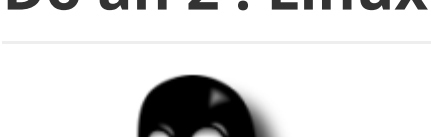
Hệ điều hành

Đồ án 2 : Linux Kernel 

Thực hiện bởi:

- Nguyễn Khánh Hoàng - MSSV: `1712457`
- Nguyễn Hữu Vinh - MSSV: `1712206`

Phần 1 (/KernelModule) : Mục tiêu hiểu về Linux kernel module và hệ thống quản lý file và device trong linux, giao tiếp giữa tiến trình ở user space và kernel space.

- Viết một module dùng để tạo ra số ngẫu nhiên.
- Module này sẽ tạo một character device để cho phép các tiến trình ở user space có thể open và read các số ngẫu nhiên

Linux Kernel Module - Random Number Generator Character Device Driver

Mã nguồn trong file **chardevdrv.c** dùng để biên dịch ra module là một character device driver, có chức năng cho phép các tiến trình ở user space mở và đọc một số ngẫu nhiên từ file thiết bị của device này.

Hướng dẫn sử dụng

1. Mở Terminal, gõ lệnh `make` , file chardevdrv.ko sẽ được tạo ra
2. Gõ lệnh `modinfo chardevdrv.ko` để xem thông tin của module
3. Gõ lệnh `sudo insmod chardevdrv.ko` để cài đặt module driver này
4. Gõ lệnh `lsmod | grep chardevdrv` để xem module đã được cài đặt thành công chưa
5. Để đọc một số ngẫu nhiên từ device này, ta dùng lệnh sau :

```
sudo dd if=/dev/randnum bs=4 count=1 | hexdump -C
```

> Lệnh trên đọc 4 byte từ file thiết bị `/dev/randnum` và xuất ra màn hình Terminal dưới dạng kí tự hexa (dùng lệnh `hexdump`). Chạy lệnh này nhiều lần, mỗi lần sẽ cho ra các kết quả ngẫu nhiên khác nhau.

6. Để gỡ module này, gõ lệnh `sudo rmmod chardevdrv`
7. Để dọn sạch các file được tạo ra trong thư mục trong quá trình biên dịch, gõ lệnh `make clean`

Phần 2 (/Hook) : Chương trình hook vào một system call:

- syscall `open` => ghi vào `dmesg` tên tiến trình mở file và tên file được mở
- syscall `write` => ghi vào `dmesg` tên tiến trình, tên file bị ghi và số byte được ghi

Hướng dẫn sử dụng:

1. Truy cập vào đường dẫn chứa mã nguồn:

```
$ cd <đường dẫn>
```

2. Sử dụng lệnh `make` để compile chương trình

```
$ make
```

3. Dùng `insmod` để hook syscall vào hệ thống

```
$ sudo insmod hookSyscall.ko
```

4. Dùng lệnh `dmesg` để kiểm tra (có thể gọi lệnh này trong terminal khác)

```
$ dmesg
```

hoặc có thể theo dõi liên tục bằng lệnh

```
$ dmesg -wH
```

5. Dùng lệnh `rmmod` để gỡ hook khỏi hệ thống

```
$ sudo rmmod hookSyscall
```