CMSC 412 - Fall 2010
William Arbaugh
10/27/2010

LAB 4 - "NOTHING" DRIVER

Introduction

The purpose of this lab is to introduce you to writing Windows drivers. You can think of a driver as a kernel extension. The code runs in ring 0, and you have full and complete access to all of the objects within the kernel. Typically, there are two types of drivers. Drivers that interact with an IO device, and those that do not. This, and the follow-on labs, focuses solely on drivers that do not interact with a hardware device.

We will no longer be using the WRK virtual machine. From now on, your development machine will be Windows XP, and your target will be Windows XP. The first part of this lab will walk you through setting up your development environment. The teaching assistants will assist you with this process in the class discussion sections.

Development Environment Set-up

You'll be using your current XP VM as both the target and host for the remainder of the semester. Follow these steps to set-up your environment:

1. Ensure your current XP machine is turned off and not in a suspended state.

2. Make a copy on your local file system of your XP virtual machine. You'll now have two instances of an XP virtual machine on your file system.

3. Arbitrarily select one machine as your target machine and the other will be your development machine. Alternatively, you can use your native host XP or Win7 version NOTE: You might want to change the name of the machines to "Target" and "Dev Host" so you don't get confused down the road.

4. Start-up your "Dev Host" machine, and download and install the latest DDK from http://www.microsoft.com/downloads/en/details.aspx?FamilyID=36A2630F-5D56-43B5-B996-7633F2EC14FF&displaylang=en

5. Star-up your your target XP host and ensure that windbg can connect to the target as we did with with the WRK VM.

Nothing driver

The "nothing driver" is a driver that does "nothing". It's sole purpose is to show you the bare minimums required for a Windows driver. The "nothing" driver is provided by Open Systems Resources (OSR) for academic purposes only.

The "nothing" driver will be provided to you during the discussion sections on October 28th.

Complete the following tasks for successful completion of Lab 4:

1. Build the nothing driver and load it using the OSR loader utility found at http://www.osronline.com/article.cfm?article=157.

2. Modify your driver to print out a statement to debugger in DriverEntry() function.

Submission

Submit a transcript of your debug output and the modified "nothing" driver.

Grading

Grading is based on your debugger output matching your source file.