

운영체제

Assignment2

김태석 교수님

2019202103

이은비

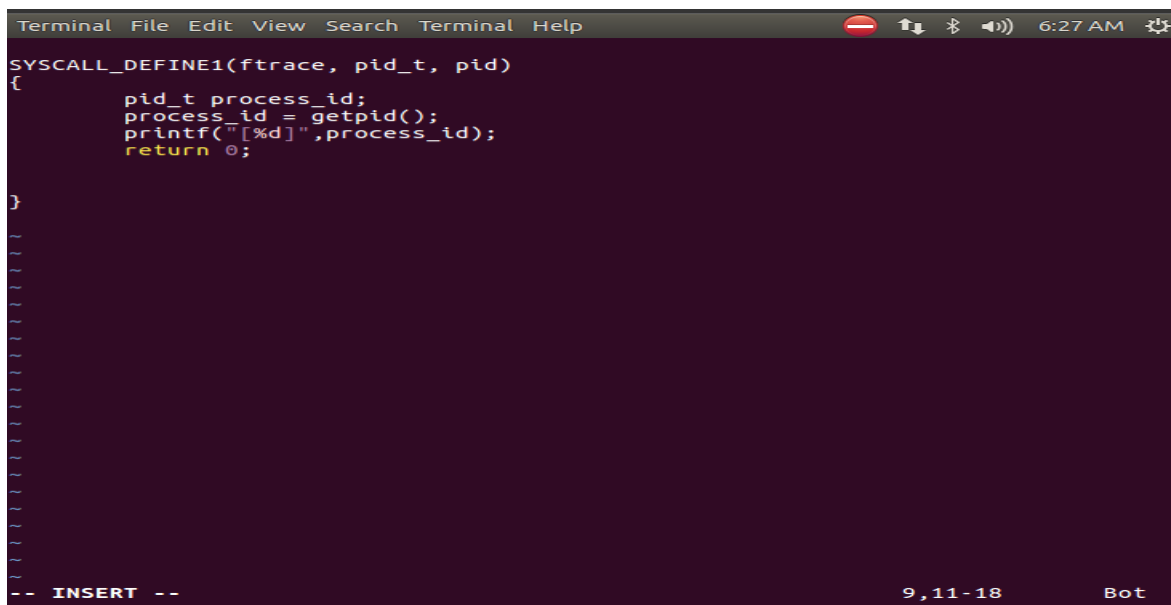
## <introduction>

ftrace라는 이름의 특정 pid에 대하여 파일에 관한 시스템 콜을 추적하는 툴을 작성합니다. 새로 ftrace라는 시스템콜을 등록하고 이미 시스템콜에 존재하는 open,read,write,lseek,close 원형을 찾아서 hijack하여서 kernel module(ftracehooking.c,iotracehooking.c)를 통해서 hooking한뒤 테스트 하기 위한 새롭게 txt파일을 만들어 앞서 언급한 open,read...와 같은 작업을 수행 후 dmesg로 결과를 확인 합니다.

## <conclusion>

먼저 강의 5주차에서의 실습을 참고하여서 ftrace라는 새로운 syscall을 작성합니다. Syscall table에 336번이라는 시스템콜 번호에 작성하고 syscall함수 구현을 위해 ftrace디렉터리 안의 ftrace.c에 매크로를 이용하여 시스템콜을 생성하도록 합니다. 이후 수정된 커널을 컴파일하고 syscall을 테스트 합니다.

<ftrace.c>



```
Terminal File Edit View Search Terminal Help
SYSCALL_DEFINE1(ftrace, pid_t, pid)
{
    pid_t process_id;
    process_id = getpid();
    printf("[pid]", process_id);
    return 0;
}
-- INSERT -- 9,11-18 Bot
```

이후에 ftracehooking.h을 만든 후 ftracehooking.c와 iotracehooking.c에서 사용하는 header를 모두 include합니다. 강의자료에 나와있는 header4개와 더불어 그외의 것들을 references를 참고하여 추가 합니다.



