Evaluación

Análisis Forense de Sistemas Informáticos

Telefónica EDUCACIÓN DIGITAL

Caso práctico final

1 | Explica en qué consiste la RFC 3227 y cuáles son sus fases, detallando cada una de ella. (1 punto)

2 | Ordena por volatilidad, de menos a más, las siguientes evidencias: (1 punto)

- Valor del registro EIP
- Eventos de Windows
- Ficheros almacenados en "Mis Documentos"
- Espacio de memoria de iexplorer.exe
- Información que se obtiene con el comando "arp -a"

3 | Define, con tus propias palabras, y el máximo nivel de detalle, el concepto de Cadena de Custodia. (1 punto)

4 | ¿Qué artefactos forenses componen el registro de Windows 7 y cuál es su localización? (1 punto)

5 | Juan trabaja para una pequeña empresa, y últimamente se ha percatado que uno de los equipos de la oficina, que tiene instalado un Windows XP de 32 bits, con Service Pack 2, está funcionando de una forma un poco sospechosa. En ese momento decide llamarte para que le asesores, y te explica una serie de peculiaridades del equipo:

- Están utilizando ese equipo como servidor de producción
- Se dispone de acceso físico al equipo
- Dispone de puertos USB

- Sólo se quiere saber el origen del posible problema, y en ningún momento de plantean llegar a juicio.

Dada estas premisas, indica cual sería tu procedimiento de actuación, para determinar el origen de dicho comportamiento sospechoso. (1 puntos)

6 | Como resultado del proceso detallado anteriormente, has obtenido un fichero (facilitado por el profesor) que debes analizar en el laboratorio. En concreto, se pide:

- Procesos ejecutándose (nombre e identificador de proceso) (0,5 puntos)
- Conexiones abiertas (0,5 puntos)
- ¿Crees que puede haber malware? Justifica tu respuesta (0,5 puntos)
- Localizar el proceso real identificado como posible malware (1 puntos)
- Obtener el hash MD5 de dicho proceso (0,5 puntos)
- ¿En qué país se encuentra el servidor con el que se comunica el proceso? (0,5 puntos)

NOTA: Se debe documentar, de la forma más profesional posible, todo el proceso de análisis del fichero, incluyendo capturas de pantalla de cada comando utilizado, así como los resultados. Además, se debe incluir la interpretación personal de los resultados, en forma de conclusiones. (1,5 puntos)

Telefónica

EDUCACIÓN DIGITAL