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).

I did this assignment by myself:

Yilin Zhou (012571026)  
2. Describe in detail the steps you used to complete the assignment. Consider your reader to be someone skilled in software development but otherwise unfamiliar with the assignment. Good answers to this question will be recipes that someone can follow to reproduce your development steps.  
Note: I may decide to follow these instructions for random assignments, so you should make sure they are accurate.

Step1: build the linux kernel successfully:

Using git to download linux code;

Install related tools;

Change the config file using command: make oldconfig;

Using this command to build: sudo make -j 2 modules && sudo make -j 2 && sudo make modules\_install && sudo make install;

Reboot and show the version result using command: uname -a;

Result is:

“Linux example-nested-vm 5.12.0-rc6+ #1 SMP Sun Apr 25 19:55:28 UTC 2021 x86\_64 GNU/Linux”;

Step2: coding(adding new features on cpuid):

Modify the cupid.c file under /linux/arch/x86/kvm, add leaf function(When eax is 0x4fffffff)

```

if(eax == 0x4fffffff){

kvm\_cpuid(vcpu, &eax, &ebx, &ecx, &edx, true);

// total number of exits

eax = atomic\_read(&exit\_counters);

// high 32 bits of the total time spent processing all exits

ebx = (atomic64\_read(&exit\_time\_length) >> 32);

// low 32 bits of the total time spent processing all exits

ecx = (atomic64\_read(&exit\_time\_length) & 0xFFFFFFFF);

printk(KERN\_INFO "exit counters =%d", atomic\_read(&exit\_counters));

printk(KERN\_INFO "exit time = %llu", atomic64\_read(&exit\_time\_length));

} else {

kvm\_cpuid(vcpu, &eax, &ebx, &ecx, &edx, false);

}

```

Counting the number and time length in vmx.c under /linux/arch/x86/kvm/vmx

Step3: install nested VM

Install related tools: sudo apt install qemu-kvm libvirt-daemon-system libvirt-clients bridge-utils

sudo virt-install --name=innerMachine --description=innerMachine --ram=1536 --vcpus=2 --disk path=/home/\*\*\*/YZ-WS.qcow2,size=30 --cdrom=/home/ubuntu-20.04.2-live-server-arm64.iso --graphics=vnc

Step4: test file

Using asm volatile function to get eax to edx info;

Set the eax equal 0x4FFFFFFF, and get the related information in cpuid.c.

3. 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?

The number of exits increased every time executing the test file at a stable rate.

Approximately how many exits does a full VM boot entail?

Around 2600000 exits.