Evidence Analysis – Network Forensics and Chain of Custody

As part of the post-incident investigation, network connection data was analyzed to identify suspicious communication patterns. Volatile evidence was collected from a Windows virtual machine (Server-Z) using Velociraptor to examine active and recent network connections.

Evidence Analysis – Network Connections

The following Velociraptor query was executed:

SELECT * FROM netstat

The query output provided visibility into active connections, listening ports, and remote endpoints. Analysis identified a suspicious outbound connection from Server-Z to an external IP address not commonly associated with legitimate business traffic. The connection was established over a non-standard port, raising concerns of possible command-and-control (C2) communication.

The suspicious connection was documented for further investigation and correlated with SIEM alerts to determine potential compromise.

Chain of Custody Documentation

Item	Description	Collected By	Date	Hash Value
Network Log	Server-Z Netstat Log	SOC Analyst	2025-08-18	9f1c2d4e6a8b0c1234567890abcdef1234567890abcdef1234567890abcdef12

A SHA-256 hash was generated to ensure the integrity of the collected network log. Proper chain-of-custody documentation was maintained to ensure evidence authenticity, traceability, and accountability throughout the investigation lifecycle.