**Bandit over the wire**

**Level 10 - Level 20**

**NIKHIL KUMAR SINGH**

**ACIPAIE21002**

**BANDIT : OVER THE WIRE**

**Level 11:**

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

Password:IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Commands:

bandit11@bandit:~$ ls

data.txt

bandit11@bandit:~$ cat data.txt

Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh

We have to Rot the text by 13.We a website

website : <https://gchq.github.io/CyberChef>

After Rot:

The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

**Password for Level 12:**5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Now exit ()

**Level 12:**

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

Password:5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Commands:

**bandit12@bandit:**~$ ls

data.txt

**bandit12@bandit:~**$ mkdir /tmp/data

bandit12@bandit:~$ cp data.txt /tmp/data

bandit12@bandit:~$ cd /tmp/data

bandit12@bandit:/tmp/data$ ls

data.txt

bandit12@bandit:/tmp/data$ xxd -r data.txt > data

bandit12@bandit:/tmp/data$ ls

data data.txt

bandit12@bandit:/tmp/data$ file data

data: gzip compressed data, was "data2.bin", last modified: Thu May 7 18:14:30 2020, max compression, from Unix

bandit12@bandit:/tmp/data$ mv data data.gz

bandit12@bandit:/tmp/data$ gzip -d data.gz

bandit12@bandit:/tmp/data$ ls

data data.txt

bandit12@bandit:/tmp/data$ file data

data: bzip2 compressed data, block size = 900k

bandit12@bandit:/tmp/data$ mv data data.bz2

bandit12@bandit:/tmp/data$ bzip2 -d data.bz2

bandit12@bandit:/tmp/data$ ls

data data.txt

bandit12@bandit:/tmp/data$ file data

data: gzip compressed data, was "data4.bin", last modified: Thu May 7 18:14:30 2020, max compression, from Unix

bandit12@bandit:/tmp/data$ mv data data.gz

bandit12@bandit:/tmp/data$ gzip -d data.gz

bandit12@bandit:/tmp/data$ ls

data data.txt

bandit12@bandit:/tmp/data$ file data

data: POSIX tar archive (GNU)

bandit12@bandit:/tmp/data$ mv data data.tar

bandit12@bandit:/tmp/data$ tar xf data.tar

bandit12@bandit:/tmp/data$ ls

data5.bin data.tar data.txt

bandit12@bandit:/tmp/data$ rm data.tar

bandit12@bandit:/tmp/data$ file data5.bin

data5.bin: POSIX tar archive (GNU)

bandit12@bandit:/tmp/data$ mv data5.bin data.tar

bandit12@bandit:/tmp/data$ tar xf data.tar

bandit12@bandit:/tmp/data$ ls

data6.bin data.tar data.txt

bandit12@bandit:/tmp/data$ file data6.bin

data6.bin: bzip2 compressed data, block size = 900k

bandit12@bandit:/tmp/data$ mv data6.bin data.bz2

bandit12@bandit:/tmp/data$ bzip2 -d data.bz2

bandit12@bandit:/tmp/data$ ls

data data.tar data.txt

bandit12@bandit:/tmp/data$ rm data.tar

bandit12@bandit:/tmp/data$ file data

data: POSIX tar archive (GNU)

bandit12@bandit:/tmp/data$ mv data data.tar

bandit12@bandit:/tmp/data$ tar xf data.tar

bandit12@bandit:/tmp/data$ ls

data8.bin data.tar data.txt

bandit12@bandit:/tmp/data$ file data8.bin

data8.bin: gzip compressed data, was "data9.bin", last modified: Thu May 7 18:14:30 2020, max compression, from Unix

bandit12@bandit:/tmp/data$ mv data data.gz

mv: cannot stat 'data': No such file or directory

bandit12@bandit:/tmp/data$ mv data8.bin data.gz

bandit12@bandit:/tmp/data$ gzip -d data.gz

bandit12@bandit:/tmp/data$ ls

data data.tar data.txt

bandit12@bandit:/tmp/data$ file data

data: ASCII text

bandit12@bandit:/tmp/data$ cat data

The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

**Password for Level 13:**8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Now , exit ()

**Level 13:**

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

Password: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

**Commands:**

**bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost**

**bandit14@bandit:~$ cat /etc/bandit\_pass/bandit14**

**4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e**

**Password for Level 14:4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e**

Now exit ()

**Level 14:**

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

Password: 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

**Commands:**

bandit14@bandit:~$ nc localhost 30000

4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

Correct!

BfMYroe26WYalil77FoDi9qh59eK5xNr

**Password for Level 15:BfMYroe26WYalil77FoDi9qh59eK5xNr**

Now exit ()

**Level 15:**

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

Password: **BfMYroe26WYalil77FoDi9qh59eK5xNr**

**Commands:**

BfMYroe26WYalil77FoDi9qh59eK5xNr

bandit15@bandit:~$ ncat --ssl localhost 30001

BfMYroe26WYalil77FoDi9qh59eK5xNr

Correct!

cluFn7wTiGryunymYOu4RcffSxQluehd

**Password for Level 16:**cluFn7wTiGryunymYOu4RcffSxQluehd

Now exit ()

**Level 16:**

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

Password: **cluFn7wTiGryunymYOu4RcffSxQluehd**

**Commands:**

bandit16@bandit:~$ cat /etc/bandit\_pass/bandit16

cluFn7wTiGryunymYOu4RcffSxQluehd

bandit16@bandit:~$ nmap localhost -p 31000- 32000

Starting Nmap 7.40 ( https://nmap.org ) at 2021-11-01 07:02 CET

Nmap scan report for localhost (127.0.0.1)

Host is up (0.00027s latency).

Not shown: 34531 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

Nmap done: 2 IP addresses (1 host up) scanned in 3.76 seconds

bandit16@bandit:~$ ncat --ssl localhost 31790

cluFn7wTiGryunymYOu4RcffSxQluehd

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-----

Above output is the Credentials for level 17 :

To logged in to Level 17:

**Commands:**

bandit16@bandit:~$ cd /tmp

bandit16@bandit:/tmp$ nano **pvt.key**

Unable to create directory /home/bandit16/.nano: Permission denied

It is required for saving/loading search history or cursor positions.

bandit16@bandit:/tmp$ ssh bandit17@localhost -i **pvt.key**

**The login Credentials is saved in pvt.key**

**Level 17:**

**ssh bandit17@localhost -i pvt.key**

**Commands:**

bandit17@bandit:~$ diff passwords.old passwords.new

42c42

< w0Yfolrc5bwjS4qw5mq1nnQi6mF03bii

---

> kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd

bandit17@bandit:~$

**Password for Level 18:**kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd

Now exit ()

**Level 18:**

**ssh bandit18@bandit.labs.overthewire.org -p 2220**

**password:**kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd

**Commands:**

bandit18@bandit.labs.overthewire.org -p 2220 /bin/sh

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

bandit18@bandit.labs.overthewire.org's password:

$ ls

readme

$ cat readme

IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x

**Password for Level 19:**IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x

Now exit ()

**Level 19:**

**ssh bandit19@bandit.labs.overthewire.org -p 2220**

**password:**IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x

**Commands:**

bandit19@bandit:~$ ls

bandit20-do

bandit19@bandit:~$ ./bandit20-do cat /etc/bandit\_pass/bandit20

GbKksEFF4yrVs6il55v6gwY5aVje5f0j

bandit19@bandit:~$

**Password for Level 20:**GbKksEFF4yrVs6il55v6gwY5aVje5f0j

Now exit ()

**Level 20:**

**ssh bandit20@bandit.labs.overthewire.org -p 2220**

**password:**GbKksEFF4yrVs6il55v6gwY5aVje5f0j

**Commands:**

**Host a Port through first terminal window:**

bandit20@bandit:~$ nc -lvnp 25000

listening on [any] 25000 ...

connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 46890

GbKksEFF4yrVs6il55v6gwY5aVje5f0j

gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr

bandit20@bandit:~$

**Make a connection through second terminal window:**

bandit20@bandit:~$ ls

suconnect

bandit20@bandit:~$ ./suconnect 25000

Read: GbKksEFF4yrVs6il55v6gwY5aVje5f0j

Password matches, sending next password

**Password for Level 21:**gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr

Now exit ()