CMPE 283: Virtualization Technologies

Assignment 4: Shadow paging vs Nested paging

Bhavya Tetali (014535144), Supriya Meduri (015262767)

Contribution of Team Members

Bhavya Tetali & Supriya Meduri:

- Collaborated together in zoom call
- Run the code in assignment 3 with shadow paging and added a screenshot.
- Run the code with shadow paging on i.e; ept=0 and added the screenshot.
- Created the documentation.

Environment Setup: We build this homework assignment on assignment-3 and hence used the same environment setup

Steps Followed:

1. Boot the Guest VM
2. Reboot the guest VM and, Record total exit count information
3. Shutdown the test (inner) VM.
4. Remove the 'kvm-intel' module from your running kernel

```
$ rmmod kvm-intel
```

5. Reload the kvm-intel module with the parameter **ept=0** (this will disable nested paging and force KVM to use shadow paging instead)

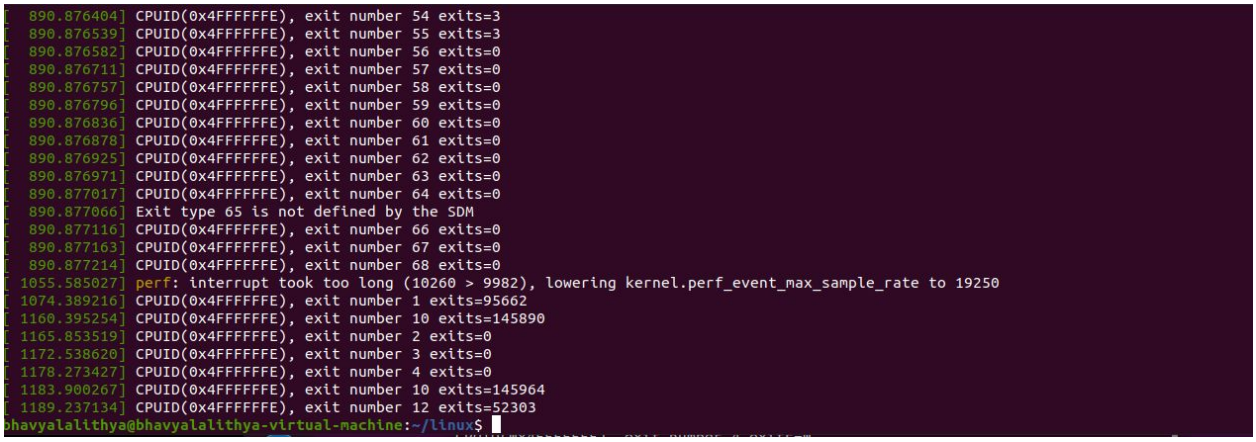
```
$ insmod /lib/modules/5

/kernel/arch/x86/kvm/kvm-intel.ko ept=0
```

6. Boot the VM again, note the exits
7. Reboot the VM and record the exits

Screenshots

Nested paging



Shadow paging

Boot

After reboot

Observations

What did you learn from the count of exits? Was the count what you expected? If not, why not?

The number of exits in shadow paging increases compared to nested paging. It is an expected outcome since, in nested paging, it will only VM exit when an EPT violation occurs. Whereas in shadow paging, it could exit every time VM tries to execute CR0, CR3, CR4 execution, or any paging related exits like a page fault.

What changed between the two runs (ept vs no-ept)?

EPT Mode:

Two-layer page tables are used to translate from Guest VA to Guest PA to Host PA, and more page access is required, the guest VM should own page table and hence all the operations on CR3 is done natively, i.e. no need to exit

No EPT Mode:

Guest VM does not own the page table in shadow paging mode, for it, the VMM must simulate CR3.