

# Task-7

How to login to ssh : use ssh command to connect to port 2220 and use [hostname@bandit.labs.overthewire.org](https://overthewire.org/wargames/bandit0/) .

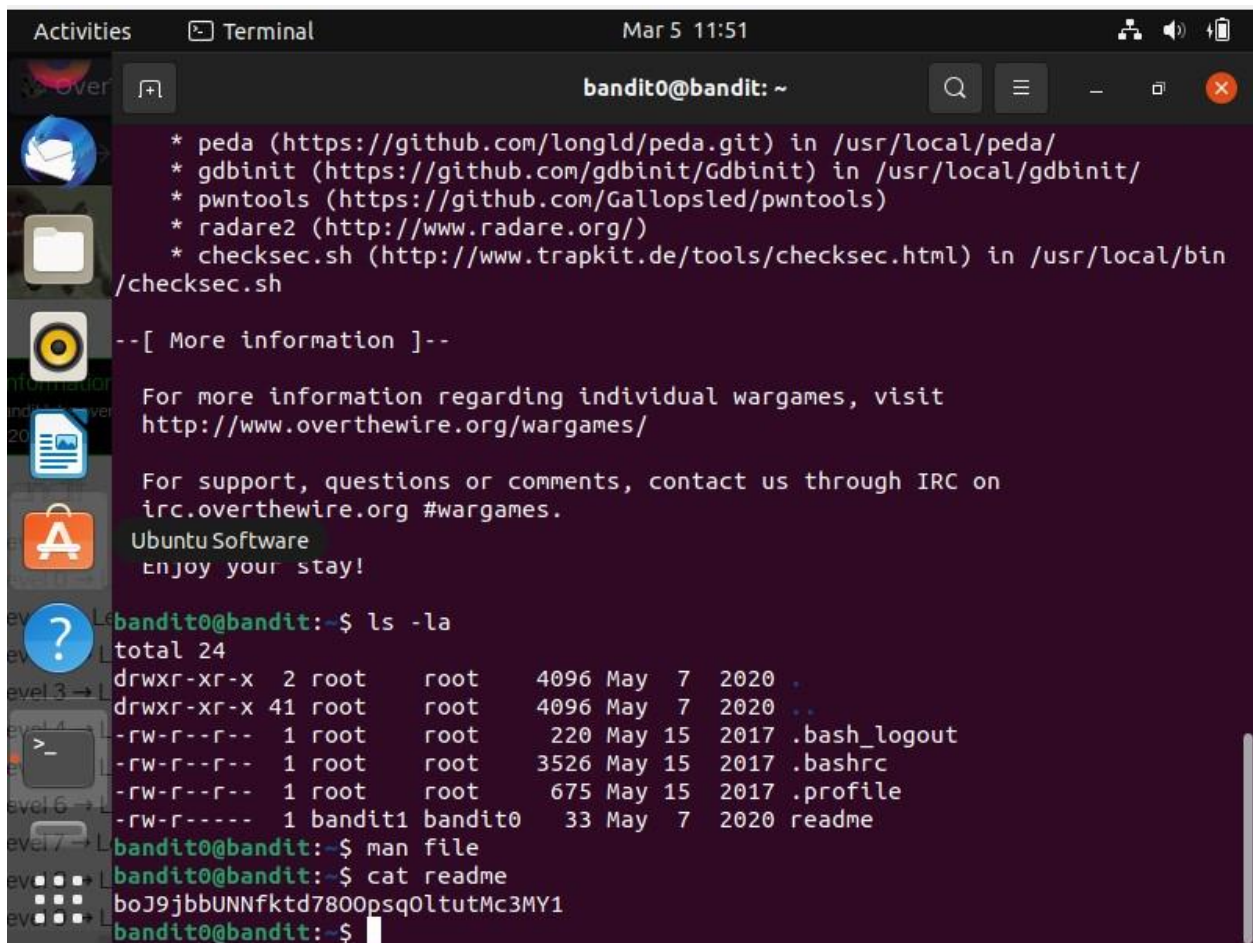
Level 0:

Hostname:bandit0

Password: bandit0

I connected to the bandit server by giving the username and password given in the overthewire.org website.

Then as per the instructions I used cat command on readme file to get the password.



```
bandit0@bandit: ~
* peda (https://github.com/longld/peda.git) in /usr/local/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
* checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin
/checksec.sh

--[ More information ]--

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

For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Ubuntu Software
enjoy your stay!

bandit0@bandit:~$ ls -la
total 24
drwxr-xr-x  2 root    root    4096 May  7  2020 .
drwxr-xr-x 41 root    root    4096 May  7  2020 ..
-rw-r--r--  1 root    root     220 May 15  2017 .bash_logout
-rw-r--r--  1 root    root   3526 May 15  2017 .bashrc
-rw-r--r--  1 root    root    675 May 15  2017 .profile
-rw-r-----  1 bandit1 bandit0   33 May  7  2020 readme
bandit0@bandit:~$ man file
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd7800psq0ltutMc3MY1
bandit0@bandit:~$
```

