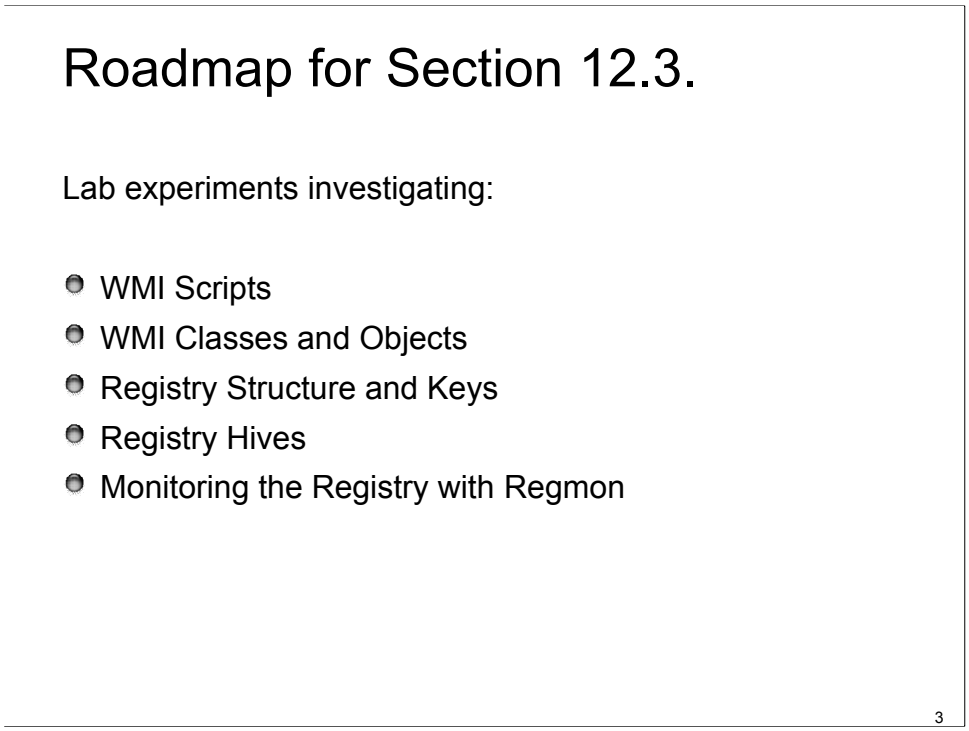
Unit OS12: Scripting

12.3. Lab Manual

Copyright Notice

- These materials are part of the *Windows Operating System Internals Curriculum Development Kit,* developed by David A. Solomon and Mark E. Russinovich with Andreas Polze
- Microsoft has licensed these materials from David Solomon Expert Seminars, Inc. for distribution to academic organizations solely for use in academic environments (and not for commercial use)

2



This LabManual includes experiments investigating the the mangement and scripting mechanisms and concepts implemented inside the Windows operating system. Students are expected to carry out Labs in addition to studying the learning materials in Unit OS12.

A thorough understanding of the concepts presented in Unit OS12: Scripting is a prerequisite for these Labs.

Lab: Using Example WMI Scripts

- List running processes with Resource Kit "ps.vbs"
- List services with "service.vbs"
- Extra credit:
  - Go to the Technet Scripting Center and pick a script
  - Copy and paste it into Notepad and save it as testscript.vbs
  - Run the script

4

Lab objective: Using WMI Scripts to Manage Systems

A powerful aspect of WMI is its support for scripting languages. Microsoft has generated hundreds of scripts that perform common administrative tasks for managing user accounts, files, the registry, processes, and hardware devices. While some scripts ship in the Windows Resource Kits, the Microsoft TechNet Scripting Center Web site serves as the central location for Microsoft scripts. Using a script from the scripting center is as easy as copying its text from your Internet browser, storing it in a file with with a .vbs extension, and running it with the command cscript script.vbs, where "script" is the name you gave the script. Cscript is the command-line interface to Windows Script Host (WSH).

