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).

Only myself: Yilin Zhou (sjsuid: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.

Step1: use the VM environment of assignment2

Step2: modify cpuid.c under arch/x86/kvm to add new feature: leaf function 0x4ffffffe, which return the exist number. And the exits number was counted in vmx.c under arch/x86/kvm/vmx.

if(eax == 0x4FFFFFFE){

if(ecx == 35 || ecx == 38 || ecx == 42 || ecx == 65){

eax = 0;

ebx = 0;

ecx = 0;

edx = 0xFFFFFFFF;

printk(KERN\_INFO "not defined exit number in SDM: %d", ecx);

}else{

eax = number\_of\_exits[(int)ecx];

printk(KERN\_INFO "number\_of\_exits =%d", number\_of\_exits[(int)ecx]);

}

}

Step3: rebuild the new linux kernel using make command：sudo make -j 2 modules && sudo make -j 2 && sudo make modules\_install && sudo make install;

Step4: reboot the machine;

Step5: using virt-manager to enter the inner vm and run the test file on inner vm;

Step6: the output of test:

CPUID(0x4FFFFFFE), exit number=0 exits=35832

CPUID(0x4FFFFFFE), exit number=1 exits=0

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=0

CPUID(0x4FFFFFFE), exit number=8 exits=0

CPUID(0x4FFFFFFE), exit number=9 exits=0

CPUID(0x4FFFFFFE), exit number=10 exits=1276322

CPUID(0x4FFFFFFE), exit number=11 exits=0

CPUID(0x4FFFFFFE), exit number=12 exits=0

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=818402

CPUID(0x4FFFFFFE), exit number=29 exits=10

CPUID(0x4FFFFFFE), exit number=30 exits=35832

CPUID(0x4FFFFFFE), exit number=31 exits=14521

CPUID(0x4FFFFFFE), exit number=32 exits=0

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=207652

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=24

CPUID(0x4FFFFFFE), exit number=47 exits=8

CPUID(0x4FFFFFFE), exit number=48 exits=2494242

CPUID(0x4FFFFFFE), exit number=49 exits=0

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=14

CPUID(0x4FFFFFFE), exit number=55 exits=12

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

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

Yes, the number of exits will increase at a stable rate, take the number 10 for example, here is the output:

CPUID(0x4FFFFFFE), exit number=10 exits=1412006

CPUID(0x4FFFFFFE), exit number=10 exits=1412024

CPUID(0x4FFFFFFE), exit number=10 exits=1412042

CPUID(0x4FFFFFFE), exit number=10 exits=1412060

Around over 3 millions totally.

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

According to my output, the number 48 and 10 have the most exits (over million times), which are the CPUID and EPT in the SDM. The least are number 29, 47, 54 and 55, all of them are lower than 20. They are MOV DR, Access to LDTR or TR, WBINVD or WBNOINVD and XSETBV in the SDM.