

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)
```

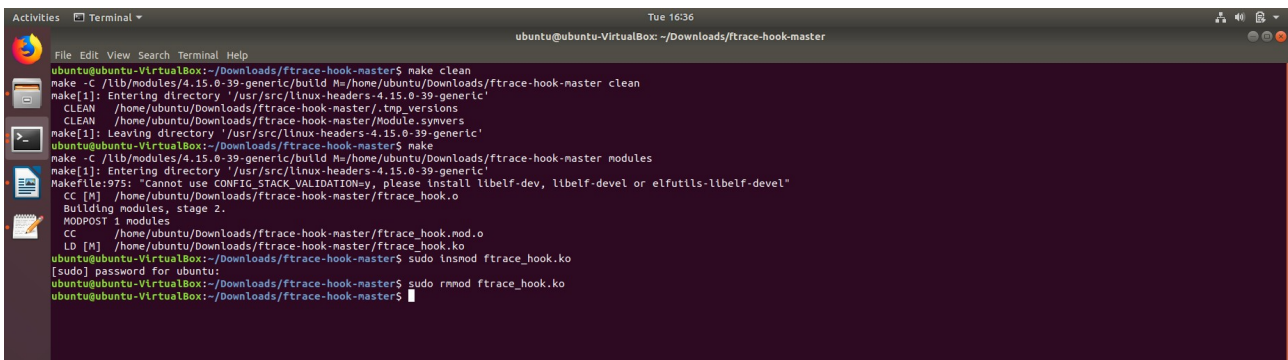
- We add the `HOOK` which is used to register the system call name ie, `sys_openat` and the two variants of the function hook, i.e, `fh_sys_openat` and `real_sys_openat`.
- On running the `make file` all the files are generated
- We do a `dmesg` to display the messages generated by the device drivers (in order 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`
- In order 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

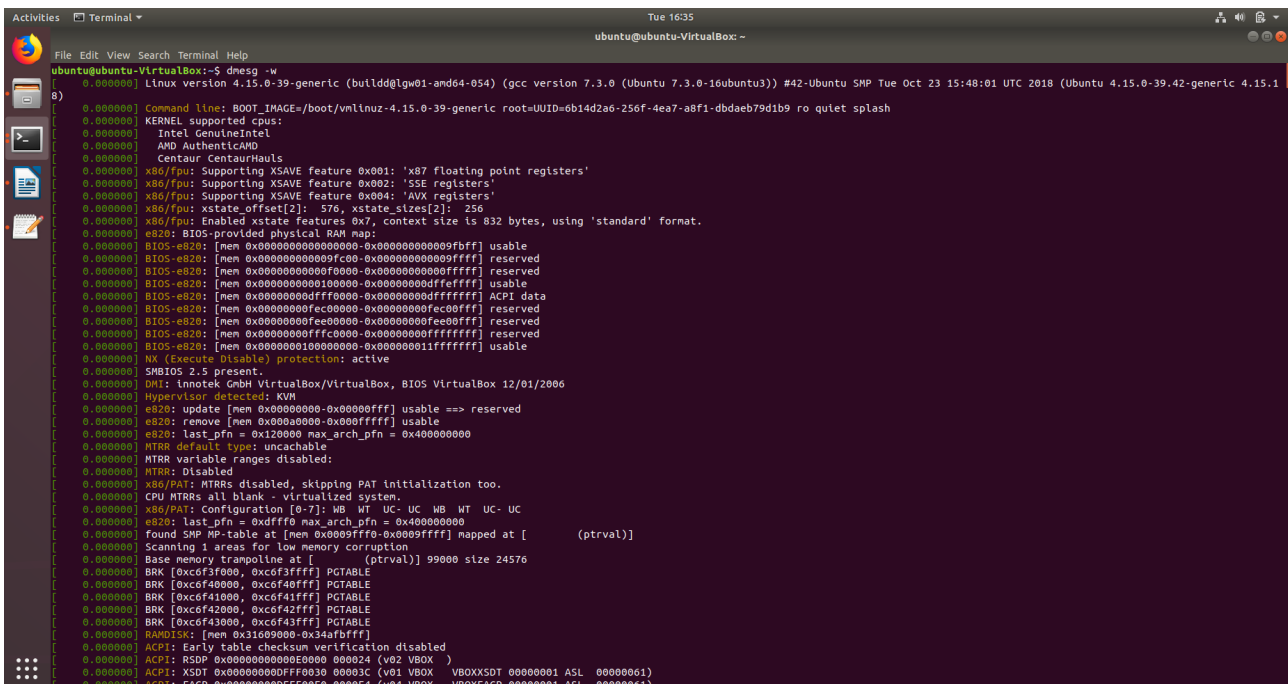
- Generating make files



```
Activities Terminal
Tue 16:36
ubuntu@ubuntu-VirtualBox: ~/Downloads/ftrace-hook-master

ubuntu@ubuntu-VirtualBox:~/Downloads/ftrace-hook-master$ make clean
make -C /lib/modules/4.15.0-39-generic/build M=/home/ubuntu/Downloads/ftrace-hook-master clean
make[1]: Entering directory '/usr/src/linux-headers-4.15.0-39-generic'
CLEAN /home/ubuntu/Downloads/ftrace-hook-master/module-synvers
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-39-generic'
ubuntu@ubuntu-VirtualBox:~/Downloads/ftrace-hook-master$ make
make -C /lib/modules/4.15.0-39-generic/build M=/home/ubuntu/Downloads/ftrace-hook-master modules
make[1]: Entering directory '/usr/src/linux-headers-4.15.0-39-generic'
Makefile:975: 'Cannot use CONFIG_STACK_VALIDATION=y, please install libelf-dev, libelf-devel or elfutils-libelf-devel'
CC [M] /home/ubuntu/Downloads/ftrace-hook-master/ftrace_hook.o
Building modules, stage 2.
MODPOST 1 modules
CC /home/ubuntu/Downloads/ftrace-hook-master/ftrace_hook.mod.o
LD [M] /home/ubuntu/Downloads/ftrace-hook-master/ftrace_hook.ko
ubuntu@ubuntu-VirtualBox:~/Downloads/ftrace-hook-master$ sudo insmod ftrace_hook.ko
[sudo] password for ubuntu:
ubuntu@ubuntu-VirtualBox:~/Downloads/ftrace-hook-master$ sudo rmmod ftrace_hook.ko
ubuntu@ubuntu-VirtualBox:~/Downloads/ftrace-hook-master$
```

- dmesg -w



```
Activities Terminal
Tue 16:35
ubuntu@ubuntu-VirtualBox: ~

ubuntu@ubuntu-VirtualBox:~$ dmesg -w
Linux version 4.15.0-39-generic (buildd@lgw01-and04-054) (gcc version 7.3.0 (Ubuntu 7.3.0-16ubuntu3)) #42-Ubuntu SMP Tue Oct 23 15:48:01 UTC 2018 (Ubuntu 4.15.0-39.42-generic 4.15.1)
Command line: BOOT_IMAGE=/boot/vmlinuz-4.15.0-39-generic root=UUID=6b14d2a6-256f-4ea7-abf1-dbaeb79d1b9 ro quiet splash
Kernel supported cpus:
Intel GenuineIntel
AMD AuthenticAMD
Centaur CentaurHauls
x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
e820: BIOS-provided physical RAM map:
BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
BIOS-e820: [mem 0x00000000000ff000-0x00000000000fffff] reserved
BIOS-e820: [mem 0x0000000001000000-0x0000000000dfffff] usable
BIOS-e820: [mem 0x0000000000dffff000-0x0000000000dfffff] ACPI data
BIOS-e820: [mem 0x0000000000fec00000-0x0000000000fec0ffff] reserved
BIOS-e820: [mem 0x0000000000fec00000-0x0000000000fec0ffff] reserved
BIOS-e820: [mem 0x0000000000fffc0000-0x0000000000ffffff] reserved
BIOS-e820: [mem 0x000000000100000000-0x00000000011fffff] usable
NX (Execute Disable) protection: active
SMBIOS 2.5 present.
DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Hypervisor detected: KVM
e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
e820: remove [mem 0x000a0000-0x000fffff] usable
e820: last_pfn = 0x120000 max_arch_pfn = 0x400000000
MTRR default type: uncachable
MTRR variable ranges disabled:
MTRR: Disabled
x86/PAT: MTRRs disabled, skipping PAT initialization too.
CPU MTRRs all blank - virtualized system.
x86/PAT: Configuration [0-7]: WB WT UC- UC WB WT UC- UC
e820: last_pfn = 0x0ffff0 max_arch_pfn = 0x400000000
found SMP MP-table at [mem 0x0009ffff-0x0009ffff] mapped at [ (ptrval)]
Scanning 1 areas for low memory corruption
Base memory trampoline at [ (ptrval)] 99000 size 24576
BRK [0xc6f3f000, 0xc6f3ffff] PGTABLE
BRK [0xc6f40000, 0xc6f40fff] PGTABLE
BRK [0xc6f41000, 0xc6f41fff] PGTABLE
BRK [0xc6f42000, 0xc6f42fff] PGTABLE
BRK [0xc6f43000, 0xc6f43fff] PGTABLE
RAMDISK: [mem 0x31609000-0x316af000]
ACPI: Early table checksum verification disabled
ACPI: RSDP 0x0000000000000000 000024 (v02 VBOX )
ACPI: XSDT 0x0000000000000000 00003C (v01 VBOX VBOXXSDT 00000001 ASL 00000001)
ACPI: FACP 0x0000000000000000 0000F4 (v04 VBOX VBOXFACP 00000001 ASL 00000001)
```

- insmod

```

Tue 16:36
ubuntu@ubuntu-VirtualBox: ~
File Edit View Search Terminal Help
28.771991 audit: type=1400 audit(1542707270.564:18): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/cups/backend/cups-pdf" pid=497 comm="apparmor_parser"
28.772063 audit: type=1400 audit(1542707270.564:19): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin/cupsd" pid=497 comm="apparmor_parser"
28.772069 audit: type=1400 audit(1542707270.564:20): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin/cupsd//third_party" pid=497 comm="apparmor_parser"
28.947774 audit: type=1400 audit(1542707270.749:21): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin/cupsd" pid=498 comm="apparmor_parser"
29.581562 audit: type=1400 audit(1542707271.372:22): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin/tcpdump" pid=500 comm="apparmor_parser"
30.395616 audit: type=1400 audit(1542707272.188:23): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/snap/core/5742/usr/lib/snapd/snap-confine" pid=518 comm="apparmor_p
arser"
30.395621 audit: type=1400 audit(1542707272.188:24): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/snap/core/5742/usr/lib/snapd/snap-confine//mount-namespace-capture-
helper" pid=518 comm="apparmor_parser"
30.444949 audit: type=1400 audit(1542707272.236:25): apparmor="STATUS" operation="profile_load" profile="unconfined" name="snap.core.hook.configure" pid=519 comm="apparmor_parser"
30.795190 audit: type=1400 audit(1542707272.584:26): apparmor="STATUS" operation="profile_load" profile="unconfined" name="snap.gnome-calculator.gnome-calculator" pid=520 comm="apparmor_parse
r"
30.939414 audit: type=1400 audit(1542707272.724:27): apparmor="STATUS" operation="profile_load" profile="unconfined" name="snap.gnome-characters.gnome-characters" pid=532 comm="apparmor_parse
r"
31.451617 Adding 1999868k swap on /dev/sda2. Priority: -2 extents:1 across:1999868k FS
64.122118 IPv6: ADDRCONF(NETDEV_UP): enp0s3: link is not ready
64.128520 IPv6: ADDRCONF(NETDEV_UP): enp0s3: link is not ready
64.133840 etool: enp0s3 NIC Link is up 1000 Mbps Full Duplex, Flow Control: RX
64.134560 IPv6: ADDRCONF(NETDEV_CHANGE): enp0s3: link becomes ready
102.888220 rtkill: input handler disabled
542.103645 ftrace_hook: loading out-of-tree module taints kernel.
542.113810 ftrace_hook: module loaded
542.120809 Address: 00000000b0c000d6
542.178493 Address: 00000000e1fa3fc
544.031707 Address: 00000000742f6ba2
544.490492 Address: 00000000e1fa3fc
544.508912 Address: 00000000742f6ba2
544.676221 Address: 00000000e1fa3fc
544.773988 Address: 00000000742f6ba2
544.858921 Address: 00000000e1fa3fc
545.092381 Address: 00000000e1fa3fc
545.342469 Address: 00000000e1fa3fc
545.515780 Address: 00000000742f6ba2
545.601827 Address: 00000000e1fa3fc
545.719430 Address: 00000000742f6ba2
545.808929 Address: 00000000e1fa3fc
545.893572 Address: 00000000742f6ba2
545.978288 Address: 00000000e1fa3fc
546.093611 Address: 00000000742f6ba2
546.219930 Address: 00000000e1fa3fc
546.328162 Address: 00000000742f6ba2
546.412651 Address: 00000000e1fa3fc
546.498977 Address: 00000000742f6ba2
546.878770 Address: 00000000e1fa3fc
547.115040 Address: 00000000742f6ba2
547.217494 Address: 00000000e1fa3fc
547.655617 Address: 00000000742f6ba2
547.768633 Address: 00000000e1fa3fc
551.001055 Address: 00000000e1fa3fc
551.002741 Address: 00000000c4d60e4

```

- rmmod

```

Tue 16:36
ubuntu@ubuntu-VirtualBox: ~
File Edit View Search Terminal Help
613.583522 Address: 00000000ccda7126
613.583607 Address: 00000000b106d68
613.583724 Address: 0000000042e8b187
613.583788 Address: 00000000e71da8db
613.583812 Address: 00000000339844d
613.584053 Address: 0000000030441b2e
613.584077 Address: 00000000b3aa5447
613.584410 Address: 0000000011aebf9
613.584457 Address: 000000001689b231
613.584573 Address: 00000000b649d0f6
613.584595 Address: 00000000c6db7d34
613.584607 Address: 00000000add22efe
613.584620 Address: 000000003a8724e9
613.584633 Address: 00000000dd6b710
613.584658 Address: 000000009ced7f54
613.584689 Address: 0000000084c6f41b
613.584727 Address: 0000000050c10f47
613.584780 Address: 000000005f94d97
613.585279 Address: 00000000a0c88aa
613.585316 Address: 00000000927e0294
613.585341 Address: 00000000ca80016
613.585394 Address: 000000002d849503
613.585412 Address: 000000000b17cc2f
613.585440 Address: 000000009b991dec
613.585450 Address: 00000000cf028dd0
613.585673 Address: 00000000a205ee6
613.585859 Address: 0000000039a4a4e1
613.585886 Address: 00000000c6937f08
613.585983 Address: 00000000a0ff37f3
613.585945 Address: 000000003ff91a41
613.585959 Address: 00000000a6e508c3
613.585974 Address: 000000008405e800
613.585990 Address: 000000003412555
613.510649 Address: 00000000fbd8443
613.511018 Address: 00000000c9b54abd
613.511037 Address: 0000000028464e35
613.513477 Address: 00000000ef4028a5
613.513518 Address: 00000000e71adfa
613.513541 Address: 00000000d3ff0eb8
613.513566 Address: 000000007e913f08
613.513578 Address: 0000000024f313fe
613.513589 Address: 000000007088a0d
613.513587 ftrace_hook: module unloaded
988.619421 kauditd_printk_skb: 7 callbacks suppressed
988.619422 audit: type=1400 audit(1542708146.946:35): apparmor="STATUS" operation="profile_load" profile="unconfined" name="libreoffice-oopslash" pid=3551 comm="apparmor_parser"
988.667431 audit: type=1400 audit(1542708146.998:36): apparmor="STATUS" operation="profile_load" profile="unconfined" name="libreoffice-senddoc" pid=3558 comm="apparmor_parser"
989.467762 audit: type=1400 audit(1542708147.796:37): apparmor="STATUS" operation="profile_load" profile="unconfined" name="libreoffice-soffice" pid=3565 comm="apparmor_parser"
989.474033 audit: type=1400 audit(1542708147.808:38): apparmor="STATUS" operation="profile_load" profile="unconfined" name="libreoffice-soffice/ppg" pid=3565 comm="apparmor_parser"
989.518577 audit: type=1400 audit(1542708147.848:39): apparmor="STATUS" operation="profile_load" profile="unconfined" name="libreoffice-xpdfimport" pid=3572 comm="apparmor_parser"

```

