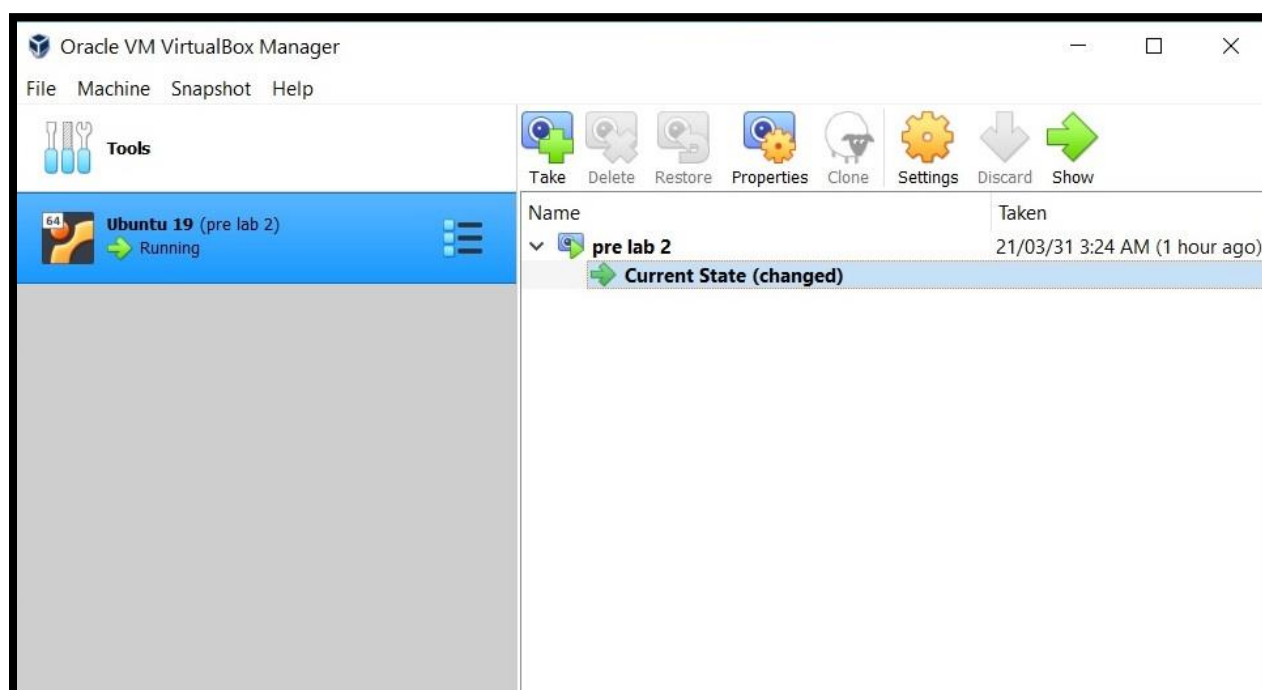


در این بخش از آزمایش قصد داریم تا یک ماژول هسته را بارگذاری و حذف کنیم و با بررسی بافر سابقه‌ی هسته مطمئن شویم که این فرآیند را به درستی طی کرده‌ایم.

در ابتدا بهتر است اشاره کنیم که ماژول‌های هسته چه هستند. Kernel Module یا ماژول‌های هسته عبارتند از تکه کدهایی که در هنگام run-time می‌توانند در کرنل بارگذاری یا از آن حذف شوند و برای اجرای آن‌ها نیازی نیست که سیستم مجدداً راه‌اندازی شود. این ماژول‌ها، عملکرد هسته را در حین اجرا توسعه می‌دهند. ماژول‌ها می‌توانند یک سرویس، فایل سیستم یا درایور سخت‌افزاری باشند. حال به انجام این بخش از آزمایش می‌پردازیم.

از آنجایی که ماژول‌های هسته به صورت مستقیم با کرنل در ارتباط هستند و هرگونه خطا و اشکال در آن‌ها می‌تواند باعث بروز اشکال در کل سیستم گردد، قبل از شروع کار از وضعیت فعلی ماشین مجازی خود snapshot می‌گیریم تا در صورت نیاز بتوانیم به شرایطی که قبل از شروع آزمایش داشتیم بازگردیم.

screen01



در مرحله‌ی بعدی برای اطمینان از اینکه هدرهای موردنیاز ما نصب شده و آپدیت هستند، مراحل زیر را طی می‌کنیم:

ابتدا دستور `sudo sed -i -re 's/([a-z]{2}\.)?archive.ubuntu.com|security.ubuntu.com/old-releases.ubuntu.com/g' /etc/apt/sources.list` و سپس به ترتیب دستورات `sudo apt-get install linux-headers-$(uname -r)` و `sudo apt-get update` را در ترمینال وارد می‌کنیم.

```
oslab@OSLab-VirtualBox: /
oslab@OSLab-VirtualBox:/$ sudo sed -i -re 's/([a-z]{2}\.)?archive.ubuntu.com|security.ubuntu.com/old-releases.ubuntu.com/g' /etc/apt/sources.list
oslab@OSLab-VirtualBox:/$ sudo apt-get update
Hit:1 http://old-releases.ubuntu.com/ubuntu disco InRelease
Hit:2 http://old-releases.ubuntu.com/ubuntu disco-updates InRelease
Hit:3 https://download.sublimetext.com apt/stable/ InRelease
Hit:4 http://old-releases.ubuntu.com/ubuntu disco-backports InRelease
Hit:5 http://old-releases.ubuntu.com/ubuntu disco-security InRelease
Reading package lists... Done
oslab@OSLab-VirtualBox:/$ sudo apt-get install linux-headers-$(uname -r)
Reading package lists... Done
Building dependency tree
Reading state information... Done
linux-headers-5.0.0-13-generic is already the newest version (5.0.0-13.14).
0 upgraded, 0 newly installed, 0 to remove and 326 not upgraded.
oslab@OSLab-VirtualBox:/$
```

دستور sed یا stream editor است که این قابلیت را به کاربر می‌دهد تا بدون باز کردن یک فایل در ادیتور و فقط با اجرای این دستور، فایل را ادیت کند و فرآیندهایی همچون search, find, replacement, deletion, insert را به روی آن فایل اجرا کند. از دستور apt-get برای مدیریت پکیج‌ها به واسطه‌ی کار با بخش APT (Advanced Packaging Tool) در لینوکس، استفاده می‌شود. از این دستور برای حذف، نصب و به روزرسانی پکیج‌ها و نرم‌افزارها استفاده می‌شود.

بعد از اینکه مطمئن شدیم هدرهای موردنظر ما نصب هستند، ادیتور sublime-text را با استفاده از دستور `sudo snap install` نصب میکنیم تا بتوانیم ادیت فایل‌های خود را در محیطی کارآمدتر انجام دهیم.

screen03

```
oslab@OSLab-VirtualBox: ~
oslab@OSLab-VirtualBox:~$ sudo snap install sublime-text
error: This revision of snap "sublime-text" was published using classic
confinement and thus may perform arbitrary system changes outside of the
security sandbox that snaps are usually confined to, which may put your
system at risk.

If you understand and want to proceed repeat the command including
--classic.
oslab@OSLab-VirtualBox:~$ sudo snap install --classic sublime-text
Download snap "sublime-text" (97) from channel "stable"      3% 305kB/s 3m10s
```

snap یک سیستم مدیریت پکیج در لینوکس است که به واسطه‌ی آن می‌توان به راحتی بسیاری از برنامه‌هایی را که در این سیستم پکیج شده‌اند را دانلود و نصب کرد. این سیستم از Ubuntu 16.04 LTS به بعد روی تمام ورژن‌های اوبونتو نصب است و تمام برنامه‌هایی که با استفاده از snap نصب شوند به صورت اتوماتیک آپدیت خواهند شد.

پس از نصب، sublime-text را باز میکنیم تا کد مربوط به ماژول خود را در آن وارد و ادیت کنیم. (از آنجایی که کد این ماژول را آماده داریم آن را کپی میکنیم و در فرمت یک فایل c ذخیره می‌کنیم)

screen04



```
File Edit Selection Find View Goto Tools Project Preferences Help
simplemod.c
1 #include <linux/init.h>
2 #include <linux/kernel.h>
3 #include <linux/module.h>
4
5
6
7 /* this function is called when the module is loaded*/
8 int simple_init(void)
9 {
10     printk(KERN_INFO "Loading Module\n");
11     return 0;
12 }
13
14
15
16
17 /* this function is called when the module is removed*/
18 void simple_exit(void)
19 {
20     printk(KERN_CRIT "Removing Module\n");
21 }
22
23
24
25 /* Macros for registering module entry and exit points.
26 */
27 module_init(simple_init);
28 module_exit(simple_exit);
29
30
31 MODULE_LICENSE("GPL");
32 MODULE_DESCRIPTION("simple module");
33 MODULE_AUTHOR("SGG");
```

دستور printk معادل دستور printf است با این تفاوت که پیام خود را در بافر سابقه هسته چاپ می‌کند.

این عبارت، نشان‌دهنده‌ی حالت و اهمیت پیام چاپ شده است. طبق جدول اولویت‌ها kern_info نشان‌دهنده‌ی یک پیام عادی است اما kern_crit یک پیام critical است که اولویت بالاتری دارد و در صورت مشاهده باید فوراً به آن رسیدگی شود. در اینجا این عبارت را تغییر دادیم تا ماژول ما چند حالت متفاوت را در بگیرد. به همین دلیل است که پیام removing module به رنگ قرمز چاپ خواهد شد.

این دو ماکرو محل ورود و خروج به ماژول Simplemod را ثبت میکنند و در محل ورود و خروج، توابع simple_init و simple_exit را فراخوانی می‌کنند.

این ماکروها نیز حاوی اطلاعات و مشخصات مربوط به ماژول می‌باشند

فایل بدون پسوند دیگری شامل قوانین مربوط به کامپایل simplemod.c را در همین دایرکتوری ایجاد می‌کنیم و نام آن را Makefile می‌گذاریم. (به دلیل تغییر دادن نام ماژول نیاز است تا در کد آماده‌ای که برای makefile داریم نیز تغییر ایجاد کنیم) هرگاه که می‌خواهیم از دستور make استفاده کنیم به یک makefile نیز نیاز است که ارتباط فایل‌های درون برنامه‌ی ما را توضیح میدهد.

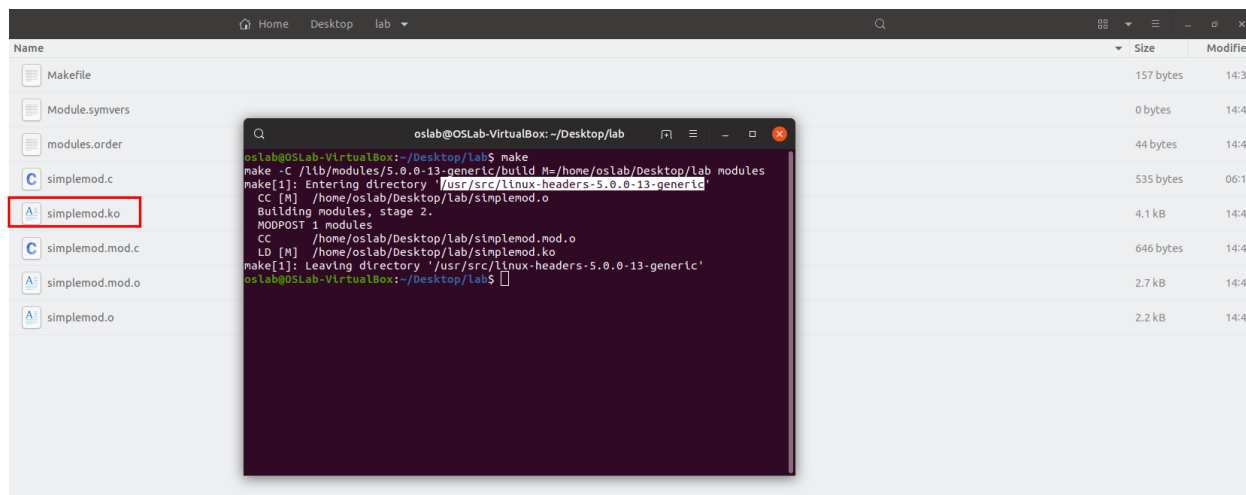
screen05



حالا در همین دایرکتوری فعلی (Desktop/lab) که فایل‌های ما درون آن قرار دارند، ترمینال را باز میکنیم و دستور make را وارد می‌کنیم. از این دستور برای کامپایل کردن ماژول‌ها و پروژه‌های بزرگ استفاده می‌شود. پس از کامپایل، فایل simplemod.ko در همین دایرکتوری ایجاد می‌شود. پسوند ko. برای ماژول‌های هسته در نظر گرفته می‌شود.

در همین مرحله، آدرس entering directory را در جایی سیو میکنیم چون برای مراحل بعدی به آن نیاز داریم.

screen06



حالا که ماژول هسته‌ای ما ساخته شده، می‌توانیم آن را به کرنل اضافه و از آن حذف کنیم. برای اینکه به این فرآیند نظارت داشته باشیم، تب جدیدی در ترمینال باز میکنیم و دستور `tail -f /var/log/syslog` را وارد می‌کنیم تا لاگ‌های سیستم را زیرنظر بگیریم و ببینیم که آیا خروجی دلخواه خود را می‌گیریم یا خیر (برای همین منظور می‌توان از دستور `dmesg` استفاده کرد که محتویات بافر سایقه هسته را چاپ می‌کند) طبق کد simplemod.c، انتظار داریم که با لود کردن ماژول پیام Loading Module و با حذف آن پیام Removing Module چاپ شوند.

حالا با استفاده از دستور `sudo insmod simplemod.ko` این ماژول را در کرنل لود میکنیم.

screen07

```
oslab@OSLab-VirtualBox:~/Desktop/lab$ make
make -C /lib/modules/5.0.0-13-generic/build M=/home/oslab/Desktop/lab modules
make[1]: Entering directory '/usr/src/linux-headers-5.0.0-13-generic'
  CC [M]  /home/oslab/Desktop/lab/simplemod.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/oslab/Desktop/lab/simplemod.mod.o
  LD [M]  /home/oslab/Desktop/lab/simplemod.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.0.0-13-generic'
oslab@OSLab-VirtualBox:~/Desktop/lab$ sudo insmod simplemod.ko
[sudo] password for oslab:
oslab@OSLab-VirtualBox:~/Desktop/lab$
```

حالا اگر به تب دوم که دستور `tail` را در آن اجرا کرده بودیم نگاه کنیم، می بینیم که عبارت “loading module” طبق انتظار ما چاپ شده است

screen08

```
oslab@OSLab-VirtualBox: ~/Desktop/lab x oslab@OSLab-VirtualBox: ~/Desktop/lab x
Mar 31 15:18:01 OSLab-VirtualBox dbus-daemon[665]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service' requested by ':1.868' (uid=1000 pid=29288 comm="rhythmbox " label="unconfined")
Mar 31 15:18:01 OSLab-VirtualBox systemd[1]: Starting Hostname Service...
Mar 31 15:18:02 OSLab-VirtualBox dbus-daemon[665]: [system] Successfully activated service 'org.freedesktop.hostname1'
Mar 31 15:18:02 OSLab-VirtualBox systemd[1]: Started Hostname Service.
Mar 31 15:18:05 OSLab-VirtualBox rhythmbox[29288]: Can't set a parent on widget which has a parent
Mar 31 15:18:32 OSLab-VirtualBox systemd[1]: systemd-hostnamed.service: Succeeded.
Mar 31 15:21:30 OSLab-VirtualBox kernel: [49460.876060] Loading Module
Mar 31 15:21:48 OSLab-VirtualBox dbus-daemon[1630]: [session uid=1000 pid=1630] Activating via systemd: service name='org.freedesktop.Tracker1.Miner.Extract' unit='tracker-extract.service' requested by ':1.53' (uid=1000 pid=2074 comm="/usr/lib/tracker/tracker-miner-fs " label="unconfined")
Mar 31 15:21:48 OSLab-VirtualBox systemd[1601]: Starting Tracker metadata extractor...
Mar 31 15:21:49 OSLab-VirtualBox dbus-daemon[1630]: [session uid=1000 pid=1630] Successfully activated service 'org.freedesktop.Tracker1.Miner.Extract'
Mar 31 15:21:49 OSLab-VirtualBox systemd[1601]: Started Tracker metadata extractor.
```

در این حالت اگر دستور `sudo lsmod` را وارد کنیم که ماژول‌های فعلی هسته را لیست می‌کند، می‌توانیم ماژول خود را میان آن‌ها ببینیم.

screen09

```
oslab@OSLab-VirtualBox: ~/Desktop/lab x  oslab@OSLab-VirtualBox: ~/Desktop/lab x
make[1]: Entering directory '/usr/src/linux-headers-5.0.0-13-generic'
CC [M] /home/oslab/Desktop/lab/simplemod.o
Building modules, stage 2.
MODPOST 1 modules
CC /home/oslab/Desktop/lab/simplemod.mod.o
LD [M] /home/oslab/Desktop/lab/simplemod.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.0.0-13-generic'
oslab@OSLab-VirtualBox:~/Desktop/lab$ sudo insmod simplemod.ko
[sudo] password for oslab:
oslab@OSLab-VirtualBox:~/Desktop/lab$ sudo lsmod
Module                               Size  Used by
simplemod                             16384  0
nls_utf8                             16384  1
isofs                                 49152  1
vboxsf                                81920  1
vboxvideo                             36864  0
snd_intel8x0                           45056  2
crct10dif_pclmul                       16384  1
crc32_pclmul                           16384  0
snd_ac97_codec                         135168  1 snd_intel8x0
ghash_clmulni_intel                   16384  0
ac97_bus                               16384  1 snd_ac97_codec
aesni_intel                           372736  0
snd_pcm                                102400  2 snd_intel8x0,snd_ac97_codec
```

با دستور `sudo lsmod | grep [module name]` می‌توانیم به دنبال یک ماژول خاص که در حال حاضر در هسته لود شده است بگردیم، اگر این دستور را برای `simplemod` اجرا کنیم، آن را می‌یابیم.

screen10

```
autofs4                               45056  2
hid_generic                           16384  0
usbhid                                53248  0
hid                                    126976  2 usbhid,hid_generic
psmouse                               151552  0
ahci                                    40960  3
libahci                               32768  1 ahci
i2c_piix4                             28672  0
e1000                                  139264  0
pata_acpi                              16384  0
video                                  45056  0
oslab@OSLab-VirtualBox:~/Desktop/lab$ sudo lsmod | grep simplemod
simplemod                               16384  0
oslab@OSLab-VirtualBox:~/Desktop/lab$
```

در این مرحله قصد داریم ماژولی که بارگذاری کردیم را از کرنل حذف کنیم. برای اینکار از دستور `sudo rmmod [module name]` استفاده می‌کنیم.

screen11

```
pata_acpi          16384  0
video              45056  0
oslab@OSLab-VirtualBox:~/Desktop/lab$ sudo lsmod | grep simplemod
simplemod           16384  0
oslab@OSLab-VirtualBox:~/Desktop/lab$ sudo rmmod simplemod
oslab@OSLab-VirtualBox:~/Desktop/lab$
```

پس از اجرای این دستور در تب دوم می بینیم که عبارت removing module چاپ شده است

screen12

```
oslab@OSLab-VirtualBox: ~/Desktop/lab x  oslab@OSLab-VirtualBox: ~/Desktop/lab x
it='tracker-extract.service' requested by ':1.53' (uid=1000 pid=2074 comm="/usr/
lib/tracker/tracker-miner-fs " label="unconfined")
Mar 31 15:23:06 OSLab-VirtualBox systemd[1601]: Starting Tracker metadata extrac
tor...
Mar 31 15:23:06 OSLab-VirtualBox dbus-daemon[1630]: [session uid=1000 pid=1630]
Successfully activated service 'org.freedesktop.Tracker1.Miner.Extract'
Mar 31 15:23:06 OSLab-VirtualBox systemd[1601]: Started Tracker metadata extrac
tor.
Mar 31 15:23:16 OSLab-VirtualBox systemd[1601]: tracker-extract.service: Succeed
ed.
Mar 31 15:23:22 OSLab-VirtualBox kernel: [49572.998118] Removing Module
Mar 31 15:23:25 OSLab-VirtualBox dbus-daemon[1630]: [session uid=1000 pid=1630]
Activating via systemd: service name='org.freedesktop.Tracker1.Miner.Extract' un
it='tracker-extract.service' requested by ':1.53' (uid=1000 pid=2074 comm="/usr/
lib/tracker/tracker-miner-fs " label="unconfined")
Mar 31 15:23:25 OSLab-VirtualBox systemd[1601]: Starting Tracker metadata extrac
tor...
Mar 31 15:23:25 OSLab-VirtualBox dbus-daemon[1630]: [session uid=1000 pid=1630]
Successfully activated service 'org.freedesktop.Tracker1.Miner.Extract'
Mar 31 15:23:25 OSLab-VirtualBox systemd[1601]: Started Tracker metadata extrac
tor.
Mar 31 15:23:35 OSLab-VirtualBox systemd[1601]: tracker-extract.service: Succeed
ed.
```

بعد از حذف کردن simplemod اگر از ماژول های هسته لیست بگیریم یا مجدداً به دنبال simplemod بگردیم، آن را نخواهیم یافت.

screen13

```

glue_helper      16384  1 aesni_intel
snd_seq          69632  2 snd_seq_midi,snd_seq_midi_event
drm_kms_helper   180224  2 vmwgfx,vboxvideo
snd_seq_device    16384  3 snd_seq,snd_seq_midi,snd_rawmidi
drm              475136  6 vmwgfx,drm_kms_helper,vboxvideo,ttm
snd_timer        36864  3 snd_seq,snd_pcm
intel_rapl_perf   16384  0
snd              81920  13 snd_seq,snd_seq_device,snd_intel8x0,snd_timer,s
nd_ac97_codec,snd_pcm,snd_rawmidi
fb_sys_fops      16384  1 drm_kms_helper
syscopyarea      16384  1 drm_kms_helper
sysfillrect      16384  1 drm_kms_helper
soundcore        16384  1 snd
input_leds       16384  0
sysimgblt        16384  1 drm_kms_helper
serio_raw        20480  0
vboxguest        339968  6 vboxsf
mac_hid          16384  0
sch_fq_codel     20480  2
parport_pc       40960  0
ppdev            24576  0
lp               20480  0
parport          53248  3 parport_pc,lp,ppdev
ip_tables        28672  0
x_tables         40960  1 ip_tables
autofs4          45056  2
hid_generic      16384  0
usbhid           53248  0
hid              126976  2 usbhid,hid_generic
psmouse          151552  0
ahci              40960  3
libahci          32768  1 ahci
i2c_piix4        28672  0
e1000            139264  0
pata_acpi        16384  0
video            45056  0
oslab@OSLab-VirtualBox:~/Desktop/lab$ sudo lsmod | grep simplemod
oslab@OSLab-VirtualBox:~/Desktop/lab$

```

همانطور که گفتیم با دستور dmesg نیز می‌توانیم پیام‌های بافر سابقه‌ی هسته را رویت کنیم. دلیل قرمز بودن عبارت remove را در بخش توضیحات کد شرح دادیم.

screen14

```

oslab@OSLab-VirtualBo... x oslab@OSLab-VirtualBo... x oslab@OSLab-VirtualBo... x
[ 6485.139969] usb 1-1: new full-speed USB device number 4 using xhci_hcd
[ 6485.298999] usb 1-1: New USB device found, idVendor=80ee, idProduct=0021, bcd
Device= 1.00
[ 6485.299001] usb 1-1: New USB device strings: Mfr=1, Product=3, SerialNumber=0
[ 6485.299002] usb 1-1: Product: USB Tablet
[ 6485.299003] usb 1-1: Manufacturer: VirtualBox
[ 6485.300727] input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:0c.0/
usb1/1-1/1-1:1.0/0003:80EE:0021.0003/input/input9
[ 6485.362221] hid-generic 0003:80EE:0021.0003: input,hidraw0: USB HID v1.10 Mou
se [VirtualBox USB Tablet] on usb-0000:00:0c.0-1/input0
[15782.279123] audit: type=1400 audit(1617154211.894:45): apparmor="STATUS" oper
ation="profile_load" profile="unconfined" name="snap.sublime-text.subl" pid=2651
7 comm="apparmor_parser"
[15782.280039] audit: type=1400 audit(1617154211.894:46): apparmor="STATUS" oper
ation="profile_load" profile="unconfined" name="snap.update-ns.sublime-text" pid
=26516 comm="apparmor_parser"
[46865.684277] gedit[24661]: segfault at 0 ip 00007f052d4f500a sp 00007f052d4d32e
0 error 4 in libgedit-3.14.so[7f052d4d3000+49000]
[46865.684298] Code: 55 49 89 c1 48 8d 35 45 e5 02 00 48 89 c3 4c 8d 05 f3 e5 02
00 31 c0 bf 00 04 00 00 e8 bf 38 fe ff 48 8b 05 d0 d9 0a 00 5a 59 <8b> 30 85 f6
0f 84 dc 00 00 00 48 8b 78 08 48 89 de e8 d0 0a fe ff
[49460.876060] Loading Module
[49572.998118] Removing Module
oslab@OSLab-VirtualBox:~/Desktop/lab$

```