Over the Wire (Bandit) writeup (Level 0-15)

Level 0-1:

Initially use ssh to login as bandit0 using the below command:
`sudo ssh bandit0@bandit.labs.overthewire.org -p 2220`
Then type in `yes` and hit enter and then enter the password `bandit0`.

Once you login as **bandit0**, run `ls` to list all the files in the current directory. You will find a readable file called **readme**. You can read the contents of the file by running `cat readme`, and this will print out the contents of the file onto your terminal.
NOTE: The contents of **readme** will be the password for the next level.

Level 1-2:

Now login as **bandit1** using `sudo ssh bandit1@bandit.labs.overthewire.org -p 2220` and enter the password obtained from the **readme** file.
Run `ls` to list the files in your current directory and you'll find a file named **-** . To view the contents of this file, you have to mention the entire path of the file because its name consists of **-** which is a flag specifier for every linux command. Run `cat /home/bandit1/-` and this will print out the contents of the file, which is the password for the next level.

Level 2-3:

Now login as **bandit2** using the command mentioned above. Then run `ls` to list the files and you will find a file that has spaces in its filename. To view the contents of this file you have to use `''` while mentioning the file name. Run `cat 'spaces in this filename'` and this will print the contents of the file. And you have your password for the next level!

Level 3-4:

Login in as **bandit3** and run `ls` to list the directory contents. You will find a directory called **inhere**. Move into the directory using `cd inhere` and run `ls` to list its contents. You will see nothing showing in the listing because the file is hidden. Now to list hidden files, run `ls -al` and this will list the hidden file named **.hidden**. Run `cat .hidden` to list the contents of the hidden file which is the password for the next level.

Level 4-5:

Login as **bandit4** and run `ls`, you will see a directory named **inhere**. Move into the directory and list its contents. You will see 10 readable files with a **-** in the beginning. Now to view the contents of these

files make sure you mention the entire path of the file. Run `cat /home/bandit4/inhere/-file00` and this will print the contents. Do this for every file till you find a readable string which will be the password for the next level.

Level 5-6:

Login as **bandit5** and run `ls`. You will find a directory called **inhere**, move into the directory and list its contents. You will find 20 directories named **maybehere**. On the challenge page you will find a hint saying the required file is **1033 bytes in size**. To list a detailed view of the directories, run `ls -al maybehere00` and this will list the contents of the file in a detailed manner, showing the file size of every file in the directory. Repeat this for every directory till you find a file whose size is 1033 bytes. Once you find that particular directory, move into it and print the contents of the required file and you have the password for the next level!

Level 6-7:

Login as **bandit6**. On the challenge page you will find a hint saying that the password to the next level is stored in a file that is somewhere on the server and its location is unknown. To find a particular file or directory, use a command called `find`. Run `find / -size 33c -user bandit7`. This will specify the size of the file, user assigned to the file and where to look. You will get an output where the file location is mentioned, i.e. `/var/lib/dpkg/info/bandit7.password`. View the contents of the file and you have the password for the next level.
NOTE: While running `cat` to view the contents of the file, make sure to mention the full path of the file.

Level 7-8:

Login as **bandit7** and run `ls` to list the contents of the current directory. You will find a text file named **data.txt**. This file contains a large amount of strings and within these strings lies our password for the next level. According to the hint on the challenge page, the password is next to the word **millionth**. Run `cat data.txt | grep millionth` and this will get you the string next to the word **millionth**. You are basically viewing the contents of the file and choosing a particular word to display on your terminal. You have the password for the next level!

Level 8-9:

Login as **bandit8** and run `ls`. You will find a file named **data.txt**. According to the hint given on the challenge page, the password in the only line of text that occurs only once. Rest other strings are repeated. Now to sort the strings, run `cat data.txt | sort | uniq -u` and this will sort the strings and print the required string, which is the password for the next level.

Level 9-10:

Login as **bandit9** and list the contents of the current directory. You will find a file named **data.txt**. When you run `cat data.txt`, it will print a number of non-readable strings. According to the hint given of the challenge page, the password is a human-readable text preceeded by several **=**. Run `file data.txt` and this will tell you that **data.txt** is a binary file. Now to find the string hidden in this binary file, run `strings data.txt` and this will print all the strings present in data.txt. You will see the password for the next level on your terminal.

Level 10-11:

Login as **bandit10** and run `ls`. You will see a file named **data.txt**. When you run `file data.txt`, it will mention that the file contains ASCII text. On the challenge page it says that the string inside **data.txt** is a **base64 encoded** text. To decode the text, run `cat data.txt | base64 -d` and this will give you the password fo the next level.

Level 11-12:

Login as **bandit11** and run `ls`. You will see a file named **data.txt** which contains a string. According to the hint given on the challenge page, all lowercase and uppercase letters have been rotated by 13 positions. To bring them back to their original letters, we'll be using a tool called `tr`. This is used to tranform/truncate letters in a string. Run `cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'`. This will give you the password for the next level.

Level 12-13:

Login as **bandit12** and run `ls`. You will see a file named **data.txt**. According to the hint given on the challenge page, this file contains a hexdump of a file which has been compressed multiple times. The hint also says to create a temporary directory using `mkdir /tmp/test`, this will create a directory named **test** inside the `tmp` directory. Copy the file into the **test** directory using `cp data.txt /tmp/test` and rename it to data using `mv data.txt data`.
Since the data inside the file is ASCII text, we have to convert the file from **.txt** form to **binary** form. Run `xxd -r data > binary` and this will create a binary file. To confirm, run `ls` and you can see a file called **binary**. If you run `file binary`, you will see that the file has been compressed using a tool called `gzip`. Run `mv binary binary.gz` and this will convert it to `.gz` extension. Now you can decompress it using `gzip -d binary.gz` and you will get a file which has been compressed using `bzip2`. Run `bzip2 -d binary` to decompress the file. This will generate a file called **binary.out**. If you run `file binary.out` you will see that it was compressed using `gzip`. Run `mv binary.out binary.gz` to change the file extension to `.gz`. Now decompress it using `gzip -d binary.gz` and you will get a file named **binary** which is archived using a tool called `tar`. To extract the data, run `tar -xf binary`. This will give you a file called **data5.bin**. When you run `file data5.bin`, you will see that it is also an archived file. This proves that multiple compressions have been performed on the password file. Repeat the above steps based on the type of file you have until you get a file named **data8.bin** which will be of **ASCII text** filetype. View its contents to get the password for the next level.

Level 13-14:

Login as **bandit13** and run `ls`. You will see a **ssh private rsa key**. This key is used to login remotely through SSH. Run `ssh -i sshkey.private bandit14@localhost` and you will be logged in as **bandit14**.
According to the hint given on the challenge page, the password of **bandit14** is stored inside `/etc/bandit_pass/bandit14`. Run `cat /etc/bandit_pass/bandit14` and this will give you the password.

Level 14-15:

According to the hint given on the challenge page, the password of **bandit14** has to be submitted to port **30000** to retrieve the password for **bandit15**. You can do this using a tool called `netcat`. Run `netcat localhost 30000` and this will allow you to enter the password of **bandit14** in the next line. Enter the password or paste it and then hit enter. This will give the password for **bandit15**.

For any clarifications, hit me up on Discord -- Rohan_Karki#3255