

CMPE283 - Assignment4 Report

Questions

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).
 - a. Deepa = scripted test file for the scenario posted in assignment4 instruction
 - b. Jae Woong = verify results in both nested paging and shadow paging
2. Include a sample of your print of exit count output from dmesg from “with ept” and “without ept”.
 - a. With ept (nested paging)

CPUID(0X4FFFFFFE): The exit Number: 0, exits = 6445

CPUID(0X4FFFFFFE): The exit Number: 1, exits = 36438

CPUID(0X4FFFFFFE): The exit Number: 2, exits = 0

CPUID(0X4FFFFFFE): The exit number 3 is not supported in KVM

CPUID(0X4FFFFFFE): The exit number 4 is not supported in KVM

CPUID(0X4FFFFFFE): The exit number 5 is not supported in KVM

CPUID(0X4FFFFFFE): The exit number 6 is not supported in KVM

CPUID(0X4FFFFFFE): The exit Number: 7, exits = 9873

CPUID(0X4FFFFFFE): The exit Number: 8, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 9, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 10, exits = 17563

CPUID(0X4FFFFFFE): The exit number 11 is not supported in KVM

CPUID(0X4FFFFFFE): The exit Number: 12, exits = 32013

CPUID(0X4FFFFFFE): The exit Number: 13, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 14, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 15, exits = 0

CPUID(0X4FFFFFFE): The exit number 16 is not supported in KVM

CPUID(0X4FFFFFFE): The exit number 17 is not supported in KVM

CPUID(0X4FFFFFFE): The exit Number: 18, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 19, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 20, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 21, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 22, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 23, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 24, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 25, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 26, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 27, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 28, exits = 14415
CPUID(0X4FFFFFFE): The exit Number: 29, exits = 5
CPUID(0X4FFFFFFE): The exit Number: 30, exits = 149875
CPUID(0X4FFFFFFE): The exit Number: 31, exits = 726
CPUID(0X4FFFFFFE): The exit Number: 32, exits = 93422
CPUID(0X4FFFFFFE): The exit number 33 is not supported in KVM
CPUID(0X4FFFFFFE): The exit number 34 is not supported in KVM
CPUID(0X4FFFFFFE): The exit number 35, is not supported
CPUID(0X4FFFFFFE): The exit number 36 is not supported in KVM
CPUID(0X4FFFFFFE): The exit Number: 37, exits = 0
CPUID(0X4FFFFFFE): The exit number 38, is not supported
CPUID(0X4FFFFFFE): The exit Number: 39, exits = 0
CPUID(0X4FFFFFFE): The exit number 40 is not supported in KVM
CPUID(0X4FFFFFFE): The exit Number: 41, exits = 0
CPUID(0X4FFFFFFE): The exit number 42, is not supported
CPUID(0X4FFFFFFE): The exit Number: 43, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 44, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 45, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 46, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 47, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 48, exits = 2577202
CPUID(0X4FFFFFFE): The exit Number: 49, exits = 22921
CPUID(0X4FFFFFFE): The exit Number: 50, exits = 0

CPUID(0X4FFFFFFE): The exit number 51 is not supported in KVM

CPUID(0X4FFFFFFE): The exit Number: 52, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 53, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 54, exits = 18

CPUID(0X4FFFFFFE): The exit Number: 55, exits = 6

CPUID(0X4FFFFFFE): The exit Number: 56, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 57, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 58, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 59, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 60, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 61, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 62, exits = 0

CPUID(0X4FFFFFFE): The exit number 63 is not supported in KVM

CPUID(0X4FFFFFFE): The exit number 64 is not supported in KVM

CPUID(0X4FFFFFFE): The exit number 65, is not supported

CPUID(0X4FFFFFFE): The exit number 66 is not supported in KVM

CPUID(0X4FFFFFFE): The exit Number: 67, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 68, exits = 0

