Assessing And Exploiting
Control Systems & IIoT

ONLINE Training Course

20 - 21 July, 2020

Price: 600 JD

Course Abstract

This is not your traditional SCADA/ICS/IIoT security course!

This course teaches hands-on penetration testing techniques used to test individual components of a control system, including embedded electronic field devices, network protocols, 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 Control Things Pentest 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) and control system protocols (modbus, DNP3, IEC 60870-5-104). 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 students the most realistic experience as possible in a portable classroom setting.

Advances in modern control systems such as the energy sector's Smart Grid has 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 Objectives

- 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.

Course Prerequisites

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. This course is designed for intermediate level security professionals, be they engineers, technicians, analysts, managers, or penetration testers.

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
- http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf - NIST 800-82 is a great introduction to industrial control systems and the security issues surrounding them.
- http://kunststube.net/encoding - Understanding ASCII, Unicode, UTF-8, UTF-16, and UTF-32

Resources Provided at the Course

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

- Latest version of the ControlThings Platform
- PDF version of the course slide deck
- A Google Hangouts virtual classroom environment
- A Slack channel for communications during and in between class sections
- Because of the virtual and discounted nature of this course, all hardware exercises will be done by the instructor as a demonstration for students. Digital artifacts such as communication captures will be provided to students for hands-on analysis.

Each Attendee Must Bring a Laptop that Meets the Following Requirements

- 64-bit processor with 64-bit operating system
- VT or other 64-bit virtualization settings enabled in your BIOS to run 64-bit VMs
- At least eight (8) GB of RAM, recommended sixteen (16) GB if possible
- At least fifty (50) GB of free hard drive space
- Windows 10.x installed on your host laptop or inside a VM
- VMware Workstation Player 15 (or later), VMware Workstation Pro 15 (or later), or VMware Fusion 11 (or later) installed BEFORE class begins. Other virtualization software such as Parallels, VirtualBox, or earlier versions of VMware products may work if the attendee is familiar with its functionality and takes full ownership of its configuration, however non-VMware software is not officially supported and VMware should be pre-installed as a backup just in case
- Access to an account with administrative permissions and the ability to disable all security software on their laptop such as Antivirus and/or firewalls if needed for the class.

Instructor Bio

Justin Searle is the Director of ICS Security at InGuardians, specializing in ICS security architecture design and penetration testing. He led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and has played key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), National Electric Sector Cybersecurity Organization Resources (NESCOR), and Smart Grid Interoperability Panel (SGIP).

Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences. He is currently a Senior Instructor for the SANS Institute and a faculty member at IANS. In addition to electric power industry conferences, Justin frequently presents at top international security conferences such as Black Hat, DEFCON, OWASP, Nullcon, and AusCERT.

Justin leads prominent open source projects including the The Control Thing Platform, Samurai Web Testing Framework (SamuraiWTF), Samurai Security Testing Framework for Utilities (SamuraiSTFU).

He has an MBA in International Technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), Web Application Penetration Tester (GWAPT), and GIAC Industrial Control Security Professional (GICSP).

Course Outline

Day 1 Outline – Assessing and Exploiting Controllers

Understanding basic control system concepts, systems, and devices

- Control system architectures
- PLCs, RTUs, and IEDs
- Understanding RTOS
- Industrial and non-Industrial
- What is IIoT and how it differs from IoT
- Field devices, buses, and loops
- DCS vs SCADA

Understanding controller logic

- Velocio PLCs vs other PLCs
- Hands-on exercise creating controller logic
- Hands-on exercise programming a PLC
- Hands-on exercise creating an HMI

Architecture Reviews of major ICS and smart grid systems

- Supervisory control and data acquisition (SCADA)
- Distribution Grid Management (DGM) and Substation Automation (SA)
- Wide Area Management, Protection, and Control (WAMPAC)
- Demand Response (DR)
- Distributed Energy Resources (DER)
- Advanced Metering Infrastructure (AMI)
- Electric Vehicles (EV)

Introduction to ControlThings Platform

- Setting up the virtual machine
- Walk through the tools and functionality
- Introduction to the student hardware kits

Introduction to the NESCOR methodology for penetration testing

- Preparing for a penetration test
- Architecture reviews
- Testing the master servers
- Testing the user interfaces
- Testing the network communications
- Testing the embedded field devices
- End-to-end assessment
- Reporting

Introduction to the NESCOR methodology for penetration testing
• Preparing for a penetration test • Architecture reviews • Testing the master servers • Testing the user interfaces • Testing the network communications • Testing the embedded field devices • End-to-end assessment • Reporting
Types of ICS user interfaces
• Traditional applications • Web applications • Terminal interfaces
Pentesting maintenance interfaces on ICS field and floor devices
• Functional analysis of field technician interfaces • Hands-on exercise capturing USB communications to tech interfaces • Hands-on exercise analyzing captured USB communications • Impersonating endpoints in field tech interface communications • Hands-on exercises impersonating vendor endpoints with Python • Exploiting vulnerabilities found during analysis

Day 2 Outline – Assessing and Exploiting ICS Communication Protocols

Performing traditional network pentests on control systems
• Overview of a traditional network penetration test methodology • Dangers of port and vulnerability scanning • Strategies to perform port and vulnerability scanning
Pentesting Different Communication Layers
• Testing of communication mediums vs communication protocols • Where security defenses should be place …… and tested

Serial communications
• RS-232, TIA-422, and TIA-485 • Fieldbus Protocols and Protocol Families • Hands-on sniffing and injection of serial Modbus RTU
Pentesting TCP/IP based ICS protocols
• Protocol capture and analysis • ModbusTCP, ProfiNet, EnternetIP/CIP, DNP3, IEC 104, IEC 61850, ICCP • Dealing with unknown protocols • Hands-on entropy analysis of network payloads • Reverse engineering unknown protocols • Hands-on ICS protocol fuzzing

FOR REGISTRATION:

General Computers & Electronics Company

Eng. Amer Alnajjar
Training Center Manager

+962 6 551 38 79 | +962 77 739 7728 | anajar@gce.com.jo