CMPE 283: Virtualization Technologies

Assignment 3: Instrumentation via hypercall

Bhavya Tetali (014535144), Supriya Meduri (015262767)

Contribution of Team Members

Bhavya Tetali:

- Modified the code in vmx.c to track the exit types by exit reason.
- Modified the code in cpuid.c to support the new LEAF node
- Created a user program to print count for all exit reasons.
- Created the documentation.

Supriya Meduri:

- Researched about exit types that are not defined by the SDM and not enabled in the KVM. And did the changes to cpuid.c to handle the exit types accordingly.
- Install cpuid package and researched about its usage.
- Created a user program to print count for a specific exit reason.
- Updated the documentation.

Environment Setup

We built this homework based on assignment-2 and hence followed the same environment setup.

Implementation

- Updated vmx.c to keep track of exit counts by exit reason. Updated cpuid.c to support new CPUID leaf 0x4FFFFFFE

- In the outer VM, do the following:

    - Remove the kvm and kvm_intel modules

```
$ sudo rmmod kvm_intel
$ sudo rmmod kvm
```

- Compile the updated kernel code

```
$ sudo make -j 8 modules M=arch/x86/kvm
```

```
oot@bhavyalalithya-virtual-machine:/home/bhavyalalithya/linux#
oot@bhavyalalithya-virtual-machine:/home/bhavyalalithya/linux# sudo make -j 8 modules M=arch/x86/kvm
 CC [M]  arch/x86/kvm/cpuid.o
 CC [M]  arch/x86/kvm/vmx/vmx.o
 LD [M]  arch/x86/kvm/kvm.o
 LD [M]  arch/x86/kvm/kvm-intel.o
 MODPOST arch/x86/kvm/Module.symvers
 LD [M]  arch/x86/kvm/kvm-intel.ko
 LD [M]  arch/x86/kvm/kvm.ko
oot@bhavyalalithya-virtual-machine:/home/bhavyalalithya/linux#
```

- Install the modules

```
$ sudo insmod arch/x86/kvm/kvm.ko
$ sudo insmod arch/x86/kvm/kvm-intel.ko
```

- In inner VM, installed cpuid package
- In the terminal run the commands to test each leaf

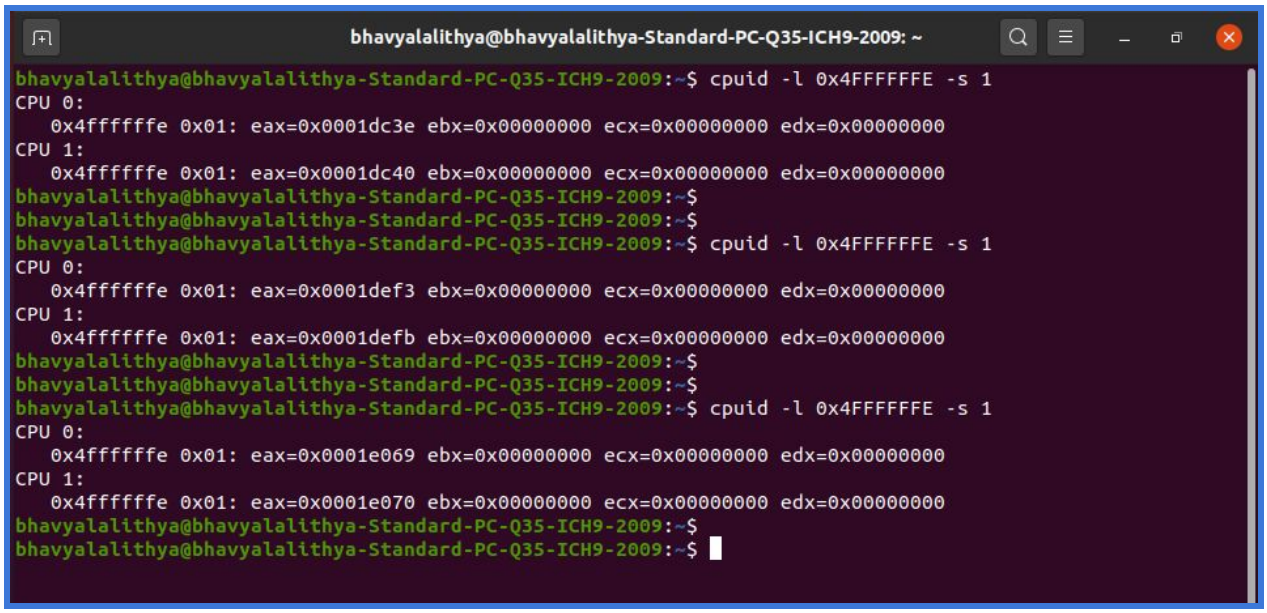
```
$ cpuid -l 0x4ffffffd -s exit_number
```

