New System Call

Under Linux Kernel 4.x

Linux Kernel

- www.kernel.org

  linux-4.13.6.tar.xz

- uname -a

  Linux ubuntu 4.13.6 #2 SMP Tue Oct 24 22:36:32 PDT 2017 i686 i686 i686 GNU/Linux

Add New System Call – alcall with args

- Step 1)
- include/linux/syscalls.h
- 在文件

  #endif /* CONFIG_ARCH_HAS_SYSCALL_WRAPPER */

  之前，添加一行

  asmlinkage long sys_alcall(int cmd, char* buf);

Add New System Call – alcall with args

- Step 2)
- kernel/sys.c
- 在文件SYSCALL_DEFINE0(gettid)函数之后，添加如下行

```
SYSCALL_DEFINE2(alcall,int,cmd,char*,buf)
{
    struct task_struct *p;
    printk("Hello new system call alcall (%d,%x)!\n",cmd,buf);
    printk("%-20s %-6s %-6s\n","Name","Pid","Stat");
    for (p = &init_task; (p = next_task(p)) != &init_task;)
        printk("%-20s %-6d %-6ld\n",p->comm,p->pid,p->state);
    return 0;
}
```

Hint:
copy_to_user
copy_from_user
sprintf
strcpy
strcat
...

Add New System Call – alcall with args

- Step 3a)
  - arch/x86/entry/syscalls/syscall_32.tbl
  - 在文件 384 i386 arch_prctl sys_arch_prctl compat_sys_arch_prct

  行之后，添加如下行

  385 i386 alcall sys_alcall
- Step 3b)
  - arch/x86/entry/syscalls/syscall_64.tbl
  - 在文件 334 common rseq __x64_sys_rseq
- 行之后，添加如下行
- 335 common alcall __x64_sys_alcall

Add New System Call – alcall with args

- Step 4)
- 重新编译内核

  make clean

  make -j5

  sudo make modules_install

  sudo make install

Add New System Call – alcall with args

- Step 5) 编写用户态测试程序 testalcall.c

```
#include <unistd.h>
#include <sys/syscall.h>
#include <sys/types.h>
#include <stdio.h>
#define __NR_alcall     335
long alcall(int cmd, char* buf){
        return syscall(__NR_alcall,cmd,buf);
}
int main(int argc, char *argv[])
{
        int cmd;
        char buf[256];
        cmd=9;
        alcall(cmd,buf);
        printf("ok! run dmesg | grep alcall in terminal!\n");
        return 0;
}
```

Add New System Call – alcall with args

- Step 6)
- 编译用户态测试程序 testalcall.c， 并执行

```
gcc  -o testalcall   testalcall.c
./testalcall
$dmesg | grep alcall
[ 1648.215250] Hello new system call alcall!
```

Enhance New System Call (1) – alcall with args

- Tasks
  - 1.Get the count of processes from new sys call
  - 2.Get the list of all processes from new sys call

Enhance New System Call (2) – alcall with args

- Tasks
  - 3.copy srcfile to desfile in new sys call

linux/fs.h, asm/uaccess.h
strcut file*
get_fs()
filp_open(), vfs_read(),vfs_write(), filp_close()

```
struct file *file = NULL;
mm_segment_t old_fs;
char buf[128] = "123456";
file = filp_open("/data/test.txt", O_RDWR | O_APPEND | O_CREAT, 0644);
if (IS_ERR(file)) {
        return 0;
}
old_fs = get_fs();
set_fs(KERNEL_DS);
vfs_write(file, buf, sizeof(buf),  0);
set_fs(old_fs);
filp_close(file, NULL);
return 0;
```

End