**Task Set 1**

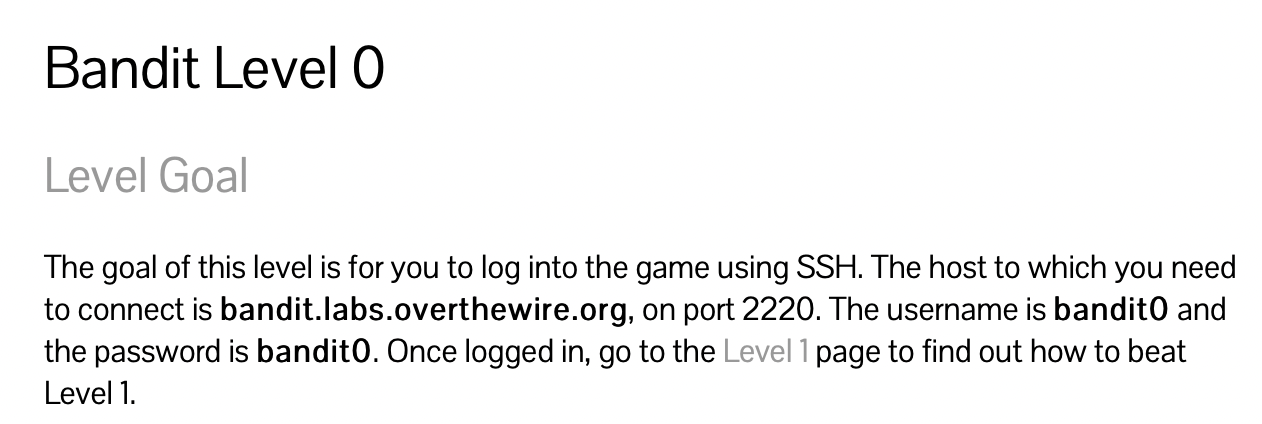
Name: Hitarth Anand Rohra

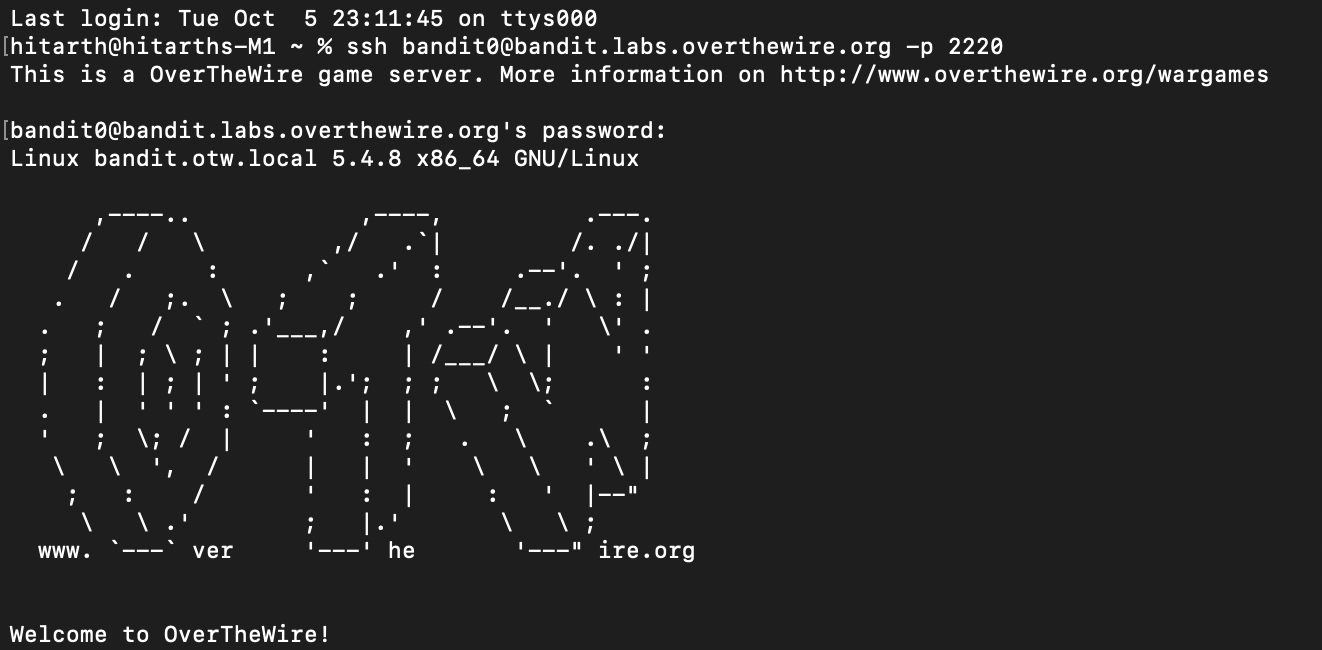
Roll no:- AM.EN.U4EAC21032

Date of Submission:- 06/10/2021

The[**Bandit**](https://overthewire.org/wargames/bandit/) wargame is an online game offered by the **OverTheWire** community. It helps us to learn various Linux commands and understand some basic features of this system.

This is a quick write-up of my solutions for this challenge:-

 **Solution set:**



**Explanation:**

* In this game we are expected to use the ***“ssh”*** command and log into the game. ***“ssh”*** command provides a secure encrypted connection between the two hosts over an insecure network.
* I had been provided with both domain name and pwd of level zero. Basic command for ssh is:

