CS 746 : Linux Kernel Programming

Assignment 1: Part 3
Where in memory is the kernel?

Submitted by

Aurobindo Mondal
143050082

Under the guidance of

Prof. Purushottam Kulkarni

Department of Computer Science and Engineering
IIT Bombay

February 19, 2016

Where in the virtual address space kernel resides ?

Kernel starts after the hypervisor area i.e. 0xffff880000000000 and ends at 0xffffffffffffffff

What are the different regions in the kernel virtual address space.

**Source/Documentation/x86/x86_64/mm.txt

Starting Address	Ending Address	Size	Description
0000000000000000	00007fffffffffff	47 bits	User Space
ffff800000000000	ffff87ffffffffff	43 bits	Guard hole, reserved for hypervisor
ffff880000000000	ffffc7ffffffffff	64 KB	Direct mapping of all phys. memory
ffffc80000000000	ffffc8ffffffffff	40 bits	Hole
ffffc90000000000	ffffe8ffffffffff	45 bits	vmalloc/ioremap space
ffffe90000000000	ffffe9ffffffffff	40 bits	hole
ffffea0000000000	ffffeaffffffffff	40 bits	Virtual memory map (1TB)
ffffec0000000000	fffffc0000000000	44 bits	kasan shadow memory (16TB)
fffffff0000000000	ffffff7fffffffff	39 bits	%esp fixup stacks
ffffffff80000000	ffffffffa0000000	512 MB	kernel text mapping, from phys 0
ffffffffa0000000	fffffffff5fffff	1525 MB	module mapping space
fffffffff600000	ffffffffffdfffff	8MB	vsyscalls

ffffffffffe00000	ffffffffffffffff	2MB	unused hole

Pseudo Code to traverse virtual address space:

On module insert :

```
Hard-code the regions in a linked list.
for each region :
      for each page in region :
            pte = do_page_walk();
            if(pte==NULL):
                  unmapp++;
            else :
                  if(pte_present):
                        present++;
                        get physical address();
                        print virtual and physical address;   // kernel text
                  else :
                        notPresent++;
                        break; // dont break if stack area
            insert all data into linked list;
      schedule();
```

On removing module :

```
print the content of linked list :
      Region Name,
      Starting Address,
      Ending Address,
      Total Size,
      Number of pages present in RAM,
      Number of pages not present in RAM but mapped,
      Number of pages unmapped.
```

Results and Observations :

```
$ sudo insmod memory.ko
$ sudo rmmod memory
$ dmesg
...
[ 2929.679664] Region Name : Kernel Text Mapping
[ 2929.679667]  Starting Virtual Address : ffffffff80000000
[ 2929.679670]  Ending Virtual Address : ffffffffa0000000
[ 2929.679672]  Total Size : 512 MB
[ 2929.679675]  Number of Pages MAPPED & PRESENT in RAM : 4096
[ 2929.679677]  Number of Pages MAPPED & NOT PRESENT in RAM : 0
[ 2929.679680]  Number of Pages UNMAPPED : 126976
[ 2929.679682]
[ 2929.679685] Region Name : Hypervisor
[ 2929.679688]  Starting Virtual Address : ffff800000000000
[ 2929.679691]  Ending Virtual Address : ffff87ffffffffff
[ 2929.679693]  Total Size : 8388607 MB
[ 2929.679696]  Number of Pages MAPPED & PRESENT in RAM : 0
[ 2929.679699]  Number of Pages MAPPED & NOT PRESENT in RAM : 0
[ 2929.679702]  Number of Pages UNMAPPED : 2147483648
[ 2929.679704]
[ 2929.679706] Region Name : Direct mapping
[ 2929.679709]  Starting Virtual Address : ffff880000000000
[ 2929.679712]  Ending Virtual Address : ffffc7ffffffffff
[ 2929.679715]  Total Size : 67108863 MB
[ 2929.679717]  Number of Pages MAPPED & PRESENT in RAM : 261636
[ 2929.679720]  Number of Pages MAPPED & NOT PRESENT in RAM : 1
[ 2929.679723]  Number of Pages UNMAPPED : 512
[ 2929.679725]
[ 2929.679727] Region Name : vmalloc
[ 2929.679730]  Starting Virtual Address : ffffc90000000000
[ 2929.679733]  Ending Virtual Address : ffffe8ffffffffff
[ 2929.679735]  Total Size : 33554431 MB
[ 2929.679738]  Number of Pages MAPPED & PRESENT in RAM : 1
[ 2929.679740]  Number of Pages MAPPED & NOT PRESENT in RAM : 1
[ 2929.679743]  Number of Pages UNMAPPED : 0
[ 2929.679745]
[ 2929.679747] Region Name : Virtual Memory map
[ 2929.679750]  Starting Virtual Address : ffffea0000000000
[ 2929.679753]  Ending Virtual Address : ffffeaffffffffff
```

```
[ 2929.679755]  Total Size : 1048575 MB
[ 2929.679758]  Number of Pages MAPPED & PRESENT in RAM : 16384
[ 2929.679761]  Number of Pages MAPPED & NOT PRESENT in RAM : 0
[ 2929.679763]  Number of Pages UNMAPPED : 268419072
[ 2929.679766]
[ 2929.679768] Region Name : Kasan shadow memory
[ 2929.679771]  Starting Virtual Address : ffffec0000000000
[ 2929.679774]  Ending Virtual Address : fffffc0000000000
[ 2929.679776]  Total Size : 16777216 MB
[ 2929.679779]  Number of Pages MAPPED & PRESENT in RAM : 0
[ 2929.679781]  Number of Pages MAPPED & NOT PRESENT in RAM : 0
[ 2929.679784]  Number of Pages UNMAPPED : 4294967296
[ 2929.679786]
[ 2929.679789] Region Name : esp fixup stacks
[ 2929.679792]  Starting Virtual Address : ffffff0000000000
[ 2929.679795]  Ending Virtual Address : ffffff7fffffffff
[ 2929.679797]  Total Size : 524287 MB
[ 2929.679800]  Number of Pages MAPPED & PRESENT in RAM : 65536
[ 2929.679803]  Number of Pages MAPPED & NOT PRESENT in RAM : 983040
[ 2929.679805]  Number of Pages UNMAPPED : 133169152
[ 2929.679807]
[ 2929.679810] Region Name : Module mapping space
[ 2929.679812]  Starting Virtual Address : ffffffffa0000000
[ 2929.679814]  Ending Virtual Address : fffffffffff5fffff
[ 2929.679817]  Total Size : 1525 MB
[ 2929.679820]  Number of Pages MAPPED & PRESENT in RAM : 0
[ 2929.679822]  Number of Pages MAPPED & NOT PRESENT in RAM : 1
[ 2929.679825]  Number of Pages UNMAPPED : 131584
[ 2929.679827]
[ 2929.679829] Region Name : vsyscalls
[ 2929.679832]  Starting Virtual Address : ffffffffff600000
[ 2929.679835]  Ending Virtual Address : ffffffffffdfffff
[ 2929.679837]  Total Size : 7 MB
[ 2929.679840]  Number of Pages MAPPED & PRESENT in RAM : 1
[ 2929.679842]  Number of Pages MAPPED & NOT PRESENT in RAM : 1
[ 2929.679845]  Number of Pages UNMAPPED : 0
[ 2929.679847]
[ 2929.680215] Exiting Module!!! Good Bye!!!
```