Windows Internals Specialist - Advanced Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

This five-day advanced-level course provides in-depth knowledge and skills for professionals seeking to master Windows Internals. Focusing on system architecture, security mechanisms, debugging, and memory management, the course equips learners with the tools to solve complex issues and optimise Windows operating system performance.

Prerequisites

- Strong understanding of Windows operating systems.
- Experience in system administration or development roles.
- Familiarity with debugging tools and basic internal processes of Windows is recommended.

Target audience

- IT professionals specialising in system administration or software development.
- Security professionals working on Windows platform hardening.
- Developers working with Windows internals, driver development, or debugging.

What You Will Learn

By the end of this course, participants will be able to:

- Understand the Windows architecture, including the OS and CPU interactions.
- Use advanced Windows debugging tools to diagnose and fix issues.
- Apply system security features and mitigations effectively.
- Optimise memory and process management in Windows environments.

Windows Internals Specialist - Advanced Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Outline

Introduction and debugging tools

- Introduction to Windows Internals.
- Advanced debugging tools:
  - Local and network debugging.
  - Debugger Data Model (NatVis, LINQ, Synthetic Variables).
  - Using JavaScript extensions and scripts.
  - Overview of WinDbg Preview and Time Travel Debugging.

OS and CPU architecture

- OS segmentation and hardware architecture.
- Hardware mitigations:
  - SMEP, SMAP, NPIEP, RUM, MBEC, CET.
  - Side channel mitigation techniques.
- Security enhancements in Kernel and User Mode.
- Vendor security features and tamper evidence.

Executive mechanisms

- Object Manager: structure and mitigations.
- Advanced Local Procedure Call (LPC, ALPC) mechanisms.
- Notification mechanisms and registry management.

Advanced processes and threads

- Process isolation techniques and secure processes.
- Image Loader and process mitigations.
- In-depth exploration of silos and secure processes.

Memory management and forensics

- Virtual and physical memory analysis techniques.
  - Mitigations like ASLR and KASLR.
  - Memory partitioning and address translation.
- Forensic techniques to trace memory management vulnerabilities.