TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Network Forensics for Incident Response

Date of the online training: **March 15-16, 2021**

Overview

A hands-on network forensics training that allows you to deep dive into analyzing captured full content network traffic in PCAP files. The training data is a completely new and unique data set captured during 30 days on an internet connected network with multiple clients, an AD server, a web server, an android tablet and some embedded devices.

We will analyze traffic from multiple intrusions by various attackers, including APT style attackers and botnet operators. The initial attack vectors are using techniques like exploitation of web vulnerabilities, spear phishing, a supply chain attack and a man-on-the-side attack!

Each attendee will be provided with a free personal single user license of NetworkMiner Professional and CapLoader. These licenses will be valid for six months from the first training day.

ERNW Enno Rey Netzwerke GmbH
Carl-Bosch-Str. 4
69115 Heidelberg
info@ernw.de

Tel. +49 – 6221 – 48 03 90
Fax +49 – 6221 – 41 90 08
BIC: GENODE61HD3
IBAN: DE43 6729 0100 0059 7891 04

Managing Directors
Florian Grunow
Michael Schaefer
VAT-ID: DE 813 376 919

Content

Day 1 : Theory and Practice using Open-Source Tools

- Investigating spear phishing email with malware attachment
- Using JA3 to analyze TLS/SSL encrypted traffic
- Leveraging passive DNS to track C2 domains
- Decoding C2 traffic from a RAT
- Analyzing decrypted HTTPS traffic from a transparent TLS inspection proxy
- Tracking lateral movement on the internal network
- Investigation of botnet infection (TrickBot)
- Analyzing exfiltration by an APT style attacker

Day 2 : Advanced Network Forensics using Netresec Tools

- Analysis of a Man-on-the-Side (MOTS) attack similar to NSA's QUANTUMINSERT and HackingTeam's "Network Injection".
- Analyzing exploitation of insecure web server, web shell deployment and lateral movement into the corporate network.
- Investigating a spear phishing attack with credential theft
- Live TLS decryption lab

Who should attend this training?

The training is built for blue teams, incident responders and SOC analysts, but can also be relevant for law enforcement investigators.

Prerequisites

- Confident using Linux command line tools
- Basic knowledge if TCP/IP communications

Requirements

Laptop with 64-bit operating system, 16GB RAM, 100GB free hard drive space and VirtualBox installed.

About the Trainers

Erik Hjelmvik is an incident responder and developer who is well known in the network forensics field for having created NetworkMiner, which is used by incident responders and law enforcement all around the world. Erik has a background in SCADA security and has spent over 5 years doing incident response at one of the best CERTs in Sweden. Nowadays Erik runs the company Netresec AB, where he develops network forensics software and occasionally teaches network forensic classes.

Booking

Recommended online booking of trainings through:

https://troopers.de/tickets/

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

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