TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Security and Penetration Testing in Industrial Control Systems

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

During this training, at first, a variety of industrial control systems will be explained for students. Then, important threats against these systems and penetration testing methods will be investigated. In the end, the methods of security of industrial control systems will be introduced.

Module 1: Introduction to Industrial Control systems

- Introduction to process control systems (e.g., RTU, PLC, DCS, SCADA, SENSOR, ETC)
- The Purdue model
- Difference between IT and OT
- Introduction to Common ICS weaknesses

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

Module 2: ICS Risk Assessment

- Methodologies for Assessing Risk within Industrial Control Systems (e.g., Risk Assessment Standards, ICS Risk Assessment
- Vulnerability Assessment, Risk Classification and Ranking, Risk rating matrix)
- Lab: Host Identification (arping, arp-scan, GRASSMARLIN)
- Lab: introduction to CSET

Module 3: Networking and ICS Protocols

- Introduction to ICS Networking Terminology, Protocols and Services (e.g., S7, modbus, DNP3, Ethernet/IP, OPC)
- Lab: Turning on a Lamp With Modbus
- Lab: ICS Protocol Traffic Analysis

Module 4: ICS/SCADA Penetration Testing

- RED Team, ICS Attacks and Incidents (e.g., packet replay, spoofing, brute force, man in the middle, social engineering, exploiting, denial of service, reconnaissance, scanning, data manipulating, unauthorized access, top ICS web application vulnerabilities, vulnerability Assessment vs penetration test, etc.).
- Reconnaissance and scanning
- Lab: ICS Recognizance With Google Hacking
- Lab: Working With Shodan/Censys Search Engines
- Lab: Manual ICS Network Scanning Techniques
- Lab: ICS Scanning Tools (plcscan, Grassmarlin, etc.)
- Lab: Manual Massive Network Scanning (nmap, masscan)
- Lab: Working With Nessus SCADA Plugin for vulnerability Assessment
- Lab: ICS Honeypot Fingerprinting
- Penetration
- Lab: Network Attacks
- Lab: Hacking an HMI by Spoofing Modbus
- Lab: Common Web Application Vulnerabilities in Industrial Control Systems
- Lab: ICS Attacking With Metalsploit
- Lab: Fuzzing ICS Protocols and softwares
- Lab: Exploiting buffer overflows in ICS softwares
- Lab: Firmware Analysis

Module 5: ICS Network Security, Policies, Best Practices

- ICS Honeypots, Firewall configuration, Network Monitoring, security policies and procedures development, Secure ICS/SCADA Architecture Design
- Lab: Running ICS Honeypots
- Lab: Working With Tofino Firewall
- Lab: Malware Analysis
- Lab: OS Hardening

Module 6: ICS Threat Intelligence

- Knowledge, Monitoring and Sharing standards of ICS specified cyber threats (e.g., The Types of Cyber Threat Intelligence, Indicators of Compromise, Threat intelligence sharing standards)
- Lab: OpenIOC Creation (or STIX/TAXII)
- Lab: Making an Active CTI Strategy on a Budget
- Lab: OSINT VS CYBINT, Running your own sensors for intelligence gathering

Module 7: Standards and Regulation

- Introduction to the various models, Methodologies, and Industry-Specific regulations that are used to govern what must be done to protect critical ICS systems (NIST / ISA / NERC CIP)

Module 8: Threat Hunting, Forensic and Incident Response

- Security Monitoring, Identification and Collection of Data, System and Network Log Analysis, Cyber Incident Response Planning
- Lab: Some Real Experience From a Ransomware Infection Forensic and IR

Module 9: Air Gapped Environments

- Making Air Gapped Networks, How to Bypass Air Gapped Networks (data transmission theories, review of bypass methods)

About the Speaker: Mohammad-Reza Zamiri

Mohammad Reza (aka d3c0der), has 7+ years of experience in ICS security and monitoring, penetration testing, bug hunting, and malware analysis. He is currently a Security Researcher at ZDResearch, and prior to that has been with Central Bank of Iran as a Senior CSIRT Engineer. He plays bass guitar in his spare time.

Publications

- A Framework for fingerprinting of ICS-Honeypots, Sep 20, 2018, 6th international conference dedicated to industrial cybersecurity, Kaspersky Lab https://ics.kaspersky.com/media/ics-conference-2018/Mohammar-Zamiri-A-Framework-For-Fingerprinting-ICS-Honeypots-En.pdf
- A Look at Malware Distribution strategies, Nov 15, 2017, 2nd offseconf, Shahid Rajaee University https://www.sru.ac.ir/en2/
- SP Access Restriction Bypass via Web Cache Proxy, Jun 17, 2011, First Sharif University Cyber Security Awareness Conference http://cert.sharif.edu

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