Operating Systems: CS 6233
Assignment: 1

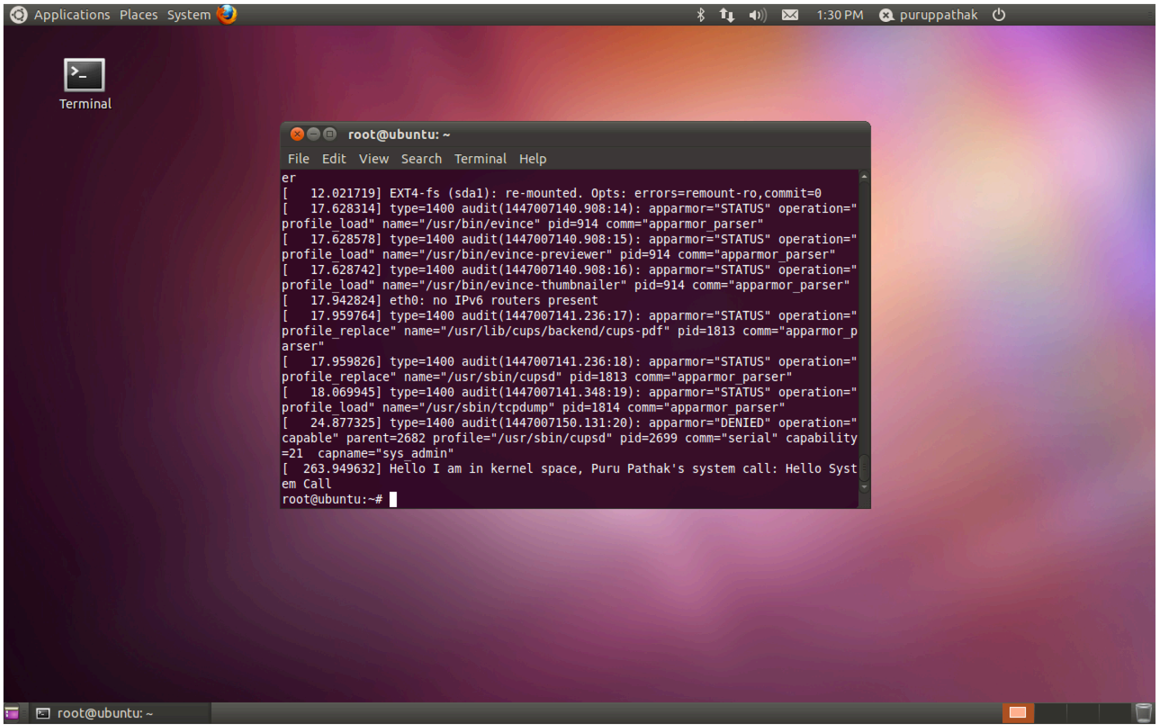
Name: Puru Pathak
NET id: ppp280

1. What are kernel APIs? What is the difference between kernel APIs and system calls?
Ans: The Kernel APIs can be defined as special interfaces which allow the programs in the user space to access the resources in the kernel section of the operating system. They basically provide a uniform level of abstraction. The difference between the kernel APIs and system calls is that with the help of Kernel API, we can program inside the kernel to create our own system calls or modify the existing system calls. On the other hand, a system call enables a program to call methods in a kernel.

2. What are roles of files in /boot/ (vmlinuz-*, initrd.img-*, grub, config*)?
Ans:
vmlinuz-* : It is a bootable compressed linux kernel.
initrd.img-* : It is a root file which mounts before the root file system.
grub: It is a boot loader, which helps user to support and choose different OSs.
config*: It is the Kernel's configuration file which lists out different options for the kernel.

3. Screenshots for tasks 1,2 and 3.

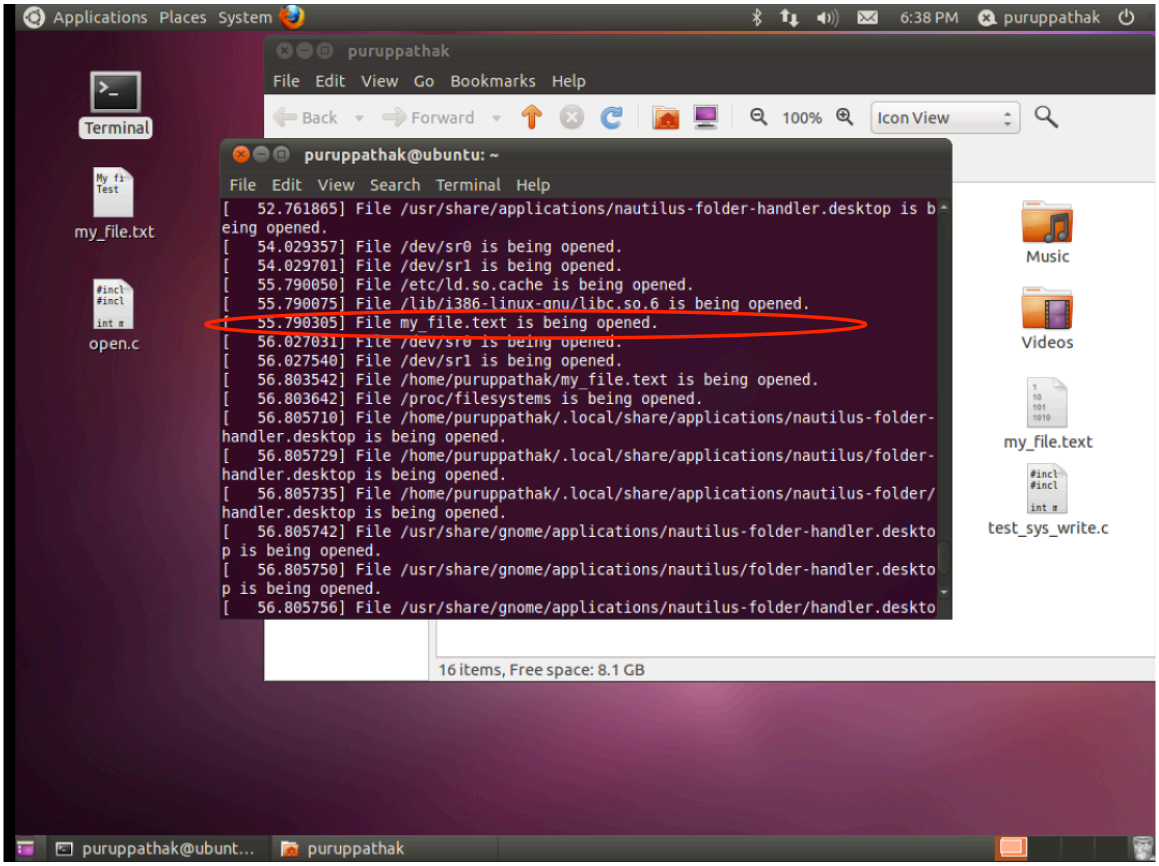
Screenshot for task-1:



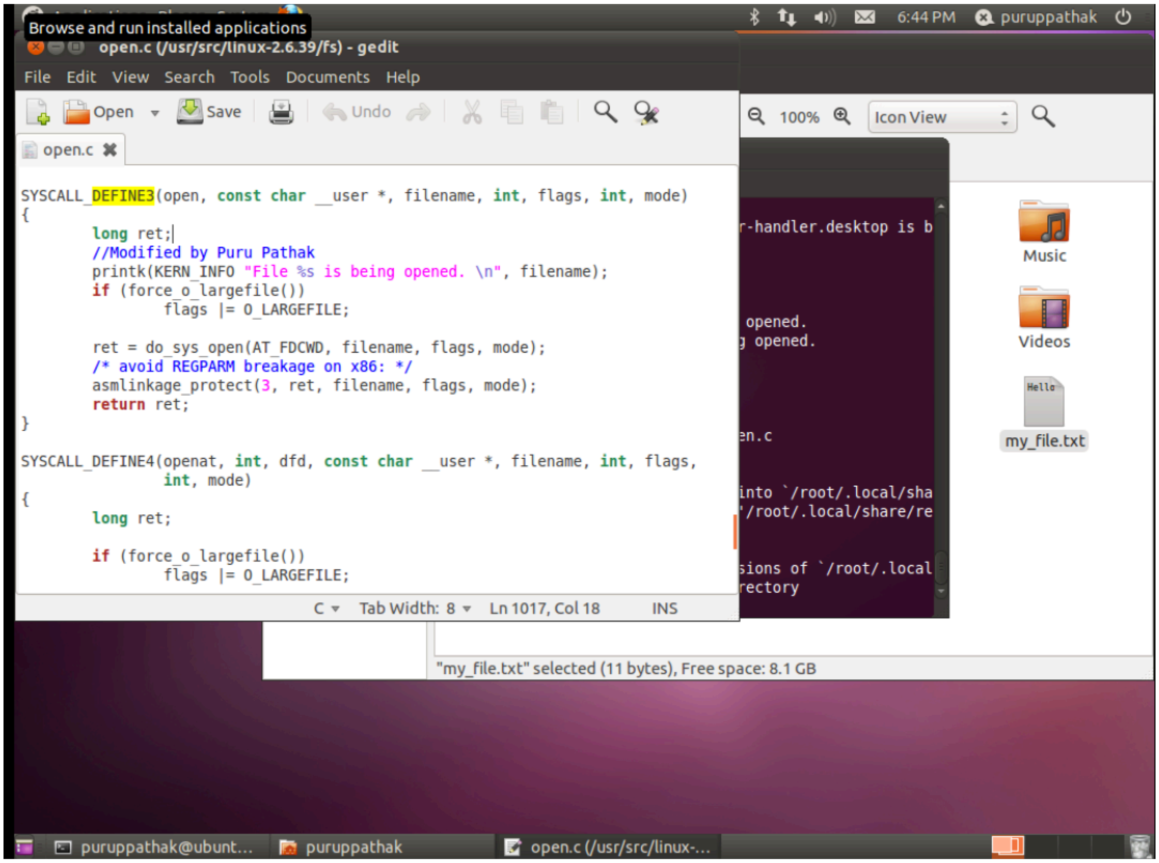
Applications Places System
1:30 PM puruppathak
Terminal
root@ubuntu: ~
File Edit View Search Terminal Help
root@ubuntu: ~

```
er
[   12.021719] EXT4-fs (sda1): re-mounted. Opts: errors=remount-ro,commit=0
[   17.628314] type=1400 audit(1447007140.908:14): apparmor="STATUS" operation="
profile_load" name="/usr/bin/evince" pid=914 comm="apparmor_parser"
[   17.628578] type=1400 audit(1447007140.908:15): apparmor="STATUS" operation="
profile_load" name="/usr/bin/evince-previewer" pid=914 comm="apparmor_parser"
[   17.628742] type=1400 audit(1447007140.908:16): apparmor="STATUS" operation="
profile_load" name="/usr/bin/evince-thumbnailer" pid=914 comm="apparmor_parser"
[   17.942824] eth0: no IPv6 routers present
[   17.959764] type=1400 audit(1447007141.236:17): apparmor="STATUS" operation="
profile_replace" name="/usr/lib/cups/backend/cups-pdf" pid=1813 comm="apparmor_p
arser"
[   17.959826] type=1400 audit(1447007141.236:18): apparmor="STATUS" operation="
profile_replace" name="/usr/sbin/cupsd" pid=1813 comm="apparmor_parser"
[   18.069945] type=1400 audit(1447007141.348:19): apparmor="STATUS" operation="
profile_load" name="/usr/sbin/tcpdump" pid=1814 comm="apparmor_parser"
[   24.877325] type=1400 audit(1447007150.131:20): apparmor="DENIED" operation="
capable" parent=2682 profile="/usr/sbin/cupsd" pid=2699 comm="serial" capability
=21  capname="sys_admin"
[  263.949632] Hello I am in kernel space, Puru Pathak's system call: Hello Syst
em Call
root@ubuntu:~# 
```

Screenshot for task-2:



```
[   52.761865] File /usr/share/applications/nautilus-folder-handler.desktop is b
eing opened.
[   54.029357] File /dev/sr0 is being opened.
[   54.029701] File /dev/sr1 is being opened.
[   55.790050] File /etc/ld.so.cache is being opened.
[   55.790075] File /lib/i386-linux-gnu/libc.so.6 is being opened.
[   55.790305] File my_file.text is being opened.
[   56.027031] File /dev/sr0 is being opened.
[   56.027540] File /dev/sr1 is being opened.
[   56.803542] File /home/puruppathak/my_file.text is being opened.
[   56.803642] File /proc/filesystems is being opened.
[   56.805710] File /home/puruppathak/.local/share/applications/nautilus-folder-
handler.desktop is being opened.
[   56.805729] File /home/puruppathak/.local/share/applications/nautilus/folder-
handler.desktop is being opened.
[   56.805735] File /home/puruppathak/.local/share/applications/nautilus-folder/
handler.desktop is being opened.
[   56.805742] File /usr/share/gnome/applications/nautilus-folder-handler.deskto
p is being opened.
[   56.805750] File /usr/share/gnome/applications/nautilus/folder-handler.deskto
p is being opened.
[   56.805756] File /usr/share/gnome/applications/nautilus-folder/handler.deskto
```

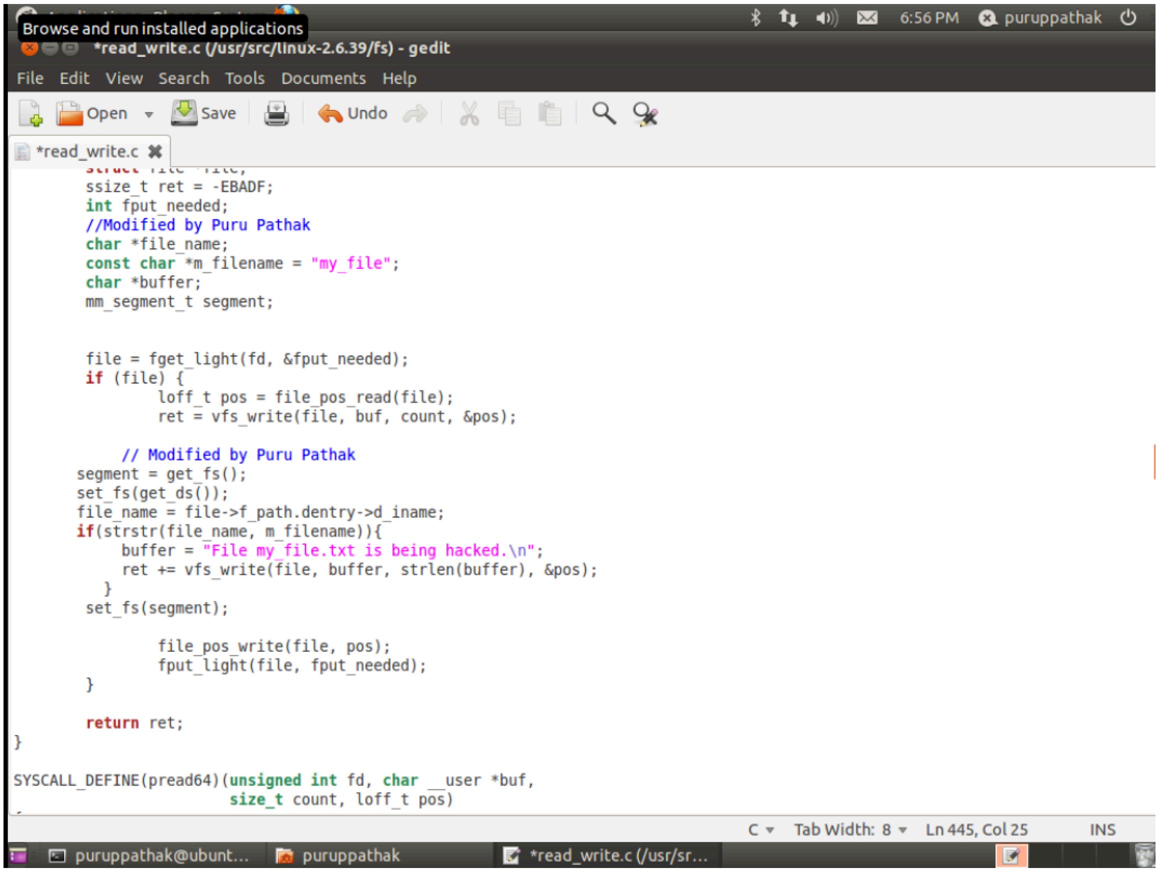


```
SYSCALL_DEFINE3(open, const char __user *, filename, int, flags, int, mode)
{
        long ret;
        //Modified by Puru Pathak
        printk(KERN_INFO "File %s is being opened. \n", filename);
        if (force_o_largefile())
                flags |= O_LARGEFILE;

        ret = do_sys_open(AT_FDCWD, filename, flags, mode);
        /* avoid REGPARM breakage on x86: */
        asmlinkage_protect(3, ret, filename, flags, mode);
        return ret;
}

SYSCALL_DEFINE4(openat, int, dfd, const char __user *, filename, int, flags,
                int, mode)
{
        long ret;

        if (force_o_largefile())
                flags |= O_LARGEFILE;
```

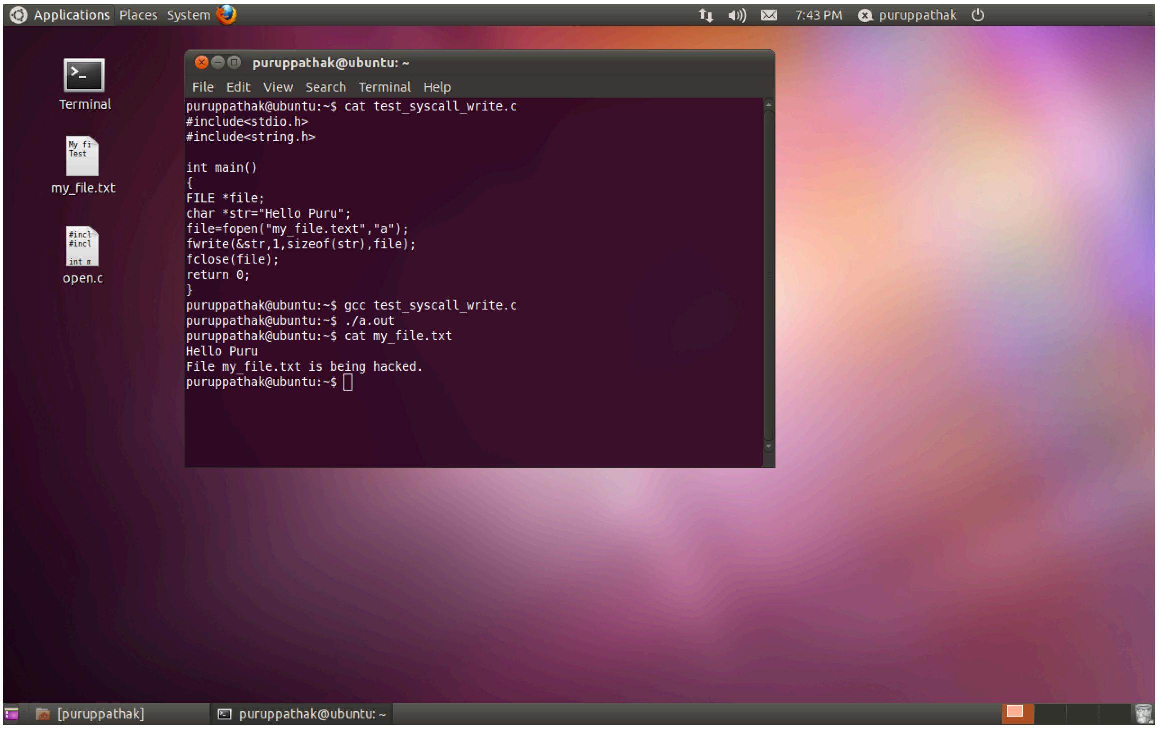
```
r-handler.desktop is b


 opened.
g opened.



en.c


into `/root/.local/sha
'/root/.local/share/re


sions of `/root/.local
rectory
```

"my_file.txt" selected (11 bytes), Free space: 8.1 GB

Screenshot for task-3:


Browse and run installed applications
*read_write.c (/usr/src/linux-2.6.39/fs) - gedit
6:56 PM
puruppathak
File Edit View Search Tools Documents Help
Open
Save
Undo
*read_write.c
C
Tab Width: 8
Ln 445, Col 25
INS
puruppathak@ubunt...
puruppathak
*read_write.c (/usr/sr...

```
        ssize_t ret = -EBADF;
        int fput_needed;
        //Modified by Puru Pathak
        char *file_name;
        const char *m_filename = "my_file";
        char *buffer;
        mm_segment_t segment;


        file = fget_light(fd, &fput_needed);
        if (file) {
                loff_t pos = file_pos_read(file);
                ret = vfs_write(file, buf, count, &pos);

            // Modified by Puru Pathak
       segment = get_fs();
       set_fs(get_ds());
       file_name = file->f_path.dentry->d_iname;
       if(strstr(file_name, m_filename)){
            buffer = "File my_file.txt is being hacked.\n";
            ret += vfs_write(file, buffer, strlen(buffer), &pos);
          }
        set_fs(segment);

                file_pos_write(file, pos);
                fput_light(file, fput_needed);
        }

        return ret;
}

SYSCALL_DEFINE(pread64)(unsigned int fd, char __user *buf,
                        size_t count, loff_t pos)
```



```
puruppathak@ubuntu:~$ cat test_syscall_write.c
#include<stdio.h>
#include<string.h>

int main()
{
FILE *file;
char *str="Hello Puru";
file=fopen("my_file.text","a");
fwrite(&str,1,sizeof(str),file);
fclose(file);
return 0;
}
puruppathak@ubuntu:~$ gcc test_syscall_write.c
puruppathak@ubuntu:~$ ./a.out
puruppathak@ubuntu:~$ cat my_file.txt
Hello Puru
File my_file.txt is being hacked.
puruppathak@ubuntu:~$ 
```

References:
wikipedia.com
kernel.org
advancelinux.com