TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Network Forensics

Date of the training: **March 18–19, 2019** in Heidelberg, Germany

Book Now using the voucher code: **TR19_HMTS** and save an additional 5% of the current valid rate of any package!

Overview

The two-day Network Forensics class consists of a mix of theory and hands-on labs, where students will learn to analyze PCAP files. The scenarios in the labs are primarily focused at network forensics for incident response but are also relevant for law enforcement/internal security etc. where the network traffic of a suspect or insider is being monitored.

Day 1 - Theory and Practice using Open Source Tools

- Theory: Ethernet signaling
- Hardware: Network TAPs and Monitor ports / SPAN ports
- Sniffers: Recommendations for high-performance packet interception
- PCAP analysis: Extracting evidence and indicators of compromise using open source tools
- Defeating Big Data: Techniques for working with large data sets
- Whitelists: Learn how to detect 0-day exploit attacks without using IDS signatures
- Challenge Day 1: Find the needle in our haystack and win an honorable prize!

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 Directors:
Enno Rey
Dr. Rainer Schiweck
Kerstin Schröter

Day 2 - Advanced Network Forensics using Netresec Tools

- NetworkMiner Professional: Learning to leverage the features available in the Pro version
  - Port Independent Protocol Identification (PIPI)
  - DNS Whitelisting
- NetworkMinerCLI: Automating content extraction with our command line tool
- CapLoader: Searching, sorting and drilling through large PCAP data sets
  - Super-fast flow transcript (aka Follow TCP/UDP stream)
  - Filter PCAP files and export frames to other tools
  - Keyword search
- Challenge Day 2

The Scenario

The scenario used in the class involves a modern progressive Bank, which provides exchange services for Bitcoin and Litecoin. We've set up clients and a server for this bank using REAL physical machines and a REAL internet connection. All traffic on the network is captured to PCAP files by a SecurityOnion sensor. In the scenario this bank gets into lots of trouble with hackers and malware, such as:

- Defacement of the Bank's web server
- Man-on-the-Side (MOTS) attack (much like NSA/GCHQ's QUANTUM INSERT)
- Backdoor infection through trojanized software
- Spear phishing
- Use of a popular RAT (njRAT) to access the victim's machine and exfiltrate the wallet.dat files for Bitcoin and Litecoin
- Infection with real malware (Nemucod, Miuref / Boaxxe and more)

Class attendees will learn to analyze captured network traffic from these events in order to:

- Investigate web server compromises and defacements
- Detect Man-on-the-Side attacks
- Identify covert backdoors
- Reassemble incoming emails and attachments
- Detect and decode RAT/backdoor traffic
- Detect malicious traffic without having to rely on blacklists, AV or third-party detection services

Professional software included FREE of charge

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.

Requirements

- At least some experience with both Linux and Wireshark.
- Attendees will need to bring a laptop that fits the following specs:
- A PC running any 64-bit Windows OS (can be a Virtual Machine)
- At least 4GB RAM
- At least 40 GB free disk space
- VirtualBox (64 bit) installed (VMWare will not be supported in the training). A VirtualBox VM will be provided on USB flash drives at the beginning of the training.

About the Speaker: Erik Hjelmvik

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.

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Booking

Recommended Online Booking of Trainings Through:

Sign-Up Form https://troopers.de/tickets/

Voucher code: **TR19_HMTS**

Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code up until March 11th, 2019 or until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German.

Zögern Sie nicht uns zu kontaktieren. Wir sprechen fließend Englisch und Deutsch.

Troopers Organization Team

+49 151 16228365 or info@troopers.de

Booking is also possible offline through your trusted partner from:

HMTS HM Training Solutions

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / info@hmtrainingsolutions.com

+49 6022 5089999 / www.hmtrainingsolutions.com