Linux os

How to add your system call

Ahmed Mohammed Shaban
Esraa Nasser Said
Omnia Khaled Badawi

Final-Project-OS

First I will show the settings of my Virtual Machine :

Number of cores: 4

The capacity of memory is 4G

The kernal virsion is 5.8.1

Second:

Steps to how to add a system call :

1.1 - Fully update your operating system by

```
sudo apt update && sudo apt upgrade -y
```

1.2 Download and install the essential packages to compile kernels by :

```
sudo apt install build-essential libncurses-dev libssl-dev libelf-dev bison flex -y
```

1.3 Clean up your installed packages.

```
sudo apt clean && sudo apt autoremove -y
```

Now Lets Go to do it :)

Now I will download the source code of the latest stable version of the Linux kernel (which is 5.8.1 as of 12 August 2020) And add i will add to my folder .

"wget -P ~/ https://cdn.kernel.org/pub/linux/kernel/v5.x/linux-5.8.1.tar.xz" And unpack it by

1.5 using tar -xvf ~/linux-5.8.1.tar.xz -C ~/

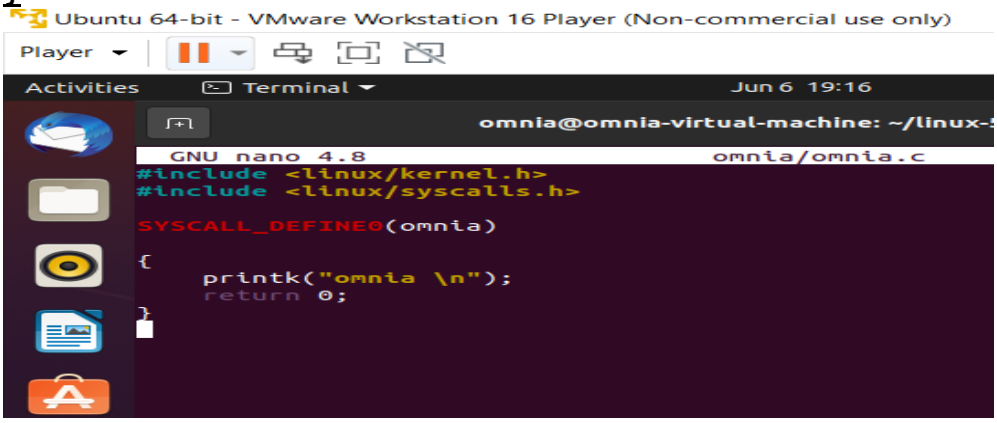
1.6 Then Reboot MY Virsual Machine

2 -

Now i will change to root and go on "linux-5.8.1".

Make a directory called Omnia and create file called Omnia.c in this file write a program

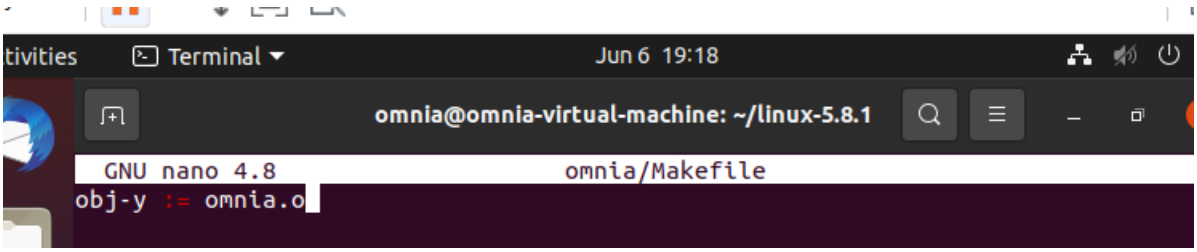
```
  #include <linux/kernel.h>
  #include <linux/syscalls.h>

  SYSCALL_DEFINE0(Omnia)
{
printk("Omnia.\n");
return 0;
}
```



Save it and exit the text editor.

