

```
syswho.h (hdc ~/oslab/oslab/hdc/usr/include) - gedit
File Edit View Search Tools Documents Help
syswho.h iam.c
#define _LIBRARY_
#include <unistd.h>
_syscall1(int,iam,const char*,name)
_syscall2(int,whoami,char*,name,unsigned int,size)
```

```
iam.c (hdc ~/oslab/oslab/hdc/usr/root) - gedit
File Edit View Search Tools Documents Help
syswho.h iam.c
#include <syswho.h>
int main(int argc,char** argv)
{
    if(argc>1)
    {
        if(iam(argv[1])<0) return -1;
        else return -1;
        return 0;
    }
}
```

```
sudo who.c (~/oslab/oslab/linux-0.11/kernel) - gedit
File Edit View Search Tools Documents Help
who.c
#include <errno.h>
#include <asm/segment.h>
char userm[30];
extern int printk();
int sys_iam(const char* name)
{
    printk("now sys_iam is running\n");
    char* curp=name;int i=0;unsigned char count=0;
    while(*curp!='\0'){
        ++count;
    }
    if(count>23){
        printk("string is too long\n");
        errno=EINVAL;return -1;
    }
    else{
        curp=name;
        count=0;
        while(*curp!='\0'){
            userm[i]=get_fs_byte(curp);
            ++i;
            ++curp;
            ++count;
        }
        userm[i]=get_fs_byte(curp);//copy '\0'
        return count;
    }
}

int sys_whoami(char *name,unsigned int size){
    unsigned char Needcount=0;unsigned char i=0;
```

```
unistd.h (~/oslab/oslab/linux-0.11/include) - gedit
File Edit View Search Tools Documents Help
Create a new document
#define _NR_umask 59
#define _NR_umask 60
#define _NR_chroot 61
#define _NR_dup2 62
#define _NR_dup2 63
#define _NR_getppid 64
#define _NR_getpgid 65
#define _NR_setsid 66
#define _NR_sigaction 67
#define _NR_sgetmask 68
#define _NR_ssetmask 69
#define _NR_setreuid 70
#define _NR_setregid 71
#define _NR_iam 72
#define _NR_whoami 73
#define _syscall0(type,name) \
type name(void) \
{ \
    long __res; \
    __asm__ volatile ("int $0x80" \
        : "=a" (__res) \
        : "0" (_NR_#name)); \
    if (__res >= 0) \
        return (type) __res; \
    errno = -__res; \
    return -1; \
}

#define _syscall1(type,name,atype,a) \
type name(atype a) \
{ \
```

```
sys.h (~/oslab/oslab/linux-0.11/include/linux) - gedit
File Edit View Search Tools Documents Help
Create a new document
extern int sys_setpgid();
extern int sys_ulimit();
extern int sys_uname();
extern int sys_umask();
extern int sys_chroot();
extern int sys_dup2();
extern int sys_getpgid();
extern int sys_getppid();
extern int sys_setsid();
extern int sys_sigaction();
extern int sys_sgetmask();
extern int sys_ssetmask();
extern int sys_setreuid();
extern int sys_setregid();
extern int sys_iam();
extern int sys_whoami();

fn_ptr sys_call_table[] = { sys_setup, sys_exit, sys_fork, sys_read,
sys_write, sys_open, sys_close, sys_waitpid, sys_creat, sys_link,
sys_unlink, sys_execve, sys_chdir, sys_time, sys_mknod, sys_chmod,
sys_chown, sys_break, sys_stat, sys_lseek, sys_getpid, sys_mount,
sys_umount, sys_setuid, sys_getuid, sys_stime, sys_ptrace, sys_alarm,
sys_fstat, sys_pause, sys_ftime, sys_stty, sys_gtty, sys_access,
sys_nice, sys_ftime, sys_sync, sys_kill, sys_rename, sys_mkdir,
sys_rmdir, sys_dup, sys_pipe, sys_times, sys_prof, sys_brk, sys_setgid,
sys_getgid, sys_signal, sys_getuid, sys_getegid, sys_acct, sys_phys,
sys_lock, sys_ioctl, sys_fcntl, sys_mpx, sys_setpgid, sys_ulimit,
sys_uname, sys_umask, sys_chroot, sys_ustat, sys_dup2, sys_getppid,
sys_getpgrp, sys_setsid, sys_sigaction, sys_sgetmask, sys_ssetmask,
sys_setreuid, sys_setregid, sys_iam, sys_whoami };
```

```
system_calls.s (~/oslab/oslab/linux-0.11/kernel) - gedit
File Edit View Search Tools Documents Help
Create a new document
state = 0 # these are offsets into the task_struct.
counter = 4
priority = 4
signal = 12
sigaction = 16 # MUST be 16 (=len of sigaction)
blocked = (33*16)

# offsets within sigaction
sa_handler = 0
sa_mask = 4
sa_flags = 8
sa_restorer = 12

nr_system_calls = 74

/*
 * Ok, I get parallel printer interrupts while using the floppy for some
 * strange reason. Urgel. Now I just ignore them.
 */
.globl system_call,sys_fork,timer_interrupt,sys_execve
.globl hd_interrupt,floppy_interrupt,parallel_interrupt
.globl device_not_available, coprocessor_error

.align 2
bad_sys_call:
    movl $-1,%eax
    iret

reschedule:
    nopl $ret from sys_call
```

```
Bochs x86 emulator, http://bochs.sourceforge.net/
Options: apmbios pcibios eltorito rombios32
ata0 master: Generic 1234 ATA-6 Hard-Disk ( 60 MBytes)
Loading from Floppy...
Loading system ...
Partition table ok.
3947/62000 free blocks
19512/20066 free inodes
3454 buffers = 3536096 bytes buffer space
Free mem: 12582912 bytes
Ok.
[usr/root]# gcc -o iam iam.c
[usr/root]# gcc -o whoami whoami.c
[usr/root]# gcc testlab2 testlab2.c
[usr/local/lib/gcc-id: No such file or directory for testlab2
[usr/root]# ls
README hello.o linux-0.00 shoelace.tar.Z whoami.c
gcclib140 iam linux.tgz shoelab2.c whoami
hello iam.c mtools.howto shoe whoami.c
[usr/root]# gcc -o testlab2 testlab2.c
[usr/root]#
```

```
Bochs x86 emulator, http://bochs.sourceforge.net/
[usr/root]# ./iam audi
now sys_iam is running
[usr/root]# ./whoami
audi
[usr/root]# ./testlab2
now sys_iam is running
Test case 1:name = "x", length = 1...PASS
Test case 2:name = "sunner", length = 6...PASS
Test case 3:name = "Twenty-three characters", length = 23...PASS
Test case 4:name = "12345678900987654321234", length = 24...
ERROR: iam(): Bad errno 1. It should be 22(EINVAL).
Test case 5:name = "abdefghijklmnopqrstuvwxyz...", length = 26...
ERROR: iam(): Bad errno 1. It should be 22(EINVAL).
Test case 6:name = "Linus Torvalds", length = 14...PASS
Test case 7:name = "NULL", length = 0...PASS
Test case 8:name = "whoami(0xhalabala, 10)", length = 22...PASS
Final result: 40%
[usr/root]#
```

```
Bochs x86 Emulator 2.3.7
Build from CVS snapshot, on June 3, 2008
00000000000i[ ] reading configuration from ./bochs/bochsrc.bxrc
00000000000i[ ] installing x module as the Bochs GUI
00000000000i[ ] using log file ./bochsout.txt
```

1: 说几个比较坑的地方，其他的照着指导做就没问题。首先define LIBRARY\_ ,这个地方要尤其注意，是define