[pwnable.kr WriteUp]

이태규(ltg2030)

[Toddler's Bottle] coin1 6PT

문제 설명

Mommy, I wanna play a game!
(if your network response time is too slow, try nc 0 9007 inside pwnable.kr server)

Running at : nc pwnable.kr 9007

```
->
        ------------------------------------------------
        -              Shall we play a game?           -
        ------------------------------------------------
        You have given some gold coins in your hand
        however, there is one counterfeit coin among them
        counterfeit coin looks exactly same as real coin
        however, its weight is different from real one
        real coin weighs 10, counterfeit coin weighes 9
        help me to find the counterfeit coin with a scale
        if you find 100 counterfeit coins, you will get reward :)
        FYI, you have 30 seconds.

        - How to play -
        1. you get a number of coins (N) and number of chances (C)
        2. then you specify a set of index numbers of coins to be weighed
        3. you get the weight information
        4. 2~3 repeats C time, then you give the answer

        - Example -
        [Server] N=4 C=2        # find counterfeit among 4 coins with 2 trial
        [Client] 0 1            # weigh first and second coin
        [Server] 20                     # scale result : 20
        [Client] 3                      # weigh fourth coin
        [Server] 10                     # scale result : 10
        [Client] 2                      # counterfeit coin is third!
        [Server] Correct!
```

Binary Search : 한글로는 이진 검색, 오름차순으로 정렬된 데이터에서 특정 값의 위치를 찾는데 사용되는 탐색이다. 이 문제의 경우 동전의 index가 1~N으로 정렬되어있다고 생각하면 Binary Search를 적용할 수 있다.

소켓 통신 : 클라이언트에서 서버와 소켓을 통해 통신을 하는 것이다. Python 에서 socket 모듈을 제공하여 이를 이용하여 소켓 통신을 하는 스크립트를 만들어 문제를 해결할 수 있다.

문제 풀이(이론)

[pwnable.kr WriteUp]

이태규(ltg2030)

1. nc pwnable.kr 9007을 하면 문제의 설명이 나온다. 문제를 읽어보면 Binary Search로 접근해야 함을 알 수 있는데 Binary Search를 적용하는 법은 다음과 같다.
   1) low~high에 9g 동전이 있다.
   2) mid를 기준으로 low~mid에 9g 동전이 있는지 확인한다.
   3) 2가 참일 경우 high=mid, 거짓일 경우 mid=low+1 로 바꾼다.
   4) 이를 반복하여 low=high, 즉 9g인 동전을 찾을 수 있다.

2. 100문제를 풀고 (k), 각 문제별로 C번 탐색을 하고 (j), low~mid의 동전에 9g이 있는지 소켓을 통해 묻는 (i) Python 스크립트를 작성했고 스크립트를 실행하여 flag를 얻었다.

문제 풀이(실습)

```
import socket
hostname="pwnable.kr"
port=9007;
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM);
s.connect((hostname,port));
data=s.recv(4000);
for k in range(0,100):
        data=s.recv(100);
        data=data.split(' ');
        n=int(data[0][2:]);
        c=int(data[1][2:]);
        low=1;
        high=n;
        for i in range(0,c):
                mid = int((low+high)/2);
                sendmes="";
                for j in range(low,mid+1):
                        sendmes=sendmes+("%d " %(j-1));
                sendmes=sendmes+"\n";
                #print(sendmes);
                s.send(sendmes);
                data=int(s.recv(100));
                if(data%10==0):
                        low=mid+1;
                else:
                        high=mid;
        sendmes="%d"%(low-1)+"\n";
        s.send(sendmes);
        data=s.recv(1000);
        print(data);
data=s.recv(1000);
print(data);
s.close();
                                                        33,1          Bot
```

- Python Script

```
Correct! (90)

Correct! (91)

Correct! (92)

Correct! (93)

Correct! (94)

Correct! (95)

Correct! (96)

Correct! (97)

Correct! (98)

Correct! (99)

Congrats! get your flag
b1NaRy_S34rch1nG_1s_3asy_p3asy

root@ubuntu:~/coin# _
```

실행 결과 b1NaRy_S34rch1nG_1s_3asy_p3asy 라는 flag를 얻었다.

실행화면