All these steps are written with respect to deployment in azure VM.

command	description
wgethttps://cdn.kernel.org/pub/linux/kernel/v4.x/linux-4.19.210.tar.xz	Install linux kernel compressed file
xz -v -d linux-4.19.210.tar.xz	Unzipping the contents
tar xvf linux-4.19.210.tar	
cd linux-4.19.210	Change to newly created kernel
mkdir assignment2	Create new dir
cd assignment2	Go to newly created dir
touch Q1.c Q2.c Q3.c Q4.c	Create 4 c files
/* edit the corresponding codes */	
nano Makefile	Create a makefile for easier compilation (edit and save the file)
cd ..	Goto linux kernel folder
nano Makefile	Edit the makefile of this folder so that the directory in which we write system calls will be recognized by the kernel, next time we boot
cd arch/x86/entry/syscalls/	Change to syscalls dir
nano syscall_64.tbl	Edit the system call table to include our system calls. General format 548 64 Varunhello __x64_sys_Varunhello
cd ..	Go till we reach linux folder
cd *include*/linux	Chang to include/linux folder

nano syscalls.h	Change syscalls.h to include our calls. General format asmlinkage long sys_Varunhello(void)
sudo apt-get install ccache sudo apt-get install bc sudo apt-get install gcc sudo apt-get install libncurses5-dev sudo apt-get install bison sudo apt-get install flex sudo apt-get install libssl-dev sudo apt-get install libelf-dev sudo apt-get update sudo apt-get upgrade	Installing basic dependencies to compile our kernel. ccache is a software development tool that caches the output of C/C++ compilation so that the next time, the same compilation can be avoided and the results can be taken from the cache.
cp -v /boot/config-$(uname -r) .config	Copy older config file to newer file. Remove CONFIG_SYSTEM_TRUSTED_KEYS to avoid any compilation errors
Sudo make olddefconfig Sudo make prepare Sudo ccache make -j5	Preparation using existing kernel config. Cache helps us reduce time when we recompile our code and -j5 depicts the number of cores -j(n+1) where n is the number of cores
Sudo make modules_install	Kernel compilation takes some time. After that, we need to install modules to use our system calls
Sudo make install	
update-initramfs -ck 4.19.210 sudo update-grub	We are changing our ram file system to boot our kernel version by default and then we are updating grand unified boot loader (grub)

shutdown -r now	After shutdown and restart, we should be able to boot to our linux version and we are good to use our system calls.

Q1

Code is

```
#include<linux/syscalls.h>
#include<linux/kernel.h>
0SYSCALL_DEFINE0(Varunhello) {
        printk("Hiii!!! Varun Here\n");
        return 0;
}
```

which will print the string to kernel logs

Q2

Code is

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

SYSCALL_DEFINE2(diviprint,
            char __user *, input,
            int, input_length)
{
    char buffer[256];
    unsigned long left_length = input_length;
    unsigned long chunklen = sizeof(buffer);
    while( left_length > 0 ){
        if(left_length < chunklen ) chunklen =left_length;
        if( copy_from_user(buffer, input, chunklen) ){
        return -EFAULT;
    }
        left_length -= chunklen;
    }
```

```
        printk("%s\n", buffer);

        return 0;
}
```
which will print the string to kernel logs provided by user

Q3

```
#include<linux/syscalls.h>
#include<linux/kernel.h>
#include<linux/cred.h>
#include<linux/sched.h>
SYSCALL_DEFINE0(Varunprocess) {
          struct task_struct *parent=current->parent;
          printk("parent_process_pid: %d \n", parent->pid);
          printk("current_process_pid: %d \n", current->pid); return 0;
}
```

Prints process id of current process and parent process

Q4

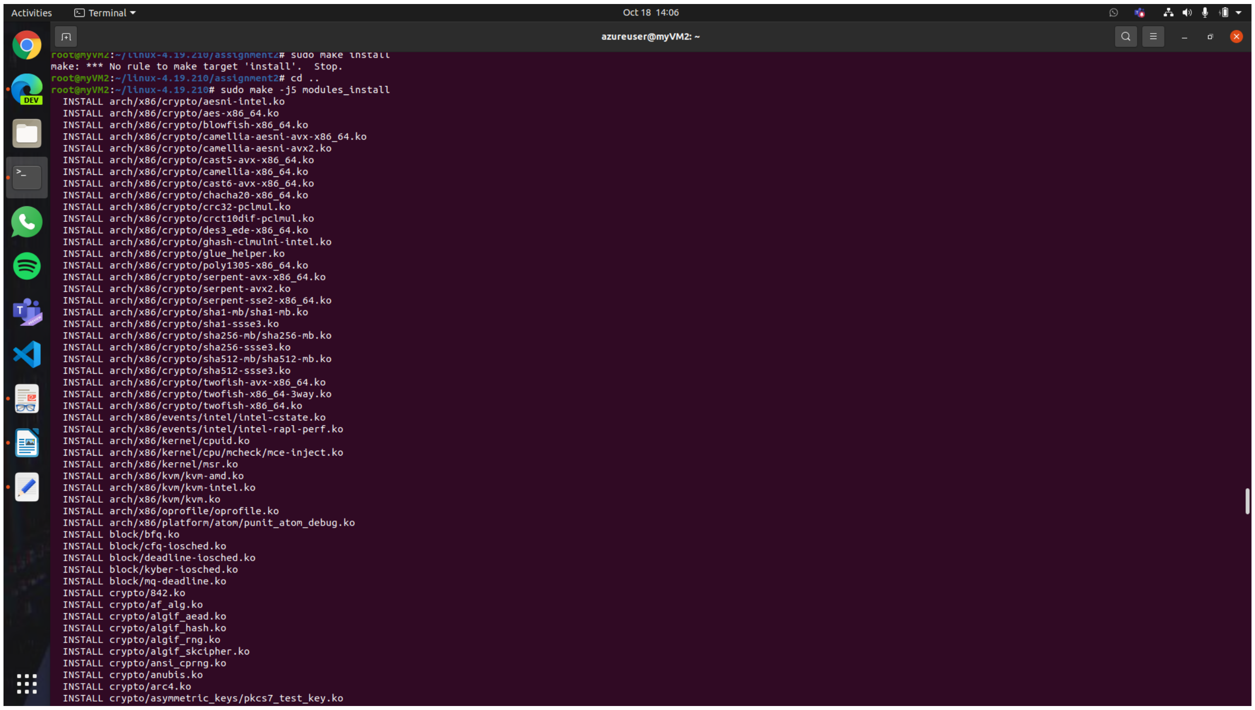
```
#include<linux/syscalls.h>
#include<linux/kernel.h>
#include<linux/cred.h>
#include<linux/sched.h>

