**INCIDENT REPORT:** BN-18974-Intro-Wireshark

**Date:** 6/18/2024

**Executive Summary:** The objective of this task was to become familiar with Wireshark, a powerful network protocol analyzer, and apply it to analyze a PCAP file containing malicious traffic. This exercise simulated real-world incident response and threat analysis scenarios. Key takeaways included the ability to filter and analyze network traffic, identify indicators of compromise (IOCs) such as C2 traffic and file downloads, and understand the potential impact of malware infections.

**Application Details:**

* Wireshark: Version 4.2.5
* PCAP Source: "The PCAP file used for this analysis was obtained from Malware Traffic Analysis (<https://www.malware-traffic-analysis.net/>)."

**Attack Narrative:**

1. Extracting the PCAP file initially posed a challenge due to a misunderstanding regarding the password. However, with Frank's assistance, the correct password was obtained, and the file was successfully extracted.
2. Opened the PCAP file in Wireshark and conducted an initial overview of the traffic.
3. Identified the IP addresses of the compromised hosts using the "Endpoints" feature.
4. Filtered for suspicious traffic patterns (e.g., DNS queries to known malicious domains, unusual outbound connections) using Wireshark display filters.
5. Analyzed packet details (TCP/UDP headers, payload content) to identify specific malware indicators (e.g., C2 communication, file downloads).
6. Followed TCP streams to view conversations between the infected hosts and the C2 server.
7. Partially reconstructed a timeline of events based on packet timestamps, revealing some of the stages of the malware infection.

**Conclusion:**

This exercise demonstrated the importance of network traffic analysis in identifying and responding to security incidents. The ability to extract valuable information from PCAP files is crucial for threat intelligence, incident response, and forensic investigations. I plan to utilize Wireshark in my future work to investigate security incidents, perform threat hunting, and analyze network traffic for anomalies. Continued practice with Wireshark will further enhance my skills in this area.