Juned OverTheWire Bandit Guide:

**Level 0** – I used the ls command to find the readme text file. Then I used the cat command to see file content.

Password: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

**Level 1** – I had used cat ‘-‘ but this did not work, I assume because – is not a typical file name, or that the way that I had used cat was not working. I then used pwd to give me the directory path, then using that as my argument. The command that worked was cat /home/bandit1/-

Password: 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

**Level 2** – This was simply using the cat command with the ‘’ signs. The command was cat ‘spaces in this filename’

Password: MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx

**Level 3** – I had first used cd to enter the InHere folder. I then used ls -a to find any hidden files. I found a hidden file called …Hiding-From-You and used cat Hiding-From-You to open it.

Password: 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

**Level 4** – Similar to level 1 where the files where I had to type out the entire directory for the cat command to work, I carried out this command until I found the readable file i.e. cat /home/bandit4/inhere/-file07

Password: 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

**Level 5** – I had used the ls command alongside the following addons ‘l’ ‘a’ ‘R’. This allowed me to see hidden files, file details, and ALL files within my current directory. The command was ls -laR

Because I could not scroll down, I piped this command into the ‘less command so that I could scroll down. I then found the file that fits the description, it was within the maybehere07 directory and was called ‘.file2’

I then used cat to read the content of the file.

Password: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

**Level 6** – As it had said that the file was located somewhere within the server, I had traversed to the root directory and then used the find command, giving it the parameters of -group and -user. The command used was find -group bandit6 -user bandit7

The file was located within the .var/lib/dpkg/info directory. I then used cat to obtain the password from that file.

Password: morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj

**Level 7** – This was simply using the grep command i.e. grep millionth data.txt

Password: dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

**Level 8** – I had sorted the data and then piped it into the cat command. I then manually went through the file and found the line of text that appeared only once. The command used was sort data.txt | cat

Password: 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

**Level 9 –** There are two ways that I had solved this. The first was that, since the Linux system is treating it as a binary file and not a text file, I used strings data.txt | cat . What this does is that the strings command only retains the readable characters of the file, then the cat command displays them. Another way is using grep -a “=” data.txt . The -a argument makes grep treat the file as a text file rather than a binary file.

Password: FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

**Level 10 –** I had used the command base64 with the -d argument which allows the file to be decoded i.e. base64 -d data.txt | cat

Password: dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

**Level 11** – I had used the tr command to shift the letters 13 places back. I had used the internet to find the actual part of the code that represents the shifting of letters. The code that I had used was cat data.txt | tr ‘A-Za-z’ ‘N-ZA-Mn-za-m’

Password: 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4

**Level 12 –** I had to watch a tutorial (https://www.youtube.com/watch?v=DMcKsu6atHw) as it was difficult. You essentially need to unzip the file again and again depending on what compression method was used on the file.

Password: FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn

**Level 13** – I had simply SSH’ed into the next level by using the private key i.e. ssh -i sshkey.private bandit14@bandit.labs.overthewire.org -p 2220

Password: The SSH Key. There is no password for this level

**Level 14** – I was given a ‘password from Level 13. I first tried to ssh into local host using port 30000 but that did not work. I then saw on the help section on the ‘OverTheWire’ site that netcat may be needed. I used the command nc localhost 30000

I then entered my ‘password’ given from Level 13, and it gave me the password in order to go onto Level 15.

Password: 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

**Level 15 –** The netcat command would not work here since SSL/TLS is not supported with that. The openssl command was recommended to be used on the ‘OverTheWire’ site. I had used this alongside the argument of s\_client with and the -connect argument to create a SSL/TLS connection i.e openssl s\_client -connect localhost:30001

I then submitted the password of the current level and it responded with the password with the next level.

Password: kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

**Level 16 –** I had used the nmap scan firstly to scan for open ports i.e. nmap -p 31000-32000

It gave me the open ports of 31046, 31518, 31691, 31790, 31960

I then tested each of these ports with the command that I had used in the previous level i.e. openssl s\_client -connect localhost:[IP GOES HERE]

I concluded that the port 31790 was the correct port but unfortunately it would not give me the output that I wanted (i.e. the password) after I had fed it the password from the previous level (i.e. level15). I do not know why but it would say ‘KEYUPDATE’ and then would say wrong password.

UPDATE: I searched up on reddit and saw that since my previous password started with ‘k’, I had to attach the -quiet flag to my openssl command for it to work.

RSA Private Key:

MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ

imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ

Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu

DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW

JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX

x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD

KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl

J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd

d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC

YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A

vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama

+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT

8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx

SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd

HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt

SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A

R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi

Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg

R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu

L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni

blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU

YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM

77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b

dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3

vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=

**Level 17 –** This was a simple use of the command ‘diff’ i.e. diff passwords.new passwords.old

It then presented the different lines in both files.

Password: x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO

**Level 18 –** I first tried to ignore the bashrc file when ssh’ing into the terminal but that did not work. Then I thought if I could edit the bashrc file in my ssh command, but that did not work. I then went ahead and tried this command (i.e. ssh bandit18@bandit.labs.overthewire.org -p 2220 vim readme) in order to open the readme file and it worked.

Password: cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8

**Level 19 –** From what I understood after watching videos, the setuid essentially gives you access of whoever the owner is of the setuid program file. In this case the owner of the file is bandit20, and I need to use the program file in order to access the password file since only bandit20 can access the password file. I used the command /home/bandit19/bandit20-do cat bandit20

Password: 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO

**Level 20** **–** I had created a listening port (port number 12345) on another terminal and then, on another terminal, used the setuid program to connect to the 12345 port and send the password obtained from the previous level (level 19) to this port 12345 and it gave me the password.

Password: EeoULMCra2q0dSkYj561DX7s1CpBuOBt