

SCADA Security

Overview

Students will gain homeland security skills, by learning to assess and secure SCADA systems. This course covers everything from field based attacks to automated vulnerability assessments for SCADA networks.

Target Audience

Course Outline

Best Practices and Perimeter Security

- Introduction to SCADA Security Concepts
- Security Approach
- Industrial Network Policy Development
- SCADA Systems Audit
- Physical Security Considerations
- Field-Based Attacks
- Logical Security Perimeter
- DMZ Architectures for SCADA Networks
- Common DMZ Elements
- Common Rulesets
- Control Center Remote Access
- Vendor Access
- Antivirus Issues

Access and Authorization Controls

- Identification
- User Account Issues
- Password Policy Enforcement
- Two-Factor Authentication on Industrial Networks
- Role Based Authentication
- Location Based Auth
- System Based Auth
- SCADA Application Integration Security Issues
- Microsoft Active Directory Integration Issues
- Gold Standard Configs Strong Auth Support IPSec
- Data Security Classifications
- Current SCADA Security Standards Implementing Current Standards• Prep for IACRB CSSA Exam

[Register Online](#)

Schedule

Class Length: 5 Days

G2R = "Guaranteed to Run" | OLL = "Online LIVE"
ILT = "Instructor-Led-Training"

This course is not currently available on the public schedule. Please contact us using the information in the footer below to inquire about future dates or to schedule a private class.

Intrusion Prevention/Detection & Advanced

Vulnerable Systems Analysis SCADA Protocol Analysis SCADA Protocol Vulnerabilities
Network Based Intrusion Detection Modbus/TCP specific Intrusion Detection Rules Log collection
Log correlation Event management Alert Management Field W AN Networks Internet Based W AN Networks Wireless SCADA Security Issues Vulnerability Assessment
Legacy Systems
Exceptions
Security Awareness Programs

Penetration Testing SCADA Systems Part 1

Pen Testing Strategies for SCADA and Industrial Networks
Replicating a Non-Production Testing Environment
Understanding the Modbus/TCP Protocol
Protocol Elements and Coil Adjustments
Capture & Replay Attacks for Modbus/TCP Spoofing Attacks for Modbus/TCP
Exploiting SSL/TLS Encapsulated SCADA Protocols
Writing a Spoofed Replay Attack Exploit W ith Perl

Penetration Testing SCADA Systems Part 2

Fundamentals of Pen Testing for SCADA Protocols
Fuzzing Modbus/TCP PLCs Dynamic Fuzz Elements Fuzzing State-Aware Protocols
Attacking Binary Protocols Writing a Custom Fuzzer Pen-Testing HMIs
Buffer Overflow Attacks for HMIs
Authentication and Authorization Attacks Against HMIs
Privilege Escalation Attacks Against HMIs
IACRB CSSA Exam Proctored On-Site

Related Courses, Certifications, Exams

- Certified SCADA Security Architect
- CSSA