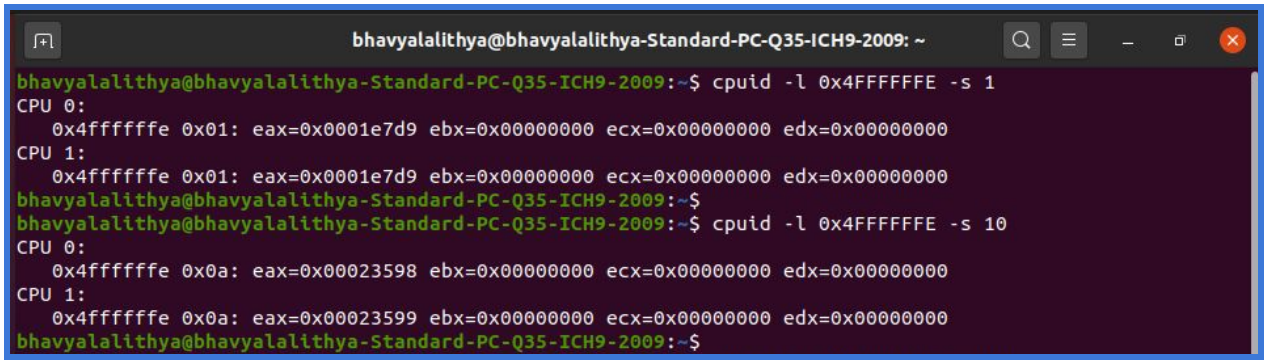
- In the outer VM, run the command “dmesg” to view the print statements

```
[ 3232.064962] psmouse serio1: VMMouse at isa0060/serio1/input0 lost synchronization, throwing 1 bytes away.
[ 3232.976233] psmouse serio1: resync failed, issuing reconnect request
[ Ubuntu Software CPUID(0x4FFFFFFE), exit number 1 exits=121918
[ 3278.103617] CPUID(0x4FFFFFFE), exit number 1 exits=121920
[ 3281.778622] CPUID(0x4FFFFFFE), exit number 1 exits=122611
[ 3281.784175] CPUID(0x4FFFFFFE), exit number 1 exits=122619
[ 3286.401716] CPUID(0x4FFFFFFE), exit number 1 exits=122985
[ 3286.403537] CPUID(0x4FFFFFFE), exit number 1 exits=122992
[ 3328.844173] INFO: NMI handler (perf_event_nmi_handler) took too long to run: 808.343 msecs
[ 3328.844177] perf: interrupt took too long (6328728 > 5910125), lowering kernel.perf_event_max_sample_rate to 250
[ 3386.904244] CPUID(0x4FFFFFFE), exit number 10 exits=144699
[ 3386.904631] CPUID(0x4FFFFFFE), exit number 10 exits=144700
[ 3388.659439] CPUID(0x4FFFFFFE), exit number 10 exits=144718
[ 3388.659988] CPUID(0x4FFFFFFE), exit number 10 exits=144719
[ 3390.518874] CPUID(0x4FFFFFFE), exit number 10 exits=144737
[ 3390.519576] CPUID(0x4FFFFFFE), exit number 10 exits=144738
[ 3397.359217] CPUID(0x4FFFFFFE), exit number 1 exits=124889
[ 3397.359473] CPUID(0x4FFFFFFE), exit number 1 exits=124889
[ 3399.613986] CPUID(0x4FFFFFFE), exit number 10 exits=144792
[ 3399.614222] CPUID(0x4FFFFFFE), exit number 10 exits=144793
[ 3414.868129] CPUID(0x4FFFFFFE), exit number 18 exits=0
[ 3414.868392] CPUID(0x4FFFFFFE), exit number 18 exits=0
[ 3509.100024] CPUID(0x4FFFFFFE), exit number 2 exits=0
