

Họ và tên: Ngô Hồng Quốc Bảo

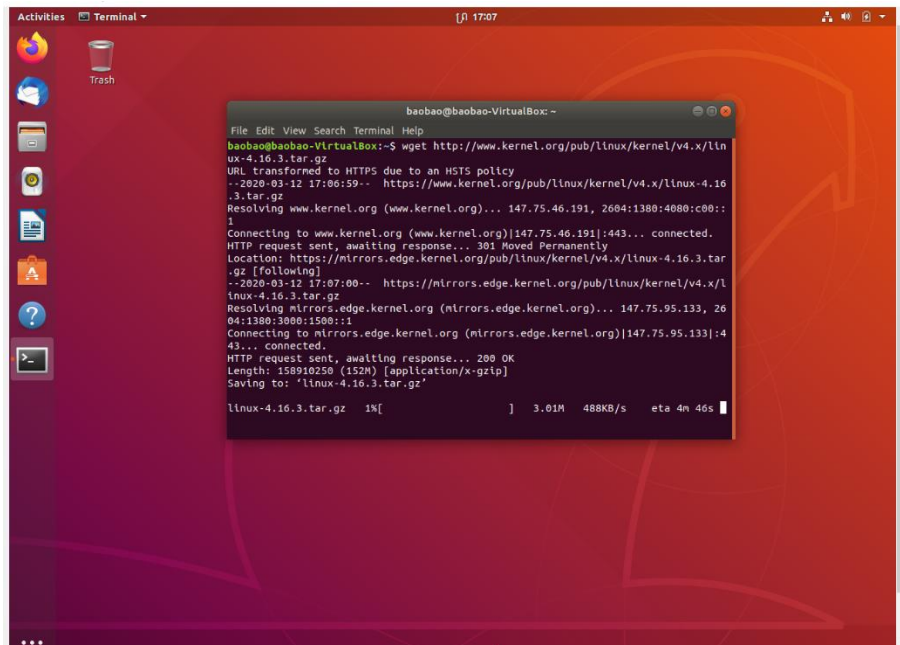
MSSV: B1809677

PROJECT

Nguyên Lý Hệ Điều Hành

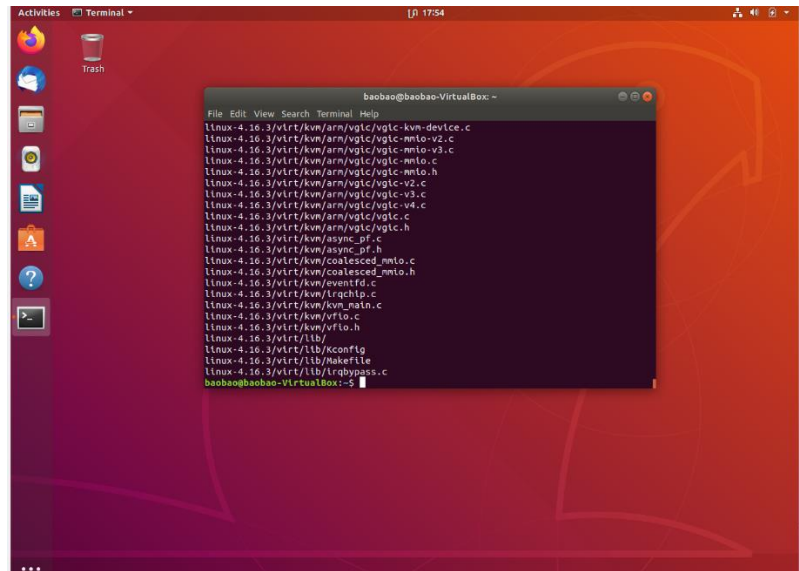
Phần 1: Xây Dựng Linux Kernel

- sudo -s (bật chế độ root user)
- Tải các tool cần thiết
 - o apt-get install -y gcc libncurses5-dev make wget
 - o apt-get install -y gcc libssl-dev
 - o apt-get install bison flex
- Tải và giải nén file linux 4.16.3:
 - o wget http://www.kernel.org/pub/linux/kernel/v4.x/linux-4.16.3.tar.gz

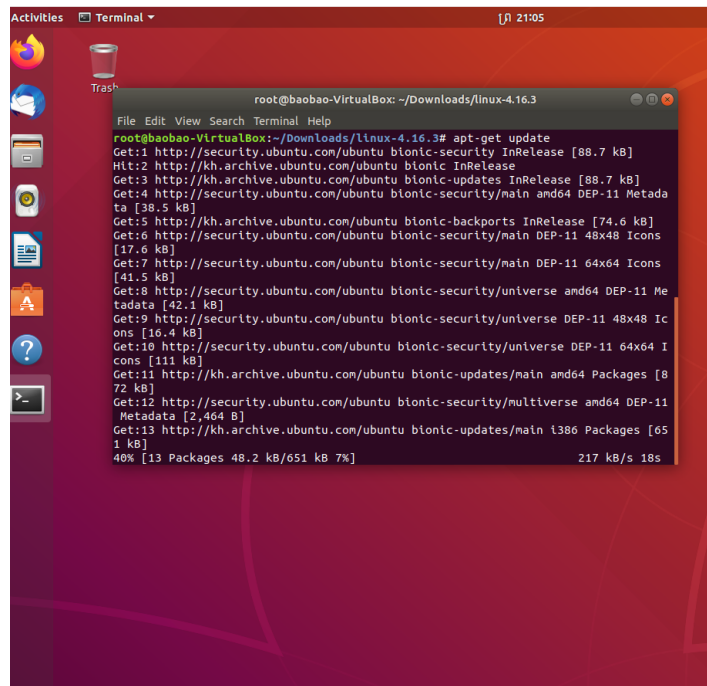


```
baobao@baobao-VirtualBox: ~  
File Edit View Search Terminal Help  
baobao@baobao-VirtualBox:~$ wget http://www.kernel.org/pub/linux/kernel/v4.x/linux-4.16.3.tar.gz  
--2020-03-12 17:06:59-- https://www.kernel.org/pub/linux/kernel/v4.x/linux-4.16.3.tar.gz  
Resolving www.kernel.org (www.kernel.org)... 147.75.46.191, 2604:1380:4080:c00::1  
Connecting to www.kernel.org (www.kernel.org)[147.75.46.191]:443... connected.  
HTTP request sent, awaiting response... 301 Moved Permanently  
Location: https://mirrors.edge.kernel.org/pub/linux/kernel/v4.x/linux-4.16.3.tar.gz [following]  
--2020-03-12 17:07:00-- https://mirrors.edge.kernel.org/pub/linux/kernel/v4.x/linux-4.16.3.tar.gz  
Resolving mirrors.edge.kernel.org (mirrors.edge.kernel.org)... 147.75.95.133, 2604:1380:3000:1500::1  
Connecting to mirrors.edge.kernel.org (mirrors.edge.kernel.org)[147.75.95.133]:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 158910250 (152M) [application/x-gzip]  
Saving to: 'linux-4.16.3.tar.gz'  
linux-4.16.3.tar.gz 1%[ ] 3.01M 488KB/s eta 4m 46s
```

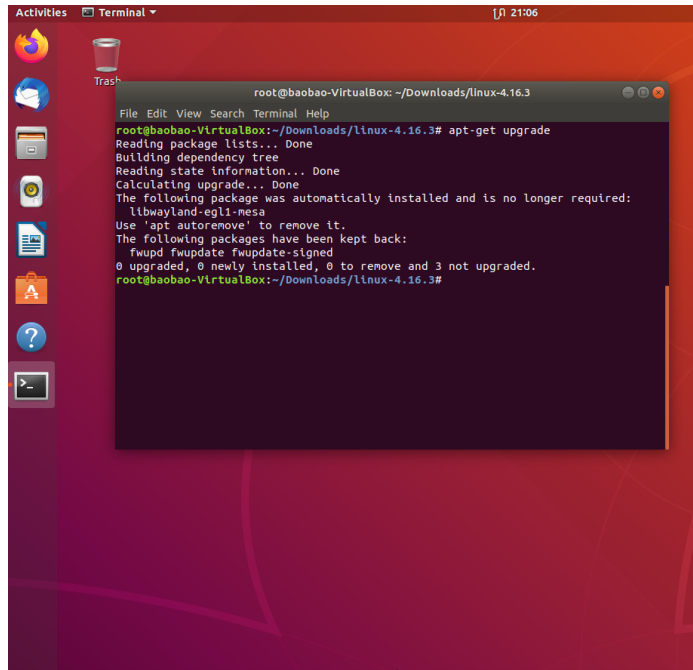
- o tar xvzf linux-4.16.3.tar.gz



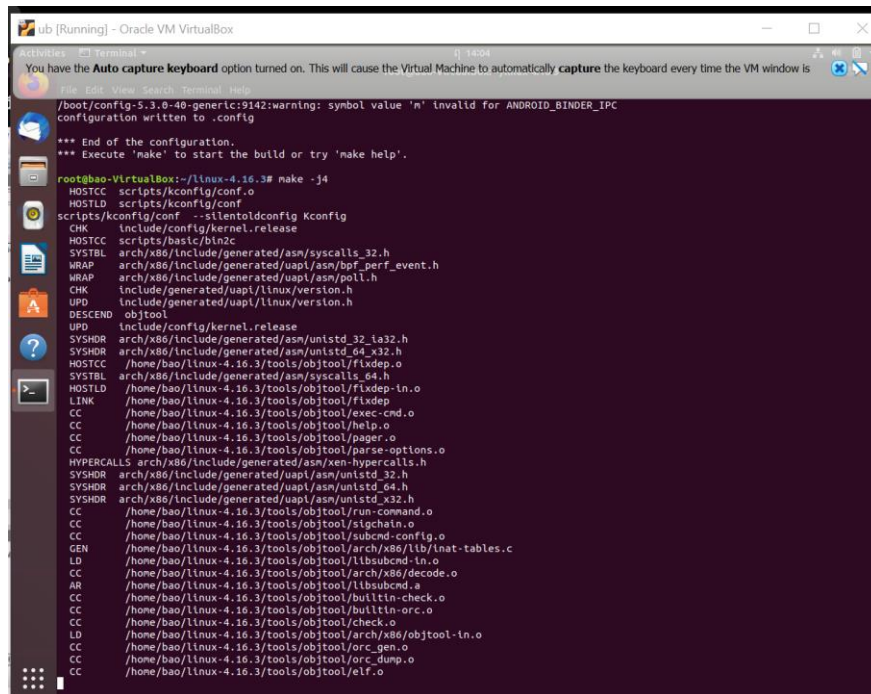
- Cập nhật và nâng cấp các gói vừa tải vào hệ thống:
 - o apt-get update



