JIFI2018
JORNADAS DE INVESTIGACIÓN
ENCUENTRO ACADÉMICO INDUSTRIAL
FACULTAD DE INGENIERÍA UCV

ANÁLISIS FORENSE DE LA MEMORIA RAM

Prof. Vincenzo Mendillo, UCV / UCAB /UNIMET

RESUMEN

Ciertos ataques, intrusiones y actividades ilícitas no dejan rastros en el disco duro del computador, por lo que sólo sería posible encontrar indicios del hecho mediante el análisis de la memoria, por ejemplo identificando qué procesos se estuvieron ejecutando y desde hace cuando, que puedan derivar en información relevante para una investigación forense. La memoria RAM es volátil, lo que quiere decir que cuando se apaga el equipo, la información que contiene se pierde. Debido a esto, si el equipo está encendido, es posible llevar a cabo el análisis en vivo, pero también existe la otra manera: a través de la obtención del volcado de memoria (memory dump) donde se copia en un archivo el contenido de toda la memoria en un momento determinado. Con este método es posible realizar el análisis con una réplica exacta o "imagen forense" de la memoria del equipo en cuestión y puede resultar el método más apropiado en muchos casos, dado que es menos intrusivo: no genera actividad en memoria que pueda contaminar la evidencia o la contaminación es mínima. A su vez, al estar almacenado en un archivo, permite realizar sucesivos análisis a futuro sin modificar ni perder la evidencia. Es una práctica recomendada capturar una imagen de la memoria durante una respuesta de incidentes. El análisis posterior puede ser realizado de manera básica utilizando herramientas que permitan extraer "cadenas" (strings) desde la imagen forense, o utilizar herramientas más avanzadas como Volatility Framework.