Informe de Ciberseguridad: Análisis Forense con Autopsy

1. Introducción

El presente informe detalla los hallazgos obtenidos durante el análisis forense digital de un sistema operativo utilizando la herramienta Autopsy. El objetivo fue identificar evidencias relevantes, reconstruir la línea de tiempo de actividades y determinar posibles incidentes de seguridad.

---

2. Metodología

- Herramienta utilizada: Autopsy (The Sleuth Kit).
- Tipo de análisis: Forense digital (análisis de archivos, registros, metadatos y línea de tiempo).
- Fuente de datos: Imagen forense del disco duro (formato .dd o .E01).

---

3. Evidencias Relevantes Identificadas

3.1. Archivos sospechosos o maliciosos

- Se identificaron archivos ejecutables (.exe, .dll) en ubicaciones no estándar (C:\Temp\script.exe).
- Presencia de scripts (.vbs, .ps1) con nombres genéricos (update.vbs, temp.ps1).
- Archivos ocultos o eliminados recuperados mediante análisis de espacio no asignado.

3.2. Registros de actividad

- Registro de eventos de Windows (Event Logs):
    - Intentos fallidos de inicio de sesión (Event ID 4625).
    - Ejecución de procesos sospechosos (Event ID 4688).
- Historial de navegación (Chrome/Edge):
    - Acceso a sitios web maliciosos o de phishing.
    - Descargas de archivos ejecutables desde dominios no confiables.

3.3. Metadatos y artefactos

- Archivos Prefetch:
    - Ejecución reciente de herramientas de hacking (mimikatz.exe, nmap.exe).
- Registro SAM y SYSTEM:
    - Modificaciones en cuentas de usuario (creación/eliminación de usuarios).
- Archivos temporales (Temp):

- Rastros de herramientas de exfiltración de datos (Rclone, 7-Zip con nombres alterados).

---

4. Línea de Tiempo de Actividades

Fecha/Hora	Evento	Significado
2024-05-10 14:30:22	Creación de usuario Admin2	Posible escalada de privilegios.
2024-05-10 15:12:45	Ejecución de mimikatz.exe	Intento de extracción de credenciales.
2024-05-10 16:05:33	Conexión a IP externa	Posible exfiltración de datos.
2024-05-11 09:20:11	Eliminación de archivos en C:\Documents	Intentos de borrado de evidencias.

---

5. Conclusiones

1. Compromiso de seguridad confirmado:
   - Se detectaron actividades maliciosas, incluyendo ejecución de herramientas de hacking (mimikatz), creación de usuarios no autorizados y conexiones a IPs sospechosas.
2. Técnicas de evasión:
   - El atacante eliminó archivos y utilizó ubicaciones temporales para evitar detección.
3. Recomendaciones:
   - Contención: Aislar el sistema afectado y resetear contraseñas.
   - Análisis adicional: Revisar logs de firewall/IDS para identificar la fuente del ataque.
   - Hardening: Implementar políticas de ejecución (AppLocker) y monitoreo de procesos.

---

6. Anexos

- Capturas de pantalla de Autopsy (opcional).
- Hashes (MD5/SHA-1) de archivos maliciosos.