SYSCALL_DEFINE0(divigetpid)
{
       printk("User id is:%u\n",task_tgid_vnr(current));
     return task_tgid_vnr(current);
}
```
Executes a system call and returns the O/P

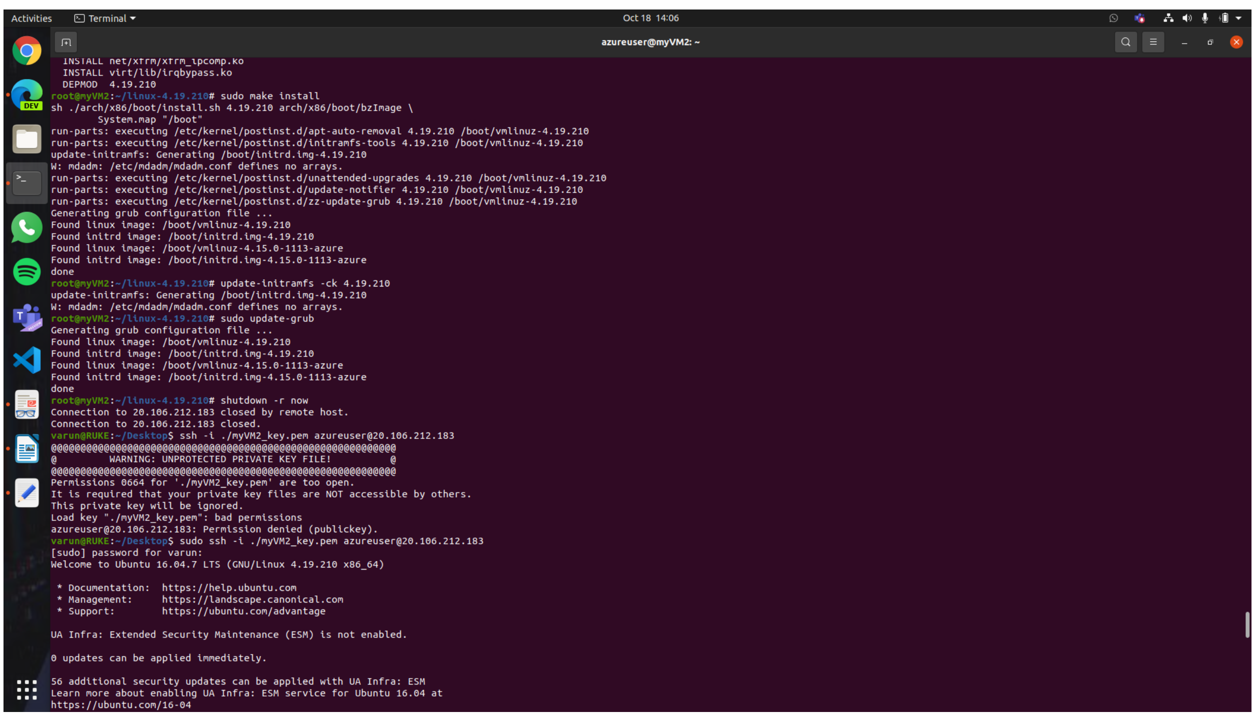
Parent and current process ids are different. Why?

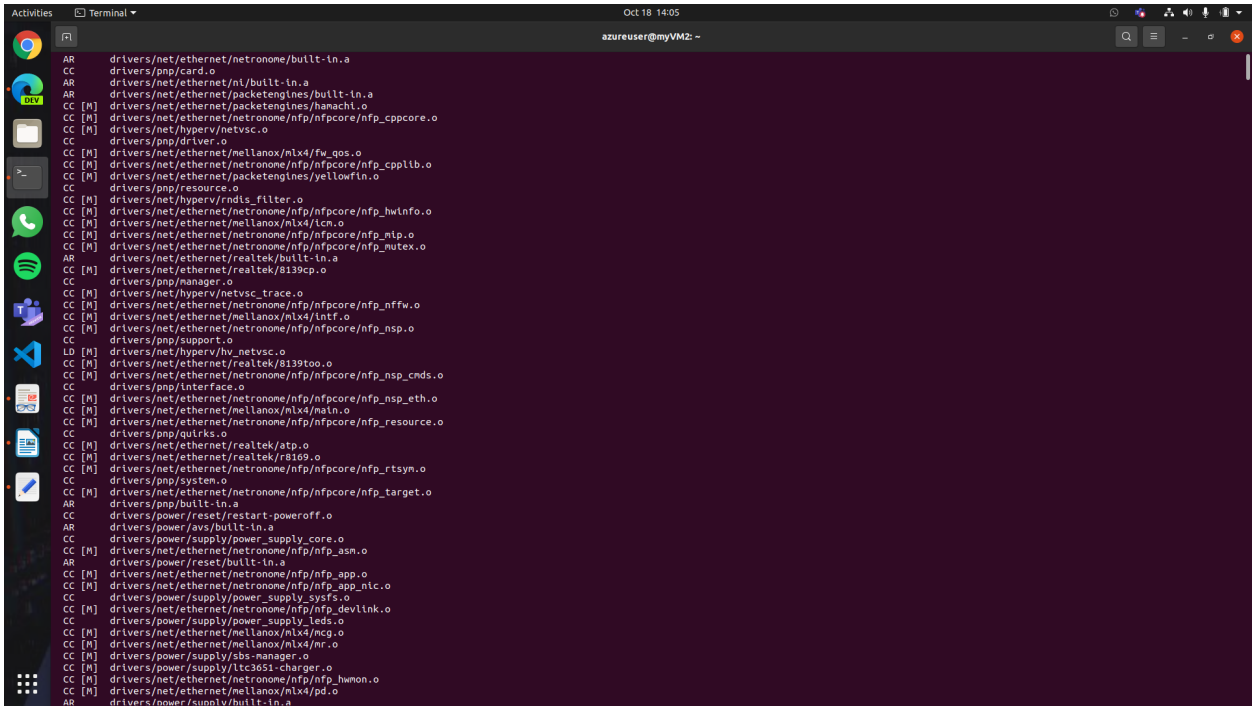
Current process is the process which encompasses the .c file which we run and all the subsequent calls we make. Hence it has some ID associated with it.

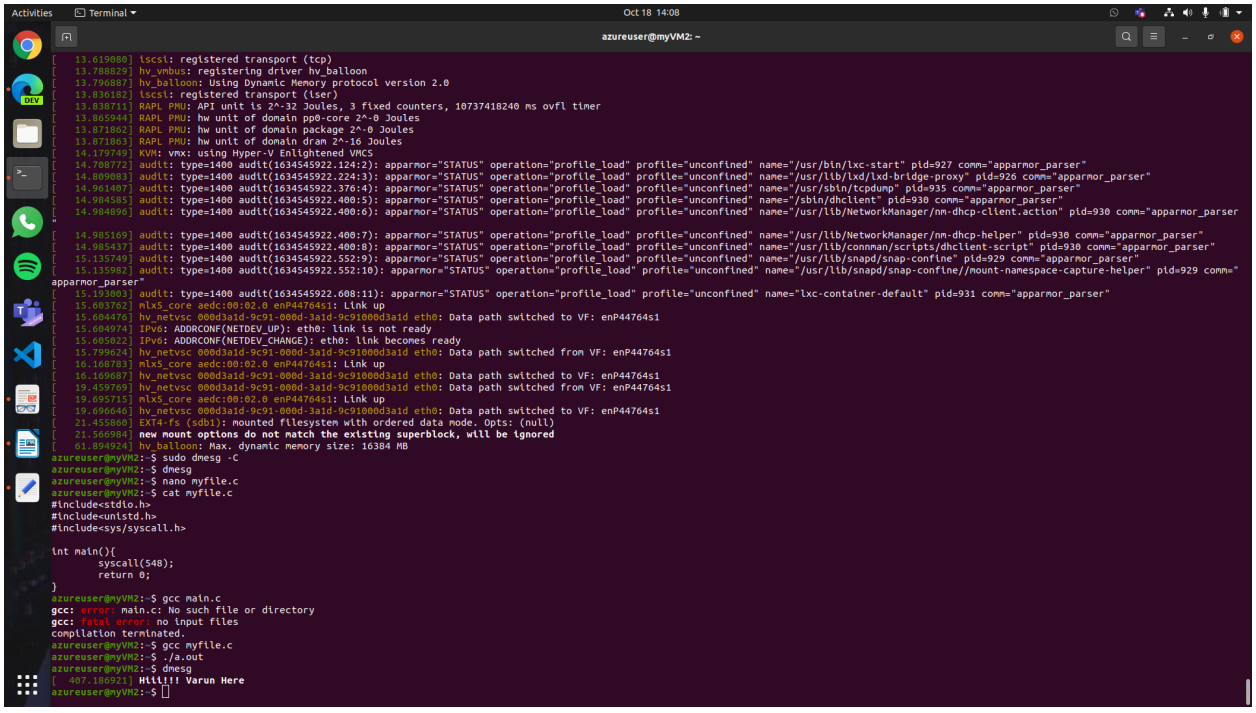
Parent process is the process which invokes our .c file and it will have an ID associated with it and since no two different processes can share same ID, both will have different IDs

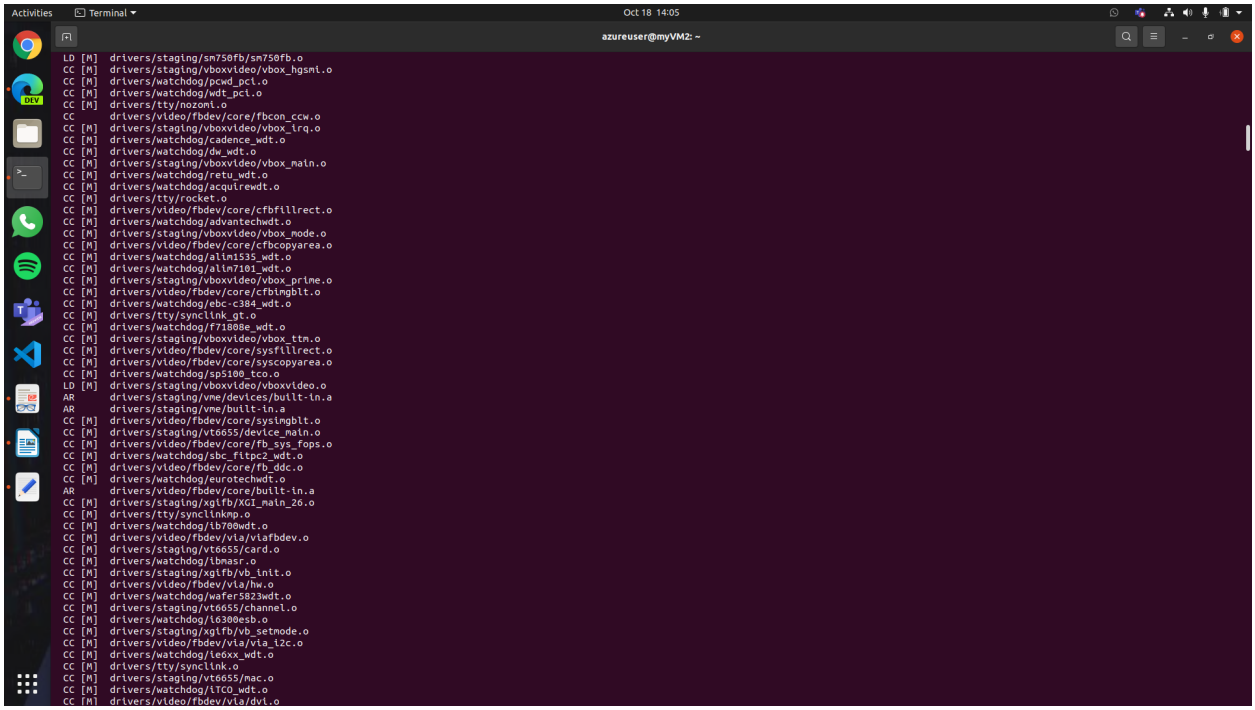
Execution screenshots






Activities
Terminal
Oct 18 14:05
azureuser@myVM2: ~
AR drivers/net/ethernet/netronome/built-in.a
CC drivers/pnp/card.o
AR drivers/net/ethernet/ni/built-in.a
AR drivers/net/ethernet/packetengines/built-in.a
CC [M] drivers/net/ethernet/packetengines/hamachi.o
CC [M] drivers/net/ethernet/netronome/nfp/nfpcore/nfp_cppcore.o
CC [M] drivers/net/hyperv/netvsc.o
CC drivers/pnp/driver.o
CC [M] drivers/net/ethernet/mellanox/mlx4/fw_qos.o
CC [M] drivers/net/ethernet/netronome/nfp/nfpcore/nfp_cpplib.o
CC [M] drivers/net/ethernet/packetengines/yellowfin.o
CC drivers/pnp/resource.o
CC [M] drivers/net/hyperv/rndis_filter.o
CC [M] drivers/net/ethernet/netronome/nfp/nfpcore/nfp_hwinfo.o
CC [M] drivers/net/ethernet/mellanox/mlx4/icm.o
CC [M] drivers/net/ethernet/netronome/nfp/nfpcore/nfp_mip.o
CC [M] drivers/net/ethernet/netronome/nfp/nfpcore/nfp_mutex.o
AR drivers/net/ethernet/realtek/built-in.a
CC [M] drivers/net/ethernet/realtek/8139cp.o
CC drivers/pnp/manager.o
CC [M] drivers/net/hyperv/netvsc_trace.o
CC [M] drivers/net/ethernet/netronome/nfp/nfpcore/nfp_nffw.o
CC [M] drivers/net/ethernet/mellanox/mlx4/intf.o
CC [M] drivers/net/ethernet/netronome/nfp/nfpcore/nfp_nsp.o
CC drivers/pnp/support.o
LD [M] drivers/net/hyperv/hv_netvsc.o
CC [M] drivers/net/ethernet/realtek/8139too.o
CC [M] drivers/net/ethernet/netronome/nfp/nfpcore/nfp_nsp_cmds.o
CC drivers/pnp/interface.o
CC [M] drivers/net/ethernet/netronome/nfp/nfpcore/nfp_nsp_eth.o
CC [M] drivers/net/ethernet/mellanox/mlx4/main.o
CC [M] drivers/net/ethernet/netronome/nfp/nfpcore/nfp_resource.o
CC drivers/pnp/quirks.o
CC [M] drivers/net/ethernet/realtek/atp.o
CC [M] drivers/net/ethernet/realtek/r8169.o
CC [M] drivers/net/ethernet/netronome/nfp/nfpcore/nfp_rtsym.o
CC drivers/pnp/system.o
CC [M] drivers/net/ethernet/netronome/nfp/nfpcore/nfp_target.o
AR drivers/pnp/built-in.a
CC drivers/power/reset/restart-poweroff.o
AR drivers/power/avs/built-in.a
CC drivers/power/supply/power_supply_core.o
CC [M] drivers/net/ethernet/netronome/nfp/nfp_asm.o
AR drivers/power/reset/built-in.a
CC [M] drivers/net/ethernet/netronome/nfp/nfp_app.o
CC [M] drivers/net/ethernet/netronome/nfp/nfp_app_nic.o
CC drivers/power/supply/power_supply_sysfs.o
CC [M] drivers/net/ethernet/netronome/nfp/nfp_devlink.o
CC drivers/power/supply/power_supply_leds.o
CC [M] drivers/net/ethernet/mellanox/mlx4/mcg.o
CC [M] drivers/net/ethernet/mellanox/mlx4/mr.o
CC [M] drivers/power/supply/sbs-manager.o
CC [M] drivers/power/supply/ltc3651-charger.o
CC [M] drivers/net/ethernet/netronome/nfp/nfp_hwmon.o
CC [M] drivers/net/ethernet/mellanox/mlx4/pd.o
AR drivers/power/supply/built-in.a


Activities
Terminal
Oct 18 14:08
azureuser@myVM2: ~
[13.619080] iscsi: registered transport (tcp)
[13.708829] hv_vmbus: registering driver hv_balloon
[13.790887] hv_balloon: Using Dynamic Memory protocol version 2.0
[13.836182] iscsi: registered transport (iser)
[13.838711] RAPL PMU: API unit is 2^-32 Joules, 3 fixed counters, 10737418240 ms ovfl timer
