PROJECT 2

Qui định

Nhóm tối đa 3 sinh viên
Bài nộp: MSSV1_MSSV2_MSSV3.zip gồm

1. Source code
2. Report: chứa báo cáo về bài làm của mình

- Thông tin sinh viên.
- Phân công chi tiết
- Đánh giá mức độ hoàn thành từ 0 – 100% (Chú thích rõ những mục làm được,chưa làm được và còn bị lỗi)
- Mô tả tổ chức/thiết kế của đồ án
- Tất cả các test case có thể có
- Hướng dẫn sử dụng các tính năng chương trình.
- Các nguồn tài liệu tham khảo.
- Không dán các đoạn source code của chương trình. Mã chương trình chỉ trình bày nếu thật sự cần thiết và nếu cần minh họa cho các mô hình cài đặt hay các cơ chế đồng bộ (minh họa dạng mã giả).

Lưu ý: Nếu làm không đúng những yêu cầu trên, bài làm sẽ không được chấm.

Đề bài

Phần 1: Mục tiêu là 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