Level 0 to 1

CONNECTING TO BANDIT SERVER:

ssh bandit0@bandit.labs.overthewire.org -p 2220

password:bandit0

If you typed in the correct password, you should now be logged into the remote machine and see a Welcome text with more information about the game.

ls

cat readme

will get password for level 1

LEVEL1 to 2

ssh bandit1@bandit.labs.overthewire.org -p 2220

and copy paste the password:

ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

ls

cat

(will get password for next level)

Level 2 to 3

ssh bandit2@bandit.labs.overthewire.org -p 2220

263JGJPfgU6LtdEvgfWU1XP5yac29mFx

ls(there is a file called “spaces in this file”)

to see it’s content :

cat “spaces in this file”

then we will get password for next level

Level 3 to 4:

ssh bandit3@bandit.labs.overthewire.org -p 2220

MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx

Ls(we saw folder “inhere”)

cd inhere(to move to this file)

ls -hal(to see hidden files)

cat .hidden(to get password for next level)

Level 4 to 5:

ssh bandit4@bandit.labs.overthewire.org -p 2220

2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

Here we have inhere directory

To move into this directory we use cd command

To list all elements w use “ls command”

Since we are looking for ASCII text among files00 to file09 we use

find . |xargs file {} \; |grep “ASCII text”

Then we got to know that ./-file07 is ASCII

So we retrieve data from that using cat ./-file07

(then we will get password for next level)

Level 5 to 6

ssh bandit5@bandit.labs.overthewire.org -p 2220

4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

ls(we have inhere directory)

To move in to this directory we use “cd inhere”

Then we use ‘ls’ command to list items

Since we are searching for file with sepcifuc attribute , we use the command

find ./inhere -readable -size 1033c \! -executable

Then we get the file

So to retrieve password from that file we use cat command

“cat maybehere07/.file2”

(Then we will get password for next level)

Level 6 to 7

ssh bandit6@bandit.labs.overthewire.org -p 2220

HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

ls

ls-hal

find / -user bandit7 -group bandit6 -size 33c 2>/dev/null

The expression “2>/dev/null” is to ignore errors

Then we wil get “/var/lib/dpkg/info/bandit17.password”

To retrieve password we use “cat /var/lib/dpkg/info/bandit17.password”

(Then we will get password for next level)

Level 7 to 8

ssh bandit7@bandit.labs.overthewire.org -p 2220

morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj

ls -hal

The size of data.txt is 4.0MB so it is hard to find a word from this large file so we use “grep” command

“grep millionth data.txt”

Then we will get Password for next level

Level 8 to 9

ssh bandit8@bandit.labs.overthewire.org -p 2220

dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

ls -hal

Then we use “sort” command to sort all lines in alphabetical order and “uniq-u” command to ensure than unique lines are printed

sort data.txt | uniq-u

(Then we will get password for next level)

Level 9 to 10

ssh bandit9@bandit.labs.overthewire.org -p 2220

4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

Ls -hal

We have text file named “data.txt”.It contains both strings and numbers which is very difficult to read beginning with “=” sign

We use combination of queries i.e first we need to sort out plain text and then the output of first command shoub be gripped with “=” sign

So the queryb looks like

cat data.txt | strings | grep ^=

(Then we will get password for next level)

Level 10 to 11

ssh bandit10@bandit.labs.overthewire.org -p 2220

FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

ls(to list)

The file named as “data.txt” has base 64 encoded data. To decode it, use
“base64 decode” command. The query is as follows:

cat data.txt | base64 –decode

Then we will get password for next level

Level 11 to 12

ssh bandit11@bandit.labs.overthewire.org -p 2220

dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

ls

(we found out that the password is stored in data.txt where all lowercase and uppercase have been rotated by 13 positions.To decode this we use command)

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

(Then we will get password for next level)

Level 12 to 13

ssh bandit12@bandit.labs.overthewire.org -p 2220

7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4

Ls

Mkdir /tmp/acm

Cp data.txt /tmp/acm

Cd /tmp/acm

Xxd -r data.txt > data

File data

Mv data file.gz

Gzip -d file.gz

ls

File file

Mv file file.bz2

Bzip2 -d file.bz2

Ls

File file

Mv file file.tar

Tar xf file.tar

Ls

File data5.bin

Rm file.tar

Rm data.txt

Ls

File data5.bin

Mv data5.bin data.tar

Tar xf data.tar

Ls

File data6.bin

Mv data6.bin data.bz2

Bzip2 -d data.bz2

Ls

File data

Mv data data.tar

Ls

Tar xf data.tar

File data8.bin

Mv data8.bin data.gz

Ls

File data

Cat data

(Then we will get password for next level)

Level 13 to 14

ssh bandit13@bandit.labs.overthewire.org -p 2220

MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS

ls(to list,we wil get ssshkey.private)

So we will use “ssh -I ssshkey.private bandit14@localhost -p 2220”

ls-hal

Since the password is in “*“/etc/bandit_pass/bandit14” we will use command cat /etc/bandit_pass/bandit14*

(we will get password for next level)

Level 14 to 15

ssh bandit14@bandit.labs.overthewire.org -p 2220

8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

(now type ‘nc’ command .’nc’ command creates a TCP connection if given a hostname or port number)

nc localhost 30000(and enter password of lvl 14)

then we will get password for next level

Level 15 to 16

ssh bandit15@bandit.labs.overthewire.org -p 2220

8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

Now we use ‘ls -hal’ command

To connect to a server, we use the following command syntax:

Format:
“openssl s_client -connect <www.abcd.com>:port_number”

Here:
“openssl s_client -connect localhost:30001”

Now enter password of this level

Then we will get password for next level

Level 16 to 17:

ssh bandit16@bandit.labs.overthewire.org -p 2220

kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

nmap localhost -p31000-32000 (Through trial and error method, SSH your way into all ports which are open. Here, port number “31790” is connected)

openssl s_client _connect localhost:31790

Now, scroll down and paste your current level password and you will be

presented an RSA private key with which we will login to the next level i.e

“bandit17".

Save the RSA private key to your local system using the name
“bandit17.key.” using vim editor.

Now, SSH your way into bandit17 using “bandit17.key” file using command:

“sudo ssh -i bandit17.key bandit17@bandit.labs.overthewire.org -p 2220"

Using “ls” command, we can observe two files namely, “passwords.new” and “passwords.old”. Open the two files and you will see a bunch of passwords with some duplications.

To remove duplications, use “diff” command i.e. “diff passwords.new passwords.old” which gives us two unique passwords and if you try to login both attempts would be unsuccessful.

If we consider all the solved levels, we can observe that all passwords are stored in the “/etc/bandit_pass” folder. Using “cd” command, move to the folder and type “ls” to see the files available

We can see that there are files ranging from “bandit0" to “bandit33". Since, we are trying to find password for bandit17, use “cat” command to see the contents of bandit17

Level17 to 18

ssh bandit17@bandit.labs.overthewire.org -p2220

EReVavePLFHtFlFsjn3hyzMlvSuSAcRD

ls(we will get passwords.new passwords.old)

diff passwords.old passwords.new

The < sign represents the lines that have been removed and the > sign represents the lines that have been added in its place

The line after the > sign is the password for the next level

Level 18 to 19

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

x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO

ls

(will get readme)

cat readme

(will get password for next level)

Level 19 to 20

ssh bandit19@bandit.labs.overthewire.org -p2220

cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8

ls

(will get bandit20-do)

ls -l

(when we list the details of the file we can see that the binary file can be executed by the current user (bandit19) and it is owned by bandit20)

./bandit20-do (./<filename> to access the file)

./bandit20-do cat /etc/bandit_pass/bandit20

(Then we will password for level20)

Level 20

ssh bandit20@bandit.labs.overthewire.org -p2220

0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO