Training:

Pentesting Industrial Control Systems

Date of the training: **March 16-17, 2020** in Heidelberg, Germany

Book now using the voucher code: TR20_HMTS and save an additional 5% of the current valid rate of any package!

Overview

On this intense two-day training, you will learn everything you need to start pentesting Industrial Control Networks. We will cover the basics to help you understand the most common ICS vulnerabilities. We will then spend some time learning and exploiting Windows & Active Directory weaknesses, as most ICS are controlled by Windows systems.

We will cover the most common ICS protocols (Modbus, S7, Profinet, Ethernet/IP, DNP3, OPC…), analyze packet captures and learn how to use these protocols to talk to Programmable Logic Controllers (PLCs). You will learn how to program a PLC, to better understand how to exploit them.

The training will end with a challenging hands-on exercise: The first CTF in which you capture a real flag! Using your newly acquired skills, you will try to compromise a Windows Active Directory, pivot to an ICS setup to take control of a model train and robotic arms. This training is heavily based on hands-on exercises, based both on simulated and real environments.

Agenda

Day 1

- Introduction to ICS
- A brief history of ICS
- Vocabulary
- The CIM model
- ICS architectures
- ICS components (PLCs, HMI, SCADA, DCS, sensors, RTUs, Historian, etc.) and their roles
- OT vs IT
- Pentesting basics & Windows security
- OSINT for ICS : Where to look to find information
- Reconnaissance : how to portscan & nessus
- Exploitation : Metasploit basics
- Common ICS vulnerabilities
- Organization & awareness
- Lack of network segmentation / Exposure
- Vulnerability management
- ICS protocols insecurity
- Third party management
- Lack of security supervision
- ICS protocols
- Modbus/TCP
- S7
- Profinet
- OPC-UA
- Programming PLCs
- Ladder logic and other programming languages
- Creation of basic ladder logic programs

Day 2

- Pentesting ICS
- Theory and general warning
- Common weaknesses of PLCs
- Talking industrial protocols : Modbus, S7 (using PLC simulators and SCADA VMs)
- Demos of specific features of Schneider PLCs
- Additional PLC features: web server, ftp, snmp, …
- Securing ICS
- Major ICS security standards
- Architecture
- Data exchange with corporate network
- Network anomaly detection
- Introduction to safety for security pros
- Capture the Flag
- Use your newly acquired skills to perform ICS pentesting in a realistic environment (Several Windows machines, network segmentation, real PLCs from different manufacturers)

Prerequisites

A basic knowledge of networking and command line is required, as well as the ability to work with virtual machines. A background in penetration testing is a plus, but not absolutely required as I'll cover the basic steps through the training.

Requirements

Attendees must bring a laptop with a recent version of VirtualBox and the ability to run 64-bit virtual machines. The bare minimum is 4GB of RAM (with 8 highly recommended) and about 50Gb of available disk space. It is also possible to use alternative virtualization software (Workstation, Fusion, etc.) but some configuration details (like networking) are usually lost when importing the virtual machines and require additional setup time.

About the Trainer

Arnaud Soullié is a manager at Wavestone, performing security audits and leading R&D projects. He has a specific interest in Active Directory security as well as ICS, two subjects that tend to collide nowadays. He teaches ICS security and pentests workshops at security conferences (BlackHat Europe 2014, BSides Las Vegas 2015/2016, Brucon 2015/2017, DEFCON 24, DEFCON 26) as well as full trainings (Hack in Paris 2015 and 2018, BlackHat Asia 2019).

Booking

Recommended online booking of trainings through:
https://troopers.de/tickets/

Voucher code: TR20_HMTS
Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German. +49 151 16228365 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