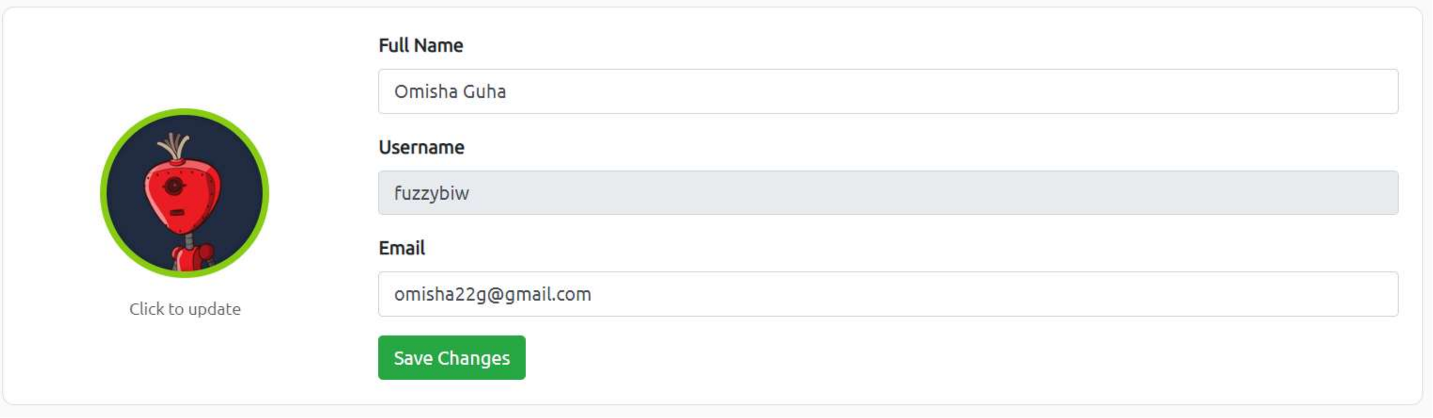
Cryptonite JTP Task 2 (Week 1) Write-ups

Omisha Guha

12/12/2022

- Made an account on TryHackMe



Full Name

Omisha Guha

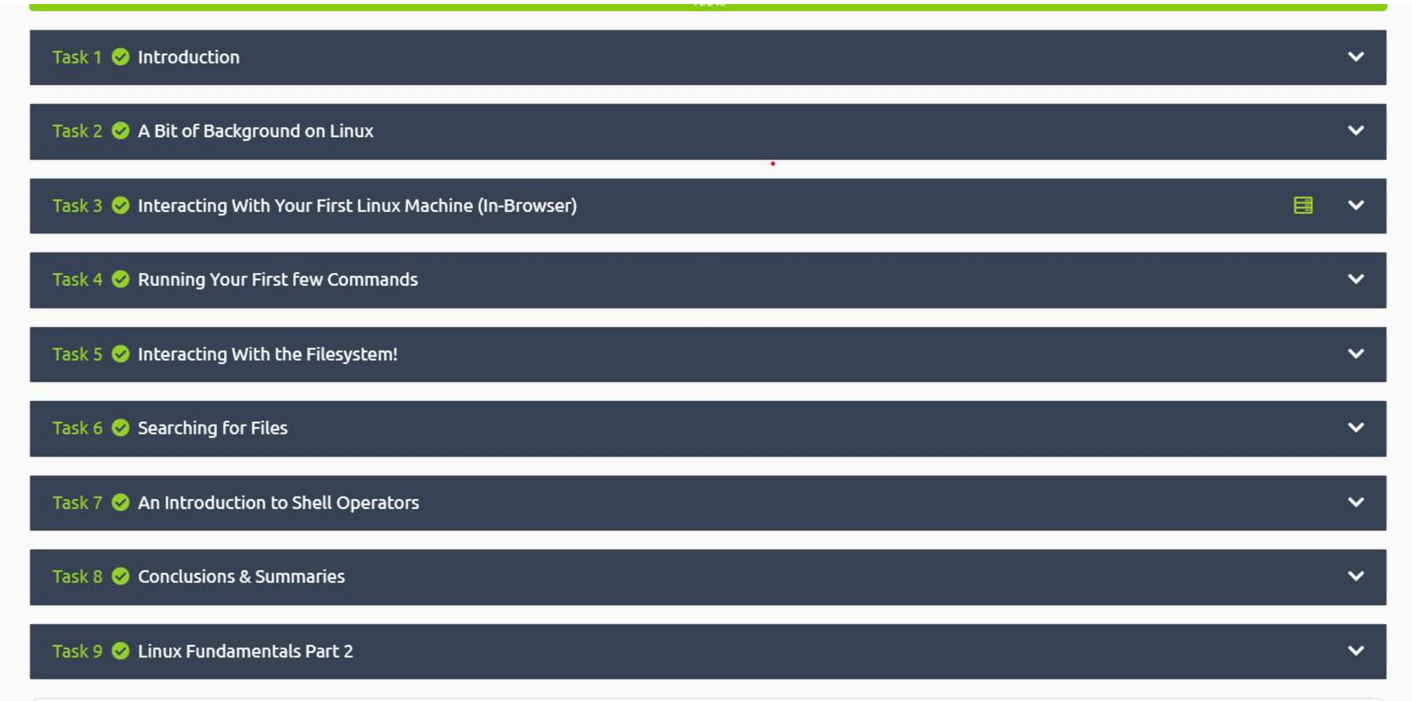
Username

fuzzybiw

Email

omisha22g@gmail.com

- Did basic Linux commands from THM Linux fundamentals 1 –



Task 1 ✓ Introduction

Task 2 ✓ A Bit of Background on Linux

Task 3 ✓ Interacting With Your First Linux Machine (In-Browser)

Task 4 ✓ Running Your First few Commands

Task 5 ✓ Interacting With the Filesystem!

Task 6 ✓ Searching for Files

Task 7 ✓ An Introduction to Shell Operators

Task 8 ✓ Conclusions & Summaries

Task 9 ✓ Linux Fundamentals Part 2

ls- **used in listing contents inside a directory**,

cd- **change directory command**,

echo- **used to display line of text/string that are passed as an argument**,

Whoami- **see the currently logged-in user**, pwd- **the full path name of your current directory (from the root directory),**

