Final Project: Section 1: Capturing, Analyzing, and Responding to Network Traffic

Network Traffic Exploration with Wireshark

Estimated time needed: 30 minutes

Welcome to section 1 of the final project for this course. Assuming the role of a network analyst, you are tasked with capturing and analyzing real-time traffic. You'll use Wireshark to conduct live packet captures, apply filters, and work with specific network protocols to understand traffic flows and data analysis.

Learning objectives

By the end of this project, you will be able to:

- Conduct live network traffic captures using Wireshark
- Apply and remove display filters to isolate specific types of traffic (e.g., DNS)
- Analyze protocol-level data using Wireshark's Protocol Hierarchy and Conversations statistics
- Interpret traffic flows and communication patterns from capture files
- Save, document, and present traffic analysis results clearly using screenshots and proper file formats

Prerequisites

- Pre-installed Kali Linux Virtual Machine (VM) with Wireshark

Tasks and steps to complete the project

Task 1: Capture live network traffic

Steps:

1. Open Wireshark and start a live packet capture
2. While capturing, visit the following websites in your browser:
    - https://www.kali.org/
    - https://www.redhat.com/en
3. Take a screenshot of the live packet capture in progress
4. Stop the live capture
5. Save the capture file to your VM Desktop in ".pcapng" format
    - Name the file: Packet capture.pcapng

Task 2: Save captured traffic file

Steps:

1. Take a screenshot showing the saved ".pcapng" file on your VM Desktop
2. Save the screenshot as "Desktop.png/jpg"

Task 3: Filter DNS Traffic

Steps:

1. In Wireshark, apply a display filter for DNS traffic: dns
2. Take a screenshot of the filtered DNS traffic
3. Save the screenshot as "Filtered DNS traffic.png/jpg"
4. Clear the DNS filter from the display

Task 4: Analyze Protocol Hierarchy

Steps:

1. Open the Protocol Hierarchy Statistics report in Wireshark
2. Filter the results by Percent Packets (highest to lowest)
3. Take a screenshot of the filtered results
4. Save the screenshot as "Protocol Hierarchy Statistics results.png/jpg"

Task 5: Review Conversation Statistics

Steps:

1. Open the Conversations Statistics report in Wireshark
2. Filter the report by Bytes (highest to lowest)
3. Take a screenshot of the filtered Conversation Statistics report
4. Save the screenshot as "Conversation Statistics report.png/jpg"

Grading criteria and deliverables

Ensure that all five screenshots are captured in high resolution, with all details clearly visible. Each screenshot must be correctly named and saved in the required format. Though this is a practice project, your submissions must meet the specified criteria for full credit.

Task 1: Capture live network traffic (2 points)

- **Requirement:** Screenshot of the live packet capture in progress
- **File name and format:** Packet capture.pcapng

Task 2: Save captured traffic file (2 points)

- **Requirement:** Screenshot showing the saved .pcapng file on your VM Desktop
- **File name and format:** Desktop.png/jpg

Task 3: Filter DNS traffic (2 points)

- **Requirement:** Screenshot of the filtered DNS traffic

- **File name and format:** Filtered DNS traffic.png/jpg

Task 4: Analyze Protocol Hierarchy Statistics (2 points)

- **Requirement:** Screenshot of the filtered Protocol Hierarchy Statistics results
- **File name and format:** Protocol Hierarchy Statistics results.png/jpg

Task 5: Review Conversation Statistics Report (2 points)

- **Requirement:** Screenshot of the filtered Conversation Statistics report
- **File name and format:** Conversation Statistics report.png/jpg

Total: 10 points