**CTF Write-up**

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

Table of Contents

[OverTheWire – Bandit 3](#_Toc140766511)

[Bandit0 3](#_Toc140766512)

[Bandit1 3](#_Toc140766513)

[Bandit2 3](#_Toc140766514)

[Bandit3 4](#_Toc140766515)

[Bandit4 5](#_Toc140766516)

[Bandit5 6](#_Toc140766517)

[Bandit6 7](#_Toc140766518)

[Bandit7 8](#_Toc140766519)

[Bandit8 9](#_Toc140766520)

[Bandit9 10](#_Toc140766521)

[Bandit10 11](#_Toc140766522)

[Bandit11 12](#_Toc140766523)

[Bandit12 13](#_Toc140766524)

[Bandit13 15](#_Toc140766525)

[Bandit14 16](#_Toc140766526)

[Bandit15 17](#_Toc140766527)

[Bandit16 18](#_Toc140766528)

[Bandit17 19](#_Toc140766529)

[Bandit18 20](#_Toc140766530)

[Bandit20 21](#_Toc140766531)

[Bandit20 22](#_Toc140766532)

# OverTheWire – Bandit

## Bandit0

Text

Description automatically generated

After ssh with bandit0 and password bandit0, I used ‘ls’ command and saw a ‘readme’ file. I used ‘cat’ command to see info in ‘readme’ file, and it shows a line of character. That will be the password to bandit1, which is NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

## Bandit1

Text

Description automatically generated

In bandit1, I used ‘ls’ command and saw a file named ‘-‘. I used ‘./’ and followed the filename and successfully open the file, then I got the password, which is rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

## Bandit2

Text

Description automatically generated

I used ‘ls’ command and saw the file named with spaces. So, when I cat the file, I used back slash ‘\’ at behind of the file before the spaces. But we also can first type spaces then press “Tab” to let it finish by itself, it’s extremely useful. aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

## Bandit3

Text

Description automatically generated

The questions said the password stored inside the ‘inhere’ folder. After cd in, I used ‘ls -a’ to see all files including hidden file. Then I ‘cat’ to get the password. 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

## Bandit4

Text

Description automatically generatedText

Description automatically generated

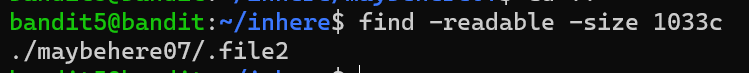
Its not a good idea to check them one by one, but luckily there just 10 files, I probably should use find command.

Up: I got a new solution, using “file ./\*” can check the info in all of the file. lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

## Bandit5

Text

Description automatically generated



Used ‘ls’ command and saw too much of directory in it, I got a hint from the question, it said maybe can use find command, and go to google and someone said man the find. After searching, I used ‘find’ command with ‘-readable’ to filter out human-readable file, ‘-size 1033c’ to find the file size with 1033 bytes. And I got a file named ‘-file2’.

Text

Description automatically generated

And I got a long line of human-readable characters. In case it’s wrong I opened another file

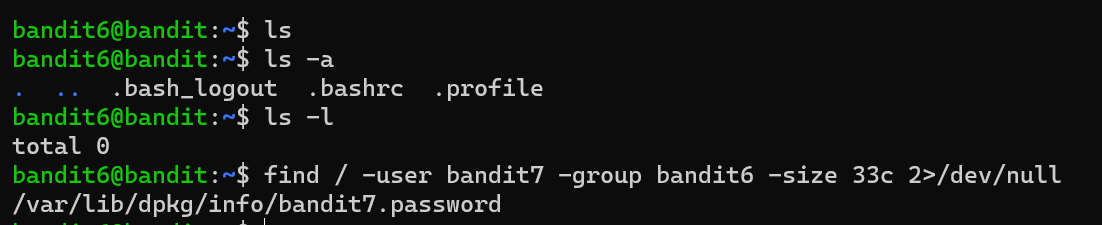
Text

Description automatically generated

And it’s not readable…So -file2 should be storing password.

