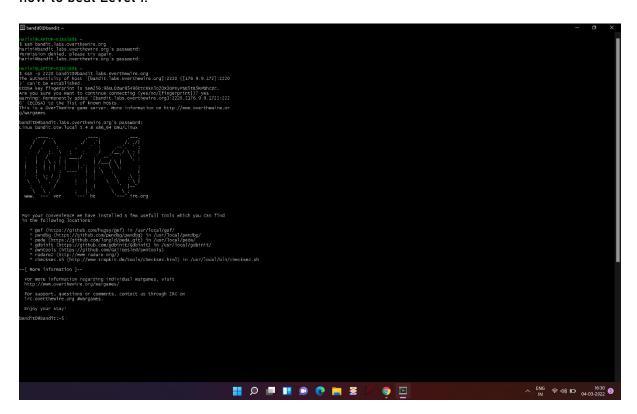# TASK-7: Over The Wire

- Bandit Level 0

Level Goal: The goal of this level is for you to log into the game using SSH. The host to which you need to connect is bandit.labs.overthewire.org, on port 2220. The username is bandit0 and the password is bandit0. Once logged in, go to the Level-1 page to find out how to beat Level 1.

- Bandit Level 0 → Level 1

Level Goal: The password for the next level is stored in a file called readme located in the home directory. Use this password to log into bandit1 using SSH. Whenever you find a password for a level, use SSH (on port 2220) to log into that level and continue the game.

Password: boJ9jbbUNNfktd78OOpsqOltutMc3MY1

- Bandit Level 1 → Level 2

Level Goal: The password for the next level is stored in a file called – located in the home directory

```
bandit1@bandit: ~
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat./-
-bash: cat./-: No such file or directory
bandit1@bandit:~$ cat ./-
CV1DtqXwVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ |
```

Password: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

- Bandit Level 2 → Level 3

Level Goal: The password for the next level is stored in a file called spaces in this filename located in the home directory.

```
bandit2@bandit: ~
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$
```

Password: UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

- Bandit Level 3 → Level 4

Level Goal: The password for the next level is stored in a hidden file in the inhere directory.

```
bandit3@bandit: ~/inhere
bandit3@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  inhere  .profile
bandit3@bandit:~$ mv inhere here
mv: cannot move 'inhere' to 'here': Permission denied
bandit3@bandit:~$ mv .inhere inhere
mv: cannot stat '.inhere': No such file or directory
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ mv .hidden hidden
mv: cannot move '.hidden' to 'hidden': Permission denied
bandit3@bandit:~/inhere$ ^C
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$
```

Password: pIwrPrtPN36QITSp3EQaw936yaFoFgAB

- **Bandit Level 4 → Level 5**

Level Goal: The password for the next level is stored in the only human-readable file in the inhere directory.

```
bandit4@bandit: ~/inhere
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ LS
-bash: LS: command not found
bandit4@bandit:~/inhere$ ls
-file00  -file02  -file04  -file06  -file08
-file01  -file03  -file05  -file07  -file09
bandit4@bandit:~/inhere$ find . -type f ! -executable -exec file {} + | grep ASCII
./-file07: ASCII text
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$ ^C
bandit4@bandit:~/inhere$
```

Password: koReBOKuIDDepwhWk7jZC0RTdopnAYKh

- **Bandit Level 5 → Level 6**

Level Goal: The password for the next level is stored in a file somewhere under the inhere directory and has all of the following properties:

1. human-readable
2. 1033 bytes in size
3. not executable

```
bandit5@bandit: ~/inhere
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere03  maybehere06  maybehere09  maybehere12  maybehere15  maybehere18
maybehere01  maybehere04  maybehere07  maybehere10  maybehere13  maybehere16  maybehere19
maybehere02  maybehere05  maybehere08  maybehere11  maybehere14  maybehere17
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable -exec file {} + | grep ASCII
./maybehere07/.file2: ASCII text, with very long lines
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7


bandit5@bandit:~/inhere$
```

Password: DXjZPULLxYr17uwoI01bNLQbtFemEgo7

- **Bandit Level 6 → Level 7**

Level Goal: The password for the next level is stored somewhere on the server and has all of the following properties:

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size


```
bandit6@bandit ~
bandit6@bandit:~$ ls
bandit6@bandit:~$ ls -a
.   ..  .bash_logout  .bashrc  .profile
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c | grep -F -v Permission | grep -F -v directory
find: '/root': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/home/bandit29-git': Permission denied
find: '/home/bandit31-git': Permission denied
find: '/lost+found': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/lvm/archive': Permission denied
find: '/etc/lvm/backup': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/20870/task/20870/fd/6': No such file or directory
find: '/proc/20870/task/20870/fdinfo/6': No such file or directory
find: '/proc/20870/fd/5': No such file or directory
find: '/proc/20870/fdinfo/5': No such file or directory
find: '/cgroup2/csessions': Permission denied
find: '/boot/lost+found': Permission denied
find: '/tmp': Permission denied
find: '/run/lvm': Permission denied
find: '/run/screen/S-bandit10': Permission denied
find: '/run/screen/S-bandit29': Permission denied
find: '/run/screen/S-bandit25': Permission denied
find: '/run/screen/S-bandit30': Permission denied
find: '/run/screen/S-bandit9': Permission denied
find: '/run/screen/S-bandit28': Permission denied
find: '/run/screen/S-bandit18': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/screen/S-bandit12': Permission denied
find: '/run/screen/S-bandit5': Permission denied
find: '/run/screen/S-bandit7': Permission denied
find: '/run/screen/S-bandit16': Permission denied
find: '/run/screen/S-bandit26': Permission denied
find: '/run/screen/S-bandit8': Permission denied
find: '/run/screen/S-bandit15': Permission denied
find: '/run/screen/S-bandit4': Permission denied
find: '/run/screen/S-bandit3': Permission denied
find: '/run/screen/S-bandit19': Permission denied
find: '/run/screen/S-bandit31': Permission denied
find: '/run/screen/S-bandit17': Permission denied
find: '/run/screen/S-bandit22': Permission denied
find: '/run/screen/S-bandit21': Permission denied
find: '/run/screen/S-bandit14': Permission denied
find: '/run/screen/S-bandit13': Permission denied
find: '/run/screen/S-bandit24': Permission denied
find: '/run/screen/S-bandit23': Permission denied
find: '/run/shm': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/tmp': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/polkit-1': Permission denied
find: '/var/log': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/ldconfig': Permission denied
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>&1 | grep -F -v Permission | grep -F -v directory
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$
```

Password: <ins>HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs</ins>

- **Bandit Level 7 → Level 8**

Level Goal: The password for the next level is stored in the file data.txt next to the word millionth

```
bandit7@bandit: ~
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ cat data.txt | grep millionth
millionth        cvX2JJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$ |
```

Password: cvX2JJa4CFALtqS87jk27qwqGhBM9plV

- **Bandit Level 8 → Level 9**

Level Goal: The password for the next level is stored in the file data.txt and is the only line of text that occurs only once

```
bandit8@bandit: ~
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ cat data.txt | sort | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
bandit8@bandit:~$ |
```

Password: UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

- **Bandit Level 9 → Level 10**

Level Goal: The password for the next level is stored in the file data.txt in one of the few human-readable strings, preceded by several '=' characters.

```
bandit9@bandit: ~
bandit9@bandit:~$ ls
data.txt
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&^
bandit9@bandit:~$ strings data.txt | grep "==="
========== the*2i"4
========== password
Z)========== is
&========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
bandit9@bandit:~$ |
```

Password: truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

- Bandit Level 10 → Level 11

Level Goal: The password for the next level is stored in the file data.txt, which contains base64 encoded data

```
bandit10@bandit: ~
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ base64 data.txt
VkdobElIQmhjMO4zYjNKaOlHbHpJRwxHZFdOM1MwZHpSbGMOVFU5eEOwbFNSbkZ5ZUVVeGFIaFVU
a1ZpVlZCUONnPTOK
bandit10@bandit:~$ cat data.txt | base64 --decode
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$
```

Password: IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

- Bandit Level 11 → Level 12

Level Goal: The password for the next level is stored in the file data.txt, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions

```
bandit11@bandit: ~
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh
bandit11@bandit:~$ tr 'A-Za-z' 'N-ZA-Mn-za-m'
^C
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
bandit11@bandit:~$ |
```

Password: 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

- Bandit Level 12 → Level 13

Level Goal: The password for the next level is stored in the file data.txt, which is a hex dump of a file that has been repeatedly compressed. For this level, it may be useful to create a directory under /tmp in which you can work using mkdir. For example: mkdir /tmp/myname123. Then copy the datafile using cp, and rename it using mv (read the manpages!)

```
bandit12@bandit /tmp/hello
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ mkdir /tmp/hello
bandit12@bandit:~$ cp data.txt /tmp/hello
bandit12@bandit:~$ cd /tmp/hello
bandit12@bandit:/tmp/hello$ file data.txt
data.txt: ASCII text
bandit12@bandit:/tmp/hello$ xxd -r data.txt info.bin
bandit12@bandit:/tmp/hello$ file info.bin
info.bin: gzip compressed data, was "data2.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/hello$ gzip -d info.bin
gzip: info.bin: unknown suffix -- ignored
bandit12@bandit:/tmp/hello$ mv info.bin info.gz
bandit12@bandit:/tmp/hello$ gzip -d info.gz
bandit12@bandit:/tmp/hello$ ls
data.txt  info
bandit12@bandit:/tmp/hello$ file info
info: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/hello$ bzip2 -d -k info.out
bzip2: Can't open input file info.out: No such file or directory.
bandit12@bandit:/tmp/hello$ bzip2 -d -k info
bzip2: Can't guess original name for info -- using info.out
bandit12@bandit:/tmp/hello$ file info.out
info.out: gzip compressed data, was "data4.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/hello$ mv info.out data2.gz
bandit12@bandit:/tmp/hello$ file data2.gz
data2.gz: gzip compressed data, was "data4.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/hello$ gzip data2.gz
gzip: data2.gz already has .gz suffix -- unchanged
bandit12@bandit:/tmp/hello$ gzip -d data2.gz
bandit12@bandit:/tmp/hello$ file data2
data2: POSIX tar archive (GNU)
bandit12@bandit:/tmp/hello$ tar -xvf data2
data5.bin
bandit12@bandit:/tmp/hello$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/hello$ tar -xvf data5.bin
data6.bin
bandit12@bandit:/tmp/hello$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/hello$ bzip2 -d data6.bin
bzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/hello$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/hello$ tar data6.bin.out
tar: Old option 'b' requires an argument.
Try 'tar --help' or 'tar --usage' for more information.
bandit12@bandit:/tmp/hello$ tar -xvf data6.bin.out
data8.bin
bandit12@bandit:/tmp/hello$ 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/hello$ mv data8.bin data8.gz
bandit12@bandit:/tmp/hello$ gzip -d data8.gz
bandit12@bandit:/tmp/hello$ file data8
data8: ASCII text
bandit12@bandit:/tmp/hello$ cat data8
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/hello$ |
```

Password: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

- Bandit Level 13 → Level 14

Level Goal: The password for the next level is stored in /etc/bandit_pass/bandit14 and can only be read by user bandit14. For this level, you don't get the next password, but you get a private SSH key that can be used to log into the next level. Note: localhost is a hostname that refers to the machine you are working on

Password: 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

- Bandit Level 14 → Level 15

Level Goal: The password for the next level can be retrieved by submitting the password of the current level to port 30000 on localhost.

Password: BfMYroe26WYalil77FoDi9qh59eK5xNr

- Bandit Level 15 → Level 16

Level Goal: The password for the next level can be retrieved by submitting the password of the current level to port 30001 on localhost using SSL encryption.

<u>Helpful note:</u> Getting "HEARTBEATING" and "Read R BLOCK"? Use -ign_eof and read the "CONNECTED COMMANDS" section on the manpage. Next to 'R' and 'Q', the 'B' command also works in this version of that command…

```
bandit15@bandit:~$ openssl s_client -ign_eof -connect localhost:30001
CONNECTED(00000003)
depth=0 CN = localhost
verify error:num=18:self signed certificate
verify return:1
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 8a eb e8 f5 31 15 46 ad-b2 a8 10 c1 51 b9 66 14   ....1.F.....Q.f.
    0010 - 7b 1c 5d f4 25 53 db e8-d4 19 63 fa a6 35 01 e4   {.].%S....c..5..
    0020 - 6e c9 3a 42 69 96 6b 6d-25 0d 46 89 c8 cd 66 1f   n.:Bi.km%.F...f.
    0030 - 9c 86 3f 56 fd ca 86 fe-3b ac 09 ca ab 37 ef 4e   ..?V....;....7.N
    0040 - 18 f2 3a 0d b5 d9 67 01-5e 35 0e 52 60 cc d7 d5   ..:...g.^5.R`...
    0050 - 99 43 d8 f1 2f eb a0 d7-6e 9f 1b a9 4e ab fb f5   .C../...n...N...
    0060 - 60 b7 ce 4d dd bf b8 21-5a 6e f8 1e 68 71 53 d2   `..M...!Zn..hqS.
    0070 - 4a 03 af 83 d1 98 2a d8-23 e9 81 cc 28 45 fb 6b   J.....*.#...(E.k
    0080 - fb 83 a3 4d fe 17 15 7f-56 f1 cd 2c 8b 88 a0 9d   ...M....V..,....
    0090 - b6 1a 51 56 92 a7 b9 20-4c 9a 6e 50 6d d9 7a 1f   ..QV... L.nPm.z.

    Start Time: 1646458174
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
    Extended master secret: yes
---
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd

closed
bandit15@bandit:~$ |
```

<u>Password:</u> cluFn7wTiGryunymYOu4RcffSxQluehd

·········· *The End* ··········