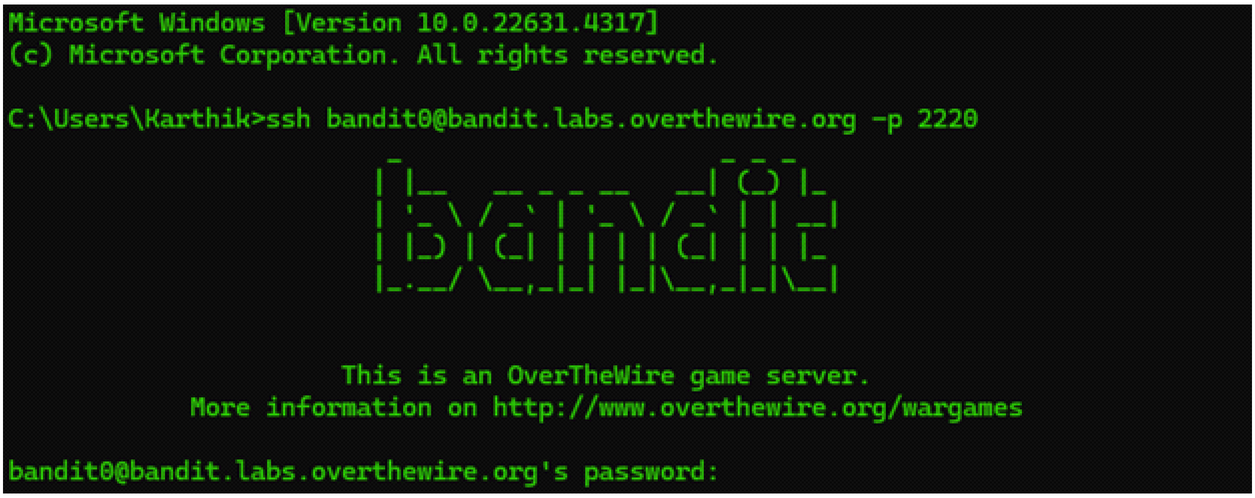
Level 0

Thursday, October 17, 2024 7:50 PM



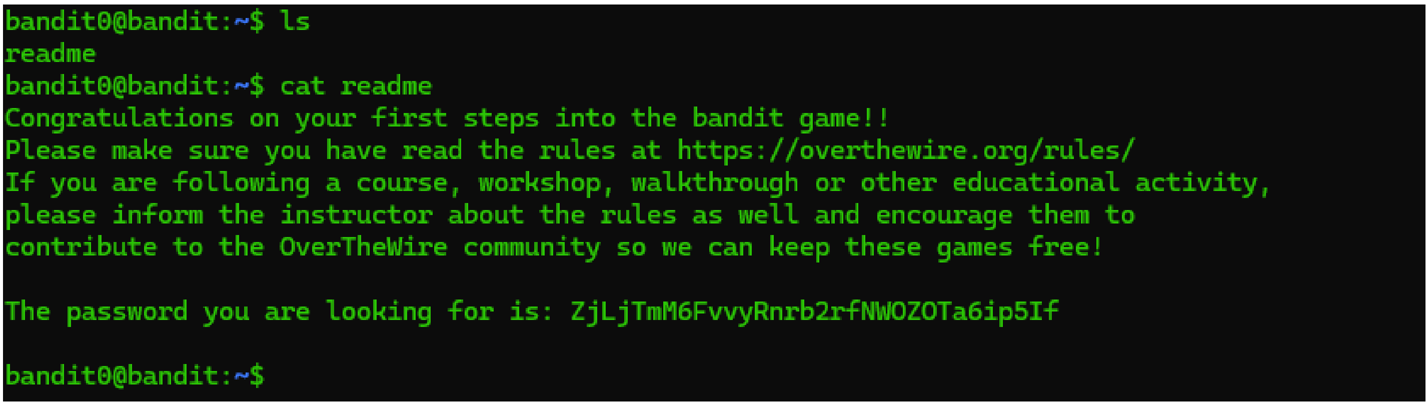
```
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Karthik>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:
```

SSH to bandit.labs.overthewire.org at port 2220. The user name is bandit0.

ssh syntax - ssh username@hostname -p (port number)

Level 0 -> 1

Thursday, October 17, 2024 7:53 PM



```
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:~$
```

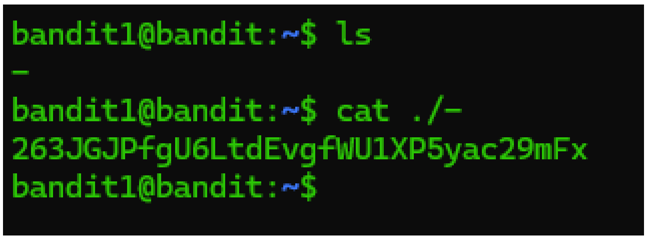
The password is stored in the file readme. Use ls to list all the files in the current working directory.
ls lists the file readme. Now to read the contents of the file readme. Use cat readme.

The password for the next level is ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If.

To proceed to the next level ssh to the same host and port using username bandit1 and the above mentioned password.

Level 1 -> 2

Thursday, October 17, 2024 7:56 PM



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

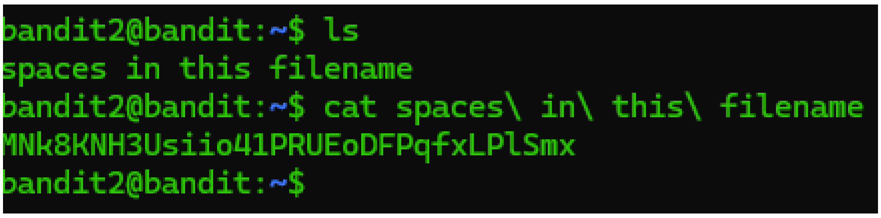
The password is stored in the file -. Using cat - will not give the desired output as it expects - to be a flag associated with the cat command. In order to read the contents of the file - we need to write cat ./-

The contents of the file is 263JGJPfgU6LtdEvgfWU1XP5yac29mFx, which is the password for the next level.

To proceed to the next level ssh to the same host and port using username bandit2 and the above mentioned password.

Level 2 -> 3

Thursday, October 17, 2024 8:00 PM



```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
bandit2@bandit:~$
```

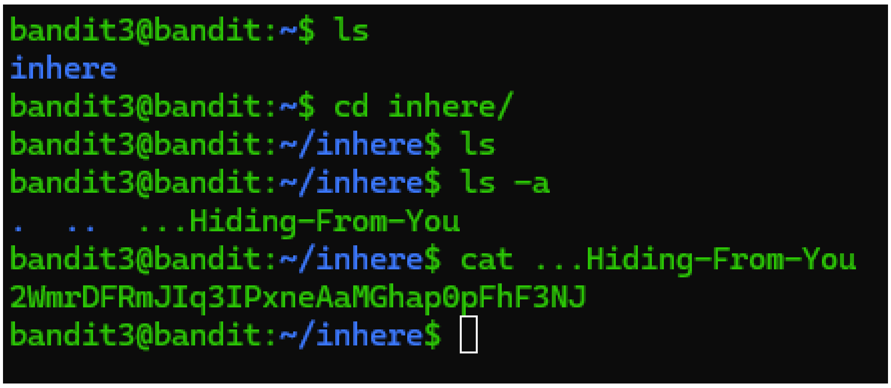
Here the password is stored in the file spaces in this filename. To read the file type the first few characters of the file name followed by a tab to make the terminal autocomplete the filename. The "\" symbol in the command cat spaces\ in\ this\ filename indicates that there is a single file whose name contains spaces.

The contents of the file is MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx, which is the password for the next level.

To proceed to the next level ssh to the same host and port using username bandit3 and the above mentioned password.

Level 3 -> 4

Friday, October 18, 2024 9:38 AM



```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  ...Hiding-From-You
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$ 
```

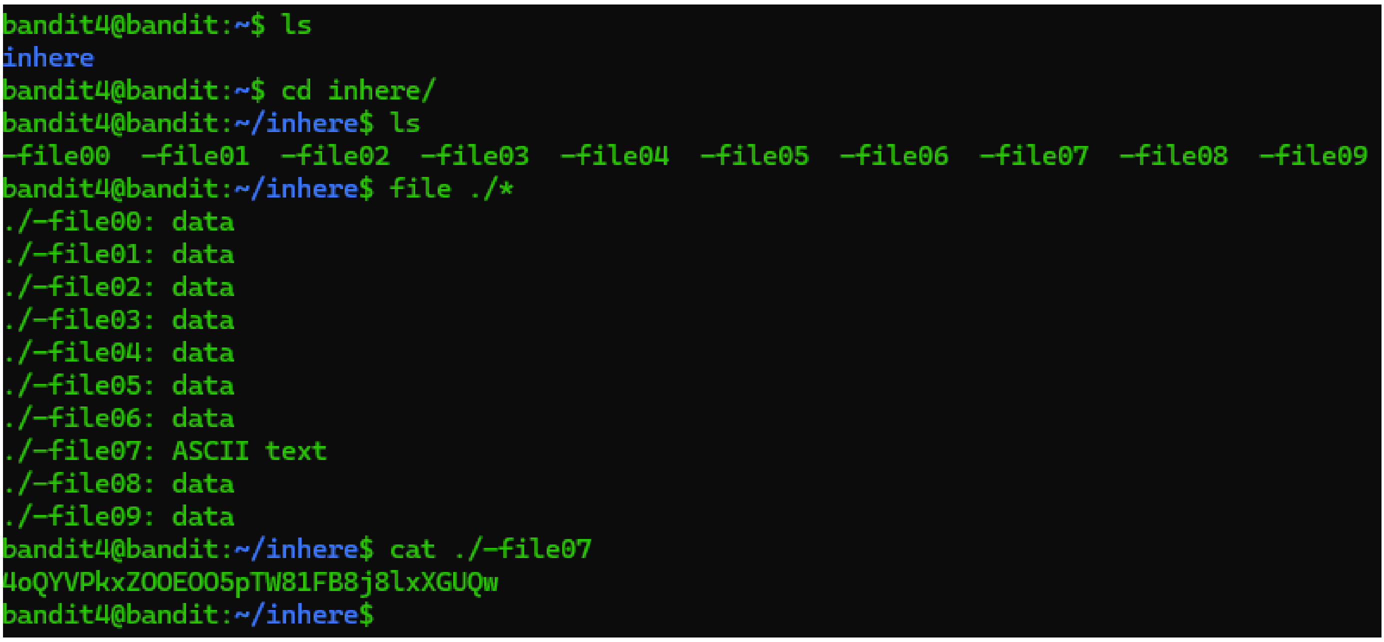
The file is located in the inhere directory. Using cd we can move into the inhere directory. Using ls we see that there is no file present in the directory. Using -a flag with ls (ls -a) to list all the files in the directory (including hidden files) we see that there is a file named ...Hiding-From-You. Read the contents of the file using cat.

