[LAB'4] return to libc

- 实验环境：Ubuntu 16.04 i386
- 实验工具：GDB

Q1：阅读源码，分析strcut程序的流程

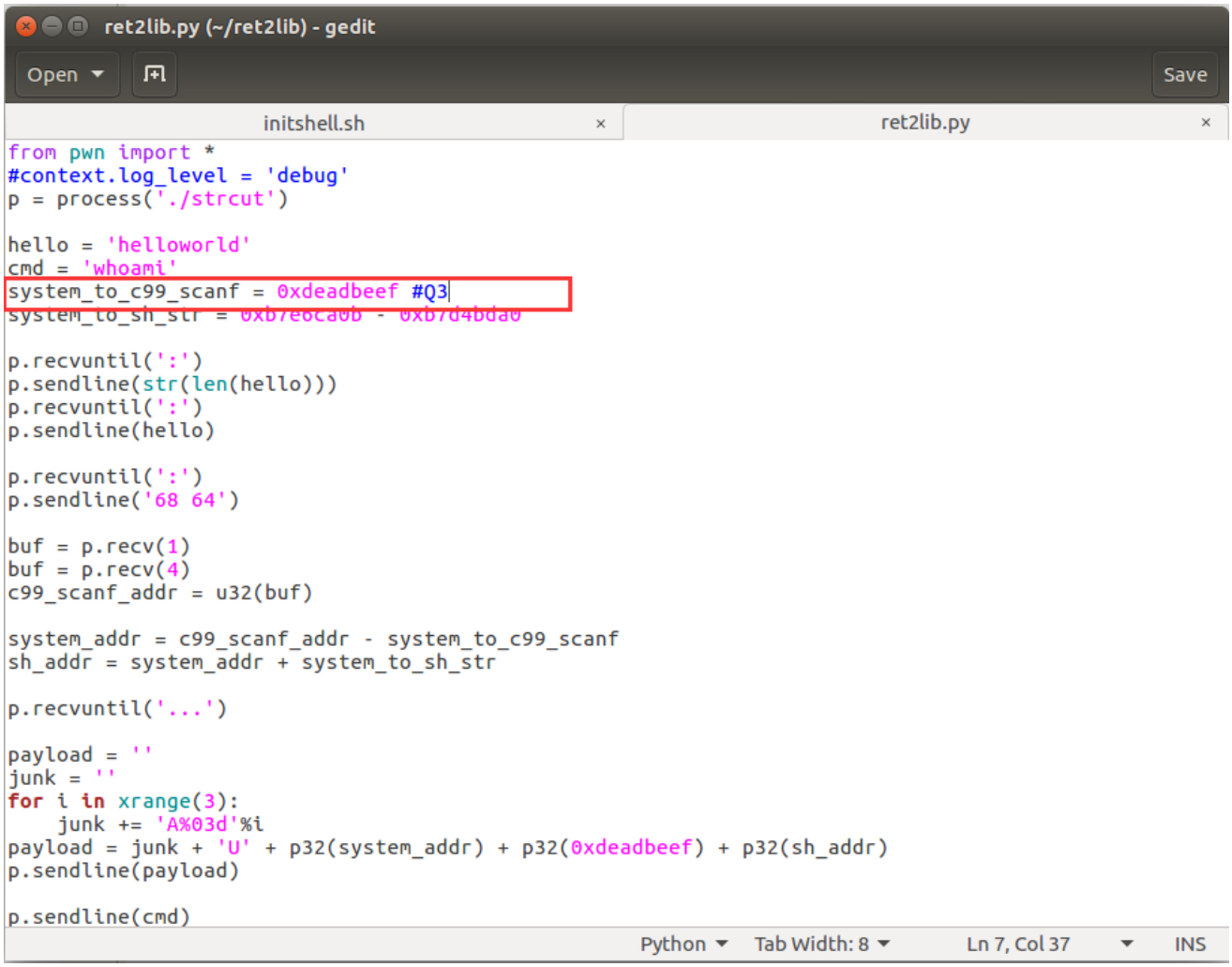
Q2：使用peda的checksec命令查看strcut开了哪些保护?

```
student@IS308-U1604: ~/ret2lib
student@IS308-U1604:~/ret2lib$ gdb strcut
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.5) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from strcut...(no debugging symbols found)...done.
gdb-peda$ checksec
CANARY    : disabled
FORTIFY   : disabled
NX        : ENABLED
PIE       : disabled
RELRO     : Partial
gdb-peda$
```

Q3：使用`readelf --syms`查看linux系统下的libc中的scanf和system的相对偏移 （Tips,/lib/i386-linux-gnu/libc.so.6)

```
18:48 [ idtest]$ readelf --syms /lib/x86_64-linux-gnu/libc.so.6  | grep system
   232: 0000000000159e20    99 FUNC    GLOBAL DEFAULT   13 svcerr_systemerr@@GLIBC_2.2.5
   607: 000000000004f440    45 FUNC    GLOBAL DEFAULT   13 __libc_system@@GLIBC_PRIVATE
  1403: 000000000004f440    45 FUNC    WEAK   DEFAULT   13 system@@GLIBC_2.2.5
18:48 [ idtest]$ readelf --syms /lib/x86_64-linux-gnu/libc.so.6  | grep isoc99_scanf
   412: 00000000000e7bec0   475 FUNC    GLOBAL DEFAULT   13 __isoc99_scanf@@GLIBC_2.7
18:48 [ idtest]$
```

修改脚本中对应的值(每个系统的libc可能不一样)，运行ret2lib.py的脚本，并完成利用



Q4：使用GDB调试程序，分析在控制指针后栈的布局（tips, 在有漏洞函数的ret处下断点）

Q5：我们可以获取scanf的地址，源自于程序的漏洞，请对此做分析与说明

Q6：为了让攻击不易被察觉，请修改ret2lib.py，使得exit命令结束后，受害程序回到main函数重新执行

Q7（选做）：获取可以实现一次攻击的载荷数据流
附加条件：关闭当前系统的ASLR

Q8（选做）：利用ROP的方式完成一个打开文件的操作(Tips, open,read,write)