P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

## Bandit6



After using series of ls commands, there’s no file or directory to do. After doing some research on Medium, I got this command. “/” after find is to let find command search the entire file system from root. “2>/dev/null” is to prevent ‘permission denied” error display in the screen.



z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

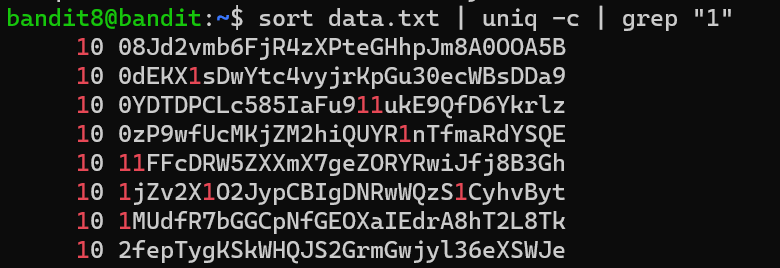
## Bandit7

Text

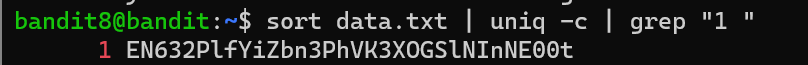
Description automatically generated

Used “ls – l” to check the size of the text file. Used “grep” to know the password TESKZC0XvTetK0S9xNwm25STk5iWrBvP is beside the word that said in the question.

## Bandit8



Using “sort” command to sort data.txt, and “uniq -c” command to count the repeated lines. Then used grap “1” to get that have 1. But we need to write with “grep “1 “ “ to ensure it’s 1 not everything that has 1.



EN632PlfYiZbn3PhVK3XOGSlNInNE00t

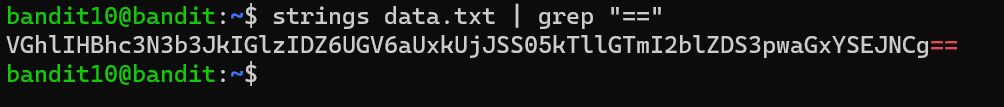
## Bandit9

A black screen with white text

Description automatically generated with low confidence

Used “strings” command to show the data, and grep to filter with several “=”. G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

## Bandit10



Usually, Base64 encrypt will include double equal sign at the last of the cipher text.

A screenshot of a computer

Description automatically generated

Use cyberchef to decrypt the cipher text to plain text. 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

## Bandit11

A black screen with white text

Description automatically generated

ROT13 encrypt is to change the first 13 alphabet to last 13 alphabets.

A screenshot of a computer

Description automatically generated with medium confidence

JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

## Bandit12

A screen shot of a computer program

Description automatically generated

According to the question, first create temporary folder for the data.txt by using “mkdir”, then copy the file to the folder created.

“xxd” creates hex dump or converts it back to binary form. Used “xxd -r [file to convert] > [converted location]”

A screenshot of a computer

Description automatically generated

Checked the file type of file decompressed by “xxd”, its “gzip”, used “gunzip -c [file to decompressed] > [file destination]” to decompress the file, “-c” is to write the standard output, and keep the file unchanged.

A computer screen with white text

Description automatically generated

“file02” is “bzip2”, used “bunzip2 -c [file to decompressed] > [file destination]”, and checked “file03” is “gzip”, similar to the previous step, got “file04”. “file04” is “tar”.

A screen shot of a computer program

Description automatically generated

Used “tar -xf [file to decompressed] to decompress the file, but without the destination, the destination fille will automatically out, “-xf” is to extract the tar file. Similar to a ”file04”, “data5.bin” use the similar command to get “data6.bin””, and it’s “bzip2”.

A computer screen shot of white text

Description automatically generated

wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

Used the similar command to get “file07” from “data6.bin”, and “data8.bin” from “file07”. When “gunzip -c data8.bin” will get the final result, which is the password for bandit13.

