Coding-Remote – The Race

Problem: If you can beat this server in a race, it will give you the flag

Hint: The proper tools must be used to pwn this race

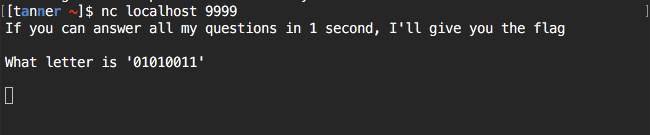
Given: nc 127.0.0.1 9999

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

Steps:

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

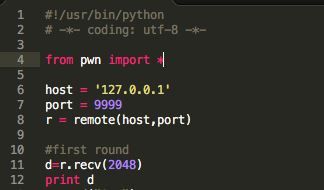
Note: Connect using nc the first time to see the first output of the server



2) Start creating a script that you will build on to beat the speed of the server timeout.

Note: Pwntools will need to be used in a python script to make it easy to connect to the server

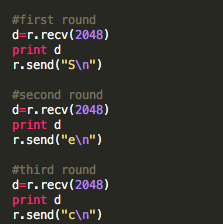
Now that we have seen the first question, let’s start putting the script together.



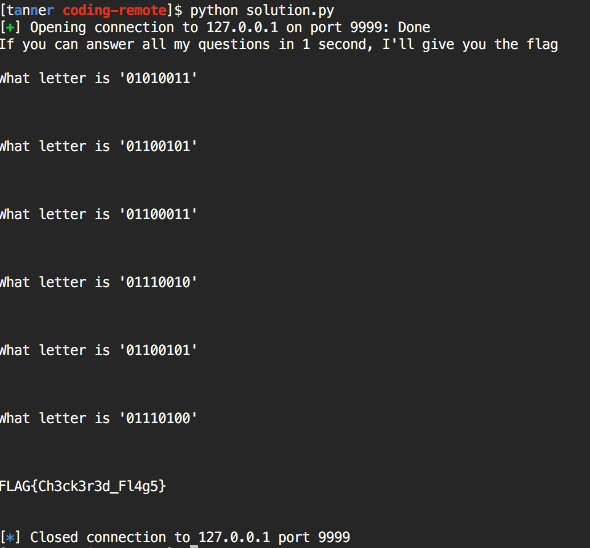
This script will connect to the server and receive that data that the server gives out, which can be seen in the first screenshot. When running this script you would see the same output as in the screenshot.

3) Build on this script until you eventually get a flag as output from the server. The reason a script must be used in this problem is because the server will timeout in 1 second. Meaning there is no possible way you can answer all the questions with human input. The input must be sent as a stream to the server and interpreted by the server in faster than 1 second.

This next screenshot is part of the solution to show how to send data back to the server because you will need to send the answers to the server.



This shows how to send data back to the server. And eventually if you run your solution script the following will show:



Example Solution Script:

#!/usr/bin/python

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

from pwn import \*

host = '127.0.0.1'

port = 9999

r = remote(host,port)

#first round

d=r.recv(2048)

print d

r.send("S\n")

#second round

d=r.recv(2048)

print d

r.send("e\n")

#third round

d=r.recv(2048)

print d

r.send("c\n")

#fourth round

d=r.recv(2048)

print d

r.send("r\n")

#fifth round

d=r.recv(2048)

print d

r.send("e\n")

#sixth round

d=r.recv(2048)

print d

r.send("t\n")

#flag

d=r.recv(2048)

d=r.recv(2048)

print d

r.close()