EL ANALISIS DE EVIDENCIAS

Sku: 4572EC

Horas: 10

OBJETIVOS

Conocer los lugares en los que las pruebas pueden residir como los medios de almacenamiento o hardware. Estudiar aspectos relacionados con los discos, volúmenes y particiones, sistemas de ficheros y archivos metadata. Realizar la evaluación de vulnerabilidades. Saber hacer el procesado de pruebas, conociendo las herramientas necesarias para ello. Analizar los diferentes tipos de dispositivos móviles existentes. Ampliar conocimientos acerca de los muchos y diversos términos existentes.

CONTENIDOS

1. Lugares donde las pruebas pueden residir. Medios de almacenamiento. Hardware, firmware, interfaces. 2. La geometría del disco. 3. Discos, volúmenes y particiones. Partición DOS. Partición GUID. Discos dinámicos y sistemas RAID. Implementación de RAID. 4. Sistemas de ficheros. Sistema de ficheros NTFS. Conceptos MFT. Índice de atributos para directorios de MFT. El atributo $DATA de MFT. Análisis forense en sistema de ficheros NTFS. 5. El archivo metadata, las unidades encriptadas y los almacenamientos dañados. El archivo metadata. Unidades encriptadas. Medios de almacenamiento corrompidos/ dañados. 6. TCP/IP. Exploración de redes IP. Medidas contra el rastreo de redes. 7. Evaluación de otras vulnerabilidades. Servicios remotos. Servicios web. Aplicaciones web. Servicios de mantenimiento remoto. Servicios de bases de datos. Servicios de correo electrónico. 8. Tipos de dispositivos móviles. Dispositivos GPS. Teléfonos móviles / tabletas. Identificación del fabricante. Identificación de operadora. Identificación/clasificación de la red. El número de modelo. Características físicas de los teléfonos móviles. Teléfonos inteligentes vs teléfonos multifunción. 9. Preparación del examen. Las herramientas. 10. Clasificación de herramientas. 11. Procesado, examen y verificación. Procesado y examen. Verificación. 12. Las pruebas multimedia y los formatos. Introducción a las pruebas multimedia. El papel de las pruebas multimedia en las investigaciones. Formatos de archivos multimedia. 13. Esteganografía. Como trabaja la esteganografía. ¿Por qué se usa la esteganografía? Quién usa la esteganografía. Identificar ficheros esteganográficos.