TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Windows Internals

Date of the training: **June 27-28, 2022** in Heidelberg, Germany

Book now using the voucher code: **TR22_HMTRAINING** and save an additional 5% of the current valid rate of any package!

Overview

This 2-days training is for anyone who wants to know how Windows works, how to understand what is happening behind the stage and how to interface with it effectively. Whether you want to analyze malware, understand (un)-documented stuff in the system, developer or just curious, there is a place for you here.

This training aims to give the audience some knowledge about the Windows operating system and practicing reverse-engineering. On the first hand, the training based on Windows 11 begins with an introduction to how the operating system works with main components, main services, objects architecture, scheduling, memory management, security, programming, etc. We will dive more and more in detail according to the expectations of the group. The course is theoretical but also practical through various small labs to interact with Windows. The objective is to understand what these various elements are used for, how they work internally but also how to interface with them via the Windows API.

On the second hand, we will present the basics of reverse engineering. First, we will recall how a processor works, then we will see the assembly language in order to write some (small) programs. Maybe also the occasion to see some bugs with compilers/debuggers, who knows... At the end, we will practice with various reverse engineering software, namely IDA and Windbg.

In the end, members of the public will have a better knowledge of Windows and more practice in reverse engineering. Knowing how works Windows could help to solve problems that seemed impossible from a system or application perspective in addition to better understand the benefits provided by the operating system or hardware.

It should be noted that this course remains an introduction to each of these fields. It is also possible, depending on the questions and needs (and the possibility to answer them), to modify the course according to the requests the same day.

Day 1 - Introduction

- Introduction to Windows internal
  - General architecture
  - Windows' versions
- Windows basics
  - CPU Protection level
  - Virtual memory & address space layout
- Windows key concepts & components
  - Process, threads, jobs, fiber, UMS…
  - Objects handles and security
  - Windows desktops and sessions
  - Hypervisor, core OS kernel, drivers, HAL, NTDLL, Win32k…
  - Main user mode components/services
- Windows subsystem & API
  - Win32, POSIX, OS/2, WinRT, Pico Process, WSL 1&2
- Some security components
  - SGX enclave, TPM, VBS, VSM, VTL-X
- System calls, kernel/hypervisor
  - Probe/capture
  - Memory paging
  - Processor mode & hooking API
  - Wow64
- Through the day, practice: Mastering Windbg
  - Presentation of Windbg
  - First steps debugging with Windbg
  - More advanced procedures with Windbg

Day 2 - Assembly programming

- First steps with MASM32
- Assembly programming
  - Some history about CPU (optional)
  - Main concepts with assembly programming
  - Registers, stack, sysenter/syscall, segment code, scheduler & thread context
  - Instructions
    - Intel documentation
    - Most useful instructions
  - Writing small programs with MASM and debugging with Windbg
    - From C code to Assembly code (and vice-versa)
    - Calling conventions (cdecl/stdcall/x64)
    - MZ-PE format details
  - Through the day, practice: Reverse engineering
    - Writing small programs in assembly
    - Windbg & assembly programming
    - Use of IDA software

Who should attend this training?

- Students
- Hackers
- Any professionnal interested in Windows/reverse engineering

Requirements

The attendees should have:

- Computer with ability to run a Windows virtual machine (in VirtualBox, VMWare or Hyper-V)
- Ability to install application from Microsoft Store (Windbg Preview)
- Ability to compile/install programs
- Basic knowledge in computer science and programming
- C programming language would be a plus
- Assembly programming language would be a great plus

About the Trainers:

Dr. Baptiste David is an IT security specialist, specialized in Windows operating system. His research is mainly focused on malware analysis, security under windows operating system, networks, kernel development and vulnerabilities. Sometimes math, physic or anything cool from that stuff is perfect for him to enhance everyday life. He although likes good food and good vine (we never change), but he is okay if you offer him beers. He has already made several conferences included: Black Hat USA, Defcon, Zero Night, Cocon, iAwacs, Ground zero summit, EICAR, ECCWS…

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Booking

Recommended online booking of trainings through:
https://troopers.de/tickets/

Voucher code: TR22_HMTRAINING
Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code until seats have run out.

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