**Level 0 to 1:**

*Level Goal:*

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.

*Commands used:*

ls – listing contents of the directory

cat – concatenate files and print on the standard output

exit – exiting the server

*Solution:*



1. used ls to find the file ‘readme’.
2. used the command cat to find the password from the file readme.
3. exited the server and went to the next level

*Links used:*

<https://man7.org/linux/man-pages/man1/ls.1.html>

<https://man7.org/linux/man-pages/man1/cat.1.html>

**Level 1 to 2:**

*Level Goal:*

The password for the next level is stored in a file called – located in the home directory.

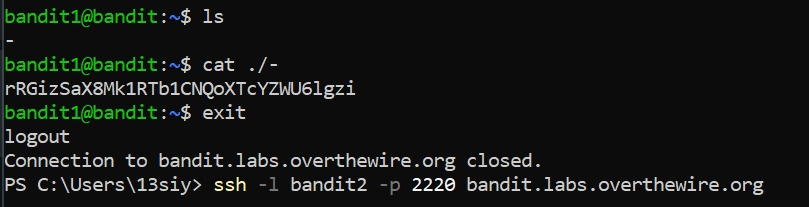
*Commands used:*

ls

cat

exit

*Solution:*



1. used ls to find the file named ‘-’.
2. used a specific case of cat with ./ to make sure that the filename is readable.
3. found the password and exited the server to go to the next level

*Links used:*

<https://stackoverflow.com/questions/42187323/how-to-open-a-dashed-filename-using-terminal>

**Level 2 to 3:**

*Level Goal:*

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

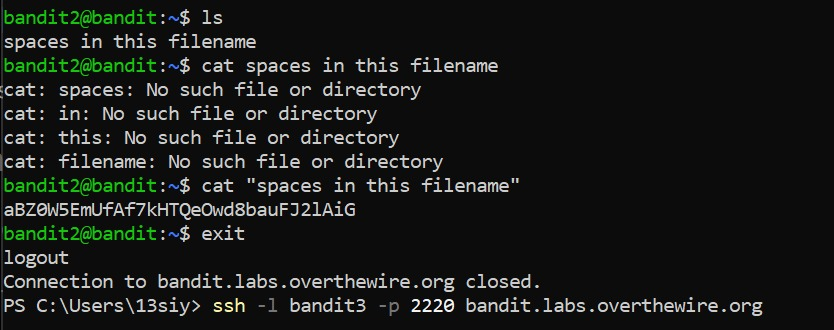
*Commands used:*

ls

cat

exit

*Solution:*



1. used ls to find the file ‘spaces in this filename’
2. tried to read the data in the file using regular cat command
3. read up on how to read file names with spaces and used quotations around the filename to find the password
4. exited the server to go to the next level

*Links used:*

<https://linuxhandbook.com/filename-spaces-linux/#:~:text=Read%20a%20file%20with%20spaces%20in%20filename&text=Basically%2C%20you%20put%20a%20%5C%20before,quotes%20instead%20of%20double%20quotes.&text=Single%20quotes%20ignore%20any%20special%20characters>.

**Level 3 to 4:**

*Level Goal:*

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

*Commands used:*

ls

cd – change the working directory

cat

exit

*Solution:*



1. used ls to find the directory mentioned
2. used the cd command to enter the inhere directory
3. used ls again to get no output
4. looked into the ls manual to find the -a flag to view all files including hidden ones
5. the output arrives as ‘. .. .hidden’ and we can see .hidden is the file needed
6. use the command cat on that file and find the password
7. exit the server and access the next level

*Links used:*

<https://man7.org/linux/man-pages/man1/ls.1.html>

**Level 4 to 5:**

*Level Goal:*

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.

*Commands used:*

ls

cd

cat

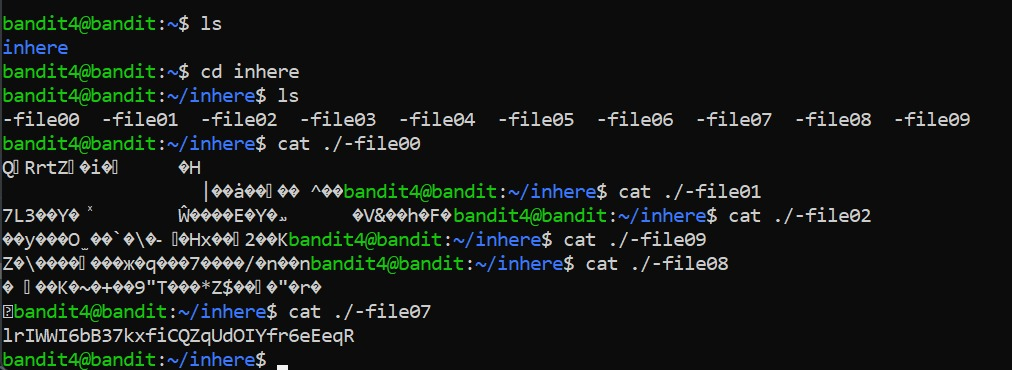
man – get a manual for the command in question

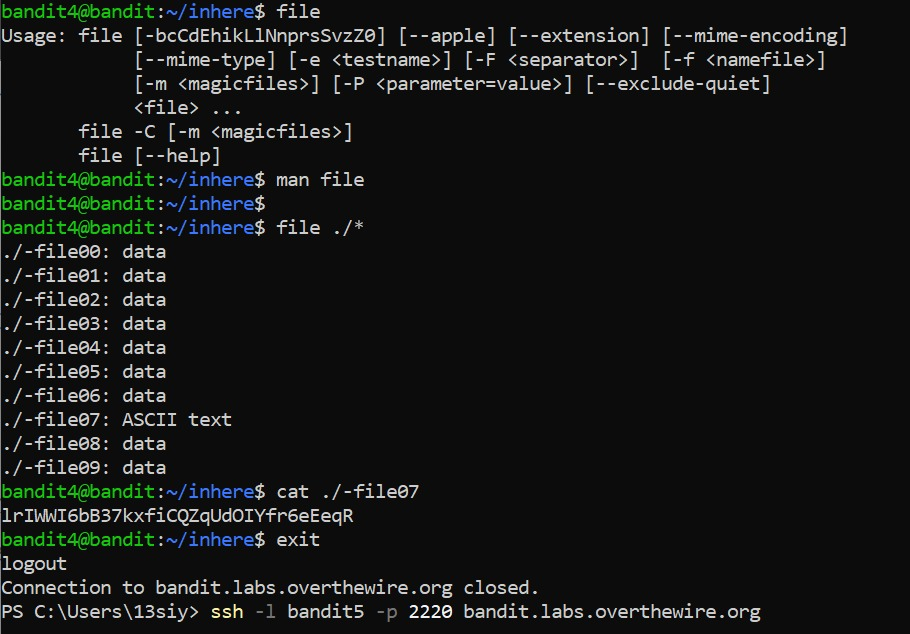
file – determine file type

reset – resets command window

exit

*Solution:*





1. used ls to find the inhere directory and entered it
2. used ls within the directory to find 10 different files within it

*method 1:*

1. went through each individual files using cat ./<filenumber> from 0-2 and then backwards from 7-9
2. accidentally stumbled upon the password in file number 7
3. reset the system to try and find a more efficient way

*method 2:*

1. looked at a manual of file and used ./\* to return the type of data stored in each file
2. file07 stored an ascii value and was the odd one out
3. used the cat command on file07 and found the password
4. exited the server and moved to the next level

*Links used:*

<https://www.javatpoint.com/linux-file?source=post_page-----72757d03001f-------------------------------->