>> Now i will create a makefile "nano Omnia/Makefile"

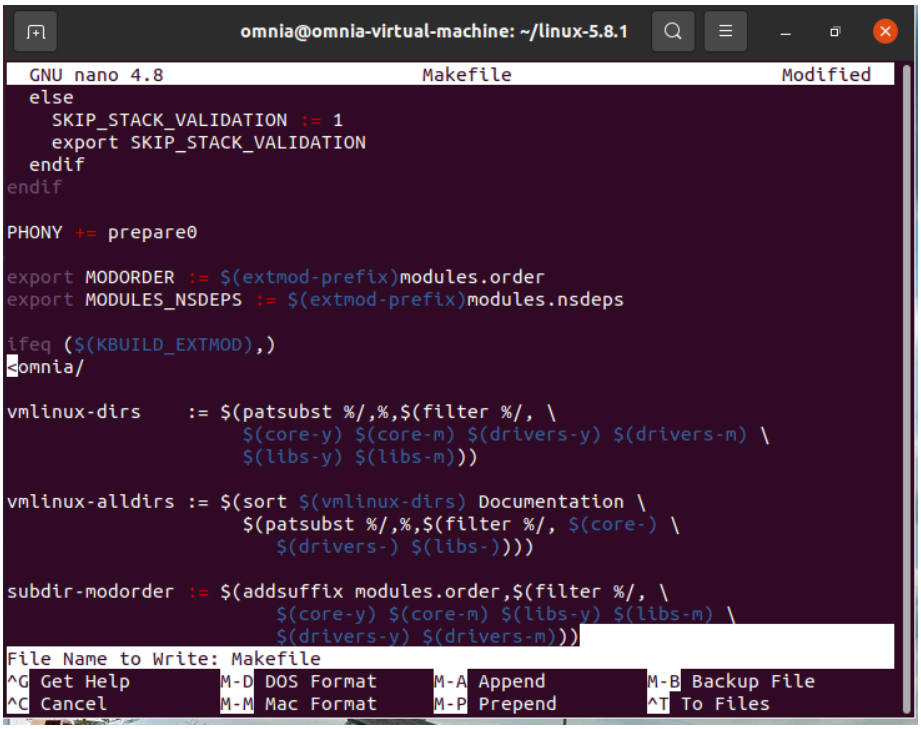
>>And write "obj-y := Omnia.o"



>>And i will open the Makefile to add the home directory to my system call to the main Makefile of the kernel.

Open the Makefile with the following command.

"nano Makefile" and i will search for core-y it will apper in the second time of searching . We did the search to see this "kernel/ certs/ mm/ fs/ ipc/ security/ crypto/ block/" I will add my home directory called Omnia .



And I will open the header file with the following command.

""nano include/linux/syscalls.h""

to add a corresponding function prototype for my system call to the header file of system calls.

Search for endif and put "asmlinkage long sys_Omnia(void);" above it .

```
asmlinkage long sys_getgid16(void);
asmlinkage long sys_geteuid16(void);
asmlinkage long sys_getegid16(void);
asmlinkage long sys_omnia(void);
#endif
```

Add my system call to the kernel's system call table. By using "nano arch/x86/entry/syscalls/syscall_64.tbl" command Note: Um 64bit if u 32bit just put 32 instead of 64.

I will navigate to the bottom of it even find a series of x32 system calls. I will put

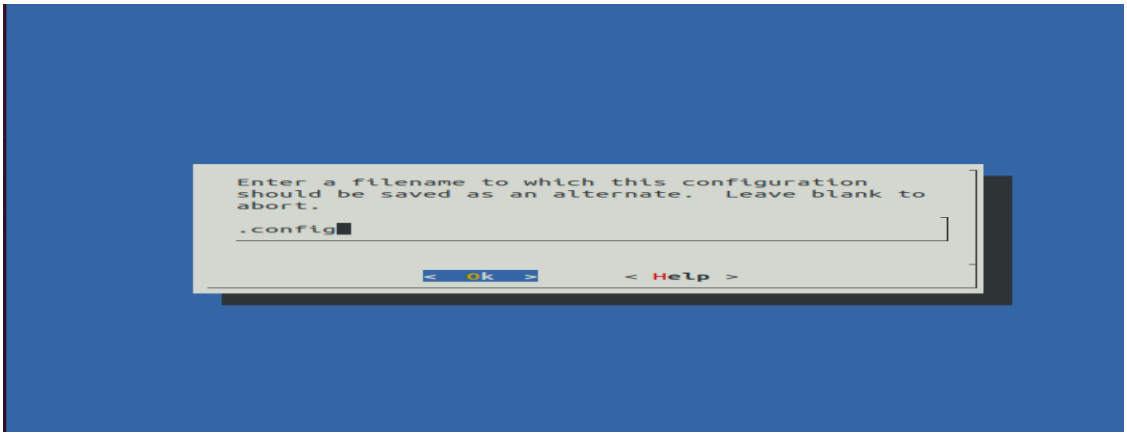
"440 common Omnia sys_Omnia" "above the section 32 "