grep- **searching plain-text data sets for lines that match the given text,**

find- **to find a particular file within a directory,**

cat- **reads contents of file and gives their content as output,**

wc- **used for counting purpose.**

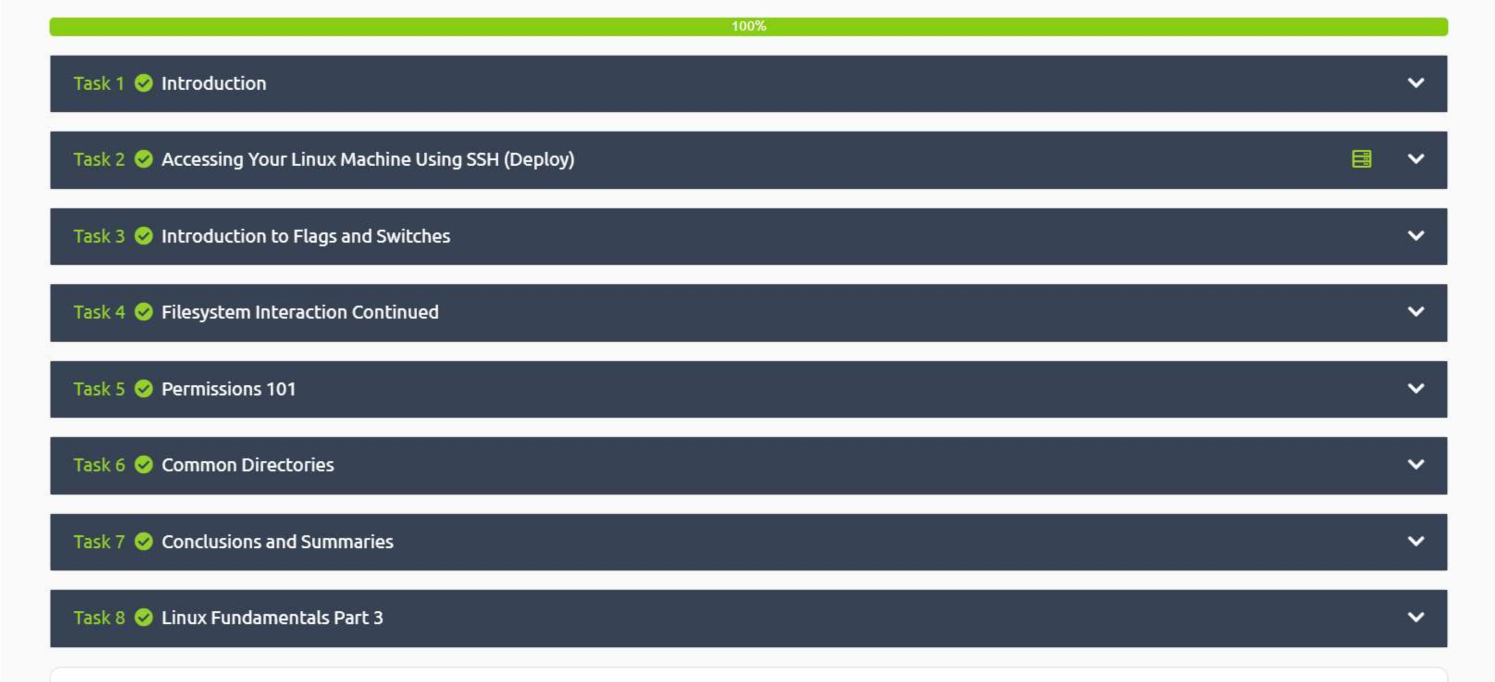
&,

&&,

>,

>> operators

- Did THM Linux fundamentals 2-



100%

Task 1 Introduction

Task 2 Accessing Your Linux Machine Using SSH (Deploy)

Task 3 Introduction to Flags and Switches

Task 4 Filesystem Interaction Continued

Task 5 Permissions 101

Task 6 Common Directories

Task 7 Conclusions and Summaries

Task 8 Linux Fundamentals Part 3

Ssh-protocol used to securely connect to a remote server/system,

flags (ls-a, etc),

man - display the user manual of any command,

touch- used to create empty files,

mkdir – make directory,

cp - copying files and directories,

mv - moves one or more files or directories, rm - remove,

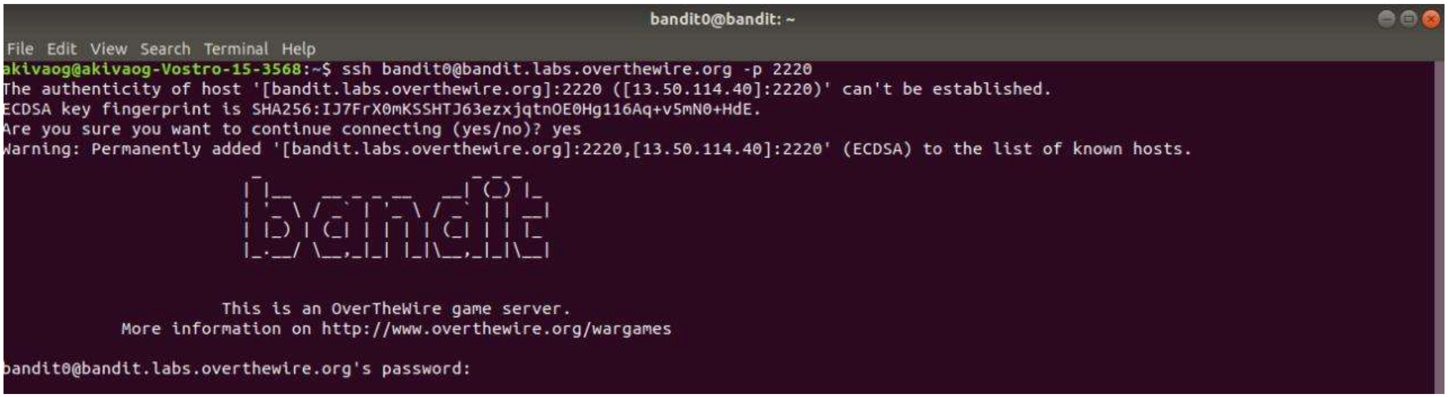
file- helps determine the type of a file and its data

Permissions(rwx),

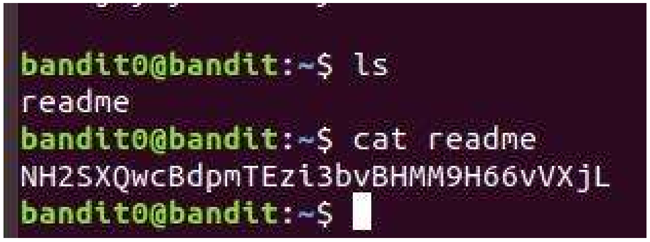
su- switch user,

and common directories.

- I went to Over The Wire website and started level 0 of bandit.



