ICS613: **ICS/OT Penetration Testing & Assessments™**

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Plan and execute safe, effective, and valuable penetration tests and security assessments using both passive and active techniques to assess operational resilience in ICS environments
- Tailor ICS penetration tests and security assessments to serve the customer's organizational and operational security objectives
- Collaborate with customers to identify realistic ICS attack scenarios targeting Crown Jewel Assets (CJA)
- Communicate and coordinate with stakeholders to define expectations, goals, and outcomes for ICS security assessments
- Understand the benefits of a top-down/bottom-up approach to active testing and how aligning penetration test methodologies to the ICS Cyber Kill chain provides appropriate adversary context to engagement activities, findings, and recommendations
- Evaluate tools and techniques for effectiveness and safety before applying them to ICS devices and networks
- Identify relevant targets and select applicable adversary TTPs for developing effective attack scenarios in ICS penetration tests and security assessments, regardless of industry sector
- Write and deliver timely status updates and accurate, actionable reports that support customer goals and outcomes

Industrial Control Systems (ICS) and Operational Technology (OT) are increasingly targeted by adversaries, yet traditional penetration testing approaches often focus on the wrong outcomes and can cause unintended disruptions with severe consequences—including production outages, injury to personnel, loss of life, and environmental hazards. ICS613: ICS/OT Penetration Testing & Assessments™ introduces engineering, operations, and security professionals with the mindset, methodologies, and techniques to safely and appropriately conduct penetration tests and security assessments, identify practical mitigations, and effectively communicate results to stakeholders and leadership to improve the operational resilience of ICS environments.

Engineering, operations, and security professionals working in industrial environments and critical infrastructure sectors around the world are increasingly required to perform penetration tests and security assessments on key systems and devices. This course provides students with the necessary knowledge and skills to perform these tasks safely while ensuring operational reliability and resiliency and achieving effective cybersecurity outcomes.

ICS613™ addresses the unique drivers and constraints of ICS environments and provides direct hands-on training to develop penetration testing and assessment capabilities specific to ICS devices, applications, architectures, communications, and process environments. By the end of this course, students will be equipped to perform real-world penetration tests and conduct security assessments of fully operational environments.

What You Will Receive

- A fully functional SANS ICS613 Student Kit that students will keep after class:
  - A CLICK PLC Plus Controller with Bluetooth and Wi-Fi, including additional modules and communication cards with a sector simulation board
  - Physical components and attachments for I/O connections to the SANS sector simulator board
  - Commercial Click PLC Programming software from KOYO Electronics
  - Commercial human machine interface (HMI) control system runtime applications from Rockwell Automation
  - Commercial OPC server application software from Matrikon
- A SANS ICS613 Windows Virtual Machine
- A SANS ICS613 Kali Virtual Machine
- Access to the in-class physical ICS range running a distributed control system (DCS) and automation components
- Unique custom tools that can be used for hardware and software asset data collection, industrial protocol network analysis, attack surface mapping, and ICS vulnerability validation

Section Descriptions

SECTION 1: ICS Assessment Types and Concepts

This section introduces students to the various types of passive and active security assessments leveraged in ICS environments.

TOPICS:

- Identify and define assessment goals and outcomes
- Choose appropriate assessment approaches aligned with industry directives, standards, and guidelines
- Apply industry frameworks and threat intelligence to security assessment
- Understand concepts, terminology, and resources related to ICS penetration testing and security assessments
- Analyze consequences and impacts to physical equipment and its operations from assessments and threat group activities

SECTION 2: ICS Assessment Engagements

This section prepares students to plan, prepare, and execute safe and effective ICS security assessments.

TOPICS:

- Outline a phased assessment methodology that includes planning, scoping, targeting, and passive and active analysis
- Collaborate and coordinate with stakeholders from engineering, operations, administrators, and cybersecurity teams
- Understand the importance of documentation, communication, and daily status reports
- Align assessment activities with the SANS Five ICS Cybersecurity Critical Controls
- Master network capture, analysis, replay, and spoofing techniques

SECTION 3: Top-Down Active Methodology

This section introduces a top-down active penetration methodology aligned to the ICS Cyber Kill Chain. Students will gain the skills to plan, prepare, and achieve engagement objectives in a simulated production DCS environment using "living off the land" techniques.

TOPICS:

- Align engagement scoping and reconnaissance with the ICS Cyber Kill Chain
- Understand how Crown Jewel Analysis (CJA) aligns with targeting activities in the ICS Cyber Kill Chain
- Understand why OT penetration test should follow an assumed breach scenario
- Understand process enumeration techniques essential for realistic ICS attack scenario development
- Identify the most effective targets and TTPs for process enumeration, regardless of industry sector

SECTION 4: Bottom-Up Passive Methodology

This section covers the bottom-up approach to ICS attack identification, delivery and execution, aligned with the ICS Cyber Kill Chain. Students will be able to develop and discuss realistic ICS attack scenarios with engagement stakeholders and gain the skills to demonstrate ICS attack impacts in controlled lab environments.

TOPICS:

- Collaborate with the customer to identify realistic ICS attack scenarios
- Focus on Attack Delivery and Attack Execution applicable to their defense readiness to identify the most effective mitigation identification
- Identify the most relevant targets and TTPs for effective attack scenario development in ICS penetration tests
- Structure accurate and actionable penetration test report
- Provide appropriate context to findings
- Identify different mitigation options balanced across cost, effectiveness and time

SECTION 5: Active Assessment and Capture-the-Flag Exercise

This lively section represents the culmination of the ICS Penetration Testing and Assessments course. Students will apply the skills mastered in the course in a comprehensive, hands-on exercise where they will continue the penetration test and assessment against their local ICS613 kit and in-class physical range. Students will be provided with the scope and rules of engagement and work to identify and prioritize the weaknesses and vulnerabilities of the target organization's industrial control systems. As a final step, students recommend next steps to improve their ICS defenses.

TOPICS:

- Conduct an unstructured ICS assessment in a real-world scenario
- Understand the impact associated with specific, learned, operational functions
- Evaluate and prioritize security recommendations to enhance ICS defenses

Who Should Attend

- Cybersecurity professionals that have a mission to assess industrial environments
- Cybersecurity professionals that must conduct cyber assessments and pen tests for regulatory compliance
- ICS red/blue/hunt/incident responders/pentesters that are looking to enhance their individual and team capabilities
- Teams conducting assessments within Federal and DoD industrial facilities or weapon systems
- Cybersecurity professionals that are looking to gain experience in safely working with industrial devices and distributed control systems
- Experienced pentesters and cyber professionals that are looking to enhance their tradecraft and skills applied to the ICS domain