CPUID EMULATION IN KVM
ASSIGNMENT 3
VIRTUAL TECHNOLOGIES

Team Members:
Puja Kumari
Tonja Jean

DECEMBER 2023

Table of Contents

1 PROJECT SCOPE

This assignment is designed to demonstrate modifying CPU Identification (CPUID) processor instruction behavior inside the KVM hypervisor. This instruction used by system utilities and operating systems for capturing detailed information about the CPU.

1.1 GITHUB REPO

https://github.com/tlavette/cmpe283assignment-3.git

2 PREREQUISITE:

Prerequisites: Prerequisites: Working completion of Assignment #1. It is helpful to have completed Assignment #2 as the we were able to omit certain steps that were completed such as building the L2 VM as described in ***Section 4.4***

3 TERMS AND DEFINITIONS

CPUID leaf node	The most significant or highest EAX command parameter of the EAX set
KVM	Kernel Based Virtual Machine
Kernel	An architecture standpoint it stands in between the Applications and CPU, Memory and Devices and is the main interface between the physical hardware and the processes running on it.
Kernel module	Code that can be loaded and unloaded to the Kernel
lsmod	Displays loaded modules
rmmod	Command used to remove running modules
modprobe	Program used to add and remove modules from the Linux Kernel
RDTSC	Read time Stamp Counter measures the number of CPU cycles since its reset.
CPU	Central Processing Unit
module	Are extensions used to create and manage various components of virtual machines such as networking, storage, and networking.
SSH	Secure Shell
GCP	Google Cloud Platform

4 IMPLEMENTATION

4.1 DYNAMIC TEAMWORK – TEAM CONTRIBUTION

The following was the overall effort dynamic placed in the completion of this assignment. We met and collaborated on the strategy and each one of us had point lead for the bulleted items, however, we spent much time collaborating via Zoom in peer configuration and code triage. We also spent time engaging in knowledge transfer as each item had slightly different requirements and needs for ultimate completion.

Tonja Jean

- Confirmed the VM module and kernel were successfully running.
- Perform collaborative review of the requirements to determine the resources needed to complete Assignment-3
- Perform code update of CPUID leaf node %eax=0x4FFFFFFC
- Modified the cupid.c and vmx.c programs for calculating the total cpu cycles for a specific exits when eax=0x4FFFFFFC
- Re-built kernel module after the code changes.
- Test and debug Collaboration
- Performed final code refactoring and compilation.
- Collected and compiled documentation.

Puja Kumari

- Confirmed the VM module and kernel were successfully running.
- Perform collaborative review of the requirements to determine the resources needed to complete for Assignment-3.
- Verified the nested VM running properly.
- Perform code update CPUID leaf node %eax=0x4FFFFFFD
- Modified the cupid.c and vmx.c programs for calculating the total exit count for a specific exit when eax=0x4FFFFFFD
- Created and compiled test program to ensure the code worked as expected.
- Performed test and debug collaboration.
- Performed final code refactoring and compilation.
- Collected and compiled documentation.

4.2 Environment Set up

The steps used in completing this lab is as follows. The user will need to consider the libraries and components needed may vary by CPU type, Server OS, memory etc. Please note it is required to use an Intel CPU Platform that supports nested environments. For this lab we used the following:

4.2.1 Server Type

Google Cloud Platform VM Server Machine Type: n1-standard-8 CPU Platform: Intel Haswell Architecture: x86/64 Boot Disk: debian-11-bullseye-v20231115 200G

4.2.2 Environment Setup – As completed in assignment 1 and included here for context.

Cloned the GitHub repository-

```
$git clone https://github.com/torvalds/linux.git

Enter root mode – $sudo bash
```

4.2.3 Install the build essentials.

```
$ apt-get install build-essential kernel-package fakeroot

  libncurses5-devlibssl-dev ccache bison flex libelf-dev
```

