

CSE2005L - Operating Systems Lab

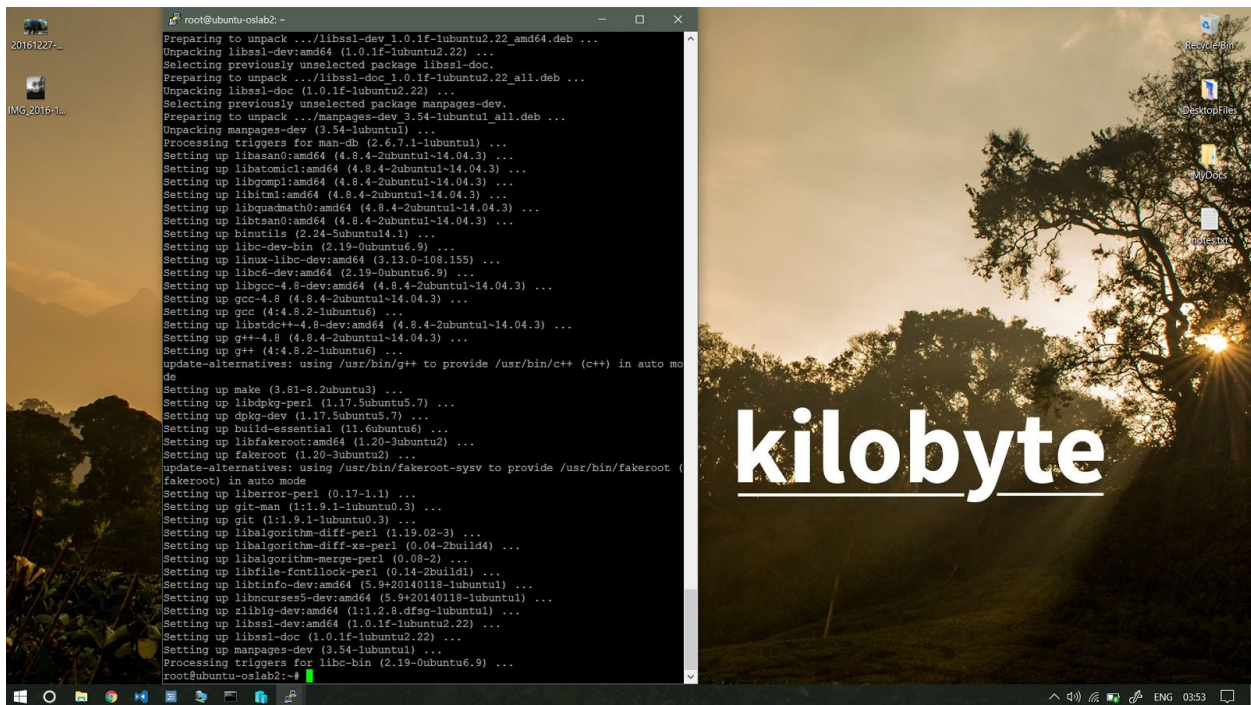
31st January, 2017

PRANAVCHENDUR T K - 15BCE1097

Implementing a System Call in the Linux Kernel

- Downloaded the kernel from kernel.org
- Install required kernel build tools

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



- Check existing Kernel Version

```
root@ubuntu-oslab2:~# uname -r  
4.4.0-62-generic
```

- Extract and set working directory to downloaded latest kernel source

```
root@ubuntu-oslab2:~# tar xf linux-4.9.8.tar.xz
```

```
root@ubuntu-oslab2:~# cd linux-4.9.8/
root@ubuntu-oslab2:~/linux-4.9.8# ls
arch  crypto    include  kernel  net      security
block Documentation init  lib      README  sound
certs drivers   ipc      MAINTAINERS REPORTING-BUGS tools
COPYING firmware Kbuild  Makefile samples  usr
CREDITS fs        Kconfig mm       scripts  virt
```

❑ System Call Definition

- **Create a new directory for new system call header files**

```
root@ubuntu-oslab2:~/linux-4.9.8# mkdir pinfo
root@ubuntu-oslab2:~/linux-4.9.8# cd pinfo/
root@ubuntu-oslab2:~/linux-4.9.8/pinfo#
```

- **Create header file**

```
root@ubuntu-oslab2:~/linux-4.9.8/pinfo# touch processInfo.h
```

- **Include line in header file**

```
root@ubuntu-oslab2:~/linux-4.9.8/pinfo# nano processInfo.h
```

```
asmlinkage long sys_listProcessInfo(void);
```

- **Create and edit listProcessInfo.c in the same directory**

```
root@ubuntu-oslab2:~/linux-4.9.8/pinfo# nano listProcessInfo.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 \
        );

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

        printk("\n\n");
    }
}

```

```
return 0;
}
```

- **Create a Makefile in the same directory**

root@ubuntu-oslab2:~/linux-4.9.8/pinfo# nano Makefile

```
obj-y:=listProcessInfo.o
```

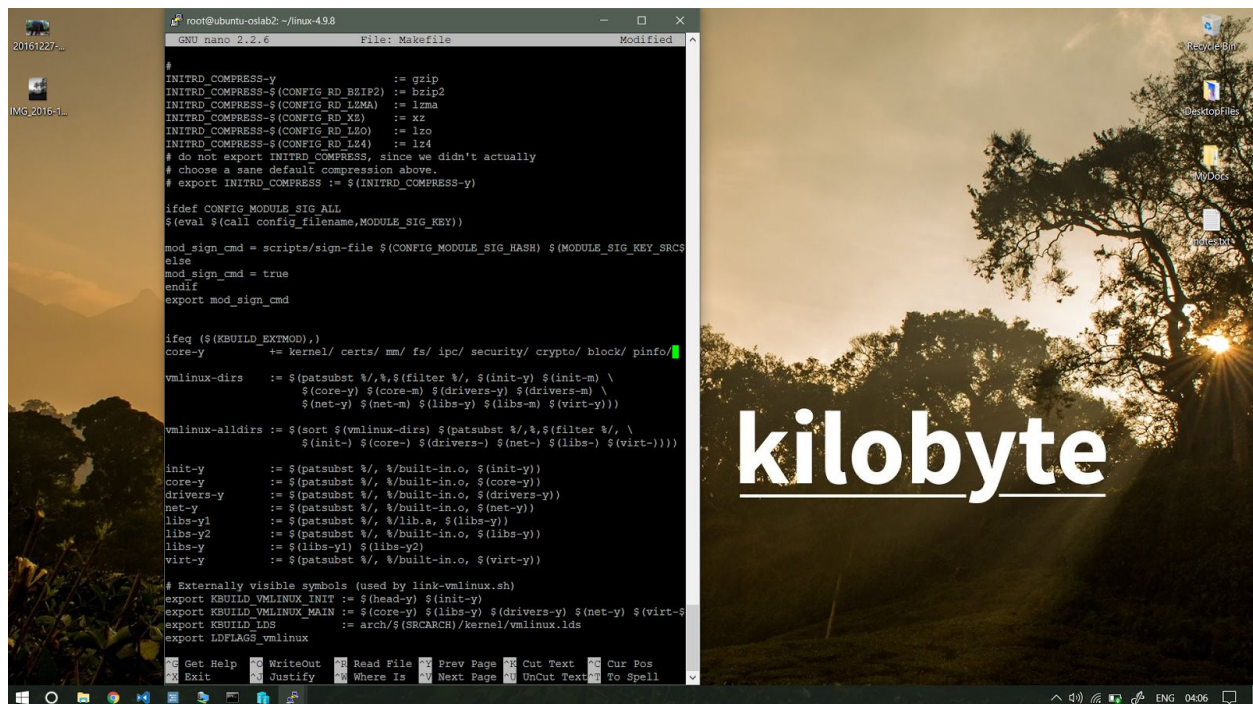
- **Modifying kernel Makefile** in the root directory to include our 'pinfo' directory

By finding

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

And modifying with

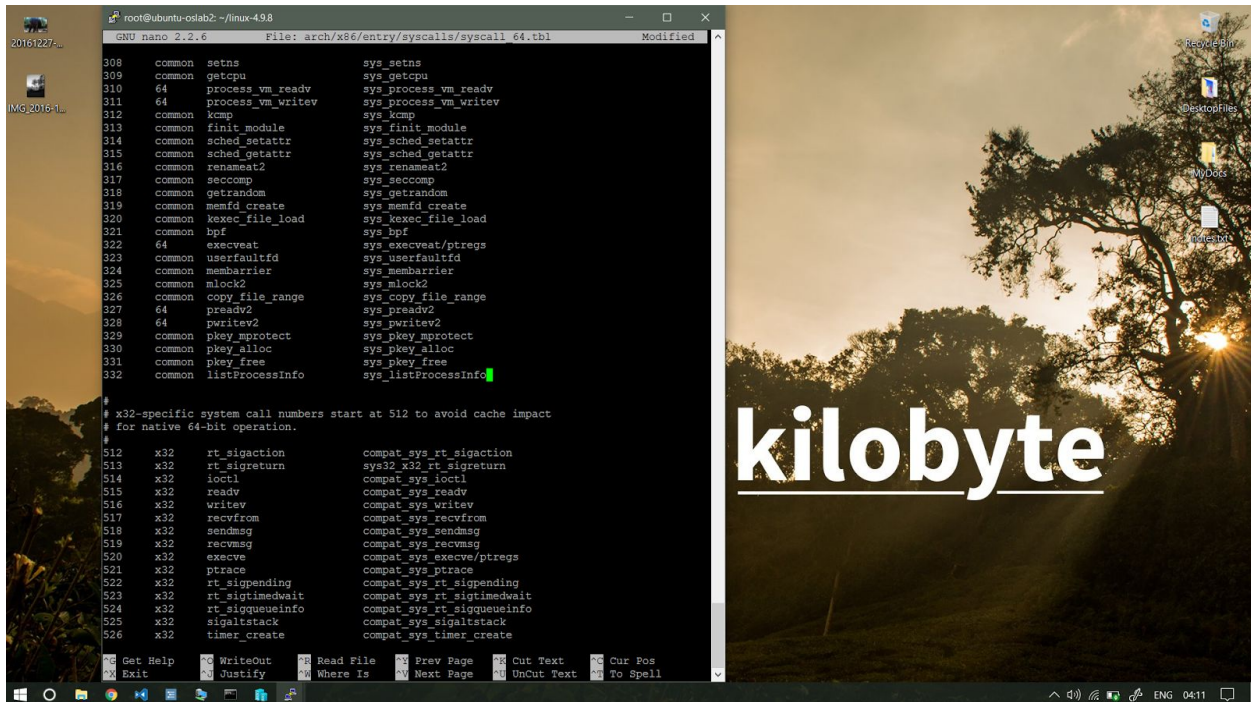
```
core -y += kernel/ mm/ fs/ ipc/ security/ crypto/ block/ pinfo/
```



- Find and modify syscall_64.tbl

```
find -name syscall_64.tbl
```

Using the above command and modify to include our system call



```
root@ubuntu-oslab2:~/linux-4.9.8# nano arch/x86/entry/syscalls/syscall_64.tbl
```

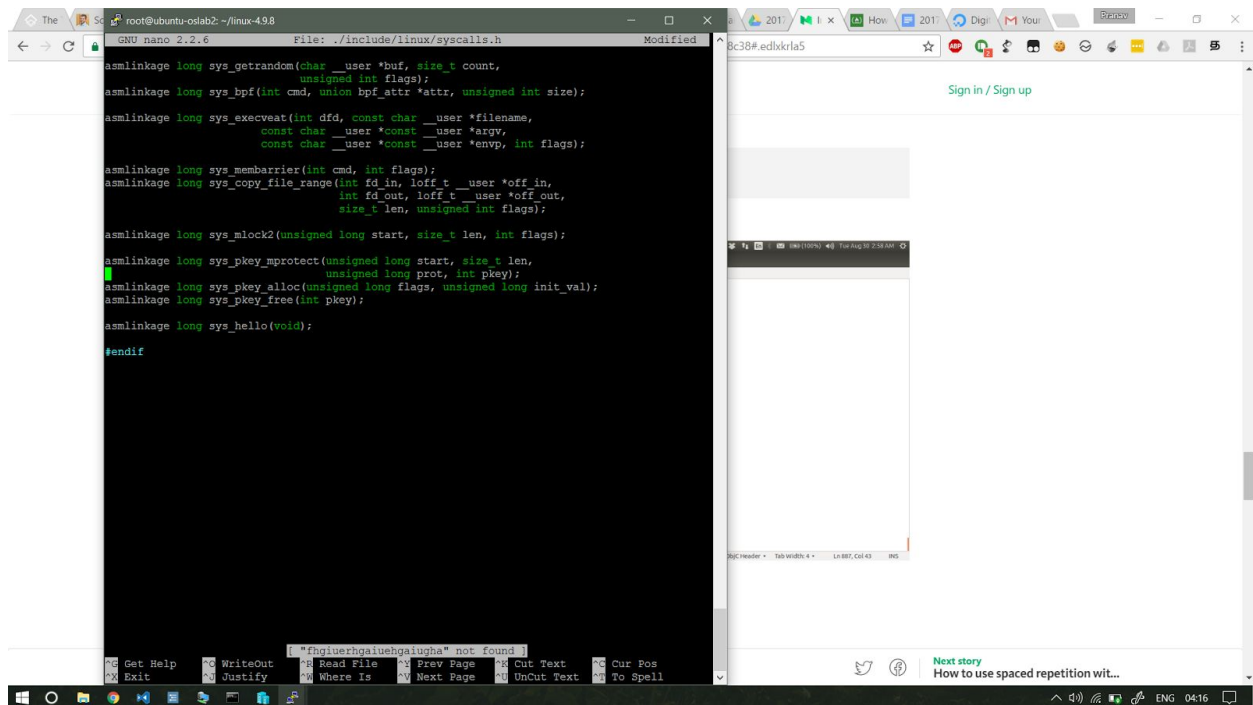
- Find and modify syscalls.h

```
root@ubuntu-oslab2:~/linux-4.9.8# find -name syscalls.h
```

```
./include/asm-generic/syscalls.h
./include/trace/events/syscalls.h
./include/linux/syscalls.h
./arch/tile/include/asm/syscalls.h
./arch/metag/include/asm/syscalls.h
./arch/x86/include/asm/syscalls.h
./arch/x86/um/shared/sysdep/syscalls.h
./arch/avr32/include/asm/syscalls.h
```


./arch/openrisc/include/asm/syscalls.h
 ./arch/score/include/asm/syscalls.h
 ./arch/nios2/include/asm/syscalls.h
 ./arch/sparc/include/asm/syscalls.h
 ./arch/powerpc/include/asm/syscalls.h
 ./arch/arc/include/asm/syscalls.h
 ./arch/sh/include/asm/syscalls.h
 ./arch/c6x/include/asm/syscalls.h

And edit file in ./include/linux



- **Copy and make previous kernel config from system**

```
root@ubuntu-oslab2:~/linux-4.9.8# cp /boot/config-$(uname -r) .config
```

Run `make menuconfig` and save changes to the .config file

```
root@ubuntu-oslab2:~/linux-4.9.8# 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:1632:warning: symbol value 'm' invalid for RXKAD
.config:3594:warning: symbol value 'm' invalid for SERIAL_8250_FINTEK
.config:7550:warning: symbol value 'm' invalid for EXT4_ENCRYPTION

```

*** End of the configuration.

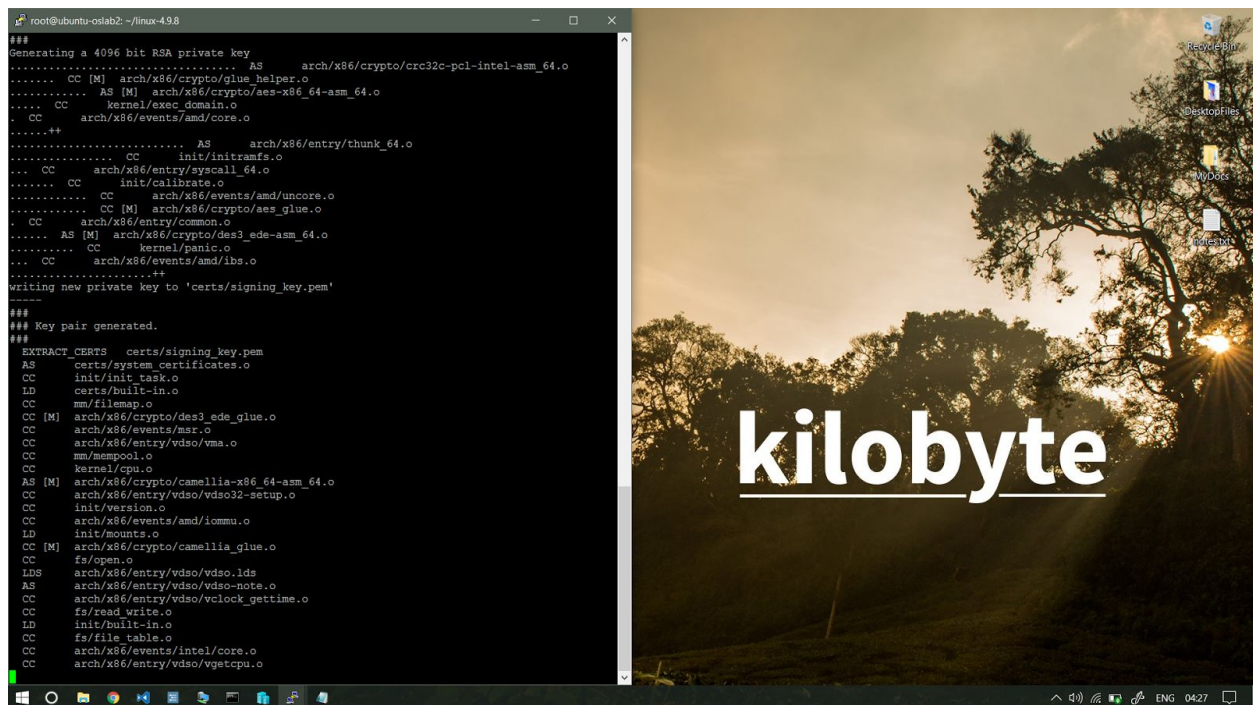
*** Execute 'make' to start the build or try 'make help'.

❑ Now, it's time to build our kernel and install it

```

sudo make -j 4 && sudo make modules_install -j 4 && sudo make
install -j 4

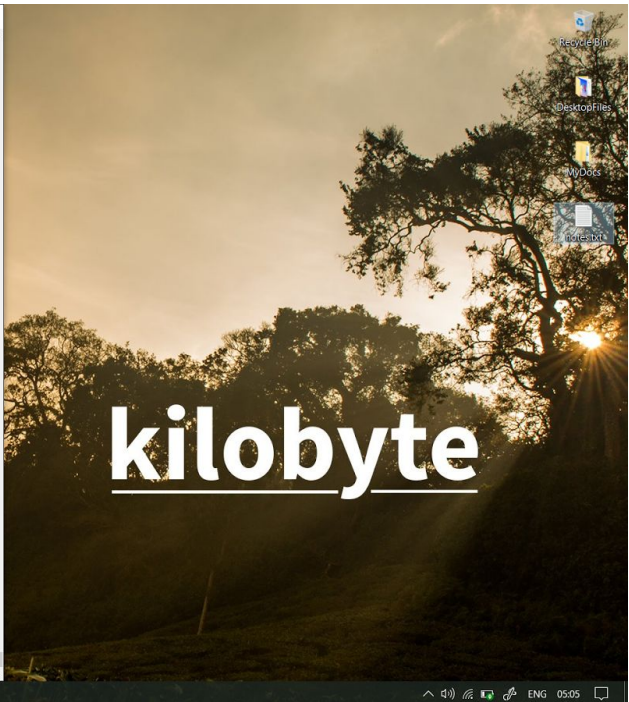
```

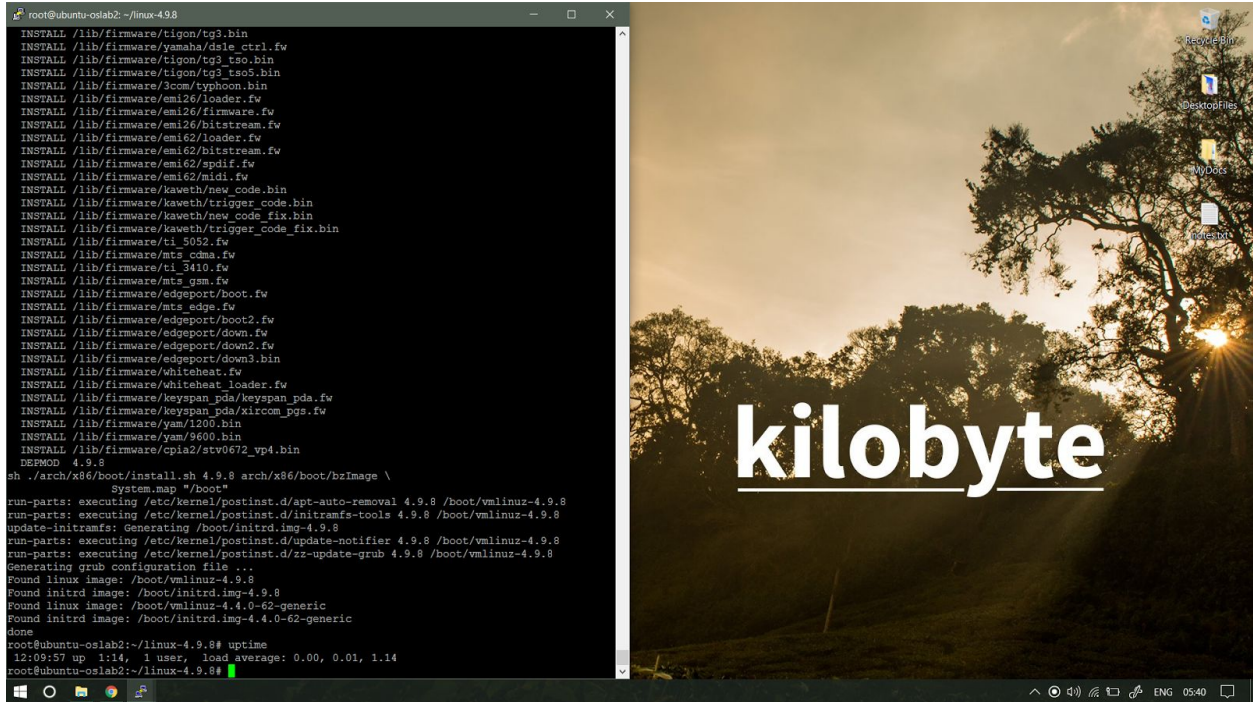


```
root@ubuntu-ct9a20: /linux-4.9.8
CC [M] net/bridge/netfilter/nft_meta_bridge.o
CC [M] net/bluetooth/btsock.o
AR arch/x86/lib/lib.a
EXPORTS arch/x86/lib/lib-kayms.o
CC [M] sound/pci/ice1712/vm8766.o
LD arch/x86/lib/built-in.o
CC [M] fs/ffs2/gc.o
CC [M] net/bridge/netfilter/nft_reject_bridge.o
CC drivers/char/misc.o
CC [M] lib/crc8.o
CC [M] sound/soc/codecs/cs35132.o
CC [M] sound/pci/ice1712/vm8776.o
CC [M] lib/bch.o
CC [M] sound/soc/codecs/cs42151.o
LD fs/jfs/built-in.o
CC [M] fs/jfs/super.o
CC drivers/char/virtio_console.o
LD [M] sound/pci/ice1712/snd-ice1712.o
CC [M] net/bridge/netfilter/nf_log_bridge.o
LD [M] sound/pci/ice1712/snd-ice17xx-ak4xxx.o
LD [M] sound/pci/ice1712/snd-ice1724.o
CC [M] fs/ffs2/symlink.o
LD [M] sound/pci/lx6464es/built-in.o
CC [M] sound/pci/lx6464es/lx6464es.o
LD net/bluetooth/bnep/built-in.o
CC [M] net/bluetooth/bnep/core.o
CC [M] fs/ffs2/build.o
CC [M] lib/ts_kmp.o
CC [M] sound/soc/codecs/cs42151-i2c.o
CC [M] fs/jfs/file.o
CC [M] net/bridge/netfilter/ebtables.o
CC [M] lib/ts_hm.o
CC [M] sound/pci/lx6464es/lx_core.o
CC [M] fs/ffs2/erase.o
CC [M] fs/jfs/inode.o
CC [M] sound/soc/codecs/cs42152.o
CC drivers/char/hpet.o
CC [M] net/bluetooth/bnep/sock.o
CC [M] lib/ts_fm.o
CC [M] fs/ffs2/background.o
LD [M] sound/pci/lx6464es/snd-lx6464es.o
CC [M] lib/notifier-error-inject.o
LD sound/pci/mixart/built-in.o
CC [M] fs/jfs/namei.o
CC [M] sound/pci/mixart/mixart.o
CC [M] sound/soc/codecs/cs42156.o
CC [M] net/bluetooth/bnep/netdev.o
CC [M] fs/ffs2/fs.o
CC drivers/char/agp/backend.o
```



```
root@ubuntu-ct9a20: /linux-4.9.8
CC arch/x86/boot/memory.o
CC arch/x86/boot/pm.o
AS arch/x86/boot/pmjump.o
CC arch/x86/boot/printk.o
CC arch/x86/boot/regs.o
CC arch/x86/boot/string.o
CC arch/x86/boot/tty.o
LDS arch/x86/boot/compressed/vmlinux.lds
CC arch/x86/boot/video.o
MODPOST 4552 modules
AS arch/x86/boot/compressed/head_64.o
VOFFSET arch/x86/boot/compressed/./voffset.h
CC arch/x86/boot/compressed/string.o
CC arch/x86/boot/video-mode.o
CC arch/x86/boot/version.o
CC arch/x86/boot/video-vga.o
CC arch/x86/boot/compressed/cmdline.o
CC arch/x86/boot/video-vesa.o
CC arch/x86/boot/compressed/error.o
CC arch/x86/boot/video-bios.o
HOSTCC arch/x86/boot/tools/build
OBJCOPY arch/x86/boot/compressed/vmlinux.bin
RELOCS arch/x86/boot/compressed/vmlinux.relocs
HOSTCC arch/x86/boot/compressed/mkpiggy
CC arch/x86/boot/compressed/cpuflags.o
CC arch/x86/boot/compressed/early_serial_console.o
CC arch/x86/boot/compressed/kaslr.o
CPUSTR arch/x86/boot/cpustr.h
CC arch/x86/boot/compressed/pagetable.o
CC arch/x86/boot/compressed/eboot.o
CC arch/x86/boot/cpu.o
AS arch/x86/boot/compressed/efi_stub_64.o
AS arch/x86/boot/compressed/efi_thunk_64.o
CC arch/x86/boot/compressed/mult.o
GZIP arch/x86/boot/compressed/vmlinux.bin.gz
MKPIGGY arch/x86/boot/compressed/piggy.S
AS arch/x86/boot/compressed/piggy.o
DATAREL arch/x86/boot/compressed/vmlinux
LD arch/x86/boot/compressed/vmlinux
ZOFFSET arch/x86/boot/zoffset.h
OBJCOPY arch/x86/boot/vmlinux.bin
AS arch/x86/boot/header.o
LD arch/x86/boot/setup.elf
OBJCOPY arch/x86/boot/setup.bin
BUILD arch/x86/boot/bzImage
Setup is 17148 bytes (padded to 17408 bytes).
System is 6967 kB
CRC 60b9adb6
Kernel: arch/x86/boot/bzImage is ready (#1)
```





□ Testing

- Create a test.c C program in any directory with the following code

```
#include <stdio.h>

#include <linux/kernel.h>

#include <sys/syscall.h>

#include <unistd.h>
int main()
{
```

```

printf("Invoking 'listProcessInfo' system call");

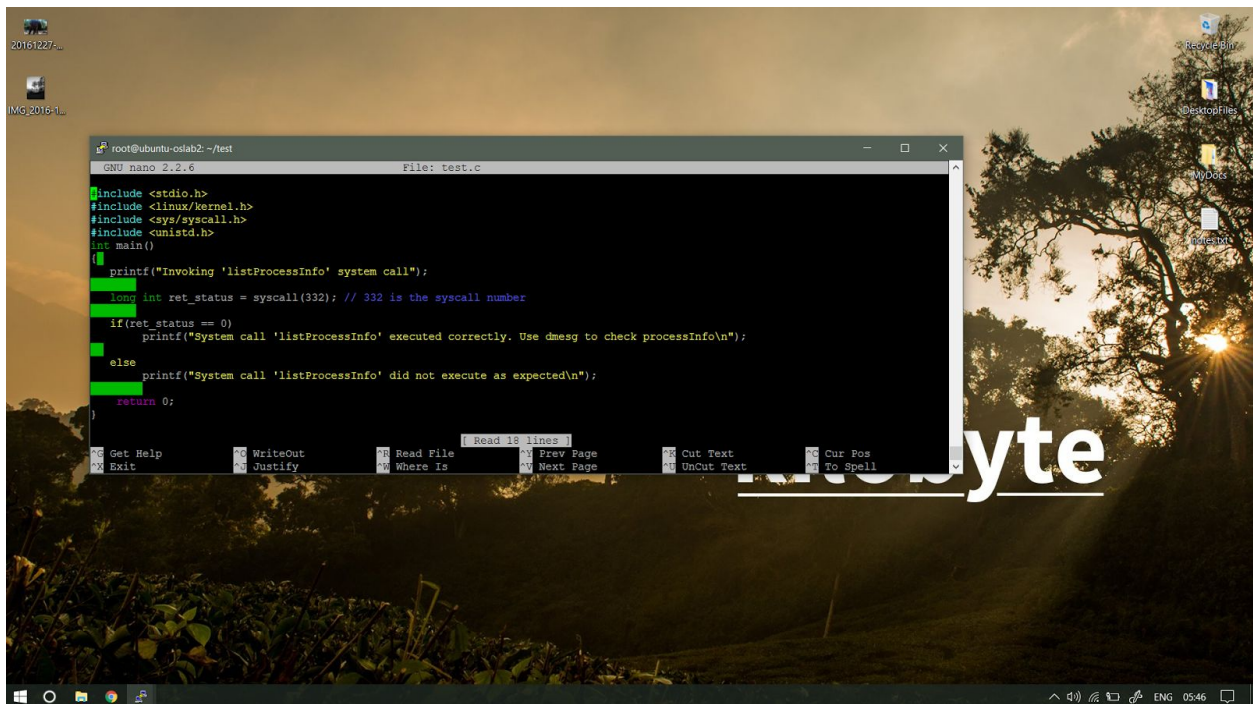
long int ret_status = syscall(332); // 332 is the syscall
number

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;
}

```



- **Compile and run the program**

```

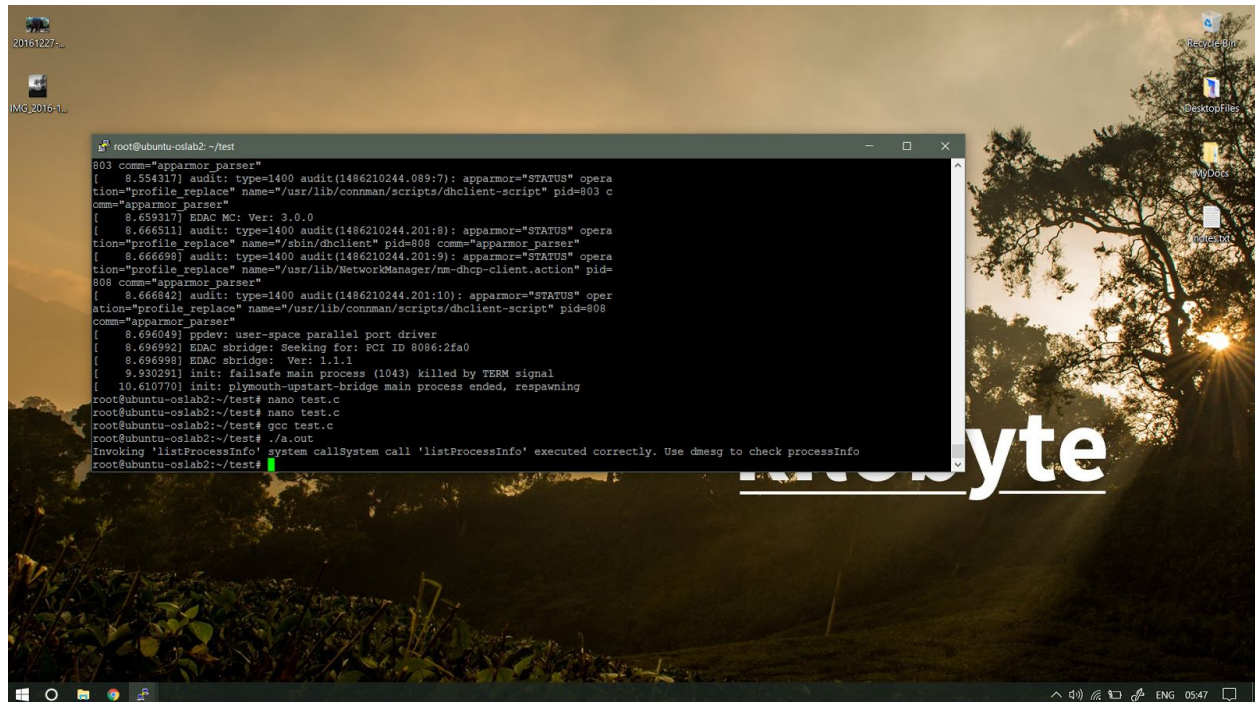
root@ubuntu-oslab2:~# mkdir test
root@ubuntu-oslab2:~# cd test/
root@ubuntu-oslab2:~/test# nano test.c

```

```

root@ubuntu-oslab2:~/test# gcc test.c
root@ubuntu-oslab2:~/test# ./a.out
Invoking 'listProcessInfo' system call
System call 'listProcessInfo' executed correctly. Use dmesg to check
processInfo

```



- Once, the program is executed, check `$ dmesg`

This will give the system log in which the process info will be printed since the processInfo is implemented as a system call

```

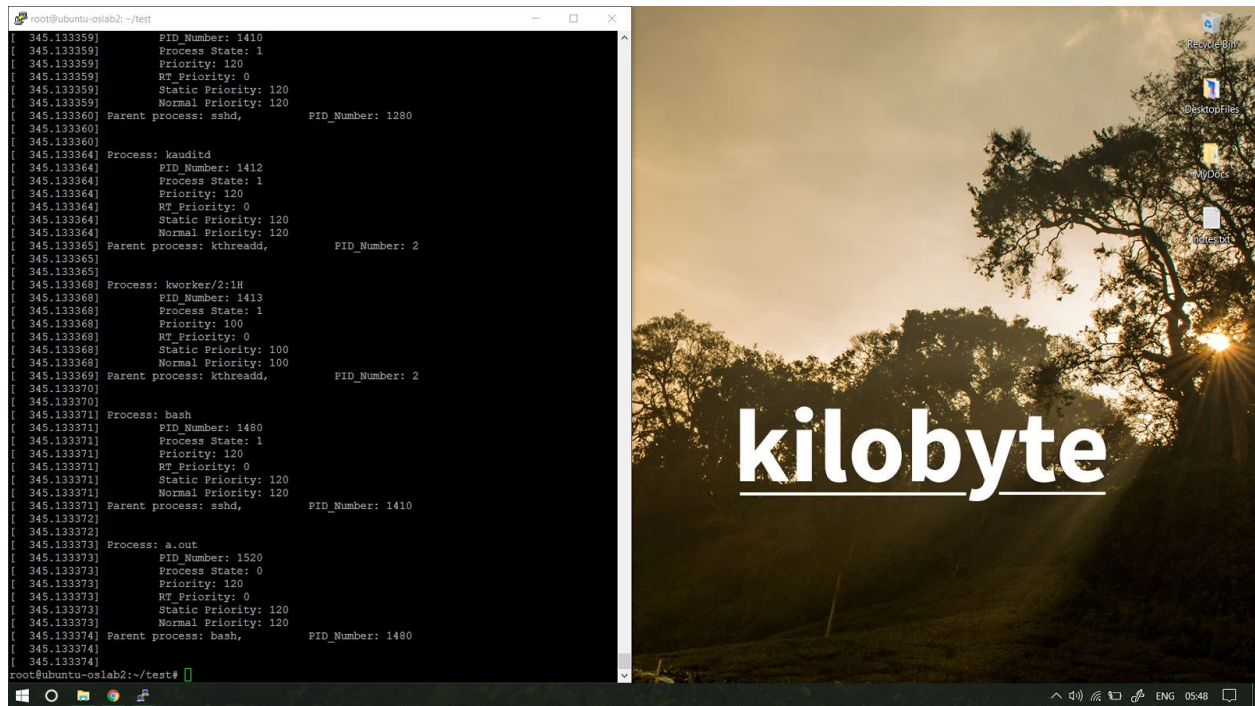
[ 345.132822] Process: init
[ 345.132822]     PID_Number: 1
[ 345.132822]     Process State: 1
[ 345.132822]     Priority: 120
[ 345.132822]     RT_Priority: 0
[ 345.132822]     Static Priority: 120
[ 345.132822]     Normal Priority: 120
[ 345.132825] Parent process: swapper/0,     PID_Number: 0
[ 345.132839]
[ 345.132839]

```

[345.132841] Process: kthreadd
[345.132841] PID_Number: 2
[345.132841] Process State: 1
[345.132841] Priority: 120
[345.132841] RT_Priority: 0
[345.132841] Static Priority: 120
[345.132841] Normal Priority: 120
[345.132842] Parent process: swapper/0, PID_Number: 0
[345.132843]

.
.
.
.
.
.
.

[345.133371] Process: bash
[345.133371] PID_Number: 1480
[345.133371] Process State: 1
[345.133371] Priority: 120
[345.133371] RT_Priority: 0
[345.133371] Static Priority: 120
[345.133371] Normal Priority: 120
[345.133371] Parent process: sshd, PID_Number: 1410
[345.133372]
[345.133372]
[345.133373] Process: a.out
[345.133373] PID_Number: 1520
[345.133373] Process State: 0
[345.133373] Priority: 120
[345.133373] RT_Priority: 0
[345.133373] Static Priority: 120
[345.133373] Normal Priority: 120
[345.133374] Parent process: bash, PID_Number: 1480
[345.133374]
[345.133374]



Kernel Build & Test Machine - Configuration

DigitalOcean - 4 Cores - 8GB Ram - 80GB SSD - Ubuntu 14.04.6 x64

