Advanced ICS/SCADA Hacking Training

Overview

Industrial Control Systems (including SCADA, DCS, SIS, PLC) are often poorly understood, yet they are used in the most critical environments in the world. Although they generally remain unseen they are responsible for the smooth running of our daily routines from the moment we turn on a tap in the morning, to turning off the lights at night. This two-day course will take a deep-dive into the fundamentals of ICS security and provide students with the knowledge that they need to safely evaluate and protect these systems against emerging cyber threats.

The course will also provide students with methodologies through which security research may be performed against ICS devices in order to identify zero-day vulnerabilities. During the course, students will have the opportunity to engage in real-life attacks against Industrial Controls Systems and their components by participating in activities such as SCADA firmware reverse engineering and ICS protocol fuzzing.

Target audience

This course has been specifically designed for all staff responsible for securing ICS/SCADA systems. Typically staff with functions involving: Network Engineering, Penetration Testing, Ethical Hacking, Forensic Research, Auditing and Security Operations, Law Enforcement.

Course outline

Day 1 - ICS Understanding & Introduction to Attacks

- ICS specific fundamentals
- Attacking industrial devices (HMIs, RTUs, IEDs, Sensors and PLCs)
- SCADA & Historian application hacking
- Attacking Industrial Firewalls

Day 2 - Protecting ICS environments

- Reverse engineering of ICS protocols
- Firmware analysis & reverse engineering
- Incident Response
- Hands-on Hacking of Real Life Control Systems

Achievements

At the end of the training, students will have an in-depth knowledge of ICS/SCADA systems attack techniques, and therefore be better equipped to protect ICS/SCADA environments.

Course pre-requisites

Students must possess a fundamental understanding of computing and networking technologies, including switching, routing, programming and Windows/UNIX based operating systems at an intermediate level. Basic penetration testing experience is desirable, but not required. It is assumed that attendees will have no knowledge of industrial control systems, Smart Grid, SCADA, or critical infrastructure.

Course Preparation

- Laptop with a 32 or 64bit operating system and at least 8GB of free RAM.
- Latest VMware Player, VMware Workstation, VMware Fusion installed before class.

Applied Risk will provide

- Controllers for the hands-on labs
- PDF version of the course slide deck
- Course material: USB & hard copy of all lab assignments

Language

The course will be given in English or Dutch, depending on the participants preferred language. The course material is in English.

Course execution

Duration: 2 full days: 09.00 – 17.00
Price: EUR 2500.- per student
Location: Amsterdam or at a location to be agreed upon

Applied Risk BV
Teleportboulevard 110, 1043 EJ
Amsterdam The Netherlands

T: +31 (020) 833 4020
E: info@applied-risk.com
W: applied-risk.com

Applied Risk