ACM Tasks

Bandit task

Level 0

```
heshaja@Ts-MacBook-Air ~ % ssh bandit0@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password:
```

Password : bandit0

Level 0 —-> 1

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
heshaja@Ts-MacBook-Air ~ %
```

ls — lists the files in the current directory

cat —- we can use this to see the contents in any line by entering as “ cat readme”
By this we can get the contents in the readme file soo we got the password for the next level

Level 1 —--> 2

After entering exit in the previous level we will be logged out
Then , we should again

```
heshaja@Ts-MacBook-Air ~ % ssh bandit1@bandit.labs.overthewire.org -p 2220
```

Password : NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

As we got the password in the previous level

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
heshaja@Ts-MacBook-Air ~ %
```

ls —- lists the files in the current directory
cat ./- —- represents that display the contents that are in the “-” file , there . represents the home directory

Level 2 —--> 3

After entering exit in the previous level we will be logged out
Then , we should again

```
heshaja@Ts-MacBook-Air ~ % ssh bandit2@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit2@bandit.labs.overthewire.org's password:
```

Password : rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
As we got the password in the previous level

```
bandit2@bandit:~$ ls
 spaces in this filename
bandit2@bandit:~$ cat "spaces in this filename"
 aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
bandit2@bandit:~$ exit
 logout
 Connection to bandit.labs.overthewire.org closed.
 heshaja@Ts-MacBook-Air ~ %
```

If we gave the code like cat spaces in this filename ,then by default it takes spaces as one directory and in as one directory like that upto filename sooo we will enter it in the “ ”.

Level 3 —-> 4

After entering exit in the previous level we will be logged out
Then , we should again

```
heshaja@Ts-MacBook-Air ~ % ssh bandit3@bandit.labs.overthewire.org -p 2220
```

Password : aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
As we got the password in the previous level

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
heshaja@Ts-MacBook-Air ~ %
```

If the formate is like this ,

cd directory then the directory will change to that directory from previous directory

cd —- is used to change the directory
ls -a —-- this is used to list all the hidden files or directories in the current working directory
cat —-- displays all the contents in the current directory

Level 4 —-> 5

After entering exit in the previous level we will be logged out
Then , we should again

```
heshaja@Ts-MacBook-Air ~ % ssh bandit4@bandit.labs.overthewire.org -p 2220
```

Password : 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
As we got the password in the previous level

```
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ find . -type f | xargs file
./-file01: data
./-file02: data
./-file08: data
./-file06: data
./-file00: data
./-file04: data
./-file05: data
./-file07: ASCII text
./-file03: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
heshaja@Ts-MacBook-Air ~ %
```

cd —- used to change the directory
ls —-- lists all the fikes that exit in the current directory

find . -type f —-- This finds all files in the current directory and its subdirectories , as we mentioned (.) so this represents the current directory .

| —-- This is a pipe, which takes the output of the command on its left and passes it as input to the command on its right.

xargs file — This checks each file found by find command and passes it as an argument to the file command, which determines the file type.

Here ./-file07 is a text file soo the password will be stored in this file / directory

cat —- displays all the contents in the current directory

Level 5 —> 6

After entering exit in the previous level we will be logged out
Then , we should again

```
heshaja@Ts-MacBook-Air ~ % ssh bandit5@bandit.labs.overthewire.org -p 2220
```

Password : lrlWWI6bB37kxfiCQZqUdOIYfr6eEeqR

As we got the password in the previous level

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
```

```
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

```
bandit5@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
heshaja@Ts-MacBook-Air ~ %
```

ls —- lists all the files and directories in the current directory

cd —- used to change the directory

find . -type f -size 1033c ——--

this means , it finds all files in the current directory and its subdirectories , as we mentioned (.) so this represents the current directory .

as in the question it mentioned that size is 1033 byte so we entered as (-size 1033c) here c represents bytes

! -executable —-- this mean that in question it is mentioned that it is not executable so we represent not by (!) .

cat —- displays all the content in the current directory

Level 6 —-> 7

After entering exit in the previous level we will be logged out
Then , we should again

