Bandit OverTheWire

- Level 0

```
bandit0@bandit:~$ ssh bandit1@bandit.labs.overthewire.org -p 2220
```

- Level 0→1

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

- Level 1→2

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat < -
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
```

- Level 2→3

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat "file name with spaces"
cat: 'file name with spaces': No such file or directory
bandit2@bandit:~$ cat "spaces in this filename"
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
```

- Level 3→4

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

- Level 4→5

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd /inhere
-bash: cd: /inhere: No such file or directory
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls
-file00  -file02  -file04  -file06  -file08
-file01  -file03  -file05  -file07  -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
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
```

- Level 5→6

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

- Level 6→7

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c
find: '/root': Permission denied
find: '/snap/core18/2632/etc/ssl/private': Permission denied
find: '/snap/core18/2632/root': Permission denied
find: '/snap/core18/2632/var/cache/ldconfig': Permission denied
find: '/snap/core18/2632/var/lib/private': Permission denied
find: '/snap/core20/1695/etc/ssl/private': Permission denied
find: '/snap/core20/1695/root': Permission denied
find: '/snap/core20/1695/var/cache/ldconfig': Permission denied
find: '/snap/core20/1695/var/cache/private': Permission denied
find: '/snap/core20/1695/var/lib/private': Permission denied
find: '/snap/core20/1695/var/lib/snapd/void': Permission denied
find: '/var/snap/lxd/common/lxd': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/lib/udisks2': Permission denied
find: '/var/lib/update-notifier/package-data-downloads/partial': Permission deni
ed
/var/lib/dpkg/info/bandit7.password
find: '/var/lib/polkit-1': Permission denied
find: '/var/lib/chrony': Permission denied
find: '/var/lib/snapd/void': Permission denied
find: '/var/lib/snapd/cookie': Permission denied
```

- Level 6→7

```
find: '/var/lib/amazon': Permission denied
find: '/var/lib/private': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/tmp/systemd-private-53bd120f119f45f09f3f9c0b8d399c1d-ModemManager.se
rvice-OY5W4n': Permission denied
find: '/var/tmp/systemd-private-53bd120f119f45f09f3f9c0b8d399c1d-chrony.service-
xzlxcE': Permission denied
find: '/var/tmp/systemd-private-53bd120f119f45f09f3f9c0b8d399c1d-systemd-resolve
d.service-hrfsqE': Permission denied
find: '/var/tmp/systemd-private-53bd120f119f45f09f3f9c0b8d399c1d-systemd-logind.
service-QR0deA': Permission denied
find: '/var/log/chrony': Permission denied
find: '/var/log/unattended-upgrades': Permission denied
find: '/var/log/amazon': Permission denied
find: '/var/log/private': Permission denied
find: '/var/cache/apparmor/c47eabf7.0': Permission denied
find: '/var/cache/apparmor/e10c1cf9.0': Permission denied
find: '/var/cache/pollinate': Permission denied
find: '/var/cache/private': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/lost+found': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/bandit29-git': Permission denied
```

```
find: '/home/bandit29-git': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/home/bandit31-git': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/ubuntu': Permission denied
find: '/run/chrony': Permission denied
find: '/run/udisks2': Permission denied
find: '/run/user/11014': Permission denied
find: '/run/user/11026': Permission denied
find: '/run/user/11028': Permission denied
find: '/run/user/11015': Permission denied
find: '/run/user/8002': Permission denied
find: '/run/user/11030': Permission denied
find: '/run/user/11025': Permission denied
find: '/run/user/11032': Permission denied
find: '/run/user/11022': Permission denied
find: '/run/user/11023': Permission denied
find: '/run/user/11021': Permission denied
find: '/run/user/11009': Permission denied
find: '/run/user/11011': Permission denied
find: '/run/user/11008': Permission denied
find: '/run/user/11007': Permission denied
find: '/run/user/11010': Permission denied
```

```
find: '/run/user/11008': Permission denied
find: '/run/user/11007': Permission denied
find: '/run/user/11010': Permission denied
find: '/run/user/11012': Permission denied
find: '/run/user/11019': Permission denied
find: '/run/user/11017': Permission denied
find: '/run/user/11016': Permission denied
find: '/run/user/11024': Permission denied
find: '/run/user/11027': Permission denied
find: '/run/user/11013': Permission denied
find: '/run/user/11020': Permission denied
find: '/run/user/11006/systemd/inaccessible/dir': Permission denied
find: '/run/user/11003': Permission denied
find: '/run/user/11002': Permission denied
find: '/run/user/11005': Permission denied
find: '/run/user/11004': Permission denied
find: '/run/user/11000': Permission denied
find: '/run/user/11001': Permission denied
find: '/run/sudo': Permission denied
find: '/run/screen/S-bandit19': Permission denied
find: '/run/screen/S-bandit16': Permission denied
find: '/run/screen/S-bandit0': Permission denied
find: '/run/screen/S-bandit1': Permission denied
find: '/run/screen/S-bandit21': Permission denied
```

```
find: '/run/screen/S-bandit21': Permission denied
find: '/run/screen/S-bandit25': Permission denied
find: '/run/screen/S-bandit7': Permission denied
find: '/run/screen/S-bandit18': Permission denied
find: '/run/screen/S-bandit24': Permission denied
find: '/run/screen/S-bandit23': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/multipath': Permission denied
find: '/run/cryptsetup': Permission denied
find: '/run/lvm': Permission denied
find: '/run/credentials/systemd-sysusers.service': Permission denied
find: '/run/systemd/propagate': Permission denied
find: '/run/systemd/unit-root': Permission denied
find: '/run/systemd/inaccessible/dir': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/etc/sudoers.d': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/multipath': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/tmp': Permission denied
find: '/sys/kernel/tracing': Permission denied
find: '/sys/kernel/debug': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/sys/fs/bpf': Permission denied
```

```
find: '/sys/kernel/debug': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/sys/fs/bpf': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/2649727/task/2649727/fd/6': No such file or directory
find: '/proc/2649727/task/2649727/fdinfo/6': No such file or directory
find: '/proc/2649727/fd/5': No such file or directory
find: '/proc/2649727/fdinfo/5': No such file or directory
find: '/boot/efi': Permission denied
find: '/dev/shm/eic-hostkey-fgnlvTg6': Permission denied
bandit6@bandit:~$ /var/lib/dpkg/info/bandit7.password
-bash: /var/lib/dpkg/info/bandit7.password: Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
```

- Level 7→8

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ grep "millionth" data.txt
millionth        TESKZC0XvTetK0S9xNwm25STk5iWrBvP
```

- Level 8→9

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

- Level 9→10

```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ grep "=" data.txt
grep: data.txt: binary file matches
bandit9@bandit:~$ strings data.txt | grep "="
TM9=\
=========== the
=Dbb
P,f=l
2v&z+=
p.g=
bktk=
=========== password
j[=Cq
=========== is=
b@!g=J
        =LG
=0 E
=0}I
F=========== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
h=57
```

- Level 10→11

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ echo 'data.txt' | base64
ZGF0YS50eHQK
```
**

- Level 11→12

```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
```
**

- Level 12→13

```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ mkdir /tmp/pc
mkdir: cannot create directory '/tmp/pc': File exists
bandit12@bandit:~$ cp data.txt /tmp/pc
bandit12@bandit:~$ cd /tmp/pc
bandit12@bandit:/tmp/pc$ ls
data5.bin  data8.bin  myfile1,bin  myfile2  myfile4  myfile9     my
data6.bin  data.txt    myfile1.bin  myfile3  myfile7  myfile.bin
bandit12@bandit:/tmp/pc$ file myfile.txt
myfile.txt: ASCII text
bandit12@bandit:/tmp/pc$ cat myfile.txt
00000000: 1f8b 0808 3d05 8b63 0203 6461 7461 322e  ....=..c..data2.
00000010: 6269 6e00 0144 02bb fd42 5a68 3931 4159  bin..D...BZh91AY
00000020: 2653 59a3 054d b200 001a ffff de6f dff7  &SY..M.......o..
00000030: fe7f ff37 ffcf db8f 3ff3 efff 8f7c bdff  ...7....?....|..
00000040: ffde 5ff9 bbbf 7fff f7ef f4ff b001 3998  .._..........9.
00000050: 1068 0000 0326 8000 0340 0000 01a0 d0d3  .h...&...@......
00000060: 101a 0064 3206 8000 0006 8000 0341 9311  ...d2........A..
00000070: a34d 1a03 47a9 e531 a880 0d0d 3200 36a1  .M..G..1....2.6.
00000080: a000 3d40 1a68 1a03 2340 1a03 4001 a032  ..=@.h..#@..@..2
00000090: 7a21 e903 20d0 0346 9900 0320 000d 0034  z!.. ..F... ...4
000000a0: 0000 3432 9a06 8000 0068 0d00 0061 3434  ..42.....h...a44
000000b0: 1a00 000f 500c 8c80 d0d3 2006 8d06 8620  ....P..... ....
000000c0: 001a 0006 8683 47a8 c864 0683 405f 0602  ......G..d..@_..
000000d0: 3030 0841 9957 fa3a 7c68 f302 5862 3c87  00.A.W.:|h..Xb<.
```

```
00000180: 122b fc27 0048 7002 01ba 5a94 ccef 424b  .+..Hx.......B
00000190: 60e6 daf0 94e2 1488 8675 8844 15f7 1973  `........u.D...s
000001a0: a2d1 bbdf b90f 1806 b4ee 0d7e bfa2 21ba  ...........~..!
000001b0: b8e6 37f8 67a2 f1da 8825 4878 9ddc 5f7e  ..7.g....%Hx.._~
000001c0: ee2a 231d c8d2 8324 5e7d 1521 b35e e5d8  .*#....$^}.!.^.
000001d0: 6b8d ab46 0b33 b5fa 96f8 6d98 478f c515  k..F.3....m.G..
000001e0: 6105 094a 5c2f dcfa c7a5 dcd7 cc63 9f08  a..J\/.......c.
000001f0: 4e1e d3da aa7c a522 65a0 5799 1fef cd04  N....|."e.W....
00000200: 1e3c b065 8b2c 008d ce9d 0801 7889 5371  .<.e.,......x.Sq
00000210: 29f2 1021 0092 7855 080f 12d9 18d1 e3c9  )..!.xU........
00000220: f362 db32 3a7d 0cb3 2c47 0fe7 3870 64b0  .b.2:}..,G..8pd.
00000230: 65c4 fe30 71af 0680 f721 a04f a720 37f9  e..0q....!.O. 7.
00000240: 3a64 a195 8344 32ad c95a 9d30 618e 9b7d  :d...D2..Z.0a..}
00000250: 7933 fe2e e48a 70a1 2146 0a9b 645a 13f2  y3....p.!F..dZ..
00000260: 0344 0200 00                             .D...
bandit12@bandit:/tmp/pc$ cat myfile9
The password is wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
```

- Level 13→14

```
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220
```

- Level 14→15

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
bandit14@bandit:~$ nc localhost 30000
^C
bandit14@bandit:~$ nc localhost 30000
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
```

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
```

- Level 15→16

```
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15 | openssl s_client -quiet -conn
ect localhost:30001
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Dec  8 15:31:23 2022 GMT
verify return:1
depth=0 CN = localhost
notAfter=Dec  8 15:31:23 2022 GMT
verify return:1
Correct!
JQttfApK4SeyHwDlI9SXGR50qclOAil1
```

- Level 17→18

```
bandit17@bandit:~$ ls
passwords.new   passwords.old
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< U79zsNCl1urwJ5rU6pg7ZSCi7ifWOWpT
---
> hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
```

- Level 18→19

```
$ ls
readme
$ cat readme
awhqfNnAbc1naukrpqDYcF95h7HoMTrC
```

- Level 19→20

```
bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ ls -l
total 16
-rwsr-x--- 1 bandit20 bandit19 14876 Dec  3 08:13 bandit20-do
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
  Example: ./bandit20-do id
bandit19@bandit:~$ id
uid=11019(bandit19) gid=11019(bandit19) groups=11019(bandit19)
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVykI6W36BkBU0mJTCM8rR95XT
```