



SCADA SECURITY

Comprehensive SCADA Security for IT Professionals & Control Engineers



1 General Details

1.1 Goal

Gain the most updated knowledge on how to design, assess and implement security of SCADA networks.

1.2 Duration

5 days

1.3 Student Requirements

All students are required to have a technical background either in computer administration or in SCADA operations administration.

1.4 Instructors

Eyal Udassin is the co-founder and a security expert at C4 Security, a penetration testing company which uncovers and mitigates technical security vulnerabilities by attacking the tested system or network.

Mr. Udassin performed hundreds of penetration tests against financial, governmental, military and SCADA clients as the technical leader of C4's red team. He specializes in protocol analysis, reverse engineering of binary code, passive and active reconnaissance of computer networks and exploiting vulnerabilities uncovered in proprietary software.

1.5 C4 Security

C4's SCADA team consists of leading experts in the field of penetration testing and application security who have acquired an in-depth understanding of attackers' methodologies and unique knowledge and tools in analyzing protocols and reverse engineering.

This team specializes in attacking and protecting command and control systems as well as added expertise in the field of homeland security.

The team has already revealed several security vulnerabilities in the most popular SCADA control systems and PI applications. Our SCADA clients list includes leading electric companies, pipeline utilities and water pumping and distribution systems.



2 Syllabus

2.1 Day 1 - Introduction

- Introduction
 - What is SCADA?
 - Introduction to Security
 - Unique Aspects of Security in SCADA Systems
- Network Terminology and Architecture Concepts
 - 7 Layers, WAN, LAN, IP, Routers etc.
- SCADA Terminology and Architecture Concepts
 - EMS, DCS, HMI, FEP etc.
- Lab – Collaborative Design of a Simple Oil Pipeline Utility Network

2.2 Day 2 – Security and SCADA

- Security Terminology and Architecture Concepts
 - Vulnerabilities, Segregation, Firewalls, NAC etc.
- SCADA threats and Attack Vectors
 - Corporate to Field
 - Field to Center
 - Field to Field
 - Remote Support
 - Unauthorized Control Center Access
- Overview of Published Vulnerabilities



2.3 Day 3 – Control Center Security

- Control Center Elements
- Brief Overview of Physical Security
- Securing the Connection to the Corporate Network
- Securing Remote Maintenance Links
- WAN Security – Fiber, Radio, GPRS, 3G, PSTN Modems
- LAN Security
- Redundancy
- Best Practice for OS Patches & Anti Virus Updates in a mission-critical environment
- SCADA-Aware One-Way Links
- Secure PI Deployment
- Lab – Improving the Design of the Previous Day
 - DMZ Architecture, Logical Security, Physical Security

2.4 Day 4 – Field Devices Security

- Introduction Field Devices
- Common Control Protocols (Modbus, DNP3, IEC60870-5-101/4)
- Protocol Vulnerabilities
- Implementation Vulnerabilities
- Layer 1 Considerations
- Lab – Attack a Field Device



2.5 Day 5 – Standards and Processes

- Regulations – US and abroad
- Information Security Official Agencies
- Relevant Standards
 - NIST, ISA, NERC CIP, PCSR, etc.
- Processes
 - Who's in charge? IT, Operations or Internal Auditing?
 - Threat Assessment
 - Education and Awareness
 - Procurement Changes
 - Secure Design
 - FAT/SAT Penetration Tests
 - Risk Assessments
- Course Summary