Quantum Scrambler

Medium | Reverse Engineering | picoCTF 2025 | browser_webshell_solvable

AUTHOR: MICHAEL CROTTY

Description

We invented a new cypher that uses "quantum entanglement" to encode the flag. Do you have what it takes to decode it? Additional details will be available after launching your challenge instance.

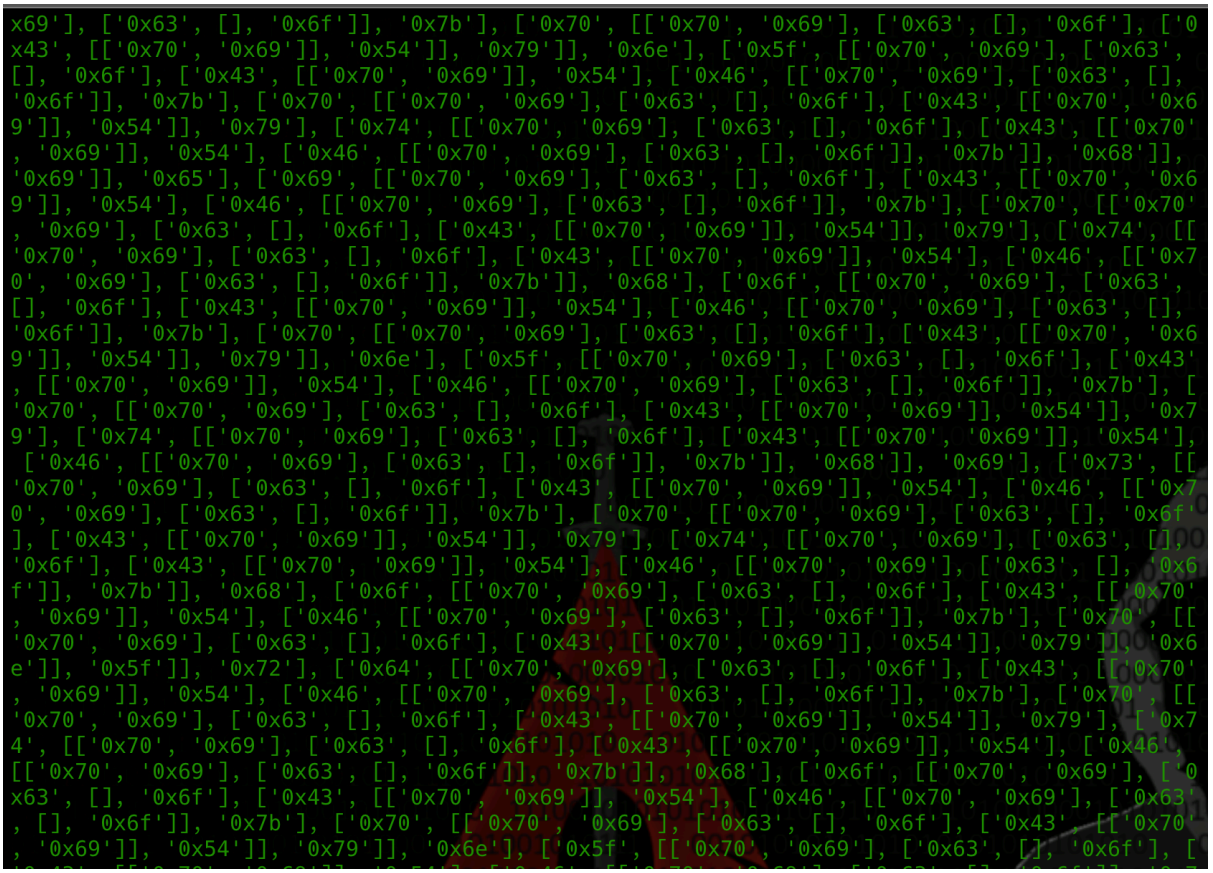
This challenge launches an instance on demand.

Its current status is: NOT_RUNNING

Launch Instance

Hints

Kali ini tantangan yang menurutku sulit, aku harus menyelesaikannya selama seharian karena kaget dengan bagaimana struktur output hasil netcat yang diberikan oleh host dan port pada kasus ini. Jadi mari kita lihat outputnya terlebih dahulu.



Ini adalah potongan outputnya, bisa kita lihat sangat tidak jelas. Namun untuk menyelesaikannya, aku masih menonton dan melihat write up dari orang lain melalui medium dan youtube dan menemukan solver yang menurutku mudah difahami dan mudah diimplementasikan. Beginilah solvernya dalam bahasa python.

```python
#!/usr/bin/env python3
from pwn import *
import ast

host = 'verbal-sleep.picoctf.net'
port = '59576'

connect = remote(host,port)
hex_value = connect.recvall() # Menerima value dari nc [host] [port] dalam bentuk bytes
list_hex = ast.literal_eval(hex_value.decode()) # value dari hex_value didecode menjadi string lalu diubah tipenya sesuai dari tipe output nc [host]

flag = ""
for i in list_hex:
    for z in i:
        if(len(str(z)) == 4):
            flag+=chr(int(z,16))

print(flag)
```

Nah, penjelasan dari kode sudah ada pada comment ya.

ketiak dijalankan ./solver.py maka akan muncul flag.

```
Quantum-Scrambler % cat solver.py
#!/usr/bin/env python3
from pwn import *
import ast

host = 'verbal-sleep.picoctf.net'
port = '59576'

connect = remote(host,port)
hex_value = connect.recvall() # Menerima value dari nc [host] [port] dalam bentuk bytes
list_hex = ast.literal_eval(hex_value.decode()) # value dari hex_value didecode menjadi stri
ng lalu diubah tipenya sesuai dari tipe output nc [host] [port]

flag = ""
for i in list_hex:
    for z in i:
        if(len(str(z)) == 4):
            flag+=chr(int(z,16))

print(flag)

Quantum-Scrambler % ls -l solver.py
-rw-r--r--@ 1 user  staff  510 20 Jan 11:33 solver.py
Quantum-Scrambler % chmod +x solver.py
Quantum-Scrambler % ./solver.py
[*] Checking for new versions of pwntools
    To disable this functionality, set the contents of /Users/user/.cache/.pwntools-cache-3.
13/update to 'never' (old way).
    Or add the following lines to ~/.pwn.conf or ~/.config/pwn.conf (or /etc/pwn.conf system
-wide):
        [update]
        interval=never
[*] You have the latest version of Pwntools (4.15.0)
[+] Opening connection to verbal-sleep.picoctf.net on port 59576: Done
[+] Receiving all data: Done (49.72KB)
[*] Closed connection to verbal-sleep.picoctf.net port 59576
picoCTF{python_is_weirdfeabf287}
```

Flag : picoCTF{python_is_weirdfeabf287}