CMPE 283 – Assignment 2

Student ID: 015293460 **Name: Parvathi Pai**
Student ID:015304393 **Name: Shreya Ghotankar**

The Assignment

Your assignment is to modify the CPUID emulation code in KVM to report back additional information
when a special CPUID "leaf function" is called.

- For CPUID leaf function %eax=0x4FFFFFFF:
  - Return the total number of exits (all types) in %eax
  - Return the high 32 bits of the total time spent processing all exits in %ebx
  - Return the low 32 bits of the total time spent processing all exits in %ecx
    - %ebx and %ecx return values are measured in processor cycles

Questions

1. For each member in your team, provide 1 paragraph detailing what parts of the lab that member implemented / researched. (You may skip this question if you are doing the lab by yourself).

Shreya Ghotankar:
* Revisited the video lecture 5
* Compiled the code with modifications
* Made changes to fix the errors occurred while compiling
* Created nested VM to run the test program
* Created documentation.

Parvathi Pai:
* Revisited the video lecture 5
* Modified the cupid.c and vmx.c modules
* Looked up how to perform testing for kernel code
* Wrote a test program
* Updated documentation

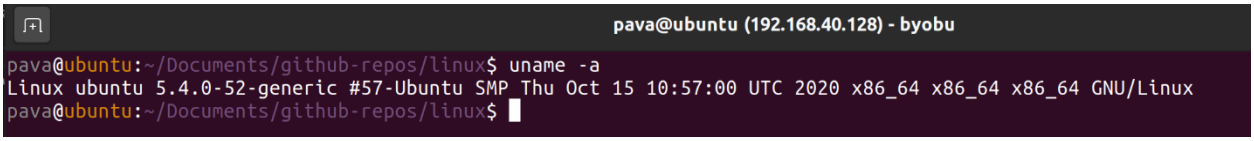
2. Describe in detail the steps you used to complete the assignment.
Steps:

Initial Setup of the VM

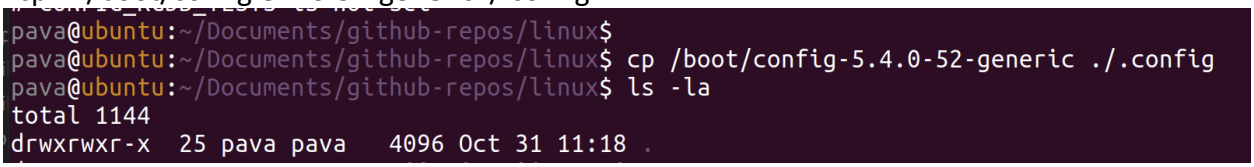
1. Clone the Kernel code from GitHub: git clone https://github.com/torvalds/linux.git
2. Kernel Code Compilation:
* Perform all the actions in the root mode using the command - sudo bash

* Install the build-essential kernel-package, bison package (parser generator) and flex libelf-dev (parser package).
apt-get install build-essential kernel-package fakeroot libncurses5-dev libssl-dev ccache bison flex libelf-dev

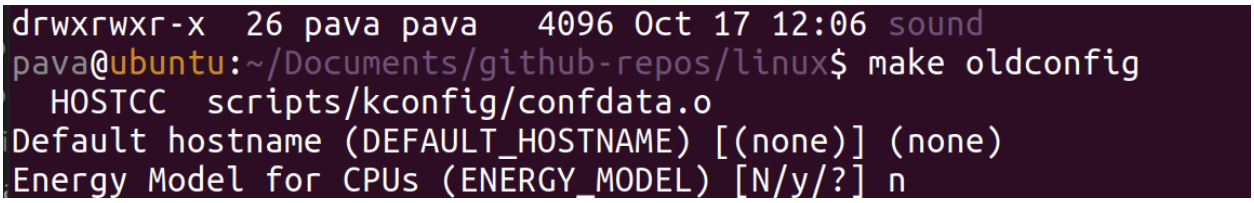
* uname -a



* Change the .Config file
cp -v /boot/config-5.4.0-52-generic ./.config



* Make the file - make oldconfig



* make -j

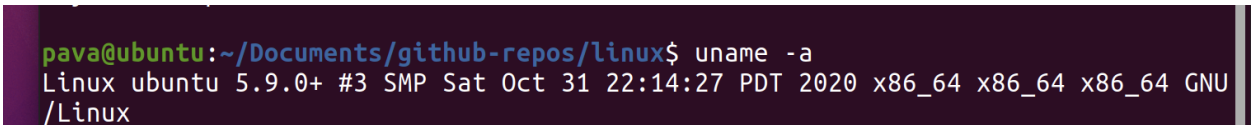
* sudo make modules

* sudo make install

* sudo make modules_install

* reboot

* Verify the updated Linux version - uname -a



Modified the Code

1. Made changes to cupid.c and vmx.c modules.
2. Setup an atomic counter to calculate the number of exits and used rdtsc(); instruction to calculate the total time spent processing exits.
3. Complie the code using – sudo make -j && make modules && make install && make modules_install.