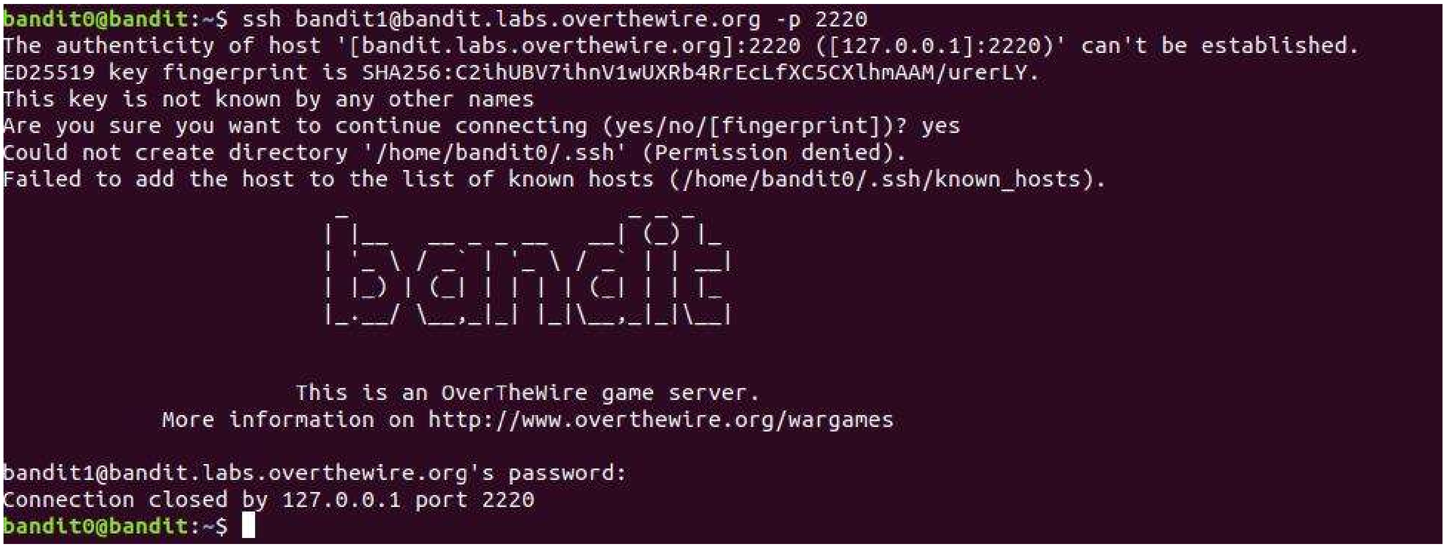
```
akivaog@akivaog-Vostro-15-3568:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([13.50.114.40]:2220)' can't be established.
ECDSA key fingerprint is SHA256:IJ7FrX0mKSSHTJ63ezxjqtnOE0Hg116Aq+v5mN0+HdE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[13.50.114.40]:2220' (ECDSA) to the list of known hosts.
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

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



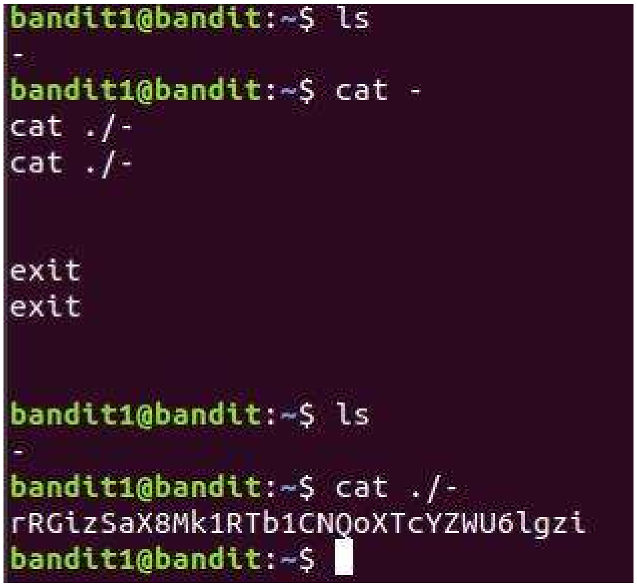
```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
bandit0@bandit:~$
```

Use ssh command to log into game, then ls so that we can see what is in the directory, open readme using cat command it contains the password of level 1.

- Then with the password from level 0 logged in to level 1;



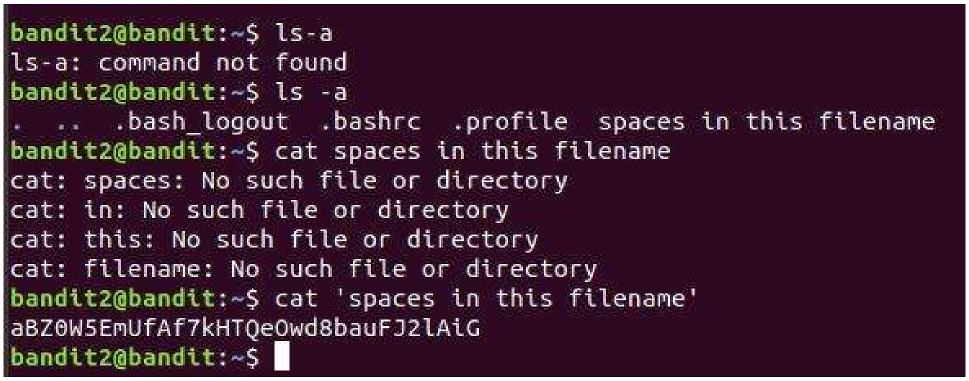
```
bandit0@bandit:~$ ssh bandit1@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit0/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit0/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit1@bandit.labs.overthewire.org's password:
Connection closed by 127.0.0.1 port 2220
bandit0@bandit:~$
```



```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat -
cat ./-
cat ./-


exit
exit


bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit1@bandit:~$ 
```

Use ls to see what is in directory, cat – does not work 😿, used ctrl+d to get out of cat, then used google to see how it is written. ./- had the password.

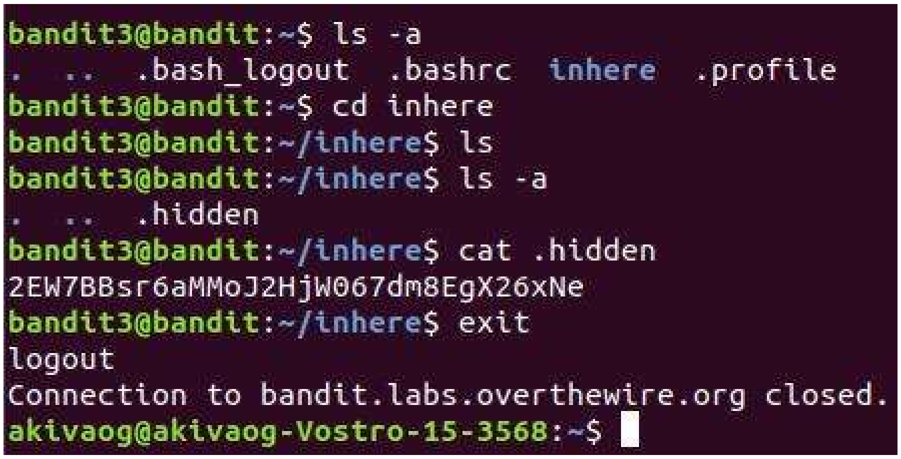
- Then with the password from level 1 to level 2 using ssh to log in.



