Lab 3: Performing packet capture and traffic analysis

Brandon Trinkle

Arizona State University

IFT 381

Professor John A. Lewis

11/2/2024

Lab 3: Performing packet capture and traffic analysis

This lab in packet capture and traffic analysis was both enjoyable and practical, especially given how I use Wireshark at work. Setting up Wireshark, capturing network traffic, and analyzing protocols like FTP, ICMP, and SSH provided a solid understanding of network data flow. This experience reinforced my ability to differentiate between normal and suspicious traffic, which is essential in my role. At work, I rely on Wireshark to troubleshoot network issues, monitor data flow, and analyze anomalies, so this lab felt directly relevant to my daily responsibilities and aligned well with my real-world needs.

The lab was well-structured, with clear instructions that made each step smooth and straightforward. The range of tools and techniques included felt comprehensive, effectively simulating real-world scenarios and allowing for a thorough exploration of network analysis. If I were to suggest an improvement, I’d add more complex cases, like multi-stage attacks or advanced malicious traffic patterns. Or even reviewing a network that was impacted, and eventually shutdown, due to an attack. This would help deepen analytical skills, preparing us for situations where threats are subtler and harder to detect.

Overall, this lab was highly effective in reinforcing essential skills in packet analysis and traffic monitoring. It left me more confident in my ability to detect and investigate network activity, which is crucial for effective cybersecurity and network management.

# 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