[13.865944] RAPL PMU: hw unit of domain pp0-core 2^-0 Joules
[13.871862] RAPL PMU: hw unit of domain package 2^-0 Joules
[13.871863] RAPL PMU: hw unit of domain dram 2^-16 Joules
[14.179749] KVM: vmx: using Hyper-V Enlightened VMCS
[14.708772] audit: type=1400 audit(1634545922.124:2): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/bin/lxc-start" pid=927 comm="apparmor_parser"
[14.809083] audit: type=1400 audit(1634545922.224:3): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/lxd/lxd-bridge-proxy" pid=926 comm="apparmor_parser"
[14.961407] audit: type=1400 audit(1634545922.376:4): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin/tcpdump" pid=935 comm="apparmor_parser"
[14.984585] audit: type=1400 audit(1634545922.400:5): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/sbin/dhclient" pid=930 comm="apparmor_parser"
[14.984896] audit: type=1400 audit(1634545922.400:6): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/NetworkManager/nm-dhcp-client.action" pid=930 comm="apparmor_parser
"
[14.985169] audit: type=1400 audit(1634545922.400:7): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/NetworkManager/nm-dhcp-helper" pid=930 comm="apparmor_parser"
[14.985437] audit: type=1400 audit(1634545922.400:8): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/connman/scripts/dhclient-script" pid=930 comm="apparmor_parser"
[15.135749] audit: type=1400 audit(1634545922.552:9): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/snapd/snap-confine" pid=929 comm="apparmor_parser"
[15.135982] audit: type=1400 audit(1634545922.552:10): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/snapd/snap-confine//mount-namespace-capture-helper" pid=929 comm="
apparmor_parser"
[15.171003] audit: type=1400 audit(1634545922.608:11): apparmor="STATUS" operation="profile_load" profile="unconfined" name="lxc-container-default" pid=931 comm="apparmor_parser"
[15.603762] mlx5_core aedc:00:02.0 enP44764s1: Link up
[15.604476] hv_netvsc 000d3a1d-9c91-000d-3a1d-9c91000d3a1d eth0: Data path switched to VF: enP44764s1
[15.604974] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15.605022] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[15.799624] hv_netvsc 000d3a1d-9c91-000d-3a1d-9c91000d3a1d eth0: Data path switched from VF: enP44764s1
[16.168783] mlx5_core aedc:00:02.0 enP44764s1: Link up
[16.169687] hv_netvsc 000d3a1d-9c91-000d-3a1d-9c91000d3a1d eth0: Data path switched to VF: enP44764s1
[19.459769] hv_netvsc 000d3a1d-9c91-000d-3a1d-9c91000d3a1d eth0: Data path switched from VF: enP44764s1
[19.695715] mlx5_core aedc:00:02.0 enP44764s1: Link up
[19.696646] hv_netvsc 000d3a1d-9c91-000d-3a1d-9c91000d3a1d eth0: Data path switched to VF: enP44764s1
[21.455860] EXT4-fs (sdb1): mounted filesystem with ordered data mode. Opts: (null)
[21.566984] new mount options do not match the existing superblock, will be ignored
[61.894924] hv_balloon: Max. dynamic memory size: 16384 MB
azureuser@myVM2:~$ sudo dmesg -C
azureuser@myVM2:~$ dmesg
azureuser@myVM2:~$ nano myfile.c
azureuser@myVM2:~$ cat myfile.c
#include<stdio.h>
#include<unistd.h>
#include<sys/syscall.h>
int main(){
syscall(548);
return 0;
}
azureuser@myVM2:~$ gcc main.c
gcc: error: main.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
azureuser@myVM2:~$ gcc myfile.c
azureuser@myVM2:~$ ./a.out
azureuser@myVM2:~$ dmesg
[407.186921] Hiiii!! Varun Here
azureuser@myVM2:~$


Activities
Terminal
Oct 18 14:05
azureuser@myVM2: ~
LD [M] drivers/staging/sm750fb/sm750fb.o
CC [M] drivers/staging/vboxvideo/vbox_hgsmi.o
CC [M] drivers/watchdog/pcwd_pci.o
CC [M] drivers/watchdog/wdt_pci.o
CC [M] drivers/tty/nozomi.o
CC drivers/video/fbdev/core/fbcon_ccw.o
CC [M] drivers/staging/vboxvideo/vbox_irq.o
CC [M] drivers/watchdog/cadence_wdt.o
CC [M] drivers/watchdog/dw_wdt.o
CC [M] drivers/staging/vboxvideo/vbox_main.o
CC [M] drivers/watchdog/retu_wdt.o
CC [M] drivers/watchdog/acquirewdt.o
CC [M] drivers/tty/rocket.o
CC [M] drivers/video/fbdev/core/cfbfillrect.o
CC [M] drivers/watchdog/advantechwdt.o
CC [M] drivers/staging/vboxvideo/vbox_mode.o
CC [M] drivers/video/fbdev/core/cfbcopyarea.o
CC [M] drivers/watchdog/alim1535_wdt.o
CC [M] drivers/watchdog/alim7101_wdt.o
CC [M] drivers/staging/vboxvideo/vbox_prime.o
CC [M] drivers/video/fbdev/core/cfbimgblt.o
CC [M] drivers/watchdog/ebc-c384_wdt.o
CC [M] drivers/tty/synclink_gt.o
CC [M] drivers/watchdog/f71808e_wdt.o
CC [M] drivers/staging/vboxvideo/vbox_ttm.o
CC [M] drivers/video/fbdev/core/sysfillrect.o
CC [M] drivers/video/fbdev/core/syscopyarea.o
CC [M] drivers/watchdog/sp5100_tco.o
LD [M] drivers/staging/vboxvideo/vboxvideo.o
AR drivers/staging/vme/devices/built-in.a
AR drivers/staging/vme/built-in.a
CC [M] drivers/video/fbdev/core/sysimgblt.o
CC [M] drivers/staging/vt6655/device_main.o
CC [M] drivers/video/fbdev/core/fb_sys_fops.o
CC [M] drivers/watchdog/sbc_fitpc2_wdt.o
CC [M] drivers/video/fbdev/core/fb_ddc.o
CC [M] drivers/watchdog/eurotechwdt.o
AR drivers/video/fbdev/core/built-in.a
CC [M] drivers/staging/xgifb/XGI_main_26.o
CC [M] drivers/tty/synclinkmp.o
CC [M] drivers/watchdog/ib700wdt.o
CC [M] drivers/video/fbdev/via/viafbdev.o
CC [M] drivers/staging/vt6655/card.o
CC [M] drivers/watchdog/ibmasr.o
CC [M] drivers/staging/xgifb/vb_init.o
CC [M] drivers/video/fbdev/via/hw.o
CC [M] drivers/watchdog/wafer5823wdt.o
CC [M] drivers/staging/vt6655/channel.o
CC [M] drivers/watchdog/i6300esb.o
CC [M] drivers/staging/xgifb/vb_setmode.o
CC [M] drivers/video/fbdev/via/via_i2c.o
CC [M] drivers/watchdog/ie6xx_wdt.o
CC [M] drivers/tty/synclink.o
CC [M] drivers/staging/vt6655/mac.o
CC [M] drivers/watchdog/iTCO_wdt.o
CC [M] drivers/video/fbdev/via/dvi.o