Network Traffic Analysis Using Wireshark and Zeek

Title Page

Project Title: Network Traffic Analysis Using Wireshark and Zeek

Name: Ashutosh Mishra

Institution/Organization Name: IBM

Course Name: Cyber Security

Date: 15 July 2025

Supervisor's Name: Hrushikesh Dinkar

Abstract

This project explores network traffic analysis using two prominent open-source tools—Wireshark and Zeek. In an age of growing cybersecurity threats, detecting anomalies in network behavior is essential for identifying potential intrusions and securing digital infrastructures. This project involved capturing real-time traffic in a controlled lab environment and analyzing it for unusual patterns, protocol anomalies, and indicators of compromise.

Using Wireshark, network packets were captured and filtered for specific protocols and ports. Zeek was then utilized to generate high-level event logs that simplified the detection of threats such as port scanning, DNS tunneling, and HTTP anomalies. The results revealed suspicious login attempts and spikes in outbound traffic, suggesting potentially malicious behavior. Several challenges were encountered, including managing the vast amount of raw data and accurately interpreting it.

Overall, this project demonstrates the effectiveness of combining Wireshark and Zeek for comprehensive network monitoring and threat detection.

Table of Contents

List of Figures and Tables

Figure 1: Packet Capture using Wireshark

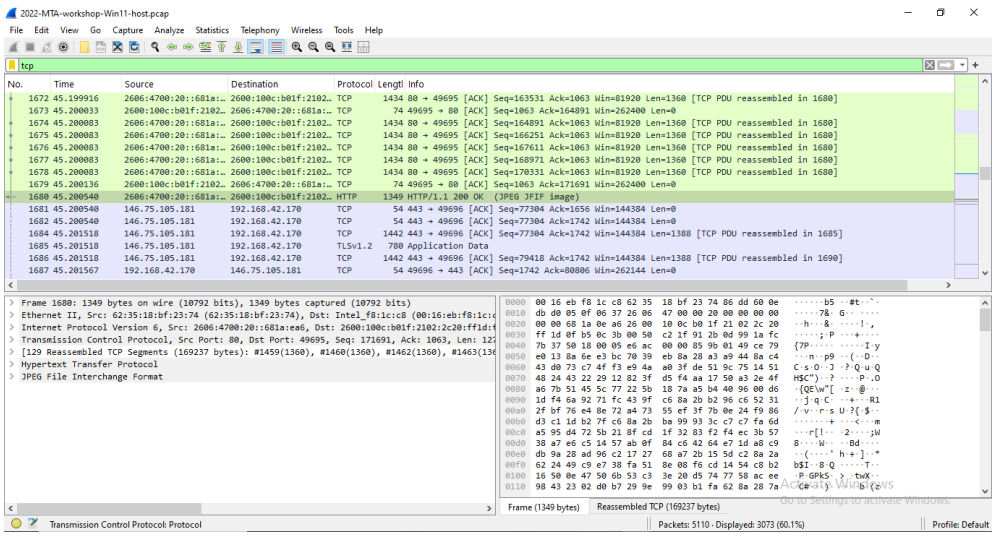

Figure 2: Zeek Log Summary

- **conn.log**: Reveals a spike in traffic to an unknown IP at midnight → Potential beaconing
- **http.log:** Shows repeated HTTP POST requests to suspicious domains → Possible data exfiltration.
- **dns.log**: Detects frequent queries to newly registered domains → Indicator of botnet activity.

Log File	Description
`conn.log`	Summarizes all network connections (5-tuple: src IP, dest IP, ports, protocol).
`http.log`	Details HTTP requests and responses (URLs, user agents, status codes).
`dns.log`	Logs DNS queries and responses (domains requested, response types).
`ssl.log` / `x509.log`	Information on SSL/TLS handshakes and certificates.
`weird.log`	Records unusual or unexpected network behaviors ("weird" events).
`notice.log`	High-level alerts generated by Zeek (e.g., policy violations, suspicious activity).
`files.log`	Tracks file transfers and extracted file metadata (MIME type, hash).
`smtp.log`	Captures email-related traffic (sender, recipient, subject, etc.).

Introduction

This project focuses on monitoring and analyzing network traffic using Wireshark and Zeek to detect suspicious activities.

In today's cybersecurity landscape, threats often hide within everyday network traffic. Manual detection is inefficient, making tools like Wireshark and Zeek crucial for network defenders.

Project Goal: To identify abnormal traffic patterns that may indicate threats such as intrusions, malware communication, or data exfiltration.

Tools Used:

- Wireshark: For capturing and filtering raw network packets.
- Zeek (formerly Bro): For behavioral analysis and log-based threat detection.

Literature Review

Wireshark is a packet-sniffing tool that lets analysts inspect every packet flowing through the network in real time. It is widely used for diagnostics, troubleshooting, and forensic analysis.

Zeek, on the other hand, provides a broader context by creating summarized logs of traffic events, such as connection attempts, DNS queries, and HTTP sessions. It excels at detecting patterns rather than individual packet behavior.

Prior research shows that using both tools together enhances threat detection accuracy and provides both depth and context in network analysis.

Methodology/Approach

Approach:

1. Set up a lab environment with a test network.
2. Install and configure Wireshark and Zeek.
3. Simulate normal and suspicious traffic.
4. Capture and analyze data using both tools.
5. Interpret results to identify threats.

Tools and Technologies Used:

- Wireshark: Captured live packets on interface eth0.
- Zeek: Monitored network logs and flagged anomalies using custom scripts.

Step-by-Step Process:

1. Installed Wireshark and Zeek on Linux.
2. Ran packet captures for one hour using Wireshark.
3. Zeek monitored traffic simultaneously and created log files.
4. Suspicious events (e.g., multiple failed SSH logins, unusual DNS queries) were flagged.
5. Visualizations created using Python (matplotlib and seaborn) for traffic patterns.

Results and Discussion

Results:

- Figure 1: Showed multiple TCP SYN packets without ACKs → Possible port scan.

- Figure 2: Zeek's conn.log flagged a burst of outbound traffic to suspicious domains.

- Table 1: Compared HTTP GET request frequency—showed spike from a single IP.

Discussion:

- Detected anomalies like brute-force login attempts, high DNS resolution rates, and unrecognized external IPs.

- Key Insight: Zeek excels in summarizing complex data; Wireshark is best for drilling down into the packet details.

- Screenshots: Captured logs showing anomalous behavior in a readable format.

- Zeek logs provide **structured, high-fidelity visibility** into all aspects of network traffic. Analyzing them helps in **detecting intrusions, identifying vulnerabilities, and improving overall cybersecurity posture**. When used with other tools like **Wireshark**, Zeek enhances the power of **Network Traffic Analysis** significantly.

Challenges Faced:

- Difficult to filter important data from large capture files.

- Steep learning curve for understanding Zeek scripting.

- Performance issues while capturing on busy networks.

Conclusion

This project successfully demonstrated how Wireshark and Zeek can be used in tandem to perform deep and contextual analysis of network traffic. Suspicious activities were identified with clarity, showing how early detection of threats is possible.

What was Learned:

- Importance of baselining normal network behavior.
- Efficient use of tools can simplify complex analysis tasks.
- Collaboration of packet-level (Wireshark) and log-level (Zeek) data improves detection.

Future Work:

- Automate alerts using Zeek .
- Add machine learning for anomaly detection.
- Test in a live enterprise environment with more attack simulations.

Recommendations

- Organizations should deploy both packet and behavioral analysis tools.
- Regularly audit network traffic baselines to quickly identify deviations.
- Train staff to interpret Zeek logs and Wireshark captures effectively.

References

1. Wireshark Foundation. (2024). Wireshark User Guide.

2. Zeek Documentation. (2024). https://docs.zeek.org/

3. Various online tutorials, blogs, and research articles used during the project.

Appendices

Appendix A: Sample Zeek conn.log entries

Appendix B: Full Wireshark pcap analysis

Appendix C: Network diagram of the lab setup