BÁO CÁO ĐỒ ÁN 2

Nguyễn Trần Hậu - MSSV 1612180

Nguyễn Chí Thức - MSSV 1612677

1/12/2018

Tóm tắt nội dung

Hướng dẫn build syscall và hook trong Linux. Nhóm em sử dụng distro Debian bản 8 dành cho 32bit với kernel bản 3.16.61 để thực hiện đồ án này.

1 Syscall

Để tạo một syscall trong hệ điều hành Linux:
→ Cần phải lấy source của kernel
→ Thêm syscal vào source
→ Build kernel từ source vừa chỉnh sửa
→ Boot distro Linux bằng kernel vừa build.

1.1 Chuẩn bị source

Trong thư mục nộp bài có thư mục *src*. Trong thư mục *src*, có 3 thư mục con là *hook*, *syscall*, và *test_syscall*

Down kernel source về, rồi giải nén vào */urs/src/*

```
wget https://cdn.kernel.org/pub/linux/kernel/v3.x/
   linux-3.16.61.tar.xz
sudo tar -xvf linux-3.16.61.tar.xz -C /usr/src/
```

Copy thư mục *pidtoname* và *pnametoid* trong thư mục *syscall* vào thư mục kernel source vừa giải nén. Đây là 2 syscall để thêm vào kernel.

Thêm vào cuối dòng *core-y* trong file *Makefile* của thư mục kernel source tên của 2 syscall như sau

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

Vào thư mục *arch/x86/syscalls/* của thư mục kernel source và thêm vào cuối file *syscall_32.tbl*

```
xxx i386 pnametoid sys_pnametoid
yyy i386 pidtoname sys_pidtoname
```

lấy số của dòng cuối cùng trong file *syscall_32.tbl*, cộng 1 ra xxx, cộng tiếp cho 1 ra yyy

Vào thư mục *include/linux/* của thư mục kernel source và thêm vào cuối file *syscalls.h*

```
asmlinkage int sys_pnametoid(char *name);
asmlinkage int sys_pidtoname(int pid, char *buf, int
    len);
```

1.2 Build và cài đặt kernel

Quay lại thư mục kernel source, build kernel

```
sudo make menuconfig
sudo make
```

Sau khi build thành công, cài đặt kernel mới rồi khởi động lại máy

```
sudo make modules_install install
sudo reboot
```

1.3 Test

Vào thư mục *test_syscall* trong thư mục *src*, chạy test

```
make test_pnametoid
make test_pidtoname
```

2 Hook

Hook là một kernel module, thay đổi syscall của hệ điều hành bằng syscall định nghĩa sẵn trong hook.
Trong hook module:
Lúc *init_module*, thay syscall cũ bằng syscall mới trong syscall table
Lúc *exit_moduel*, thay syscall mới bằng syscall cũ trong syscall table

Vào thư mục *hook* trong thư mục *src*, build hook

```
make
```

Sau khi build hook thành công, cài đặt hook là kernel module vào hệ điều hành

```
sudo insmod hook_module.ko
```

Để kiểm tra hook hoạt động, vào *dmesg* để đọc log.

Tài liệu

[1] Basics of Making a Rootkit: From syscall to hook!
`https://uwnthesis.wordpress.com/2016/12/26/basics-of-making-a-rootkit-from-syscall-to-hook/`

[2] Linux kernel articles
`https://blog.guillaume-gomez.fr/Linux-kernel/1/1`