4.2.4 Confirm KVM is not already loaded, remove actively loaded, and perform add the kernel modules.

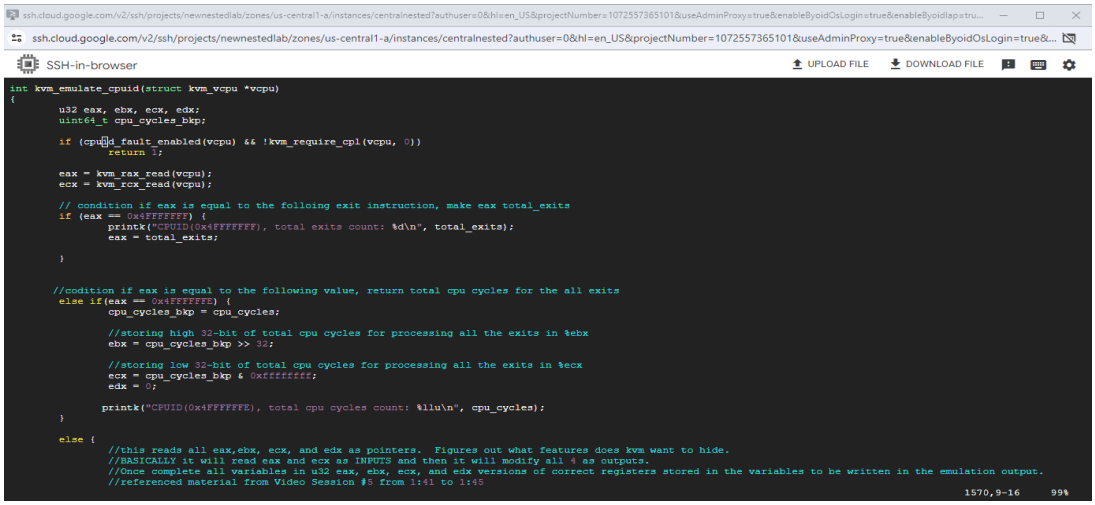
```
lsmod | grep kvm
lsmod | grep kvm_intel
Remove KVM modules actively loaded.
rmmod kvm_intel and rmmod kvm
modprobe kvm
mod probe kvm_intel
```

4.3 Update Kernel Code Files

4.3.1 Update kvm hypervisor files: cupid.c and vmx.c files

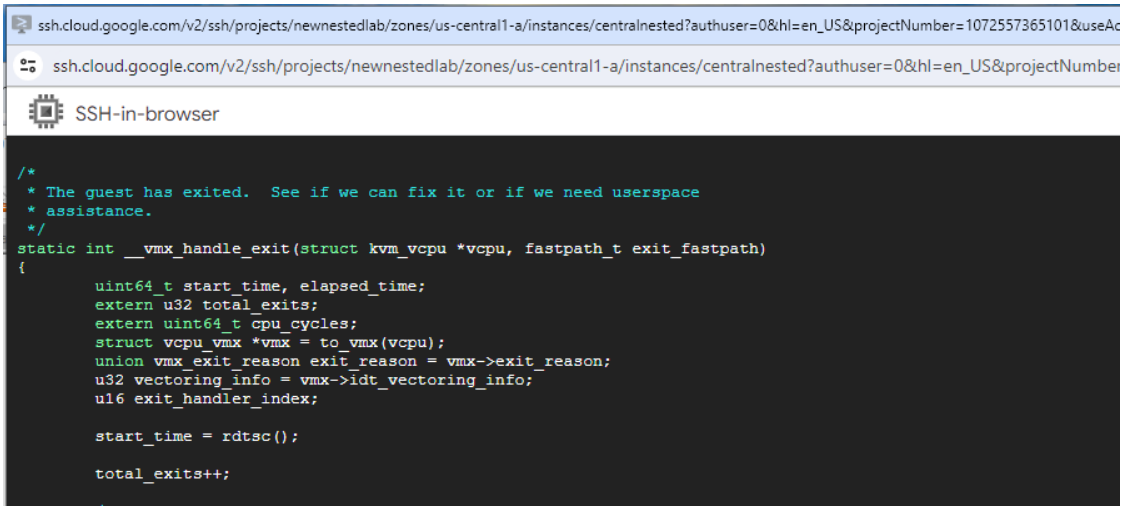
cpuid.c

Modified **kvm_emulate_cpuid** code for CPUID exit handling.



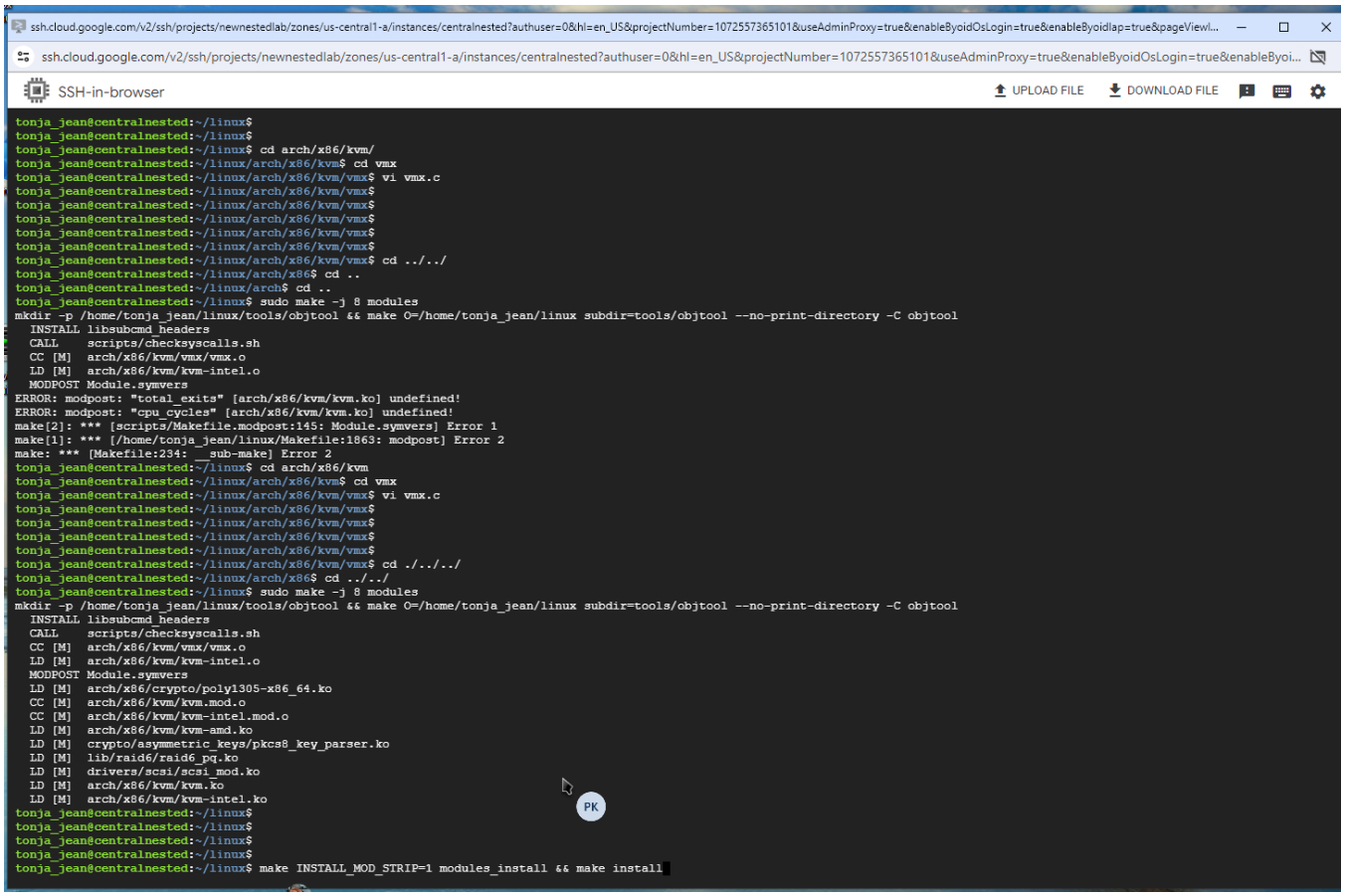
vmx.c

Modified vmx.c code **vmx_handle_exit** to increment the total number of exits**.**



sudo make modules -j 8 modules

Initial run errors found. These were corrected in the vmx.c file and the job reran.



make INSTALL_MOD_STRIP=1 && make install

Collaboration Session:

4.4 Create L2 VM and Test CPUID Assignment

4.4.1 Create Nested L2 VM

sudo apt-get install virt-manager
sudo apt-get install libvirt-bin libvert-doc
sudo apt-get install gemu-system
sudo virt-manager