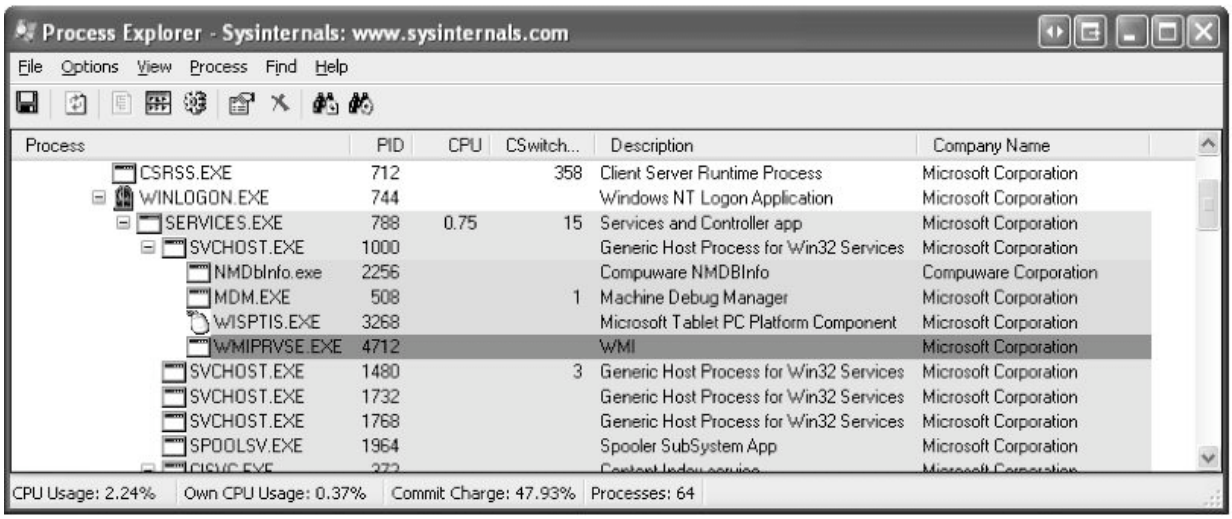
Lab: WMI Jobs

- Run Process Explorer and select Options|Highlight Jobs
- Run Psinfo.exe or wmic.exe
  - Uses WMI to query XP/Server 2003 Product Activation
- Note the child of a Svchost that appears
  - Find the service in the Svchost
  - View the properties of the Job object in the Properties tab of the child process

5

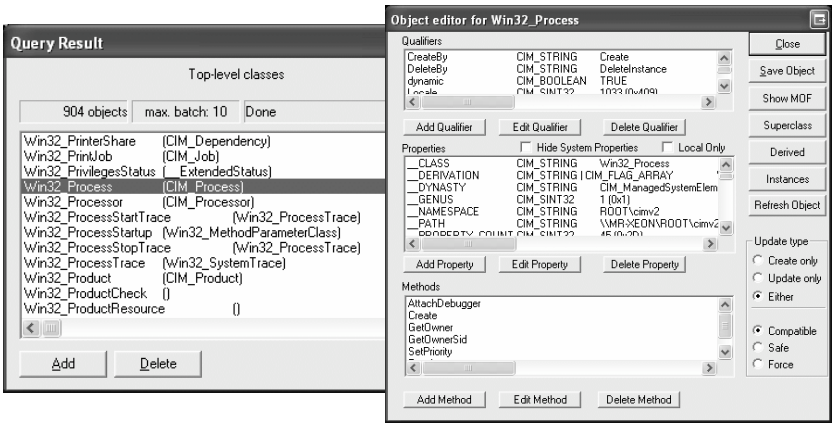
Lab objective: Viewing Wmiprvse Creation

You can see Wmiprvse being created by running Process Explorer from www.sysinternals.com and executing Wmic. A Wmiprvse process will appear beneath the Svchost process that hosts the RPC service. If Process Explorer job highlighting is enabled, it will appear with the job highlight color because, to prevent a runaway provider from consuming all virtual memory resources on a system, Wmiprvse executes in a job object that limits the number of child processes it can create and the amount of virtual memory each process and all the processes of the job can allocate.



Lab: Viewing WMI Classes

- Use WBEMTEST (included with Windows 2000 and higher)
  - Connect to root\cimv2
  - Select Enum Classes and check Recursive
  - Then double-click on one to view its defined properties



6

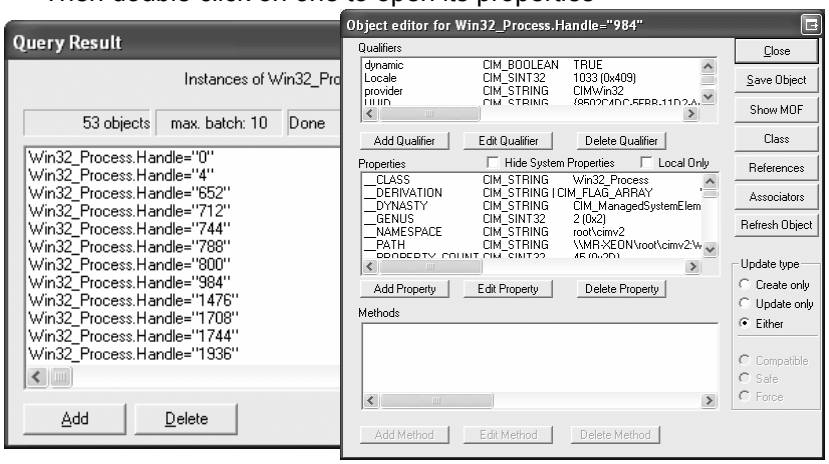
Lab objective: Viewing the MOF Definitions of WMI Classes

You can view the MOF definition for any WMI class by using the WbemTest tool that comes with Windows. In this experiment, we'll look at the MOF definition for the Win32_NTEventLogFile class:

1. Run Wbemtest from the Start menu's Run dialog box.
2. Click the Connect button, change the Namespace to root\cimv2, and connect.
3. Select Enum Classes, select the Recursive option button, and then click OK.
4. Find Win32_NTEventLogFile in the list classes, and double-click it to see its class properties.
5. Click the Show MOF button to open a window that displays the MOF text.

Lab: Viewing WMI Objects

- Double click on any class from the class list and click Instances
- Then double click on one to open its properties



7

Lab objective: Viewing WMI Objects

You can view the active instances of any WMI class by using the WbemTest tool that comes with Windows.

Run Wbemtest from the Start menu's Run dialog box.

1. Click the Connect button, change the Namespace to root\cimv2, and connect.
2. Select Enum Classes, select the Recursive option button, and then click OK.
3. Double click on any class in the class list and click the Instances button see its instances.
4. Double click on one particular instance to open window that displays its properties.

Lab: Fun with the Hardware Key

- Open Regedit and navigate to HKLM\Hardware\Description\System\CentralProcessor\0
- Change ProcessorNameString to “Cray Supercomputer 10,000GHz”
- Right-click on My Computer and view Properties

8

Lab objective: Fun with the Hardware Key

You can fool your coworkers or friends into thinking that you have the latest and greatest processor by modifying the value of the ProcessorNameString value under HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0. The System applet of the control panel displays the ProcessorNameString value on the General page. Changes you make to other values in that key, such as the ~MHz, do not have any affect on what the System applet displays, however, because the system caches many of the values for use by functions that applications use to query the system’s processor capabilities.

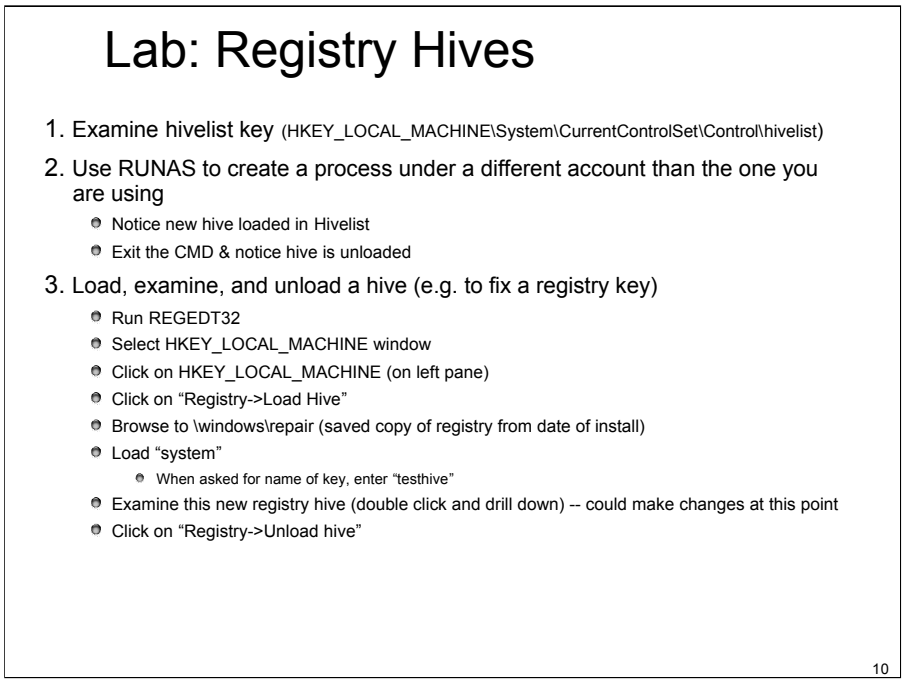
Lab: Viewing the List of Profiles Stored on a Computer

