DHRUV GARG 16 BCE 1190

IMPLEMENTING A SYSTEM CALL

LAB 3

PROCESS 1: INSTALL THE LATEST KERNEL

Step 1: Check the current kernel version and run the following commands to update existing system libraries.

```
vmdhruv@ubuntu:~$ uname -r
3.13.0-32-generic
vmdhruv@ubuntu:~$
```

Run the commands:

sudo apt-get update

sudo apt-get install git fakeroot build-essential ncurses-dev xz-utils libssl-dev bc

Step 2: Downloaded Linux 4.7.1 kernel and extracted the .tar file.

cd into the extracted directory

```
vmdhruv@ubuntu:~/Downloads$ ls
linux-4.7.1.tar.gz
vmdhruv@ubuntu:~/Downloads$ tar xf linux-4.7.1.tar.gz
vmdhruv@ubuntu:~/Downloads$ ls
linux-4.7.1  linux-4.7.1.tar.gz
vmdhruv@ubuntu:~/Downloads$ cd linux-4.7.1
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ ls
arch      Documentation  ipc          Makefile        scripts
block     drivers        Kbuild       mm              security
certs     firmware       Kconfig      net             sound
COPYING   fs             kernel       README          tools
CREDITS   include        lib          REPORTING-BUGS  usr
crypto    init           MAINTAINERS  samples         virt
```

The extracted folder contains directories like arch, crypto, fs, etc.

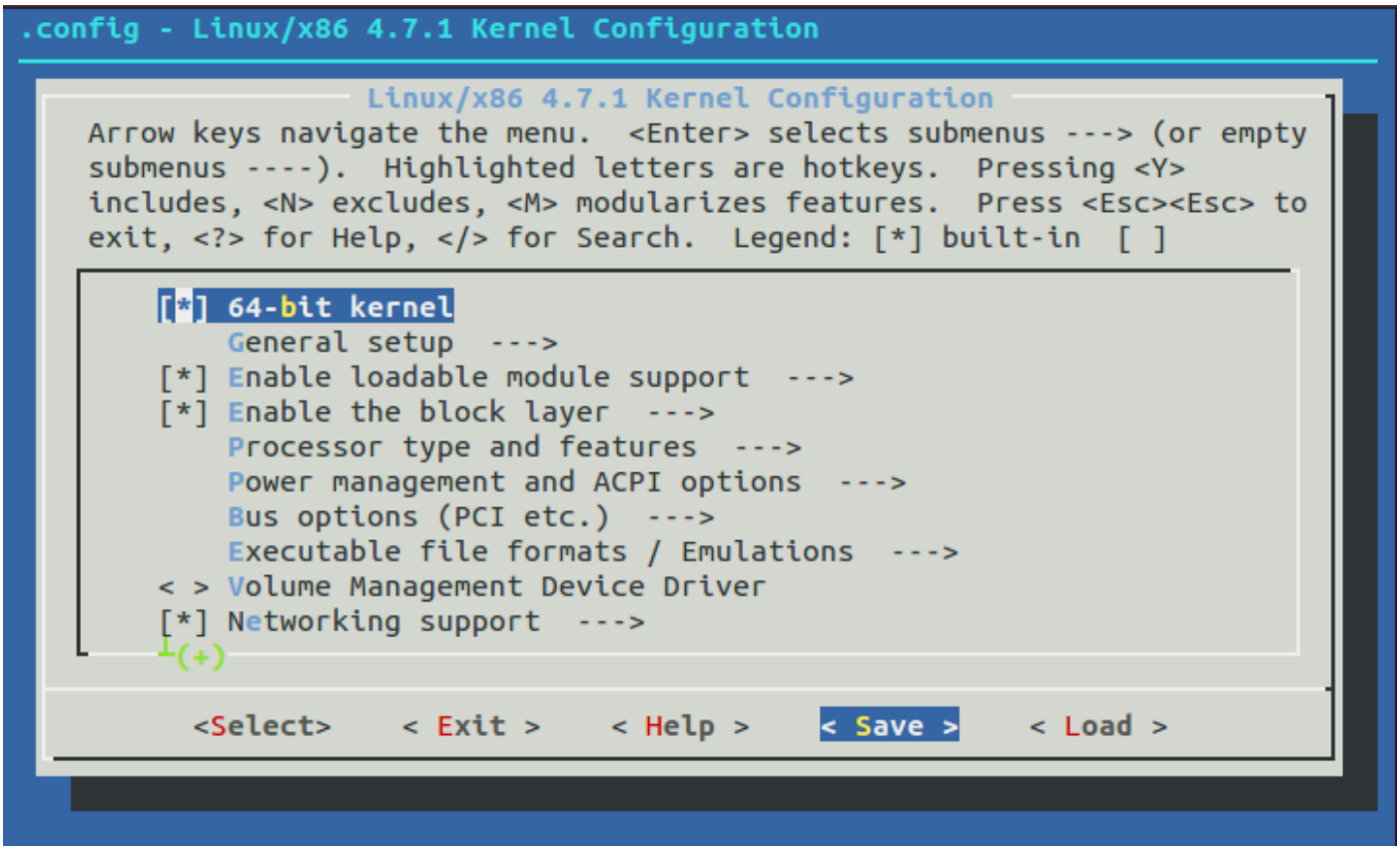
Step 3: Configuring the kernel

```
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ cp /boot/config-$(uname -r)
.config
```

```
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ make menuconfig
  HOSTCC  scripts/basic/fixdep
  HOSTCC  scripts/kconfig/mconf.o
  SHIPPED scripts/kconfig/zconf.tab.c
  SHIPPED scripts/kconfig/zconf.lex.c
  SHIPPED scripts/kconfig/zconf.hash.c
  HOSTCC  scripts/kconfig/zconf.tab.o
  HOSTCC  scripts/kconfig/lxdialog/checklist.o
  HOSTCC  scripts/kconfig/lxdialog/util.o
  HOSTCC  scripts/kconfig/lxdialog/inputbox.o
  HOSTCC  scripts/kconfig/lxdialog/textbox.o
  HOSTCC  scripts/kconfig/lxdialog/yesno.o
  HOSTCC  scripts/kconfig/lxdialog/menubox.o
  HOSTLD  scripts/kconfig/mconf
scripts/kconfig/mconf  Kconfig
.config:1475:warning: symbol value 'm' invalid for RXKAD
.config:2023:warning: symbol value 'm' invalid for SCSI_DH
.config:5245:warning: symbol value 'm' invalid for USB_ISP1760_HCD
.config:6511:warning: symbol value 'm' invalid for VME_BUS
.config:6544:warning: symbol value 'm' invalid for GENERIC_PHY


*** End of the configuration.
*** Execute 'make' to start the build or try 'make help'.
```

