Blue Team Training

SCADA Security & Reliability

Practical ICS Security Training

This course focuses on gaining a general exposure to and knowledge of practical ICS security in a real ICS environment. It is geared towards individuals that need to gain a greater understanding of what tools exist and how they can be utilized to asses and monitor ICS networks, including both incident detection and response. Emphasis during the course will be on defending ICS networks against attackers (blue-teaming). However, understanding an attacker's perspective (red-teaming) is a very important part of learning how to defend ICS networks against an attack. The instructors will guide students through a subset of the vast number of different tools and techniques that exist, focusing on ones that have proven useful for both assessing and defending ICS networks.

During the first day of the course, the students will be introduced to many of the tools in ICS security from operating systems and basic system administration to vulnerability assessment tools, packet capture, and traffic analysis. Students will learn how to configure their computers to utilize these tools in both a live boot and a virtual environment. During the second day of the course, the instructors will facilitate a red-team/blue-team exercise, where the students will gain hands-on experience with the tools and techniques on real ICS equipment.

You Will Learn

- Basic Linux and Windows System Administration
- Creating Live CD and Persistent USB Installations
- Configuring Virtual Machines for ICS Network Assessment and Monitoring
- Packet Capture and Traffic Analysis, using tcpdump, Wireshark, and NetworkMiner
- Network Scanning and Vulnerability Assessment Tools, such as Nmap and Nessus
- Network Security Monitoring (NSM) Tools, such as Snort, Suricata, and Bro IDS

Required Equipment

Students are required to bring their own laptop computer. Students should be able to install software on their laptop and should have sufficient hard-drive space to install multiple virtual machines (32GB minimum).

Prerequisites

Students are expected to have basic knowledge of, at a minimum, the following skills:

- Linux and Windows operating systems
- Ethernet and TCP/IP networking, including the OSI 7-Layer model, addressing, and subnets;
- General network hardware, such as switches, routers, and firewalls;
- ICS network protocols

It is also recommended that students have basic knowledge of certain networking tools, such as ping, Wireshark, and nmap.

You Will Receive

Students will each receive persistent USB installations of *Kali Linux* and *Security Onion Linux*, as well as copies of the books *RTFM: Red Team Field Manual*, *Blue Team Handbook: Incident Response Edition*, and *Cybersecurity for Industrial Control Systems*.

Duration: 2 days

Level: Beginner/Intermediate

Cost: $1,295

Blue Team Training

SCADA Security & Reliability

Advanced ICS Security Exercise

This 1-day course is an aggressive, advanced, facilitated exercise where students are asked to either attack or defend a system with little prior instruction. This course is geared towards experienced cyber security professionals that desire exposure to the ICS environment. Students are broken into red or blue teams early in the day, generally based upon their previous experience or desire to experience a particular side. Students are also encouraged to collaborate and help each other learn about different attack and defense tools and techniques.

Due to the short duration of this course, the assumption is that the red-team has already breached the external network defenses and has gained access to the ICS network. The red-team will be issues a series of challenges generally following a reconnaissance, compromise, and attack process, although they will not be required to follow these exactly. Meanwhile, the blue-team will be asked to monitor and report on the performance of the system through a series of tasks, keeping the ICS equipment running. In the afternoon, the teams will be given the opportunity to present what worked, what didn't, and things that they observed during the exercise. After that, the students are given the opportunity to experiment freely with the equipment using any tools in their arsenal.

Students will be allowed to utilize their own tools, techniques, and equipment during this course as long as they are able to demonstrate them to the instructors and other students. Confidential tools, while useful, are disapproved for use during this course. Active malware, intentionally destructive tests against any equipment, and targeted attacks against the instructors or other students are disapproved and will result in dismissal from the class and possible legal action.

You Will Learn

- How different tools and techniques react in the ICS environment
- How to possibly defend against attacks on an ICS environment

Required Equipment

Students are required to bring their own laptop computer. Students should be able to install software on their laptop and should have sufficient hard-drive space to install multiple virtual machines (32GB minimum).

Prerequisites

Students are expected to have a working knowledge of, at a minimum, the following skills:

- Linux and Windows operating systems and systems administration
- Virtual machines, such as VMWare or VirtualBox
- Packet capture and traffic analysis tools, such as tcpdump, Wireshark, and NetworkMiner
- Penetration testing tools, such as Nmap, Metasploit, netcat, hping, and scapy
- Network Security Monitoring tools, such as snort, Suricata, and Bro IDS
- Shell scripting and programming with languages such as bash, sh, ruby, and python

You Will Receive

Students will each receive persistent USB installations of *Kali Linux* and *Security Onion Linux*, as well as copies of the books *RTFM: Red Team Field Manual*, *Blue Team Handbook: Incident Response Edition*, and *Cybersecurity for Industrial Control Systems*.

Duration: 1 day

Level: Advanced

Cost: $895

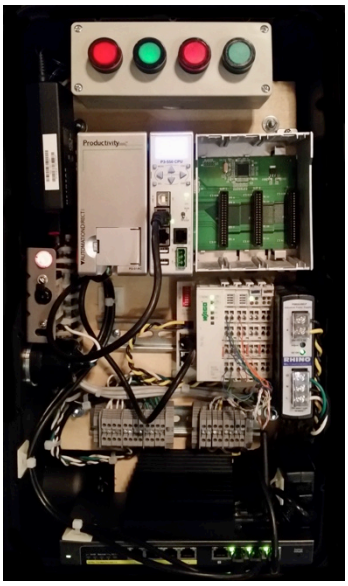
ISO 9001:2008 Certified

Blue Team Training

SCADA Security & Reliability

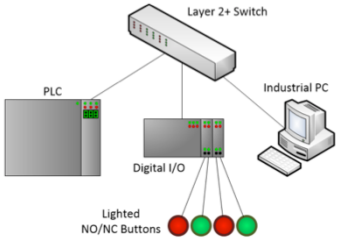
Kenexis Portable ICS Lab

The Kenexis Portable ICS Lab system is a compact industrial control system in a carry-on size rugged enclosure. The Portable ICS Lab includes a controller, inputs and outputs, a computer, a network switch, and power supplies. It is designed for demonstrations, labs, training, and can even be setup as a honeypot to attract bad actors looking for an industrial control system to affect. The basic ICS Lab system comes with a downloadable, recoverable configuration, and minimal programming. Additional configuration kits for the basic ICS Lab system are available as well as a variety of different training modules. For those users that desire a particular vendor's controller and I/O module, the option exists to use those in the basic ICS Lab system as well.



Features

- Injection Molded Wheeled Case
  - Environmentally Sealed
  - TSA Approved Carry-On (22"H x 14"W x 9"D)
- Programmable Logic Controller
  - Capable of Using EtherNet/IP or Modbus/TCP
- Digital I/O
  - Eight 24VDC Inputs, Eight 24VDC Outputs
- Industrial PC (fan less)
  - Intel Atom 2.0 GHz Processor, 2GB RAM, 240GB SSD
  - LAN Gigabit Port, WLAN 802.11 b/g/n
  - Simulated Background Network Traffic
  - Simulated HMI to PLC Network Traffic
- Layer 2+ PoE Network Switch
- Four NO/NC Lighted Buttons
- Marine-Grade 120VAC Input Power Connector
- 10 Amp AC Circuit Breaker
- Convenience 120VAC Power Plug
- 12VDC/30W, 24VDC/100W, and 48VDC/60W Power Supplies



Purchasing

* Students attending the ICS Network Blue-Team Training courses can purchase an individual Portable ICS Lab at the end of the course for a discounted rate of $8,500.

Quantity 1 = $10,000 each

Quantity 2-4 = $8,500 each*

Quantity 5-9 = $7,500 each

Quantity 10+ = $6,500 each

About Kenexis

Kenexis is an independent engineering consulting firm headquartered in Columbus, Ohio, with offices in Houston, Singapore, and Dubai. Kenexis was established in 2004, and is a privately held. Kenexis clients span the globe in many industries. Kenexis has performed engineering services for over 500 different major process industry customers in locations spanning over 20 countries.