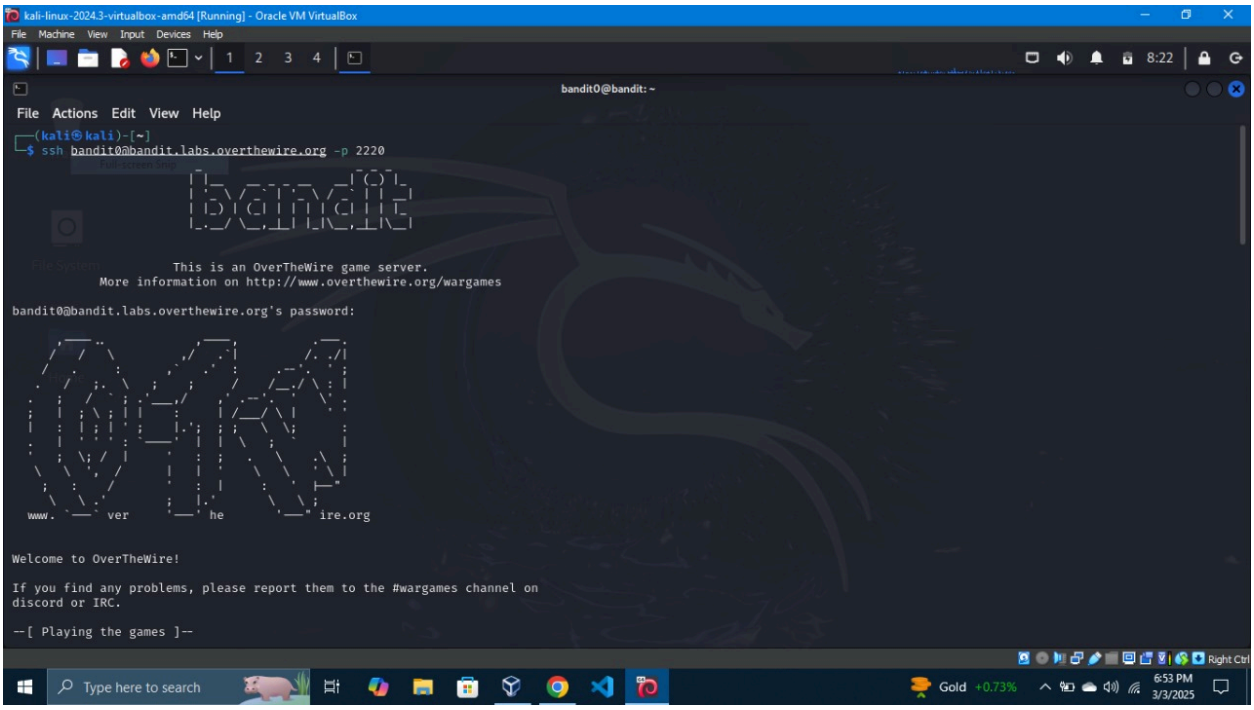
Bandit OverTheWire Writeup:

Level 0:

Task : 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.



Log into the level with ssh in server:bandit.labs.overthewire.org in the port 2220 .

command : ssh bandit0@bandit.labs.overthewire.org -p 2220

username : bandit0

password : bandit0

Level 0 - 1:

Task : 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.

```
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
```

After entering the bandit0 use ls to view the directories.

Use cat to view the content of the readme file.

command : ls and cat readme

password : ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

Level 1 - 2:

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

```
bandit1@bandit:~$ ls -alps
total 24
4 -rw-r-----  1 bandit2 bandit1   33 Sep 19  2024 -
4 drwxr-xr-x  2 root    root    4096 Sep 19  2024 ./
4 drwxr-xr-x 70 root    root    4096 Sep 19  2024 ../
4 -rw-r--r--  1 root    root     220 Mar 31  2024 .bash_logout
4 -rw-r--r--  1 root    root    3771 Mar 31  2024 .bashrc
4 -rw-r--r--  1 root    root     807 Mar 31  2024 .profile
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$
```

Using the previous level passkey the current level is accessed and password for next level is is in a file called - .

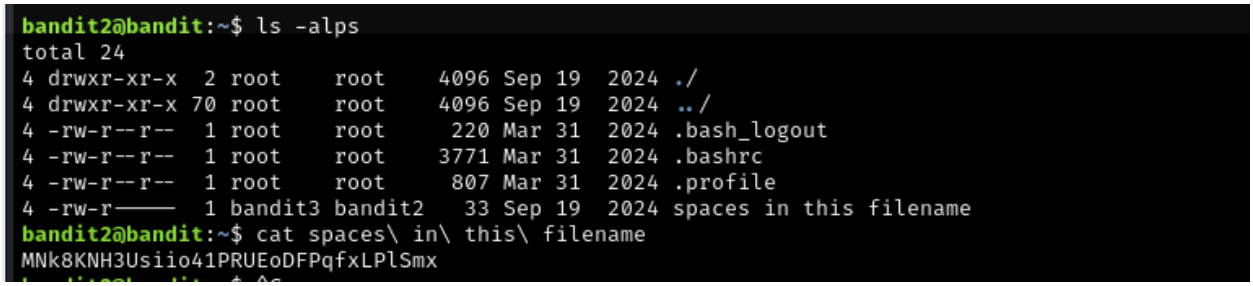
use ls and cat to get the password.

command : ls -alps and cat ./-

password : 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

Level 2 - 3:

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

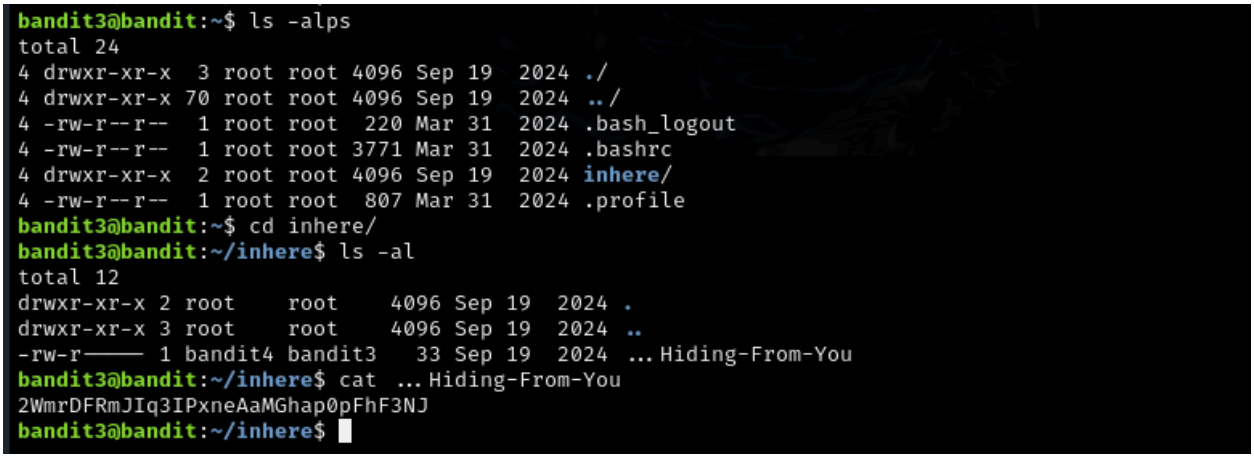


command : cat spaces\ in\ this\ filename \are used to show the space in the command

password : MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx

Level 3 - 4:

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



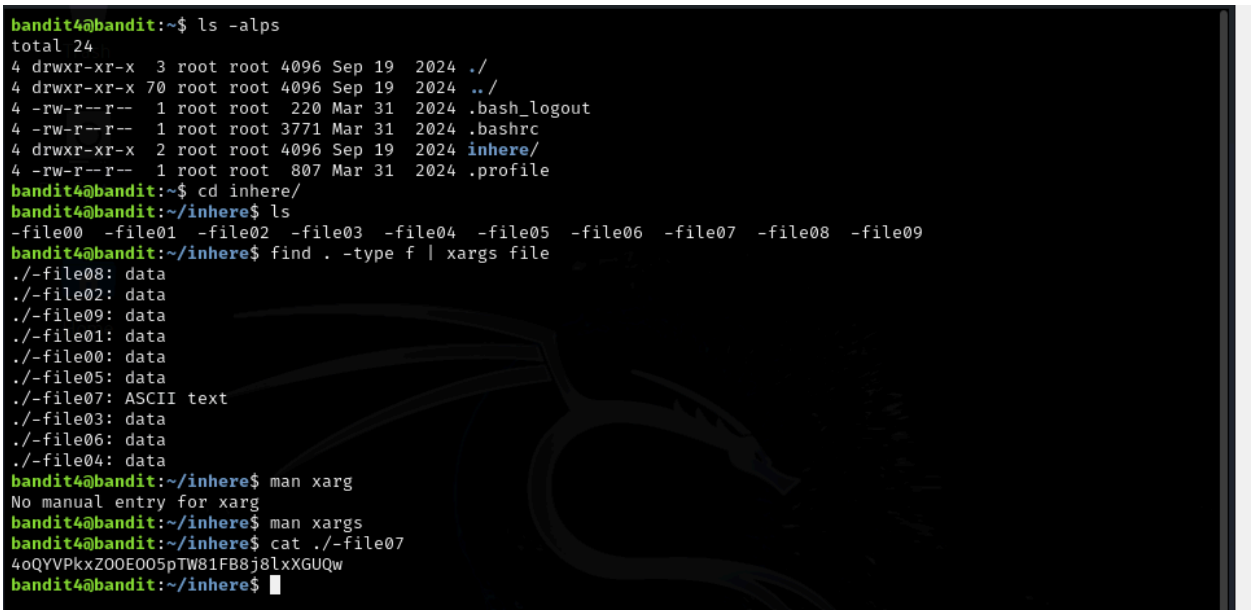
In this level the password is hidden inside the directory inhere.

command : cd for changing directory

password : 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

Level 4 - 5:

Task : 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.



In this level the directories as many files in which the password is in the human readable file. the command find is used to get the readable file in the directory.

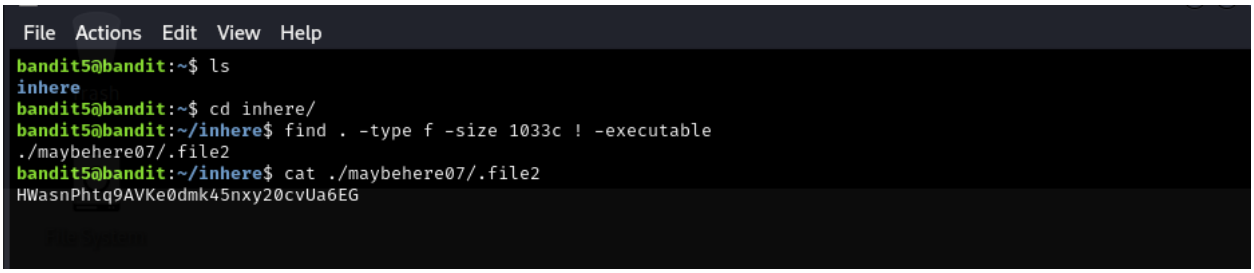
command : ls -alps, cd, find . -type f | xargs file and cat

password : 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

Level 5 - 6 :

Task : The password for the next level is stored in a file somewhere under the **inhere** directory and has all of the following properties:

- human-readable
- 1033 bytes in size
- not executable



the command find . -type f -size 1033c ! executable says the properties of the given directories.

password : HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

Level 6 - 7:

Task : The password for the next level is stored **somewhere on the server** and has all of the following properties:

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

```
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6  -size 33c
find: '/drifter/drifter14_src/axTLS': Permission denied
find: '/root': Permission denied
find: '/snap': Permission denied
find: '/tmp': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/1774579/task/1774579/fdinfo/6': No such file or directory
find: '/proc/1774579/fdinfo/5': No such file or directory
find: '/home/bandit31-git': Permission denied
find: '/home/ubuntu': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/drifter8/chroot': Permission denied
find: '/home/drifter6/data': Permission denied
find: '/home/bandit29-git': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/lost+found': Permission denied
find: '/etc/polkit-1/rules.d': Permission denied
find: '/etc/multipath': Permission denied
find: '/etc/stunnel': Permission denied
find: '/etc/xinetd.d': Permission denied
find: '/etc/credstore.encrypted': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/sudoers.d': Permission denied
find: '/etc/credstore': Permission denied
find: '/dev/shm': Permission denied
find: '/dev/mqueue': Permission denied
find: '/var/log/amazon': Permission denied
find: '/var/log/unattended-upgrades': Permission denied
find: '/var/log/chrony': Permission denied
find: '/var/log/private': Permission denied
find: '/var/tmp': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/pollinate': Permission denied
find: '/var/cache/private': Permission denied
find: '/var/cache/apparmor/2425d902.0': Permission denied
find: '/var/cache/apparmor/baad73a1.0': Permission denied
find: '/var/lib/polkit-1': Permission denied
find: '/var/lib/amazon': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/chrony': Permission denied
find: '/var/lib/snapd/void': Permission denied
find: '/var/lib/snapd/cookie': Permission denied
```

```
find: '/run/user/11015': Permission denied
find: '/run/user/11003': Permission denied
find: '/run/user/11014': Permission denied
find: '/run/user/11009': Permission denied
find: '/run/user/11010': Permission denied
find: '/run/user/11019': Permission denied
find: '/run/user/11022': Permission denied
find: '/run/user/11002': Permission denied
find: '/run/user/11017': Permission denied
find: '/run/user/8002': Permission denied
find: '/run/user/11032': Permission denied
find: '/run/chrony': Permission denied
find: '/run/udisks2': Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:~$
```

The password is stored somewhere in the server so the command find / -type f -user bandit7 -group bandit6 -size 33c is used to get the packets.

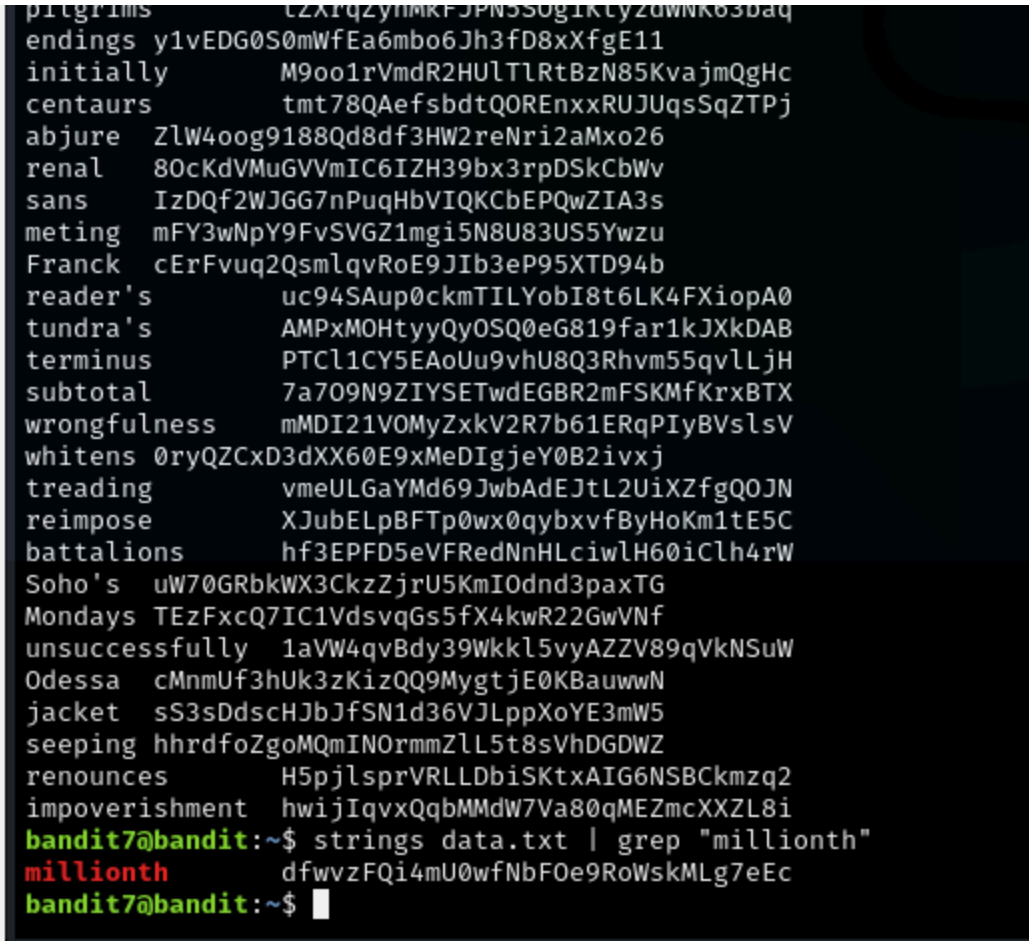
command : find / -type f -user bandit7 -group bandit6 -size 33c

password : morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj

Level 7 - 8 :