Note:

The linux kernel configuration GUI would show the existing kernel version 3.13.0 but I forgot to take a screenshot at that time. Hence inserted the GUI interface which comes when configuring 4.7.1.



Step 4: Compile the kernel and its modules using the make command, and install the kernel.

```
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ sudo make -j 4 && sudo make
modules_install -j 4 && sudo make install -j 4
[sudo] password for vmdhruv:
```

Kernel compilation begins.

```
CC [M]  arch/x86/crypto/cast6_avx_glue.o
AS [M]  arch/x86/crypto/twofish-avx-x86_64-asm_64.o
CC      mm/filemap.o
CC [M]  arch/x86/crypto/twofish_avx_glue.o
CC      kernel/softirq.o
AS [M]  arch/x86/crypto/serpent-avx-x86_64-asm_64.o
CC [M]  arch/x86/crypto/serpent_avx_glue.o
AS [M]  arch/x86/crypto/camellia-aesni-avx2-asm_64.o
CC [M]  arch/x86/crypto/camellia_aesni_avx2_glue.o
AS [M]  arch/x86/crypto/serpent-avx2-asm_64.o
CC [M]  arch/x86/crypto/serpent_avx2_glue.o
LD      arch/x86/crypto/crc32c-intel.o
LD [M]  arch/x86/crypto/aes-x86_64.o
LD [M]  arch/x86/crypto/camellia-x86_64.o
LD [M]  arch/x86/crypto/blowfish-x86_64.o
LD [M]  arch/x86/crypto/twofish-x86_64.o
LD [M]  arch/x86/crypto/twofish-x86_64-3way.o
LD [M]  arch/x86/crypto/salsa20-x86_64.o
CC      kernel/resource.o
LD [M]  arch/x86/crypto/serpent-sse2-x86_64.o
LD [M]  arch/x86/crypto/aesni-intel.o
LD [M]  arch/x86/crypto/ghash-clmulni-intel.o
LD [M]  arch/x86/crypto/sha1-ssse3.o
LD [M]  arch/x86/crypto/crc32-pclmul.o
LD [M]  arch/x86/crypto/sha256-ssse3.o
LD [M]  arch/x86/crypto/sha512-ssse3.o
LD [M]  arch/x86/crypto/crct10dif-pclmul.o
LD [M]  arch/x86/crypto/camellia-aesni-avx-x86_64.o
LD [M]  arch/x86/crypto/cast5-avx-x86_64.o
LD [M]  arch/x86/crypto/cast6-avx-x86_64.o
LD [M]  arch/x86/crypto/twofish-avx-x86_64.o
LD [M]  arch/x86/crypto/serpent-avx-x86_64.o
LD [M]  arch/x86/crypto/camellia-aesni-avx2.o
LD      arch/x86/crypto/built-in.o
CC      mm/mempool.o
```

