Syllabus: Windows internals master

About TrainSec Academy

TrainSec is an online learning hub for current and aspiring cybersecurity pros who understand the need for excellence. Level up or change career using skill-expanding modular learning way. We turn beginners into experts and experts into masters. TrainSec is designed for those who are serious about being at the vanguard of the latest knowledge, skills and trends. We're already working with the best.

Course Overview

The Windows Internals Master path provides the essential knowledge, skills, and tools to become a proficient Windows researcher and developer. Through a combination of theoretical concepts and hands-on exercises, participants will learn how the Windows kernel works, how OS components interact, and how to apply this knowledge for debugging, research, and development.

Course Objectives

By completing this course, you will be able to:

- Understand Windows architecture and its executive components.
- Analyze the workings of kernel objects and user-mode components.
- Debug applications and drivers using WinDbg.
- Use Sysinternals tools for system analysis.
- Understand x86/x64 processor features as utilized by Windows.

Course Format

- **URL**: https://trainsec.net/windows-internals-master/
- **Scope and Mode**: 400+ learning materials, spanning over 70+ hours of online videos and presentations.
- **Format**: Pre-recorded videos, presentations, interactive labs, discussion groups, and personal trainer support.
- **Pace**: Self-paced.
- **Platform**: TrainSec.net Learning Platform and Discord server.

Course Content

Windows Internals: Day 1 *(34 lessons)*

This course provides the fundamental knowledge of Windows concepts and architecture, including processes, threads, virtual memory, system calls, DLLs, handles, and objects. This will serve as a good foundation for the following courses, which focus on programming.

Windows Internals: Day 2 *(49 lessons)*

This course continues where Day 1 left off, digging deeper into processes – process creation and destruction, types of processes, and more. Job objects are also described, including their extension called Silos that is the basis of Windows container implementation. Finally, threads are discussed, including scheduling and management.

Windows Internals: Day 3 *(49 lessons)*

This course deals with various kernel mechanisms. From interrupts and exceptions, through thread synchronization, NT global flags, Event Tracing for Windows, and finally Wow64.

Windows Internals: Day 4 *(31 lessons)*

This course deals with memory management. From process virtual memory page states and protection to virtual address translation performed by the CPU, to the various user-mode and kernel-mode APIs as they relate to memory.

Windows Internals: Day 5 *(48 lessons)*

The last “day” in the Windows Internals series deals with two topics. The I/O system is described, including the use of device drivers and their integration into the system as a whole. Then, many security mechanisms are discussed, from access tokens and security descriptors to access checks and integrity levels, among others.

x64 Architecture and Programming (Part 1) *(81 lessons)*

This course teaches the basics of the x86/x64 assembly language from the ground up. It focuses on integrating it into C/C++ applications but also shows how to write standalone applications with assembly only.

x64 Architecture and Programming (Part 2) *(41 lessons)*

Picking up where Part 1 left off, this course dives into the architecture of modern x64 processors, describing their mode of operations, focusing on those used by modern operating systems like Windows, while describing the various mechanisms of the processor used on Windows, such as system calls, interrupts, and more.

Mastering WinDbg *(67 lessons)*

This course dives into the WinDbg debugger and how to effectively use it in user-mode and kernel-mode debugging, as well as the analysis of kernel-mode dump files.

Sysinternals Tools Deep Div e (Part 1) *(34 lessons)*

The Sysinternals tools are powerful and free tools that provide deep insight into Windows. This course dives deeper into the following tools while discussing Windows Internals details: Process Explorer, WinObj, DebugView, VMMap, CPU Stress, Not My Fault, and LiveKd.

Required Materials

- **Prerequisites**: Experience with C programming, power-user level knowledge of Windows, and basic OS concepts.
- **Tools: WinDbg, Sysinternals Suite, Visual Studio.**
- **Additional Resources:** https://discord.com/invite/qugcNyWdaU

Instructor Information

- **Name**: Pavel Yosifovich
- **Title**: Windows Internals Expert
- **Bio**: Software developer, trainer, and author. Co-author of "Windows Internals" 7th edition (2017), and author of "Windows Kernel Programming, 2nd ed" (2023).
- **Social Handle**: @zodiacon

Contact & Support

For any course-related or billing-related inquiries, please contact info@trainsec.net