**Level 5 to 6:**

*Level Goal:*

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

*Commands used:*

ls

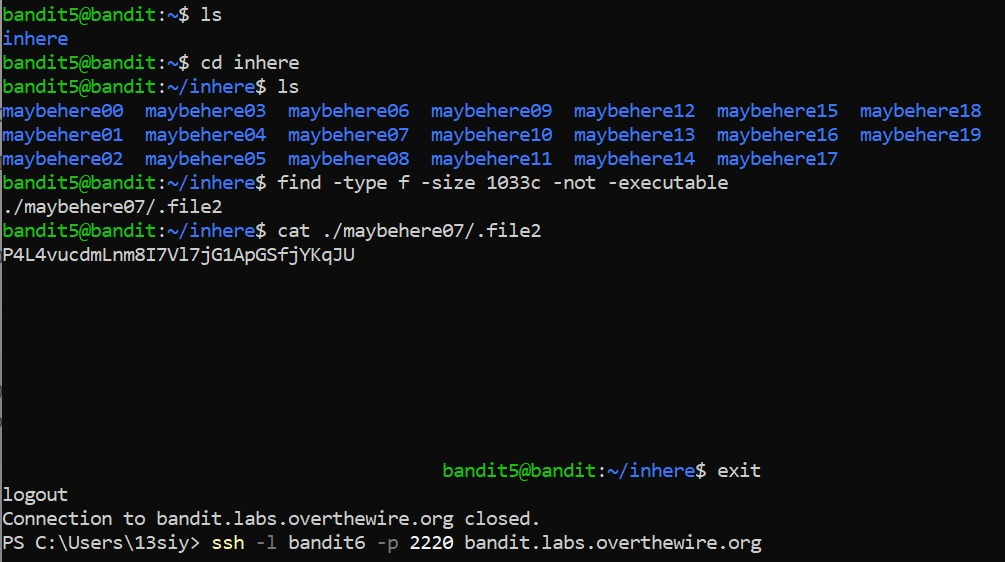
cd

cat

find – finds the file with the given flags/specifications

exit

*Solution:*



1. used ls command to find inhere directory
2. entered mentioned directory and used ls command again to find 18 directories
3. decided against using cat on individual directories as in the previous level and follow the limitations given in the question
4. find the file using the file command with the flags mentioned in the question after looking into the working of the find command
5. used the cat command on the file that showed up and found the password
6. exited the server and moved onto the next level

*Links used:*

<https://www.tecmint.com/35-practical-examples-of-linux-find-command/?source=post_page-----aa853b431c1d-------------------------------->