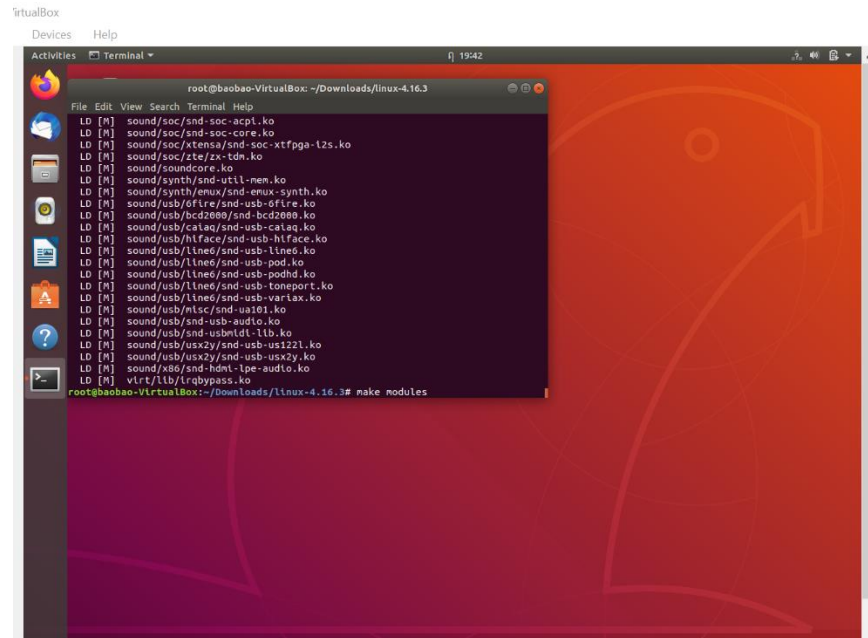
- o apt-get upgrade



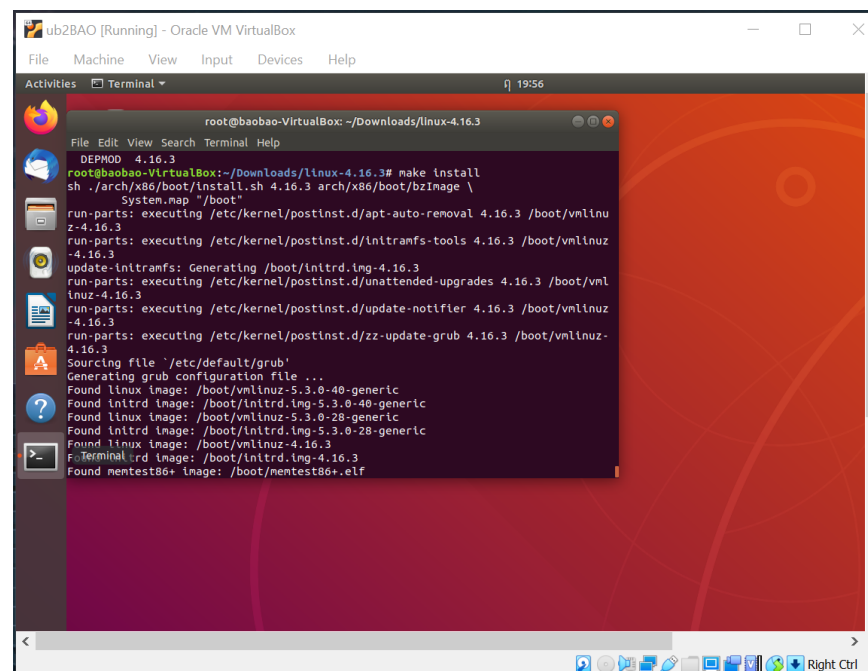
- Cài kernel vào hệ thống:
 - o make -j4



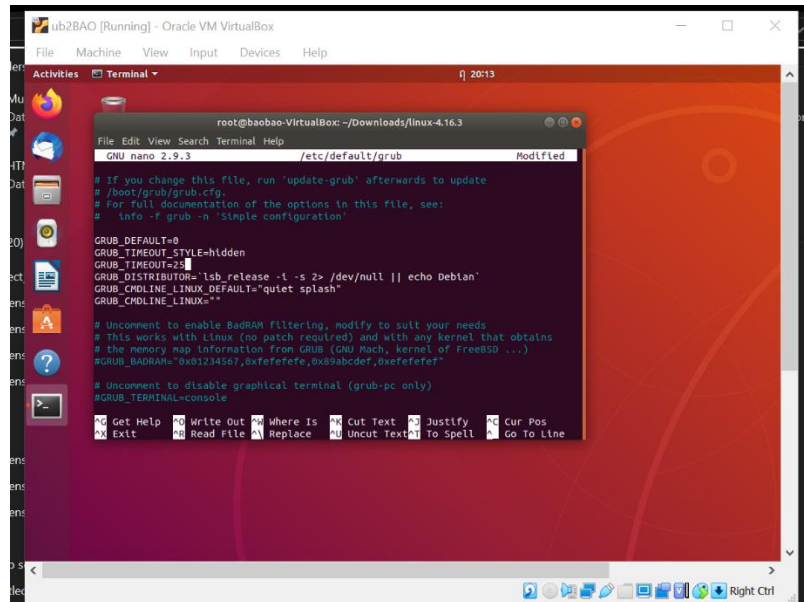
- o make modules



- make modules_install
- make install



- nano /etc/default/grub (thay đổi cấu hình grub)



The screenshot shows a terminal window titled 'root@baobao-VirtualBox: ~/Downloads/linux-4.16.3'. The terminal is running the nano editor to edit the file /etc/default/grub. The file content includes comments about updating grub, distribution information (lsb_release), and kernel boot options. The terminal window is overlaid on a desktop environment with various icons on the left and a taskbar at the bottom.

```
root@baobao-VirtualBox: ~/Downloads/linux-4.16.3
GNU nano 2.9.3 /etc/default/grub Modified

# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
# info -f grub -n 'Simple configuration'

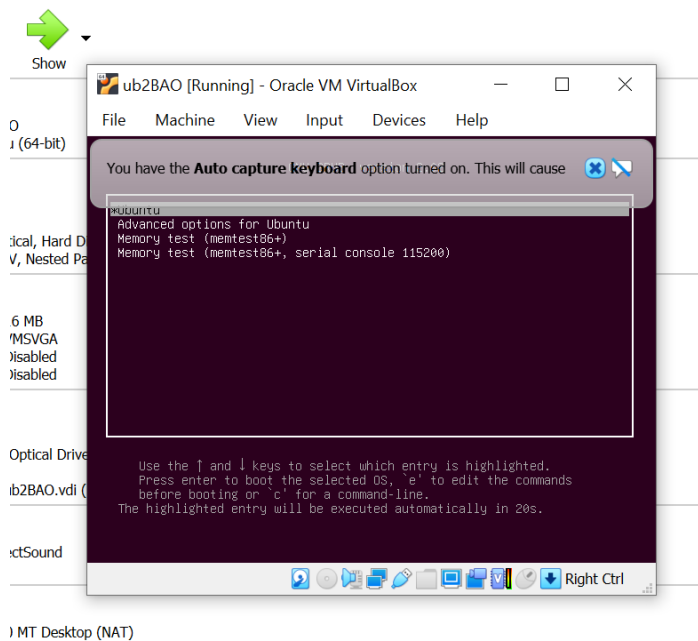
GRUB_DEFAULT=0
GRUB_TIMEOUT_STYLE=hidden
GRUB_TIMEOUT=25
GRUB_DISTRIBUTOR=`lsb_release -t -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="quiet splash"
GRUB_CMDLINE_LINUX=""

# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GRUB Mach, kernel of FreeBSD ...)
#GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

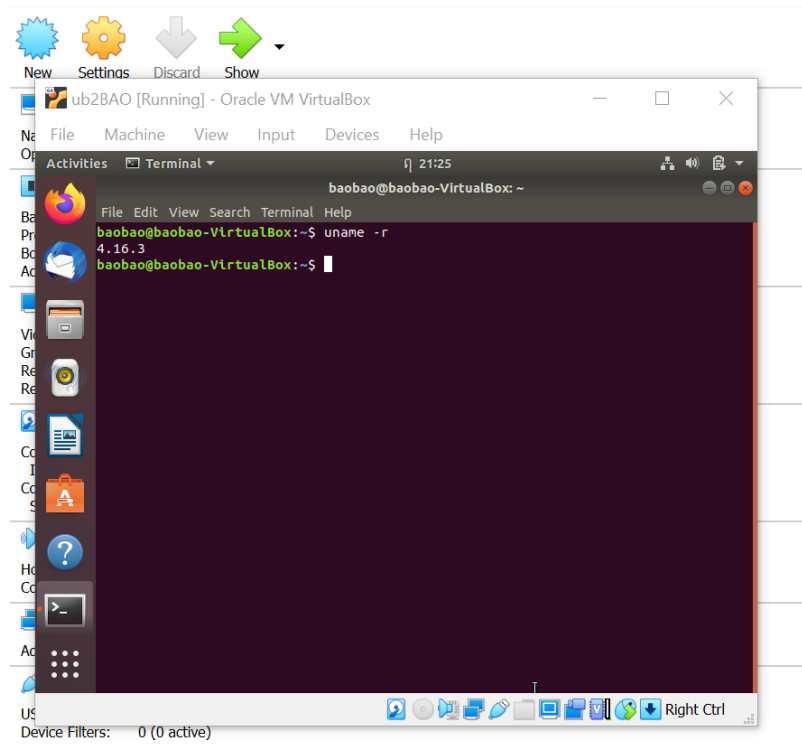
# Uncomment to disable graphical terminal (grub-pc only)
#GRUB_TERMINAL=console

Get Help  Write Out  Where Is  Cut Text  Justify  Cur Pos
Exit      Read File   Replace  Uncut Text To Spell  Go To Line
```

