

Syllabus: Windows Master Developer

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. We turn beginners into experts and experts into masters. TrainSec is designed for those who are serious about being at the forefront of the latest knowledge, skills and trends. We're already working with the best.

Course Overview

The Windows Master developer path takes you from a “generic” C programmer to a master Windows programmer in user mode and kernel mode.

Course Objectives

By completing this course, you will learn:

- Windows architecture and main components.
- Working with the Windows API.
- Building COM servers and clients.
- Windows Kernel fundamentals.
- Writing kernel mode drivers.
- User and kernel Debugging with WinDbg.

Course Format

- URL: <https://trainsec.net/windows-master-developer-2/>
- Scope and Mode: 384 Learning materials, spanning on 90+ hours of online videos and presentations.
- Format: Pre-recorded Videos and Presentations, discussion group and personal trainer support.
- Pace: Self-paced
- Platform: TrainSec.net Learning Platform, Discord server.

Course Content

Building low level applications, services, and components requires a good understanding of the inner workings of Windows and its fundamental objects and capabilities, such as processes, threads, virtual memory, DLLs, synchronization, and



much more. Using these foundations, the next requirement is an intimate knowledge of the many parts of the Windows API, which is the primary way to accomplish things on Windows. Going deeper into the kernel requires an even deeper understanding of some kernel mechanisms that are utilised when writing kernel mode drivers, in addition to the kernel API itself. By the end of this path, you'll have mastered the user mode and kernel mode APIs and have the knowledge and confidence to tackle any low level Windows development project.

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 System Programming 1 - 48 lessons

This course begins the journey of user mode development, covering the basics of the Windows API. It digs deeper into handles and objects and their APIs, and working with processes.

Windows System Programming 2 - 64 lessons

Continuing from where “Windows System Programming 1” left off, the course deals with job objects, using threads effectively, file I/O APIs, and working with virtual memory.

Windows System Programming 3 - 46 lessons

Continuing from where “Windows System Programming 2” left off, the course looks into building and consuming Dynamic Link Libraries (DLLs), and Windows security APIs. Finally, an introduction to the Component Object Model (COM) is provided. COM is dealt with in greater details in the next two courses.

COM Programming 1 - 58 lessons

COM has been around since 1993 and is still used everywhere in Windows. This course explores the foundations and motivation for of COM, writing COM servers and clients, and includes working with the Active Template Library (ATL) as a helper library for working with COM.

COM Programming 2 - 36 lessons

This course continues the COM journey by describing how to use COM automation accessible from scripting environments, how to build COM EXE servers, and finally the somewhat tricky topic of COM threading and apartments.

Windows Kernel Programming 1 - 74 lessons

The course provides the foundation for writing kernel mode drivers on Windows. The drivers covered are the so called “software drivers” – these don’t interact with hardware – instead interacting with Windows by performing operations not possible to do from user mode, or registering for kernel notifications related to processes, threads, Registry and more.

Windows Kernel Programming 2 - 24 lessons

Continuing from “Windows Kernel Programming 1”, the course teaches the basics of file system min-filters, and covers some other interesting kernel driver techniques.

Required Materials

- Prerequisites: Experience working with the C programming language, User level working knowledge of Windows, Basic familiarity with general OS concepts, Basic knowledge of C++ (Recommended), Basic familiarity with Visual Studio (Recommended).
- Software/Tools: IDA PRO or Ghidra (will be covered during the course).
- Additional Resources: <https://discord.com/invite/qugcNyWdaU>

Instructor Information

- Name: Pavel Yosifovich
- Email: pavel@TrainSec.net
- Trainers Biography:
Pavel: Software developer, trainer, consultant, author, and speaker. Co-author of “*Windows Internals*” 7th edition (2017). Author of “*Windows Kernel Programming, 2nd ed*” (2023), “*Windows 10 System Programming Part 1*” (2020) and Part 2 (2021), and “*Windows Native API Programming*” (2024).

Contact & Support

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