Suricata - Feature #682
Add DEP and ASLR to Windows Binary
12/14/2012 08:36 AM - Rich Rumble

Status: Assigned
Priority: Normal
Assignee: Community Ticket
Category: TBD
Target version: TBD
Effort: low
Difficulty: low
Label:

Description
The windows Suricata.exe does not have the DEP or ASLR flags set, I'm not sure how to define the peflags in the code, but I've been able to set them on the already compiled code using "peflags" from Cygwin:

peflags --dynamicbase=true --nxcompat=true /cygdrive/c/Suricata\ 1.4rc1-1-32bit/suricata.exe

Doing it afterward seems to have no effect other than DEP and ASLR being used! I know Pidgin/LibPurple recently added these flags in the code (http://pidgin.im/pipermail/commits/2012-September/021591.html) as well.

-rich

History
#1 - 12/14/2012 08:51 AM - Rich Rumble
Looks like LD can also set these if that helps?
man ld
...
--dynamicbase
The image base address may be relocated using address space layout randomization (ASLR). This feature was introduced with MS Windows Vista for i386 PE targets.
--nxcompat
The image is compatible with the Data Execution Prevention. This feature was introduced with MS Windows XP SP2 for i386 PE targets.

-rich

#2 - 12/15/2012 04:21 AM - Victor Julien
- Tracker changed from Optimization to Feature
- Status changed from New to Assigned
- Assignee set to Peter Manev

#3 - 12/15/2012 08:26 AM - Peter Manev
Is there a way to determine for sure, after a windows msi install , that the suricata.exe has the DEP or ASLR flags set and those are used correctly?

thanks

#4 - 12/15/2012 03:33 PM - Rich Rumble
As far as I know, once those flags are compiled in or added, it's up to the OS from that point. I don't see any additional requirements, libraries or extensive code needed to take advantage of these features. I know you can use Process Explorer from Microsoft's Sysinternals suite to see that the OS is reading the flags, whether or not the OS is doing what it's supposed to from that point, I have no idea. Really I think it's just setting a flag on the exe, and the OS taking it from there...

-rich

#5 - 12/16/2012 11:19 AM - Peter Manev
- % Done changed from 0 to 80

Thank you Rich.

The flags are now set on the new 1.4 msi pkg.

We should look for a way to do this in the configure stage under Cygwin (not just using peflags on the exe)....

#6 - 12/17/2012 01:12 AM - Victor Julien

03/18/2022 1/2
Eric, can you figure out a way to do this automatically? I think we need to test if the command is available and then run it at the correct time.

#7 - 12/17/2012 03:56 PM - Rich Rumble
I know VLC and Libpurple recently added such code
http://git.videolan.org/?p=vlc.git;a=commitdiff;h=60aa14b737e0f00d34c5789b7e7c62557dd7a10d;hp=54104ba864c568d95b52587bb481529401317d9e
https://developer.pidgin.im/ticket/15290
I think each went about it slightly differently. LD flags seem to be a good way
LD_HARDENING_OPTIONS ?= -Wl,--dynamicbase -Wl,--nxcompat (from pidgin/libpurple)
-rich

#8 - 03/10/2013 09:46 AM - Victor Julien
- Target version changed from 1.4.1 to 2.0beta1

#9 - 07/09/2013 07:30 AM - Victor Julien
- Target version changed from 2.0beta1 to 2.0beta2

#10 - 11/21/2013 04:32 AM - Victor Julien
- Target version changed from 2.0beta2 to 2.0rc1

#11 - 01/31/2014 06:50 AM - Victor Julien
- Target version changed from 2.0rc1 to TBD

#12 - 07/17/2018 08:35 AM - Victor Julien
- Assignee changed from Eric Leblond to Anonymous
  - Effort set to low
  - Difficulty set to low

#13 - 02/23/2019 10:11 PM - Andreas Herz
  - Assignee set to Community Ticket