Course Outline

Troubleshooting Windows Infrastructure-From Zero to Hero

Duration: 3 days

Introduction

This is a deep dive course on infrastructure monitoring! We would like to say, "Finally!" It took a long time to prepare good examples, tools and scenarios for you! Regular monitoring ensures that you always have up-to-date knowledge about how particular components of your infrastructure operate.

The most important thing in monitoring is to work out the baseline that can be a good reference to identify problems and to analyze some specific conditions of infrastructure components to operate. In vast majority of cases operating system troubleshooting involves monitoring, from analysis of the boot process to network performance or even particular processes. During the course you will become familiar with great monitoring tools and their efficient usage and several techniques for monitoring infrastructure components and their particular working phases.

The course covers the following operating systems: Windows 7, Windows 8/8.1, Windows Server 2008 R2, Windows Server 2012/R2.

Paula Januszkiewicz is the world-known Security Expert. Loves to perform Penetration Tests, IT is a word-- renowned Security Expert. Paula loves to perform Penetration Tests, IT Security Audits, and after all she says: 'harden'em all'! Enterprise Security MVP and trainer (MCT) and Microsoft Security Trusted Advisor.
Paula says: You will not find better course on troubleshooting Windows But be careful – it is a real deep-- dive. After this course you will understand mechanisms that affect potential issues. Be prepared for the great tracing examples and issues to be solved!

Target Audience:

- Enterprise administrators
- Infrastructure architects
- Security professionals
- Systems engineers
- Network administrators,
- IT Professionals
- Security consultants and other people responsible for implementing network and perimeter security.

Pre-requisites

To attend this training you should have good hands-on experience in administering Windows infrastructure. At least 8 years in the field is recommended. You should have good understanding of how operating system works. Ideally you should have read "Windows Internals" by Mark Russinovich book.

Topics Covered:

- Module 1: Virtualization performance analysis

  This module allows students to understand how virtualization impacts performance. Exercises contain usage of tools and making business related decisions based on the measurements. Training cover optimization techniques for known hypervisors.

- Module 2: Operating system monitoring

  This module covers generic system monitoring to learn the basics of monitoring. It is a great introduction to go further with detailed monitoring.

- Module 3: Advanced Memory Analysis

  This module explains to students what is happening in the memory, how it works, how to get into it and how to monitor it. Students except for memory analysis will practice debugging memory dumps.

- Module 4: Advanced disk performance analysis

  Within this module students will become familiar with disk performance monitoring – starting with RAIDs, ending up with cluster configuration techniques. For some server roles cluster size really matters, so that administrators can achieve the best performance in specific infrastructure configuration.

- Module 5: Xperf and usage scenarios

  Several tools allow to get very detailed information about the system performance. This is needed when you have to figure out these delicate problems that slow servers down. Students in this module gain knowledge about how to monitor several operating system components and how to cope with the everyday situations like: processor usage, disk usage, memory usage, network activity, slow booting and other.

- Module 6: Kernel Mode and User Mode monitoring techniques

  From the continuity perspective blue screen is always an unpleasant experience. From the debugging perspective – we have just been protected from malicious things that could have happen to operating system integrity. Blue screen is positive in its own way – it helps to intricate who caused the problem, it needs to be analyzed though. Within this module students will become familiar with kernel mode and user mode techniques and tools.

- Module 7: Network monitoring

  Starting from simple network sniffing, ending up with advanced network monitoring to the size of the buffers written. Several techniques used during the training