## Bandit13

A computer screen shot of a computer screen

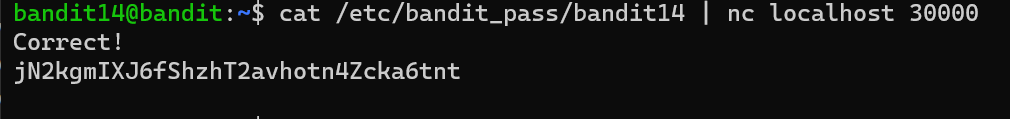
Description automatically generated

Used “ssh” and public key provided to connect bandit14 without password. “-i” is to select a file from which the identity (private key) for public key authentication is read. Then add “sshkey.private” which is the public key provided. And typed “bandit14@localhost” to log in to bandit14 as localhost. But not successful, so ai went to another website and found out to use original login method, which is “[bandit14@bandit.labs.overthewire.org -p 2220](mailto:bandit14@bandit.labs.overthewire.org%20-p%202220)” as it said I was attempting to log in as port 22 (ssh), but not their own port. (?)

A screen shot of a computer

Description automatically generated

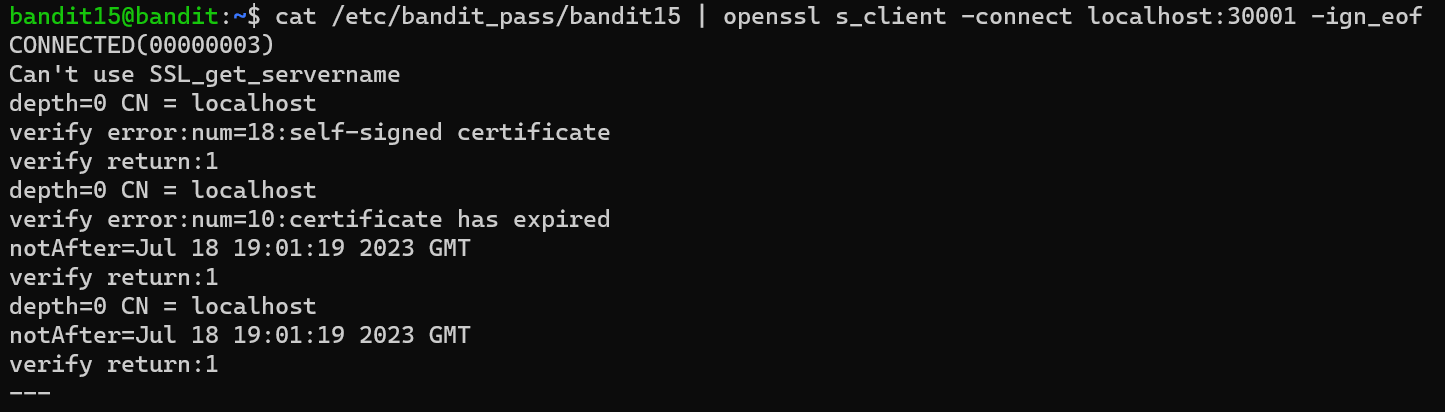
## Bandit14



jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

We know that the password is stored in “/etc/bandit\_pass/”, for “bandit14” just use command above and netcat the question required, then will get the password.

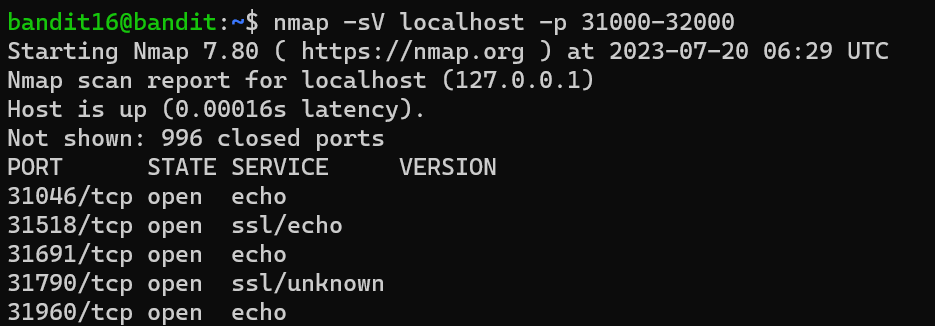
## Bandit15



JQttfApK4SeyHwDlI9SXGR50qclOAil1

Enter command above to connect by openssl, then will get the password.