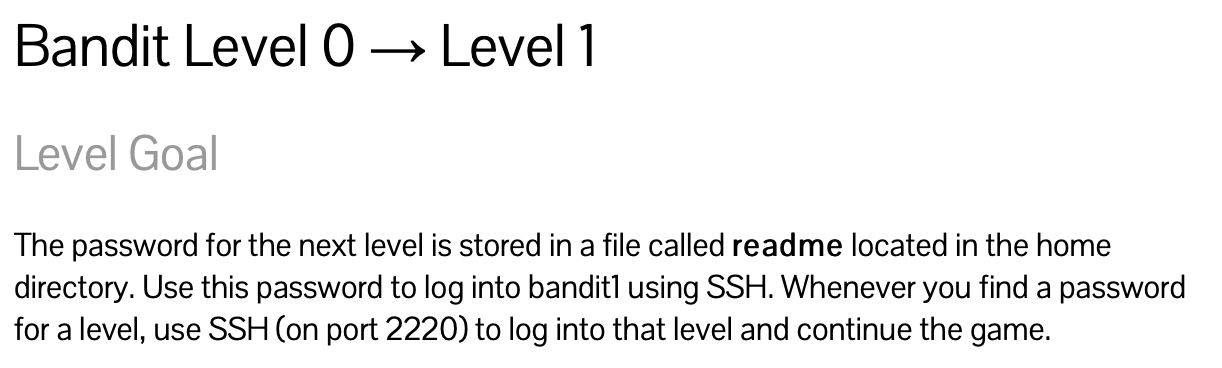
***“ssh*** [***bandit0@bandit.labs.overthewire.org***](mailto:bandit0@bandit.labs.overthewire.org)***”***

But here they have changed the default port to 2200.

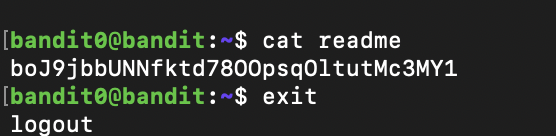
Hence the command changes to:

***“ssh*** [***bandit0@bandit.labs.overthewire.org***](mailto:bandit0@bandit.labs.overthewire.org) ***-p 2220”***

And we are successfully connected.

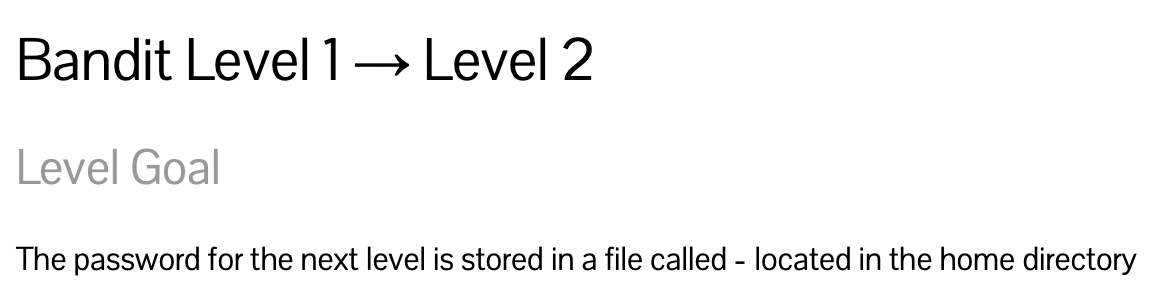


Solution Set:

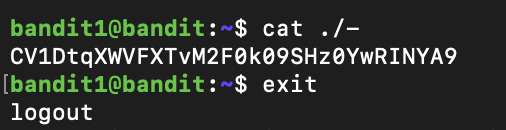


**Explanation:**

We are provided with the information that the password is in the ***“readme”***file, hence we use the ***“cat readme”*** command and we have found our password for the next level.



