This doc will help me to remind how to use the command of linux. I site where I am learning is https://overthewire.org/wargames/bandit.

LEVEL 0:
To start we have to connect via ssh to the host -> ssh bandit0@bandit.labs.overthewire.org -p 2220
the psw is bandit0

LEVEL 1:

Now we ha ve to read the readme and to repeat our connect but this time to -> ssh bandit1@bandit.labs.overthewire.org -p 2220 with this psw that we had find before
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

LEVEL 2:
Now you have to read in a file named "-", that is not a normal file because you have to read it with this command "cat <"
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

LEVEL 3:
Now you have a file named "space in this filename", thus you have a file that has spaces. To read it you have to digit cat "spaces in this filename"
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

LEVEL 4:
We have a file that is hidden. To find it we use the command "ls -a"
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

LEVEL 5:
In this directory we have all the file that start with – so like this format "-file00" to read it you have to specific "cat ./-file00" the command "./" specific that we are now in the current directory.
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

LEVEL 6:

Now we have to find a file that is of 1033 bytes in size and not executable. We use the find command "find .

-type f -size 1033c ! -executable"

P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

LEVEL 6:

You have to search a file with this caratteristics -> owned by user bandit7 owned by group bandit 6 and with

33bytes in size.

The command syntax is: find / -type f -user bandit7 -group bandit6 -size 33c

z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

LEVEL 7:
You have to search a word in a file.txt
grep 'millionth' data.txt
TESKZC0XvTetK0S9xNwm25STk5iWrBvP

LEVEL 8:
You have to search a word that is the only line of the text that occurs only once
sort data.txt | uniq -u
The uniq -u command only shows lines that appear once, but requires the lines to be consecutive to determine whether or not they repeat. If the lines are not sorted, some non-consecutive duplicate lines may not be correctly identified as such.
EN632PlfYiZbn3PhVK3XOGSlNInNE00t

LEVEL 9:
In a file not legible you have to find the legible character
strings data.txt | grep '^='
G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

LEVEL 10
The psw now is stored in a file which contains base64 encoded data
base64 -d data.txt
6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

LEVEL 11
You have to rotate the letter of 13 positions
cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

LEVEL 12
You have to do a lot of passage.
mkdir tmp/Giacomo
cp data.txt ./tmp/Giacomo
mv data.txt new_data.txt
xxd -r new_data.txt > data
file data
(.gz) gzip -d file.gz
(.bz2) bzip2 -d file.bz2
(.tar) tar xf file.tar

LEVEL 13
this level is just a connection to the next level. You have a secret rsa key and to connect to the next level
ssh -i sshkey.private -p 2220 bandit14@bandit.labs.overthewire.org

LEVEL 14
You have to send your password “fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq” to you localhost and at the 30000 port
echo "fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq" | nc localhost 30000
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

LEVEL 15
Here you have to stabilize a ssh connection and then as you can see the prompt is waiting for you. Type the password “jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt”.
openssl s_client -connect localhost:30001
JQttfApK4SeyHwDlI9SXGR50qclOAil1

LEVEL 16
I initially used nmap to look for open ports in the 31000-3200 range

nmap -p 31000-32000 localhost
openssl s_client -connect localhost:31790
chmod 700 private.key
(in /tmp) ssh -i key.private -p 2220 bandit17@bandit.labs.overthewire.org

LEVEL 17
diff passwords.new passwords.old
hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg

LEVEL 18
ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme
awhqfNnAbc1naukrpqDYcF95h7HoMTrC

LEVEL 19
./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVykI6W36BkBU0mJTCM8rR95XT

LEVEL 20
TERMINAL 2
ssh bandit20@bandit.labs.overthewire.org -p 2220
nc -lvp 9999
TERMINAL 1
./suconnect 9999
TERMINAL 2
VxCazJaVykI6W36BkBU0mJTCM8rR95XT
TERMINAL 1
NvEJF7oVjkddltPSrdKEFOllh9V1IBcq

LEVEL 21
you have to read the exercise cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff

LEVEL 22
echo I am user bandit23 | md5sum | cut -d ' ' -f 1
cat tmp/8ca319486bfbbc3663ea0fbe81326349
QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G

LEVEL 23
echo "cat /etc/bandit_pass/bandit24 > /tmp/giacomo/pass.txt" > pass.sh
chmod 777 pass.sh
cat /tmp/giacomo/pass.txt
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar

LEVEL 24
You have to go brute force a nc connection putting firstly the psw and after a digit composed by 4-digit from 0000 to 9999
So you write a code that:
echo “VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar i_loop” | nc localhost 30002 | grep -v “Wrong”
Remember to specify #!/bin/bash
uNG9058gUE7snukf3bvZOrxhtnjzSGzG