**BÁO CÁO ĐỒ ÁN 2**

**LINUX KERNEL MODULE**

**Bộ môn: Hệ điều hành**

1. **Thông tin thành viên nhóm:**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | MSSV | Họ tên | Ghi chú |
| 1 | 1712083 | Danh Phi Long | Nhóm trưởng |
| 2 | 1712121 | Nguyễn Tấn Phát |  |
| 3 | 1712452 | Lê Hận Thương Hoài |  |

1. **Bảng phân công công việc:**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | MSSV | Họ tên | Công việc |
| 1 | 1712083 | Danh Phi Long | Module + Hook |
| 2 | 1712121 | Nguyễn Tấn Phát | Readme |
| 3 | 1712452 | Lê Hận Thương Hoài | Report |

1. **Nội dung thực hiện đồ án:**
   1. **Ý tưởng thực hiện đồ án**

Phần 1: 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 tiền trình ở user space có thể open và read các số ngẫu nhiên

Phần 2: Chương trình hook vào một system call:

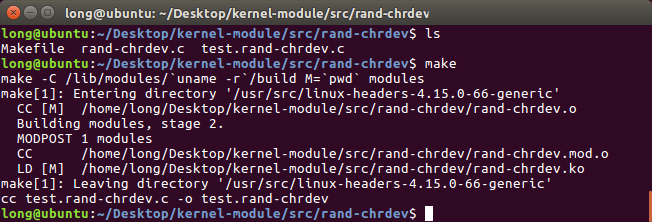
* syscall open => ghi vào dmesg tên tiến trình mở file và tên file được mở
* syscall write => ghi vào dmesg tên tiến trình, tên file bị ghi và số byte được ghi
  1. **Chức năng của chương trình**

**Thông tin phần mềm**

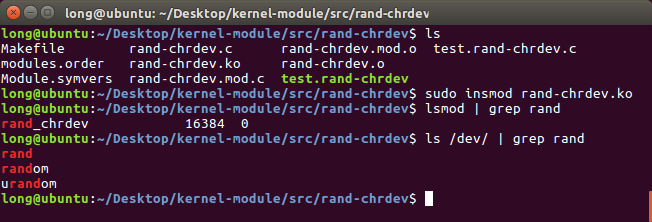
* Được viết bằng **C.**
* Source có chứa **Comments**.

**Demo**

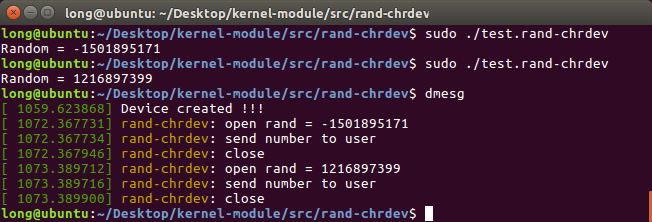
* Built and make file:

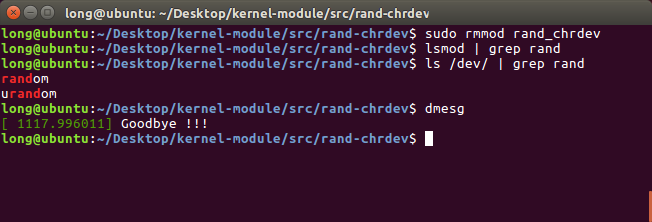
****

* Nạp module:

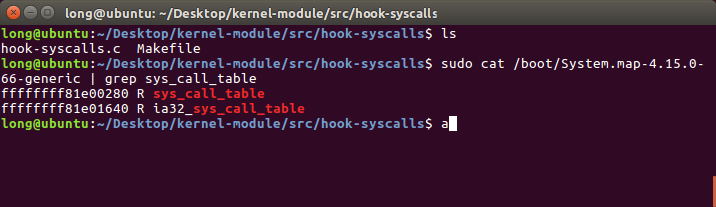
****

* Character device:

****

****

* Cách tìm sys\_table\_call thủ công:

****

* 1. **Đánh giá mức độ hoàn thành đồ án**

|  |  |  |
| --- | --- | --- |
| **STT** | **Chức năng** | **Mức độ hoàn thành** |
| 1 | Viết module dùng để tạo ra số ngẫu nhiên | 100% |
| 2 | Tạo một character device để cho phép các tiền trình ở user space có thể open và read các số ngẫu nhiên | 100% |
| 3 | Hook vào một system call | 100% |

1. **Tài liệu tham khảo**

*https://uwnthesis.wordpress.com/2016/12/26/basics-of-making-a-rootkit-from-syscall-to-hook*