Research Report 2 Wireshark

## What did you do:

To begin this assignment, I followed the proper protocols within my organization and obtained permission to use Wireshark for network analysis. With approval in hand, I proceeded to install Wireshark on my computer. The installation process was straightforward, and once the software was up and running, I began my exploration.

I started by selecting the network interface through which I wanted to capture packets. Wireshark allows users to choose from available network adapters to monitor specific network traffic. After selecting the appropriate interface, I initiated the packet capture and let it run for five minutes. During this capture period, Wireshark displayed real-time information about the identified networks and protocols as data packets traversed the network.

Wireshark's user-friendly interface made it easy to analyze the output. Each captured packet was listed in a comprehensive packet list, and selecting a packet provided detailed information in various sections of the user interface. The packet details included source and destination IP addresses, protocol type, packet size, timestamp, and payload data.

## What are the results:

Upon analyzing the results, I found that my organization's network primarily used common and expected protocols. HTTP was used for web traffic, DNS for domain name resolution, and TCP and UDP for general data transfer. The presence of these standard protocols indicated normal network communication between devices.

During the packet capture, I did not come across any immediate indications of cyber attacks. The captured packets showed typical patterns of communication between authorized devices and servers. However, the absence of immediate signs of attacks does not guarantee absolute security. Attackers can be stealthy, and their activities might not always be apparent in a short packet capture.

While analyzing the attack surface presented by the network and packets, a few potential vulnerabilities caught my attention. For instance, some devices were communicating over HTTP instead of the more secure HTTPS for web traffic. This could expose sensitive data to potential eavesdropping or man-in-the-middle attacks. Furthermore, I noticed that some devices were using older versions of certain protocols, which might have known security issues. Addressing these vulnerabilities should be a priority to enhance the network's security posture.

## What did you learn:

This assignment provided valuable insights into various aspects of digital networks, packets, and the attack surface:

Network Identification: Wireshark's ability to identify and interpret different network protocols was eye-opening. It allowed me to see the diversity of protocols in use within my organization's network, highlighting the complexity of modern network infrastructures.

Packet Capturing: Capturing and analyzing packets offered a deep understanding of network activities. It is a powerful tool for troubleshooting network issues and diagnosing performance problems. In the context of security, packet capturing is a crucial aspect of network monitoring to identify and respond to potential security incidents.

Cybersecurity Attacks: While the current packet capture did not reveal any cyber attacks, it reinforced the importance of continuous monitoring and analysis of network traffic. Cyber attackers constantly evolve their tactics, techniques, and procedures, so regular network analysis is essential to detect and mitigate emerging threats.

Attack Surface: Analyzing the attack surface is a vital aspect of cybersecurity risk management. Identifying potential vulnerabilities allows organizations to take proactive measures to secure their systems and data.

Importance of Secure Protocols: The use of secure protocols, such as HTTPS, is critical to protect sensitive data from interception and unauthorized access. Encouraging the adoption of secure protocols within the organization is essential for maintaining a robust security posture.

In the future, I plan to conduct more extensive network analysis using Wireshark, including deep dives into specific network segments and conducting forensic analyses in the event of a suspected security incident. By gaining expertise in network analysis, I aim to contribute to my organization's efforts in maintaining a secure and resilient network infrastructure.

The knowledge gained from this assignment can be of significant value to the organization in various ways. Understanding the network's attack surface allows the organization to prioritize security measures and allocate resources effectively. Regular network analysis enables the early detection of potential threats, helping to prevent data breaches and other security incidents. Additionally, the insights gained from packet analysis can contribute to improving the organization's network performance and optimizing resource utilization.