Packet Capture Objectives and Analysis

Project Overview:

In this project, you will work with a specific packet capture file (.pcap format) to answer a set of predefined objectives. By addressing these objectives, you will gain a deeper understanding of the packet capture, identify any actions or issues present in the network traffic, and provide a summary analysis along with security recommendations.

This project aims to enhance your analytical skills in packet analysis, allowing you to effectively diagnose network problems or security concerns.

Project Submission:

Your project will be due on 1/15/2025. Students will have a week to complete the project. The submission should include two separate documents (.pdf or .docx):

1. A filled-out objectives document addressing the specific objectives related to the packet capture.
2. A detailed report documenting your analysis process, the objectives addressed, the issues identified, and recommendations for improving network security.

Project Objectives:

1. Analyze the provided packet capture file to gain insights into network traffic.
2. Address a list of specific objectives related to the packet capture.
3. Propose actionable next steps to improve network security and performance.
4. Document the analysis process for future reference and reproducibility.

Project Tasks:

1. **Select a Packet Capture File:**
    a. Load the provided .pcap packet capture file into Wireshark to begin your analysis.
2. **Analyze Network Traffic:**
    a. **Answer Objectives:** Address the list of given objectives related to the packet capture. This may include identifying specific traffic patterns, analyzing protocols in use, and recognizing any anomalies.
    b. **Inspect Packets:** Examine the packet details to identify abnormal traffic patterns, such as unusual protocols, unrecognized IPs, or suspicious payloads.
    c. **Track Connections:** Follow specific TCP or UDP streams to understand communication between endpoints.
    d. **Detect Anomalies:** Look for signs of potential security issues (e.g., red or black color labeled packets, unauthorized access attempts, or data exfiltration) or performance problems (e.g., excessive retransmissions, slow response times, or high latency).
3. **Identify and Assess Issues:**
    a. **Security Concerns:** Identify any vulnerabilities or threats, such as unencrypted traffic, potential intrusions, or denial-of-service attempts.
    b. **Performance Issues:** Determine if there are any performance-related problems like excessive packet loss, jitter, or network congestion.
    c. **Misconfigurations:** Detect any network misconfigurations such as incorrect IP assignments, routing problems, or improper use of protocols.
4. **Summary Analysis and Recommendations:**
    a. Based on your analysis and the objectives addressed, provide a summary analysis of the packet capture. This should include:

- A brief overview of the findings from the packet capture analysis.
- Identification of any security vulnerabilities or performance issues discovered.
- A set of actionable recommendations to enhance security or resolve performance issues, such as:
    - Implementing encryption
    - Reconfiguring network devices
    - Upgrading network infrastructure or protocols
    - Monitoring and logging suspicious traffic

5. **Documentation and Justification:**
    a. **Write a Report:** Provide a detailed report explaining your analysis process, including the filters and techniques used in Wireshark, the issues or anomalies you identified, and your recommendations.
        i. **Introduction:** Give a brief overview of the packet capture scenario and the objectives of your analysis.
        ii. **Packet Analysis Process:** Document the step-by-step process of your investigation, explaining the filters you applied and how you examined the traffic.
        iii. **Issues and Findings:** Describe the specific issues you identified, such as security vulnerabilities, performance problems, or misconfigurations.
        iv. **Next Steps and Recommendations:** Propose your recommendations for improving security, performance, or resolving the identified issues, and explain why these changes are necessary.
        v. **Conclusion:** Summarize the key takeaways from your analysis and any final thoughts or recommendations for ongoing network monitoring.

Items for Submission:

1. **Completed Objectives:** A filled-out objectives document addressing the specific objectives related to the packet capture.
2. **Analysis Report:** A detailed report documenting your analysis process, the objectives addressed, the issues identified, and recommendations for improving network security.

Rubric:

If you do not score a 10 or higher for your project based on the rubric below you will have the opportunity to make changes to your project and resubmit it.

	0 Points - Missing	1 Point - Does Not Meet Expectations	2 Points - Meets Expectations	3 Points - Exceeds Expectations	Points Awarded
Completion of Objectives	No objective document was submitted.	Some objectives completed, but many remain unexplored.	All objectives attempted and most completed correctly.	All objectives completed correctly and thorough exploration of the packet capture.	
Packet Analysis	No filtering or analysis performed.	Basic filtering/analysis performed, but incomplete.	Correct filters and techniques used to find issues.	Advanced filtering and in-depth analysis of packet data.	
Understanding of Network Protocols	No protocol analysis or explanation provided.	Some protocols mentioned, but incomplete or inaccurate explanation.	Correct identification and basic explanation of key protocols.	Advanced understanding and detailed explanation of all relevant protocols in context.	

Recommendations	No recommendations provided.	Recommendations are incomplete or irrelevant.	Recommendations address most issues.	Detailed and actionable recommendations with strong justification.	
Documentation	No report or documentation provided.	Incomplete documentation with missing key details.	Clear documentation of the analysis process and findings.	Well-organized, detailed documentation with comprehensive analysis.	
				Score	