*Mi*nistry of Higher Education and
Scientific Research, Iraq
University of Babylon
information technology collage
Information Security Department
Study: Morning

Secure network troubleshooting analyzer using Wireshark

A Graduate Project Submitted to the department of Information Security of the College of Information Technology, University of Babylon, in Partial Fulfillment of the Requirements for the Bachelor's degree in the Information Security of Information Technology.

By

Ayat Mohammed Jasem

Supervised by

Assist. Lect. Ameer Sameer Hamood

2023-2024

Abstract

Creating a secure network troubleshooting analyzer using Wireshark involves several key steps:

1.Define Scope: Determine the specific objectives of your analyzer. What types of issues are you aiming to troubleshoot?

2.Setup Environment: Establish a controlled network environment where you can capture traffic safely. Ensure that you have necessary permissions to capture traffic, especially if you're monitoring a production network.

3.Install Wireshark: Download and install Wireshark on your monitoring machine. Ensure that it's the latest version.

4.Capture Traffic: Start capturing network traffic using Wireshark.

5.Analyze Traffic: Use Wireshark's powerful analysis tools to examine captured packets. Look for anomalies, patterns, and potential issues such as excessive bandwidth usage, suspicious protocols, or unusual traffic patterns.

6.Implement Filters: Set up filters within Wireshark to narrow down your analysis and focus on relevant packets.

7.Interpret Results: Interpret the findings from your analysis, Identify any deviations or abnormalities that may indicate problems.

8.Troubleshoot Issues: Once you've identified potential issues, delve deeper into troubleshooting.

9.Document Findings: Document your analysis process, findings, and resolutions.

10.Enhance Security: Ensure analyzer itself is secure. Protect captured data, restrict access to sensitive information.

By following these steps, you can develop a secure network troubleshooting analyzer using Wireshark that helps you diagnose and resolve network issues effectively while maintaining the integrity and security of your network infrastructure.