CAPACITACIÓN

COMPUTO FORENSE

DESTAPANDO EVIDENCIA DIGITAL

En este curso el participante adquiere el conocimiento y habilidades del cómputo forense a través de la aplicación de técnicas científicas y analíticas especializadas en infraestructura tecnológica que le permitan identificar, preservar, analizar y presentar datos combinando los aspectos teóricos con la resolución de casos prácticos.

Dirigido a: Aquellos profesionales de seguridad de la información, auditores, **hackers éticos**, organizaciones que hayan sido víctima de delitos informáticos, personal que maneja incidentes de seguridad de información digital.

Beneficios:

- El candidato será capaz de recolectar y analizar evidencias, así como reconstruir las actividades realizadas cuando sea atacado.
- Conocer los pasos más comunes a seguir para duplicar evidencia localizada en medios de almacenamiento
- El participante podrá analizar la estructura y operación de los sistemas de archivos **FAT** y **NTFS, Ext4** desde el punto de vista de la investigación forense, así como los datos contenidos en los mismos
- Conocerá las técnicas para responder a incidentes en plataformas **Windows** o **Linux** de acuerdo a las mejores prácticas
- Comprenderá los aspectos legales relacionados con el cómputo forense

Duración: 24 Hrs.

Requisitos:

- Conocimientos básicos en plataforma **Microsoft Windows ®** y **Linux**
- Conocimientos en **Networking TCP/IP**

INCLUYE:

- Instalaciones adecuadas
- Material y manuales de cursos
- Instructores Certificados
- Box lunch
- Servicio de cafetería continua
- Estacionamiento
- Registro **STPS**

TEMARIO

Computo Forense

- Introducción
- Proceso de investigación del cómputo forense
- Credibilidad de los datos
- Evidencia digital
- Procedimientos para responder
- Metodología general de cómputo forense

Investigación Forense en Sistemas de Archivos

- Análisis de sistema de archivos **FAT** y **NTFS**
- **Laboratorio:** Recuperación de evidencia mediante **FTK Imager**y **Autopsy**

Recuperación de archivos borrados y particiones borradas

- Conceptos básicos de estructuras de discos
- Ejercicio de generación de una imagen de una memoria **USB**
- Exploración y análisis de volúmenes
- Extracción y recuperación de particiones
- Recuperación de archivos borrados y particiones

Investigación Forense empleando AccessData FTK

- Recuperación de archivos eliminados
- Búsqueda de cadenas de texto
- Análisis de Metadatos
- Intrusión a Servidores empleando **FTK Imager**y **Autopsy**

Esteganografía (Steganography) de archivos de imágenes Forense

- Técnica que permite ocultar una información
- Ocultar archivo dentro de otro
- **Esteganografía** con **Outguess**
- Uso de la herramienta de **Outguess** con **Kali Linux**

Aplicaciones Crack de Passwords

- Ataque de fuerza bruta
- Descifrar contraseñas
- Algoritmos de cifrado o hash (**DES**, **SHA-1**)
- Uso de **John theRipper** para romper contraseñas

Log y correlación de eventos

- Análisis de bitácoras con **Logwatch**

Forense de tráfico de red

- Herramientas para la captura y análisis
- Análisis de datagramas **UPD** y **TCP**
- Identificación de patrones de tráfico asociado a diversas actividades maliciosas
- Recuperación de información importante del tráfico de red
- Análisis de incidentes en **Windows** y **Linux** basado en evidencia de capturas de red
- Intrusión a servidores empleando **Snort** y **WireShark**

Investigación de ataques inalámbricos (Wireless Attacks)

- Visión general de los Estándares **IEEE 802.X**
- Ataques de negación de servicio (**DoS**)
- Interceptación de las comunicaciones
- Inyección de tráfico en la red **Wi-Fi**
- Comprensión de seguridad en **WEP**, **WPA** y **WPA2**
- Ataque a seguridad **WEP** y **WPA2** e Investigación

Investigación de ataques a sitios Web(Web Attacks)

Legislación relacionada al cómputo forense

- Legislación mexicana relacionada
- Denominaciones de los delitos informáticos