Alex Smith

Digital Forensics in Cybersecurity – D431 Task 1

Investigative Plan of Action: Forensic Best Practices

A1: Strategy

STEP 1: Preparation of the Investigation Team

Objective: To brief the investigation team on the critical aspects of the case involving John Smith, I will establish who, what, when, where, and why to set clear goals for the investigation

1. **Who:** John Smith, a mechanical engineer suspected of taking proprietary information, and other potential witnesses or relevant parties

2. **What:** Unauthorized access and potential theft of proprietary information, in violation of NDAs and AUPs

3. **When:** Establish the timeline of the suspected activities to narrow down the evidence collection period

4. **Where:** Focus on John Smith's workstation, network activity logs, email accounts, work phone or any removable storage devices he may have used

5. **Why:** To determine the extent of the policy violation and mitigate potential damage to the company

Goal: The primary goal is to collect as much relevant evidence as possible to support while minimizing disruption to the organization's operations

STEP 2: Data Acquisition

Securing the Scene:

- Remove all unnecessary personnel to prevent tampering of evidence

- Document the scene with photographs and detailed notes before beginning evidence collection

Data Acquisition Procedures:

- **Memory Acquisition:** Execute a memory acquisition on John Smith's workstation to capture volatile data, which can be lost if the machine is powered down. Memory acquisition is a crucial step in digital forensics where the data stored in a computer's RAM (Random Access Memory) is captured for analysis. RAM is a temporary storage area for data that the computer is currently using. Since the contents of RAM are lost when the computer is turned off or restarted, it is crucial to capture this data quickly

- **Disk Imaging:** Create a forensic image of the workstation's storage using tools like FTK Imager or EnCase. Calculate and record hash values (MD5, SHA-1) to ensure data integrity

- **Use of Write Blockers:** Utilize hardware or software write blockers to prevent any changes to the source data during the acquisition process

- **Data Extraction Tools:** Employ forensic tools like FTK (Forensic Toolkit) or EnCase to comprehensively extract data

A2: Tools and Techniques

Forensic Tools:

- FTK (Forensic Toolkit): Ideal for data imaging, analysis, and reporting, FTK offers powerful features for indexing and searching data, which simplifies the process of finding relevant evidence

- EnCase: Useful in disk imaging, data analysis, and secure evidence management, supporting multiple file systems. It also provides robust reporting tools for thorough analysis and documentation
-

Techniques:

- **Hash Value Verification:** Use hash values (MD5, SHA-1) to verify the integrity of the collected data

- **Keyword Searching:** Employ keyword searches to locate specific terms related to the investigation

- **Timeline Analysis**: Involves creating a chronological sequence of events to grasp the context and order of activities related to the policy violation

A3: Collection and Preservation of Evidence

Chain of Custody:

- Document every step of evidence handling to maintain a clear chain of custody, including who collected the evidence, when, where, and how it was stored and accessed

- Use evidence bags and tamper-evident seals to secure physical devices

Data Housing:

- Store collected evidence in a secure, access-controlled environment.

- Use digital storage solutions with redundancy and regular backups to prevent data loss.

A4: Examination of Evidence

Best Practices and Procedures:

- **Initial Triage:** Quickly assess the evidence to identify the most relevant items for detailed analysis. Disconnect any devices from the internet and do not connect mobile devices to any evidence.

- **Detailed Analysis:** Use forensic tools to perform a thorough examination of digital evidence. Focus on file contents, metadata, logs, and communication records.

- **Indicators:** Look for unauthorized access attempts, modifications to files or settings, suspicious communications, and unusual activity patterns.

Immediate Indicators:

- Specific keywords or phrases related to proprietary information.
- Anomalous timestamps indicating potential tampering or unauthorized access.
- Unusual network traffic patterns or connections to suspicious IP addresses.

A5: Approach to Drawing Conclusions

Investigation Protocols:

- Conduct the investigation in strict accordance with company policy and legal requirements.
- Ensure that all findings are based on unaltered, verifiable evidence.
- Use multiple sources or methods to ensure reliability.

A6: Presentation of Details and Conclusions

Presentation Format:

- **Technical Summary:** Create a thorough report for senior management, detailing how evidence was collected, analyzed, and the conclusions drawn. Ensure the report is easy to understand for non-technical individuals by using plain language and explanations of the methodologies used.
- **Executive Summary:** Create a concise, non-technical executive summary highlighting key findings and their implications for the organization.

- **Presentation Tools:** Use PowerPoint or other visual aids to present the findings clearly and effectively.

Details to Include:

- Overview of the investigation process and key steps taken.
- Summary of evidence collected and its relevance to the case.
- Clear, logical conclusions based on the evidence.
- Recommendations for future actions or improvements in policies and security measures.

References:

National Institute of Standards and Technology (NIST) Special Publication 800-86:

- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). **Guide to Integrating Forensic Techniques into Incident Response**. NIST Special Publication 800-86. National Institute of Standards and Technology.
- URL: NIST SP 800-86

National Institute of Standards and Technology (NIST) Special Publication 800-88:

- Kissel, R., Regenscheid, A., Scholl, M., & Stine, K. (2014). **Guidelines for Media Sanitization**. NIST Special Publication 800-88 Revision 1. National Institute of Standards and Technology.
- URL: NIST SP 800-88

EnCase Forensic Imager:

- OpenText. (2023). **EnCase Forensic Imager**.
- URL: OpenText EnCase

FTK Imager User Guide:

- Exterro. (2023). **FTK Imager User Guide**. Exterro.
- URL: FTK Imager Guide