Coding-Remote-Dynamic

Problem: If you answer 10000 problems, the flag is yours. I want the decimal version of these numbers.

Hint: Your pwn level is over 9000!

Given: nc 127.0.0.1 11111

Notes: Pwntools library will be used. To learn more about how to use and get pwntools visit this [link](https://github.com/Gallopsled/pwntools).

Steps:

1) Connect to the server and see what the output is.

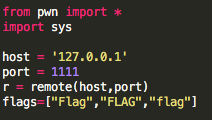
Note: before you start making your script is easier to connect using netcat and see the output.



2) From connecting to the server, you can notice that the information that is sent back is in base64. Let’s decode this base64 string that the server gave us and see what it is.

NTY1== 🡪 565

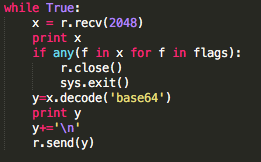
3) Now we know that we are given a base64 encoded version of a decimal number. From the problem statement we know we have to give the server the correct decimal value for 10000 different problems. Time to build a script. This script should, 1) connect to the server, 2) get info from the server, and 3) send the data back to the server. This needs to be in a loop to go until the server gives you the flag.



Note: This short snippet of the script connects to the remote server at 127.0.0.1 at port 1111.

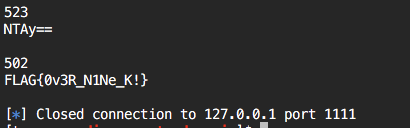
Also, notice that there is a list of flags keywords. Since we know the format of the flags start with the word flag, then keep this list to check if the information we get back from the server is the flag.

4) Now we will create the loop to get info from the server and send information back to the server.



Note: We make a loop of while true to keep going while the server is sending back information. The variable ‘x’ receives the data for the server. We then use the list of flag keywords we created to check if the data we are getting from the server is the flag. If we receive the flag, we want to close the connection. Then if ‘x’ is not the flag we want to decode the base64 string we received to turn it back to the decimal value. We then can print out the number we are sending back (more of a debugging feature). IMPORTANT: we are mimicking a raw\_input() type of input in python. This means our input we send to the server needs to have a newline included which is copying when you hit enter after giving the string. We then send this data to the server.

If the data we send back passes 10000 answers, we should receive the flag.



Sample script:

#!/usr/bin/python

# -\*- coding: utf-8 -\*-

from pwn import \*

import sys

host = '127.0.0.1'

port = 1111

r = remote(host,port)

flags=["Flag","FLAG","flag"]

while True:

x = r.recv(2048)

print x

if any(f in x for f in flags):

r.close()

sys.exit()

y=x.decode('base64')

print y

y+='\n'

r.send(y)

r.close()