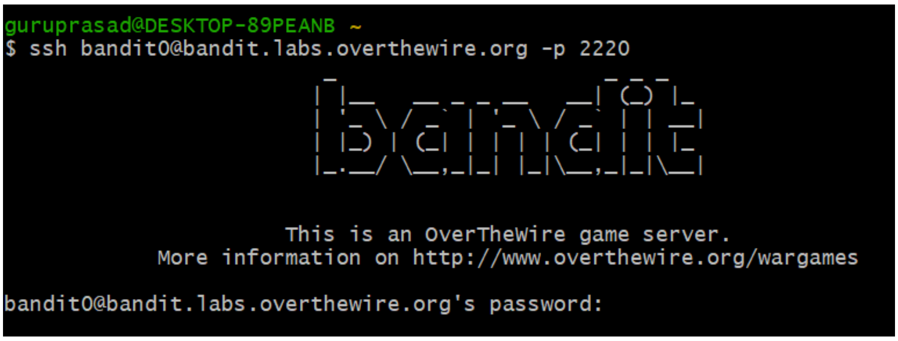
BANDIT OVERTHEWIRE WRITE-UP

- BANDIT LEVEL 0

  This level aimed at ensuring a secure ssh connection.



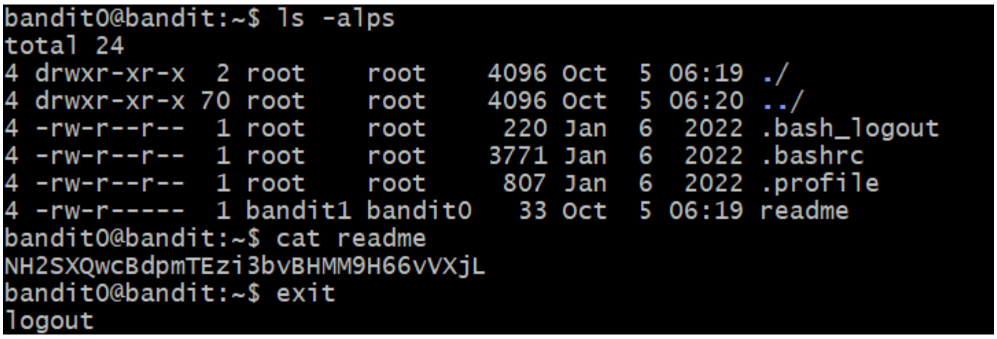
```
guruprasad@DESKTOP-89PEANB ~
$ ssh bandit0@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

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

I just had to enter the command,

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

and enter the password: bandit0 which was already given.

- BANDIT LEVEL 0-1



```
bandit0@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  2 root    root    4096 Oct  5 06:19 ./
4 drwxr-xr-x 70 root    root    4096 Oct  5 06:20 ../
4 -rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
4 -rw-r--r--  1 root    root     807 Jan  6  2022 .profile
4 -rw-r-----  1 bandit1 bandit0   33 Oct  5 06:19 readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
bandit0@bandit:~$ exit
logout
```

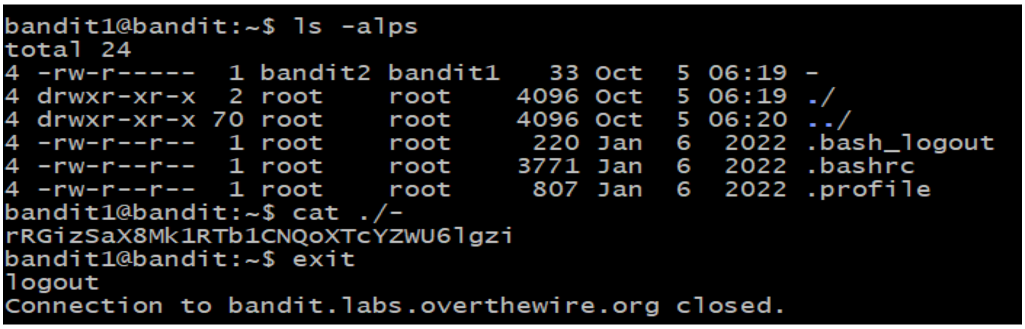
I used the command ls which is used to examine the files in the directory and then cat the readme file as suggested by the hint of this level which gave me the password.

Commands used: cat, ls

cat: reads all the data from a file and gives its content as output.

ls: It is a Linux shell command that lists all the directories in the computer

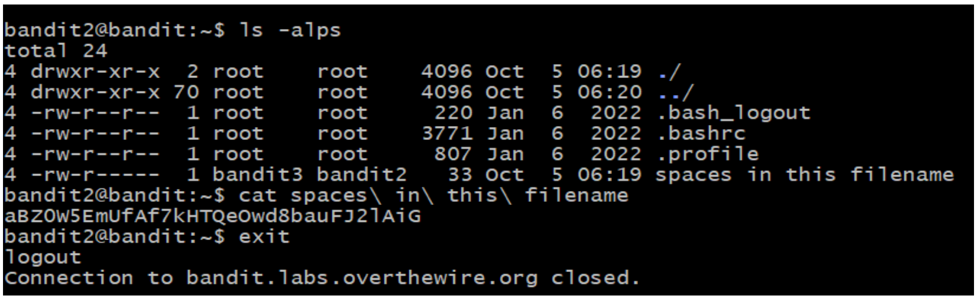
- BANDIT LEVEL 1-2



```
bandit1@bandit:~$ ls -alps
total 24
4 -rw-r-----  1 bandit2 bandit1   33 Oct  5 06:19 -
4 drwxr-xr-x  2 root    root    4096 Oct  5 06:19 ./
4 drwxr-xr-x 70 root    root    4096 Oct  5 06:20 ../
4 -rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
4 -rw-r--r--  1 root    root     807 Jan  6  2022 .profile
bandit1@bandit:~$ cat ./-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

In this level, the password was enclosed in a file named, ‘-‘. So I listed the files in the directory and cat the file named ‘-‘, while providing its address in the directory. While using cat command , I used ./ before ‘-‘ as it doesn’t yield an output otherwise.

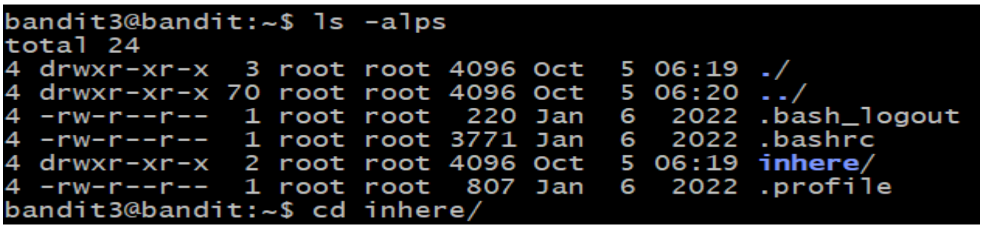
- BANDIT LEVEL 2-3



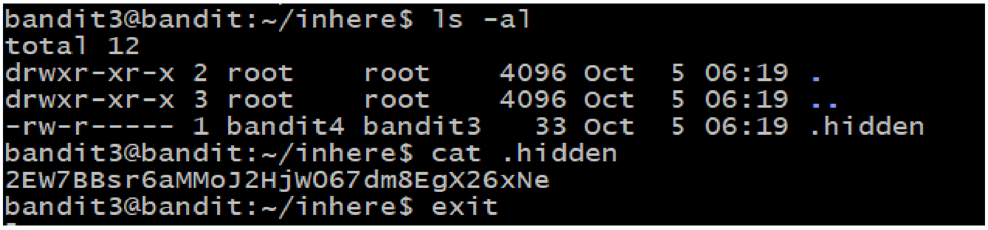
```
bandit2@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  2 root    root    4096 Oct  5 06:19 ./
4 drwxr-xr-x 70 root    root    4096 Oct  5 06:20 ../
4 -rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
4 -rw-r--r--  1 root    root     807 Jan  6  2022 .profile
4 -rw-r-----  1 bandit3 bandit2   33 Oct  5 06:19 spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
bandit2@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Here, the password was enclosed in a file named ‘spaces in this filename’.
Used backslashes before every space which helps in eliminating any issues while getting the output. It is required for files having spaces in its name.

- BANDIT LEVEL 3-4



