

Syllabus

Intro to ICS/SCADA



CVBERIUM ARENA
-SIMULATOR-

Description

The Intro to ICS/SCADA program was constructed primarily for the security industry and was meant to equip participants with understanding the ICS world. Energy companies, telecommunications, transportation, healthcare, and many other such industries are perceived as critical infrastructure for the state's continual maintenance. SCADA (Supervisory Control and Data Acquisition) systems are considered the "weak link" in the defense chain, for reasons you will discover throughout the training.

Target Audience

This course targets participants new to the world of OT to give them an understanding of the way these systems work.

Pre-requisites

Networking

Objectives

- Getting familiar with the Industrial Control System world
- Expand ICS knowledge in both methodologies and techniques

Module 1: ICS overview

Students will get an overview of the ICS/SCADA and learn the basics and structure of Industrial Control Systems during this module.

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)

ICS security overview

- Basic Security Concepts

- Physical Security

- Digital Security

- ICS Lifecycle Challenges

Module 2: ICS Protocols

Students will get an overview of the general ICS/SCADA protocols of Industrial Control Systems during this module and learn to understand how they work.

ICS Network

- Known ICS Protocols

- Modbus

- DNP3

- How to Approach Protocols Research

- ICS Protocol Fuzzing