Description

Delve into a comprehensive overview of Industrial Control Systems (ICS), distinguishing between IT and OT landscapes. Explore the intricacies of ICS systems, from the differences between DCS and SCADA to components like HMI, Supervisory Systems, RTUs, and PLCs. Shift focus to ICS protocols, shedding light on the ICS network, prominent protocols like Modbus and DNP3, and the nuances of ICS network analysis. Conclude with insights into ICS security, encompassing both physical and digital security measures, challenges across the ICS lifecycle, and hands-on exercises in scanning, network attack analysis, and data enumeration.

INTRO TO ICS

Module 1: ICS Overview

Dive into the world of Industrial Control Systems (ICS), distinguishing between IT and OT environments. Understand the nuances between DCS and SCADA, exploring key components like the Human Machine Interface (HMI), Supervisory Systems, RTUs, and PLCs.

IT vs. OT
Types of ICS Systems
DCS vs. SCADA
SCADA components
Human Machine Interface (HMI)
Supervisory System
Remote Terminal Units (RTUs)
Programmable Logic Controller (PLCs)

Module 2: ICS Protocols

Explore the intricacies of the ICS network landscape, delving into established ICS protocols. Gain insights into prominent protocols such as Modbus and DNP3 and master the art of ICS network analysis.

ICS Network
Known ICS Protocols
Modbus
DNP3
ICS Network Analysis

Module 3: ICS Security

Delve into the realm of ICS security, starting with foundational concepts and branching into both physical and digital protective measures. Understand the unique challenges across the ICS lifecycle. Engage in hands-on exercises, from scanning devices and analyzing network threats to enumerating ICS data and tampering with registers.

ICS Security Overview
Basic Security Concepts
Physical Security
Digital Security
ICS Lifecycle Challenges
Hands-On
Scanning Devices
Analyzing Network Attacks
Enumerating ICS Data
Tempering with Registers

CX ICS | LEVEL: 7 | DURATION: 24h