**Level 6 to 7:**

*Level Goal:*

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

*Commands used:*

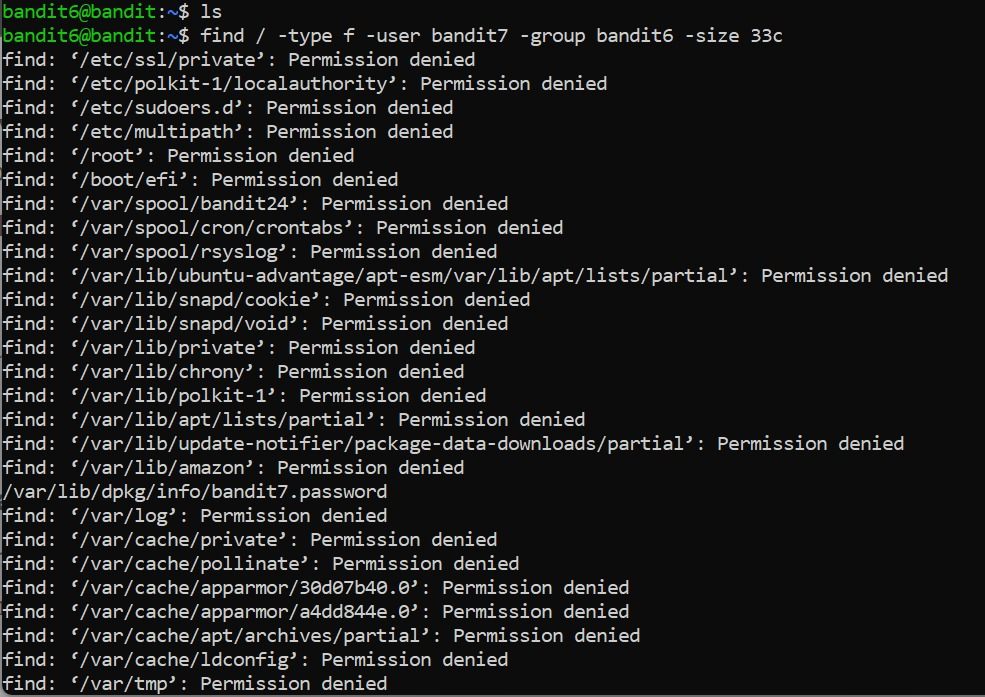
ls

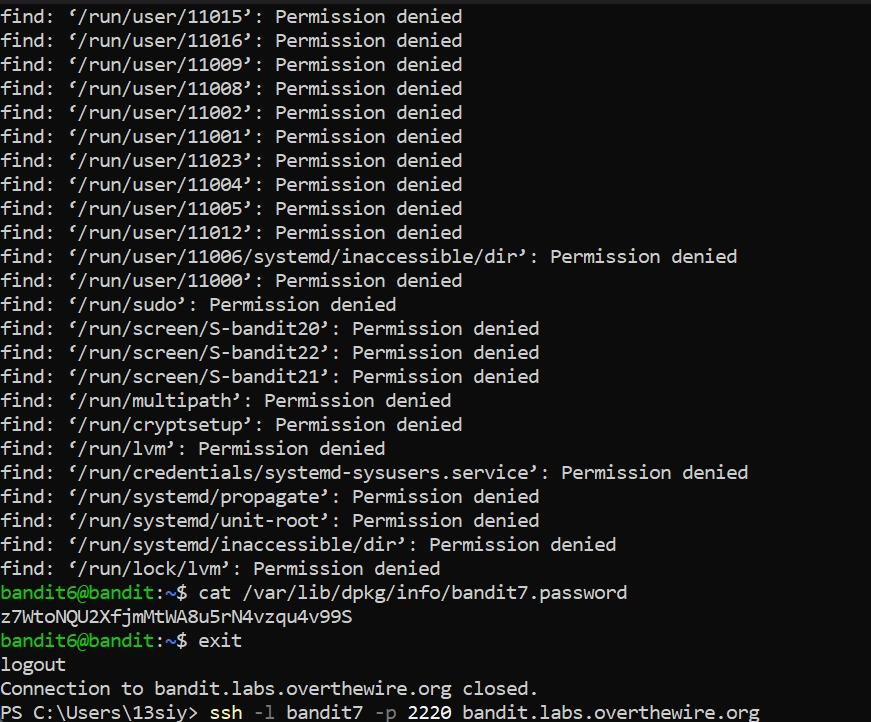
cat

find

exit

*Solution:*

**



1. used ls command to get no output
2. used find with the given specifications to get a long list of files which I was denied permission to
3. while scrolling down it, realized that one of the files did not have a permission denied next to it
4. decided to concatenate that file and found the password
5. exited the server and accessed the next level

*Links used:* none

*Note:* want to know if there is a way to acquire only the file I have been given access to, rather than having to go through all the files and spot one by chance.

**Level 7 to 8:**

*Level Goal:*

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

*Commands used:*

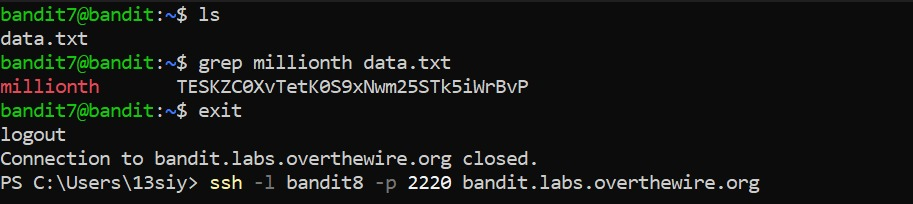
ls

cat

grep - searches a file for a particular pattern of characters, and displays all lines that contain that pattern

exit

*Solution:*



1. used the ls command to find the file data.txt and try to concatenate the file.
2. got a block of data so long it didn’t even allow me to enter commands into the server anymore
3. closed powershell and re-entered the server to try again
4. looked into the grep command since it was the second on the list of suggested commands
5. decided to use it with the word ‘millionth’ and the file data.txt
6. found the password and exited to access the next level

*Links used:*

<https://www.geeksforgeeks.org/grep-command-in-unixlinux/>

**Level 8 to 9:**

*Level Goal:*

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

*Commands used:*

ls

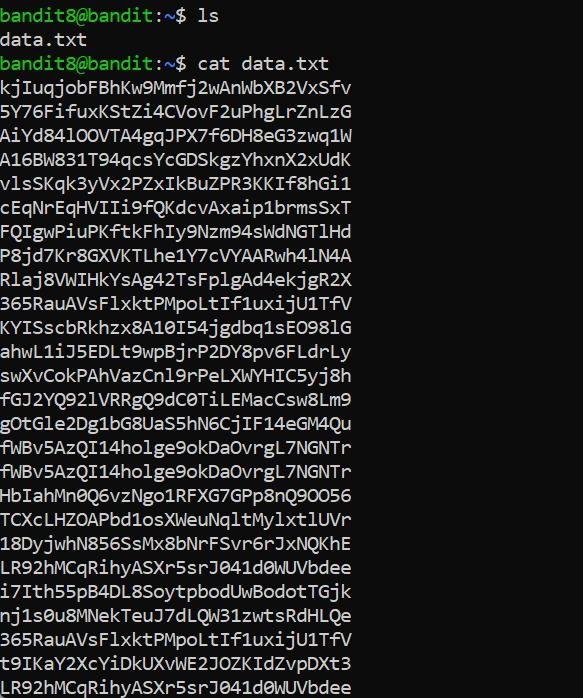
cat

uniq – reports or filters out the repeated lines in a file

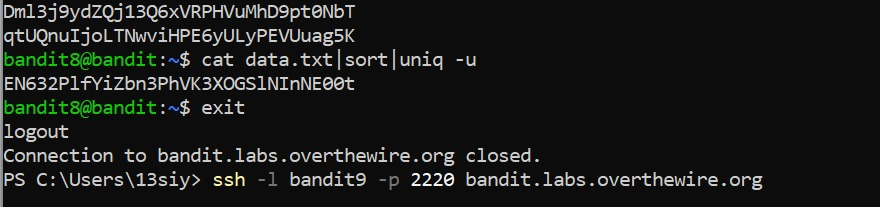
sort – sorts the data given

exit

*Solution:*



1. used the ls command to find the data.txt file and concatenated it
2. found a huge block of data
3. read up on the uniq utility and ran it as a part of the cat command, with the flag -u to find the unique line of data
4. got the same block of data (no noticeable difference)
5. re-read the function of uniq utility and realized that it only works on sorted data



1. used the cat command with both the sort and uniq utilities (with -u flag) and found the password
2. exit the server and entered the next level