Setup KVM

1. We followed the instructions in this manual to set up the KVM in our Ubuntu –

https://help.ubuntu.com/community/KVM/Installation

2. In the Installation section of the KVM guide we made use of Cosmic (18.10) or later packages.

sudo apt-get install qemu-kvm libvirt-daemon-system libvirt-clients bridge-utils

3. Installed the virt-manager using- sudo apt-get install virt-manager

Starting the nested virtual machine using KVM

1) Downloaded ubuntu iso

2) Created new VM from Virtual Machine Manager application

3) Created a test program and compiled it.

Result:

From test program and verification -

```
shreyaghotankar:~/Documents/Personal/Code$gcc test.c
shreyaghotankar:~/Documents/Personal/Code$./a.out
CPUID(0x4FFFFFFF), exits=148163329, cycles spent in exit=7591676608
shreyaghotankar:~/Documents/Personal/Code$
```

```
pava@pava-Standard-PC-Q35-ICH9-2009:~/Downloads$ ./a.out
CPUID(0x4FFFFFFF), exits=27366381, cycles spent in exit=1645120720
pava@pava-Standard-PC-Q35-ICH9-2009:~/Downloads$ ./a.out
CPUID(0x4FFFFFFF), exits=27385123, cycles spent in exit=1647733628
```

From host VM kern.log – tail -n20 /var/log/kern.log

```
Nov  1 15:53:12 ubuntu kernel: [ 3441.842012] Exit duration=7591676608
Nov  1 15:53:12 ubuntu kernel: [ 3441.842013] Updated ebx exit duration=1
Nov  1 15:58:28 ubuntu kernel: [ 3441.842013] updated low 32 bits in ecx=3296709312
Nov  1 15:58:28 ubuntu kernel: [ 3757.980787] Update the registers
Nov  1 15:58:28 ubuntu kernel: [ 3757.980789] Update exit counters EAX=148247431
Nov  1 15:58:28 ubuntu kernel: [ 3757.980790] Total number of exits in eax=148247431
Nov  1 15:58:28 ubuntu kernel: [ 3757.980790] Exit duration=7602203432
Nov  1 15:58:28 ubuntu kernel: [ 3757.980791] Updated ebx exit duration=1
Nov  1 15:59:01 ubuntu kernel: [ 3757.980791] updated low 32 bits in ecx=3307236136
Nov  1 15:59:01 ubuntu kernel: [ 3791.493776] Update the registers
Nov  1 15:59:01 ubuntu kernel: [ 3791.493779] Update exit counters EAX=148253688
Nov  1 15:59:01 ubuntu kernel: [ 3791.493779] Total number of exits in eax=148253688
Nov  1 15:59:01 ubuntu kernel: [ 3791.493780] Exit duration=7603044366
Nov  1 15:59:01 ubuntu kernel: [ 3791.493780] Updated ebx exit duration=1
Nov  1 16:01:43 ubuntu kernel: [ 3791.493781] updated low 32 bits in ecx=3308077070
Nov  1 16:01:43 ubuntu kernel: [ 3952.955288] Update the registers
Nov  1 16:01:43 ubuntu kernel: [ 3952.955290] Update exit counters EAX=148276807
Nov  1 16:01:43 ubuntu kernel: [ 3952.955291] Total number of exits in eax=148276807
Nov  1 16:01:43 ubuntu kernel: [ 3952.955291] Exit duration=7606604213
Nov  1 16:01:43 ubuntu kernel: [ 3952.955292] Updated ebx exit duration=1
```

Comment on the frequency of exits –

1. Does the number of exits increase at a stable rate? Or are there more exits performed during certain VM operations?

No, the number of exits increase is not at stable rate. There are other VM instructions/operations because of which the exits are performed like EPT violation, RDRAND, I/O instruction, RDTSCP etc.

2. Approximately how many exits does a full VM boot entail?

The number of exits after the first build, reboot and enter nested VM using the KVM is 187,420. This is not very accurate as there might have been a shutdown period and hardware interrupts in-between.

References

1. https://help.ubuntu.com/community/KVM/Installation
2. https://elixir.bootlin.com/linux/v5.10-rc2/source/include/asm-generic/atomic-instrumented.h
3. https://www.kernel.org/doc/html/v4.12/core-api/atomic_ops.html
4. https://lwn.net/Kernel/