



## Descripción

Sumérgete en el complejo y fascinante mundo del desarrollo de exploits con nuestro curso integral. Desde principios fundamentales de programación hasta las sutilezas avanzadas de técnicas de explotación, este curso está diseñado para equiparte con las habilidades y conocimientos para dominar el arte de identificar vulnerabilidades y crear exploits precisos. Con ejercicios prácticos y orientación experta, estarás preparado para asegurar sistemas de manera efectiva y navegar por el paisaje en constante evolución de la ciberseguridad.

# CX401 – INTRO A SISTEMAS DE CONTROL INDUSTRIAL (ICS)

## Módulo 1: Visión General de ICS

Sumérgete en el mundo de los Sistemas de Control Industrial (ICS), distinguiendo entre los entornos de IT y OT. Entiende las sutilezas entre DCS y SCADA, explorando componentes clave como la Interfaz Hombre-Máquina (HMI), Sistemas Supervisorios, Unidades Terminales Remotas (RTUs) y Controladores Lógicos Programables (PLCs).

### IT vs. OT

Tipos de Sistemas ICS

### DCS vs. SCADA

Componentes de SCADA

Interfaz Hombre-Máquina (HMI)

Sistema Supervisorio

Unidades Terminales Remotas (RTUs)

Controlador Lógico Programable (PLCs)

## Módulo 2: Protocolos de ICS

Explora las complejidades del paisaje de la red de ICS, profundizando en los protocolos establecidos de ICS. Obtén perspectivas sobre protocolos prominentes como Modbus y DNP3 y domina el arte del análisis de redes ICS.

### Red de ICS

Protocolos de ICS Conocidos

Modbus

DNP3

Análisis de la Red de ICS

## Módulo 3: Seguridad de ICS

Profundiza en el ámbito de la seguridad de ICS, comenzando con conceptos fundamentales y ramificando hacia medidas protectoras físicas y digitales. Entiende los desafíos únicos a lo largo del ciclo de vida de ICS. Participa en ejercicios prácticos, desde escanear dispositivos y analizar amenazas de red hasta enumerar datos de ICS y manipular registros.

### Visión General de la Seguridad de ICS

Conceptos Básicos de Seguridad

Seguridad Física

Seguridad Digital

Desafíos del Ciclo de Vida de ICS

### Práctica

Escaneo de Dispositivos

Análisis de Ataques de Red

Enumeración de Datos de ICS

Manipulación de Registros