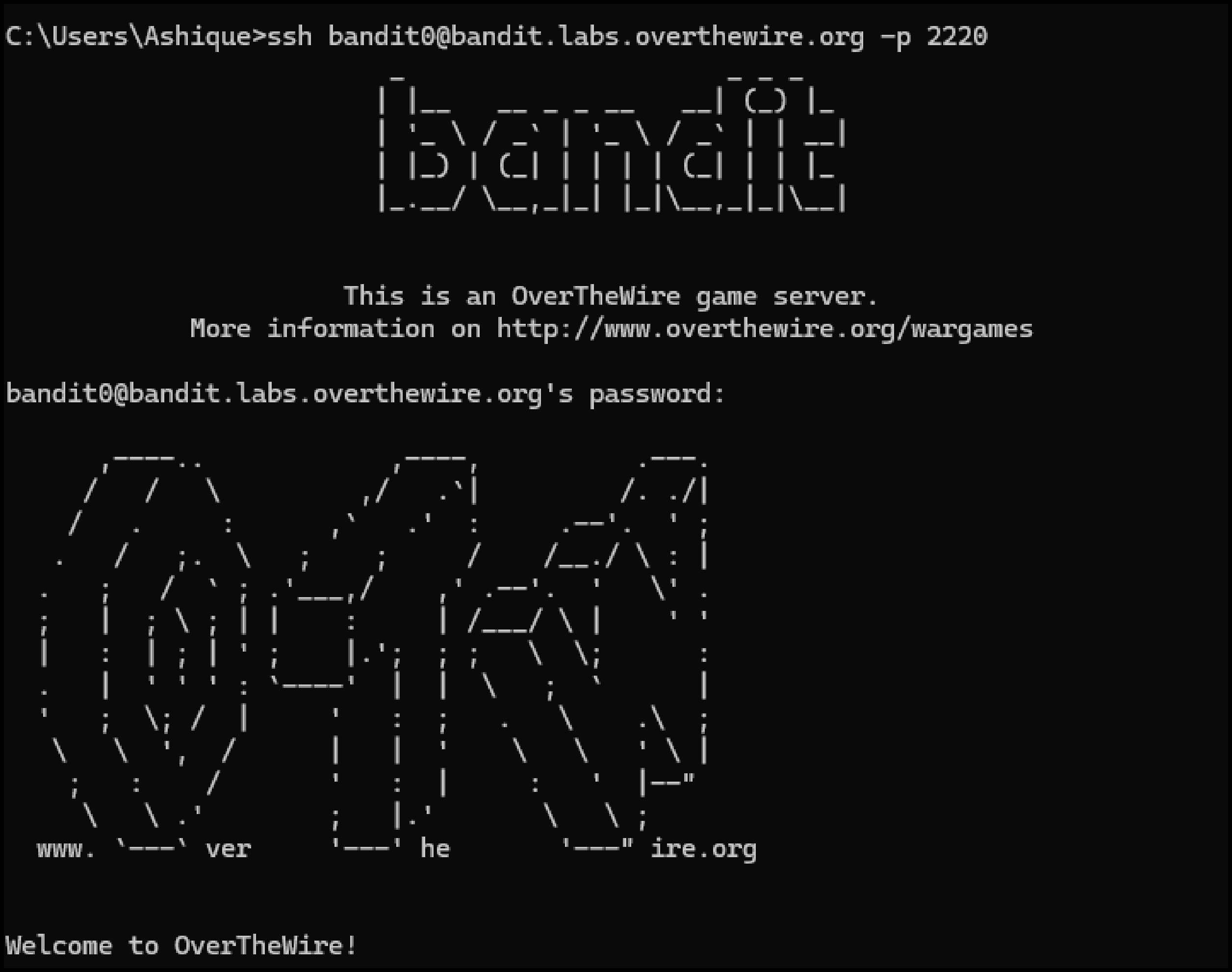
The Game of Bandit

Author: Rezvee Parvez

Level 0: Entering the *Game*!



