Training:

Incident Analysis

Date of the online training: **March 24-25, 2021**

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 (hopefully ;-)) 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)
- Correlate 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.

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.

About the Trainers

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 studied Digital Forensics and wrote his Master thesis about a forensic analysis of Ceph (distributed storage). Since 2019 he is been working as an incident responder and pentester at ERNW Research GmbH.

Dennis Kniel works as an IT security researcher at ERNW Research GmbH in Heidelberg. His main expertise lies in the analysis of incidents and in penetration tests of enterprise networks and web applications. He studied Applied Computer Science (B.Sc.) and Mobile Computing (M.Sc.) at the University of Applied Sciences Worms and wrote his Master thesis on the automation of incident response.

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