Lab 8: Implementing Security Monitoring and Logging

Brandon Trinkle

Arizona State University

IFT 381

Professor John A. Lewis

11/9/2024

**Lab 8: Implementing Security Monitoring and Logging**

During this lab on implementing security monitoring and logging, I navigated the tasks with ease and did not encounter any significant challenges. The lab instructions were clear and provided step-by-step guidance, which helped in completing activities like monitoring failed logon attempts, setting up Snort for network monitoring, and configuring health checks for server availability. My previous experience with tools like the Windows Event Viewer and Snort allowed me to efficiently identify audit failures and establish network intrusion prevention measures.

A key area where I excelled was in analyzing the cryptographic error related to Event ID 5061. I was able to interpret the logs accurately, diagnose the issue, and suggest corrective actions, such as reviewing user permissions and ensuring proper key storage configurations. This ability to quickly assess and address system errors is vital in real-world environments where monitoring logs is crucial for ensuring system security.

However, while the lab was straightforward, it could be enhanced to better prepare students for real-world applications. Including more complex scenarios involving multi-system interactions and network segmentation would make the lab more realistic. Additionally, exploring advanced Snort configurations, such as using inline mode instead of legacy blocking, would align with current industry practices for intrusion prevention and provide a deeper understanding of modern security measures.

Overall, this lab offered practical experience in using security tools to monitor and secure systems. The skills developed here are directly applicable to real-world IT infrastructure, reinforcing my ability to implement effective security solutions in professional settings.

# 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