CRYPTONITE

TASK PHASE-1

**D.vishwatej**

**BANDIT LEVEL1-LEVEL11**

**LEVEL0:-**

**The goal is to log into the host** bandit.labs.overthewire.org **using ssh.**

**Logging into the host is done by using**

**$ ssh <username>@<host> -pxxx**

**here pxxx is the port required. Therefore, used command is**

**ssh** [**bandit0@bandit.labs.overthewire.org**](mailto:bandit0@bandit.labs.overthewire.org) **-p2220**

**Now type the password as bandit0 -----(given in question).**

**RESOURCES USED:-** [**https://www.wikihow.com/Use-SSH**](https://www.wikihow.com/Use-SSH)

**LEVEL0-LEVEL1:-**

**The goal is to find the file readme and know the password for the next level.**

**Ls command- lists directory contents**

**cat command- opens the file and prints the output**

**find command- searches tfor the file in the current directory**

**To know that there is a file named readme in the files , i used ls command. It shows readme.**

**To read the file we can use the cat command as**

**$ cat readme**

**It opens the file and shows the password for level 1.**

**PASSWORD:- NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL**

**RESOURCES USED:-** [**https://www.wikihow.com/Use-SSH**](https://www.wikihow.com/Use-SSH)

**LEVEL1-LEVEL2:-**

**Login to the host using $ ssh** [**bandit1@bandit.labs.overthewire.org**](mailto:bandit1@bandit.labs.overthewire.org) **-p2220**

**The goal is to find the file - and know the password for the next level.**

**To know that there is a file named - in the files , i used ls command. It shows - .**

**To read the file we can use the cat command as follows**

**$ cat <-**

**NOTE:- If the file name ‘– ‘ is directly used we get command not found error thus we use cat <-**

**PASSWORD:-rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi  
RESOURCES USED:-**[**https://stackoverflow.com/questions/42187323/how-to-open-a-dashed-filename-using-terminal**](https://stackoverflow.com/questions/42187323/how-to-open-a-dashed-filename-using-terminal)

**LEVEL2-LEVEL3:-**

**Login to the host using $ ssh** [**bandit2@bandit.labs.overthewire.org**](mailto:bandit1@bandit.labs.overthewire.org) **-p2220**

**The goal is to find the file spaces in this filename and know the password for the next level.**

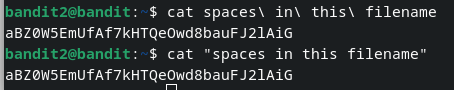
**To know that there is a file named spaces in this filename in the files , i used ls command. It shows spaces in this filename.**

**To read the file we can use the cat command as follows**

**$ cat spaces\ in\ this\ filename**

**NOTE:- A space in a filename can cause errors when loading a file or when transferring files between computers. Thus we use ‘\ ‘ to separate the words of the filename.**

**An alternative method of double quotes can also be used.**



**PASSWORD:-aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG**

**RESOURCES USED:-** [**https://linuxhandbook.com/filename-spaces-linux/**](https://linuxhandbook.com/filename-spaces-linux/)

**LEVEL3-LEVEL4:-**

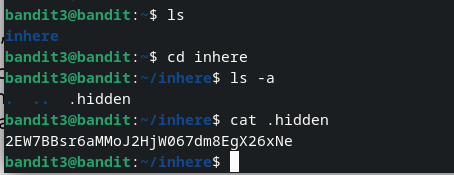
**Login to the host using $ ssh** [**bandit3@bandit.labs.overthewire.org**](mailto:bandit1@bandit.labs.overthewire.org) **-p2220**

**I used the ls command. It showed the inhere sub directory. To move into the inhere directory we use**

**$ cd inhere**

**now if we run ls command in inhere, we don’t find any files because the file is hidden. To access to the hidden files we have to use the ls -a command. This shows the name of the hidden file as .hidden . We use the cat command to read the hidden file.**

**Cat .hidden**



**PASSWORD:- 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe**

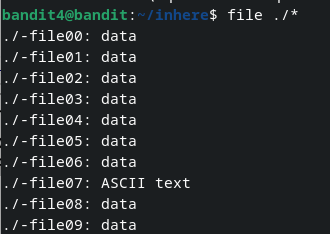
**RESOURCES USED:-** [**https://www.wikihow.com/Use-SSH**](https://www.wikihow.com/Use-SSH)

**LEVEL4-LEVEL5:-**

**Login to the host using $ ssh** [**bandit4@bandit.labs.overthewire.org**](mailto:bandit1@bandit.labs.overthewire.org) **-p2220**

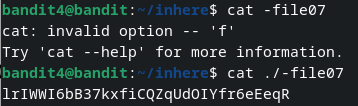
**I used the ls command to know the subdirectories.**

**It shows inhere. I used the cd inhere command to move into the directory. It shows 10 files with names as -file00 till -file 09. We now have to know the file which consists the password. Thus I used the file./\* command to know the type of data present in each file.**

****

**This shows that the password is present in - file07.**

**Now I tried to open the file by using cat -file07 and encountered with the following error.**

****

**Then I used $ cat ./-file07 and got the password.**

**PASSWORD:- lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR**

**LEVEL5-LEVEL6:-**

**Login to the host using $ ssh** [**bandit5@bandit.labs.overthewire.org**](mailto:bandit1@bandit.labs.overthewire.org) **-p2220**

**I use the ls command and then the cd inhere command to move into the inhere sub directory.**

**Then I used the ls command again to see the files inside the inhere directory. To search for the required file we can use the find command. Type the following command**

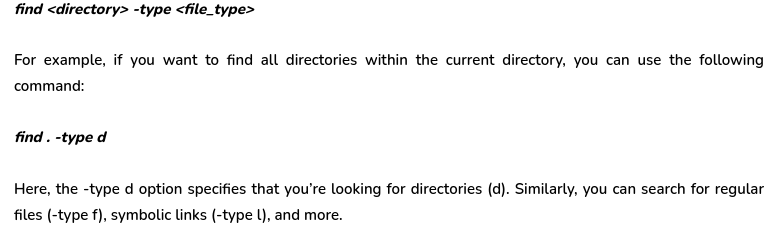
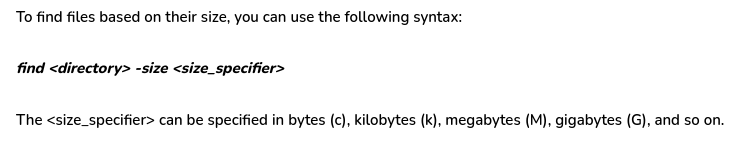
**$ find . -type f -size 1033c ! -executable**

**shows that the type of the file is regular.**

**Shows that the file to be searched has file size of 1033 bytes**

**shows that the file to be searched is not executable**

**PASSWORD:-P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU**

****

**SOURCE:-https://www.znetlive.com/blog/how-to-use-linux-find-command-to-search-for-files/**

**LEVEL6-LEVEL7:-**

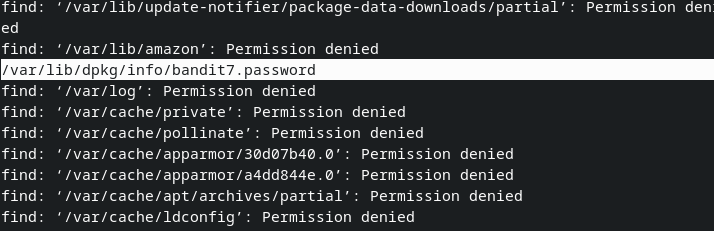
**Login to the host using $ ssh** [**bandit6@bandit.labs.overthewire.org**](mailto:bandit1@bandit.labs.overthewire.org) **-p2220**

**Using the properties given in question form the find command as follows**

**$ find / -user bandit7 -group bandit6 -size 33c**

**NOTE:- I did not mention any directory after the / to apply find for all the files.**

**We then get the output as follows. One of the lines consists of the path to the password.**

**I used the path to run the cat command**

**$ cat /var/lib/dpkg/info/bandit7.password**

**PASSWORD:- z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S**

**LEVEL7-LEVEL8:-**

**Login to the host using $ ssh** [**bandit7@bandit.labs.overthewire.org**](mailto:bandit1@bandit.labs.overthewire.org) **-p2220**

**First I used the ls command to see the files inside. It showed data.txt.**

**I ran the cat data.txt command. This gives all the data inside the file , thus we have to use another command. To find a word or string in a long list we must use the grep command as follows to get the password.**

**$ cat data.txt | grep millionth**

**PASSWORD:- TESKZC0XvTetK0S9xNwm25STk5iWrBvP**

**RESOURCES USED:-** [**https://stackoverflow.com/questions/9665292/linux-search-for-a-particular-word-in-a-list-of-files-under-a-directory**](https://stackoverflow.com/questions/9665292/linux-search-for-a-particular-word-in-a-list-of-files-under-a-directory)

**LEVEL8-LEVEL9:-**

**Login to the host using $ ssh** [**bandit8@bandit.labs.overthewire.org**](mailto:bandit1@bandit.labs.overthewire.org) **-p2220**

**First used the ls command. Output given out as data.txt. We need to find the non repeating statement . So we use**

**$ cat data.txt| sort| uniq -u**

**reads and prints the data.txt file**

**sorts the strings in each line**

**prints the unique string only**

**PASSWORD:- EN632PlfYiZbn3PhVK3XOGSlNInNE00t**

**RESOURCES USED:-** [**https://www.geeksforgeeks.org/sort-command-linuxunix-examples/**](https://www.geeksforgeeks.org/sort-command-linuxunix-examples/)

**LEVEL9-LEVEL10:-**

**Login to the host using $ ssh** [**bandit9@bandit.labs.overthewire.org**](mailto:bandit1@bandit.labs.overthewire.org) **-p2220**

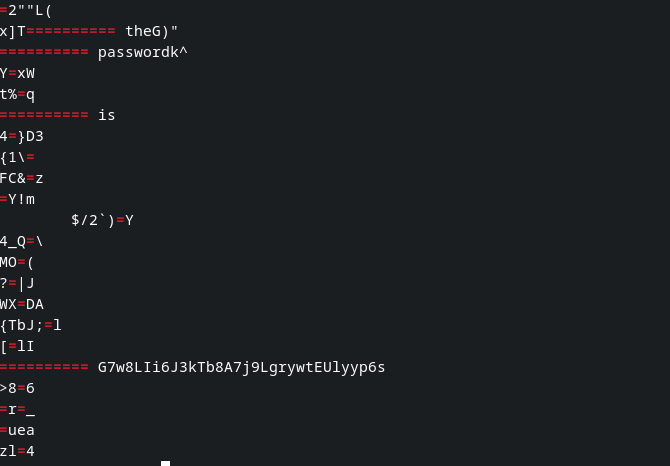
**Run the ls command to see the data.txt file.**

**Since we want the human readable only files we use the strings command.**

**Since it is given that there are a lot of = in front of password we use grep command.**

**The final command will be**

**$ cat data.txt| strings| grep =**

****

**thus we can see the password.**

**PASSWORD:- G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s**

**RESOURCES USED:-** [**https://www.javatpoint.com/linux-strings-command**](https://www.javatpoint.com/linux-strings-command)

**LEVEL10-LEVEL11:-**

**Login to the host using $ ssh** [**bandit10@bandit.labs.overthewire.org**](mailto:bandit1@bandit.labs.overthewire.org) **-p2220**

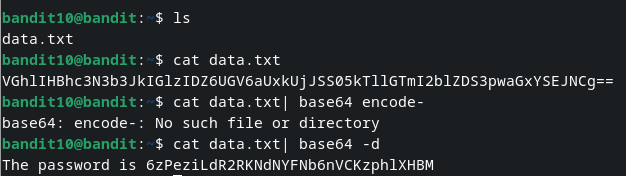
**As we run the cat command for data.txt file we receive a string which is encoded in base64.**

**To decode it we must use base64-d command which simply decodes a base64 encrypted string to normal string.**

**The command run is**

**$ cat data.txt| base64 -d**

**This shows the password.**

****

**PASSWORD:-6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM**

**RESOURCES USED:-** [**https://www.sanfoundry.com/base64-command-usage-examples-linu/**](https://www.sanfoundry.com/base64-command-usage-examples-linu/)

**LEVEL11-LEVEL12:-**

**Login to the host using $ ssh** [**bandit11@bandit.labs.overthewire.org**](mailto:bandit1@bandit.labs.overthewire.org) **-p2220**

**As we run the cat command for data.txt file we receive a string which is encoded by rotating 13 times. To decode it we must use the** tr 'A-Za-z' 'N-ZA-Mn-za-m' command.

**Thus the final command would be**

**$ cat data.txt| tr 'A-Za-z' 'N-ZA-Mn-za-m'**

**This decrypts the statement and gives us the password.**



**PASSWORD:- JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv**

**RESOURCES USED:-https://stackoverflow.com/questions/5442436/using-rot13-and-tr-command-for-having-an-encrypted-email-address**