Task : The password for the next level is stored in the file **data.txt** next to the word **millionth**

```
bandit7@bandit:~$ ls -alps
total 4108
   4 drwxr-xr-x  2 root    root       4096 Sep 19  2024 ./
   4 drwxr-xr-x 70 root    root       4096 Sep 19  2024 ../
   4 -rw-r--r--  1 root    root        220 Mar 31  2024 .bash_logout
   4 -rw-r--r--  1 root    root       3771 Mar 31  2024 .bashrc
4088 -rw-r-----  1 bandit8 bandit7 4184396 Sep 19  2024 data.txt
   4 -rw-r--r--  1 root    root        807 Mar 31  2024 .profile
bandit7@bandit:~$ cat data.txt
momentary       MBLQ2×4SPU4Y6XIscWooXopjdSntWOhY
vicuña  6nKKKgzHbJvPFsEFQgzd2wqJWcv8TGGQ
equities        ZhOy86fNIP8sWsOLLYiHrtjRsrpu1bND
various Eg1ZcmYmpvkXS10Vu04areb2hhT9Pkft
redefinition's  vPzYXGDGwByIVBRIKQDRHn5xqoekZKME
Allison 4JPUMGRznD4JAyy1SX2Cf5zAwEhT7AP7
compels 8XgWaEyaUVmm1FLZksXE6vRBAKfm7xGB
misstep 0p0wfzDrUfyAbU6V5MVGlrvDKjmc6a0Z
coagulating     Ff0C46bfOMzwOojIDTWJAq9O59WdKSdw
Onega's YiR7TkXXHKpt0Oqs2EtFzRSXu8XGCqQA
checkmate       XjaNSCEGpEdkJIMfCnwWGJuRQ6fUIoUq
Lyndon  7m6zWzaFwemeBJ7jKzXO1REfc9QtC9SQ
archivist       j1kdDmGHBGtcor81a2lIZzVd9ulFtifz
Jerri's 2fCe8FdpTJFt4gtanwmG7a8A1AYlEpDQ
underarms       ZSucs304S5mq2TONuDqpN5gwz7HsbCOQ
scrooge SYI06iTGl1SdxwJV21kH4fty0AAer8Rv
Elnora  i1GGmWJChr5PUq8N8s9nt6nhYvoUtoRu
salver  uZf07mMWSaF4hLwFmGKIKt0qrSeTIPjy
hemorrhaged     rgsv7OD3SHSx6OIfJTpI4p60BApaOsEI
fount's U4XHsnP97BgOI3v027KBrpwtMvR9qF1I
autograph's     OOgaDupjr2RbwoOA98oN4jzlYq2Q1Rwc
tranquillizes   5ncuXd3UAIy3SOQRnVS8s3Sp7iEb0hrX
edgiest OJtPY7WKKVMFSkTHwYTUnWoZzRIQ76Ii
miles   C8GP1U4YQzLz6wdWbKsWBexSS361WShV
inconvenience's kJM03FuxWnwIyXyOQ3CgUjMM4RKPnyGc
hurled  fYt4KTyYNxGpjSagdMXaggeaF1lj5TP1
strollers       Gf1nIaOalC8w7MfeHQbFSRbmBdvK6MLk
Lincoln's       HoRRZZXAEt2vO3wM51A4sfCukDlHLlMy
showerier       Qi4hcuzmfLfi79r0r1WqtE99n0Cxih5c
Head    ZoXDgeBUXPiKQIquLtWwqM1ZI8jzdkzF
Mormonism's     mQGJw2ifm0p6Y6jPBPtLr679JY3gz0Mc
riming  fUq82ZhW36YYujQ0RhvzvxWEBH1E7ffM
eviscerating    55uIcXOb4z4JJ8nOrVsqIm2GUF4Swhom
fluoride's      GULiK1R5hxj9ZSCA3xhWGNCFsac7j44d
threnodies      2HEh1JzLBinyNbno1gW4UUp5SbQMTm4V
insecticide     V0gn5D80tLV3ksiTke5eM64RTPpOSE9W
muscat  1RuOF1vdEX0BrGNZqlrDsicRhcot0BnN
shortsightedly  NKLJBXieAA8pcGwcT19rAh91EAIs2qcT
screen  HHW3ECeI3LTZE9qsIHVbQiW3YzBUaUxc
Adenauer        6nkup8SIXcOvtEToTGtqVf7srh9mxYCo
hedonists       iF2vetNKv6QIoFaMZZH99sWH30PMrtEF
insured bKsaAcccEj9l35At2jqdbl5uFfS9w3js
```



the data.txt file has many strings which are difficult to find . so, the command strings text_file | grep “word” is given to get the password.

command : strings data.txt | grep “millionth”

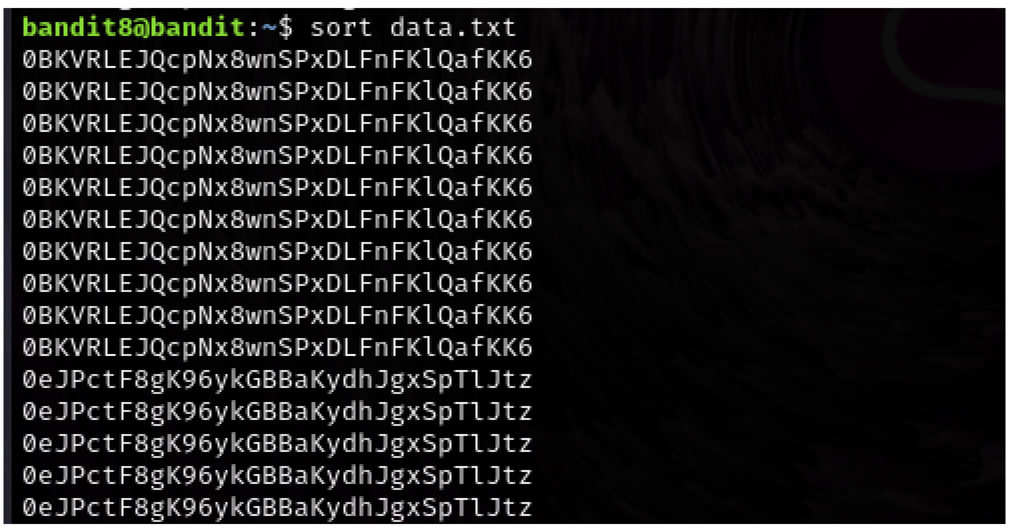
password : dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

Level 8 - 9:

Task : The password for the next level is stored in the file **data.txt** and is the only line of text that occurs only once

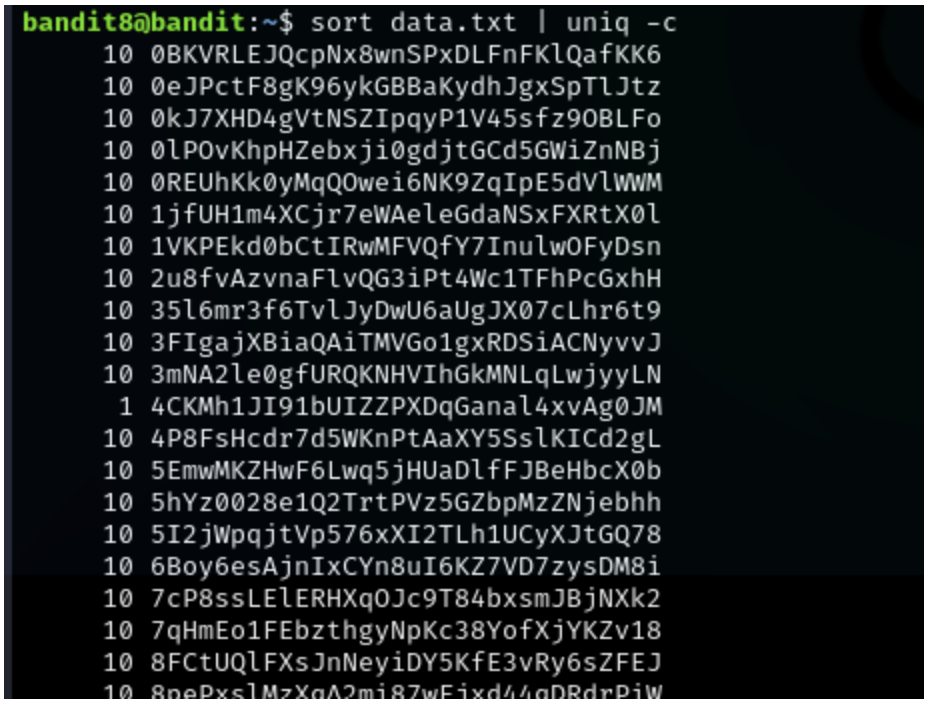
```
bandit8@bandit:~$ cat data.txt
aMKlTMrptUxxTypCHocCTrqYRkR2gT8h
PRerp5EfTVxJHKuCZDXfAfRyCQSdPjMi
0BKVRLEJQcpNx8wnSPxDLFnFKlQafKK6
6Boy6esAjnIxCYn8uI6KZ7VD7zysDM8i
tgHSfEXcbYCejWXfsWDO4VXXbqtTVcqS
KZJOZECxhLxDhxDbGzdNy8m0uplzvP11
w6×5XtaoRWDqMCsYxgZIWuOKVdiGByAu
0kJ7XHD4gVtNSZIpqyP1V45sfz9OBLFo
Wr4hWlUhGCKJpGDCeio8C1pLVt7DZm3X
Su9w1lri9UACf53cL1evAMKXVgI0nfqe
6Boy6esAjnIxCYn8uI6KZ7VD7zysDM8i
CgUjZiluCoMEvzNAge1Nbv3g9tpLQQj2
ysKmfYcysVfnViisRBcXzgjjXMDgnKKv
1VKPEkd0bCtIRwMFVQfY7InulwOFyDsn
```

cat is used to view the data.txt file which is the only file.



```
bandit8@bandit:~$ sort data.txt
0BKVRLEJQcpNx8wnSPxDLFnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLFnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLFnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLFnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLFnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLFnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLFnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLFnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLFnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLFnFKlQafKK6
0eJPctF8gK96ykGBBaKydhJgxSpTlJtz
0eJPctF8gK96ykGBBaKydhJgxSpTlJtz
0eJPctF8gK96ykGBBaKydhJgxSpTlJtz
0eJPctF8gK96ykGBBaKydhJgxSpTlJtz
0eJPctF8gK96ykGBBaKydhJgxSpTlJtz
```

sort is used to arrange the strings in order to find the number of times the strings are repeated.



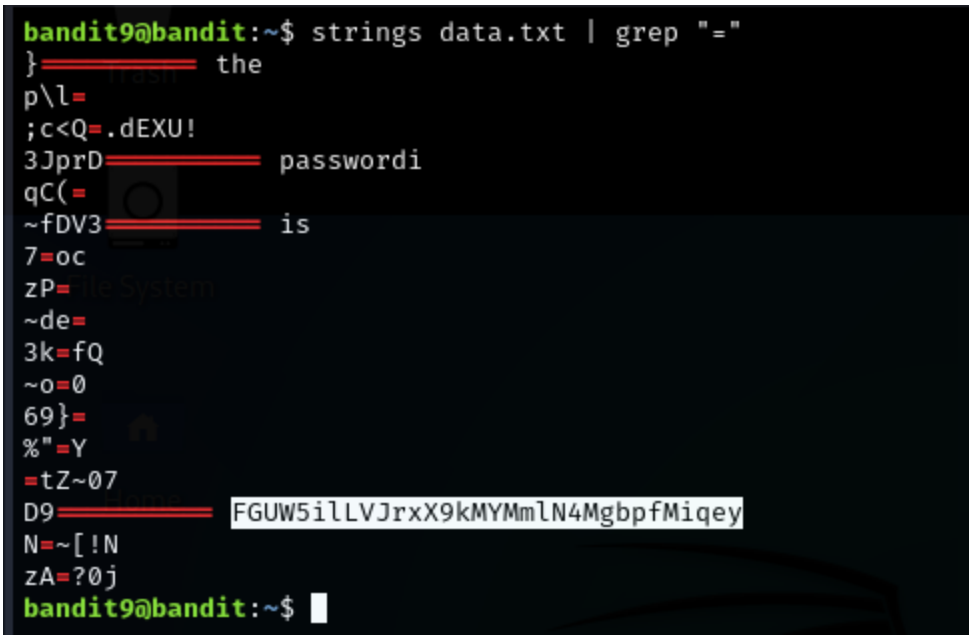
uniq -c is used to get the count of the unique strings present in the data.txt.

command : sort data.txt | uniq -c

password : 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

Level 9 - 10 :

Task : 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.



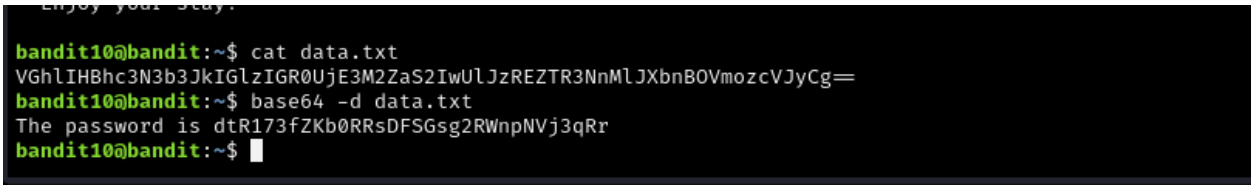
strings data.txt gives the whole strings content of the file but the | grep “=” gives the strings which has the characters.

command : strings data.txt | grep “=”

password : FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

Level 10 - 11 :

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



the encoded data was in the data.txt file . We can also use other sources like cyberchief and base64 platform instead of base64 -d in linux.

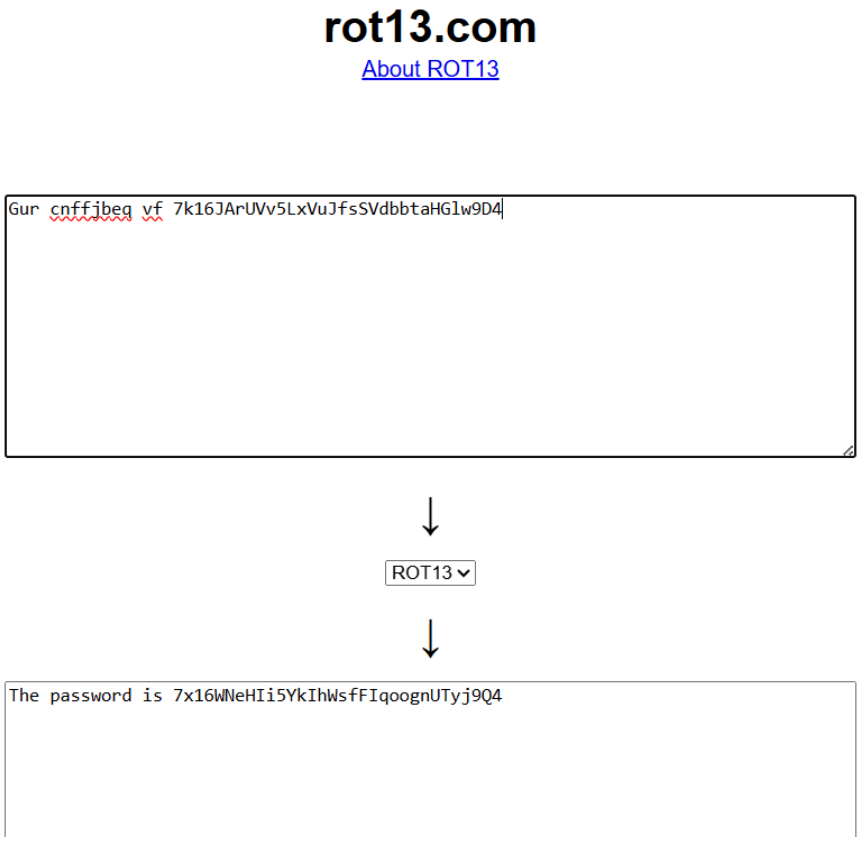
command : base64 -d data.txt

Tool : base64

password : dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

Level 11 - 12 :

Task : The password for the next level is stored in the file **data.txt**, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions



rot 13 is a tool used to decode the data. It is a online tool, the alternate for rot13 is cyberchief which is also a online platform.

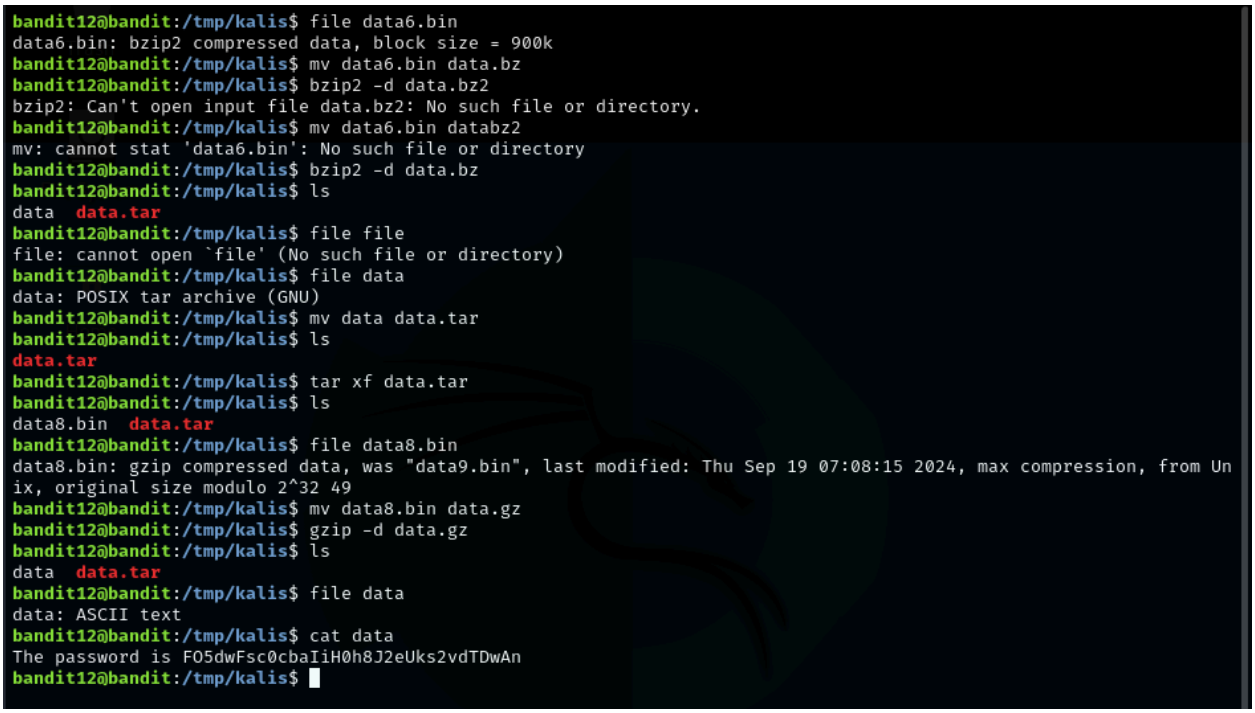
Tool : rot13

password : 7×16WNeHIi5YkIhWsfFIqoognUTyj9Q4

Level 12 - 13 :

Task : 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. Use mkdir with a hard to guess directory name. Or better, use the command “mktemp -d”. Then copy the datafile using cp, and rename it using mv (read the manpages!)

```
bandit12@bandit:~$ mkdir /tmp/kalis
bandit12@bandit:~$ cp data.txt /tmp/kalis
bandit12@bandit:~$ cd /tmp/kalis
bandit12@bandit:/tmp/kalis$ ls
data.txt
bandit12@bandit:/tmp/kalis$ xxd -r data.txt > data
bandit12@bandit:/tmp/kalis$ ls
data  data.txt
bandit12@bandit:/tmp/kalis$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix, o
riginal size modulo 2^32 574
bandit12@bandit:/tmp/kalis$ mv data file.gz
bandit12@bandit:/tmp/kalis$ gzip -d file.gz
bandit12@bandit:/tmp/kalis$ ls
data.txt  file
bandit12@bandit:/tmp/kalis$ file file
file: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/kalis$ mv file file.bz2
bandit12@bandit:/tmp/kalis$ bzip2 -d file.bz2
bandit12@bandit:/tmp/kalis$ ls
data.txt  file
bandit12@bandit:/tmp/kalis$ file file
file: gzip compressed data, was "data4.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix, o
riginal size modulo 2^32 20480
bandit12@bandit:/tmp/kalis$ mv file file.gz
bandit12@bandit:/tmp/kalis$ gzip -d file.gz
bandit12@bandit:/tmp/kalis$ ls
data.txt  file
bandit12@bandit:/tmp/kalis$ file file
file: POSIX tar archive (GNU)
bandit12@bandit:/tmp/kalis$ mv file file.tar
bandit12@bandit:/tmp/kalis$ tar xf file.tar
bandit12@bandit:/tmp/kalis$ ls
data5.bin  data.txt  file.tar
bandit12@bandit:/tmp/kalis$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/kalis$ rm file.tar
bandit12@bandit:/tmp/kalis$ rm data
rm: cannot remove 'data': No such file or directory
bandit12@bandit:/tmp/kalis$ rm data.txt
bandit12@bandit:/tmp/kalis$ ls
data5.bin
bandit12@bandit:/tmp/kalis$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/kalis$ mv data5.bin data.tar
bandit12@bandit:/tmp/kalis$ tar xf data.tar
bandit12@bandit:/tmp/kalis$ ls
data6.bin  data.tar
bandit12@bandit:/tmp/kalis$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
```



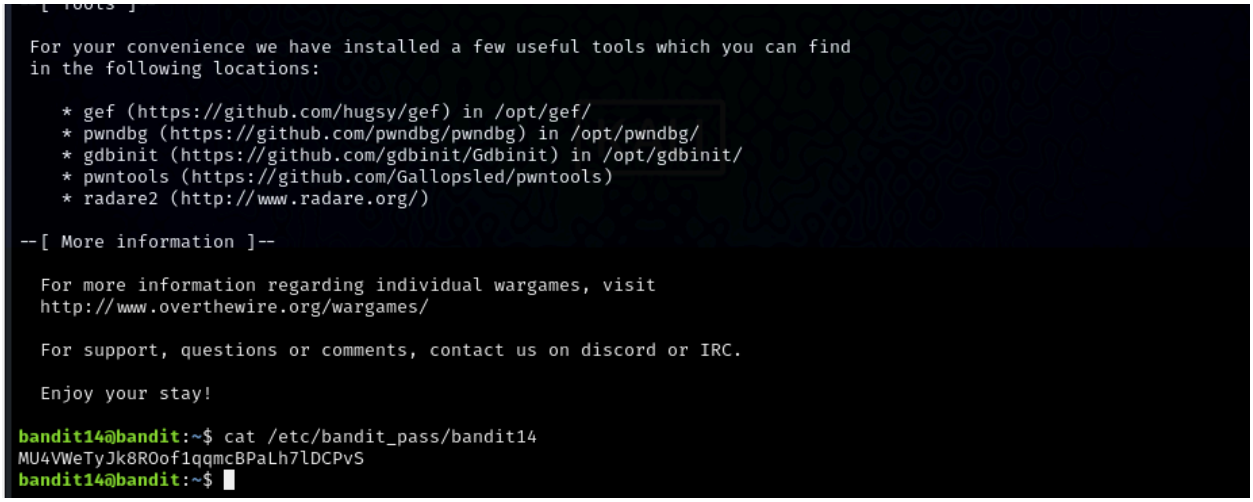
Create a working directory and copy `data.txt` .**Convert Hexdump:** Use `xxd -r` to restore the binary file. Extract gzip, then bzip2, then another gzip. Extract multiple tar archives, decompressing as needed. **Retrieve Password:** Once the final file is ASCII text, use `cat` to display the password.

commands : mkdir, tar, gzip, bzip2, xxd, cp, mv, file

password : FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn

Level 13 - 15 :

Task : The password for the next level is stored in **/etc/bandit_pass/bandit14 and can only be read by user bandit14**. For this level, you don't get the next password, but you get a private SSH key that can be used to log into the next level. **Note: localhost** is a hostname that refers to the machine you are working on. The password for the next level can be retrieved by submitting the password of the current level to **port 30000 on localhost**.



