**Trường Đại học Khoa học Tự Nhiên**

Khoa Công nghệ thông tin

\*\*\*\*\*\*\*\*\*\*



**BÁO CÁO ĐỒ ÁN**

MÔN HỌC: HỆ ĐIỀU HÀNH

TÊN ĐỒ ÁN: VIẾT SYSTEMCALL CHO HỆ THỐNG VÀ HOOK VÀO MỘT SYSTEMCALL CÓ SẴN

Nhóm:

18120168 – Nguyễn Đại Dương

18120183 – Trần Quang Huy

TP.HCM, ngày 12 tháng 1 năm 2021

MỤC LỤC

[I. Thông tin thành viên nhóm 3](#_Toc61385674)

[II. Yêu cầu đồ án 3](#_Toc61385675)

[III. Phân chia công việc 3](#_Toc61385676)

[IV. Các bước thực hiện đồ án 3](#_Toc61385677)

[1. Cài đặt chuẩn bị để viết systemcall 3](#_Toc61385678)

[2. Hook syscall: 5](#_Toc61385679)

[V. Tài liệu tham khảo 7](#_Toc61385680)

# Thông tin thành viên nhóm

|  |  |  |
| --- | --- | --- |
| MSSV | Họ tên | Email |
| 18120168 | Nguyễn Đại Dương | daiduongnguyen168@gmail.com |
| 18120183 | Trần Quang Huy | 18120183@student.hcmus.edu.vn |

# Yêu cầu đồ án

* ***Yêu cầu 1: Cài đặt 2 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

# Phân chia công việc

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | **Dương** | **Huy** |
| Yêu cầu 1 | X |  |
| Yêu cầu 2 |  | X |

Mức độ hoàn thiện: 100%

1. **Các bước thực hiện đồ án**
2. Cài đặt chuẩn bị để viết systemcall

* Cài đặt các gói cần thiết cho việc biên dịch kernel:
* sudo apt-get install gcc
* sudo apt-get install libncurses5-dev
* sudo apt-get install bison
* sudo apt-get install flex
* sudo apt-get install libssl-dev
* sudo apt-get install libelf-dev
* sudo apt-get update
* sudo apt-get upgrade
* Download kernel 4.4.2

wget https://mirrors.edge.kernel.org/pub/linux/kernel/v4.x/linux-4.4.2.tar.gz

* Giải nén vào thư mục **usr/src**

sudo tar –xvf linux-4.4.2.tar.xz –C /usr/src/

* Sửa Make file trong linux-4.4.2

sudo gedit Makefile

* Tìm dòng: core-y += kernel/ mm/ fs/ ipc/ security/ crypto/ block/

Sửa thành:

core-y += kernel/ mm/ fs/ ipc/ security/ crypto/ block/ pidtoname/ pnametoid/

* Tạo thư mục pidtoname và pnametoid trong linux-4.4.2 (chứa source code cho system call sẽ định nghĩa)

sudo mkdir pidtoname pnametoid

* Định nghĩa mã cho systemcall mới

Sửa file syscall\_64.tbl

* cd /urs/src/linux-4.4.2/arch/x86/entry/syscalls/
* sudo gedit syscall\_64.tbl

Thêm vào cuối file

* 400 64 pnametoid sys\_pnametoid
* 401 64 pidtoname sys\_pidtoname
* Định nghĩa hàm trong systemcall header file

Sửa file syscalls.h (thêm vào cuối trước #endif)

* cd /usr/src/linux-4.4.2/include/linux
* sudo gedit syscalls.h

Thêm vào cuối trước #endif:

* *asmlinkage long sys\_pnametoid(char\* name);*
* *asmlinkage long sys\_pidtoname(int pid, char\* buf, int len);*
* Biên dịch lại kernel
* sudo make menuconfig (save, không cần thiết setup them)
* sudo make -j4 && sudo make modules\_install module
  1. Sau khi chạy xong reboot. Khi khởi động vào Ubuntu, hệ điều sẽ tự động bật kernel-4.4.2
* Test systemcall: (Trong thư mục Test)
* make
* Kết quả chạy test:

Text

Description automatically generated

* 1. Hook syscall:

1. Cài đặt:

Để thực hiện hook ta cần tìm địa chỉ sys\_call\_table:

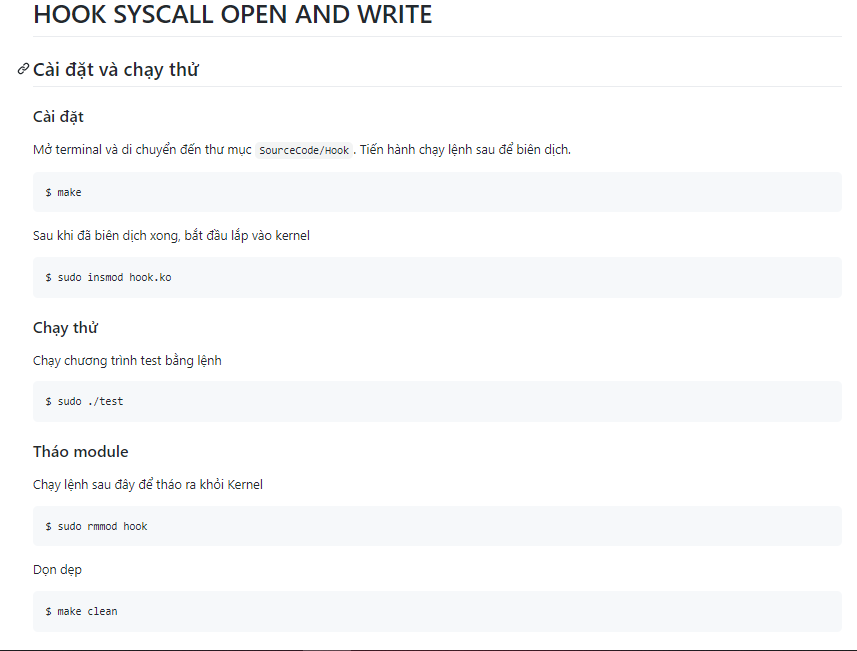
**grep -w sys\_call\_table /boot/System.map-$(uname -r)**

Địa chỉ này được copy vào phần init để hook. Trong phần cài đặt của nhóm, việc tìm địa chỉ này đã đưọc thực hiện tự động.

Cách thực hiện hook được mô tả như sau:

* Bước 1: Tìm địa chỉ sys\_call\_table
* Bước 2: Lấy địa chỉ của syscall open và write
* Bước 3: Tắt lớp bảo vệ syscall
* Bước 4: Thay syscall open và write bằng hàm hook của mình
* Bước 5: Hàm hook thực hiện các công việc
* Bước 6: Khi xong việc, trả lại syscall ban đầu cho hệ thống và bật lại lớp bảo vệ syscall

1. Test:



Text

Description automatically generated

# Tài liệu tham khảo

[Github @84436](https://github.com/84436/OS-Project-02)

[Github @nguyentathung943](https://github.com/nguyentathung943/Systemcall_and_Hook)

[The Linux Kernel Module Programming Guide - System Calls](http://www.iitk.ac.in/LDP/LDP/lkmpg/2.4/html/x939.html)

[Hacking Rootkit Development 10 - Hooking Syscall Open](https://www.youtube.com/watch?v=qFA3kFj4uwY)