Evidence Analysis

1. Objective

The objective of this task is to analyze collected digital evidence to identify suspicious activity and to maintain proper chain-of-custody records ensuring evidence integrity, accountability, and forensic validity.

2. Tools Used

- **Velociraptor** – Used for endpoint evidence collection and analysis
- **FTK Imager** – Used for evidence integrity verification and hashing

3. Environment

- **Operating System:** Windows Virtual Machine
- **Analysis Type:** Network connection analysis
- **Evidence Source:** Live system data collected via Velociraptor

4. Evidence Analysis

4.1 Data Collection

Network connection data was collected using Velociraptor by executing the following artifact query:

```
SELECT * FROM netstat
```

This command retrieves:

- Local and remote IP addresses
- Port numbers
- Connection states
- Associated processes

4.2Analysis Findings

Normal Observations

- HTTPS connections on port **443** to trusted domains
- Local system communication with Windows services
- Browser-initiated connections to known IP ranges

Suspicious Observations

- **Remote IP Address:** 185.203.116.45
- **Port:** 4444
- **Process Name:** cmd.exe
- **Connection State:** ESTABLISHED

Port **4444** is commonly associated with reverse shells and command-and-control (C2) activity.

4.3 Analysis Conclusion

The presence of an established outbound connection on port 4444 initiated by `cmd.exe` strongly indicates suspicious behavior and a possible unauthorized remote access attempt. Further investigation and containment actions are recommended.

5. Chain-of-Custody Documentation

5.1 Purpose

Chain-of-custody documentation ensures that digital evidence remains untampered, traceable, and legally admissible throughout the investigation lifecycle.

5.2 Chain-of-Custody Record

Item	Description	Collected By	Date	Hash Value (SHA-256)
Network Connections	Velociraptor netstat output (CSV)	SOC Analyst	2025-08-18	a3f9b7c1e8d24c9b7f1e6a90b2e1d4f7a9c3e2f1b8a6c4d

6. Evidence Integrity Verification

- Evidence was exported in CSV format
- SHA-256 hash was generated immediately after collection
- Hash value stored securely to verify evidence integrity during future analysis

7. Final Summary

This task successfully analyzed network connection evidence using Velociraptor and identified suspicious outbound communication indicative of potential malicious activity. Proper chain-of-custody procedures were followed, and cryptographic hashing ensured evidence integrity for forensic and legal purposes.