Curso Hacking ICS / SCADA 2022

Domingos 14 y 21 de Agosto del 2022. De 9:00am a 12:00am (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Presentación

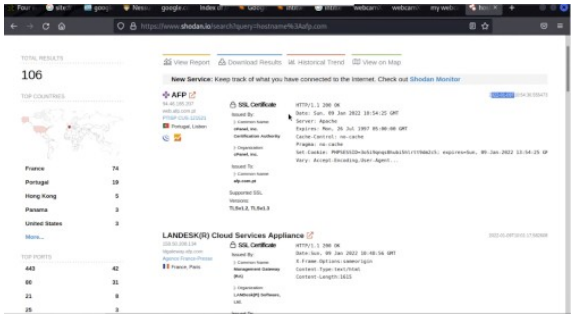
Los procesos para la automatización industrial, utilizan sistemas de control industrial (ICS) y sistemas de control para la supervisión y adquisición de datos (SCADA), con el propósito de controlar procesos industriales de forma local o remota, además de vigilar, recopilar, y procesar datos en tiempo real.

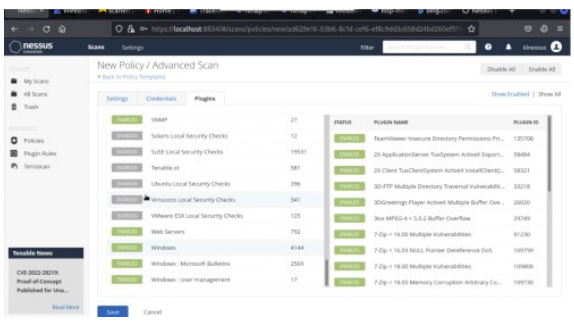
ICS / SCADA se han convertido en objetivos de alta prioridad para los ciberatacantes. Con la naturaleza dinámica de los sistemas de control industrial, muchos profesionales no comprenden completamente las características y los riesgos de muchos dispositivos. Además personal TI para soporte, quien proporciona las vías de comunicación y defensas de la red, no siempre comprende los controladores y limitaciones operacionales de los sistemas.

Este curso proporciona un conjunto sólido de conocimientos y habilidades estandarizadas para los profesionales en ciberseguridad. Estando dirigido para todos aquellos involucrados con los sistemas de control industrial, para estén en la capacidad de mantener el entorno a salvo, seguro, y con resiliencia ante las amenazas actuales y emergentes. Paralelamente se aborda la necesidad de los profesionales involucrados con los sistema de control industrial, comprendan mejor el importante rol el cual desempeñan en ciberseguridad. Y esto empieza garantizando un sistema de control sea diseñado con la ciberseguridad incorporada, además de tener el mismo nivel de atención de la fiabilidad del sistema a lo largo de su ciclo de vida.

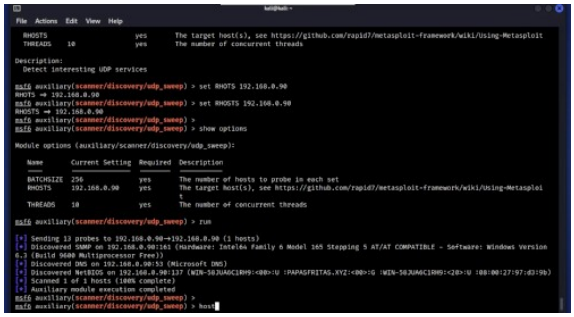
Temario

- Tecnología Operacional – OT
- Terminología OT Esencial
- Convergencia OT / IT
- Modelo Purdue
- Retos del OT
- Introducción a Sistemas de Control Industrial - ICS
- Sistemas para Control Distribuido - DCS
- Control para la Supervisión y Adquisición de Datos - SCADA
- Controlador Lógico Programable - PLC
- Sistema básico para Control de Procesos - BPCS
- Sistemas Instrumentados de Seguridad - SIS
- Tecnologías y Protocolos OT
- Vulnerabilidades de OT
- Amenazas en OT
- Ataques basados en HMI
- Ataques para el Lago del Canal
- Hacking PLC
- Hacking a través de RF





- Malware OT
- Hacking OT
- Metodología de Hacking para OT
- Identificar Sistemas ICS/SCADA
- Obtener Contraseñas por Defecto
- Escanear Sistemas ICS/SCADA
- Escaneo de Vulnerabilidades
- Esnifar y Analizar Tráfico OT
- Explotar Vulnerabilidades OT



Material

Todos los participantes al Curso Virtual de Hacking ICS / SCADA tendrán la posibilidad de descargar los videos de cada sesión, un día después de impartida la misma.

- **Kali Linux:**
  Link de Descarga: https://www.kali.org/get-kali/

Fechas y Horario

El Curso Virtual de Hacking ICS / SCADA tiene una duración total de seis (6) horas, las cuales se dividen en dos (2) sesiones de tres (3) horas cada una.

- **Fechas:**

  Domingos 14 y 21 de Agosto del 2022

- **Horario:**

  De 9:00 am a 12:00 pm (UTC -05:00). 6 horas en total.

[*] El Curso se dicta sin ningún requisito mínimo en el número de participantes.

Inversión y Forma de Pago:

Acceso a todos los videos y material:

S/. 175 Soles o $ 55 Dólares

Acceso al aula virtual por 30 días, todos los videos, material, evaluaciones, certificado de participación y certificado de aprobación.

S/. 260 Soles o $ 80 Dólares

El pago del curso se realiza mediante alguno de los siguientes mecanismos:

Residentes en Perú	Residentes en Otros Países
Deposito bancario o transferencia interbancaria en la siguiente cuenta: Scotiabank ScotiaBank Cuenta de Ahorros en Soles: 324-0003164 A nombre de: Alonso Eduardo Caballero Quezada CCI: 009-324-203240003164-58	Transferencia de dinero mediante Western Union y MoneyGram o pago por Paypal: MoneyGram · Western Union · PayPal Escriba por favor un mensaje de correo electrónico a caballero.alonso@gmail.com para proporcionarle los datos requeridos.

Confirmado el pago se enviará al correo electrónico del participante, los datos necesarios para conectarse hacia la plataforma, además de toda la información pertinente para su participación en el curso

El curso se realiza utilizando el sistema para video conferencias de nombre Anymeeting. El cual proporciona transmisión de audio y video HD en alta calidad, tanto para el instructor y los participantes, entre otras características ideales para el dictado de cursos virtuales o en línea.

INTERMEDIA ANYMEETING

Más Información

Para obtener más información sobre este curso virtual, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico: caballero.alonso@gmail.com

Teléfono: +51 949 304 030

Sitio Web: https://www.reydes.com

Instructor

Alonso Eduardo Caballero Quezada. EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). He sido instructor, expositor y conferencista en el OWASP LATAM Tour, OWASP Perú Chapter Meeting, OWASP LATAM at Home, PERUHACK, PERUHACKNOT, 8.8 Lucky Perú, Ekoparty University Talks Perú. Cuento con más de diecisiete años de experiencia en el área y desde hace trece años laboro como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Pertenecí por muchos años al grupo internacional RareGaZz y grupo Peruano PeruSEC. He dictado cursos para España, Ecuador, México, Bolivia y Perú, presentándome también en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre.