ASSIGNMENT 3 – SYSTEM CALL HOOKING

JOHN THOMAS
P2CSN17017

REPORT

System call hooking is to intercept a system call and modify the behaviour of the applications which call those system calls.There will be a real system call and a modified system call which the user enters.

- In the code the ftrace_hook to hook the system call sys_openat.
  I removed the clone and exec system calls which are used to clone and execute a process and added the sys_openat system call.

- Signature of sys_openat obtained from elixir bootlin

asmlinkage long sys_openat(int dirfd, const char __user *filename, int flags, umode_t mode);

- In the code, I made modifications by adding the following lines

long fd = real_sys_openat(dirfd, filename, flags, mode);

I used a variable fd to store the return value of the real function real_sys_openat which is used to get the file descriptor of the file.

printk(KERN_INFO "Address : %p\n", fcheck(fd));

- Then I used a fcheck(), which is used to return the address of the entry in the open file table of the file descriptor.I added the header file #include <linux/fdtable.h> to use the fcheck()

  Then fd is returned which contains the value from the real system call.

Now In the structure struct ftrace_hook,
static struct ftrace_hook demo_hooks[] = {
    HOOK("sys_openat", fh_sys_openat, &real_sys_openat)

- We add the HOOK which is used to register the system call name ie,sys_openat and the two variants of the function hook, i.e, fh_sys_openat and real_sys_openat.

- On running the make file all the files are generated
- We do a dmesg to display the messages generated by the device drivers (inorder to see the output of the code)

- Then, we insert the module ftrace_hook into the kernel using insmod command ,which prints the addresses in the other tab where we did the dmesg -w

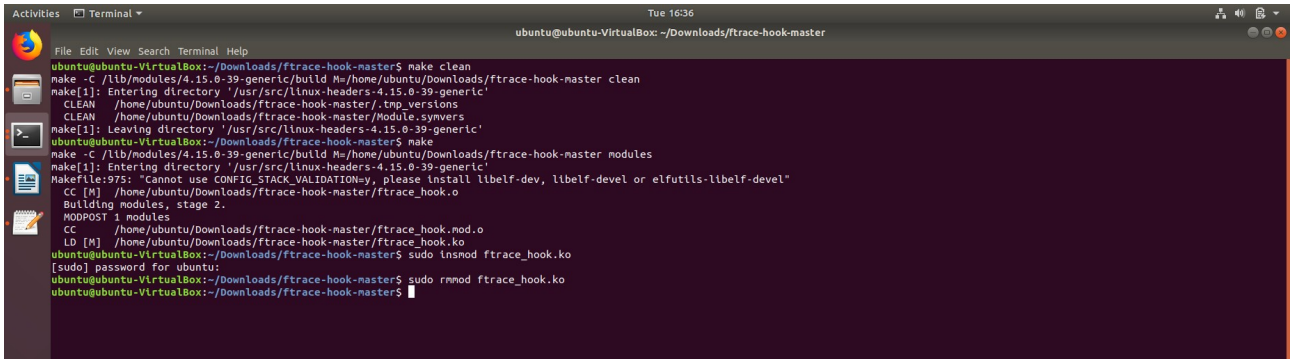
- Inorder to remove the modules we use the rmmod command which unloads the ftrace_hook module from the kernel.

SHELL COMMANDS

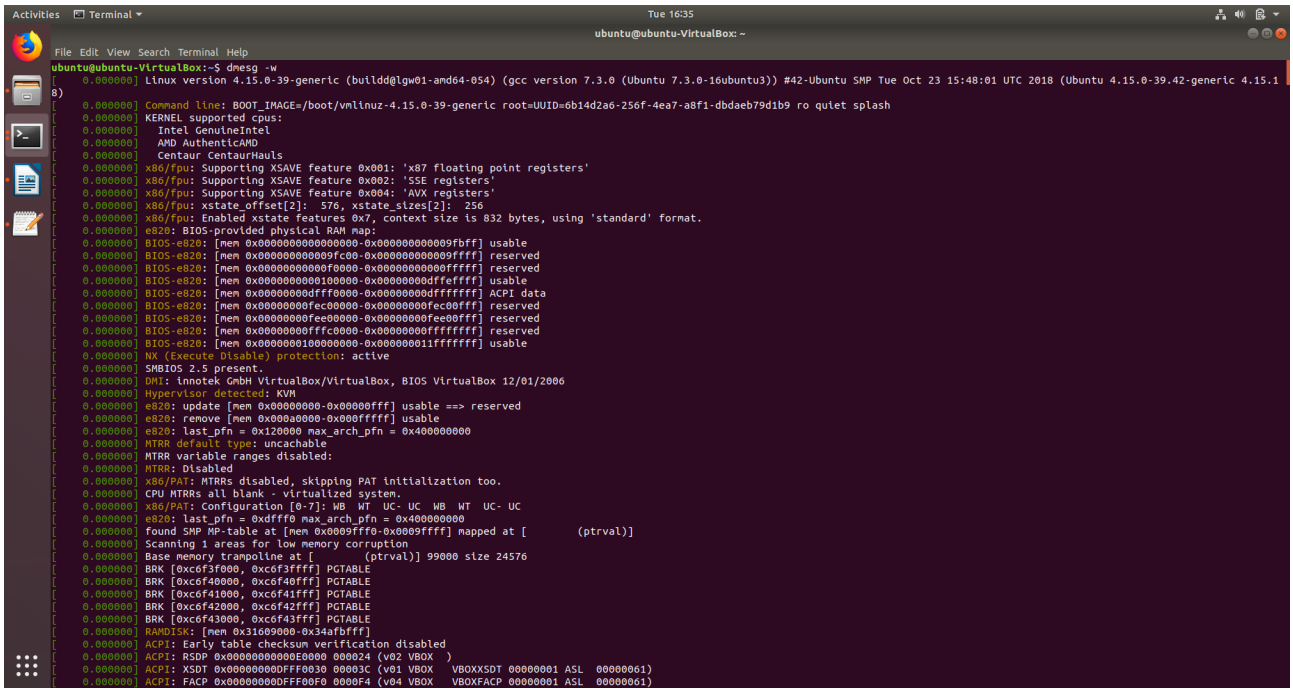
- insmod command is used to load the ftrace_hook module into the kernel.
- rmmod command unloads the ftrace_hook from the kernel.
- dmesg command displays all the messages generated by the device.
- Make command which calls the makefile, which creates the kernel objects.

SCREENSHOTS

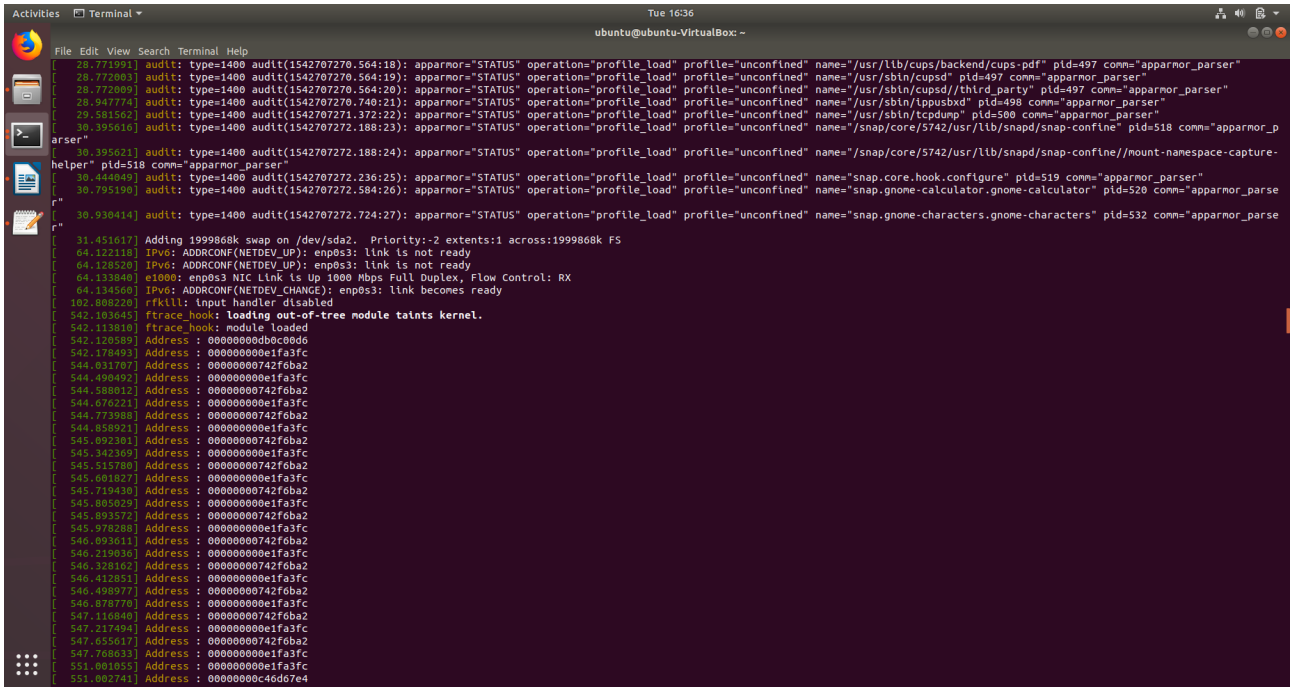
- Generating make files



- dmesg – w



- insmod



- rmmod