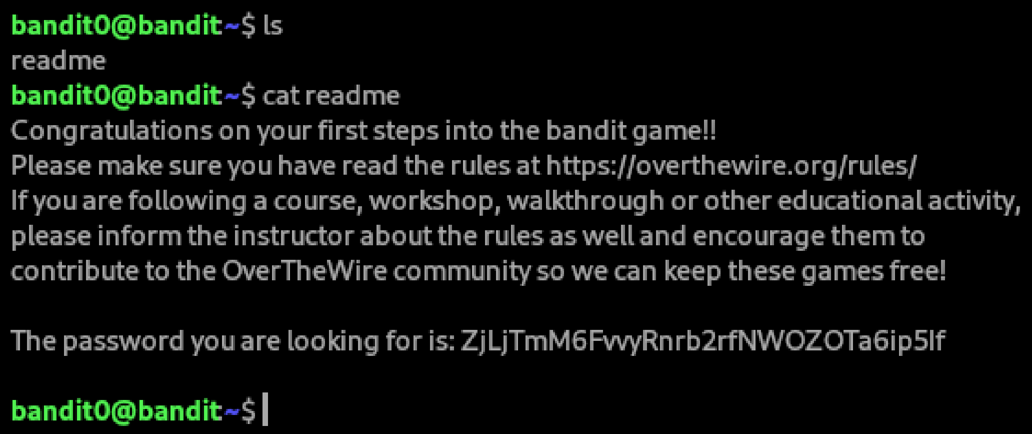
```
C:\Users\Ashique>ssh bandit0@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

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

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!
```

The Password was *bandit0* provided on the website

Username: bandit0@bandit.labs.overthewire.org

Port: 2220

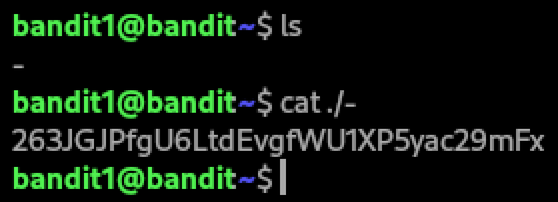
Level 0-1: First Steps



```
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: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

bandit0@bandit~$
```

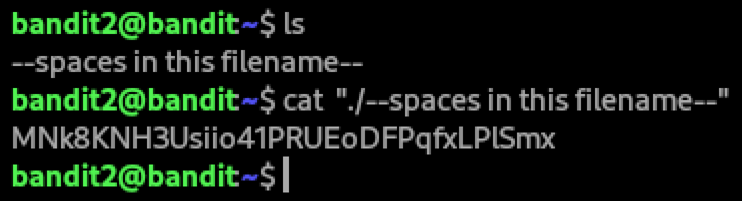
The password was found in the “readme” file

Level 1-2: Capturing Password from the (-) Dash filename



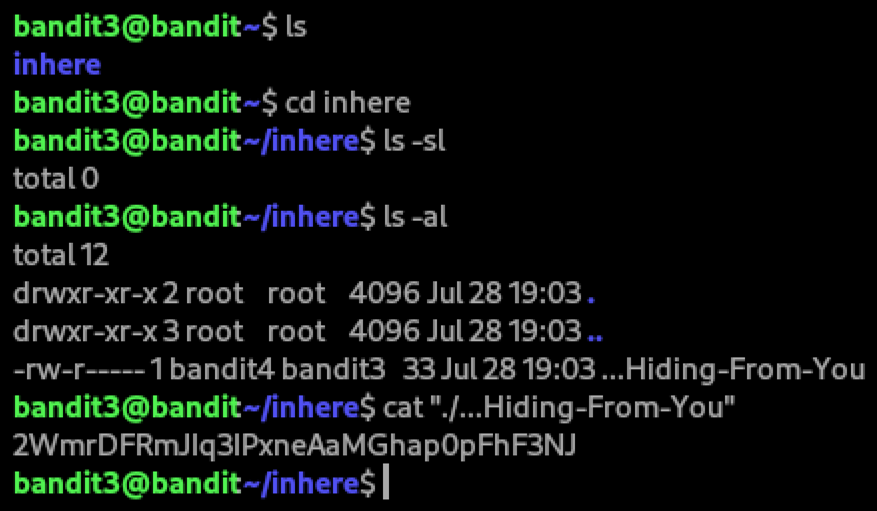
```
bandit1@bandit~$ ls
-
bandit1@bandit~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit~$
```

