

Note asupra stivei neexecutabile

Yousra Aafer

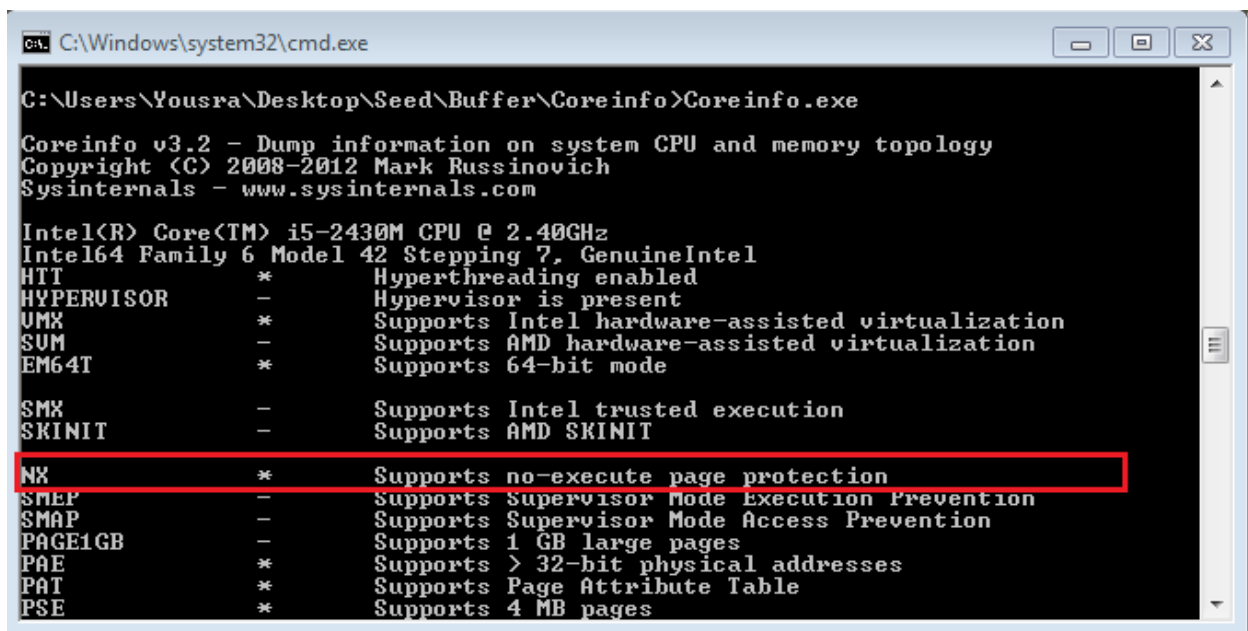
Implicit, nucleul setează stiva ca neexecutabilă. Pentru a permite executarea de cod de pe stivă, avem nevoie să specificăm următoarea opțiune la compilarea programului: `gcc -z execstack -o test test.c`

Totuși, în următoarele cazuri, execuția de cod de pe stivă poate fi totuși posibilă fără a specifica `-z execstack`:

1. UCP gazdă nu suportă bitul NX:

Bitul NX (Never eXecute), cunoscut și ca XD (eXecute Disable) reprezintă o tehnologie suportată de UCP pentru a proteja împotriva execuției codului din zone de memorie neexecutabile, cum este stiva, heap etc..

Pentru a verifica dacă mașina suportă bitul NX, executați programul Coreinfo.exe (pe care îl puteți descărca de pe situl Microsoft) și să verificați fanionul NX..



```
C:\Windows\system32\cmd.exe

C:\Users\Yousra\Desktop\Seed\Buffer\Coreinfo>Coreinfo.exe

Coreinfo v3.2 - Dump information on system CPU and memory topology
Copyright (C) 2008-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Intel(R) Core(TM) i5-2430M CPU @ 2.40GHz
Intel64 Family 6 Model 42 Stepping 7, GenuineIntel
HTT * Hyperthreading enabled
HYPERVISOR - Hypervisor is present
VMX * Supports Intel hardware-assisted virtualization
SVM - Supports AMD hardware-assisted virtualization
EM64T * Supports 64-bit mode

SMX - Supports Intel trusted execution
SKINIT - Supports AMD SKINIT
NX * Supports no-execute page protection
SMEP - Supports Supervisor Mode Execution Prevention
SMAP - Supports Supervisor Mode Access Prevention
PAGE1GB - Supports 1 GB large pages
PAE * Supports > 32-bit physical addresses
PAT * Supports Page Attribute Table
PSE * Supports 4 MB pages
```

În cazul de mai sus, sistemul suportă fanionul NX.

2. UCP gazdă suportă bitul NX, dar este inactiv:

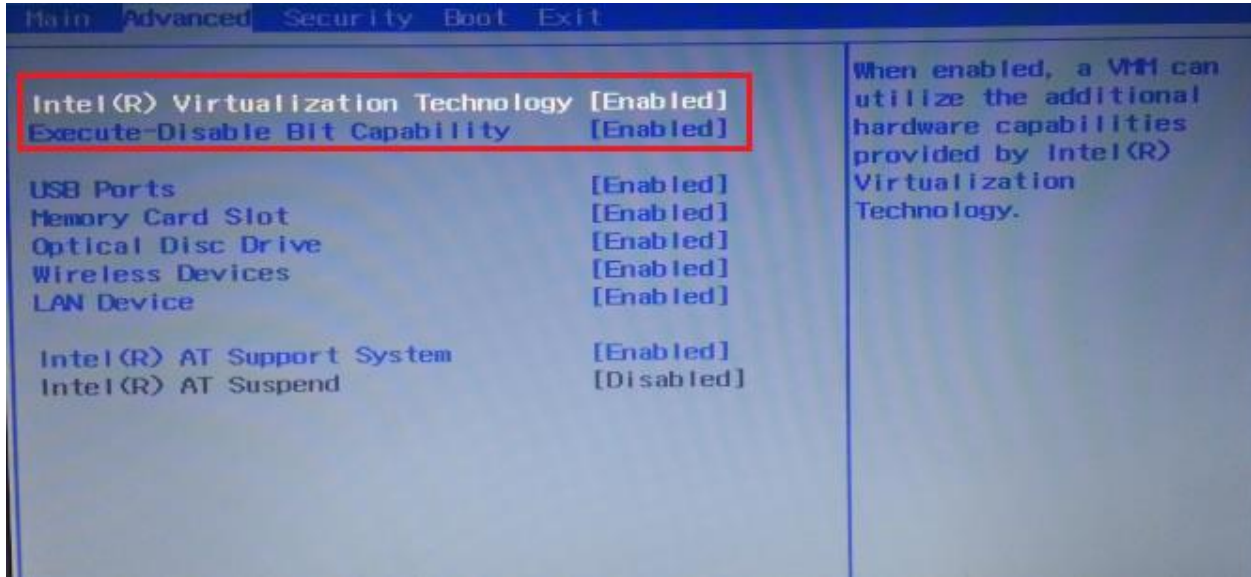
Unii producători de BIOS dezactivează bitul NX.

Pentru a verifica dacă bitul NX este activ pe gazda dumneavoastră (mașină windows), intrați în BIOS la boot și căutați în tab-ul Advanced o intrare numită: **NX bit**, sau **Execute Disable Bit**.

Dacă este dezactivat, puteți să-l reactivați.

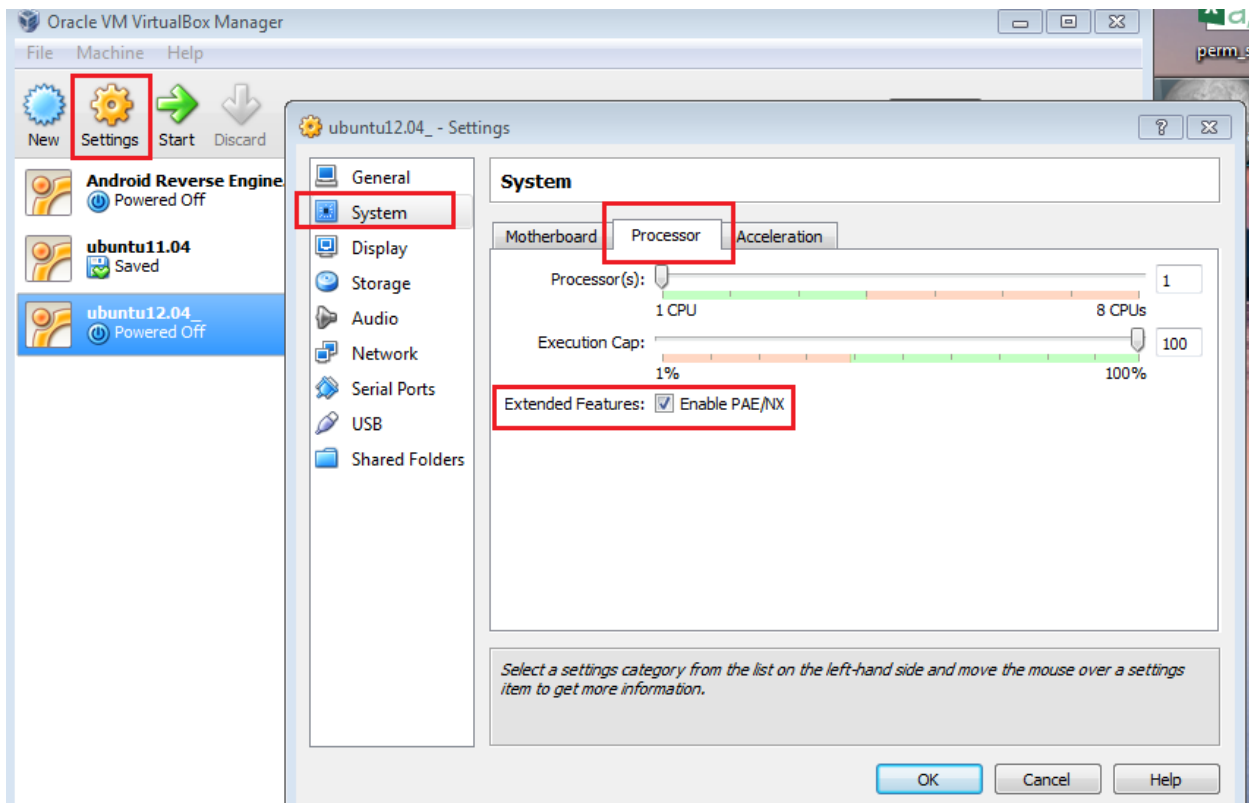
3. UCP gazdă suportă bitul NX, dar acesta nu e activat în medii virtualizate:

Uneori, SO gazdă nu furnizează implicit mediilor virtualizate unele caracteristici ale UCP. Pentru a activa bitul NX pe un mediu virtual, intrați în Windows BIOS și căutați în tab-ul Advanced o intrare care conține **Virtualization Technology**. Dacă e dezactivată, activați-o.



4. Bitul NX este dezactivat în setările imaginii virtuale (cel mai probabil motiv)

Verificați bitul NX din setările imaginii virtuale executând următoarele:



Observații despre diferențele dintre Ubuntu11.04 și Ubuntu12.04 în privința bitului NX:

Dacă bitul NX nu este suportat sau este dezactivat pe mediul virtualizat, atunci Ubuntu11.04 și Ubuntu12.04 se comportă diferit:

On Ubuntu12.04:

Protecția NX nu va fi suportată de loc.

De fapt, dacă examinăm jurnalul de boot al Ubuntu12.04 pe o gazdă cu NX dezactivat, atunci găsim următorul mesaj: **[0.000000] Notice: NX (Execute Disable) protection missing in CPU!**

On Ubuntu11.04:

Chiar dacă bitul NX nu este suportat sau este dezactivat, protecția NX va fi aprozimată prin limitele de segmente x86. Astfel nu se va putea executa cod pe o regiune de memorie neexecutabilă, cum este stiva.

Examinând jurnalul de boot al Ubuntu11.04, am găsit următoarele mesaje:

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

[0.000000] NX (Execute Disable) protection: approximated by x86 segment limits