Notes on Non-Executable Stack

Yousra Aafer

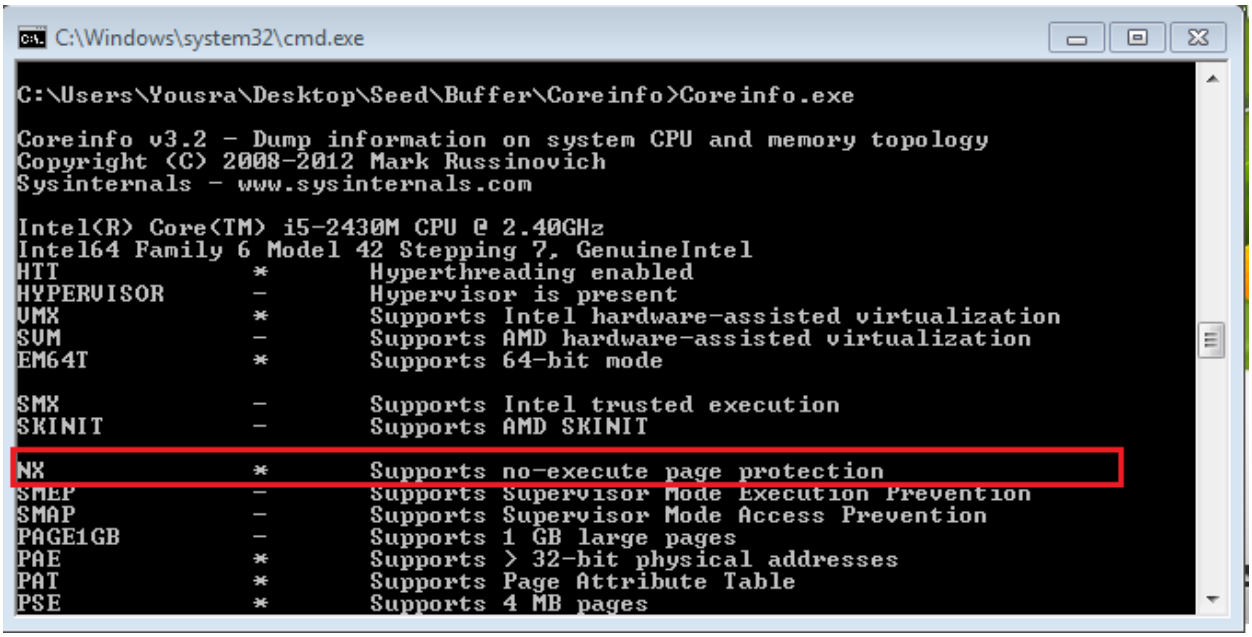
By default, the kernel sets the stack as non-executable. To allow executing code on the stack, we need to specify the following option when compiling the program: gcc –z execstack –o test test.c

However, in the following cases, executing the code on the stack might be still possible without specifying the –z execstack:

1. Host CPU does not support the NX bit:

The NX bit (Never eXecute), known also as XD (eXecute Disable) is a technology supported by the CPU to protect against executing code on non-executable memory regions such stack, heap, etc..

To check if a Window machine supports NX bit, run Coreinfo.exe (You can download it from Microsoft website) and look for NX flag.



In the above case, the system supports the NX flag.

2. Host CPU supports NX bit, but it is not enabled:

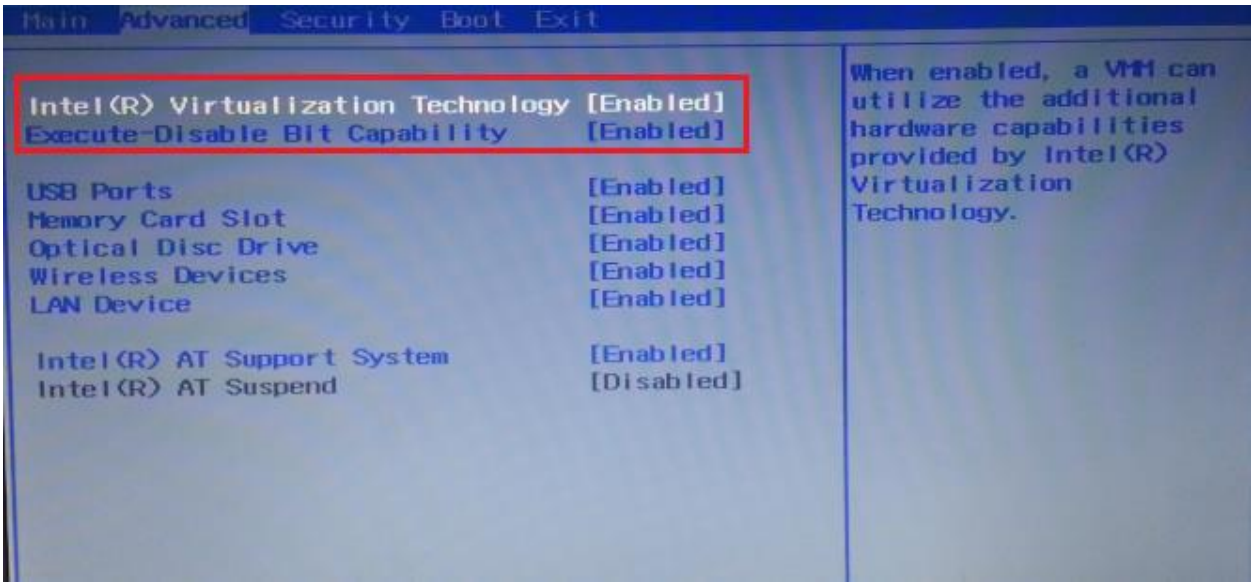
Some BIOS manufacturers disable the NX bit.

