**Writeup adarsha2.mitmpl2023@learners.manipal.edu**

**BY: ADARSHA KRISHNA K 230790050**

**Level 0:** Password is given in question as **bandit0**

**Level 0-1:** Its told that the password for level 1 is in the readme file located in the home directory.

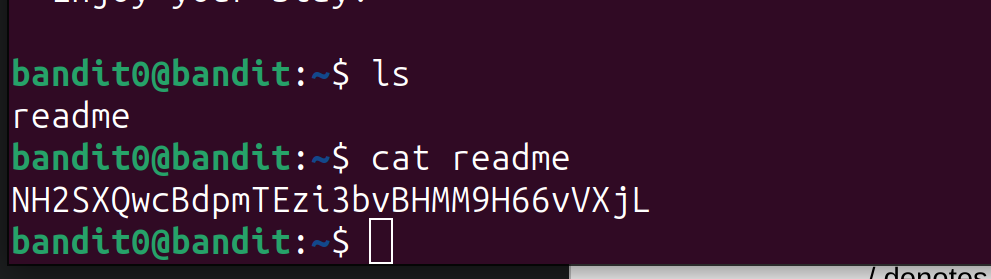
After logging in to SSH we usually get into home directory, to confirm we can run command pwd

Output: /home/bandit0

I used command cat , it can be used to display contents of a file into the terminal window.

Command: cat readme

Output: **NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL**

****

**Level 1-2:**

Similarly as before i had used a cat to display, same will apply here.

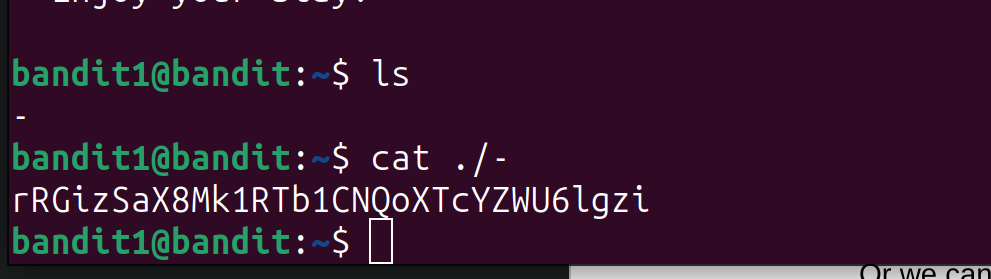
Command: cat ./-

- is the file name

./ denotes relative path

Or we can also specify full path /home/bandit1/-

Output: **rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi**

****

**Level 2-3:**

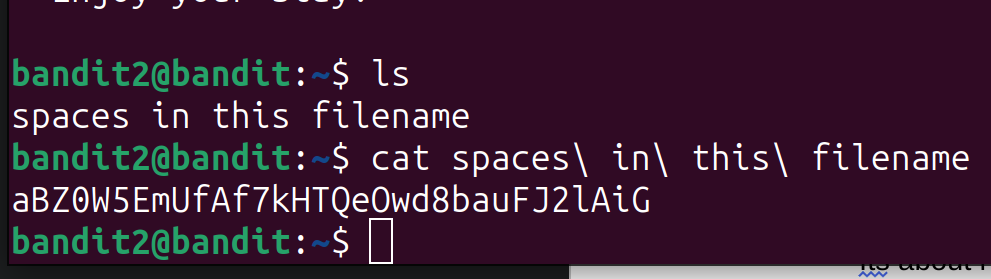
They had given a hint to search about ”spaces in filename”.

I came up to a stackoverflow article explaining “How to cat file with space in filename in BASH?”

So we can enclose the name with “” or ‘’ or add \ in between of words. I went to 3rd way, so command i entered is:

cat spaces\ in\ this\ filename

Output: **aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG**

****

**Level 3-4:**

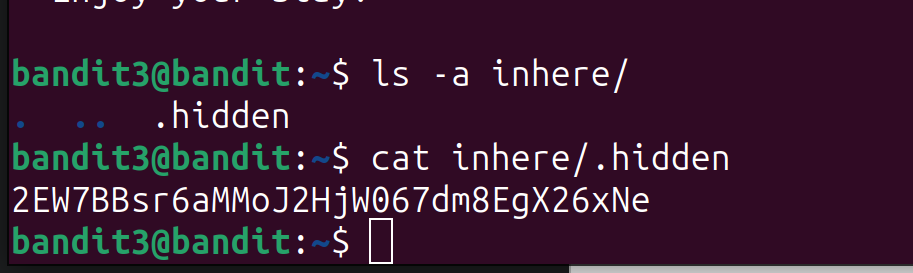
Its about hidden file. Files can be made hidden by adding . at 1st character of file name. With ls command we can use -a option to list out with hidden files.

