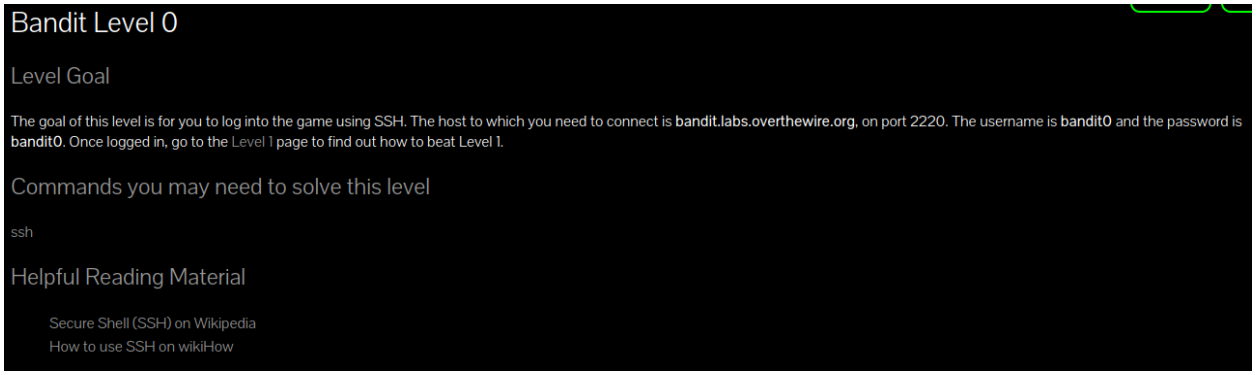
OverTheWire Wargames
Bandit

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.

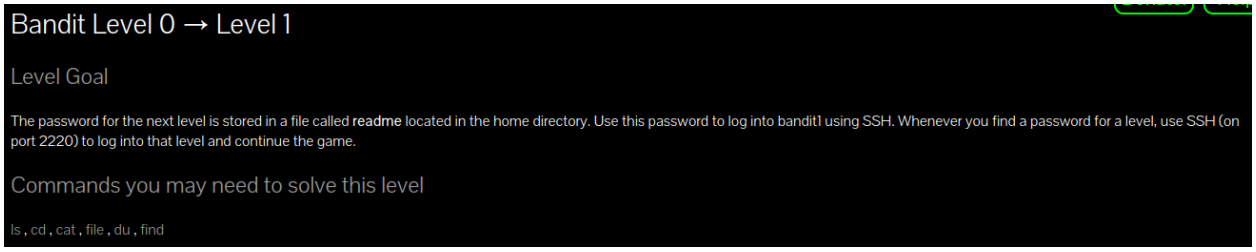


SSH is an encrypted communication that uses TCP/22.

```
ssh bandit0@bandit.labs.overthewire.org -p2220
```

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.



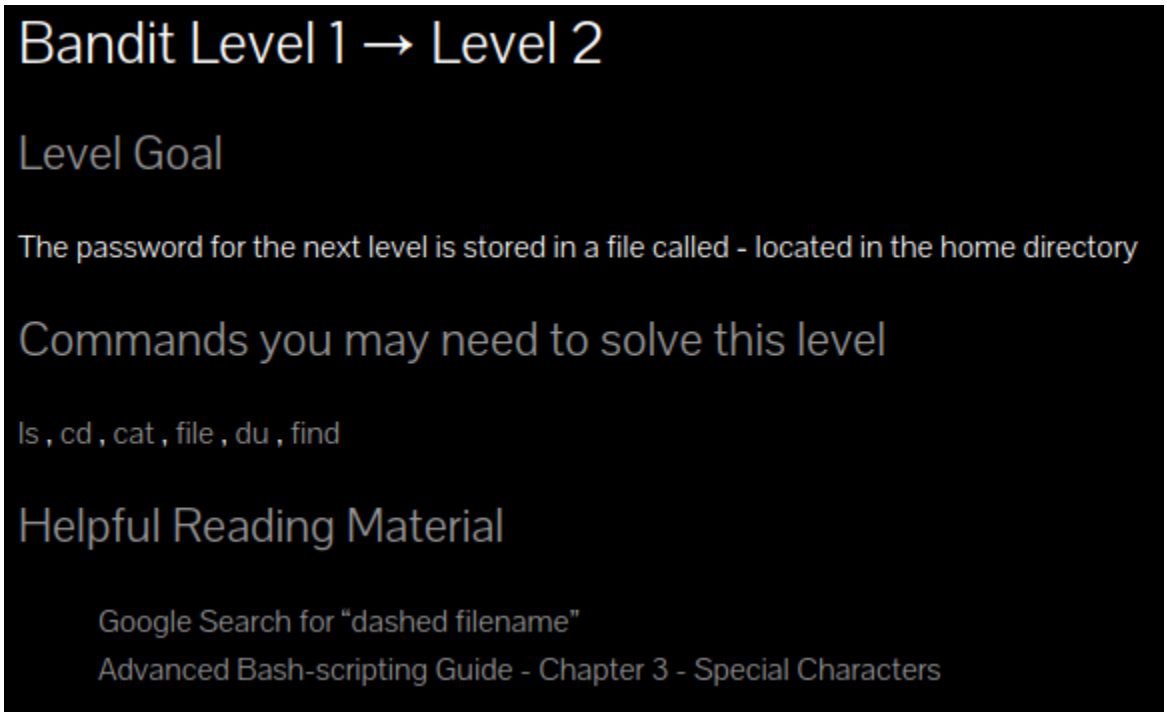
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

Use this ASCII text as a password for level 1 - level 2.

```
ssh bandit1@bandit.labs.overthewire.org -p2220
```

Level 1 - Level 2:

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



https://www.webservertalk.com/dashed-filename

The link above briefly explained the dashed in filename.

Use ls command to list out the files in the home directory.

cat < <-filename>

cat < -

Or

cat ./<-filename>

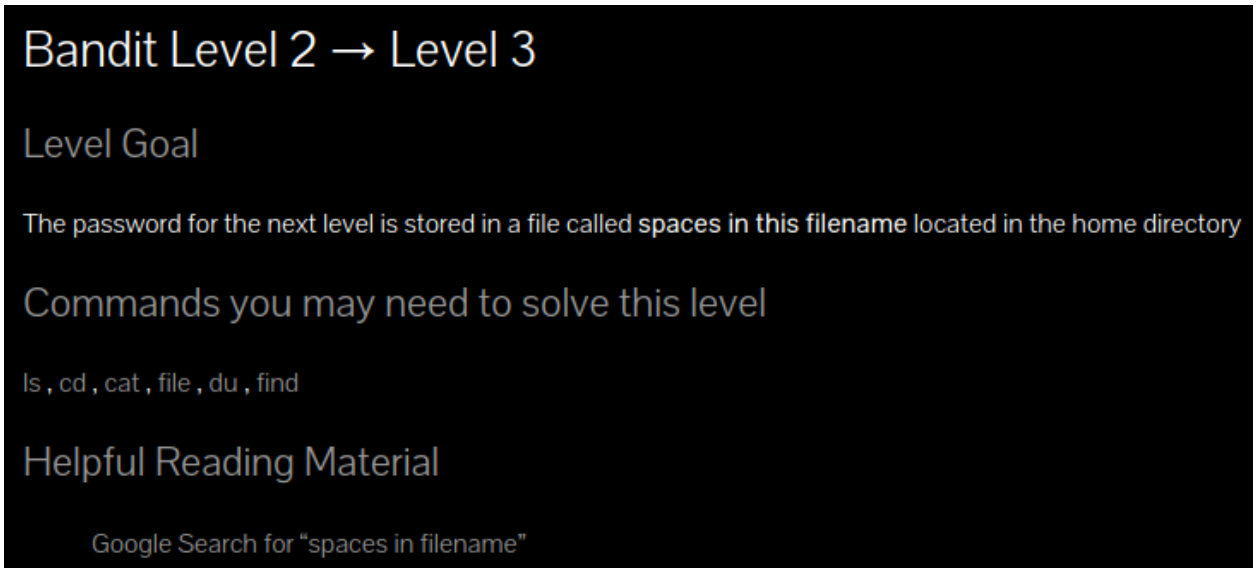
cat ./-

rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

Level 2 - Level 3:

ssh bandit2@bandit.labs.overthewire.org -p 2220

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



ls command to list the files

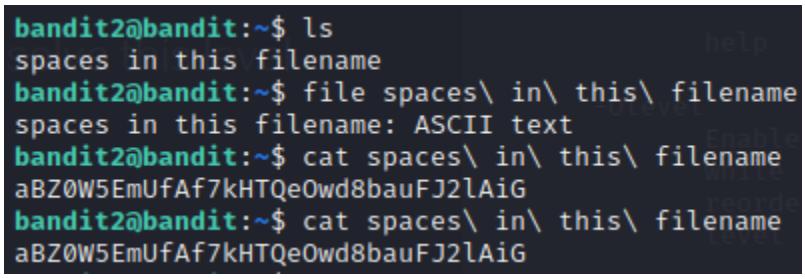
spaces in this filename

To concatenate the file use backslash before the spaces

cat spaces\ in\ this\ filename

The cat command displays the content of a file.