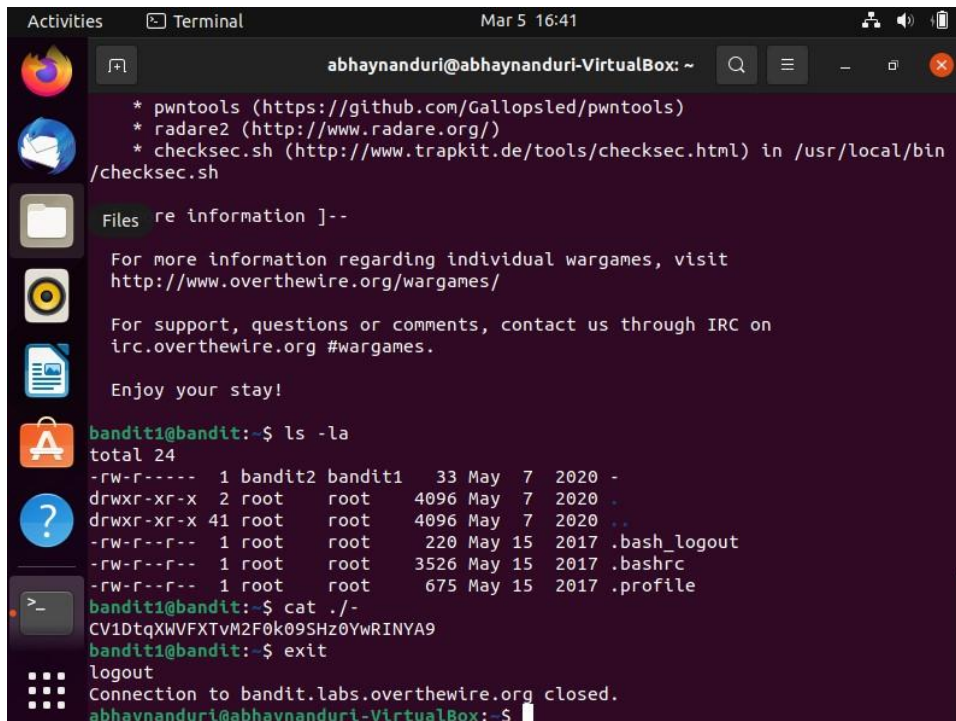
## Level 1

Hostname: bandit1

Password: boJ9jbbUNNfktd78OOpsqOltutMc3MY1

Logic:

Opening a file named '-' using cat command normally isn't possible as cat expects us to give an option. So, we write the whole path to open the file. Since the file exists in the current file, we use "cat ./-". Here "." means "current directory".



```
abhaynanduri@abhaynanduri-VirtualBox: ~
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
* checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin
/checksec.sh

Files re information ]--

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

For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Enjoy your stay!

bandit1@bandit:~$ ls -la
total 24
-rw-r----- 1 bandit2 bandit1 33 May 7 2020 -
drwxr-xr-x 2 root root 4096 May 7 2020 .
drwxr-xr-x 41 root root 4096 May 7 2020 ..
-rw-r--r-- 1 root root 220 May 15 2017 .bash_logout
-rw-r--r-- 1 root root 3526 May 15 2017 .bashrc
-rw-r--r-- 1 root root 675 May 15 2017 .profile

bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
abhaynanduri@abhaynanduri-VirtualBox:~$
```

## Level 2

Hostname: bandit2

Password: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

Logic:

The file here contains spaces so the linux system is going to confuse it with concatenating multiple files. So we enclose it in single quotes.

Or we can use “\” instead of spaces.

The screenshot shows a terminal window titled "bandit3@bandit: ~" with a search bar and window controls. The terminal output includes:

- Tool links: `* pwntools (https://github.com/Gallopsled/pwntools)`, `* radare2 (http://www.radare.org/)`, and `* checksec.sh (http://www.trapkit.de/tools/checksec.html)` in `/usr/local/bin/checksec.sh`.
- Files section: `Files re information ]--`
- Informational text: "For more information regarding individual wargames, visit <http://www.overthewire.org/wargames/>" and "For support, questions or comments, contact us through IRC on [#wargames](http://irc.overthewire.org)."
- User prompt: "Enjoy your stay!"
- Command execution: `bandit2@bandit:~$ ls -la`
- File listing output:

```
total 24
drwxr-xr-x  2 root   root   4096 May  7  2020 .
drwxr-xr-x 41 root   root   4096 May  7  2020 ..
-rw-r--r--  1 root   root    220 May 15  2017 .bash_logout
-rw-r--r--  1 root   root   3526 May 15  2017 .bashrc
-rw-r--r--  1 root   root    675 May 15  2017 .profile
-rw-r-----  1 bandit3 bandit2 33 May  7  2020 spaces in this filename
```
- File content: `bandit2@bandit:~$ cat 'spaces in this filename'` outputs `UmHadQcIWmgdLOKQ3YNgjWxGoRMb5luK`
- User actions: `bandit2@bandit:~$ exit` and `logout`
- Connection status: "Connection to bandit.labs.overthewire.org closed."
- Final command: `abhaynanduri@abhaynanduri-VirtualBox:~$ ssh -p2220 bandit3@bandit.labs.overthewire.org`

