Capacitación de informática forense

C.D.F.I

Cybersecurity & Digital Forensics Investigator

Cybersecurity & Digital Forensics Investigator (CDFI), es el curso diseñado con meta de adentrarnos a la metodología que utiliza un informático forense para recuperar evidencia de un suceso informático. CDFI le proporcionará una visión especializada de las herramientas y metodologías que se utilizan para llevar a cabo un proyecto de informática forense.

El participante al curso logrará un conocimiento invaluable que le proporcionará herramientas cognitivas que ayuden a su organización a responder en el área forense a un suceso informático.

Dirigido a:

A estudiantes y profesionales de buscan conocimiento entorno a Ciberseguridad, informática forense y criminología digital.

Beneficios:

- Contar con los conocimientos necesarios para realizar levantamientos y análisis de evidencias digitales.
- Desarrollar la capacidad de utilizar variadas herramientas e interpretar los datos obtenidas de éstas.
- Conociendo como se lleva a cabo el levantamiento de evidencias siguiendo los métodos aceptados de forma nacional e internacional.

Duración:

30 horas divididas en **5** sesiones

El registro incluye:

- Diploma con valor curricular
- Acceso a las grabaciones al terminar el curso
- Manual CDFI

Requisitos:

- Laptop de 4GB de RAM, 20GB de almacenaje disponible, procesador i3 o superior o algo equivalente.
- **No se requieren conocimientos previos**
- **No hay restricciones de edad**
- **No hay restricciones de país**

TEMARIO

Sesión 1

Informática Forense y criminalística

- Introducción a la informática forense
  - Metodología de informática forense
  - Cadena de custodia
  - Objetivos de un análisis forense
- Conceptos pre-eliminares de la informática forense
  - Malware
  - Vectores de ataque
  - Perfil de cibercriminal
  - Grupos de cibercriminales
- Perfil de un analista forense
  - Conceptos requeridos
  - Formación requerida

Sesión 2

Investigación digital y laboratorio

- Manejo de escena del crimen
  - Preservación de la escena del crimen
  - Documentación de la escena del crimen
  - Recolección de evidencia digital en caliente vs en frio
  - Procedimiento de encendido y apagado de dispositivos en la escena del crimen
- Metodología para la obtención de evidencia digital
  - Adquisición de autorización
  - Evaluación de riesgos
  - Información preliminar de la escena
  - Formulario de recolección de evidencia
  - Recopilación de evidencia electrónica
  - Aseguramiento y manejo de la evidencia
  - Cadena de custodia
  - Duplicación de datos
  - Verificación de integridad de la imagen
  - Recuperación de datos perdidos o eliminados

Sesión 3

Evidencia digital

- Análisis forense a sistemas Windows
  - Sistemas de archivos
  - Evidencia forense bit a bit
  - Software de apoyo
  - Practica de cadena de custodia

Sesión 4

Análisis forense de Windows y Linux

- Análisis forense a sistemas Linux
  - Sistemas de archivos
  - Evidencia forense bit a bit
  - Software de apoyo
  - Practica de cadena de custodia

Sesión 5

Análisis forense de dispositivos móviles y recuperación de información

- Generación de la cadena de custodia
  - Software de recuperación de datos
  - Evaluar evidencia y caso
  - Preparar el informe final
  - Testificando como testigo experto
  - Cerrando el caso
- Legislación asociada a la informática forense
- Análisis forense a móviles
  - Sistemas de archivos y arquitectura
  - Configurando el laboratorio forense y los emuladores
  - Acceso a la información de los dispositivos
  - Adquiriendo la evidencia digital
  - Análisis de la evidencia digital

Apoyo post-curso

- Obtendrás las grabaciones del curso al terminar este.
- El acceso a las grabaciones del curso es perpetuo.
- Se te responderán dudas durante el curso en vivo.
- Se te dará acceso perpetuo a el grupo de comunidad de WhiteSuit Hacking donde se te dará apoyo perpetuo y resolución de dudas.

Post Explotación y Pivoteo