MÔN: HỆ ĐIỀU HÀNH

BÁO CÁO

***ĐỒ ÁN 02: KERNEL MODULE &***

***HOOK SYSTEM CALL***

1. **Thành viên:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **HỌ & TÊN** | **MSSV** | **PHÂN CÔNG** |
| 1 | Nguyễn Khánh Hoàng |  | Phần 1 |
| 2 | Nguyễn Hữu Vinh | 1712206 | Phần 2 |

1. **Phần 1:**
2. **Phần 2:**
3. **Mô tả**: Viết chương trình hook vào một system call

* System call **Open**: Ghi vào dmesg tên tiến trình mở file và tên file được mở
* System call **Write**: Ghi vào dmesg tên tiến trình ghi file, tên file bị ghi và số byte được ghi

1. Mức độ hoàn thành:

* Hook system call Open: hoàn thành
  + Ghi vào dmesg tiến trình mở file, tên file được mở
* Hook system call Write: hoàn thành
  + Ghi vào dmesg tiến trình ghi file, tên file bị ghi, số byte được ghi

1. Tổ chức:

* Hook system call Open: hookOpen.c

Chứa mã nguồn chương trình hook system call open

* Hook system call Write: hookWrite.c

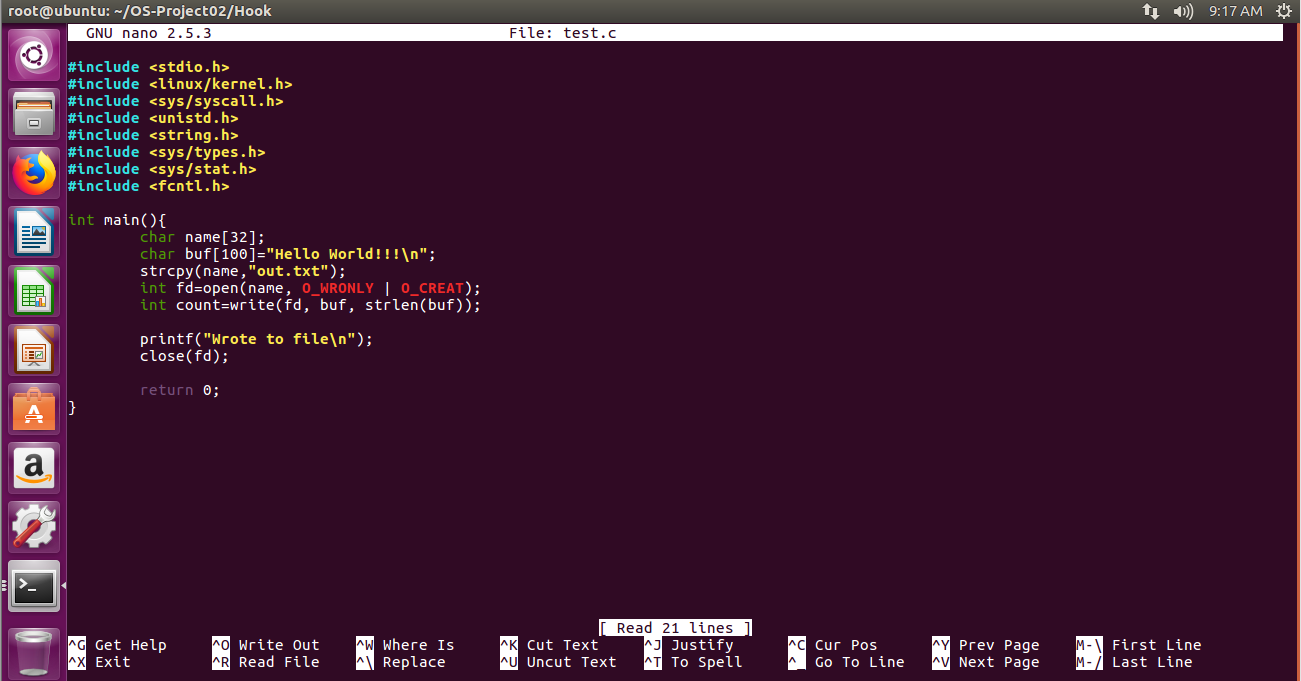
Chứa mã nguồn chương trình hook system call write