CPUID(0X4FFFFFFE): The exit number 69, is not supported

Total_count:: 2960922

```
ej@ej-Standard-PC-i440FX-PIIX-1996:~/Downloads$ ./test4
CPUID(0X4FFFFFFE): The exit Number: 0, exits = 6445
CPUID(0X4FFFFFFE): The exit Number: 1, exits = 36438
CPUID(0X4FFFFFFE): The exit Number: 2, exits = 0
CPUID(0X4FFFFFFE): The exit number 3 is not supported in KVM
CPUID(0X4FFFFFFE): The exit number 4 is not supported in KVM
CPUID(0X4FFFFFFE): The exit number 5 is not supported in KVM
CPUID(0X4FFFFFFE): The exit number 6 is not supported in KVM
CPUID(0X4FFFFFFE): The exit Number: 7, exits = 9873
CPUID(0X4FFFFFFE): The exit Number: 8, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 9, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 10, exits = 17563
CPUID(0X4FFFFFFE): The exit number 11 is not supported in KVM
CPUID(0X4FFFFFFE): The exit Number: 12, exits = 32013
CPUID(0X4FFFFFFE): The exit Number: 13, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 14, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 15, exits = 0
CPUID(0X4FFFFFFE): The exit number 16 is not supported in KVM
CPUID(0X4FFFFFFE): The exit number 17 is not supported in KVM
CPUID(0X4FFFFFFE): The exit Number: 18, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 19, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 20, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 21, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 22, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 23, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 24, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 25, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 26, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 27, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 28, exits = 14415
CPUID(0X4FFFFFFE): The exit Number: 29, exits = 5
CPUID(0X4FFFFFFE): The exit Number: 30, exits = 149875
CPUID(0X4FFFFFFE): The exit Number: 31, exits = 726
CPUID(0X4FFFFFFE): The exit Number: 32, exits = 93422
```



```
CPUID(0X4FFFFFFE): The exit Number: 37, exits = 0
CPUID(0X4FFFFFFE): The exit number 38, is not supported
CPUID(0X4FFFFFFE): The exit Number: 39, exits = 0
CPUID(0X4FFFFFFE): The exit number 40 is not supported in KVM
CPUID(0X4FFFFFFE): The exit Number: 41, exits = 0
CPUID(0X4FFFFFFE): The exit number 42, is not supported
CPUID(0X4FFFFFFE): The exit Number: 43, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 44, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 45, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 46, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 47, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 48, exits = 2577202
CPUID(0X4FFFFFFE): The exit Number: 49, exits = 22921
CPUID(0X4FFFFFFE): The exit Number: 50, exits = 0
CPUID(0X4FFFFFFE): The exit number 51 is not supported in KVM
CPUID(0X4FFFFFFE): The exit Number: 52, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 53, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 54, exits = 18
CPUID(0X4FFFFFFE): The exit Number: 55, exits = 6
CPUID(0X4FFFFFFE): The exit Number: 56, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 57, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 58, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 59, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 60, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 61, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 62, exits = 0
CPUID(0X4FFFFFFE): The exit number 63 is not supported in KVM
CPUID(0X4FFFFFFE): The exit number 64 is not supported in KVM
CPUID(0X4FFFFFFE): The exit number 65, is not supported
CPUID(0X4FFFFFFE): The exit number 66 is not supported in KVM
CPUID(0X4FFFFFFE): The exit Number: 67, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 68, exits = 0
CPUID(0X4FFFFFFE): The exit number 69, is not supported
Total_count:: 2960922
```

b. Without ept (shadow paging)

CPUID(0X4FFFFFFE): The exit Number: 0, exits = 12890

CPUID(0X4FFFFFFE): The exit Number: 1, exits = 63632

CPUID(0X4FFFFFFE): The exit Number: 2, exits = 0

CPUID(0X4FFFFFFE): The exit number 3 is not supported in KVM

CPUID(0X4FFFFFFE): The exit number 4 is not supported in KVM

CPUID(0X4FFFFFFE): The exit number 5 is not supported in KVM

CPUID(0X4FFFFFFE): The exit number 6 is not supported in KVM

CPUID(0X4FFFFFFE): The exit Number: 7, exits = 13015

CPUID(0X4FFFFFFE): The exit Number: 8, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 9, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 10, exits = 30845

CPUID(0X4FFFFFFE): The exit number 11 is not supported in KVM

CPUID(0X4FFFFFFE): The exit Number: 12, exits = 136396

CPUID(0X4FFFFFFE): The exit Number: 13, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 14, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 15, exits = 0

