**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**

# 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 |

1. **Phân công chi tiết**

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

1. **Đánh giá mức độ hoàn thành**

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

1. **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

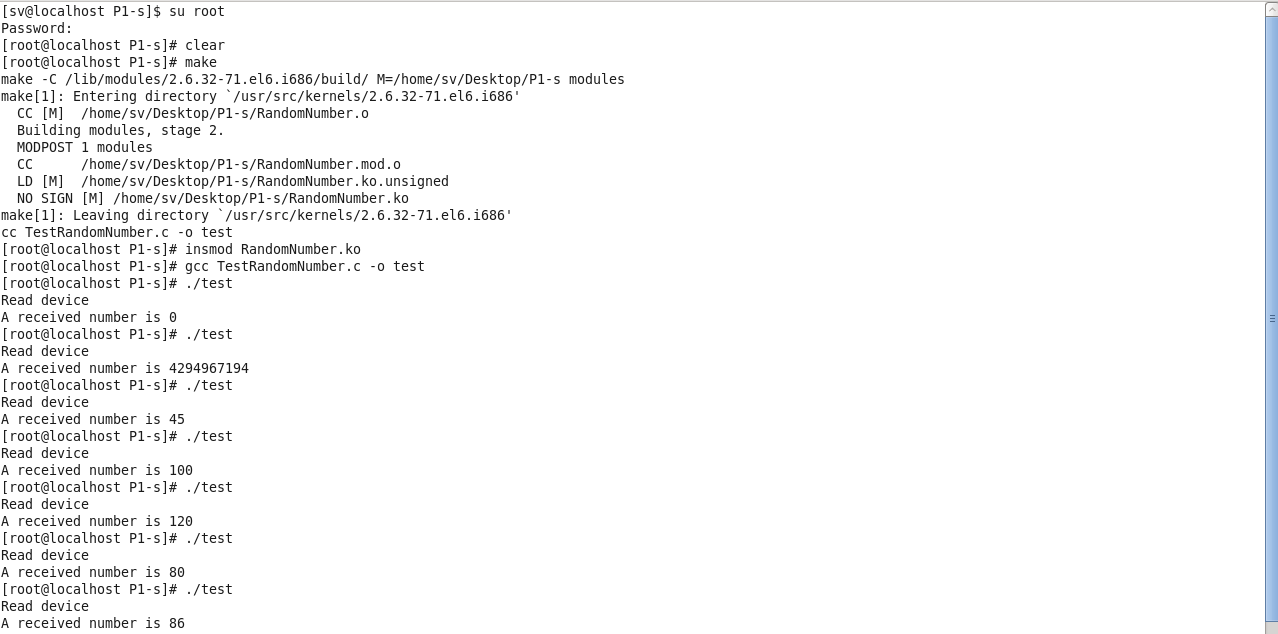
* **File TestRandomNumber.c** : Dùng để test chương trình
* **File Makefile** : File qui định cách thực thi lệnh make
* **Bài 2:**
* **asmlinkage long (\*ref\_sys\_open)(const char \_\_user \*filename, int flags, umode\_t mode);**
* **asmlinkage long (\*ref\_sys\_write)(unsigned int fd, const char \_\_user \*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

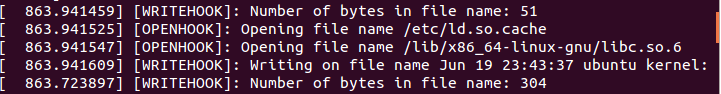
* **asmlinkage long new\_sys\_open(const char \_\_user \*filename, int flags, umode\_t mode) :** Hàm này dùng để thay thế systemcall open
* **asmlinkage long new\_sys\_write(unsigned int fd, const char \_\_user \*buf, size\_t count) :** Tương tự như hàm ở trên, hàm này cũng dùng để thay thế systemcall 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

1. **Tất cả các test case có thể có**

* Bài 1

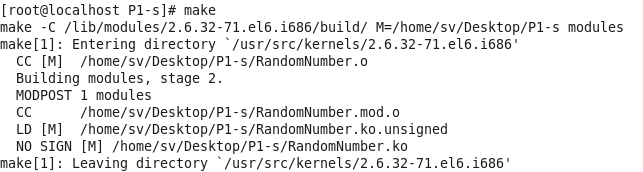
****

* Bài 2



1. **Hướng dẫn sử dụng các tính năng chương trình**

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



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



* + Biên dịch file test TestRandomNumber.c



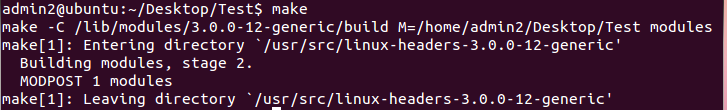
* + Chạy file test



* + Gỡ bỏ driver sử dụng lệnh ‘rmmod’



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



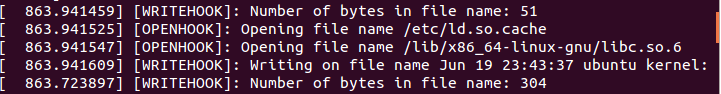
* + Gắn hook module



* + Dùng lệnh dmesg để kiểm tra kết quả in ra



* + Một số kết quả



* + Gỡ module và kết thúc



1. **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>