TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Insight into Windows Internals

Date of the training: **March 18–19, 2019** in Heidelberg, Germany

Book Now using the voucher code: **TR19_HMTS** and save an additional 5% of the current valid rate of any package!

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 is an applied workshop on Windows internals. It delivers basic knowledge on the core components and inner working principles of the Windows 10 operating system (e.g., objects, handles, memory management functionalities). The training includes hands-on exercises for the analysis of the implementation and operation of these components.

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 Insight GmbH
Carl-Bosch-Str. 4
69115 Heidelberg
BIC: GENODE61HD3

Tel. +49 – 6221 – 48 03 90
Fax +49 – 6221 – 41 90 08
Ust-ID DE 304 445 827
IBAN: DE84 6729 0100 0067 1236 03

Managing Directors:
Enno Rey
Dr. Rainer Schiweck
Kerstin Schröter

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 60 GB free disk space.

About the Speaker: Aleksandar Milenkoski

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.

About the Speaker: Dominik Phillips

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.

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Booking

Recommended Online Booking of Trainings Through:

Sign-Up Form https://troopers.de/tickets/

Voucher code: **TR19_HMTS**

Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code up until March 11th, 2019 or until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German.

Zögern Sie nicht uns zu kontaktieren. Wir sprechen fließend Englisch und Deutsch.

Troopers Organization Team

+49 151 16228365 or info@troopers.de

Booking is also possible offline through your trusted partner from:

HMTS HM Training Solutions

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / info@hmtrainingsolutions.com

+49 6022 5089999 / www.hmtrainingsolutions.com