**Solution Set:**

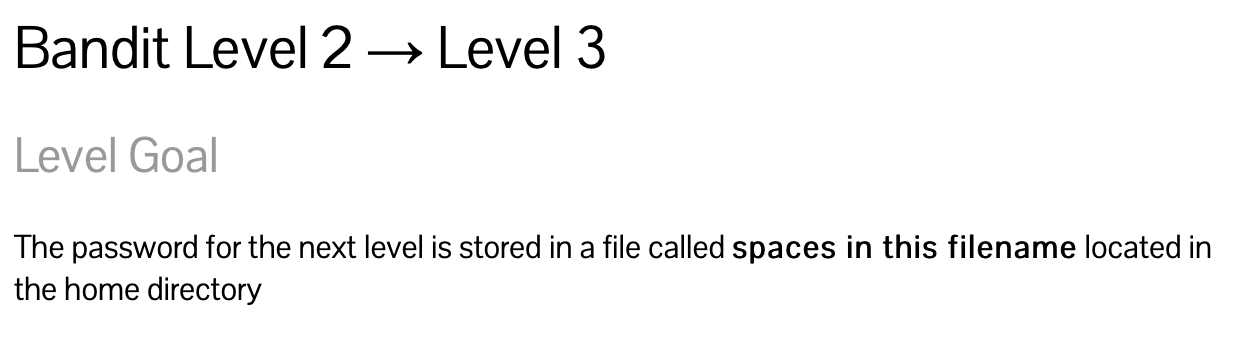


**Explanation:**

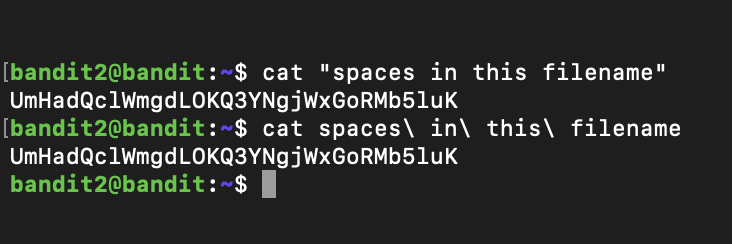
Here we have been given that the password is stored in the file “-” so we cannot directly run ***“cat -”***,when we use this command the system awaits for the next to be given but we don't have any other command so we use “-” is ***“cat ./-”*** for files starting with “-” and hence we get our password for the next level.

