Tarea online AFI01.

Título de la tarea: Análisis de Memoria RAM

Ciclo formativo y módulo: Curso de especialización en ciberseguridad en entornos de las tecnologías de la información - Análisis Forense Informático.

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Resultados de aprendizaje

- **RA1.** Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.

Contenidos

1.- Análisis forense informático.
- 1.1.- Objetivos y fases.
- 1.2.- Metodología.
- 1.3.- Identificación.
- 1.4.- Adquisición, Preservación y Cadena de Custodia.
- 1.5.- Herramientas Necesarias.
- 1.6.- Reporte.

1.- Descripción de la tarea.

Caso práctico

Pixabay (Dominio público)

María está trabajando en un caso y ha recibido la imagen de memoria RAM de un servidor que ha tenido un comportamiento anómalo.

Un compañero sobre el terreno ha capturado la memoria RAM de la máquina antes de que la apagasen y se la ha enviado al laboratorio para ser analizada por María.

El coordinador de la investigación le ha hecho varias preguntas a María que deberá responder sobre la evidencia.

¿Qué te pedimos que hagas?

- **Apartado 1: Analiza la memoria RAM**

  Lo ideal es usar la herramienta Volatility (versión 2), la tienes disponible en Volatility
  - La memoria RAM está disponible en este enlace (https://mega.co.nz/#!1UpjkTab!RP_QeooLaxA7bixLxkHLIqhWKfQ9G_0M58NSUchRn68)
  - Descomprime la memoria RAM
  - Debes de ejecutar Volatility desde consola ya sea en Windows o Linux
  - Tienes varias guías de vídeo que te pueden ayudar en el proceso:
    - https://www.youtube.com/watch?v=RFYbevw6hxI
    - https://www.youtube.com/watch?v=iU9mqB4h3Tg
  - Otras herramientas que te pueden ser útiles
    - Floss: https://github.com/mandiant/flare-floss

- **Apartado 2: Contestando a las preguntas**
  - ¿Qué pasaría si se hubiera apagado este servidor?
  - ¿Qué tipo de comandos ha ejecutado el cibercriminal? ¿Qué sugiere?
  - ¿Cómo se han ejecutado los comandos?
  - ¿Qué actividad maliciosa has visto?
  - ¿Puedes identificar desde que IP vino el ataque?
  - ¿Qué tipo de ataque pudo ser? ¿Qué tipo de malware se ha encontrado?

NOTA IMPORTANTE

Para todos los apartados es necesario entregar las capturas de pantalla de los principales pasos realizados, explicando el proceso seguido en cada uno de ellos. Las capturas de pantalla realizadas deben tener como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil. Aquellos apartados/subapartados que no cumplan esta condición no serán corregidos.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

- Ordenador personal con, al menos, 4 Gigabytes de memoria RAM
- Conexión a Internet para consultar ejemplos de la Unidad 1.
- Sistemas Operativos Windows 10, Ubuntu 18.04, Ubuntu 20.04
- Navegador web.

Recomendaciones

- Antes de abordar la tarea:
  - lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
  - Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- Te recomendamos ver las guías que se han recomendado.
- Te recomendamos tambien investigar todas las capacidades y módulos de Volatility.

Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_Nombre_AFI01_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna **Begoña Sánchez Mañas para la primera unidad del MP de AFI**, debería nombrar esta tarea como...

sanchez_manas_begona_AFI01_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación implicados

Criterios de evaluación RA1

- a. Se han identificado los dispositivos a analizar para garantizar la preservación de evidencias.
- b. Se han utilizado los mecanismos y las herramientas adecuadas para la adquisición y extracción de las evidencias.
- c. Se ha asegurado la escena y conservado la cadena de custodia.
- d. Se ha documentado el proceso realizado de manera metódica.
- e. Se ha considerado la línea temporal de las evidencias.
- f. Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.
- g. Se han presentado y expuesto las conclusiones del análisis forense realizado

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1.a: Se ha conseguido usar la herramienta de Volatily y leer de manera correcta la evidencia	0,5 puntos
Apartado 1.b: Se ha conseguido determinar el sistema operativo a partir de la memoria RAM.	1 punto
Apartado 1.c: Se ha obtenido la lista de procesos de la memoria RAM.	1 punto
Apartado 2.a: Se han valorado la volatilidad de la información	1 punto
Apartado 2.b: Se ha conseguido obtener los comandos ejecutados partiendo de la memoria RAM.	1 punto
Apartado 2.c: Se ha entendido el modo de introducción de los comandos.	1 punto
Apartado 2.d: Se ha encontrado actividad maliciosa	1 punto
Apartado 2.e: Se ha identificado el origen del ataque	1,5 puntos

Apartado 2.f: Se ha entendido el tipo de ataque y el malware implicado.	2 puntos

NOTA IMPORTANTE

Aquellos apartados/subapartados en los que las capturas de pantalla no sean claras o no tengan como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, no serán corregidos.