Now Installition:

I will install the new kernel and prepare your operating system to boot into it.

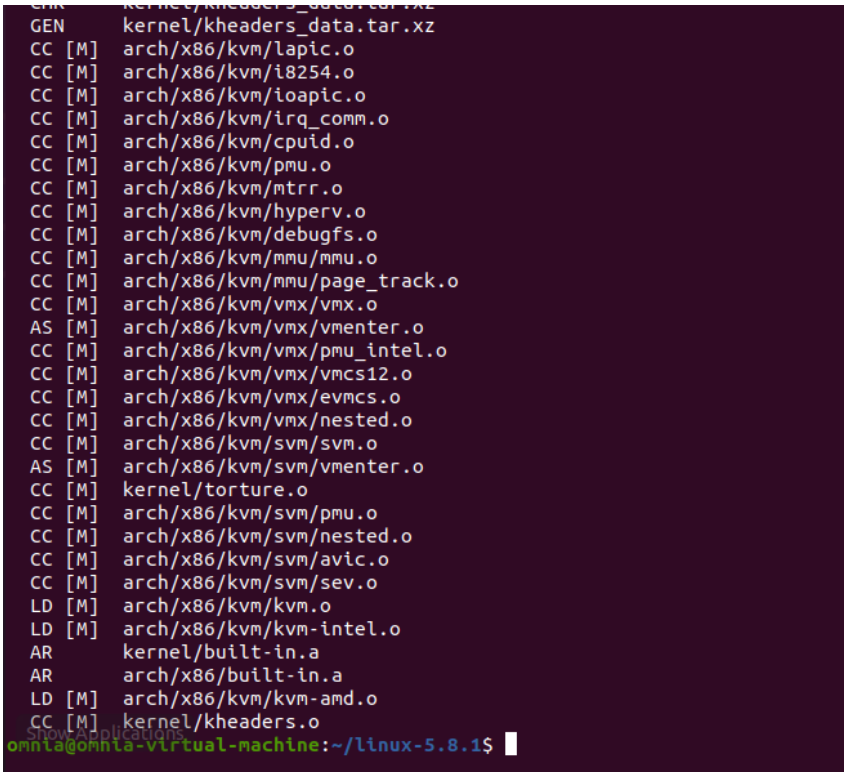
First : Configure the kernel. use "make menuconfig"

Use Tab to move between options. Make no changes to keep it in default settings.



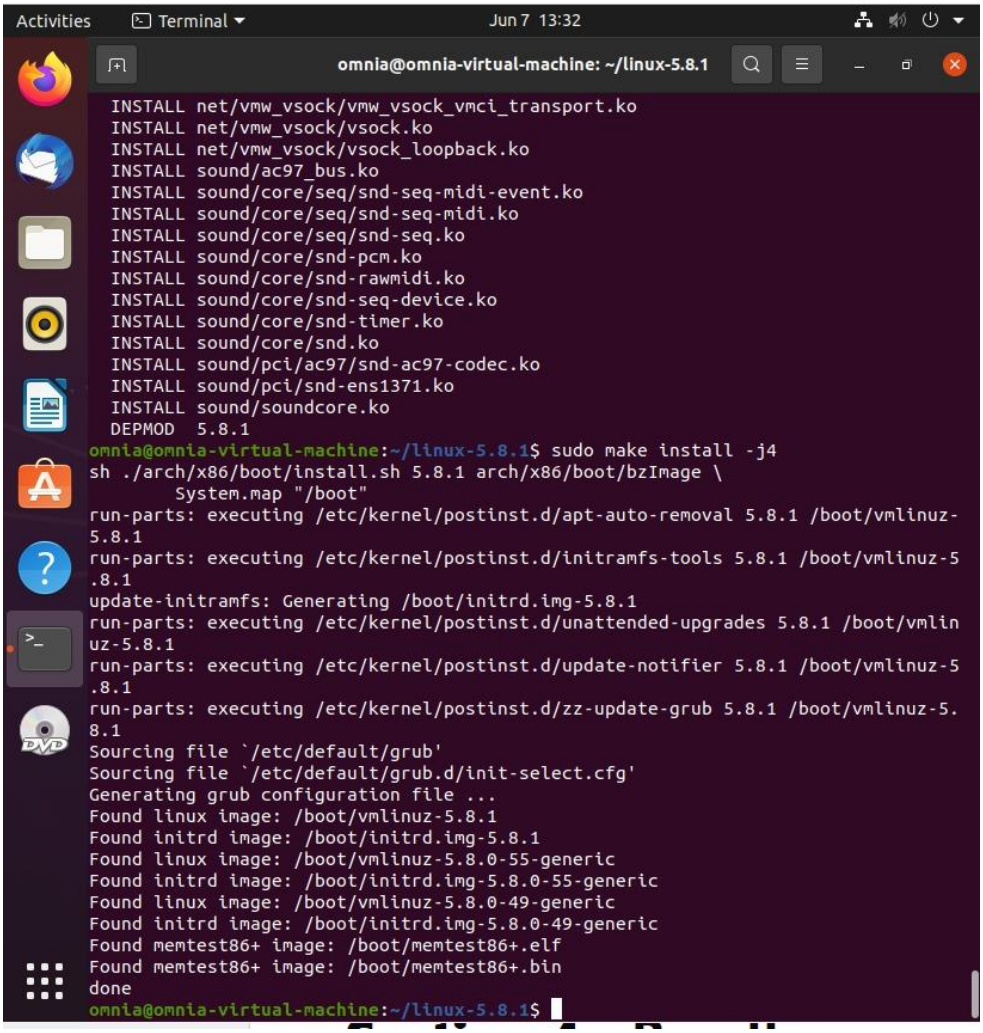
And find out how many logical cores you have. in my machine um using 4

Compile the kernel's source code. : by "make –j4"



Prepare the installer of the kernel.By using "sudo make modules_install –j4"

And Install the kernel.



Update the bootloader of the operating system with the new kernel. by using "sudo update-grub"

Now : I will reboot my computer.

The result:

First i will change my working directory to my home directory.

Now i will Create a C file to generate a report of the success or failure of your system call.

using nano Omnia.c and put this program :

```
#include <linux/kernel.h>
#include <sys/syscall.h>
#include <stdio.h>
#include <unistd.h>
#include <string.h>
#include <errno.h>

#define __NR_identity 440
```

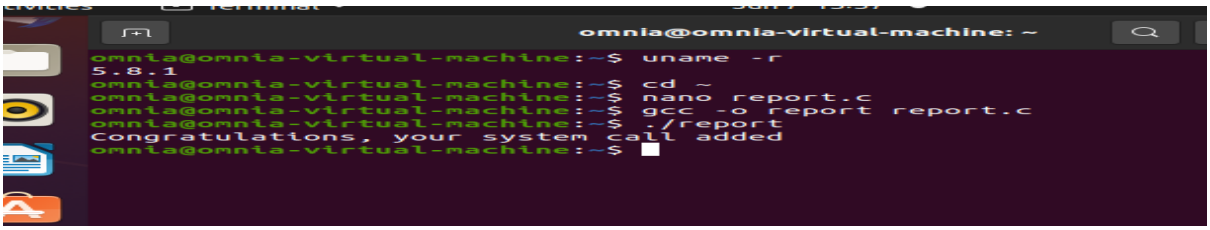
```
long identity_syscall(void)
{
    return syscall(__NR_identity);
}

int main(int argc, char *argv[])
{
    long activity;
    activity = identity_syscall();

    if(activity < 0)
    {
        perror("Sorry Try again .");
    }

    else
    {
        printf("Congratulations ,your system call added\n");
    }

    return 0;
}
```

```c
#include <linux/kernel.h>
#include <sys/syscall.h>
#include <stdio.h>
#include <unistd.h>
#include <string.h>
#include <errno.h>

#define __NR_identity 440

long identity_syscall(void)
{
    return syscall(__NR_identity);
}

int main(int argc, char *argv[])
{
    long activity;
    activity = identity_syscall();

    if(activity < 0)
    {
        perror("Sorry Try again.");
    }

    else
    {
        printf("Congrats The system call added \n");
    }

    return 0;
}
```

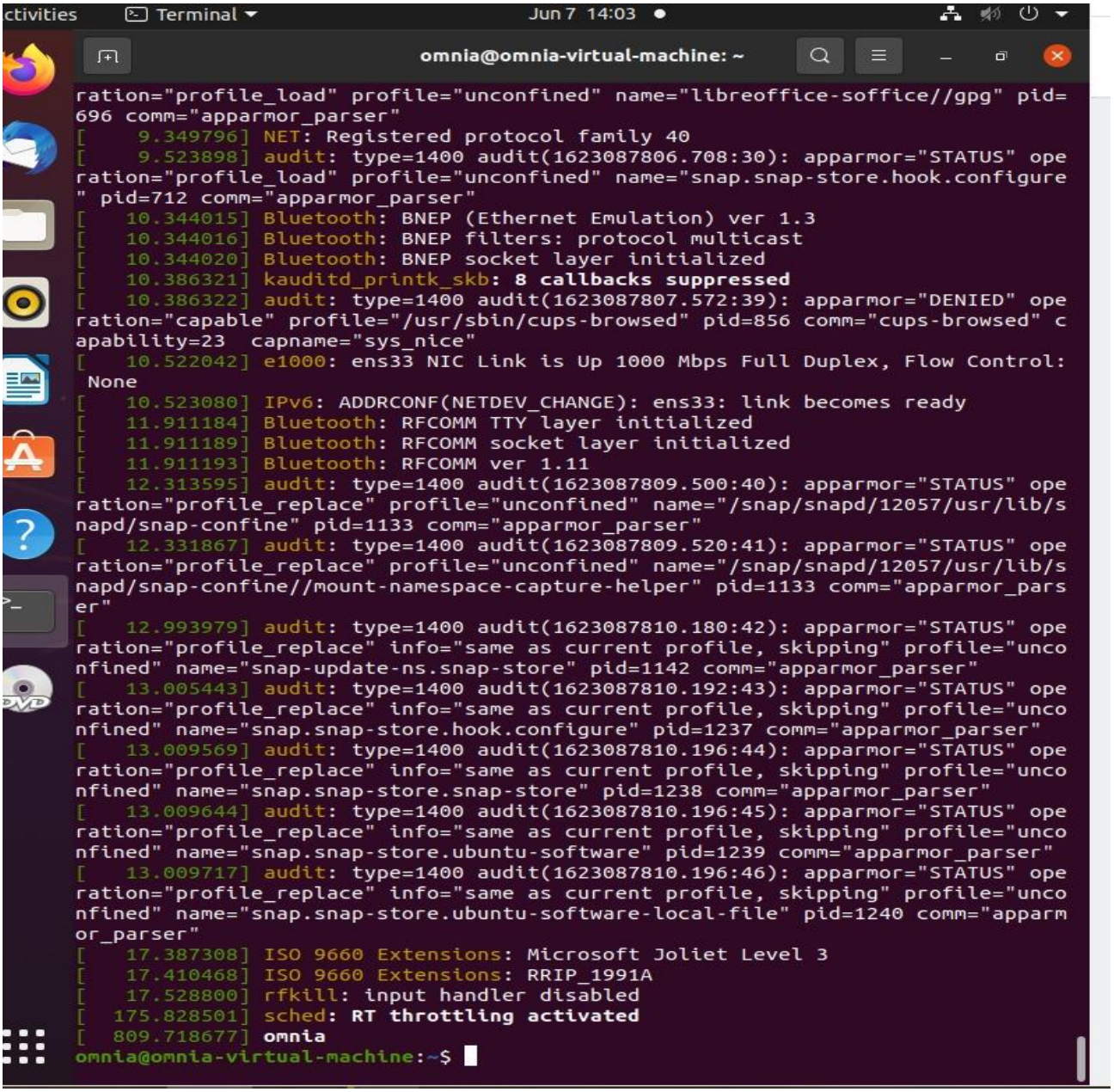
Now compile the program by usin **gcc**

gcc -o Omnia Omnia.c

Run and you see



The print function :


ctivities
Terminal
Jun 7 14:03
omnia@omnia-virtual-machine: ~
ration="profile_load" profile="unconfined" name="libreoffice-soffice//gpg" pid=
696 comm="apparmor_parser"
[9.349796] NET: Registered protocol family 40
[9.523898] audit: type=1400 audit(1623087806.708:30): apparmor="STATUS" ope
ration="profile_load" profile="unconfined" name="snap.snap-store.hook.configure
" pid=712 comm="apparmor_parser"
[10.344015] Bluetooth: BNEP (Ethernet Emulation) ver 1.3
[10.344016] Bluetooth: BNEP filters: protocol multicast
[10.344020] Bluetooth: BNEP socket layer initialized
[10.386321] kauditd_printk_skb: 8 callbacks suppressed
[10.386322] audit: type=1400 audit(1623087807.572:39): apparmor="DENIED" ope
ration="capable" profile="/usr/sbin/cups-browsed" pid=856 comm="cups-browsed" c
apability=23 capname="sys_nice"
[10.522042] e1000: ens33 NIC Link is Up 1000 Mbps Full Duplex, Flow Control:
None
[10.523080] IPv6: ADDRCONF(NETDEV_CHANGE): ens33: link becomes ready
[11.911184] Bluetooth: RFCOMM TTY layer initialized
[11.911189] Bluetooth: RFCOMM socket layer initialized
[11.911193] Bluetooth: RFCOMM ver 1.11
[12.313595] audit: type=1400 audit(1623087809.500:40): apparmor="STATUS" ope
ration="profile_replace" profile="unconfined" name="/snap/snapd/12057/usr/lib/s
napd/snap-confine" pid=1133 comm="apparmor_parser"
[12.331867] audit: type=1400 audit(1623087809.520:41): apparmor="STATUS" ope
ration="profile_replace" profile="unconfined" name="/snap/snapd/12057/usr/lib/s
napd/snap-confine//mount-namespace-capture-helper" pid=1133 comm="apparmor_pars
er"
[12.993979] audit: type=1400 audit(1623087810.180:42): apparmor="STATUS" ope
ration="profile_replace" info="same as current profile, skipping" profile="unco
nfined" name="snap-update-ns.snap-store" pid=1142 comm="apparmor_parser"
[13.005443] audit: type=1400 audit(1623087810.192:43): apparmor="STATUS" ope
ration="profile_replace" info="same as current profile, skipping" profile="unco
nfined" name="snap.snap-store.hook.configure" pid=1237 comm="apparmor_parser"
[13.009569] audit: type=1400 audit(1623087810.196:44): apparmor="STATUS" ope
ration="profile_replace" info="same as current profile, skipping" profile="unco
nfined" name="snap.snap-store.snap-store" pid=1238 comm="apparmor_parser"
[13.009644] audit: type=1400 audit(1623087810.196:45): apparmor="STATUS" ope
ration="profile_replace" info="same as current profile, skipping" profile="unco
nfined" name="snap.snap-store.ubuntu-software" pid=1239 comm="apparmor_parser"
[13.009717] audit: type=1400 audit(1623087810.196:46): apparmor="STATUS" ope
ration="profile_replace" info="same as current profile, skipping" profile="unco
nfined" name="snap.snap-store.ubuntu-software-local-file" pid=1240 comm="apparm
or_parser"
[17.387308] ISO 9660 Extensions: Microsoft Joliet Level 3
[17.410468] ISO 9660 Extensions: RRIP_1991A
[17.528800] rfkill: input handler disabled
[175.828501] sched: RT throttling activated
[809.718677] omnia
omnia@omnia-virtual-machine:~$