```
heshaja@Ts-MacBook-Air ~ % ssh bandit6@bandit.labs.overthewire.org -p 2220
```

Password :

As we got the password in the previous level

```
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
```

After entering this we get all the file names in that we will have
(/var/lib/dpkg/info/bandit7.password)

```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
bandit6@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
heshaja@Ts-MacBook-Air ~ %
```

find —---- This is the command used for searching files.

/ —--- This specifies the directory to start the search from. In this case, it starts from the root directory /.

-type f —---- This specifies that we are searching for regular files (not directories or other types of files).

-user bandit7 —---- This specifies that the file's owner should be the user bandit7

-group bandit6 —--- This specifies that the file's group should be bandit6

-size 33c —--- This specifies that the file's size should be 33 bytes.

cat —--- displays all the contents in the current directory .

Level 7 ——--> 8 :

After entering exit in the previous level we will be logged out
Then , we should again

```
heshaja@Ts-MacBook-Air ~ % ssh bandit7@bandit.labs.overthewire.org -p 2220
```

Password : z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

As we got the password in the previous level

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth       TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
heshaja@Ts-MacBook-Air ~ %
```

ls ——- lists all files and directories in the current directory .

string data.txt ——— this command extracts the printable strings from data.txt file .

| ——- This is a pipe, which takes the output of the command on its left and passes it as input to the command on its right.

grep “millionth” ——— by using grep it will search the word millionth and prints and shows the matching files .

Level 8 ——--> 9 :

After entering exit in the previous level we will be logged out
Then , we should again

```
heshaja@Ts-MacBook-Air ~ % ssh bandit8@bandit.labs.overthewire.org -p 2220
```

Password : TESKZC0XvTetK0S9xNwm25STk5iWrBvP

As we got the password in the previous level

```
bandit8@bandit:~$ cat data.txt
```

We will get all the strings in this data.txt file

```
bandit8@bandit:~$ sort data.txt | uniq -c
```

sort data.txt —- sorts data.txt contained strings or information into alphabetical order

| —-- This is a pipe, which takes the output of the command on its left and passes it as input to the command on its right.

uniq -c —--- as it is mentioned in the question that the password is stored in one line text so

By using (uniq -c) we can known how many times the text is repeated .

Level 9 —--> 10 :

After entering exit in the previous level we will be logged out
Then , we should again

```
heshaja@Ts-MacBook-Air ~ % ssh bandit9@bandit.labs.overthewire.org -p 2220
```

Password : EN632PlfYiZbn3PhVK3XOGSlNInNE00t

As we got the password in the previous level

```
bandit9@bandit:~$ strings data.txt | grep "="
=2""L(
x]T========== theG)"
========== passwordk^
Y=xW
t%=q
========== is
4=}D3
{1\=
FC&=z
=Y!m
        $/2`)=Y
4_Q=\
MO=(
?=|J
WX=DA
{TbJ;=l
[=lI
========== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
>8=6
=r=_
=uea
zl=4
bandit9@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
heshaja@Ts-MacBook-Air ~ %
```

strings data.txt —-- this command extracts the printable strings from data.txt file .

| —- This is a pipe, which takes the output of the command on its left and passes it as input to the command on its right.

grep “=” —--- finds the text that starts with “=” as it is mentioned in the question that password is stored after several “=” characters .

Level 10 —--> 11 :

After entering exit in the previous level we will be logged out
Then , we should again

```
heshaja@Ts-MacBook-Air ~ % ssh bandit10@bandit.labs.overthewire.org -p 2220
```

Password : G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

As we got the password in the previous level

```
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTllGTmI2blZDS3pwaGxYSEJNCg==
bandit10@bandit:~$ base64 -d data.txt
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
heshaja@Ts-MacBook-Air ~ %
```

cat data.txt —- display the contents in data.txt file .

base64 -d data.txt —-- by using base64 -d this will decode the content stored in the data.txt file .

Level 11 —-->12 :

After entering exit in the previous level we will be logged out
Then , we should again

```
heshaja@Ts-MacBook-Air ~ % ssh bandit11@bandit.labs.overthewire.org -p 2220
```

Password : 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

As we got the password in the previous level

```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSKBbJ8puQm5lIEi
bandit11@bandit:~$ cat data.txt | tr abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ nopqrstuvwxyzabcdefghijklmNOPQRSTUVWXYZABCDEFGHIJKLM
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
bandit11@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

ls —-- lists all the files and directories in the current directory

cat data.txt —-- displays all the contents that are present in the data.txt

| —- This is a pipe, which takes the output of the command on its left and passes it as input to the command on its right.

tr [set1] [set2] —- this is the syntax while using tr tag

set1 will be the alphabets of lower and upper case and set2 will the alphabets after shifting 13 positions lowercase and uppercase .

Then we will get our password

Level 12 —-> 13 :

After entering exit in the previous level we will be logged out
Then , we should again

```
heshaja@Ts-MacBook-Air ~ % ssh bandit12@bandit.labs.overthewire.org -p 2220
```

Password : JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

As we got the password in the previous level

```
bandit12@bandit:~$
bandit12@bandit:~$ cat data.txt
```

```
bandit12@bandit:~$ mkdir /tmp/heshaja
bandit12@bandit:~$ cp data.txt /tmp/heshaja
bandit12@bandit:~$ cd /tmp/heshaja
bandit12@bandit:/tmp/heshaja$ ls
data.txt
bandit12@bandit:/tmp/heshaja$ xxd -r data.txt > data
bandit12@bandit:/tmp/heshaja$ ls
data  data.txt
bandit12@bandit:/tmp/heshaja$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu Oct  5 06:19:20 2023, max compression, from Unix, original size modulo 2^32 573
bandit12@bandit:/tmp/heshaja$ mv data file.gz
bandit12@bandit:/tmp/heshaja$ gzip -d file.gz
bandit12@bandit:/tmp/heshaja$ ls
data.txt  file
bandit12@bandit:/tmp/heshaja$ file file
file: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/heshaja$ mv file file.bz2
bandit12@bandit:/tmp/heshaja$ bzip2 -d file.bz2
bandit12@bandit:/tmp/heshaja$ ls
data.txt  file
bandit12@bandit:/tmp/heshaja$ file file
file: gzip compressed data, was "data4.bin", last modified: Thu Oct  5 06:19:20 2023, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/heshaja$ mv file file.gz
bandit12@bandit:/tmp/heshaja$ gzip -d file.gz
bandit12@bandit:/tmp/heshaja$ ls
data.txt  file
bandit12@bandit:/tmp/heshaja$ file file
file: POSIX tar archive (GNU)
bandit12@bandit:/tmp/heshaja$ mv file file.tar
bandit12@bandit:/tmp/heshaja$ tar xf file.tar
bandit12@bandit:/tmp/heshaja$ ls
data5.bin  data.txt  file.tar
bandit12@bandit:/tmp/heshaja$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/heshaja$ rm file.tar
bandit12@bandit:/tmp/heshaja$ rm data.txt
bandit12@bandit:/tmp/heshaja$ ls
data5.bin
bandit12@bandit:/tmp/heshaja$ file file
file: cannot open `file' (No such file or directory)
bandit12@bandit:/tmp/heshaja$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/heshaja$ mv data5.bin data.tar
bandit12@bandit:/tmp/heshaja$ tar xf data.tr
tar: data.tr: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
bandit12@bandit:/tmp/heshaja$ tar xf data.tar
bandit12@bandit:/tmp/heshaja$ ls
data6.bin  data.tar
bandit12@bandit:/tmp/heshaja$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/heshaja$ mv data6.bin data.bz2
bandit12@bandit:/tmp/heshaja$ bzip2 -d data.bz2
bandit12@bandit:/tmp/heshaja$ ls
data  data.tar
bandit12@bandit:/tmp/heshaja$ file file
file: cannot open `file' (No such file or directory)
bandit12@bandit:/tmp/heshaja$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/heshaja$ mv data data.tar
bandit12@bandit:/tmp/heshaja$ ls
data.tar
bandit12@bandit:/tmp/heshaja$ tar xf data.tar
bandit12@bandit:/tmp/heshaja$ ls
data8.bin  data.tar
bandit12@bandit:/tmp/heshaja$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Oct  5 06:19:20 2023, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/heshaja$ mv data8.bin data.gz
bandit12@bandit:/tmp/heshaja$ gzip -d data.gz
bandit12@bandit:/tmp/heshaja$ ls
data  data.tar
bandit12@bandit:/tmp/heshaja$ file data
data: ASCII text
bandit12@bandit:/tmp/heshaja$ cat data
The password is wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
bandit12@bandit:/tmp/heshaja$ exit
logout
Connection to bandit.labs.overthewire.org closed.
heshaja@Ts-MacBook-Air ~ %
```

Level 13 —-->14 :

After entering exit in the previous level we will be logged out
Then , we should again

```
heshaja@Ts-MacBook-Air ~ % ssh bandit13@bandit.labs.overthewire.org -p 2220
```

Password : wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

As we got the password in the previous level

```
bandit13@bandit:~$ ls
 sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220
 The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
 ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
 This key is not known by any other names
 Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

After entering yes there we will get access to bandit14

ls —-- lists all the files amd directories that are present in the current directory

As mentioned in the question if we enter “ ssh -i sshkey.private bandit14@localhost -p 2220 “ and entered yes we will get access to bandit14 level

Level 14 —–> 15 :

```
[bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
 fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
[bandit14@bandit:~$ nc localhost 30000

 Wrong! Please enter the correct current password
[fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
[bandit14@bandit:~$ nc localhost 30000
[fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
 Correct!
 jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt


[bandit14@bandit:~$ exit
 logout
 Connection to localhost closed.
[bandit13@bandit:~$ exit
 logout
 Connection to bandit.labs.overthewire.org closed.
 heshaja@Ts-MacBook-Air ~ %
```

As mentioned in the question the password of level 15 can be checked by nc localhost 30000 after giving the password we got after entering

“ cat /etc/bandit_pass/bandit14 “

password : fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq

cat —-- displays all the contents that are present in the provided file

Level 15 —–> 16:

After entering exit in the previous level we will be logged out
Then , we should again

```
[heshaja@Ts-MacBook-Air ~ % ssh bandit15@bandit.labs.overthewire.org -p 2220
```

Password : jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

As we got the password in the previous level

```
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
bandit15@bandit:~$ ncat --ssl localhost 30001
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
Correct!
JQttfApK4SeyHwDlI9SXGR50qclOAil1


Ncat: Input/output error.
bandit15@bandit:~$
bandit15@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
heshaja@Ts-MacBook-Air ~ %
```

As mentioned in the question the password that we got “jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt “ after entering “ cat /etc/bandit_pass/bandit15 “ should be submitted to localhost 30001 using ssl encryption so after that we will get the password for level 16

ncat —-- we initialised the network connection using ncat
It is a networking utility that reads and writes data across network connections . ncat means netcat.

--ssl —---> this flag is used for connections

Level 16 —-> 17:

After entering exit in the previous level we will be logged out
Then , we should again

```
heshaja@Ts-MacBook-Air ~ % ssh bandit16@bandit.labs.overthewire.org -p 2220
```

Password : JQttfApK4SeyHwDlI9SXGR50qclOAil1

As we got the password in the previous level

```
bandit16@bandit:~$ cat /etc/bandit_pass/bandit16
JQttfApK4SeyHwDlI9SXGR50qclOAil1
```

```
bandit16@bandit:~$ nmap localhost -p 31000-32000
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-10 08:24 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00018s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown
```

Here we used nmap to known what are the networks that are available in between 31000 to 32000 in that we got 31790 is working

Then we will enter the password that we got after entering
“ cat /etc/bandit_pass/bandit16 “

```
bandit16@bandit:~$ ncat --ssl localhost 31790
JQttfApK4SeyHwDlI9SXGR50qclOAil1
Correct!
-----BEGIN 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=
-----END RSA PRIVATE KEY-----
```

ncat — ncat —-- we initialised the network connection using ncat
It is a networking utility that reads and writes data across network connections . ncat means netcat.

--ssl —-- this flag is used for connections

```
bandit16@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
heshaja@Ts-MacBook-Air ~ % cd Desktop
heshaja@Ts-MacBook-Air Desktop % vim key
heshaja@Ts-MacBook-Air Desktop % chmod 400 key
heshaja@Ts-MacBook-Air Desktop % ssh -i key bandit17@bandit.labs.overthewire.org -p 2220
```

We will enter data that we got in vim key and
“ :q! “ —- by entering this we will exit the editing vim key
chmod 400 key —- to change the permissions (mode) of files and directories.

After that if we enter ” ssh -i key bandit17@bandit.labs.overthewire.org -p 2220 ”
We will go to level 17

Level 17 —--> 18 :

```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< p6ggwdNHncnmCNxuAt0KtKVq185ZU7AW
---
> hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
bandit17@bandit:~$ exit
```

ls —- lists the files and directories in the current directory
diff —-- compares the two files

Level 18 —--> 19 :

```
heshaja@Ts-MacBook-Air Desktop % ssh bandit18@bandit.labs.overthewire.org -p 2220
```

Password : hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg

As we got it in the previous level

```
Byebye !
Connection to bandit.labs.overthewire.org closed.
heshaja@Ts-MacBook-Air Desktop % ssh bandit18@bandit.labs.overthewire.org -p 2220 "ls"
```

It will ask password then we will enter the same password
“ hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg ”

```
heshaja@Ts-MacBook-Air Desktop % ssh bandit18@bandit.labs.overthewire.org -p 2220 "cat ~/readme"
```

It will ask password then we will enter the same password
“ hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg ”

Then we will get the password for next level

```
bandit18@bandit.labs.overthewire.org's password:
awhqfNnAbc1naukrpqDYcF95h7HoMTrC
heshaja@Ts-MacBook-Air Desktop %
```

cat ~/readme —- this mean that display the contents that are present in readme file which is in the homedirectory “ ~ “

Level 19 —> 20 :

```
heshaja@Ts-MacBook-Air Desktop % ssh bandit19@bandit.labs.overthewire.org -p 2220
```

Password : awhqfNnAbc1naukrpqDYcF95h7HoMTrC

As we got it from previous level

```
bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ file bandit20-do
bandit20-do: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, BuildID[sha1]=037b97b430
734c79085a8720c90070e346ca378e, for GNU/Linux 3.2.0, not stripped
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
  Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVykI6W36BkBU0mJTCM8rR95XT
bandit19@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
heshaja@Ts-MacBook-Air Desktop %
```

ls — this will show all the files and directories that are present in the current directory

file —- command is used to determine the type of a file.

./bandit20-do —-- by using this we are trying to execute a script or program located in the current directory.

Level 20 —-> 21 :

```
heshaja@Ts-MacBook-Air Desktop % ssh bandit20@bandit.labs.overthewire.org -p 2220
```

Password : VxCazJaVykI6W36BkBU0mJTCM8rR95XT

As we got it in the previous level