Level 2-3: -spaces in this filename-



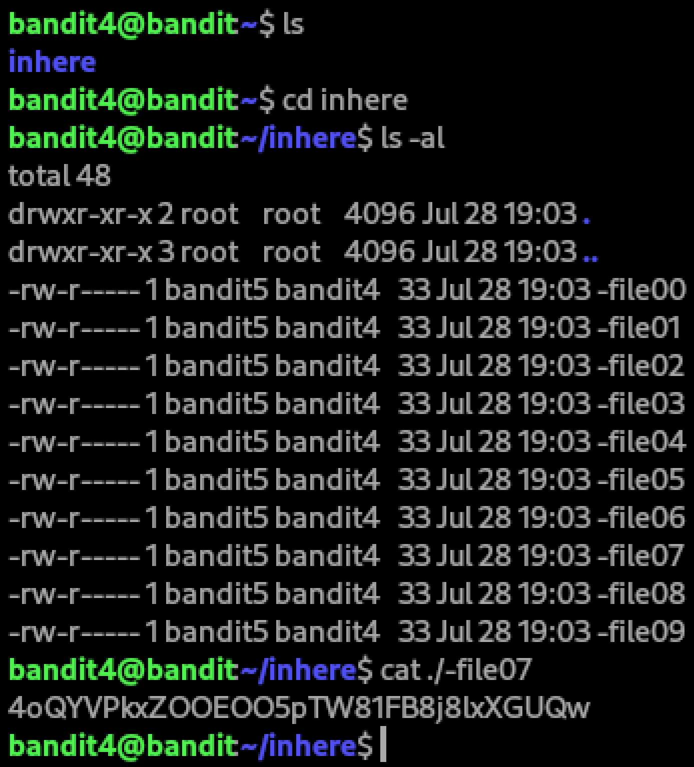
```
bandit2@bandit~$ ls
--spaces in this filename--
bandit2@bandit~$ cat "./--spaces in this filename--"
MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
bandit2@bandit~$
```

Level 3-4: Hidden file in the inhere directory



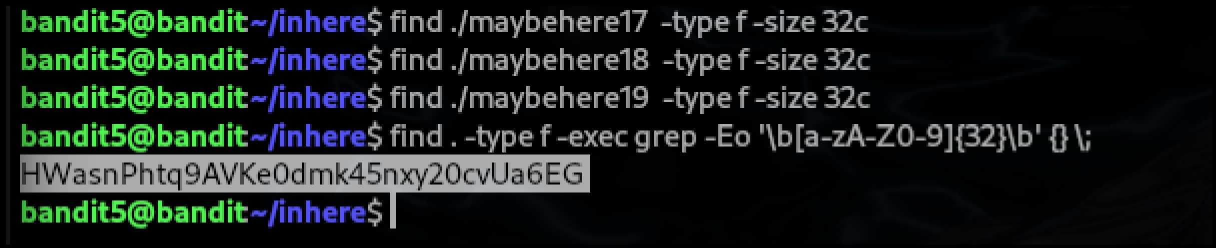
```
bandit3@bandit~$ ls
inhere
bandit3@bandit~$ cd inhere
bandit3@bandit~/inhere$ ls -sl
total 0
bandit3@bandit~/inhere$ ls -al
total 12
drwxr-xr-x 2 root    root    4096 Jul 28 19:03 .
drwxr-xr-x 3 root    root    4096 Jul 28 19:03 ..
-rw-r----- 1 bandit4 bandit3   33 Jul 28 19:03 ...Hiding-From-You
bandit3@bandit~/inhere$ cat "./...Hiding-From-You"
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit~/inhere$ 
```

