5. Narnia
6. Behemoth
7. Utumno
8. Maze
9. Vortex
10. Manpage

Each wargame specializes in teaching a particular security concept. We will solve each and every wargame including it's internal levels and cover important concepts if necessary.

This document covers all the commands used to complete levels upto 15 and their respective explanations.

BANDIT – LEVEL(1-15)

1. Level 0

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.

```
sid@sid-HP-Laptop-14s-dy2xxx:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
bandit0@bandit.labs.overthewire.org:~$

  _ _ _ _ _
 | b | a | n | d | i | t |
 | _ | _ | _ | _ | _ |
 | b | a | n | d | i | t |
 | _ | _ | _ | _ | _ |
 | b | a | n | d | i | t |
 | _ | _ | _ | _ | _ |

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

bandit0@bandit.labs.overthewire.org's password:
```

```
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbini
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IR

Enjoy your stay!

bandit0@bandit:~$
```

Password: bandit0

2. Level 0 – Level 1

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.

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNWOZ0Ta6ip5If

bandit0@bandit:~$
```

Password: ZjLjTmM6FvvyRnrb2rfNWOZ0Ta6ip5If

Command: cat readme

Explanation: cat displays the contents of the file, readme revealing the password.

3. Level 1 – Level 2

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

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat < -
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$
```

Password: 263JGJPfgU6LtdEvfgWU1XP5yac29mFx

Command: cat ./-

Explanation: The ./ specifies the current directory and helps interpret - as a file, not an option for cat.

3. Level 2 – Level 3

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

```
sid@sid-HP-Laptop-14s-dy2xxx:~$ ssh bandit2@bandit.labs.overthewire.org -p 2220
```

ENCORE

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

```
bandit2@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit2@bandit.labs.overthewire.org's password:
```



```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
MNk8KNH3Usiio41PRUEoDFPqfxLPLSmx
bandit2@bandit:~$
```

Password: MNk8KNH3Usiio41PRUEoDFPqfxLPISmx

Command: cat "spaces in this filename"

Explanation: Quotes handle filenames with spaces.

4. Level 3 – Level 4

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

```
sid@sid-HP-Laptop-14s-dy2xxx:~$ ssh bandit3@bandit.labs.overthewire.org -p 2220
```

LOGICAL

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

bandit3@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

Password: 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

Command: `ls -a cat .hidden`

Explanation: `ls -a` lists all files, including hidden ones. `cat` displays the contents of `.hidden`.

5. Level 4 – Level 5

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.

```
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$ find . |xargs file {} \; |grep "ASCII text"
./-file07: ASCII text
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
bandit4@bandit:~/inhere$
```

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ find ./inhere/ -size 1033c ! -executable -exec file {} + | grep -i "text"
./inhere/maybeh ere07/.file2: ASCII text, with very long lines (1000)
bandit5@bandit:~$
```

Password: 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

Command: ls -l inhere/ cat inhere/<filename>

Explanation: ls -l lists file permissions. Identify the readable file and use cat to read it.

6. Level 5 – Level 6

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

```
sid@sid-HP-Laptop-14s-dy2xxx:~$ ssh bandit5@bandit.labs.overthewire.org -p 2220
```

```

  _ _ _ _ _
 | B | A | N | D | I | T |
 | _ | _ | _ | _ | _ |

```

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

bandit5@bandit.labs.overthewire.org's password:

```

  _ _ _ _ _
 | O | V | E | R |
 | _ | _ | _ | _ |
 | T | H | E | W |
 | _ | _ | _ | _ |
 | I | R | E |
 | _ | _ | _ | _ |
 | . | . | . | . |
 | _ | _ | _ | _ |
 | W | W | W | . |
 | _ | _ | _ | _ |
 | v | e | r |
 | _ | _ | _ | _ |
 | h | e |
 | _ | _ | _ | _ |
 | . | . | . | . |
 | _ | _ | _ | _ |
 | i | r | e | . |
 | _ | _ | _ | _ |
 | o | r | g |
 | _ | _ | _ | _ |

```

Welcome to OverTheWire!


```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ find ./inhere/ -size 1033c ! -executable -exec file {} + | grep -i "text"
./inhere/maybehere07/.file2: ASCII text, with very long lines (1000)
bandit5@bandit:~$ cat ./inhere/maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

Password: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

Command: find ./inhere/ -size 1033c ! -executable -exec file {} + | grep -i "text"
cat ./inhere/maybehere07/.file2

Explanation: find locates the file by size and readability. cat displays its content. The c in 1033 is used to represent bytes. ! -executable means non executable file.