[ 3509.100642] CPUID(0x4FFFFFFE), exit number 2 exits=0
[ 3512.403309] CPUID(0x4FFFFFFE), exit number 3 exits=0
[ 3512.403933] CPUID(0x4FFFFFFE), exit number 3 exits=0
[ 3528.130209] CPUID(0x4FFFFFFE), exit number 4 exits=0
[ 3528.130612] CPUID(0x4FFFFFFE), exit number 4 exits=0
[ 3633.652186] CPUID(0x4FFFFFFE), exit number 3 exits=0
[ 3633.652560] CPUID(0x4FFFFFFE), exit number 3 exits=0
[ 3635.626459] CPUID(0x4FFFFFFE), exit number 4 exits=0
[ 3635.971681] CPUID(0x4FFFFFFE), exit number 4 exits=0
[ 4245.687579] psmouse serio1: VMMouse at isa0060/serio1/input0 lost synchronization, throwing 1 bytes away.
[ 4246.231858] psmouse serio1: resync failed, issuing reconnect request
[ 6403.393767] CPUID(0x4FFFFFFE), exit number 1 exits=253279
[ 6445.418221] CPUID(0x4FFFFFFE), exit number 1 exits=258143
[ 7319.657930] CPUID(0x4FFFFFFE), exit number 1 exits=287687
[ 7323.041549] CPUID(0x4FFFFFFE), exit number 10 exits=147448
[ 7326.304783] CPUID(0x4FFFFFFE), exit number 2 exits=0
[ 7327.984366] CPUID(0x4FFFFFFE), exit number 3 exits=0
[ 7329.457077] CPUID(0x4FFFFFFE), exit number 4 exits=0
[ 7347.240542] CPUID(0x4FFFFFFE), exit number 10 exits=147520
[ 7347.241776] CPUID(0x4FFFFFFE), exit number 10 exits=147521
[ 7889.803359] CPUID(0x4FFFFFFE), exit number 1 exits=299586
[ 7891.784561] CPUID(0x4FFFFFFE), exit number 1 exits=299647
[ 7894.969051] CPUID(0x4FFFFFFE), exit number 1 exits=299713
[ 7904.442289] CPUID(0x4FFFFFFE), exit number 10 exits=147668
[ 7908.174054] CPUID(0x4FFFFFFE), exit number 18 exits=0
[ 7912.791946] CPUID(0x4FFFFFFE), exit number 14 exits=0
[ 7914.887739] CPUID(0x4FFFFFFE), exit number 12 exits=325861
root@bhavyalalithya-virtual-machine:/home/bhavyalalithya/linux#
```

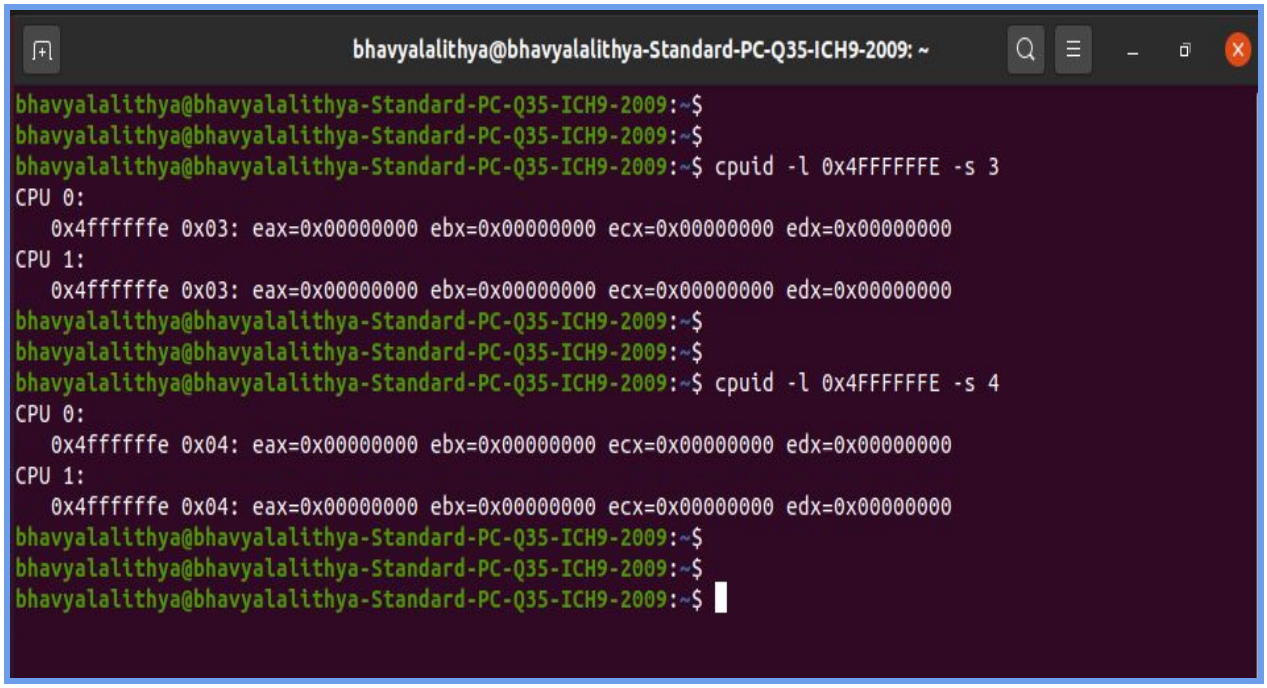
Screenshots

The below two screenshots shows exits count for exit reason 1 & 8, obtained using cpuid command.

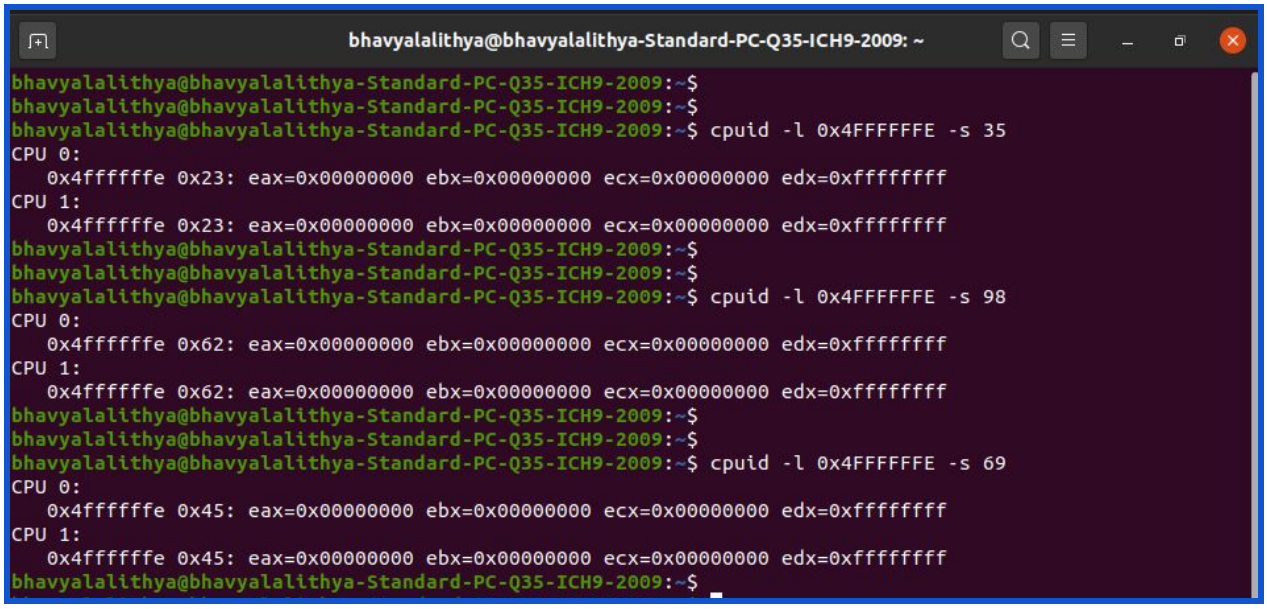




The below screenshot shows exits count for exit reason 3 & 4. Exits 3 and 4 are some of the exits that are not enabled in KVM, so their exits count is 0.

