BÁO CÁO ĐỒ ÁN 2
MÔN: HỆ ĐIỀU HÀNH

---

1. Thành viên:

- Nguyễn Quý Thanh - 18127210.
- Nguyễn Thị Tâm Phúc - 18127182.
- Nguyễn Phạm Thanh Vy - 18127258.

2. Yêu cầu:

a. Các bạn hãy cài đặt hai syscall dưới đây:

i. **int pnametoid (char *name):** syscall này sẽ nhận vào name và trả về pid nếu tìm thấy và trả về -1 nếu không tìm thấy.

ii. **int pidtoname (int pid, char* buf, int len)**: syscall này sẽ nhận vào pid, ghi process name vào trong biến buff với max len là len – 1 phần tử, cuối cùng sẽ tự động thêm NULL. Giá trị trả về là -1 nếu lỗi, 0 nếu len buffer truyền vào lớn hơn len của process name, và n với n là độ dài thật sự của process name, trong trường hợp len buffer truyền vào nhỏ hơn len của proccess name.

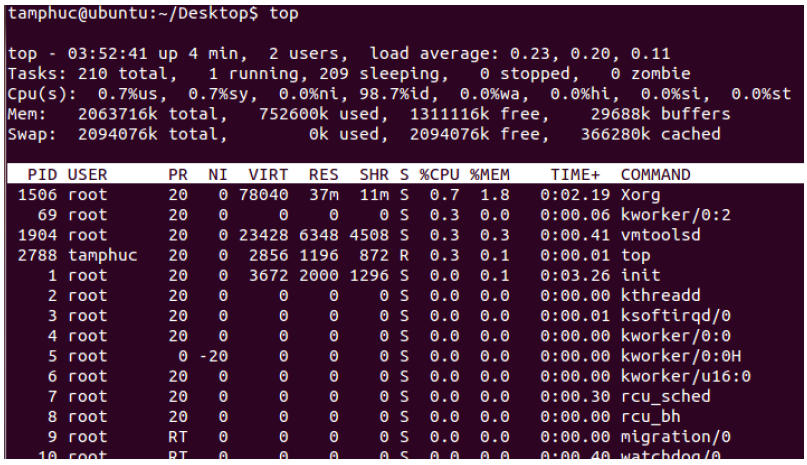
b. Hook vào 2 syscall dưới đây:

i. **syscall open** => ghi vào dmesg tên tiến trình mở file và tên file được mở.

ii. **syscall write** => ghi vào dmesg tên tiến trình, tên file bị ghi và số byte được ghi.

3. Mức độ hoàn thành: 100%.

4. Demo:



```
tamphuc@ubuntu:~/Desktop$ gcc test.c -o test
tamphuc@ubuntu:~/Desktop$ ./test
Choose the following options:
1. pnametoid
2. pidtoname
You choose: 1
Enter your name: firefox
System call return 2593
tamphuc@ubuntu:~/Desktop$ ./test
Choose the following options:
1. pnametoid
2. pidtoname
You choose: 1
Enter your name: rcu_sched
System call return 7
tamphuc@ubuntu:~/Desktop$ ./test
Choose the following options:
1. pnametoid
2. pidtoname
You choose: 1
Enter your name: Xorg
System call return 1506
```

```
tamphuc@ubuntu:~/Desktop$ ./test
Choose the following options:
1. pnametoid
2. pidtoname
You choose: 2
Enter your pid: 89
System call returned -1
Cannot find the process with pid = 89
tamphuc@ubuntu:~/Desktop$ ./test
Choose the following options:
1. pnametoid
2. pidtoname
You choose: 2
Enter your pid: 1904
System call returned 0
Your process name: vmtoolsd
tamphuc@ubuntu:~/Desktop$ ./test
Choose the following options:
1. pnametoid
2. pidtoname
You choose: 2
Enter your pid: 3
System call returned 0
Your process name: ksoftirqd/0
tamphuc@ubuntu:~/Desktop$
```

```
thanhqng@thanhqng: ~
[ 4712.184927] "sudo" open "/etc/group"
[ 4712.184944] "sudo" open "/etc/group"
[ 4712.184965] "sudo" open "/etc/group"
[ 4712.184987] "sudo" open "/etc/group"
[ 4712.185015] "sudo" open "/etc/group"
[ 4712.185041] "sudo" open "/etc/group"
[ 4712.185069] "sudo" open "/etc/group"
[ 4712.185279] "rs:main Q:Reg" write 149B to "/var/log/auth.log"
[ 4712.185399] "sudo" open "/etc/passwd"
[ 4712.185410] "sudo" open "/etc/group"
[ 4712.185421] "sudo" open "/etc/passwd"
[ 4712.185464] "sudo" open "/etc/passwd"
[ 4712.185527] "sudo" open "/etc/login.defs"
[ 4712.185583] "sudo" open "/etc/login.defs"
[ 4712.185670] "sudo" open "/etc/passwd"
[ 4712.185699] "sudo" open "/etc/login.defs"
[ 4712.185779] "sudo" open "/var/run/utmp"
[ 4712.185971] "rs:main Q:Reg" write 103B to "/var/log/auth.log"
[ 4712.187547] "rs:main Q:Reg" write 1984B to "/var/log/syslog"
[ 4712.187571] "rs:main Q:Reg" write 1984B to "/var/log/kern.log"
[ 4712.187653] "rmmod" open "/etc/ld.so.cache"
[ 4712.187682] "rmmod" open "/lib/i386-linux-gnu/libc.so.6"
[ 4712.188008] "rmmod" open "/proc/cmdline"
[ 4712.188066] "rmmod" open "/sys/module/Hook/initstate"
```