EC-Council

EC-Council

Computer Hacking Forensic Investigator

Todo crimen deja detrás un rastro de evidencia

Descripción del curso

La Investigación Forense de Hackeo Informática (CHFI) es el proceso de detectar ataques de hackeo y extraer adecuadamente evidencia para informar el delito y realizar auditorías para prevenir futuros ataques.

La informática forense es simplemente la aplicación de técnicas de investigación y análisis informático con el fin de determinar la evidencia legal potencial. Se puede buscar evidencia en una amplia gama de delitos informáticos o uso indebido, incluidos, entre otros, el robo de secretos comerciales, el robo o la destrucción de la propiedad intelectual y el fraude.

Los investigadores de CHFI pueden recurrir a una variedad de métodos para descubrir datos que residen en un sistema informático o para recuperar información de archivos eliminados, cifrados o dañados conocida como recuperación de datos informáticos.

INCIDENT

¿Quién debería asistir?

- Policía y otro personal de aplicación de la ley
- Personal de defensa y militar
- Profesionales de seguridad de comercio electrónico
- Administradores de sistemas
- Profesionales del derecho
- Banca, Seguros y otros profesionales.
- Agencias gubernamentales
- Gerentes de TI

Agenda del curso

Duración: 40 horas

Module 01: Computer Forensics in Today's World

Module 02: Computer Forensics Investigation Process

Module 03: Understanding Hard Disks and File Systems

Module 04: Data Acquisition and Duplication

Module 05: Defeating Anti-Forensics Techniques

Module 06: Windows Forensics

Module 07: Linux and Mac Forensics

Module 08: Network Forensics

Module 09: Malware Forensics

Module 10: Investigating Web Attacks

Module 11: Dark Web Forensics

Module 12: Cloud Forensics

Module 13: Email and Social Media Forensics

Module 14: Mobile Forensics

Module 15: IoT Forensics

SAVANT CONSULTORES

EC-Council

Objetivos de aprendizaje

- Realizar respuesta ante incidentes y análisis forense
- Realizar colecciones de evidencia electrónica
- Realizar adquisiciones forenses digitales
- Realizar imágenes de flujo de bits / adquisición de los medios digitales incautados durante el proceso de investigación.
- Examinar y analizar textos, gráficos, multimedia e imágenes digitales.
- Realizar exámenes exhaustivos de las unidades de disco duro de la computadora y otros medios electrónicos de almacenamiento de datos
- Recupere información y datos electrónicos de los discos duros de las computadoras y otros dispositivos de almacenamiento de datos.
- Seguir procedimientos estrictos de manejo de datos y evidencia
- Mantener la pista de auditoría (es decir, la cadena de custodia) y la integridad de la evidencia.
- Trabajar en el examen técnico, análisis y reporte de evidencia basada en computadora.
- Preparar y mantener archivos de casos.
- Utilizar herramientas forenses y métodos de investigación para encontrar datos electrónicos, incluido el historial de uso de Internet, documentos de procesamiento de texto, imágenes y otros archivos.
- Recopilar información volátil y no volátil de Windows, MAC y Linux
- Recuperar archivos borrados y particiones en Windows, Mac OS X y Linux
- Realizar búsquedas de palabras clave, incluido el uso de palabras o frases objetivo
- Investigar eventos para evidencia de amenazas o ataques internos
- Apoyar la generación de informes de incidentes y otras garantías.
- Investigar y analizar todas las actividades de respuesta relacionadas con incidentes cibernéticos.
- Planificar, coordinar y dirigir actividades de recuperación y tareas de análisis de incidentes.
- Examinar toda la información disponible y la evidencia o artefactos relacionados con un incidente o evento.
- Recopilar datos utilizando métodos de tecnología forense de acuerdo con los procedimientos de manejo de evidencia, incluida la recopilación de copias impresas y documentos electrónicos
- Realizar ingeniería inversa para archivos de malware conocidos y sospechosos
- Realizar eva detallada
- dentificar datos, imágenes y / o actividades que pueden ser objeto de una investigación interna
- Establezca inteligencia sobre amenazas y puntos clave de aprendizaje para respaldar la creación de perfiles proactiva y el modelado de escenarios
- Busque en el espacio de archivo donde se emplean las tecnologías de tipo PC
- Archivar tiempos MAC (Modificado, Accedido y Crear fechas y horas) como evidencia de acceso y secuencias de eventos
- Examinar el tipo de archivo y la información del encabezado del archivo
- Revise las comunicaciones por correo electrónico, incluido el correo web y los programas de mensajería instantánea de Internet
- Examinar el historial de navegación de Internet.
- Genere informes que detallen el enfoque y un seguimiento de auditoría que documente las acciones tomadas para respaldar la integridad del proceso de investigación interna
- Recupere archivos activos, del sistema y ocultos con información de sello de fecha / hora
- Romper (o intentar descifrar) archivos protegidos con contraseña
- Realizar detección anti forense
- Mantener la conciencia y seguir el manejo de evidencia de laboratorio, examen de evidencia, seguridad de laboratorio y políticas y procedimientos de seguridad de laboratorio.
- Desempeñe un papel de socorrista asegurando y evaluando una escena del delito cibernético, realizando entrevistas

Examen

Duración: 3 horas

Nombre del examen: EC-Council Computer Hacking Forensic Investigator
Código del examen: 312-49
Cantidad de preguntas: 150
Formato: Selección múltiple
Disponibilidad: EC-Council Exam Portal
Puntuación para pasar: 60% a 85%

Certificación

El examen **C|HFI** puede ser tomado después de finalizar la aistencia al curso oficial completo de **C|HFI**.
Los candidatos que pasan con éxito el examen recibirá su certificado **C|HFI** y los privilegios de membresía.
Se espera que los miembros se adhieran a los requisitos de recertificación a través de los requisitos de Educación Continua..

Información general

- El costo del curso oficial incluye el voucher para tomar el examen
- Courseware digital con más de 1,000 páginas repletas de contenido organizado metodológicamente
- Acceso al portal Aspen.eccouncil.org donde puede acceder miles de herramientas
- Subscripción por seis meses a los laboratorios virtuales para mayor comodidad con más de 50 laboratorios

EC-Council Accredited Training Center

C|HFI™ Computer Hacking Forensic INVESTIGATOR

C|EI Certified EC-Council Instructor

SAVANT CONSULTORES

EC-Council