System call 추적 테스트를 위한 프로그램 실행을 위해 임의의 txt파일을 작성합니다.

```
os2019202103@ubuntu:~/Downloads/linux-4.19.67/ftrace$ cat abc.txt
HELLO WORLD
GOOD BYE
```

컴파일을 따로 한 후 테스트 프로그램을 실행합니다. dmesg로 결과를 확인합니다.

```
[ 13.811697] audit: type=1400 audit(1635312108.250:6): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/NetworkManager/nm-dhcp-helper" pid=604 comm="apparmor_parser"
[ 13.811706] audit: type=1400 audit(1635312108.250:7): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/connman/scripts/dhclient-script" pid=604 comm="apparmor_parser"
[ 13.829333] piix4_smbus 0000:00:07.3: SMBus Host Controller not enabled!
[ 13.902041] audit: type=1400 audit(1635312108.338:8): apparmor="STATUS" operation="profile_load" profile="unconfined" name="webbrowser-app" pid=609 comm="apparmor_parser"
[ 13.902049] audit: type=1400 audit(1635312108.338:9): apparmor="STATUS" operation="profile_load" profile="unconfined" name="webbrowser-app//oxide_helper" pid=609 comm="apparmor_parser"
[ 13.975437] random: crng init done
[ 13.975446] random: 7 urandom warning(s) missed due to ratelimiting
[ 14.072937] audit: type=1400 audit(1635312108.510:10): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/snapd/snap-confine" pid=626 comm="apparmor_parser"
[ 14.072947] audit: type=1400 audit(1635312108.510:11): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/snapd/snap-confine//mount-namespace-capture-helper" pid=626 comm="apparmor_parser"
[ 14.077692] Bluetooth: Core ver 2.22
[ 14.077723] NET: Registered protocol family 31
[ 14.077731] Bluetooth: HCI device and connection manager initialized
[ 14.077741] Bluetooth: HCI socket layer initialized
[ 14.077750] Bluetooth: L2CAP socket layer initialized
[ 14.077762] Bluetooth: SCO socket layer initialized
[ 14.226212] usbcore: registered new interface driver btusb
[ 14.260513] cryptd: max_cpu_glen set to 1000
[ 14.292028] AVX2 version of gcm_enc/dec engaged.
[ 14.292036] AES CTR mode by8 optimization enabled
[ 14.549188] Adding 998396k swap on /dev/sda5. Priority:-2 extents:1 across:998396k FS
```

## <고찰>

처음 ftrace.c를 컴파일하고 test프로그램을 진행 하였을때 자료형을 잘못 선언하여 그 값이 0이 아닌 -1이 나와 다시 수정하고 재 컴파일하는 과정을 거쳤습니다.

iotracehooking.c에서 원래 찾은 시스템 콜의 원형은 vi include/linux/syscalls.h에서 패턴 찾기로 찾아asm linkage long sys\_lseek(unsigned int fd, off\_t offset, unsigned int whence);같은 형태여서 asm linkage int ftrace(const struct pt\_regs \*regs)와 아래 struct pt\_regs \*regs를 추가하여 작성 하려고 하였으나 잘 이해가 되지 않아 다시 vi arch/x86/entry/syscalls/syscall\_64.tbl에서 시스템콜 번호를 확인 하고 이후에 \_\_syscall\_definex(num,name,자료형,변수..)의 형태로 바꾸었습니다.

ftracehooking.c와 iotracehooking.c 에서 구조정도만 작성하고 각각의 sub syscall에서 context를 제대로 작성하지 못했습니다.

## <references>

시스템콜 추가하기 /<https://pr0gr4m.tistory.com/entry/Linux-Kernel-5-systemcall-%EC%B6%94%EA%B0%80%ED%95%98%EA%B8%B0>