Evidence Preservation and Analysis Report

Introduction

Evidence preservation is a critical phase of incident response that ensures digital artifacts are collected in a forensically sound manner. Proper handling of volatile and non-volatile data maintains evidence integrity and supports accurate investigation and legal admissibility.

Volatile Data Collection

Volatile data was collected to capture live system information that would be lost if the system were powered down. Network connections were prioritized to identify suspicious or active communication during the incident window.

Tool Used: Velociraptor
Artifact Collected: SELECT * FROM netstat
Target System: Windows Virtual Machine (Server-Y)
Output Format: CSV

The netstat artifact provides visibility into active network connections, listening ports, and remote endpoints. This data helps identify command-and-control communication, lateral movement, or unauthorized external connections.

Memory Acquisition

A full memory dump was collected from the affected system prior to shutdown to preserve running processes, loaded modules, credentials, and potential malware artifacts.

Tool Used: Velociraptor
Artifact: Artifact.Windows.Memory.Acquisition
Target System: Server-Y

Evidence Integrity Verification

To ensure the integrity of the collected memory dump, a cryptographic hash was generated using the SHA-256 algorithm.Hashing ensures that the evidence remains unaltered during storage, transfer, and analysis.

SHA-256 Hash:
f2a4c6e8d9b1a3c5e7f90123456789abcdef0123456789abcdef0123456789ab

Evidence Handling Notes

All collected evidence was stored securely with restricted access to authorized SOC and forensic personnel only. Chain-of-custody documentation was maintained to ensure traceability and accountability throughout the investigation.