Ankit Shringarpure -2042

Bandwidth Over The Wire

Level 0 → Level 1

Explanation:
In this level, the task is to log in to the Bandit server using SSH. After successful login, a file named readme is present in the home directory. Reading this file reveals the password for the next level.

Code:

ssh bandit0@bandit.labs.overthewire.org -p 2220

ls

cat readme

Level 1 → Level 2

Explanation:
The password is stored in a file named -. Since - is treated as an option by commands, it must be accessed using a relative path.

Code:

ls

cat ./-

Level 2 → Level 3

Explanation:
The password is stored in a file whose name contains spaces. Quotation marks are required to correctly read the file.

Code:

ls

cat "spaces in this filename"

Level 3 → Level 4

Explanation:
The password is hidden inside a hidden file. Hidden files start with a dot (.) and are not visible with a normal ls command.

Code:

cd inhere

ls -a

cat .hidden

Level 4 → Level 5

Explanation:
Multiple files are present, but only one file contains readable text. The file command is used to identify the correct file.

Code:

cd inhere

file ./*

cat ./-file07

Level 5 → Level 6

Explanation:
The password file has specific properties: exact size, non-executable, and stored inside directories. The find command is used to locate it.

Code:

find . -type f -size 1033c ! -executable

cat ./maybehere07/.file2

Level 6 → Level 7

Explanation:
The password file is owned by a specific user and group and is located anywhere on the system.

Code:

find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null

cat /var/lib/dpkg/info/bandit7.password

Level 7 → Level 8

Explanation:
The password is stored in a large file next to a specific word.

Code:

cat data.txt | grep millionth

Level 9 → Level 10

Explanation:
The password is hidden in binary data. Extracting readable strings reveals it.

Code:

strings data.txt | grep =

Level 10 → Level 11

Explanation:
The data is encoded in Base64 format. Decoding reveals the password.

Code:

base64 -d data.txt

Level 11 → Level 12

Explanation:
The password is encrypted using the ROT13 cipher.

Code:

```
cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
```

Level 12 → Level 13

Explanation:
The file is compressed multiple times using different formats. Each layer must be decompressed.

Code:

```
xxd -r data.txt data

file data

gzip -d data.gz

bzip2 -d data.bz2

tar -xf data.tar

cat final_file
```

Level 13 → Level 14

Explanation:
An SSH private key is provided instead of a password.

Code:

```
chmod 600 sshkey.private
```

ssh -i sshkey.private bandit14@localhost -p 2220

cat /etc/bandit_pass/bandit14

Level 14 → Level 15

Explanation:
The password must be sent to a local service using Netcat.

Code:

cat /etc/bandit_pass/bandit14 | nc localhost 30000

Level 15 → Level 16

Explanation:
Secure communication is required using SSL encryption.

Code:

openssl s_client -connect localhost:30001

Level 16 → Level 17

Explanation:
Multiple services are running on different ports. Port scanning identifies the correct one.

Code:

nmap localhost -p 31000-32000

openssl s_client -connect localhost:31790

Level 17 → Level 18

Explanation:
Two files contain passwords. Comparing them reveals the changed line.

Code:

diff passwords.old passwords.new

Level 18 → Level 19

Explanation:
The system logs out immediately. Executing a command directly during login bypasses this.

Code:

ssh bandit18@bandit.labs.overthewire.org -p 2220
cat readme

Level 19 → Level 20

Explanation:
A special binary allows command execution as another user.

Code:

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

Level 20 → Level 21

Explanation:

A local service expects the password to be sent back.

Code:

nc -lvp 4444

./suconnect 4444