Curso Hacking OT 2024

Sábados 20 y 27 de Abril del 2024. De 9:00am a 12:00am (UTC -05:00)

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

Presentación

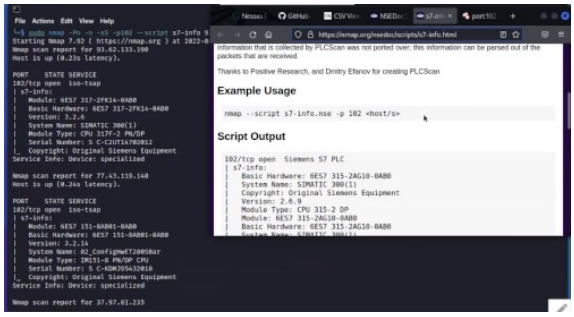
La tecnología operacional, OT por sus siglas en inglés, tiene un rol muy importante en la sociedad actual, pues dirige un diverso conjunto de hardware y software diseñados para trabajar juntos, como un sistema integrado, u homogéneo, teniendo como propósito controlar y supervisar dispositivos físicos industriales. Estos dispositivos incluyen interruptores, bombas, luces, sensores, cámaras para vigilancia, ascensores, robots, válvulas y sistemas para refrigeración y calefacción.

OT se han convertido en una objetivo atractivo y de alta prioridad para los ciberatacantes. Con la naturaleza dinámica y altamente crítica de este tipo de sistemas, muchos profesionales no comprenden completamente las características y los riesgos de esta área. Además personal de 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.

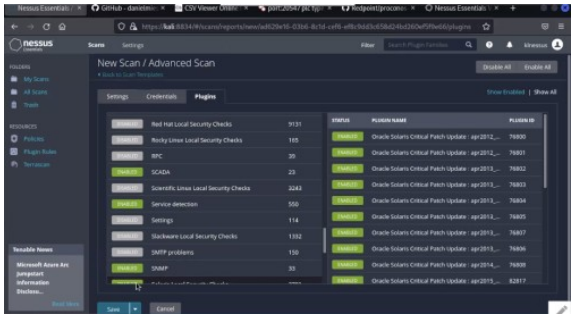
Este curso proporciona un conjunto sólido de conocimientos y habilidades estandarizadas para los profesionales en ciberseguridad. Estando dirigido a todos aquellos involucrados con tecnologías operacional, para estén en la capacidad de mantener el entorno a salvo, seguro, y con resiliencia ante las ciberamenazas actuales y emergentes. De manera paralela se abarca la necesidad de los profesionales involucrados con la tecnología operacional, comprendan mejor el importante y crítico rol el cual desempeñan en ciberseguridad. Y esto empieza garantizando un sistema de tecnología operacional, esté diseñado con ciberseguridad incorporada, además de tener el mismo nivel de atención en lo referente a la fiabilidad del sistema en el transcurso de su ciclo de vida.

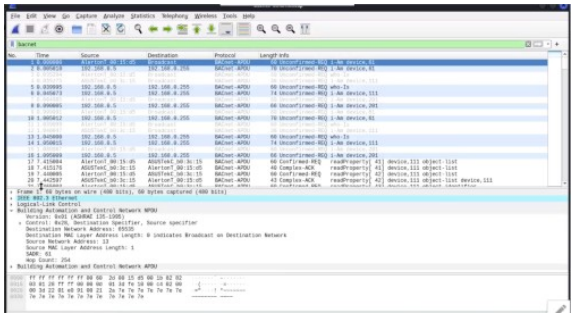
Temario

- Tecnología Operacional – OT
- ¿Qué es Tecnología Operacional?
- Terminología OT Esencial
- Convergencia OT / IT
- Beneficios de Fusionar OT con IT
- Modelo Purdue
- Retos del OT
- Introducción a Sistemas de Control Industrial – ICS
- Componentes de un ICS
- Arquitectura de un 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



- Ataques 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
- Metodología de Hacking para OT
- Identificar Sistemas ICS/SCADA
- Obtener Contraseñas por Defecto
- Escanear Sistemas ICS/SCADA
- Escaneo de Vulnerabilidades
- Analizar Tráfico Modbus/TCP
- Explotar Vulnerabilidades OT





Fechas y Horario

El Curso Virtual de OT Tecnología Operacional tiene una duración total de seis (6) horas, las cuales se dividen en dos (2) sesiones de tres (3) horas cada una.

- **Fechas:**

  Sábados 20 y 27 de Abril del 2024

- **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.

Beneficios e Inversión:

- Acceso a las sesiones en vivo
- Acceso al aula virtual por 45 días
- Video de las dos (2) sesiones
- Material utilizado durante el desarrollo del curso
- Asesoría personalizada
- Libro "Fundamentos de Hacking Ético" escrito por el instructor
- Certificado digital de participación
- Certificado digital de aprobación. Puntuación mínima 70/100. Por una duración total de 16 horas

S/. 225 Soles o $ 70 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	Pago a través de PayPal. O también transferencia de dinero mediante Western Union y MoneyGram PayPal Escriba por favor un mensaje de correo electrónico a reydes@gmail.com para proporcionarle los datos pertinente para realizar el pago.

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

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

ISC2 Certified in Cybersecurity (CC), LPI Security Essentials Certificate, EXIN Ethical Hacking Foundation Certificate, 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, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE). 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 dieciocho años de experiencia en el área y desde hace catorce 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. Mi correo electrónico es ReYDeS@gmail.com y mi página personal está en: https://www.ReYDeS.com