Level 4-5: Only human-readable file in the inhere directory



```
bandit4@bandit~$ ls
inhere
bandit4@bandit~$ cd inhere
bandit4@bandit~/inhere$ ls -al
total 48
drwxr-xr-x 2 root    root    4096 Jul 28 19:03 .
drwxr-xr-x 3 root    root    4096 Jul 28 19:03 ..
-rw-r----- 1 bandit5 bandit4   33 Jul 28 19:03 -file00
-rw-r----- 1 bandit5 bandit4   33 Jul 28 19:03 -file01
-rw-r----- 1 bandit5 bandit4   33 Jul 28 19:03 -file02
-rw-r----- 1 bandit5 bandit4   33 Jul 28 19:03 -file03
-rw-r----- 1 bandit5 bandit4   33 Jul 28 19:03 -file04
-rw-r----- 1 bandit5 bandit4   33 Jul 28 19:03 -file05
-rw-r----- 1 bandit5 bandit4   33 Jul 28 19:03 -file06
-rw-r----- 1 bandit5 bandit4   33 Jul 28 19:03 -file07
-rw-r----- 1 bandit5 bandit4   33 Jul 28 19:03 -file08
-rw-r----- 1 bandit5 bandit4   33 Jul 28 19:03 -file09
bandit4@bandit~/inhere$ cat ./-file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
bandit4@bandit~/inhere$ 
```

Level 5-6: Hidden in the inhere directory with some properties



```
bandit5@bandit~/inhere$ find ./maybehere17  -type f -size 32c
bandit5@bandit~/inhere$ find ./maybehere18  -type f -size 32c
bandit5@bandit~/inhere$ find ./maybehere19  -type f -size 32c
bandit5@bandit~/inhere$ find . -type f -exec grep -Eo '\b[a-zA-Z0-9]{32}\b' {} \;
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
bandit5@bandit~/inhere$ 
```

Code Explanation:

`find . -type f` = Find files only, not directories

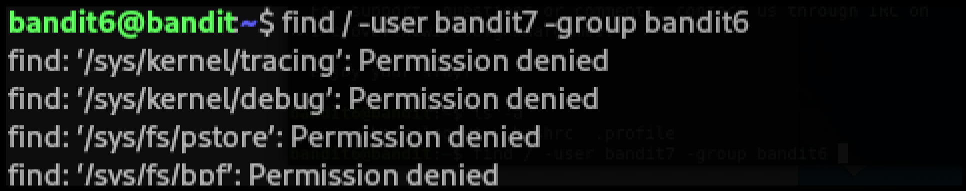
`-exec grep -Eo ‘\b.   .    .    .\b’{}\;` = Execute Command

`grep -Eo ‘\b[a-zA-Z0-9]{32}\b’{}\;` = the command is finding the files that contain capital and small letters, also all decimal numbers.

{32} = The Password of the file will only be 32 characters, noticed earlier

\b’{}\; = Executable closing clause

Level 6-7: somewhere on the server with properties

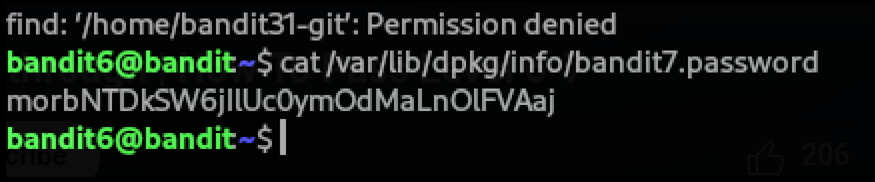


```
bandit6@bandit~$ find / -user bandit7 -group bandit6
find: '/sys/kernel/tracing': Permission denied
find: '/sys/kernel/debug': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/sys/fs/bpf': Permission denied
```

The properties were:

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

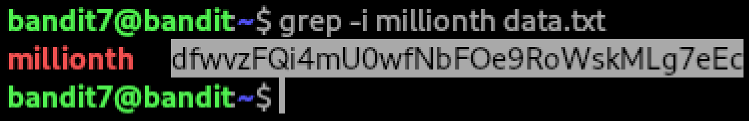
Note: I just noticed that it is 33 bytes in size, so if I add “*-size 33c*” with the command, then it could have found me the exact file.



```
find: '/home/bandit31-git': Permission denied
bandit6@bandit~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit~$
```