- reboot (reboot lại hệ thống)

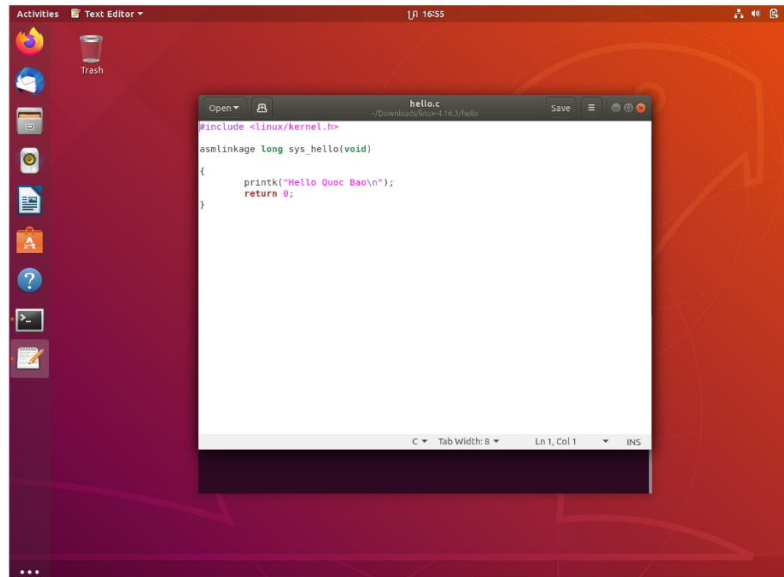


- uname -r (kiểm tra phiên bản của hệ thống)

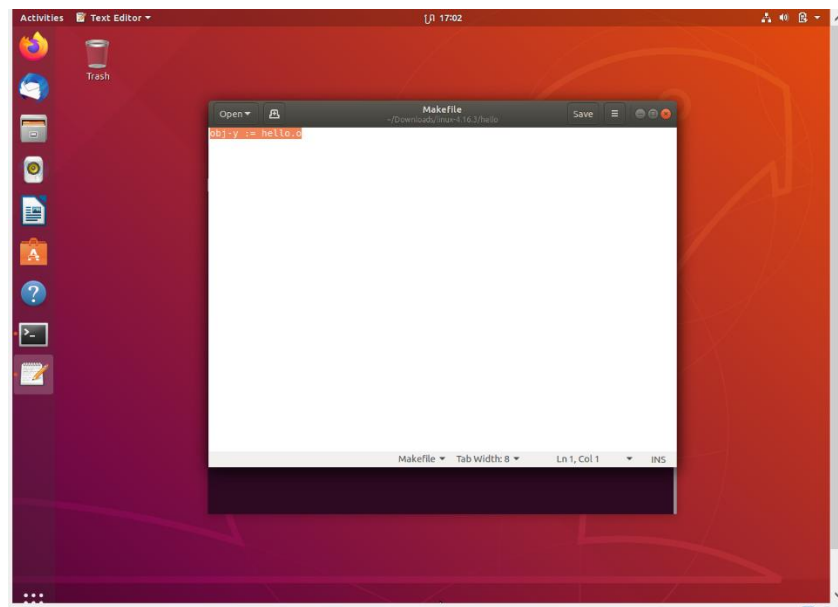


Phần 2: Thêm lời gọi hệ thống vào Linux Kernel

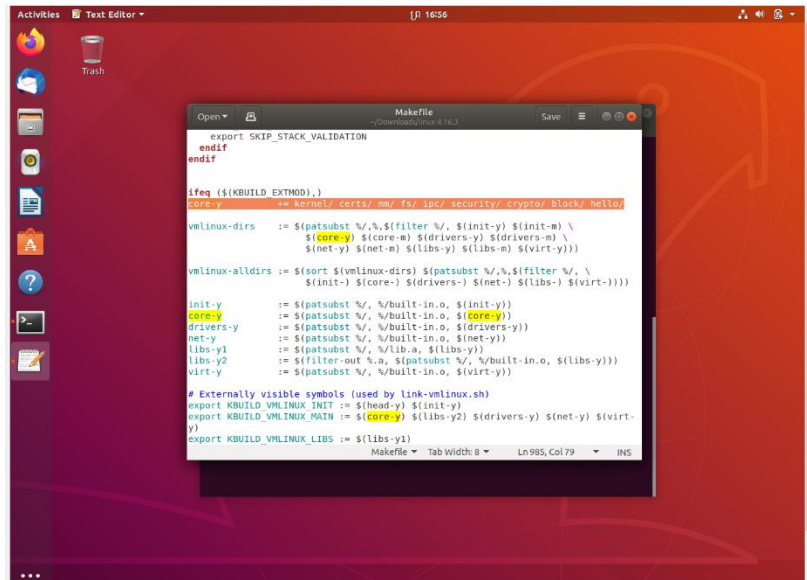
- Tạo file system call tên `sys_hello()`
 - o `mkdir hello`
 - o `cd hello`
 - o `gedit hello.c`