7. Level 6 – Level 7

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

```
bandit6@bandit: /home/bandit7
bandit6@bandit:/home$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:/home$ ^C
bandit6@bandit:/home$ cd /var/lib/dpkg/info/bandit7.password
-bash: cd: /var/lib/dpkg/info/bandit7.password: Not a directory
bandit6@bandit:/home$ cd var
-bash: cd: var: No such file or directory
bandit6@bandit:/home$ ls
bandit0  bandit17  bandit25  bandit30  bandit7  drifter15  formulaone0  krypton4
bandit1  bandit18  bandit26  bandit30-git  bandit8  drifter2  formulaone1  krypton5
bandit10 bandit19  bandit27  bandit31  bandit9  drifter3  formulaone2  krypton6
bandit11 bandit2  bandit27-git  bandit31-git  drifter0  drifter4  formulaone3  krypton7
bandit12 bandit20  bandit28  bandit32  drifter1  drifter5  formulaone5  ubuntu
bandit13 bandit21  bandit28-git  bandit33  drifter10  drifter6  formulaone6
bandit14 bandit22  bandit29  bandit4  drifter12  drifter7  krypton1
bandit15 bandit23  bandit29-git  bandit5  drifter13  drifter8  krypton2
bandit16 bandit24  bandit3  bandit6  drifter14  drifter9  krypton3
bandit6@bandit:/home$ cd bandit7
bandit6@bandit:/home/bandit7$ ls
data.txt
bandit6@bandit:/home/bandit7$ cat data.txt
cat: data.txt: Permission denied
bandit6@bandit:/home/bandit7$ ls -la
total 4108
drwxr-xr-x  2 root   root      4096 Sep 19 07:08 .
drwxr-xr-x 70 root   root      4096 Sep 19 07:09 ..
-rw-r--r--  1 root   root       220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root   root      3771 Mar 31 2024 .bashrc
-rw-r----- 1 bandit8 bandit7 4184396 Sep 19 07:08 data.txt
-rw-r--r--  1 root   root       807 Mar 31 2024 .profile
bandit6@bandit:/home/bandit7$ vim data.txt
[1]+  Stopped                  vim data.txt
bandit6@bandit:/home/bandit7$ sudo cat data.txt
sudo: /usr/bin/sudo must be owned by uid 0 and have the setuid bit set
bandit6@bandit:/home/bandit7$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:/home/bandit7$
```

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

Password: morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj

Command: find / -user bandit7 -group bandit6 -size33c 2>/dev/null

Explanation: find searches files by user and size. 2>/dev/null suppresses errors.

8. Level 7 -Level 8

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

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

Password: dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

Command: grep "millionth" data.txt

Explanation: grep searches for the string millionth in data.txt.

Grep – global regular expression print. Used to search for patterns in a file.

9. Level 8 – Level 9

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

```
* radare2 (http://www.radare.org/)

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit8@bandit:~$
```

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

Password: 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

Command: sort data.txt | uniq -u

Explanation: sort organizes lines, and uniq -u identifies unique lines. Uniq alone just removes the consecutive duplicate lines. The -u flag removes all the duplicate lines in the file.

10. Level 9 – Level 10

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.


```
bandit9@bandit: ~  
bandit9@bandit:~$ ls  
data.txt  
bandit9@bandit:~$ strings data.txt | grep "==="  
}===== the  
3JprD===== passwordi  
~fDV3===== is  
D9===== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey  
bandit9@bandit:~$
```

Password: FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

Command: strings data.txt | grep "=="

Explanation: strings extracts readable text from binary files. grep filters lines with ==.