The contents of the file is 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ, which is the password for the next level.

To proceed to the next level ssh to the same host and port using username bandit4 and the above mentioned password.

Level 4 -> 5

Friday, October 18, 2024 9:48 AM



```
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
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
bandit4@bandit:~/inhere$
```

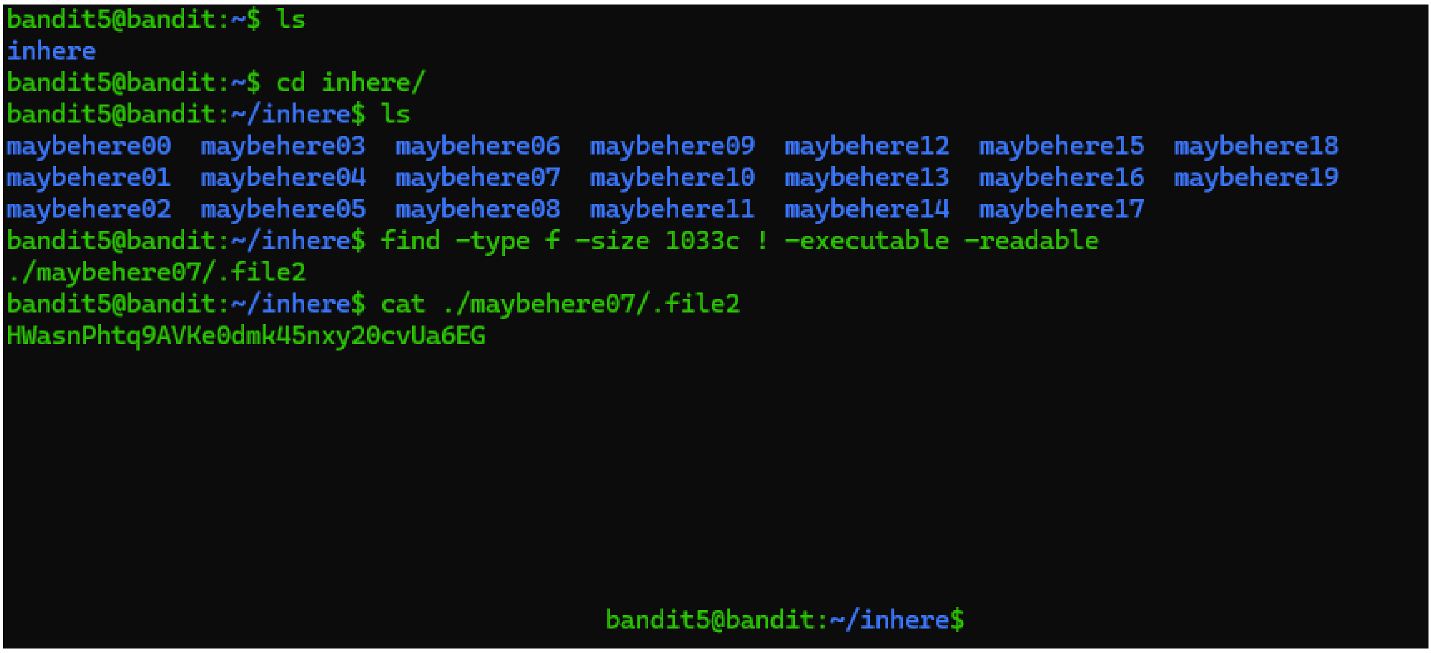
Here the password is located in a human readable file in the inhere directory. After going to the inhere directory we see many files. Using the file ./* we can see the type of the contents of the file. Here -file07 contains ASCII text which is a human readable format.

The contents of the file is 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw, which is the password for the next level.

To proceed to the next level ssh to the same host and port using username bandit5 and the above mentioned password.

Level 5 -> 6

Friday, October 18, 2024 11:18 AM



```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere03  maybehere06  maybehere09  maybehere12  maybehere15  maybehere18
maybehere01  maybehere04  maybehere07  maybehere10  maybehere13  maybehere16  maybehere19
maybehere02  maybehere05  maybehere08  maybehere11  maybehere14  maybehere17
bandit5@bandit:~/inhere$ find -type f -size 1033c ! -executable -readable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG







                                        bandit5@bandit:~/inhere$
```

The password for the next level is stored somewhere in the inhere directory and has the following properties:

1. Human readable
2. 1033 bytes in size
3. Not executable

Using the command find -type f -size 1033c ! -executable -readable, we can look for a file which satisfies the following properties.

In the find command, -type f is used to indicate that we are searching for a file (and not a directory), -size 1033c is used to indicate that the file has 1033 bytes, ! -executable means that the file is not executable and -readable means that the file is in a human readable format.

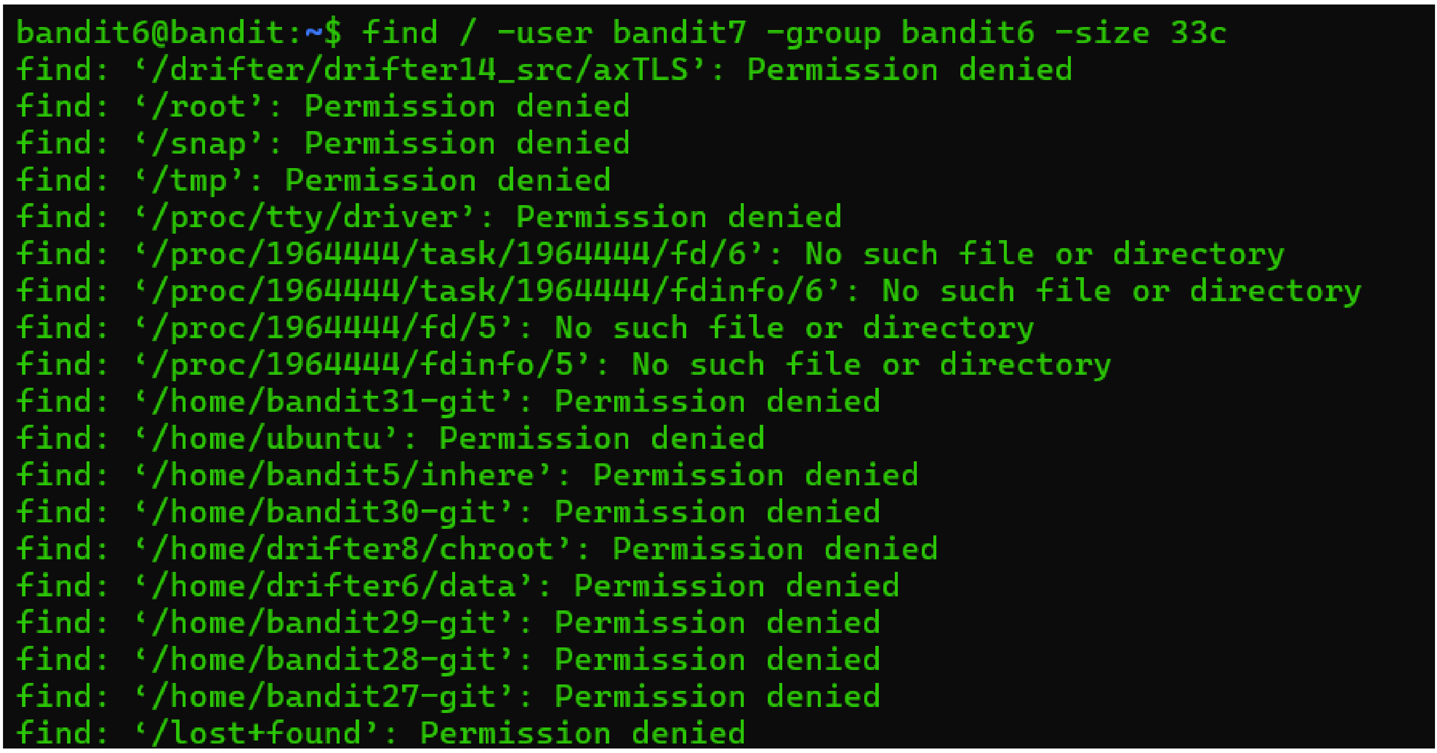
Running the command, we find out that the file is in the location inhere/maybehere07/.file2.

The contents of the file is HWasnPhtq9AVKe0dmk45nxy20cvUa6EG, which is the password for the next level.

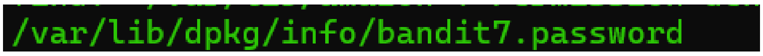
To proceed to the next level ssh to the same host and port using username bandit6 and the above mentioned password

Level 6 -> 7

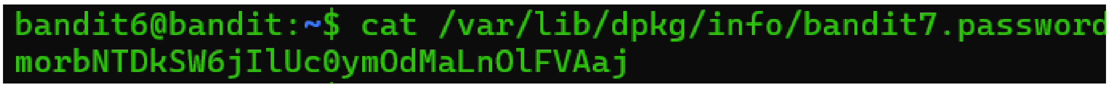
Friday, October 18, 2024 11:24 AM



```
bandit6@bandit:~$ find / -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/1964444/task/1964444/fd/6’: No such file or directory
find: ‘/proc/1964444/task/1964444/fdinfo/6’: No such file or directory
find: ‘/proc/1964444/fd/5’: No such file or directory
find: ‘/proc/1964444/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
```



```
/var/lib/dpkg/info/bandit7.password
```



```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
```

In this level 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

Using the command find / -user bandit7 -group bandit6 -size 33c we can search for the file. Here / indicates searching the entire system, -user bandit7 indicates that the file is owned by the user bandit7, -group bandit6 means that it is owned by the group bandit6 and -size 33c means its size is 33 bytes.

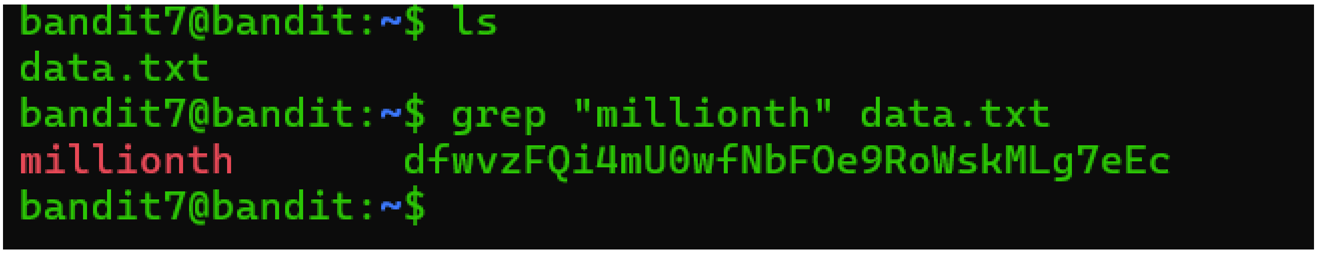
While running this command, we may see many "permission denied" errors for directories we don’t have access to. However, one result appears without error: /var/lib/dpkg/info/bandit7.password

The contents of the file is morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj, which is the password for the next level.

To proceed to the next level ssh to the same host and port using username bandit7 and the above mentioned password

Level 7 -> 8

Friday, October 18, 2024 11:40 AM



```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ grep "millionth" data.txt
millionth       dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$
```

The password is stored in the file data.txt next to the word **millionth. To search for the word millionth in the file data.txt we have to use the grep command.**

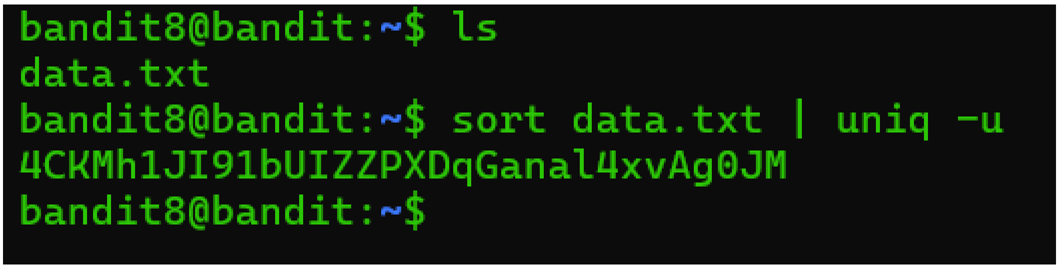
This command searches directly within the file data.txt for the word "millionth"

The password is dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc.

To proceed to the next level ssh to the same host and port using username bandit8 and the above mentioned password.

Level 8 -> 9

Friday, October 18, 2024 12:00 PM



```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:~$
```

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

To search for the password we have to use the command, sort data.txt | uniq -u.

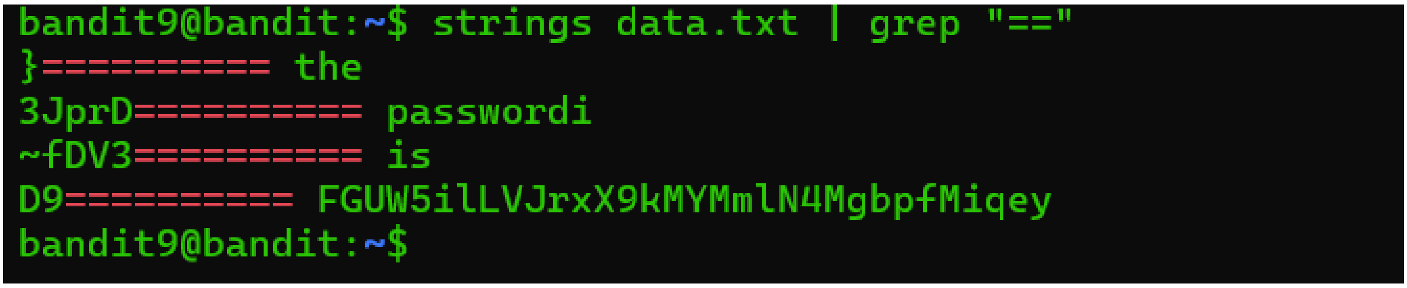
The sort command is used to sort the lines in data.txt, putting identical lines next to each other. The uniq -u command only shows lines appearing exactly once.

The password is 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM.

To proceed to the next level ssh to the same host and port using username bandit9 and the above mentioned password.

Level 9 -> 10

Friday, October 18, 2024 12:20 PM



```
bandit9@bandit:~$ strings data.txt | grep "=="
}========== the
3JprD========== passwordi
~fDV3========== is
D9========== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
bandit9@bandit:~$
```

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. We can use the strings command and pipe it with grep to get the desired result.

strings command is used to search for human readable text in a file. When we pipe it with grep, we can filter out the output according to our needs.

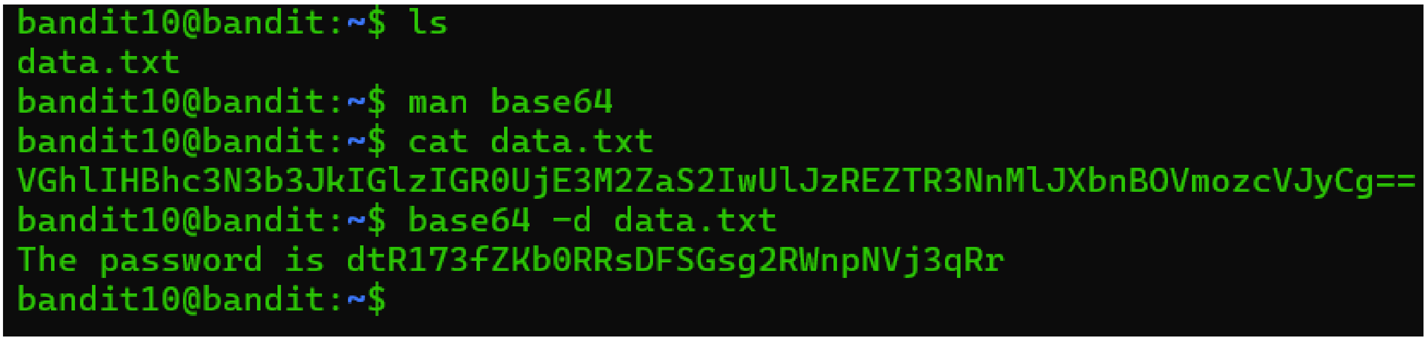
Here strings data.txt | grep "==" command looks for human readable text in data.txt, and grep filters out lines containing multiple (in this case 2) "=" symbols.

The password is FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

To proceed to the next level ssh to the same host and port using username bandit10 and the above mentioned password.

Level 10 -> 11

Friday, October 18, 2024 12:32 PM



```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ man base64
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==
bandit10@bandit:~$ base64 -d data.txt
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit:~$
```

The password for the next level is stored in the file **data.txt**, which contains base64 encoded data.
To decode this data we can use the base64 command. The command base64 -d data.txt decoded the data the data.txt to ascii format.

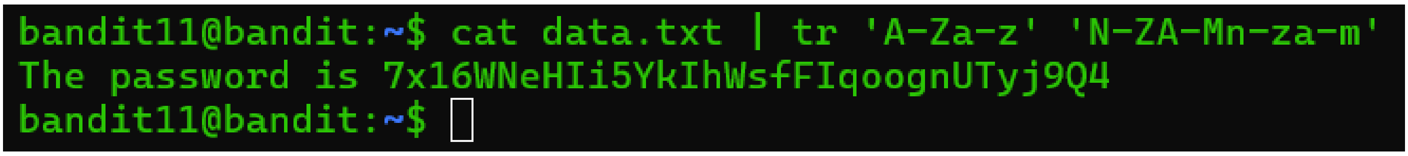
Here, the flag -d is used to decode the base64 data in data.txt to ASCII format.

The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

To proceed to the next level ssh to the same host and port using username bandit11 and the above mentioned password.

Level 11 -> 12

Friday, October 18, 2024 12:56 PM



```
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
bandit11@bandit:~$
```

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. Here we can decipher this code using the tr (translate) command.

