ID:013771511
Name:Meghana Yoganarasimha

Assignment 2: Modifying instruction behavior in KVM

Prerequisites:

1. Linux environment is setup as dual boot OS in my laptop as part of assignment 1.I had installed ubuntu 4.15 version.
2. Created new folder under home called Virt_2 and cloned the linux git repository(https://github.com/torvalds/linux.git) in this folder with below commit id:

   ```
   commit 4710e78940d8d957f24b8f085f961f1279f8fbff
   ```

3. Once the new linux code was cloned, built the kernel by using below commands:
   a. Switched to root mode
      ```
      sudo bash
      ```
   b. Installed the tools required to build kernel:
      ```
      apt-get install build-essential kernel-package
      fakeroot libncurses5-dev libssl-dev ccache bison flex
      libelf-dev
      ```
   c. Executed beelow make commands to build the kernel
      ```
      make menuconfig
      make -j 8
      make modules_install -j 8
      make install -j 8
      ```
   d. Rebooted the machine to install the new kernel built
4. Once the machine is rebooted linux kernel was upgraded from 4.15 to 4.19+ version and verified it by executing the below command:
   ```
   uname -a
   ```

Implementation :

1. In the linux git cloned folder , navigated to linux/arch/x86/kvm/ folder
2. Explored the exit handling flow.
3. Mainly 3 files will be involved with the exit handling flow that deals with cpuid leaf leaf 0x4FFFFFFF and they are x86.c,kvm.c,cpuid.c
4. In x86.c, modified the kvm code around exit handling function to calculate the number of exits and the processor cycles spent on it.
   Modified function : vcpu_enter_guest()

5. Declared the calculated variables as extern variables in cuid.h file so that it can be passed to exit handler function
   extern int exit_count;
   extern u64 exit_execution_cycles;
6. Based on the calculated values passed, modified the cpiud.c file for kvm_emulate_cpuid() function to store the values calculated.
   Modified function : kvm_emulate_cpuid()
   Functionality :
   - Introduced a new if block to get executed on cpuid leaf 0x4FFFFFFF
   - Stored the exit_count calculated to eax register.
   - Splitted the processor execution cycle from 64 bit temp variable to ebx and ecx register.
7. After the above implementation, built the modified kernel again with the above mentioned make commands and rebooted the system.

Testing:

1. Installed the virt-manager on linux environment.
   `sudo apt-get install virt-manager`
2. Once the tool was installed, then created a new VM using the manager.
3. Installed ubuntu 18.04 iso on the new VM launched.
4. Configured the VM.
5. Installed cpuid on vm with below command:
   `sudo apt install cpuid`
6. In the terminal of new VM tested the implemented functionality with below command
   `cpuid -l 0x4FFFFFFF`

Output:

```
mmmmmm@mmmmmm-Standard-PC-i440FX-PIIX-1996:~$ cpuid -l 0x4FFFFFFF
CPU 0:
   0x4fffffff 0x00: eax=0x01f1db77 ebx=0x00000007 ecx=0x9e79ab82 edx=0xffffffff
mmmmmm@mmmmmm-Standard-PC-i440FX-PIIX-1996:~$ cpuid -l 0x4FFFFFFF
CPU 0:
   0x4fffffff 0x00: eax=0x01f1ea32 ebx=0x00000007 ecx=0x9f45fab7 edx=0xffffffff
mmmmmm@mmmmmm-Standard-PC-i440FX-PIIX-1996:~$ cpuid -l 0x4FFFFFFF
CPU 0:
```

0x4fffffff 0x00: eax=0x01f1f34e ebx=0x00000007 ecx=0x9f9b2e93 edx=0xffffffff
mmmmmm@mmmmmm-Standard-PC-i440FX-PIIX-1996:~$