Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de
Magister en Ciberseguridad

AUTORES:

Alvarez Wagnio Jonathan Diego

Llumiguano Chela Jessica Viviana

Romero Suarez Jose Paulo

Siza Hilaño Jairo Joel

TUTORES:

Alejandro Cortés

Iván Reyes

TEMA:

Metodología verificable para adquisición y preservación de evidencia forense en contenedores Docker

Enero–2026

REINVENTEMOS EL FUTURO

Resumen

Durante el desarrollo práctico del presente proyecto se implemento un entorno de laboratorio con la finalidad de examinar como se puede extraer y conservar evidencia digital proveniente de contenedores Docker. Para plasmarlo se configuro una máquina de pruebas con Docker conjuntamente con diversas herramientas de monitoreo. Se uso como entorno vulnerable DVWA para generar actividades sospechosas y comportamientos que se asemejen a ataques reales.

El inicio del proceso comienza con la preparación técnica del ambiente, instalación de dependencias y arranque del contenedor. Posteriormente se realiza varias acciones dentro de DVWA, como inyección SQL, ataque de fuerza bruta, manipulación de parámetros, XSS y carga de archivos con el objetico de generar tranzas reales en los registros, tráfico de red y modificación en el sistema interno del contenedor para generar evidencia verídica.

Posteriormente se aplicaron tres métodos de adquisición para esta investigación: la captura en vivo, el Snapshot y la obtención post-mortem, la captura en vivo contempla la recolección de logs, metadatos, tráfico de red y estadísticas del proceso activo. En la fase del snapshot se genera una imagen congelada del contenedor para analizar su estado en un punto especifico del tiempo, además del registro del consumo de recursos. En la etapa de post mortem se detiene el contenedor y se extrae el sistema de archivos conjuntamente con su configuración final. Toda información extraída de cada una de las fases es almacenada en carpetas separadas y se genera hashes para asegurar la autenticidad.

Con la finalidad de simplificar todo el procedimiento de extracción se creó un script automatizado el cual ejecuta cada una de las fases de manera ordenada y autónoma, previo a la ejecución el script creado verifica que el entorno este correctamente configurado, genera carpetas de evidencia para posteriormente ejecutar capturas correspondientes y seguidamente calcular hashes criptográficos.

Palabras clave: Docker, evidencia digital, DVWA, captura en vivo, snapshot, post-mortem, script automatizado, integridad criptográfica.

Abstract

During the practical development of this project, a laboratory environment was implemented in order to examine how digital evidence can be extracted and preserved from Docker containers. To achieve this, a test machine was configured with Docker together with various monitoring tools. DVWA was used as a vulnerable environment to generate suspicious activities and behaviors that resemble real attacks.

The process begins with the technical preparation of the environment, installation of dependencies, and startup of the container. Subsequently, several actions are performed within DVWA, such as SQL injection, brute force attack, parameter manipulation, XSS, and file upload, with the aim of generating real transactions in the logs, network traffic, and modifications in the internal system of the container to generate verifiable evidence.

Three acquisition methods were then applied for this investigation: live capture, snapshot, and post-mortem acquisition. Live capture involves the collection of logs, metadata, network traffic, and statistics from the active process. In the snapshot phase, a frozen image of the container is generated to analyze its status at a specific point in time, in addition to recording resource consumption. In the post-mortem stage, the container is stopped and the file system is extracted along with its final configuration. All information extracted from each of the phases is stored in separate folders and hashes are generated to ensure authenticity.

In order to simplify the entire extraction procedure, an automated script was created which executes each of the phases in an orderly and autonomous manner. Prior to execution, the script verifies that the environment is correctly configured, generates evidence folders to subsequently execute the corresponding captures, and then calculates cryptographic hashes.

Keywords: Docker, digital evidence, DVWA, live capture, snapshot, post-mortem, automated script, cryptographic integrity.