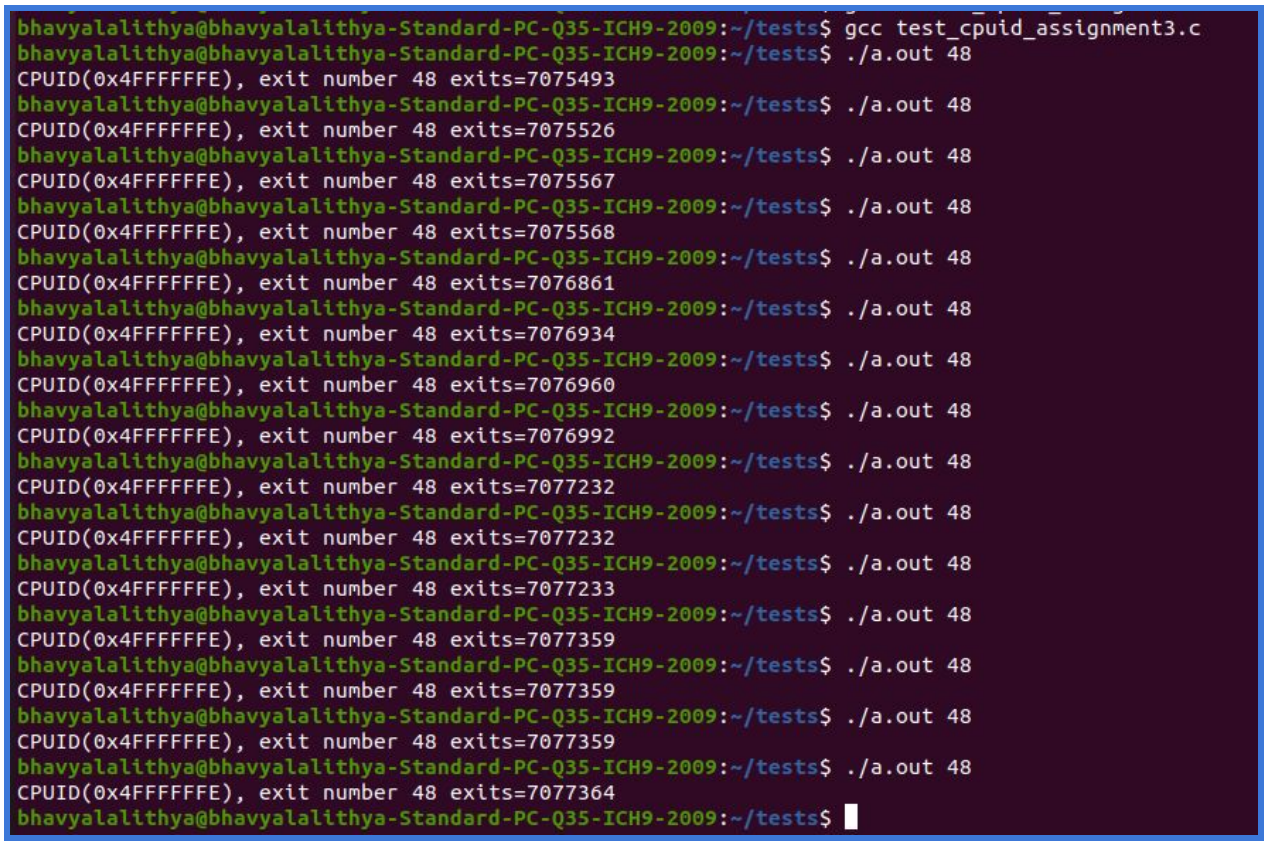


The below screenshot shows exits count for exit reason 3 & 4. Exits 3 and 4 are some of the exits that are not enabled in KVM, so their exits count is 0.



