### Network Traffic Analysis Using Wireshark and Zeek

**Project Title:** Network Traffic Analysis Using Wireshark and Zeek  
**Name:** Piyush Rai  
**Institution:** KCC institute technology and management   
**Course Name:** cyber security   
**Date:** 17 july  
**Supervisor's Name:** Hrushikesh Dinkar

#### Abstract

This project focuses on analyzing network traffic using two powerful tools: Wireshark and Zeek. The primary goal is to detect suspicious activities, protocol anomalies, and potential intrusions within a controlled lab environment. Wireshark provides packet-level inspection, while Zeek offers higher-level insights through log-based monitoring. By capturing and analyzing traffic, this project identifies unusual communication patterns and highlights how network-based threats can be detected. The findings demonstrate how these tools can complement each other in real-world network defense scenarios.

#### Table of Contents

1. Title Page
2. Abstract
3. Table of Contents
4. List of Figures and Tables
5. Introduction
6. Literature Review
7. Methodology/Approach
8. Results and Discussion
9. Conclusion
10. Recommendations
11. References
12. Appendices (If applicable)

#### List of Figures and Tables

* Figure 1: Wireshark Packet Capture Snapshot

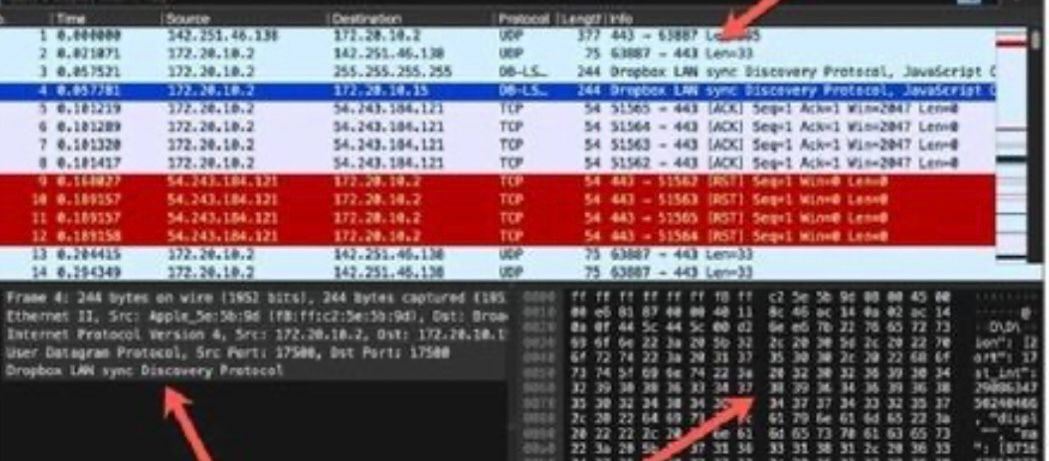
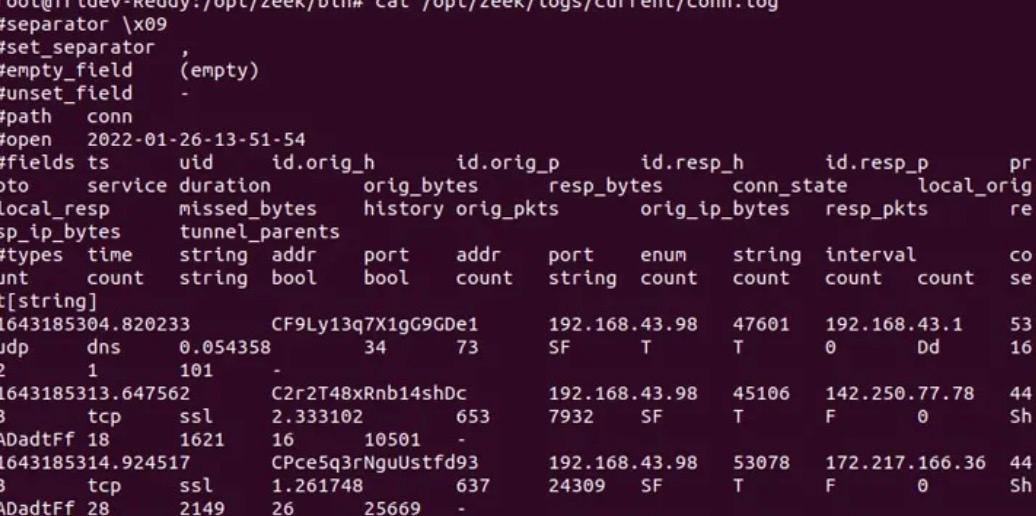


Figure 2: Zeek Log Analysis Sample



#### Introduction

This project involves analyzing network traffic to identify threats using Wireshark and Zeek. In today's cybersecurity landscape, monitoring network activity is critical for detecting intrusions and anomalies. This project simulates a controlled lab network to capture traffic and analyze it using both tools. Wireshark is used for packet-level detail, while Zeek helps in protocol and behavior-based analysis.

#### Literature Review

Wireshark is a well-known open-source network protocol analyzer. It allows deep inspection of hundreds of protocols and is commonly used for troubleshooting and security analysis. Zeek (formerly Bro) operates at a higher level, parsing traffic into structured logs which can be used for detecting threats, policy violations, and more.

#### Methodology/Approach

**Approach:**  
To analyze network traffic in a lab environment, traffic was captured during simulated user activity. Suspicious traffic patterns such as port scans, DNS tunneling, and malformed packets were observed.

**Tools and Technologies:**

* **Wireshark:** For packet-level traffic capture and visualization.
* **Zeek:** For log generation, behavior analysis, and detecting suspicious patterns.

**Step-by-Step Process:**

1. Set up a virtual lab using Kali Linux and a vulnerable machine (e.g., Metasploitable).
2. Use Wireshark to capture live traffic during different types of simulated attacks.
3. Deploy Zeek to analyze the same traffic and generate logs.
4. Examine logs like conn.log, http.log, and dns.log for anomalies.
5. Compare findings from both tools.

#### Results and Discussion

**Results:**

* Wireshark identified ARP scanning and unusual HTTP requests.
* Zeek flagged anomalies such as repeated failed login attempts and unusual DNS queries.
* Both tools confirmed SYN flood patterns.

**Discussion:**  
Wireshark was effective in visually inspecting traffic patterns, but Zeek's logs made it easier to identify behavioral patterns over time. Zeek provided a higher-level summary that helped correlate events quickly. Wireshark was better for low-level protocol inspection.

**Challenges:**

* Filtering relevant data from large PCAP files.
* Understanding Zeek scripting for customized analysis.
* Synchronizing timestamps between Zeek and Wireshark captures.

#### Conclusion

This project successfully demonstrated how Wireshark and Zeek can be used together to identify network anomalies and potential threats. While Wireshark excels in packet-level inspection, Zeek offers powerful behavior-based insights. Combining both provides a comprehensive view of network activity and helps in faster threat detection and response.

Recommendations

* Use Zeek alongside SIEMs for better real-time analytics.
* Train security teams on log interpretation to improve threat detection.
* Regularly update and customize Zeek scripts for your network environment.

#### References

* Wireshark Official Documentation: https://www.wireshark.org/docs/
* Zeek Official Site: https://zeek.org/
* Packet Analysis with Wireshark by Chris Sanders

Appendices

* Sample conn.log and http.log outputs
* Sample PCAP file (if shareable)