TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Incident Analysis

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 is a practical Incident Analysis workshop, focusing on Windows systems and a bit traffic analysis with lots of hands on exercises. It is designed for anybody with IT background, willing to learn some of the essential steps during an incident analysis. This is not an advanced class, but more of an incident analysis 101 with a steep learning curve. Topics such as incident handling and incident response will not be part of this course.

During this course you will learn a lot about windows/malware internals, and how to:

- Identify Indicators of Compromise
- Analyze network traffic for suspicious behavior
- Investigate disk images
- Analyze memory dumps with volatility
- Differentiate malware from harmless software
- Analyze malware (behavior)
- Corelate gathered logfiles to a specific incident

The language of this course depends on the attendees: if only Germans attend the training, it will be done in Deutsch, otherwise the training will be done in English.

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

- TCP/IP Knowledge
- Be familiar with a shell

Good to have, but not necessary:

- Experience with at least one programming language
- Basic knowledge about hacking techniques

Requirements

- A laptop with administrative privileges and pre-installed VirtualBox
- Wireshark usage

About the Trainers:

Dr.-Ing. Andreas Dewald is working as an IT-Security Researcher at ERNW Research GmbH in Heidelberg and is an associated Post-Doc of the University of Erlangen-Nuremberg (FAU), where he worked as a researcher and lecturer from 2012 to January 2016 at the Chair for IT-Security Infrastructures. From 2013 to 2016, he led the Applied Forensic Computing research group after he finished his PhD in December 2012. Supervised by Prof. Dr.-Ing. Felix Freiling, his thesis was about the formalization of digital evidence and its embedding in forensic computing.

Frank Block is a security researcher working for ERNW Research GmbH with more than 10 years of experience, and an external PhD student at the University of Erlangen-Nuremberg (Department Informatik) with a focus on memory forensics. His main expertise lies with the analysis of incidents and the penetration testing of enterprise networks and web applications. When not involved in customer projects, he enjoys doing research in all kinds of areas (e.g. Wireless technologies) and gives trainings on topics such as hacking and incident analysis.

Florian Bausch is an IT Security and Incident Response Consultant @ ERNW Research GmbH.

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: 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