

Rainbow test

Autor

@pwnedshell

Descripción

¿Eres lo suficientemente rápido en las matemáticas arcoíris?

Solución

Al conectarse mediante **netcat** somos recibidos con el siguiente *output*:

Se observan diferentes números y símbolos de colores.

El reto consiste en darse cuenta de que hay que solucionar la ecuación del color al que corresponde la palabra PROBLEM. Dependiendo del color de esta palabra, cada vez habrá que escoger ciertos números y ciertos caracteres. Todo en menos de 5 segundos.

Rainbow test 1

Hmmm esto es tarea de scripting, concretamente de la librería pun de python.

Esta librería concede distintas herramientas y funciones para conectarse remotamente y obtener la salida de la terminal, poder manipularla y enviar los datos correspondientes.

Un ejemplo de script explicado sería el siguiente:

```
import re
from pwn import *
# Uso de la librería pwntools para conectarse remotamente y poder manejar entrada/salida
p = remote("IP_DESTINO", PUERTO_DESTINO)
# Recogemos el output entero
output = p.readuntil(b'(2 decimals): ')
# 5 H |
# Buscamos este string -> \x1b[92mPROBLEM\x1b[0m
color = int(re.search(b'\x1b\[([0-9]+)mPROBLEM', output).group(1))
# Info sobre los colores y sus significados
# https://chrisyeh96.github.io/2020/03/28/terminal-colors.html
colors = {
   90: "black",
   91: "red",
   92: "green"
   93: "yellow",
   94: "blue",
   95: "magenta",
   96: "cyan",
   97: "white",
print("[\x1b["+str(color)+"m"\x1b[0m] The chosen color is\x1b["+str(color)+"m", colors[color], "\x1b[0m")]
                HIIHH
# Encontrar por regex según el color y juntar la ecuación
regex = "(" + str(color) + "m\s([0-9]|\.|\-|\+|\/|x|\=)+)"
results = re.findall(bytes(regex, "utf-8"), output)
ecuation = "".join([elem[0].decode("utf-8").split(" ")[1] for elem in results])
# Reemplazar el símbolo x por *, evaluar la expresión, redondear a 2 decimales y convertir a string
solution = str(round(eval(ecuation.replace("x", "*")[:-1]), 2))
print("[\x1b["+str(color)+"m*\x1b[0m] The solution is", solution)
```

Rainbow test 2

```
# Enviar solución y recibir respuesta
p.sendline(bytes(solution, "utf-8"))
flag = p.recvline().decode("utf-8")

print(flag)

[+] Opening connection to ******* on port ****: Done
[*] The chosen color is yellow
[*] The solution is 0.35
[*] Congrats rainbow mathematician! HackOn{Ny4n_c4t_l0v3s_y0u}

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

Flag

```
{\tt HackOn\{Ny4n\_c4t\_l0v3s\_y0u\}}
```

Rainbow test 3