**CRYPTONITE**

TASKPHASE

**WEEK 2**  D.VISHWATEJ

**BANDIT LEVEL 12- LEVEL 21:-**

**LEVEL12:-**

Login to the host using $ ssh [bandit12@bandit.labs.overthewire.org](mailto:bandit1@bandit.labs.overthewire.org) -p2220

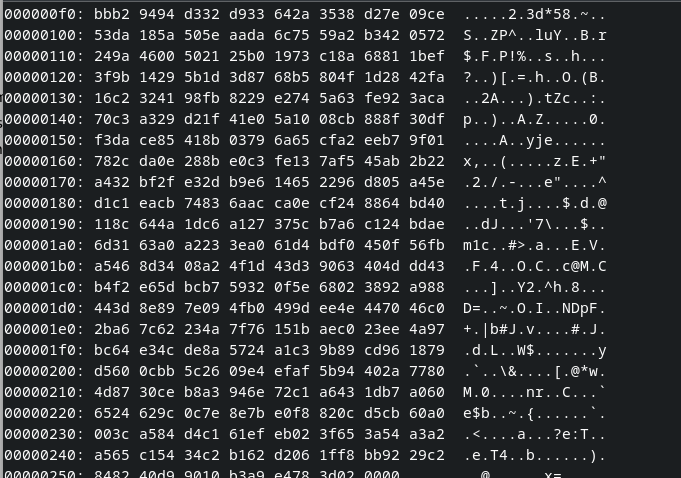
The goal is to decompress the hexdump file to retrieve the password from the file data.txt which is repeatedly compressed.

First , use the cat command to read the file

Ls

cat data.txt

we get the output as follows



The command used for decrypting the hexdump file into normal file is xxd -r

thus i used the command

$ xxd -r data.txt > new

but the permission is denied.

Using the hint in the question

i created a new directory using the following command

$ mkdir /tmp/vishwa2006

now as we have made a new directory which has various permissions we copy the data.txt file into the new directory using the command

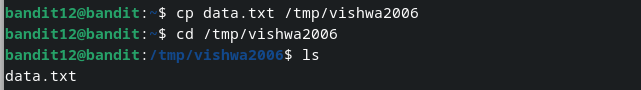
$ cp data.txt /tmp/vishwa2006

Now we dive into the new directory and check the files inside

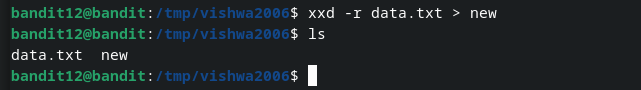
$ cd /tmp/vishwa2006

$ ls

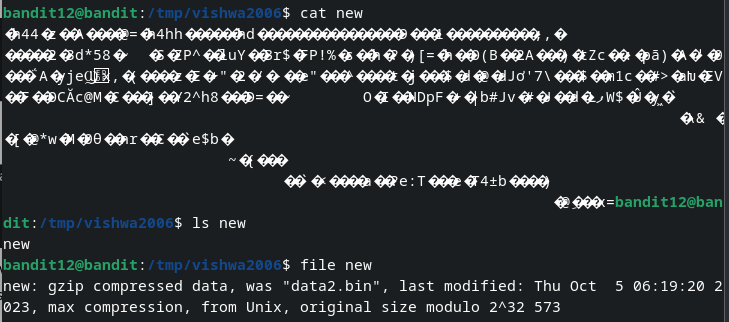
it shows



Now as we have permission , we use xxd -r command to decrypt the hexdump file and direct it to a file called new



Now if we run the cat command on the decrypted ‘new’ file we get unreadable characters. If we run file command on new to know its type we get it is a gzip file….

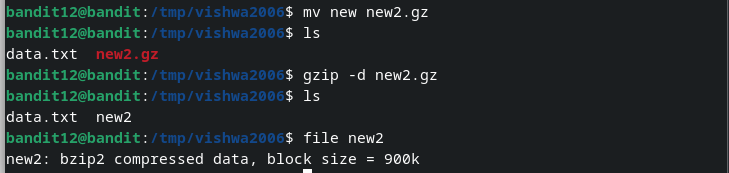


if we try to decompress the file new using gzip -d we get



This is because the file extension is wrong. We thus change the name of the file using mv command.