*Links used:*

<https://www.geeksforgeeks.org/uniq-command-in-linux-with-examples/>

**Level 9 to 10:**

*Level Goal:*

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

*Commands used:*

ls

cat

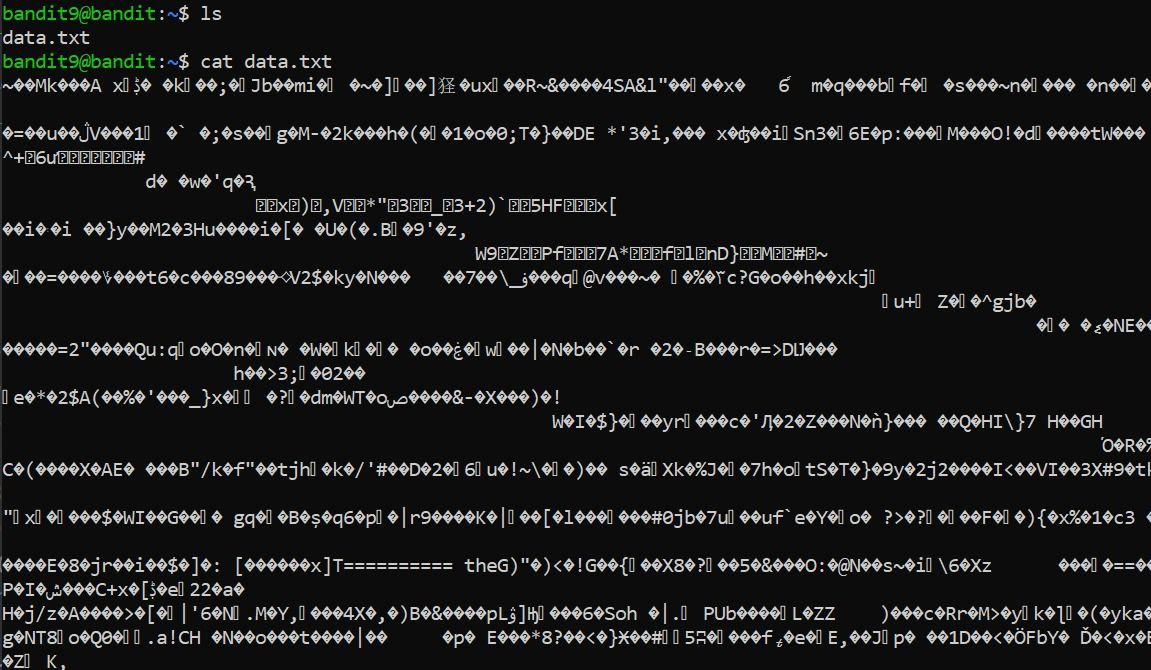
reset

grep

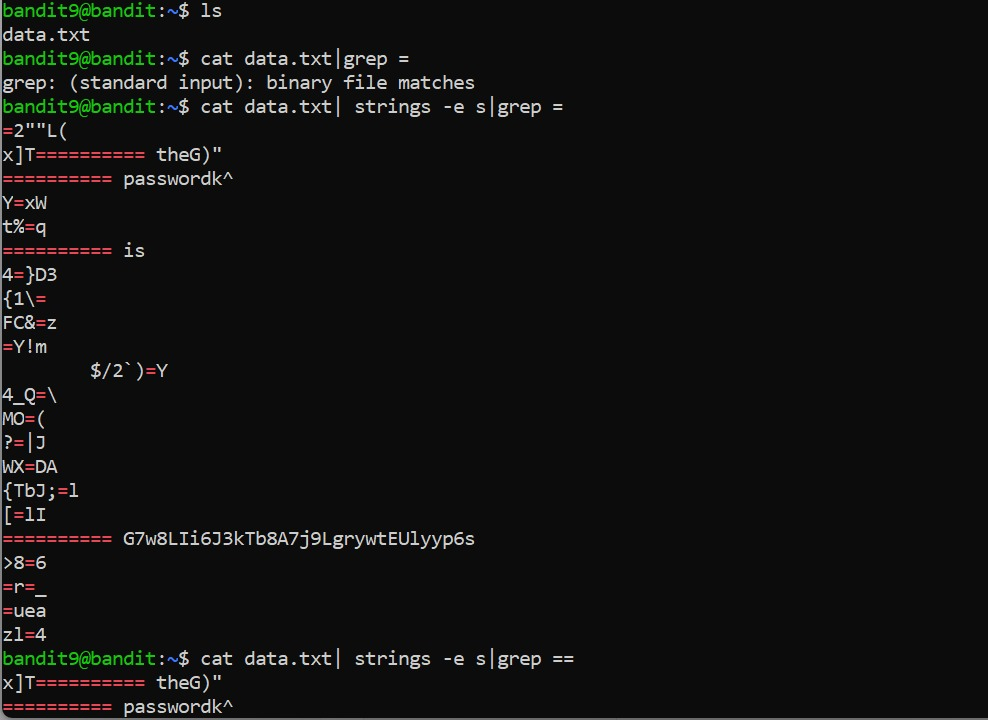
strings - return each string type of characters that are printable in the file