```
bandit2@bandit:~$ ls-a
ls-a: command not found
bandit2@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  .profile  spaces in this filename
bandit2@bandit:~$ cat spaces in this filename
cat: spaces: No such file or directory
cat: in: No such file or directory
cat: this: No such file or directory
cat: filename: No such file or directory
bandit2@bandit:~$ cat 'spaces in this filename'
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
bandit2@bandit:~$ 
```

Used ls –a to see all files as given instructions opened the ‘spaces in this filename’ using cat command which has password for level 3.

- Then with the password from level 2 to level 3 using ssh to log in.

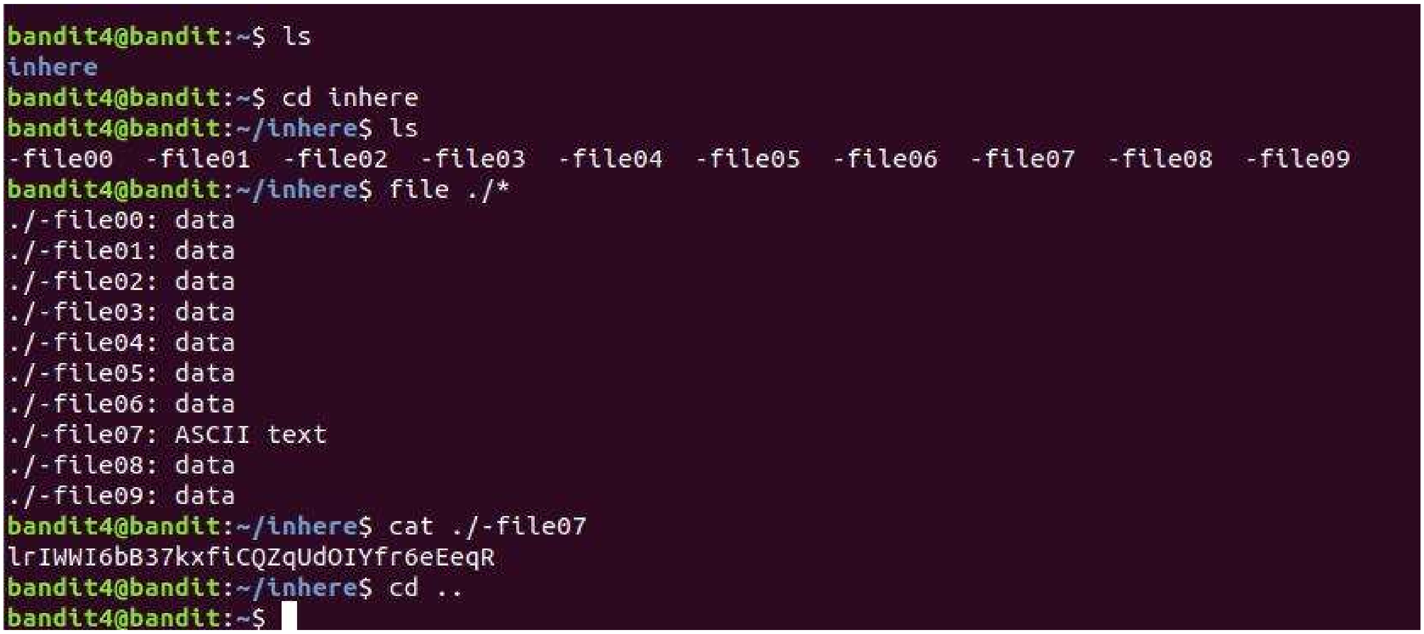


```
bandit3@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  inhere  .profile
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
akivaog@akivaog-Vostro-15-3568:~$ 
```

ls-a to see all files even hidden ones and then open the hidden file to get password for level 4.

- Then with the password from level 3 to level 4 using ssh to log in.

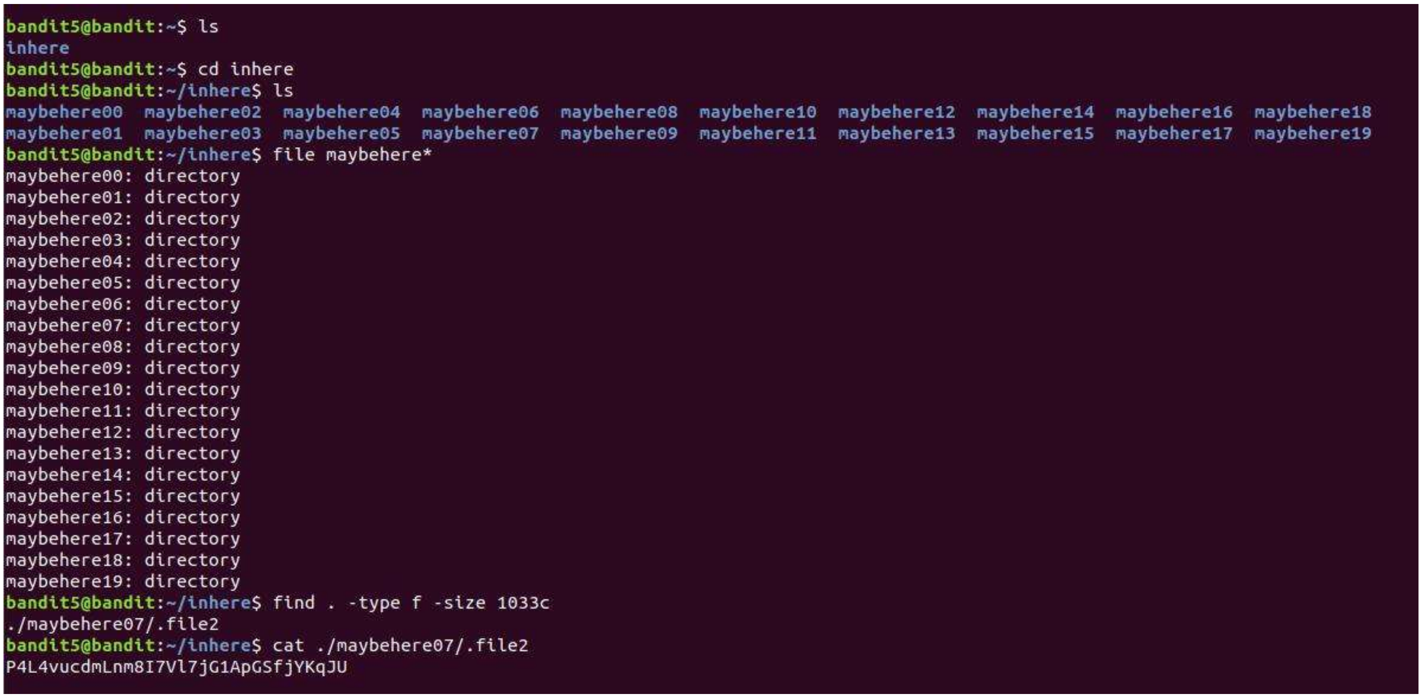
Ls to view files and directories then, cd inhere to enter directory, use (file. /*) (searched from internet) to see which file is ASCII text it is -file07 open file using cat to get password for the next level.



```
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
bandit4@bandit:~/inhere$ cd ..
bandit4@bandit:~$ 
```

13/12/2022

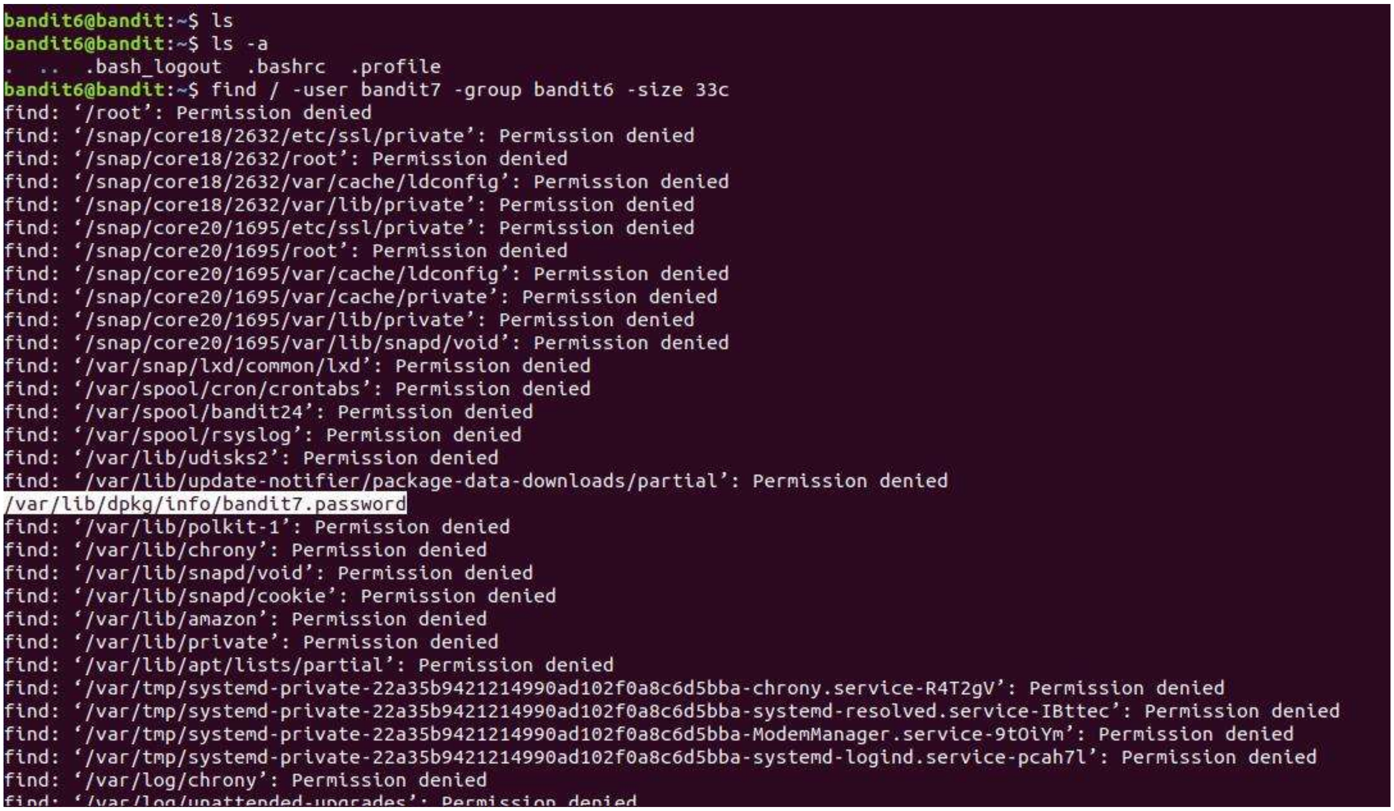
- Took the password from level 4 to log into level 5.



```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere02  maybehere04  maybehere06  maybehere08  maybehere10  maybehere12  maybehere14  maybehere16  maybehere18
maybehere01  maybehere03  maybehere05  maybehere07  maybehere09  maybehere11  maybehere13  maybehere15  maybehere17  maybehere19
bandit5@bandit:~/inhere$ file maybehere*
maybehere00: directory
maybehere01: directory
maybehere02: directory
maybehere03: directory
maybehere04: directory
maybehere05: directory
maybehere06: directory
maybehere07: directory
maybehere08: directory
maybehere09: directory
maybehere10: directory
maybehere11: directory
maybehere12: directory
maybehere13: directory
maybehere14: directory
maybehere15: directory
maybehere16: directory
maybehere17: directory
maybehere18: directory
maybehere19: directory
bandit5@bandit:~/inhere$ find . -type f -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

On this level the inhere directory had 20 more directories inside it, so I had to use the find command to find which of the directories had a file of size 1033.

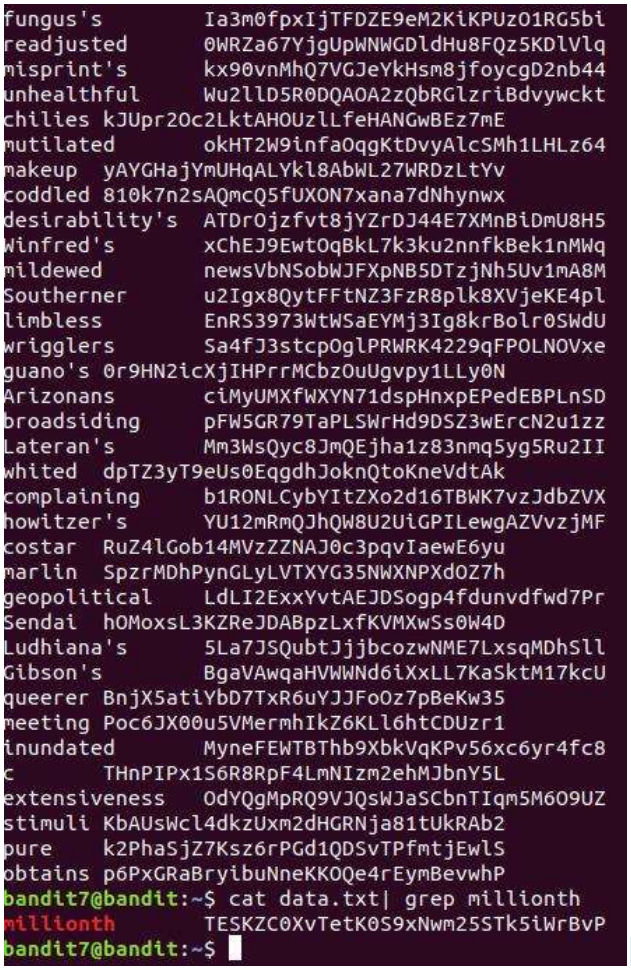
- Used the password found in level 5 to log into level 6.



```
bandit6@bandit:~$ ls
bandit6@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  .profile
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c
find: ‘/root’: Permission denied
find: ‘/snap/core18/2632/etc/ssl/private’: Permission denied
find: ‘/snap/core18/2632/root’: Permission denied
find: ‘/snap/core18/2632/var/cache/ldconfig’: Permission denied
find: ‘/snap/core18/2632/var/lib/private’: Permission denied
find: ‘/snap/core20/1695/etc/ssl/private’: Permission denied
find: ‘/snap/core20/1695/root’: Permission denied
find: ‘/snap/core20/1695/var/cache/ldconfig’: Permission denied
find: ‘/snap/core20/1695/var/cache/private’: Permission denied
find: ‘/snap/core20/1695/var/lib/private’: Permission denied
find: ‘/snap/core20/1695/var/lib/snapd/void’: Permission denied
find: ‘/var/snap/lxd/common/lxd’: Permission denied
find: ‘/var/spool/cron/crontabs’: Permission denied
find: ‘/var/spool/bandit24’: Permission denied
find: ‘/var/spool/rsyslog’: Permission denied
find: ‘/var/lib/udisks2’: Permission denied
find: ‘/var/lib/update-notifier/package-data-downloads/partial’: Permission denied
/var/lib/dpkg/info/bandit7.password
find: ‘/var/lib/polkit-1’: Permission denied
find: ‘/var/lib/chrony’: Permission denied
find: ‘/var/lib/snapd/void’: Permission denied
find: ‘/var/lib/snapd/cookie’: Permission denied
find: ‘/var/lib/amazon’: Permission denied
find: ‘/var/lib/private’: Permission denied
find: ‘/var/lib/apt/lists/partial’: Permission denied
find: ‘/var/tmp/systemd-private-22a35b9421214990ad102f0a8c6d5bba-chrony.service-R4T2gV’: Permission denied
find: ‘/var/tmp/systemd-private-22a35b9421214990ad102f0a8c6d5bba-systemd-resolved.service-IBttec’: Permission denied
find: ‘/var/tmp/systemd-private-22a35b9421214990ad102f0a8c6d5bba-ModemManager.service-9tOiYm’: Permission denied
find: ‘/var/tmp/systemd-private-22a35b9421214990ad102f0a8c6d5bba-systemd-logind.service-pcah7l’: Permission denied
find: ‘/var/log/chrony’: Permission denied
find: ‘/var/log/unattended-upgrades’: Permission denied
```

In level 6 I used the find command to search the whole directory to search for the file with the specifications in the prompt after the file is found cat to open it and get the password.

- Use the password to get into level 7.



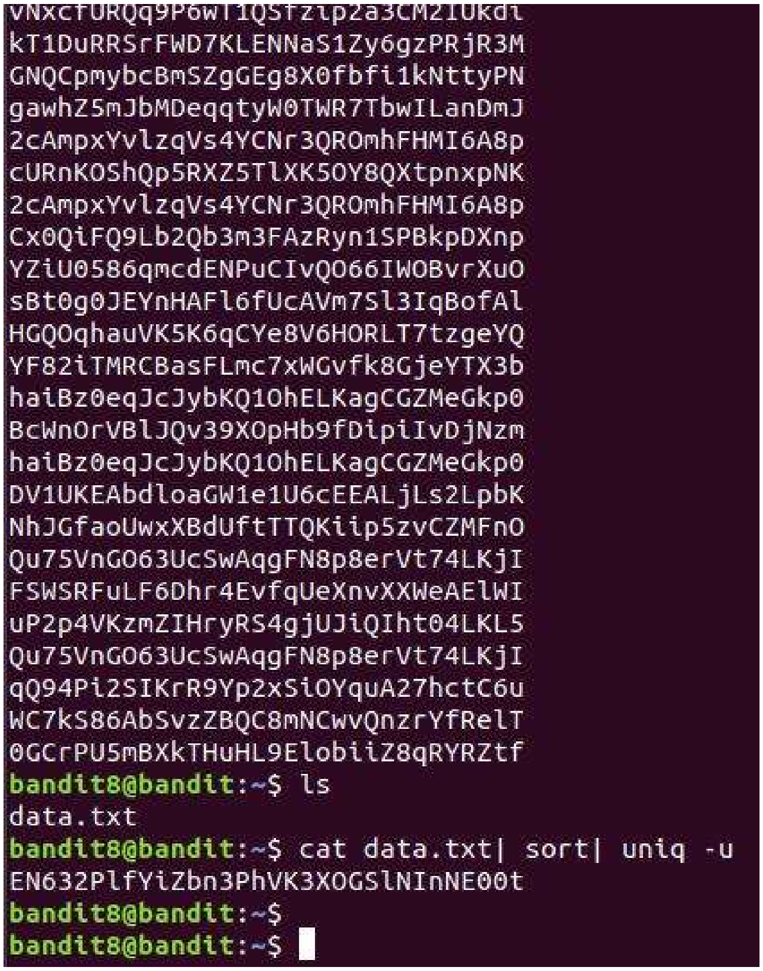
```
fungus's        Ia3m0fpxIjTFDZE9eM2KiKPUzO1RG5bi
readjusted      0WRZa67YjgUpWNWGDldHu8FQz5KDlVlq
misprint's      kx90vnMhQ7VGJeYkHsm8jfoycgD2nb44
unhealthful     Wu2llD5R0DQAOA2zQbRGlzriBdvywckt
chilies kJUpr2Oc2LktAHOUzlLfeHANGwBEz7mE
mutilated       okHT2W9infaOqgKtDvyAlcSMh1LHLz64
makeup  yAYGHajYmUHqALYkl8AbWL27WRDzLtYv
coddled 810k7n2sAQmcQ5fUXON7xana7dNhynwx
desirability's  ATDrOjzfvt8jYZrDJ44E7XMnBiDmU8H5
Winfred's       xChEJ9EwtOqBkL7k3ku2nnfkBek1nMWq
mildewed        newsVbNSobWJFXpNB5DTzjNh5Uv1mA8M
Southerner      u2Igx8QytFFtNZ3FzR8plk8XVjeKE4pl
limbless        EnRS3973WtWSaEYMj3Ig8krBolr0SWdU
wrigglers       Sa4fJ3stcpOglPRWRK4229qFPOLNOVxe
guano's 0r9HN2icXjIHPrrMCbzOuUgvpy1LLy0N
Arizonans       ciMyUMXfWXYN71dspHnxpEPedEBPLnSD
broadsiding     pFW5GR79TaPLSWrHd9DSZ3wErcN2u1zz
Lateran's       Mm3WsQyc8JmQEjha1z83nmq5yg5Ru2II
whited  dpTZ3yT9eUs0EqgdhJoknQtoKneVdtAk
complaining     b1RONLCybYItZXo2d16TBWK7vzJdbZVX
howitzer's      YU12mRmQJhQW8U2UiGPILewgAZVvzjMF
costar  RuZ4lGob14MVzZZNAJ0c3pqvIaewE6yu
marlin  SpzrMDhPynGLyLVTXYG35NWXNPXdOZ7h
geopolitical    LdLI2ExxYvtAEJDSogp4fdunvdfwd7Pr
Sendai  hOMoxsL3KZReJDABpzLxfKVMXwSs0W4D
Ludhiana's      5La7JSQubtJjjbcozwNME7LxsqMDhSll
Gibson's        BgaVAwqaHVWWNd6iXxLL7KaSktM17kcU
queerer BnjX5atiYbD7TxR6uYJJFoOz7pBeKw35
meeting Poc6JX00u5VMermhIkZ6KLl6htCDUzr1
inundated       MyneFEWTBThb9XbkVqKPv56xc6yr4fc8
c       THnPIPx1S6R8RpF4LmNIzm2ehMJbnY5L
extensiveness   OdYQgMpRQ9VJQsWJaSCbnTIqm5M6O9UZ
stimuli KbAUsWcl4dkzUxm2dHGRNja81tUkRAb2
pure    k2PhaSjZ7Ksz6rPGd1QDSvTPfmtjEwlS
obtains p6PxGRaBryibuNneKKOQe4rEymBevwhP
bandit7@bandit:~$ cat data.txt| grep millionth
millionth       TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@bandit:~$ 
```

Piping- passing information from one program process or command to another

Messed up my whole terminal using cat

Use cat data.txt piped with grep command to find the password.

- Use password to log into level 8



```
vNxcfURQq9P6wT1QSfzip2a3CM2lUkdi
kT1DuRRSrFWD7KLENNaS1Zy6gzPRjR3M
GNQCpmybcBmSZgGEg8X0fbfi1kNttyPN
gawhZ5mJbMDeqqtyW0TWR7TbwILanDmJ
2cAmpxYvlzqVs4YCNr3QROmhFHMI6A8p
cURnKOShQp5RXZ5TlXK5OY8QXtpnxpNK
2cAmpxYvlzqVs4YCNr3QROmhFHMI6A8p
Cx0QiFQ9Lb2Qb3m3FAzRyn1SPBkpDXnp
YZiU0586qmcdENPuCIvQO66IWOBvrXuO
sBt0g0JEYnHAFl6fUcAVm7Sl3IqBofAl
HGQOqhauVK5K6qCYe8V6HORLT7tzgeYQ
YF82iTMRCBasFLmc7xWGvfk8GjeYTX3b
haiBz0eqJcJybKQ1OhELKagCGZMeGkp0
BcWnOrVBlJQv39XOpHb9fDipiIvDjNzm
haiBz0eqJcJybKQ1OhELKagCGZMeGkp0
DV1UKEAbdloaGW1e1U6cEEALjLs2LpbK
NhJGfaoUwxXBdUftTTQKiip5zvCZMFnO
Qu75VnGO63UcSwAqgFN8p8erVt74LKjI
FSWSRFuLF6Dhr4EvfqUeXnvXXWeAElWI
uP2p4VKzmZIHryRS4gjUJiQIht04LKL5
Qu75VnGO63UcSwAqgFN8p8erVt74LKjI
qQ94Pi2SIKrR9Yp2xSiOYquA27hctC6u
WC7kS86AbSvzZBQC8mNCwvQnzrYfRelT
0GCrPU5mBXkTHuHL9ElobiiZ8qRYRZtf
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ cat data.txt| sort| uniq -u
EN632PlfYiZbn3PhVK3XOGSlNInNE00t
bandit8@bandit:~$
bandit8@bandit:~$ 
```

I had to learn new commands for this one, from the ones mentioned in the prompt.

grep: Print lines matching a pattern

sort: Sort lines of text files

uniq :Report or omit repeated lines

Strings: Print the strings of printable characters in files

Base64: base64 encode/decode data and print

tr: Translate or delete characters

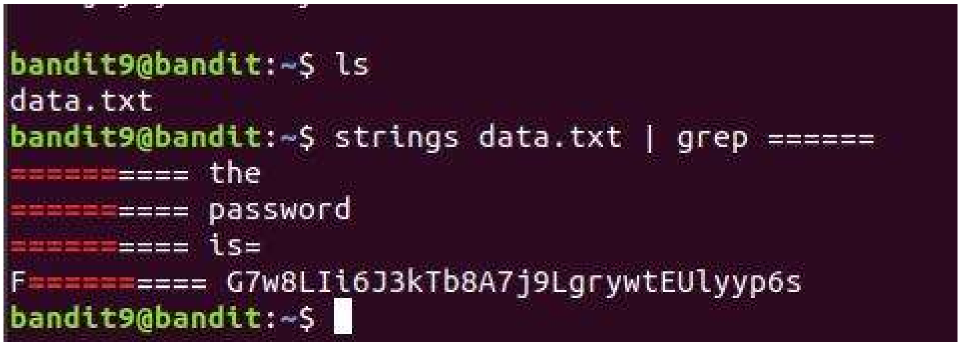
tar: The GNU version of the tar archiving utility

gzip : Compress or expand files

xxd : Make a hexdump or do the reverse

14/12/22

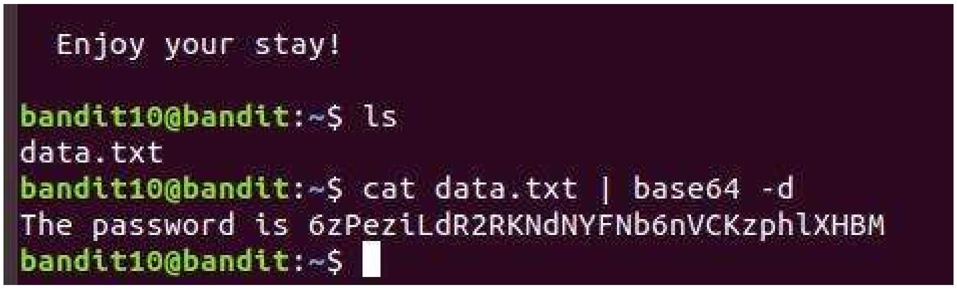
- Logging on to level 9.



```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt | grep ======
========== the
========== password
========== is=
F========== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
bandit9@bandit:~$ 
```

If I use the cat command, it filled my screen with useless data. So, I used strings command and grep to get the password for the next level.

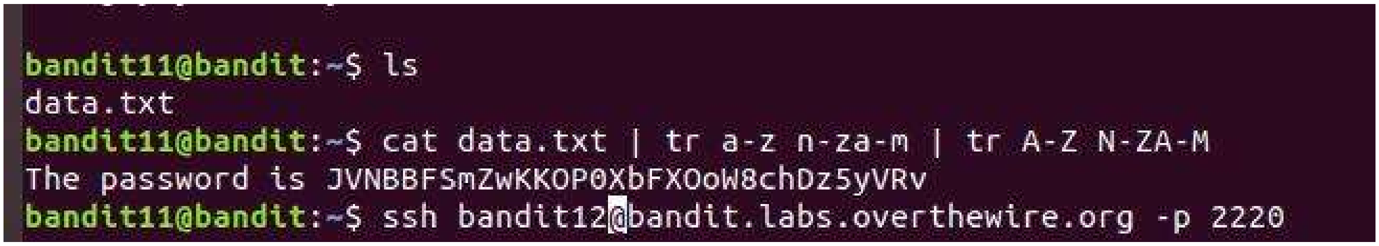
- Logging on to level 10.



```
 Enjoy your stay!

bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt | base64 -d
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$ 
```

The prompt tells us that the password is encrypted in Base64. So, piping cat command and base64 command with d flag to read and decode the text gives the password for level 11.

- Logging on to level 11.

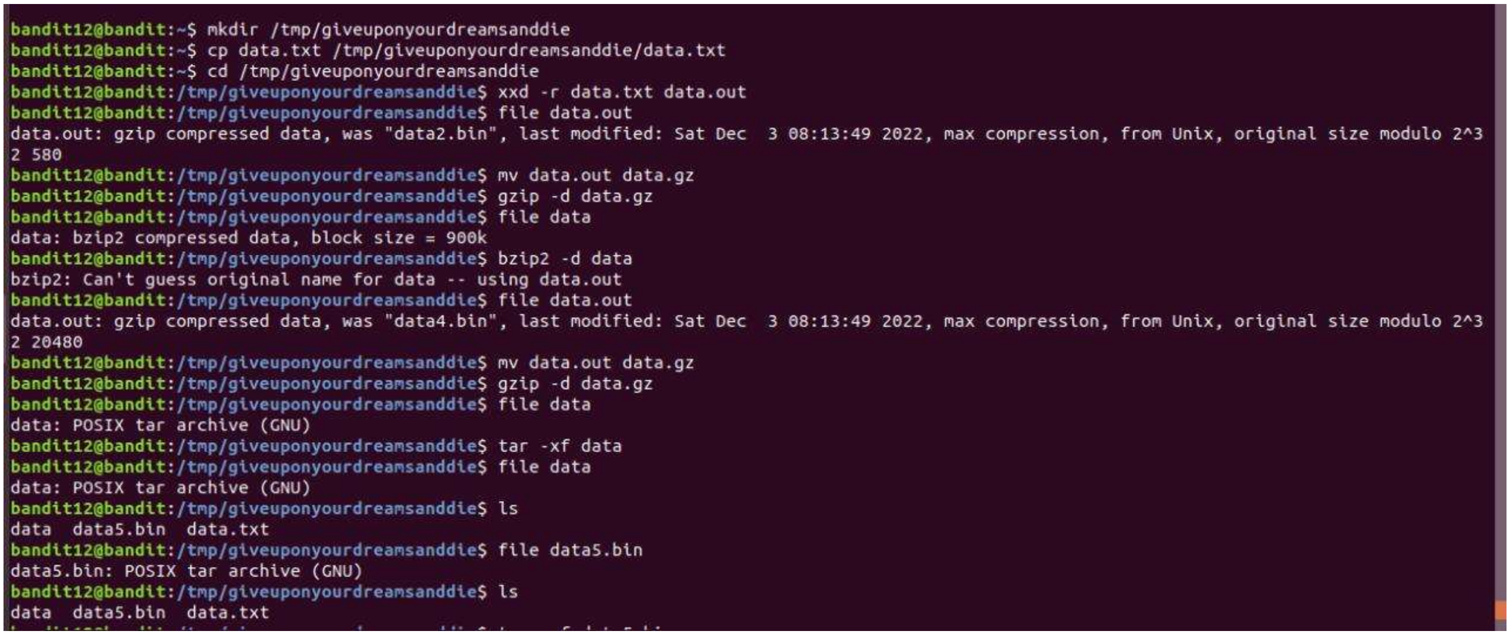


```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt | tr a-z n-za-m | tr A-Z N-ZA-M
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
bandit11@bandit:~$ ssh bandit12@bandit.labs.overthewire.org -p 2220
```

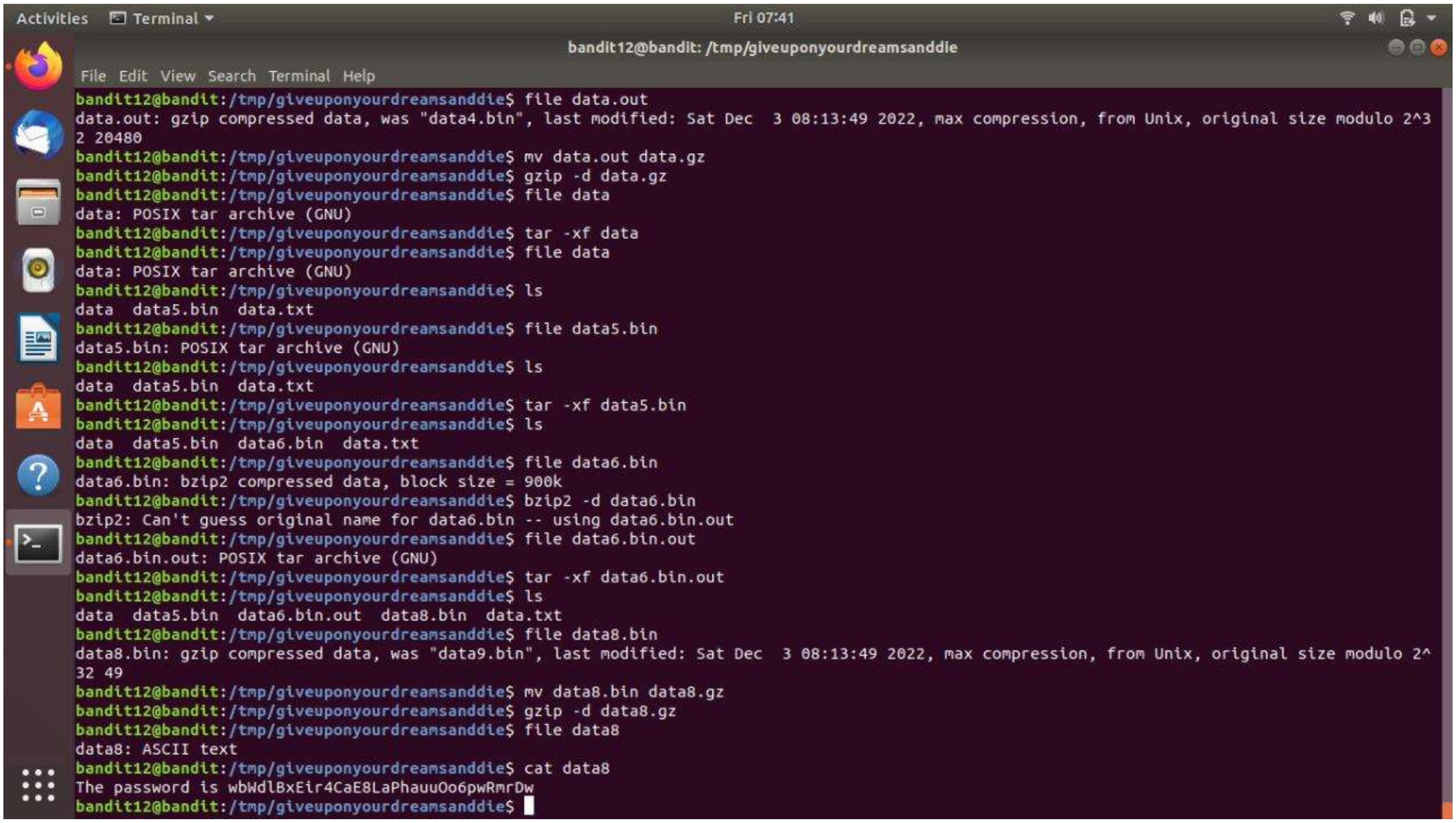
The prompt tells us that the password has changed the letters such that all the lowercase and uppercase letters have been rotated 13 positions. I used the ‘tr’ command. I used n-z and a-m because tr will not continue to translate after the Z. This gives us the password for level 12.

16/12/22

- Logging on to level 12.



```
bandit12@bandit:~$ mkdir /tmp/giveuponyourdreamsanddie
bandit12@bandit:~$ cp data.txt /tmp/giveuponyourdreamsanddie/data.txt
bandit12@bandit:~$ cd /tmp/giveuponyourdreamsanddie
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ xxd -r data.txt data.out
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ file data.out
data.out: gzip compressed data, was "data2.bin", last modified: Sat Dec  3 08:13:49 2022, max compression, from Unix, original size modulo 2^3
2 580
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ mv data.out data.gz
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ gzip -d data.gz
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ file data
data: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ bzip2 -d data
bzip2: Can't guess original name for data -- using data.out
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ file data.out
data.out: gzip compressed data, was "data4.bin", last modified: Sat Dec  3 08:13:49 2022, max compression, from Unix, original size modulo 2^3
2 20480
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ mv data.out data.gz
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ gzip -d data.gz
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ tar -xf data
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ ls
data  data5.bin  data.txt
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ ls
data  data5.bin  data.txt
```


Activities
Terminal
Fri 07:41
bandit12@bandit: /tmp/giveuponyourdreamsanddie
File Edit View Search Terminal Help

```
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ file data.out
data.out: gzip compressed data, was "data4.bin", last modified: Sat Dec  3 08:13:49 2022, max compression, from Unix, original size modulo 2^3
2 20480
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ mv data.out data.gz
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ gzip -d data.gz
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ tar -xf data
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ ls
data  data5.bin  data.txt
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ ls
data  data5.bin  data.txt
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ tar -xf data5.bin
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ ls
data  data5.bin  data6.bin  data.txt
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ bzip2 -d data6.bin
bzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ tar -xf data6.bin.out
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ ls
data  data5.bin  data6.bin.out  data8.bin  data.txt
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Sat Dec  3 08:13:49 2022, max compression, from Unix, original size modulo 2^
32 49
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ mv data8.bin data8.gz
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ gzip -d data8.gz
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ file data8
data8: ASCII text
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ cat data8
The password is wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
bandit12@bandit:/tmp/giveuponyourdreamsanddie$ 
```

This level sucked, it took me multiple google searches and 2 nightmarish hours to figure it out. I started by moving the file to the /tmp/giveuponyourdreamsanddie directory. I then use xxd to convert it out of a hex format and back into the compressed format. Then I used file command to determine what sort of file it was. It was a gzip file, so I renamed it to .gz then used the gzip command to uncompress it. This process repeats using gzip, bzip2, tar and file. Till eventually I got an ASCII file.