$ mv new new2.gz



Now the new2.gz file has been decompressed.(The extension changes as shown in th image)

it is now as bzip2 compressed file.

similar to 1st case now we change extension to bz2. then use bzip2 -d command to decrypt it. after its decryption we check the file type of new2 again, now it is gzip again.

we change its extension to gz

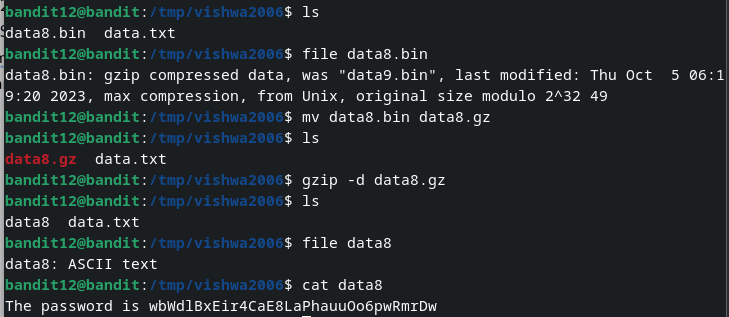
$ mv new2.out new3.gz

as we check the file type of new3 it is POSIX tar archive (GUI)

we change extension to new3.tar using mv command.

after we decompress the file using the tar xf command we can find the data5.bin file in the contents.

similarly after repeated decompression of files from data2.bin to data9.bin we get the final password in form of ascii text.



PASSWORD:- wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

RESOURCES USED:- <https://www.geeksforgeeks.org/cp-command-linux-examples/>

<https://www.geeksforgeeks.org/mv-command-linux-examples/>

OTHER COMMANDS USED FOR HELP:- man gzip

man bzip2

**LEVEL13:-**

Login to the host using $ ssh [bandit13@bandit.labs.overthewire.org](mailto:bandit1@bandit.labs.overthewire.org) -p2220

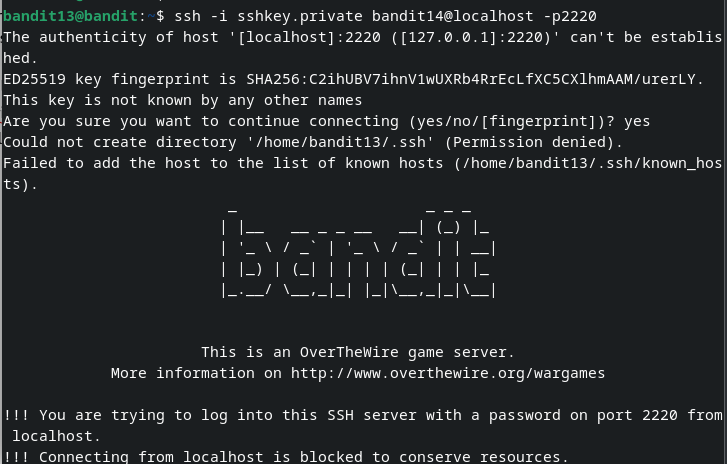
Using the ls command we get to know that there is a file named as sshkey.private

Using cat command we get a long string named as private key.

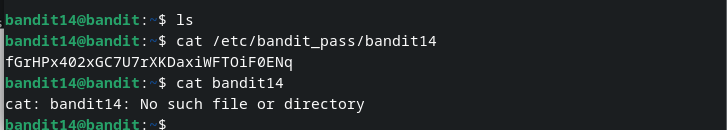
Now we use the command ssh -i filename user@ hostname -port0000

$ssh -i sshkey.private bandit14@localhost -p2220

this takes us directly into the next level.



If we want to know the password , we use the path given in etc/bandit\_pass/bandit14



PASSWORD:- fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq

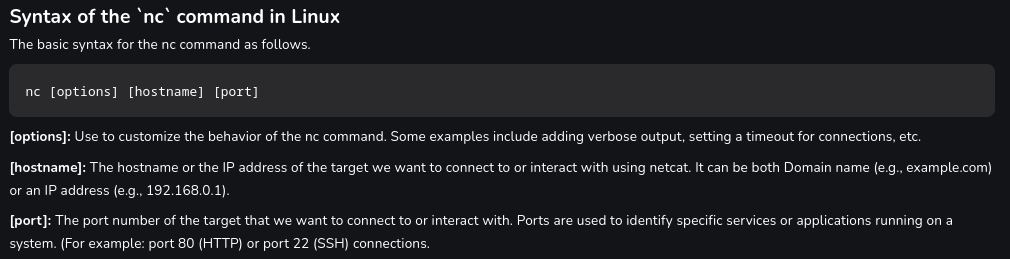
RESOURCES USED:- <https://www.cloudbolt.io/blog/linux-how-to-login-with-a-ssh-private-key/>

**LEVEL14:-**

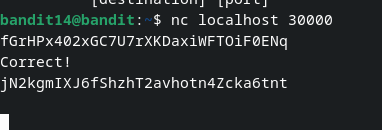
We are now already logged in in bandit14@bandit .

COMMANDS TO BE KNOWN FOR SOLVING THIS LEVEL:- nc

**nc** :-The Netcat ( nc ) command is **a command-line utility for reading and writing data between two computer networks.**



We follow the above command, then enter the password to get the password for the next level.