Installing Virt-Manager

```
tonja_jean@centralnested:~/linux$
tonja_jean@centralnested:~/linux$ sudo apt-get install qemu-kvm libvirt-daemon-system libvirt-clients bridge-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'qemu-system-x86' instead of 'qemu-kvm'
libvirt-clients is already the newest version (7.0.0-3+deb11u2).
libvirt-clients set to manually installed.
libvirt-daemon-system is already the newest version (7.0.0-3+deb11u2).
libvirt-daemon-system set to manually installed.
qemu-system-x86 is already the newest version (1:5.2+dfsg-11+deb11u3).
The following NEW packages will be installed:
  bridge-utils
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 37.9 kB of archives.
After this operation, 124 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 https://deb.debian.org/debian bullseye/main amd64 bridge-utils amd64 1.7-1 [37.9 kB]
Fetched 37.9 kB in 0s (138 kB/s)
Selecting previously unselected package bridge-utils.
(Reading database ... 104349 files and directories currently installed.)
Preparing to unpack .../bridge-utils_1.7-1_amd64.deb ...
Unpacking bridge-utils (1.7-1) ...
Setting up bridge-utils (1.7-1) ...
Processing triggers for man-db (2.9.4-2) ...
tonja_jean@centralnested:~/linux$
tonja_jean@centralnested:~/linux$
tonja_jean@centralnested:~/linux$ sudo kvm-ok
INFO: /dev/kvm exists
KVM acceleration can be used
```

```
tonja_jean@centralnested:~/linux$ uname -a
Linux centralnested 6.7.0-rc3+ #6 SMP PREEMPT_DYNAMIC Sun Dec 17 02:46:03 UTC 2023 x86_64 GNU/Linux
tonja_jean@centralnested:~/linux$  sudo adduser 'puja' libvirt
adduser: The user `puja' does not exist.
tonja_jean@centralnested:~/linux$ sudo getent group | grep libvirt
libvirt:x:116:
libvirt-qemu:x:64055:libvirt-qemu
tonja_jean@centralnested:~/linux$ sudo adduser 'libvirt-qemu:x:64055:libvirt-qemu' libvirt
adduser: The user `libvirt-qemu:x:64055:libvirt-qemu' does not exist.
tonja_jean@centralnested:~/linux$ sudo getent group | grep kvm
kvm:x:110:
tonja_jean@centralnested:~/linux$ sudo adduser libvirt-qemu:x:64055:libvirt-qemu libvirt
adduser: The user `libvirt-qemu:x:64055:libvirt-qemu' does not exist.
tonja_jean@centralnested:~/linux$ users
tonja_jean tonja_jean
tonja_jean@centralnested:~/linux$ sudo adduser 'tonja_jean' libvirt
Adding user `tonja_jean' to group `libvirt' ...
Adding user tonja_jean to group libvirt
Done.
tonja_jean@centralnested:~/linux$ sudo getent group | grep libvirt
libvirt:x:116:tonja_jean
libvirt-qemu:x:64055:libvirt-qemu
tonja_jean@centralnested:~/linux$
tonja_jean@centralnested:~/linux$
tonja_jean@centralnested:~/linux$
tonja_jean@centralnested:~/linux$
tonja_jean@centralnested:~/linux$ sudo adduser 'tonja_jean' kvm
Adding user `tonja_jean' to group `kvm' ...
Adding user tonja_jean to group kvm
Done.
tonja_jean@centralnested:~/linux$ sudo getent group | grep kvm
kvm:x:110:tonja_jean
```

Virt-manager running successfully on the VM

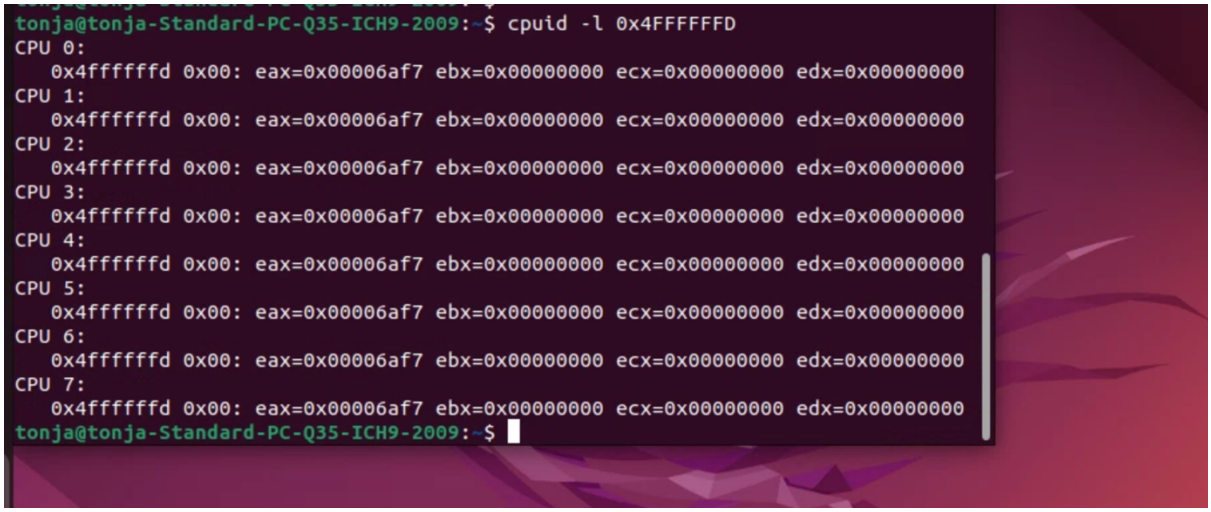
```
tonja_jean@centralnested:~/linux$ sudo virsh list --all
 Id   Name   State
--------------------

tonja_jean@centralnested:~/linux$ sudo systemctl status libvirtd
● libvirtd.service - Virtualization daemon
     Loaded: loaded (/lib/systemd/system/libvirtd.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2023-12-17 19:31:23 UTC; 6min ago
TriggeredBy: ● libvirtd.socket
             ● libvirtd-admin.socket
             ● libvirtd-ro.socket
       Docs: man:libvirtd(8)
             https://libvirt.org
   Main PID: 1081 (libvirtd)
      Tasks: 19 (limit: 32768)
     Memory: 31.9M
        CPU: 223ms
     CGroup: /system.slice/libvirtd.service
             └─1081 /usr/sbin/libvirtd

Dec 17 19:31:21 centralnested systemd[1]: Starting Virtualization daemon...
Dec 17 19:31:23 centralnested systemd[1]: Started Virtualization daemon.
tonja_jean@centralnested:~/linux$
```

4.4.2 Installed GEMO compatible Ubuntu OS on the inner VM using Chrome Remote Desktop

4.5 PERFORM CPUID CONFIRMATION TEST - RESULTS

Run cupid command from inside the inner VM to test the functionality and checked the dmesg log in the outer VM to verify the exit responses.

Test 3: Tested functionality for %eax=04xFFFFFFD –



Verified in dmesg log

```
[  320.816362] CPU(0x4FFFFFFD), Exit no - 0, exit count: 27383
[  320.822657] CPU(0x4FFFFFFD), Exit no - 0, exit count: 27383
[  320.831250] CPU(0x4FFFFFFD), Exit no - 0, exit count: 27383
[  320.838746] CPU(0x4FFFFFFD), Exit no - 0, exit count: 27383
[  320.845869] CPU(0x4FFFFFFD), Exit no - 0, exit count: 27383
[  320.852833] CPU(0x4FFFFFFD), Exit no - 0, exit count: 27383
[  320.859838] CPU(0x4FFFFFFD), Exit no - 0, exit count: 27383
[  320.867082] CPU(0x4FFFFFFD), Exit no - 0, exit count: 27383
tonja jean@centralnested:~/linux$
```

Test 4: Tested functionality for %eax=04xFFFFFFC –

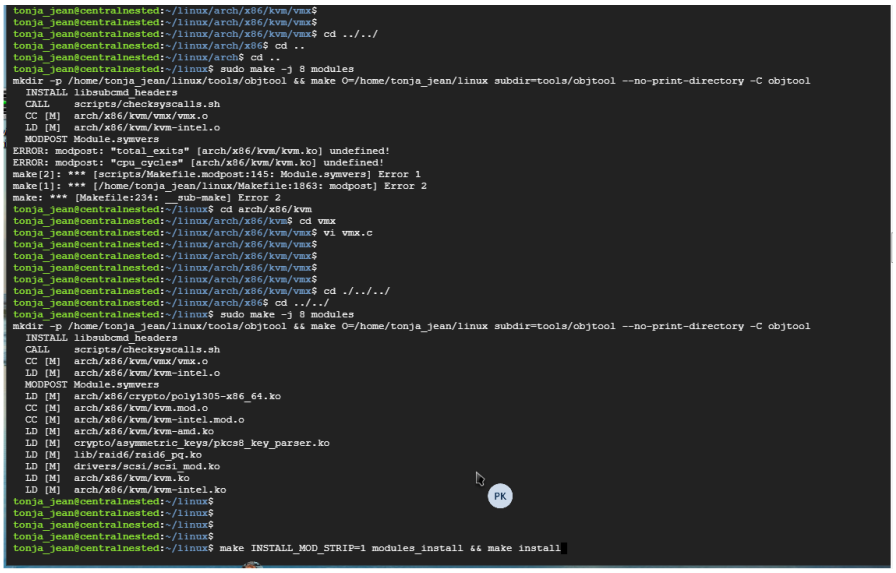
```
tonja@tonja-Standard-PC-Q35-ICH9-2009:~$ cpuid -l 0x4FFFFFFC
CPU 0:
   0x4fffffc 0x00: eax=0x4fffffc ebx=0x00000000 ecx=0x00239d68 edx=0x00000000
CPU 1:
   0x4fffffc 0x00: eax=0x4fffffc ebx=0x00000000 ecx=0x00239d68 edx=0x00000000
CPU 2:
   0x4fffffc 0x00: eax=0x4fffffc ebx=0x00000000 ecx=0x00239d68 edx=0x00000000
CPU 3:
   0x4fffffc 0x00: eax=0x4fffffc ebx=0x00000000 ecx=0x00239d68 edx=0x00000000
CPU 4:
   0x4fffffc 0x00: eax=0x4fffffc ebx=0x00000000 ecx=0x00239d68 edx=0x00000000
CPU 5:
   0x4fffffc 0x00: eax=0x4fffffc ebx=0x00000000 ecx=0x00239d68 edx=0x00000000
CPU 6:
   0x4fffffc 0x00: eax=0x4fffffc ebx=0x00000000 ecx=0x00239d68 edx=0x00000000
CPU 7:
   0x4fffffc 0x00: eax=0x4fffffc ebx=0x00000000 ecx=0x00239d68 edx=0x00000000
tonja@tonja-Standard-PC-Q35-ICH9-2009:~$
```

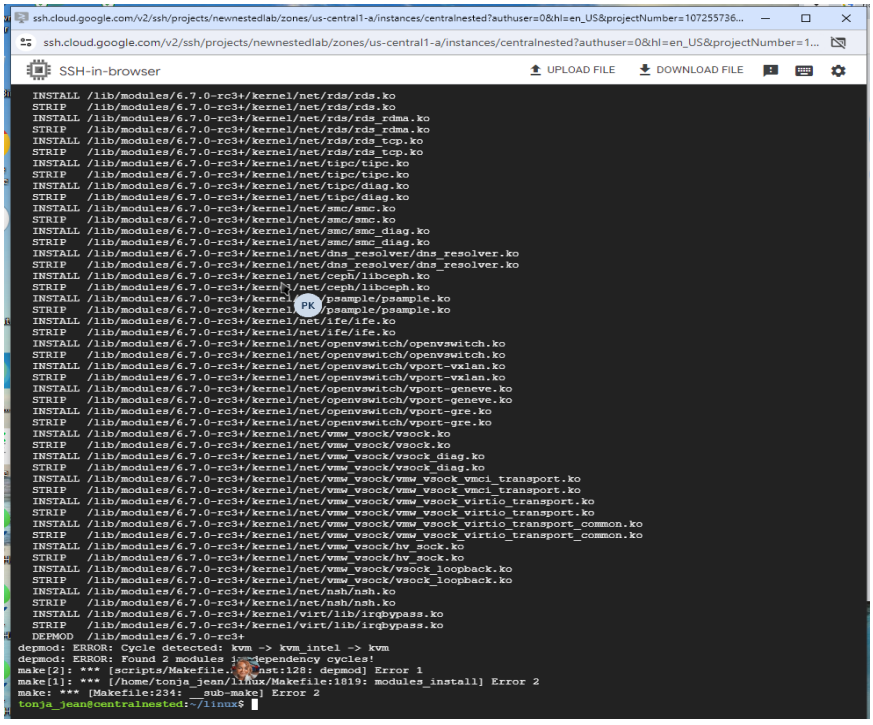
Verified in dmesg log –

```
[  403.631831] Exit no - 0,high 32-bit cpu cycles count: 0
[  403.631837] Exit no - 0,low 32-bit cpu cycles count: 2334056
[  403.638072] Exit no - 0,high 32-bit cpu cycles count: 0
[  403.644705] Exit no - 0,low 32-bit cpu cycles count: 2334056
[  403.654397] Exit no - 0,high 32-bit cpu cycles count: 0
[  403.660379] Exit no - 0,low 32-bit cpu cycles count: 2334056
[  403.682020] Exit no - 0,high 32-bit cpu cycles count: 0
[  403.688420] Exit no - 0,low 32-bit cpu cycles count: 2334056
[  403.695948] Exit no - 0,high 32-bit cpu cycles count: 0
[  403.702499] Exit no - 0,low 32-bit cpu cycles count: 2334056
[  403.711262] Exit no - 0,high 32-bit cpu cycles count: 0
[  403.717780] Exit no - 0,low 32-bit cpu cycles count: 2334056
[  403.725382] Exit no - 0,high 32-bit cpu cycles count: 0
[  403.732172] Exit no - 0,low 32-bit cpu cycles count: 2334056
[  403.739491] Exit no - 0,high 32-bit cpu cycles count: 0
```

4.6 DEBUGGING

Errors with kvm_emulate_cpuid





Building modules

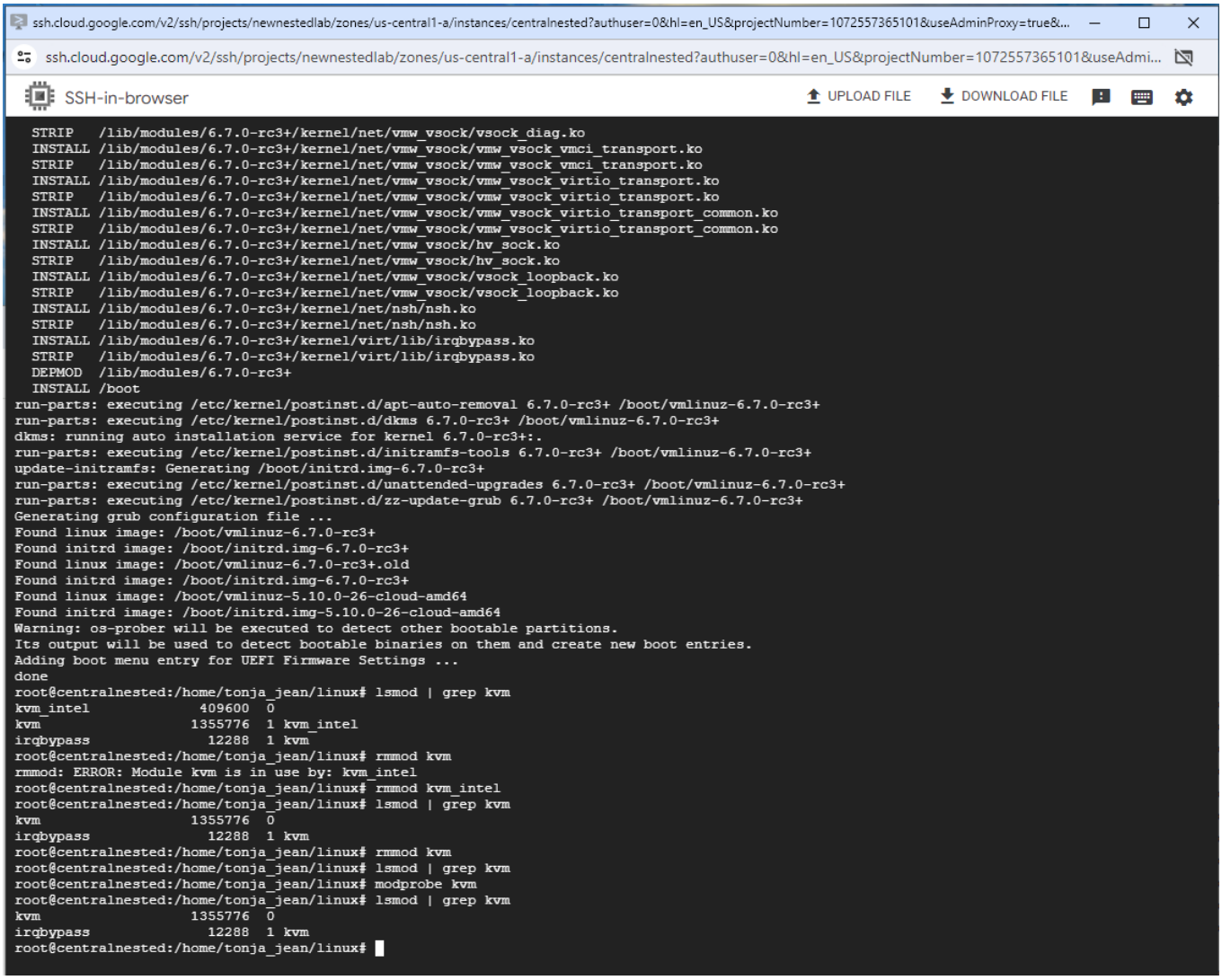
First run errors:

```
arch/x86/kvm/cpuid.c: In function ‘kvm_emulate_cpuid’:
arch/x86/kvm/cpuid.c:1576:3: error: the address of ‘edx’ will always evaluate as ‘true’ [-Werror=address]
 1576 |   kvm_cpuid(vcpu, &eax, &eax, &ebx, &ecx, &edx, false);
      |   ^~~~~~~~~
arch/x86/kvm/cpuid.c:1576:3: error: too many arguments to function ‘kvm_cpuid’
arch/x86/kvm/cpuid.c:1509:6: note: declared here
 1509 | bool kvm_cpuid(struct kvm_vcpu *vcpu, u32 *eax, u32 *ebx,
      |      ^~~~~~~~~
cc1: all warnings being treated as errors
make[4]: *** [scripts/Makefile.build:243: arch/x86/kvm/cpuid.o] Error 1
make[3]: *** [scripts/Makefile.build:480: arch/x86/kvm] Error 2
make[2]: *** [scripts/Makefile.build:480: arch/x86] Error 2
make[1]: *** [/home/tonja_jean/linux/Makefile:1911: .] Error 2
make: *** [Makefile:234: __sub-make] Error 2
tonja_jean@centralnested:~/linux$
```

Corrected the errors in the code cuid.c and reran followed with
Check for kvm already loaded, clear, and load.

```
lsmod | grep kvm
lsmod | grep kvm_intel
rmmod kvm
modprobe kvm
lsmod | grep kvm
```

Resolved – cleared loaded kvm and reloaded



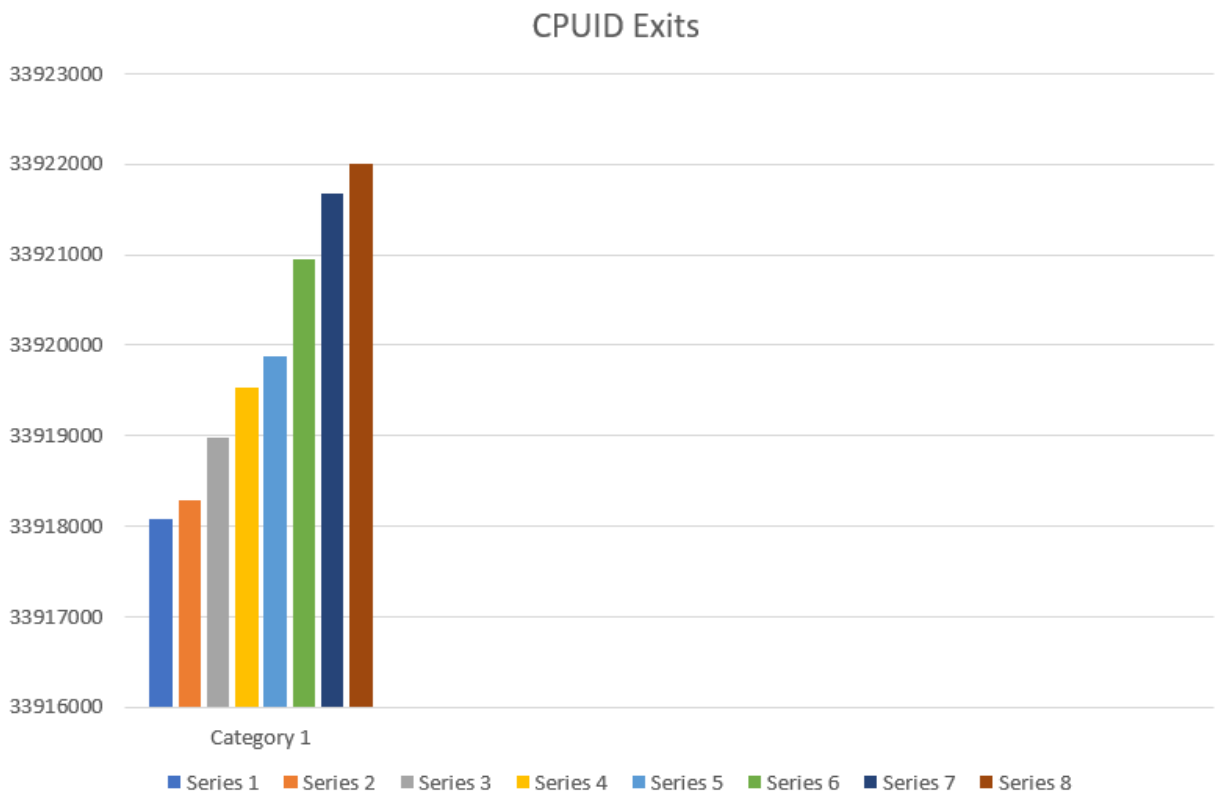
5 SUMMARY AND QUESTIONS

1. Team Members: Described in Section 4.1

   Puja Kumari

   Tonja Jean

2. Detailed Steps: Sections 4.2 – 4.5
3. The frequency of exists appears to gradually increase without major spikes in the trend.



During this boot, a full boot cycle appeared to handle 271,359,410 exits.

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

Most Frequent Exit:

- Exit number 48 - EPT Violation

- Exit number 1- External Interrupt

Least Frequent Exit :

- Exit number 54 - WBINVD
- Exit number 55 - XSETBV