CPUID(0X4FFFFFFE): The exit number 16 is not supported in KVM

CPUID(0X4FFFFFFE): The exit number 17 is not supported in KVM

CPUID(0X4FFFFFFE): The exit Number: 18, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 19, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 20, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 21, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 22, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 23, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 24, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 25, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 26, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 27, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 28, exits = 28604

CPUID(0X4FFFFFFE): The exit Number: 29, exits = 13

CPUID(0X4FFFFFFE): The exit Number: 30, exits = 271410

CPUID(0X4FFFFFFE): The exit Number: 31, exits = 1320

CPUID(0X4FFFFFFE): The exit Number: 32, exits = 227699

CPUID(0X4FFFFFFE): The exit number 33 is not supported in KVM

CPUID(0X4FFFFFFE): The exit number 34 is not supported in KVM

CPUID(0X4FFFFFFE): The exit number 35, is not supported

CPUID(0X4FFFFFFE): The exit number 36 is not supported in KVM

CPUID(0X4FFFFFFE): The exit Number: 37, exits = 0

CPUID(0X4FFFFFFE): The exit number 38, is not supported

CPUID(0X4FFFFFFE): The exit Number: 39, exits = 0

CPUID(0X4FFFFFFE): The exit number 40 is not supported in KVM

CPUID(0X4FFFFFFE): The exit Number: 41, exits = 0

CPUID(0X4FFFFFFE): The exit number 42, is not supported

CPUID(0X4FFFFFFE): The exit Number: 43, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 44, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 45, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 46, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 47, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 48, exits = 11697515

CPUID(0X4FFFFFFE): The exit Number: 49, exits = 36600

CPUID(0X4FFFFFFE): The exit Number: 50, exits = 0

CPUID(0X4FFFFFFE): The exit number 51 is not supported in KVM

CPUID(0X4FFFFFFE): The exit Number: 52, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 53, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 54, exits = 36

CPUID(0X4FFFFFFE): The exit Number: 55, exits = 12

CPUID(0X4FFFFFFE): The exit Number: 56, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 57, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 58, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 59, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 60, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 61, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 62, exits = 0

CPUID(0X4FFFFFFE): The exit number 63 is not supported in KVM

CPUID(0X4FFFFFFE): The exit number 64 is not supported in KVM

CPUID(0X4FFFFFFE): The exit number 65, is not supported

CPUID(0X4FFFFFFE): The exit number 66 is not supported in KVM

CPUID(0X4FFFFFFE): The exit Number: 67, exits = 0

CPUID(0X4FFFFFFE): The exit Number: 68, exits = 0

CPUID(0X4FFFFFFE): The exit number 69, is not supported

Total_count:: 12519987


```
ej@ej-Standard-PC-i440FX-PIIX-1996:~/Downloads$ ./test4
CUID(0X4FFFFFFE): The exit Number: 0, exits = 12890
CUID(0X4FFFFFFE): The exit Number: 1, exits = 63632
CUID(0X4FFFFFFE): The exit Number: 2, exits = 0
CUID(0X4FFFFFFE): The exit number 3 is not supported in KVM
CUID(0X4FFFFFFE): The exit number 4 is not supported in KVM
CUID(0X4FFFFFFE): The exit number 5 is not supported in KVM
CUID(0X4FFFFFFE): The exit number 6 is not supported in KVM
CUID(0X4FFFFFFE): The exit Number: 7, exits = 13015
CUID(0X4FFFFFFE): The exit Number: 8, exits = 0
CUID(0X4FFFFFFE): The exit Number: 9, exits = 0
CUID(0X4FFFFFFE): The exit Number: 10, exits = 30845
CUID(0X4FFFFFFE): The exit number 11 is not supported in KVM
CUID(0X4FFFFFFE): The exit Number: 12, exits = 136396
CUID(0X4FFFFFFE): The exit Number: 13, exits = 0
CUID(0X4FFFFFFE): The exit Number: 14, exits = 0
CUID(0X4FFFFFFE): The exit Number: 15, exits = 0
CUID(0X4FFFFFFE): The exit number 16 is not supported in KVM
CUID(0X4FFFFFFE): The exit number 17 is not supported in KVM
CUID(0X4FFFFFFE): The exit Number: 18, exits = 0
CUID(0X4FFFFFFE): The exit Number: 19, exits = 0
CUID(0X4FFFFFFE): The exit Number: 20, exits = 0
CUID(0X4FFFFFFE): The exit Number: 21, exits = 0
CUID(0X4FFFFFFE): The exit Number: 22, exits = 0
CUID(0X4FFFFFFE): The exit Number: 23, exits = 0
CUID(0X4FFFFFFE): The exit Number: 24, exits = 0
CUID(0X4FFFFFFE): The exit Number: 25, exits = 0
CUID(0X4FFFFFFE): The exit Number: 26, exits = 0
CUID(0X4FFFFFFE): The exit Number: 27, exits = 0
CUID(0X4FFFFFFE): The exit Number: 28, exits = 28604
CUID(0X4FFFFFFE): The exit Number: 29, exits = 13
CUID(0X4FFFFFFE): The exit Number: 30, exits = 271410
CUID(0X4FFFFFFE): The exit Number: 31, exits = 1320
CUID(0X4FFFFFFE): The exit Number: 32, exits = 227699
CUID(0X4FFFFFFE): The exit number 33 is not supported in KVM
CUID(0X4FFFFFFE): The exit number 34 is not supported in KVM
CUID(0X4FFFFFFE): The exit number 35, is not supported
```



```
CPUID(0X4FFFFFFE): The exit number 34 is not supported in KVM
CPUID(0X4FFFFFFE): The exit number 35, is not supported
CPUID(0X4FFFFFFE): The exit number 36 is not supported in KVM
CPUID(0X4FFFFFFE): The exit Number: 37, exits = 0
CPUID(0X4FFFFFFE): The exit number 38, is not supported
CPUID(0X4FFFFFFE): The exit Number: 39, exits = 0
CPUID(0X4FFFFFFE): The exit number 40 is not supported in KVM
CPUID(0X4FFFFFFE): The exit Number: 41, exits = 0
CPUID(0X4FFFFFFE): The exit number 42, is not supported
CPUID(0X4FFFFFFE): The exit Number: 43, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 44, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 45, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 46, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 47, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 48, exits = 11697515
CPUID(0X4FFFFFFE): The exit Number: 49, exits = 36600
CPUID(0X4FFFFFFE): The exit Number: 50, exits = 0
CPUID(0X4FFFFFFE): The exit number 51 is not supported in KVM
CPUID(0X4FFFFFFE): The exit Number: 52, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 53, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 54, exits = 36
CPUID(0X4FFFFFFE): The exit Number: 55, exits = 12
CPUID(0X4FFFFFFE): The exit Number: 56, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 57, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 58, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 59, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 60, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 61, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 62, exits = 0
CPUID(0X4FFFFFFE): The exit number 63 is not supported in KVM
CPUID(0X4FFFFFFE): The exit number 64 is not supported in KVM
CPUID(0X4FFFFFFE): The exit number 65, is not supported
CPUID(0X4FFFFFFE): The exit number 66 is not supported in KVM
CPUID(0X4FFFFFFE): The exit Number: 67, exits = 0
CPUID(0X4FFFFFFE): The exit Number: 68, exits = 0
CPUID(0X4FFFFFFE): The exit number 69, is not supported
Total_count:: 12519987
```

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

- a. The total count of exits from ept (nested paging) was 2.9 million right after boot, whereas no-ept (shadow paging) took 12.5 million. This is because the reasons for shadow paging's exits are when accessing CR3, CR4, or INVLPG, and page fault, which result in more exits. But exits for nested paging occur due to fewer number of reasons, e.g. nested page fault, ept violation.

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

- a. The key difference between nested paging and shadow paging is that its mechanism on how to translate the final physical address on the host machine.
- b. For shadow paging, VMM handles in-use CR3 and fully imitated page table called shadow page table with various exit handlings. Typically the table is flushed when CR3 is switched inside VM. It entails more number and types of exits in order to virtualize memory in VM with shadow paging.
- c. For nested paging, VMM owns nested page table. Compared to shadow paging, it only contains "final translation" of each GPT. The final decision of page table walk is determined successful only if the corresponding mapping is present at nested page table. Also, TLB with nested paging include ID and Tags, which helps to utilize TLB and avoid excessive flushing.