Command: ls -a inhere/

Output: . .. .hidden

Command: cat inhere/.hidden

Output: **2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe**

****

**Level 4-5:**

They told password contained in human readable format, so it will be in text. I checked all files in inhere folder, there lots of files were there, so i used (\*) in partial name of file as all files were named similarly,

Command: cat inhere/-file0\*

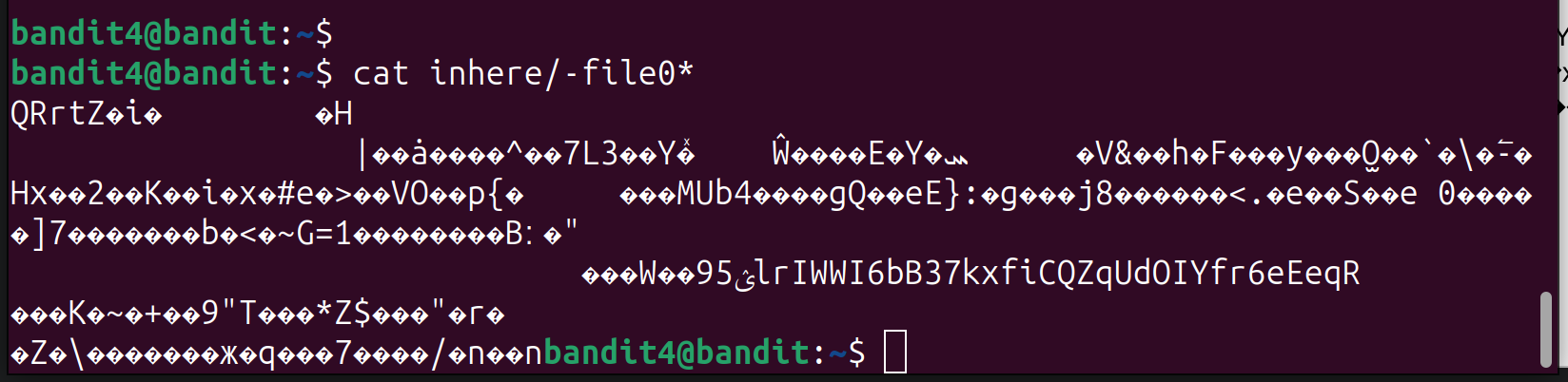
Output: QRrtZ�i� �H

|��ȧ����^��7L3��Y�ͯ Ŵ����E�Y�ܚ �V&��h�F���y���O̫��`�\�-⃐�Hx��2��K��i�x�#e�>��VO��p{� ���MUb4����gQ��eE}:�g���j8������<.�e��S��e 0�����]7�������b�<�~G=1��������B׃�"

���W��9ؽ5lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

���K�~�+��9"T���\*Z$���"�r�

KEY: **lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR**

****

**Level 5-6:**

They gave a clue that the file is of size 1033 bytes!

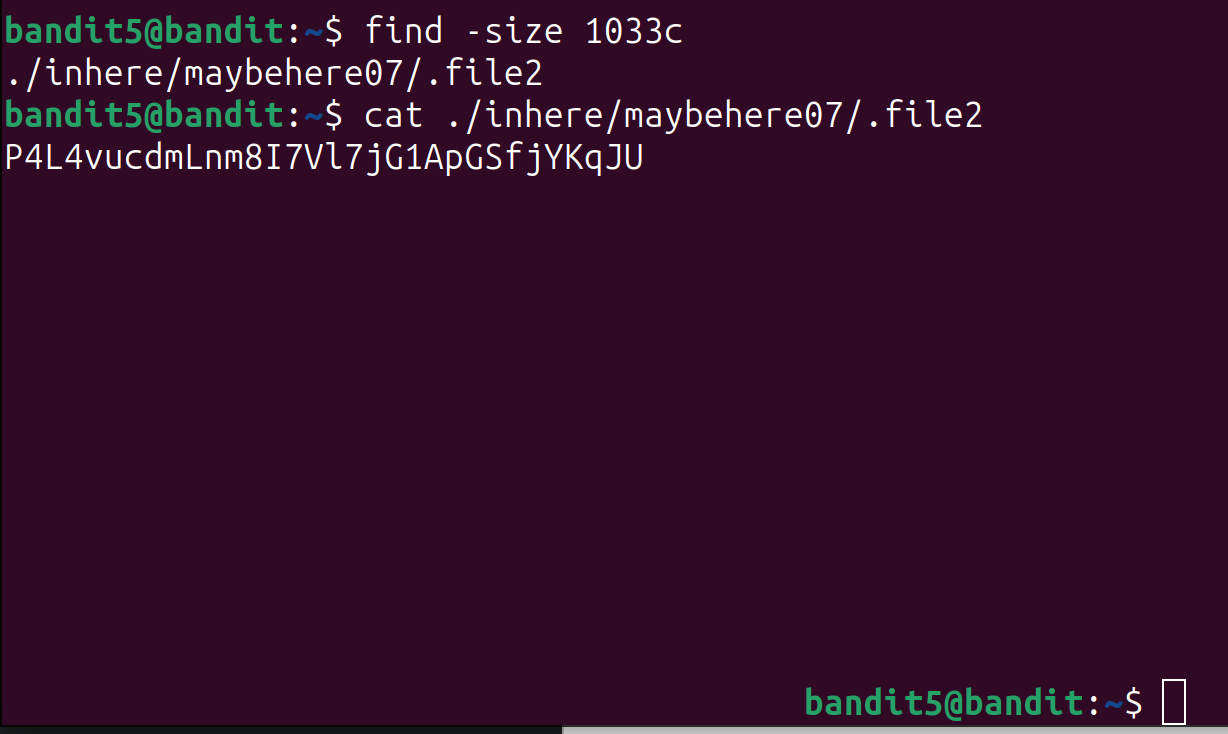
So using find command,

Command: find -size 1033c

Output: ./inhere/maybehere07/.file2

Command: cat ./inhere/maybehere07/.file2

Output:**P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU**



**Level 6-7:**

Similar as previous learning more about find command helps to solve this level

Command: find / -size 33c -user bandit7 -group bandit6

Output: find: ‘/var/lib/amazon’: Permission denied

**/var/lib/dpkg/info/bandit7.password (this has permission)**

find: ‘/var/log’: Permission denied

find: ‘/var/cache/private’: Permission denied

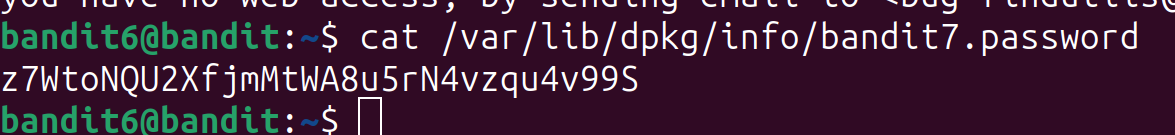
find: ‘/var/cache/pollinate’: Permission denied

find: ‘/var/cache/apparmor/30d07b40.0

Displaying it!

Command: cat /var/lib/dpkg/info/bandit7.password

Output: **z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S**

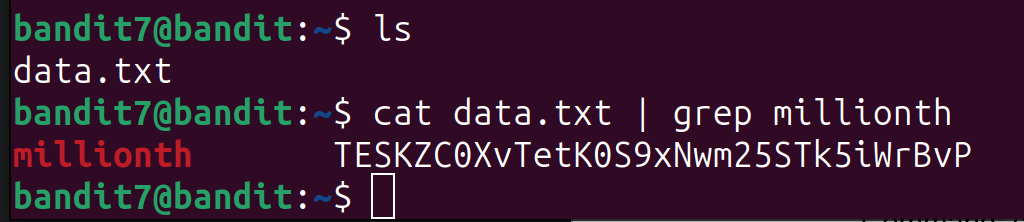
****

**Level 7-8:**

Using grep and cat with pipe | to filter the line matches the specified string “**millionth**”

Command: cat data.txt | grep millionth

Output: millionth **TESKZC0XvTetK0S9xNwm25STk5iWrBvP**

****

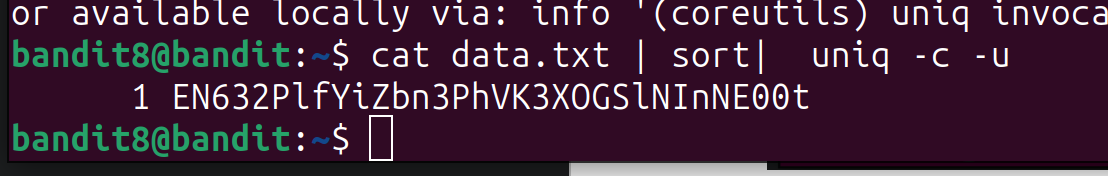
**Level 8-9:**

They told there is a unique line in data.txt file

First we will sort (ascending order by default) the output of cat data.txt then its piped to uniq command which will display unique (-u) with no. of duplicates (-c)

Command: cat data.txt | sort| uniq -c -u

Output:1 **EN632PlfYiZbn3PhVK3XOGSlNInNE00t**

****

**Level 9-10:**

Its told that password has been preceded by several =, so we will use grep to match the pattern

If I directly use cat and pipe to grep then it will show error as the contents are not in text format, so we have to convert it to string then use grep.

Command: strings data.txt | grep "="

Output: ========== **G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s**

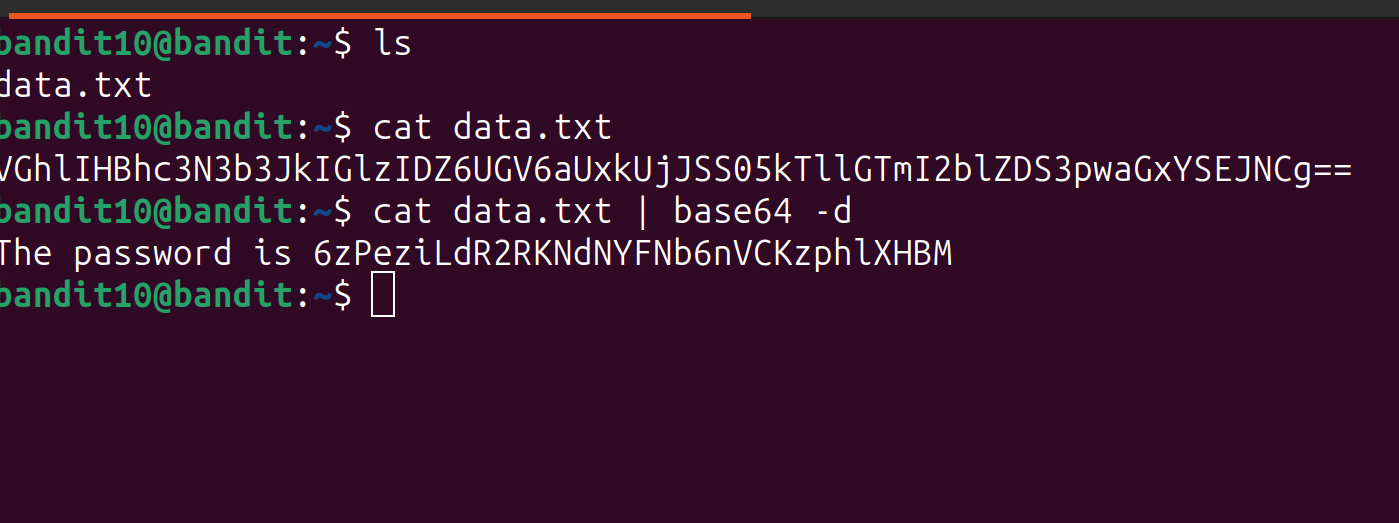
****

**Level 10-11:**

Its been told that password is encrypted in base64 format, so we will use base64 command to decode it to text format.

Command: cat data.txt | base64 -d

Output: The password is **6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM**

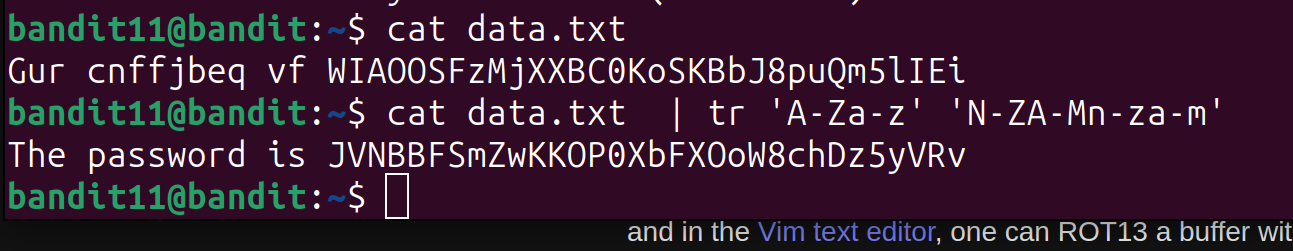
****

**Level 11-12:**

In the question its states that password is encrypted in rot13 format, by looking at wikipedia, it can be made with tr command, so to reverse we just pipe encrypted text to tr as the same way it was encrypted.

Command: cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m’

Output: The password is **JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv**

****