

# ICS/SCADA

## ● Module 1: Introduction to ICS/SCADA Network Defense ▲

### LAB: Security Model

- IT Security Model
- ICS/SCADA Security Model

### LAB: Allowing a Service

- Security Posture
- Risk Management in ICS/SCADA
- Risk Assessment
- Defining Types of Risk
- Security Policy

## ● Module 2: TCP/IP 101 ▲

- Introduction and Overview
- Introducing TCP/IP Networks
- Internet RFCs and STDs
- TCP/IP Protocol Architecture
- Protocol Layering Concepts
- TCP/IP Layering
- Components of TCP/IP Networks
- ICS/SCADA Protocols

- Review of the Hacking Process
- Hacking Methodology
- Intelligence Gathering
- Footprinting
- Scanning
- Enumeration
- Identify Vulnerabilities
- Exploitation
- Covering Tracks

## **LAB: Hacking ICS/SCADA Networks Protocols**

- How ICS/SCADA Are Targeted
  - Study of ICS/SCADA Attacks
  - ICS/SCADA as a High-Value Target
  - Attack Methodologies In ICS
-

## ● Module 4: Vulnerability Management ▲

- Challenges of Vulnerability Assessment
- System Vulnerabilities
- Desktop Vulnerabilities
- ICS/SCADA Vulnerabilities
- Interpreting Advisory Notices
- CVE
- ICS/SCADA Vulnerability Sites
- Life Cycle of a Vulnerability and Exploit
- Challenges of Zero-Day Vulnerability
- Exploitation of a Vulnerability
- Vulnerability Scanners
- ICS/SCADA Vulnerability Uniqueness
- Challenges of Vulnerability Management Within ICS/SCADA

### **LAB: Vulnerability Assessment**

- Prioritizing Vulnerabilities
- CVSS
- OVAL

## ● Module 5: Standards and Regulations for Cybersecurity ▲

- ISO 27001
- ICS/SCADA
- NERC CIP
- CFATS
- ISA99
- IEC 62443
- NIST SP 800-82

## ● Module 6: Securing the ICS network ▲

- Physical Security
- Establishing Policy – ISO Roadmap
- Securing the Protocols Unique to the ICS
- Performing a Vulnerability Assessment
- Selecting and Applying Controls to Mitigate Risk
- Monitoring
- Mitigating the Risk of Legacy Machines

## Module 7: Bridging the Air Gap ▲

- Do You Really Want to Do This?
- Advantages and Disadvantages
- Guard
- Data Diode
- Next Generation Firewalls

## Module 8: Introduction to Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) ▲

- What IDS Can and Cannot Do
- Types IDS
- Network
- Host
- Network Node
- Advantages of IDS
- Limitations of IDS
- Stealthing the IDS
- Detecting Intrusions