Title: Incident Analysis Report - Shiba Insider Case

Analyst: [Arhaam Harris]
Date: [15-4-2025]
Platform: Blue Team Labs Online (BTLO)
Tools Used: Wireshark, Metadata2.com, Steghide Online

1. Overview

The objective of this investigation was to analyze a potential insider threat titled "Shiba Insider" hosted on BTLO. A network capture (PCAP) file and an image were provided as part of the challenge. The attacker had allegedly posted an image online with a hidden message. The task was to uncover the attacker's identity using open-source analysis tools.

2. Tools and Methodology

- **Wireshark:** Used to analyze the PCAP file and extract HTTP traffic.
- **Metadata2.com:** Online tool used to extract metadata from the image file.
- **Steghide Online:** Used to reveal hidden data embedded in the image via steganography.

3. Investigation Steps

Step 1: PCAP Analysis with Wireshark

- Loaded the PCAP file in Wireshark.
- Inspected HTTP requests and responses.

- Found an interesting HTTP request to:
  http://192.168.176.145:8099/hide.txt?message=how+do+i+open+file

- The response message was: use your own password\n

Step 2: Credential Discovery

- Identified HTTP POST traffic containing credentials:
  Username: fakeblue
  Password: redforever

Step 3: Image File Analysis

- Extracted metadata from the image using Metadata2.com.

- Found the following metadata value:
  ID: 0726ba878ea47de571777a

Step 4: Steganography Analysis

- Used Steghide Online to extract hidden information from the image using discovered credentials.

- Retrieved the same ID embedded inside the image.

Step 5: Attacker Profile Discovery

- Appended the ID to the BTLO user URL:

https://blueteamlabs.online/home/user/0726ba878ea47de571777a

- Profile name retrieved: **insider**

4. Key Findings

- The image contained a hidden ID value both in metadata and steganographically.
- The HTTP traffic revealed credentials used to access hidden content.
- Using the extracted ID, the attacker's profile was discovered on BTLO.

5. Conclusion

The attacker used both metadata and steganography to hide identifying information within an image. By thoroughly analyzing the network traffic and the image file, the insider was successfully identified as "**insider**" on BTLO.

6. Recommendations

- Train users to recognize and report phishing emails and suspicious image files.
- Monitor HTTP traffic for anomalies like hidden query parameters.
- Regularly scan metadata and hidden content in media files shared within the organization.

End of Report