Compilation of kernel 4.7.1 succeeded.

```
  INSTALL /lib/firmware/ti_3410.fw
  INSTALL /lib/firmware/ti_5052.fw
  INSTALL /lib/firmware/mts_cdma.fw
  INSTALL /lib/firmware/mts_gsm.fw
  INSTALL /lib/firmware/mts_edge.fw
  INSTALL /lib/firmware/edgeport/boot.fw
  INSTALL /lib/firmware/edgeport/boot2.fw
  INSTALL /lib/firmware/edgeport/down.fw
  INSTALL /lib/firmware/edgeport/down2.fw
  INSTALL /lib/firmware/edgeport/down3.bin
  INSTALL /lib/firmware/whiteheat_loader.fw
  INSTALL /lib/firmware/whiteheat.fw
  INSTALL /lib/firmware/keyspan_pda/keyspan_pda.fw
  INSTALL /lib/firmware/keyspan_pda/xircom_pgs.fw
  INSTALL /lib/firmware/cpia2/stv0672_vp4.bin
  INSTALL /lib/firmware/yam/1200.bin
  INSTALL /lib/firmware/yam/9600.bin
  DEPMOD  4.7.1
sh ./arch/x86/boot/install.sh 4.7.1 arch/x86/boot/bzImage \
                System.map "/boot"
run-parts: executing /etc/kernel/postinst.d/apt-auto-removal 4.7.1 /boot/vmlinuz-4.7.1
run-parts: executing /etc/kernel/postinst.d/initramfs-tools 4.7.1 /boot/vmlinuz-4.7.1
update-initramfs: Generating /boot/initrd.img-4.7.1
run-parts: executing /etc/kernel/postinst.d/pm-utils 4.7.1 /boot/vmlinuz-4.7.1
run-parts: executing /etc/kernel/postinst.d/update-notifier 4.7.1 /boot/vmlinuz-4.7.1
run-parts: executing /etc/kernel/postinst.d/zz-update-grub 4.7.1 /boot/vmlinuz-4.7.1
Generating grub configuration file ...
Warning: Setting GRUB_TIMEOUT to a non-zero value when GRUB_HIDDEN_TIMEOUT is set is no longer supported.
Found linux image: /boot/vmlinuz-4.7.1
Found initrd image: /boot/initrd.img-4.7.1
Found linux image: /boot/vmlinuz-3.13.0-32-generic
Found initrd image: /boot/initrd.img-3.13.0-32-generic
Found memtest86+ image: /boot/memtest86+.elf
Found memtest86+ image: /boot/memtest86+.bin
done
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$
```

Step 5: To use the new kernel the next time we boot up, we use the following two commands.

update-initramfs -c -k 4.7.1

update-grub

```
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ sudo update-initramfs -c -k 4.7.1
update-initramfs: Generating /boot/initrd.img-4.7.1
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ sudo update-grub
Generating grub configuration file ...
Warning: Setting GRUB_TIMEOUT to a non-zero value when GRUB_HIDDEN_TIMEOUT is set is no longer supported.
Found linux image: /boot/vmlinuz-4.7.1
Found initrd image: /boot/initrd.img-4.7.1
Found linux image: /boot/vmlinuz-3.13.0-32-generic
Found initrd image: /boot/initrd.img-3.13.0-32-generic
Found memtest86+ image: /boot/memtest86+.elf
Found memtest86+ image: /boot/memtest86+.bin
done
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$
```

PROCESS 2: IMPLEMENTING A SYSTEM CALL IN THE NEWLY INSTALLED KERNEL

Step 1: Check that the kernel version is updated.

```
vmdhruv@ubuntu:~$ uname -r
4.7.1
vmdhruv@ubuntu:~$
```

Step 2: Move into the linux-4.7.1 directory and make a new directory called 'info'

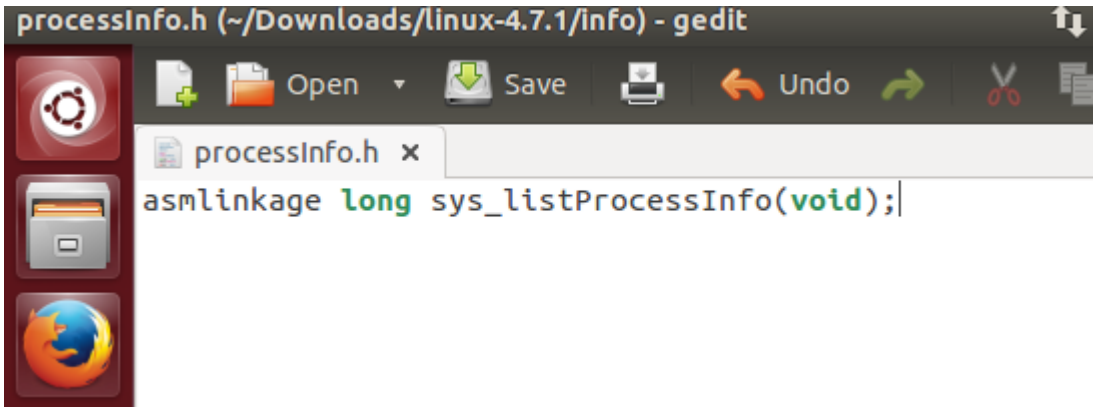
```
vmdhruv@ubuntu:~/Downloads$ cd linux-4.7.1
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ mkdir info
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ ls
arch            firmware  kernel          net             tools
block           fs        lib             README          usr
certs           include   MAINTAINERS     REPORTING-BUGS  virt
COPYING         info      Makefile        samples         vmlinux
CREDITS         init      mm              scripts         vmlinux.o
crypto          ipc       modules.builtin security
Documentation   Kbuild    modules.order   sound
drivers         Kconfig   Module.symvers  System.map
```

Step 3: cd into 'info'

```
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ cd info
vmdhruv@ubuntu:~/Downloads/linux-4.7.1/info$
```

Step 4: Create a header file 'processInfo.h' and write the following "asmlinkage long sys_listProcessInfo(void);" line into it.

```
vmdhruv@ubuntu:~/Downloads/linux-4.7.1/info$ gedit processInfo.h &
[1] 2481
vmdhruv@ubuntu:~/Downloads/linux-4.7.1/info$
```



