

Nhóm tối đa 3 sv

Deadline:

Nộp bài: MSSV1_MSSV2_MSSV3.[zip|rar]

Bài nộp gồm:

- Mã nguồn
- Readme: hướng dẫn sử dụng + ghi chú
- Docs: mô tả tổ chức/thiết kế của đồ án

PROJECT 2

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 tiến 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

Link tham khảo <https://uwnthesis.wordpress.com/2016/12/26/basics-of-making-a-rootkit-from-syscall-to-hook>