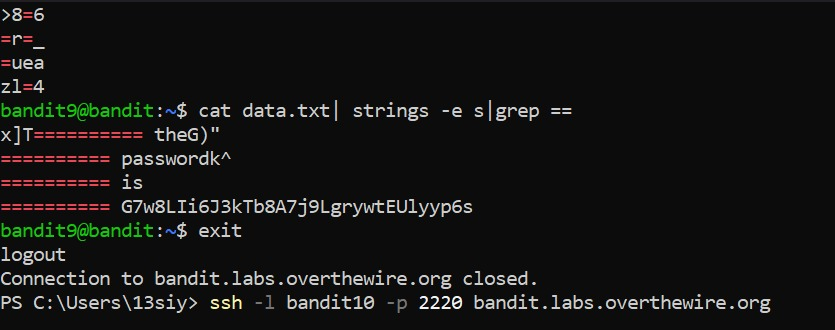
exit

*Solution:*



1. used ls and cat commands to no avail (encountered a block of text)





1. reset the window and re-entered the ls command
2. used the cat command with grep = as per the directive
3. got an error of some sort so read up on the strings utility that was on the list of suggested commands
4. decided to try it and entered it as a utility of the cat command alongside grep, using the flag -e as suggested in the second link given below (encoding)
5. got an output of a block of text but noticed the words password and something that appeared to be a correct flag next to a lot of ==’s
6. re-read the question and realized the password would be next to *several* =’s not one
7. re-entered the cat command as before and added an extra = to find the password
8. exited the server and accessed the next level

*Links used:*

<https://www.educba.com/linux-string-command/>

<https://www.tutorialspoint.com/unix_commands/strings.htm?source=post_page-----de8c95ce4efc-------------------------------->

**Level 10 to 11:**

*Level Goal:*

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

*Commands used:*

ls

cat

base64 - encodes binary strings into text representations using the base64 encoding format

exit

*Solution:*



1. read up on the base64 command as it would be needed according to the question
2. used the ls command to find the data.txt file
3. used cat on it without base64 utility to see the output
4. used cat again with base64 along with the -d flag to decode the data given in the file
5. found the password and exited to access the next level

*Links used:*

<https://en.wikipedia.org/wiki/Base64>

<https://linuxhint.com/bash_base64_encode_decode/>

**Level 11 to 12:**

*Level Goal:*

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

*Commands used:*

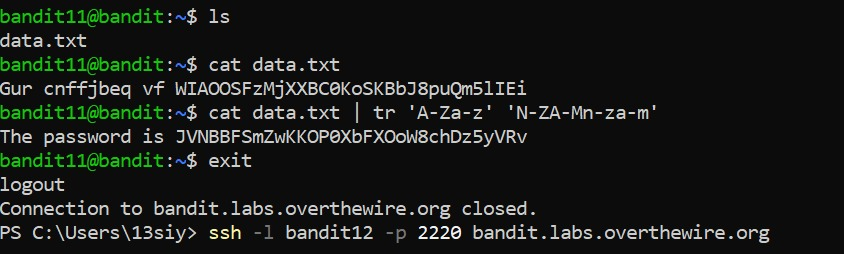
ls

cat

tr – used to translate/ transform data from one form to another

exit

*Solution:*

**

1. read up on rot13 and the tr command as it would be needed according to the question
2. used the ls command to find the data.txt file
3. used cat on it without tr utility to see the output
4. used cat again with tr along with the required inputs to get the password
5. exited the server

*Links used:*

<https://en.wikipedia.org/wiki/ROT13>

<https://linuxize.com/post/linux-tr-command/?source=post_page-----df6e59deda05-------------------------------->

**List of passwords**

level 0 password: NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

level 1: rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

level 2: aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

level 3: 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

level 4: lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

level 5: P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

level 6: z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

level 7: TESKZC0XvTetK0S9xNwm25STk5iWrBvP

level 8: EN632PlfYiZbn3PhVK3XOGSlNInNE00t

level 9: G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

level 10: 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

level 11: JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv