ICS/SCADA Cyber Security

Course Outline

(Version 1)

Module 01: Introduction to ICS/SCADA Network Defense

- Module Objectives
- Typical Security Model
- Security Model Explained
- Authorization
- Purdue Reference Model
- Overview of ICS/SCADA Operations
- Human Machine Interface (HMI)
- ICS/SCADA Overview
- Microcontroller
- LAB: Security Model
- Selecting a Security Posture
- Defining Risk
- Types of Risk
- Managing Risk
- Security Policy
- Allowing a Service
- LAB: Allowing a Service
- ICS/SCADA generations
- ICS/SCADA
- ICS/SCADA Attacks
- Defining “Vulnerability”
- Finding Targets
- NetBios from the Internet
- Attack Surface
- Protocols

- Siemens
- Modbus
- BACnet
- Challenges with ICS/SCADA Risk
- Asset Identification and System Characterization
- Vulnerability Identification and Threat Modelling
- Risk Calculation and Management
- SCADA Framework
- IT and ICS Comparison
- Standards
- LAB: Standards
- Module Summary

Module 02: TCP/IP 101

- Module Objectives
- Network Protocols
- Transport Protocols
- Headers
- Encapsulation
- De-encapsulation
- TCP/IP
- Flow of Data
- Switch Connecting two Machines
- Router Connecting Two Networks
- Analyzing Traffic with Protocol Analyzers
- IPv4 Header
- UDP Header
- TCP Header
- TCP Header Composition
- Viewing TCP/IP Headers
- It is all in the Packet!

- TCP Flags Under the Hood
- What Is a Threat?
- Know Your Adversary
- Threat Containment
- LAB: TCP/IP
- Network Protocols
- IP
- IP Header
- IP Protocol Type
- ARP: Address Resolution Protocol
- ARP on the Host
- UDP Header
- TFTP: Trivial File Transfer Protocol
- TCP: Transmission Control Protocol
- TCP Connection
- TCP Connection Close
- TCP Connection Reset
- TCP Data Flow
- LAB: Protocol Analysis
- ICS/SCADA Protocols
- Modbus
- Modbus Protocol Types
- Modbus Protocol and OSI Model
- Modbus Recon
- LAB: Modbus Protocol Analysis
- Module Summary

Module 03: Introduction to Hacking

- Module Objective
- Motives, Goals, and Objectives of Information Security Attacks
- What is Hacking

- Why Ethical Hacking
- What is Ethical Hacking
- Mindset of the Attacker
- Create a Security Testing Plan
- Testing Methodology Resources
- Types of Testing
- Roles of Ethical Hacking
- Hacking Methodology First Step
- The Steps to a Successful Ethical Hack
- Footprinting and Reconnaissance
- Objectives of Footprinting
- Footprinting Tasks
- Footprinting Using Google
- Google Hacking Database
- Web Site Footprinting
- Web Site Mirroring
- Web Site Archives
- Whois
- LAB: Footprinting and Recon
- Scanning
- Live Systems
- Ports
- Services
- Enumeration
- Identify Vulnerabilities
- Vulnerability Research
- Manual Identification Vulnerability
- Automatic Identification of Vulnerability
- ICS CERT Guidance
- Common ICS Architectures
- Two Firewalls Architecture

- Control System as a DMZ
- Data DMZ
- Modems and Wardialing
- Vendor Support
- IT Controlled Communication Gear
- Corporate VPN
- Database Links
- Exploration
- LAB Hacking Steps
- Penetration Testing
- ICS/SCADA Testing
- ICS/SCADA Uniqueness
- Information Gathering
- BACnet Public Facing
- DNP3 Public Facing
- Internal Testing
- LAB: ICS/SCADA Initial Testing
- Module Summary

Module 04: Vulnerability Management

- Module Objectives
- Defining “Vulnerability”
- Vulnerability Scanners
- Vulnerability Assessment
- The Challenge of Vulnerability Assessment
- Vulnerability Scanners
- Vulnerability Assessment
- Vulnerability Assessment
- Good and the Bad
- Zero Day
- Malware Ecosystem

- Industrial Control Systems
- Havex and Dragonfly
- Traditional Malware Threat to ICS/SCADA
- Permanent Attacks
- Vulnerability Management
- Vulnerability Management Asset Identification
- Asset Identification Using Nmap
- Emulate the Ports
- Conpot
- ICS/SCADA Scanning with Nessus
- Modbus/TCP Coil Access
- LAB: Vulnerability Management
- Metasploit and ICS/SCADA
- Metasploit and Modbus
- Modbus Detect Module
- Metasploit and Bacnet
- Vulnerability Severity
- Microsoft Exploitability Index
- Common Vulnerability Scoring System (CVSS)
- Base Metrics
- Online Calculator
- Temporal Metrics
- Environmental Metrics
- CVSS Example
- Temporal Score Impact
- Environment Score
- LAB: Mastering the CVSS
- Module Summary

Module 05: Standards and Regulation for Cybersecurity

- Module Objectives

- Standards and Regulations
- Iso 27001
- NERC CIP
- CFATS
- ISA99
- IEC 62443
- IEC 62443
- IEC 62443
- IEC 62443
- IEC 62443 Sample Network
- Security Level 1
- Security Level 1
- Level 1
- Level 2
- Security Level 2
- Level Two
- Security Level 3
- Level 3
- NIST SP 800-82
- Defense in Depth Strategy
- Industry Best Practices for ICS
- ICS/SCADA Regulations Workshop
- Module Summary

Module 06: Securing the ICS/SCADA Network

- Module Objectives
- Physical Security
- Establishing policy
- Securing the ICS Protocols
- Server Isolation with IPsec
- IPsec Authentication Header (AH)

- IPsec Encapsulation Security Payload (ESP) Header
- IPsec Security Association (SA)
- IPsec Modes
- Transport mode
- Tunnel mode
- Firewall Improvements
- Windows Firewall Snap-In
- IPsec Rules
- Firewall Scripting
- Isolating a Server
- Group Policy Object
- Server Isolation Steps
- Domain Isolation
- ICS Vulnerability Assessment
- ICS Risk Management
- ICS Cyber Risk Assessment
- Methodology for Industrial Networks
- ICS Testing Priorities
- ICS CERT Cybersecurity Evaluation Tool (CSET)
- Entry Points
- Physical to Logical Assets
- Threat Identification
- Threat Vectors
- Risk Reduction and Mitigation
- LAB: ICS/SCADA Security
- Module Summary

Module 07: Bridging the Air Gap

- Module Objectives
- ICS/SCADA Connections
- Example Connection Types

- Data Diode
- Guard
- Next Generation Firewall
- ICS Monitoring
- Monitoring and Detection
- Logs
- Syslog equivalent
- WMIC vs PowerShell
- Get-CIMinstance
- What to Monitor
- Additional Context
- Best Practices
- Log Aggregation
- Zone Monitoring
- SIEM
- Data Historians
- Splunk
- Monitoring Across Secure Boundaries
- Information Management
- Reports
- Alerts
- Incident Investigation and Response
- Log Storage and Retention
- Strong Authentication
- Labs: ICS Monitoring
- Module Summary

Module 08: Introduction to Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

- Module Objectives
- Why Intrusion Detection?

- Fortress Mentality
- De-Perimeterization
- Intrusion Detection 101
- What is Intrusion Detection?
- IDS Features
- Stealth the IDS
- False Positives!
- Topology Concerns
- Recommended in Most Circles
- Other uses of IDS
- Under Attack
- Stop the Attack
- Intrusion Prevention
- Types of IPS
- Host-Based Intrusion Prevention System
- Network Intrusion Prevention
- Intrusion Analysis
- ICMP
- UDP
- TCP
- Identifying the OS
- Passive Fingerprinting
- Methodology
- Signs of Compromise
- LAB: Intrusion Detection
- Log Analysis
- Malware
- Server Message Block (SMB) Communication
- Malware on the Wire
- WannaCry
- WannaCry

- WannaCry
- APT Defined
- APT Characteristics
- APT Command and Control (C2)
- APT Artifacts
- APT Methodology: The Cyber Kill Chain
- APT Proxy Infrastructure
- MITRE ATT&CK Matrix
- Event Correlation
- ICS Malware
- Dropper
- Infection Vectors
- ICS Specific Malware
- LAB: ICS/SCADA Malware
- Module Summary