Computer Hacking Forensic Investigator v10

Duración: 40Hrs.

Descripción:

CHFI v10 incluye todos los elementos esenciales del análisis y la evaluación forense digital necesarios para el mundo digital actual. Desde la identificación de las huellas de una infracción hasta la recopilación de pruebas para un enjuiciamiento, CHFI v10 guía a los estudiantes a través de cada paso del proceso con aprendizaje experiencial. Este curso ha sido probado y aprobado por veteranos y los mejores profesionales de la industria de la ciencia forense cibernética.

CHFI v10 está diseñado por profesionales de la industria tanto para profesionales como para aspirantes a profesionales de carreras que incluyen analistas forenses, investigadores de delitos cibernéticos, analistas forenses de defensa cibernética, personal de respuesta a incidentes, auditores de tecnología de la información, analistas de malware, consultores de seguridad y directores de seguridad.

¿Por qué CHFI v10?

- EC-Council es una de las pocas instituciones acreditadas por ANSI 17024 a nivel mundial que se especializa en Seguridad de la Información.
- La credencial de Computer Hacking Forensic Investigator (CHFI) es una certificación acreditada por ANSI 17024.
- El programa CHFI v10 ha sido rediseñado y actualizado después de una investigación exhaustiva del mercado actual los requisitos, el análisis de tareas de trabajo y el reciente enfoque de la industria en las habilidades forenses.
- Está diseñado y desarrollado por expertos experimentados en la materia y profesionales forenses digitales.
- El programa CHFI v10 incluye una amplia cobertura de los procesos de Malware Forensics, junto con nuevos módulos como Dark Web Forensics e IoT Forensics.
- También cubre metodologías forenses detalladas para la infraestructura de nube pública, incluido Amazon AWS y Celeste.
- El programa se desarrolla con un enfoque en profundidad en los procesos de adquisición y examen de datos volátiles (RAM Forensics, Tor Forensics, etc.).
- CHFI v10 es un curso completo neutral para el proveedor que cubre todas las principales tecnologías de investigación forense y Soluciones.
- CHFI tiene laboratorios detallados para una experiencia de aprendizaje práctico. En promedio, el 50% del tiempo de capacitación se dedica a laboratorios, cargados en CyberQ (Cyber Ranges) de EC-Council.
- Cubre todas las bases de conocimientos y habilidades relevantes para cumplir con las normas de cumplimiento normativo, como ISO. 27001, PCI DSS, SOX, HIPPA, etc.
- Viene con un gran número de libros blancos para lectura adicional.
- El programa presenta una metodología de investigación forense repetible a partir de un forense digital versátil profesional, aumentando la empleabilidad.
- El material didáctico está repleto de plantillas de investigación forense para la recopilación de pruebas, la cadena de custodia, informes finales de investigación, etc.
- El programa viene con laboratorios virtuales basados en la nube, cargados en Rangos Cibernéticos avanzados, lo que permite a los estudiantes practicar diversas técnicas de investigación en tiempo real y en entornos simulados de forma realista.

Computer Hacking Forensic Investigator v10

Duración: 40Hrs.

Cómo se beneficiará

Certified Hacking Forensic Investigator v10 ha sido diseñado por expertos de la industria para proporcionar un enfoque imparcial para aplicar prácticas de investigación complejas, lo que permite a los profesionales forenses:

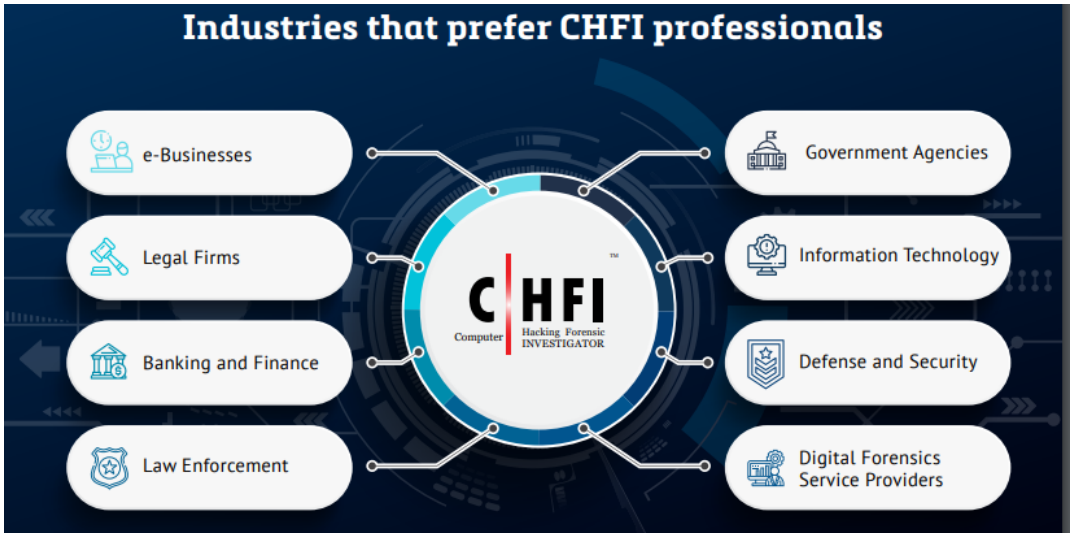
- Desempeñar un papel activo en la investigación y conservación de pruebas digitales y no digitales de un ataque.
- Contrario a la serie de compromisos.
- Utilice inteligencia de amenazas para anticipar y alertar a los equipos cibernéticos en caso de futuros ataques.

¿Quién debe asistir?

El programa CHFI está diseñado para todos los profesionales de TI involucrados con la seguridad del sistema de información, la informática forense y la respuesta a incidentes.

Público objetivo

- Policía y otro personal encargado de hacer cumplir la ley
- Personal de defensa y seguridad
- Profesionales de e-Business Security
- Profesionales legales
- Banca, Seguros y otros profesionales
- Agencias gubernamentales
- Gerentes de TI



Computer Hacking Forensic Investigator v10

Duración: 40Hrs.

Carrera con CHFI

Enfoque de aprendizaje metodológico detallado
CHFI presenta un enfoque metodológico para la informática forense que incluye búsqueda e incautación, cadena de custodia, adquisición, preservación, análisis y reporte de evidencia digital.

Análisis forense de la web oscura e IoT
El primer programa de certificación que le ofrece módulos de Dark Web e IoT Forensics

Amplia cobertura sobre malware forense

Cubre las últimas muestras de malware como Emotet y Eternal Blue, también conocido como WannaCry.

Metodologías forenses para infraestructura en la nube
Domine las herramientas y técnicas para garantizar la seguridad en varias plataformas en la nube: Amazon Web Services, Microsoft Azure Cloud y Google Cloud Platform.

50 GB de archivos de pruebas elaborados
CHFI v10 le proporciona 50 GB de archivos de pruebas elaborados con fines de investigación, lo que le ayuda a tener experiencia práctica en la recopilación de pruebas.

50+ laboratorios complejos
El único programa que proporciona un aprendizaje completo con un entorno simulado con más de 50 laboratorios complejos para garantizar que obtenga las habilidades necesarias para su próximo trabajo.

Temario

- Informática forense en el mundo actual
- Proceso de investigación de informática forense
- Comprensión de los discos duros y los sistemas de archivos
- Adquisición y duplicación de datos
- Derrotando las técnicas anti-forenses
- Windows Forensic (¡nuevo!)
- Análisis forense de Linux y Mac (¡nuevo!)
- Análisis forense de redes
- Investigación de ataques web
- Análisis forense de la Dark Web (¡Nuevo!)
- Análisis forense de bases de datos
- Análisis forense en la nube
- Investigación de delitos relacionados con el correo electrónico
- Análisis forense de malware
- Forense móvil
- Análisis forense de IoT (¡nuevo!)