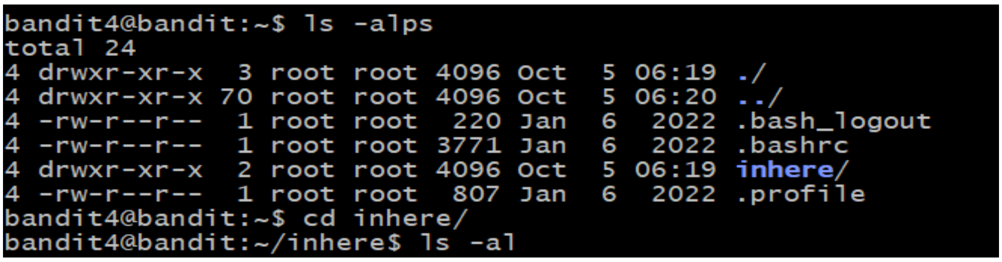
```
bandit3@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root root 4096 Oct  5 06:19 ./
4 drwxr-xr-x 70 root root 4096 Oct  5 06:20 ../
4 -rw-r--r--  1 root root  220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root root 3771 Jan  6  2022 .bashrc
4 drwxr-xr-x  2 root root 4096 Oct  5 06:19 inhere/
4 -rw-r--r--  1 root root  807 Jan  6  2022 .profile
bandit3@bandit:~$ cd inhere/
```



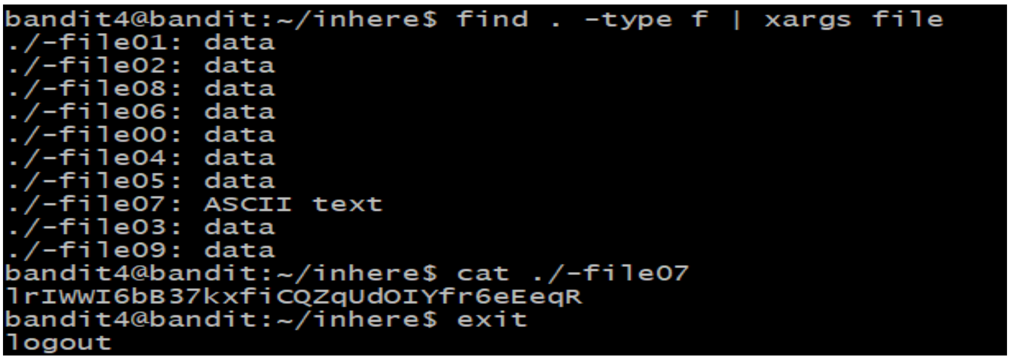
```
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root    root    4096 Oct  5 06:19 .
drwxr-xr-x 3 root    root    4096 Oct  5 06:19 ..
-rw-r----- 1 bandit4 bandit3   33 Oct  5 06:19 .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$ exit
```

I used the cd command which is used to change the directory from the current working directory of the file.
In this level since this file is hidden, we cat the hidden file which gives the password.

- BANDIT LEVEL 4-5



```
bandit4@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root root 4096 Oct  5 06:19 ./
4 drwxr-xr-x 70 root root 4096 Oct  5 06:20 ../
4 -rw-r--r--  1 root root  220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root root 3771 Jan  6  2022 .bashrc
4 drwxr-xr-x  2 root root 4096 Oct  5 06:19 inhere/
4 -rw-r--r--  1 root root  807 Jan  6  2022 .profile
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls -al
```

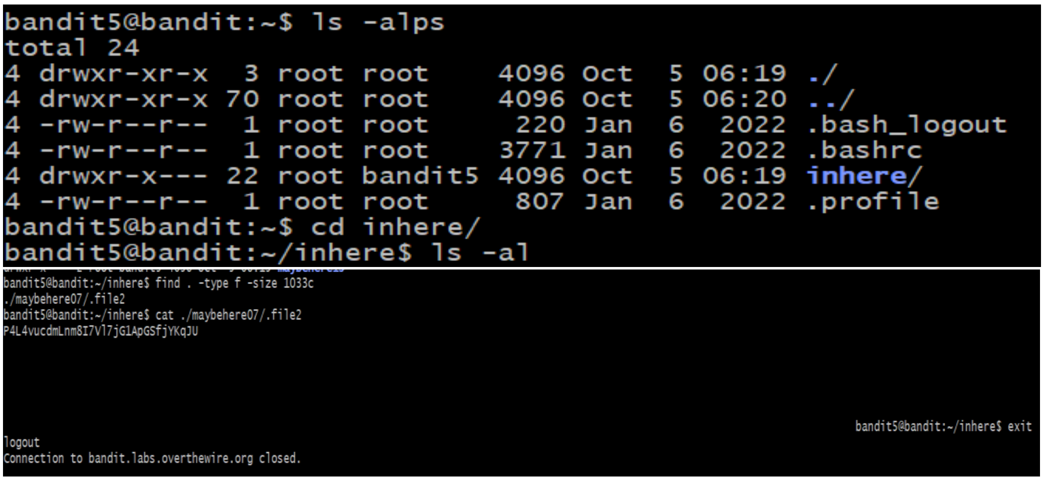


```
bandit4@bandit:~/inhere$ find . -type f | xargs file
./-file01: data
./-file02: data
./-file08: data
./-file06: data
./-file00: data
./-file04: data
./-file05: data
./-file07: ASCII text
./-file03: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$ exit
logout
```

We're basically using **find** to get the **full paths** of all files in the current directory, and then passing those paths as STDIN to the file command, which will return the file type. We use **xargs** to perform the file command for each line.

xargs command is used to build and execute commands from standard input.

- BANDIT 5-6

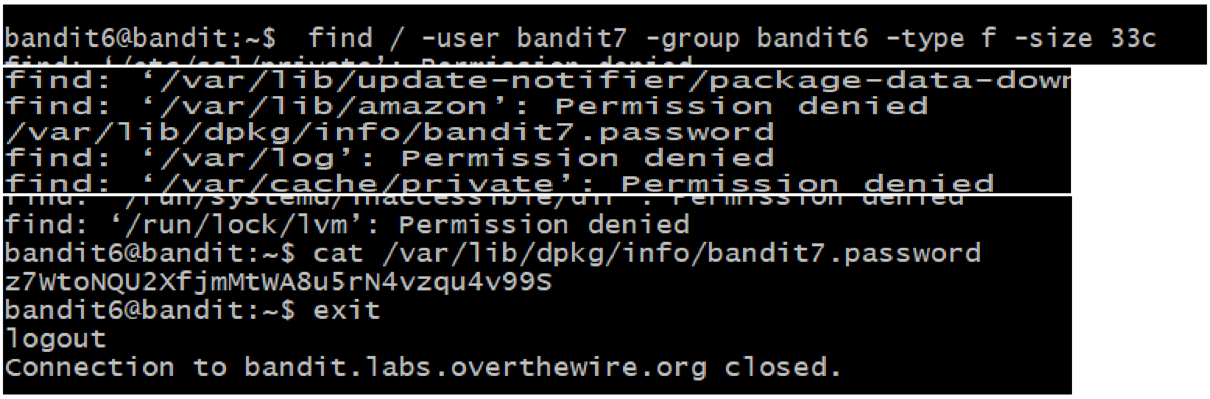


```
bandit5@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root root     4096 Oct  5 06:19 ./
4 drwxr-xr-x 70 root root     4096 Oct  5 06:20 ../
4 -rw-r--r--  1 root root      220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root root     3771 Jan  6  2022 .bashrc
4 drwxr-x--- 22 root bandit5 4096 Oct  5 06:19 inhere/
4 -rw-r--r--  1 root root      807 Jan  6  2022 .profile
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ ls -al
bandit5@bandit:~/inhere$ find . -type f -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU



                                                        bandit5@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Since there are too many files in this case, we use the file command using the type and space parameters to help us find the required easily.

Here c command is used which interprets the command as intended by the program.

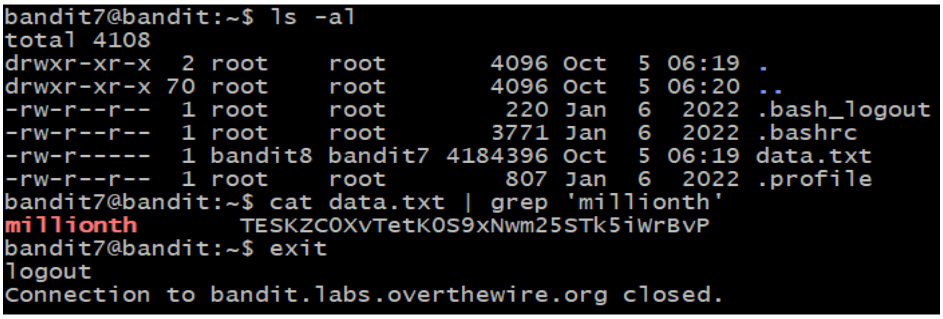
- BANDIT 6-7



```
bandit6@bandit:~$  find / -user bandit7 -group bandit6 -type f -size 33c
find: '/var/lib/update-notifier/package-data-down
find: '/var/lib/amazon': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/log': Permission denied
find: '/var/cache/private': Permission denied
find: '/run/lock/lvm': Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
bandit6@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

The scope of the search here includes the entire drive of computer, so we have used the slash (/) after the find command.

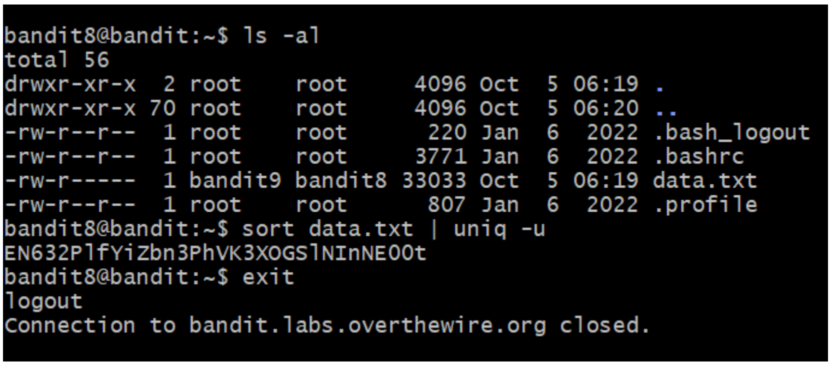
- BANDIT 7-8



```
bandit7@bandit:~$ ls -al
total 4108
drwxr-xr-x  2 root    root       4096 Oct  5 06:19 .
drwxr-xr-x 70 root    root       4096 Oct  5 06:20 ..
-rw-r--r--  1 root    root        220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root    root       3771 Jan  6  2022 .bashrc
-rw-r-----  1 bandit8 bandit7 4184396 Oct  5 06:19 data.txt
-rw-r--r--  1 root    root        807 Jan  6  2022 .profile
bandit7@bandit:~$ cat data.txt | grep 'millionth'
millionth       TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Here , the grep command is used. Also the pipe, the pipe connects the standard output from the first command and feeds it as a standard input to the second command

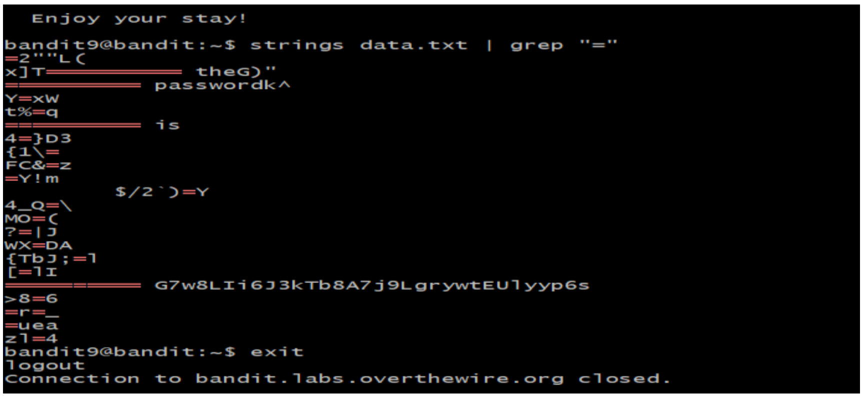
- BANDIT 8-9



```
bandit8@bandit:~$ ls -al
total 56
drwxr-xr-x  2 root    root    4096 Oct  5 06:19 .
drwxr-xr-x 70 root    root    4096 Oct  5 06:20 ..
-rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
-rw-r-----  1 bandit9 bandit8 33033 Oct  5 06:19 data.txt
-rw-r--r--  1 root    root     807 Jan  6  2022 .profile
bandit8@bandit:~$ sort data.txt | uniq -u
EN632PlfYiZbn3PhVK3XOGSlNInNE00t
bandit8@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Here the sort and uniq command is used , the sort command sorts all the data in alphabetic order, while the uniq command eliminates all instances if duplicated data, as in this case, it appears only once.

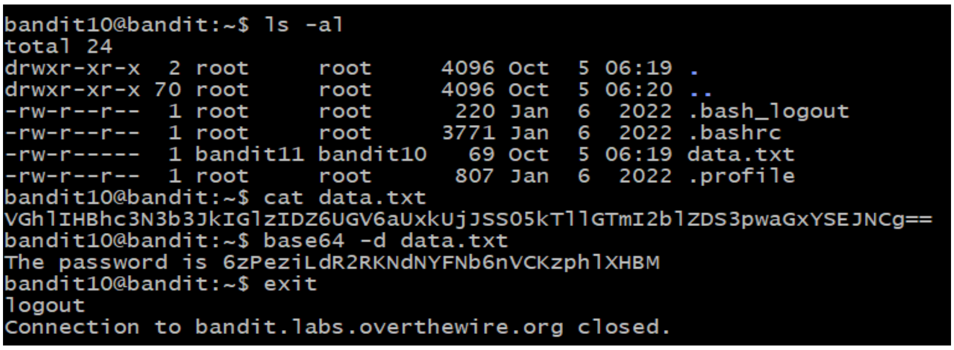
- BANDIT 9-10



```
  Enjoy your stay!

bandit9@bandit:~$ strings data.txt | grep "="
=2""L(
x]T========== theG)"
========== passwordk^
Y=xW
t%=q
========== is
4=}D3
{1\=
FC&=z
=Y!m
        $/2`)=Y
4_Q=\
MO=(
?=|J
WX=DA
{TbJ;=l
[=lI
========== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
>8=6
=r=_
=uea
zl=4
bandit9@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Strings command is used here, it searches the whole file for any string values it can examine and displays them in the output. Here it greps only the records containing the ‘=’ character.

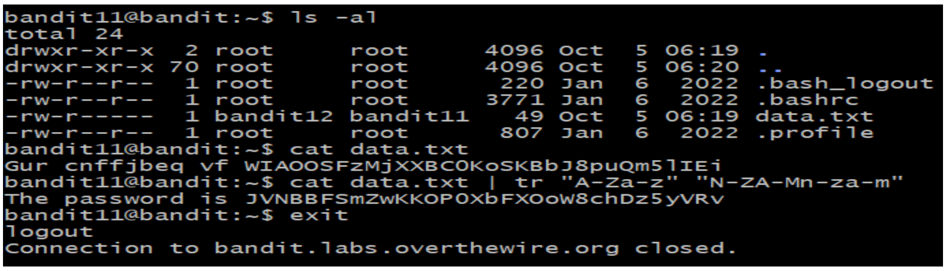
- BANDIT 10-11



```
bandit10@bandit:~$ ls -al
total 24
drwxr-xr-x  2 root     root     4096 Oct  5 06:19 .
drwxr-xr-x 70 root     root     4096 Oct  5 06:20 ..
-rw-r--r--  1 root     root      220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root     root     3771 Jan  6  2022 .bashrc
-rw-r-----  1 bandit11 bandit10   69 Oct  5 06:19 data.txt
-rw-r--r--  1 root     root      807 Jan  6  2022 .profile
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTllGTmI2blZDS3pwaGxYSEJNCg==
bandit10@bandit:~$ base64 -d data.txt
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

This level introduced me to base 64 encoding. Here the password was in encoded in base 64 form, we had to decode it. So when I used cat data.txt , it gives a code in encoded form. To decode it, we use base64 –d data.txt which gives the decoded password.

- BANDIT 11-12



```
bandit11@bandit:~$ ls -al
total 24
drwxr-xr-x  2 root     root     4096 Oct  5 06:19 .
drwxr-xr-x 70 root     root     4096 Oct  5 06:20 ..
-rw-r--r--  1 root     root      220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root     root     3771 Jan  6  2022 .bashrc
-rw-r-----  1 bandit12 bandit11   49 Oct  5 06:19 data.txt
-rw-r--r--  1 root     root      807 Jan  6  2022 .profile
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSKBbJ8puQm5lIEi
bandit11@bandit:~$ cat data.txt | tr "A-Za-z" "N-ZA-Mn-za-m"
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
bandit11@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Here, all the lowercase and uppercase letters are rotated by 13 position, so we can use tr command to set it as per 13 position to get the password.
tr command is used when characters have to be deleted or translated from the stdin and is to be written at the output. It can be used for case conversion or deleting characters.