Assignment 2: Q2 (System Call)

SHREY MARWAHA – 2019334

Adding A System Call to The Linux Kernel (5.9.1) In Ubuntu (20.04.1 LTS)

Part 1: Preparation

The linux 5.9.1 source code is downloaded and it's extracted using the following.

- '*wget -P ~/* https://cdn.kernel.org/pub/linux/kernel/v5.x/linux5.9.1.tar.xz'

- A new directory sh_task_info is make which contains 2 files – ***sh_task_info.c*** and ***Makefile***.

- sh_task_info.c – functions take **int pid** and **char* filename** as parameters and uses writes it to a file. In ***SYSCALL_DEFINE2(sh_task_info, int, pid, char*, filename)*** iterates over all the process by using '***for_each_process()***' and compares the pid of each process with the given pid .

- Makefile contains the following code: '***obj-y := sh_task_info.o***'

- In the root of folder linux 5.9.1 we edit ***Makefile*** and append ' ***sh_task_info/***' to the core-y:

- In the file ***nano include/linux/syscalls.h*** we Add a corresponding function prototype for your system call to the header file of system calls just above ***#endif*** in the bottom.

- Add system call to the kernel's system call table by '**nanoarch/x86/entry/syscalls/syscall_64.tbl**'

Part 2: Compilation and Installation

- First a .config file is created with command '***make menuconfig***'.

- It was compiled with the three parallel commands by '***sudo make -j4 && sudo make modules_install -j4 && sudo make install -j4***'.

- Reboot the machine after this step.

Part 3: Testing

- The file '**report.c**' is the sample test code, compares the process IDs by using syscall. If the input process ID and the updated pid match, and there is no error in the given pid and the filename sh_task_info() is executed correctly.

- It should be compiled with '**gcc report.c –o report**'

• The executable is run with '**./report**' and provide the **PID** and **FILENAME**

```
shrey@shrey-VirtualBox:~$ ./report

Enter the pid: 10
Enter the file name: /home/shrey/Desktop/output.txt

Congratulations! Your system call is functional.
Run the command dmesg in the terminal and find out!

shrey@shrey-VirtualBox:~$ dmesg
```

• If the execution is successful, then we can check the kernel log via '**dmesg**'. The attributes corresponding to pid will be printed on the console.

• The following attributes are printed in **kernel log** and printed in **the file** provided:-

1. PROCESS
2. PID NUMBER
3. PROCESS STATE
4. PRIORITY
5. RT_PRIORITY
6. STATIC PRIORITY
7. NORMAL PRIORITY

```
[ 5861.705897]
              PROCESS: ksoftirqd/0
              PID_NUMBER: 10
              PROCESS STATE: 1
              PRIORITY: 120
              RT_PRIORITY: 0
              STATIC PRIORITY: 120
              NORMAL PRIORITY: 120
shrey@shrey-VirtualBox:~$
```

• Alternatively, we can check the log with '**cat <FILENAME>.txt'**.

```
1
2 Process: ksoftirqd/0
3 PID_NUMBER: 10
4 PROCESS STATE: 1
5 PRIORITY: 120
6 RT_PRIORITY: 0
7 STATIC PRIORITY: 120
8 NORMAL PRIORIY: 120
```

Part 4: Errors Handled

i. If the user enters invalid pid data type, ie. anyother data type other that int such as float or char etc

```
shrey@shrey-VirtualBox:~$ ./report

Enter the pid: 5
Enter the file name: shr.txt
Sorry,system call appears to have failed.: No such process
shrey@shrey-VirtualBox:~$
```

ii. If the user enters pid <=0 or greater than 32768, the function returns the errno 22 EINVAL invalid argument.

```
shrey@shrey-VirtualBox:~$ ./report

Enter the pid: 0
Enter the file name: output.txt
Sorry,system call appears to have failed.: Invalid argument
shrey@shrey-VirtualBox:~$
```

iii. If the file to be written does not exist then then, it will automatically creates a new file with the provided name in the /home directory.

iv. User has the choice to enter directly the directory rather than entering the whole directory in the **filename**

Eg. instead of providing filename as '*/home/shrey/Desktop/output.txt*' user has the choice to enter as '*Desktop/output.txt*'

```
shrey@shrey-VirtualBox:~$ ./report

Enter the pid: 1
Enter the file name: Desktop/shr.txt

Congratulations! Your system call is functional.
Run the command dmesg in the terminal and find out!
```

v. If user enters wrong directory address or any directory that doesn't even exist then the program will show '*Killed*'

```
shrey@shrey-VirtualBox:~$ ./report

Enter the pid: 10
Enter the file name: /home/Desktop/output.txt
Killed
shrey@shrey-VirtualBox:~$
```

vi. If user doesn't provide any directory for file then the program will by default take the directory as **home directory.**