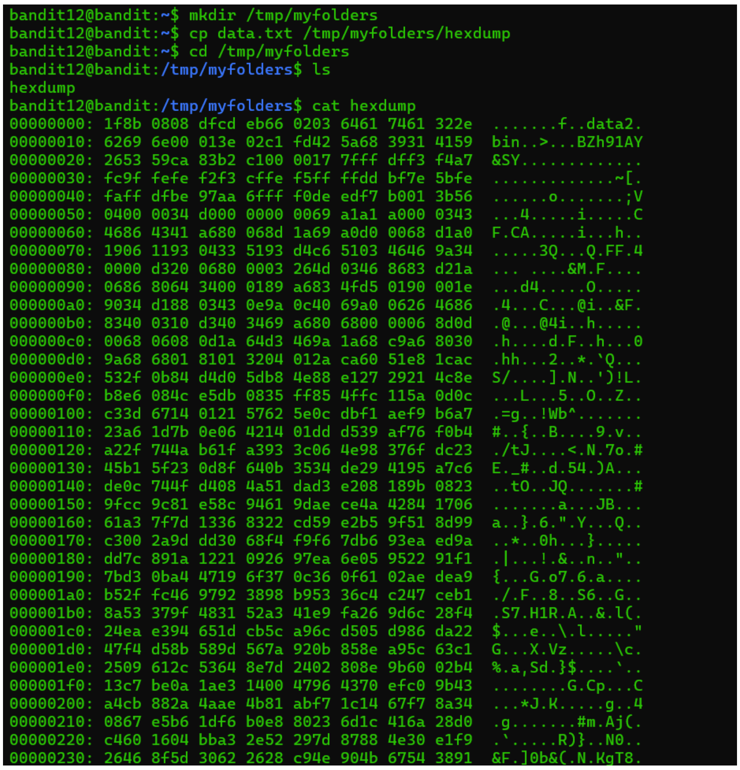
The command tr 'A-Za-z' 'N-ZA-Mn-za-m' translates all lowercase and uppercase letters in the file by rotating each letter 13 positions forward in the alphabet, and decoding the password stored in data.txt

The password is 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4

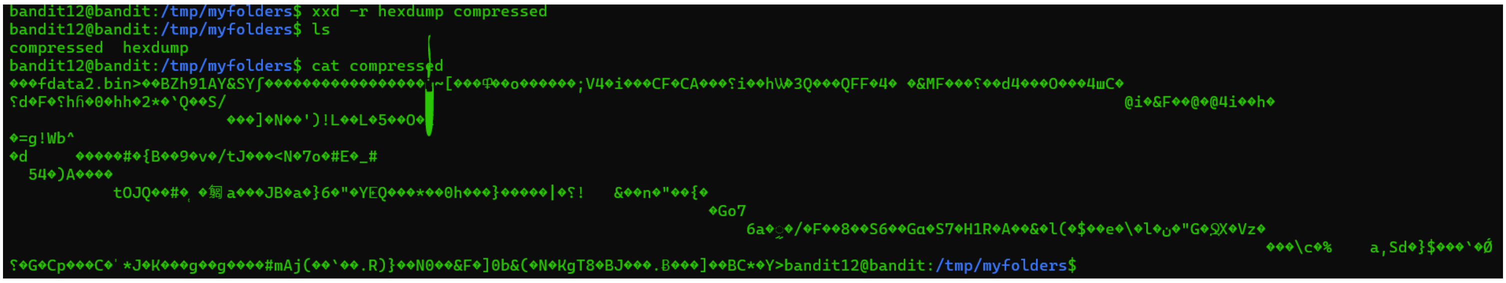
To proceed to the next level ssh to the same host and port using username bandit12 and the above mentioned password.

Level 12 -> 13

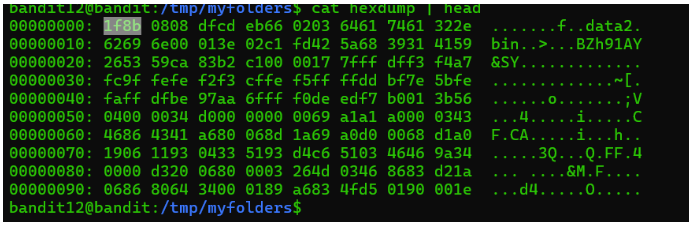
Friday, October 18, 2024 1:20 PM



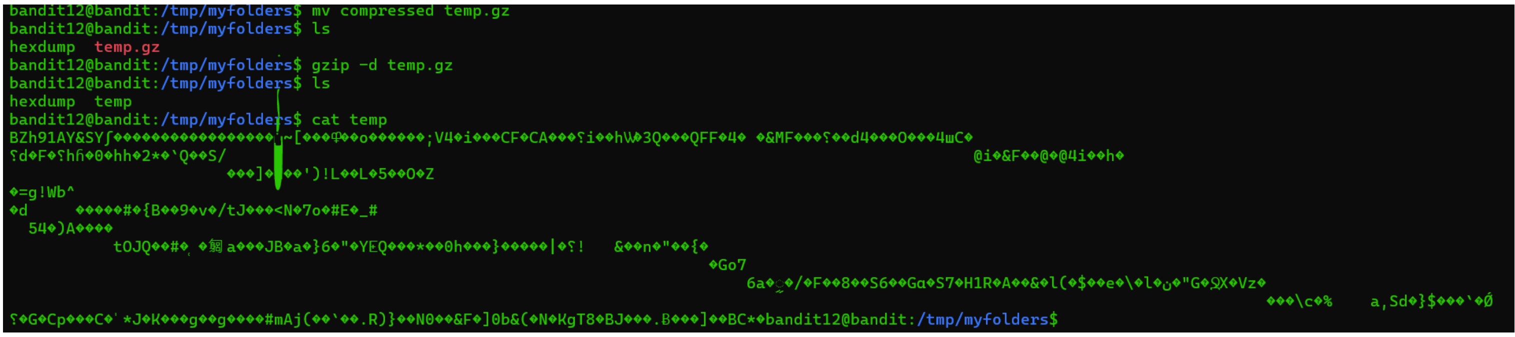
```
bandit12@bandit:~$ mkdir /tmp/myfolders
bandit12@bandit:~$ cp data.txt /tmp/myfolders/hexdump
bandit12@bandit:~$ cd /tmp/myfolders
bandit12@bandit:/tmp/myfolders$ ls
hexdump
bandit12@bandit:/tmp/myfolders$ cat hexdump
00000000: 1f8b 0808 dfcd eb66 0203 6461 7461 322e  .......f..data2.
00000010: 6269 6e00 013e 02c1 fd42 5a68 3931 4159  bin..>...BZh91AY
00000020: 2653 59ca 83b2 c100 0017 7fff dff3 f4a7  &SY.............
00000030: fc9f fefe f2f3 cffe f5ff ffdd bf7e 5bfe  .............~[.
00000040: faff dfbe 97aa 6fff f0de edf7 b001 3b56  ......o.......;V
00000050: 0400 0034 d000 0000 0069 a1a1 a000 0343  ...4.....i.....C
00000060: 4686 4341 a680 068d 1a69 a0d0 0068 d1a0  F.CA.....i...h..
00000070: 1906 1193 0433 5193 d4c6 5103 4646 9a34  .....3Q...Q.FF.4
00000080: 0000 d320 0680 0003 264d 0346 8683 d21a  ... ....&M.F....
00000090: 0686 8064 3400 0189 a683 4fd5 0190 001e  ...d4.....O.....
000000a0: 9034 d188 0343 0e9a 0c40 69a0 0626 4686  .4...C...@i..&F.
000000b0: 8340 0310 d340 3469 a680 6800 0006 8d0d  .@...@4i..h.....
000000c0: 0068 0608 0d1a 64d3 469a 1a68 c9a6 8030  .h....d.F..h...0
000000d0: 9a68 6801 8101 3204 012a ca60 51e8 1cac  .hh...2..*.`Q...
000000e0: 532f 0b84 d4d0 5db8 4e88 e127 2921 4c8e  S/....].N..')!L.
000000f0: b8e6 084c e5db 0835 ff85 4ffc 115a 0d0c  ...L...5..O..Z..
00000100: c33d 6714 0121 5762 5e0c dbf1 aef9 b6a7  .=g..!Wb^.......
00000110: 23a6 1d7b 0e06 4214 01dd d539 af76 f0b4  #..{..B....9.v..
00000120: a22f 744a b61f a393 3c06 4e98 376f dc23  ./tJ....<.N.7o.#
00000130: 45b1 5f23 0d8f 640b 3534 de29 4195 a7c6  E._#..d.54.)A...
00000140: de0c 744f d408 4a51 dad3 e208 189b 0823  ..tO..JQ.......#
00000150: 9fcc 9c81 e58c 9461 9dae ce4a 4284 1706  .......a...JB...
00000160: 61a3 7f7d 1336 8322 cd59 e2b5 9f51 8d99  a..}.6.".Y...Q..
00000170: c300 2a9d dd30 68f4 f9f6 7db6 93ea ed9a  ..*..0h...}.....
00000180: dd7c 891a 1221 0926 97ea 6e05 9522 91f1  .|...!.&..n.."..
00000190: 7bd3 0ba4 4719 6f37 0c36 0f61 02ae dea9  {...G.o7.6.a....
000001a0: b52f fc46 9792 3898 b953 36c4 c247 ceb1  ./.F..8..S6..G..
000001b0: 8a53 379f 4831 52a3 41e9 fa26 9d6c 28f4  .S7.H1R.A..&.l(.
000001c0: 24ea e394 651d cb5c a96c d505 d986 da22  $...e..\.l....."
000001d0: 47f4 d58b 589d 567a 920b 858e a95c 63c1  G...X.Vz.....\c.
000001e0: 2509 612c 5364 8e7d 2402 808e 9b60 02b4  %.a,Sd.}$....`..
000001f0: 13c7 be0a 1ae3 1400 4796 4370 efc0 9b43  ........G.Cp...C
00000200: a4cb 882a 4aae 4b81 abf7 1c14 67f7 8a34  ...*J.K.....g..4
00000210: 0867 e5b6 1df6 b0e8 8023 6d1c 416a 28d0  .g.......#m.Aj(.
00000220: c460 1604 bba3 2e52 297d 8788 4e30 e1f9  .`.....R)}..N0..
00000230: 2646 8f5d 3062 2628 c94e 904b 6754 3891  &F.]0b&(.N.KgT8.
```



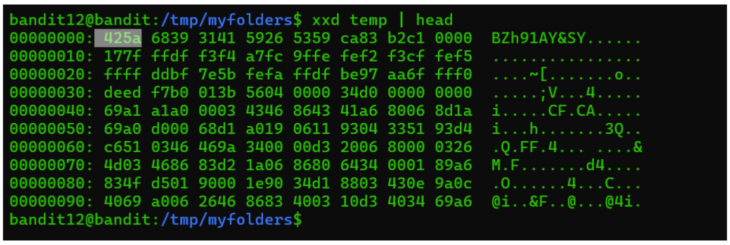
```
bandit12@bandit:/tmp/myfolders$ xxd -r hexdump compressed
bandit12@bandit:/tmp/myfolders$ ls
compressed  hexdump
bandit12@bandit:/tmp/myfolders$ cat compressed
���fdata2.bin>��BZh91AY&SYʃ������������������~[���Ҩ��o������;V4�i���CF�CA���ʕi��hW�3Q���QFF�4� �&MF���ʕ��d4���O���4шC�
ʕd�F�ʕhɦ�0�hh�2*�`Q��S/                                                                                              @i�&F��@�@4i��h�
                      ���]�N��')!L��L�5��O�

�=g!Wb^
�d     �����#�{B��9�v�/tJ���<N�7o�#E�_#
  54�)A����
         tOJQ��#� �䵒 a���JB�a�}6�"�YEQ���*���0h���}�����|�ʕ!   &��n�"��{�
                                                                              �Go7
                                                                                  6a�ͅ�/�F��8��S6��Gɑ�S7�H1R�A��&�l(�$��e�\�l�ن�"G�ΩX�Vz�
                                                                                                                                    ���\c�%    a,Sd�}$���`�Ǿ
ʕ�G�Cp���C�ʹ*J�K���g��g����#mAj(��`��.R)}��N0��&F�]0b&(�N�KgT8�BJ���.Ƀ���]��BC*�Y>bandit12@bandit:/tmp/myfolders$
```



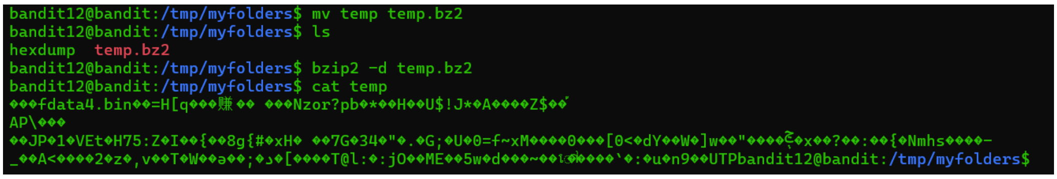
```
bandit12@bandit:/tmp/myfolders$ cat hexdump | head
00000000: 1f8b 0808 dfcd eb66 0203 6461 7461 322e  .......f..data2.
00000010: 6269 6e00 013e 02c1 fd42 5a68 3931 4159  bin..>...BZh91AY
00000020: 2653 59ca 83b2 c100 0017 7fff dff3 f4a7  &SY.............
00000030: fc9f fefe f2f3 cffe f5ff ffdd bf7e 5bfe  .............~[.
00000040: faff dfbe 97aa 6fff f0de edf7 b001 3b56  ......o.......;V
00000050: 0400 0034 d000 0000 0069 a1a1 a000 0343  ...4.....i.....C
00000060: 4686 4341 a680 068d 1a69 a0d0 0068 d1a0  F.CA.....i...h..
00000070: 1906 1193 0433 5193 d4c6 5103 4646 9a34  .....3Q...Q.FF.4
00000080: 0000 d320 0680 0003 264d 0346 8683 d21a  ... ....&M.F....
00000090: 0686 8064 3400 0189 a683 4fd5 0190 001e  ...d4.....O.....
bandit12@bandit:/tmp/myfolders$
```



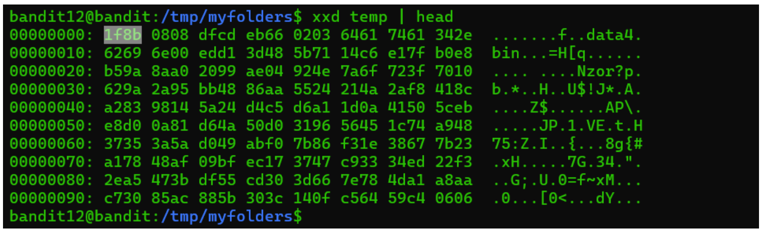
```
bandit12@bandit:/tmp/myfolders$ mv compressed temp.gz
bandit12@bandit:/tmp/myfolders$ ls
hexdump  temp.gz
bandit12@bandit:/tmp/myfolders$ gzip -d temp.gz
bandit12@bandit:/tmp/myfolders$ ls
hexdump  temp
bandit12@bandit:/tmp/myfolders$ cat temp
BZh91AY&SYʃ������������������~[���Ҩ��o������;V4�i���CF�CA���ʕi��hW�3Q���QFF�4� �&MF���ʕ��d4���O���4шC�
ʕd�F�ʕhɦ�0�hh�2*�`Q��S/                                                                        @i�&F��@�@4i��h�
                      ���]���')!L��L�5��O�Z

�=g!Wb^
�d     �����#�{B��9�v�/tJ���<N�7o�#E�_#
  54�)A����
         tOJQ��#� �䵒 a���JB�a�}6�"�YEQ���*���0h���}�����|�ʕ!   &��n�"��{�
                                                                              �Go7
                                                                                  6a�ͅ�/�F��8��S6��Gɑ�S7�H1R�A��&�l(�$��e�\�l�ن�"G�ΩX�Vz�
                                                                                                                                    ���\c�%    a,Sd�}$���`�Ǿ
ʕ�G�Cp���C�ʹ*J�K���g��g����#mAj(��`��.R)}��N0��&F�]0b&(�N�KgT8�BJ���.Ƀ���]��BC*�bandit12@bandit:/tmp/myfolders$
```



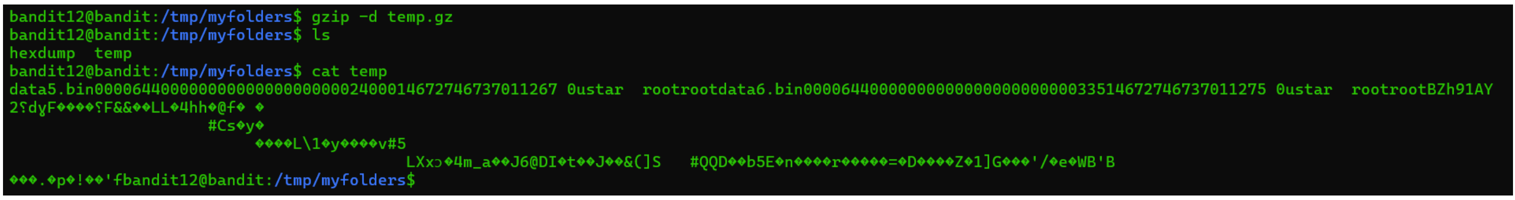
```
bandit12@bandit:/tmp/myfolders$ xxd temp | head
00000000: 425a 6839 3141 5926 5359 ca83 b2c1 0000  BZh91AY&SY......
00000010: 177f ffdf f3f4 a7fc 9ffe fef2 f3cf fef5  ................
00000020: ffff ddbf 7e5b fefa ffdf be97 aa6f fff0  ....~[.......o..
00000030: deed f7b0 013b 5604 0000 34d0 0000 0000  .....;V...4.....
00000040: 69a1 a1a0 0003 4346 8643 41a6 8006 8d1a  i.....CF.CA.....
00000050: 69a0 d000 68d1 a019 0611 9304 3351 93d4  i...h.......3Q..
00000060: c651 0346 469a 3400 00d3 2006 8000 0326  .Q.FF.4... ....&
00000070: 4d03 4686 83d2 1a06 8680 6434 0001 89a6  M.F.......d4....
00000080: 834f d501 9000 1e90 34d1 8803 430e 9a0c  .O......4...C...
00000090: 4069 a006 2646 8683 4003 10d3 4034 69a6  @i..&F..@...@4i.
bandit12@bandit:/tmp/myfolders$
```



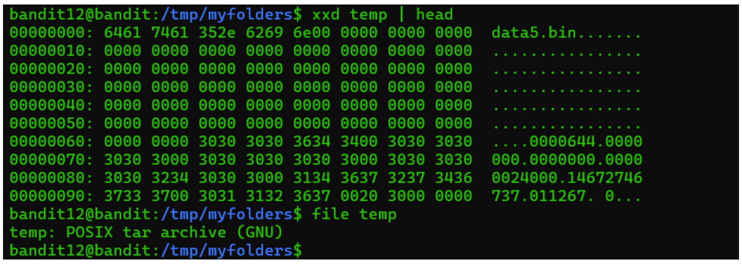
```
bandit12@bandit:/tmp/myfolders$ mv temp temp.bz2
bandit12@bandit:/tmp/myfolders$ ls
hexdump  temp.bz2
bandit12@bandit:/tmp/myfolders$ bzip2 -d temp.bz2
bandit12@bandit:/tmp/myfolders$ cat temp
���fdata4.bin��=H[q���赚�� ���Nzor?pb�*��H��U$!J*�A����Z$��
AP\���
��JP�1�VEt�H75:Z�I��{��8g{#�xH� ��7G�34�"�.�G;�U�0=f~xM����0���[0<�dY��W�]w��"����ꩿ�x��?��:��{�Nmhs����-
_��A<����2�z�,v��T�W��ə��;�ɔ�[����T@l:�:jO��ME��5w�d���~��ꩿ����`�:�u�n9��UTPbandit12@bandit:/tmp/myfolders$
```



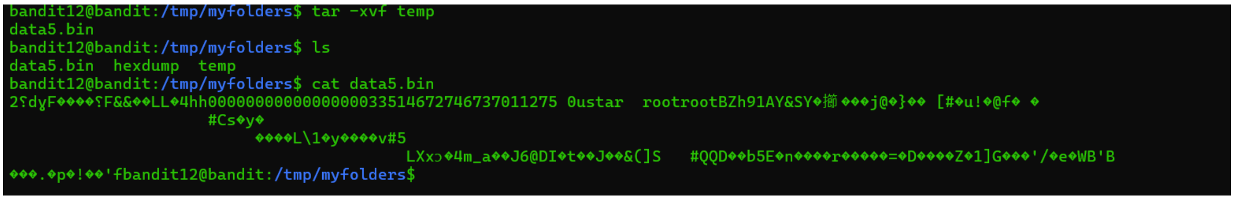
```
bandit12@bandit:/tmp/myfolders$ xxd temp | head
00000000: 1f8b 0808 dfcd eb66 0203 6461 7461 342e  .......f..data4.
00000010: 6269 6e00 edd1 3d48 5b71 14c6 e17f b0e8  bin...=H[q......
00000020: b59a 8aa0 2099 ae04 924e 7a6f 723f 7010  .... ....Nzor?p.
00000030: 629a 2a95 bb48 86aa 5524 214a 2af8 418c  b.*..H..U$!J*.A.
00000040: a283 9814 5a24 d4c5 d6a1 1d0a 4150 5ceb  ....Z$......AP\.
00000050: e8d0 0a81 d64a 50d0 3196 5645 1c74 a948  .....JP.1.VE.t.H
00000060: 3735 3a5a d049 abf0 7b86 f31e 3867 7b23  75:Z.I..{...8g{#
00000070: a178 48af 09bf ec17 3747 c933 34ed 22f3  .xH.....7G.34.".
00000080: 2ea5 473b df55 cd30 3d66 7e78 4da1 a8aa  ..G;.U.0=f~xM...
00000090: c730 85ac 885b 303c 140f c564 59c4 0606  .0...[0<...dY...
bandit12@bandit:/tmp/myfolders$
```



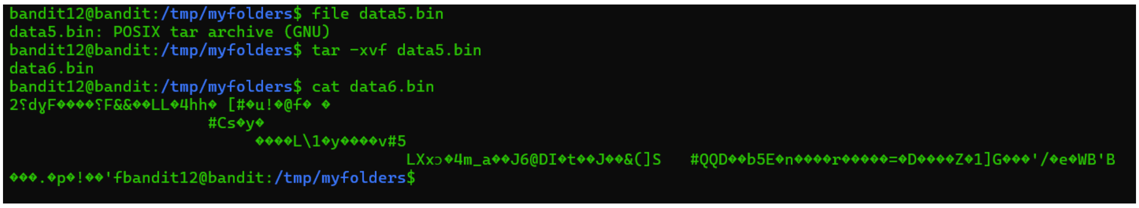
```
bandit12@bandit:/tmp/myfolders$ gzip -d temp.gz
bandit12@bandit:/tmp/myfolders$ ls
hexdump  temp
bandit12@bandit:/tmp/myfolders$ cat temp
data5.bin0000644000000000000000000000024000146727467370112670ustar  rootrootdata6.bin0000644000000000000000000000033514672746737011275 0ustar  rootrootBZh91AY
2ʕdyF����ʕF&��LL�4hh�@f� �
                     #Cs�y�
                          ����L\1�y����v#5
                                          LXxɔ�4m_a��J6@DI�t��J��&(]S   #QQD��b5E�n����r�����=�D����Z�1]G���'/�e�WB'B
���.�p�!��'fbandit12@bandit:/tmp/myfolders$
```



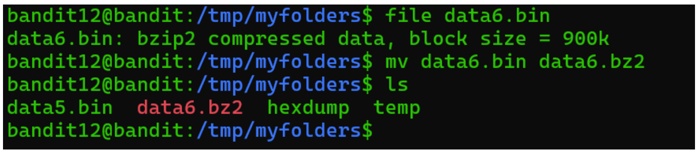
```
bandit12@bandit:/tmp/myfolders$ xxd temp | head
00000000: 6461 7461 352e 6269 6e00 0000 0000 0000  data5.bin.......
00000010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000040: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000050: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000060: 0000 0000 3030 3030 3634 3400 3030 3030  ....0000644.0000
00000070: 3030 3000 3030 3030 3030 3000 3030 3030  000.0000000.0000
00000080: 3030 3234 3030 3000 3134 3637 3237 3436  0024000.14672746
00000090: 3733 3700 3031 3132 3637 0020 3000 0000  737.011267. 0...
bandit12@bandit:/tmp/myfolders$ file temp
temp: POSIX tar archive (GNU)
bandit12@bandit:/tmp/myfolders$
```



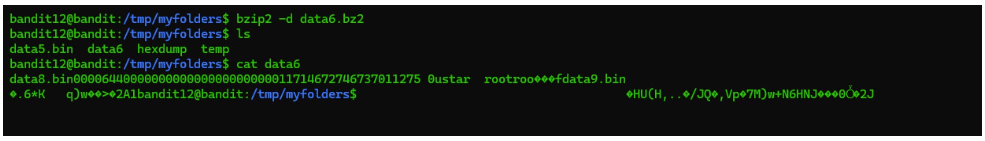
```
bandit12@bandit:/tmp/myfolders$ tar -xvf temp
data5.bin
bandit12@bandit:/tmp/myfolders$ ls
data5.bin  hexdump  temp
bandit12@bandit:/tmp/myfolders$ cat data5.bin
2ʕdyF����ʕF&��LL�4hh000000000000000000335146727467370112750ustar  rootrootBZh91AY&SY�擜���j@�}�� [#�u!�@f� �
                     #Cs�y�
                          ����L\1�y����v#5
                                          LXxɔ�4m_a��J6@DI�t��J��&(]S   #QQD��b5E�n����r�����=�D����Z�1]G���'/�e�WB'B
���.�p�!��'fbandit12@bandit:/tmp/myfolders$
```



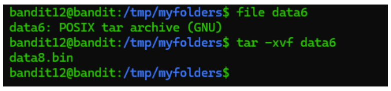
```
bandit12@bandit:/tmp/myfolders$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/myfolders$ tar -xvf data5.bin
data6.bin
bandit12@bandit:/tmp/myfolders$ cat data6.bin
2ʕdyF����ʕF&��LL�4hh� [#�u!�@f� �
                     #Cs�y�
                          ����L\1�y����v#5
                                          LXxɔ�4m_a��J6@DI�t��J��&(]S   #QQD��b5E�n����r�����=�D����Z�1]G���'/�e�WB'B
���.�p�!��'fbandit12@bandit:/tmp/myfolders$
```



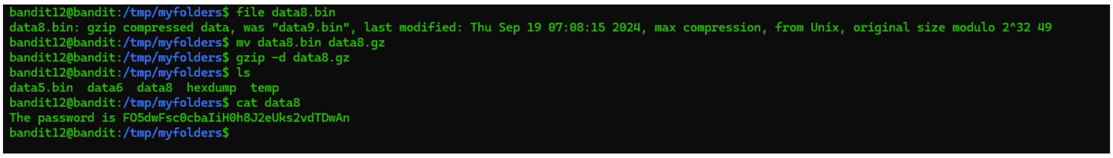
```
bandit12@bandit:/tmp/myfolders$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/myfolders$ mv data6.bin data6.bz2
bandit12@bandit:/tmp/myfolders$ ls
data5.bin  data6.bz2  hexdump  temp
bandit12@bandit:/tmp/myfolders$
```



```
bandit12@bandit:/tmp/myfolders$ bzip2 -d data6.bz2
bandit12@bandit:/tmp/myfolders$ ls
data5.bin  data6  hexdump  temp
bandit12@bandit:/tmp/myfolders$ cat data6
data8.bin000064400000000000000000000117146727467370112750ustar  rootroo���fdata9.bin
�.6*K   q)w��>�2A1bandit12@bandit:/tmp/myfolders$                                    �HU(H,..�/JQ�,Vp�7M)w+N6HNJ���0Ǒ�2J
```



```
bandit12@bandit:/tmp/myfolders$ file data6
data6: POSIX tar archive (GNU)
bandit12@bandit:/tmp/myfolders$ tar -xvf data6
data8.bin
bandit12@bandit:/tmp/myfolders$
```



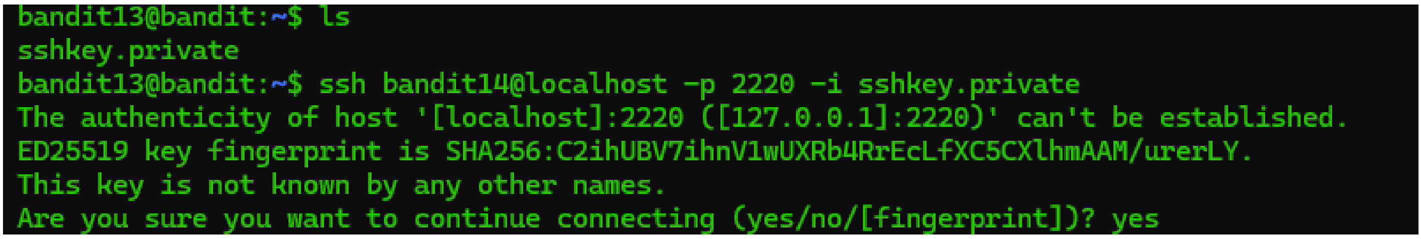
```
bandit12@bandit:/tmp/myfolders$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/myfolders$ mv data8.bin data8.gz
bandit12@bandit:/tmp/myfolders$ gzip -d data8.gz
bandit12@bandit:/tmp/myfolders$ ls
data5.bin  data6  data8  hexdump  temp
bandit12@bandit:/tmp/myfolders$ cat data8
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
bandit12@bandit:/tmp/myfolders$
```

The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn

To proceed to the next level ssh to the same host and port using username bandit13 and the above mentioned password.

Level 13 -> 14

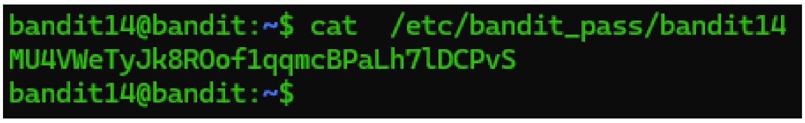
Friday, October 18, 2024 2:25 PM



```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh bandit14@localhost -p 2220 -i sshkey.private
The authenticity of host '[localhost]: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
```

The password for the next level is stored in **/etc/bandit_pass/bandit14 and can only be read by user bandit14. To log in as user bandit14, we can ssh to localhost using the private ssh key sshkey.private**

In the command ssh bandit14@localhost -p 2220 -i sshkey.private, the -i flag is used to login to the user bandit14 using key based authentication instead of password based authentication. sshkey.private is the key used to log in.



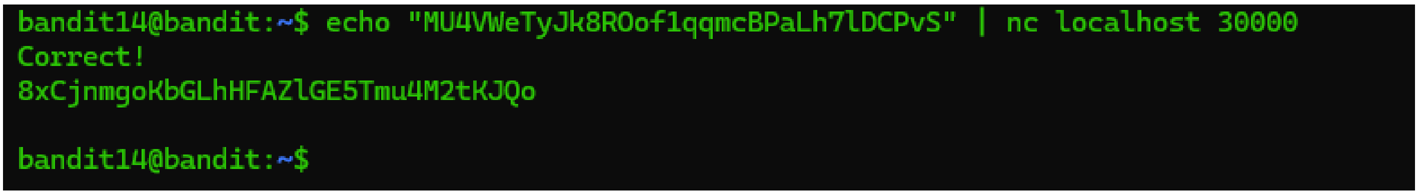
```
bandit14@bandit:~$ cat  /etc/bandit_pass/bandit14
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
bandit14@bandit:~$
```

Once we are logged in as bandit14 we can cat the file **/etc/bandit_pass/bandit14**

The password is MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS

Level 14 -> 15

Friday, October 18, 2024 2:37 PM



```
bandit14@bandit:~$ echo "MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS" | nc localhost 30000
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

bandit14@bandit:~$
```

The password for the next level can be retrieved by submitting the password of the current level to **port 30000 on localhost**.

We can use netcat to retrieve the password.

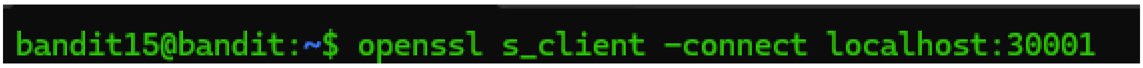
Here the command echo "MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS" | nc localhost 30000,

Sends to the service running on port 30000 on localhost the content , and we get the password as the response.

The password to the next level is 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

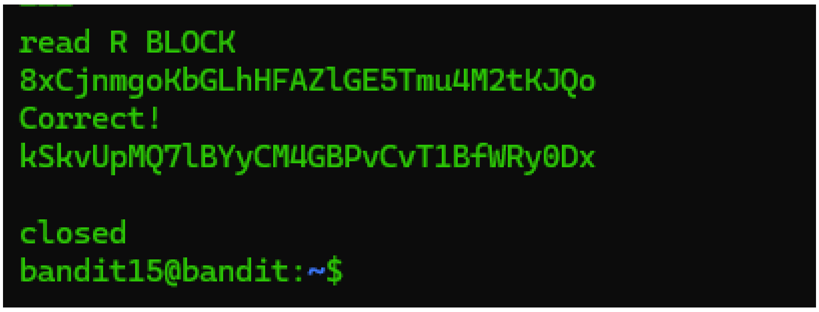
Level 15 -> 16

Friday, October 18, 2024 2:47 PM



```
bandit15@bandit:~$ openssl s_client -connect localhost:30001
```

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. Here we can use the openssl command to connect to localhost on port 30001 using SSL/TLS.



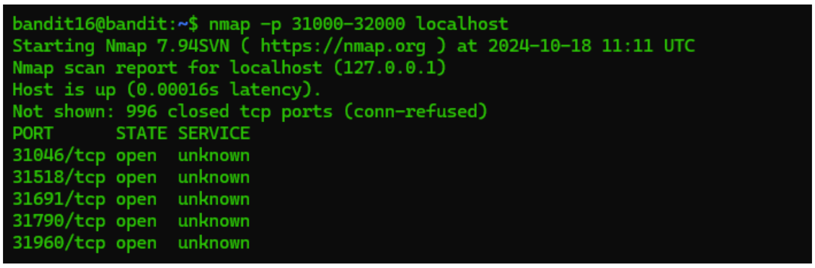
```
read R BLOCK
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
Correct!
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

closed
bandit15@bandit:~$
```

Here we are sending the password of the previous level to the server. The server then responds with the password of the next level.

The password for the next level is kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

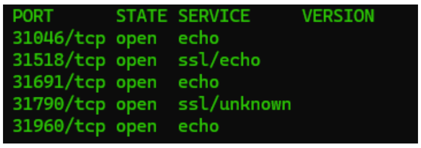
Level 16 -> 17

Friday, October 18, 2024 3:05 PM



```
bandit16@bandit:~$ nmap -p 31000-32000 localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 11:11 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00016s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown
```

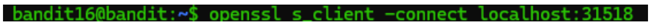
The credentials for the next level can be retrieved by submitting the password of the current level to **a port on localhost in the range 31000 to 32000. Here we use nmap to scan all the ports in the range 31000 to 32000 to determine which ports are open.**



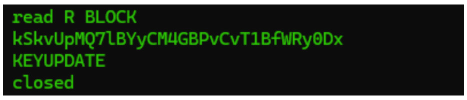
```
PORT      STATE SERVICE     VERSION
31046/tcp open  echo
31518/tcp open  ssl/echo
31691/tcp open  echo
31790/tcp open  ssl/unknown
31960/tcp open  echo
```

Using the command nmap -sV -p 31046,31518,31691,31790,31960 localhost, we scan only the list of ports which are open. The -sV flag is used to detect the service running on the port.

Here port 31518 and 31790 are running SSL.

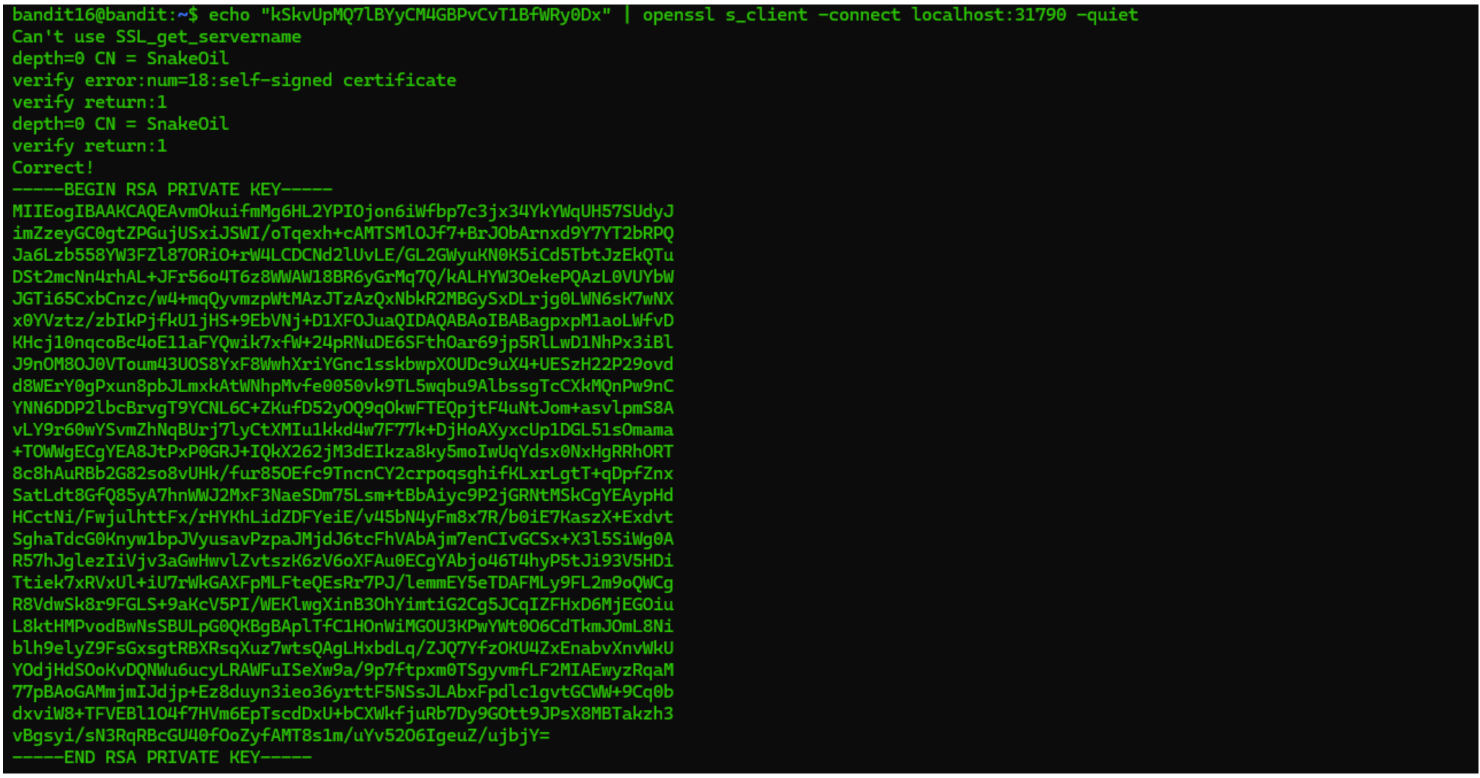


```
bandit16@bandit:~$ openssl s_client -connect localhost:31518
```



