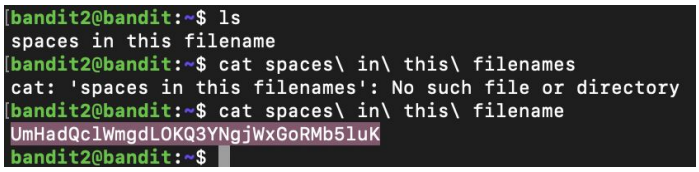
Bandits Writeup

-Ria Singh

Lvl 0-1: ls shows us there exists a readme file. The contents of readme give us the flag.

Lvl 1-2: ls shows that there is a "-" file. As we cannot just directly open a file/folder named with a symbol, we use ./ to override the meaning of the symbol

Lvl 2-3: ls again shows us that there is a file "spaces in this filename". We cannot open a file having white space in its name, which will give an error. Thus to override the white space, use "\" before each space in the filename.



Lvl 3-4: ls again, this time we get a directory "inhere". Looking in the directory, we don't see shit. Must be some hidden files. So use ls -a. We see a file ".hidden". Again the dot symbol in the beginning of the filename will cause error. Use "./" while opening the file.

Lvl 4-5: ls again, find inhere dir, ls in the directory shows several files. You can either open all those files one by one, but it's tiresome and in some scenarios if

you have hundreds of files it'd be stupid. So let's see what kinda files are these. One of them is an ASCII text file. Bingo, open that, capture your flag.

```
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 ./-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
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

Lvl 5-6: Repeating the process till inhere dir, we'll see there'll be many maybehere files. Now on the bandit site, they said the flag is in the while which is in 1033 bytes in size. Now find the one of that size and obtain your flag.

```
bandit5@bandit:~/inhere$ find -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

Lvl 6-7: Similar to prev one, this time we're told that the flag is in the file which is a)owned by user bandit7, b)owned by group bandit6, and c) 33 bytes in size. Using the appropriate command as shown below,

```
bandit6@bandit:~$ find -size 33c
bandit6@bandit:~$ -user bandit7 -group bandit6
-bash: -user: command not found
bandit6@bandit:~$ find -size 33c  -user bandit7 -group bandit6
bandit6@bandit:~$ find -size 33c -user bandit7 -group bandit6
bandit6@bandit:~$ find / -size 33c -user bandit7 -group bandit6
```

We'll get a bunch of files, but there's an interesting on bandit7.password. Open that.

```
/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:~$
```

Lvl 7-8: This time while roaming around we find a data.txt file. You can just try to open and read it's content directly, but sadly they've put a whole lot of useless

texts to hide the password. Going to the bandit page, this time they said the password is along the word, “millionth”. Find the sentence with this word and get your flag.

```
bandit7@bandit:~$ cat data.txt | grep "millionth"
millionth       cvX2JJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$
```

Lvl 8-9: Again for the love of god don’t simply cat the file. Bandit site says the password is the only line of text which occurs once. So we sort the text first and extract the unique line.

```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ sort data.txt | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
bandit8@bandit:~$
```

Lvl 9-10: Bandit site says password is in the data.txt which has a “human readable string” and is preceded by “=”. Again you can use strings directly on data.txt but inadvisable for irl situations. So we make use of grep to filter the strings which are preceded by “=”.

```
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:~$
```

Lvl 10-11: Acc to Bandit site, the text in data.txt is base64 encrypted. Decode it, get the flag.

```
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$
```

Lvl 11-12: This time it is supposed to be ROT13 encoded. Go to rot13.com to decode the text obtained from data.txt

```
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh
bandit11@bandit:~$
```

rot13.com

About ROT13

Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh

↓

ROT13

↓

The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Lvl 12-13: There have been a lot of compressions, so we extract data from them one by one.

```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ mkdir /tmp/ria
bandit12@bandit:~$ cp data.txt /tmp/ria
bandit12@bandit:~$ cd /tmp/ria
bandit12@bandit:/tmp/ria$ ls
data.txt
bandit12@bandit:/tmp/ria$ file data.txt
data.txt: ASCII text
bandit12@bandit:/tmp/ria$ xxd -r data > data1
xxd: data: No such file or directory
bandit12@bandit:/tmp/ria$ xxd -r data.txt > data1
bandit12@bandit:/tmp/ria$ ls
data1  data.txt
bandit12@bandit:/tmp/ria$ file data1
data1: gzip compressed data, was "data2.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/ria$ zcat data1 >data2
bandit12@bandit:/tmp/ria$ ls
data1  data2  data.txt
bandit12@bandit:/tmp/ria$ file data2
data2: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/ria$ bzcat data2 > datat3
bandit12@bandit:/tmp/ria$ ls
data1  data2  datat3  data.txt
bandit12@bandit:/tmp/ria$ file data3
data3: cannot open `data3' (No such file or directory)
bandit12@bandit:/tmp/ria$ file datat3
datat3: gzip compressed data, was "data4.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/ria$ zcat datat3 > data4
bandit12@bandit:/tmp/ria$ ls
data1  data2  data4  datat3  data.txt
bandit12@bandit:/tmp/ria$ file data4
data4: POSIX tar archive (GNU)
bandit12@bandit:/tmp/ria$ tar -x -f data4
bandit12@bandit:/tmp/ria$ ls
data1  data2  data4  data5.bin  datat3  data.txt
bandit12@bandit:/tmp/ria$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/ria$ tar -x -f data5.bin
bandit12@bandit:/tmp/ria$ ls
data1  data2  data4  data5.bin  data6.bin  datat3  data.txt
bandit12@bandit:/tmp/ria$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/ria$ bzcat data6.bin > data7
bandit12@bandit:/tmp/ria$ ls
data1  data2  data4  data5.bin  data6.bin  data7  datat3  data.txt
bandit12@bandit:/tmp/ria$ data7
-bash: data7: command not found
bandit12@bandit:/tmp/ria$ file data7
data7: POSIX tar archive (GNU)
bandit12@bandit:/tmp/ria$ tar -x -f data7
bandit12@bandit:/tmp/ria$ ls
data1  data2  data4  data5.bin  data6.bin  data7  data8.bin  datat3  data.txt
bandit12@bandit:/tmp/ria$ 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/ria$ zcat data8.bin > data9
bandit12@bandit:/tmp/ria$ ls
data1  data4      data6.bin  data8.bin  datat3
data2  data5.bin  data7      data9      data.txt
bandit12@bandit:/tmp/ria$ file data9
data9: ASCII text
bandit12@bandit:/tmp/ria$ cat data9
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
```

Lvl 13-14: There's only a private SSH key file, and "localhost" is the hostname which refers to the machine. Login to the bandit14@localhost.

```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ cat sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxkkOE83W2cOT7IWhFc9aPaaQmQDdgzuXCv+ppZHa++buSkN+
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AIoYp0MZyETq46t+jk9puNwZwIt9XgB
```

```
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
Could not create directory '/home/bandit13/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRkKlo20X3OPnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
```

It is said on the bandit site that the password is in /etc/bandit_pass/bandit14.

```
bandit14@bandit:~$ ls
bandit14@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  .profile  .ssh
bandit14@bandit:~$ cd .ssh
bandit14@bandit:~/.ssh$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~/.ssh$
```

Lvl 14-15: On site it says that submitting the latest password we hold to port 30000 on localhost will provide a password of the next level. Using netcat to listen on localhost port 30000.

```
bandit14@bandit:~$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr

bandit14@bandit:~$
```