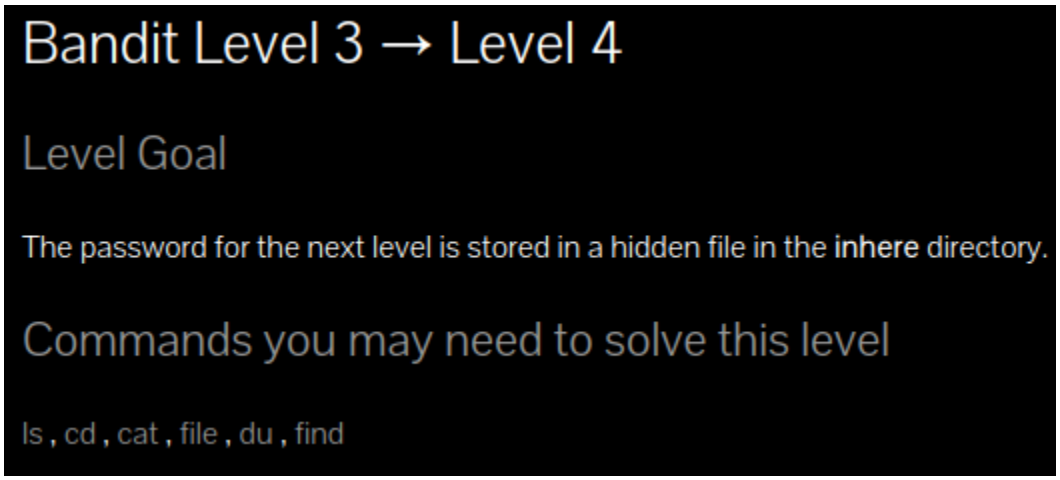
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG



Level 3 - Level 4:

ssh bandit3@bandit.labs.overthewire.org -p 2220

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

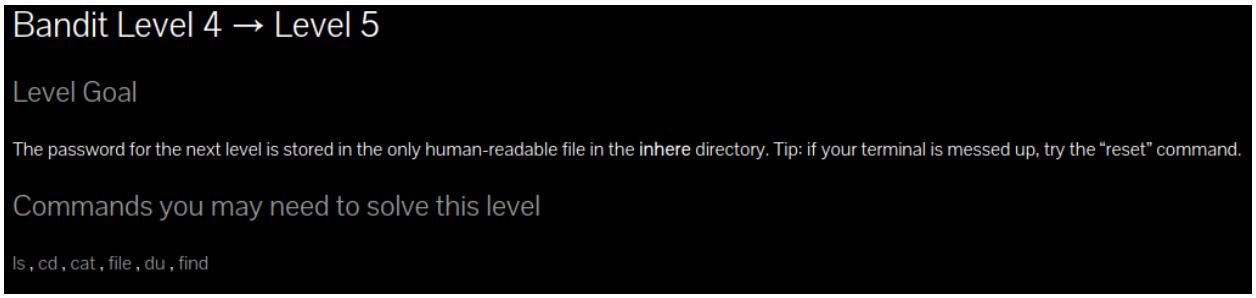


Use the find command to find the hidden files in inhere directory.
find command is the most flexible and powerful search tool.
cd inhere
find
.
./.hidden
cat ./.hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ file inhere/
inhere/: directory
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -l
total 0
bandit3@bandit:~/inhere$ find
.
./.hidden
bandit3@bandit:~/inhere$ file ./.hidden
./.hidden: ASCII text
bandit3@bandit:~/inhere$ cat ./.hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$
```

Level 4 - Level 5:
ssh bandit4@bandit.labs.overthewire.org -p 2220

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.



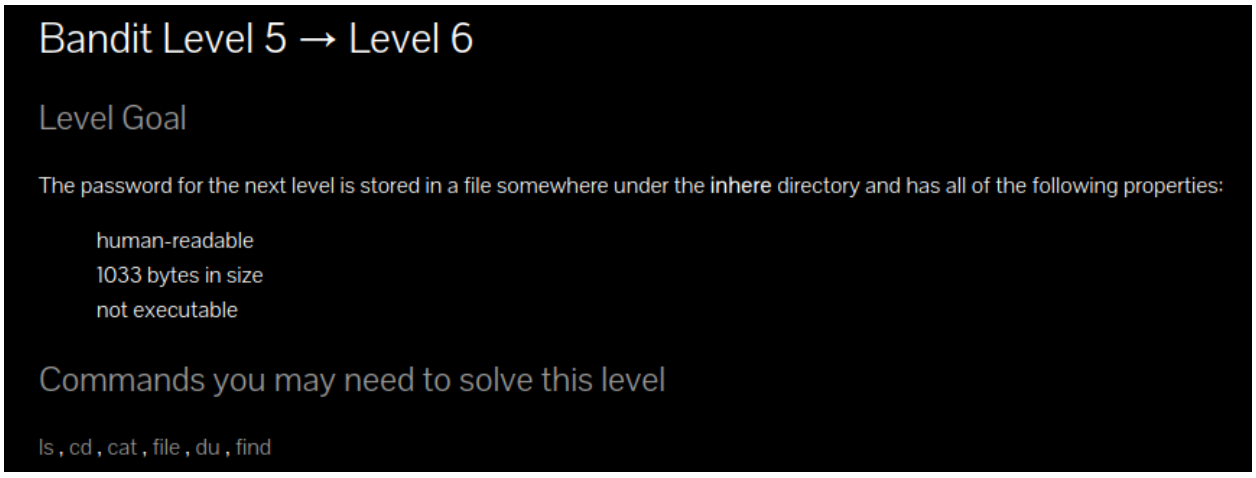
Use `file ./*` to get all file types in the current directory or use loop, idk how to use loop in bash.