- Open Regedit and navigate to HKLM\Software\Microsoft\ Windows NT\CurrentVersion\ProfileList
- Examine the list of profiles stored on the system
  - Find the LOCAL_SERVICE and NETWORK_SERVICE profiles
  - Find your own profile information
- View the corresponding list in Control Panel-> System->Advanced->Settings in the User Profile section

9

Lab objective: Watching Profile Loading and Unloading

You can see a profile load into the registry and then unload by using the Runas command to launch a process in an account that's not currently logged on to the machine. While the new process is running, run Regedit and note the loaded profile key under HKEY_USERS. After terminating the process, perform a refresh in Regedit by pressing the F5 key and the profile should no longer be present.



Lab objective: Manually Loading and Unloading Hives

Regedt32 on Windows 2000 and Regedit on Windows XP and Windows Server 2003 have the ability to load hives that you can access through its File menu. This capability can be useful in troubleshooting scenarios where you want to view or edit a hive from an unbootable system or a backup medium.

In this experiment, you'll use Regedt32 (if you're running Windows 2000) or Regedit (if you're running Windows XP and Windows Server 2003) to load a version of the HKLM\SYSTEM hive that Windows Setup creates and stores in \Windows\Repair during the install process.

1. Hives can be loaded only underneath HKLM or HKU, so open Regedit or Regedt32, select HKLM, and choose Load Hive from the Regedit File menu or the Regedt32 Registry menu.
2. Navigate to the \Windows\Repair directory in the Load Hive dialog box, select System.bak, and open it. When prompted, enter Test as the name of the key under which it will load.
3. Open the newly created HKLM\Test key, and explore the contents of the hive.
4. Open HKLM\System\CurrentControlSet\Control\Hivelist, and locate the entry \Registry\Machine\Test, which demonstrates how the configuration manager lists loaded hives in the HiveList key.
5. Select HKLM\Test, and choose Unload Hive from the Regedit File menu or the Regedt32 Registry menu to unload the hive.

Regmon Lab

1. Run Notepad
2. Change Font and point size
3. Enable Word wrap
4. Run Regmon & filter to Notepad.exe
5. Exit Notepad
6. In Regmon log, find location of user-specific Notepad settings
7. Double click on a line to jump to Regedit
8. Delete top level Notepad user settings key
9. Re-run Notepad and confirm font and word wrap reset to default setting

11

Lab objective: Using Regmon to Locate Application Registry Settings

In some troubleshooting scenarios, you might need to determine where in the registry the system or an application stores particular settings. This experiment has you use Regmon to discover the location of Notepad's settings. Notepad, like most Windows applications, saves user preferences—such as word-wrap mode, font and font size, and window position—across executions. By having Regmon watching when Notepad reads or writes its settings, you can identify the registry key in which the settings are stored. Here are the steps for doing this:

1. Have Notepad save a setting that you can easily search for in a Regmon trace. You can do this by running Notepad, setting the font to Times New Roman, and then exiting Notepad.
2. Run Regmon. Open the highlighting filter dialog box and enter notepad.exe in the Include filter. This will have Regmon log only activity that has notepad.exe in either the Process or Path columns.
3. Run Notepad again, and after it has launched stop Regmon's event capture by toggling Capture Events in the Regmon File menu.
4. Scroll to the top line of the resultant log and select it.
5. Press Ctrl+F to open a Find dialog box, and search for times new. Regmon should highlight a line like the one shown in the following graphic that represents Notepad reading the font value from the Registry. Other operations in the immediate vicinity should relate to other Notepad settings.
6. Finally, double-click the highlighted line. Regmon will execute Regedit (if it's not already running) and cause it to navigate to and select the Notepad referenced registry value.