PASSWORD:- jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

RESOURCES USED:- <https://www.geeksforgeeks.org/practical-uses-of-ncnetcat-command-in-linux/>

**LEVEL15**:-

Login to the host using $ ssh [bandit15@bandit.labs.overthewire.org](mailto:bandit1@bandit.labs.overthewire.org) -p2220

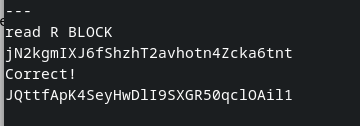
The goal is to use ssl encryption do retrieve the password from the localhost.

The command syntax which is used for ssl encryption is

$ openssl s\_client -connect hostname :[port]

$ openssl s\_client -connect localhost :30001

Then we enter the password. this gives the password for next level



PASSWORD:- JQttfApK4SeyHwDlI9SXGR50qclOAil1

**LEVEL16:-**

Login to the host using $ ssh [bandit16@bandit.labs.overthewire.org](mailto:bandit1@bandit.labs.overthewire.org) -p2220.

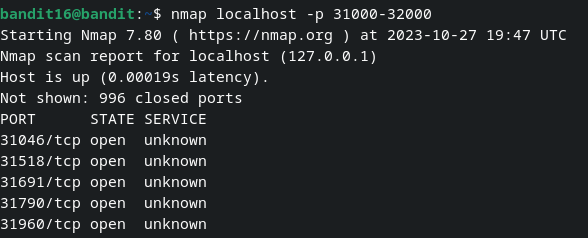
The goal is to retrieve the password from the specific file present in the ports range.

the command which helps us to scan for open ports is nmap.

The command to be used is

$ nmap localhost -p 31000-32000

This command gives all of the open ports in the server.

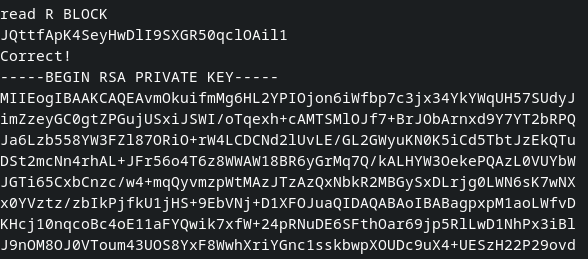
****

Now to know the service version present in the different ports we need to use the sV command along with the nmap scanning command.

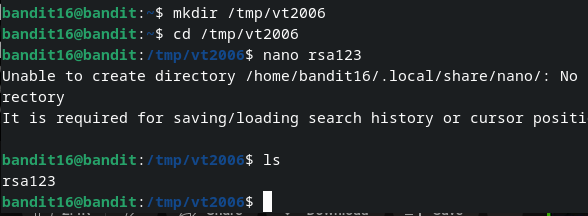
$ nmap localhost -p 31046,31518,31691,31790,31960 -sV

this gives the version of all the open ports.

There are two open ports with ssl service in them. After we input password in both of them we get the private key from port 31790.



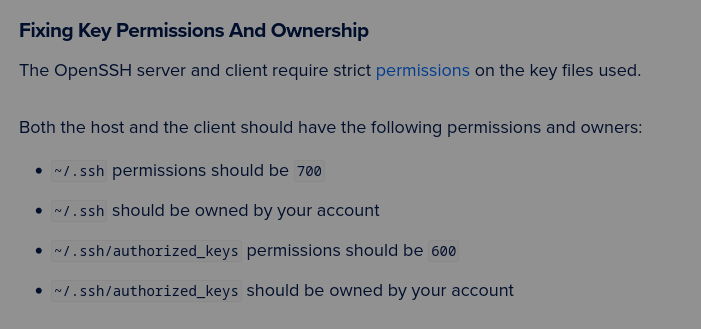
Now i copied the entire rsa private key. This is now only a simple text, i have to save it in a file this is done by nano command .This file is to be made in a tmp directory thus the following process must be followed.



nano command is a line editor command where we paste the key and convert it to a file.

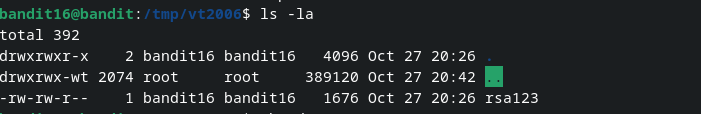
After we save the file then we can use the $ssh -i filename bandit17@localhost -p2220 command to directly login into the next level.

NOTE:- the permissions of the rsa key must be changed because it must be kept secure. We thus use chmod command to change permission to 600.



logic behind the permissions:-

use ls -la command to know permissions



in 3rd line we can see -rw-rw-r

this says that the user can read and write it, groups can read and write it , people can read it.

4 stands for permission to read and 2 stands for permission to write.

Thus the user gets 6. and others get a 0.

Thus we used 600 with chmod command.

