

Certified Computer Hacking Forensic Investigator

Descrición

CHFiv9, a última versión do programa foi deseñada por profesionais expertos/as no manexo de evidencias dentro de investigacións de cibercrímenes. Foi desenvolto por un panel de investigadores/as expertos/as da industria e ademais establecéronse os estándares para as mellores prácticas en investigacións dixitais. Tamén está dedicado a aumentar o nivel de coñecemento, comprensión e habilidades en ciberseguridade e investigación.

O curso trata o uso de ferramentas de investigación tales como EnCase, Access Data FTK & ProDiscover proporcionando así as habilidades necesarias para a identificación de pegadas dixitais; ademais de incluír unha enorme recompilación de evidencias no caso de persecución penal incluíndo RAW, imaxes .dd, arquivos de audio e vídeo, arquivos MS Office, etc.

A certificación fortifica o nivel de aplicación de coñecementos de quen estea interesado/a na integridade das redes e investigacións dixitais.

As probas de selección realizaranse mediante plataforma online, sen necesidade de desprazamento presencial ao CNTG, a poderá realizar a persoa inscrita ao curso dende o seu domicilio ou lugar de traballo, tendo en conta que a plataforma online abrirase automaticamente na data e hora indicada para iso.

A persoa inscrita recibirá un mail dende a entidade adxudicataria co acceso a esta proba uns 2 días antes da mesma.

A plataforma online de probas de selección é compatible coas versións estables máis recentes de todos os navegadores web e sistemas operativos máis populares (Windows, MacOS, Android ou calquera distribución Linux).

Por tanto, para acceder á plataforma simplemente necesitarase un equipo de sobremesa, portátil con acceso a unha conexión estable de Internet.

Recomendable ter coñecemento/nivel medio de comprensión lectora en inglés debido a

que a proba de nivel pode incluír preguntas en inglés e o exame oficial de certificación ao que se opta neste curso xeralmente realízase en Inglés.

Para seguir o curso é necesario que o equipo conte con altofalantes ou auriculares.

O CNTG facilitará os correos electrónicos das persoas inscritas á empresa organizadora das probas para que esta poida crearlles e comunicarlles as ligazóns de acceso tanto á proba como ao curso.

Obxectivos

O obxectivo da formación é axudarlle a dominar a metodoloxía dun/ha Hacker Forensic Investigator. Os/As asistentes, unha vez superado o exame correspondente, lograrán obter unha das certificacións de maior interese global: CHFI – Computer Hacking Forensic Investigator.

Ao finalizar este curso, o alumnado será capaz de:

- Dar resposta a incidentes e forenses
- Realizar recompilacións de evidencia electrónica
- Realizar adquisicións forenses dixitais
- Realizar bit-stream imaging / adquisición dos medios dixitais confiscados durante o proceso de investigación
 - Examinar e analizar texto, gráficos, multimedia e imaxes dixitais
 - Levar a cabo exames exhaustivos das unidades de disco duro do computador e outros medios de almacenamento de datos electrónicos
 - Recuperar información e datos electrónicos de discos duros de computadoras e outros dispositivos de almacenamento de datos
 - Seguir estritos procedementos de manexo de probas
 - Manter a pista de auditoría (é dicir, a cadea de custodia) e a integridade da evidencia
 - Facer traballos de exame técnico, análise e notificación de probas baseadas en computadoras
 - Preparar e manter os expedientes
 - Utilizar ferramentas forenses e métodos de investigación para atopar datos electrónicos, incluíndo historia de uso da internet, documentos de procesamento de textos, imaxes e outros arquivos
 - Reunir información volátil e non volátil de Windows, Mac e Linux
 - Recuperar arquivos e particións eliminados en Windows, Mac OS X e Linux
 - Realizar procuras de palabras chave incluíndo o uso de palabras ou frases obxectivo
 - Investigar eventos para evidenciar ameazas ou ataques internos

- Apoiar a xeración de informes de incidentes e outras garantías
- Investigar e analizar todas as actividades de resposta relacionadas con incidentes cibernéticos
- Planificar, coordinar e dirixir as actividades de recuperación e as tarefas de análise de incidente

Dirixido a

Este curso está dirixido a todos os interesados e interesadas en investigacións forenses dixitais, avogados/as, consultores/as legais, corpos oficiais, oficiais de policía, defensa/milicia, detectives e investigadores/as, responsables de incidentes e membros de equipo, xerentes de seguridade da información defensores de redes, profesionais IT, directores/as IT/xerentes, enxeñeiros/as en sistemas/redes, analistas e consultores/as de seguridade.

Coñecementos previos:

- Coñecementos básicos de TI/ciberseguridade, investigación dixital e resposta de incidentes
- O cursar o CEH é unha vantaxe
- Recomendable ter coñecemento nivel medio comprensión lectora de inglés

Perfil do docente

Docentes con máis de 5 anos de experiencia en áreas de alta especialización técnica neste ámbito. Dispoñen das certificacións oficiais de EC-Council, para impartir estes cursos.

DURACIÓN	48 horas
PROGRAMA	Programación 2020/21
MATRÍCULA	Gratuíta
METODOLOXÍA	Virtual
TIPO	CURSO

Certified Computer Hacking Forensic Investigator

CERTIFICACIÓN OFICIAL	Sí
EXAME CERTIFICACIÓN	EC-Council 312-49: Computer Hacking Forensic Investigator
BENEFICIOS	
HORARIO	De luns a xoves de 16:30 a 20:30 horas.
PERIODO INSCRIPCIÓN	17/12/2020 - 18/12/2020
PROBA DE SELECCIÓN	18/01/2021, 16:00
LUGAR DE DOCENCIA	
Nº PRAZAS	16 (Mínimo 10)

Temario

- Módulo 01: A informática forense no mundo actual
- Módulo 02: Proceso de investigación na informática forense
- Módulo 03: Entendendo os discos duros e o sistema de ficheiros
- Módulo 04: Adquisición e duplicación de datos
- Módulo 05: Defensa contra técnicas anti-forense
- Módulo 06: Análise forense do sistema operativo
- Módulo 07: Forense de rede
- Módulo 08: Investigación de ataques web
- Módulo 09: Forense de base de datos
- Módulo 10: Forense en cloud
- Módulo 11: Forense de malware
- Módulo 12: Investigación de ataques por email
- Módulo 13: Forense en dispositivos móbiles
- Módulo 14: Redacción e presentación de informes forenses