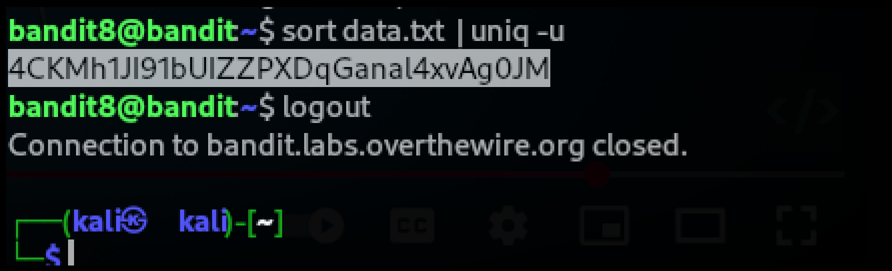
Found the password.

Level 7-8: data.txt next to the word millionth



```
bandit7@bandit~$ grep -i millionth data.txt
millionth    dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit~$
```

Level 8-9: data.txt only line of text is password; others were binary



```
bandit8@bandit~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit~$ logout
Connection to bandit.labs.overthewire.org closed.

┌──(kali㉿ kali)-[~]
└─$ 
```

Code Explanation

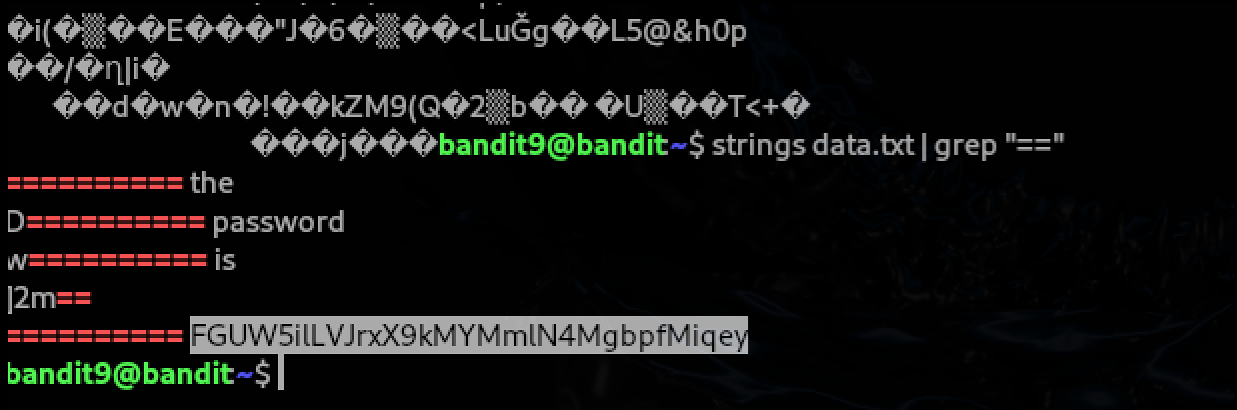
`sort data.txt` = Puts all the lines in lexicographical order

`| uniq` = Removes duplicate lines

`-u` = Print the unique lines

Level 9-10: stored in the file data.txt with conditions.

Conditions were
 -Few human-readable strings
 -Preceeded by several (==) characters



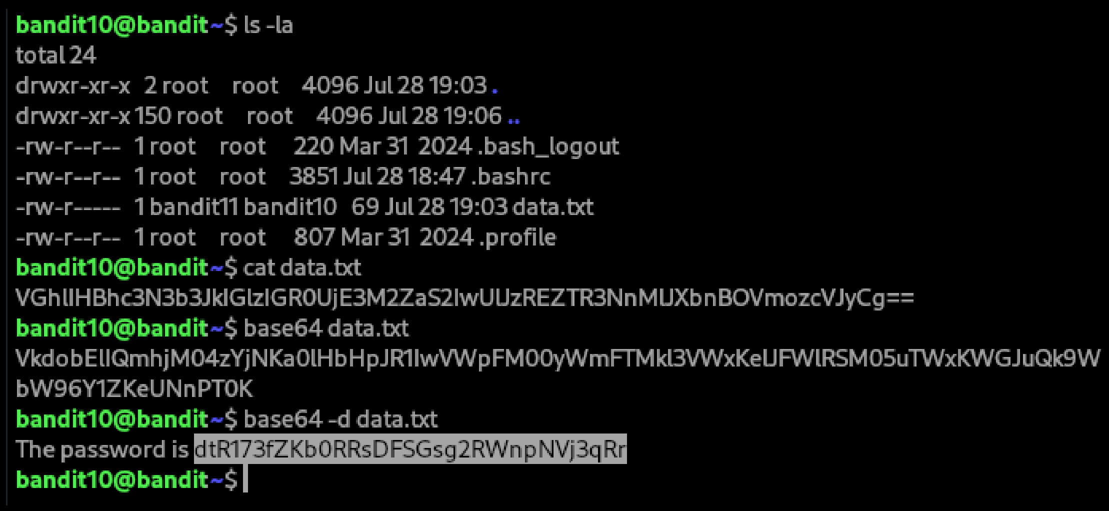
```
�i(�▒��E����"J�6�▒��<LuĞg��L5@&h0p
��/�ɳ|i�
   ��d�w�n�!��kZM9(Q�2▒b�� �U▒��T<+�
                 ���j����bandit9@bandit~$ strings data.txt | grep "=="
=========== the
D=========== password
w=========== is
|2m==
=========== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
bandit9@bandit~$ 
```