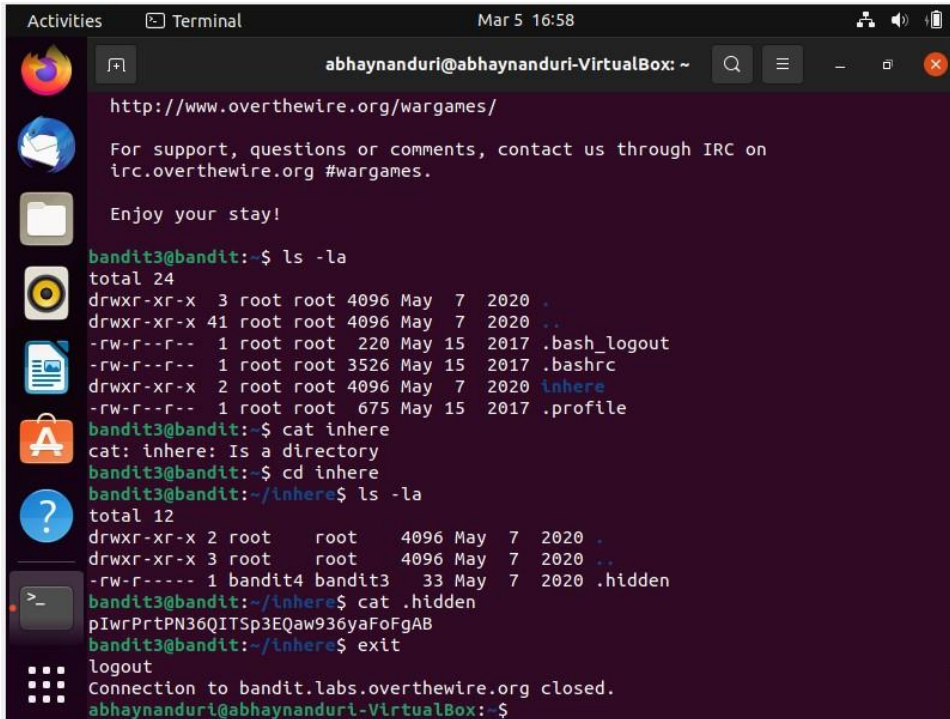
Level 3

Hostname: bandit3

Password: UmHadQcIWmgdLOKQ3YNgjWxGoRMb5luK

Logic:

The file containing password is hidden so we use `ls -la` to reveal it and open it.



```
Activities Terminal Mar 5 16:58
abhaynanduri@abhaynanduri-VirtualBox: ~
http://www.overthewire.org/wargames/
For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.
Enjoy your stay!
bandit3@bandit:~$ ls -la
total 24
drwxr-xr-x  3 root root 4096 May  7 2020 .
drwxr-xr-x 41 root root 4096 May  7 2020 ..
-rw-r--r--  1 root root  220 May 15 2017 .bash_logout
-rw-r--r--  1 root root 3526 May 15 2017 .bashrc
drwxr-xr-x  2 root root 4096 May  7 2020 inhere
-rw-r--r--  1 root root  675 May 15 2017 .profile
bandit3@bandit:~$ cat inhere
cat: inhere: Is a directory
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -la
total 12
drwxr-xr-x  2 root  root  4096 May  7 2020 .
drwxr-xr-x  3 root  root  4096 May  7 2020 ..
-rw-r-----  1 bandit4 bandit3  33 May  7 2020 .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtpN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
abhaynanduri@abhaynanduri-VirtualBox:~$
```

Level 4

Hostname: bandit4

Password: lwrPrtpN36QITSp3EQaW936yaFoFgAB

Logic:

We need to check for the type of data we are reading in the directory. It is achieved by using `file` command and to see the type of all the given files we use `"file ./*"`. `"*"` is for all files in the directory.

```
Activities Terminal Mar 5 17:42
bandit4@bandit: ~/Inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/Inhere$ ls -la
total 48
drwxr-xr-x 2 root root 4096 May 7 2020 .
drwxr-xr-x 3 root root 4096 May 7 2020 ..
-rw-r----- 1 bandit5 bandit4 33 May 7 2020 -file00
-rw-r----- 1 bandit5 bandit4 33 May 7 2020 -file01
-rw-r----- 1 bandit5 bandit4 33 May 7 2020 -file02
-rw-r----- 1 bandit5 bandit4 33 May 7 2020 -file03
-rw-r----- 1 bandit5 bandit4 33 May 7 2020 -file04
-rw-r----- 1 bandit5 bandit4 33 May 7 2020 -file05
-rw-r----- 1 bandit5 bandit4 33 May 7 2020 -file06
-rw-r----- 1 bandit5 bandit4 33 May 7 2020 -file07
-rw-r----- 1 bandit5 bandit4 33 May 7 2020 -file08
-rw-r----- 1 bandit5 bandit4 33 May 7 2020 -file09
bandit4@bandit:~/Inhere$ file ./-file07
./-file07: ASCII text
bandit4@bandit:~/Inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZCORTdopnAYKh
bandit4@bandit:~/Inhere$
```

