INVESTIGACION FORENSE AVANZADA EN SISTEMAS OPERATIVOS WINDOWS

UN APOYO A LA LEY DE DELITOS INFORMATICOS DE COSTA RICA

INTRODUCCION

Los ataques y fraudes informáticos dirigidos contra los activos de información de las compañías son una realidad que se materializa cada vez con mayor frecuencia; ante esto la ley de delitos informáticos contempla tipos penales que pueden ser utilizados para la judicialización de las conductas delictivas siempre y cuando se sustenten en un debido proceso de adquisición de la evidencia, manejo de custodia e investigación forense.

Adicionalmente las compañías esperan que en el momento que se vulnere un control de seguridad o se materialice un riesgo, los responsables de TIC o de Seguridad de la Información estén en la capacidad de analizarlo y determinar quién, qué, cómo, cuándo y dónde ocurrió.

Para responder a esas preguntas, se requiere desarrollar un conocimiento avanzado en investigación forense que pueda ser aplicado en entornos corporativos.

Esta capacitación pretende así desarrollar de forma práctica el conocimiento para toma de evidencia a través de la red de datos, adquisición de la información residente en la memoria ram y el análisis detallado de todos los artefactos del sistema operativo donde sea posible procesamiento de evidencia.

OBJETIVO DE LA CAPACITACIÓN

Utilizar herramientas y metodologías para realizar investigaciones de algunos de los delitos contemplados en la Nueva Ley de Delitos Informáticos de Costa Rica sobre sistemas operativos Windows.

CONTENIDO

Al finalizar la capacitación, se habrán abordado los siguientes contenidos:

- Cómo aplicar una metodología de investigación en la empresa para investigar casos de fraude informático desde el interior de la organización.
- Manejo de la cadena de custodia de la evidencia a lo largo del proceso de investigación.
- Técnicas para analizar incidentes sobre sistemas operativos Windows asociados a la ley de delitos informáticos de Costa Rica.
- Caso práctico de investigación de una extorsión utilizando recursos corporativos.
- Manejo de diversas herramientas de uso libre para analizar casos de fuga de información y determinar qué, quién, cómo, cuándo y dónde ocurrió.
- Captura y análisis de evidencia volátil en memoria ram.

QUIENES DEBEN ASISTIR A ESTE TALLER

- Responsables de TIC, Seguridad de la información o auditoría de sistemas interesados en desarrollar las habilidades para investigar incidentes de seguridad o fraudes informáticos sobre sistemas operativos Windows.
- Especialistas del Derecho interesados en conocer el fundamento probatorio de los casos de delitos informáticos en sistemas operativos Windows.

METODOLOGÍA

- Clases lectivas: Presentación explícita del contenido y de los aspectos conceptuales y técnicos asociados a cada tema en formato Powerpoint.
- Ejercicios prácticos: Se realizarán varios ejercicios prácticos a partir de casos de delitos informáticos reales para desarrollar las destrezas necesarias para la solución de los mismos tomando como base la metodología expuesta.

ENTREGABLES

Cada participante recibirá:

- CD con herramientas de uso libre (software) para las prácticas en clase
- Copia de la presentación en powerpoint realizada por el instructor
- Lecturas complementarias para profundizar en el tema.

- Certificado de asistencia

DURACIÓN

24 horas /3 dias

FACILITADOR: MSc./MBA/ Ing. Manuel Santander

Con trece (13) años de experiencia profesional, es actualmente uno de los expertos mas destacados en investigación forense y penetration testing en Suramérica. Ocupa el cargo de **Arquitecto de Seguridad de la Información y líder del proceso de atención de incidentes** en Las Empresas Públicas de Medellín E.S.P., la segunda empresa más grande de Colombia. Excelente ingeniero ha participado en diferentes casos de investigación y como consultor ha asesorado múltiples empresas en la identificación de vulnerabilidades y en el diseño e implementación de controles.

CERTIFICACIONES VIGENTES DE SANS INSTITUTE

GIAC GOLD Certified Forensic Analyst (GCFA) #148

• GIAC GOLD Certified Intrusion Analyst (GCIA) #864

GIAC Certified Incident Handler (GCIH) #10863

GIAC Certified Firewall Analyst (GCFW) #2213

GIAC .NET Security (GNET) #31

GIAC Certified Security Essentials (GSEC) # 21748

ESTUDIOS

Ingeniero de Sistemas de la Universidad EAFIT (Colombia)

Master of Science in Information Security Engineering de SANS Technology Institute

MBA de la Universidad EAFIT (Colombia)

Ha sido coautor de los cursos de SANS Institute Browser Forensics y Protecting your personal privacy on the internet.

EXPERIENCIA DOCENTE

Actualmente es docente en temas de Seguridad de la Información, Comunicaciones y Auditoría en varias universidades Colombianas.

También es instructor de SANS Institute en la modalidad de Local Mentor de diplomados y cursos en el área de Seguridad de la Información.

Es conferencista permanente en diversos eventos en sur y centroamérica en delitos informáticos y seguridad de la información.

Es instructor habitual de Corporacion e Inversiones CAES S.A.