sedian

Seguridad Digital
de Andalucía

Ficha técnica

Herramientas de análisis forense bajo GPL

Modalidad: Charla virtual

Fecha de celebración: 31/10/2019

JUNTA DE ANDALUCIA
CONSEJERÍA DE ECONOMÍA, CONOCIMIENTO, EMPRESAS Y UNIVERSIDAD

ÍNDICE

1.Datos básicos de la acción formativa

Nombre de la acción formativa: Herramientas de análisis forense bajo GPL

Modalidad: Webinar

Fechas y lugar de celebración: 31/10/2019 (Online)

Horario: 10:00 a 11:00 horas

Número de personas participantes: hasta un máximo de 100

2.Descripción

Era cuestión de tiempo. Tu organización ha sido víctima de una ataque ransomware. Pasados los primeros momentos de incertidumbre y toma de decisiones críticas que ayudaron a mitigar la amenaza, es el momento de conocer la causa de esta infección.

La Informática Forense es la disciplina de ayuda a resolver las cuestiones ¿Qué?, ¿Por Qué?, ¿Quién?, ¿Cómo?, ¿Dónde? y ¿Cuándo?; de forma que podamos determinar la intensidad, intención y alcance del ataque. Para ello, se sirve de una serie de herramientas especializadas que debes conocer, destacando la distro CAINE (para licencia GPL) y la aplicación AUTOPSY.

En este Webinar aprenderás la práctica del procedimiento forense. Comenzaremos con la adquisición y preservación de las evidencias hasta la redacción del informe forense que pretende dar solución a las preguntas formuladas.

3.Objetivos

- Aprender los pasos que conforman una investigación informática forense, desde la preservación de la evidencia hasta el informe pericial que deja constancia de los hechos acontecidos.
- Revisar el software comercial y de dominio público utilizado en las investigaciones. Se hará especial hincapié en trabajar con la distribución Caine y la aplicación Autopsy.
- Conocer casos de uso de la herramienta Autopsy.

4.Contenidos

1.Conceptos claves, procedimientos y técnicas

a) La evidencia digital, cadena de custodia y consideraciones legales
b) El procedimiento del análisis forense por etapas.
a) Función de Hash. Algoritmos que pueden no ser admitidos legalmente.
b) Espacio asignado (Allocated) y sin asignar (Un-allocated).
c) Captura de la información en vivo (Dispositivo encendido).
d) Captura de la información Post-Mortem (Dispositivo apagado).
e) Las clonaciones físicas y lógicas.
f) Metadatos de archivos.

2.Despliegue y uso del software forense (I)

a) FTK Imager para Windows.
b) Instalación y descripción de la distribución Caine.
c) Preservar la evidencia con bloqueadores de escritura.
d) Adquisición de la información con GUYMAGER.

3.Despliegue y uso del software forense (II) (Autopsy)

a) La herramienta Autopsy.
b) Los módulos de ingestión de la información.
c) Análisis de la información.
d) Adquisición en sistemas vivos.
e) Interpretación del “Score”
f) Etiquetado manual de la información en categorías.
g) El filtro de ingestión de hash. Etiquetado automático STIX y CybOX.
h) El proyecto VIC. Importación manual de hashsets.
i) Autopsy y el procedimiento de triaje en vivo por medio de USB.

4.Despliegue y uso del software forense (III) (Casos de uso)

a) Práctica “Reto Avión”.
b) Práctica “Reto BarceLonas”.
c) Práctica “Reto Info”.

5.Docente

Antonio Salazar Graván: Especialista en Sistemas Microsoft, cuenta con numerosas certificaciones de este fabricante (MCITP, MCSA, MCTS) y más de 10 años de experiencia impartiendo formación oficial.

Linkedin: https://www.linkedin.com/in/antonio-salazar-graván-8066214b

6.Video de la sesión y presentación utilizada

En la sección “**Videos**” de la intraweb SEDIAN encontrarás la sesión grabada así como la presentación utilizada por el ponente.