

中国科学技术大学

《网络安全》

实验报告

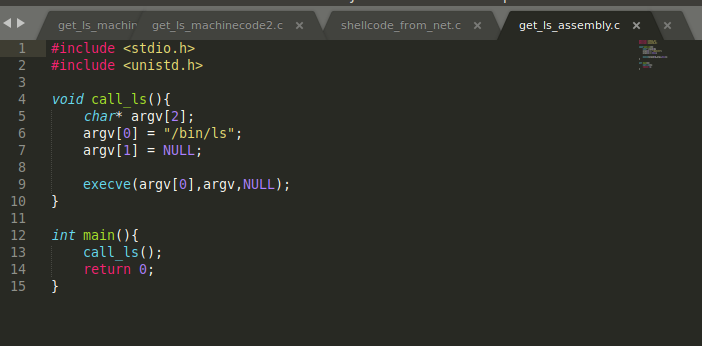
姓名：吴佳明

学号：SA19221027

年级：硕士研究生一年级

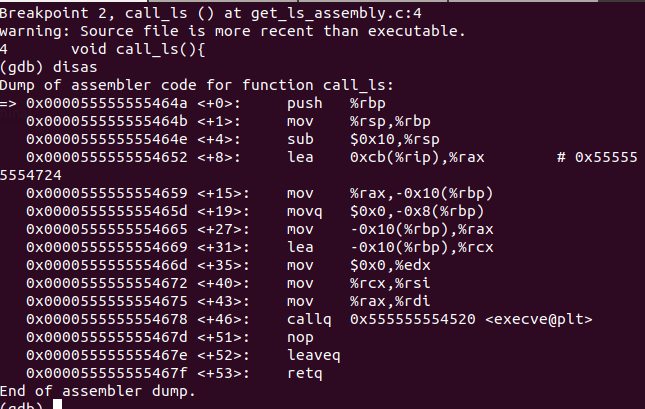
本实验基于ubuntu18 64bit

首先，写一个使用execve调用/bin/ls的c语言程序。



然后使用gcc进行编译，并用gdb进行调试。

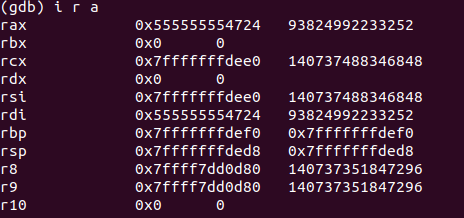
先在call\_ls函数入口处设置断点，反汇编。



接着在execve函数入口处设置断点，反汇编。



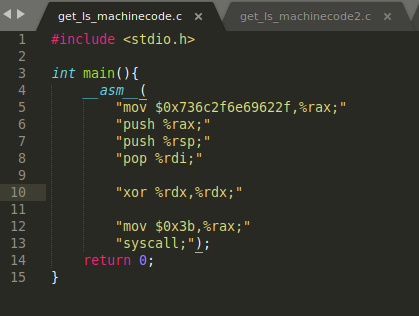
可以看到，将寄存器eax的值设置为0x3b后，进行系统调用syscall，此时查看寄存器的值。



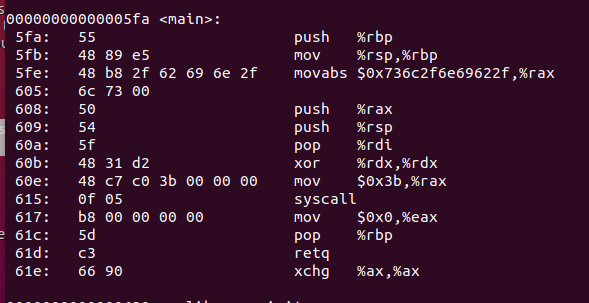


可以看到，此时，寄存器rdx内容为0，寄存器rdi指向字符串”/bin/ls”。

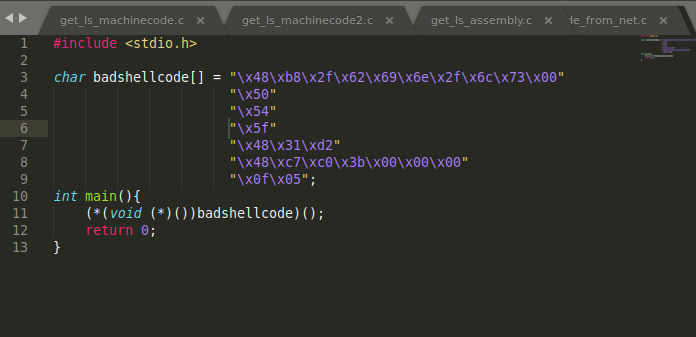
由此，可以写出如下汇编代码。



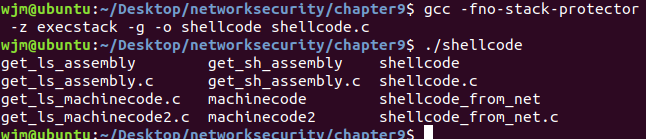
使用gcc进行编译，使用objdump反汇编。



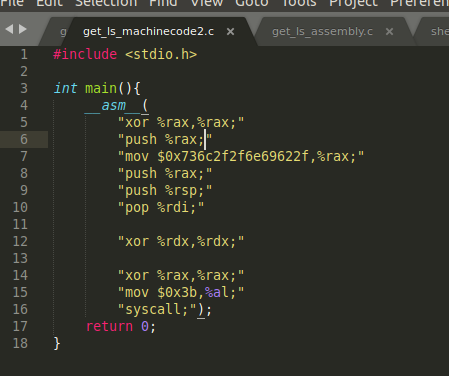
于是，写出如下文件。



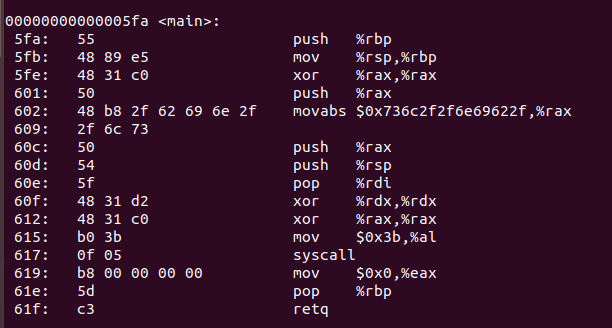
使用gcc编译，并执行，结果如下。



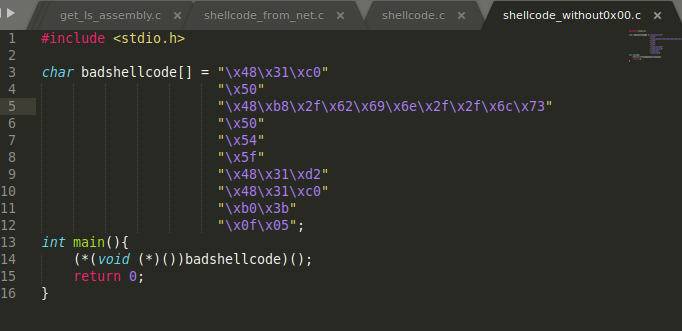
下面完善shellcode，将shellcode中的\x00去除。



使用gcc编译，objdump进行反汇编。



写出如下文件。



使用gcc编译，并运行，结果如下。