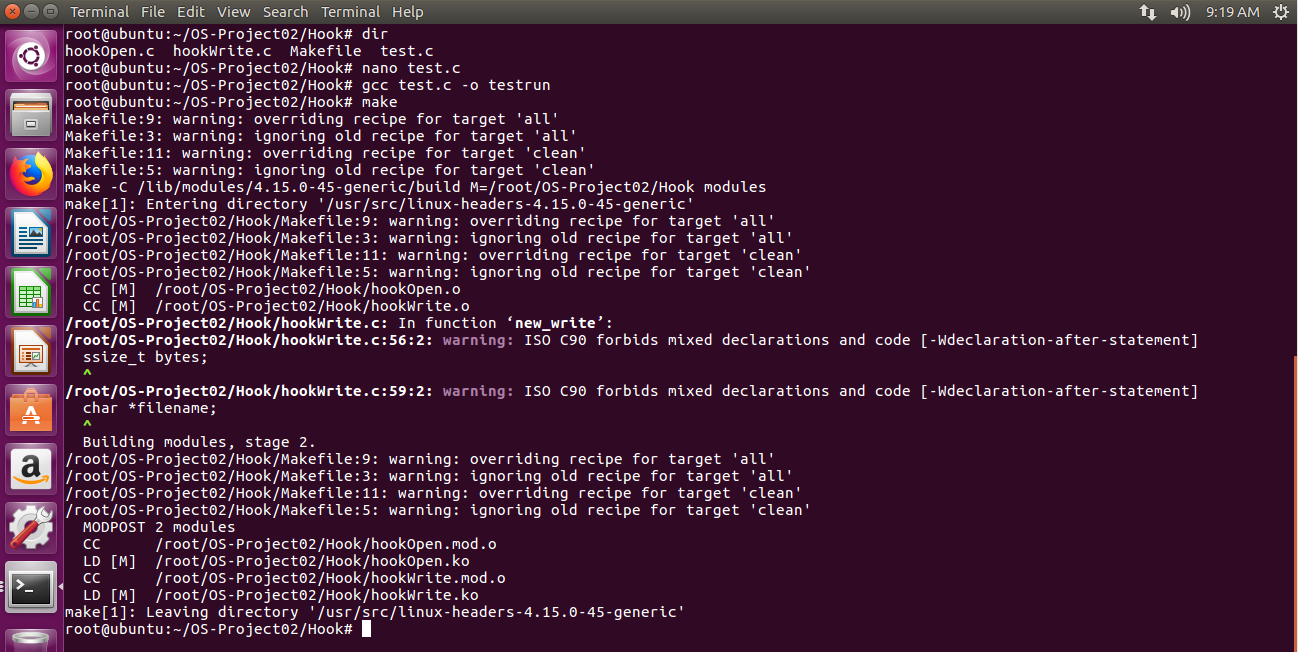
* Makefile

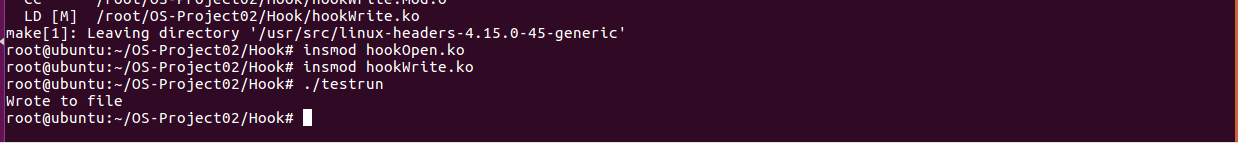
File qui định để thực thi lệnh make

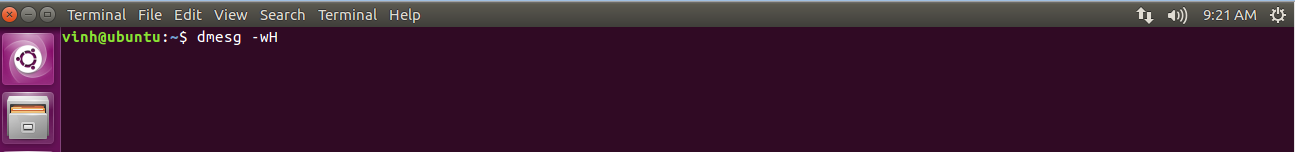
1. Ảnh minh họa:

Chương trình test.c:

Tiến hành compile test.c sang testrun và compile các chương trình hook

Gắn hook module và chạy testrun để kiểm tra

Dùng lệnh dmesg để kiểm tra kết quả in ra

Gỡ hook module

1. Nguồn tham khảo:

* https://github.com/GreenCandlePrinter/syscall-hook/blob/master/syscall-hook.c
* https://stackoverflow.com/questions/2103315/linux-kernel-system-call-hooking-example
* https://stackoverflow.com/questions/8250078/how-can-i-get-a-filename-from-a-file-descriptor-inside-a-kernel-module