

CURSO PROFESIONAL DE PENTESTING CONTRA ICS/SCADA

Spartan-Cybersecurity



CPICS-100



ADVERTENCIA

Todos los derechos reservados. Ninguna parte de esta publicación, en su totalidad o en parte, puede ser reproducida copiada, transferida o cualquier otro derecho reservado a su propietario, incluyendo la fotocopia y cualquier otra copia, cualquier transferencia o transmisión utilizando cualquier red u otros medios de comunicación, cualquier emisión para el aprendizaje a distancia, en cualquier forma o por cualquier medio, como cualquier sistema de almacenamiento, transmisión o recuperación de información, sin autorización escrita del autor.

TODO nuestro contenido publicado se realiza con fines educativos, informativos y éticos.

TODAS las técnicas expuestas en este curso son desarrolladas y ejecutadas en entornos controlados.

¡NO SOMOS RESPONSABLES DEL MAL USO QUE LE PUEDAN DAR!



TABLA DE CONTENIDO

1. Introducción al Curso de Pentesting en ICS/SCADA – (CPICS)
 - a. Bienvenida y objetivos del curso
 - b. Requisitos previos y materiales necesarios
 - c. Estructura y metodología del curso

2. Fundamentos de CPICS (Control de Procesos Industriales Cibernéticos)
 - a. Definición y componentes clave
 - b. Relevancia en la seguridad industrial

3. Configuración del Entorno de Trabajo
 - a. Herramientas y software necesarios
 - b. Configuración de laboratorios virtuales y físicos
 - c. Instalación de ControlThings

4. Comparativa entre IT y OT (Tecnologías de la Información vs. Tecnologías de Operación)
 - a. Diferencias fundamentales y convergencias
 - b. Implicaciones en seguridad

5. Profundización en ICS (Sistemas de Control Industrial)
 - a. Breve historia y evolución
 - b. Arquitectura y componentes de ICS
 - c. Tipos y topologías de ICS
 - d. Sistemas discretos, analógicos y digitales: comparativa y casos de uso



6. Introducción a SCADA (Control de Supervisión y Adquisición de Datos)
 - a. View Componentes clave: HMI, View, Monitor, Control
 - b. Funcionamiento y aplicaciones

7. Casos de estudio en ICS/SCADA
 - a. Stuxnet
 - b. Blackenergy
 - c. Triconex
 - d. Casos recientes de 2023: tendencias y lecciones aprendidas

8. Dispositivos IoT y IIoT en el ámbito industrial
 - a. Diferencias y similitudes
 - b. Impacto en la seguridad de ICS/SCADA

9. Componentes Clave de ICS
 - a. ¿PLC, RTU, IED, PAC: funciones y diferencias
 - b. Comunicaciones críticas y protocolos industriales (Modbus, DNP3, OPC UA, Ethernet/IP, PROFIBUS)

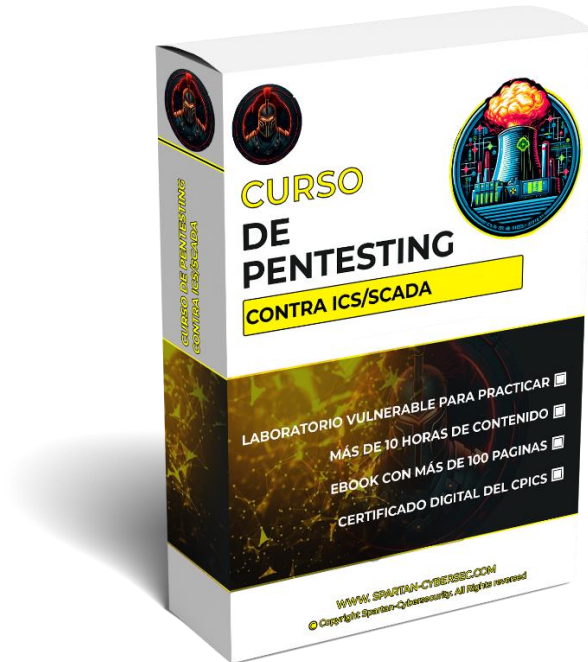
10. Enumeración de dispositivos de Control Industrial
 - a. OSINT aplicado a ICS
 - b. Enumeración y detección de servicios de control industrial
 - i. Nmap
 1. Escaneo de puertos
 2. Utilizando s7-enumerate.nse
 - ii. Metasploit
 - iii. Python Tools
 1. Utilizando plcscan



11. Atacando Modbus
 - a. Explotación de vulnerabilidades en Modbus
 - b. Inyección de comandos Modbus maliciosos con herramientas
 - i. Mbtget
 - ii. MSF
 - iii. Python

12. Hacking de SCADA e Interfaces HMI
 - a. Man in the Middle
 - b. Buffer Overflow
 - c. ARP Spoofing en HMI
 - d. Análisis de tráfico en SCADA
 - e. Detección de tráfico con protocolos inseguros
 - f. Credenciales por defecto en SCADA
 - g. Uso de Wireshark y filtros específicos para SCADA
 - h. Password Spraying
 - i. Uploading Malicious PLC Programs

DETALLES DEL CURSO



Material entregable:

- ✓ Acceso a laboratorio.
- ✓ Acceso a más de 8 horas de contenido en MATERIAL GRABADO.
- ✓ Acceso a un grupo exclusivo del curso para interactuar con los demás estudiantes y el profesor.
- ✓ E-Book Virtual.
- ✓ Certificado del CPICS por parte de Spartan-Cybersecurity.

Costo del curso: \$200 USD

Comunícate con el área de ventas:

Whatsapp: <https://wa.link/j265a0>

Telegram: https://t.me/Spartan_Cybersecurity

CUPOS LIMITADOS.