Maestría en

CIBERSEGURIDAD

Trabajo final de Maestría previo a la obtención del título de Magíster en Ciberseguridad

AUTORES:

Gabriel Eduardo Anagumbla Monga

Bolívar Octavio Suárez Cabezas

Esteban Andrés Canchigña Llumiquinga

Segundo Amable Tisalema Tisalema

TUTORES:

Ing. Alejandro Cortés López

Ing. Iván Reyes Chacón

Análisis forense de una máquina virtual y localización de información en Sistemas Linux

QUITO – ECUADOR | 2024

RESUMEN

El proyecto de Análisis Forense de una Máquina Virtual y Localización de Información en Sistemas Linux tiene como enfoque la definición de una serie de etapas y parámetros a tener en cuenta para llevar a cabo un análisis forense de un equipo con sistema operativo Linux en sus distribuciones Kali, Caine, Alma y Debian, mediante laboratorios, obteniendo diferentes resultados que permita la identificación, recolección y análisis de evidencia digital en máquinas virtuales en el hipervisor VMWare y verificar la validez de la metodología propuesta.

En el Estado del Arte se presenta los principios básicos de la forense digital y la virtualización, junto con las herramientas existentes para el estudio de máquinas virtuales en el sistema operativo Linux. A continuación, se especificará las normas y estándares para la obtención de evidencias junto con sus técnicas en donde se podrá denotar la diferencia entre un análisis forense convencional y el forense en ambientes virtuales, los cuales incluyen las especificidades de los sistemas de archivos y la administración de memoria.

En la metodología se detallará la importancia de la construcción de un ambiente de laboratorio en el que se recrean incidentes de seguridad en máquinas virtuales Linux. Se utilizan instrumentos como Volatility, Autopsy y LiME (Loadable Kernel Module) para obtener y examinar datos pertinentes, tales como registros de actividades, procesos en funcionamiento y conexiones de red.

Finalmente, en el análisis de resultados se podrá verificar la recopilación de pruebas que se ha llevado a cabo con el objetivo de mantener la integridad de los datos, siguiendo las prácticas óptimas en el campo y evidenciar la efectividad en el desarrollo de mejores prácticas.

Palabras Claves: forense, Linux, evidencia, memoria RAM, análisis

ABSTRACT

The Forensic Analysis of a Virtual Machine and Information Localization in Linux Systems project focuses on defining a series of steps and parameters to be taken into account when performing a forensic analysis of a computer with a Linux operating system in its Kali distributions, Caine, Alma and Debian, using laboratories, obtaining different results that allow the identification, collection and analysis of digital evidence in virtual machines in the VMWare hypervisor and verify the validity of the proposed methodology.

The State of the Art presents the basic principles of digital forensics and virtualization, together with existing tools for the study of virtual machines in the Linux operating system. The standards and norms for evidence collection will be specified below, together with their techniques, where the difference between conventional forensic analysis and forensic analysis in virtual environments can be denoted, which include the specifics of file systems and memory management.

The methodology will detail the importance of building a laboratory environment in which security incidents are recreated on Linux virtual machines. Instruments such as Volatility, Autopsy and FTK Imager are used to obtain and examine relevant data, such as activity logs, processes in operation and network connections.

Finally, the results analysis will verify the collection of evidence that has been conducted with the objective of maintaining data integrity, following the best practices in the field and demonstrating effectiveness in developing best practices.

Keywords: forensic, Linux, evidence, RAM memory, analysis