TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Windows Instrumentation With Frida

Date of the training: **March 16-17, 2020** in Heidelberg, Germany

Book now using the voucher code: **TR20_HMTS** and save an additional 5% of the current valid rate of any package!

Overview

This training will focus on Windows introspection through function hooking. Attendees will learn how they can enumerate, change and subvert application functionality using Frida. These skills are widely applicable for defense, offense and research.

Are you a defender trying to prototype a new detection? Are you a Red Team operator looking to augment your post-exploitation capabilities? Are you a researcher who needs to understand what an application does and how it can be influenced? Function hooking on Windows is a very powerful capability to have in your toolkit no matter what your primary interest is. This training will deliver concrete, real-world knowledge which attendees can take away and directly apply in the field. While Frida has traditionally been used for Android/IOS pentesting and vulnerability research, this training will show that it can be one of the best tools in your arsenal when it comes to 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 Director:
Kerstin Schröter

Prerequisites

- During the course many labs will require students to prototype hooking logic in JavaScript. As such JavaScript experience will be very helpful but not strictly required.
- A detailed knowledge of Windows internals is not required but basic familiarity with the Windows API will be beneficial.
- Attendees need to verify they are able to run PwnAdventure3 on a Windows VM. It can be set on the lowest setting and does not have to run fast. This is important as a substantial portion of the training will consist of hacking PwnAdventure3.

Requirements

- A laptop with VMWare Workstation / Player / Fusion. VirtualBox is not supported.
- Enough system resources to run x2 virtual machines simultaneously.
- 30GB free hard disk space.
- Attendees need not bring their own VM, those will be handed out, fully configured, during the training.

Agenda

Day 1

- Introduction to function hooking
- A closer look at familiar tools: Procmon / API Monitor
- Rapid instrumentation with Frida
- Tracing API calls
- Fermion, an electron UI for Frida
- Hooking to => Change application behaviour
- Hooking to => Inspect data
- Hooking to => Subvert application controls
- Calling native functions from Frida
- Bug-hunting HackSysExtremeVulnerableDriver
- Hooking ShowSnaps

Day 2

- Setting up PwnAdventure3
- Abusing the implicit trust of the game server
- Finding a trigger mechanism
- Unintended use of game functionality
- Solving “Unbearable Revenge”
- Finding game objects in memory
- In-line network proxy
- Prototyping a parser
- Crafting packets
- Applicability of function hooking & porting knowledge to other frameworks

About the Trainer

Hannes Molsen is the Product Security Manager of Dräger, a more than 125-year-old family company known, e.g., for medical devices and safety systems. He is responsible for creating and maintaining an environment which enables Dräger to ship devices and applications that are secure to sustain in an interconnected world. Throughout the entire system’s lifecycle, to protect life, data and system functionality.
At Draeger as well as during his activities as self-employed Security Professional, he also tests devices and applications, and gives security trainings for developers, product managers and software architects.
Before taking this position, he was working as a passionate secure coder, with over 10 years of experience in web application development, software for embedded systems and interconnected devices. He is also actively involved with the grass roots organization “I am the cavalry”, supporting the efforts to connect manufacturers and the security research community to become safer, sooner, together.

Booking

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

Voucher code: TR20_HMTS
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. +49 151 16228365 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