Network Traffic Analysis using Wireshark and Zeek

Name: CHITRANSH TRIPATHI

Institution/Organization Name:

UNITED COLLEGE OF ENGINEERING AND RESEARCH

Course Name: CYBERSECURITY

Date: 28-07-2025

Supervisor's Name: MR. NIKHIL PANDEY

Abstract

This project explores the use of Wireshark and Zeek for network traffic analysis to identify suspicious activities, performance issues, and general behavior of network systems. Wireshark is a packet-level analyzer that provides real-time traffic capture and deep inspection, while Zeek offers high-level network event monitoring and logging. The integration of both tools creates a powerful system for understanding network communications in detail. The project focuses on capturing network data, analyzing it for anomalies, and interpreting logs to gain insights into traffic behavior. Key results include the detection of scanning attempts, irregular DNS queries, and identification of unencrypted sensitive data. Challenges faced included handling vast volumes of data and distinguishing between legitimate and suspicious traffic patterns.

Table of Contents

Introduction

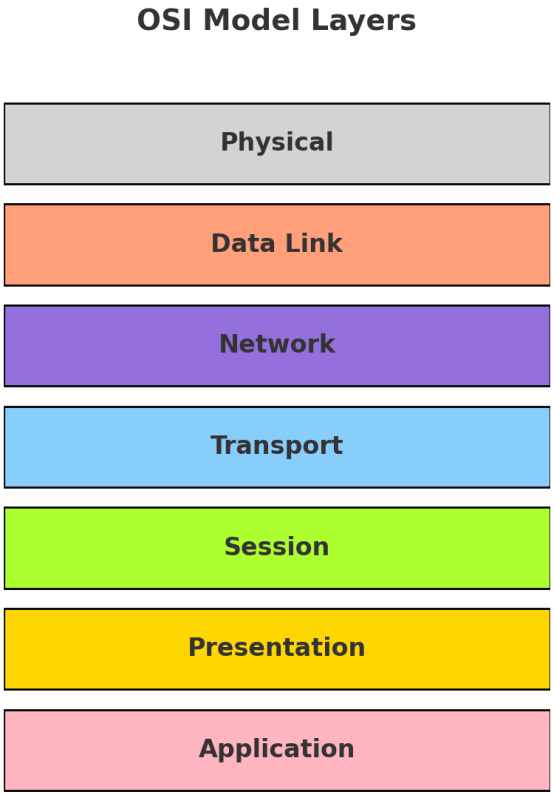


Figure 1: Colorful OSI Model Diagram

With the rise in cyber threats and increasingly complex IT infrastructures, understanding network traffic has become critical for cybersecurity. This project focuses on analyzing network traffic using Wireshark and Zeek, two of the most widely used open-source tools in the field. Wireshark provides low-level visibility by capturing individual packets, while Zeek offers

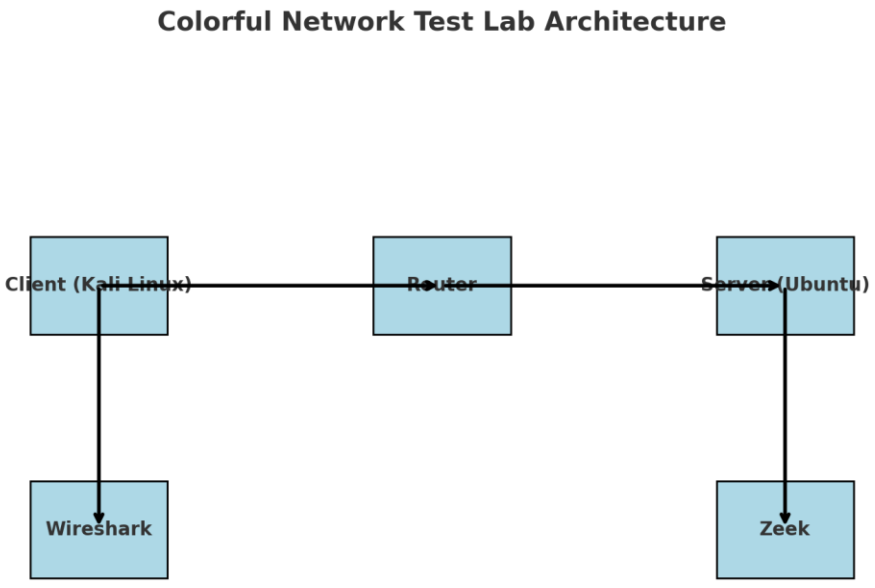
an abstracted, log-based view of traffic, enabling behavioral analysis. The primary goal is to gain insights into what happens over a network, detect threats, and better understand typical versus atypical traffic patterns. The tools used are capable of identifying intrusions, scanning behavior, data leaks, and misconfigurations, making them essential for network security monitoring and incident response.

Wireshark vs Zeek Feature Comparison

- Packet vs Log-Based
- Real-Time vs Scripting
- Forensics vs Monitoring

Figure 2: Wireshark vs Zeek Feature Comparison

Figure 3: Colorful Network Test Lab Architecture



Literature Review

Wireshark is one of the most popular packet sniffers available and is often used in educational and professional environments. It provides in-depth visibility into each frame of communication between systems. Studies have shown its effectiveness in detecting anomalies such as packet flooding, malformed packets, and protocol violations.

Zeek, formerly known as Bro, is a powerful network analysis framework used by researchers and security professionals. It differs from Wireshark in that it logs metadata about traffic instead of capturing raw packets. Zeek scripts can be used to detect suspicious behaviors, including brute-force attacks, command and control channels, and data exfiltration. Research has demonstrated Zeek's utility in real-time network monitoring and intrusion detection systems (IDS). By using Wireshark and Zeek together, analysts gain a comprehensive view of both micro-level packet data and macro-level behavioral data.

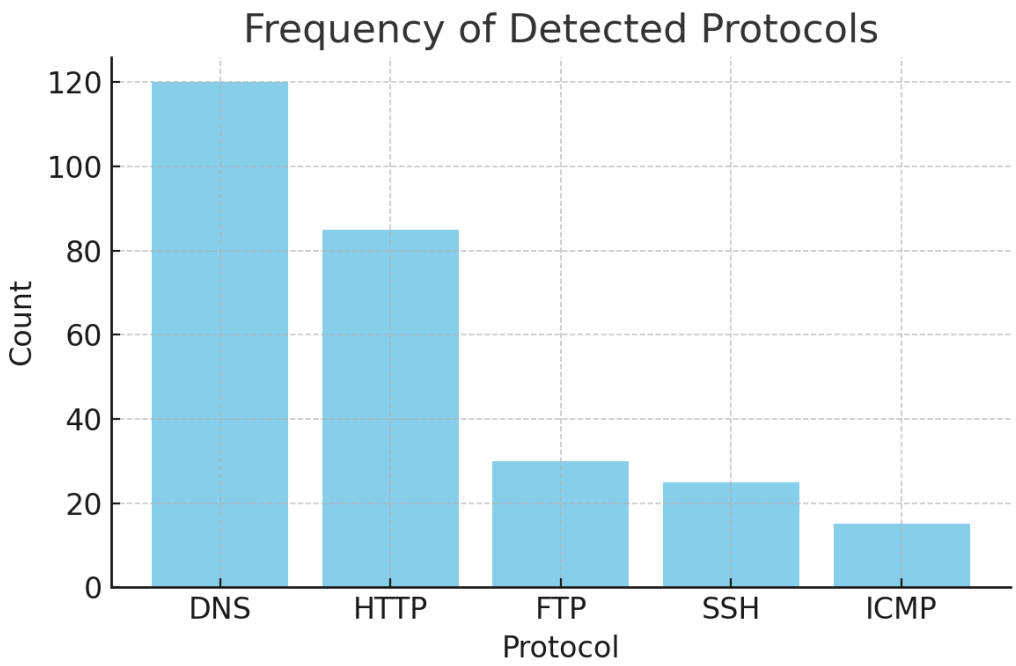


Figure 4: Frequency of Detected Protocols

Methodology/Approach

Figure 5: Colorful Infographic - Wireshark + Zeek Combined Analysis

Results and Discussion

Zeek conn.log View

ts	uid	id.orig_h	id.resp_h	proto	service	duration
1723430400.123	C123abc	192.168.1.2	10.0.0.1	tcp	ssh	2.3
1723430401.456	C124abc	192.168.1.2	8.8.8.8	udp	dns	0.01

Figure 6: Simulated Zeek conn.log Output

Wireshark Packet View

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000	192.168.1.2	93.184.216.34	HTTP	546	GET /index.html
2	0.003	93.184.216.34	192.168.1.2	HTTP	720	200 OK
3	0.009	192.168.1.2	192.168.1.1	DNS	80	Standard query A example.com

Figure 5: Simulated Wireshark Packet Capture View

The experiment produced a variety of results through real-time packet inspection and log analysis:

Results:
- DNS queries were observed, including legitimate and potentially suspicious domains.
- Detected TCP port scans initiated from one machine to multiple others.
- HTTP requests were logged, including URLs and user agents.
- Detected unencrypted credentials in FTP sessions.

Discussion:
The layered approach of using both tools helped validate

observations. For instance, Wireshark revealed actual packet contents, while Zeek's logs showed the behavior of connections over time. One key observation was the ease of identifying brute-force SSH attempts using Zeek's 'conn.log' and 'ssh.log' files. Anomalies were correlated between tools for cross-verification. However, a major challenge was filtering out irrelevant data. Real networks generate huge volumes of traffic, and focusing on significant events required tuning filters and scripts. Interpreting log files also required familiarity with Zeek's format and context.

Conclusion

The project successfully demonstrated how Wireshark and Zeek can be used to analyze network traffic for security and monitoring purposes. Both tools bring unique strengths—Wireshark excels in micro-level, packet-by-packet analysis, while Zeek offers scalable event-driven monitoring. Together, they provide a holistic view of a network's state. Through various experiments, the project identified multiple indicators of compromise and abnormal patterns, highlighting the importance of proactive traffic monitoring. The exercise enhanced the understanding of protocols, attack signatures, and network forensics. Future work could explore automated alerting, machine learning for anomaly detection, or integrating outputs into a SIEM system.

Recommendations

- Use Wireshark during forensic analysis when deep packet inspection is required.
- Deploy Zeek in enterprise environments for passive logging and long-term trend analysis.
- Create automated filters in Zeek to trigger alerts for high-risk behaviors (e.g., port scans, excessive DNS lookups).
- Consider combining the tools with other SIEM systems like Splunk or ELK Stack to enhance security monitoring capabilities.

References

[1] Wireshark Official Documentation: https://www.wireshark.org/docs/
[2] Zeek Network Security Monitor: https://docs.zeek.org/en/current/
[3] Richard Bejtlich, “The Practice of Network Security Monitoring”, No Starch Press, 2013.
[4] Paxson, Vern. “Bro: A System for Detecting Network Intruders in Real-Time.” 1999.

Appendices

Appendix A: Sample Zeek Logs
- conn.log
- dns.log
- http.log

Appendix B: Screenshots of Wireshark Captures
- TCP three-way handshake
- FTP credential capture
- HTTP GET request analysis