Course 40076A:

MVA Workshop: Troubleshooting Windows Systems with SysInternals Tools

Course Outline

Module 1: Introducing the Sysinternals Tools for Windows Client

This unit provides a brief introduction to the Sysinternals Suite of tools and allows students to download and configure the tools for use in subsequent labs.

Lab : Preparing for the Labs

- After completing this unit, students will be able to:
- Download, configure, and run the Sysinternals tools.
- Disable the security warning.
- Explore the Sysinternals tools that they will be using in this workshop.

Module 2: Understanding Windows Core Concepts

This unit covers basic Windows Internals concepts such as memory management and how threads and processes interact. Students use tools such as Process Explorer, Performance Manager, and Task Manager to explore the various data structures discussed in this unit.

Lab : Making Visible the Invisible

After completing this unit, students will be able to:

- Use Process Explorer v16.04 to view the relationship between the parent and child processes.
- Use Performance Monitor v3.1 and Task Manager to examine processes.
- Use Process Explorer to examine threads and context switching.

Module 3: Exploring Process Explorer

This unit provides students with a closer look at Process Explorer. In the lab, students have the opportunity to work with Process Explorer to obtain information such as the program that has a particular file or folder open and the associated dynamic-link libraries (DLLs) that the processes have opened or loaded.

Lab : Working with Process Explorer

After completing this unit, students will be able to:

- Use Process Explorer v16.04 as the default program for viewing process information.
- View DLLs and handles to open processes.
- Map a system thread to a device driver.
- View and adjust thread priorities.

Module 4: Process Monitor

This unit introduces Process Monitor for performing real-time monitoring of the file system, registry, and process and thread activity. Students will learn how to use Process Monitor to help troubleshoot Windows devices and find related diagnostic information.

Lab : Working with Process Monitor

After completing this unit, students will be able to:

- Examine how the Windows operating system loader searches for dynamic-link libraries (DLLs).
- Locate application registry settings.
- Trace the startup of a process.
- Trace how Internet Explorer uses Windows integrity mechanisms.
- View software restriction policy (SRP) enforcement.

Module 5: PsTools

This unit introduces some of the commonly used PsTools command-line utilities that can be used to manage remote and local computers. In the lab, students will use PsTools to obtain information about system components, folder permissions, number of processors, and disk volumes. They will also use PsTools to terminate processes and to translate machine and user account names to their security identifiers (SIDs).

Lab : Working with PsTools

After completing this unit, students will be able to:

- Find system information interactively across local or remote systems by using PsExec.
- Obtain information about folder permissions by using Accesschk.
- Obtain information about system components, number of processors, and disk volumes by using PsInfo.
- Use PsKill to terminate a process.
- Translate machine and user account names to their equivalent security identifiers (SIDs).

Module 6: Autoruns

This unit focuses on the enhanced Task Manager in Windows 8.1 and Autoruns, which is one of the Sysinternals tools. These tools help in identifying the apps and services that start automatically when a computer starts.

Lab : Managing Autostart Apps

After completing this unit, students will be able to:

- Examine autostart processes.
- Add an app to the autostart process.
- Remove an app from the autostart process.
- Use Autoruns to manage autostarts.