

# Systems Lab

**19004113**

# Tasnimul Hasnat

## Bandit0

**cat readme**

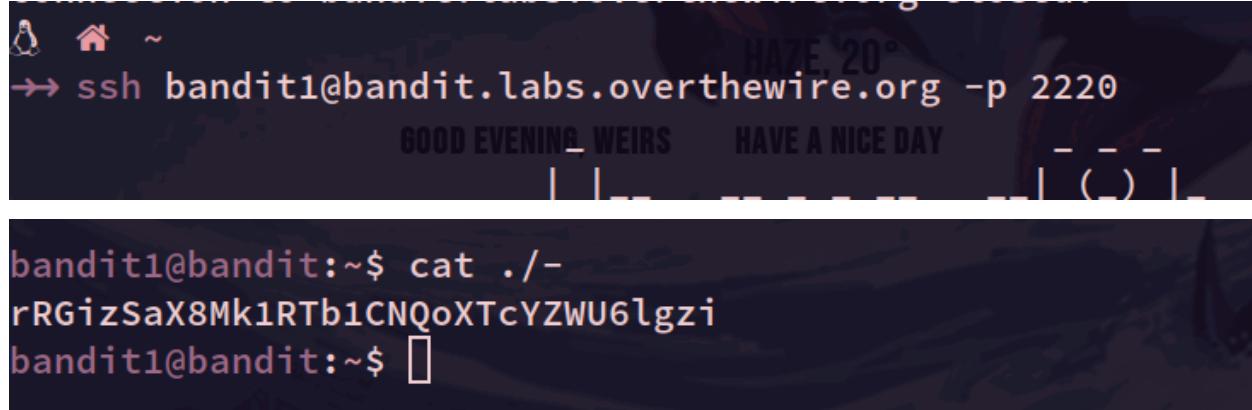
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

```
💡 🏠 ~  
→ ssh bandit0@bandit.labs.overthewire.org -p 2220
```

```
bandit0@bandit:~$ cat readme  
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL  
bandit0@bandit:~$ 
```

## Bandit1

```
cat .-/  
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
```

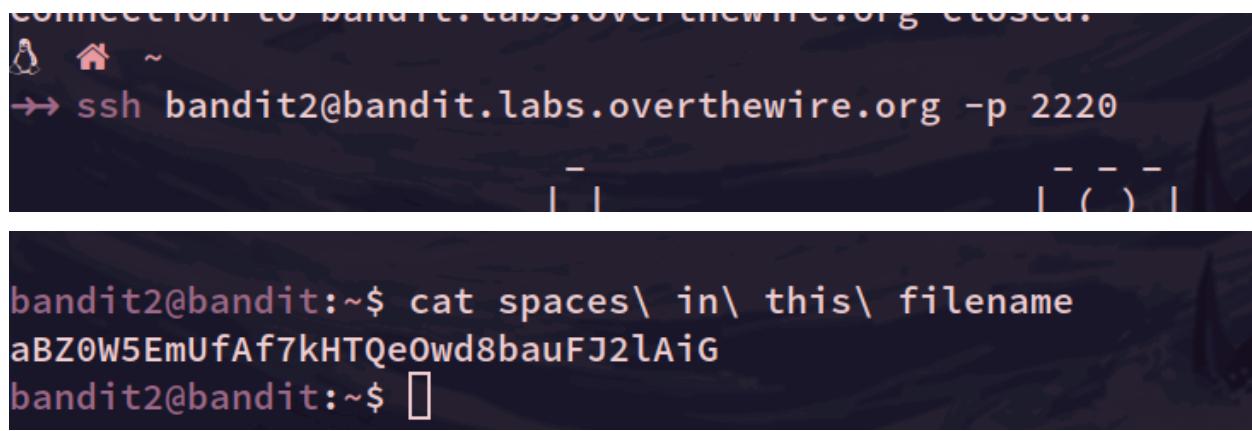


A terminal window showing a session on bandit1. The prompt is bandit1@bandit:~\$. The command cat .-/ is entered, followed by the output rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi. The terminal has a dark background with a space-themed wallpaper.

```
bandit1@bandit:~$ cat .-/  
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi  
bandit1@bandit:~$ 
```

## Bandit2

```
cat spaces\ in\ this\ filename  
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
```



A terminal window showing a session on bandit2. The prompt is bandit2@bandit:~\$. The command cat spaces\ in\ this\ filename is entered, followed by the output aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG. The terminal has a dark background with a space-themed wallpaper.

```
bandit2@bandit:~$ cat spaces\ in\ this\ filename  
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG  
bandit2@bandit:~$ 
```

## Bandit3

```
cat inhere/.hidden
```

```
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
```

```
Connection to bandit.labs.overthewire.org closed.
```

```
└─ home ~  
→ ssh bandit3@bandit.labs.overthewire.org -p 2220
```

```
bandit3@bandit:~$ cat inhere/.hidden  
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe  
bandit3@bandit:~$
```

## Bandit4

```
cat -- inhere/-file07
```

```
lrIWWI6bB37kxfiCQZqUdO1Yfr6eEeqR
```

```
logout  
Connection to bandit.labs.overthewire.org closed.  
└─ home ~  
→ ssh bandit4@bandit.labs.overthewire.org -p 2220
```

```
bandit4@bandit:~$ cat inhere/-file07  
lrIWWI6bB37kxfiCQZqUdO1Yfr6eEeqR  
bandit4@bandit:~$
```

## Bandit5

```
find . -readable -size 1033c ! -executable -exec cat {} \;
```

```
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

```
maybehere01/ maybehere03/ maybehere05/ maybehere07/ maybehere09/ maybehere11/ ma  
bandit5@bandit:~$ find . -readable -size 1033c ! -executable -exec cat {} \;  
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

## Bandit6

```
find / -user bandit7 -a -group bandit6 -a -size 33c -exec  
cat {} \; 2>/dev/null  
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
```

```
bandit6@bandit:~$ find / -user bandit7 -a -group bandit6 -a -size 33c -exec cat {} \; 2>/dev/null  
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S  
bandit6@bandit:~$
```

## Bandit7

```
grep millionth data.txt | cut -f 2  
TESKZC0XvTetK0S9xNwm25STk5iWrBvP
```

```
bandit7@bandit:~$ grep millionth data.txt | cut -f 2  
TESKZC0XvTetK0S9xNwm25STk5iWrBvP  
bandit7@bandit:~$
```

## Bandit8

```
sort data.txt | uniq -u  
EN632PlfYiZbn3PhVK3XOGSlNInNE00t
```

```
bandit8@bandit:~$ sort data.txt | uniq -u  
EN632PlfYiZbn3PhVK3XOGSlNInNE00t  
bandit8@bandit:~$
```

## Bandit9

```
strings data.txt | grep =*  
G7w8Lli6J3kTb8A7j9LgrywtEUlyyp6s
```

```
~$ strings data.txt | grep =*
```

```
%~|-[SCC  
n.E===== G7w8LIIi6J3kTb8A7j9LgrywtEUlyyp6s  
~H+ES-
```

## Bandit10

```
base64 -d data.txt | cut -d' ' -f 4  
6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
```

```
bandit10@bandit:~$ base64 -d data.txt | cut -d' ' -f 4  
6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM  
bandit10@bandit:~$ 
```

## Bandit11

```
tr a-zA-Z n-za-mN-ZA-M < data.txt |cut -d" " -f 4  
JVNBBSmZwKKOP0XbFXOoW8chDz5yVRv
```

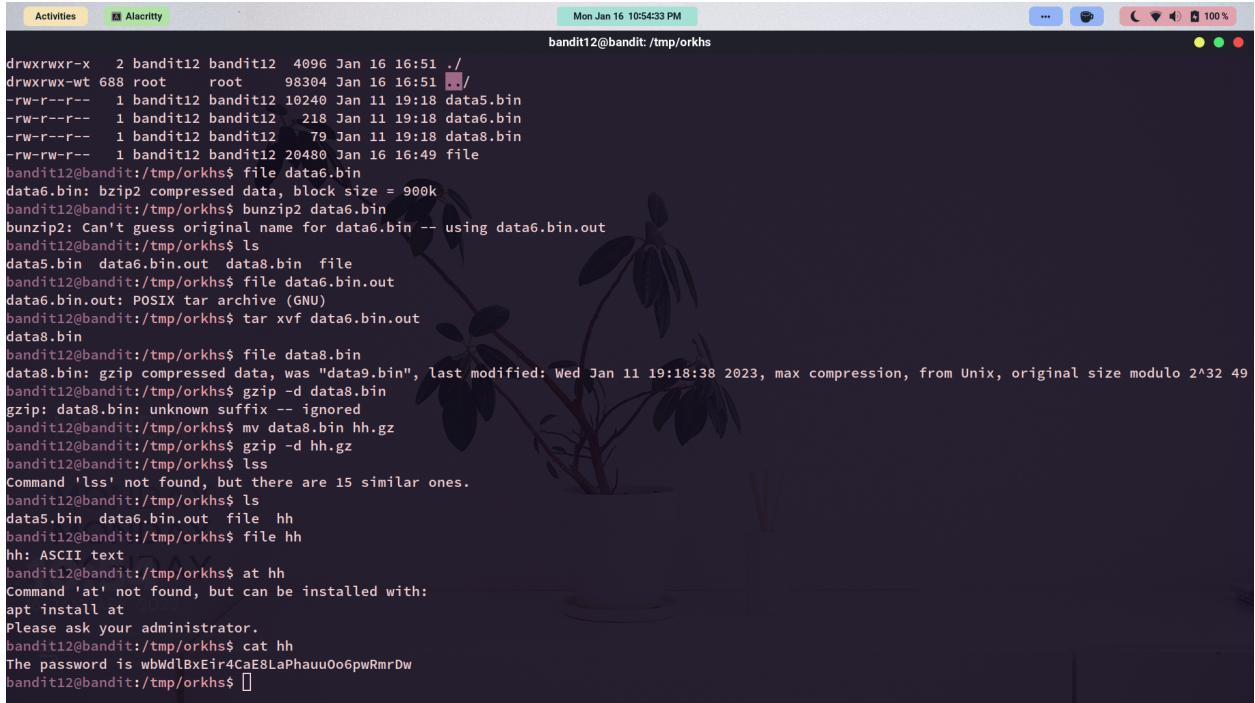
```
bandit11@bandit:~$ tr a-zA-Z n-za-mN-ZA-M < data.txt |cut -d" " -f 4  
JVNBBSmZwKKOP0XbFXOoW8chDz5yVRv  
bandit11@bandit:~$ 
```

## Bandit12

```
Lot of commands xxd -r,gzip -d , bunzip2, tar xvf etc  
wbWdlBxEir4CaE8LaPhuuOo6pwRmrDw
```

```
Activities Alacrity Mon Jan 16 10:51:19 PM bandit12@bandit: /tmp/orkhs Xfce VH# Tx@$#-]9@bandit12@bandit:~$ B@zE^-D$0 bandit12@bandit:~$ mkdir /tmp/orkhs bandit12@bandit:~$ xxd -r data.txt > /tmp/orkhs/file.gz bandit12@bandit:~$ cd /tmp/orkhs bandit12@bandit:/tmp/orkhs$ gzip -d file.gz bandit12@bandit:/tmp/orkhs$ file file file: bzip2 compressed data, block size = 900k bandit12@bandit:/tmp/orkhs$ mv file file.bz2 bandit12@bandit:/tmp/orkhs$ bunzip file.bz2 Command 'bunzip' not found, did you mean: command 'gunzip' from deb gzip (1.10-4ubuntu4.1) command 'bunzip2' from deb bzip2 (1.0.8-5build1) command 'ebunzip' from deb eb-utils (4.4.3-13) command 'unzip' from deb unzip (6.0-26ubuntu3.1) command 'lunzip' from deb lunzip (1.13-1) command 'funzip' from deb unzip (6.0-26ubuntu3.1) command 'runzip' from deb rzip (2.1-4.1) Try: apt install <deb name> bandit12@bandit:/tmp/orkhs$ bunzip2 file.bz2 bandit12@bandit:/tmp/orkhs$ ll total 108 drwxrwxr-x 2 bandit12 bandit12 4096 Jan 16 16:50 ./ drwxrwx-wt 686 root root 98304 Jan 16 16:50 ./ -rw-rw-r-- 1 bandit12 bandit12 434 Jan 16 16:49 file bandit12@bandit:/tmp/orkhs$ file file file: gzip compressed data, was "data4.bin", last modified: Wed Jan 11 19:18:38 2023, max compression, from Unix, original size modulo 2^32 20480 bandit12@bandit:/tmp/orkhs$ mv file file.gz bandit12@bandit:/tmp/orkhs$ gzip -d file.gz bandit12@bandit:/tmp/orkhs$ file file file: POSIX tar archive (GNU) bandit12@bandit:/tmp/orkhs$ ll total 124
```

```
Activities Alacrity Mon Jan 16 10:52:36 PM bandit12@bandit: /tmp/orkhs drwxrwx-wt 686 root root 98304 Jan 16 16:50 ./ -rw-rw-r-- 1 bandit12 bandit12 434 Jan 16 16:49 file bandit12@bandit:/tmp/orkhs$ file file file: gzip compressed data, was "data4.bin", last modified: Wed Jan 11 19:18:38 2023, max compression, from Unix, original size modulo 2^32 20480 bandit12@bandit:/tmp/orkhs$ mv file file.gz bandit12@bandit:/tmp/orkhs$ gzip -d file.gz bandit12@bandit:/tmp/orkhs$ file file file: POSIX tar archive (GNU) bandit12@bandit:/tmp/orkhs$ ll total 124 drwxrwxr-x 2 bandit12 bandit12 4096 Jan 16 16:50 ./ drwxrwx-wt 687 root root 98304 Jan 16 16:51 ./ -rw-rw-r-- 1 bandit12 bandit12 20480 Jan 16 16:49 file bandit12@bandit:/tmp/orkhs$ tar xvf file data5.bin bandit12@bandit:/tmp/orkhs$ tar xvf data5.bin data6.bin bandit12@bandit:/tmp/orkhs$ tar xvf data6.bin data8.bin bandit12@bandit:/tmp/orkhs$ tar xvf data8.bin bandit12@bandit:/tmp/orkhs$ file data data5.bin data6.bin data8.bin bandit12@bandit:/tmp/orkhs$ file data8.bin data8.bin: gzip compressed data, was "data9.bin", last modified: Wed Jan 11 19:18:38 2023, max compression, from Unix, original size modulo 2^32 49 bandit12@bandit:/tmp/orkhs$ ll total 144 drwxrwxr-x 2 bandit12 bandit12 4096 Jan 16 16:51 ./ drwxrwx-wt 688 root root 98304 Jan 16 16:51 ./ -rw-r--r-- 1 bandit12 bandit12 10240 Jan 11 19:18 data5.bin -rw-r--r-- 1 bandit12 bandit12 218 Jan 11 19:18 data6.bin -rw-r--r-- 1 bandit12 bandit12 79 Jan 11 19:18 data8.bin -rw-rw-r-- 1 bandit12 bandit12 20480 Jan 16 16:49 file bandit12@bandit:/tmp/orkhs$ file data6.bin data6.bin: bzip2 compressed data, block size = 900k bandit12@bandit:/tmp/orkhs$ ]
```



```
Activities Alacritty Mon Jan 16 10:54:33 PM bandit12@bandit: /tmp/orkhs  
drwxrwxr-x 2 bandit12 bandit12 4096 Jan 16 16:51 ./  
drwxrwx-wt 688 root root 98304 Jan 16 16:51 ..  
-rw-r--r-- 1 bandit12 bandit12 10240 Jan 11 19:18 data5.bin  
-rw-r--r-- 1 bandit12 bandit12 218 Jan 11 19:18 data6.bin  
-rw-r--r-- 1 bandit12 bandit12 79 Jan 11 19:18 data8.bin  
-rw-rw-r-- 1 bandit12 bandit12 20480 Jan 16 16:49 file  
bandit12@bandit:/tmp/orkhs$ file data6.bin  
data6.bin: bzip2 compressed data, block size = 900k  
bandit12@bandit:/tmp/orkhs$ bunzip2 data6.bin  
bunzip2: Can't guess original name for data6.bin -- using data6.bin.out  
bandit12@bandit:/tmp/orkhs$ ls  
data5.bin data6.bin.out data8.bin file  
bandit12@bandit:/tmp/orkhs$ file data6.bin.out  
data6.bin.out: POSIX tar archive (GNU)  
bandit12@bandit:/tmp/orkhs$ tar xvf data6.bin.out  
data8.bin  
bandit12@bandit:/tmp/orkhs$ file data8.bin  
data8.bin: gzip compressed data, was "data9.bin", last modified: Wed Jan 11 19:18:38 2023, max compression, from Unix, original size modulo 2^32 49  
bandit12@bandit:/tmp/orkhs$ gzip -d data8.bin  
gzip: data8.bin: unknown suffix -- ignored  
bandit12@bandit:/tmp/orkhs$ mv data8.bin hh.gz  
bandit12@bandit:/tmp/orkhs$ gzip -d hh.gz  
bandit12@bandit:/tmp/orkhs$ ls  
Command 'lss' not found, but there are 15 similar ones.  
bandit12@bandit:/tmp/orkhs$ ls  
data5.bin data6.bin.out file hh  
bandit12@bandit:/tmp/orkhs$ file hh  
hh: ASCII text  
bandit12@bandit:/tmp/orkhs$ at hh  
Command 'at' not found, but can be installed with:  
apt install at  
Please ask your administrator.  
bandit12@bandit:/tmp/orkhs$ cat hh  
The password is wbWdlBxEir4CaE8LaPhauu0o6pwRmrDw  
bandit12@bandit:/tmp/orkhs$
```

## Bandit13

**ssh -i sshkey.private**

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

**fGrHPx402xGC7U7rXKDaxiWFT0iF0ENq**

```
bandit13@bandit:~$ ssh -i sshkey.private bandit14@bandit.labs.overthewire.org -p 2220  
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([127.0.0.1]:2220)' can't be established.  
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfxC5CXlhmAAM/urerLY.
```

## Bandit14

**nc localhost 30000**

**jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt**

```
asad  
bandit14@bandit:~$ nc localhost 30000  
fGrHPx402xGC7U7rXKDaxiWFT0iF0ENq  
Correct!  
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
```

## Bandit15

```
openssl s_client -connect localhost:30001  
JQttfApK4SeyHwDII9SXGR50qcIOAil1
```

```
Enjoy your stay.  
MONDAY  
bandit15@bandit:~$ openssl s_client -connect localhost:30001  
CONNECTED(00000003)  
Can't use SSL_get_servername  
depth=0 CN = localhost  
read R BLOCK  
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt  
Correct!  
JQttfApK4SeyHwDII9SXGR50qcloAil1
```

## Bandit16

```
nmap -p 31000-32000 localhost; openssl s_client  
-connect localhost:31790  
VwOSWtCA7IRKkTfbr2IDh6awj9RNZM5e
```

```
Enjoy your stay.  
MONDAY  
bandit16@bandit:~$ nmap -p 31000-32000 localhost; openssl s_client -connect localhost:31790  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-16 16:59 UTC
```

```
Activities Alacrity Mon Jan 16 11:00:39 PM bandit16@bandit: ~
Max Early Data: 0
---
read R BLOCK
JQttfApK4SeyHwDlI9SXGR50qc1oAil1
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmoOkufMg6HL2YPI0jon6iwfbp7c3jx34YkyWqUH57SudyJ
imZzeygCogtZPGujUsxJSWt/oTqexh+cAMTSmLoJ7tBrJ0bArnx9dY7T2bRPQ
Ja6Lzb58yW3Fz1870Ri0+rW4LCDCNd2luVLE/GL2GWyuKN0k5icd5tb2JzeqkTu
DSt2mcNn4rhAL-JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePOAzL9UVbW
JGT165cxhCncz/w4+mqQyvmzpWtMAzTzAzQxNbkr2MBGy5xDrJg0LNW6sK7wNX
x0YYztt/zbIKPjfkU1jHs+9EbVnj+01XFOJuQIDAQABaoIBAggxpMla0LwFvD
KHcj10ncoBc4oE11aFVwiK7xfw+24pRNuDE6SFth0ar69jp5RLwD1NhPx3iBl
J9nOM80JOVToum43U0S8YxF8WwhXriYngc1sskbwpXOUdc9uX4+UESzh22P29ovd
d8WEry+0gPxun8pbJLmxkAtwNhpMt0e050vk9TL5wqb9uAlbssgTcXkMqPw9nC
YNN6DP21bcBrvgT9YCNLc+CZKuf052yo09qokwFTEqjtF4UntJom+asvlpm8A
vLY9r60wYSwmZhNqBUrj7lyCtXMIu1kkd4w7F77k+djHoAXyxcUp1DGL51s0mama
+T0WwgCgyEA8JtPxP0GRj+IQKx262jN3dEIka8ky5moIwUgYdsx0NxhgRRh0RT
8c8hAurBb2G82so8Uhk/fur850Ef9TncnCY2crpqsgshifKLxrLgtT+qDpfZnx
Satldt8Gf85yA7hnWwJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEaypHd
HCctNi/FwjulhttFc/rHYKhLidzDFYe1E/+45bN4yFm8x7R/0e1E7kasZ+Exdvt
SghaTdcG0KnywlbpVYusavZpazMjdz6tcFhVAbAjm7enCIVgCSx-X3L55iWg0A
R57hJggleZiivjv3aq0hwlvLztzsK6zVeoXFau0EcgyAbljo4674hyPstJi93V5Hdi
TtieK7xRYxUl+iu7rWkGAXFpMLFteQEsRr7Pj/lemmEV5eTDAFMly9FL2m9oQWcg
R8VdwSk8r9FGLs+9aKcV5Pi/WEKlwgXinB3OhYimiG2c5JcqIZFhxDMejG0iu
L8ktHMPvodBwNsSBULpg00KbgBap1Tfc1HonwimGU03KpwWt0o06CdtkmJ0mLBni
b1h9elyZ9FsGxsgrBXRsXuz7wtsqAglXbdLq/ZQ7Yfz0KU4ZxEnabvXnvkU
YodjHds0oKvdQNw6ucyLRAWfuSeXw9a/9p7ftpxm0Tsgyvmlf2MIAEwyzRqaM
77pBaogAMmjI3dj+eZ8duy31eo36yrttFSNsJLabxFpd1c1gvtgCW+9Cq0b
dxviv8-TFVEBl104f7HVM6EpTscdUxU-bCXWkfjuRb7Dy960tt93Psx8MBTakz3
vBgsyi/s3RqRbGU40foOzyfAMT8s1m/uYv52061geuZ/ujbjY=
-----END RSA PRIVATE KEY-----
closed
bandit16@bandit:~$ []
```

## Bandit17

**diff passwords.new passwords.old**  
**hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg**

```
bandit17@bandit:~$ diff passwords.new passwords.old
42c42
< hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
---
> 810zq8IK64u5A9Lb2ibdTGBtlcSZsoe8
bandit17@bandit:~$ []
```

# Bandit18

**scp -P 2220**

```
bandit18@bandit.labs.overthewire.org:/home/bandit18/readme 000j && cat 000j && rm 000j  
awhqfNnAbc1naukrpqDYcF95h7HoMTrC
```

```
byebye :  
Connection to bandit.labs.overthewire.org closed.  
Δ ~  
→ scp -P 2220 bandit18@bandit.labs.overthewire.org:/home/bandit18/readme 000j && cat 000j && rm 000j  
[ 100% ]  
23:04 PM  
CPU: 4% | Mem: 54% | Disk: 14%  
  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
bandit18@bandit.labs.overthewire.org's password:  
readme  
awhqfNnAbc1naukrpqDYcF95h7HoMTrC  
Δ ~
```

# Bandit19

```
./bandit20-do cat /etc/bandit_pass/bandit20  
VxCazJaVykl6W36BkBU0mJTCM8rR95XT
```

```
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20  
VxCazJaVykI6W36BkBU0mJTCM8rR95XT  
bandit19@bandit:~$
```

# And Some Extras

## Bandit20

```
nc -l localhost 3300
./suconnect 3300
NvEJF7oVjkddItPSrdKEFOllh9V1IBcq
```

## Bandit21

```
cat /tmp/t7O6lds9S0RqQh9aMcZ6ShpAoZKF7fgv
WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff
```

## Bandit22

```
echo I am user bandit23 | md5sum | cut -d ' ' -f 1 | xargs
-I {} cat /tmp/{}
QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G
```

## Bandit23

```
mkdir /tmp/danke && cp /etc/bandit_pass/bandit24
/tmp/danke/pass
VAfGXJ1PBSsPSnvsjl8p759leLZ9GGar
```

## Bandit24

```
for i in {0000..9999};do res=$(echo
"VAfGXJ1PBSsPSnvsjl8p759leLZ9GGar $i" | nc localhost
30002) ; echo "$i $res";sleep 1; done
p7TaowMYrmu23Ol8hiZh9UvD0O9hpx8d
```