To check if the NX bit is enabled on your host (windows machine), go to the windows BIOS during system bootup, and check in the Advanced tab and look for an entry like: **NX bit**, or **Execute Disable Bit**.

If it is disabled, you can press enter to enable it.

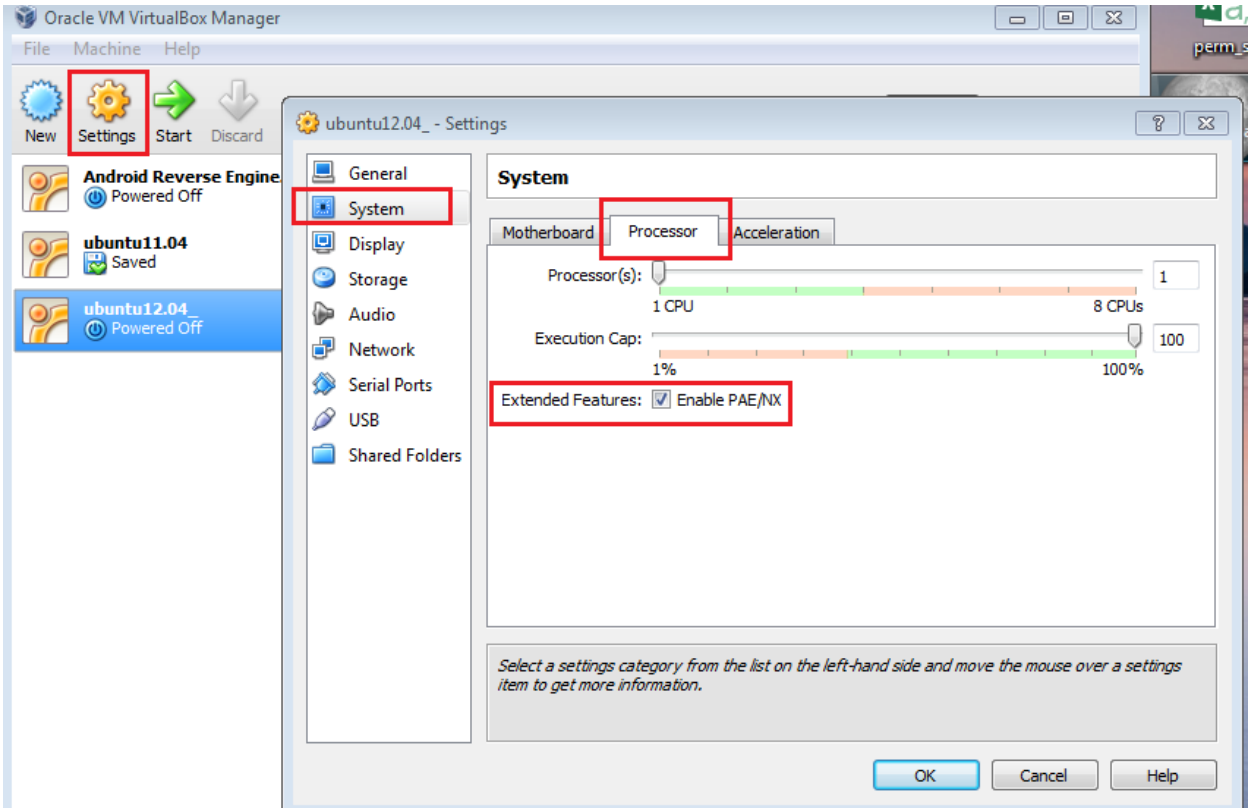
3. Host CPU supports NX bit but it is not enabled on virtualized environment:

Sometimes, the host OS does not provide some CPU features to the virtualized environment by default. To turn on the NX bit on the virtual environment, go to the Windows BIOS and look in the advanced tab for an entry containing **Virtualization Technology**. If it is disabled, you can press enter to enable it.



4. NX bit is disabled on virtual image settings: (most probable reason)

Check if the NX bit on the virtual image settings is enabled by doing the following.



Notes on the Differences between Ubuntu11.04 and Ubuntu12.04 concerning the NX bit:

If the NX bit is not supported or disabled on the virtualized environment, Ubuntu11.04 and Ubuntu12.04 behave differently:

On Ubuntu12.04:

NX protection will not be supported at all.

In fact, looking at the boot log of Ubuntu12.04 on an NX disabled host, we find the following message:

[0.000000] Notice: NX (Execute Disable) protection missing in CPU!

On Ubuntu11.04:

Even if NX bit is not supported or disabled, NX protection will be approximated by x86 segments limit. And thus, it will not be possible to execute code on a non-executable memory region such as stack.

Looking at the boot log of Ubuntu11.04, we found the following message:

[0.000000] Notice: NX (Execute Disable) protection missing in CPU!
[0.000000] NX (Execute Disable) protection: approximated by x86 segment limits