ENHANCED SECURITY MONITORING & EVIDENCE COLLECTION SYSTEM

AUTHOR: DIAMARIS GONZÁLEZ RODRÍGUEZ
ADVISOR: LISABEL RODRÍGUEZ ESPINOSA, J.D.
COMPUTER SCIENCE

ABSTRACT

As cyber threats become more sophisticated, attackers leverage stealth techniques such as fileless malware and memory-based exploits, bypassing traditional security measures. Organizations struggle to detect unauthorized logins and preserve forensic evidence essential for incident response and compliance. The Enhanced Security Monitoring & Evidence Collection System proactively identifies security threats, integrates forensic techniques, and automates evidence preservation, strengthening cybersecurity resilience.

BACKGROUND

Modern cyber threats often operate entirely in volatile memory, leaving little trace on disk-based security solutions. Memory forensics plays a crucial role in identifying malicious activities, unauthorized logins, and hidden processes that evade standard detection methods. This project combines event-driven security monitoring and advanced forensic analysis to empower security professionals with actionable insights for mitigating intrusions and safeguarding digital infrastructures.

PROBLEM

Many security breaches occur due to unauthorized login attempts and stealth malware that bypass conventional security measures. Threat actors often manipulate system memory, leaving limited traces on disk. Real-time monitoring and forensic analysis are crucial for detecting these threats before significant damage occurs. Existing solutions lack a structured approach to memory forensics, making investigation difficult.

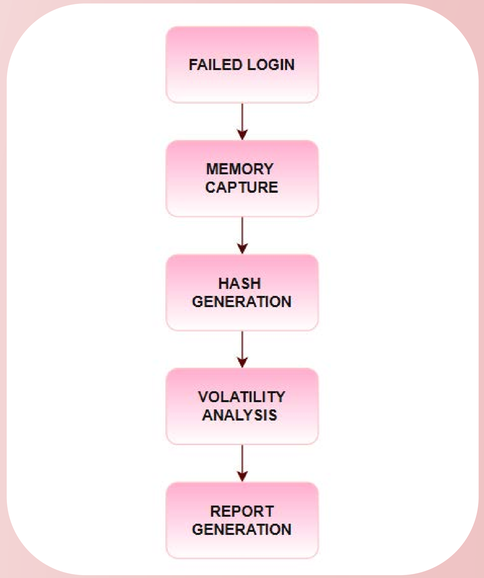

Figure 1: Forensics Analysis Process

RESULTS AND ANALYSIS

This tool was successfully tested, demonstrating its ability to detect unauthorized login attempts, collect forensic evidence, and generate structured security reports. The system accurately identified suspicious login attempts in real time by continuously monitoring Windows Event Logs, reducing response time, and improving security awareness. Upon detecting failed logins, it triggered memory dump collection, ensuring forensic preservation of volatile system data crucial for post-incident investigations. Additionally, cryptographic hashing verifies data integrity, preventing tampering and ensuring reliable forensic evidence. Using Volatility, the collected memory dumps were analyzed for hidden threats, injected malicious code, and suspicious activity. The system generated JSON-based security reports containing detailed event logs and forensic findings, supporting compliance and legal investigations.

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

STDOUT:
ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[22:14:53] Dump 1 initiated: C:\Users\Engr.Rehan\Desktop\sime\evidence\memory-31.dmp
[22:14:53] Dump 1 writing: Estimated dump file size is 55 MB.
[22:14:53] Dump 1 complete: 56 MB written in 0.2 seconds
[22:14:54] Dump count reached.


STDERR:
[SUCCESS] Hashes saved to: evidence\hashes_20250211_221454.txt
[SUCCESS] Hashes saved to: evidence\hashes_20250211_221454.txt
[SUCCESS] Hashes saved to: evidence\hashes_20250211_221454.txt
[SUCCESS] Security report generated: reports\security_report_20250211_221454604302.json
[ALERT] Failed login from C:\Windows\System32\svchost.exe at 2025-02-11 22:12:51
[*] Starting evidence collection...
```

Figure 2: Real-time Monitoring and Evidence Collection

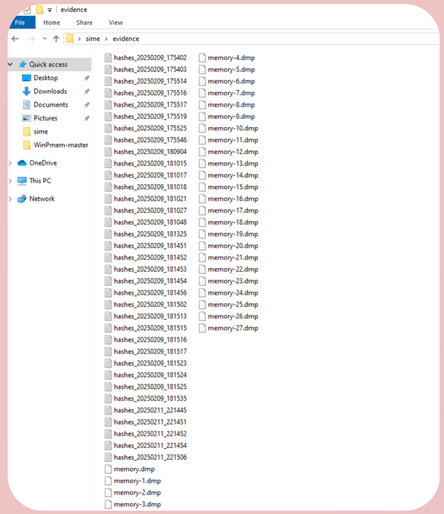

Figure 3: Memory Dump and File Hashing

Figure 4: Generated Security Reports

```
{
  "metadata": {
    "generated_at": "2025-02-11T22:15:06.924894",
    "system": "DESKTOP-80D0HBR",
    "analyst": "Security Team",
    "report_version": "1.1"
  },
  "security_events": [
    {
      "timestamp": "2025-02-11 22:12:51",
      "source_ip": "C:\\Windows\\System32\\svchost.exe",
      "event_id": 4625,
      "message": "[ALERT] Failed login from C:\\Windows\\System32\\svchost.exe at 2025-02-11 22:12:51",
      "event_data": [
        "S-1-5-18", "DESKTOP-80D0HBR$", "WORKGROUP", "0x3e7", "S-1-0-0", "diama", "DESKTOP-80D0HBR",
        "0xc000006d", "%%2313", "0xc000006a", "2", "User32", "Negotiate", "DESKTOP-80D0HBR", "-",
        "-", "0", "0x3ec", "C:\\\\Windows\\\\System32\\\\svchost.exe", "127.0.0.1", "0"
      ]
    }
  ],
  "evidence": {
    "memory_dumps": [],
    "hash_files": [
      "C:\\Users\\diama\\Desktop\\sime\\evidence\\hashes_20250211_221506.txt",
      "C:\\Users\\diama\\Desktop\\sime\\evidence\\hashes_20250211_221506.txt",
      "C:\\Users\\diama\\Desktop\\sime\\evidence\\hashes_20250211_221506.txt"
    ],
    "volatility_reports": []
  }
}
```

Figure 5: Security Report Metadata

CONCLUSION

The Enhanced Security Monitoring & Evidence Collection System strengthens cybersecurity by detecting unauthorized logins, preserving forensic evidence, and analyzing security threats in real time. It automates event monitoring, memory dump collection, and file integrity verification, ensuring reliable forensic investigations. By integrating event-driven monitoring and forensic techniques, this system provides a proactive cybersecurity tool, enabling organizations to detect, analyze, and mitigate security risks effectively. Future enhancements could include monitoring for modifications of malware, rootkits, or any suspicious devices connected during the login process.

ACKNOWLEDGEMENTS

I want to sincerely thank my advisor, Lisabel Rodríguez Espinosa, J.D, for her support and guidance throughout this project. Her expertise and advice have been invaluable in shaping this work, and her encouragement has been greatly appreciated during every step of its development.

REFERENCES

[1] R. Smith and M. J. Thompson, “Indicators of Compromise: A Real-Time Analysis of Memory Artifacts for Threat Detection,” International Journal of Cyber Threat Intelligence, vol. 38, no. 5, pp. 124–138, 2025.