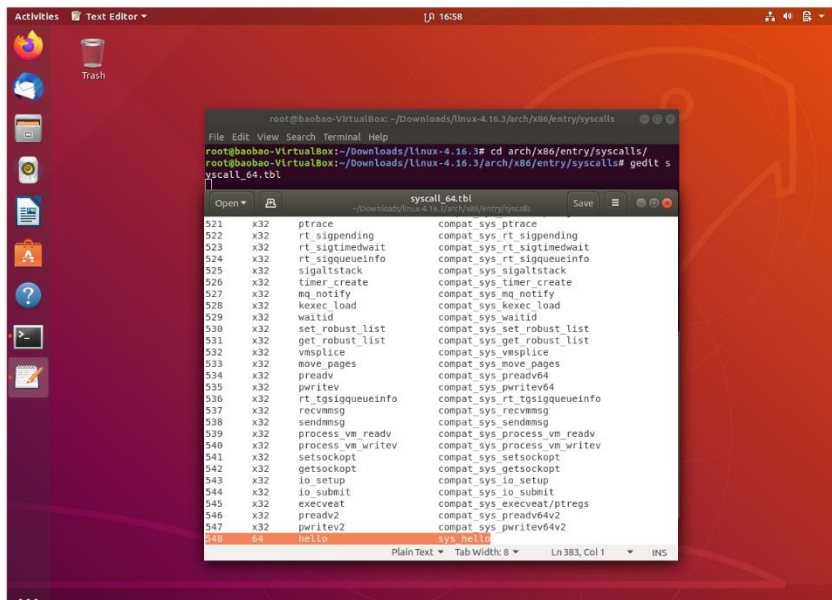
- gedit makefile
- Thêm "obj-y := hello.o" vào file Makefile để chắc chắn file hello.c được thêm vào kernel source code.



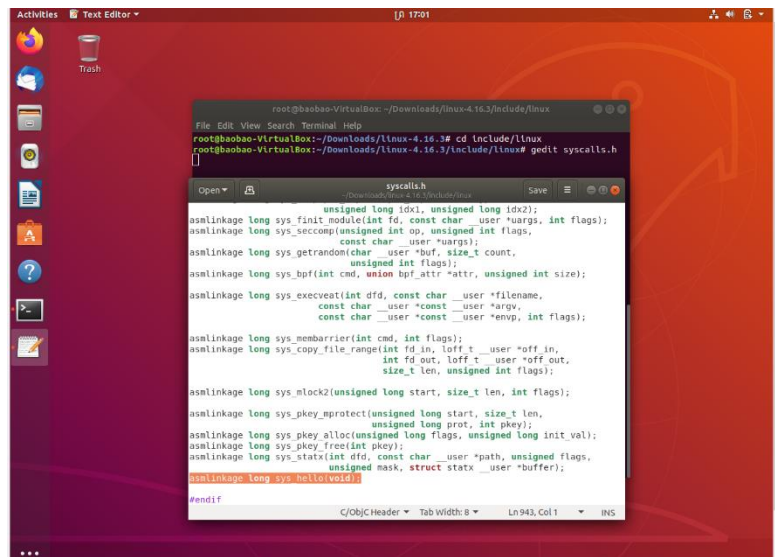
- Quay về thư mục cha và mở file Makefile
 - o cd ../
 - o gedit Makefile
 - o core-y += kernel/ certs/ mm/ fs/ ipc/ security / crypto/ block/ **hello/**
(thêm "hello/" vào sau câu lệnh trong file Makefile để thông báo với trình biên dịch là system call mới nằm trong thư mục hello)



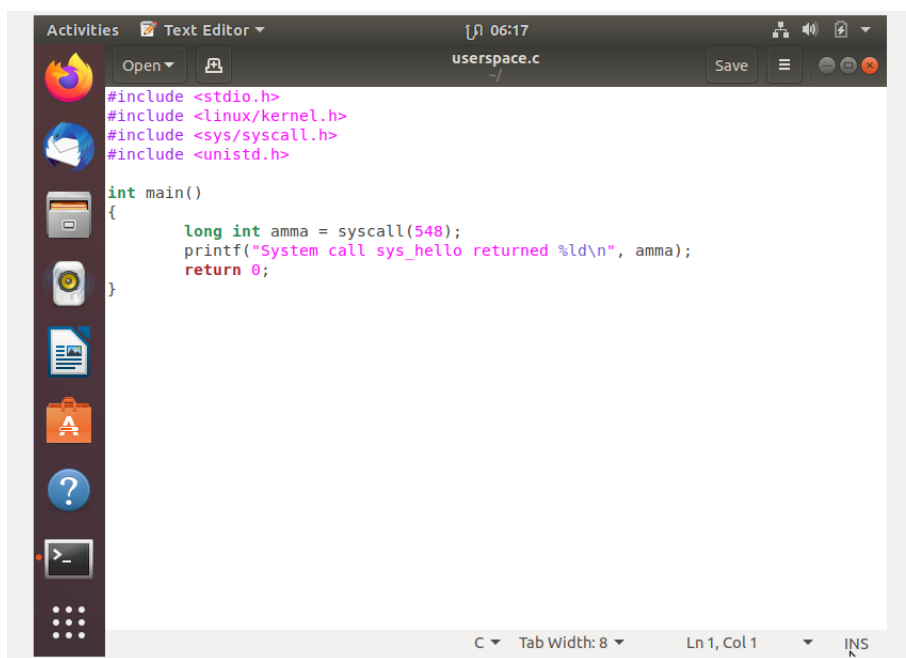
- Vào thư mục syscalls, mở file syscall_64.tbl:
 - o cd arch/x86/entry/syscalls/
 - o gedit syscall_64.tbl
 - o thêm dòng “548 64 hello sys_hello” vào cuối



