Windows Internals Fundamentals

Abstract

The Windows OS is the most used in organizations around the world. Protecting a Windows system, as well as identifying malicious activity requires a good understanding of its architecture and mechanisms.

This bootcamp will take the security professional on a journey to the Windows kernel and other system components, revealing their operations and mechanisms. Various tools are used – built-in Windows tools, the Sysinternals tools, WinDbg, and tools written by the instructor.

By the end of the bootcamp, you'll feel comfortable analyzing Windows behavior with a deep understanding of its major mechanisms.

Sessions

Session 1: System Architecture

- Windows Versions
- Tools
- Processes
- Virtual Memory
- Threads
- User mode vs. Kernel mode
- System Architecture
- User/Kernel Transitions

Session 2: Processes & Jobs

- Creating and terminating processes
- The loader
- DLL explicit and implicit linking
- Protected processes and PPL
- UWP Processes
- Minimal and Pico processes
- Jobs

Session 3: Kernel Mechanisms

- Object Management
- Objects and Handles
- Synchronization
- (Some) Synchronization Primitives
- Wow64
- Windows Global Flags

Session 4: Memory Management

- Overview
- Page States
- Memory APIs

- Heaps
- Memory Mapped Files

Session 5: I/O System

- I/O System overview
- Device Drivers
- Plug & Play
- I/O Processing and Data Flow
- IRPs

Session 6: Security

- Virtualization Based Security
- Security components
- Credential guard
- User Access Control (UAC)
- Integrity Levels
- Protecting objects
- SIDs
- Tokens
- Privileges
- Access checking