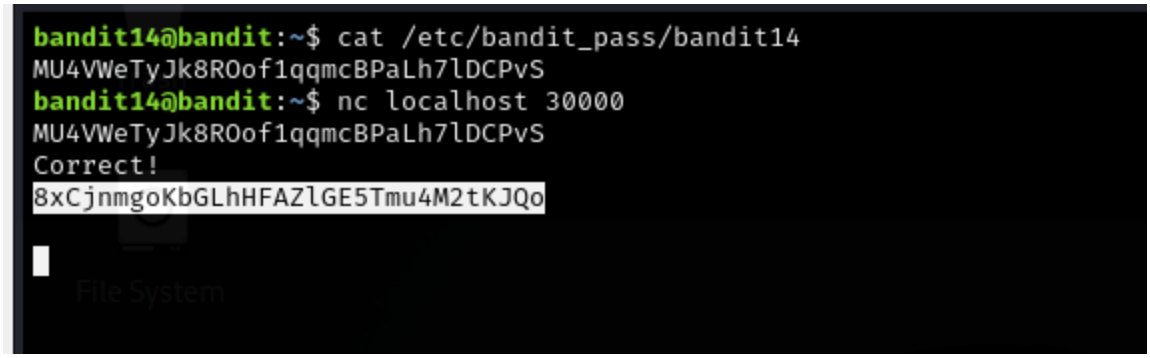
password for level 15 is derived here . The password is saved in the ssh privatekey by using bandit14@localhost the privatekey is derived from the same level.

command : ssh -i sshkey.private bandit14@localhost -p 2220

cat /etc/bandit_pass/bandit14

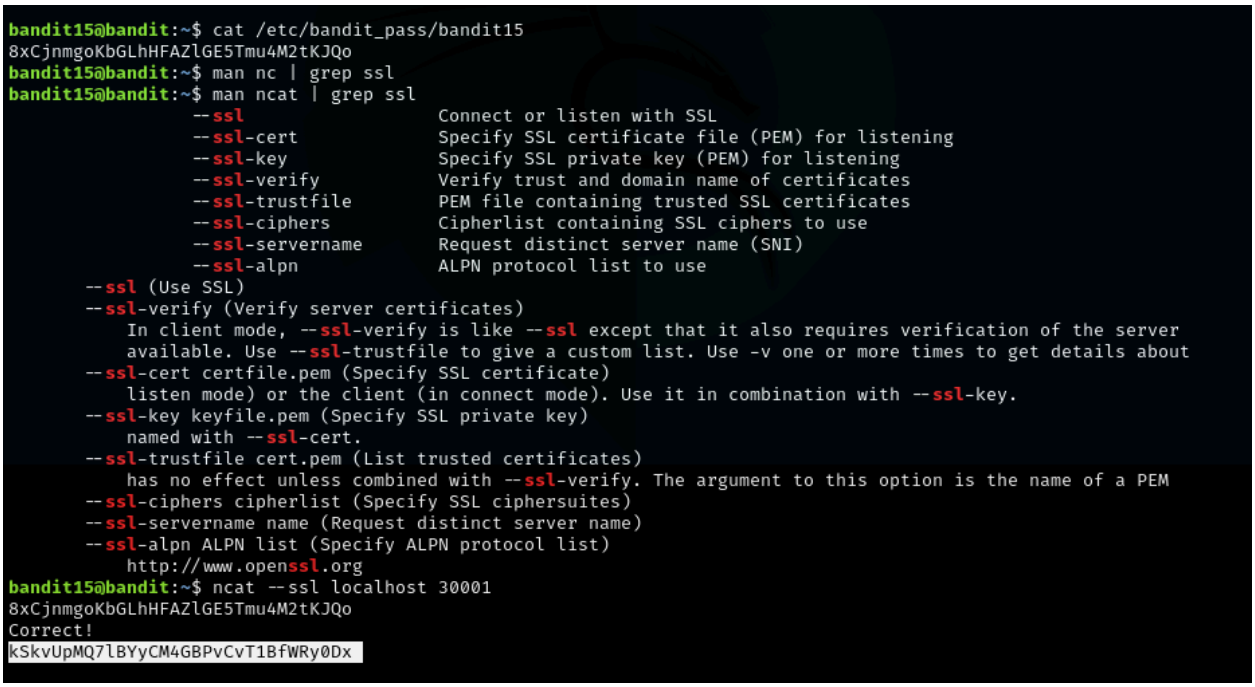
password of 14 : MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS

password of 15 : 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo



Level 15 - 16 :

Task : The password for the next level can be retrieved by submitting the password of the current level to **port 30001 on localhost** using SSL/TLS encryption.



the password for next level is derived by giving the password fo current level.

command : ncat —ssl localhost 30001

password : kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

Level 16 - 17 :

Task : The credentials for the next level can be retrieved by submitting the password of the current level to **a port on localhost in the range 31000 to 32000**. First find out which of these ports have a server listening on them. Then find out which of those speak SSL/TLS and which don’t. There is only 1 server that will give the next credentials, the others will simply send back to you whatever you send to it.

```
bandit16@bandit:~$ nc localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
bandit16@bandit:~$ ncat --ssl localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RllwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8×7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

The open ports are first checked between 31000 to 32000. nmap is used to find which port is open and which is active. The result is a private sshkey a file is created to store the private keys of the levels and that file only has the permission to the user.

command : nmap and nc.

Level 17 - 18 :

Task : here are 2 files in the homedirectory: **passwords.old and passwords.new**. The password for the next level is in **passwords.new** and is the only line that has been changed between **passwords.old and passwords.new**

Find the one line that is different between the two files.