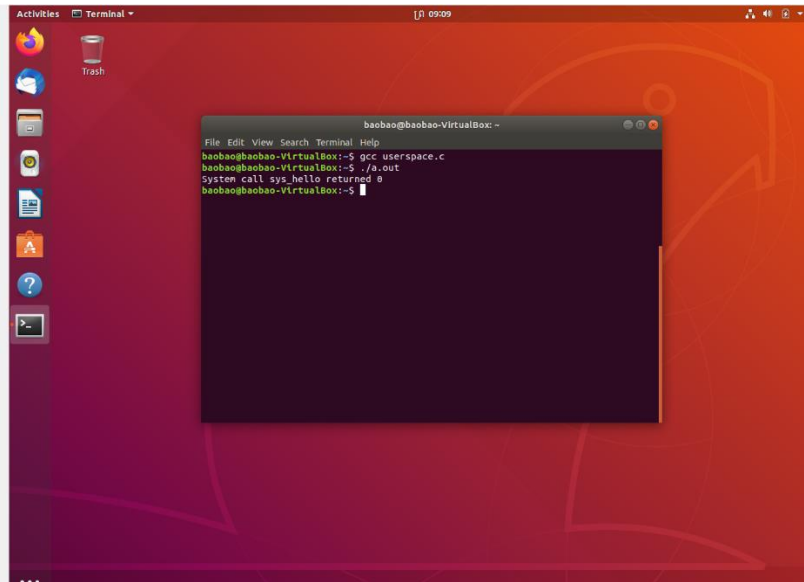
- Truy cập vào thư mục linux và mở file syscalls.h:
 - o cd include/linux/
 - o gedit syscalls.h
 - o Thêm dòng “asmlinkage long sys_hello(void)” vào cuối tệp trên lệnh “endif”



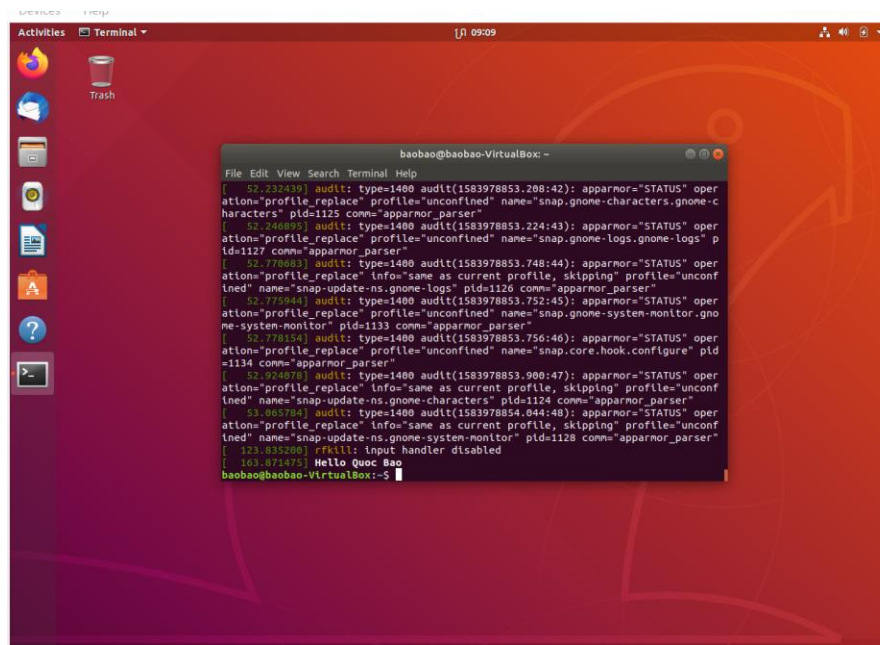
- Quay về home và tạo file userspace.c:
 - cd ~ (quay về home)
 - gedit userspace.c (tạo file userspace.c)



- Chạy file userspace.c:
 - gcc userspace.c
 - ./a.out
 - Nếu xuất hiện dòng "System call sys_hello returned 0" là đúng
 - Ngược lại, xuất hiện dòng "System call sys_hello returned -1" là sai



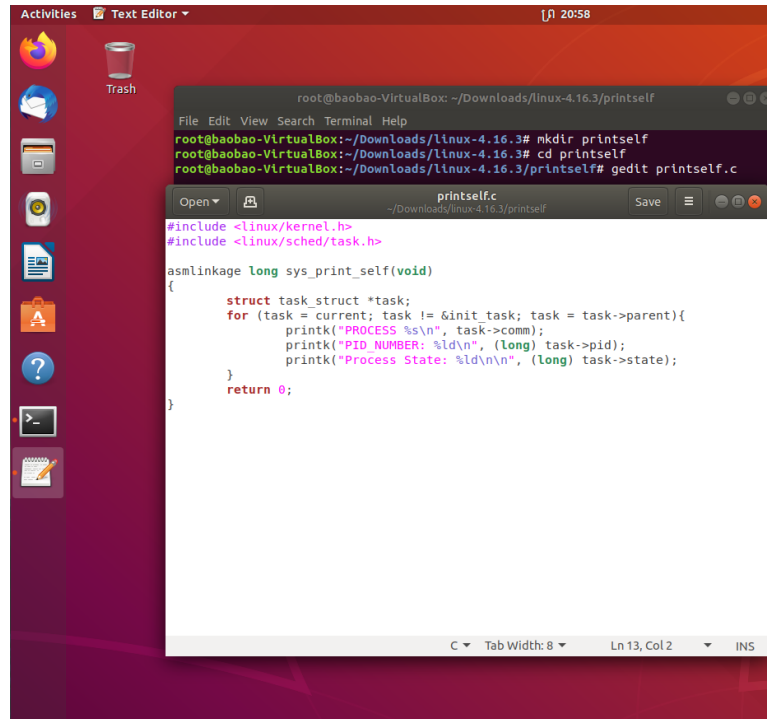
- dmesg (in lời nhắn ra terminal)



Phần 3: Làm Việc Với Tiến Trình

- Những câu lệnh của phần 3 sẽ tương tự và cùng mục đích như phần 2 , ngoại trừ một số khác biệt.
- Tạo file system_call tên sys_print_self():
 - o mkdir printself
 - o cd printself

- gedit printself.c
- câu lệnh “task->comm”: để lấy tên chương trình
- câu lệnh “task->pid”: để lấy process id
- câu lệnh “task->state”: để lấy trạng thái tiến trình



