Windows 11 Kernel Debugging Assignment

CSIS 443

Professor OMalley

James Riley Dorough

Liberty University

November 29th, 2021

**Introduction**

To complete this lab, I was unable to get a vm working for windows 10 or 11. However, thanks to David Cothran I was able to acquire screenshots to demonstrate the commands running. I was unable to find any information on the !pic, ImageBaseAddress, or !numa commands. Only some information discerned from the screenshots and related topics.

**Lab Work & Implication**

|  |  |
| --- | --- |
| **!idt** | This shows the user a list of all the interrupt service routines within the system’s interrupt dispatch table.  https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/-idt |
| **!pic** | No information found about this command itself. However, I was able to find information pertaining to IRQ numbers. Interrupt request numbers delineate which device on a shared bus has made the interrupt request.  https://kb.iu.edu/d/ailq#:~:text=The%20IRQ%20number%20is%20a,or%20action%20to%20take%20place. |
| **!peb** | Returns information from the process environment block. Since no hexadecimal address is provides, the command will return the process environment block info for the current process context is shown.  https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/-peb |
| **ImageBaseAddress** | I believe that this command returns the address where the image is to be loaded in memory |
| **!process 0 0** | Outputs a list of all running processes with their session id, location in memory, parent information, and process or image title.  https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/getting-started-with-windbg--kernel-mode- |
| **!devnode 0 0** | This displays information about nodes in the device tree. The inclusion of a zero in the address switch tells the system to start at the root of the main device tree. A zero in the flags switch tells the command to display all children of the device node.  https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/-devnode |
| **!vm** | Provides an overview of virtual memory use statistics. The lack of a specified flag will cause the command to default to flag zero which displays system wide virtual memory statistics and memory statistics for the running processes  https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/-vm |
| **!numa** | Non-uniform memory access attempts to make memory access faster per additional cpu core.  https://en.wikipedia.org/wiki/Non-uniform\_memory\_access |

**Graphical user interface, text, application

Description automatically generatedCalendar

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application, email

Description automatically generatedGraphical user interface, text, application, email

Description automatically generatedGraphical user interface, text

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, application

Description automatically generated**