운영체제

Assignment 2

최상호 교수님 수업
학번: 2020603037
이름: 채 규성

Assignment2

Introduction:

이 문제는 특정 pid 값을 매개로 해당 프로세스가 동작할 때 파일에 관한 시스템 콜을 추적하고 그 과정에 대한 요약을 출력하는 추적 함수들을 만들어 구현하는 문제이다. 문제의 각 스텝을 보아 요구하는 사항을 추려보면 다음과 같다고 할 수 있겠다.

1. 새로운 시스템 콜을 만들 수 있는가
2. 기존 시스템 콜을 hooking하고 커널 모듈에서 실행할 수 있는가
3. 커널 로그 메시지를 출력할 수 있는가

Conclusion & Analysis:

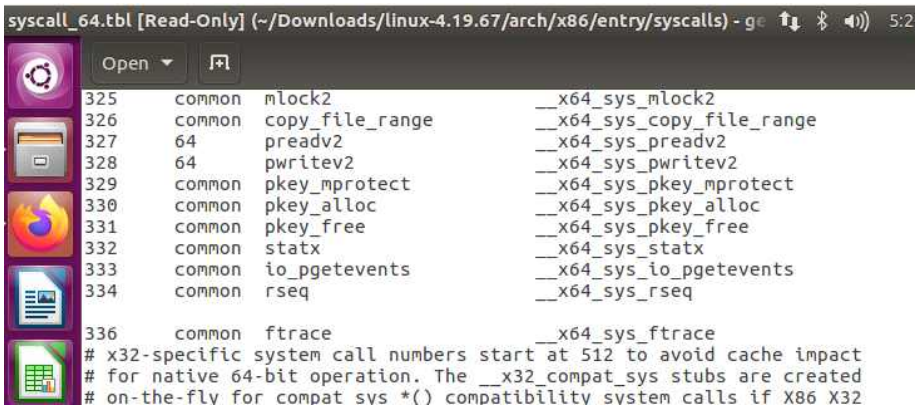

그림 1

그림 2>

그림 1은 시스템 콜 테이블에 ftrace를 등록해 놓은 것이다. test.c 파일은 강의 자료실에 올라온 것을 사용하였다. 그림 2는 gcc 컴파일러로 test.c파일을 실행 했을 때 보이는 화면으로 정상적으로 실행은 되었으나 커널 로그가 출력되지 못한 상황이다.

모듈 또한 제대로 작동하지 않았다. .ko파일이 보이지 않는다는 것을 알 수 있다.

고찰:

hooking함수들을 구현하는 과정을 잘 알지 못 했다. man 명령어와 시스템 콜 테이블 참조로 각 함수들의 번호와 원형은 알 수 있었지만, 트레이싱 할 때 대체해야 할 함수들을 정의하는 방법은 자료 예시를 통해서 DEFINEx로 틀만 작성할 줄은 알았으나 세부 동작 구현을 어떻게 해야 할지 몰라서 어려웠다. c파일들이 불안정했고 모듈 또한 제대로 작성되지 않았다. a.out을 실행할 때 모듈이 동작하면서 추가적인 파일을 생성

Reference:

https://man7.org/linux/man-pages/index.html