

Trường : Đại học Khoa học Tự nhiên Tp.HCM

Khoa : Công nghệ thông tin

Môn : Hệ điều hành

12/9/2018

System call và Hook

Sinh viên:

ĐOÀN QUANG TUẤN

1612780

LÊ HOÀNG SANG

1612554

I. Mở đầu.

1. Giới thiệu đề án

- Viết syscall cho hệ thống
- Hook vào một system call có sẵn

2. Giới thiệu nhóm

Nhóm gồm 2 thành viên:

STT	MSSV	Tên	Email
1	1612780	Đoàn Quang Tuấn	1612780@student.hcmus.edu.vn
2	1612554	Lê Hoàng Sang	1612554@student.hcmus.edu.vn

3. Kết quả

Viết và chạy thành công 2 system call:

- pnametoid: nhập vào tên tiến trình, trả về PID
- pidtoname: nhập vào PID, trả về tên tiến trình

Hook thành công vào 2 syscall của kernel có sẵn:

- open(): ghi vào dmesg tên tiến trình nào mở file và tên file mở
- write(): ghi vào dmesg tên tiến trình, tên file bị ghi và số byte được ghi

4. Hệ thống sử dụng

Ubuntu 12.04 LTS

Linux kernel 3.16.36

II. Nội dung.

1. Viết system call cho hệ thống

1.1. Cách triển khai một system call trong linux (pnametoid, pidtoname)

- Tải linux kernel cho hệ điều hành và giải nén vào thư mục /usr/src/:

`wget https://www.kernel.org/pub/linux/kernel/v3.x/linux-3.16.36.tar.xz`

`tar -xvf linux-3.16.36.tar.xz -C /usr/src/`

- Di chuyển vào thư mục /usr/src/linux-3.16.36:

`cd /usr/src/linux-3.16.36`

- Tạo thư mục pname (pid) và di chuyển vào thư mục đó:

`mkdir pname`

`(mkdir pid)`

- Tạo file nametoid.c (idtoname.c) và viết hàm pnametoid() (pidtoname()):

`gedit nametoid.c`

`(gedit idtoname.c)`

Nội dung: (tệp đính kèm)

linux-3.16.36/pname/nametoid.c

linux-3.16.36/pid/idtoname.c

- Tạo file nametoid.h (idtoname.h):

`gedit nametoid.h`

`(gedit idtoname.h)`

Nội dung: (tệp đính kèm)

linux-3.16.36/pname/nametoid.h

linux-3.16.36/pid/idtoname.h

- Tạo file Makefile:

`gedit Makefile`

Nội dung: (tệp đính kèm) Makefile

linux-3.16.36/pname/Makefile

linux-3.16.36/pid/Makefile

`obj-y := nametoid.o`

`obj-y := idtoname.o`

- Trở về thư mục /usr/src/linux-3.16.36 và mở file Makefile:

`cd ..`

cat -n Makefile | grep -i core-y

nano +(line number from the cat command here) Makefile

- Sửa file Makefile:

Thêm /nametoid (/idtoname) vào cuối dòng *core-y += kernel/ mm/ fs/ ipc/ security/ crypto/ block/*

Nội dung: (tệp đính kèm)

linux-3.16.36/Makefile

core-y += kernel/ mm/ fs/ ipc/ security/ crypto/ block/ nametoid/ idtoname

- Thêm system call nametoid (idtoname) vào system call table:

gedit arch/x86/syscalls/syscall_64.tbl

Nội dung: (tệp đính kèm)

linux-3.16.36/ arch/x86/syscalls/syscall_64.tbl

318 common nametoid pnametoid

319 common idtoname pidtoname

(318, 319 là các số dùng để gọi syscall từ userspace. Các số này chưa tồn tại trong bảng syscall của file syscall_64.tbl.)

- Thêm prototype của system call vào cuối file include/linux/syscalls.h (trước dòng #endif):

gedit include/linux/syscalls.h

Nội dung: (tệp đính kèm) syscalls.h

asmlinkage int pnametoid(char process_name);*

asmlinkage int pidtoname (int pid, char buf, int len);*

- Tiến hành biên dịch kernel:

make menuconfig

Chọn save, rồi exit.

make

- Cài đặt kernel mới được biên dịch:

make install

make modules_install install

- Khởi động lại máy:

reboot

(Nhấn giữ phím Shift để chọn kernel vừa biên dịch)

- Tạo và viết file test cho system call - testPnametoid.c (testPidtoname.c):

Nội dung: (tệp đính kèm)

linux-3.16.36/test/testPnametoid.c

linux-3.16.36/test/testPidtoname.c

- Biên dịch file test:

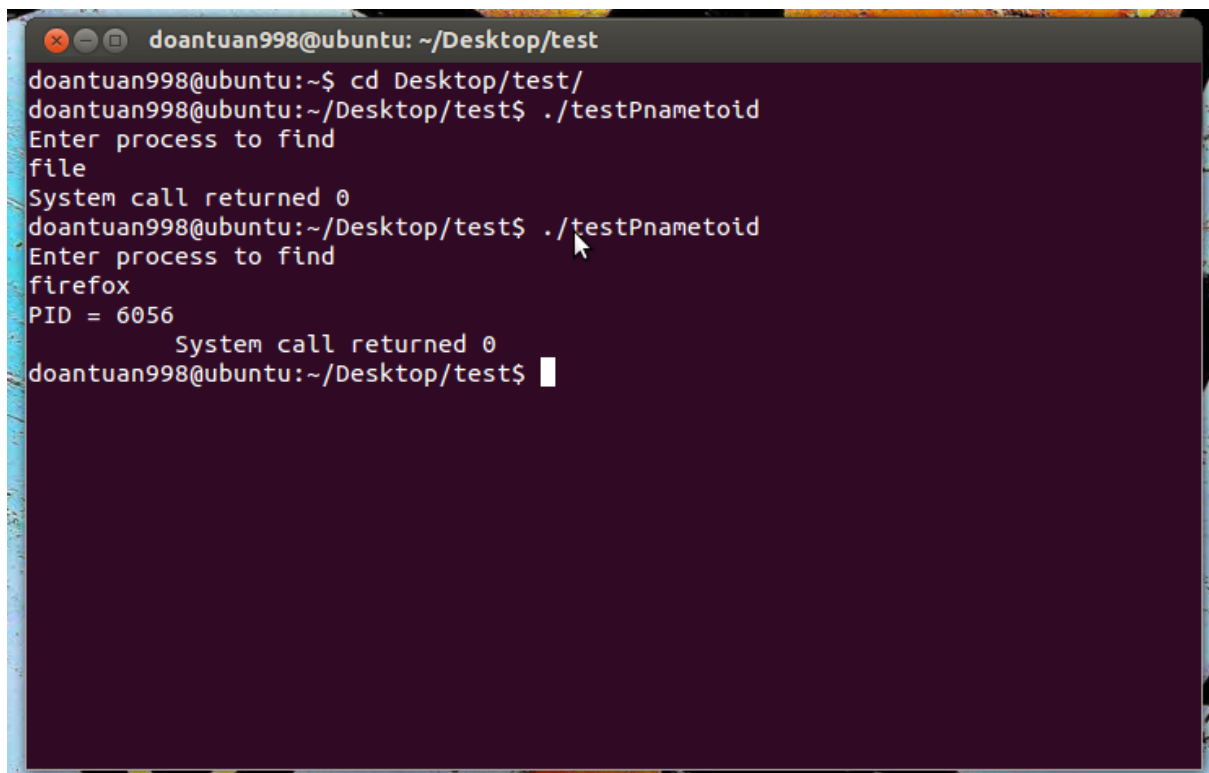
gcc testPnametoid.c -o testPnametoid

gcc testPidtoname.c -o testPidtoname

- Chạy file test:

./testPnametoid

./testPidtoname



```
doantuan998@ubuntu: ~/Desktop/test
doantuan998@ubuntu:~$ cd Desktop/test/
doantuan998@ubuntu:~/Desktop/test$ ./testPnametoid
Enter process to find
file
System call returned 0
doantuan998@ubuntu:~/Desktop/test$ ./testPnametoid
Enter process to find
firefox
PID = 6056
System call returned 0
doantuan998@ubuntu:~/Desktop/test$
```

```
doantuan998@ubuntu: ~/Desktop/test
doantuan998@ubuntu:~/Desktop/test$ ./testPidtoname
Enter process ID to find
6056
Process name: firefox
System call returned 0
doantuan998@ubuntu:~/Desktop/test$
```

1.2. Mã nguồn

Danh sách các file được tạo mới và chỉnh sửa:

```
doantuan998@ubuntu: ~/Desktop
linux-3.16.36/
├── arch
│   └── x86
│       └── syscalls
│           └── syscall_64.tbl
├── include
│   └── linux
│       └── syscalls.h
├── Makefile
├── pid
│   ├── idtoname.c
│   ├── idtoname.h
│   ├── idtoname.o
│   └── Makefile
├── pname
│   ├── Makefile
│   ├── nametoid.c
│   ├── nametoid.h
│   └── nametoid.o
└── test
    ├── testPidtoname
    ├── testPidtoname.c
    ├── testPidtoname.c~
    ├── testPnametoid
    ├── testPnametoid.c
    └── testPnametoid.c~

8 directories, 17 files
doantuan998@ubuntu:~/Desktop$ ^C
doantuan998@ubuntu:~/Desktop$
```

2. Hook vào một system call có sẵn

2.1. Tạo hook

- Tìm địa chỉ của syscall table bằng lệnh:

cat /boot/System.map-3.16.36 | grep sys_call_table

- Tạo thư mục hook và di chuyển vào đó:

mkdir hook

cd hook

- Tạo file hook.c:

sudo gedit hook.c

Nội dung: (file đính kèm)

hook/hook.c

- Tạo file Makefile:

sudo gedit Makefile

Nội dung: (file đính kèm)

hook/Makefile

- Biên dịch:

make

- Nạp module vào kernel:

insmod hook.ko

- Mở file để test:

- Tháo module ra khỏi kernel:

rmmod hook.ko

- Kiểm tra (terminal mới):

dmesg -wH

2.2. Mã nguồn

```
root@ubuntu: ~  
doantuan998@ubuntu:~/Desktop/test$ ./testPidtoname  
Enter process ID to find  
6056  
Process name: firefox  
System call returned 0  
doantuan998@ubuntu:~/Desktop/test$ sudo su  
[sudo] password for doantuan998:  
root@ubuntu:/home/doantuan998/Desktop/test# cd  
root@ubuntu:~# tree hook  
hook  
├── hook.c  
├── hook.c~  
├── hook.ko  
├── hook.mod.c  
├── hook.mod.o  
├── hook.o  
├── Makefile  
├── modules.order  
└── Module.symvers  
  
0 directories, 9 files  
root@ubuntu:~#
```


Tài liệu tham khảo

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

<https://medium.freecodecamp.org/building-and-installing-the-latest-linux-kernel-from-source-6d8df5345980>

https://medium.com/@ssreehari/implementing-a-system-call-in-linux-kernel-4-7-1-6f98250a8c38?fbclid=IwAR0W5EUNbPX8IsBCQPRjRd0DFUBtGc3qLopxHXXymZA_BV3h-E0EW57SMZE