PASSWORD:- VwOSWtCA7lRKkTfbr2IDh6awj9RNZM5e

RESOURCES USED:- <https://docs.digitalocean.com/support/how-to-troubleshoot-ssh-authentication-issues/#fixing-key-permissions-and-ownership>

<https://beebom.com/how-use-nano-linux/>

<https://www.techtarget.com/searchsecurity/feature/How-to-use-Nmap-to-scan-for-open-ports>

**LEVEL17:-**

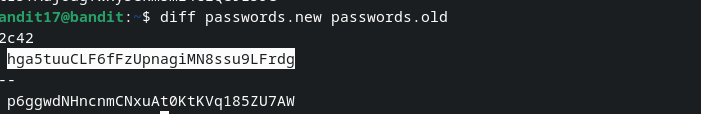
As we are already logged in in level 17…

we use ls command to look at what files are present ,

it shows passwords.old and passwords.new

To know the password we must know the string which is different in the files. The command which fulfills this task is diff command .

$ diff passwords.new passwords.old



The password is present in password.new so the 1st line is the password.

PASSWORD:- hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg

**LEVEL18:-**

Login to the host using $ ssh [bandit18@bandit.labs.overthewire.org](mailto:bandit1@bandit.labs.overthewire.org) -p2220.

When logging in due to the modification of .bashrc we get a message byebye! and we are logged out of the server.

Thus we can use two commands at once

$ ssh bandit18@bandit.labs.overthewire.org -p2220 ls

Then we use the following command

$ ssh bandit18@bandit.labs.overthewire.org -p2220 cat readme

PASSWORD:- awhqfNnAbc1naukrpqDYcF95h7HoMTrC

**LEVEL19:-**

Login to the host using $ ssh [bandit19@bandit.labs.overthewire.org](mailto:bandit1@bandit.labs.overthewire.org) -p2220.

To execute a file the command used is ./

Now we use that command along with the cat command and using the path given in question.

$ ./bandit20-do cat /etc/bandit\_pass/bandit20

this gives us the password for the next level.

PASSWORD:- VxCazJaVykI6W36BkBU0mJTCM8rR95XT

**LEVEL20:**-

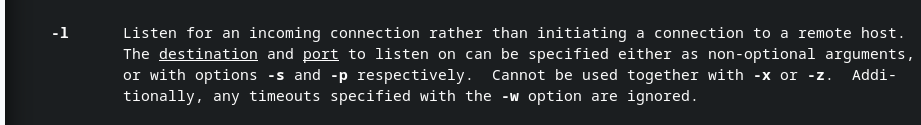
Login to the host using $ ssh [bandit20@bandit.labs.overthewire.org](mailto:bandit1@bandit.labs.overthewire.org) -p2220

To solve this level we use two shells simultaneously, one for logging into the port and listening and one for sending the password string.

In one shell , we use nc -l [port]

$ nc -l 2006

This command is used to make the port listen to a incoming connection.



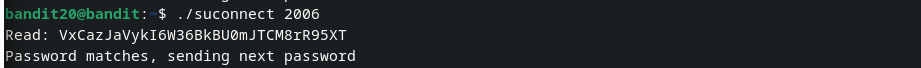
In other shell , type

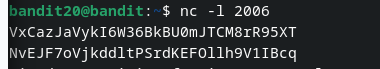
$ ./suconnect 2006

This command is used to send the password from one shell to other for checking.

Now we type password in the shell with nc command.

We receive the password for next level.





PASSWORD:- NvEJF7oVjkddltPSrdKEFOllh9V1IBcq

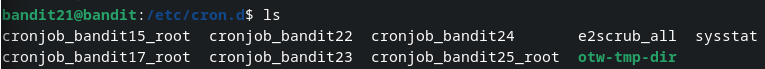
**LEVEL21:-**

Login to the host using $ ssh [bandit21@bandit.labs.overthewire.org](mailto:bandit1@bandit.labs.overthewire.org) -p2220

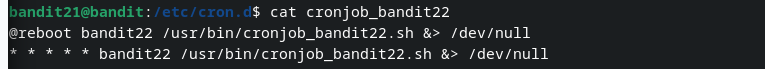
We now use ls command , but we dont find any file inside . Thus we use the path present in the question to enter the directory.

$ cd /etc/cron.d/

Now we use ls command to see all the files inside.

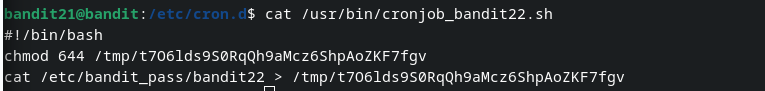


we require password for level 22 so we open cronjob\_bandit22 using cat command.



It says that this file is being run at regular intervals.

If we use the path given in above file and use cat command again we will find the bash file which will repeat.



This says that it changes permissions of the /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv file and the password is in the file.

Thus we use cat command once again for that file to get the password.

PASSWORD:- WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff