

CMPE 283: Virtual Technologies

Assignment 4: Shadow Paging vs Nested Paging

Dharahasini Gangalapudi (015961361)

Environment Setup

- The same environment setup as assignments 2 & 3

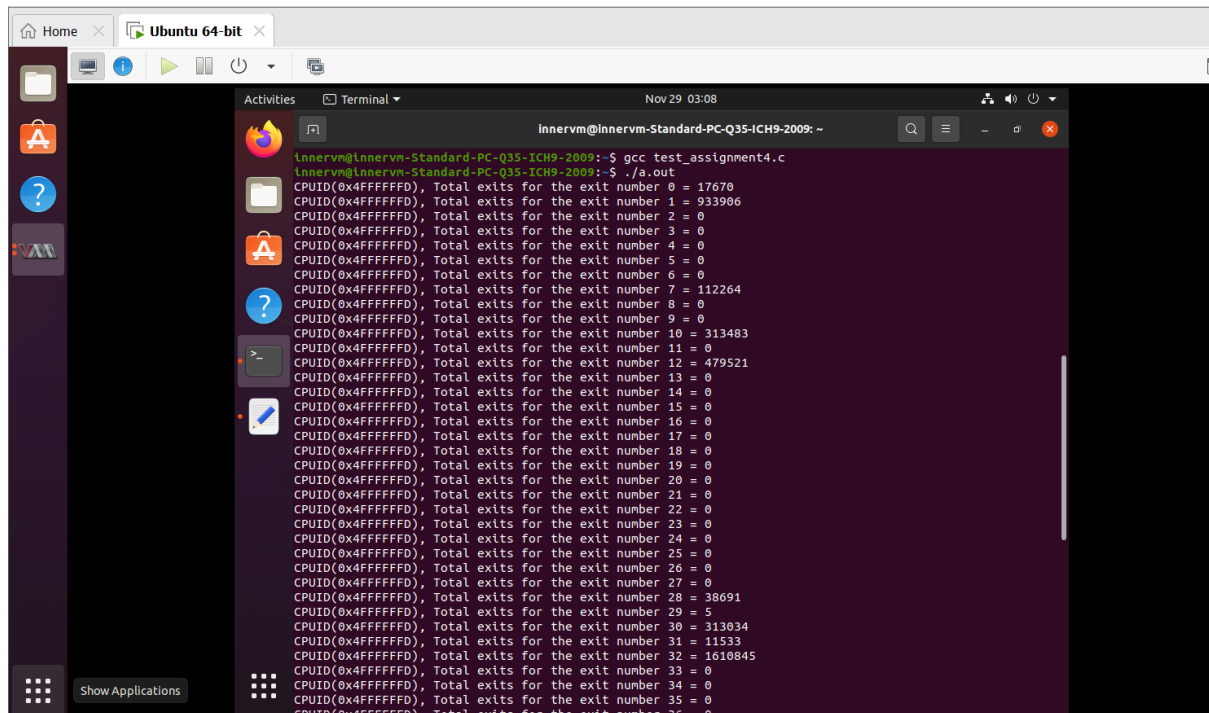
Steps followed

- Boot the inner VM and note the exit count.
- Now, reboot the inner VM and note the exit count.
- Shutdown the inner VM and remove the 'kvm-intel-module' from the existing kernel using the command below
 - `rmmod kvm-intel`
- Now, put `ept=0` and reload the `kvm-intel-module` to enable shadow paging and disable the nested paging using the below command
 - `Insmod lib/modules/{present linux kernel version}/kernel/arch/x86/kvm/kvm-intel.ko ept=0`
- Now, boot and reboot the inner VM and note the total number of exits respectively.

Output screenshots:

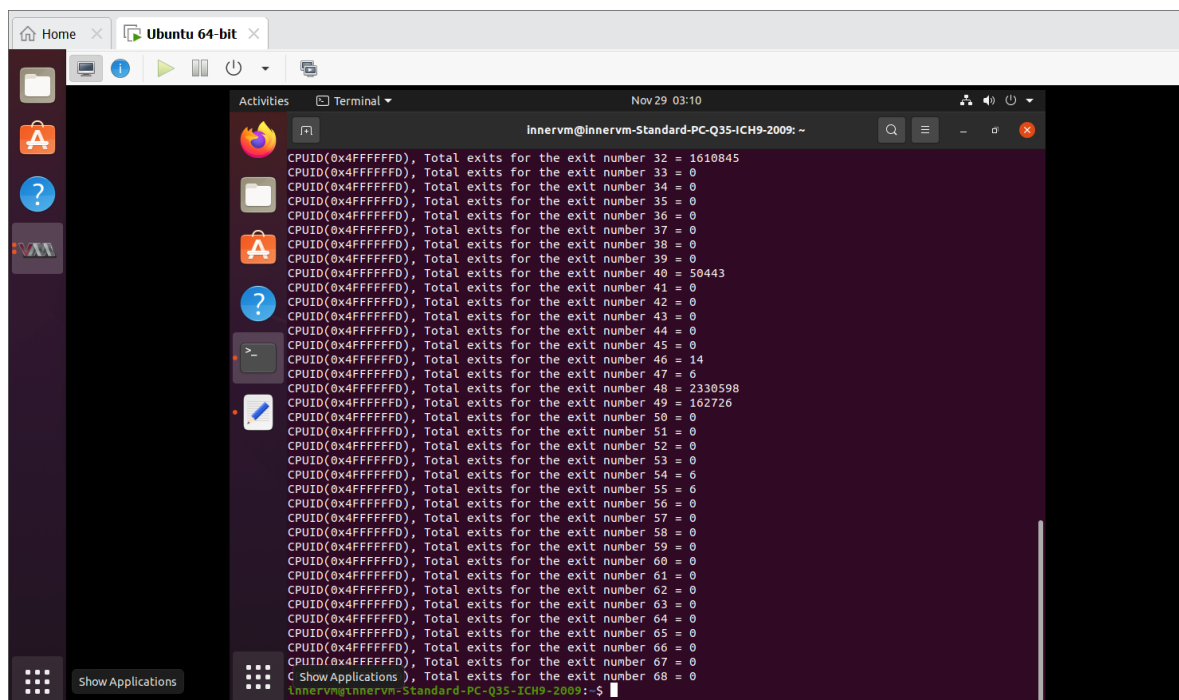
Nested Paging

Before reboot



A terminal window titled "Ubuntu 64-bit" showing the output of a program. The prompt is "innervm@innervm-Standard-PC-Q35-ICH9-2009: ~". The command executed is "gcc test_assignment4.c" followed by "./a.out". The output consists of 36 lines, each reporting the total exits for a specific exit number (0 to 35). The values for exit numbers 0 through 31 are 0, while exit number 32 is 1610845. Exit numbers 33 through 35 are 0.

```
innervm@innervm-Standard-PC-Q35-ICH9-2009: ~  
innervm@innervm-Standard-PC-Q35-ICH9-2009: $ gcc test_assignment4.c  
innervm@innervm-Standard-PC-Q35-ICH9-2009: $ ./a.out  
CPUID(0x4FFFFFFD), Total exits for the exit number 0 = 17670  
CPUID(0x4FFFFFFD), Total exits for the exit number 1 = 933906  
CPUID(0x4FFFFFFD), Total exits for the exit number 2 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 3 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 4 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 5 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 6 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 7 = 112264  
CPUID(0x4FFFFFFD), Total exits for the exit number 8 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 9 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 10 = 313483  
CPUID(0x4FFFFFFD), Total exits for the exit number 11 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 12 = 479521  
CPUID(0x4FFFFFFD), Total exits for the exit number 13 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 14 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 15 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 16 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 17 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 18 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 19 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 20 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 21 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 22 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 23 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 24 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 25 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 26 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 27 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 28 = 38691  
CPUID(0x4FFFFFFD), Total exits for the exit number 29 = 5  
CPUID(0x4FFFFFFD), Total exits for the exit number 30 = 313034  
CPUID(0x4FFFFFFD), Total exits for the exit number 31 = 11533  
CPUID(0x4FFFFFFD), Total exits for the exit number 32 = 1610845  
CPUID(0x4FFFFFFD), Total exits for the exit number 33 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 34 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 35 = 0
```



A terminal window titled "Ubuntu 64-bit" showing the output of a program. The prompt is "innervm@innervm-Standard-PC-Q35-ICH9-2009: ~". The command executed is "C Show Applications" followed by ". Total exits for the exit number 68 = 0". The output consists of 36 lines, each reporting the total exits for a specific exit number (0 to 35). The values for exit numbers 0 through 31 are 0, while exit number 32 is 1610845. Exit numbers 33 through 35 are 0.

```
innervm@innervm-Standard-PC-Q35-ICH9-2009: ~  
C Show Applications ). Total exits for the exit number 68 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 32 = 1610845  
CPUID(0x4FFFFFFD), Total exits for the exit number 33 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 34 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 35 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 36 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 37 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 38 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 39 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 40 = 50443  
CPUID(0x4FFFFFFD), Total exits for the exit number 41 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 42 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 43 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 44 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 45 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 46 = 14  
CPUID(0x4FFFFFFD), Total exits for the exit number 47 = 6  
CPUID(0x4FFFFFFD), Total exits for the exit number 48 = 2330598  
CPUID(0x4FFFFFFD), Total exits for the exit number 49 = 162726  
CPUID(0x4FFFFFFD), Total exits for the exit number 50 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 51 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 52 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 53 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 54 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 55 = 6  
CPUID(0x4FFFFFFD), Total exits for the exit number 56 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 57 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 58 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 59 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 60 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 61 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 62 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 63 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 64 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 65 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 66 = 0  
CPUID(0x4FFFFFFD), Total exits for the exit number 67 = 0  
C Show Applications ). Total exits for the exit number 68 = 0  
innervm@innervm-Standard-PC-Q35-ICH9-2009: ~
```

After reboot

The screenshot shows a Linux desktop environment with a terminal window open. The terminal displays the output of a command, showing a list of CPUIDs and their corresponding exit numbers. The output is as follows:

```

innervm@innervm-Standard-PC-Q35-ICH9-2009:~$ ./a.out
CPUID(0x4FFFFFFD), Total exits for the exit number 0 = 35344
CPUID(0x4FFFFFFD), Total exits for the exit number 1 = 1101974
CPUID(0x4FFFFFFD), Total exits for the exit number 2 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 3 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 4 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 5 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 6 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 7 = 135230
CPUID(0x4FFFFFFD), Total exits for the exit number 8 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 9 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 10 = 590886
CPUID(0x4FFFFFFD), Total exits for the exit number 11 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 12 = 536171
CPUID(0x4FFFFFFD), Total exits for the exit number 13 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 14 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 15 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 16 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 17 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 18 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 19 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 20 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 21 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 22 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 23 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 24 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 25 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 26 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 27 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 28 = 77613
CPUID(0x4FFFFFFD), Total exits for the exit number 29 = 9
CPUID(0x4FFFFFFD), Total exits for the exit number 30 = 602481
CPUID(0x4FFFFFFD), Total exits for the exit number 31 = 13447
CPUID(0x4FFFFFFD), Total exits for the exit number 32 = 1821462
CPUID(0x4FFFFFFD), Total exits for the exit number 33 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 34 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 35 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 36 = 0

```

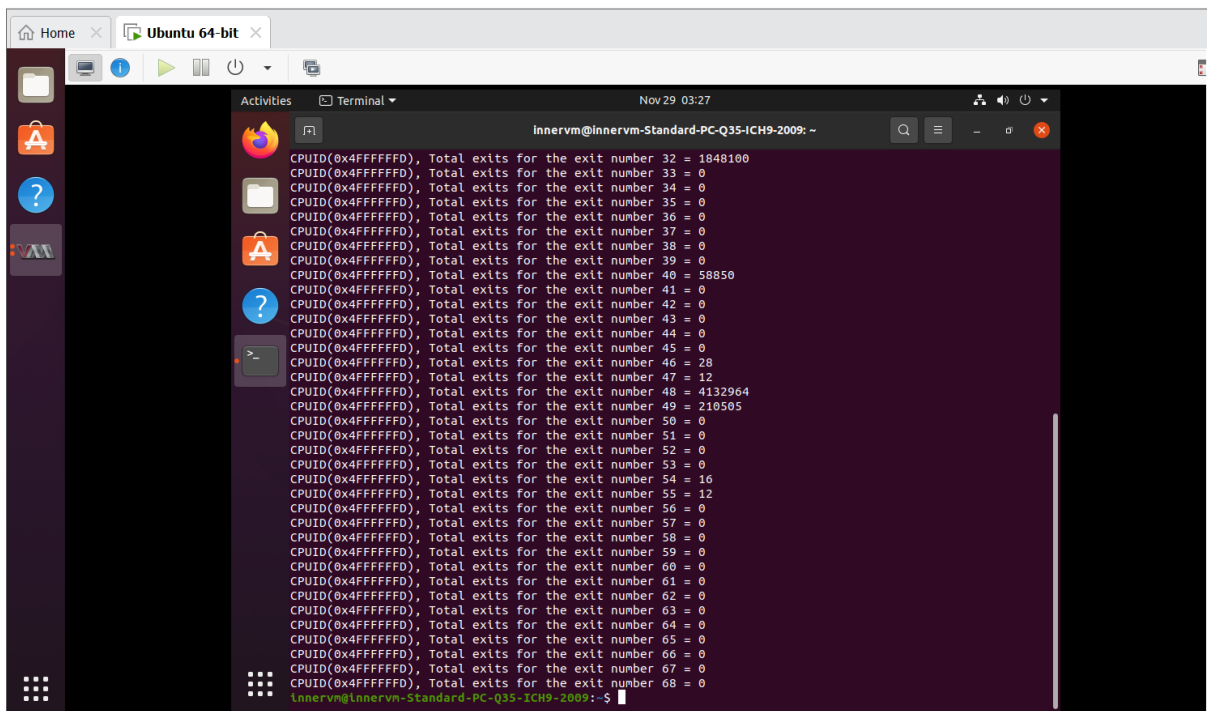
The screenshot shows a terminal window titled "Ubuntu 64-bit" with a dark purple background. The terminal displays a continuous stream of output from a program, likely a stress test or benchmark. The output consists of multiple lines, each starting with "CPUID(0x4FFFFFFD), Total exits for the exit number" followed by a specific exit number. The exit numbers range from 32 to 68, with some numbers appearing multiple times. For example, exit number 32 is 1821462, exit number 40 is 57958, and exit number 48 is 4119595. The terminal window has a title bar with "Home", "Activities", and "Terminal" buttons. The system clock in the top right corner shows "Nov 29 03:15".

```

CPUID(0x4FFFFFFD), Total exits for the exit number 32 = 1821462
CPUID(0x4FFFFFFD), Total exits for the exit number 33 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 34 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 35 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 36 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 37 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 38 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 39 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 40 = 57958
CPUID(0x4FFFFFFD), Total exits for the exit number 41 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 42 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 43 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 44 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 45 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 46 = 28
CPUID(0x4FFFFFFD), Total exits for the exit number 47 = 12
CPUID(0x4FFFFFFD), Total exits for the exit number 48 = 4119595
CPUID(0x4FFFFFFD), Total exits for the exit number 49 = 208533
CPUID(0x4FFFFFFD), Total exits for the exit number 50 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 51 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 52 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 53 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 54 = 14
CPUID(0x4FFFFFFD), Total exits for the exit number 55 = 12
CPUID(0x4FFFFFFD), Total exits for the exit number 56 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 57 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 58 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 59 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 60 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 61 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 62 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 63 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 64 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 65 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 66 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 67 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 68 = 0
lnnervm@lnnervm-Standard-PC-Q35-ICH9-2009:~$

```

Before reboot



After reboot

Home x Ubuntu 64-bit x

Activities Terminal Nov 29 03:29 innervm@innervm-Standard-PC-Q35-ICH9-2009: ~

```
innervm@innervm-Standard-PC-Q35-ICH9-2009: ~$ ./a.out
CPUID(0x4FFFFFFD), Total exits for the exit number 0 = 35344
CPUID(0x4FFFFFFD), Total exits for the exit number 1 = 1107046
CPUID(0x4FFFFFFD), Total exits for the exit number 2 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 3 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 4 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 5 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 6 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 7 = 137346
CPUID(0x4FFFFFFD), Total exits for the exit number 8 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 9 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 10 = 593465
CPUID(0x4FFFFFFD), Total exits for the exit number 11 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 12 = 545915
CPUID(0x4FFFFFFD), Total exits for the exit number 13 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 14 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 15 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 16 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 17 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 18 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 19 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 20 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 21 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 22 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 23 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 24 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 25 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 26 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 27 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 28 = 77613
CPUID(0x4FFFFFFD), Total exits for the exit number 29 = 9
CPUID(0x4FFFFFFD), Total exits for the exit number 30 = 603294
CPUID(0x4FFFFFFD), Total exits for the exit number 31 = 13676
CPUID(0x4FFFFFFD), Total exits for the exit number 32 = 1848100
CPUID(0x4FFFFFFD), Total exits for the exit number 33 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 34 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 35 = 0
CPUID(0x4FFFFFFD), Total exits for the exit number 36 = 0
```

[illegible]

Observations

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

- The total number of exits in shadow paging is more when compared to nested paging. The reason behind this nested paging will do only VM exit whenever an EPT violation occurs. But in shadow paging, when VM executes CR0, CR3, CR4, or any other related exits, it can exit every time.

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

- EPT Mode
 - There is no need to exit in EPT mode as the translation from guest VM to guest PA to host PA is done with a two-layer page table and more page access is required. So then the guest VM has to own the page table and so the operation on CR3 is done natively.
- No EPT Mode
 - In shadow paging, the guest VM does not own the page table. So to do this CR3 should be simulated by the VMM.