Proof of Concept Report

Name : Sanika Ramesh Raskar

Intern ID : 236

⚒️ Tool Name:

Digital Footprint Tools(Hollowshunter HxD)

🕰️ History:

Hollowshunter was designed to tackle the increasing threat of fileless malware and in-memory attacks, which are typically overlooked by conventional antivirus software and disk-based tools. Originally installed as a process hollowing specialist detection tool, it has since become a robust memory analysis tool.

HxD, initially designed as an independent hex editor, was reconfigured and reengineered by cybersecurity professionals to support digital forensics operations to enable investigators to examine and extract traces from volatile memory comprehensively. Used in conjunction with Hollowshunter, HxD is now a favorite toolkit for incident response, malware analysis, and threat hunting operations.

📄 Description:

Hollowshunter HxD facilitates the identification of electronic evidence through scanning of volatile memory for user activity traces, including browser histories, session information, and injected-processes. It is particularly useful for the identification of fileless malware and temporary artifacts. It also extracts critical information from memory dumps or live systems, thereby facilitating timeline reconstruction and forensic analysis.

📌 What Is This Tool About?

Hollowshunter HxD is a hex analysis and memory forensics tool employed to uncover digital evidence due to malicious behavior or user activity in the system memory. During digital footprint examination, the tool detects hidden or abnormal processes like process hollowing and extracts meaningful remnants from volatile memory (RAM) that include browser artifacts, session residue, and injected code.

Through its focus on contemporary process and memory activity, Hollowshunter HxD reveals signs of fileless malware, running processes, and in-memory digital evidence not visible to traditional disk-based technology. Its worth is especially realized in live incident response situations, memory forensic analysis, and APT investigations.

⭐ Key Characteristics / Features:

- This application detects process hollowing, code injection, and memory manipulation
- Detects digital traces in memory, including browser traces and session information.
- Offers live memory testing and snapshot features
- Converts system-level information: handles, DLLs, threads, modules
- Functions as a hexadecimal editor with temporary memory access.
- Facilitates search, diff, highlighting, and pattern matching
- Not installed and portable
- Both RAM dumps (.dmp) and live system memory dumps
- GUI and CLI interface for general use
- Compatible with Volatility plugins developed to support in-depth memory analysis.
- Highly capable of identifying fileless malware, injected shellcodes, and concealed backdoor methods.
- Facilitates exportation of memory regions for offboard analysis
- Produces forensic logs and session-based reports
- Discovers anomalies by analyzing behavioral or structural features.
- Augments digital forensic software such as Autopsy, X-Ways, and Volatility

🔧 Types / Modules Available:

- Process Hollowing Detector – Identifies hollowed or injected processes
- Memory Artifact Extractor – Pulls browser history and session data from RAM
- Browser Trace Parser – Pulls cached cookies and URLs from temporary memory.
- Handle & Module Mapper – Shows currently running process handles and loaded modules
- Snapshot Viewer – Captures and compares memory snapshots.
- Anomaly Detection Engine – Detects anomalous behavior and shellcode that is in memory

🎯 How Will This Tool Help?

- Detects hidden or implanted mechanisms used during cyber attacks.
- Gets browser and session traces directly from memory.
- Tracks the user activity and web usage independently of disk artifacts.
- Assists with fileless malware detection and in-memory persistence.
- Facilitates forensic examination and live incident response
- Supplements timeline reconstruction and threat profiling

📜 15-Liner Summary:

1. Catches process hollowing and code injection
2. Copies browser and session data from the volatile memory.
3. Light, lightweight, and no installation required
4. Supports both GUI and command-line interface
5. Useful for analyzing RAM dumps and live systems
6. Identifies irregularities in hexadecimal and ASCII representations.
7. Exports memory areas for offline analysis later.
8. Integrates with forensic utilities such as Volatility.
9. Supports keyword filtering (e.g., search queries, URLs)
10. Enables memory change comparison through snapshots
11. Beneficial when monitoring fileless malware activity
12. Exhibits effective usage in incidents and forensic investigations.
13. Maps loaded modules and process handles
14. Offers forensics-capable logging and documentation
15. Perfect for cybercrime squads and digital forensic units

⏱️ Time to Use / Best Case Scenarios:

- While dealing with live incidents to obtain volatile memory
- After they have acquired a RAM dump from an offending host
- When researching fileless malware or in-memory exploits
- Before they shut down or restart (to preserve footprints)
- While investigating suspicious background processes
- In initial phases of threat actor profiling
- In cases when disk forensics generates little output
- During the investigation of memory-based browser traces
- In order to verify if malware hijacked legitimate processes

🕵️ When to Use During Investigation:

- In memory forensics after suspected compromise
- While monitoring fileless or memory-resident malware
- In browser usage, phishing or social engineering attacks
- For insider threat incidents involving system abuse
- When considering unauthorized process injections
- In remote access tool or its traces related cases
- While restoring a user's in-memory session activity
- Inflight threat identification during live response

👨‍💻 Best Person to Use This Tool & Required Skills:

👤 Best User:

- Digital Forensics Investigator
- Malware Analyst
- Incident Responder
- Threat Hunter

🧠 Required Skills:

- Learning memory forensics and process injection.
- Hexadecimal and ASCII data interpretation capability.
- Experience with Volatility or similar memory analysis tools.
- Basic knowledge of browser memory data structures
- Proficiency in operating both CLI and GUI-based tools

🧩 Flaws / Suggestions to Improve:

- Does not support acquisition of cloud-based memory
- Limited cross-compatibility with Linux and macOS platforms
- Lacks real-time alerting or behavior scoring
- No inherent hash validation for memory areas
- Visual reporting would be complemented by graph-based summaries
- Requires more support for encrypted or obfuscated memory areas
- Can support automatic pattern/shellcode detection
- GUI design is dated and not for beginners

✅ Good About the Tool:

- Lightweight and portable (no installation required)
- Great for RAM dump and live memory examination
- Effective at identifying process hollowing and code injection
- Supports searching, highlighting, and diffing in memory
- It integrates perfectly with forensic tools like Volatility
- Capable of searching for session and browser traces.
- Quick execution, even in handling large memory dumps.
- Both command-line and GUI support
- Best suited for fileless malware investigations.
- Creates forensics-ready output for documentation