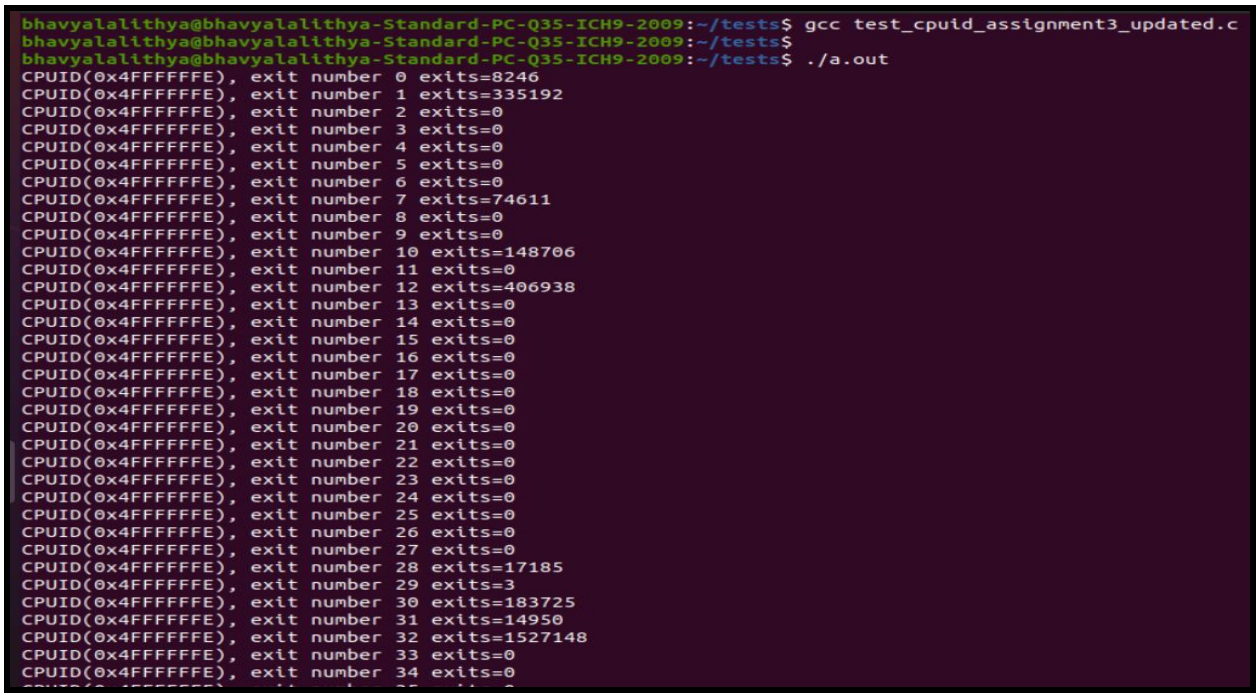
Frequency of exits for exit 48

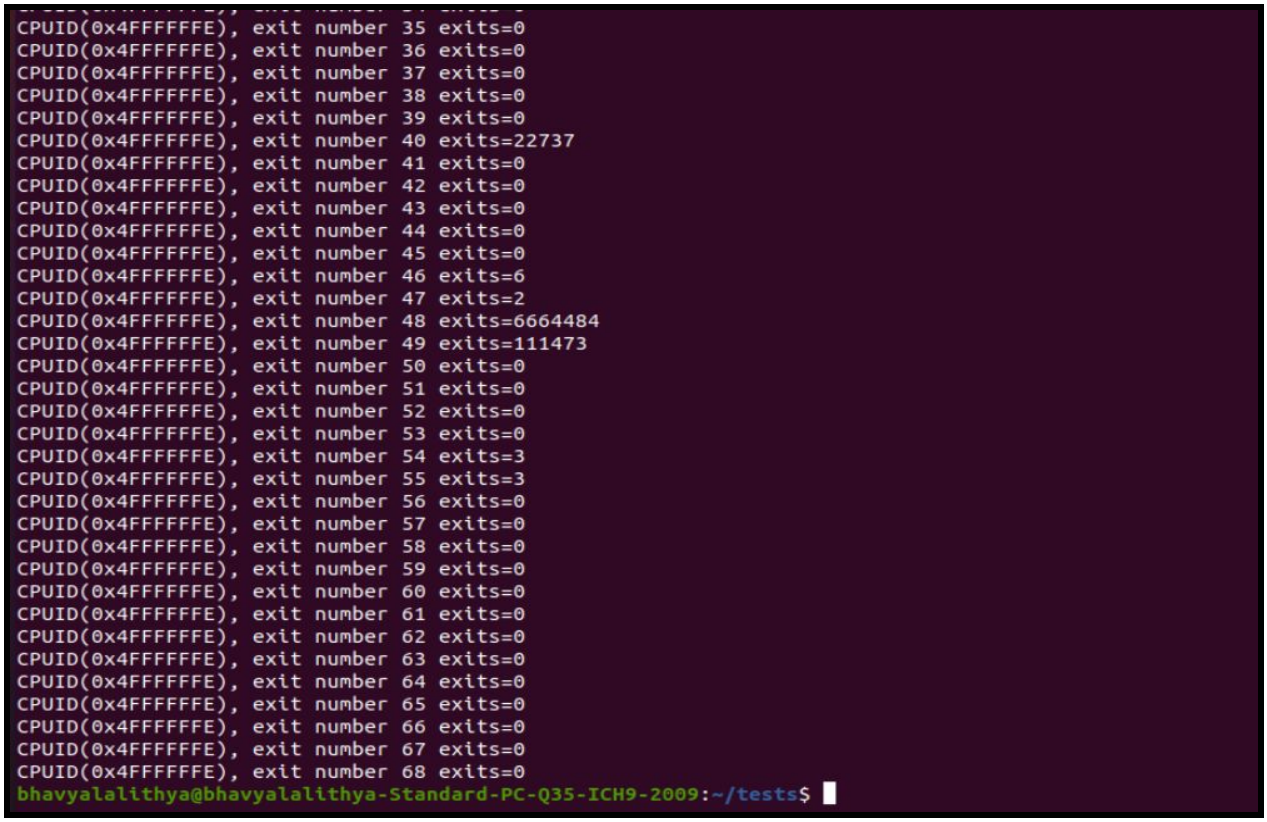
The below screenshot shows the output generated by user program code for exit reason 48.



Before boot

Below screenshots shows exits count for all the exit reasons before booting inner VM.





After boot

Below screenshots shows exits count for all the exit reasons before booting inner VM.

```
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$ ./a.out
CPUID(0x4FFFFFFE), exit number 0 exits=16170
CPUID(0x4FFFFFFE), exit number 1 exits=422199
CPUID(0x4FFFFFFE), exit number 2 exits=0
CPUID(0x4FFFFFFE), exit number 3 exits=0
CPUID(0x4FFFFFFE), exit number 4 exits=0
CPUID(0x4FFFFFFE), exit number 5 exits=0
CPUID(0x4FFFFFFE), exit number 6 exits=0
CPUID(0x4FFFFFFE), exit number 7 exits=91887
CPUID(0x4FFFFFFE), exit number 8 exits=0
CPUID(0x4FFFFFFE), exit number 9 exits=0
CPUID(0x4FFFFFFE), exit number 10 exits=293295
CPUID(0x4FFFFFFE), exit number 11 exits=0
CPUID(0x4FFFFFFE), exit number 12 exits=452172
CPUID(0x4FFFFFFE), exit number 13 exits=0
CPUID(0x4FFFFFFE), exit number 14 exits=0
CPUID(0x4FFFFFFE), exit number 15 exits=0
CPUID(0x4FFFFFFE), exit number 16 exits=0
CPUID(0x4FFFFFFE), exit number 17 exits=0
CPUID(0x4FFFFFFE), exit number 18 exits=0
CPUID(0x4FFFFFFE), exit number 19 exits=0
CPUID(0x4FFFFFFE), exit number 20 exits=0
CPUID(0x4FFFFFFE), exit number 21 exits=0
CPUID(0x4FFFFFFE), exit number 22 exits=0
CPUID(0x4FFFFFFE), exit number 23 exits=0
CPUID(0x4FFFFFFE), exit number 24 exits=0
CPUID(0x4FFFFFFE), exit number 25 exits=0
CPUID(0x4FFFFFFE), exit number 26 exits=0
CPUID(0x4FFFFFFE), exit number 27 exits=0
CPUID(0x4FFFFFFE), exit number 28 exits=34699
CPUID(0x4FFFFFFE), exit number 29 exits=5
CPUID(0x4FFFFFFE), exit number 30 exits=445658
CPUID(0x4FFFFFFE), exit number 31 exits=17088
CPUID(0x4FFFFFFE), exit number 32 exits=1716619
CPUID(0x4FFFFFFE), exit number 33 exits=0
CPUID(0x4FFFFFFE), exit number 34 exits=0
```

```
CPUID(0x4FFFFFFE), exit number 35 exits=0
CPUID(0x4FFFFFFE), exit number 36 exits=0
CPUID(0x4FFFFFFE), exit number 37 exits=0
CPUID(0x4FFFFFFE), exit number 38 exits=0
CPUID(0x4FFFFFFE), exit number 39 exits=0
CPUID(0x4FFFFFFE), exit number 40 exits=28855
CPUID(0x4FFFFFFE), exit number 41 exits=0
CPUID(0x4FFFFFFE), exit number 42 exits=0
CPUID(0x4FFFFFFE), exit number 43 exits=0
CPUID(0x4FFFFFFE), exit number 44 exits=0
CPUID(0x4FFFFFFE), exit number 45 exits=0
CPUID(0x4FFFFFFE), exit number 46 exits=12
CPUID(0x4FFFFFFE), exit number 47 exits=4
CPUID(0x4FFFFFFE), exit number 48 exits=7041766
CPUID(0x4FFFFFFE), exit number 49 exits=152486
CPUID(0x4FFFFFFE), exit number 50 exits=0
CPUID(0x4FFFFFFE), exit number 51 exits=0
CPUID(0x4FFFFFFE), exit number 52 exits=0
CPUID(0x4FFFFFFE), exit number 53 exits=0
CPUID(0x4FFFFFFE), exit number 54 exits=6
CPUID(0x4FFFFFFE), exit number 55 exits=6
CPUID(0x4FFFFFFE), exit number 56 exits=0
CPUID(0x4FFFFFFE), exit number 57 exits=0
CPUID(0x4FFFFFFE), exit number 58 exits=0
CPUID(0x4FFFFFFE), exit number 59 exits=0
CPUID(0x4FFFFFFE), exit number 60 exits=0
CPUID(0x4FFFFFFE), exit number 61 exits=0
CPUID(0x4FFFFFFE), exit number 62 exits=0
CPUID(0x4FFFFFFE), exit number 63 exits=0
CPUID(0x4FFFFFFE), exit number 64 exits=0
CPUID(0x4FFFFFFE), exit number 65 exits=0
CPUID(0x4FFFFFFE), exit number 66 exits=0
CPUID(0x4FFFFFFE), exit number 67 exits=0
CPUID(0x4FFFFFFE), exit number 68 exits=0
bhavyalalithya@bhavyalalithya-Standard-PC-Q35-ICH9-2009:~/tests$
```

Observations

Q) Comment on the frequency of exits – does the number of exits increase at a stable rate? Or are there more exits performed during certain VM operations? Approximately how many exits does a full VM boot entail?

Ans:- The frequency of exits is not increasing at a stable rate (as observed in the frequency of exits for exit 48 screenshot). From the above screenshots(before and after boot), we can observe that VM boot for exit 28 entails up to ~17k exits after full boot.

Q) Of the exit types defined in the SDM, which are the most frequent? Least?

Ans:-

From the above screenshots (that shows exit counts for all exit reasons), we can see that:

Following are the most Frequent Exits:

- Exit number 48 - EPT Violation
- Exit number 32 - WRMSR
- Exit number 1 - External Interrupt

Following are the least Frequent Exits:

- Exit number 54 - WBINVD
- Exit number 55 - XSETBV
- Exit number 29 - MOV DR