Code Explanation

strings data.txt = string only print ASCII strings

| grep”==” = And also find with several (==) Characters\

Level 10-11: Stored in data.txt, which contains base64 encoded data

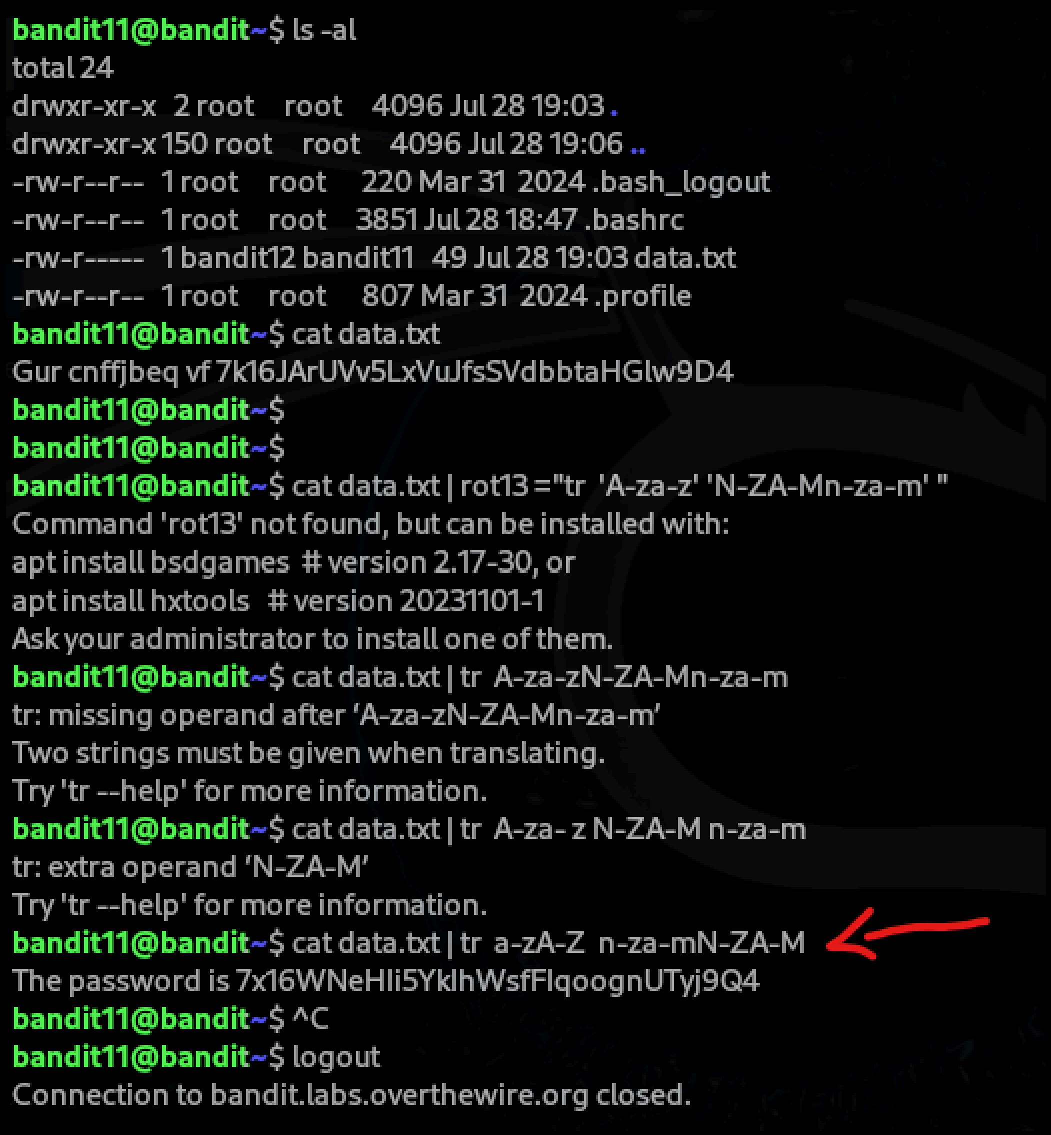


```
bandit10@bandit~$ ls -la
total 24
drwxr-xr-x  2 root    root    4096 Jul 28 19:03 .
drwxr-xr-x 150 root   root    4096 Jul 28 19:06 ..
-rw-r--r--  1 root    root     220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root    root    3851 Jul 28 18:47 .bashrc
-rw-r-----  1 bandit11 bandit10  69 Jul 28 19:03 data.txt
-rw-r--r--  1 root    root     807 Mar 31  2024 .profile
bandit10@bandit~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==
bandit10@bandit~$ base64 data.txt
VkdobElIQmhjM04zYjNKa0lHbHpJR1IwVWpFM00yWmFTMkl3VWxKelJFWlRSM05uTWxKWGJuQk9W
bW96Y1ZKeUNnPT0K
bandit10@bandit~$ base64 -d data.txt
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit~$
```

Code Explanation :

base64 -d data.txt = base64 (-d) decode the file data.txt

Level 11-12: Playing with Rot13



```
bandit11@bandit~$ ls -al
total 24
drwxr-xr-x  2 root    root    4096 Jul 28 19:03 .
drwxr-xr-x 150 root   root    4096 Jul 28 19:06 ..
-rw-r--r--  1 root    root    220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root    root    3851 Jul 28 18:47 .bashrc
-rw-r-----  1 bandit12 bandit11  49 Jul 28 19:03 data.txt
-rw-r--r--  1 root    root    807 Mar 31 2024 .profile
bandit11@bandit~$ cat data.txt
Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGIw9D4
bandit11@bandit~$
bandit11@bandit~$
bandit11@bandit~$ cat data.txt | rot13 ="tr  'A-za-z' 'N-ZA-Mn-za-m' "
Command 'rot13' not found, but can be installed with:
apt install bsdgames  # version 2.17-30, or
apt install hxtools  # version 20231101-1
Ask your administrator to install one of them.
bandit11@bandit~$ cat data.txt | tr  A-za-zN-ZA-Mn-za-m
tr: missing operand after ‘A-za-zN-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-M n-za-m
tr: extra operand ‘N-ZA-M’
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~$ ^C
bandit11@bandit~$ logout
Connection to bandit.labs.overthewire.org closed.
```

Code Explanation

`cat data.txt` = Reads data.txt

`| tr a-zA-Z n-za-mN-ZA-M` = Translate the rot13 combination