****

**BÁO CÁO ĐỒ ÁN 2:**

***Systemcall-Hook***

*Sinh viên thực hiện:*

*Lê Hồng Quang-18127190*

*Nguyễn Đình Thảo-18127219*

Các cài đặt cần thiết:

* Trên Terminal gõ uname -r để kiểm tra phiên bản : 3.13.0-32-generic
* Cài đặt các gói cần thiết cho việc biên dịch kernel:

sudo apt-get install libncurses5-dev libncursesw5-dev

sudo apt-get install libssl-dev

sudo apt-get install libelf-dev

sudo apt-get install bison

sudo apt-get install flex

sudo apt-get install bc

sudo apt-get install perl

-Sử dụng gói phù hợp với phiên bản (phiên bản ubuntu 12.04 LTS)

wget <https://mirrors.edge.kernel.org/pub/linux/kernel/v3.x/linux-3.13.9.tar.xz>

-Giải nén thư mục:

sudo tar -xvf linux-3.13.9.tar.xz -C /usr/src/

-Di chuyển vào thư mục:

cd /usr/src/linux-3.13.9

1. Viết Systemcalls:
2. **int pnametoid (char \*process\_name)**

-Tạo thư mục pnametoid và di chuyển vào thư mục đó:

sudo mkdir pnametoid

cd pnametoid

sudo gedit pnametoid.c

sudo gedit pnametoid.h

sudo gedit Makefile

-Trở về thư mục trước đó

cd ..

sudo gedit Makefile

Sử dung cộng cụ Tìm đến dòng

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

Bổ sung them khoảng trắng và pnametoid/ vào cuối dòng

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

- Thêm system call pnametoid vào system call table:

sudo gedit arch/x86/entry/syscalls/syscall\_64.tbl

350 common pnametoid sys\_pnametoid

-Thêm systemcall mới vào systemcall header file trước #endif:

sudo gedit include/linux/syscalls.h

asmlinkage int sys\_pnametoid(char\* process\_name);

1. **int pidtoname (int pid, char\* buf, int len)**

-Tạo thư mục pidtoname và di chuyển vào thư mục đó:

sudo mkdir pidtoname

cd pidtoname

sudo gedit pidtoname.c

sudo gedit pidtoname.h

sudo gedit Makefile

-Trở về thư mục trước đó

cd ..

sudo gedit Makefile

Sử dung cộng cụ Tìm đến dòng

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

Bổ sung them khoảng trắng và pidtoname/ vào cuối dòng

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

- Thêm system call pnametoid vào system call table:

sudo gedit arch/x86/entry/syscalls/syscall\_64.tbl

355 common pidtoname sys\_pidtoname

-Thêm systemcall mới vào systemcall header file trước #endif:

sudo gedit include/linux/syscalls.h

asmlinkage int sys\_pidtoname (int pid, char\* buf, int len);

\*Biên dịch mã nguồn

sudo make menuconfig: save->ok->exit

sudo make

sudo make modules\_install install

-Sau khi biên dịch , cần restart máy lại để cập nhật bản kernel vừa build:reboot

-Nhấn giữ Shift trái để chọn phiên bản kernel linux-3.13.9

\*Viết file test cho systemcall:

cd /Desktop

sudo mkdir test

cd test

sudo gedit testpname.c

sudo gedit testpid.c

\*Biên dịch file test:

gcc testname.c -o testpname

gcc testid.c -o testpid

Chạy file test: ./testname ./testid

1. Viết Hook:

* Tìm địa chỉ bảng syscall

cat /boot/System.map-3.13.9 | grep sys\_call\_table

-cd /Desktop

-mkdir hook

-cd hook

sudo gedit hook.c

sudo gedit Makefile

-Biên dịch

sudo make

-Nạp module vào kernel

insmod hook.ko

-Bây giờ hãy mở một teminal khác, gõ lệnh sau để xóa dmesg và sau đó đọc tail output của nó sau khi bạn insert module và chạy testpname hoặc testpid

Dmesg -C

./testpname hoặc ./testpid

-rmmod hook.ko

Dmesg -wH

Đánh giá bài làm

|  |  |  |
| --- | --- | --- |
| MSSV | Phân công | Mức độ hoàn thành |
| 18127190 | Viết 2 system call và hook | 100% |
| 18127219 | Viết báo cáo | 100% |

Tài liệu tham khảo:

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

file hướng dẫn của giáo viên