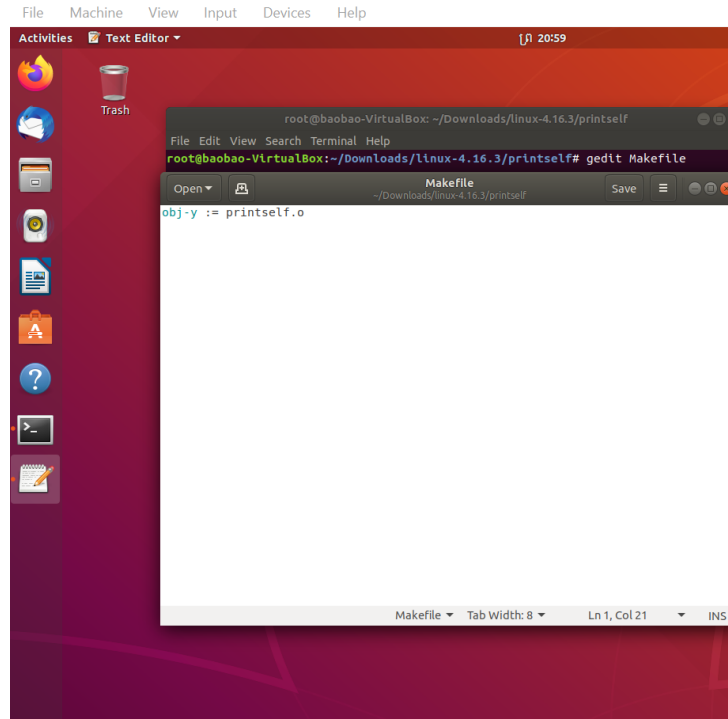
```
root@baobao-VirtualBox: ~/Downloads/linux-4.16.3/printself
File Edit View Search Terminal Help
root@baobao-VirtualBox:~/Downloads/linux-4.16.3# mkdir printself
root@baobao-VirtualBox:~/Downloads/linux-4.16.3# cd printself
root@baobao-VirtualBox:~/Downloads/linux-4.16.3/printself# gedit printself.c

printself.c
~/Downloads/linux-4.16.3/printself
Save

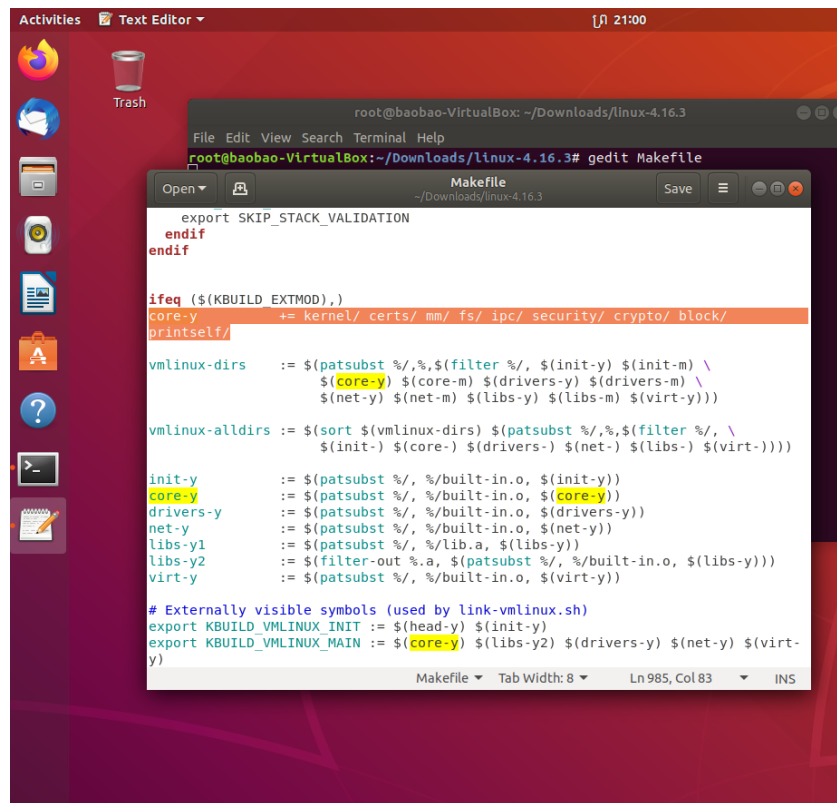
#include <linux/kernel.h>
#include <linux/sched/task.h>

asmlinkage long sys_print_self(void)
{
    struct task_struct *task;
    for (task = current; task != &init_task; task = task->parent){
        printk("PROCESS %s\n", task->comm);
        printk("PID NUMBER: %ld\n", (long) task->pid);
        printk("Process State: %ld\n", (long) task->state);
    }
    return 0;
}
```

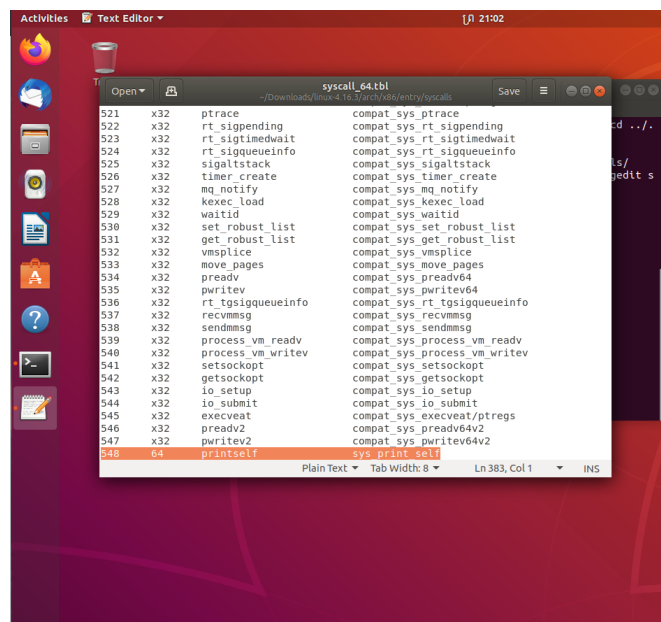
- gedit Makefile rồi thêm “obj-y := printself.o”



- Quay về thư mục cha linux-4.16.3 rồi mở file Makefile:
 - o `cd ../`
 - o `gedit Makefile`
 - o Tìm kiếm “core-y += kernel/ certs/ mm/ fs/ ipc/ security / crypto/ block/ **printself**/” (thêm printself vào)



- Vào thư mục syscalls, mở file syscall_64.tbl:
 - o cd arch/x86/entry/syscalls/
 - o gedit syscall_64.tbl
 - o thêm dòng “548 64 hello sys_print_self” vào cuối

