Syllabus: Windows Security Researcher

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 Security Researcher path provides the necessary knowledge, understanding, and tools to be a successful Windows OS researcher, malware analyst and reverse engineer.

Course Objectives

By completing this course, you will be able to:

- Windows architecture and main components.
- Processes, threads, memory, DLLs and their interconnection.
- Windows security mechanisms and features.
- x86/x64 architecture and assembly language.
- Malware Analysis and Reverse Engineering.

Course Format

- **URL**: https://TrainSec.net/windows-security-researcher/
- **Scope and Mode**: 385 Learning materials, spanning on 68 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

Windows is the most used OS in the world, and thus is a favoured target of malicious actors. Researching and finding OS vulnerabilities, dissecting viruses, worms, and other malicious entities is critically important in today's security landscape. This

path provides the necessary knowledge and understanding to allow research and reverse engineering of the OS and malicious payloads.

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 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 whole. Then many security mechanisms are discussed, from access tokens, 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 stand alone applications with assembly only.

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.

trainsec
where pros train pros.

Malware Analyst Professional – Level 1

56 lessons

In this malware analysis and reverse engineering course, you will delve into the inner core of dissecting different malware types and variants, understand the adversarial mindset behind them and the used TTPs. At the end of the course, you will gain the power and knowledge to win against any malware coming your way.

Malware Analyst Professional – Level 2

50 lessons

In this level 2 course, we will continue to dive into the profound and inner levels of the art of malware dissection and reverse engineering. You will learn about advanced malware evasion, privilege escalation, lateral movement, process injection and hooking techniques, shellcode analysis, advanced static and dynamic analysis techniques while analysing sophisticated ransomware, info stealers and spyware families.

Required Materials

- **Prerequisites**: Basic knowledge in reading C and basics in C++, Power user level working knowledge of Windows, Basic familiarity with general OS concepts.
- **Software/Tools**: IDA PRO or Ghidra (will be covered during the course).
- **Additional Resources**: https://discord.com/invite/qugcNyWdaU

Instructor Information

- **Name**: Uriel Kosayev, Pavel Yosifovich
- **Email**: uriel@TrainSec.net, pavel@TrainSec.net
- **Trainers Biography**:
  Uriel: Security researcher, consultant, and the author of the "*Antivirus Bypass Techniques book"* who lives both on the offensive and defensive fronts. Passionate about malware research, and red teaming while providing real-world security solutions.
  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).

Contact & Support

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