Informe de Análisis Forense de Memoria

Alumno: Aníbal Giordani

Herramienta utilizada: Volatility 3

Descripción de la evidencia

Sistema operativo analizado: Windows 10.

Tamaño del volcado de memoria: [Completar con el tamaño del archivo memdump.mem].

Ruta del volcado: C:\Users\aniba\Desktop\ciber\memory_dump\memdump.mem

Herramientas utilizadas:
- Volatility 3 Framework v2.26.2
- Plugins: windows.pslist, windows.netscan, windows.cmdline, windows.filescan, windows.svcscan, windows.registry.printkey, windows.malfind.

Listado de procesos sospechosos y justificación

```
python vol.py -f memdump.mem windows.pslist
```

```
python vol.py -f memdump.mem windows.psscan
```

No se identificaron procesos claramente sospechosos.

Todos los procesos observados corresponden a servicios habituales del sistema operativo (svchost.exe, explorer.exe, etc.).

No se hallaron nombres extraños o ubicaciones inusuales.

Análisis de conexiones de red y posibles amenazas

```
python vol.py -f memdump.mem windows.netscan
```

Se revisaron conexiones activas con windows.netscan.

Puertos utilizados: HTTP (80), HTTPS (443), DNS (53).

No se observaron conexiones sospechosas a direcciones IP desconocidas.

Extracción de credenciales o información relevante

Este comando falló, no está implementado en Volatility 3

python vol.py -f memdump.mem windows.hashdump

El plugin windows.hashdump no está disponible en Volatility 3.

Se revisaron claves del registro con windows.registry.printkey.

No se encontraron configuraciones extrañas en HKLM\Software\Microsoft\Windows\CurrentVersion\Run.

Cualquier hallazgo sospechoso

python vol.py -f memdump.mem windows.malfind

Comando adicional para analizar archivos cargados:

python vol.py -f memdump.mem windows.filescan

windows.malfind no detectó código inyectado ni comportamientos maliciosos.

windows.filescan mostró archivos legítimos del sistema, sin DLLs ocultas ni ejecutables desconocidos.

Medidas de mitigación y recomendaciones finales

Durante el análisis forense de la memoria no se encontraron evidencias concluyentes de actividad maliciosa. Aun así, como buena práctica y por prevención, se recomiendan las siguientes acciones:

1. **Revisar servicios activos** como *SECOMNService* y *ZTHELPER*, que si bien pueden ser legítimos, podrían ser verificados con el proveedor del sistema o consultando su origen.

2. **Actualizar el sistema operativo y los programas instalados** para reducir la superficie de ataque.

3. **Reforzar la monitorización de eventos** en tiempo real mediante herramientas EDR o Sysmon.

4. **Hacer un backup actualizado** del sistema si se considera estable y confiable.

5. **Establecer un punto de control o snapshot**, útil en caso de que aparezcan síntomas posteriores.