

# TASK - 7 : BANDIT

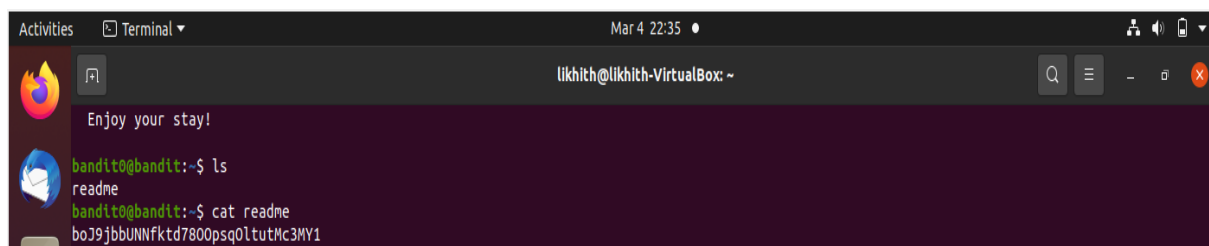
## LEVEL 0

PASSWORD : bandit0

```
jahnavidingari@jahnavidingari:~$ ssh bandit0@bandit.labs.overthewire.org -p 222
```

## LEVEL 0 to 1

PASSWORD : boJ9jbbUNNfktd7800psq0ltutMc3MY1

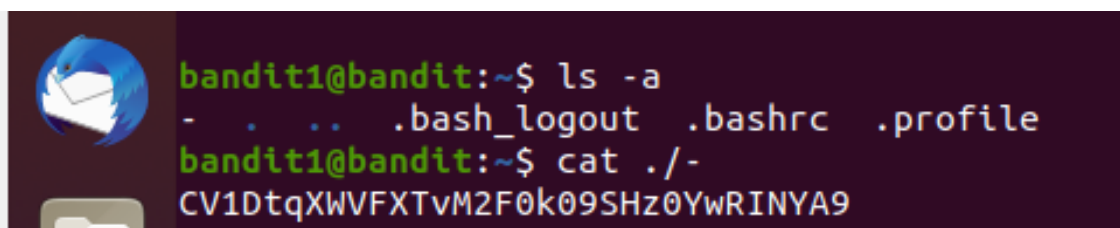


The screenshot shows a terminal window titled "likhith@likhith-VirtualBox: ~". It displays the following commands and output:

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd7800psq0ltutMc3MY1
```

## LEVEL 1 to 2 :

PASSWORD:CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9



The screenshot shows a terminal window with the following commands and output:

```
bandit1@bandit:~$ ls -a
- . . . .bash_logout .bashrc .profile
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
```

## LEVEL 2 to 3 :

PASSWORD : UmHadQclWmgdLOKQ3YNgjwxGoRMb5luK

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjwxGoRMb5luK
```

## LEVEL 3 to 4 :

PASSWORD : pIwrPrtPN36QITSp3EQaw936yaFoFgAB

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -la
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
```

## LEVEL 4 to 5 :

PASSWORD: koReBOKuIDDepwhWk7jZCORTdopnAYKh

```
bandit4@bandit:~$ ls -la
.  ..  .bash_logout  .bashrc  inhere  .profile
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -la
.  ..  -file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ file ./-*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZCORTdopnAYKh
```

## LEVEL 5 to 6 :

PASSWORD :DXjZPULLxYr17uwoI01bNLQbtFemEgo7

```
bandit5@bandit:~/inhere$ ls -la
.   maybeh ere00 maybeh ere02 maybeh ere04 maybeh ere06 maybeh ere08 maybeh ere10 maybeh ere12 maybeh ere14 maybeh ere16 maybeh ere18
..  maybeh ere01 maybeh ere03 maybeh ere05 maybeh ere07 maybeh ere09 maybeh ere11 maybeh ere13 maybeh ere15 maybeh ere17 maybeh ere19
bandit5@bandit:~/inhere$ find -type f -size 1033c
./maybeh ere07/.file2
bandit5@bandit:~/inhere$ cat ./maybeh ere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

## LEVEL 6 to 7 :

PASSWORD:HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

```
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
find: /usr/lib/dpkg/info: not found
```

```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
```

## LEVEL 7 to 8 :

PASSWORD:cvX2JJJa4CFALtqS87jk27qwqGhBM9pIV

```
bandit7@bandit:~$ ls -la
.   ..  .bash_logout .bashrc data.txt .profile
bandit7@bandit:~$ awk '/^millionth/ {print $2;}' data.txt
cvX2JJJa4CFALtqS87jk27qwqGhBM9pIV
```

## LEVEL 8 to 9 :

PASSWORD : UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUHR

```
bandit8@bandit:~$ ls -la
.   ..  .bash_logout .bashrc data.txt .profile
bandit8@bandit:~$ cat data.txt | sort | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUHR
```

## LEVEL 9 to 10 :

PASSWORD : TruKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

```
bandit9@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit9@bandit:~$ strings data.txt | grep "="
===== the*2i"4
=:G e
===== password
<I=zSGi
Z)====== is
A=|t&E
Zdb=
C^ LAh=3G
*SF=s
&===== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.H&^
```

## LEVEL 10 to 11 :

PASSWORD:IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

```
bandit10@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBScg==
```

```
bandit10@bandit:~$ echo VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBScg== | base64 --decode
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
```

## Level 11 to 12 :

PASSWORD:5Te8Y4drgCRfCx8ugdwwEX8KFC6k2EUu

```
bandit11@bandit:~$ ls -a
. .. .bash_logout .bashrc data.txt .profile
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHH
bandit11@bandit:~$ echo Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHH
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHH
bandit11@bandit:~$ echo Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHH | tr [a-zA-Z] [n-za-mN-ZA-M]
The password is 5Te8Y4drgrCRfCx8ugdwuEX8Kfc6k2EUu
```

## LEVEL 12 to 13 :

PASSWORD : 8ZjyCRiBWFYkneahHwxCv3wb2a10RpYL

```
bandit12@bandit:~$ ls -a
. .. .bash_logout .bashrc data.txt .profile
bandit12@bandit:~$ mkdir /tmp/cognizance003
bandit12@bandit:~$ cp data.txt /tmp/cognizance003
bandit12@bandit:~$ cd /tmp/cognizance003
bandit12@bandit:/tmp/cognizance003$ ls
data.txt
bandit12@bandit:/tmp/cognizance003$ file data.txt
data.txt: ASCII text
bandit12@bandit:/tmp/cognizance003$ cat data.txt
00000000: 1f8b 0808 0650 b45e 0203 6461 7461 322e .....P.^..data2.
00000010: 6269 6e00 013d 02c2 fd42 5a68 3931 4159 bin...=...BZh91AY
00000020: 2653 598e 4f1c c800 001e 7fff fbfb 7fda 85Y.O.....
00000030: 9e7f 4f76 9fcf fe7d 3fff f67d abde 5e9f ..Ov...}?.^..
00000040: f3fe 9fbf f6f1 feee bfdf a3ff b001 3b1b .....;..
00000050: 5481 a1a0 1ea0 1a34 d0d0 001a 68d3 4683 T.....4...h.F.
00000060: 4680 0680 0034 1918 4c4d 190c 4000 0001 F....4...LM..@...
00000070: a000 c87a 81a3 464d a8d3 43c5 1068 0346 ...z...FM...C..h.F
00000080: 8343 40d0 3400 0340 66a6 8068 0cd4 f500 .C@.4...@f...h....
00000090: 69ea 6800 0f50 68f2 4d00 680d 06ca 0190 i..h..Ph.M.h.....
000000a0: 0000 69a1 a1a0 1ea0 194d 340d 1ea1 b280 ..l.....M4.....
000000b0: 7500 3406 2340 034d 3400 0000 3403 d400 ...4.#@.M4...4...
000000c0: 1a07 a832 3400 f51a 0003 43d4 0068 0d34 ...24....C..h.4
000000d0: 6868 f51a 3d43 2580 3e58 061a 2c89 6bf3 hh...=C%.>X...k.
000000e0: 0163 08ab dc31 91cd 1747 599b e401 0b06 .C...1...GY.....
000000f0: a8b1 7255 a3b2 9cf9 75cc f106 941b 347a ..rU....U.....4Z
00000100: d616 55cc 2ef2 9d46 e7d1 3050 b5fb 76eb ..U....F..0P..v.
00000110: 01f8 60c1 2201 33f0 0de0 4aa6 ec8c 914f ..'".3...J...0
00000120: cf8a aed5 7b52 4270 8d51 6978 c159 8b5a ....{RBp.Qlx.Y.Z
00000130: 2164 fb1f c26a 8d28 b414 e690 bfdd b3e1 ld...j.(.....
00000140: f414 2f9e d041 c523 b641 ac08 0c0b 06f5 ../.A.#A.....
00000150: dd64 b862 1158 3f9e 897a 8cae 32b0 1fb7 .d.b.X?..z..2...
00000160: 3c82 af41 20fd 6e7d 0a35 2833 41bd de0c <..A .n).5(3A...
00000170: 774f ae52 a1ac 0fb2 8c36 ef58 537b f30a wO.R.....6.XS{..
00000180: 1510 cab5 cb51 4231 95a4 d045 b95c ea09 ....QB1...E.\..
00000190: 9fa0 4d33 ba43 22c9 b5be d0ea eeb7 ec85 ..M3.C".....
000001a0: 59fc 8bf1 97a0 87a5 0df0 7acd d555 fc11 Y.....Z...U..
000001b0: 223f fdc6 2be3 e809 c974 271a 920e acbc "?..+....t'.....
000001c0: 0de1 f1a6 393f 4cf5 50eb 7942 86c3 3d7a ...9?L.P.yB...=z
000001d0: fe6d 173f a84c bb4e 742a fc37 7b71 508a .m.?..L.Nt*.7{qP.
000001e0: a2cc 9cf1 2522 8a77 39f2 716d 34f9 8620 ...%".w9.qm4...
000001f0: 4e33 ca36 eec0 cd4b b3e8 48e4 8b91 5bea N3.6...K..H...[.
00000200: 01bf 7d21 0b64 82c0 3341 342a e98b 4d7e ..}!d..3A$..M~
00000210: c95c 1b1f cac9 a04a 1988 43b2 6b55 c6a6 .\.....J...C.KU..
00000220: 075c 1eb4 8ecf 5cdf 4653 064e 84da 263d .\....\FS.N..&=
00000230: b15b bcea 7109 5c29 c524 3afc d715 4894 .[.q.\).$....H.
00000240: 7426 072f fc28 ab05 9603 b3fc 5dc9 14e1 t&./.(.....]...
00000250: 4242 393c 7320 98f7 681d 3d02 0000 BB9<s ..h.=...
bandit12@bandit:/tmp/cognizance003$ xxd -r data.txt data
bandit12@bandit:/tmp/cognizance003$ 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/cognizance003$ xxd -r data.txt data
bandit12@bandit:/tmp/cognizance003$ 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/cognizance003$ mv data data.gz
bandit12@bandit:/tmp/cognizance003$ gzip -d data.gz
bandit12@bandit:/tmp/cognizance003$ ls
data  data.txt
bandit12@bandit:/tmp/cognizance003$ file data
data: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/cognizance003$ mv data data.bz2
bandit12@bandit:/tmp/cognizance003$ ls
data.bz2  data.txt
bandit12@bandit:/tmp/cognizance003$ man bzip2
bandit12@bandit:/tmp/cognizance003$ bzip -d data.bz2
-bash: bzip: command not found
bandit12@bandit:/tmp/cognizance003$ gzip -d data.bz2
gzip: data.bz2: unknown suffix -- ignored
bandit12@bandit:/tmp/cognizance003$ ls
data.bz2  data.txt
bandit12@bandit:/tmp/cognizance003$ bzip2 -d data.bz2
bandit12@bandit:/tmp/cognizance003$ ls
data  data.txt
bandit12@bandit:/tmp/cognizance003$ mv data data.gz
bandit12@bandit:/tmp/cognizance003$ gzip -d data.gz
bandit12@bandit:/tmp/cognizance003$ ls
data  data.txt
bandit12@bandit:/tmp/cognizance003$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/cognizance003$ man tar
bandit12@bandit:/tmp/cognizance003$ mv data  data.tar
bandit12@bandit:/tmp/cognizance003$ tar -x -f data.tar
bandit12@bandit:/tmp/cognizance003$ ls
data5.bin  data.tar  data.txt
bandit12@bandit:/tmp/cognizance003$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/cognizance003$ ls
data5.bin  data.tar  data.txt
bandit12@bandit:/tmp/cognizance003$ mv data5.bin data5.tar
bandit12@bandit:/tmp/cognizance003$ tar -x -f data6.tar
tar: data6.tar: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
bandit12@bandit:/tmp/cognizance003$ tar -x -f data5.tar
bandit12@bandit:/tmp/cognizance003$ ls
data5.tar  data6.bin  data.tar  data.txt
bandit12@bandit:/tmp/cognizance003$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/cognizance003$ mv data6.bin data6.tar
bandit12@bandit:/tmp/cognizance003$ tar -x -f data6.tar
bandit12@bandit:/tmp/cognizance003$ ls
data5.tar  data6.tar  data8.bin  data.tar  data.txt
```

```

bandit12@bandit:/tmp/cognizance003$ mv data data.bz2
bandit12@bandit:/tmp/cognizance003$ ls
data.bz2  data.txt
bandit12@bandit:/tmp/cognizance003$ man bzip2
bandit12@bandit:/tmp/cognizance003$ bzip -d data.bz2
-bash: bzip: command not found
bandit12@bandit:/tmp/cognizance003$ gzip -d data.bz2
gzip: data.bz2: unknown suffix -- ignored
bandit12@bandit:/tmp/cognizance003$ ls
data.bz2  data.txt
bandit12@bandit:/tmp/cognizance003$ bzip2 -d data.bz2
bandit12@bandit:/tmp/cognizance003$ ls
data  data.txt
bandit12@bandit:/tmp/cognizance003$ mv data data.gz
bandit12@bandit:/tmp/cognizance003$ gzip -d data.gz
bandit12@bandit:/tmp/cognizance003$ ls
data  data.txt
bandit12@bandit:/tmp/cognizance003$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/cognizance003$ man tar
bandit12@bandit:/tmp/cognizance003$ mv data  data.tar
bandit12@bandit:/tmp/cognizance003$ tar -x -f data.tar
bandit12@bandit:/tmp/cognizance003$ ls
data5.bin  data.tar  data.txt
bandit12@bandit:/tmp/cognizance003$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/cognizance003$ ls
data5.bin  data.tar  data.txt
bandit12@bandit:/tmp/cognizance003$ mv data5.bin data5.tar
bandit12@bandit:/tmp/cognizance003$ tar -x -f data6.tar
tar: data6.tar: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
bandit12@bandit:/tmp/cognizance003$ tar -x -f data5.tar
bandit12@bandit:/tmp/cognizance003$ ls
data5.tar  data6.bin  data.tar  data.txt
bandit12@bandit:/tmp/cognizance003$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/cognizance003$ mv data6.bin data6.tar
bandit12@bandit:/tmp/cognizance003$ tar -x -f data6.tar
bandit12@bandit:/tmp/cognizance003$ ls
data5.tar  data6.tar  data8.bin  data.tar  data.txt
bandit12@bandit:/tmp/cognizance003$ file data8.bin
data8.bin: cannot open 'data8.bin' (No such file or directory)
bandit12@bandit:/tmp/cognizance003$ 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/cognizance003$ mv data8.bin data8.gz
bandit12@bandit:/tmp/cognizance003$ file data8
data8: cannot open 'data8' (No such file or directory)
bandit12@bandit:/tmp/cognizance003$ gzip -d data8.gz
bandit12@bandit:/tmp/cognizance003$ file data8
data8: ASCII text
bandit12@bandit:/tmp/cognizance003$ cat data8
The password is 874vCRjBWEYkneahHwxCy3wh2a10RnYl

```

## LEVEL 13 to 14 :

PASSWORD : 4wcYUJFw0k0XLShlDzztnTBHlqxU3b3e

```

bandit13@bandit:~$ ls -la
.  .. .bash_logout .bashrc .profile sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit 14@localhost
ssh: Could not resolve hostname bandit: No address associated with hostname
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
Could not create directory '/home/bandit13/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWf85496EtCRkKLo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

```

```

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHlqxU3b3e

```

## LEVEL 14 to 15 :

PASSWORD : BfMYroe26WYalil77FoDi9qh59eK5xNr

```
bandit14@bandit:~$ telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^J'.
4wcYUJFw0k0XLShLDzztnTBHtqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
```

## LEVEL 15 to 16 :

PASSWORD : cluFn7wTiGryunymYOu4RcffSxqluehd

```
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
BfMYroe26WYalil77FoDi9qh59eK5xNr
bandit15@bandit:~$ man nc | grep ssl
bandit15@bandit:~$ man nc
bandit15@bandit:~$ man ncat
bandit15@bandit:~$ 
bandit15@bandit:~$ man ncat | grep ssl
--ssl                Connect or listen with SSL
--ssl-cert            Specify SSL certificate file (PEM) for listening
--ssl-key             Specify SSL private key (PEM) for listening
--ssl-verify          Verify trust and domain name of certificates
--ssl-trustfile        PEM file containing trusted SSL certificates
--ssl-ciphers          Cipherlist containing SSL ciphers to use

--ssl (Use SSL)
--ssl-verify (Verify server certificates)
    In client mode, --ssl-verify is like --ssl except that it also requires verification of the server certificate. Ncat comes with a
    certificates; these will also be used if available. Use --ssl-trustfile to give a custom list. Use -v one or more times to get
--ssl-cert certfile.pem (Specify SSL certificate)
    (in connect mode). Use it in combination with --ssl-key.
--ssl-key keyfile.pem (Specify SSL private key)
    This option gives the location of the PEM-encoded private key file that goes with the certificate named with --ssl-cert.
--ssl-trustfile cert.pem (List trusted certificates)
    with --ssl-verify. The argument to this option is the name of a PEM file containing trusted certificates. Typically, the file will
--ssl-ciphers cipherlist (Specify SSL ciphersuites)
    http://www.openssl.org
bandit15@bandit:~$ ncat --ssl localhost 30001
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxqluehd
```