Or

We can give the exact address of the file ***“cat /home/bandit1/-”.***



**Solution Set:**



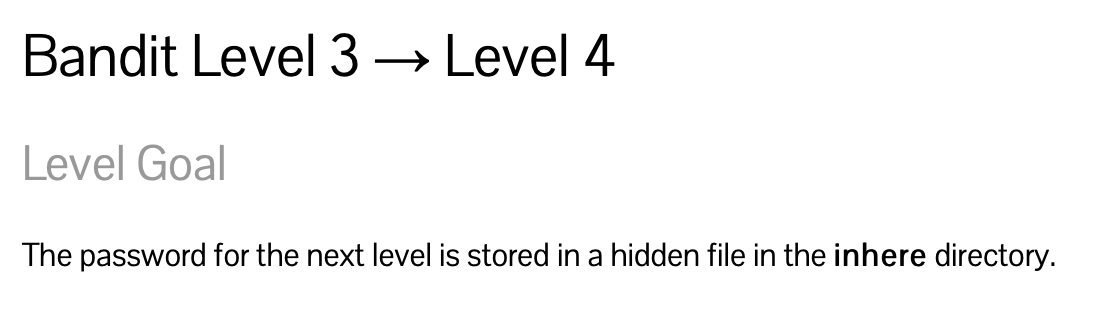
**Explanation:**

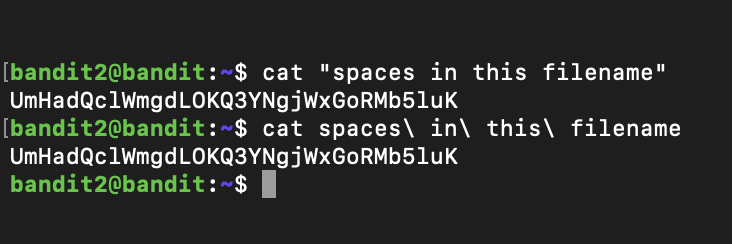
We have been told in this level that this file has spaces in between so it's a unique file name so either we can give file name in quotes **(*cat “spaces in the filename”*)** to get the password of the next level.

Or

We can write file name using spaces and slash

***“cat spaces\ in\ this\ filename”***this treats spaces as a special character.

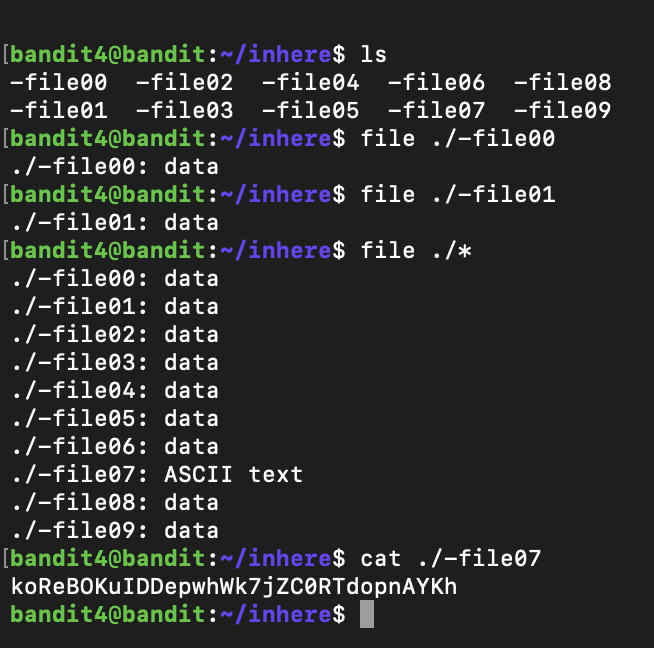
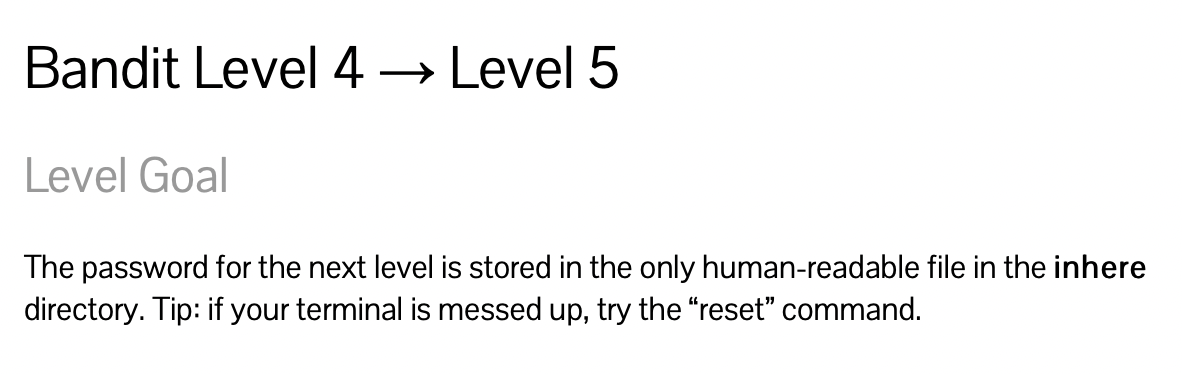
**Solution Set:**



**Explanation:**

Here we have been told that the password for the next level is present in a hidden file inside directory “inhere”, so here we can simply list the command “ ls”, as it only works for non-hidden files, we use ***“ls -a”***here **“-a”** is used to show all the files(irrespective of hidden and non hidden).

Hence we can read **“cat .hidden”** and get the password.