```
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$ file ./*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
```

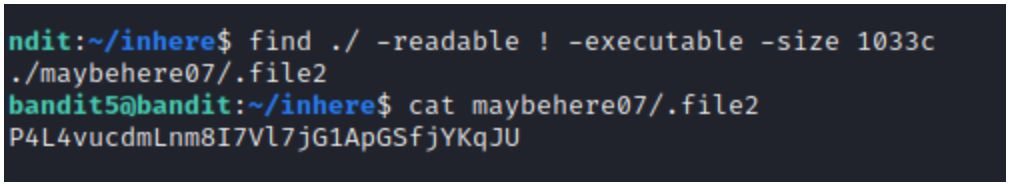
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

Bandit level 5 - 6

ssh bandit5@bandit.labs.overthewire.org -p 2220

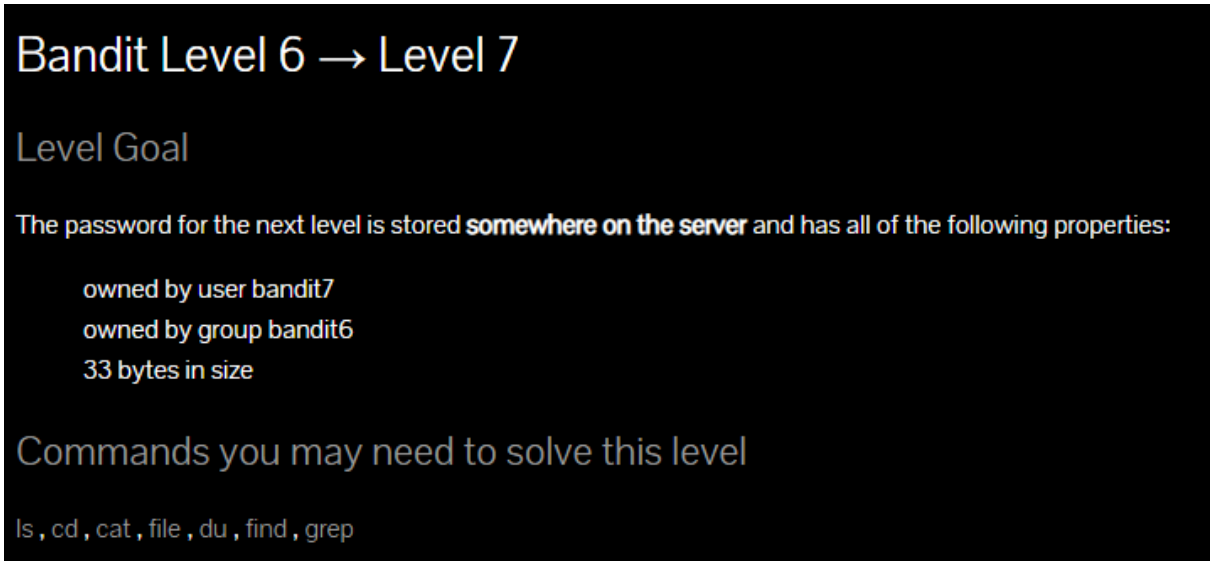


use the properties to solve this problem



-readable = file is readable
! -executable = the file is not executable
-size 1033c = 1033 bytes in size
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

Level 6 - Level 7 to login
`ssh bandit6@bandit.labs.overthewire.org -p2220`
`Password:` P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU



To search by the user we use -user, -group to show the owner of the group, and -size to search the size.

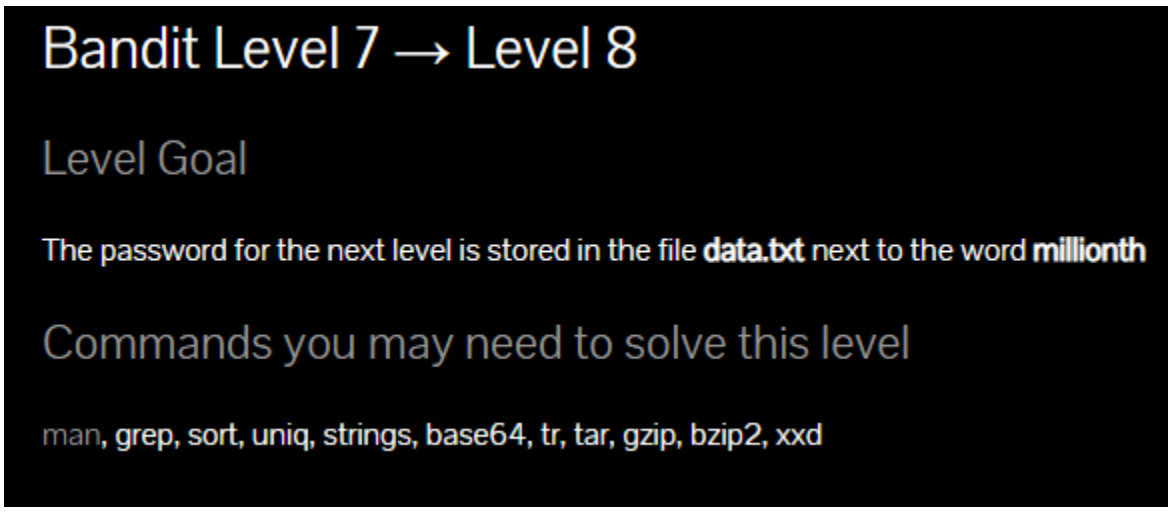
find / -group bandit6 -user bandit7 -size 33c | grep password
Or
find / -group bandit6 -user bandit7 -size 33c 2>/dev/null
To remove the permission denied messages

It outputs the path of our password /var/lib/dpkg/info/bandit7.password

Move to the directory by using cd /var/lib/dpkg/info/ then cat the file OR cat /var/lib/dpkg/info/bandit7.password

It displays the password for our next level:
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

Level 7 - 8
ssh bandit7@bandit.labs.overthewire.org -p 2220

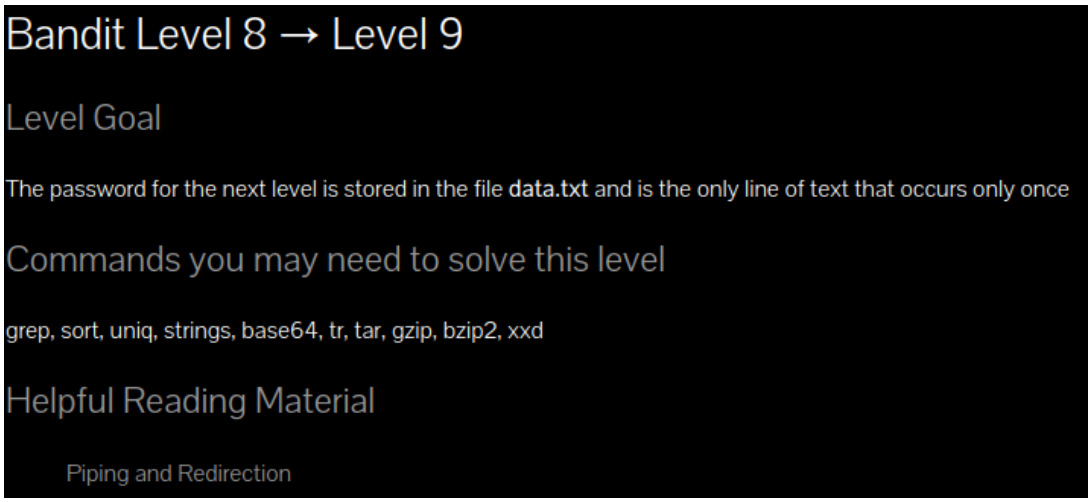


In this level, I used grep to filter the **millionth.** Grep is a powerful tool for filtering, you can use other tools to retrieve the password.

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ cat data.txt | grep millionth
millionth       TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@bandit:~$
```

TESKZC0XvTetK0S9xNwm25STk5iWrBvP

Level 8 - 9



Use sort and uniq command

```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ less data.txt
bandit8@bandit:~$ man sort
bandit8@bandit:~$ man uniq
bandit8@bandit:~$ man sort
bandit8@bandit:~$ sort data.txt | uniq -u
EN632PlfYiZbn3PhVK3XOGSlNInNE00t
bandit8@bandit:~$ man sort
bandit8@bandit:~$ exit
logout
```

EN632PlfYiZbn3PhVK3XOGSlNInNE00t

Level 9 - 10

Bandit Level 9 → Level 10

Level Goal

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.

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

Use strings command and grep to filter the '=' characters

```
bandit9@bandit:~$ strings data.txt | grep ====
f========== theM
========== password
========== is
========== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
```

G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

Level 10 - 11

Bandit Level 10 → Level 11

Level Goal

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

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

Helpful Reading Material

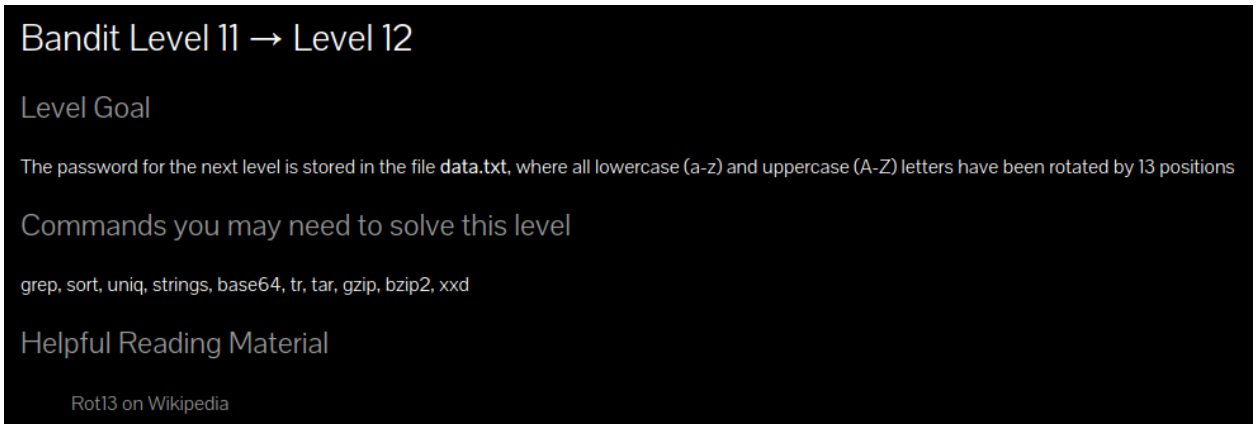
Base64 on Wikipedia

Use base64 command, -d to decode the base64 data

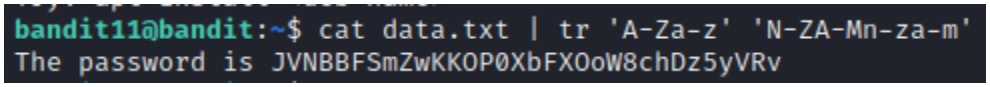
```
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTllGTmI2blZDS3pwaGxYSEJNCg==
bandit10@bandit:~$ cat data.txt | base64 -d
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$ man base64
bandit10@bandit:~$ echo 'VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTllGTmI2blZDS3pwaGxYSEJNCg==' | base64 -d
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
```

6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

Level 11 - 12



Use tr to translate the data



JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

Level 12 - 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 using mkdir. For example: mkdir /tmp/myname123. Then copy the datafile using cp, and rename it using mv (read the manpages!)

Use file to identify what file to decompress
Rename it to specific file extension to decompress it.
gzip - .gz
bzip2 .bz
tar - .tar

gzip -d <filename> to decompress gzip compressed data
bzip2 -d <filename> to decompress bzip compressed data
tar -xf <filename to decompress tar file