CS490 Windows Internals

Lab Setup Guide

The tools referenced in the labs are from the following sources:

- Windows Support Tools
- Windows Resource Kit Tools
- Windows Debugging Tools
- Kernrate (only needed for Unit 3)
- Freeware tools from www.sysinternals.com

For a general description of these tool sources and their use for exploring Windows OS internals, see *Windows Internals, 5th edition* pp. 24-31.

HARDWARE REQUIREMENTS:

- Any supported Windows 2000, Windows XP, or Windows Server 2003 system
- Disk space: at least 1GB free after installation

ACCOUNT REQUIREMENTS:

Some of the labs require local administrator rights: specifically, any lab using Windbg for performing local kernel debugging as well as labs using Filemon and Regmon from Sysinternals.com.

INSTALLATION STEPS:

1. Install Windows Support Tools

   To install: run \support\tools\setup.exe from the Windows CD
   (make sure to install the Support Tools that matches the OS you are running on, e.g. XP Support Tools for XP, etc)

2. Install Windows Server 2003 Resource Kit Tools

http://www.microsoft.com/downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd&DisplayLang=en

© 2005-2010 David A. Solomon, Mark Russinovich and Kenny Zhu

3. Install Debugging Tools for Windows

http://www.microsoft.com/whdc/ddk/debugging

You may need to install Microsoft .NET framework version 4.0 from http://www.microsoft.com/downloads/en/details.aspx?FamilyID=9cfb2d51-5ff4-4491-b0e5-b386f32c0992&displaylang=en before installing the debugging tools. Configure symbols (required for kernel debugging) as explained on the "Getting Started" page, available from the above web page. If the symbol server doesn't work, you may download the symbol package for your version of Windows directly from http://www.microsoft.com/whdc/devtools/debugging/symbolpkg.mspx . For additional information, see *Windows Internals, 5th edition* pp. 26-31.

4. Install Sysinternals tools

The CRK refers to a number of tools from www.sysinternals.com. A zip file with the tools as they existed at the time of the CRK release is available for download from the MSDN Curriculum Repository from http://www.msdnaacr.net/curriculum/pfvro.aspx?ID=6202 (the recommended folder to unzip to is c:\sysint).

However, the latest version of the Sysinternals tools (which may include bug fixes and enhancements) are available individually from www.sysinternals.com. You can choose whether to download the latest version of the tools needed for labs or use the older versions in the zip file.

This zip file also contains a few tools from the Windows 2000 Resource Kit that are no longer included with the Windows Server 2003 Resouce Kit that are referred to in some labs. These tools are in the \sysint\reskit subfolder in the zip file.

5. One lab requires the use of Kernrate (a kernel profiling tool):

http://www.microsoft.com/whdc/system/sysperf/krview.mspx

© 2005-2010 David A. Solomon, Mark Russinovich and Kenny Zhu