GSPT®

Scada Penetration Tester

Sabemos que la única forma de aprender es haciendo. Por lo mismo todos los laboratorios son con desafíos de hacking en un ambiente en vivo. Con servidores y servicios dentro de nuestro laboratorio de hacking, para que nuestros alumnos tengan una experiencia real.

100% Laboratorio en vivo

G|SPT® está diseñado para formar profesionales con habilidades "practicas" de Pentesting y conocimiento de los sistemas industriales siguiendo metodología abiertas y reconocidas internacionalmente.

GSPT® es un entrenamiento intensivo de hacking de sistemas SCADA.

El programa tiene foco en que el alumno conozca el diseño, funcionamiento y vulnerabilidades de los sistemas industriales, para adelantarse a los futuros atacantes de los sistemas SCADA.

A diferencia de otros entrenamientos teóricos, este entrenamiento brinda las habilidades practicas para luego de terminado el entrenamiento, poder realizar auditorias reales de seguridad y pentesting de seguridad en clientes industriales.

En el laboratorio podrá obtener un profundo conocimiento de las nuevas técnicas, herramientas y metodologías. Comenzando por explorar el perímetro, descubrir servicios, protocolos, direcciones IP y vulnerabilidades asociadas. Por supuesto ninguna red real es atacada, pues nuestro laboratorio esta cerrado únicamente para los alumnos del entrenamiento.

Usted también aprenderá los fundamentos de la ingeniería reversa en hardware. En este aprenderá de placas, PCB, Chips I2C y SPI, entre otros. También aprenderá como obtener acceso a su memoria (inclusive si esta prendido).

GSPT® Scada Penetration Tester

G|SPT®

SCADA Penetration Tester consiste en 13 módulos base diseñados para obtener una profunda inmersión en Pentesting de Sistemas Industriales ICS/SCADA.

MÓDULOS G|SPT

- Arquitectura ICS
- Metodología Nescor para Pentesting en Sistemas Industriales
- Enumeración y Descubrimiento
- Network Pentesting ICS
- Pentesting Interfaces de Usuario HMI (Human Machine Interfaces)
- Pentesting Protocolos de Red ICS
- Pentesting ICS Field & Floor Devices
- Software Defined Radio (SDR)
- Reversing de Hardware
- Fuzzing a Protocolos de Red ICS
- Fuzzing AMI Smart Meter
- Ataques Físicos hacia ataques remotos I2C/SPI Bus Sniffing

Estado del Arte...

Cada modulo incluye las ultimas técnicas y ataques conocidos, los cuales están diseñados por expertos auditores, ethical hackers y pentesters con mas de 15 años de experiencia.

GSPT® Scada Penetration Tester

Audiencia:
Este curso esta dirigido a oficiales de seguridad, auditores, profesionales de seguridad, administradores de sistemas, administradores de redes y cualquier profesional con necesidad de proteger la integridad de su infraestructura industrial SCADA.

Duración:
5 días de 9AM a 6:30PM (45 horas)

Certificación:
El examen de certificación dura 48 Horas de corrido (24 Horas para realizar la auditoria y 24 horas para crear un informe de auditoría)

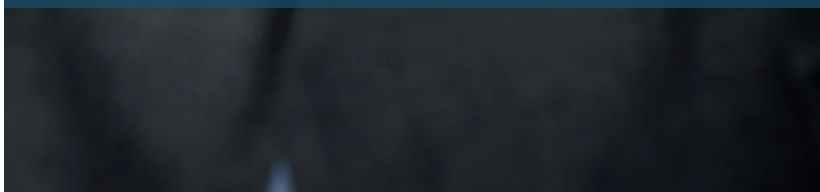
El examen práctico se realiza conectándose a una red con servidores Industriales SCADA reales a los cuales se les debe realizar una auditoria de seguridad como se realizaría en un cliente real. El alumno para aprobar debe enviar un informe de auditoria con evidencia del acceso a los PLC's o

Sistemas SCADA. El alumno tiene 24 horas para realizar las pruebas y 24 horas para entregar su informe.

Los resultados son revisados por un comité, el cual en 72 horas responderá al alumno para confirmar si aprobó o no su examen.

El examen de certificación esta 100% en Español

Esta es una certificación que reconoce no solo el conocimiento en el uso de técnicas de hacking y auditoria en Sistemas ICS/SCADA, sino la práctica y experiencia en el mundo real. Siendo un real diferenciador para sus certificados.



GSPT® Scada Penetration Tester

GSPT®
Scada Penetration Tester

INCLUYE

- Kit Alumno Electronico 100% Español
- Manual de Laboratorio 100% Español
- 1 voucher para tomar Examen G|WPT
- Diploma de Asistencia

GLOBALSECURE
ACADEMY