TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Insight into Windows Internals

Date of the online training: **March 22-23, 2021**

Overview

This training delivers basic knowledge on the core components and inner working principles of the Windows 10 operating system (e.g., objects, handles, memory management functionalities). It includes hands-on exercises for the analysis of the implementation and operation of these components. This training covers topics that are essential for conducting reverse-engineering, debugging, and other analysis tasks in the context of Windows.

This training focuses on the traditional (non-virtualized) architecture of Windows 10. However, it also takes into account virtualization as a factor driving a major change in the architecture of Windows systems, first introduced in Windows 10.

The training covers topics that are essential for conducting reverse-engineering, debugging, and other analysis tasks in the context of Windows.

ERNW Enno Rey Netzwerke GmbH
Carl-Bosch-Str. 4
69115 Heidelberg
info@ernw.de

Tel. +49 – 6221 – 48 03 90
Fax +49 – 6221 – 41 90 08
BIC: GENODE61HD3
IBAN: DE43 6729 0100 0059 7891 04

Managing Directors
Florian Grunow
Michael Schaefer
VAT-ID: DE 813 376 919

Agenda

Introduction to the Windows debugger (WinDbg): this includes exercising a variety of debugging scenarios, such as early-boot debugging, kernel-mode debugging, and user-mode debugging

- Overview and analysis of the core components of Windows, deployed in kernel- and user-land
- Traditional Windows architecture
- Objects
- Handles
- Drivers
- Memory management functionalities
- System calls
- Processes and threads
- System services and system support processes
- Virtualized Windows architecture
- Virtual Secure Mode (VSM)
- Hyper-V
- Partitions
- Virtual Trust Levels (VTLs)
- Communication interfaces between partitions

Prerequisites

- Familiarity with Windows and basic knowledge on computer architecture.

Requirements

- Laptop with administrative privileges and VirtualBox installed; the laptop should have more than 8 GB RAM and more than 200 GB free disk space.

About the Trainer

Dr. Aleksandar Milenkoski works as a Security Analyst at ERNW GmbH. From 2011 to 2014 he was employed as a Researcher at the Karlsruhe Institute of Technology (KIT). From 2014 to 2016 he was employed at the University of Würzburg, where he obtained his PhD degree. His doctoral thesis is about evaluating security features of the Windows and Linux operating systems, and various security mechanisms. For his research activities, he was awarded by SPEC (Standard Performance Evaluation Corporation), the Bavarian Foundation for Science, and the University of Würzburg. His current work is focusing on reverse engineering core components of the Windows 10 operating system.

Dominik Phillips works as a Windows System Analyst at ERNW GmbH since 2008. He has participated in numerous analysis and development projects focusing on the internals of Windows. In addition, he regularly holds trainings on analyzing and reverse engineering the architecture, the internal working principles, and the workflow of Windows. His current work is focused on reverse engineering core components of the Windows 10 operating system.

Booking

Recommended online booking of trainings through:

https://troopers.de/tickets/

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German. +49 6221 480390 or info@troopers.de

Booking is also possible offline through your trusted partner:

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / info@hmtrainingsolutions.com

+49 6022 5089999 / www.hmtrainingsolutions.com