TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training

Industrial Control Systems:

Build, Break, Secure

Date of the online training: **March 29-31, 2021**

Overview

Discover the world of Industrial Control Systems with an attack mindset! In this 3-day training, we will follow a hands-on approach, growing from a very simple local process to a realistic ICS environment with 3 words in mind:

- Build: how does it work?
- Break: what are the weaknesses and how to exploit it?
- Secure: what can we do to fix it?

You will perform a lot of lab sessions, including programming a PLC in ladder logic, analyzing network captures of ICS protocols, perform Modbus & OPC-UA requests, using Metasploit to compromise a Windows host and gather sensitive information from an Active Directory, and much more! The last half-day is dedicated to the Capture-the-Flag, in which you will apply the newly acquired techniques to compromise a corporate network, pivot to the ICS network and take control of the process to capture a flag with a robotic arm.

Moreover, the training doesn't stop on the last day! Each participant will receive a 30-day access to the *ICS Cybersecurity Academy* e-learning portal, which allow to watch the training content in video, as well as perform all the exercises on a cloud platform.

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

Agenda

Day 1

- Introduction to Industrial Control Systems
- Automation basics & programming PLC
- ICS protocols
- Hacking the process
- Attacking the non-ICS part of the PLC
- PLC proprietary protocols
- An introduction to safety

Day 2

- Process supervision: SCADA and DCS
- Linking to corporate environments: Windows & Active Directory security
- SCADA/DCS specific vulnerabilities
- Industry 4.0 & IIoT
- ICS cybersecurity general approach

Day 3

- Data exchange between ICS and the outside world
- ICS security assessments
- Capture the Flag

The whole afternoon is dedicated to applying the pentesting skills to a custom-designed ICS setup, composed of a corporate Active Directory with several servers and workstations, an ICS network composed of servers, HMIs and PLCs from several vendors. This setup controls a model train and some robot arms that need to be used to capture a flag on the train! This CTF environment was migrated to the cloud and can be used remotely.

Who should attend this training?

This training aims at bridging the gap between IT and ICS: it is designed to allow OT professionals to understand the security challenges of ICS with an offensive mindset, while allowing IT professionals to discover the world of Industrial Control Systems and adapt their cybersecurity knowledge to this new world.

Prerequisites

The training is heavily hands-on. While no ICS or pentest knowledge is required, it is recommended for to have basic networking and computers skills (using virtual machines, the command line, understanding TCP/IP…).

Requirements

Attendees need to bring a laptop with VirtualBox, capable of running 64-bits virtual machines (8GB RAM & 50GB free disk space recommended).

About the Trainers

Arnaud Soullié (@arnaudsoullie) is a manager at Wavestone. For 10 years, he has been performing security audits and pentest on all type of targets. He specializes in Industrial Control Systems and Active Directory security. He has spoken at numerous security conferences on ICS topic : BlackHat Europe, BruCon, 4SICS, BSides Las Vegas, DEFCON... He is also the creator of the DYODE project, an open-source data diode aimed at ICS. He teaches ICS cybersecurity trainings at conferences and online at www.ics-cybersecurity.academy

Booking

Recommended online booking of trainings through:

https://troopers.de/troopers21/trainings

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