Assessing and Exploiting Control Systems & IIoT Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

This is not your traditional SCADA, ICS, IIoT security course! How many courses send you home with lifetime access to course updates and a $500 kit including your own PLC and a set of hardware RF hacking tools?!? This course teaches hands-on penetration testing techniques used to test individual components of a control system, including embedded electronic field devices, network protocols, RF communications, Human Machine Interfaces (HMIs), and various forms of master servers and their ICS applications. Skills you will learn in this course will apply directly to systems such as the Smart Grid, PLCs, RTUs, smart meters, building management, manufacturing, Home Area Networks (HAN), smart appliances, SCADA, substation automation, synchrophasors, and even IoT.

This course is structured around the formal penetration testing methodology created by UtiliSec for the United States Department of Energy. Using this methodology and the ControlThings Platform (previously SamuraiSTFU), an open source Linux distribution for pentesting energy sector systems and other critical infrastructure, we will perform hands-on penetration testing tasks on user interfaces (on master servers and field device maintenance interfaces), control system protocols (modbus, DNP3, IEC 60870-5-104), proprietary RF communications (433MHz, 869MHz, 915MHz), and embedded circuit attacks (memory dumping, bus snooping, JTAG, and firmware analysis). We will tie these techniques and exercises back to control system devices that can be tested using these techniques. The course exercises will be performed on a mixture of real world and simulated devices to give attendees the most realistic experience possible in a portable classroom setting.

Advances in modern control systems, including initiatives such as the Smart Grid and Industry 4.0, have brought great benefits for asset owners/operators and customers alike, however these benefits have often come at a cost from a security perspective. With increased functionality and additional inter-system communication, modern control systems bring a greater risk of compromise that vendors, asset owners/operators, and society in general must accept to realize the desired benefits. To minimize this risk, penetration testing in conjunction with other security assessment types must be performed to minimize vulnerabilities before attackers can exploit critical infrastructures that exist in all countries around the world. Ultimately, this is the goal of this course, to help you know how, when, and where this can be done safely in your control systems.

Course Length and Content:

This course is broken into individual modules, with each being offered individually or combined into course lengths from 1-5 days in length. Here is a list of the current modules and their approximate length, which can be slightly increased or decreased depending on conference or client needs.

Assessing and Exploiting Control System Architectures - 0.5 Days
Assessing and Exploiting Control Network Captures - 1.0 Days
Assessing and Exploiting Production Control Networks - 0.5 Days
Assessing and Exploiting Controller Logic - 0.5 Days
Assessing and Exploiting Control Protocols - 0.5 Days
Assessing and Exploiting Proprietary Serial Protocols - 0.5 Days
Assessing and Exploiting Proprietary RF Protocols - 1.0 Days
Assessing and Exploiting Embedded Memory - 0.5 Days
Assessing and Exploiting Embedded Firmware - 0.5 Days

Assessing and Exploiting Control Systems & IIoT Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Prerequisites

This course is designed for intermediate level security professionals, be they engineers, technicians, analysts, managers, or penetration testers. Basic penetration testing experience is desirable, but not required. It is assumed that attendees will have no knowledge of ICS, Smart Grid, SCADA, or critical infrastructure.

Recommended Reading before the Course:

For those with little or no ICS experience, these Wikipedia articles provide a brief introduction to the concepts and history of control systems that will be helpful to know for class.

- http://bit.ly/2WzuVZu (Large YouTube Playlist of Basic ICS Concepts)
- http://en.wikipedia.org/wiki/ICS
- http://en.wikipedia.org/wiki/SCADA
- http://en.wikipedia.org/wiki/Distributed_control_system
- https://en.wikipedia.org/wiki/Programmable_logic_controller
- http://en.wikipedia.org/wiki/Smart_grid

NIST 800-82 is a great introduction to industrial control systems, the security issues surrounding them, and basic cyber defenses

- http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

Since this course will be getting very deep into the technical weeds of communications, it would be helpful to have a basic understanding of the following encoding methods: ASCII, Unicode, UTF-8, UTF-16, and UTF-32

- http://kunststube.net/encoding

Assessing and Exploiting Control Systems & IIoT Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

- Attendees will be able to explain the steps and methodology used in performing penetration tests on Industrial Control Systems and Industrial Internet of Things.
- Attendees will be able to use the free and open source tools in ControlThings Platform to discover and identify vulnerabilities in web applications.
- Attendees will be able to exploit several hardware, network, serial, user interface, RF, and server-side vulnerabilities.

Resources Provided on the Course:

The following items (or rough equivalents depending on availability) are provided to each attendee to use in class and keep after course completion:

- Velocio Ace 1600 PLC (Programmable Logic Controller)
- vBuilder software to program the PLC to keep (non-expiring)
- vFactory software to program an HMI for the PLC (non-expiring)
- RTL-SDR (Software Defined Radio)
- Great Scott Gadgets Yardstick sub-GHz Radio
- Great Scott Gadgets GreatFET
- Breadboard with SPI and I2C EEPROMs
- TivaC Launchpad (ARM m4) for Firmware exercises
- Latest version of the ControlThings Platform on USB
- PDF version of the course slide deck
- Lifetime access to future updates to the course modules presented in class, restricted to the individual that attended the course