Curso Informática Forense 2024

Domingos 6, 13, 20 y 27 de Octubre del 2024. De 9:00 am a 12:00 pm (UTC -05:00)

Presentación

En la actualidad todas las empresas y organizaciones deben estar preparadas para enfrentar exitosamente diversos tipos de crímenes cibernéticos, los cuales se suscitan y afectan sus sistemas de cómputo y redes. Consecuentemente se ha incrementado la demanda por profesionales forenses debidamente entrenados y experimentados, quienes estén en la capacidad investigar crímenes cibernéticos relacionados a fraudes, amenazas internas, espionaje industrial, inadecuado uso de los empleados, e intrusiones hacia computadoras y redes Las agencias del gobierno a nivel mundial también requieren profesionales forenses debidamente entrenados y con amplia experiencia en el ámbito del forense digital.

Objetivos

Este curso enseña a los participantes a desarrollar un profundo conocimiento sobre forense digital aplicado al sistema operativo Microsoft Windows. Es fundamental comprender las capacidades forenses y artefactos en estos sistemas. Aprender a identificar, capturar, autenticar, y analizar datos forenses. Entender como se puede rastrear detalladamente la actividad realizada del usuario a través de la red, además de como organizar sus hallazgos para ser utilizado en una respuesta de incidentes, investigaciones internas, y litigios civiles o penales. Utilizar los nuevos conocimientos adquiridos para validar las herramientas de seguridad, mejorando las evaluaciones de seguridad, identificar amenazas internas, rastrear atacantes, y mejorar las políticas de seguridad. Aunque se conozca o no, el sistema operativo Windows silenciosamente registra una gran cantidad de datos sobre el propio sistema y los usuarios. Este curso enseña una metodología para forense de computadoras con etapas de identificación, preservación, análisis y documentación. Se exponen técnicas y procedimientos de investigación manuales, también se utilizan herramientas forenses.

Alonso Eduardo Caballero Quezada.

ISC2 Certified in Cybersecurity (CC), 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), y 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 veinte años de experiencia en el área, y desde hace dieciséis años laboro como consultor e instructor en 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 PerúMi correo electrónico es ReYDeS@gmail.com y mi página personal está en: www.ReYDeS.com

Fechas & Horarios

Duración: Catorce (14) horas. Una (1) sesión previamente grabada de dos (2) horas, y cuatro (4) sesiones en vivo de tres (3) horas de duración cada una.

Fechas:

Domingos 6, 13, 20, y 27 de Octubre del 2024

Horarios:

De 9:00 am a 12:00 pm (UTC -05:00)

Más Información

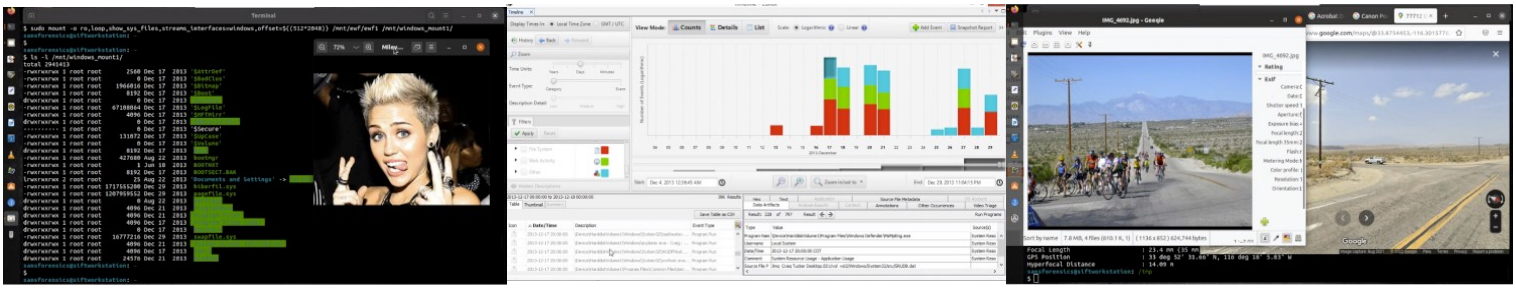
Para obtener más información sobre este curso, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico:

reydes@gmail.com

Teléfono: +51 949 304 030

Sitio Web: www.reydes.com



Temario

- Proceso Investigación Forense
- Evolución del Sistema de Archivos Windows
- FTK Imager
- Adquisición de la Memoria RAM
- Evidencia Encriptada
- Obtener Archivos Protegidos
- Imagen con Contenidos Personalizado
- Discos de Estado Sólido (SSD)
- Nivelación de Uso y SSD Trim
- Artefactos Forenses en SSD
- Adquisición de un USB y Disco Duro
- Montar una Imagen
- Visualización Previa de una Unidad
- Recuperar Archivos Borrados
- The Sleuth Kit (TSK)
- Flujos de Datos Alternativos
- Volume Shadow Copy
- Autopsy
- Búsqueda de Cadenas
- Reconstrucción de Datos
- Análisis Forense a la Memoria RAM
- Volatility Framework
- Forense de Correos Electrónicos
- Forense al Registro de Windows
- Lo Esencial del Registro
- Análisis de Información de Usuarios y Grupos
- Análisis de la Configuración del Sistema
- Análisis de la Actividad del Usuario
- Análisis de la Actividad USB
- Archivos de Enlace
- Metadatos en Documentos Office
- Metadatos en Documentos PDF
- Metadatos en Archivos de Medios (EXIF)
- Análisis de Miniaturas
- Análisis de la Papelera de Reciclaje
- Análisis de Archivos Prefetch
- Fundamentos del Registro de Eventos
- Análisis del Registro de Eventos (Logs)
- Registro de Eventos en Windows
- Forense al Navegador Web
- Fundamentos de los Navegadores
- Internet Explorer
- Archivos del Historial Cache / Archivos Temporales
- Cookies, Historial de Descarga

Material

- SIFT Workstation
- Imágenes Forenses Windows
- Herramientas Windows

Beneficios e Inversión

- Acceso a las sesiones en vivo
- Acceso al aula virtual por 45 días
- Video de las cinco (5) sesiones
- Material utilizado durante el desarrollo del curso
- Dos (2) horas de asesoría en vivo personalizada por videoconferencia.
- Libro "Fundamentos de Forense Digital" escrito por el instructor
- Certificado digital de participación
- Certificado digital de aprobación (CMIF). Puntuación mínima 70/100). Por una duración total de 24 horas

S/. 450 Soles o $ 140 Dólares

El pago del curso se realiza:

Residentes en Perú

Depósito bancario Scotiabank

Cuenta de Ahorros en Soles: 324-0003164
A nombre de: Alonso Eduardo Caballero Quezada

O también pagos con Yape o Plin. Escriba un mensaje de correo electrónico a reydes@gmail.com para proporcionarle los datos pertinentes.

Residentes en otros países

Pago a través de Paypal PayPal

O también transferencia de dinero mediante Western Union y MoneyGram

Escriba por favor un mensaje de correo electrónico a reydes@gmail.com para proporcionarle los datos.

Confirmado el pago se enviará los datos para conectarse hacia la plataforma

Certificados

Certificados; constancias de participación y aprobación; expedidos a nombre de la empresa Peruana MILESEC EIRL.