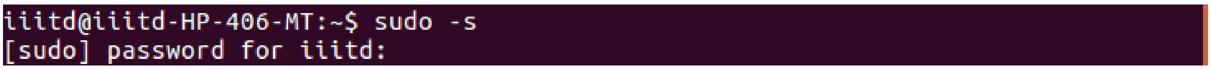
MT18052_Lab2 Assignment

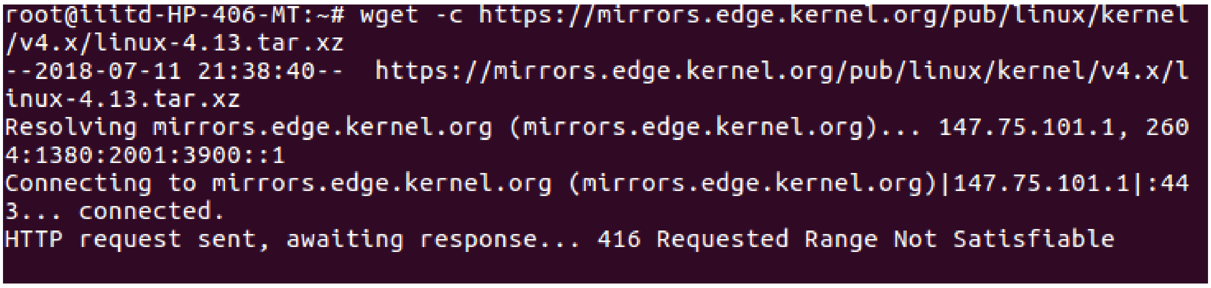
Adding a System Call to Linux Kernel

Step 1: Switch to root user to avoid typing sudo again and again.



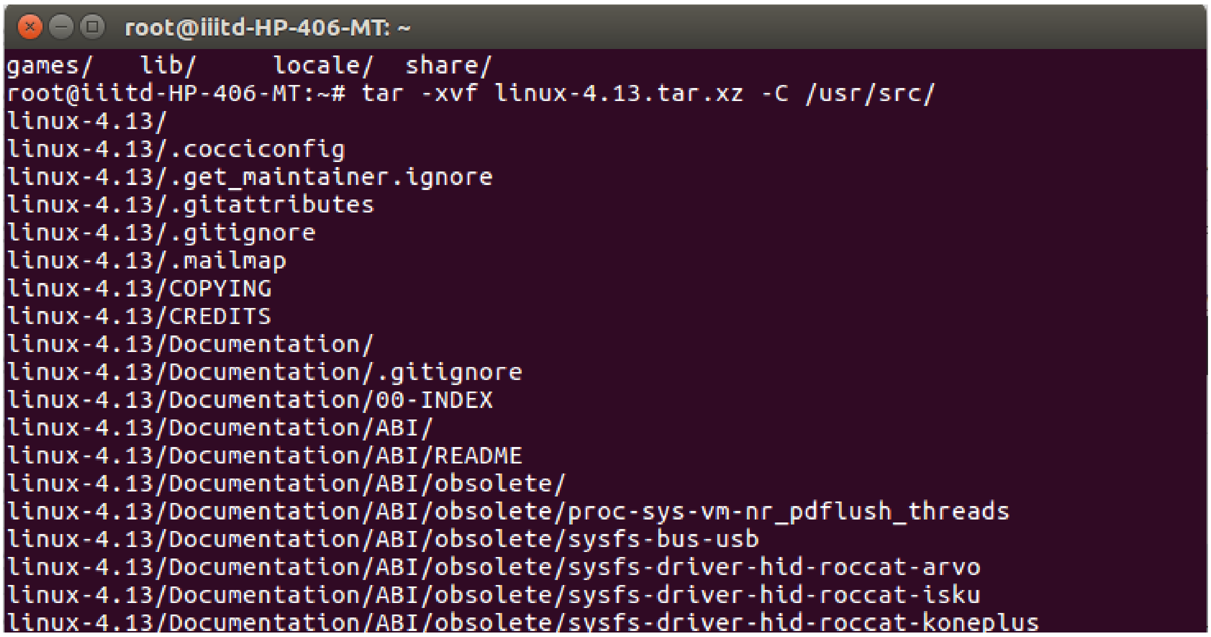
```
iiitd@iiitd-HP-406-MT:~$ sudo -s
[sudo] password for iiitd:
```

Step 2: Download kernel



```
root@iiitd-HP-406-MT:~# wget -c https://mirrors.edge.kernel.org/pub/linux/kernel
/v4.x/linux-4.13.tar.xz
--2018-07-11 21:38:40--  https://mirrors.edge.kernel.org/pub/linux/kernel/v4.x/l
inux-4.13.tar.xz
Resolving mirrors.edge.kernel.org (mirrors.edge.kernel.org)... 147.75.101.1, 260
4:1380:2001:3900::1
Connecting to mirrors.edge.kernel.org (mirrors.edge.kernel.org)|147.75.101.1|:44
3... connected.
HTTP request sent, awaiting response... 416 Requested Range Not Satisfiable
```

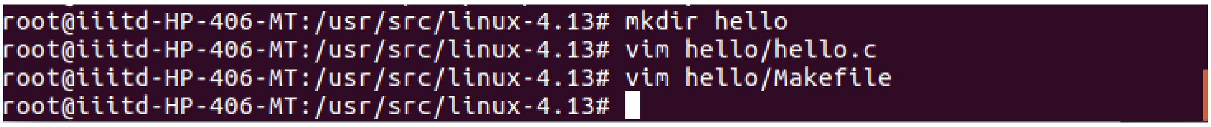
Step 3: Extract tar file to /usr/src



root@iiitd-HP-406-MT: ~

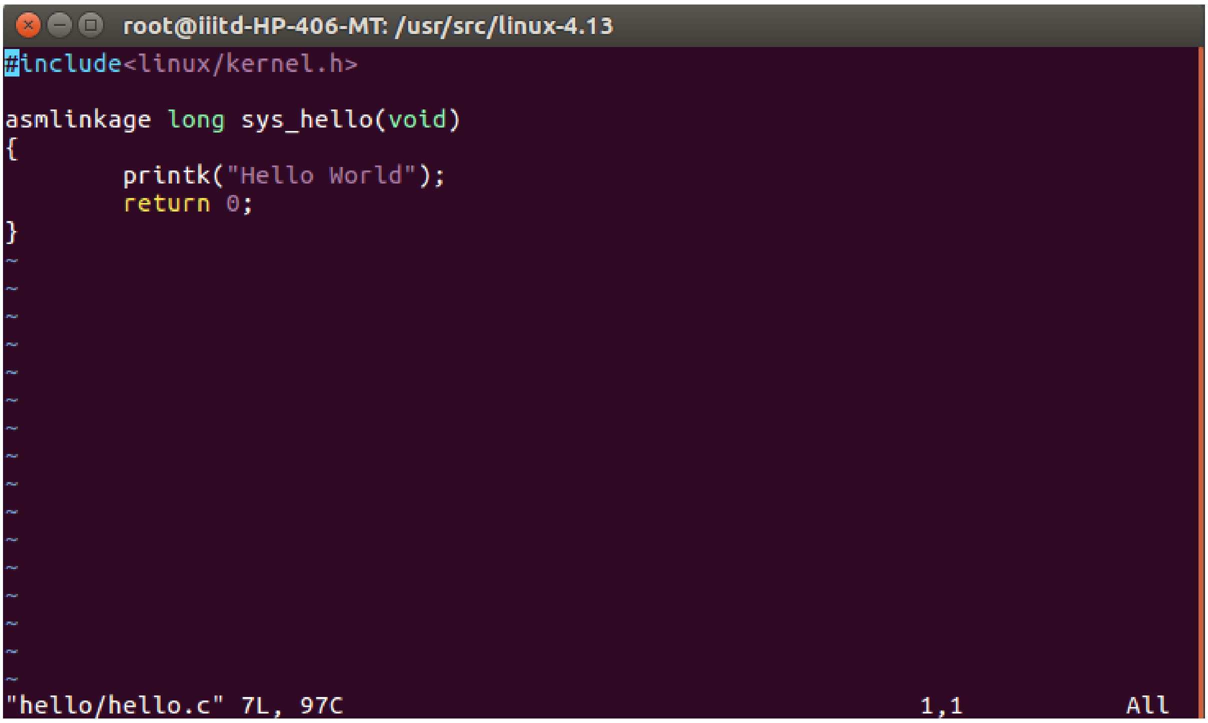
```
games/   lib/     locale/  share/
root@iiitd-HP-406-MT:~# tar -xvf linux-4.13.tar.xz -C /usr/src/
linux-4.13/
linux-4.13/.cocciconfig
linux-4.13/.get_maintainer.ignore
linux-4.13/.gitattributes
linux-4.13/.gitignore
linux-4.13/.mailmap
linux-4.13/COPYING
linux-4.13/CREDITS
linux-4.13/Documentation/
linux-4.13/Documentation/.gitignore
linux-4.13/Documentation/00-INDEX
linux-4.13/Documentation/ABI/
linux-4.13/Documentation/ABI/README
linux-4.13/Documentation/ABI/obsolete/
linux-4.13/Documentation/ABI/obsolete/proc-sys-vm-nr_pdflush_threads
linux-4.13/Documentation/ABI/obsolete/sysfs-bus-usb
linux-4.13/Documentation/ABI/obsolete/sysfs-driver-hid-roccat-arvo
linux-4.13/Documentation/ABI/obsolete/sysfs-driver-hid-roccat-isku
linux-4.13/Documentation/ABI/obsolete/sysfs-driver-hid-roccat-koneplus
```

Step 4: make hello directory and add hello.c and Makefile to compile hello.c



```
root@iiitd-HP-406-MT:/usr/src/linux-4.13# mkdir hello
root@iiitd-HP-406-MT:/usr/src/linux-4.13# vim hello/hello.c
root@iiitd-HP-406-MT:/usr/src/linux-4.13# vim hello/Makefile
root@iiitd-HP-406-MT:/usr/src/linux-4.13# 
```

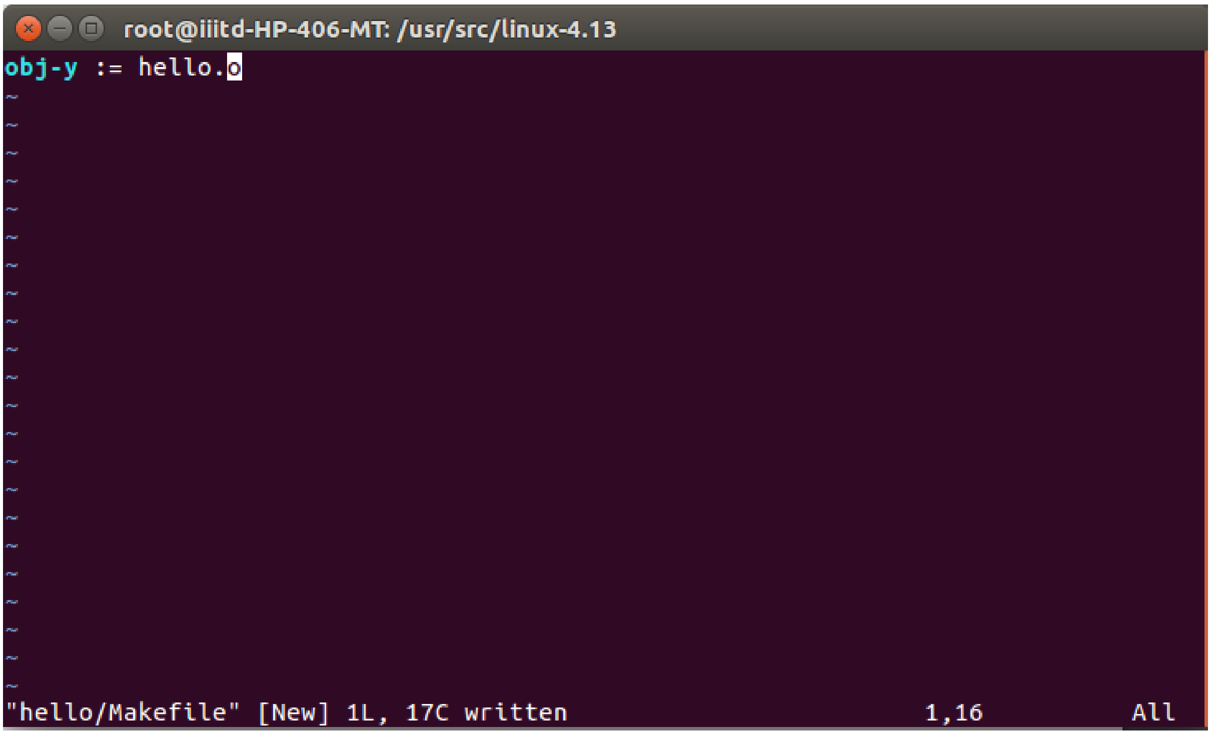
hello.c content



root@iiitd-HP-406-MT: /usr/src/linux-4.13

```
#include<linux/kernel.h>

asmlinkage long sys_hello(void)
{
        printk("Hello World");
        return 0;
}
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"hello/hello.c" 7L, 97C                                       1,1           All
```

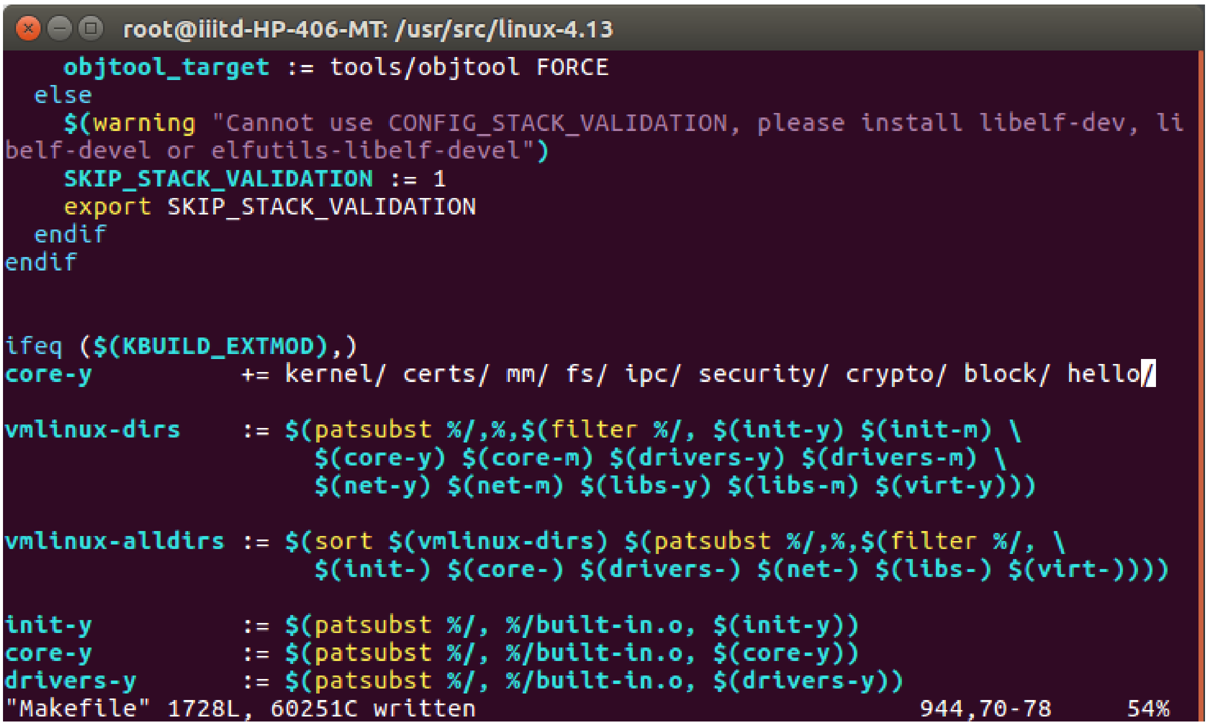
Content of Makefile in hello directory



root@iiitd-HP-406-MT: /usr/src/linux-4.13

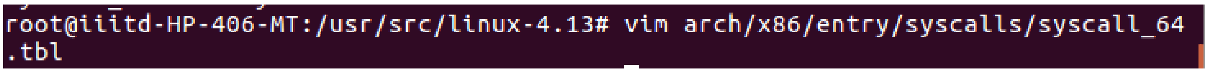
```
obj-y := hello.o
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"hello/Makefile" [New] 1L, 17C written                         1,16          All
```

Step 5: Add hello directory path to kernel compilation Makefile



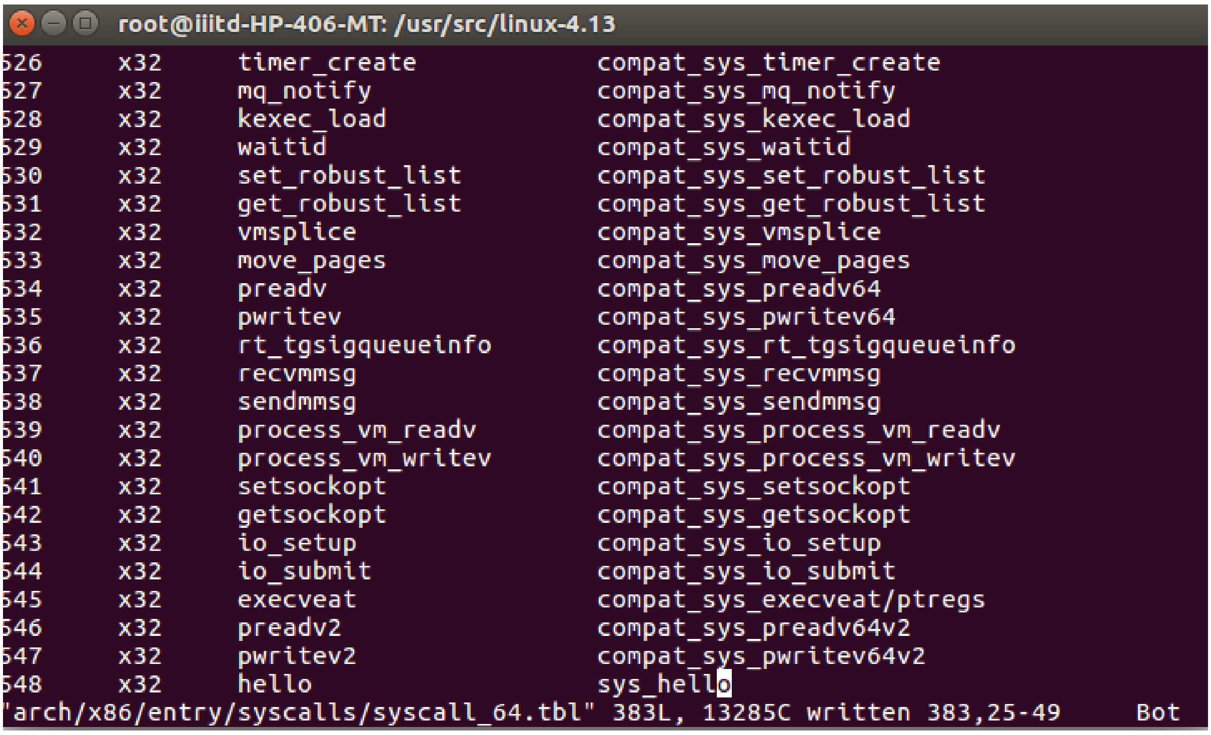
```
    objtool_target := tools/objtool FORCE
  else
    $(warning "Cannot use CONFIG_STACK_VALIDATION, please install libelf-dev, li
belf-devel or elfutils-libelf-devel")
    SKIP_STACK_VALIDATION := 1
    export SKIP_STACK_VALIDATION
  endif
endif


ifeq ($(KBUILD_EXTMOD),)
core-y          += kernel/ certs/ mm/ fs/ ipc/ security/ crypto/ block/ hello/

vmlinux-dirs    := $(patsubst %/,%,$(filter %/, $(init-y) $(init-m) \
                     $(core-y) $(core-m) $(drivers-y) $(drivers-m) \
                     $(net-y) $(net-m) $(libs-y) $(libs-m) $(virt-y)))

vmlinux-alldirs := $(sort $(vmlinux-dirs) $(patsubst %/,%,$(filter %/, \
                     $(init-) $(core-) $(drivers-) $(net-) $(libs-) $(virt-))))

init-y          := $(patsubst %/, %/built-in.o, $(init-y))
core-y          := $(patsubst %/, %/built-in.o, $(core-y))
drivers-y       := $(patsubst %/, %/built-in.o, $(drivers-y))
"Makefile" 1728L, 60251C written                              944,70-78      54%
```

Step 6: Add system call to syscall_64.tbl



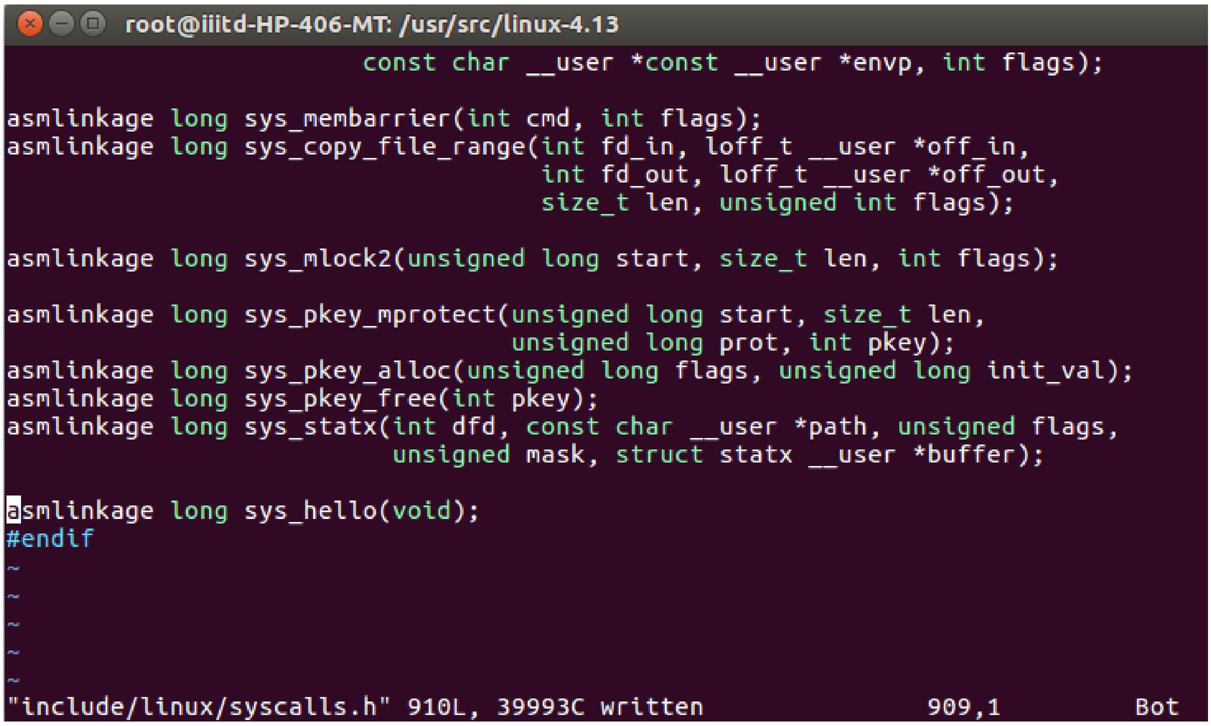
```
root@iiitd-HP-406-MT:/usr/src/linux-4.13# vim arch/x86/entry/syscalls/syscall_64
.tbl
```

syscall_64.tbl content



```
526     x32     timer_create            compat_sys_timer_create
527     x32     mq_notify               compat_sys_mq_notify
528     x32     kexec_load              compat_sys_kexec_load
529     x32     waitid                  compat_sys_waitid
530     x32     set_robust_list         compat_sys_set_robust_list
531     x32     get_robust_list         compat_sys_get_robust_list
532     x32     vmsplice                compat_sys_vmsplice
533     x32     move_pages              compat_sys_move_pages
534     x32     preadv                  compat_sys_preadv64
535     x32     pwritev                 compat_sys_pwritev64
536     x32     rt_tgsigqueueinfo       compat_sys_rt_tgsigqueueinfo
537     x32     recvmmsg                compat_sys_recvmmsg
538     x32     sendmmsg                compat_sys_sendmmsg
539     x32     process_vm_readv        compat_sys_process_vm_readv
540     x32     process_vm_writev       compat_sys_process_vm_writev
541     x32     setsockopt              compat_sys_setsockopt
542     x32     getsockopt              compat_sys_getsockopt
543     x32     io_setup                compat_sys_io_setup
544     x32     io_submit               compat_sys_io_submit
545     x32     execveat                compat_sys_execveat/ptregs
546     x32     preadv2                 compat_sys_preadv64v2
547     x32     pwritev2                compat_sys_pwritev64v2
548     x32     hello                   sys_hello
"arch/x86/entry/syscalls/syscall_64.tbl" 383L, 13285C written 383,25-49     Bot
```

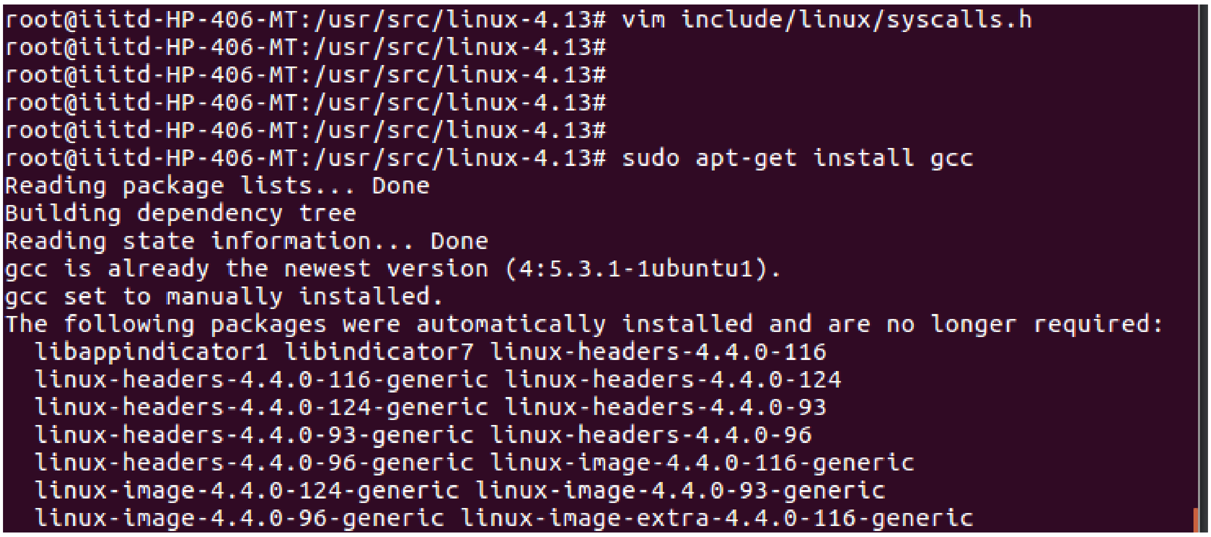
Step 7: add sys_hello system call definition to include/linux/syscalls.h file



```
                        const char __user *const __user *envp, int flags);

asmlinkage long sys_membarrier(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_hello(void);
#endif
~
~
~
~
~
"include/linux/syscalls.h" 910L, 39993C written               909,1         Bot
```

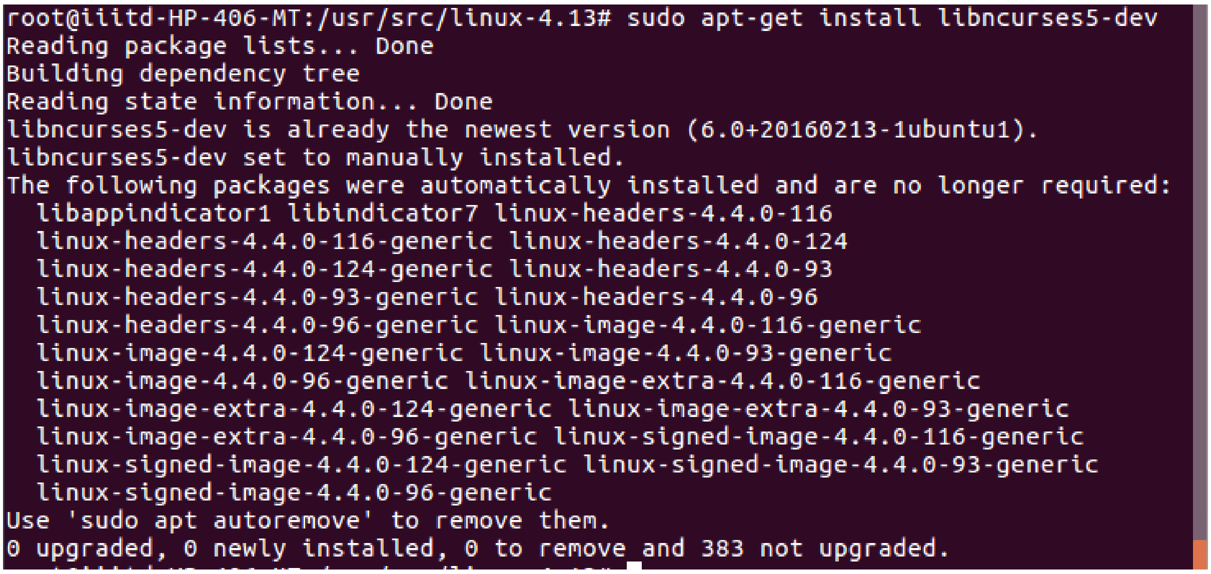
Step 8: Update gcc

apt-get install gcc



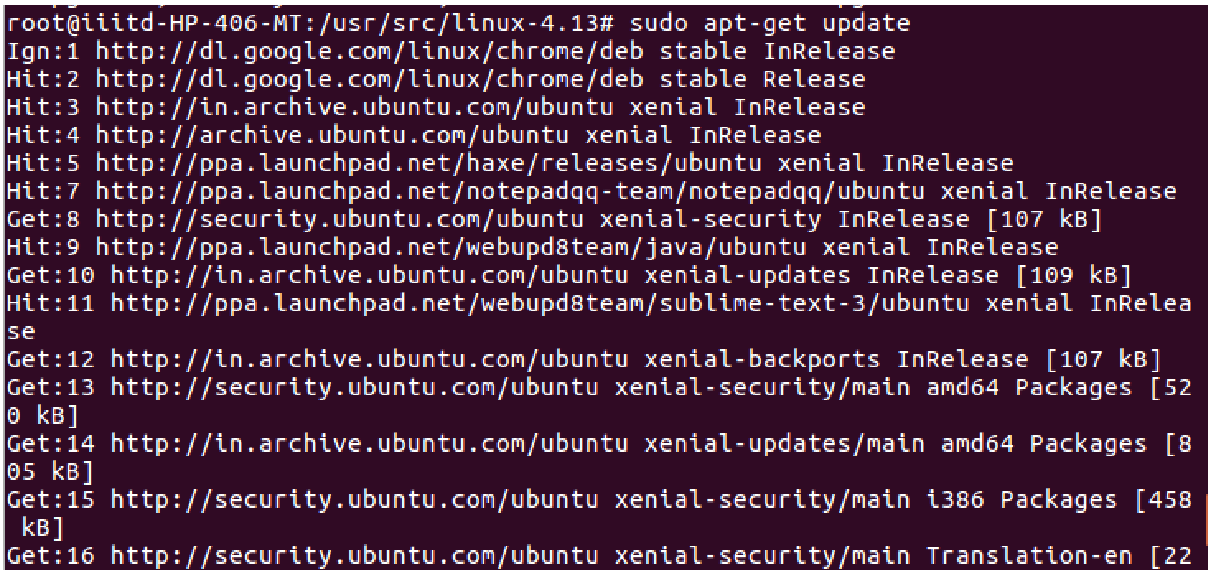
```
root@iiitd-HP-406-MT:/usr/src/linux-4.13# vim include/linux/syscalls.h
root@iiitd-HP-406-MT:/usr/src/linux-4.13#
root@iiitd-HP-406-MT:/usr/src/linux-4.13#
root@iiitd-HP-406-MT:/usr/src/linux-4.13#
root@iiitd-HP-406-MT:/usr/src/linux-4.13#
root@iiitd-HP-406-MT:/usr/src/linux-4.13# sudo apt-get install gcc
Reading package lists... Done
Building dependency tree
Reading state information... Done
gcc is already the newest version (4:5.3.1-1ubuntu1).
gcc set to manually installed.
The following packages were automatically installed and are no longer required:
  libappindicator1 libindicator7 linux-headers-4.4.0-116
  linux-headers-4.4.0-116-generic linux-headers-4.4.0-124
  linux-headers-4.4.0-124-generic linux-headers-4.4.0-93
  linux-headers-4.4.0-93-generic linux-headers-4.4.0-96
  linux-headers-4.4.0-96-generic linux-image-4.4.0-116-generic
  linux-image-4.4.0-124-generic linux-image-4.4.0-93-generic
  linux-image-4.4.0-96-generic linux-image-extra-4.4.0-116-generic
```

Step 9: apt-get install libncurses5-dev



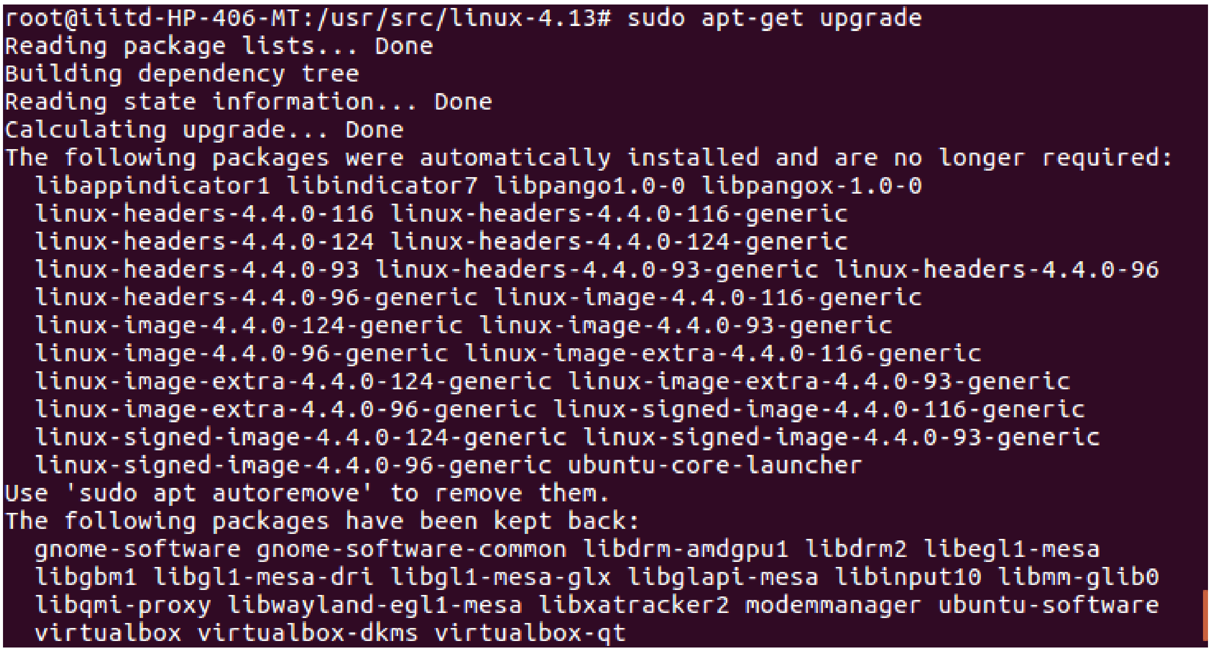
```
root@iiitd-HP-406-MT:/usr/src/linux-4.13# sudo apt-get install libncurses5-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
libncurses5-dev is already the newest version (6.0+20160213-1ubuntu1).
libncurses5-dev set to manually installed.
The following packages were automatically installed and are no longer required:
  libappindicator1 libindicator7 linux-headers-4.4.0-116
  linux-headers-4.4.0-116-generic linux-headers-4.4.0-124
  linux-headers-4.4.0-124-generic linux-headers-4.4.0-93
  linux-headers-4.4.0-93-generic linux-headers-4.4.0-96
  linux-headers-4.4.0-96-generic linux-image-4.4.0-116-generic
  linux-image-4.4.0-124-generic linux-image-4.4.0-93-generic
  linux-image-4.4.0-96-generic linux-image-extra-4.4.0-116-generic
  linux-image-extra-4.4.0-124-generic linux-image-extra-4.4.0-93-generic
  linux-image-extra-4.4.0-96-generic linux-signed-image-4.4.0-116-generic
  linux-signed-image-4.4.0-124-generic linux-signed-image-4.4.0-93-generic
  linux-signed-image-4.4.0-96-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 383 not upgraded.
```

Step 10: apt-get update



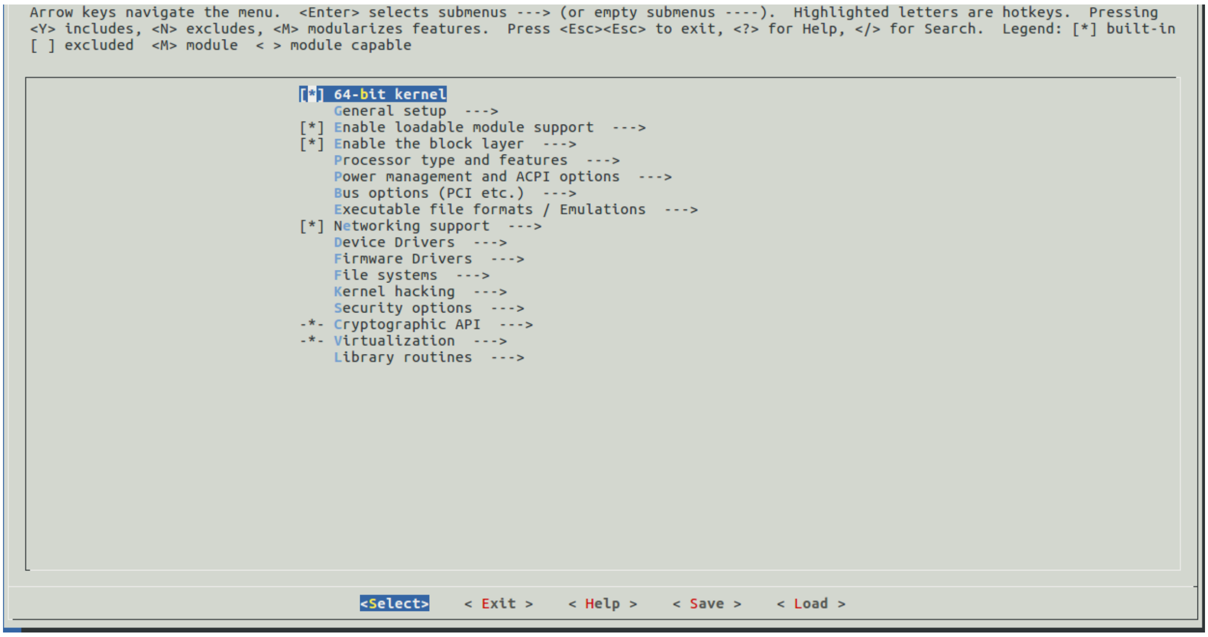
```
root@iiitd-HP-406-MT:/usr/src/linux-4.13# sudo apt-get update
Ign:1 http://dl.google.com/linux/chrome/deb stable InRelease
Hit:2 http://dl.google.com/linux/chrome/deb stable Release
Hit:3 http://in.archive.ubuntu.com/ubuntu xenial InRelease
Hit:4 http://archive.ubuntu.com/ubuntu xenial InRelease
Hit:5 http://ppa.launchpad.net/haxe/releases/ubuntu xenial InRelease
Hit:7 http://ppa.launchpad.net/notepadqq-team/notepadqq/ubuntu xenial InRelease
Get:8 http://security.ubuntu.com/ubuntu xenial-security InRelease [107 kB]
Hit:9 http://ppa.launchpad.net/webupd8team/java/ubuntu xenial InRelease
Get:10 http://in.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Hit:11 http://ppa.launchpad.net/webupd8team/sublime-text-3/ubuntu xenial InRelea
se
Get:12 http://in.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Get:13 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [52
0 kB]
Get:14 http://in.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [8
05 kB]
Get:15 http://security.ubuntu.com/ubuntu xenial-security/main i386 Packages [458
 kB]
Get:16 http://security.ubuntu.com/ubuntu xenial-security/main Translation-en [22
```

Step 11: apt-get upgrade



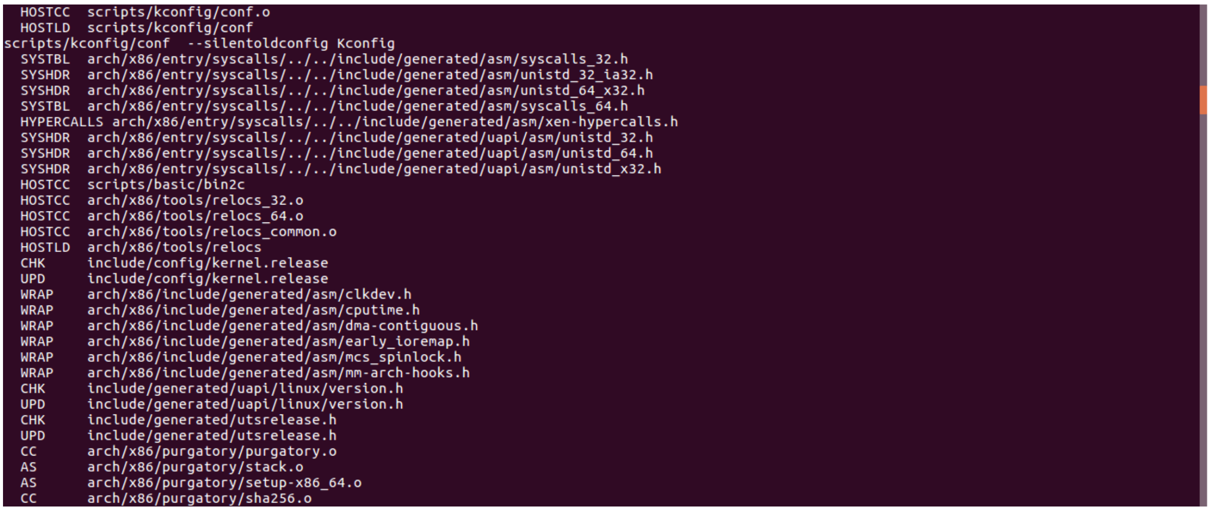
```
root@iiitd-HP-406-MT:/usr/src/linux-4.13# sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libappindicator1 libindicator7 libpango1.0-0 libpangox-1.0-0
  linux-headers-4.4.0-116 linux-headers-4.4.0-116-generic
  linux-headers-4.4.0-124 linux-headers-4.4.0-124-generic
  linux-headers-4.4.0-93 linux-headers-4.4.0-93-generic linux-headers-4.4.0-96
  linux-headers-4.4.0-96-generic linux-image-4.4.0-116-generic
  linux-image-4.4.0-124-generic linux-image-4.4.0-93-generic
  linux-image-4.4.0-96-generic linux-image-extra-4.4.0-116-generic
  linux-image-extra-4.4.0-124-generic linux-image-extra-4.4.0-93-generic
  linux-image-extra-4.4.0-96-generic linux-signed-image-4.4.0-116-generic
  linux-signed-image-4.4.0-124-generic linux-signed-image-4.4.0-93-generic
  linux-signed-image-4.4.0-96-generic ubuntu-core-launcher
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  gnome-software gnome-software-common libdrm-amdgpu1 libdrm2 libegl1-mesa
  libgbm1 libgl1-mesa-dri libgl1-mesa-glx libglapi-mesa libinput10 libmm-glib0
  libqmi-proxy libwayland-egl1-mesa libxatracker2 modemmanager ubuntu-software
  virtualbox virtualbox-dkms virtualbox-qt
```

Step 12: make menuconfig



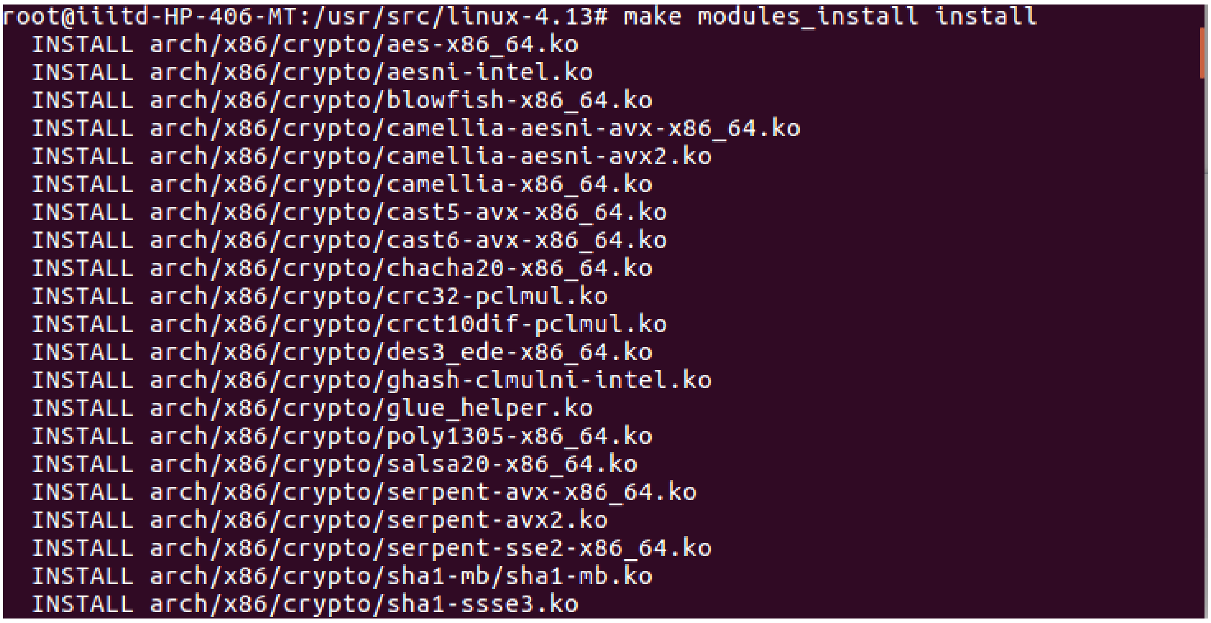
```
Arrow keys navigate the menu.  <Enter> selects submenus ---> (or empty submenus ----).  Highlighted letters are hotkeys.  Pressing
<Y> includes, <N> excludes, <M> modularizes features.  Press <Esc><Esc> to exit, <?> for Help, </> for Search.  Legend: [*] built-in
[ ] excluded  <M> module  < > module capable

                                  [*] 64-bit kernel
                                      General setup  --->
                                  [*] Enable loadable module support  --->
                                  [*] Enable the block layer  --->
                                      Processor type and features  --->
                                      Power management and ACPI options  --->
                                      Bus options (PCI etc.)  --->
                                      Executable file formats / Emulations  --->
                                  [*] Networking support  --->
                                      Device Drivers  --->
                                      Firmware Drivers  --->
                                      File systems  --->
                                      Kernel hacking  --->
                                      Security options  --->
                                  -*- Cryptographic API  --->
                                  -*- Virtualization  --->
                                      Library routines  --->
```

Step 13: make



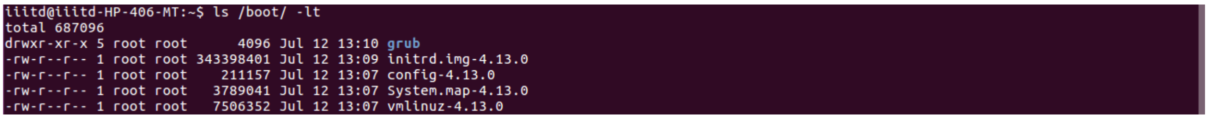
```
  HOSTCC  scripts/kconfig/conf.o
  HOSTLD  scripts/kconfig/conf
scripts/kconfig/conf  --silentoldconfig Kconfig
  SYSTBL  arch/x86/entry/syscalls/../../include/generated/asm/syscalls_32.h
  SYSHDR  arch/x86/entry/syscalls/../../include/generated/asm/unistd_32_ia32.h
  SYSHDR  arch/x86/entry/syscalls/../../include/generated/asm/unistd_64_x32.h
  SYSTBL  arch/x86/entry/syscalls/../../include/generated/asm/syscalls_64.h
  HYPERCALLS arch/x86/entry/syscalls/../../include/generated/asm/xen-hypercalls.h
  SYSHDR  arch/x86/entry/syscalls/../../include/generated/uapi/asm/unistd_32.h
  SYSHDR  arch/x86/entry/syscalls/../../include/generated/uapi/asm/unistd_64.h
  SYSHDR  arch/x86/entry/syscalls/../../include/generated/uapi/asm/unistd_x32.h
  HOSTCC  scripts/basic/bin2c
  HOSTCC  arch/x86/tools/relocs_32.o
  HOSTCC  arch/x86/tools/relocs_64.o
  HOSTCC  arch/x86/tools/relocs_common.o
  HOSTLD  arch/x86/tools/relocs
  CHK     include/config/kernel.release
  UPD     include/config/kernel.release
  WRAP    arch/x86/include/generated/asm/clkdev.h
  WRAP    arch/x86/include/generated/asm/cputime.h
  WRAP    arch/x86/include/generated/asm/dma-contiguous.h
  WRAP    arch/x86/include/generated/asm/early_ioremap.h
  WRAP    arch/x86/include/generated/asm/mcs_spinlock.h
  WRAP    arch/x86/include/generated/asm/mm-arch-hooks.h
  CHK     include/generated/uapi/linux/version.h
  UPD     include/generated/uapi/linux/version.h
  CHK     include/generated/utsrelease.h
  UPD     include/generated/utsrelease.h
  CC      arch/x86/purgatory/purgatory.o
  AS      arch/x86/purgatory/stack.o
  AS      arch/x86/purgatory/setup-x86_64.o
  CC      arch/x86/purgatory/sha256.o
```

Step 14: make modules_install install



```
root@iiitd-HP-406-MT:/usr/src/linux-4.13# make modules_install install
  INSTALL arch/x86/crypto/aes-x86_64.ko
  INSTALL arch/x86/crypto/aesni-intel.ko
  INSTALL arch/x86/crypto/blowfish-x86_64.ko
  INSTALL arch/x86/crypto/camellia-aesni-avx-x86_64.ko
  INSTALL arch/x86/crypto/camellia-aesni-avx2.ko
  INSTALL arch/x86/crypto/camellia-x86_64.ko
  INSTALL arch/x86/crypto/cast5-avx-x86_64.ko
  INSTALL arch/x86/crypto/cast6-avx-x86_64.ko
  INSTALL arch/x86/crypto/chacha20-x86_64.ko
  INSTALL arch/x86/crypto/crc32-pclmul.ko
  INSTALL arch/x86/crypto/crct10dif-pclmul.ko
  INSTALL arch/x86/crypto/des3_ede-x86_64.ko
  INSTALL arch/x86/crypto/ghash-clmulni-intel.ko
  INSTALL arch/x86/crypto/glue_helper.ko
  INSTALL arch/x86/crypto/poly1305-x86_64.ko
  INSTALL arch/x86/crypto/salsa20-x86_64.ko
  INSTALL arch/x86/crypto/serpent-avx-x86_64.ko
  INSTALL arch/x86/crypto/serpent-avx2.ko
  INSTALL arch/x86/crypto/serpent-sse2-x86_64.ko
  INSTALL arch/x86/crypto/sha1-mb/sha1-mb.ko
  INSTALL arch/x86/crypto/sha1-ssse3.ko
```

Step 15: check files created in /boot directory for verification of step 14.

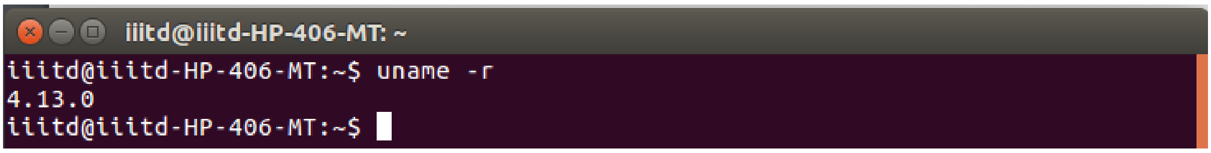


```
iiitd@iiitd-HP-406-MT:~$ ls /boot/ -lt
total 687096
drwxr-xr-x 5 root root      4096 Jul 12 13:10 grub
-rw-r--r-- 1 root root 343398401 Jul 12 13:09 initrd.img-4.13.0
-rw-r--r-- 1 root root    211157 Jul 12 13:07 config-4.13.0
-rw-r--r-- 1 root root   3789041 Jul 12 13:07 System.map-4.13.0
-rw-r--r-- 1 root root   7506352 Jul 12 13:07 vmlinuz-4.13.0
```

Step 16: shutdown -r now (reboot the system)

Step 17: select new kernel from linux advanced options.

Step 18: uname -r (check kernel version)

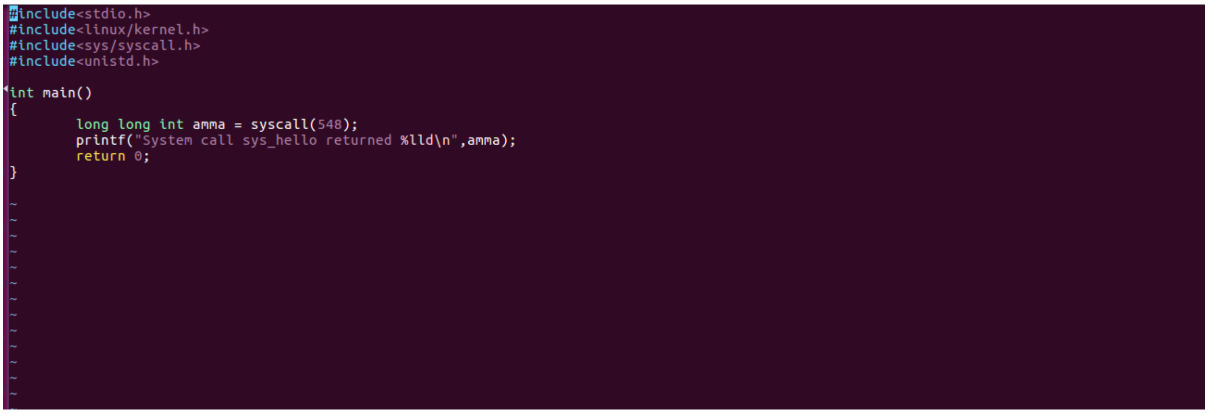


```
iiitd@iiitd-HP-406-MT:~$ uname -r
4.13.0
iiitd@iiitd-HP-406-MT:~$
```

Step 19: create usespace.c to execute system call.

Step 20: gcc usespace.c to compile code

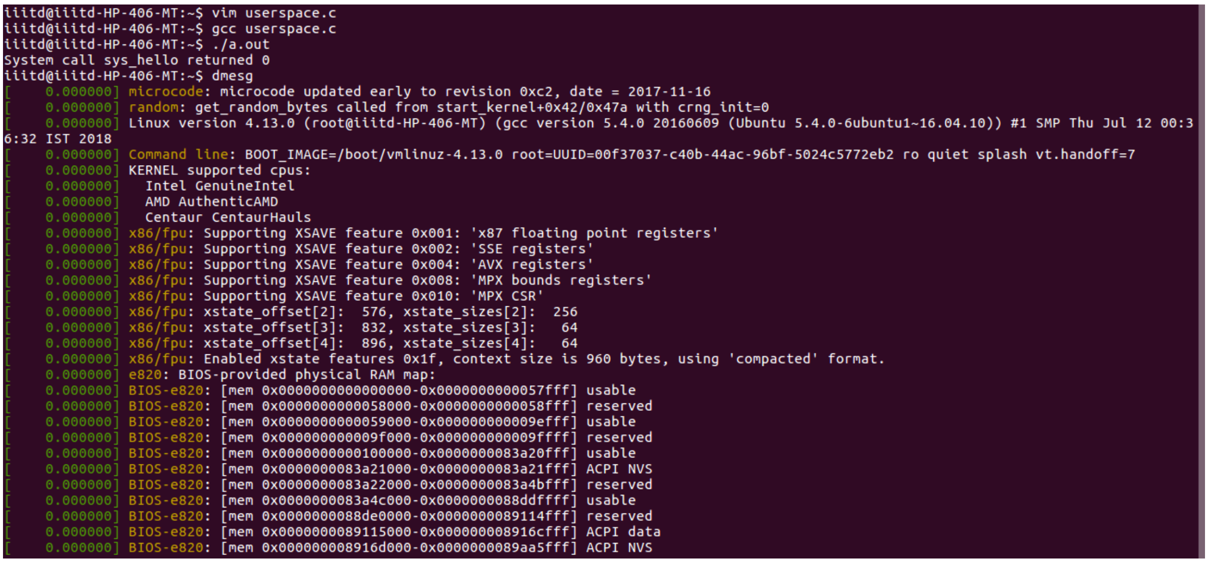
Step 21: ./a.out to execute program



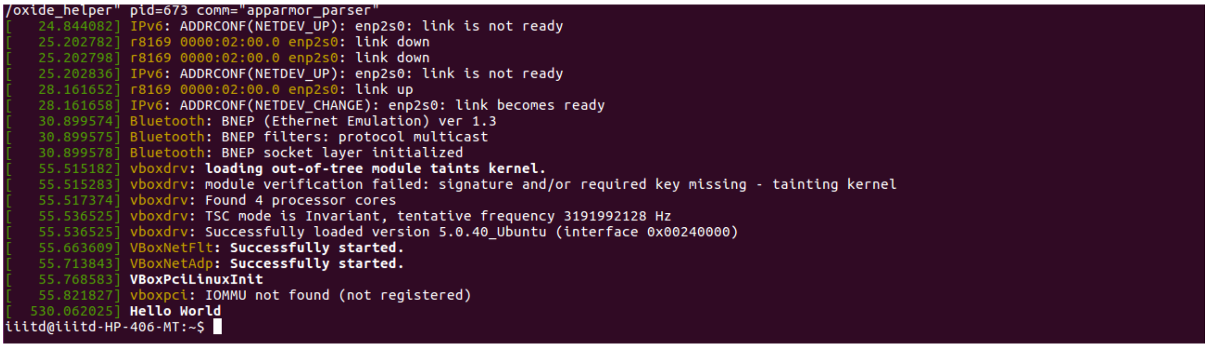
```
#include<stdio.h>
#include<linux/kernel.h>
#include<sys/syscall.h>
#include<unistd.h>

int main()
{
        long long int amma = syscall(548);
        printf("System call sys_hello returned %lld\n",amma);
        return 0;
}
```

Step 22: dmesg to check kernel message

Output of ./a.out and dmesg



```
iiitd@iiitd-HP-406-MT:~$ vim userspace.c
iiitd@iiitd-HP-406-MT:~$ gcc userspace.c
iiitd@iiitd-HP-406-MT:~$ ./a.out
System call sys_hello returned 0
iiitd@iiitd-HP-406-MT:~$ dmesg
[    0.000000] microcode: microcode updated early to revision 0xc2, date = 2017-11-16
[    0.000000] random: get_random_bytes called from start_kernel+0x42/0x47a with crng_init=0
[    0.000000] Linux version 4.13.0 (root@iiitd-HP-406-MT) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.10)) #1 SMP Thu Jul 12 00:3
6:32 IST 2018
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-4.13.0 root=UUID=00f37037-c40b-44ac-96bf-5024c5772eb2 ro quiet splash vt.handoff=7
[    0.000000] KERNEL supported cpus:
[    0.000000]   Intel GenuineIntel
[    0.000000]   AMD AuthenticAMD
[    0.000000]   Centaur CentaurHauls
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x008: 'MPX bounds registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x010: 'MPX CSR'
[    0.000000] x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
[    0.000000] x86/fpu: xstate_offset[3]:  832, xstate_sizes[3]:   64
[    0.000000] x86/fpu: xstate_offset[4]:  896, xstate_sizes[4]:   64
[    0.000000] x86/fpu: Enabled xstate features 0x1f, context size is 960 bytes, using 'compacted' format.
[    0.000000] e820: BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x0000000000057fff] usable
[    0.000000] BIOS-e820: [mem 0x0000000000058000-0x0000000000058fff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000059000-0x000000000009efff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009f000-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x0000000083a20fff] usable
[    0.000000] BIOS-e820: [mem 0x0000000083a21000-0x0000000083a21fff] ACPI NVS
[    0.000000] BIOS-e820: [mem 0x0000000083a22000-0x0000000083a4bfff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000083a4c000-0x0000000088ddffff] usable
[    0.000000] BIOS-e820: [mem 0x0000000088de0000-0x0000000089114fff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000089115000-0x000000008916cfff] ACPI data
[    0.000000] BIOS-e820: [mem 0x000000008916d000-0x0000000089aa5fff] ACPI NVS
```



```
/oxide_helper" pid=673 comm="apparmor_parser"
[   24.844082] IPv6: ADDRCONF(NETDEV_UP): enp2s0: link is not ready
[   25.202782] r8169 0000:02:00.0 enp2s0: link down
[   25.202798] r8169 0000:02:00.0 enp2s0: link down
[   25.202836] IPv6: ADDRCONF(NETDEV_UP): enp2s0: link is not ready
[   28.161652] r8169 0000:02:00.0 enp2s0: link up
[   28.161658] IPv6: ADDRCONF(NETDEV_CHANGE): enp2s0: link becomes ready
[   30.899574] Bluetooth: BNEP (Ethernet Emulation) ver 1.3
[   30.899575] Bluetooth: BNEP filters: protocol multicast
[   30.899578] Bluetooth: BNEP socket layer initialized
[   55.515182] vboxdrv: loading out-of-tree module taints kernel.
[   55.515283] vboxdrv: module verification failed: signature and/or required key missing - tainting kernel
[   55.517374] vboxdrv: Found 4 processor cores
[   55.536525] vboxdrv: TSC mode is Invariant, tentative frequency 3191992128 Hz
[   55.536525] vboxdrv: Successfully loaded version 5.0.40_Ubuntu (interface 0x00240000)
[   55.663609] VBoxNetFlt: Successfully started.
[   55.713843] VBoxNetAdp: Successfully started.
[   55.768583] VBoxPciLinuxInit
[   55.821827] vboxpci: IOMMU not found (not registered)
[  530.062025] Hello World
iiitd@iiitd-HP-406-MT:~$ 
```