Curso Virtual Forense de Redes 2021

Domingos 6, 13, 20 y 27 de Junio del 2021. De 9:00 am a 12:15 pm (UTC -05:00)

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

Presentación

En la actualidad es muy común trabajar en cualquier investigación forense relacionada a un componente de red. El forense de computadoras siempre será un habilidad fundamental y crítica para esta profesión, pues obviar las comunicaciones de red, es similar a ignorar las imágenes proporcionadas por las cámaras de seguridad correspondientes a un crimen cometido. Ya sea se enfrente un incidente relacionado con una intrusión, un caso de robo de datos, uso indebido por parte de los empleados, o se esté involucrado en el descubrimiento pro activo del adversario, la red frecuentemente proporciona una vista incomparable del incidente. Esta evidencia puede proporcionar la prueba necesaria para mostrar intención, descubrir los atacantes han estado activos por meses o más, o incluso puede resultar útil para probar definitivamente la ocurrencia de un delito.

Objetivos

Este curso enseña a construir los conocimientos fundamentales necesarios para realizar investigaciones eficientes y efectivas. Enfocándose en aquello necesario para expandir la mentalidad del forense digital, desde los datos residuales contenidos en los medios de almacenamiento de un sistema o dispositivo, hasta las comunicaciones transitorias las cuales ocurrieron anteriormente o continúen ocurriendo. Incluso si un atacante remoto muy hábil compromete un sistema con un exploit no detectable, el sistema debe comunicarse a través de la red. Sin los canales de comando y control para la extracción de datos, el valor de un sistema comprometido se reduce casi a cero. Expresado de otra manera; mientras los atacantes se comunican a través de la red, este curso enseña como escucharlos y analizarlos de diversas maneras.

Alonso Eduardo Caballero Quezada es 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). Ha sido instructor en el OWASP LATAM Tour, expositor en OWASP Perú Chapter Meeting y OWASP LATAM at Home , además de Conferencista en PERUHACK, instructor en PERUHACKNOT, y conferencista en 8.8 Lucky Perú. Cuenta con más de dieciséis años de experiencia en el área y desde hace doce años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Perteneció por muchos años al grupo internacional RareGaZz y PeruSEC. Ha dictado cursos en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre. Su correo electrónico es **ReYDeS@gmail.com** y su página personal está en: **https://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 Junio 2021

Horario:

De 9:00 am a 12:15 pm (UTC -05:00)

Más Información

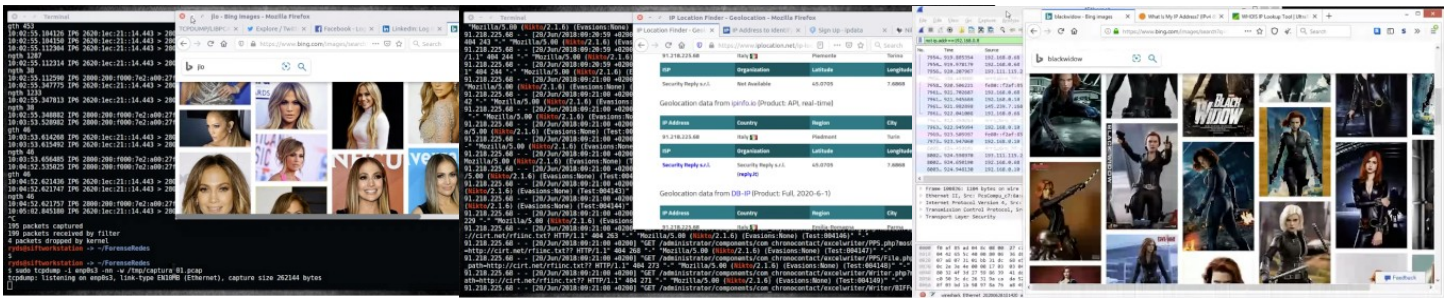
Para obtener más información sobre este curso virtual, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico:

caballero.alonso@gmail.com

Teléfono: (+51) 949 304 030

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



Temario: (Actualizado)

- Introducción al Forense de Redes
- Brechas de Datos
- Diferencias entre Forense de Computadoras y Redes
- Profundizar Conocimientos Técnicos
- Entender la Seguridad de Red
- Objetivos de la Seguridad de Red
- Consideraciones sobre Manipulación de Evidencia
- Identificar Fuentes de Evidencia
- Conocer el Manejo de Evidencia
- Recolección del Trafico de la Red
- Recolección de Logs de la Red
- Captura de Memoria
- Capturar y Analizar Paquetes de Datos
- Interceptar el Tráfico de la Red
- Sniffing y Análisis de Paquetes
- Evidencia en Redes Inalámbricas
- Entender la Protección y Seguridad Inalámbrica
- Ataques Comunes a Redes Inalámbricas
- Analizar y Capturar Tráfico Inalámbrico
- Rastrear un Intruso en la Red
- Entender los Sistemas de Detección y Prevención de Intrusos.
- Diferencias entre IDS e IPS
- El Registro de Sucesos
- Entender los Formatos de los archivos Logs
- Descubrir la Conexión entre los Logs y el Forense
- Proxys, Firewall y Routers
- Analizar un Proxy
- Investigar un Firewall
- Conocer un Router
- Saltándose Protocolos Prohibidos
- Entender los VPNs
- Funcionamiento de “Tunneling”
- Tipos de Protocolos para “Tunneling”
- Investigar Malware
- Conocer el Malware
- Tipos de Malware y su Impacto
- Entender el Comportamiento de un Malware
- Realizar un Forense a Malware
- Cerrando o Resolviendo el Caso
- Revisar la Adquisición y Análisis de la Evidencia
- Reportar el Caso

Material

- SANS SIFT
- Herramientas Windows

Inversión y Forma de Pago

Este curso tiene un costo de:

S/. 350 Soles o $ 110 Dólares

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

Residentes en Perú

Depósito bancario en la siguiente cuenta:

Scotiabank

Scotiabank Perú SAA
Cuenta de Ahorros en Soles: 324-0003164
A nombre de: Alonso Eduardo Caballero Quezada
Código de Cuenta Interbancario (CCI): 009-324-203240003164-58

Residentes en otros países

Transferencia de dinero mediante Western Union y MoneyGram o pago por Paypal

Escribir por favor un mensaje de correo electrónico caballero.alonso@gmail.com para indicarle los datos necesarios para realizar el pago.

Confirmado el depósito o la transferencia se enviará al correo electrónico del participante, los datos necesarios para conectarse a la plataforma, además de la información pertinente para su participación en el curso.

INTERMEDIA ANYMEETING

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.