Assignment 8: The Jean Incident

CSCI 297E: Ethical Hacking

Due Date: 2024-05-24

Overview

In this assignment, you will analyze the M57 Jean case, a simulated corporate espionage scenario designed to teach digital forensic investigation techniques. You will use various forensic tools to examine digital evidence and uncover the activities and intentions of the involved parties.

Objectives

- Understand the context and details of the M57 Jean case.
- Use forensic tools to analyze disk images and other digital evidence.
- Document your findings and present a comprehensive forensic report.

Resources

- **Case Description**: M57 Jean Case Description
- **Disk Images**: Download the disk images from the provided resources on the case description page.
- **Forensic Tools**: FTK, EnCase, Autopsy, or other forensic tools of your choice.
- **Documentation**: Document your findings in a text file and create the final report.

Tasks

1. Case Familiarization

Read the M57 Jean case description to understand the background, key players, and the scenario.

2. Disk Image Analysis

Download the disk images provided in the case resources. Use your forensic tool of choice to mount and analyze these images. Focus on the following:

- Identify key files and directories related to the investigation.
- Look for any suspicious activities, such as unauthorized access or data exfiltration.
- Recover deleted files and examine their contents.

3. Timeline Reconstruction

Create a timeline of events based on your analysis. Include key activities, file accesses, and any other relevant information that helps reconstruct the events in the case.

4. Identify the Suspect

Based on the evidence you have gathered, identify the suspect(s) involved in the corporate espionage. Provide a detailed explanation of how you arrived at your conclusion.

5. Document Your Findings

Write a comprehensive forensic report documenting your findings. Your report should include the following sections:

- **Introduction**: Brief overview of the case and objectives.
- **Methodology**: Tools and techniques used in your analysis.
- **Findings**: Detailed description of the evidence you discovered.
- **Timeline**: Reconstructed timeline of events.
- **Conclusion**: Summary of your findings and identification of the suspect(s).
- **Appendices**: Any additional information, such as screenshots or logs, that support your findings.

6. Submit Your Report

Submit your final report on canvas.

Deadline

All submissions are due by the end of the week. Late submissions will not be accepted.

Evaluation

Your assignment will be evaluated based on the following criteria:

- Completeness and accuracy of the forensic analysis.
- Clarity and organization of the report.
- Correct usage of forensic tools and techniques.
- Ability to identify and document key evidence.
- Professionalism and thoroughness of the final report.