PRÁCTICA 3: Analizando la RAM - Retos Atenea/INCIBE

El análisis de memoria es también un pilar fundamental en los retos Atenea organizados por el Instituto Nacional de Ciberseguridad (INCIBE), una plataforma que promueve la formación en ciberseguridad mediante desafíos prácticos. En particular, los retos relacionados con la memoria ayudan a los participantes a desarrollar habilidades en la investigación de incidentes, detección de malware y recuperación de información crítica. Este tipo de ejercicios es esencial para formar profesionales capaces de responder a incidentes y garantizar la seguridad de los sistemas informáticos.

INTENTA RESOLVER AL MENOS DOS DE LOS RETOS QUE APARECEN A CONTINUACIÓN

RETO 1

La policía ha detenido a un sujeto y tenemos como evidencia el ordenador encendido.
Se le ha realizado una captura de RAM y análisis de la memoria no volátil. En ella se ha encontrado un extraño fichero que no saben de que puede ser.

Objetivo:

- Investigar y averiguar el contenido de este fichero.

Recursos necesarios:

- Volatility
- Descarga la práctica aquí

RETO 2

Sospechamos que el volcado de memoria adjunto se corresponde con una máquina que ha sido infectada de forma persistente por algún tipo de malware, posiblemente un dropper. Nos gustaría identificar el dominio dañino utilizado por el mismo.

Objetivo:

- Investigar y averiguar la forma de infección y el dominio dañino.
- Hacer investigaciones avanzadas mediante el uso de plugins específicos para procesar artefactos específicos del SO.

Recursos necesarios:

- Volatility
- Plugins Volatility
- Descarga la práctica aquí

RETO 3

Durante la respuesta a un incidente se ha realizado un volcado de memoria de una máquina comprometida. Localiza el dominio contactado por el código dañino.

Recursos necesarios:

- Volatility
- Plugins Volatility
- Descarga la práctica aquí