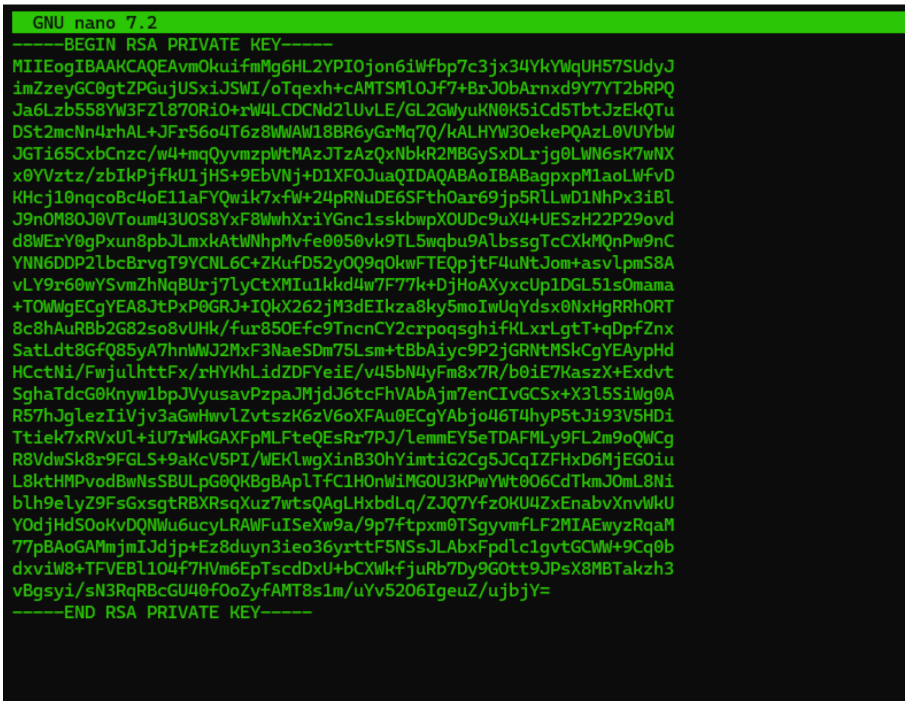
```
read R BLOCK
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
KEYUPDATE
closed
```

When we try to connect to port 31518 using openssl, and then provide it the password, it doesn't provide us the credentials for the next level. Let us now try connecting to port 31790.



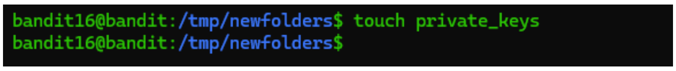
```
bandit16@bandit:~$ echo "kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx" | openssl s_client -connect localhost:31790 -quiet
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
Correct!
-----BEGIN RSA PRIVATE KEY-----
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/v45bN4yFm8x7R/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-----
```

Here we get a response that includes a RSA private key. We can use this key to log in to the next level.



```
  GNU nano 7.2
-----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/v45bN4yFm8x7R/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-----
```

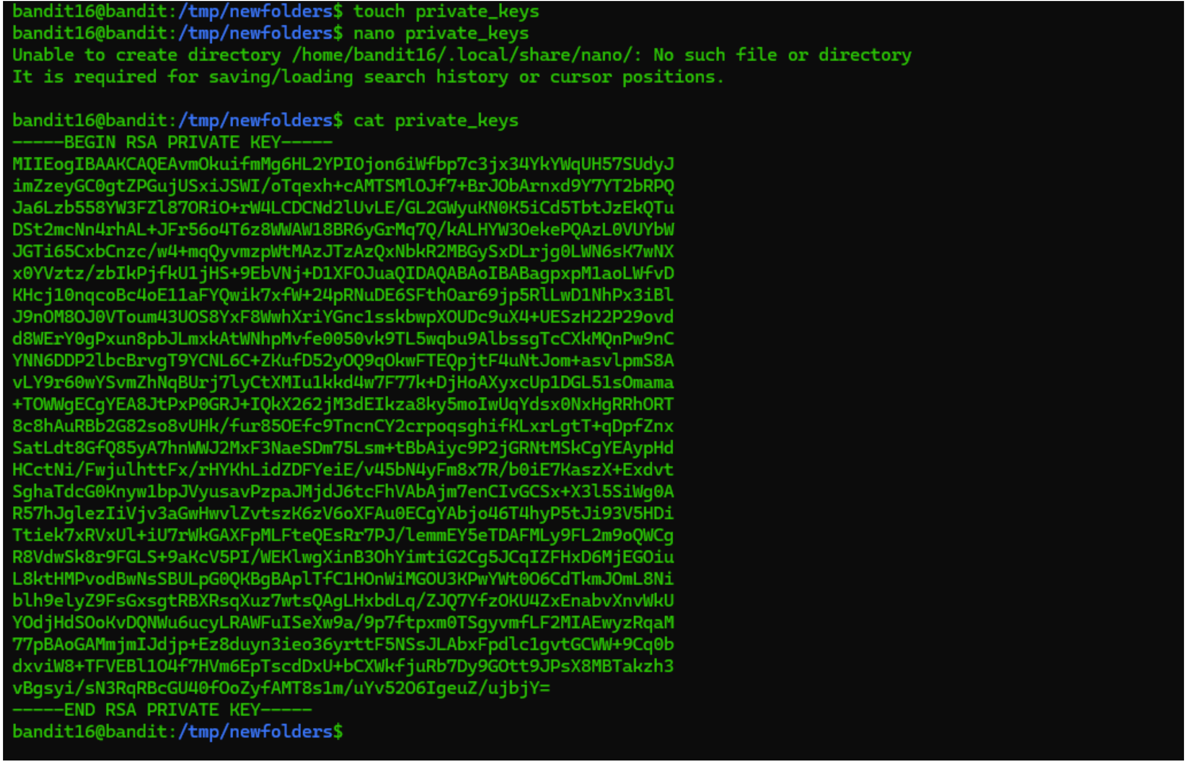
Open a cli text editor, like nano, and save the key into a file



```
bandit16@bandit:/tmp/newfolders$ touch private_keys
bandit16@bandit:/tmp/newfolders$
```

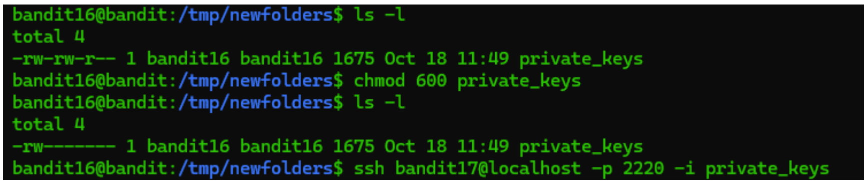
In order to have permission to write to a file, create a directory in /tmp (here I have created /tmp/newfolders). Then I have created a file private_keys using the touch command.

Save the contents of the RSA private key in the file.



```
bandit16@bandit:/tmp/newfolders$ touch private_keys
bandit16@bandit:/tmp/newfolders$ nano private_keys
Unable to create directory /home/bandit16/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit16@bandit:/tmp/newfolders$ cat private_keys
-----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/v45bN4yFm8x7R/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-----
bandit16@bandit:/tmp/newfolders$
```

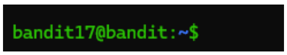
Here we have written the contents of RSA key in the file private_keys



```
bandit16@bandit:/tmp/newfolders$ ls -l
total 4
-rw-rw-r-- 1 bandit16 bandit16 1675 Oct 18 11:49 private_keys
bandit16@bandit:/tmp/newfolders$ chmod 600 private_keys
bandit16@bandit:/tmp/newfolders$ ls -l
total 4
-rw------- 1 bandit16 bandit16 1675 Oct 18 11:49 private_keys
bandit16@bandit:/tmp/newfolders$ ssh bandit17@localhost -p 2220 -i private_keys
```

Here we have changed the permission of private_keys using the chmod command, and the logged into bandit17 using ssh.

Using ls -l we can see that initially, the file private_keys had the permission rw-rw-r, which means that the owner, group as well as all other users can read the file. But a private key is supposed to be private and only accessible to the owner and no one else. Hence, we use chmod 600 so that only the owner has the permission to read and write to the file. This allows the ssh client to use the key for authorization. If the permissions on your private SSH key allow access to others, the SSH client will refuse to use that key for authentication.

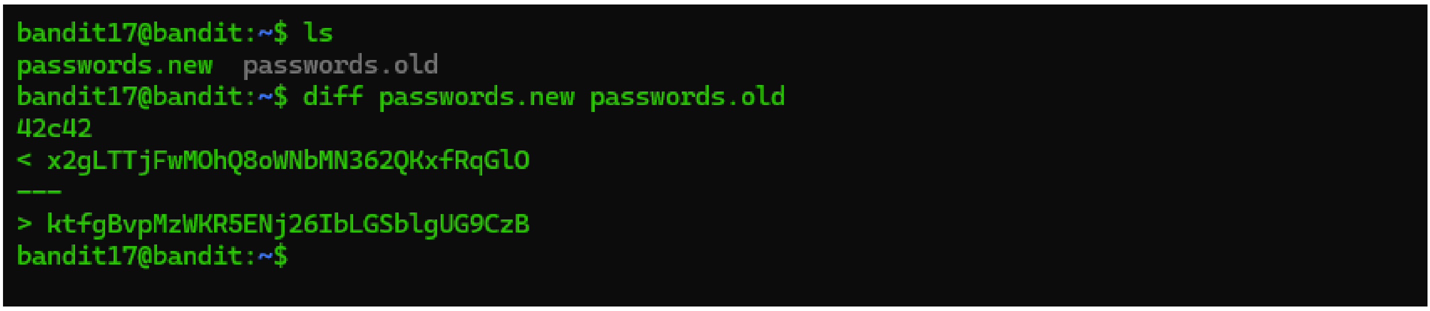


```
bandit17@bandit:~$
```

We have successfully logged in as bandit17

Level 17 -> 18

Friday, October 18, 2024 3:59 PM



```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.new passwords.old
42c42
< x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
---
> ktfgBvpMzWKR5ENj26IbLGSblgUG9CzB
bandit17@bandit:~$
```

There 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.**

Using the diff command we can compare both the files. We see that the only line changed is x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO

This is the password for the next level.