**Solution Set:**

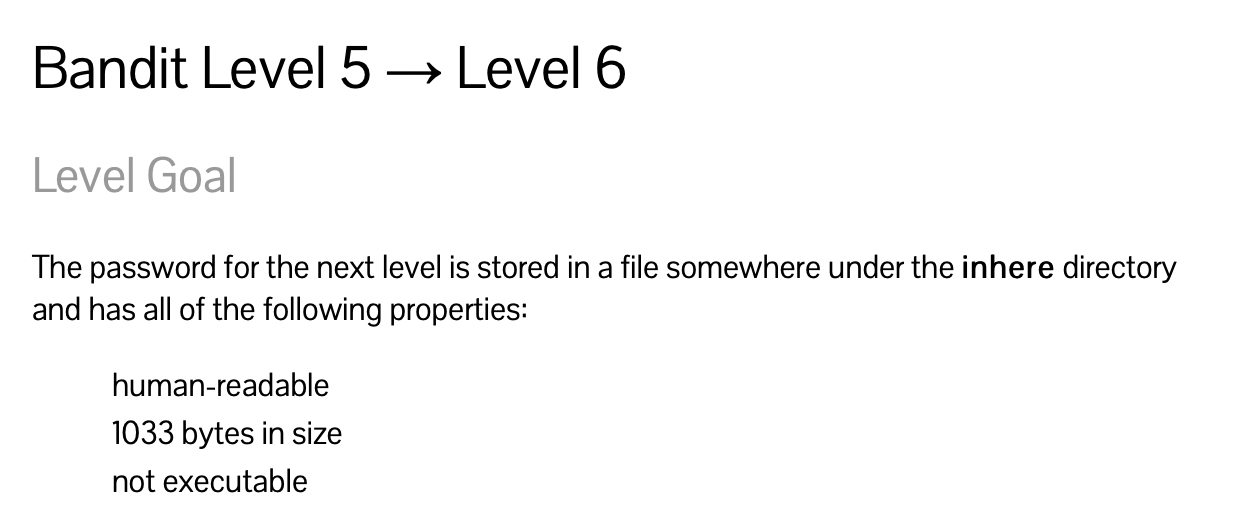
**Explanation:**

* In Level 4 we have been told that the file here is stored in the directory **“inhere”** which is only human readable file. We can see there are 10 files in this directory using “ls”, so we can use command***“file ./-file00”*** to check the data of each file manually.

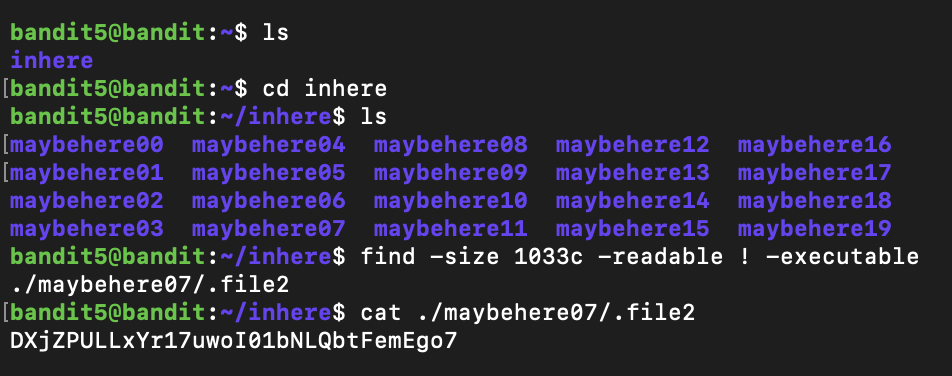
Or

We can use *“file./ \*”* which tells the type of all the files in nnnnthe given directory.

* Then we can open the file having data type ASCII text to get the password for the next level.



**Solution Set:**

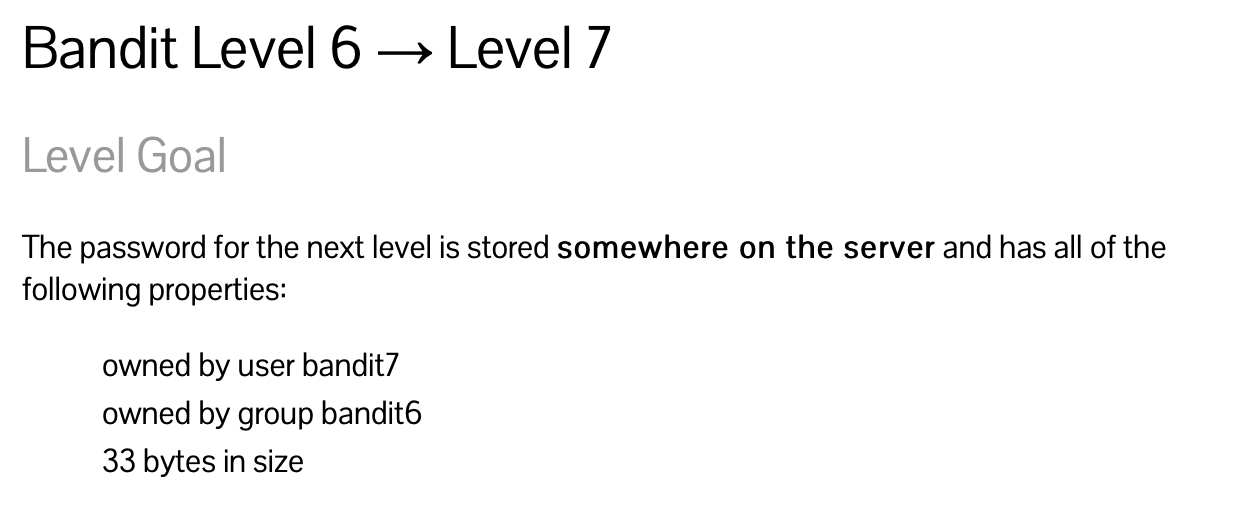


**Explanation:**

To find any file we use ***“find”* command**, ***“-readable”*** switch to check whether the file is readable or not,***“-size c”*** switch to check the size of the file*,* ***“-executable”*** switch to check whether the file is executable or not.

***“find -size 1033c -readable ! -executable”***

and we can hence find the password using the ***“cat”*** command.



Solution Set:

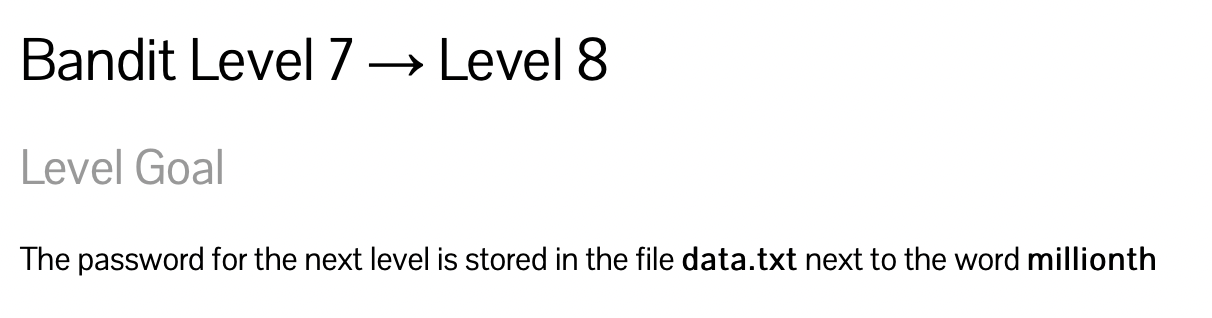


Explanation:

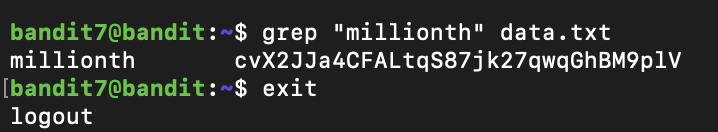
* As we have been told that the file is somewhere in the server, we will go to the root directory to begin our search by using the command ***“cd /”***.Now we will search in the root directory using the command :

***“find -size 33c -user bandit7 -group bandit6”***

* Now we can see we are not allowed to read many files, so we will read the file where permission is not denied and get our password for the next level.



