ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

THÁI NHẬT TÂN – 18127204
TRẦN NGỌC BẢO TRÂN - 18127234

ĐỒ ÁN MÔN HỆ ĐIỀU HÀNH

|Đề tài|

KERNEL LINUX

|Giáo viên bộ môn|

ThS. Chung Thùy Linh

Thành phố Hồ Chí Minh – 2020

LỜI CẢM ƠN

Nhóm chúng em xin gửi lời cảm ơn chân thành nhất và sự tri ân sâu sắc đối với cô Chung Thùy Linh đã tạo điều kiện cho nhóm tìm hiểu và hoàn thành đồ án. Và nhóm cũng xin chân thành cảm ơn cô đã nhiệt tình hướng dẫn và giúp đỡ để nhóm hoàn thành tốt đồ án cuối kỳ.

Trong quá trình thực hiện, khó tránh khỏi những sai sót, rất mong cô có thể bỏ qua và góp ý để nhóm có thể rút kinh nghiệm cho những đồ án tiếp theo.

Chúng em chân thành cảm ơn !

1. Thông tin sinh viên

MSSV	Họ và tên
18127204	Thái Nhật Tân
18127234	Trần Ngọc Bảo Trân

2. Phân công chi tiết

Công việc	Thái Nhật Tân	Trần Ngọc Bảo Trân
Bài 1	x	
Bài 2		x

3. Đánh giá mức độ hoàn thành

- Mức độ hoàn thành: 100%
- Không có mục nào bị lỗi, không làm được

4. Mô tả tổ chức/ thiết kế của đồ án

- **Bài 1:**
  - Trong bài này, ta sẽ tạo 3 file. Đó là file RandomNumber.c và file TestRandomNumber.c và file Makefile
  - **File RandomNumber.c** :Dùng để tạo ra số ngẫu nhiên, cho phép các tiến trình ở user có thể open và read các số ngẫu nhiên. Trong file này gồm có những hàm chính sau:
    - **static int __init CharDev_init(void)** : hàm thực hiện công việc khởi tạo, đăng ký module drive
    - **static void __exit CharDev_exit(void)** : hàm thực hiện công việc hủy đăng ký, gỡ bỏ module drive
    - **static int my_open(struct inode *i, struct file *f)** : hàm thực hiện thao tác mở file thiết bị
    - **static int my_release(struct inode *i, struct file *f)** : hàm này được gọi khi đóng một thiết bị
    - **static ssize_t my_read(struct file *f, char* buffer, ssize_t len, loff_t *offset)** : hàm thực hiện thao tác đọc dữ liệu từ file thiết bị
    - **static struct file_operations fops ={**
      .open = my_open,
      .read = my_read,
      .release = my_release,

};

Trong hàm này, các thuộc tính sẽ nhận giá trị là tên các hàm sẽ được thực hiện tương ứng với các thao tác: mở, đóng, đọc, ghi

- **File TestRandomNumber.c** : Dùng để test chương trình
- **File Makefile** : File qui định cách thực thi lệnh make

- **Bài 2:**
- **asmlinkage long (*ref_sys_open)(const char __user *filename, int flags, umode_t mode);**
- **asmlinkage long (*ref_sys_write)(unsigned int fd, const char __user *buf, size_t count);**
  Hai hàm trên đóng vai trò các hàm tạm thời. Mục đích là để lưu lại địa chỉ mặc định trong system call table của hàm Open và Write
- **asmlinkage long new_sys_open(const char __user *filename, int flags, umode_t mode) :** Hàm này dùng để thay thế systemcall open
- **asmlinkage long new_sys_write(unsigned int fd, const char __user *buf, size_t count) :** Tương tự như hàm ở trên, hàm này cũng dùng để thay thế systemcall write
- **int make_rw(unsigned long address) :** Hàm này dùng để tắt thuộc tính read-only của system call table
- **int make_ro(unsigned long address) :** Hàm này dùng để bật thuộc tính read-only của system call table
- **static int __init entry_point(void) :** Hàm này khởi tạo khi hook syscall
- **static void __exit exit_point(void) :** Hàm dùng để thoát khi gỡ hook syscall