11. Level 10 - Level 11

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

```
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit10@bandit:~$
```

```
bandit10@bandit:~$ ls  
data.txt  
bandit10@bandit:~$ grep data.txt  
^Z  
[1]+  Stopped                  grep --color=auto data.txt  
bandit10@bandit:~$ grep data.txt | base64  
^Z  
[2]+  Stopped                  grep --color=auto data.txt | base64  
bandit10@bandit:~$ base64 -d data.txt  
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr  
bandit10@bandit:~$
```

Password: dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

Command: base64 -d data.txt

Explanation: base64 -d decodes the contents of data.txt. The -d signifies decoding

12. Level 11 – Level 12

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

```
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit11@bandit:~$
```

```
bandit11@bandit:~$ cat data.txt | tr
tr: missing operand
Try 'tr --help' for more information.
bandit11@bandit:~$ cat data.txt | tr 'N-ZA-Mn-za-m'
tr: missing operand after 'N-ZA-Mn-za-m'
Two strings must be given when translating.
Try 'tr --help' for more information.
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
bandit11@bandit:~$
```

Password: 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4

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

Explanation: the tr (translate) command decode the ROT13 passwd back to normal. This command is used to both encode and decode in ROT13 cipher.

13. Level 12 – Level 13

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!)

```
bandit12@bandit: /tmp/tmp.BUja0t3WHc  x  sid@sid-HP-Laptop-14s-dy2xxx: ~  x  v
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ mv data5.bin data5.tar
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ tar -xvf data5.tar
data6.bin
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ file data
data: cannot open 'data' (No such file or directory)
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ mv data6.bin data6.bz2
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ ls
compressed_file.hex  compressed_file.tar  data5.tar  data6.bz2
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ bunzip2 data6.bz2
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ ls
compressed_file.hex  compressed_file.tar  data5.tar  data6
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ file data6
data6: POSIX tar archive (GNU)
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ mv data6 data6.tar
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ tar -xvf data6.tar
data8.bin
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ mv data8.bin data8.gz
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ gunzip data8.gz
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ ls
compressed_file.hex  compressed_file.tar  data5.tar  data6.tar  data8
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ file data8
data8: ASCII text
bandit12@bandit: /tmp/tmp.BUja0t3WHc$ cat data8
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
bandit12@bandit: /tmp/tmp.BUja0t3WHc$
```

Password: FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn

Command: mkdir /tmp/mydir

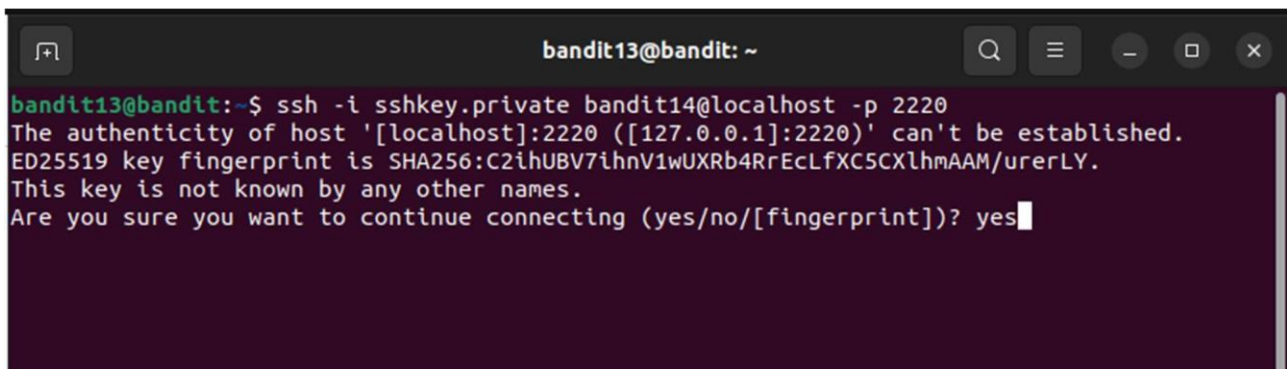
cp data.txt /tmp/mydir

```
cd /tmp/mydir file data.txt # Use the file type to decide decompression commands:
xxd -r data.txt # For hex
gzip -d file.gz
tar -xf file.tar
bzip2 -d file.bz
```

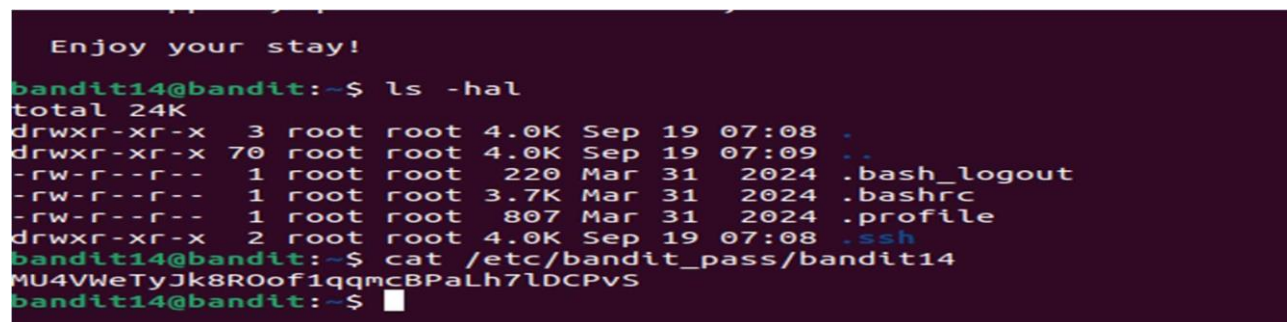
Explanation: Create a temporary file in /tmp and store the contents in it. Then decompress it based on its relative compressed modes and obtain the psswd from data8 file. Properties of a file can be obtained from file command.

14. Level 13 – Level 14

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



```
bandit13@bandit: ~
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
```



```
Enjoy your stay!
bandit14@bandit:~$ ls -hal
total 24K
drwxr-xr-x  3 root root 4.0K Sep 19 07:08 .
drwxr-xr-x 70 root root 4.0K Sep 19 07:09 ..
-rw-r--r--  1 root root  220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root root 3.7K Mar 31 2024 .bashrc
-rw-r--r--  1 root root 807 Mar 31 2024 .profile
drwxr-xr-x  2 root root 4.0K Sep 19 07:08 .ssh
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8ROof1qqmcBPALh7lDCPvS
bandit14@bandit:~$
```

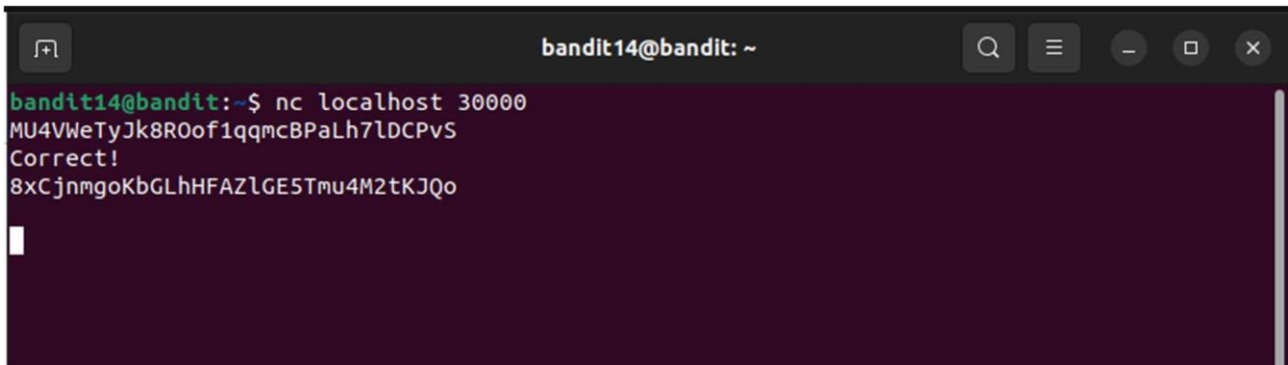
Password: MU4VWeTyJk8ROof1qqmcBPALh7lDCPvS

Command: ssh -i sshkey.private bandit14@localhost
cat /etc/bandit_pass/bandit14

Explanation: ssh is used to access bandit14 locally and then obtain the psswd from the file cat /etc/bandit_pass/bandit14 stored in bandit 14.

15. Level 14 – Level 15

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

A terminal window titled 'bandit14@bandit: ~' with standard window controls. The terminal shows the command 'nc localhost 30000' being executed. The output consists of three lines: a long alphanumeric string 'MU4VWeTyJk8R0of1qqmcBPALh7LDCPvS', the word 'Correct!', and another long alphanumeric string '8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo'. A cursor is visible on the line following the second password.

```
bandit14@bandit:~$ nc localhost 30000
MU4VWeTyJk8R0of1qqmcBPALh7LDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

```

Password: 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

Command: nc localhost 30000

Explanation: The command nc localhost 30000 is used to connect to a server running on your local machine (localhost) at port 30000. Then enter your current psswd to obtain the next level's psswd.