Level 5

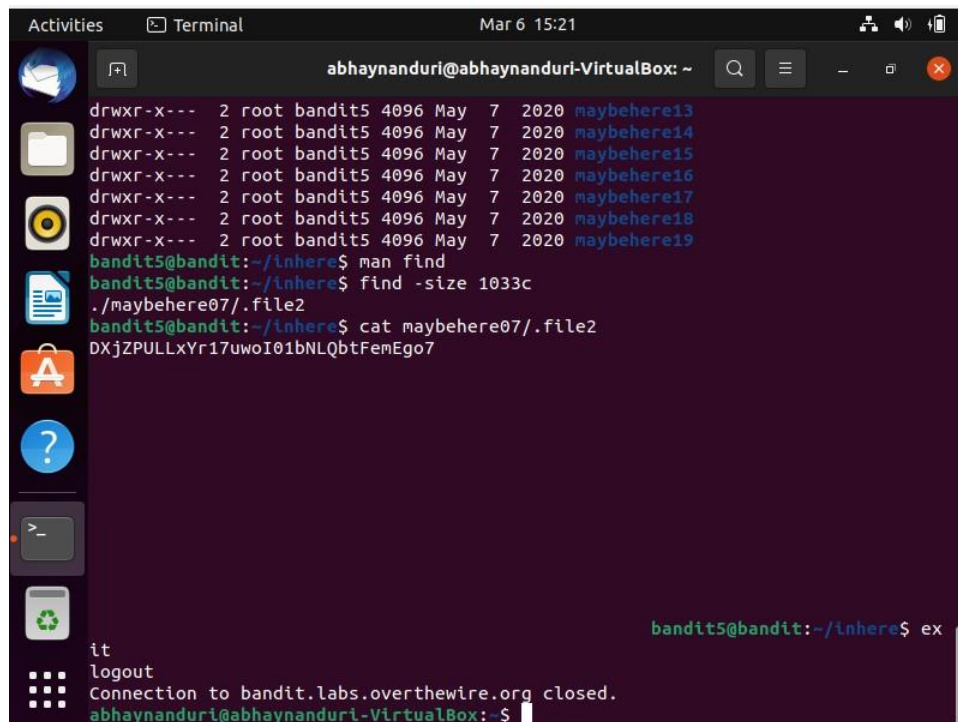
Hostname: bandit5

Password: koReBOKuIDDepwhWk7jZCORTdopnAYKh

Logic:

Use find command with given parameters to acquire the file. Then open it.





```
abhaynanduri@abhaynanduri-VirtualBox: ~
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere13
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere14
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere15
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere16
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere17
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere18
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere19
bandit5@bandit:~/inhere$ man find
bandit5@bandit:~/inhere$ find -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
bandit5@bandit:~/inhere$ ex
it
logout
Connection to bandit.labs.overthewire.org closed.
abhaynanduri@abhaynanduri-VirtualBox:~$
```

Level 6

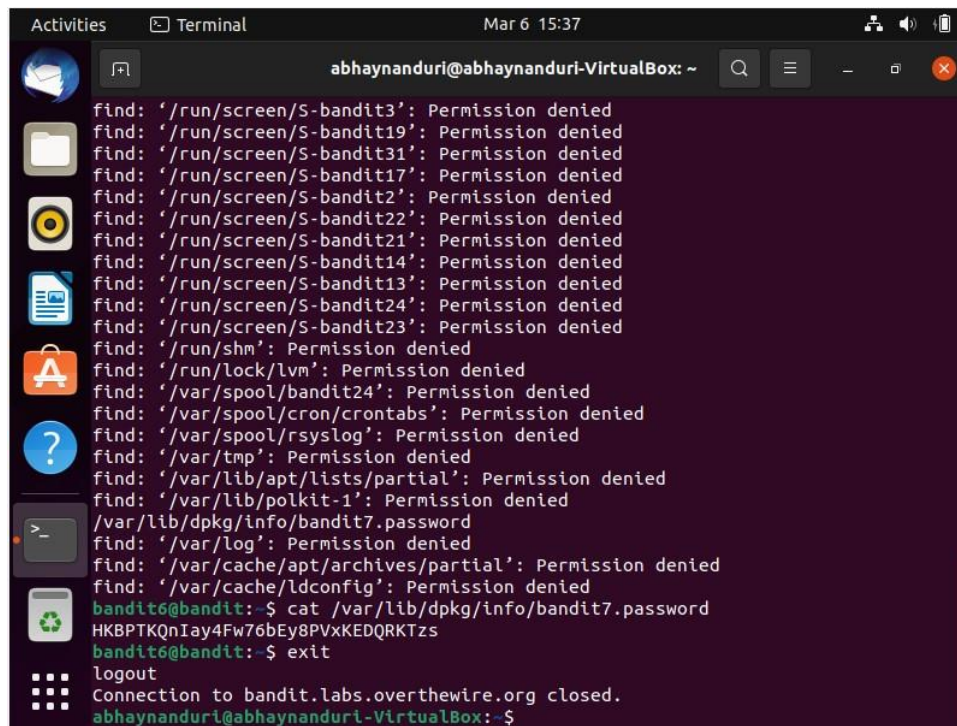
Hostname: bandit6

Password: DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Logic:

Using ls (even ls -la) will show that the directory is empty. So, we use the find command to find any hidden paths with the given parameters.