5. **Tất cả các test case có thể có**
   - Bài 1

```
[sv@localhost P1-s]$ su root
Password:
[root@localhost P1-s]# clear
[root@localhost P1-s]# make
make -C /lib/modules/2.6.32-71.el6.i686/build/ M=/home/sv/Desktop/P1-s modules
make[1]: Entering directory `/usr/src/kernels/2.6.32-71.el6.i686'
  CC [M]  /home/sv/Desktop/P1-s/RandomNumber.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/sv/Desktop/P1-s/RandomNumber.mod.o
  LD [M]  /home/sv/Desktop/P1-s/RandomNumber.ko.unsigned
  NO SIGN [M] /home/sv/Desktop/P1-s/RandomNumber.ko
make[1]: Leaving directory `/usr/src/kernels/2.6.32-71.el6.i686'
cc TestRandomNumber.c -o test
[root@localhost P1-s]# insmod RandomNumber.ko
[root@localhost P1-s]# gcc TestRandomNumber.c -o test
[root@localhost P1-s]# ./test
Read device
A received number is 0
[root@localhost P1-s]# ./test
Read device
A received number is 4294967194
[root@localhost P1-s]# ./test
Read device
A received number is 45
[root@localhost P1-s]# ./test
Read device
A received number is 100
[root@localhost P1-s]# ./test
Read device
A received number is 120
[root@localhost P1-s]# ./test
Read device
A received number is 80
[root@localhost P1-s]# ./test
Read device
A received number is 86
```

- Bài 2

```
[  863.941459] [WRITEHOOK]: Number of bytes in file name: 51
[  863.941525] [OPENHOOK]: Opening file name /etc/ld.so.cache
[  863.941547] [OPENHOOK]: Opening file name /lib/x86_64-linux-gnu/libc.so.6
[  863.941609] [WRITEHOOK]: Writing on file name Jun 19 23:43:37 ubuntu kernel:
[  863.723897] [WRITEHOOK]: Number of bytes in file name: 304
```

6. Hướng dẫn sử dụng các tính năng chương trình

- **Bài 1:**
  - Dùng lệnh ‘make’ để build chương trình

```
[root@localhost P1-s]# make
make -C /lib/modules/2.6.32-71.el6.i686/build/ M=/home/sv/Desktop/P1-s modules
make[1]: Entering directory `/usr/src/kernels/2.6.32-71.el6.i686'
  CC [M]  /home/sv/Desktop/P1-s/RandomNumber.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/sv/Desktop/P1-s/RandomNumber.mod.o
  LD [M]  /home/sv/Desktop/P1-s/RandomNumber.ko.unsigned
  NO SIGN [M] /home/sv/Desktop/P1-s/RandomNumber.ko
make[1]: Leaving directory `/usr/src/kernels/2.6.32-71.el6.i686'
```

  - Nạp driver vào nhân hệ thống sử dụng lệnh ‘insmod’

```
[root@localhost P1-s]# insmod RandomNumber.ko
```

  - Biên dịch file test TestRandomNumber.c

```
[root@localhost P1-s]# gcc TestRandomNumber.c -o test
```

- Chạy file test

```
[root@localhost P1-s]# ./test
Read device
A received number is 114
```

- Gỡ bỏ driver sử dụng lệnh 'rmmod'

```
[root@localhost P1-s]# rmmod RandomNumber
```

- **Bài 2:**
  - Tiến hành complie cho chương trình hook

```
admin2@ubuntu:~/Desktop/Test$ make
make -C /lib/modules/3.0.0-12-generic/build M=/home/admin2/Desktop/Test modules
make[1]: Entering directory `/usr/src/linux-headers-3.0.0-12-generic'
  Building modules, stage 2.
  MODPOST 1 modules
make[1]: Leaving directory `/usr/src/linux-headers-3.0.0-12-generic'
```

  - Gắn hook module

```
admin2@ubuntu:~/Desktop/Test$ sudo insmod Test.ko
[sudo] password for admin2:
```

  - Dùng lệnh dmesg để kiểm tra kết quả in ra

```
admin2@ubuntu:~/Desktop/Test$ dmesg
```

  - Một số kết quả

```
[  863.941459] [WRITEHOOK]: Number of bytes in file name: 51
[  863.941525] [OPENHOOK]: Opening file name /etc/ld.so.cache
[  863.941547] [OPENHOOK]: Opening file name /lib/x86_64-linux-gnu/libc.so.6
[  863.941609] [WRITEHOOK]: Writing on file name Jun 19 23:43:37 ubuntu kernel:
[  863.723897] [WRITEHOOK]: Number of bytes in file name: 304
```

  - Gỡ module và kết thúc

```
admin2@ubuntu:~/Desktop/Test$ sudo rmmod Test
admin2@ubuntu:~/Desktop/Test$
```

7. Các nguồn tài liệu tham khảo

- https://uwnthesis.wordpress.com/2016/12/26/basics-of-making-a-rootkit-from-syscall-to-hook/
- https://vimentor.com/vi/course/linux-kernel-basic
- https://sites.google.com/site/embedded247/ddcourse/device-drivers-phan-6-cac-thao-tac-doi-voi-file-thiet-bi