Bandit Level 20 - Level 21

There is a setuid binary in the homedirectory, that does the following:

1. Makes a connection to the localhost on a port you specify
2. Reads a line of text from the connection
3. Compares it to the password in previous level (the password to enter bandit20)
4. If these passwords match then it will transmit the password to next level (bandit21)

To achieve this we need two terminal windows. One terminal will listen and the other will send. Log into bandit20 on both terminals.

“Screenshot 2024-10-24 at 1.43.47 PM 1.png” could not be found.

On the terminal on the right, we will use this for listening on an arbirtary port number 8888.

```
bandit20@bandit:~$ nc -lvp 8888
Listening on 0.0.0.0 1234
```

The flag -l is to listen, -v is Verbose to gives is detailed output and -p is to specify port number.

The terminal on the left we will connect to the terminal on the right by passing in the port number 8888 to suconnect.

```
bandit20@bandit:~$ ./suconnect 8888
```

The terminal on the left will output that we are connected.

```
Connection received on localhost 50986
```

Underneath the above we can submit the password to bandit level 20.

```
Connection received on localhost 50986
0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
```

The terminal the left will then display the following.

```
Read: 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
Password matches, sending next password
```

The terminal on the right will receive the password.

```
EeoULMCra2q0dSkYj561DX7s1CpBuOBt
bandit20@bandit:~$
```