Windows Internals Specialist - Intermediate Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

The Windows Internals Specialist (Intermediate) course is a comprehensive five-day programme designed to deepen your understanding of the core components and operation of the Windows operating system. By mastering advanced debugging, memory management, and system architecture, you will develop the skills needed to troubleshoot complex issues and optimise system performance. This course builds on foundational knowledge to provide a detailed exploration of Windows OS internals, equipping learners to apply advanced debugging tools, analyse system behaviour, and improve security posture.

Prerequisites

- A solid understanding of Windows OS fundamentals
- Experience with debugging tools and basic system architecture
- Knowledge of core programming concepts (C, C++) is recommended but not essential

Target Audience

This course is designed for:

- System administrators and engineers responsible for managing Windows-based environments
- Security professionals aiming to improve system security through a deeper understanding of Windows internals
- Developers interested in enhancing their debugging and troubleshooting skills
- IT professionals working in complex technical environments that require Windows optimisation

What You Will Learn

By the end of this course, participants will:

- Understand and work with advanced Windows OS concepts such as memory protection models, hypervisor, and runtime execution.
- Utilise Windows debugging tools for local and remote analysis.
- Master the design and implementation of critical Windows OS components such as the Object Manager, Process and Thread Management, and Memory Management.
- Gain insight into the security framework within Windows, focusing on authentication, authorisation, and AppContainers.
- Apply knowledge of Windows internals to troubleshoot, optimise, and secure Windows-based systems effectively.

Windows Internals Specialist - Intermediate Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Outline

Introduction to Windows Internals

- Overview of Windows OS design
- Key system components and their functions

Windows Debugging Tools

- Introduction to local and network debugging
- Utilising commands and extension commands

OS Design and Architecture

- Memory protection model and hypervisor security
- Understanding runtime execution and access control models
- Sessions, objects, and handles in Windows

Hardware Architecture

- Processor support, system calls, and interrupt processing
- Working with timers and APCs for efficient system management

Process and Thread Management

- Visualising processes and threads using system tools
- Job management, thread scheduling, and priority boosting
- Debugging and optimising processes and threads

Memory Management

- Memory manager components, paging, and virtual-to-physical address translation
- Managing process and system memory usage
- Working with memory-mapped files and shared memory

System Mechanisms

- WoW64 subsystem and limitations
- Object Manager and boot processes in Windows
- Session management and isolation

Security Framework

- Overview of Windows security components
- Authentication and authorisation processes
- Managing AppContainers and improving system security

I/O Systems

- Windows driver model and driver communication
- Analysing driver routines and their roles in system performance