Step 5: We will define our system call in 'listProcessInfo.c'. Create a new .c file and compile it.

```
vmdhruv@ubuntu:~/Downloads/linux-4.7.1/info$ gedit listProcessInfo.c &
[2] 2507
[1]   Done                    gedit processInfo.h
vmdhruv@ubuntu:~/Downloads/linux-4.7.1/info$
```

listProcessInfo.c (~/Downloads/linux-4.7.1/info) - gedit

Open Save Undo

listProcessInfo.c

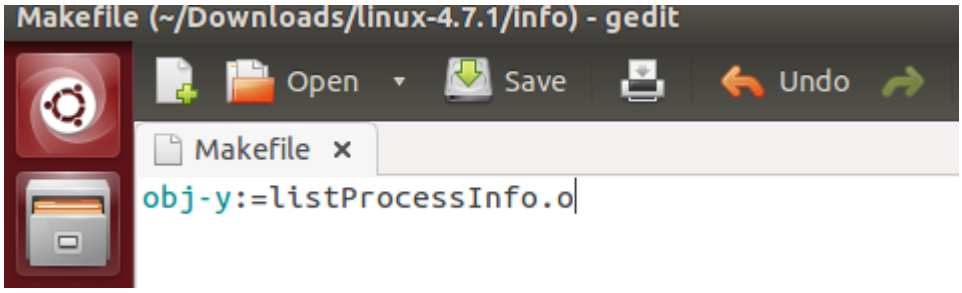
```c
#include<linux/kernel.h>
#include<linux/init.h>
#include<linux/sched.h>
#include<linux/syscalls.h>
#include "processInfo.h"
asmlinkage long sys_listProcessInfo(void) {
    struct task_struct *proces;

    for_each_process(proces) {

    printk(
      "Process: %s\n \
       PID_Number: %ld\n \
       Process State: %ld\n \
       Priority: %ld\n \
       RT_Priority: %ld\n \
       Static Priority: %ld\n \
       Normal Priority: %ld\n", \
       proces->comm, \
       (long)task_pid_nr(proces), \
       (long)proces->state, \
       (long)proces->prio, \
       (long)proces->rt_priority, \
       (long)proces->static_prio, \
       (long)proces->normal_prio \
    );
```

```c
    if(proces->parent)
       printk(
         "Parent process: %s, \
          PID_Number: %ld", \
          proces->parent->comm, \
          (long)task_pid_nr(proces->parent) \
       );

    printk("\n\n");

   }

   return 0;
}
```

Step 6: Write a make file in the current directory 'info' with the following line.

obj-y:=listProcessInfo.o

```
vmdhruv@ubuntu:~/Downloads/linux-4.7.1/info$ gedit Makefile &
[1] 2548
vmdhruv@ubuntu:~/Downloads/linux-4.7.1/info$
```



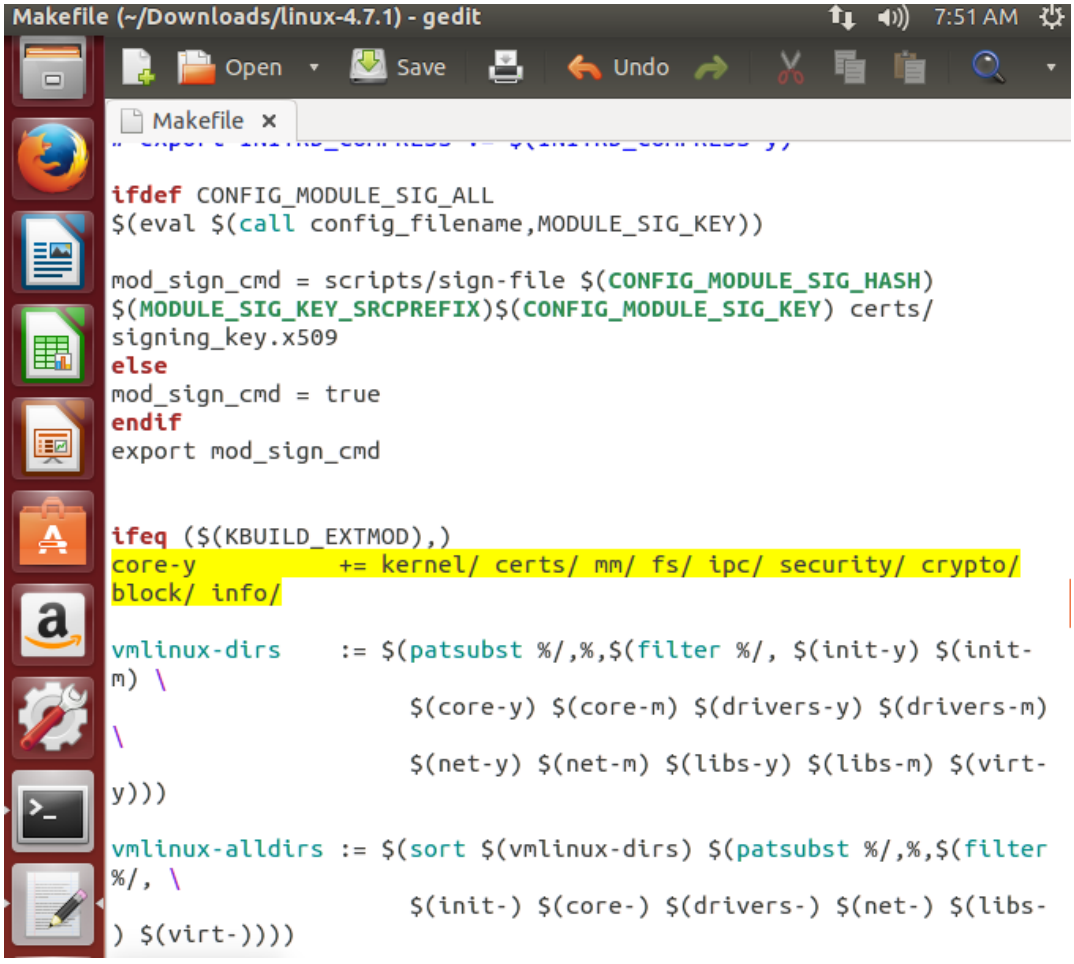
Step 7: Modify the necessary kernel files to integrate our system call into the kernel.

Open the kernel's Makefile (found in the linux-4.7.1 directory) and look for the following line:

core -y += kernel/ mm/ fs/ ipc/ security/ crypto/ block/

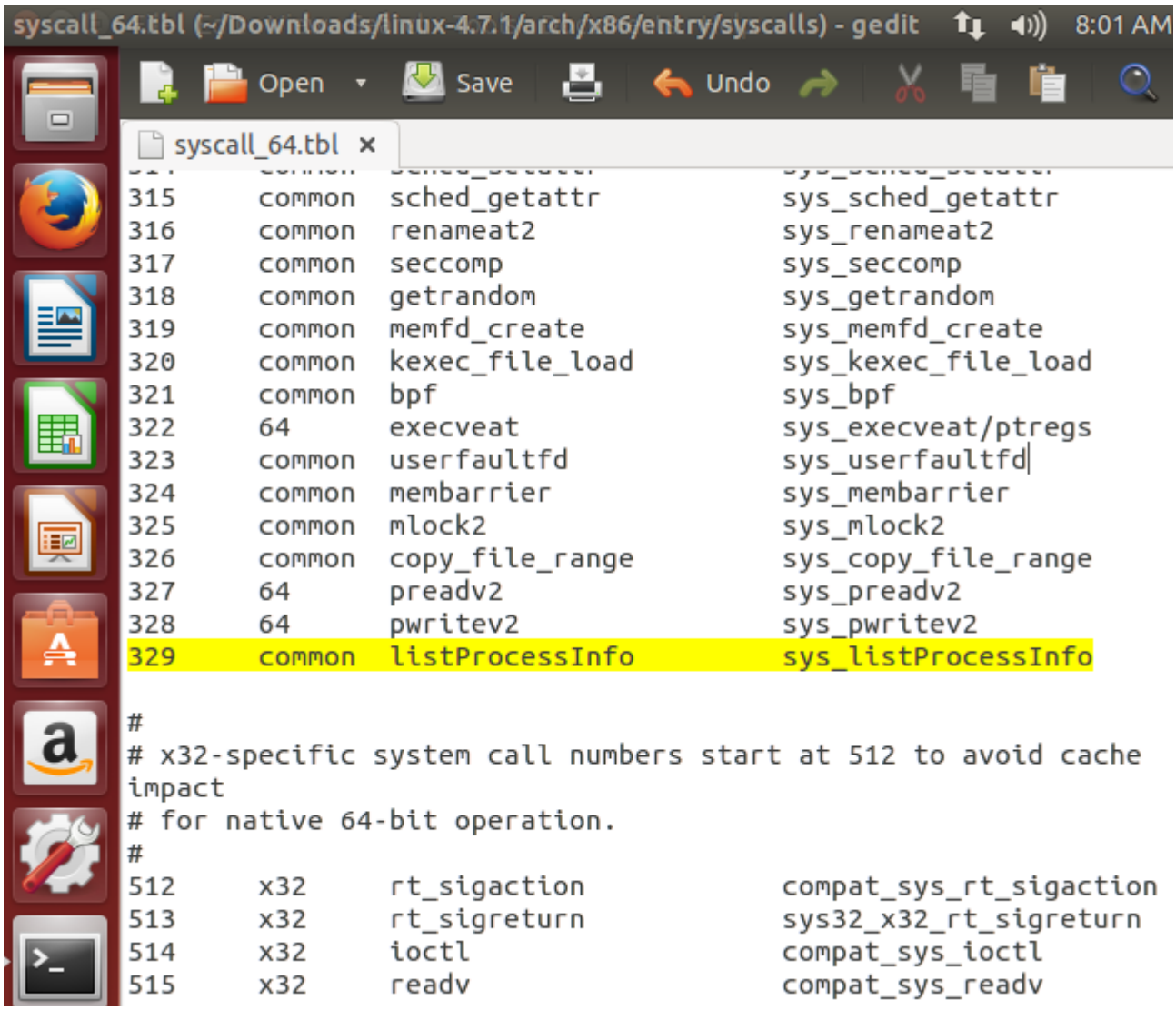
And, change it to include info/.

```
vmdhruv@ubuntu:~/Downloads/linux-4.7.1/info$ cd ../
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ gedit Makefile &
[1] 2563
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$
```



Step 8: Alter the syscall_64.tbl. To find the file, we use the 'find' command. Select the path that has /arch/x86/entry/syscalls/syscall_64.tbl and open the file in gedit.

```
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ find -name syscall_64.tbl
./arch/x86/entry/syscalls/syscall_64.tbl
./tools/perf/arch/x86/entry/syscalls/syscall_64.tbl
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ gedit ./arch/x86/entry/sysca
lls/syscall_64.tbl &
[1] 2578
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$
```

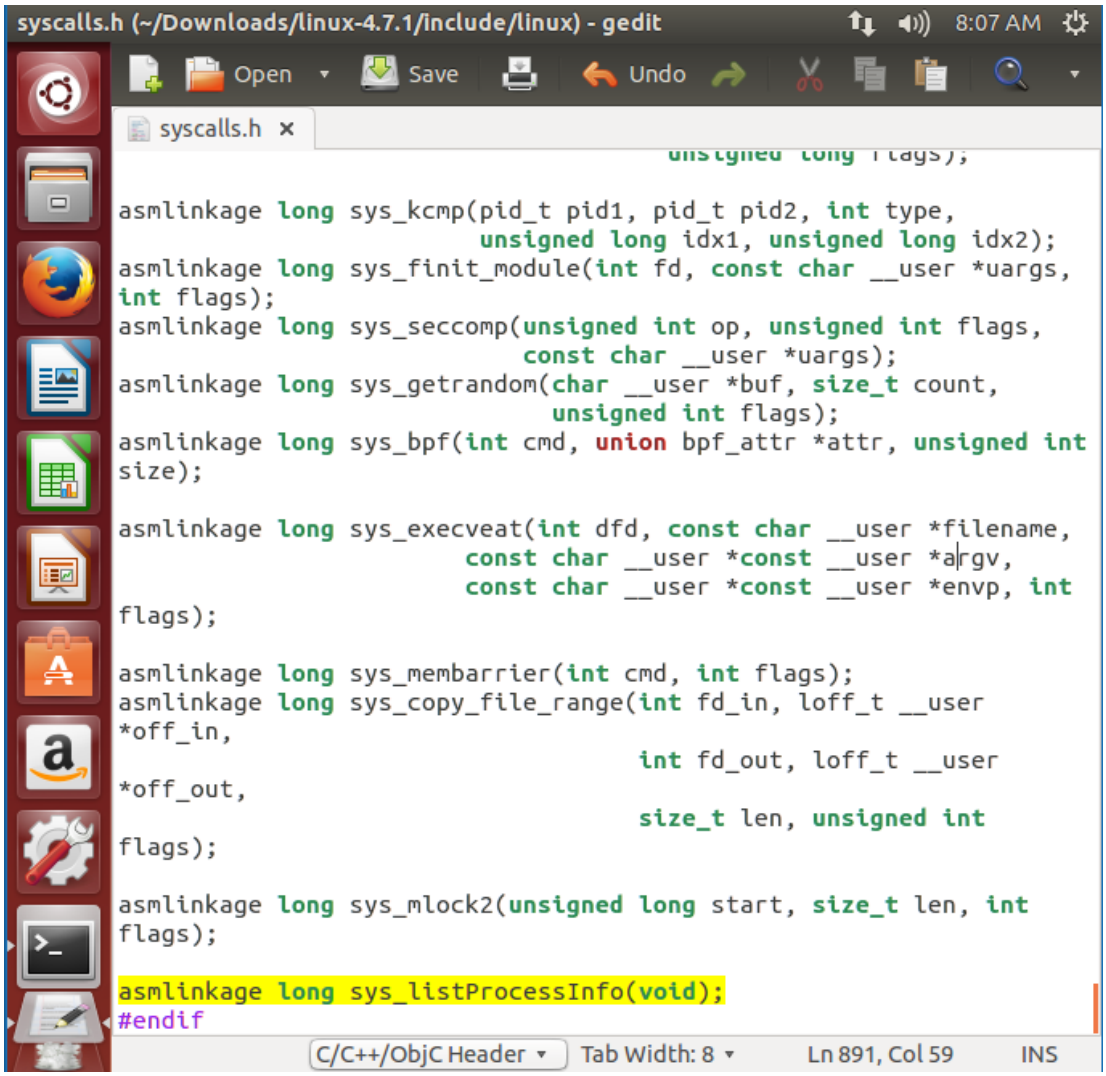


Step 9: Finally, we need to alter the 'syscalls.h' file. We again use 'find' command to find the path.

Choose the path which contains /include/linux/ and open the file using gedit.

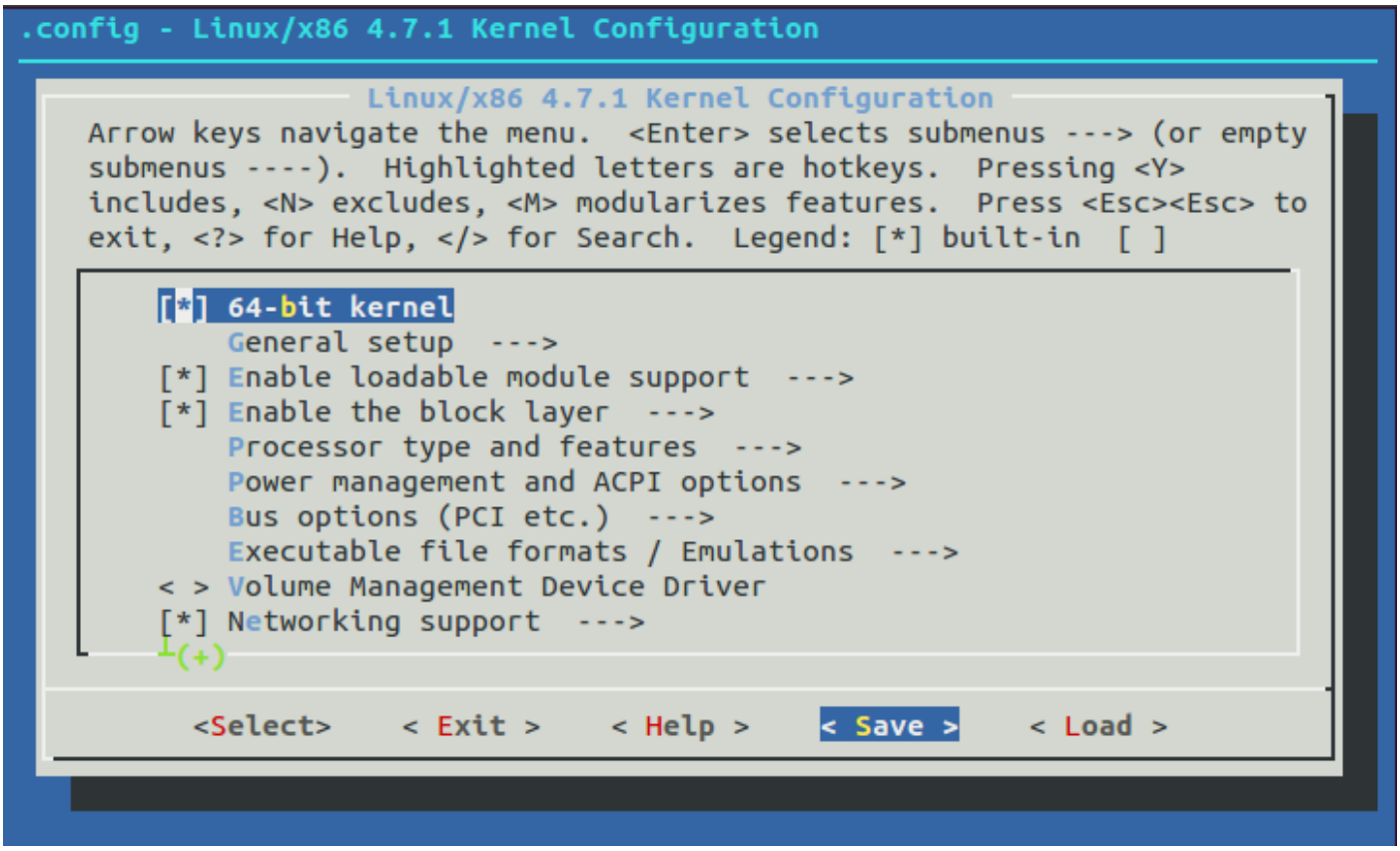
```
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ find -name syscalls.h
./arch/powerpc/include/asm/syscalls.h
./arch/sh/include/asm/syscalls.h
./arch/sparc/include/asm/syscalls.h
./arch/metag/include/asm/syscalls.h
./arch/openrisc/include/asm/syscalls.h
./arch/tile/include/asm/syscalls.h
./arch/avr32/include/asm/syscalls.h
./arch/c6x/include/asm/syscalls.h
./arch/x86/include/asm/syscalls.h
./arch/x86/um/shared/sysdep/syscalls.h
./arch/score/include/asm/syscalls.h
./arch/arc/include/asm/syscalls.h
./arch/nios2/include/asm/syscalls.h
./include/config/ftrace/syscalls.h
./include/config/advise/syscalls.h
./include/trace/events/syscalls.h
./include/linux/syscalls.h
./include/asm-generic/syscalls.h
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ gedit ./include/linux/syscal
ls.h &
[1] 2596
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$
```

Add the following line at the end of the file, just before the '#endif'



Step 10: Configure the new kernel.

```
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ cp /boot/config-$(uname -r)
.config
```



Step 11: Compile the kernel and its modules using the make command, and install the kernel.

```
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$ sudo make -j 2 && sudo make
modules_install -j 2 && sudo make install -j 2
[sudo] password for vmdhruv:
```

Compiling the kernel for the 2nd time has begun.

```
  CHK     include/generated/bounds.h
  CC      arch/x86/kernel/asm-offsets.s
  CHK     include/generated/asm-offsets.h
  CALL    scripts/checksyscalls.sh
  CC      init/main.o
  CC      arch/x86/crypto/crc32c-intel_glue.o
  CC [M]  arch/x86/crypto/glue_helper.o
  CC [M]  arch/x86/crypto/aes_glue.o
  CHK     include/generated/compile.h
  CC      init/do_mounts.o
  CC [M]  arch/x86/crypto/camellia_glue.o
  CC [M]  arch/x86/crypto/blowfish_glue.o
  CC [M]  arch/x86/crypto/twofish_glue.o
  CC      init/do_mounts_rd.o
  CC [M]  arch/x86/crypto/twofish_glue_3way.o
  CC      init/do_mounts_initrd.o
  CC      init/do_mounts_md.o
  CC [M]  arch/x86/crypto/salsa20_glue.o
  CC [M]  arch/x86/crypto/serpent_sse2_glue.o
  CC      init/initramfs.o
  CC [M]  arch/x86/crypto/aesni-intel_glue.o
  CC      init/init_task.o
  CC      init/version.o
  CC [M]  arch/x86/crypto/fpu.o
  LD      init/mounts.o
  LD      init/built-in.o
  CC [M]  arch/x86/crypto/ghash-clmulni-intel_glue.o
  CC [M]  arch/x86/crypto/sha1_ssse3_glue.o
  CC [M]  arch/x86/crypto/crc32-pclmul_glue.o
  CC      kernel/fork.o
  CC [M]  arch/x86/crypto/sha256_ssse3_glue.o
  CC [M]  arch/x86/crypto/sha512_ssse3_glue.o
  CC [M]  arch/x86/crypto/crct10dif-pclmul_glue.o
  CC [M]  arch/x86/crypto/camellia_aesni_avx_glue.o
```

Step 12: After the kernel has compiled successfully, we reboot the system.

```
  INSTALL sound/usb/caiaq/snd-usb-caiaq.ko
  INSTALL sound/usb/hiface/snd-usb-hiface.ko
  INSTALL sound/usb/misc/snd-ua101.ko
  INSTALL sound/usb/snd-usb-audio.ko
  INSTALL sound/usb/snd-usbmidi-lib.ko
  INSTALL sound/usb/usx2y/snd-usb-us122l.ko
  INSTALL sound/usb/usx2y/snd-usb-usx2y.ko
  INSTALL virt/lib/irqbypass.ko
  DEPMOD  4.7.1
sh ./arch/x86/boot/install.sh 4.7.1 arch/x86/boot/bzImage \
                System.map "/boot"
run-parts: executing /etc/kernel/postinst.d/apt-auto-removal 4.7.1 /
boot/vmlinuz-4.7.1
run-parts: executing /etc/kernel/postinst.d/initramfs-tools 4.7.1 /b
oot/vmlinuz-4.7.1
update-initramfs: Generating /boot/initrd.img-4.7.1
run-parts: executing /etc/kernel/postinst.d/pm-utils 4.7.1 /boot/vml
inuz-4.7.1
run-parts: executing /etc/kernel/postinst.d/update-notifier 4.7.1 /b
oot/vmlinuz-4.7.1
run-parts: executing /etc/kernel/postinst.d/zz-update-grub 4.7.1 /bo
ot/vmlinuz-4.7.1
Generating grub configuration file ...
Warning: Setting GRUB_TIMEOUT to a non-zero value when GRUB_HIDDEN_T
IMEOUT is set is no longer supported.
Found linux image: /boot/vmlinuz-4.7.1
Found initrd image: /boot/initrd.img-4.7.1
Found linux image: /boot/vmlinuz-4.7.1.old
Found initrd image: /boot/initrd.img-4.7.1
Found linux image: /boot/vmlinuz-3.13.0-32-generic
Found initrd image: /boot/initrd.img-3.13.0-32-generic
Found memtest86+ image: /boot/memtest86+.elf
Found memtest86+ image: /boot/memtest86+.bin
done
vmdhruv@ubuntu:~/Downloads/linux-4.7.1$
```

Step 13: To test the system call, we write a c code in the 'test.c' file and compile it.

```
#include <stdio.h>
#include <linux/kernel.h>
#include <sys/syscall.h>
#include <unistd.h>
int main()
{
    printf("Invoking 'listProcessInfo' system call");

    long int ret_status = syscall(329); // 329 is the syscall number

    if(ret_status == 0)
         printf("System call 'listProcessInfo' executed correctly. Use dmesg to check processInfo\n");

    else
         printf("System call 'listProcessInfo' did not execute as expected\n");

     return 0;
}
```

Step 14: Run the 'test.c' code.

```
vmdhruv@ubuntu:~$ uname -r
4.7.1
vmdhruv@ubuntu:~$ gedit test.c &
[1] 2463
vmdhruv@ubuntu:~$ ls
a.out    Documents  examples.desktop  Pictures  Templates  test.c~
Desktop  Downloads  Music             Public    test.c     Videos
[1]+  Done                    gedit test.c
vmdhruv@ubuntu:~$ gcc test.c
vmdhruv@ubuntu:~$ ./a.out
Invoking 'listProcessInfo' system callSystem call 'listProcessInfo'
executed correctly. Use dmesg to check processInfo
vmdhruv@ubuntu:~$
```

Step 15: Use 'dmesg' command to see the kernel log.

```
File  Edit  View  Search  Terminal  Help
[  687.934336]         Static Priority: 120
[  687.934336]         Normal Priority: 120
[  687.934339] Parent process: gnome-session,          PID_Number: 1
942
[  687.934339]
[  687.934340] Process: kworker/u256:0
[  687.934340]         PID_Number: 2445
[  687.934340]         Process State: 0
[  687.934340]         Priority: 120
[  687.934340]         RT_Priority: 0
[  687.934340]         Static Priority: 120
[  687.934340]         Normal Priority: 120
[  687.934344] Parent process: kthreadd,          PID_Number: 2
[  687.934344]
[  687.934345] Process: kworker/0:0
[  687.934345]         PID_Number: 2457
[  687.934345]         Process State: 1
[  687.934345]         Priority: 120
[  687.934345]         RT_Priority: 0
[  687.934345]         Static Priority: 120
[  687.934345]         Normal Priority: 120
[  687.934349] Parent process: kthreadd,          PID_Number: 2
[  687.934349]
[  687.934350] Process: a.out
[  687.934350]         PID_Number: 2477
[  687.934350]         Process State: 0
[  687.934350]         Priority: 120
[  687.934350]         RT_Priority: 0
[  687.934350]         Static Priority: 120
[  687.934350]         Normal Priority: 120
[  687.934353] Parent process: bash,          PID_Number: 2318
[  687.934353]
[  689.060232] systemd-hostnamed[2488]: Warning: nss-myhostname is n
ot installed. Changing the local hostname might make it unresolveabl
e. Please install nss-myhostname!
vmdhruv@ubuntu:~$
```