Over the wire Bandit: WriteUp

Level 0 + Level 0->1

About Challenge: 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”**

Application Used: used online website **“https://ssheasy.com/”** to solve the following SSH problem till the rest of the levels

Methodology: ls command is used to give us list of folders available while cat “filename” is used to give the content in it, here filename readme contained the password to next level which came out to be **“NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL”** , the list of commands given in “commands you may need to solve this level” gave it away the use of ls, cat etc.

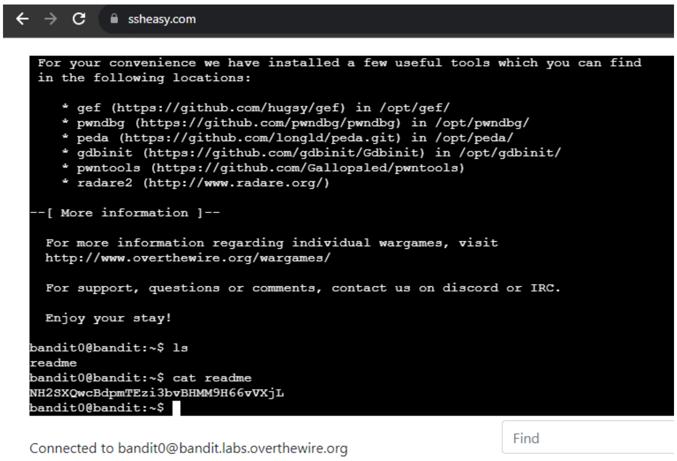
Solution: Using ls we found readme existed and using cat readme we got the password to next level i.e. “**NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL”**

>ls

readme

>cat readme

NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL



```
 For your convenience we have installed a few useful tools which you can find
 in the following locations:

    * gef (https://github.com/hugsy/gef) in /opt/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
    * peda (https://github.com/longld/peda.git) in /opt/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

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

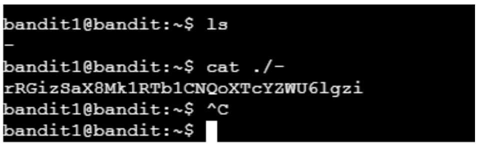
Connected to bandit0@bandit.labs.overthewire.org

Level 1->2

To proceed to next level we needed to login to bandit1 using password we obtained from level0->1, so we had to type “**exit**” in order to logout from bandit0

Like the previous level we use “ls” command to find the file “-“ as per the challenge however the “helpful reading material” sections awares us we can’t simply type “cat –“ to access it and we had to go for “cat ./-“ from where we obtain the password now successfully as “rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi” for next level

Problem faced: Using “cat –“ directly which was not as it was supposed to be



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

Level 2->3

To proceed to next level just like before we had to type “exit” to logout from bandit1 and login to bandit2 with the password we got

In this level using ls we saw that the file existed in form of

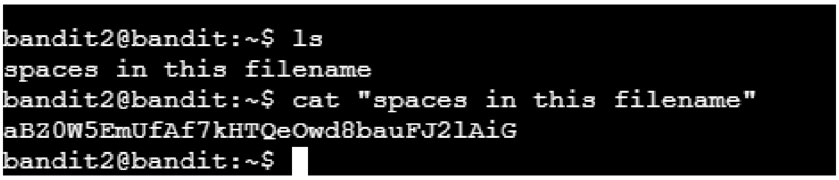
spaces in this filename

when read through reading material we saw that not all filename approves spaces and so was the case going through chatgpt it was known that for linux we can use quotation in such case and use it like a string so now using

>cat “spaces in this filename”

aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

the following was our password to go through next level



```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat "spaces in this filename"
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
bandit2@bandit:~$
```

Level 3->4

Like all previous level we need to exit to logout from bandit2 and login to bandit3 using password we got

Now the challenge here was to go through a hidden file

after going through list of commands we saw we can get it using the cd command

>ls

inhere

>cd inhere

>ls -a

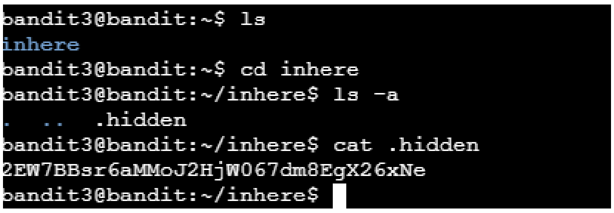
.hidden

>cat .hidden

2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

which is our password to next level

Problem faced: 2-3 error before finally learning the cd command stuff



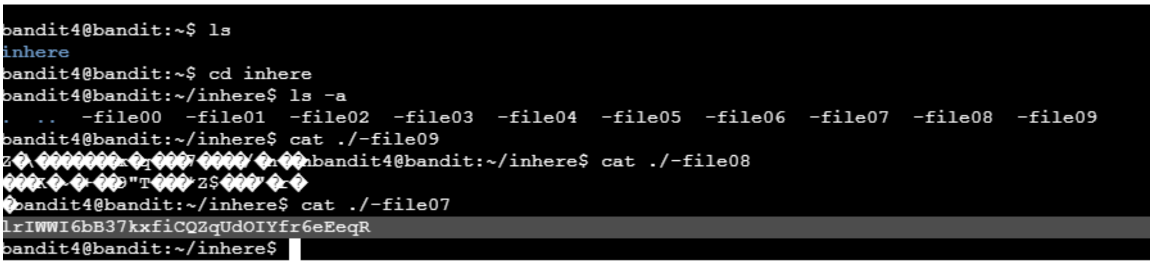
```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$
```

Level 4->5

Challenge: The password for the next level is stored in the only human-readable file in the inhere directory

Like everytime we logout from previous bandit to current bandit4 using the password we got from level above here using ls we get all the filename available and there were 10 -file00 to -file09 so we had to use cat -fileXY (XY= 00, 01, 02,….,09) till we get a human readable file as mentioned in the challenge

from there we obtained the password in -file07 with the password being lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR



```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -a
.  ..  -file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ cat ./-file09
Z�\�������x�q���7����/�n��nbandit4@bandit:~/inhere$ cat ./-file08
���K�~�+��9"T���'Z$���'�r�
�bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$
```

Level 5->6

Logout from bandit4 and login to bandit5 using the password above

Challenge: 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

Here we need to use "find" command and it's find type, size attributes so that we can check all the things mentioned like 1033 be its byte size

travel through inhere using cd then specify the find command as per the challenge we get "./maybehere07/.file2" which is the file human readable, 1033bytes and not executable

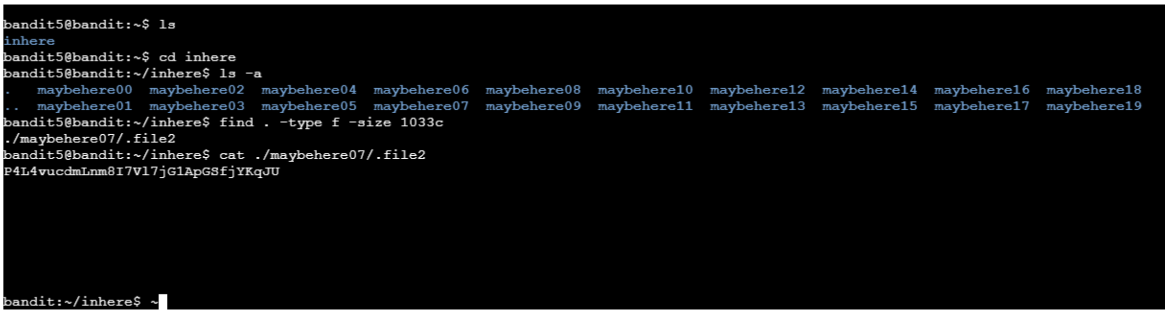
typing

>cat ./maybehere07/.file2

P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

we get our password to next level

Problem Faced: while executing find command



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




bandit:~/inhere$ ~
```

Level 6->7

Logout from bandit5 and login to bandit6 by typing exit and using password obtained from previous level

Challenge: 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 following code of find we saw a list in which everything was permission denied except the line with “bandit7.password” in it

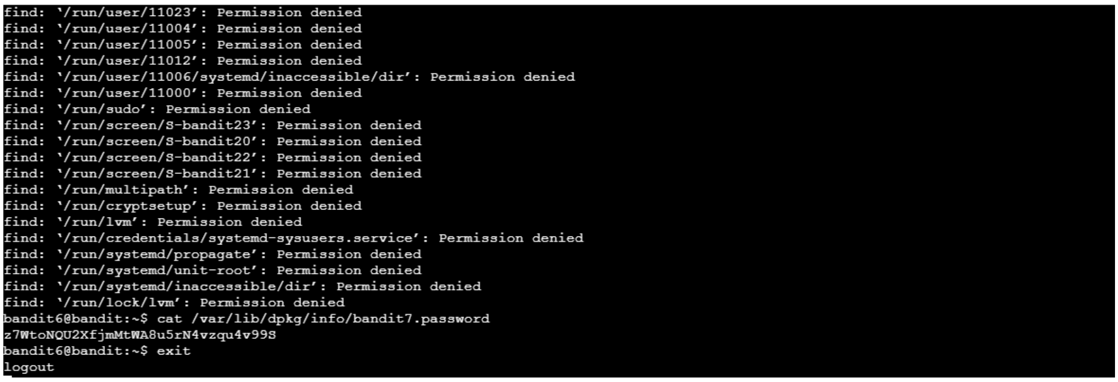
Code used:

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

{using given filter from challenge to use “user bandit7, group bandit6 and size be 33 bytes”}

after seeing one of the files be named as

/var/lib/dpkg/info/bandit7.password use it with “cat” command to obtain the password which was “z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S”



```
find: ‘/run/user/11023’: Permission denied
find: ‘/run/user/11004’: Permission denied
find: ‘/run/user/11005’: Permission denied
find: ‘/run/user/11012’: Permission denied
find: ‘/run/user/11006/systemd/inaccessible/dir’: Permission denied
find: ‘/run/user/11000’: Permission denied
find: ‘/run/sudo’: Permission denied
find: ‘/run/screen/S-bandit23’: Permission denied
find: ‘/run/screen/S-bandit20’: Permission denied
find: ‘/run/screen/S-bandit22’: Permission denied
find: ‘/run/screen/S-bandit21’: Permission denied
find: ‘/run/multipath’: Permission denied
find: ‘/run/cryptsetup’: Permission denied
find: ‘/run/lvm’: Permission denied
find: ‘/run/credentials/systemd-sysusers.service’: Permission denied
find: ‘/run/systemd/propagate’: Permission denied
find: ‘/run/systemd/unit-root’: Permission denied
find: ‘/run/systemd/inaccessible/dir’: Permission denied
find: ‘/run/lock/lvm’: Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
bandit6@bandit:~$ exit
logout
```

Level 7->8

Logout from bandit6 and login to bandit7 using “exit” command and from the password we obtained in the level previous

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

Using “man grep” the manual to grep function was learnt by me in order to do the following level

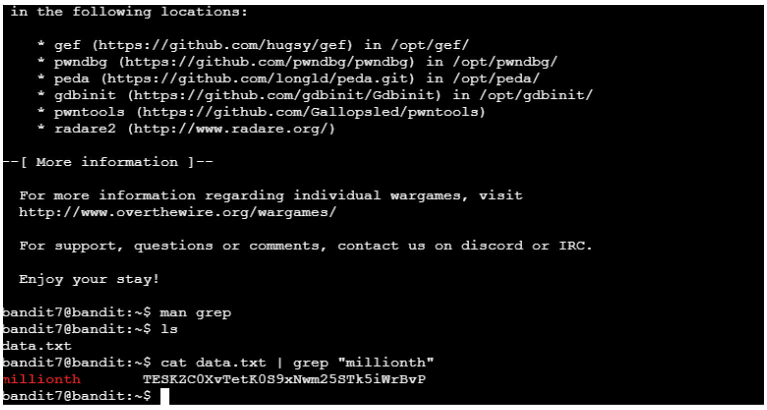
Grep, when used within an SSH session, it allows you to search for specific patterns or text within files on a remote server.

so using

>cat data.txt | grep “millionth”

we got our password to next level being

“TESKZC0XvTetK0S9xNwm25STk5iWrBvP”



```
 in the following locations:

    * gef (https://github.com/hugsy/gef) in /opt/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
    * peda (https://github.com/longld/peda.git) in /opt/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

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

Level 8->9

Logout of Bandit7 and login to bandit8 using “exit” command and the password we obtain above

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

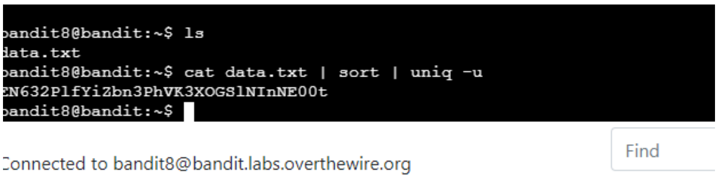
Sort and unique command given in command you may need to solve section had to be gone through in order to get the file which appears only once which we get using unique method

Using

>cat data.txt | sort | uniq -u

the password to next level was obtained which was

“EN632PlfYiZbn3PhVK3XOGSlNInNE00t”



```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ cat data.txt | sort | uniq -u
EN632PlfYiZbn3PhVK3XOGSlNInNE00t
bandit8@bandit:~$
```

Connected to bandit8@bandit.labs.overthewire.org

Level 9->10

Logout from bandit8 using “exit” command and login to bandit9 using the password above

Challenge: 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.

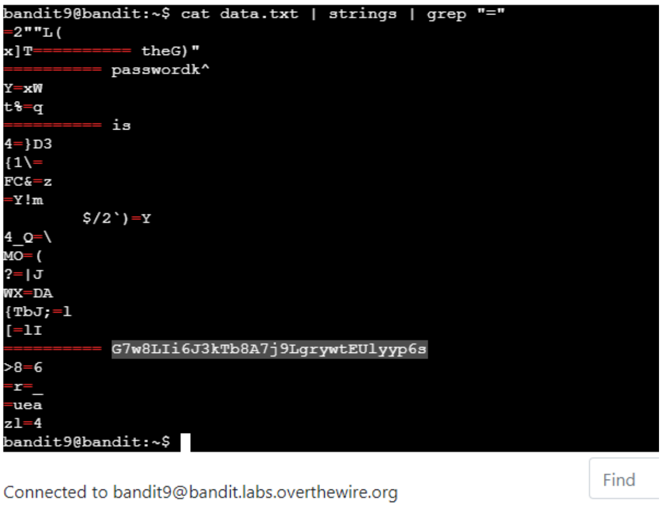
in this we had to go through “string” alongside grep to get the password so using the command

>cat data.txt | strings | grep “=”

we got many lines as output out of which our password for next lvl was

“G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s”

Problem faced: there were many password options I went through the above cuz it resembled previous passwords a lot



```
bandit9@bandit:~$ cat data.txt | strings | grep "="
=2""L(
x]T========== theG)"
========== passwordk^
Y=xW
t%=q
========== is
4=}D3
{1\=
FC&=z
=Y!m
        $/2`)=Y
4_Q=\
MO=(
?=|J
WX=DA
{TbJ;=l
[=lI
========== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
>8=6
=r=_
=uea
zl=4
bandit9@bandit:~$
```

Connected to bandit9@bandit.labs.overthewire.org

Level 10->11

Logout of bandit9 using “exit” and login to bandit10 from the given password

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

In this we find the file data.txt and when we use

>cat data.txt

we will obtain a code which is in base64 form so we had to decode it which is

“VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTllGTmI2blZDS3pwaGxYSEJNCg==”

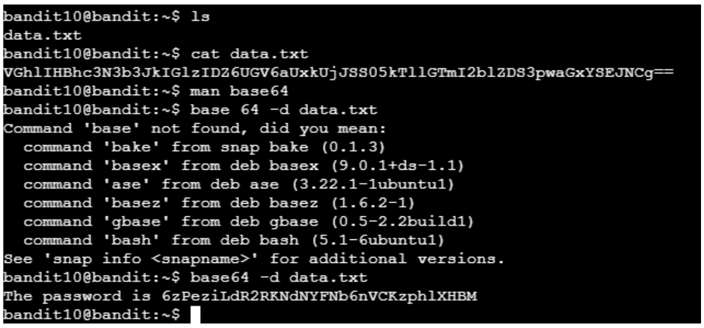
using

>base64 -d data.txt we can get the decoded password

“The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM”

and therefore our password for next level is:

“6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM”



```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTllGTmI2blZDS3pwaGxYSEJNCg==
bandit10@bandit:~$ man base64
bandit10@bandit:~$ base 64 -d data.txt
Command 'base' not found, did you mean:
  command 'bake' from snap bake (0.1.3)
  command 'basex' from deb basex (9.0.1+ds-1.1)
  command 'ase' from deb ase (3.22.1-1ubuntu1)
  command 'basez' from deb basez (1.6.2-1)
  command 'gbase' from deb gbase (0.5-2.2build1)
  command 'bash' from deb bash (5.1-6ubuntu1)
See 'snap info <snapname>' for additional versions.
bandit10@bandit:~$ base64 -d data.txt
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$
```

Level 11->12

Logout of bandit10 using “exit” and login to bandit11 using password above

Challenge: 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

using man tr we get to know the use of “tr”, here while using

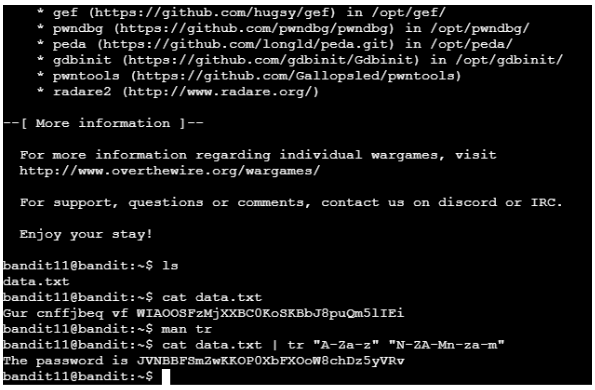
>cat data.txt

we will get the output which would be rotated by 13 position, in order to get the correct password we can use tr and set it as per 13 position to get the right password

>cat data.txt | tr “A-Za-Z” “N-ZA-Mn-za-m”

The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

is obtained as the output meaning the password for bandit12 will be JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv



```
    * gef (https://github.com/hugsy/gef) in /opt/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
    * peda (https://github.com/longld/peda.git) in /opt/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSKBbJ8puQm5lIEi
bandit11@bandit:~$ man tr
bandit11@bandit:~$ cat data.txt | tr "A-Za-z" "N-ZA-Mn-za-m"
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
bandit11@bandit:~$
```