**Logotipo

Descripción generada automáticamente con confianza media**

**Práctica de Volatility realizada por Juan Luis Domínguez López.**

Índice

[1. Introducción a Volatility 3](#_Toc181816748)

[2. Creación de una Imagen de Memoria 3](#_Toc181816749)

[3. Análisis de la Imagen con Volatility. Una vez que tengas la imagen de memoria, puedes utilizar Volatility para extraer información relevante. Los comandos más relevantes vistos en clase y los más conocidos son: 3](#_Toc181816750)

[4. Escenarios Prácticos 7](#_Toc181816751)

# Introducción a Volatility

* Qué es Volatility.

Volatility es una herramienta de análisis forense de memoria que permite analizar volúmenes de memoria volátil (RAM) capturados de sistemas en ejecución. Se utiliza para realizar investigaciones y estudios sobre incidentes de seguridad, obtener información sobre el estado de un sistema, identificar malware y mucho más. En tu manual, podrías estructurarlo en varias secciones para cubrir la introducción a Volatility, el proceso de creación y análisis de la imagen de memoria, así como los comandos clave para realizar el análisis forense.

# Creación de una Imagen de Memoria

* Proceso de capturar una imagen de memoria en Windows:
  + Uso de la herramienta DumpIT.

# Análisis de la Imagen con Volatility. Una vez que tengas la imagen de memoria, puedes utilizar Volatility para extraer información relevante. Los comandos más relevantes vistos en clase y los más conocidos son:

* **Ver la información básica del sistema:** Este comando proporciona detalles sobre la imagen de memoria, como el perfil del sistema operativo y las fechas.

Texto

Descripción generada automáticamente

volatility -f win-xp-laptop-2005-06-25.img --profile= WinXPSP2x86 imageinfo

* **Listar procesos activos:** Muestra los procesos en ejecución al momento de capturar la memoria.

Imagen que contiene Texto

Descripción generada automáticamente

volatility -f win-xp-laptop-2005-06-25.img --profile= WinXPSP2x86 pslist

* **Detección de malware o rootkits:** Utilizando el comando malfind se puede identificar regiones de memoria sospechosas, a menudo asociadas con malware.

Texto

Descripción generada automáticamente

volatility -f win-xp-laptop-2005-06-25.img --profile= WinXPSP2x86 malfind

* **Listar procesos con información de direcciones de memoria:** Muestra los procesos activos con sus direcciones de memoria y detalles de módulos cargados.

Imagen de la pantalla de un computador

Descripción generada automáticamente con confianza baja

volatility -f win-xp-laptop-2005-06-25.img --profile= WinXPSP2x86 psxview

* **Listar los módulos cargados**: Muestra los módulos (DLLs, controladores, etc.) cargados en el sistema durante la ejecución.

Texto

Descripción generada automáticamente

volatility -f win-xp-laptop-2005-06-25.img --profile= WinXPSP2x86 modules

* **Escanear el volcado para detectar kernels rootkits**: El plugin kdbgscan busca estructuras de depuración del núcleo para detectar rootkits.

Texto

Descripción generada automáticamente

volatility -f win-xp-laptop-2005-06-25.img --profile= WinXPSP2x86 kdbgscan

* **Escanear las conexiones de red (incluidas las desconectadas)**: Muestra tanto las conexiones activas como las desconectadas en la memoria.

Texto

Descripción generada automáticamente

volatility -f win-xp-laptop-2005-06-25.img --profile= WinXPSP2x86 connscan

* **Escanear y listar archivos en memoria**: Muestra archivos que estaban en uso en la memoria.

Texto

Descripción generada automáticamente

volatility -f win-xp-laptop-2005-06-25.img --profile= WinXPSP2x86 filescan

# Escenarios Prácticos

* **Abrir programas**: Iniciar un programa en el sistema (por ejemplo, un navegador web o un editor de texto) y luego capturar la memoria para ver los cambios asociados al proceso.
* **Escribir en la línea de comandos**: Ejemplo de cómo capturar la entrada de un comando en la memoria (por ejemplo, escribir un comando simple como dir o ipconfig en la línea de comandos de Windows).
* **Infectar la imagen con un virus**: En este escenario, puedes simular la ejecución de un archivo malicioso, como un archivo .exe que activa un virus, y luego realizar el análisis con Volatility para detectar cambios en la memoria relacionados con la infección (por ejemplo, ejecución de procesos sospechosos, cambios en el registro, etc.).