## Bandit16



First used “nmap” to scan for open ports, “-sV” is to do a service/version detection scan in localhost and specify the ports with “-p”.

Then got 5 open ports, the one we need is ssl, but 31518 and 31790 are 2 provide ssl, but 31518 only supports echo, we I chose 31790.

A screen shot of a computer

Description automatically generated

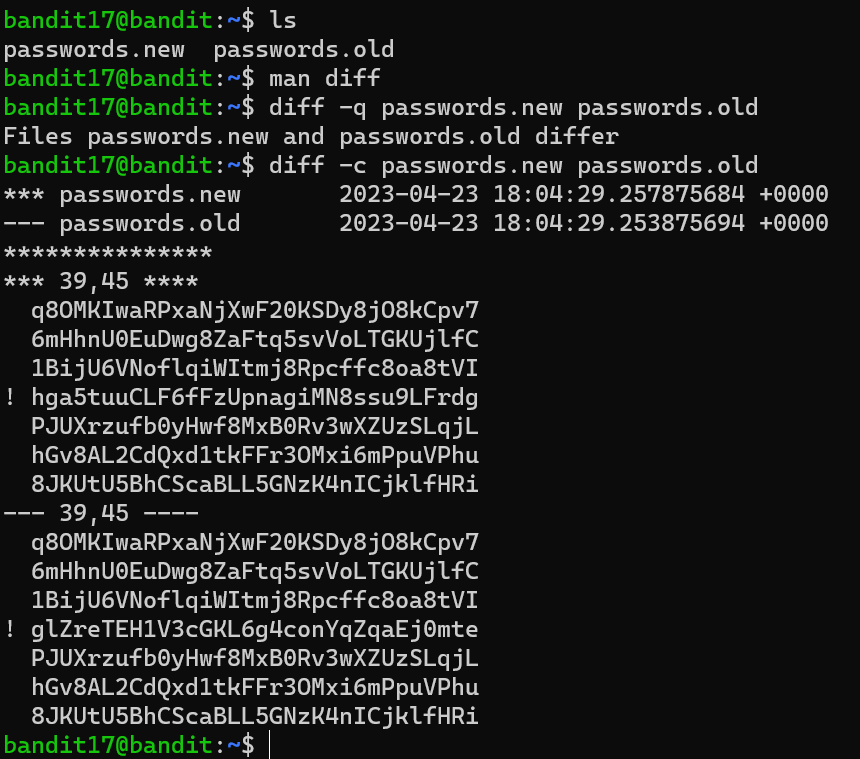
Used the similar command and will get the RSA private key. “cat /etc/bandit\_pass/bandit16 | openssl s\_client -connect localhost:31790 -ign\_eof”, and get the RSA private key.

Then, “mkdir /tmp/tmp\_key/sshkey17.txt”, save the key to “sshkey17.txt”, and change the file permissions to only readable, which is “chmod 400 sshkey17.txt”

Lastly, use “ssh bandit17@bandit.labs.overthewire.org -p 2220 -i /tmp/tmp\_key/sshkey17.txt” to get through bandit17.

After got in, I got the password VwOSWtCA7lRKkTfbr2IDh6awj9RNZM5e is “/etc/bandit\_pass/bandit17”

## Bandit17



hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg

Used “diff” command to find the difference between two files, “-q” is just showing the brief, “-c” shows the columns.

## Bandit18

A screen shot of a computer

Description automatically generated

After enter password to enter bandit18 as usual, “bye bye!” message will pop out and kick me out, this is because “.bashrc” file had been modified. So, I did some research and found out to use ssh as normal then put command behind it.

A screenshot of a computer screen

Description automatically generated

awhqfNnAbc1naukrpqDYcF95h7HoMTrC

## Bandit20

A computer screen shot of a computer

Description automatically generated

Red color file is setuid file, as the question, run the file with cat password,

A screenshot of a computer screen

Description automatically generated

The bandit20 shows when running file, it will run as bandit20

VxCazJaVykI6W36BkBU0mJTCM8rR95XT

## Bandit20