

The Race

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

Given: nc 127.0.0.1 19999

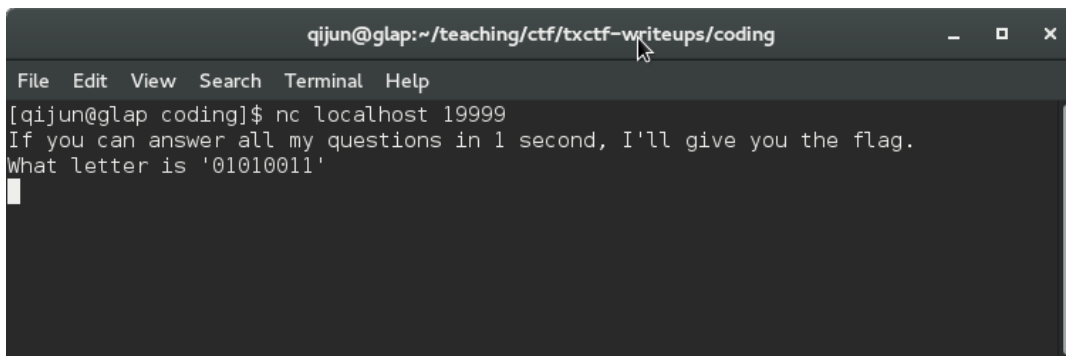
Notes:

Pwntools library will be used in this solution. To learn more about how to use and get pwntools visit <https://github.com/Gallopsled/pwntools>.

Steps:

1) Connect to server using the tool 'nc' (netcat), and see what the output is. Obviously, it gives the ASCII code of a character in the binary form. You will need to send the character back based on the ASCII code.

In this screenshot, the ASCII code is '01010011'. You can check the code on <http://www.ascii-code.com/>. The corresponding character is 'S'.



```
qijun@glap:~/teaching/ctf/txctf-writeups/coding
File Edit View Search Terminal Help
[qijun@glap coding]$ nc localhost 19999
If you can answer all my questions in 1 second, I'll give you the flag.
What letter is '01010011'
```

2) Start creating a Python script that you will build on to beat the speed of the server timeout. We will use Pwntools in the 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.

```
1  #!/usr/bin/python
2  # -*- coding: utf-8 -*-
3  from pwn import *
4
5  host = '127.0.0.1'
6  port = 19999
7  r = remote(host, port)
8
9  d = r.recv(2048)
10 print d
```

This script imports pwn, which is the python library of Pwntools. It will connect to the server 127.0.0.1 on port 19999 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) We must use a script to retrieve the flag, 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 extract the ASCII code from the server's output, convert it to a character, and then send the character back to the server. So, the process of responding to each question is automated. You need to repeat the code snippet for all questions until you get the flag.

```
13     s=d.split(" ")[-2]
14     print s
15     c=chr(int(s,2))
16     print c
17     r.send(c+'\n')
```

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

```
[+] Opening connection to 127.0.0.1 on port 19999: Done
If you can answer all my questions in 1 second, I'll give you the flag.
What letter is '01010011'

01010011
S
What letter is '01100101'

01100101
e
What letter is '01100011'

01100011
c
What letter is '01110010'

01110010
r
What letter is '01100101'

01100101
e
What letter is '01110100'

01110100
t
FLAG{Ch3ck3r3d_Fl4g5}

[*] Closed connection to 127.0.0.1 port 19999
```

Now, you can build a complete script to solve this problem.