And You will see that there is only one file for which we have access so we open that and we get the password



```
Activities Terminal Mar 6 15:37
abhaynanduri@abhaynanduri-VirtualBox: ~
find: '/run/screen/S-bandit3': Permission denied
find: '/run/screen/S-bandit19': Permission denied
find: '/run/screen/S-bandit31': Permission denied
find: '/run/screen/S-bandit17': Permission denied
find: '/run/screen/S-bandit2': Permission denied
find: '/run/screen/S-bandit22': Permission denied
find: '/run/screen/S-bandit21': Permission denied
find: '/run/screen/S-bandit14': Permission denied
find: '/run/screen/S-bandit13': Permission denied
find: '/run/screen/S-bandit24': Permission denied
find: '/run/screen/S-bandit23': Permission denied
find: '/run/shm': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/tmp': Permission denied
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:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
abhaynanduri@abhaynanduri-VirtualBox:~$
```

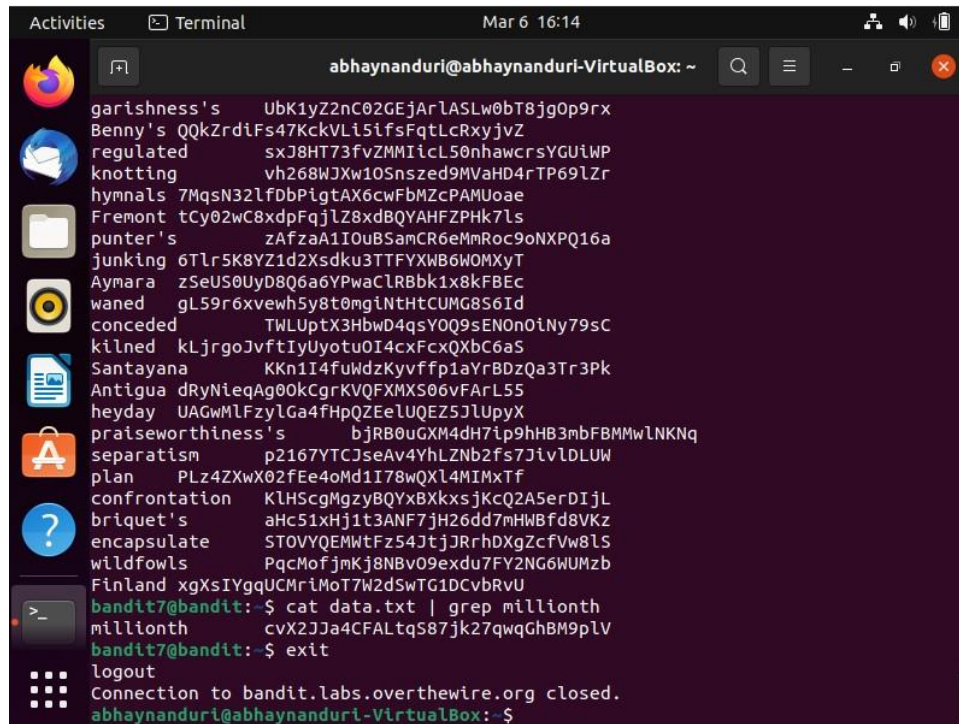
## Level 7

Hostname: bandit7

Password HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Logic:

The password is said to be in file data.txt and associated with word millionth so we pipeline cat with grep command to get the line with string millionth in it.



```
Activities Terminal Mar 6 16:14
abhaynanduri@abhaynanduri-VirtualBox: ~
garishness's UbK1yZ2nC02GEjArLASLw0bT8jg0p9rx
Benny's QQkZrdiFs47KckVLI5ifsFqtLcRxyjvZ
regulated sxJ8HT73fvZMMiicL50nhawcrsYGUIWP
knotting vh268WJXw10Snszed9MVAHD4rTP69lZr
hymnals 7MqsN32lfDbPigtAX6cwFbMZcPAMUoae
Fremont tCy02wC8xdpFqjLZ8xdBQYAHFZPHk7Ls
punter's zAfzaA1IOuBSamCR6eMmRoc9oNXpQ16a
junking 6Tlr5K8YZ1d2Xsdu3TTFYXWB6WOMxyT
Aymara zSeUS0UyD8Q6a6YPwaCLRBbk1x8kFBEC
waned gL59r6xvewh5y8t0mgiNtHtCUMG8S6Id
conceded TWLUptX3HbwD4qsYQ09sENOn0iNy79sc
kilned kLjrGoJvftIyUyotu0I4cxFcXQXbC6aS
Santayana KKn1I4fuWdzKyvffp1aYrBDzQa3Tr3Pk
Antigua dRyNiegAg00kCgrKVQFXMXS06vFARL55
heyday UAGWMLFzylGa4fHpQZEelUQEZ5JlUpyX
praiseworthiness's bJR80uGXM4dH7ip9Hb3mbFBMMwLNKNq
separatism p2167YTCJseAv4YhLZNb2fs7JivLDLUW
plan PLz4ZXwX02fEe4oMd1I78wQXL4MIMxTf
confrontation KLHScgMgzyBQYxBXkxsjKcQ2A5erDIjL
briquet's aHc51xHj1t3ANF7jH26dd7mHwBfd8VKz
encapsulate STOVYQEMWtFz54JtjJRrhDXgZcfVw8lS
wildfowls PqcMofjmKj8NBv09exdu7FY2NG6WUMzb
Finland xgXsIYgqUCMrIMoT7W2dSwTG1DCvbRvU
bandit7@bandit:~$ cat data.txt | grep millionth
millionth cvX2JJJa4CFALtqS87jk27qwqGhBM9plv
bandit7@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
abhaynanduri@abhaynanduri-VirtualBox:~$
```

Level 8

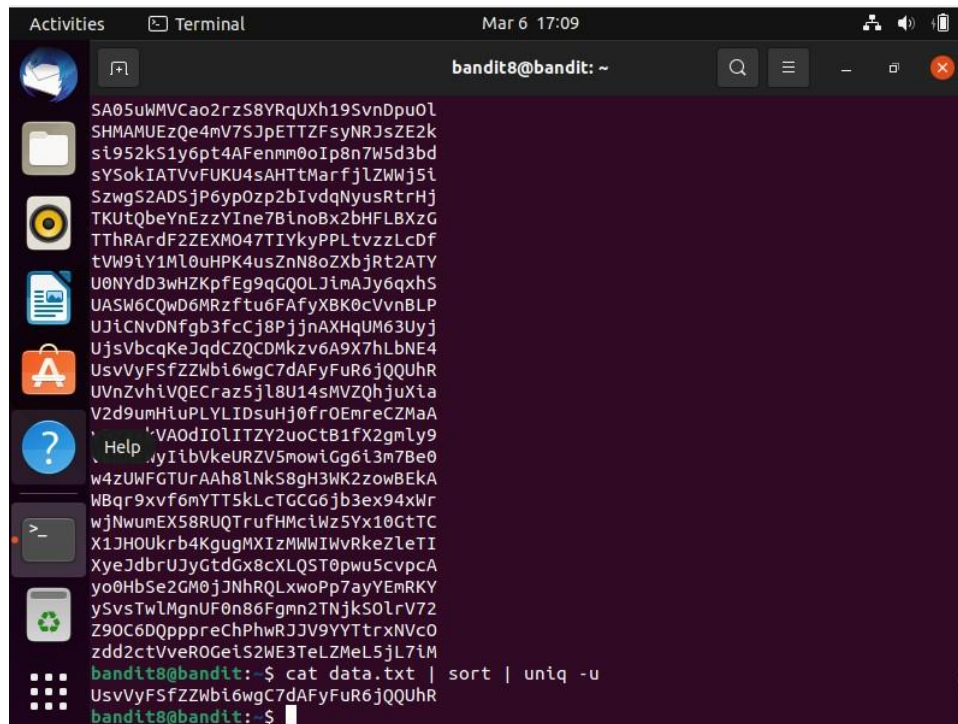
Hostname: bandit8

Password cvX2JJJa4CFALtqS87jk27qwqGhBM9plv

Logic:

By pipelining cat and sort command we get to know that many lines repeat so we pipeline an extra command uniq to find the password





## Level 9

Hostname: bandit9

Password: UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Logic:

Strings command gives printable strings in file. So, we use grep to find strings with "=" in it.

```
Activities Terminal Mar 6 17:25
abhaynanduri@abhaynanduri-VirtualBox: ~
irc.overthewire.org #wargames.
Enjoy your stay!
bandit9@bandit:~$ man strings
bandit9@bandit:~$ ls -la
total 40
drwxr-xr-x  2 root    root      4096 May  7  2020 .
drwxr-xr-x 41 root    root      4096 May  7  2020 ..
-rw-r--r--  1 root    root        220 May 15  2017 .bash_logout
-rw-r--r--  1 root    root      3526 May 15  2017 .bashrc
-rw-r-----  1 bandit10 bandit9 19379 May  7  2020 data.txt
-rw-r--r--  1 root    root        675 May 15  2017 .profile
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.
abhaynanduri@abhaynanduri-VirtualBox:~$
```

Level 10

Hostname: bandit10

Password: truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Logic:

Use base64 to decode the encryption in data.txt

```
Activities Terminal Mar 6 17:33
abhaynanduri@abhaynanduri-VirtualBox: ~
--[ More information ]--
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/
For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.
Enjoy your stay!
bandit10@bandit:~$ man base64
bandit10@bandit:~$ ls -la
total 24
drwxr-xr-x  2 root    root    4096 May  7  2020 .
drwxr-xr-x 41 root    root    4096 May  7  2020 ..
-rw-r--r--  1 root    root     220 May 15  2017 .bash_logout
-rw-r--r--  1 root    root    3526 May 15  2017 .bashrc
-rw-r----- 1 bandit11 bandit10  69 May  7  2020 data.txt
-rw-r--r--  1 root    root    675 May 15  2017 .profile
bandit10@bandit:~$ base64 data.txt
Terminal _mhjM04zYjNKa0LHbHpJRwxHZFd0M1MwZHpSbGM0VFU5eE0wbFNSbkZ5ZUVVeGFiaFVU
a1ZpVLZCU0NnPT0K
bandit10@bandit:~$ man base64
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
abhaynanduri@abhaynanduri-VirtualBox:~$
```

Level 11

Hostname: bandit11

Password: IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Logic: This is a special type of cipher used by Julius Ceasar. All lower-case letters and upper-case letters are rotated by 13 letters each.

Input	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
Output	NOPQRSTUVWXYZABCDEFGHIJKLMnopqrstuvwxyzabcdefghijklm

```
Activities Terminal Mar 6 17:47
abhaynanduri@abhaynanduri-VirtualBox: ~
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
* checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin
~/checksec.sh
Files
--[ More information ]--

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

For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Enjoy your stay!
bandit11@bandit:~$ ls -la
total 24
drwxr-xr-x  2 root    root    4096 May  7  2020 .
drwxr-xr-x 41 root    root    4096 May  7  2020 ..
-rw-r--r--  1 root    root    220 May 15  2017 .bash_logout
-rw-r--r--  1 root    root   3526 May 15  2017 .bashrc
-rw-r-----  1 bandit12 bandit11  49 May  7  2020 data.txt
-rw-r-----  1 root    root    675 May 15  2017 .profile
bandit11@bandit:~$ cat data.txt | tr 'a-zA-Z' 'n-za-mN-ZA-M'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
bandit11@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
abhaynanduri@abhaynanduri-VirtualBox:~$
```

## Level 12

Hostname: bandit12

Password: 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Logic: we decrypt the hexdump using xxd command and make a temporary directory as specified. Now we repeatedly unzip the files.

```
Activities Terminal Mar 6 18:44
abhaynanduri@abhaynanduri-VirtualBox: ~
bandit12@bandit:/tmp/CP0shit$ ls
data5.bin data6.bin data.txt itstarnow
bandit12@bandit:/tmp/CP0shit$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/CP0shit$ mv data6.bin istg.bz2
bandit12@bandit:/tmp/CP0shit$ bzip2 -d istg.bz2
bandit12@bandit:/tmp/CP0shit$ ls
data5.bin data.txt istg itstarnow
bandit12@bandit:/tmp/CP0shit$ file istg
istg: POSIX tar archive (GNU)
bandit12@bandit:/tmp/CP0shit$ tar -xf istg
bandit12@bandit:/tmp/CP0shit$ ls
data5.bin data8.bin data.txt istg itstarnow
bandit12@bandit:/tmp/CP0shit$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu May 7 18:
14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/CP0shit$ mv data8.bin istgx2.gz
bandit12@bandit:/tmp/CP0shit$ gzip -d istgx2.gz
bandit12@bandit:/tmp/CP0shit$ ls
data5.bin data.txt istg istgx2 itstarnow
bandit12@bandit:/tmp/CP0shit$ file istgx2
istgx2: ASCII text
bandit12@bandit:/tmp/CP0shit$ mv istgx2 finallyascii.txt
bandit12@bandit:/tmp/CP0shit$ cat finallyascii.txt
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/CP0shit$ exit
logout
Connection to bandit.labs.overthewire.org closed.
abhaynanduri@abhaynanduri-VirtualBox:~$
```

## Level 13

Hostname: bandit13

Password: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Logic:

We use ssh command using hostname@localhost and -i option as shown below. The password for level 14 is in level 14 itself so we get the level 14 password in the specified path of the Level 13 problem statement.



```
Activities Terminal Mar 6 19:02 bandit14@bandit: ~
--[ More information ]--
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/
For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.
~ . . . ~
Rhythmbox
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh bandit14@localhost -i sshkey.private
Could not create directory '/home/bandit13/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKLo20X30PnyPSB5tB5RPbhczc.
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_ho
sts).
This is a OverTheWire game server. More information on http://www.overthewire.o
rg/wargames
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

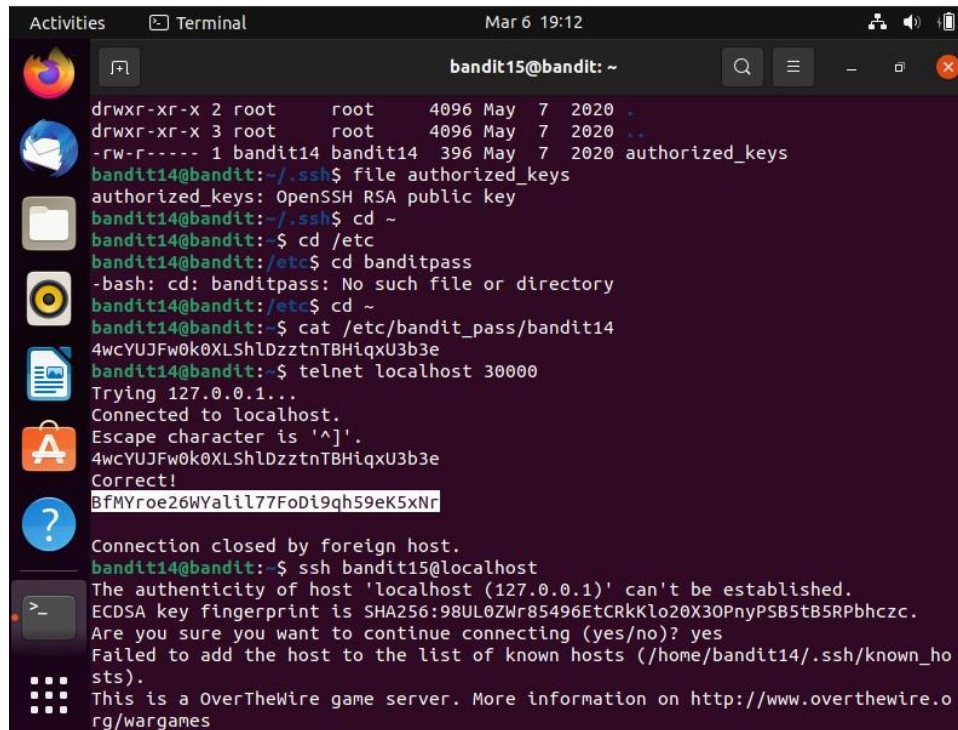
```
Activities Terminal Mar 6 19:08 bandit14@bandit: ~
Enjoy your stay!
Thunderbird Mail :~$ ls
bandit14@bandit:~$ ls -la
total 24
drwxr-xr-x 3 root root 4096 May 7 2020 .
drwxr-xr-x 41 root root 4096 May 7 2020 ..
-rw-r--r-- 1 root root 220 May 15 2017 .bash_logout
-rw-r--r-- 1 root root 3526 May 15 2017 .bashrc
-rw-r--r-- 1 root root 675 May 15 2017 .profile
drwxr-xr-x 2 root root 4096 May 7 2020 .ssh
bandit14@bandit:~$ cd .ssh
-bash: cd: command not found
bandit14@bandit:~$ cd ./.ssh
bandit14@bandit:~/.ssh$ ls -la
total 12
drwxr-xr-x 2 root root 4096 May 7 2020 .
drwxr-xr-x 3 root root 4096 May 7 2020 ..
-rw-r----- 1 bandit14 bandit14 396 May 7 2020 authorized_keys
bandit14@bandit:~/.ssh$ file authorized_keys
authorized_keys: OpenSSH RSA public key
bandit14@bandit:~/.ssh$ cd ~
bandit14@bandit:~$ cd /etc
bandit14@bandit:/etc$ cd banditpass
-bash: cd: banditpass: No such file or directory
bandit14@bandit:/etc$ cd ~
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShLDzztnTBHiqXU3b3e
bandit14@bandit:~$
```

Level 14

Hostname: bandit14

Password: 4wcYUFw0k0XLSHlDzztnTBHiqxU3b3e

Logic: We connect to telnet interface by using given port on localhost and password of level 14. And we get the password of level 15



```
Activities Terminal Mar 6 19:12
bandit15@bandit: ~
drwxr-xr-x 2 root root 4096 May 7 2020 .
drwxr-xr-x 3 root root 4096 May 7 2020 ..
-rw-r----- 1 bandit14 bandit14 396 May 7 2020 authorized_keys
bandit14@bandit:~/.ssh$ file authorized_keys
authorized_keys: OpenSSH RSA public key
bandit14@bandit:~/.ssh$ cd ~
bandit14@bandit:~$ cd /etc
bandit14@bandit:/etc$ cd banditpass
-bash: cd: banditpass: No such file or directory
bandit14@bandit:/etc$ cd ~
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUFw0k0XLSHlDzztnTBHiqxU3b3e
bandit14@bandit:~$ telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
4wcYUFw0k0XLSHlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
Connection closed by foreign host.
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_ho
sts).
This is a OverTheWire game server. More information on http://www.overthewire.o
rg/wargames
```

Level 15

Hostname: bandit15

Password: BfMYroe26WYalil77FoDi9qh59eK5xNr