About the Course

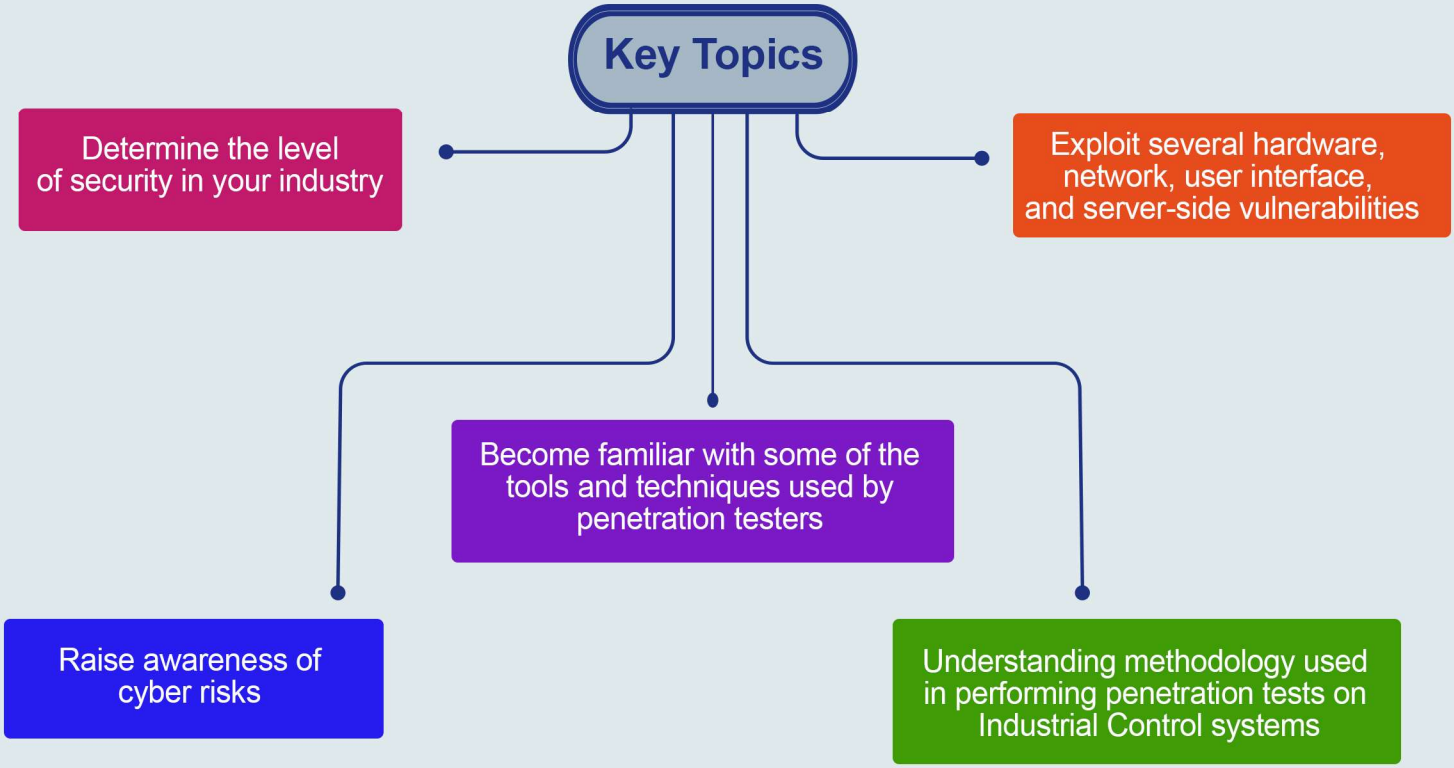
The growing openness of industrial systems (OT) significantly increases their exposure to the risks of cyber-attacks. The impact of an Industrial Control System (ICS) breach goes beyond data loss, it can result in huge financial manufacturing losses and, in the case of critical infrastructure, could potentially impact lives. This course can help overcome the many issues associated with industrial systems and is about the process of penetration testing industrial automation and control systems. Attendees will gain familiarity with the overall tools and techniques that attackers may use to compromise their systems, and witness the instructor demonstrating practical applications of such tools.

Learning Objectives

1. IACS Penetration Testing
2. External passive and active reconnaissance
3. Passive and active vulnerability discovery
4. Wireless exploitation techniques
5. Client-side attack techniques
6. Useful tools to enable ICS penetration testing

Terminus System

Key Topics



Pre Requisites

It is necessary to take the following courses:

- Ethical Hacking & Penetration Testing Concepts
- Ethical Hacking & Penetration Testing Tools
- Industrial Systems Security Essentials
- Industrial Information Security Design & Implementation

Terminus System

What You Will Receive

- Course Presentation File
- Complementary Files
- Industrial Systems Ethical Hacking & Penetration Testing eBook

Who Should Attend

- IT professionals and penetration testers interested in pen testing for ICS
- ICS Consultants
- ISA/IEC 62443 Security Experts

Syllabus

ICS Architectures and Network Pentesting

- Introduction to the NESCOR methodology for penetration testing
- Architecture Reviews of major ICS and smart grid systems and protocols
- Introduction to SamuraiSTFU (Security Testing Framework for Utilities)
- Performing traditional network pentests on control systems

Pentesting Network Architecture

- Network separation between control and node networks
- Network protocol vulnerabilities
- Identification of network access points
- Traffic capture
- Interception/modification of Command and Control
- Denial of service

Pentesting Master Server User Interfaces

- Type of ICS user interfaces
- User interface mapping
- Vulnerability discovery
- Application exploitation

Pentesting ICS Network Protocols

- Different levels of network communication penetration testing
- Serial communications
- Pentesting RF communications between master servers and field devices
- Pentesting TCP/IP based ICS protocols

Syllabus

Pentesting ICS Field and Floor Devices

- Pentesting technician interfaces on ICS field and floor devices
- Analyzing field and floor device firmware
- Overview of pentesting field and floor device embedded circuits
- Analysis of embedded electronics in ICS field and floor devices
- Dumping data at rest on embedded circuits
- Bus Snooping on embedded circuits
- Analyzing data obtained from data dumping and bus snooping
- End-to-end analysis and reporting
- Strategies for end-to-end analysis after targeted pentesting
- Strategies for reporting and remediation recommendations

Pentesting Node Service

- Weak authentication/authorization
- Sandbox issues

Pentesting RTU/PLC/IED Firmware

- Removal and overwriting
- Password/crypto key capture

Pentesting System

- Control server
- IO Server
- HMI
- Data Historian
- Engineering workstations

Hands-on Training

- Lab 1: Reconnaissance using tools such as Shodan, Spiderfoot, DNS
- Lab 2: Discover possible targets on ICS networks using Wireshark and Nmap
- Lab 3: Vulnerability discovery for ICS using Nessus
- Lab 4: Man-in-the-Middle Attack against Ethernet IP communications
- Lab 5: Wireless Attack Vectors
- Lab 6: Client-side attacks against an HMI using Metasploit