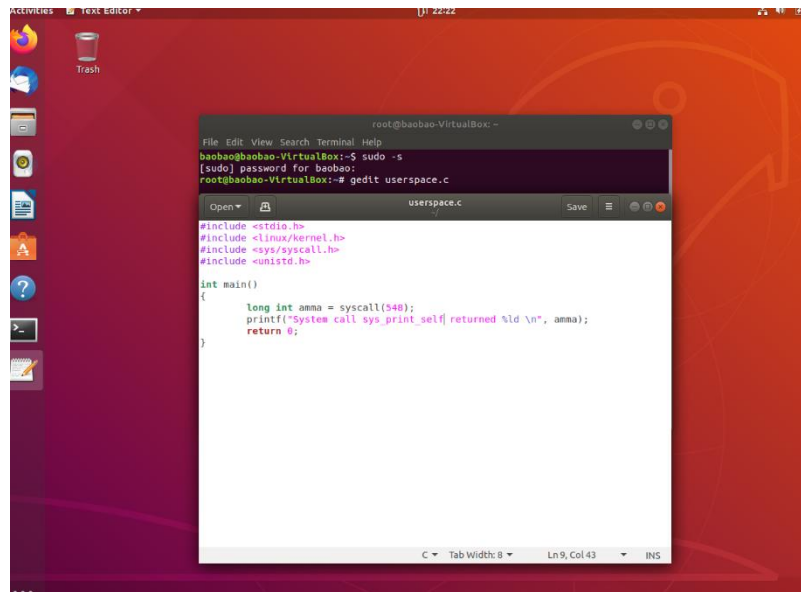


- Truy cập vào thư mục linux và mở file syscalls.h:
 - o `cd include/linux/`
 - o `gedit syscalls.h`
 - o Thêm dòng `"asmlinkage long sys_print_self(void)"` vào cuối tệp trên lệnh `"endif"`

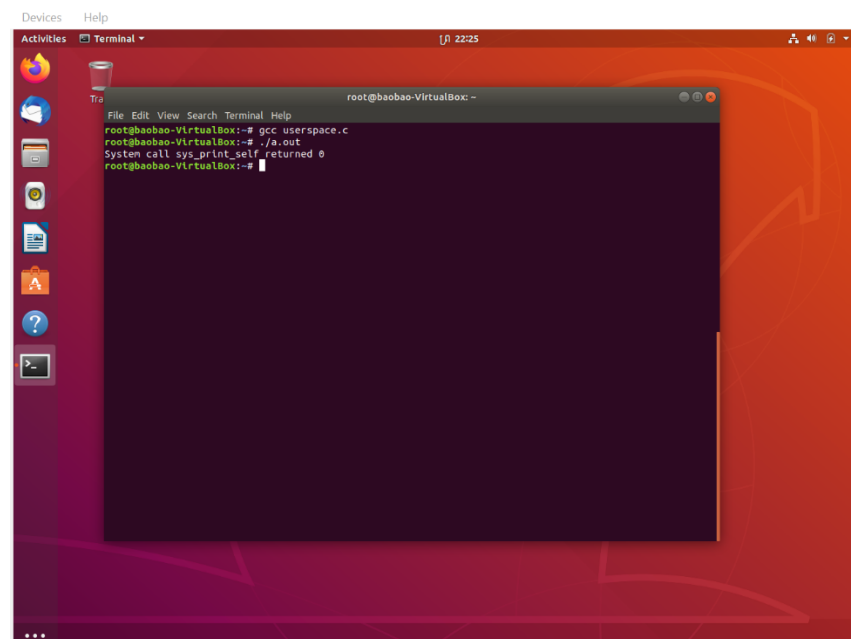
```

asmlinkage long sys_finit_module(int fd, const char __user *uargs, int flags);
asmlinkage long sys_seccomp(unsigned int op, unsigned int flags,
                             const char __user *uargs);
asmlinkage long sys_getrandom(char __user *buf, size_t count,
                              unsigned int flags);
asmlinkage long sys_bpf(int cmd, union bpf_attr *attr, unsigned int size);
asmlinkage long sys_execveat(int dfd, const char __user *filename,
                             const char __user *const *argv,
                             const char __user *const *envp, int flags);
asmlinkage long sys_mmapbarrier(int cmd, int flags);
asmlinkage long sys_copy_file_range(int fd_in, loff_t __user *off_in,
                                     int fd_out, loff_t __user *off_out,
                                     size_t len, unsigned int flags);
asmlinkage long sys_mlock2(unsigned long start, size_t len, int flags);
asmlinkage long sys_pkey_mprotect(unsigned long start, size_t len,
                                   unsigned long prot, int pkey);
asmlinkage long sys_pkey_alloc(unsigned long flags, unsigned long init_val);
asmlinkage long sys_pkey_free(int pkey);
asmlinkage long sys_statx(int dfd, const char __user *path, unsigned flags,
                          unsigned mask, struct statx __user *buffer);
asmlinkage long sys_print_self(void);
#endif
  
```

- Vì đây là tạo một syscall mới nên ta phải chạy cập nhật, biên dịch lại kernel:
 - o `apt-get update`
 - o `apt-get upgrade`
 - o `make -j4`
 - o `make modules_install install`
 - o `shutdown -r now` (reboot lại máy)
- Quay về home và tạo thư mục userspace.c:
 - o `cd ~`
 - o `gedit userspace`



- Chạy file userspace.c:
 - o gcc userspace.c
 - o ./a.out



- dmesg (in lời nhắn ra màn hình)


```
Activities Terminal [J] 22:23
root@baobao-VirtualBox: ~
File Edit View Search Terminal Help
[ 22.130905] audit: type=1400 audit(1584026500.352:48): apparmor="STATUS" operation="profile_replace"
pid=1172 comm="apparmor_parser"
[ 22.130905] audit: type=1400 audit(1584026500.352:48): apparmor="STATUS" operation="profile_replace"
pid=1167 comm="apparmor_parser"
[ 40.515390] rkill: input handler disabled
[ 108.130980] PROCESS a.out
[ 108.130987] PID_NUMBER: 2005
[ 108.130988] Process State: 0
[ 108.130988] PROCESS bash
[ 108.130988] PID_NUMBER: 1862
[ 108.130989] Process State: 1
[ 108.130989] PROCESS sudo
[ 108.130990] PID_NUMBER: 1861
[ 108.130990] Process State: 1
[ 108.130991] PROCESS bash
[ 108.130991] PID_NUMBER: 1852
[ 108.130992] Process State: 1
[ 108.130992] PROCESS gnome-terminal-
[ 108.130993] PID_NUMBER: 1844
[ 108.130993] Process State: 1
[ 108.130994] PROCESS systemd
[ 108.130994] PID_NUMBER: 1368
[ 108.130994] Process State: 1
[ 108.130995] PROCESS systemd
[ 108.130995] PID_NUMBER: 1
[ 108.130996] Process State: 1
root@baobao-VirtualBox:~#
```