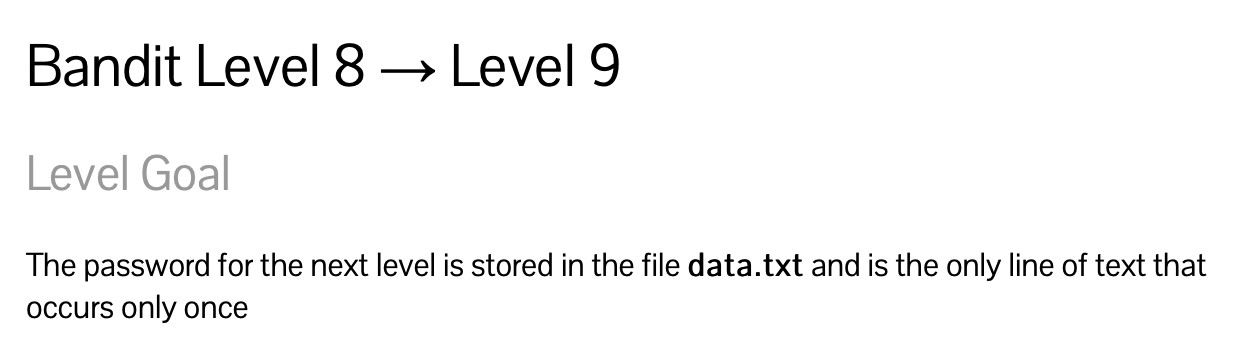
Solution Set:



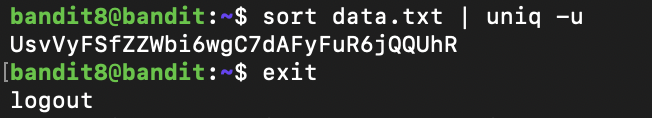
Explanations:

In this level we are asked to find the millionth word in the file ***“data.txt”***,so we will make use of the command ***“grep”***,this command gives the text stored in the file at a particular line.

**(*grep “millionth” data.txt*)** and we will get the password for the next level.



Solution Set:

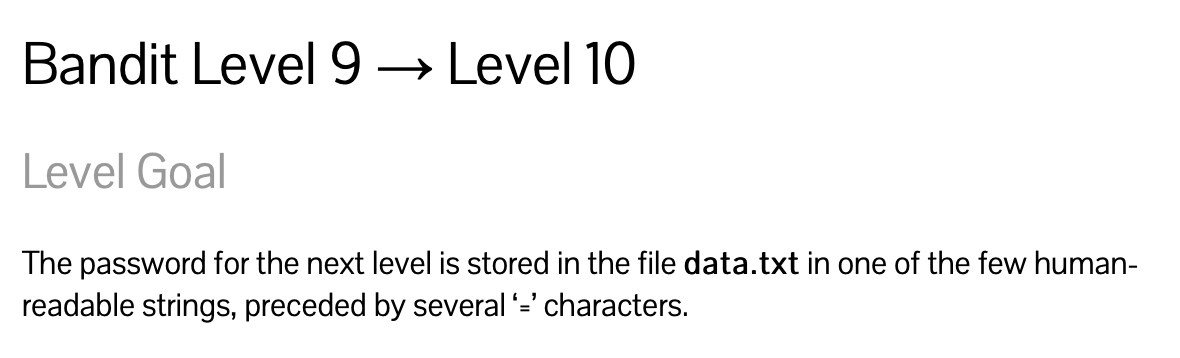


Explanation:

We have been informed that our password in this level occurs only once and rest everything occurs more than once.

We have a ***“uniq -u”*** command for searching the text occurring once in the file, but the ***“uniq -u”*** command only works for a sorted list(ascending or descending), so we will first sort the file using ***“sort data.txt”*** and then use the **“uniq -u”** command for finding the password.

***“sort data.txt | uniq -u”***



Solution Set:



Explanations:

In this level we are intended to find the readable content in the file, for which we will use ***“strings”*** which returns the readable data inside the file and the password followed by several ‘=’ is our password. ***“strings data.txt”***

**Passwords Acquired:**

**Level 1- boJ9jbbUNNfktd78OOpsqOltutMc3MY1**

**Level 2- CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9**

**Level 3- UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK**

**Level 4- pIwrPrtPN36QITSp3EQaw936yaFoFgAB**

**Level 5- koReBOKuIDDepwhWk7jZC0RTdopnAYKh**

**Level 6- DXjZPULLxYr17uwoI01bNLQbtFemEgo7**

**Level 7- HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs**

**Level 8- cvX2JJa4CFALtqS87jk27qwqGhBM9plV**

**Level 9- UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR**

**Level 10- truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk**