Lab 10: Performing Incident Response and Forensic Analysis

Brandon Trinkle

Arizona State University

IFT 381

Professor John A. Lewis

11/2/2024

**Lab 10: Performing Incident Response and Forensic Analysis**

During this lab, I found myself fully engaged and enjoyed every aspect of forensic analysis. Analyzing PCAP files, disk images, and email evidence allowed me to apply and strengthen my skills in incident response. My ability to trace compromised credentials, pinpoint unauthorized access attempts, and compile a detailed timeline of events highlighted my strengths in this domain. Each task provided valuable practice in using forensic techniques to gather and interpret digital evidence.

The lab’s design was effective in replicating real-world forensic scenarios, and the instructions were clear and supportive of my learning experience. I particularly appreciated the comprehensive range of tools and techniques provided, as they allowed me to explore various aspects of forensic investigation in depth. Each step, from analyzing network packets to documenting findings, reinforced critical skills required for effective incident response and helped to build confidence in handling similar scenarios.

One recommendation for improvement would be to incorporate additional complex scenarios, perhaps involving more advanced social engineering tactics or multi-stage attacks, to further deepen forensic analysis skills. Adding these elements could better simulate the nuanced challenges faced in real-world cybersecurity roles. Overall, the lab was a valuable and enjoyable experience that provided insight into forensic analysis and strengthened my readiness for handling actual incident responses.

# References

Jones & Bartlett Learning. (2024, November 2). *Lab Access for Fundamentals of Information Systems Security*. Retrieved from Jones & Bartlett Learning: https://navigate2.jblearning.com/course/view.php?id=129690