# Đồ Án 3: Viết systemcall cho hệ thống và hook vào một system call có sẵn

Nhóm: tối đa 3 sinh viên Deadline: 3 tuần

# Yêu cầu: 1. Các bạn hãy cài đặt hai syscall duới đây:

## int pnametoid (char \*name)

Syscall này sẽ nhận vào name và trả về pid nếu tìm thấy và trả về -1 nếu không tìm thấy

## int pidtoname (int pid, char\* buf, int len)

Syscall này sẽ nhận vào pid, ghi process name vào trong biến buff với max len là len – 1 phần từ cuối cùng sẽ tự động thêm NULL Giá trị trả về là -1 nếu lỗi, 0 nếu len buffer truyền vào lớn hơn len của process name, và n với n là độ dài thật sự của process name, trong trường hợp len buffer chuyền vào nhỏ hơn len của proccess name.

# Yêu cầu 2: Hook vào 2 syscall dưới đây:

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